DUMITRU BUŞNEAG
(COORDONATOR)

FLORENTINA BOBOC DANA PICIU

ARITMETICĂ
şi
TEORIA NUMERELOR

EDITURA UNIVERSITARIA

CRAIOVA
1999

Referenți științifici : **Prof. univ. dr. Alexandru Dincă** – Universitatea din Craiova.
Prof. univ. dr. François Gramain – Université Jean Monnnet, Saint -Étienne, France.

Dumitru Busneag, Florentina Boboc, Dana Piciu:
Arithmetic and number theory

Tehnoredactare computerizată: Florentina Boboc, Dana Piciu
Bun de tipar: 11.05.1999
Tipografia Universității din Craiova
Str. Al. I. Cuza
Craiova, România.

Published in Romania by EDITURA UNIVERSITARIA CRAIOVA

ISBN: 973 – 9271 – 73 - 1

CUVÂNT ÎNAINTE

Această lucrare este o ediție revizuită şi îmbunătățită a lucrării **Elemente de aritmetică şi teoria numerelor**, având aceiaşi autori, şi care a fost publicată în anul 1998, la editura Radical din Craiova (I.S.B.N. 973-9253-52-0).

Față de vechea ediție, pe lângă îndreptarea unor mici erori (atât de redactare cât şi de tehnoredactare), am adus îmbunătățiri paragrafelor 4 şi 7 de la Capitolul 7, ca şi paragrafului 3 de la Capitolul 11.

În finalul Capitolului 12 am introdus un nou paragraf (paragraful 6) în care se prezintă rezolvarea în numere întregi a sistemelor de ecuații liniare cu coeficienți întregi.

Pentru fiecare capitol s-au introdus exerciții suplimentare cu soluții complete.

În finalul lucrării s-au ataşat următoarele anexe:

Anexa 1: Tabelul cu numerele prime (evidențiind numerele prime gemene) de la 1 la 10.000.

Anexa 2: Funcția $\pi(x)$ şi estimările sale.

Anexa 3: Numerele lui Fermat, numerele lui Mersenne şi numere perfecte.

Dacă lucrarea inițială avea 254 pagini format A_5 , prezenta ediție are 288 pagini (acelaşi format).

Craiova, 20 aprilie 1999. Autorii.

L. Kronecker : Dumnezeu a creat numerele naturale – restul este munca omului .

CAPITOLUL 1 :
MULŢIMEA NUMERELOR NATURALE $\mathbb{N}$.

§ 1 Triplete Peano

DEFINIŢIA 1.1. **Numim triplet Peano un triplet (N, 0, s) unde N este o mulţime nevidă, $0 \in N$ iar $s:N \to N$ este o funcţie astfel încât sunt verificate axiomele :**

P_1 : $0 \notin s(N)$
P_2 : s este o funcţie injectivă
P_3 : dacă $P \subseteq N$ este o submulţime astfel încât $0 \in P$ şi $(n \in P \Rightarrow s(n) \in P)$, atunci $P=N$.

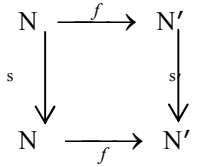
În cele ce urmează, acceptăm ca axiomă existenţa unui triplet Peano (cititorului dornic de aprofundarea acestei chestiuni îi recomandăm lucrările [7] şi [19]) .

LEMA 1.2. **Dacă (N, 0, s) este un triplet Peano, atunci $N=\{0\} \cup s(N)$.**

Demonstraţie Dacă notăm $P=\{0\} \cup s(N)$, atunci $P \subseteq N$ şi cum P verifică P_3, deducem că $P=N$.■

TEOREMA 1.3. **Fie (N, 0, s) un triplet Peano iar (N′, 0′, s ′) un alt triplet format dintr-o mulţime nevidă N′, un element $0' \in N'$ şi o funcţie $s':N' \to N'$. Atunci :**

1) Există o unică funcţie $f:N \to N'$ astfel încât $f(0)= 0'$, iar diagrama



este comutativă (adică $f \circ s = s' \circ f$) .

2) Dacă (N′, 0′, s′) este un triplet Peano, atunci f este bijecție.

Demonstrație 1) Pentru a proba existența lui f, vom considera toate relațiile $R \subseteq N \times N'$ a.î. :

$r_1 : (0, 0') \in R$

r_2 : Dacă $(n, n') \in R$, atunci $(s(n), s'(n')) \in R$ iar prin R_0 vom nota intersecția acestor relații .

Vom demonstra că R_0 este o relație funcțională şi astfel f va fi funcția ce va avea drept grafic pe R_0 (astfel, din $(0, 0') \in R_0$ vom deduce că $f(0)=0'$ iar dacă $n \in N$ şi $f(n)=n' \in N'$, $(n , n') \in R_0$, deci $(s(n), s'(n')) \in R_0$, adică, $f(s(n))=s'(n')=s'(f(n))$.

Pentru a demonstra că R_0 este o relație funcțională, vom demonstra că pentru orice $n \in N$, există $n' \in N'$ a. î. $(n, n') \in R_0$ iar dacă pentru $n \in N$ şi n', $n'' \in N'$ avem $(n, n') \in R_0$ şi $(n, n'') \in R_0$, atunci $n' = n''$.

Pentru prima parte, fie $P=\{n \in N$: există $n' \in N'$ a. î. $(n, n') \in R_0\} \subseteq N$. Cum $(0, 0') \in R_0$ deducem că $0 \in P$. Fie acum $n \in P$ şi $n' \in N'$ a.î. $(n, n') \in R_0$. Din definiția lui R_0 deducem că $(s(n), s'(n')) \in R_0$; obținem că $s(n) \in P$ şi cum (N, 0, s) este triplet Peano, deducem că P=N.

Pentru a doua parte, fie

$Q=\{n \in N$: dacă $n', n'' \in N'$ şi $(n, n'), (n, n'') \in R_0 \Rightarrow n' = n''\} \subseteq N$

şi să demonstrăm la început că $0 \in Q$.

În acest sens, vom demonstra că dacă $(0, n') \in R_0$ atunci $n'=0'$. Dacă prin absurd, $n' \neq 0'$, atunci vom considera relația $R_1=R_0 \setminus \{(0, n')\} \subseteq N \times N'$. Din $n' \neq 0'$ deducem că $(0, 0') \in R_1$ iar dacă pentru $m \in N'$ avem $(n, m) \in R_1$, atunci $(n, m) \in R_0$ şi $(n , m) \neq (0, n')$. Astfel $(s(n), s'(m)) \in R_0$ şi cum $(s(n), s'(m)) \neq (0, n')$ (căci $s(n) \neq 0$ conform cu P_1), deducem că $(s(n), s'(m)) \in R_1$. Cum R_1 verifică r_1 şi r_2 ar trebui ca $R_0 \subseteq R_1$ – absurd (căci R_1 este inclusă strict în R_0).

Pentru a proba că $0 \in Q$, fie $n', n'' \in N'$ a. î. $(0, n'), (0 , n'') \in R_0$. Atunci, ținând cont de cele stabilite mai sus, deducem că $n'=n''=0'$, deci $0 \in Q$.

Fie acum $n \in Q$ şi $n' \in N'$ a. î. $(n, n') \in R_0$; vom demonstra că dacă $(s(n), n'') \in R_0$, atunci $n''=s'(n')$. Să presupunem prin absurd că $n'' \neq s'(n')$ şi să considerăm relația $R_2 = R_0 \setminus \{(s(n), n'')\}$. Vom demonstra că R_2 verifică r_1 şi r_2 .

Într–adevăr, $(0, 0') \in R_2$ (căci $0 \neq s(n)$) iar dacă $(p, p') \in R_2$, atunci $(p, p') \in R_0$ şi $(p, p') \neq (s(n), n'')$.

Deducem că $(s(p), s'(p')) \in R_0$ şi dacă presupunem $(s(p), s'(p')) = (s(n), n'')$, atunci $s(p) = s(n)$, deci $p=n$. De asemenea, $s'(p') = n''$.

Atunci $(n, n') \in R_0$ şi $(n, p') \in R_0$ iar cum $n \in Q \Rightarrow n' = p'$, deci $n'' = s'(p') = s'(n')$, ceea ce contrazice faptul că $n'' \neq s(n')$. Prin urmare, $(s(p), s'(p')) \neq (s(n), n'')$, ceea ce ne arată că $(s(p), s'(p')) \in R_2$, adică R_2 satisface r_1 şi r_2 . Din nou ar trebui ca $R_0 \subset R_2$ – absurd !.

Deci $(s(n), n'') \in R_0 \Rightarrow n'' = s'(n')$ astfel că dacă $r, s \in N'$ şi $(s(n), r)$, $(s(n), s) \in R_0$, atunci $r = s = s'(n)$, adică $s(n) \in Q$, deci $Q=N$.

Pentru a proba unicitatea lui f, să presupunem că mai există $f': N \to N'$ a.î. $f'(0)=0'$ şi $s'(f'(n))=f'(s(n))$ pentru orice $n \in N$.

Considerând $P=\{n \in N : f(n)=f'(n)\} \subseteq N$, atunci $0 \in P$ iar dacă $n \in P$ (adică $f(n)=f'(n)$), atunci $s'(f(n))=s'(f'(n)) \Rightarrow f(s(n))=f'(s(n)) \Rightarrow s(n) \in P$ şi atunci $P=N$, adică $f=f'$.

2) Să arătăm la început că f este injectivă. Pentru aceasta vom considera $P=\{n \in N$: dacă $m \in N$ şi $f(m)=f(n) \Rightarrow m=n\} \subseteq N$ şi să demonstrăm la început că $0 \in P$. Pentru aceasta fie $m \in N$ a. î. $f(0)=f(m)$ şi să demonstrăm că $m=0$. Dacă prin absurd $m \neq 0$, atunci $m=s(n)$ cu $n \in N$ iar egalitatea $f(m)=f(0)$ devine $f(s(n))=f(0)=0'$, de unde $s'(f(n))=0'$, ceea ce este absurd deoarece prin ipoteză $(N', 0', s')$ este un triplet Peano.

Fie acum $n \in P$; pentru a demonstra că $s(n) \in P$, fie $m \in N$ a.î. $f(m)=f(s(n))$.

Atunci $m \neq 0$ (căci în caz contrar ar rezulta că $0'=f(0)=f(s(n))=s'(f(n))$, absurd !), deci conform Lemei 1.2., $m=s(p)$ cu $p \in N$ iar egalitatea $f(m)=f(s(n))$ devine $f(s(p))=f(s(n)) \Leftrightarrow s'(f(p))=s'(f(n))$, adică $f(p)=f(n)$ şi cum $n \in P$, atunci $n=p$ şi astfel $m=s(p)=s(n)$.

Pentru a demonstra surjectivitatea lui f să considerăm

$$P'=\{n' \in N' : \text{există } n \in N \text{ a. î. } n'=f(n)\} \subseteq N' .$$

Cum $f(0)=0'$ deducem că $0' \in P'$. Fie acum $n' \in P'$; atunci există $n \in N$ a.î. $n'=f(n)$. Deoarece $s'(n')=s'(f(n))=f(s(n))$, deducem că $s'(n') \in P'$ şi cum

tripletul $(N', 0', s')$ este un triplet Peano, deducem că $P'=N'$, adică f este şi surjectivă, deci bijectivă . ■

Observaţie Conform Teoremei 1.3. (cunoscută şi sub numele de *teorema de recurenţă*) un triplet Peano este unic până la o bijecție.

În cele ce urmează vom alege un triplet Peano oarecare $(\mathbb{N}, 0, s)$ şi pe care îl vom fixa ; elementele lui $\mathbb{N}$ le vom numi *numere naturale* .

Elementul 0 va purta numele de *zero* . Notăm $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Vom nota $1=s(0)$, $2=s(1)$, $3=s(2)$, e.t.c., astfel că $\mathbb{N}=\{0, 1, 2, \ldots\}$. Funcţia s poartă numele de *funcţia succesor* . Axiomele $P_1 - P_3$ sunt cunoscute sub numele de *axiomele lui Peano* .

Axioma P_3 poartă numele de *axioma inducţiei matematice*.

§2 Adunarea numerelor naturale

TEOREMA 2.1. Există o unică operaţie algebrică pe $\mathbb{N}$ pe care o vom nota prin „+" şi o vom numi adunarea numerelor naturale astfel încât pentru orice m, n$\in\mathbb{N}$ să avem :

A_1 : $0+m=m$

A_2 : $s(n)+m=s(n+m)$.

Demonstraţie Să probăm la început unicitatea şi pentru aceasta să presupunem că mai există o operaţie algebrică $\oplus$ pe $\mathbb{N}$ a.î. sunt verificate A_1 şi A_2.

Fie $P=\{n\in\mathbb{N} \mid n+m=n\oplus m$, pentru orice $m\in\mathbb{N}\}\subseteq\mathbb{N}$.

Din A_1 deducem că $0\in P$ iar din A_2 deducem că dacă $n\in P$, atunci $s(n)+m=s(n)\oplus m \Leftrightarrow s(n+m)=s(n\oplus m)$, ceea ce este adevărat deoarece s este injectivă şi am presupus că $n\in P$. Deci $P=\mathbb{N}$, adică cele două operaţii coincid.

Considerăm un element $m\in\mathbb{N}$ (pe care îl fixăm) şi tripletul $(\mathbb{N}, m, s)$; conform Teoremei 1.3. există o unică funcţie $f_m:\mathbb{N}\to\mathbb{N}$ a. î. $f_m(0)=0$ şi $s(f_m(n))= =f_m(s(n))$ pentru orice $n\in\mathbb{N}$.

Pentru $n\in\mathbb{N}$ definim $n+m=f_m(n)$. Atunci $0+m=f_m(0)=m$ iar $s(n)+m= =f_m(s(n))=s(f_m(n))=s(n+m)$. ■

Observaţie Axiomele A_1–A_2 poartă numele de *axiomele adunării numerelor naturale*.

PROPOZIŢIA 2.2. **Pentru orice m, n∈ℕ avem**

A_1^0 **: n+0=n**

A_2^0 **: n+s (m)= s(n+m) .**

Demonstraţie Fie P={m∈ℕ: m+0=m }⊆ℕ. Dacă în A_1 facem pe m=0, deducem că 0+0=0, adică 0∈P. Dacă m∈P, (adică m+0=m), atunci s(m)+0=s(m+0)=s(m), adică s(m)∈P, deci P=ℕ. Analog se probează şi a doua relaţie.■

PROPOZIŢIA 2.3. **Dubletul (ℕ, +) este monoid comutativ cu proprietatea de simplificare.**

Demonstraţie Din cele stabilite anterior, deducem că 0 este element neutru pentru adunarea numerelor naturale.

Pentru a proba comutativitatea adunării să considerăm

P={n∈ℕ : n+m=m+n pentru orice m∈ℕ} ⊆ℕ .

Evident 0∈P. Dacă n∈P, adică n+m=m+n pentru orice m∈ℕ, atunci s(n)+m=m+s(n) ⇔ s(n+m)=s(m+n) ⇔ n+m=m+n, ceea ce este adevărat. Deducem că P=ℕ, adică adunarea numerelor naturale este comutativă .

Pentru a demonstra asociativitatea adunării numerelor naturale, să considerăm

P ={p∈ℕ: (m+n)+p=m+(n+p) pentru orice m, n∈ℕ}⊆ℕ.

Evident 0∈P. Fie acum n∈P. Atunci (s(n)+m)+p=s(n+m)+p= =s(n+(m+p)) iar s(n)+(m+p)=s(n+(m+p)) şi cum (n+m)+p=n+(m+p) deducem că s(n)∈P, adică P=ℕ.

Pentru partea finală fie

P={p∈ℕ : dacă m+p=n+p ⇒ m=n}⊆ℕ.

Evident 0∈P şi să presupunem că p∈P. Atunci m+s(p)=n+s(p) ⇔s(m+p)=s(n+p) ⇔ m+p=n+p ⇔ m=n (căci p∈P), adică s(p)∈P şi astfel din nou P=ℕ. ■

Observaţie Dacă n∈ℕ, atunci s(n)=s(n+0)=n+s(0)=n+1.

PROPOZIŢIA 2.4. **Dacă m, n∈ℕ şi m+n=0, atunci m=n=0.**

Demonstraţie Dacă $m \neq 0$ sau $n \neq 0$, atunci există $p, q \in \mathbb{N}$ a. î. $m = s(p)$ sau $n = s(q)$. În primul caz, obţinem că $m+n = s(p)+n = s(p+n) \neq 0$ – absurd ! şi analog în al doilea caz. Deci $m = n = 0$. ■

§3 Înmulţirea numerelor naturale

PROPOZIŢIA 3.1. Există o unică operaţie algebrică pe $\mathbb{N}$ notată „·" şi numită înmulţirea numerelor naturale a.î. pentru orice $m, n \in \mathbb{N}$ să avem :

I_1 : $m \cdot 0 = 0$

I_2 : $m \cdot s(n) = mn + m$.

Demonstraţie Fie $m \in \mathbb{N}$ fixat ; considerând tripletul $(\mathbb{N}, 0, f_m)$, unde $f_m : \mathbb{N} \to \mathbb{N}$ este definită prin $f_m(n) = n+m$ pentru orice $n \in \mathbb{N}$, atunci conform Teoremei 1.3. există o unică funcţie $g_m : \mathbb{N} \to \mathbb{N}$ a.î. $g_m(0) = 0$ şi $f_m \circ g_m = g_m \circ s$.

Definim $m \cdot n = g_m(n)$ şi astfel $m \cdot 0 = g_m(0) = 0$ iar $m \cdot s(n) = g_m(s(n)) = f_m(g_m(n)) = f_m(m \cdot n) = m \cdot n + m$. Unicitatea operaţiei de înmulţire cu proprietăţile I_1 şi I_2 se probează ca în cazul adunării. ■

Observaţie I_1 şi I_2 poartă numele de *axiomele înmulţirii numerelor naturale*.

În cele ce urmează, dacă nu este pericol de confuzie, vom scrie $m \cdot n = mn$ pentru $m, n \in \mathbb{N}$.

Analog ca în cazul adunării numerelor naturale, se demonstrează că pentru oricare numere naturale m, n avem :

I_1^0 : **$0 \cdot m = 0$**

I_2^0 : **$s(n) \cdot m = nm + m$.**

LEMA 3.2. Înmulţirea numerelor naturale este distributivă la stânga faţă de adunarea numerelor naturale.

Demonstraţie Fie $P = \{p \in \mathbb{N} : m(n+p) = mn + mp$ pentru oricare $m, n \in \mathbb{N}\} \subseteq \mathbb{N}$.

Ţinând cont de I_1 deducem că $0 \in P$.

Să presupunem acum că $p \in P$ şi fie $m, n \in \mathbb{N}$.

Avem $m(n+s(p)) = m(s(n+p)) = m(n+p)+m = mn+mp+m = mn+ms(p)$, adică $s(p) \in P$ şi astfel $P = \mathbb{N}$. ■

PROPOZIŢIA 3. 3. **Dubletul ($\mathbb{N}$, ·) este monoid comutativ.**

Demonstraţie Pentru a proba asociativitatea înmulţirii fie $P=\{p\in\mathbb{N} : (mn)p=m(np)$ pentru oricare $m, n\in\mathbb{N}\}\subseteq\mathbb{N}$. În mod evident, $0\in P$. Să presupunem acum că $p\in P$ şi să demonstrăm că $s(p)\in P$. Avem $(mn)s(p)=(mn)p+mn$ iar $m(ns(p))=m(np+n)=m(np)+mn$ (conform Lemei 3.2.), de unde egalitatea $(mn)s(p)=m(ns(p))$, adică $s(p)\in P$, deci $P=\mathbb{N}$.

Deoarece pentru orice $n\in\mathbb{N}$ avem $n\cdot 1=n\cdot s(0)=n\cdot 0+n=n$ iar $1\cdot n=s(0)\cdot n=0\cdot n+n=n$ deducem că 1 este elementul neutru al înmulţirii numerelor naturale.

Pentru a proba comutativitatea înmulţirii numerelor naturale fie

$$P=\{n\in\mathbb{N} : nm=mn \text{ pentru orice } m\in\mathbb{N}\}\subseteq\mathbb{N}.$$

În mod evident $0\in P$ şi să presupunem că $n\in\mathbb{N}$. Atunci pentru orice $m\in\mathbb{N}$, $s(n)\cdot m=n\cdot m+m$ iar $m\cdot s(n)=mn+m$, de unde $s(n)\cdot m=m\cdot s(n)$, adică $s(n)\in P$, deci $P=\mathbb{N}$. ■

§4 Relaţia naturală de ordine de pe $\mathbb{N}$.

DEFINIŢIA 4.1. **Pentru $m, n\in\mathbb{N}$ vom scrie $m\leq n$ (şi vom spune că m este mai mic sau egal decât n sau că n este mai mare sau egal decât m) dacă există $p\in\mathbb{N}$ a.î. $m+p=n$; convenim în acest caz să notăm $p=n-m$.**

Dacă $p\in\mathbb{N}^*$, atunci $m\leq n$ şi $m\neq n$; în acest caz vom scrie $m<n$ şi vom spune că m este strict mai mic decât n.

LEMA 4.2. **Dacă $m, n\in\mathbb{N}$ şi $m<n$, atunci $s(m)\leq n$.**

Demonstraţie Deoarece $m<n$, există $p\in\mathbb{N}^*$ a.î. $m+p=n$. Cum $p\in\mathbb{N}^*$, există $k\in\mathbb{N}$ a. î. $p=s(k)$ (conform Lemei 1.2.). Atunci din $m+p=n$ deducem că $m+s(k)=n \Rightarrow s(m+k)=n \Rightarrow s(m)+k=n \Rightarrow s(m)\leq n$. ■

COROLAR 4.3. **Pentru orice $n\in\mathbb{N}$, $n<s(n)$.**

PROPOZIŢIA 4.4. **Dubletul ($\mathbb{N}$, $\leq$) este o mulţime total ordonată.**

Demonstraţie Deoarece pentru orice $n\in\mathbb{N}$, $n+0=n$ deducem că $n\leq n$, adică relaţia $\leq$ este reflexivă. Fie acum $m, n\in\mathbb{N}$ a. î. $m\leq n$ şi $n\leq m$. Atunci există $p, q\in\mathbb{N}$ a.î. $m+p=n$ şi $n+q=m$. Deducem că $n+(p+q)=n$, de unde $p+q=0$ (conform

Propoziției 2.3.), iar de aici p=q=0 (conform Propoziției 2.4.), adică m=n, deci relația $\leq$ este antisimetrică .

Fie acum m, n, p$\in\mathbb{N}$ a. î. m$\leq$n şi n$\leq$p. Atunci există r, s$\in\mathbb{N}$ a. î. m+r=n şi n+s=p. Deducem imediat că m+(r+s)=p, adică m$\leq$p, deci relația $\leq$ este şi tranzitivă, adică $\leq$ este o relație de ordine pe $\mathbb{N}$.

Pentru a proba că ordinea $\leq$ de pe $\mathbb{N}$ este totală, fie m$\in\mathbb{N}$ fixat iar

$$P_m=\{n\in\mathbb{N}: n\leq m \text{ sau } m\leq n\}\subseteq\mathbb{N}.$$

În mod evident $0\in P_m$ şi fie $n\in P_m$. Dacă n=m, atunci cum n<s(n) avem m<s(n), adică $s(n)\in P_m$. Dacă n<m, atunci conform Lemei 4.2. avem s(n)$\leq$m şi din nou $s(n)\in P_m$. Dacă m<n, cum n<s(n) avem că m<s(n) şi din nou $s(n)\in P_m$. Rezultă că $P_m=\mathbb{N}$ şi cum m este oarecare deducem că ordinea $\leq$ de pe $\mathbb{N}$ este totală. ■

Observație Relația de ordine $\leq$ definită anterior pe $\mathbb{N}$ poartă numele de *ordinea naturală* de pe $\mathbb{N}$.

TEOREMA 4.5. Dubletul ($\mathbb{N}$, $\leq$) este o mulțime bine ordonată .

Demonstrație Trebuie să demonstrăm că orice submulțime nevidă A$\subseteq\mathbb{N}$ are un cel mai mic element. Pentru aceasta fie:

$$P=\{n\in\mathbb{N}: n\leq x \text{ pentru orice } x\in A\}\subseteq\mathbb{N}.$$

Evident $0\in P$. Dacă pentru orice $n\in P$ ar rezulta $s(n)\in P$, atunci am deduce că P=$\mathbb{N}$. Astfel că alegând un $x_0\in A$ atunci $x_0\in P$, deci $s(x_0)\in P$. În particular ar rezulta că $s(x_0)\leq x_0$ – absurd !.

Deducem că P$\neq\mathbb{N}$, adică există a$\in$P a.î. s(a)$\notin$P.

Vom demonstra că a$\in$A şi că a este cel mai mic element al lui A.

Dacă a$\notin$A, atunci pentru orice x$\in$A avem a<x, de unde s(a)$\leq$x (conform Lemei 4.2.), adică $s(a)\in P$ – absurd !, deci a$\in$A şi cum a $\in$P deducem că a $\leq$x pentru orice x$\in$A, adică a este cel mai mic element al lui A . ■

COROLAR 4.6. Orice şir descrescător de numere naturale este staționar.

Demonstrație Fie $(a_n)_{n\in\mathbb{N}}$ un şir descrescător de numere naturale iar

$A=\{a_n : n\in\mathbb{N}\}\subseteq\mathbb{N}$. Conform Teoremei 4.5 mulțimea A are un cel mai mic element a_k; atunci pentru orice $m\geq k$ avem $a_m \geq a_k$ şi cum $a_k \leq a_m$ deducem că $a_m = a_k$, adică şirul $(a_n)_{n\in\mathbb{N}}$ este staționar . ■

COROLAR 4.7. **În $\mathbb{N}$ nu putem găsi un şir strict descrescător şi infinit de numere naturale**.

COROLAR 4.8. **Fie $P\subseteq\mathbb{N}$ a.î. pentru orice $n\in\mathbb{N}$ $(x<n \Rightarrow x\in P) \Rightarrow n\in P$. Atunci $P=\mathbb{N}$.**

Demonstrație Fie $A=\mathbb{N}\setminus P\subseteq\mathbb{N}$ şi să presupunem prin absurd că $A\neq\emptyset$.

Conform Teoremei 4.5. mulțimea A va avea un cel mai mic element $a\in A$. Cum pentru $x\in\mathbb{N}$, $x<a \Rightarrow x\notin A \Rightarrow x\in P$, conform ipotezei $P=\mathbb{N}$, adică $a\in P$ şi astfel $a\notin A$ – absurd !. Deci $A=\emptyset$, de unde $P=\mathbb{N}$. ■

COROLAR 4. 9. (Teorema împărțirii cu rest în $\mathbb{N}$). **Pentru oricare două numere naturale m, n cu $n\neq 0$, există şi sunt unice două numere naturale c şi r a.î. $m=n\cdot c+r$ şi $r<n$.**

Demonstrație Fie $A=\{s\in\mathbb{N}$: există $p\in\mathbb{N}$ a.î. $m=np+s\}\subseteq\mathbb{N}$.

Deoarece $m=0\cdot m+m$ deducem că $m\in A$, adică $A\neq\emptyset$. Conform Teoremei 4.5. mulțimea A posedă un element minimal $r\in A$. Atunci există $c\in\mathbb{N}$ a.î. $m=c\cdot n+r$ şi să demonstrăm că $r<n$.

Dacă prin absurd $r\not<n$, atunci conform Propoziției 4.4., $r\geq n$, adică există $u\in\mathbb{N}$ a.î. $r=n+u$. Deducem că $m=nc+r=nc+n+u=n(c+1)+u$, adică $u\in A$, deci $r\leq u$ şi cum $u\leq r$ deducem că $u=r$, adică $n=0$ – absurd !.

Pentru a demonstra unicitatea lui c şi r să presupunem că $m=cn+r=$ $=c'n+r'$, cu $r, r'<n$ şi să arătăm că $c=c'$ şi $r=r'$.

Să presupunem de exemplu că $c<c'$, adică $c+u=c'$ cu $u\in\mathbb{N}^*$.

Atunci $m=nc'+r'=n(c+u)+r'=nc+nu+r'$, deci $r=nu+r'>n$ – absurd !.

Deci $c=c'$ şi deducem imediat că şi $r=r'$. ■

Observație Numărul c poartă numele de *câtul împărțirii lui m la n* iar r se zice *restul* acestei împărțiri .

TEOREMA 4.10. **Fie $m, n, m', n', p\in\mathbb{N}$ a.î. $m\leq n$ şi $m'\leq n'$. Atunci:**

i) $m+m' \leq n+n'$ **şi** $mm' \leq nn'$

ii) $mp \leq np$ **şi** $m^p \leq n^p$.

Demonstraţie i) Putem scrie $m+r=n$ şi $m'+r'=n'$, cu $r, r' \in \mathbb{N}$. Din $(m+m')+(r+r')=n+n'$ deducem că $m+m' \leq n+n'$. De asemenea $nn'=(m+r)(m'+r')=mm'+mr'+r\cdot m'+r\cdot r'$ şi cum $m\cdot r'+r\cdot m'+r\cdot r' \in \mathbb{N}$ deducem că $mm' \leq nn'$.

ii) Se deduce ca şi i) ţinând cont de i) precum şi de regulile de calcul din $\mathbb{N}$ stabilite mai înainte. ■

§5. Reprezentarea numerelor naturale într-o bază dată

Din cele mai vechi timpuri s-a impus găsirea unor procedee de scriere a numerelor naturale care să permită o rapidă estimare a ordinului lor de mărime, precum şi elaborarea unor reguli simple de a efectua principalele operaţii cu acestea (adunarea, înmulţirea). Acestei probleme i s-au dat rezolvări specifice diferitelor etape de dezvoltare a matematicilor (adaptarea sistemului de numeraţie zecimal cu care suntem obişnuiţi azi s-a încheiat abia în secolele XVI-XVII când acesta a cunoscut o largă răspândire în Europa).

În cele ce urmează vom fundamenta ceea ce înseamnă *scrierea numerelor naturale în baza u*, unde $u \in \mathbb{N}$, $u \geq 2$.

LEMA 5.1. Fie u un număr natural >1. Oricare ar fi numărul natural a>0, există numerele naturale n, $q_0, q_1, \ldots, q_{n-1}, a_0, a_1, \ldots, a_n$ a. î.:

$$a=uq_0+a_0, \quad 0 \leq a_0 < u$$
$$q_0=uq_1+a_1, \quad 0 \leq a_1 < u$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$q_{n-2}=uq_{n-1}+a_{n-1}, \quad 0 \leq a_{n-1} < u$$
$$q_{n-1}=a_n, \quad 0 \leq a_n < u$$

Demonstraţie. Dacă $a<u$, luăm $n=0$, $a_0=a$ şi lema este adevărată. Dacă $a \geq u$, fie $q_0, a_0 \in \mathbb{N}$ astfel încât $a=uq_0+a_0$, $0 \leq a_0 < u$.

Cum $a \geq u$, avem $q_0>0$. Există $q_1, a_1 \in \mathbb{N}$ astfel încât $q_0=uq_1+a_1$, $0 \leq a_1 < u$ şi aşa mai departe.

Dacă $q_i \neq 0$, atunci din $1<u$ rezultă $q_i < uq_i \leq uq_i+a_i=q_{i-1}$, de unde:

$$a>q_0>q_1>\ldots>q_{i-1}>q_i>\ldots\geq 0.$$

Este clar că există n astfel încât $q_{n-1} \neq 0$ şi $q_n=0$. Rezultă că $0<q_{n-1}=a_n<u$ şi lema este demonstrată. ■

LEMA 5.2. **Fie u, a_0, $a_1,\ldots,a_n \in \mathbb{N}$ astfel încât u>1, $0 \le a_i < u$ pentru $0 \le i < n$ şi $0 < a_n < u$. Atunci:**

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

Demonstraţie Cum $a_i \le u-1$ pentru i=0, 1,…, n, atunci:

$$\sum_{i=0}^{n} a_i u^i \le \sum_{i=0}^{n} (u-1)u^i = u^{n+1} - 1 < u^{n+1}$$, de unde rezultă lema. ■

TEOREMA 5.3. **Fie u un număr natural >1. Oricare ar fi numărul a>0, există numerele naturale n, $a_n, a_{n-1}, \ldots, a_0$ unic determinate astfel încât: $a = a_n u^n + a_{n-1} u^{n-1} + \ldots + a_1 u + a_0$, unde $0 < a_0 < u$ şi $0 \le a_i < u$ pentru orice $0 \le i \le n-1$.**

Demonstraţie Conform Lemei 5.1., există n, $q_0,\ldots, q_{n-1}$ şi $a_0, a_1, \ldots, a_n$ a.î.:

$a = uq_0 + a_0$, $0 \le a_0 < u$

$q_0 = uq_1 + a_1$, $0 \le a_1 < u$

……

$q_{n-2} = uq_{n-1} + a_{n-1}$, $0 \le a_{n-1} < u$

$q_{n-1} = a_n$, $0 \le a_n < u$.

Înmulţim aceste egalităţi respectiv cu 1, u, $u^2,\ldots,u^n$. Adunând apoi termen cu termen egalităţile ce se obţin, rezultă:

$a = a_n u^n + a_{n-1} u^{n-1} + \ldots + a_1 u + a_0$.

Rămâne să dovedim unicitatea numerelor n, $a_n,\ldots,a_1$, a_0. Fie de asemenea numerele naturale $n', a'_{n'}, a'_{n'-1}, \ldots, a'_1, a'_0$ a.î. $a = a'_{n'} u^{n'} + a'_{n'-1} u^{n'-1} + \ldots + a'_1 u + a'_0$ cu $0 < a'_{n'} < u$ şi $0 \le a'_i < u$ pentru $0 \le i < n'$.

Dacă $n < n'$, atunci $n+1 \le n'$ şi din Lema 5.2. rezultă:

$$a = \sum_{i=0}^{n} a_i u^i < u^{n+1} \le u^{n'} \le \sum_{i=0}^{n'} a'_i u^i = a$$, deci a<a (contradicţie).

Analog se arată că nu este posibil ca $n' < n$, de unde $n = n'$.

Să demonstrăm acum că $a_i = a'_i$, $0 \le i \le n$. Dacă n=0, atunci $a_0 = a = a'_0$. Presupunem că n>0 şi că afirmaţia este adevărată pentru n-1. Din egalităţile:

$a = a_0 + u(a_n u^{n-1} + \ldots + a_1) = a'_0 + u(a'_{n'} u^{n'-1} + \ldots + a'_1)$, unde $0 \le a_0 < u$ şi $0 \le a'_0 < u$ rezultă, folosind unicitatea câtului împărţirii lui a prin u că $a_0 = a'_0$ şi $a_n u^{n-1} + \ldots + a_2 u + a_1 = a'_{n'} u^{n'-1} + \ldots + a'_2 u + a'_1$.

Folosind ipoteza de inducţie, din ultima egalitate deducem că $a_i = a'_i$, i=1,2,…,n.

Teorema este astfel complet demonstrată. ■

Suntem acum în măsură să definim ceea ce este cunoscut sub numele de *sistem de numeraţie în baza u*, unde u este un număr natural >1.

La fiecare număr natural a>0 facem să corespundă secvenţa finită de numere naturale $a_n a_{n-1}\ldots a_1 a_0$, unde $a_i<u$, $0\le i\le n$, $a_n\neq 0$ şi $a=\sum_{i=0}^{n} a_i u^i$.

Aşadar, $a_n a_{n-1}\ldots a_1 a_0 \overset{def}{=} a_n u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0$.

Din Teorema 5.3. rezultă că se stabileşte astfel o corespondenţă biunivocă între numerele naturale >0 şi secvenţele finite $a_n a_{n-1}\ldots a_1 a_0$ de numere naturale $a_i<u$, cu $a_n\neq 0$. Când se impune să atragem atenţia asupra bazei sistemului de numeraţie, se obişnuieşte să se scrie $a_n a_{n-1}\ldots a_1 a_{o(u)}$ sau $\overline{a_n a_{n-1}\ldots a_1 a_{o(u)}}$.

Dacă baza sistemului de numeraţie este zece (notată 10) el este numit *sistemul zecimal*. Cifrele sistemului de numeraţie se numesc *cifre zecimale*. Ele sunt numerele mai mici ca zece şi se notează în ordine cu 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Secvenţa de cifre zecimale 75038 sau mai precis $75038_{(10)}$ reprezintă, aşadar, numărul natural: $7\times10^4 + 5\times10^3 + 0\times10^2 + 3\times10 + 8$.

Dacă u=2, atunci avem *sistemul de numeraţie binar*, cifrele binare fiind 0 şi 1. Astfel: $11010_{(2)}=1\times2^4 + 1\times2^3 + 0\times2^2 + 1\times2 + 0 = 26_{(10)}$.

Printre sistemele de numeraţie mai des folosite se numără şi cel de bază $u=16_{(10)}=10000_{(2)}$ numit *sistemul de numeraţie hexazecimal*, cifrele hexazecimale fiind 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, F.

Astfel, avem $27_{(10)}=1A_{(16)}=11011_{(2)}$.

Iată o listă de probleme care se pun în mod natural în legătură cu reprezentarea numerelor într-o bază:

(I) Stabilirea raportului de mărime între două numere reprezentate în aceeaşi bază.

(II) Stabilirea unor reguli (algoritmi) de efectuare a sumei, produsului etc. a două numere reprezentate în aceeaşi bază.

(III) Elaborarea unor algoritmi pentru reprezentarea unui număr într-o bază dată.

În continuare se va arăta cum pot fi soluţionate aceste probleme pentru numere naturale. Să începem cu problema (I).

În teorema următoare se dă un criteriu foarte comod de a stabili raportul de mărime între două numere naturale reprezentate în aceeaşi bază.

TEOREMA 5.4. Fie a şi b două numere naturale, $a=a_m a_{m-1}\ldots a_1 a_{0(u)}$ şi $b=b_n b_{n-1}\ldots b_1 b_{0(u)}$. Atunci $a<b$ dacă şi numai dacă $m<n$ şi $a_p<b_p$, unde p este cel mai mare i astfel încât $a_i\neq b_i$.

Demonstraţie Dacă m<n, din Lema 5.2. rezultă $a < u^{m+n} \le u^n \le b$, deci a<b. Dacă m=n şi $a_p<b_p$, unde $p=\max\{i|a_i\neq b_i\}$, atunci
$b-a=(b_p-a_p)u^p + (b_{p-1}u^{p-1} +\ldots+b_0) - (a_{p-1}u^{p-1} + \ldots+ a_0) > (b_p-a_p)u^p + (b_{p-1}u^{p-1} +\ldots+ + b_0)- u^p\ge u^p + (b_{p-1}u^{p-1} +\ldots+ b_0)- u^p\ge 0$, de unde b-a>0, deci a<b.

Reciproc, presupunem că a<b. Atunci m≤n, deoarece m>n implică b<a. Dacă m<n, nu mai avem nimic de demonstrat. Dacă m=n, fie $p=\max\{i|a_i\neq b_i\}$. Avem $a_p<b_p$, întrucât $a_p>b_p$ implică, conform primei părţi a demonstraţiei, b<a. Teorema este demonstrată. ■

Astfel pentru numerele 125302 şi 95034 date în baza zece avem 125302>95034. La fel, pentru numerele 101101 şi 100110 date în baza doi avem 101101>100110.

Referitor la problema (II) se va arăta cum se face adunarea şi înmulţirea numerelor naturale reprezentate într-o bază u. În particular, dacă u=10, se regăsesc cunoscutele procedee de adunare şi înmultire a numerelor naturale.

Fie a şi b două numere naturale, $a=a_ma_{m-1}\ldots a_1a_{0(u)}$, $b=b_nb_{n-1}\ldots b_1b_{0(u)}$. Trebuie să găsim cifrele c_0, c_1,… ale numărului a+b în baza u. Putem scrie $a=a_0+a_1u+a_2u^2+\ldots$ şi $b=b_0+b_1u+b_2u^2+\ldots$. Cum $a_0<u$ şi $b_0<u$, rezultă că $a_0+b_0<2u$, deci $a_0+b_0=u\varepsilon_1+c_0$, $0\le c_0<u$, $\varepsilon_1=0$ sau $\varepsilon_1=1$; mai precis, avem $\varepsilon_1=0$ şi $c_0=a_0+b_0$ dacă $a_0+b_0<u$ iar $\varepsilon_1=1$ şi $c_0=a_0+b_0-u$ dacă $u\le a_0+b_0<2u$. Rezultă $a+b=c_0+(a_1+b_1+\varepsilon_1)u+(a_2+b_2)u^2+\ldots$. Evident, $a_1+b_1+\varepsilon_1<2u$, de unde $a_1+b_1+\varepsilon_1=u\varepsilon_2+c_1$, $0\le c_1<u$, unde $\varepsilon_2=0$ sau $\varepsilon_2=1$. Avem $a+b=c_0+c_1u+ +(a_2+b_2+\varepsilon_2)u^2+\ldots$, ş.a.m.d.

Se deduce că cifrele c_0, c_1, c_2,… ale sumei a+b sunt $c_i= (a_i+b_i+\varepsilon_i)$ mod u, i=0, 1, 2, …, unde $\varepsilon_0=0$, şi pentru i>0:

$\varepsilon_i=0 \Leftrightarrow a_{i-1}+b_{i-1}+\varepsilon_{i-1}<u$ şi atunci $c_{i-1}= a_{i-1}+b_{i-1}+\varepsilon_{i-1,}$

$\varepsilon_i=1 \Leftrightarrow a_{i-1}+b_{i-1}+\varepsilon_{i-1}\ge u$ şi atunci $c_{i-1}= a_{i-1}+b_{i-1}+\varepsilon_{i-1}-u$.

Când m=n, numărul a+b are:

1) m cifre dacă $a_n+b_n+\varepsilon_n<u$,

2) m+1 cifre dacă $a_n+b_n+\varepsilon_n\ge u$, cifra de rang m+1 fiind în acest caz $c_{m+1}=1$.

Dacă m≠n, de exemplu m>n, atunci cele de mai sus rămân adevărate luând $b_{n+1}=\ldots=b_m=0$.

Se observă că pentru a efectua a+b în baza u mai trebuie să cunoaştem, sau să avem posibilitatea să consultăm, tabla adunării numerelor naturale <u. De exemplu, dacă u=5, tabla adunării numerelor naturale <5, cu rezultatele exprimate în baza 5, este cea din tabelul 1. În acest tabel la intersecţia liniei numărului i cu coloana numărului j este pus i+j reprezentat în baza 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

Tabelul 1. Tabla adunării în baza 5

Cititorul poate singur acum să redacteze un algoritm al adunării numerelor naturale în baza u, luând ca motivație teoretică a acestuia considerațiile de mai sus. Observăm că în acest algoritm apare variabila ε care are valoarea inițială $\varepsilon_0=0$ iar valorile ε_i, $i \geq 1$, sunt egale cu 1 când $a_{i-1}+ b_{i-1}+ \varepsilon_{i-1} \geq u$, respectiv 0 când $a_{i-1}+b_{i-1}+\varepsilon_{i-1}<u$. Se spune că varibila ε realizează transportul unității de la cifrele de rang i la cele de rang i+1, i=0, 1,….

În calculul cu "creionul şi hârtia" al sumei a două numere naturale, operațiile din algoritmul adunării în baza u se sistematizează astfel:

$$\begin{array}{l} a_m a_{m-1} \ldots a_1 a_0 + \\ b_m b_{m-1} \ldots b_1 b_0 \\ \hline c_{m+1} c_m c_{m-1} \ldots c_1 c_0 \\ \varepsilon_m \varepsilon_{m-1} \ldots \varepsilon_1 \varepsilon_0 \end{array}$$

ultima linie, care descrie transportul unității, de regulă se omite.

Astfel, dacă u=2, $a=1011101_{(2)}$, $b=101101_{(2)}$, atunci a+b se face după cum urmează:

$$\begin{array}{r} 1011101+ \\ 101101 \\ \hline 10001010 \\ 1111101 \end{array}$$

deci $a+b=10001010_{(2)}$. S-a folosit şi tabla adunării numerelor naturale <2, care este:

+	0	1
0	0	1
1	1	10

rezultatele fiind reprezentate în baza 2.

În continuare se va arăta că înmulțirea a două numere naturale în baza u se reduce la următoarele tipuri de operații:

1) înmulțirea unui număr natural a cu o putere u^j a bazei u;

2) înmulțirea unui număr natural a cu o cifră a sistemului de numerație (deci cu un număr natural j, $0 \le j < u$);

3) adunarea în baza u.

Fie $a = a_m a_{m-1} \dots a_1 a_{0(u)} = a_m u^m + a_{m-1} u^{m-1} + \dots + a_1 u + a_0$.

Atunci $au^j = a_m u^{m+j} + a_{m-1} u^{m-1+j} + \dots + a_1 u^{1+j} + a_0 u^j = a_m a_{m-1} \dots a_1 a_0 \underbrace{00\dots0}_{j}{}_{(u)}$

și acum este clar cum se face în baza u o înmulțire de tipul 1).

Dacă i și j sunt două numere naturale <u, atunci $ij < u^2$, de unde, folosind teorema împărțirii cu rest pentru numerele naturale, avem:

$$ij = uq(i, j) + r(i, j),\ 0 \le r(i, j) < u,\ 0 \le q(i, j) < u \qquad (*)$$

câtul q(i, j) și restul r(i, j) împărțirii numărului ij prin u depinzând de i și j.

Fie acum a un număr natural dat în baza u

$$a = a_m a_{m-1} \dots a_1 a_{0(u)} = \sum_{i=0}^{m} a_i u^i$$

și j o cifră a sistemului de numerație de bază u, deci $0 \le j < u$. Avem:

$$aj = \sum_{i=0}^{m} a_i j u^i = \sum_{i=0}^{m} (uq(a_i, j) + r(a_i, j)) u^i = \sum_{i \ge 0} r(a_i, j) u^i + \sum_{i \ge 0} q(a_i, j) u^{i+1},$$

deci efectuarea produsului aj în baza u revine la a face suma în baza u a numerelor a′ și a′′ reprezentate în baza u:

$$a' = r(a_0, j) + r(a_1, j)u + r(a_2, j)u^2 + \dots$$

și $a'' = q(a_0, j) + q(a_1, j)u^2 + \dots$

Așadar, s-a lămurit cum se face în baza u și o înmulțire de tipul 2).

În sfârșit, dacă $b = b_n b_{n-1} \dots b_1 b_{0(u)} = \sum_{j=0}^{n} b_j u^j$, atunci $ab = \sum_{j=0}^{n} ab_j u^j$, deci produsul ab se poate efectua făcând suma în baza u a numerelor $ab_j u^j$, j=0, 1, 2, …, n. Dar $ab_j u^j = (ab_j) u^j$. Așadar ab_j este o operație de tipul 2) și în sfârșit $(ab_j)u^j$ e o operație de tipul 1).

Cititorul se poate convinge ușor că regula de înmulțire a numerelor naturale în baza zece se motivează din punct de vedere teoretic prin considerațiile de mai sus, luând u=10. Un instrument important al înmulțirii numerelor în baza zece este tabla înmulțirii numerelor <10. Pe de altă parte, se observă că în regula de înmulțire a numerelor în baza u trebuie să cunoaștem numerele q(i, j) și r(i, j), $0 \le i, j < u$,din relația (*). Din relația (*) rezultă că q(i, j) și r(i, j) sunt cifrele numărului ij, $0 \le i, j < u$, reprezentat în baza u [dacă ij<u, avem q(i, j)=0]. Așadar, procedeul de înmulțire expus uzează de tabla înmulțirii numerelor naturale <u, cu rezultatele reprezentate în baza u.

În tabelele 2 şi 3 sunt date tablele înmulțirii în baza u=5, respectiv u=2.

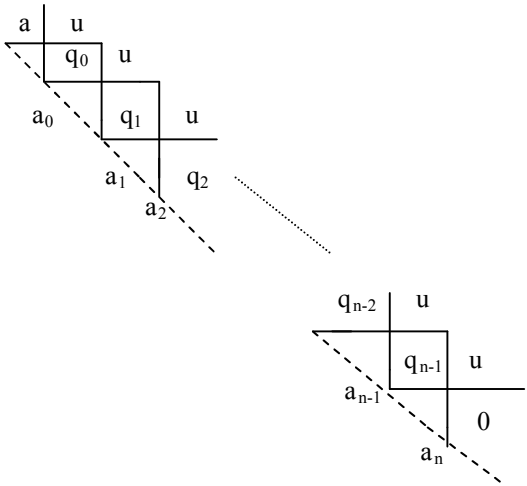
×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

Tabelul 2: Tabla înmulțirii în baza 5

×	0	0
0	0	0
1	0	11

Tabelul 3: Tabla înmulțirii în baza 2

Pentru calculul cu "creionul şi hârtia" calculele pot fi sistematizate ca în figura următoare:



Să ne ocupăm acum da problema (III).

Trebuie observat că numărul natural a ce urmează să fie reprezentat într-o bază u este dat, de regulă, într-o bază v şi de fapt se face trecerea lui a din baza v în baza u. Se pot distinge 3 variante:

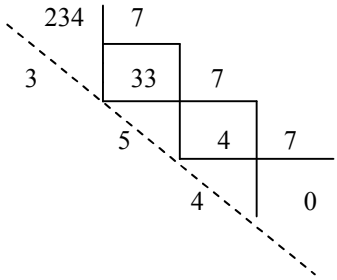
1) Trecerea lui a din baza v în baza u cu efectuarea calculelor în baza v;

2) Trecerea lui a din baza v în baza u cu efectuarea calculelor în baza u;

3)Trecerea lui a din baza v în baza u cu efectuarea calculelor într-o bază intermediară w;

Pentru a trece pe a din baza v în baza u cu metoda 1) se reprezintă mai întâi u în baza v şi apoi se aplică algoritmul sistemelor de numerație pentru a şi u cu efectuarea calculelor în baza v. Cum în calculatoare numerele sunt, de regulă, reprezentate în baza v=2, metoda 1) se aplică atunci când se livrează rezultatele numerice (de regulă în baza u=10), execuția algoritmului sistemelor de numerație putând fi astfel încredințată calculatorului (calculele se fac în baza v=2). Aceeaşi metodă se aplică şi când se trece cu "hârtia şi creionul" un număr din baza v=10, într-o altă bază u, preferându-se calculele în baza v=10 din motive lesne de înțeles.

Pentru exemplificare, să trecem numărul a=234 dat în baza v=10 în baza u=7. Algoritmul sistemelor de numerație este în acest caz:



de unde $a=453_{(7)}$.

Pentru a trece pe $a=a_n a_{n-1}\ldots a_1 a_{0(v)}$ din baza v în baza u cu metoda 2) se reprezintă mai întâi a_0, $a_1,\ldots,a_n$ şi v în baza u cu ajutorul algoritmului sistemelor de numerație. Se introduce a_0, a_1, …, a_n şi v astfel reprezentați în expresia

$$a_n v^n + a_{n-1} v^{n-1} + \ldots + a_1 v + a_0$$

şi se face calculul acesteia folosind algoritmului adunării şi algoritmul înmulțirii în baza u. Se obține, în final, reprezentarea lui a în calculator. Numerele date de

regulă în baza u=2; efectuarea calculelor în baza u=2 poate fi încredințată calculatorului.

Metoda 3) este evident o combinatie a primelor două. Astfel, dacă dorim să trecem un număr a dintr-o bază v≠2, într-o bază u≠2, folosind un calculator care lucrează cu numere reprezentate în baza 2, atunci trecem pe a în baza 2 cu metoda 2) şi apoi îl trecem în baza u cu metoda 1). Procedând astfel, toate calculele pot fi încredințate calculatorului. Când v≠10 şi u≠10, iar trecerea de la baza b la baza u vrem să o facem cu "creionul şi hârtia", preferăm baza intermediară w=10 pentru a putea executa toate calculele în baza 10, cu care suntem obişnuiți.

Observații 1. Trecerea unui număr natural a din baza v în baza u se simplifică considerabil când $v=u^r$, r număr natural >1. Metoda se justifică prin faptul că un număr natural $b<u^r$ poate fi scris în mod unic sub forma

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

De aici, rezultă că pentru a reprezenta numărul $a=a_na_{n-1}\ldots a_1a_{0(v)}=$ $= a_nv^n + a_{n-1}v^{n-1} + \ldots + a_1v + a_0$ în baza u, unde $v=u^r$ cu r >1, fiecare cifră a_i se scrie ca în (**), anume $a_i=c_{ir-1}u^{r-1}+\ldots+c_{i1}u+c_{i0}$ şi se înlocuieşte fiecare a_i cu secvența, $c_{ir-1}\ldots c_{i1}c_{i0}$, deci obținem secvența

$$c_{nr-1}\ldots c_{n1}c_{n0}c_{n-1,r-1}\ldots c_{n-1,1}c_{n-1,0}\ldots c_{01}c_{00}.$$

Înlăturând cifrele egale cu 0 de la începutul secvenței de mai sus se obține repreprezentarea lui a în baza u.

Astfel, pentru a reprenta numărul $a=375_{(8)}$ în baza u=2 (deci $v=u^3$), scriem mai întâi:

$$a_0=5=1\times2^2+0\times2+1\times1=c_{02}\cdot2^2+c_{01}\cdot2+c_{00}$$
$$a_1=7=1\times2^2+1\times2+1\times1=c_{12}\cdot2^2+c_{11}\cdot2+c_{10},$$
$$a_3=3=0\times2^2+1\times2+1\times1=c_{22}\cdot2^2+c_{21}\cdot2+c_{20},$$

aşadar secvența de mai sus este în acest caz:

011 111 101.

2. Când $v^r = u$, r>1, trecerea unui număr din baza v în baza u se face printr-o metodă care urmează calea inversă a metodei de la observația 1. În acest caz, pentru a trece în baza u numărul $a=a_na_{n-1}\ldots a_1a_{0(v)}$ se separă de la dreapta la stânga grupe de câte r cifre (ultima grupă având cel mult r cifre) şi fiecare grupă va reprezenta o cifră în baza u, cu care vom înlocui grupa respectivă. Se obține astfel reprezentarea lui a în baza u.

Astfel, dacă u=8 şi v=2, deci $v^3=u$, numărul $a=11\ 111\ 101_{(2)}$ are în baza 8 reprezentarea $a=375_{(8)}$ pentru că cifrele lui a în baza 2 pot fi grupate astfel:

$$\underbrace{11}\ \underbrace{111}\ \underbrace{101}$$

şi grupele obținute reprezintă în baza 2 respectiv cifrele 3, 7 şi 5 ale bazei 8.

3)Inconvenientul sistemului binar de numeraţie constă în faptul că reprezentarea numerelor mari necesită secvenţe de cifre binare exagerat de lungi. Aceasta complică mult lectura numerelor precum şi aprecierea ordinului lor de mărime. O metodă de a atenua aceste inconveniente este de a folosi sisteme de numeraţie cu baze mixte. Un exemplu este sistemul de numeraţie zecimal codat în binar, rezervându-se câte patru poziţii binare fiecărei cifre zecimale. Astfel, numărul $a=793_{(10)}$ se reprezintă în sistemul zecimal codat în binar după cum urmează:

$$\underbrace{0111}_{7}\ \underbrace{1001}_{9}\ \underbrace{0011}_{3}$$

În practică se foloseşte curent sistemul de numeraţie cu bază mixtă . Astfel expresia: 8 ani, 3 luni, 2 săptămâni, 15 ore şi 35 minute este un model de reprezentare a timpului într-un sistem de numeraţie cu şase baze.

Observaţie Acest paragraf a fost redactat în cea mai mare parte după lucrarea [14].

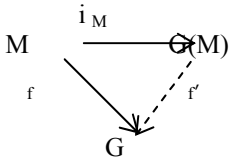
CAPITOLUL 2 :
INELUL NUMERELOR ÎNTREGI $\mathbb{Z}$

§1 Construcţia lui $\mathbb{Z}$

În vederea construirii mulţimii numerelor întregi $\mathbb{Z}$, vom prezenta la început Teorema lui Malţev de scufundare a unui monoid comutativ cu proprietatea de simplificare într-un grup comutativ urmând ca prin particularizarea la cazul monoidului $(\mathbb{N}, +)$ să obţinem grupul aditiv $(\mathbb{Z}, +)$.

TEOREMA 1.1. (Malţev) Fie $(M, \cdot)$ un monoid comutativ cu proprietatea de simplificare. Atunci există un grup comutativ G(M) şi un morfism injectiv de monoizi $i_M: M \to G(M)$ ce verifică următoarea proprietate de universalitate :

Pentru orice grup comutativ G şi orice morfism de monoizi $f: M \to G$ există un unic morfism de grupuri $f': G(M) \to G$ a.î. diagrama



este comutativă (adică $f' \circ i_M = f$).

Demonstrație Pe mulțimea $M' = M \times M$ definim relația $(x, y) \sim (x', y') \overset{def}{\Leftrightarrow} xy' = yx'$ și să probăm că $\sim$ este o echivalență pe M' compatibilă cu structura de monoid a lui M' (adică $\sim$ este o congruență pe monoidul produs $M' = M \times M$). În mod evident, relația $\sim$ este reflexivă și simetrică. Dacă $(x, y) \sim (x', y')$ și $(x', y') \sim (x'', y'')$ atunci $xy' = yx'$ și $x'y'' = x''y'$, de unde $xx'y'y'' = x'x''yy'$, deci $xy'' = yx''$ (am simplificat prin $x'y'$), adică $(x, y) \sim (x'', y'')$, deci relația $\sim$ este și tranzitivă, de unde concluzia că $\sim$ este o echivalență pe M' .

Fie acum $(x, y), (x', y'), (a, b), (a', b') \in M'$ a.î. $(x, y) \sim (a, b)$ și $(x', y') \sim (a', b')$ și să probăm că și $(xx', yy') \sim (aa', bb')$.

Avem deci $xb = ya$ și $x'b' = y'a'$, de unde $xx'bb' = yy'aa'$, adică $(xx', yy') \sim (aa', bb')$, adică relația $\sim$ este o congruență pe monoidul produs M' în care reamintim că operația de compunere se definește prin $(x, y) \cdot (x', y') = (xx', yy')$. Vom considera monoidul cât $G(M) = M'/\sim$ iar pentru $(x, y) \in M'$ vom nota prin $[x, y]$ clasa sa de echivalență în $G(M)$.

Datorită faptului că relația $\sim$ este o congruență pe M' deducem imediat că $G(M)$ devine în mod canonic monoid comutativ, definind pentru $[x, y], [x', y'] \in G(M)$, $[x, y] \cdot [x', y'] = [xx', yy']$ (elementul neutru al lui $G(M)$ va fi $[e, e]$, e fiind elementul neutru al lui M). Deoarece pentru $[x, y] \in G(M)$, $[x, y] \cdot [y, x] = [xy, xy] = [e, e]$ deducem că $[y, x] = [x, y]^{-1}$, adică $G(M)$ este grup (comutativ).

Definim $i_M : M \to G(M)$ prin $i_M(x) = [x, e]$ pentru orice $x \in M$. Pentru $x, y \in M$ avem $i_M(x) \cdot i_M(y) = [x, e] \cdot [y, e] = [xy, e] = i_M(xy)$ adică i_M este morfism de monoizi. Dacă $i_M(x) = i_M(y)$, atunci $[x, e] = [y, e] \Leftrightarrow xe = ye \Leftrightarrow x = y$, adică i_M este chiar morfism injectiv de monoizi .

Să arătăm acum că dubletul $(G(M), i_M)$ verifică proprietatea de universalitate din enunț. Pentru aceasta fie G un grup comutativ oarecare și $f: M \to G$ un morfism de monoizi. Pentru $[x, y] \in G(M)$, definim $f'([x, y]) = f(x) \circ (f(y))^{-1}$. Observăm că dacă $[x, y] = [x', y']$, atunci $xy' = x'y$, deci $f(x) \circ f(y') = f(x') \circ f(y) \Leftrightarrow f(x) \circ (f(y))^{-1} = f(x') \circ (f(y'))^{-1}$, adică f' este corect definită.

Să probăm acum că f' este morfism de grupuri.

Avem $f'([x, y]\cdot[x', y'])=f'([xx', yy'])=f([xx')[f(yy')]^{-1}=$

$=f(x)f(x')[f(y)\cdot f(y')]^{-1}=(f(x)[f(y)]^{-1})(f(x')[f(y')]^{-1})=f'([x, y])f'([x', y'])$. Pentru $x\in M$ avem $(f'\circ i_M)(x)=f'(i_M(x))=f'([x, e])=f(x)[f(e)]^{-1}=f(x)$, de unde concluzia că $f'\circ i_M=f$.

Pentru a proba unicitatea lui f' (cu proprietatea din enunț) să presupunem că mai există un morfism de grupuri $f'':G(M)\to G$ a.î. $f''\circ i_M=f$.

Atunci, pentru $[x, y]\in G(M)$ avem $[x, y]=[x, e]\cdot[e, y]=[x, e]\cdot[y, e]^{-1}$, de unde $f''([x, y])=f''([x, e]\cdot[y, e]^{-1})=f''(i_M(x)\circ(i_M(y)^{-1}))=f''(i_M(x))\circ(f''(i_M(y)))^{-1}=$

$=f(x)\circ(f(y))^{-1}=f'([x, y])$, adică $f''=f'$. ■

Observaţii

1. Dacă f este un morfism injectiv de grupuri , atunci şi f' este morfism injectiv de grupuri .

Într-adevăr, dacă $[x, y]\in G(M)$ şi $f'([x, y])=e$, atunci $f(x)(f(y))^{-1}=e$, deci $f(x)=f(y)$, de unde $x=y$, adică $[x, y]=[x, x]=e$.

2. Dacă pe mulțimea dubletelor (G, f) cu G grup abelian şi $f:M\to G$ morfism injectiv de monoizi definim relația $(G, f)\le(G', f')\Leftrightarrow$ există $h:G\to G'$ a.î. h este morfism injectiv de grupuri şi $h\circ f=f'$, atunci se verifică imediat că relația de mai sus este o relație de ordine iar dubletul $(G(M), i_M)$ din Teorema lui Malțev este cel mai mic element față de această relație de ordine.

DEFINIŢIA 1.2. Considerăm monoidul $(\mathbb{N}, +)$ (ce are proprietatea de simplificare conform Propoziției 2.3. de la Capitolul 1) şi urmând tehnica dată de Teorema lui Malțev, mulțimea subiacentă grupului aditiv $(G(\mathbb{N}), +)$ se notează prin $\mathbb{Z}$ şi poartă numele de mulţimea numerelor întregi .

Ținând cont de faptul că $i_{\mathbb{N}}:\mathbb{N}\to\mathbb{Z}$, $i_{\mathbb{N}}(n)=[n, 0]$ pentru orice $n\in\mathbb{N}$ este morfism injectiv de monoizi, vom identifica fiecare număr natural $n\in\mathbb{N}$ prin elementul întreg $[n, 0]$ astfel că $\mathbb{N}$ va fi privită în continuare ca submulțime a lui $\mathbb{Z}$.

Fie acum $z=[m, n]\in\mathbb{Z}$. Dacă $m=n$, atunci $z=0$. Dacă $m<n$, atunci există $p\in\mathbb{N}^*$ a.î. $m+p=n$ (în acest caz convenim să notăm $p=n-m$ şi astfel $m+(n-m)=n$) iar $z=[0, p]=-[p, 0]$ se identifică cu numărul întreg $-p$ iar dacă

$n<m$, atunci există $q\in\mathbb{N}^*$ a.î. $n+q=m$ şi astfel $z=[q, 0]$ identificându-se cu numărul natural q.

Ţinând cont de acestea putem scrie pe $\mathbb{Z}$ sub forma $\mathbb{Z}=(-\mathbb{N}^*)\cup\mathbb{N}$ unde $-\mathbb{N}^*=\{-n|n\in\mathbb{N}^*\}$ sau $\mathbb{Z}=\{0, \pm1, \pm2, \ldots.\}$. Vom nota $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

§2 Înmulţirea numerelor întregi

LEMA 2.1. **Fie $x, y, z, t, x', y', z', t'\in\mathbb{N}$ a.î. $[x, y]=[x', y']$ şi $[z, t]=[z', t']$. Atunci $[xz+yt, xt+yz]=[x'z'+y't', x't'+y'z']$.**

Demonstraţie Din ipoteză avem $x+y'=y+x'$ şi $z+t'=z'+t$ astfel că

$$[xz+yt, xt+yz]=[x'z'+y't', x't'+y'z']\Leftrightarrow$$

$$(xz+yt)+(x't'+y'z')=(xt+yz)+(x'z'+y't')\Leftrightarrow$$

$x(z-t)+y(t-z)=x'(z'-t')+y'(t'-z')\Leftrightarrow(x-y)(z-t)=(x'-y')(z'-t')$ ceea ce este adevărat deoarece $x-y=x'-y'$ şi $z-t=z'-t'$. ■

Fie acum $\alpha=[x, y]$ şi $\beta=[z, t]$ două numere întregi.

Definind $\alpha\cdot\beta=[xz+yt, xt+yz]$, conform Lemei 2.1. deducem că această definiţie este corectă .

PROPOZIŢIA 2.2. **$(\mathbb{Z}, +, \cdot)$ este domeniu de integritate.**

Demonstraţie Conform celor de mai înainte $(\mathbb{Z}, +)$ este grup comutativ. Să demonstrăm acum că $(\mathbb{Z}, \cdot)$ este monoid comutativ iar pentru aceasta fie $\alpha=[x, y]$, $\alpha'=[x', y']$, $\alpha''=[x'', y'']$ trei elemente oarecare din $\mathbb{Z}$.

Atunci :

$\alpha(\alpha'\alpha'')=[x,y][x'x''+y'y'',x'y''+y'x'']$

$=[x(x'x''+y'y'')+y(x'y''+y'x''), x(x'y''+y'x'')+y(x'x''+y'y'')]$

$=[xx'x''+xy'y''+x'yy''+x''yy', xx'y''+xx''y'+x'x''y+yy'y'']$ iar

$(\alpha\alpha')\alpha''=[xx'+yy', xy'+x'y][x'', y'']$

$=[(xx'+yy')x''+(xy'+x'y)y'', (xx'+yy')y''+(xy'+x'y)x'']$

$=[xx'x''+xy'y''+x'yy''+x''yy', xx'y''+xx''y'+x'x''y+yy'y'']$,

de unde deducem că $\alpha(\alpha'\alpha'')=(\alpha\alpha')\alpha''$ adică înmulţirea numerelor întregi este asociativă.

În mod evident, $\alpha\alpha'=\alpha'\alpha$ (deoarece înmulţirea numerelor naturale este comutativă), adică înmulţirea numerelor întregi este comutativă.

Deoarece $\alpha[1, 0]=[x, y][1, 0]=[x, y]=\alpha$, deducem că elementul neutru pentru înmulțirea numerelor întregi este $[1, 0]$.

Să arătăm acum că înmulțirea numerelor întregi este distributivă față de adunarea numerelor întregi .

Într – adevăr,

$\alpha(\alpha'+\alpha'')=[x, y][x'+x'' , y'+y'']$

$=[x (x'+x'')+y(y'+y''),\ x(y'+y'')+y (x'+x'')]$

$=[xx'+xx''+yy'+yy'', xy'+xy''+yx'+yx'']$ iar

$\alpha\alpha'+\alpha\alpha''=[x, y][x',y']+[x, y] [x'', y'']$

$=[xx'+yy', xy'+yx']+[xx''+yy'', xy''+yx'']$

$=[xx'+yy'+xx''+yy'',\ xy'+yx'+xy''+yx'']$ de unde se observă că $\alpha(\alpha'+\alpha'')=\alpha\alpha'+\alpha\alpha''$.

Am probat până acum că $(\mathbb{Z}, +, \cdot)$ este un inel comutativ unitar. Pentru a arăta că inelul $\mathbb{Z}$ nu are divizori ai lui zero, fie $\alpha\alpha'=0=[0, 0]$ cu $\alpha\neq 0$. Atunci $xx'+yy'=xy'+x'y$, de unde $(x-y)(x'-y')=0$. Cum $\alpha\neq 0$ (adică $x-y\neq 0$) rezută că $(x'-y')=0 \Leftrightarrow x'=y' \Leftrightarrow \alpha'=0$. ■

§3 Relația de ordine naturală de pe $\mathbb{Z}$.

DEFINIŢIA 3.1. Pentru $x, y\in\mathbb{Z}$ definim relația $x\leq y$ prin $x\leq y \Leftrightarrow y-x\in\mathbb{N}$.

TEOREMA 3.2. Dubletul $(\mathbb{Z}, \leq)$ este mulțime total ordonată.

Demonstrație Fie $x, y, z\in\mathbb{Z}$; deoarece $x-x=0\in\mathbb{N}$ deducem că $x\leq x$.

Dacă $x\leq y$ şi $y\leq x$ atunci există $m, n\in\mathbb{N}$ a.î. $y-x=m$ şi $x-y=n$, de unde $m+n=0$ şi deci $m=n=0$, adică $x=y$.

Dacă $x\leq y$ şi $y\leq z$, atunci există $m, n\in\mathbb{N}$ a.î. $x+m=y$ şi $y+n=z$. Cum $x+(m+n)=z$ deducem că $x\leq z$, adică $(\mathbb{Z}, \leq)$ este o mulțime ordonată. Faptul că ordonarea de pe $\mathbb{Z}$ este totală rezultă din aceea că $\mathbb{Z}=(-\mathbb{N}^*)\cup\mathbb{N}$ iar $(-\mathbb{N}^*)\cap\mathbb{N}=\emptyset$. ■

Observație Din felul în care am definit relația de ordine $\leq$ pe $\mathbb{Z}$ deducem că $\mathbb{N}=\{x\in\mathbb{Z} : x\geq 0\}$ iar $-\mathbb{N}=\{x\in\mathbb{Z} : x\leq 0\}$.

PROPOZIŢIA 3.3. Fie $x, y, z\in\mathbb{Z}$ a.î. $x\leq y$.

Atunci i) $-y \leq -x$

ii) dacă $z \geq 0$ atunci $xz \leq yz$

iii) dacă $z \leq 0$ atunci $xz \geq yz$.

Demonstrație

i) Din $x \leq y$ deducem că $y-x \in \mathbb{N}$ şi cum $(-x)-(-y)=y-x \in \mathbb{N}$ rezultă că $-y \leq -x$.

ii) Cum $y-x \in \mathbb{N}$ şi $z \in \mathbb{N}$ avem $(y-x)z \in \mathbb{N}$ adică $yz-xz \in \mathbb{N}$, deci $xz \leq yz$.

iii) Cum $-z \in \mathbb{N}$ şi $y-x \in \mathbb{N}$ deducem că şi $(y-x)(-z) \in \mathbb{N}$ iar cum $(y-x)(-z)=xz-yz \in \mathbb{N}$ rezultă că $xz \geq yz$. ■

CAPITOLUL 3:
CORPUL NUMERELOR RAȚIONALE $\mathbb{Q}$.

§1 Construcția corpului $\mathbb{Q}$ al numerelor raționale

Şi în cazul construcției corpului $\mathbb{Q}$ al numerelor raționale vom adopta tehnica folosită în cazul construcției inelului $\mathbb{Z}$ al numerelor întregi. (în sensul că vom prezenta chestiunea într-un context mai general, urmând ca printr-o particularizare la cazul domeniului de integritate $(\mathbb{Z}, +, \cdot)$ să obținem corpul $\mathbb{Q}$).

Fie $(A, +, \cdot)$ un domeniu de integritate (adică un inel unitar şi comutativ fără divizori ai lui zero) .

DEFINIȚIA 1.1. Numim sistem multiplicativ în A, orice submulțime $S \subseteq A$ a.î. $0 \notin S$, $1 \in S$, iar dacă $x, y \in S$ atunci şi $x \cdot y \in S$.

Exemple

1. $S=A^*=A\setminus\{0\}$ este un sistem multiplicativ al lui A.

2. Dacă $\wp \subset A$ este un ideal prim, atunci $S_\wp = A\setminus\wp$ este de asemenea un sistem multiplicativ al lui A.

3. Dacă $a \in A$, $a \neq 0, 1$, atunci $S_a=\{a^k : k \in \mathbb{Z}\}$ este un sistem multiplicativ al lui A.

Pentru un sistem multiplicativ $S \subseteq A$ să considerăm mulțimea $A \times S=\{(a, s) | a \in A, s \in S\}$ iar pe aceasta relația binară definită prin $(a,s) \sim (a', s') \overset{def}{\Leftrightarrow} as'=a's$. Analog ca în cazul Teoremei lui Malțev se demonstrează facil că $\sim$ este o echivalență pe $A \times S$.

Să notăm $A[S^{-1}]=^{A\times S}/_{\sim}$ iar pentru $(a, s)\in A\times S$ vom nota prin $\frac{a}{s}$ clasa sa de echivalență în $A[S^{-1}]$.

<u>LEMA 1.2.</u> Fie $a, b, a', b'\in A$ şi $s, t, s', t'\in S$ a.î. $\frac{a}{s}=\frac{b}{t}$ şi $\frac{a'}{s'}=\frac{b'}{t'}$.

Atunci $\frac{as'+sa'}{ss'}=\frac{bt'+b't}{tt'}$ şi $\frac{aa'}{ss'}=\frac{bb'}{tt'}$.

<u>Demonstraţie</u> Avem că $at=bs$ şi $a't'=b's'$ astfel că $\frac{as'+sa'}{ss'}=\frac{bt'+b't}{tt'}\Leftrightarrow$

$(as'+sa')tt'=(bt'+b't)ss'\Leftrightarrow as'tt'+sa'tt'=bt'ss'+b'tss'\Leftrightarrow ats't'-bss't'=tsb's'-$

$-tsa't'\Leftrightarrow(at-bs)s't'=(b's'-a't')ts$, ceea ce este adevărat (căci $at-bs=b's'-a't'=0$).

Înmulțind membru cu membru egalitățile $at=bs$ şi $a't'=b's'$ obținem că $ata't'=bsb's'\Leftrightarrow\frac{aa'}{ss'}=\frac{bb'}{tt'}$. ■

Ca un corolar al Lemei 1.2. de mai înainte deducem că dacă pentru $\frac{a}{s},\frac{b}{t}\in A[S^{-1}]$ definim $\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}$ şi $\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$, atunci cele două operații sunt corect definite .

<u>PROPOZIŢIA 1.3.</u> $(A[S^{-1}], +, \cdot)$ este inel comutativ unitar în care $\{\frac{a}{s}\mid a, s\in S\}\subseteq U(A[S^{-1}])$ iar $i_S:A\to A[S^{-1}]$, $i_S(a)=\frac{a}{1}$ pentru orice $a\in A$ este un morfism injectiv de inele ce verifică următoarea proprietate de universalitate :

Pentru orice inel comutativ unitar B şi orice morfism de inele $f:A\to B$ a.î. $f(S)\subseteq U(B)$, există un unic morfism de inele $f':A[S^{-1}]\to B$ a.î. $f'\circ i_S=f$, (unde prin U(B) am notat mulțimea elementelor inversabile ale lui B) .

<u>Demonstraţie</u> Deoarece sunt simple calcule într-un inel comutativ, lăsăm pe seama cititorului verificarea faptului că $(A[S^{-1}], +, \cdot)$ este inel comutativ unitar .

Dacă $s\in S$, atunci elementul neutru al lui $A[S^{-1}]$ față de operația de înmulțire este $1=\frac{s}{s}=\frac{1}{1}$ astfel că dacă a, $s\in S$, atunci $\frac{a}{s}\in U(A[S^{-1}])$ iar $\left(\frac{a}{s}\right)^{-1}=\frac{s}{a}$ (deoarece $\frac{a}{s}\cdot\frac{s}{a}=\frac{as}{as}=\frac{1}{1}=1$).

Fie acum B un inel comutativ unitar şi $f:A\to B$ un morfism de inele pentru care $f(S)\subseteq U(B)$.

Pentru $\frac{a}{s}\in A[S^{-1}]$, cu $a\in A$ şi $s\in S$, scriind $\frac{a}{s}=\frac{a}{1}\cdot\frac{1}{s}=\frac{a}{1}\cdot\left(\frac{s}{1}\right)^{-1}=i_S(a)\cdot(i_S(s))^{-1}$, definind $f'\left(\frac{a}{s}\right)=f(a)\circ(f(s))^{-1}$, se verifică imediat că f′ are proprietățile din enunț . ■

Observație

Din Propoziția 1.3. de mai înainte deducem că dacă A este un domeniu de integritate şi $S=A^*=A\setminus\{0\}$, atunci $A[S^{-1}]$ este un corp comutativ, numit *corpul total de fracții al lui A .*

DEFINIȚIA 1.4. Corpul total de fracții al inelului $(\mathbb{Z}, +, \cdot)$ se notează prin $\mathbb{Q}$ şi poartă numele de *corpul numerelor raționale* . Elementele lui $\mathbb{Q}$ se mai numesc şi *fracții.* Dacă $x=\frac{p}{q}\in\mathbb{Q}$ atunci p se numeşte *numărătorul* fracției x iar q *numitorul* său.

Deoarece $i_{\mathbb{Z}}:\mathbb{Z}\to\mathbb{Q}$, $i_{\mathbb{Z}}(a)=\frac{a}{1}$, pentru orice $a\in\mathbb{Z}$ este în particular funcție injectivă, putem să îl privim pe $\mathbb{Z}$ ca o submulțime a lui $\mathbb{Q}$, adică $\mathbb{Z}\subseteq\mathbb{Q}$. Prin urmare, $\mathbb{N}\subseteq\mathbb{Z}\subseteq\mathbb{Q}$.

§2 Relația de ordine naturală de pe $\mathbb{Q}$

Fie $x\in\mathbb{Q}$, adică $x=\frac{p}{q}$ cu $p\in\mathbb{Z}$ iar $q\in\mathbb{Z}^*$.

Dacă $q<0$, atunci $-q>0$ şi cum $x=\frac{p}{q}=\frac{-p}{-q}$ putem presupune că orice număr $x\in\mathbb{Q}$ se scrie sub forma $x=\frac{p}{q}$, cu $q>0$ (adică $q\in\mathbb{N}^*$).

DEFINIȚIA 2.1. **Fie x, y$\in\mathbb{Q}$, x $=\frac{p}{q}$, y $=\frac{r}{s}$ cu q, s$\in\mathbb{N}$*. Vom defini pe $\mathbb{Q}$ relația $\leq$ prin x$\leq$y $\Leftrightarrow$ps-qr $\leq$0.**

PROPOZIȚIA 2.2. **($\mathbb{Q}$, $\leq$) este o mulțime total ordonată** .

Demonstrație Reflexivitatea este imediată. Pentru antisimetrie, să presupunem că x$\leq$y și y$\leq$x. Atunci ps-qr $\leq$0 și qr-ps $\leq$0, de unde ps-qr=0, adică ps=qr deci x=y.

Pentru tranzitivitate, să mai alegem z=$\frac{t}{u}$ cu u$\in\mathbb{N}$* a.î. x$\leq$y și y$\leq$z, adică ps-qr $\leq$0 și ur-st $\leq$0.

Cum q, s, u$\in\mathbb{N}$* deducem că (ps-qr)u$\leq$0 și (ur-st)q$\leq$0, adică pus-qru$\leq$0 și qru-stq $\leq$0, de unde pus-stq $\leq$0$\Leftrightarrow$s(pu-tq)$\leq$0, adică pu - tq $\leq$0, deci x$\leq$z . ■

Faptul că ordinea $\leq$ de pe $\mathbb{Q}$ este totală rezultă din aceea că ordinea naturală $\leq$ de pe $\mathbb{Z}$ este totală .

Observație Relația de ordine $\leq$ de pe $\mathbb{Q}$ definită mai înainte poartă numele de *ordinea naturală de pe $\mathbb{Q}$.*

În continuare vom nota $\mathbb{Q}_+$={x$\in\mathbb{Q}$ | x$\geq$0} iar prin $\mathbb{Q}_+$*={x$\in\mathbb{Q}$ | x>0}.

CAPITOLUL 4:
CORPUL NUMERELOR REALE $\mathbb{R}$

§1.Inele ordonate

Relațiile de ordine de pe inelul $\mathbb{Z}$ şi corpul $\mathbb{Q}$ se înscriu într-un context mai general pe care îl vom prezenta în cele ce urmează şi care ne va fi de folos şi pentru ordinea naturală de pe mulțimea numerelor reale $\mathbb{R}$.

DEFINITIA 1.1. Dacă A este un domeniu de integritate (adică un inel comutativ unitar fără divizori ai lui zero), prin *ordonare* pe A înțelegem o submulțime nevidă $P \subseteq A$ a.î. :

Ord 1: Pentru orice $x \in A$ avem în mod exclusiv $x \in P$ sau $x = 0$ sau $-x \in P$.

Ord 2: Dacă $x, y \in P$ atunci $x+y, xy \in P$.

În acest caz vom spune că inelul A este *ordonat de P* iar *P este mulțimea elementelor pozitive ale lui A.*

Să presupunem acum că A este ordonat de P. Cum $1 \neq 0$ şi $1 = 1^2 = (-1)^2$ deducem că $1 \in P$ (adică 1 este pozitiv).

Ținând cont de **Ord 2** deducem inductiv că pentru orice $n \in \mathbb{N}^*$, $\underbrace{1+1+...+1}_{de\ n\ ori}$ este pozitiv.

Un element $x \in A$, $x \neq 0$, $x \notin P$ (adică $-x \in P$) se zice *negativ* .

Dacă $x, y \in A$ sunt negative, atunci xy este pozitiv (căci $-x, -y \in P$ iar $(-x)(-y) = xy \in P$).

Analog deducem că dacă x este negativ iar y este pozitiv, atunci xy este negativ şi că pentru orice $x \neq 0$ din A, x^2 este pozitiv.

Dacă A este corp, cum pentru $x \neq 0$ pozitiv avem $xx^{-1} = 1$ deducem că şi x^{-1} este pozitiv**.**

Fie acum $A' \subseteq A$ un subinel iar $P' = P \cap A'$. Se verifică imediat că A' este ordonat de P' (P'se va numi *ordonarea indusă* de P pe A') .

Mai general, fie A', A două inele ordonate iar P', P respectiv mulțimile elementelor pozitive din A' şi A .

Dacă $f:A' \to A$ este un morfism injectiv de inele, vom spune că f *păstrează* *ordinea* dacă pentru orice $x \in P'$ deducem că $f(x) \in P$ (echivalent cu a zice că $P' \subseteq f^{-1}(P)$).

Fie acum $x, y \in A$. Definim $x < y$ (sau $y > x$) prin $y-x \in P$.

Astfel $x > 0$ înseamnă $x \in P$ iar $x < 0$ înseamnă că $-x \in P$ (spunem atunci că x este *negativ*).

Se verifică imediat că dacă $x, y, z \in A$, atunci :

IN_1: Dacă $x < y$ şi $y < z$, atunci $x < z$.

IN_2: Dacă $x < y$ şi $z > 0$, atunci $xz < yz$.

IN_3: Dacă $x < y$ atunci $x+z < y+z$.

IN_4: Dacă A este corp, $x > 0$, $y > 0$ şi $x < y$ atunci $y^{-1} < x^{-1}$.

Dacă $x, y \in A$ definim $x \leq y$ prin $x < y$ sau $x = y$. Fie acum A un domeniu de integritate ordonat de P iar K corpul său total de fracţii.

Dacă $P_K = \{ \frac{a}{b} \in K \mid a, b > 0 \}$, atunci P_K defineşte o ordonare pe K.

Într-adevăr, dacă $x \in K$, $x \neq 0$, $x = \frac{a}{b}$ atunci putem presupune că $b > 0$ (deoarece $x = \frac{a}{b} = \frac{-a}{-b}$). Dacă $a > 0$, atunci $x \in P_K$. Dacă $-a > 0$ atunci $-x = \frac{-a}{b} \in P_K$.

Nu putem avea simultan $x, -x \in P_K$ căci scriind $x = \frac{a}{b}$ şi $-x = \frac{c}{d}$, cu a, b, c, $d \in A$ şi a, b, c, $d > 0$, atunci $-\frac{a}{b} = \frac{c}{d}$ deci $-(ad) = bc$, absurd (căci $bc \in P$ şi $ad \in P$). Deci P_K satisface **Ord 1.**

Cum $xy = \frac{ac}{bd}$ (iar $ac, bd > 0$) şi $x+y = \frac{ad+bc}{bc}$ (iar $ad+bc, bc > 0$) deducem că P_K satisface şi **Ord 2** .

Observaţie Aplicând cele de mai sus lui $\mathbb{Q}$ (care este corpul total de fracţii al domeniului de integritate $\mathbb{Z}$) obţinem de fapt ceea ce am stabilit în legătură cu ordonarea naturală de pe $\mathbb{Q}$ de la Capitolul 3 (evident $\mathbb{N}^*$ este o ordonare pe $\mathbb{Z}$).

Fie acum A un inel ordonat. Pentru $x \in A$ definim :

$$|x| = \begin{cases} x, \text{ dacă } x \geq 0 \\ -x, \text{ dacă } x < 0 \end{cases}$$

($|x|$ poartă numele de *valoarea absolută* sau *modulul* lui x).

LEMA 1.2. Pentru orice $x \in A$, $|x|$ este unicul element $z \in A$ a.î. $z \geq 0$ şi $z^2 = x^2$.

Demonstraţie Să observăm că $|x|^2 = x^2$ şi $|x| \geq 0$ pentru orice $x \in A$. Pe de altă parte, dacă $a \in A$ şi $a > 0$ atunci există cel mult două elemente $z \in A$ a.î. $z^2 = a$ (căci polinomul $t^2 - a \in A[X]$ are cel mult două rădăcini). Dacă $w^2 = a$, atunci $w \neq 0$ şi $(-w)^2 = w^2 = a$, deci există cel mult un $z \in A$ pozitiv a.î. $z^2 = a$ şi cu aceasta lema este probată . ■

DEFINIŢIA 1.3. Pentru $a \geq 0$, definim elementul $\sqrt{a}$ ca fiind acel element $z \geq 0$ a.î. $z^2 = a$ (evident, dacă un astfel de z există !).

Se verifică acum uşor că dacă pentru a, b ≥ 0, $\sqrt{a}, \sqrt{b}$ există, atunci $\sqrt{ab}$ există şi $\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$.

Evident, pentru orice $x \in A$, $|x| = \sqrt{x^2}$.

LEMA 1.4. Dacă A este un inel ordonat, atunci

VA_1: Pentru orice $x \in A$, $|x| \geq 0$, iar $|x| > 0$ dacă $x \neq 0$

VA_2 : Pentru orice $x, y \in A$, $|xy| = |x| \cdot |y|$

VA_3 : Pentru orice $x, y \in A$, $|x+y| \leq |x| + |y|$.

Demonstraţie Cum VA_1 şi VA_2 sunt imediate, să probăm pe VA_3 :

$|x+y|^2 = (x+y)^2 = x^2 + 2xy + y^2 \leq |x|^2 + 2|xy| + |y|^2 = |x|^2 + 2|x| \cdot |y| + |y|^2 =$

$= (|x| + |y|)^2$, de unde $|x + y| \leq |x| + |y|$. ■

Fie acum K un corp comutativ ordonat pentru care există un morfism (injectiv) de corpuri $f : \mathbb{Q} \to K$ (deci K va fi de caracteristică 0).

Se arată imediat că dacă $x \in \mathbb{Z}$, atunci

$$f(x) = \begin{cases} \underbrace{1_K + \ldots + 1_K}_{de\ x\ ori}, & \text{dacă } x \geq 0 \\ 0, & \text{dacă } x = 0 \\ \underbrace{(-1_K) + \ldots + (-1_K)}_{de\ -x\ ori}, & \text{dacă } x < 0 \end{cases}$$

Mai mult, dacă $x \in \mathbb{Z}^*$, cum în $\mathbb{Q}$ avem $x \cdot \frac{1}{x} = 1$ deducem că $1_K = f(1) = f\left(x \cdot \frac{1}{x}\right) = f(x) \cdot f\left(\frac{1}{x}\right)$, de unde $f\left(\frac{1}{x}\right) = f(x)^{-1}$ în K. Atunci dacă $x = \frac{m}{n} \in \mathbb{Q}$ avem $f(x) = f\left(\frac{m}{n}\right) = f\left(m \cdot \frac{1}{n}\right) = m \cdot f\left(\frac{1}{n}\right) = m \cdot (n \cdot 1_K)^{-1}$. Rezultă că f este unic determinat ; vom identifica atunci pe $\mathbb{Q}$ cu un subcorp al lui K (f se va numi scufundarea canonică a lui $\mathbb{Q}$ în K).

Dacă $x = \frac{m}{n}$, $y = \frac{m'}{n'} \in \mathbb{Q}$ (cu n, n′>0) şi x≤y, atunci mn′-m′n≤0, deci m′n-mn′≥0, iar $f(x) = m(n1_K)^{-1}$, $f(y) = m'(n'1_K)^{-1}$. Din m′n-mn′≥0 şi $1_K \geq 0$ deducem că $(m'n-mn')1_K \geq 0 \Leftrightarrow m'(n1_K) - m(n'1_K) \geq 0 \Leftrightarrow m'(n1_K) \geq m(n'1_K)$, de unde $m'(n'1_K)^{-1} \geq m(n\,1_K)^{-1} \Leftrightarrow f(y) \geq f(x)$.

Obţinem astfel următorul rezultat :

<u>TEOREMA 1.5.</u> Dacă K este un corp ordonat de caracteristică 0, atunci scufundarea canonică a lui $\mathbb{Q}$ în K, f :$\mathbb{Q} \to$K, $f\left(\frac{m}{n}\right) = m \cdot (n \cdot 1_K)^{-1}$, (cu n>0) păstrează ordinea.

În continuare prin K vom desemna un corp comutativ ordonat de caracteristică 0 iar un element $x \in \mathbb{Z}$ îl vom identifica cu $f(x) = x \cdot 1_K$.

DEFINIŢIA 1.6. **Un şir de elemente $(x_n)_{n\geq 0}$ din K se zice şir *Cauchy* dacă pentru orice $\varepsilon\in K$, $\varepsilon>0$, există $n_\varepsilon\in\mathbb{N}$ a.î. pentru orice m, $n\in\mathbb{N}$, $m, n\geq n_\varepsilon$ să avem $|x_n - x_m|<\varepsilon$.**

Vom spune despre şirul $(x_n)_{n\geq 0}$ că este *convergent* la un element $x\in K$, dacă pentru orice $\varepsilon\in K$, $\varepsilon>0$, există $n_\varepsilon\in\mathbb{N}$ a.î. pentru orice $n\geq n_\varepsilon$ să avem $|x_n - x|<\varepsilon$.

Observaţii

1.Să presupunem că şirul $(x_n)_{n\geq 0}$ este convergent la două elemente $x,y\in K$. Atunci pentru $\varepsilon\in K$, $\varepsilon>0$ şi $n\in\mathbb{N}^*$ suficient de mare avem :

$$|x-y| \leq |x-x_n+x_n-y| \leq |x-x_n| + |x_n-y| \leq 2\varepsilon$$

iar cum ε este oarecare deducem că $|x-y|=0$ (căci dacă $|x-y|\neq 0$, atunci $|x-y|>0$ şi am avea $|x-y|<|x-y|$, absurd !).

Dacă $(x_n)_{n\geq 0}$ este convergent la un element $x\in K$, vom scrie

$$x=\lim_{n\to\infty} x_n .$$

2. Orice şir convergent este şir Cauchy.

DEFINIŢIA 1.7. **Corpul ordonat K în care orice şir Cauchy este convergent se zice *complet* .**

DEFINIŢIA 1.8. **Corpul ordonat K se numeşte *arhimedean* dacă pentru orice $x\in K$, există $n\in\mathbb{N}$ a.î. $x \leq n\cdot 1_K$.**

TEOREMA 1.9. **Corpul $\mathbb{Q}$ al numerelor raţionale nu este complet .**

Demonstraţie Într-adevăr, să considerăm şirul $(x_n)_{n\geq 0}$ de numere raţionale dat prin $x_0=1$ şi $x_{n+1}=\dfrac{4+3x_n}{3+2x_n}$ pentru orice $n\geq 0$. Prin inducţie matematică relativă la n se probează că $x_n^2<2$, şi că $(x_n)_{n\geq 0}$ este crescător (căci $x_{n+1}-x_n=\dfrac{4+3x_n}{3+2x_n}-x_n=\dfrac{2\left(2-x_n^{\,2}\right)}{3+2x_n}>0$) iar de aici că el este şir Cauchy.

Dacă acest şir ar avea limita $l\in\mathbb{Q}$, atunci cu necesitate $l=\dfrac{4+3l}{3+2l}$, de unde $l^2=2$, absurd căci $l\notin\mathbb{Q}$. Deci $(x_n)_{n\geq 0}$ nu are limită în $\mathbb{Q}$, adică corpul $\mathbb{Q}$ nu este complet. ■

Pentru K corp ordonat şi $S \subseteq K$, prin *majorant* al lui S în K înţelegem un element $z \in K$ a.î. $x \leq z$, pentru orice $x \in S$.

Prin marginea superioară a lui S, notată prin sup(S) înţelegem cel mai mic majorant al lui S din K (evident dacă acesta există).

TEOREMA 1.10. Fie K un corp arhimedean complet. Atunci orice submulţime nevidă S a lui K ce admite un majorant are margine superioară.

Demonstraţie Pentru $n \in \mathbb{N}$, fie

$$T_n = \{y \in \mathbb{Z} \mid nx \leq y \text{ pentru orice } x \in S\}.$$

Atunci T_n este mărginită de orice element de forma nx cu $x \in S$ şi este nevidă deoarece dacă b este un majorant al lui S, atunci orice întreg y a.î. $nb \leq y$ este în T_n (deoarece K este arhimedean) .

Fie y_n cel mai mic element al lui T_n .Atunci există $x_n \in S$ a.î. $y_n - 1 < nx_n \leq y_n$, de unde $\frac{y_n}{n} - \frac{1}{n} < x_n \leq \frac{y_n}{n}$.

Să notăm $z_n = \frac{y_n}{n}$ şi să demonstrăm că şirul $(z_n)_{n \in \mathbb{N}}$ este Cauchy.

Pentru aceasta fie m, $n \in \mathbb{N}$ a.î. $\frac{y_n}{n} \leq \frac{y_m}{m}$ atunci $\frac{y_m}{m} - \frac{1}{m} < \frac{y_n}{n} \leq \frac{y_m}{m}$ căci în caz contrar, $\frac{y_n}{n} \leq \frac{y_m}{m} - \frac{1}{m}$, deci $\frac{y_m}{m} - \frac{1}{n}$ este majorant pentru S, ceea ce este absurd căci x_m este mai mare.

Atunci $\left| \frac{y_n}{n} - \frac{y_m}{m} \right| \leq \frac{1}{n}$ de unde deducem că $(z_n)_{n \in \mathbb{N}}$ este Cauchy.

Fie $w = \lim_{n \to \infty} z_n$ şi să demonstrăm la început că w este un majorant pentru S.

Să presupunem prin absurd că există $x \in S$ a.î. $w < x$. Există atunci $n \in \mathbb{N}$ a.î. $| z_n - w | \leq \frac{x - w}{2}$ astfel că $x - z_n = x - w + w - z_n \geq x - w - | w - z_n | \geq$

$\geq x - w - \frac{x - w}{2} \geq \frac{x - w}{2} > 0$ deci $x > z_n$ contrazicând faptul că z_n este majorant al lui S.

Să demonstrăm acum că $w = \sup S$.

Fie u<w; atunci există n∈ℕ suficient de mare a.î. $|z_n - x_n| \le \frac{1}{4} < \frac{w-u}{4}$.

Putem alege n suficient de mare a.î. $|z_n - w| \le \frac{w-u}{4}$ căci $\lim_{n\to\infty} z_n = w$.

Astfel, $x_n - u = w-u+x_n-z_n+z_n-w \ge w-u-|x_n-z_n|-|z_n-w| \ge$

$\ge w-u-\frac{w-u}{4}-\frac{w-u}{4} \ge \frac{w-u}{4} > 0$, deci u<$x_n$ (adică u nu este majorant– absurd !). ■

§2 Construcţia corpului ℝ al numerelor reale

Vom prezenta construcţia corpului numerelor reale cu ajutorul şirurilor Cauchy de numere raţionale (definite mai înainte într-un context mai general).

DEFINIŢIA 2.1. Un şir de numere raţionale $\gamma=(c_n)_{n\ge0}$ se zice şir *nul* dacă pentru orice ε∈ℚ, ε>0, există n_0∈ℕ a.î. pentru orice n≥n_0, $|c_n| \le \varepsilon$

Dacă $\alpha=(a_n)_{n\ge0}$ şi $\beta=(b_n)_{n\ge0}$ sunt două şiruri de numere raţionale, definim suma şi produsul lor prin $\alpha+\beta=(a_n+b_n)_{n\ge0}$ şi respectiv $\alpha\beta=(a_nb_n)_{n\ge0}$

LEMA 2.2. Orice şir Cauchy $\alpha=(a_n)_{n\ge0}$ de numere raţionale este mărginit.

Demonstraţie Există k∈ℕ a.î. pentru orice n ≥ k , $|a_n - a_k| \le 1$, de unde $|a_n| \le |a_k|+1$. Alegând M=max ($|a_0|, \ldots, |a_{k-1}|, |a_k|+1$) deducem că $|a_n| \le M$ pentru orice n∈ℕ. ■

În cele ce urmează prin **C(ℚ)** vom nota mulţimea şirurilor Cauchy de numere raţionale.

PROPOZIŢIA 2.3. (C(ℚ), +, ·) este inel unitar comutativ.

Demonstraţie Fie $\alpha=(x_n)_{n\ge0}$, $\beta=(y_n)_{n\ge0}$, **0**=(0, 0, …) şi **1**=(1, 1, …). Să demonstrăm la început că α+β şi αβ sunt din **C(ℚ).**

Pentru ε∈$\mathbb{Q}_+$*, există n_ε', n_ε''∈ℕ a.î. pentru orice m, n ≥ n_ε' să avem $|x_m-x_n| < \frac{\varepsilon}{2}$ şi pentru orice m, n ≥ n_ε'', $|y_m-y_n| < \frac{\varepsilon}{2}$. Alegând n_ε=max (n_ε', n_ε''),

deducem că pentru orice m, n $\geq n_\varepsilon$, $|x_m-x_n|$, $|y_m-y_n| < \frac{\varepsilon}{2}$, astfel că $|(x_m+y_m)-(x_n+y_n)| = |(x_m-x_n)+(y_m-y_n)| \leq |x_m-x_n|+|y_m-y_n| < \frac{\varepsilon}{2}+\frac{\varepsilon}{2} = \varepsilon$, adică $\alpha+\beta \in \mathbf{C}(\mathbb{Q})$.

Pentru cazul produsului $\alpha\beta$ vom ține cont de Propoziția 1.2. Conform acesteia, există $M_1, M_2 \in \mathbb{Q}_+^*$ a.î. $|x_n| \leq M_1$ și $|y_n| \leq M_2$ pentru orice $n \in \mathbb{N}$.

Notând $M = \max(M_1, M_2)$ și alegând $\varepsilon \in \mathbb{Q}_+^*$, există $n_\varepsilon', n_\varepsilon'' \in \mathbb{N}$ a.î.

$$|x_m - x_n| \leq \frac{\varepsilon}{2M}, \text{ pentru } m, n \geq n_\varepsilon' \text{ și}$$

$$|y_m - y_n| \leq \frac{\varepsilon}{2M}, \text{ pentru } m, n \geq n_\varepsilon''.$$

Astfel, pentru $m, n \geq n_\varepsilon = \max(n_\varepsilon', n_\varepsilon'')$, avem

$$|x_m y_m - x_n y_n| = |x_m(y_m-y_n) + y_n(x_m-x_n)| = |x_m||y_m-y_n| + |y_n||x_m-x_n| \leq$$

$$\leq M \cdot \frac{\varepsilon}{2M} + M \cdot \frac{\varepsilon}{2M} = \varepsilon, \text{ adică și } \alpha\beta \in \mathbf{C}(\mathbb{Q}).$$

În mod evident, $-\alpha = (-x_n)_{n\geq 0} \in \mathbf{C}(\mathbb{Q})$ ca și $\mathbf{0}, \mathbf{1} \in \mathbf{C}(\mathbb{Q})$.

Deducem acum imediat că $(\mathbf{C}(\mathbb{Q}), +, \cdot)$ este inel comutativ și unitar. ■

În continuare, vom nota prin

$$\mathbf{N}(\mathbb{Q}) = \{(x_n)_{n\geq 0} \in \mathbf{C}(\mathbb{Q}) \mid \lim_{n\to\infty} x_n = 0\}.$$

(convenim să numim elementele lui $\mathbf{N}(\mathbb{Q})$ *șiruri nule*).

LEMA 2.4 $\mathbf{N}(\mathbb{Q})$ **este ideal al inelului** $\mathbf{C}(\mathbb{Q})$.

Demonstrație Analog ca în cazul sumei din propoziția precedentă, se demonstrează imediat că dacă $\alpha, \beta \in \mathbf{N}(\mathbb{Q})$, atunci $\alpha-\beta \in \mathbf{N}(\mathbb{Q})$.

Fie acum $\alpha = (a_n)_{n\geq 0} \in \mathbf{C}(\mathbb{Q})$ și $\beta = (b_n)_{n\geq 0} \in \mathbf{N}(\mathbb{Q})$. Conform Lemei 2.2. există $M \in \mathbb{Q}_+^*$ a.î. $|a_n| \leq M$ pentru orice $n \in \mathbb{N}$.

Deoarece $\beta = (b_n)_{n\geq 0} \in \mathbf{N}(\mathbb{Q})$ pentru $\varepsilon \in \mathbb{Q}_+^*$, există $n_\varepsilon \in \mathbb{N}$ a.î. pentru orice $n \geq n_\varepsilon$ să avem $|b_n| \leq \frac{\varepsilon}{M}$.

Atunci pentru $n \geq n_\varepsilon$, $|a_n b_n| = |a_n||b_n| \leq M \cdot \frac{\varepsilon}{M} = \varepsilon$, astfel că $\alpha\beta \in \mathbf{N}(\mathbb{Q})$, adică $\mathbf{N}(\mathbb{Q})$ este ideal al inelului comutativ $\mathbf{C}(\mathbb{Q})$. ■

LEMA 2.5. **Fie $\alpha \in C(\mathbb{Q})$ a.î. $\alpha \notin N(\mathbb{Q})$, $\alpha=(a_n)_{n\geq 0}$. Atunci există $c\in\mathbb{Q}_+^*$ şi $n_0\in\mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \geq c$.**

Demonstraţie Dacă prin absurd lema nu ar fi adevărată, atunci pentru $\varepsilon\in\mathbb{Q}_+^*$ există o infinitate de numere naturale $n_1<n_2<\ldots$ a.î. $|a_{n_i}|<\frac{\varepsilon}{3}$ pentru orice $i \geq 1$.

Cum $\alpha\in C(\mathbb{Q})$, există $p\in\mathbb{N}$ a.î. pentru orice m, n≥p să avem $|a_n - a_m|\leq\frac{\varepsilon}{3}$. Fie $n_i \geq p$; atunci pentru orice m ≥p, $|a_m| \leq |a_m - a_{n_i}| + |a_{n_i}| \leq \frac{2\varepsilon}{3}$ şi pentru orice m, n≥p, $|a_n| \leq |a_n - a_m| + |a_m| \leq \frac{\varepsilon}{3}+\frac{2\varepsilon}{3}=\varepsilon$, adică $\alpha\in N(\mathbb{Q})$, absurd ! . ■

TEOREMA 2.5. **$(C(\mathbb{Q}) / N(\mathbb{Q}) , +, \cdot)$ este corp comutativ.**

Demonstraţie Faptul că $C(\mathbb{Q}) / N(\mathbb{Q})$ este inel comutativ rezultă din aceea că $C(\mathbb{Q})$ este inel comutativ iar $N(\mathbb{Q})$ este ideal în $C(\mathbb{Q})$.

Fie acum $\alpha\in C(\mathbb{Q})$ a.î. $\alpha\notin N(\mathbb{Q})$ şi $\overline{\alpha}=\alpha+N(\mathbb{Q})\in C(\mathbb{Q}) / N(\mathbb{Q})$. Vom demonstra că există $\overline{\beta}\in C(\mathbb{Q})/N(\mathbb{Q})$ a.î. $\overline{\alpha}\cdot\overline{\beta}=\overline{1}$, unde $\overline{1}=\mathbf{1}+N(\mathbb{Q})$ (reamintim că $\mathbf{1}=(1, 1, \ldots)\in C(\mathbb{Q})$).

Cum $\alpha\notin N(\mathbb{Q})$, conform Lemei 2.4. există $\varepsilon\in\mathbb{Q}_+^*$ şi $n_0\in\mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \geq \varepsilon$. În particular, deducem că pentru $n \geq n_0$, $a_n\neq 0$.

Fie $\beta=(b_n)_{n\geq 0}$ cu

$$b_n = \begin{cases} 1 \text{ dacă } 0 \leq n \leq n_0 \\ a_n^{-1} \text{ dacă } n \geq n_0 \end{cases}$$

Să arătăm că $\beta\in C(\mathbb{Q})$ şi că $\overline{\alpha}\cdot\overline{\beta}=\overline{1}$.

Putem alege deci $c\in\mathbb{Q}_+^*$ şi $n_0\in\mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \geq c>0$; de unde va rezulta că $\frac{1}{|a_n|}\leq\frac{1}{c}$.

Pentru $\varepsilon\in\mathbb{Q}_+^*$ există $p \geq n_0$ a.î. pentru orice m, $n \geq p$ să avem

$$|a_n - a_m| \leq \varepsilon c^2 .$$

Atunci pentru orice m, n $\geq$ p avem $\left|\frac{1}{a_n}-\frac{1}{a_m}\right|=\left|\frac{a_m-a_n}{a_m\cdot a_n}\right|\leq\frac{\varepsilon\cdot c^2}{c^2}=\varepsilon$,

adică $\beta\in\mathbf{C}(\mathbb{Q})$**.**

Cum $\alpha\beta$ diferă de **1** numai într-un număr finit de termeni (eventual pentru $n\leq n_0$) deducem că $\alpha\beta$-**1**$\in\mathbf{N}(\mathbb{Q})$**,** adică $\overline{\alpha}\cdot\overline{\beta}=\overline{1}$, deci $\overline{\beta}=\left(\overline{\alpha}\right)^{-1}$, adică **C(**$\mathbb{Q}$**) / N(**$\mathbb{Q}$**)** este corp . ■

<u>DEFINIŢIA 2.6.</u> Mulţimea C($\mathbb{Q}$**) / N(**$\mathbb{Q}$**) se notează prin** $\mathbb{R}$ **şi poartă numele de <u>mulţimea numerelor reale.</u>**

Corpul ($\mathbb{R}$**,+, ·) poartă numele de <u>corpul numerelor reale.</u>**

<u>Observaţie</u> Deoarece se probează imediat că funcţia $i_Q:\mathbb{Q}\to\mathbb{R}$, $i_Q(a)=\overline{(a,a,....)}$ pentru orice a $\in\mathbb{Q}$ este morfism de corpuri (deci în particular funcţie injectivă) putem privi pe $\mathbb{Q}$ ca subcorp al lui $\mathbb{R}$.

Elementele din $\mathbf{I}=\mathbb{R}\setminus\mathbb{Q}$ se zic *<u>numere iraţionale.</u>*

<u>LEMA 2.7.</u> Pentru $\alpha=(a_n)_{n\geq 0}\in\mathbf{C}(\mathbb{Q})$ **este verificată doar una din condiţiile :**

(1) $\alpha\in\mathbf{N}(\mathbb{Q})$

(2) Există $c\in\mathbb{Q}_+^*$ **a.î. pentru n suficient de mare să avem** $a_n\geq c$

(3) Există $c\in\mathbb{Q}_+^*$ **a.î. pentru n suficient de mare să avem** $a_n\leq -c$

<u>Demonstraţie</u> Evident (2) şi (3) se exclud reciproc.

Să presupunem acum că $\alpha\notin\mathbf{N}(\mathbb{Q})$. Conform Lemei 2.5. există $n_0\in\mathbb{N}$ şi $c\in\mathbb{Q}_+^*$ a.î. pentru orice $n\geq n_0$, $|a_n|\geq c$ astfel că $a_n\geq c$ dacă $a_n>0$ şi $a_n\leq -c$ dacă $a_n<0$.

Să presupunem acum că $a_n>0$ pentru suficient de mulţi n şi $a_m<0$ pentru suficient de mulţi m. Pentru astfel de n şi m avem $a_n-a_m\geq 2c>0$ ceea ce contrazice faptul că $\alpha\in\mathbf{C}(\mathbb{Q})$**.**

Deci (2) sau (3) în sens disjunctiv trebuie să aibă loc . ■

<u>§3 Ordonarea lui</u> $\mathbb{R}$

Fie $P=\{\overline{\alpha}\mid\alpha\in\mathbf{C}(\mathbb{Q})$ şi verifică (2) din Lema 2.7.$\}\subseteq\mathbb{R}$

LEMA 3.1. **P este o ordonare pe $\mathbb{R}$.**

Demonstraţie Conform Lemei 2.7. deducem că P satisface **Ord 1**.

Fie acum $\alpha=(a_n)_{n\geq 0}$ şi $\beta=(b_n)_{n\geq 0} \in \mathbf{C(\mathbb{Q})}$ a.î. $\overline{\alpha}, \overline{\beta} \in P$.

Există $c_1, c_2 \in \mathbb{Q}_+^*$ şi $n_1, n_2 \in \mathbb{N}$ a.î. pentru $n \geq n_1$, $a_n \geq c_1$ şi pentru $n \geq n_2$, $b_n \geq c_2$.

Pentru $n \geq \max(n_1, n_2)$, $a_n+b_n \geq c_1+c_2 >0$ şi $a_n b_n \geq c_1 c_2 >0$ astfel că $\alpha+\beta$, $\alpha\beta$ verifică (2) din Lema 2.7. ,adică $\overline{\alpha}+\overline{\beta}, \overline{\alpha}\cdot\overline{\beta} \in P$, deci P satisface şi **Ord 2**.

Observaţii

1. Din cele de mai sus deducem că dacă $\overline{\alpha}, \overline{\beta} \in \mathbb{R}$, $\alpha=(x_n)_{n\geq 0}$, $\beta=(y_n)_{n\geq 0}$, atunci $\overline{\alpha} \leq \overline{\beta}$ este echivalent cu aceea că $\overline{\beta}$ - $\overline{\alpha} \in P$, adică $\overline{(\beta-\alpha)} \in P$, deci cu existenţa lui $n_0 \in \mathbb{N}$ şi $c \in \mathbb{Q}_+^*$ a.î. y_n-$x_n \geq c$ pentru orice $n \geq n_0$.

Convenim să numim ordinea de mai înainte *ordonarea naturală* de pe $\mathbb{R}$.

2. Pentru $a \in \mathbb{Q}$ convenim să notăm pe $i_{\mathbb{Q}}(a)$ prin $\overline{a}$, adică $\overline{a} = \overline{(a, a, ...)}$.

TEOREMA 3.2. **Ordonarea naturală de pe $\mathbb{R}$ (dată de P) este arhimedeeană**.

Demonstraţie Conform Definiţiei 1.8., pentru $\alpha=(a_n)_{n\geq 0} \in \mathbf{C(\mathbb{Q})}$ va trebui să demonstrăm că există $m_\alpha \in \mathbb{N}$ a.î. $\overline{\alpha} \leq \overline{m_\alpha}$.

Conform Lemei 2.2. există $M \in \mathbb{Q}_+^*$ a.î. $a_n \leq M$ pentru orice $n \in \mathbb{N}$. Alegând $m_\alpha \in \mathbb{N}$ a.î. $M \leq m_\alpha$ deducem că $a_n \leq m_\alpha$ pentru orice $n \in \mathbb{N}$, adică $\overline{\alpha} \leq \overline{m_\alpha}$.

■

Următorul rezultat este imediat.

LEMA 3.3. **Dacă $\alpha=(a_n)_{n\geq 0} \in \mathbf{C(\mathbb{Q})}$ şi există $c \in \mathbb{Q}_+^*$ şi $n_0 \in \mathbb{N}$ a.î. pentru orice $n \geq n_0$, $|a_n| \leq c$, atunci $\left|\overline{\alpha}\right| \leq \overline{c}$.**

Observaţie Conform Teoremei 3.2., fiind dat $\varepsilon \in \mathbb{R}$, $\varepsilon>0$, există $\varepsilon_1 \in \mathbb{Q}_+^*$ a.î. $\varepsilon<\varepsilon_1$ astfel că în definiţia limitei unui şir din $\mathbb{R}$ nu contează dacă ε este real sau raţional.

LEMA 3.4. **Fie $\alpha=(a_n)_{n\geq 0} \in \mathbf{C(\mathbb{Q})}$. Atunci $\overline{\alpha} = \lim_{n\to\infty} \overline{a_n}$ (adică orice şir Cauchy de numere raţionale converge în $\mathbb{R}$).**

Demonstraţie Fie $\varepsilon \in \mathbb{Q}_+^*$. Există $n_0 \in \mathbb{N}$ a.î. pentru orice $m, n \geq n_0$,

$|a_m - a_n| \le \varepsilon$. Atunci pentru $m \ge n_0$ avem $|\overline{\alpha} - \overline{a_m}| = |\overline{\alpha - a_m}| \le \overline{\varepsilon}$ (căci $\alpha - a_m = (a_n - a_m)_{n \ge 0}$), adică $\overline{\alpha} = \lim_{n\to\infty} \overline{a_n}$. ■

TEOREMA 3.5. **Corpul $\mathbb{R}$ este complet .**

Demonstrație Fie $(x_n)_{n\ge 0}$ un şir Cauchy de numere reale.

Conform Lemei 3.4., pentru orice $n \in \mathbb{N}$ găsim $a_n \in \mathbb{Q}$ a.î. $|x_n - \overline{a_n}| < \frac{1}{n}$

(în partea dreaptă este vorba de fapt de $(\overline{n})^{-1}$!)

Cum $(x_n)_{n\ge 0}$ este Cauchy, deducem că fiind dat $\varepsilon > 0$ (de exemplu $\varepsilon \in \mathbb{Q}$) există $n_0 \in \mathbb{N}$ a.î. pentru orice m, $n \ge n_0$ să avem $|x_n - x_m| \le \frac{\varepsilon}{3}$.

Fie $n_1 \in \mathbb{N}$, $n_1 \ge n_0$ a.î. $\frac{1}{n_1} \le \frac{\varepsilon}{3}$. Atunci pentru orice m, $n \ge n_1$ avem

$$\left|\overline{a_n} - \overline{a_m}\right| = \left|\overline{a_n} - x_n + x_n - x_m + x_m - \overline{a_m}\right| \le \left|\overline{a_n} - x_n\right| + \left|x_n - x_m\right| + \left|x_m - \overline{a_n}\right| \le$$

$$\le \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon .$$ Adică $\left(\overline{a_n}\right)_{n\ge 0}$ este şir Cauchy de numere raționale. Conform Lemei 3.4. există $x = \lim_{n\to\infty} \overline{a_n}$ în $\mathbb{R}$. Deoarece pentru n suficient de mare $|x_n - x| \le$

$\le |x_n - \overline{a_n}| + |\overline{a_n} - x|$ deducem că $x = \lim_{n\to\infty} x_n$, adică $\mathbb{R}$ este complet. ■

DEFINIŢIA 3.6. **Un corp ordonat K se zice *complet ordonat* dacă orice parte nevidă minorată a sa are o margine inferioară.**

Observație Fie K un corp complet ordonat şi $A \subset K$, $A \ne \emptyset$, A majorată. Atunci $-A$ este minorată, sup A există şi $\sup(A) = -\inf(-A)$.

LEMA 3.7. **Dacă $x, y \in \mathbb{Q}$, atunci :**

(i) $x \le y \Leftrightarrow i_{\mathbb{Q}}(x) \le i_{\mathbb{Q}}(y)$;

(ii) $x < y \Leftrightarrow i_{\mathbb{Q}}(x) < i_{\mathbb{Q}}(y)$;

(iii) pentru orice $\alpha \in \mathbb{R}$ există $x, y \in \mathbb{Z}$ a.î. $i_Q(x) \le \alpha \le i_Q(y)$.

Demonstrație (i) Să presupunem că $x \le y$, adică $y - x \ge 0$. Cum $i_{\mathbb{Q}}(y) - i_{\mathbb{Q}}(x) = i_{\mathbb{Q}}(y - x)$ deducem că $i_{\mathbb{Q}}(y) \ge i_{\mathbb{Q}}(x) \Leftrightarrow i_{\mathbb{Q}}(x) \le i_{\mathbb{Q}}(y)$.

Reciproc, să presupunem că $i_Q(x) \le i_Q(y)$, adică $i_Q(y-x) \ge 0 \Rightarrow y-x \in P$, deci pentru $\varepsilon>0$ $y-x>\varepsilon>0 \Rightarrow y \ge x \Leftrightarrow x \le y$.

(ii) Rezultă din injectivitatea lui i_Q.

(iii) Fie $\alpha \in \mathbb{R}$ şi $(x_n)_{n\ge 0} \in \alpha$. Atunci $(x_n)_{n\ge 0} \in \mathbf{C}(\mathbb{Q})$, deci pentru $\varepsilon \in \mathbb{Q}_+^*$ există $n_\varepsilon \in \mathbb{N}$ a.î. $|x_n - x_{n_\varepsilon}| < \varepsilon$ pentru orice $n \ge n_\varepsilon$ sau $x_{n_\varepsilon} - \varepsilon < x_n < x_{n_\varepsilon} + \varepsilon$ pentru orice $n \ge n_\varepsilon$.

Luând $x, y \in \mathbb{Z}$ a.î. $x < x_{n_\varepsilon} - \varepsilon$ şi $x_{n_\varepsilon} + \varepsilon < y$ deducem că $x_n - x > 0$ şi $y - x_n > 0$ pentru orice $n \ge n_\varepsilon$ deci

$$(x_n)_{n\ge 0} - (x, x, \ldots) = (x_n - x)_{n\ge 0} \in P \quad \text{şi}$$

$$(y, y, \ldots) - (x_n)_{n\ge 0} = (y - x_n)_{n\ge 0} \in P,$$

adică $i_Q(x) \le \alpha \le i_Q(y)$.

LEMA 3.8. **Fie $\alpha, \beta \in \mathbb{R}$ şi $(u_n)_{n\ge 0}, (v_n)_{n\ge 0} \in \mathbf{C}(\mathbb{Q})$ a.î.**

$$\mathbf{i_{\mathbb{Q}}(u_m) \le \alpha \le \beta \le i_{\mathbb{Q}}(v_m)}$$

pentru orice $m \in \mathbb{N}$ şi $(u_m)_{m\ge 0} - (v_m)_{m\ge 0} \in \mathbf{N}(\mathbb{Q})$. Atunci $\alpha = \beta$.

Demonstraţie Fie $\varepsilon>0$. Există $m_0 \in \mathbb{N}$ a.î. $|v_{m_0} - u_{m_0}| < \frac{\varepsilon}{3}$. Fie acum $(x_n)_{n\ge 0} \in \alpha$ şi $(y_n)_{n\ge 0} \in \beta$. Din condiţia (1) deducem că $i_{\mathbb{Q}}(u_m) \le \alpha$, deci pentru $m = m_0$ avem $(x_n - u_{m_0})_{n\ge 0} \in P$ prin urmare există $n_\varepsilon' \in \mathbb{N}$ a.î. $x_n - u_{m_0} > -\frac{\varepsilon}{3}$ pentru $n \ge n_\varepsilon'$.

Tot din (1) rezultă că $\beta \le i_Q(v_m)$ deci pentru $m = m_0$ avem $(v_{m_0} - y_n)_{n\ge 0} \in P$, adică există $n_\varepsilon'' \in \mathbb{N}$ a.î. $v_{m_0} - y_n > -\frac{\varepsilon}{3}$, pentru orice $n \ge n_\varepsilon''$, de unde $y_n - x_n <$

$$< v_{m_0} + \frac{\varepsilon}{3} - u_{m_0} + \frac{\varepsilon}{3} = v_{m_0} - u_{m_0} + \frac{2\varepsilon}{3} \le \left| v_{m_0} - u_{m_0} \right| + \frac{2\varepsilon}{3} \le \frac{\varepsilon}{3} + \frac{2\varepsilon}{3} = \varepsilon,$$

prin urmare, $y_n - x_n < \varepsilon$ pentru orice $n \ge \max(n_\varepsilon', n_\varepsilon'')$. Dar $\alpha \le \beta$. Atunci $(y_n - x_n)_{n\ge 0} \in P$, deci există $n_\varepsilon''' \in \mathbb{N}$ a.î. $y_n - x_n > -\varepsilon$, pentru orice $n \ge n_\varepsilon'''$.

Atunci $|x_n - y_n| < \varepsilon$ pentru orice $n \ge \max(n_\varepsilon', n_\varepsilon'', n_\varepsilon''')$, de unde $\alpha = \beta$. ■

TEOREMA 3.9. **Corpul $(\mathbb{R}, \le)$ este complet ordonat.**

Demonstrație Fie $A\subset\mathbb{R}$ nevidă și minorată iar A_0 mulțimea minoranților lui A. Cum $A_0\neq\emptyset$, există $\beta\in A_0$ a.î. $\beta\leq\alpha$ pentru orice $\alpha\in A$. Din Lema 3.8., (iii) rezultă existența unui $z\in\mathbb{Z}$ a.î. $i_{\mathbb{Q}}(z)\leq\beta$, adică $i_{\mathbb{Q}}(z)\in A_0$.

Fie $x_0=\max\{z\in\mathbb{Z} \mid i_Q(z)\in A_0\}$; atunci $i_{\mathbb{Q}}(x_0)\in A_0$ și $i_{\mathbb{Q}}(x_0+1)\notin A_0$. Presupunem că am obținut un $x_k\in\mathbb{Q}$ $(k\geq 0)$ a.î. $i_{\mathbb{Q}}(x_k)\in A_0$ și $i_{\mathbb{Q}}(x_k+\frac{1}{10^k})\notin A_0$

Notând $n_k=\max\{0\leq n\leq 9 \mid i_{\mathbb{Q}}(x_k)+\frac{n}{10^{k+1}}\in A_0\}$ și $x_{k+1}=x_k+\frac{n_k}{10^{k+1}}$ se obține, prin inducție, un șir $(x_k)_{k\geq 0}\in\mathbb{Q}$ a.î.

(1) $i_{\mathbb{Q}}(x_k)\in A_0$ pentru orice $k\in\mathbb{N}$;

(2) $i_{\mathbb{Q}}(x_k+\frac{1}{10^k})\notin A_0$ pentru orice $k\in\mathbb{N}$;

(3) $x_{k+1}=x_k+\frac{n_k}{10^{k+1}}$.

Din (3) și din definiția lui n_k rezultă $x_{k+1}=x_k+\frac{n_k}{10^{k+1}}$, de unde pentru $n>k$ obținem $x_n-x_k=x_n-x_{n-1}+x_{n-1}-x_{n-2}+\ldots+x_{k+1}-x_k\leq$

$$\leq\frac{9}{10^n}+\frac{9}{10^{n-1}}+\ldots+\frac{9}{10^{k+1}}=\frac{9}{10^{k+1}}\left(1+\frac{1}{10}+\ldots+\frac{1}{10^{n-(k+1)}}\right)=\frac{9}{10^{k+1}}\cdot\frac{1-\frac{1}{10^{n-k}}}{1-\frac{1}{10}}<$$

$$<\frac{9}{10^{k+1}}\cdot\frac{10}{9}=\frac{1}{10^k}$$

deci $(x_n)_{n\geq 0}\in\mathbf{C}(\mathbb{Q})$. Fie $\alpha=\overline{(x_n)_{n\geq 0}}\in\mathbb{R}$ și să demonstrăm că $\alpha=\inf A$.

Pentru aceasta vom demonstra că

$(*)$ $i_{\mathbb{Q}}(x_k)\leq\alpha\leq i_{\mathbb{Q}}(x_k+\frac{1}{10^k})$ pentru orice $k\in\mathbb{N}$.

Din (3) deducem că $x_0\leq x_1\leq\ldots\leq x_k\leq\ldots$, deci $(x_n-x_k)_{n\geq 0}\in P$ pentru orice $k\in\mathbb{N}$, adică $i_{\mathbb{Q}}(x_k)\leq\overline{(x_n)_{n\geq 0}}=\alpha$ pentru orice $k\in\mathbb{N}$.

Am demonstrat mai înainte că $x_n - x_k < \frac{1}{10^k}$, pentru n>k, adică $\left(x_k + \frac{1}{10^k}\right) - x_n > 0$ pentru n >k, deci $\alpha \le i_{\mathbb{Q}}\left(x_k + \frac{1}{10^k}\right)$ pentru orice $k \in \mathbb{N}$.

Am arătat astfel inegalitățile $(*)$.

Să demonstrăm acum că α este minorant al lui A. Să presupunem că există $\gamma \in A$ a.î. $\gamma < \alpha$. Atunci $i_{\mathbb{Q}}(x_k) \le \gamma \le \alpha \le i_{\mathbb{Q}}\left(x_k + \frac{1}{10^k}\right)$ pentru orice $k \in \mathbb{N}$.

Dar $\lim_{k\to\infty}\left(x_k + \frac{1}{10^k} - x_k\right) = \lim_{k\to\infty} \frac{1}{10^k} = 0$, de unde ținând cont de Lema 3.9. deducem că $\gamma = \alpha$, absurd, deci $\alpha \in A_0$.

Să arătăm acum că α este cel mai mare minorant al lui A. Presupunem că există $\beta \in A_0$ a.î. $\alpha < \beta$. Din (3) deducem că pentru fiecare $k \in \mathbb{N}$ există $\alpha_k \in A$ a.î. $\alpha_k < i_{\mathbb{Q}}(x_k + \frac{1}{10^k})$. Cum β este minorant al lui A şi $\alpha_k \in A$ deducem că $\beta \le \alpha_k$ de unde $i_{\mathbb{Q}}(x_k) \le \alpha \le \beta \le i_{\mathbb{Q}}(x^k + \frac{1}{10^k})$ de unde deducem (conform Lemei 3.9.) că $\alpha = \beta$, absurd !. Deci $\alpha = \inf A$. ■

CAPITOLUL 5 :

CORPUL NUMERELOR COMPLEXE

§1 Construcția corpului numerelor complexe $\mathbb{C}$

Scopul acestui paragraf este de a identifica corpul $\mathbb{R}$ al numerelor reale cu un subcorp al unui corp comutativ $\mathbb{C}$ în care ecuația $x^2 = -1$ are soluție.

Pentru aceasta vom considera $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ iar pentru $(x, y), (z, t) \in \mathbb{C}$ definim :

$$(x, y) + (z, t) = (x+z, y+t)$$
$$(x, y) \cdot (z, t) = (xz-yt, xt+yz).$$

TEOREMA 1.1. ($\mathbb{C}$, +, ·) este corp comutativ în care ecuația $x^2 = -1$ are soluție.

Demonstraţie Faptul că $(\mathbb{C}, +)$ este grup abelian se probează imediat (elementul neutru este $(0, 0)$, iar pentru $(x, y)\in\mathbb{C}$, $-(x, y)=(-x, -y)$).

În mod evident înmulţirea este comutativă.

Pentru a proba că $(\mathbb{C}^*, \cdot)$ este grup, fie $(x, y), (z, t), (r, s)\in\mathbb{C}$. Deoarece $(x, y)[(z, t)\cdot(r, s)]=[(x, y)(z, t)]\cdot(r, s)=(xzr-xts-yzs-ytr, xzs+xtr+yzr-yts)$ deducem că înmulţirea este asociativă.

Cum $(x, y)(1, 0)=(1, 0)(x, y)=(x, y)$ deducem că elementul neutru faţă de înmulţire este $(1, 0)$.

Fie acum $(x, y)\in\mathbb{C}^*$ (adică $x\neq0$ sau $y\neq0$). Egalitatea $(x, y)(x', y')=(1, 0)$ este echivalentă cu $xx'-yy'=1$ şi $xy'+yx'=0$, de unde $x'=\frac{x}{x^2+y^2}$ şi $y'=-\frac{y}{x^2+y^2}$, adică $(x, y)^{-1}=\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$.

Cum pentru $(x, y), (z, t), (r, s)\in\mathbb{C}$, $(x, y)\cdot[(z, t)+(r, s)]=(x, y)\cdot(z, t)+(x, y)\cdot(r, s)=(xz+xr-yt-ys, xt+xs+yz+yr)$ deducem că înmulţirea este distributivă faţă de adunare, adică $(\mathbb{C}, +, \cdot)$ este corp comutativ.

Să notăm $i=(0, 1)$. Cum $i^2=(0, 1)(0, 1)=(-1, 0)=-(1, 0)$ deducem că ecuaţia $x^2=-1$ are soluţie în $\mathbb{C}$. ■

Observaţie Se probează imediat că $i_{\mathbb{R}}:\mathbb{R}\to\mathbb{C}$, $i_{\mathbb{R}}(x)=(x, 0)$ pentru orice $x\in\mathbb{R}$, este morfism de corpuri (deci funcţie injectivă). În felul acesta $\mathbb{R}$ poate fi privit ca subcorp al lui $\mathbb{C}$. Am construit astfel şirul de mulţimi $\mathbb{N}\subseteq\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$.

Deoarece pentru $z=(x, y)\in\mathbb{C}$ putem scrie $z=(x, 0)+(y, 0)(0, 1)$, ţinând cont de identificările anterioare deducem că z se poate scrie (formal) sub forma $z=x+iy$ (cu $i=(0, 1)$ iar $i^2=-1$).

Mulţimea $\mathbb{C}$ poartă numele de *mulţimea numerelor complexe*, iar $(\mathbb{C}, +, \cdot)$ *corpul numerelor complexe.* Elementele din $\mathbb{C}\setminus\mathbb{R}$ se zic *pur imaginare*.

Dacă $z=x+iy\in\mathbb{C}$ cu $x, y\in\mathbb{R}$, atunci x se zice *partea reală* a lui z iar yi *partea imaginară* a lui z (y se numeşte *coeficientul părţii imaginare*).

Pentru $z\in\mathbb{C}$, $z=x+iy$, definim $\bar{z}=x-iy$ (ce se va numi *conjugatul* lui z) şi $|z|=\sqrt{x^2+y^2}$ ($|z|$ poartă numele de *modulul* lui z).

PROPOZIŢIA 1.2. Fie $z, z_1, z_2\in\mathbb{C}$. Atunci

1) $\mathbf{z}\in\mathbb{R} \Leftrightarrow z=\bar{z}$

2) $\overline{\bar{z}}=z \ , z\cdot\bar{z}=|z|^2$

3) $\overline{z_1\pm z_2}=\overline{z_1}\pm\overline{z_2}$, $\overline{z_1 z_2}=\overline{z_1}\ \overline{z_2}$, $\overline{\left(\frac{z_1}{z_2}\right)}=\frac{\overline{z_1}}{\overline{z_2}}$ **(cu $z_2\neq 0$)**

4) $|z|=|\bar{z}|$, $|z_1+z_2|\le|z_1|+|z_2|$, $|z_1\ z_2|=|z_1|\ |z_2|$, $\left|\frac{z_1}{z_2}\right|=\frac{|z_1|}{|z_2|}$ **(cu $z_2\neq 0$).**

Demonstraţie 1) Fie z=a+ib. Dacă $z\in\mathbb{R}$, atunci b=0, deci $\bar{z}=a=z$ iar dacă $z=\bar{z}$ atunci b =-b adică b=0, deci $z\in\mathbb{R}$.

Să mai probăm inegalitatea $|z_1+z_2|\le|z_1|+|z_2|$ (celelalte probându-se imediat). Alegem $z_1=x_1+iy_1$ şi $z_2=x_2+iy_2$ cu $x_1, x_2, y_1, y_2\in\mathbb{R}$ şi astfel

$|z_1+z_2|\le|z_1|+|z_2| \Leftrightarrow \sqrt{(x_1+x_2)^2+(y_1+y_2)^2} \le \sqrt{x_1^2+y_1^2}+\sqrt{x_2^2+y_2^2} \Leftrightarrow$

$x_1^2+x_2^2+2x_1x_2+y_1^2+y_2^2+2y_1y_2 \le x_1^2+y_1^2+x_2^2+y_2^2+$

$+2\sqrt{(x_1^2+y_1^2)(x_2^2+y_2^2)} \Leftrightarrow$

$(x_1x_2+y_1y_2)^2 \le (x_1^2+y_1^2)(x_2^2+y_2^2) \Leftrightarrow (x_1y_2-x_2y_1)^2\ge 0$ ceea ce este evident.

Egalitate avem dacă $\frac{x_1}{y_1}=\frac{x_2}{y_2}=\lambda$ cu $\lambda\in\mathbb{R}$, adică $z_1=\lambda\ z_2$. ■

Observaţie Asociind fiecărui număr complex z=a+ib matricea $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ se probează imediat că corpul $(\mathbb{C},+,\cdot)$ este izomorf cu corpul $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,\ b\in\mathbb{R}\right\}$, operaţiile de adunare şi înmulţire fiind cele obişnuite din $M_2(\mathbb{R})$.

§2 Teorema fundamentală a algebrei

Dacă L şi K sunt două corpuri a.î. K este subcorp al lui L, spunem despre L că este o *extindere* a lui K.

Reamintim un rezultat clasic din algebră :

LEMA 2.1. Dacă K este un corp comutativ iar f∈K[X], grad(f) ≥1, atunci există o extindere L a lui K în care f are toate rădăcinile.

Utilizând teorema fundamentală a polinoamelor simetrice obținem imediat :

LEMA 2.2. Fie f∈K[X], cu grad(f) ≥1 iar K este corp comutativ. Dacă L este o extensie a lui K în care f are toate rădăcinile $x_1, \dots x_n$ iar $g \in K[X_1, \dots X_n]$ este un polinom simetric, atunci $g(x_1, \dots x_n) \in K$.

Teorema următoare (ce se bazează pe cele două rezultate anterioare) este cunoscută sub numele de *teorema fundamentală a algebrei* (sau *teorema D'Alembert-Gauss*):

TEOREMA 2.3.(D'Alembert-Gauss) Orice polinom f∈ℂ[X] cu grad(f) ≥1 are cel puțin o rădăcină în ℂ.

Demonstrație Fie $f=a_0+a_1X+\dots+a_nX^n \in \mathbb{C}[X]$ $(a_n \neq 0)$ și $\overline{f} = \overline{a_0} + \overline{a_1}X + \dots + \overline{a_n}X^n$ unde pentru orice $0 \leq i \leq n$, $\overline{a_i}$ este conjugatul lui a_i.

Atunci $f\,\overline{f} = \sum_{k=0}^{2n} c_k X^k$, unde $c_k = \sum_{i+j=k} a_i \overline{a_j}$, $0 \leq k \leq 2n$ și cum $c_k = \overline{c_k}$ pentru orice $0 \leq k \leq 2n$, deducem că $f\overline{f} \in \mathbb{R}[X]$.

Să presupunem că teorema este demonstrată pentru polinoamele din $\mathbb{R}[X]$. Atunci există $a \in \mathbb{C}$ a.î. $(f\overline{f})(a) = 0 \Leftrightarrow f(a)\overline{f}(a) = 0 \Leftrightarrow f(a) = 0$ sau $f(\overline{a}) = 0$.

Deci este suficient să presupunem că $f \in \mathbb{R}[X]$. Dacă gradul lui f este impar, cum funcția polinomială a lui f este continuă iar la $\pm\infty$ ia valori de semne contrare deducem că există $a \in \mathbb{R}$ a.î. $f(a)=0$.

Fie acum $n=\text{grad}(f)$, $n=2^k p$, cu $k \in \mathbb{N}$ și p impar ; facem inducție matematică după k. Pentru $k=0$ totul rezultă din cele de mai înainte (gradul lui f fiind impar în această situație). Să presupunem afirmația adevărată pentru toate polinoamele $f \in \mathbb{R}[X]$ al căror grad se divide prin 2^{k-1} și nu se divide prin 2^k.

Conform Lemei 2.1. există o extindere L a lui ℂ în care f are toate rădăcinile $x_1, \dots x_n$.

Pentru $a \in \mathbb{R}$ considerăm elementele $z_{ij}^a = x_i x_j + a(x_i + x_j)$, $1 \leq i < j \leq n$ (în număr de C_n^2) .

Considerând polinomul $f_a = \prod_{1 \le i < j \le n} \left(X - z_{ij}^a\right)$ acesta va avea gradul egal cu $C_n^2 = \frac{n(n-1)}{2} = \frac{2^k p\left(2^{k-1} p - 1\right)}{2} = 2^{k-1} p'$ cu p′ impar. Coeficienții lui f_a sunt polinoame simetrice de z_{ij}^a. Mai mult, având în vedere expresiile lui z_{ij}^a, $1 \le i < j \le n$, rezultă că acești coeficienți, ca polinoame de $x_1, x_2, \ldots x_n$ sunt simetrice, deoarece orice permutare a acestora are ca efect schimbarea elementelor z_{ij}^a, $1 \le i < j \le n$ între ele . Conform Lemei 2.2. obținem că $f_a \in \mathbb{R}[X]$.

Cum $2^{k-1} |$ grad (f_a) și $2^k \nmid$ grad (f_a), conform ipotezei de inducție rezultă că f_a are cel puțin o rădăcină complexă. Există deci o pereche (i, j) cu $1 \le i < j \le n$ a.î. $z_{ij}^a \in \mathbb{C}$. Făcând pe a să parcurgă mulțimea infinită $\mathbb{R}$ rezultă că există a, $b \in \mathbb{R}$, $a \ne b$ a.î. z_{ij}^a și $z_{ij}^b \in \mathbb{C}$.

Din $z_{ij}^a = x_i x_j + a\left(x_i + x_j\right)$ și $z_{ij}^b = x_i x_j + b\left(x_i + x_j\right)$ rezultă că $z_{ij}^a - z_{ij}^b = (a-b)\left(x_i + x_j\right) \in \mathbb{C}$, deci $x_i + x_j \in \mathbb{C}$; atunci $x_i x_j \in \mathbb{C}$, adică x_i , $x_j \in \mathbb{C}$ și astfel teorema este demonstrată. ■

Observații

1. Din Teorema 2.3. deducem imediat că dacă $f \in \mathbb{C}[X]$, grad$(f) \ge 1$, atunci f are toate rădăcinile în $\mathbb{C}$. Acest lucru ne permite să afirmăm că Teorema fundamentală a algebrei exprimă faptul că corpul $\mathbb{C}$ al numerelor complexe este *algebric închis* .

2.Din Teorema 2.3. deducem imediat că în $\mathbb{C}[X]$ polinoamele ireductibile sunt exact polinoamele de gradul 1 iar în $\mathbb{R}[X]$ sunt cele de gradul 1 precum și cele de forma aX^2+bX+c cu $b^2-4ac<0$.

CAPITOLUL 6:
ELEMENTE DE ARITMETICĂ

§1 Divizibilitate pe $\mathbb{N}$

DEFINIŢIA 1.1. Fie a, b$\in\mathbb{N}$, b$\neq$0.Vom spune că *b divide a* şi vom scrie b|a, dacă există c$\in\mathbb{N}$ a.î. a=bc (nu definim divizibilitatea prin 0!). În acest caz vom spune că b este un *divizor* al lui a (sau că a este *multiplu* de b).

În mod evident, relaţia de divizibilitate de pe $\mathbb{N}$ este reflexivă, antisimetrică şi tranzitivă, adică ($\mathbb{N}$, |) este o mulţime parţial ordonată în care 1 este cel mai mic element (element iniţial) iar 0 este cel mai mare element (element final).

DEFINIŢIA 1.2. Un număr p$\in\mathbb{N}$, p$\geq$2 se zice *prim* dacă singurii săi divizori sunt 1 şi p.

Cele mai mici numere prime sunt 2, 3, 5, 7, etc. (vom demonstra mai târziu că există o infinitate de numere prime).

Reamintim că în Capitolul 1 [§.4, Corolarul 4.9.] am demonstrat teorema împărţirii cu rest în $\mathbb{N}$: dacă a, b$\in\mathbb{N}$, b$\geq$1, atunci există şi sunt unici c, r$\in\mathbb{N}$ a.î. a =bc+r, iar 0$\leq$r<b; numărul c numindu-se *câtul* împărţirii lui b la a, iar r *restul* acestei împărţirii (evident b|a dacă şi numai dacă r=0).

TEOREMA 1.3. Fiind date două numere a, b$\in\mathbb{N}$, există d$\in\mathbb{N}$ (vom nota d=(a,b)) a.î. d|a, d|b, iar dacă mai avem d′$\in\mathbb{N}$ a.î. d′ | a şi d′| b, atunci d′| d (adică în mulţimea parţial ordonată ($\mathbb{N}$, |) pentru orice două elemente a şi b există (a, b)).

Demonstraţie Conform teoremei împărţirii cu rest, putem scrie $a=bc_1+r_1$, cu $c_1, r_1\in\mathbb{N}$, iar $0 \leq r_1< b$.

Dacă $r_1=0$ atunci b|a şi în mod evident d=(a, b)=b.

Dacă $r_1\neq0$, atunci conform aceleiaşi teoreme de împărţire cu rest putem scrie $b=r_1c_2+r_2$,cu $c_2, r_2\in\mathbb{N}$, iar $0\leq r_2<r_1$.

Dacă $r_2=0$, atunci $d=r_1$. Într-adevăr, din $b=r_1c_2$ deducem că d|b, iar din $a=bc_1+r_1$ deducem că d|a . Dacă mai avem d′$\in\mathbb{N}$ a.î. d′ |a şi d′ |b, atunci cum $r_1=a-bc_1$, deducem că d′ $|r_1=d$.

Dacă $r_2 \neq 0$, atunci din nou putem scrie $r_1 = r_2 c_3 + r_3$, cu $0 \leq r_3 < r_2$, şi algoritmul descris până acum continuă, obţinându-se un şir descrescător de numere naturale : $r_1, r_2, \ldots$ a.î. $r_{j-2} = r_{j-1} c_j$ ($j \geq 3$). Conform Corolarului 4.6. de la Capitolul 1, §4, şirul $r_1, r_2, r_3, \ldots$ este stationar.

Astfel, dacă pentru un anumit k, $r_{k+1}=0$, atunci $d=r_k$, pe când, dacă $r_{k+1}=1$ atunci $d=1$. ■

De exemplu : Dacă a=49 şi b=35 avem :

$49 = 1 \cdot 35 + 14$ $\quad (c_1=1, r_1=14)$

$35 = 2 \cdot 14 + 7$ $\quad (c_2=2, r_2=7)$

$14 = 2 \cdot 7$ $\quad (c_3=2, r_3=0)$

de unde deducem că (49, 35)=7.

Dacă a=187 şi b=35 avem:

$187 = 5 \cdot 35 + 12$ $\quad (c_1=5, r_1=12)$

$35 = 2 \cdot 12 + 11$ $\quad (c_2=2, r_2=11)$

$12 = 1 \cdot 11 + 1$ $\quad (c_3=1, r_3=1)$

de unde deducem că (187, 35)=1.

Observaţii : 1. Numărul d poartă numele de *cel mai mare divizor comun* al lui a şi b.

2. Algoritmul de găsire a celui mai mare divizor comun a două numere naturale descris mai înainte poartă numele de ***algoritmul lui Euclid*** **.**

3. Dacă pentru a, $b \in \mathbb{N}$ avem (a, b)=1, vom spune despre a şi b că sunt *prime între ele.*

4. Inductiv se arată că pentru oricare n numere naturale $a_1, a_2, \ldots, a_n$ ($n \geq 2$) există $d \in \mathbb{N}$ a.î. $d | a_i$ pentru orice $1 \leq i \leq n$ şi dacă mai avem $d' \in \mathbb{N}$ a.î. $d' | a_i$ pentru orice $1 \leq i \leq n$, atunci $d' | d$. Numărul d se notează prin $d=(a_1, a_2, \ldots, a_n)$ şi poartă numele de *cel mai mare divizor comun* al numerelor $a_1, a_2, \ldots, a_n$.

§2. Divizibilate pe $\mathbb{Z}$

DEFINIŢIA 2.1. Dacă a, $b \in \mathbb{Z}$, $b \neq 0$, vom spune că b divide a (vom scrie b|a) dacă există $c \in \mathbb{Z}$ a.î. a=bc (ca şi în cazul lui $\mathbb{N}$ nu vom defini, nici în cazul lui $\mathbb{Z}$ divizibilitatea prin 0).

Evident, dacă $a \in \mathbb{Z}$ atunci $1 | a$, $-1 | a$ şi $a | 0$.

Numerele prime în $\mathbb{Z}$ se definesc ca fiind acele numere întregi p cu proprietatea că $p \neq -1, 0, 1$, iar singurii divizori ai lui p sunt $\pm 1, \pm p$. Evident, numerele prime din $\mathbb{Z}$ sunt numerele de forma $\pm p$, cu $p \geq 2$ număr prim în $\mathbb{N}$.

Se verifică imediat că dacă a, b, $c \in \mathbb{Z}$, atunci :

1) $a|a$ $(a \neq 0)$

2) Dacă $a|b$ şi $b|a$, atunci $a = \pm b$ (deci în $\mathbb{Z}$ relaţia de divizibilitate nu mai este antisimetrică).

3) Dacă $a|b$ şi $b|c$, atunci $a|c$.

TEOREMA 2.2. (Teorema împărţirii cu rest în $\mathbb{Z}$) Dacă a, $b \in \mathbb{Z}$ $b>0$, atunci există c, $r \in \mathbb{Z}$ a.î. $a=cb+r$, cu $0 \leq r < b$.

Demonstraţie Fie $P=\{a-xb \mid x \in \mathbb{Z}\}$; evident în P avem şi numere naturale. Fie $r=a-cb$ cel mai mic număr natural din P (cu $c \in \mathbb{Z}$). (un astfel de număr există conform Teoremei 4.5. de la Capitolul 1). Avem $0 \leq r < b$ căci dacă $r=a-cb \geq b$ am $0 \leq a-(c+1)b < r$, ceea ce contrazice minimalitatea lui r. ■

Observaţie 1. Putem formula teorema împărţirii cu rest din $\mathbb{Z}$ şi sub forma : Dacă a, $b \in \mathbb{Z}$, $b \neq 0$, atunci există c, $r \in \mathbb{Z}$ a.î. $a=cb+r$, iar $0 \leq r < |b|$.

2. Numerele c şi r cu proprietatea de mai sus poartă numele de *câtul*, respectiv *restul* împărţirii lui a la b, şi sunt unice cu proprietatea respectivă, căci dacă am mai avea c'şi $r' \in \mathbb{Z}$ a.î. $a=c'b+r'$,cu $0 \leq r' < |b|$, atunci $cb+r=c'b+r' \Leftrightarrow (c-c')b = r'-r$, adică $b|r'-r$. Cum $0 \leq r, r' < |b|$, dacă am presupune, de exemplu, că $r' > r$, atunci $r'-r < |b|$, iar condiţia $b \mid r'-r$ implică $r'-r = 0 \Leftrightarrow r' = r$ şi cum $(c-c')b=r'-r=0$, deducem imediat că $c=c'$.

DEFINIŢIA 2.3. Numim *ideal* al inelului $(\mathbb{Z}, +, \cdot)$ orice submulţime nevidă $\underline{a} \subseteq \mathbb{Z}$ a.î.

i) Dacă $x, y \in \underline{a}$, atunci $x-y \in \underline{a}$

ii) Dacă $x \in \underline{a}$ şi $b \in \mathbb{Z}$, atunci $bx \in \underline{a}$.

PROPOZIŢIA 2.4. Fie $\underline{a} \in \mathbb{Z}$ un ideal. Atunci există $d \in \mathbb{N}$ a.î. $\underline{a}=d\mathbb{Z}$.

Demonstraţie Dacă $\underline{a}=\{0\}$, atunci $d=0$. Să presupunem că $\underline{a} \neq \{0\}$. Atunci există $x \in \underline{a}$, $x \neq 0$. Dacă $x>0$, atunci $x \in \mathbb{N}^*$, iar dacă $x<0$, cum $\underline{a}$ este un ideal, $-x \in \underline{a}$, şi atunci $-x \in \mathbb{N}^*$.

În concluzie $\underline{a}\cap\mathbb{N}^*\neq\emptyset$. Conform Teoremei 4.5 de la Capitolul 1, putem alege $d\in\underline{a}\cap\mathbb{N}^*$ ca fiind cel mai mic element din $\underline{a}\cap\mathbb{N}^*$ şi să demonstrăm că $\underline{a}=d\mathbb{Z}$. Cum $d\in\underline{a}$ şi $\underline{a}$ este ideal al inelului $\mathbb{Z}$, incluziunea $d\mathbb{Z}\subseteq\underline{a}$ este imediată. Fie acum $a\in\underline{a}$. Conform Teoremei 2.2. putem scrie $a=cd+r$, cu $c, r\in\mathbb{Z}$ şi $0\leq r<d$. (căci $d\in\mathbb{N}^*$). Scriind $r=a-cd$ cum $a, d\in\underline{a}$, deducem că $r\in\underline{a}$. Datorită minimalităţii lui d deducem că $r=0$ şi astfel $a=cd\in d\mathbb{Z}$, de unde şi incluziunea inversă $\underline{a}\subset d\mathbb{Z}$, care ne asigură egalitatea $\underline{a}=d\mathbb{Z}$. ■

<u>PROPOZIŢIA 2.5.</u> Fie $a_1, a_2, \ldots, a_n\in\mathbb{Z}$. Dacă notăm prin $< a_1, a_2, \ldots, a_n >$ idealul generat de $\{a_1, a_2, \ldots, a_n\}$, atunci $< a_1, a_2, \ldots, a_n >= \{k_1a_1+\ldots+k_na_n \mid k_i\in\mathbb{Z}, 1\leq i\leq n\}$.

<u>Demonstratie</u> Dacă notăm $\underline{a}=\{k_1a_1+\ldots+k_na_n \mid k_i\in\mathbb{Z}, 1\leq i\leq n\}$, se arată imediat că $\underline{a}$ este ideal al lui $\mathbb{Z}$ ce conţine $\{a_1, a_2, \ldots, a_n\}$. Cum $< a_1, a_2, \ldots, a_n >$ este cel mic ideal al lui $\mathbb{Z}$ ce include $\{a_1, a_2, \ldots, a_n\}$, deducem că $< a_1, a_2, \ldots, a_n >\subseteq \underline{a}$. Pentru incluziunea inversă ţinem cont de faptul că $< a_1, a_2, \ldots, a_n> = \bigcap_{\substack{\underline{b}\subseteq Z \text{ ideal}\\ \{a_1,\ldots,a_n\}\subseteq\underline{b}}}\underline{b}$ şi fie deci $\underline{b}\subseteq\mathbb{Z}$ un ideal a.î. $\{a_1, a_2, \ldots, a_n\}\subseteq\underline{b}$.

Atunci pentru orice $k_1,\ldots,k_n\in\mathbb{Z}$ avem $k_1a_1+\ldots+k_na_n\in\underline{b}$, adică $\underline{a}\subseteq\underline{b}$ şi cum $\underline{b}$ este oarecare, deducem că $\underline{a}\subseteq\cap\underline{b}=< a_1, a_2, \ldots, a_n >$, de unde egalitatea dorită. ■

Fiind date $a_1, a_2, \ldots, a_n\in\mathbb{Z}$ prin *<u>cel mai mare divizor comun al numerelor</u>* $\underline{a_1,a_2,\ldots,a_n}$ înţelegem acel număr $d\in\mathbb{Z}$ a.î. $d|a_i$ pentru orice $1\leq i\leq n$ şi în plus dacă mai avem $d'|a_i$ pentru orice $1\leq i\leq n$, atunci $d'|d$.

Evident, dacă un astfel de d există, atunci şi $-d$ are aceeaşi proprietate . Convenim să alegem pentru rolul de cel mai mare divizor comun al numerelor întregi $a_1, a_2, \ldots, a_n$ acel număr natural d cu proprietăţile de mai înainte şi vom nota $d=(a_1, a_2, \ldots, a_n)$ (vezi şi §1 pentru cazul numerelor naturale).

<u>TEOREMA 2.6.</u> Fiind date n numere întregi $a_1, a_2, \ldots, a_n$ ($n\geq 2$), dacă notăm prin d numărul natural a cărui existenţă este asigurată de Propoziţia 2.4. pentru idealul $\underline{a}=< a_1, a_2, \ldots, a_n>$, atunci $d=(a_1, a_2, \ldots, a_n)$.

<u>Demonstraţie</u> Într-adevăr, cum fiecare $a_i\in< a_1, a_2, \ldots, a_n>=d\mathbb{Z}$ deducem că $a_i\in d\mathbb{Z}$, adică $d|a_i$ pentru $1\leq i\leq n$.

Fie acum $d' \in \mathbb{Z}$ a.î. $d'|a_i$ pentru $1 \le i \le n$. Cum $d \in d\mathbb{Z}$, există $k_1, \ldots, k_n \in \mathbb{Z}$ a.î. $d = \sum_{i=1}^{n} k_i a_i$ şi astfel deducem că $d'|d$, adică $d=(a_1, a_2, \ldots, a_n)$. ■

COROLAR 2.7. Fiind date n numere întregi $a_1, a_2, \ldots, a_n$ ($n \ge 2$), $d=(a_1, a_2, \ldots, a_n)$ dacă şi numai dacă există $k_1, \ldots, k_n \in \mathbb{Z}$ a.î. $d=k_1a_1+\ldots+k_na_n$.

§3. Teorema fundamentală a aritmeticii

Fie $a \in \mathbb{Z}^*$ şi $p \in \mathbb{N}$, $p \ge 2$, un număr prim. În mod evident, există $k \in \mathbb{N}$ a.î. $p^k|a$ şi $p^{k+1} \nmid a$ (altfel zis k este cel mai mare număr natural cu proprietatea $p^k \mid a$).

Convenim să notăm $k=o_p(a)$ şi să-l numim *ordinul* sau *exponentul* lui p în a. Dacă a=0 vom lua $o_p(0)=-\infty$, iar $o_p(a)=0 \Leftrightarrow p \nmid a$.

PROPOZIŢIA 3.1. Orice număr natural nenul se scrie ca un produs de numere naturale prime.

Demonstraţie Fie A=mulţimea numerelor naturale nenule ce nu se scriu ca produs de numere naturale prime. Dacă prin absurd propoziţia nu ar fi adevărată, atunci $A \neq \emptyset$.

Conform Teoremei 4.5 de la Capitolul 1 mulţimea A va conţine un element minimal x. În particular, $x > 1$ şi cum x nu este prim putem scrie $x=m \cdot n$ cu $1<m$, $n<x$. Cum m, $n<x$, iar $x=\inf(A)$, deducem că m, $n \notin A$, deci m şi n se scriu ca produse de numere prime. Atunci şi $x=m \cdot n$ se scrie ca produs de numere prime-absurd . Deci $A=\emptyset$ şi cu aceasta propoziţia este demonstrată. ■

COROLAR 3.2. Pentru orice $n \in \mathbb{Z}^*$ există numerele întregi prime $p_1, \ldots, p_m$ a.î. $n = p_1^{k_1} \ldots p_m^{k_m}$ cu $k_1, \ldots, k_m \in \mathbb{N}$.

Putem folosi şi notaţia : $n = (-1)^{\varepsilon(n)} \prod_{\substack{p \ prim \\ p \ge 2}} p^{e(p)}$ unde $\varepsilon(n) \in \{0,1\}$ (după cum n este pozitiv sau negativ) iar exponenţii e(p) sunt numere naturale nenule numai pentru un număr finit de p-uri.

LEMA 3.3. Dacă a, b, $c \in \mathbb{Z}$ a.î. (a, b)=1 şi a|bc, atunci a|c.

Demonstraţie Într-adevăr, cum (a, b)=1 conform Corolarului 2.7. există $r, s \in \mathbb{Z}$ a.î. $ra+sb=1$, de unde $c=rac+sbc$. Cum a|bc deducem că $a|rac+sbc=c$, adică a|c . ■

Observaţie Dacă (a, b)≠1, atunci lema de mai înainte nu mai este adevărată tot timpul căci, de exemplu, 6|3·8=24, dar 6∤3 şi 6∤8 .

COROLAR 3.4.Dacă p, a, b∈ℤ a.î. p este prim şi p|ab, atunci p|a sau p|b.

Demonstraţie Într-adevăr, singurii divizori ai lui p în ℤ sunt ±1, ±p.

Atunci (p,b)=1 sau p|b. Dacă p|b totul este în regulă, iar dacă (p, b)=1, atunci se aplică Lema 3.5. ■

Observaţie Putem utiliza corolarul de mai înainte şi sub forma : dacă p, a, b∈ℤ a.î. p este prim iar p∤a, p∤b, atunci p∤ab .

COROLARUL 3.5. Presupunem că p, a, b∈ℤ iar p este prim. Atunci $o_p(ab)=o_p(a)+o_p(b)$.

Demonstraţie Dacă $\alpha=o_p(a)$, $\beta=o_p(b)$, atunci $a=p^{\alpha}c$ şi $b=p^{\beta}d$, cu p∤c şi p∤d. Atunci $ab=p^{\alpha+\beta}cd$ şi cum p∤cd , deducem că $o_p(ab)=\alpha+\beta=o_p(a)+o_p(b)$. ■

TEOREMA 3.6. (Teorema fundamentală a aritmeticii) Pentru orice număr întreg nenul n, există o descompunere a lui în factori primi $n=(-1)^{\varepsilon(n)}\prod_{\substack{p\ prim\\ p\geq 2}} p^{e(p)}$ cu exponenţii e(p) în mod unic determinaţi de n (de fapt $e(p)=o_p(n)$).

Demonstraţie Scrierea lui n sub forma din enunţ rezultă din Corolarul 3.2. Să probăm acum unicitatea acestei scrieri.

Aplicând pentru un prim q, o_q în ambii membrii ai egalităţii $n=(-1)^{\varepsilon(n)}\prod_{\substack{p\ prim\\ p\geq 2}} p^{e(p)}$ obţinem : $o_q(n)=\varepsilon(n)o_q(-1)+\sum_p e(p)\,o_q(p)$.

Însă $o_q(-1)=0$ iar $o_q(p)=\begin{cases}0, pentru\ p\neq q\\ 1, pentru\ p=q\end{cases}$ de unde deducem că $e(q)=o_q(n)$ şi astfel teorema este demonstrată. ■

COROLAR 3.7. Pentru orice n∈ℕ* există şi sunt unice numerele prime distincte $p_1, p_2, \ldots, p_m$ şi numerele naturale $k_1, k_2, \ldots, k_m$ a.î. $n=p_1^{k_1}\ldots p_m^{k_m}$ (spunem că această scriere a lui n este *descompunerea lui n în factori primi*)

COROLAR 3.8. **Fie a, b, c, n∈$\mathbb{N}^*$ a.î. (a,b)=1 şi ab=c^n. Atunci există x, y∈$\mathbb{N}^*$ a.î. a=x^n şi b=y^n.**

Demonstraţie Fie $a = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$, $b = q_1^{l_1} \cdot ... \cdot q_t^{l_t}$ descompunerea numerelor a şi b în factori primi (deci $k_i \geq 1$ şi $l_j \geq 1$ pentru i=1, 2,…,s şi j=1, 2,…,t). Din (a,b)=1 deducem că $\{p_1,\ldots,p_s\} \cap \{q_1,\ldots,q_t\} = \emptyset$. Obţinem deci că $c^n = p_1^{k_1} \cdot ... \cdot p_s^{k_s} q_1^{l_1} \cdot ... \cdot q_t^{l_t}$, egalitate ce dă descompunerea lui c^n în factori primi.

Însă, conform Teoremei 3.6., descompunerea unui număr natural în produs de puteri de numere prime distincte este unică (abstracţie făcând de ordinea factorilor).

Astfel, dacă $c = p_1^{n_1} \cdot ... \cdot p_s^{n_s} q_1^{m_1} \cdot ... \cdot q_t^{m_t}$, atunci

$c^n = p_1^{nn_1} \cdot ... \cdot p_s^{nn_s} q_1^{nm_1} \cdot ... \cdot q_t^{nm_t}$, de unde deducem că $nn_i=k_i$ şi $nm_j=l_j$ $1 \leq i \leq s$, $1 \leq j \leq t$.

Atunci putem considera $x = p_1^{n_1} \cdot ... \cdot p_s^{n_s}$ şi $y = q_1^{m_1} \cdot ... \cdot q_t^{m_t}$. ■

TEOREMA 3.9. (Legendre) Dacă n∈$\mathbb{N}$ iar p este un număr prim, atunci exponentul lui p în n ! este dat de $\sum_{k \in N^*} \left[\frac{n}{p^k} \right]$.

Demonstraţie În mod evident exponentul e_p al lui p în n! este dat de $e_p = 1 \cdot k_1 + 2 \cdot k_2 + ...$, unde k_1 este numărul numerelor luate dintre 1, 2, …, n care se divid cu p dar nu cu p^2, k_2 este numărul numerelor luate dintre 1, 2, …, n care se divid cu p^2 dar nu cu p^3, etc.

Să calculăm acum un k_i . Numerele ce se divid prin p^i dintre 1, 2, …, n sunt $1 \cdot p^i$, $2 \cdot p^i$, …, $t_i \cdot p^i$, cu $t_i \cdot p^i \leq n < (t_i+1) \cdot p^i$, deoarece dacă j este luat dintre 1, 2,..,n şi $p^i | j$ avem $j = t \cdot p^i$ şi cum $1 \leq j \leq n$ avem $1 \leq t \cdot p^i \leq n$. Dar $t_i \leq \frac{n}{p^i} < t_i + 1$, deci $t_i = \left[\frac{n}{p^i} \right]$.

Numerele luate dintre 1, 2, …, n care se divid cu p^{i+1} se află toate printre numerele luate dintre 1, 2, …, n care se divid cu p^i.

Dacă din numerele luate dintre 1, 2, …, n care se divid cu p^i (ce sunt în număr de t_i) extragem toate numerele luate dintre 1, 2, …, n care se divid cu p^{i+1} (ce sunt în număr de $t_{i+1}=\left[\frac{n}{p^{i+1}}\right]$) obţinem numai numerele luate dintre 1, 2,…,n care se divid cu p^i dar nu se divid cu o putere mai mare a lui p (deoarece nu se divid cu p^{i+1}).

Conform celor de mai sus numărul acestora este egal cu $k_i=t_i-t_{i+1}$.

Avem deci $e_p = 1\cdot(t_1-t_2)+2\cdot(t_2-t_3)+....=t_1+t_2+....=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+....$.

(această sumă este finită deoarece va exista un $k\in\mathbb{N}^*$ a.î. $p^k\le n<p^{k+1}$ şi atunci $\left[\frac{n}{p^s}\right]=0$ pentru orice $s\ge k+1$). ■

Observaţie Dacă p>n atunci $e_p=0$.

§4. Congruenţe pe $\mathbb{Z}$

DEFINIŢIA 4.1. Fie $n\in\mathbb{N}$, $n\ge 2$ un număr fixat. Vom spune că a, $b\in\mathbb{Z}$ sunt *congruente modulo n* dacă n|a-b ; în acest caz scriem $a\equiv b(n)$.

PROPOZIŢIA 4.2. Relaţia de congruenţă modulo n este o echivalenţă pe $\mathbb{Z}$ compatibilă cu operaţiile de adunare şi înmulţire de pe $\mathbb{Z}$ (adică este o congruenţă pe inelul $(\mathbb{Z}, +, \cdot)$).

Demonstraţie Faptul că relaţia de congruentă modulo n este o relaţie de echivalenţă pe $\mathbb{Z}$ se probează imediat. Pentru a proba compatibilitatea acesteia cu operaţiile de adunare şi înmulţire de pe $\mathbb{Z}$, fie a, b, a′, $b'\in\mathbb{Z}$ a.î. $a\equiv b(n)$ şi $a'\equiv b'(n)$, adică a-b=kn şi a′-b′=k′n, cu k, $k'\in\mathbb{Z}$. Atunci a+a′-(b+b′)=(k+k′)n, adică $a+a'\equiv b+b'(n)$ şi scriind aa′-bb′=a(a′-b′)+b′(a-b)=ak′n+b′kn=(ak′+b′k)n deducem că şi $aa'\equiv bb'(n)$. ■

COROLAR 4.3. Fie $a_i, b_i\in\mathbb{Z}$ a.î. $a_i\equiv b_i(n)$ pentru orice i=1, 2,…,k. Atunci: $\sum_{i=1}^{k}a_i\equiv\sum_{i=1}^{k}b_i(n)$ şi $\prod_{i=1}^{k}a_i\equiv\prod_{i=1}^{k}b_i(n)$. În particular, dacă a, $b\in\mathbb{Z}$ a.î. $a\equiv b(n)$ şi $k\in\mathbb{N}^*$, atunci $a^k\equiv b^k(n)$.

Pentru $x\in\mathbb{Z}$ vom nota prin $\hat{x}$ clasa de echivalență a lui x modulo n. Deoarece resturile împărțirii unui număr oarecare din $\mathbb{Z}$ prin n sunt 0, 1,…,n-1, se deduce imediat că dacă notăm mulțimea claselor de echivalență modulo n prin $\mathbb{Z}_n$, atunci $\mathbb{Z}_n=\{\hat{0},\hat{1},...,\overset{\wedge}{n-1}\}$, iar pentru $k\in\{0, 1,\ldots,n-1\}$ avem $\hat{k}=\{k+nt \mid t\in\mathbb{Z}\}$.

Pe mulțimea $\mathbb{Z}_n$ se definesc operațiile de adunare şi înmulțire astfel: $\hat{x}+\hat{y}=\overset{\wedge}{x+y}$ şi $\hat{x}\cdot\hat{y}=\overset{\wedge}{x\cdot y}$ (ținând cont de Propoziția 4.2. deducem că acestea sunt bine definite).

PROPOZIȚIA 4.4. ($\mathbb{Z}_n$, +, ·) este inel comutativ în care unitățile sale sunt $U(\mathbb{Z}_n, +, \cdot)=\{\hat{x}\in\mathbb{Z}_n \mid (x, n)=1\}$.

Demonstrație Cum verificarea anumitor axiome nu ridică probleme deosebite, vom reaminti doar că elementul neutru din $\mathbb{Z}_n$ față de adunare este $\hat{0}$, $-\hat{x}=\overset{\wedge}{n-x}$, iar elementul neutru față de înmulțire este $\hat{1}$.

Dacă $\hat{x}\in U(\mathbb{Z}_n)$, atunci există $\hat{y}\in\mathbb{Z}_n$ a.î. $\hat{x}\cdot\hat{y}=\hat{1}\Leftrightarrow\overset{\wedge}{x\cdot y}=\hat{1}\Leftrightarrow n \mid xy-1$, de unde deducem că (x, n)=1.

Reciproc, dacă $x\in\{0,1,\ldots,n-1\}$ şi (x, n)=1, atunci, conform Corolarului 2.7. există r, $s\in\mathbb{Z}$ a.î. $r\cdot n+s\cdot x=1$, de unde deducem că $\hat{s}\hat{x}=\hat{1}\Leftrightarrow\hat{x}^{-1}=\hat{s}$, deci $x\in U(\mathbb{Z}_n)$. ■

De exemplu : $U(\mathbb{Z}_{12})=\{\hat{1},\hat{5},\hat{7},\overset{\wedge}{11}\}$.

Observație Dacă pentru un număr natural $n\geq 1$ definim $\varphi(1)=1$ iar pentru $n\geq 2$, $\varphi(n)$=numărul numerelor naturale $m<n$ a.î. (m, n)=1, atunci $|U(\mathbb{Z}_n)|=\varphi(n)$.

Funcția $\varphi:\mathbb{N}^*\to\mathbb{N}$ definită mai sus poartă numele de *indicatorul lui Euler*.

COROLARUL 4.5. ($\mathbb{Z}_n$, +, ·) este corp ⇔ n este prim.

Observație Dacă în inelul $\mathbb{Z}$ considerăm idealul $\underline{a}=n\mathbb{Z}$, urmărind tehnica factorizării unui inel (comutativ) printr-un ideal, dacă am fi construit inelul factor $\mathbb{Z}/n\mathbb{Z}$ se obținea de fapt tot $\mathbb{Z}_n$.

Fie acum $a, b\in\mathbb{N}^*$, $n\in\mathbb{Z}$, $n\geq 2$ şi d=(a, n).

PROPOZIŢIA 4.6. **Ecuaţia $\hat{a}\hat{x}=\hat{b}$ are soluţie în $\mathbb{Z}_n$ dacă şi numai dacă d|b ; dacă d|b atunci ecuaţia are exact d soluţii în $\mathbb{Z}_n$.**

Demonstraţie Dacă $\hat{x}_0 \in \mathbb{Z}_n$ este o soluţie a ecuaţiei $\hat{a}\hat{x}=\hat{b}$, atunci n|ax$_0$-b, de unde deducem că d|b (căci d|n şi d|a).

Reciproc, să presupunem că d|b. Cum d=(a, n), conform Corolarului 2.7., există $x'_0, y'_0 \in \mathbb{Z}$ a.î. d = $a x'_0 - n y'_0$.

Dacă c=b/d, atunci $a(x'_0 c) - n(y'_0 c) = b$, adică $\hat{a}(\hat{x'_0 c}) = \hat{b}$, deci $\hat{x'_0 c}$ este o soluţie a ecuaţiei $\hat{a}\hat{x}=\hat{b}$.

Să presupunem acum că $\hat{x}_0$ şi $\hat{x}_1$ sunt două soluţii ale ecuaţiei $\hat{a}\hat{x}=\hat{b}$. Atunci n|ax$_0$-b şi n|ax$_1$-b, de unde n|a(x$_1$-x$_0$). Dacă notăm n′=n/d şi a′=a/d, atunci (a′, n′)=1 şi obţinem că n′|x$_1$-x$_0$, adică x$_1$=x$_0$+kn′, cu k∈$\mathbb{Z}$.

Pe de altă parte se verifică imediat că $\hat{x_0 + kn'}$ este soluţie a ecuaţiei $\hat{a}\hat{x}=\hat{b}$ cu k∈{0, 1,…,d-1}.

Cum nu e posibil să avem $\hat{x_0 + k} = \hat{x_0 + k'}$ pentru k, k′∈{0, 1,…,d-1} şi k≠k′ (căci ar trebui ca n|n′(k-k′) ⇔ d|k-k′-absurd !), deducem că dacă $\hat{x}_0 \in \mathbb{Z}_n$ este o soluţie a ecuaţiei $\hat{a}\hat{x}=\hat{b}$, atunci această ecuaţie are d soluţii şi anume: $\hat{x}_0, \hat{x_0 + n'}, \ldots, \hat{x_0 + (d-1)n'}$.

Exemplu. Să considerăm în $\mathbb{Z}_{15}$ ecuaţia $\hat{6}\cdot\hat{x}=\hat{3}$. Avem d=(6, 15)=3 şi 3|3, deci ecuaţia va avea soluţie în $\mathbb{Z}_{15}$. Cum n′=15/3=5 iar $\hat{3}$ este o soluţie particulară, celelalte soluţii vor fi $\hat{3+5} = \hat{8}$ şi $\hat{3+2\cdot 5} = \hat{13}$. În concluzie, ecuaţia $\hat{6}\cdot\hat{x}=\hat{3}$ are în $\mathbb{Z}_{15}$ d=3 soluţii: $\hat{3}, \hat{8}$ şi $\hat{13}$. ■

COROLAR 4.7. Dacă n este număr prim, atunci ecuația $\hat{a}\hat{x} = \hat{b}$ are soluție unică $\mathbb{Z}_n$ dacă şi numai dacă (a, n)=1 $\Leftrightarrow$ n ł a.

§5. Fracţii periodice

Fiind dată fracția $\alpha = \frac{p}{q} \in \mathbb{Q}$, (cu $q \in \mathbb{N}^*$), prin împărțirea lui p la q putem scrie pe α sub formă de *fracţie zecimală*: $\alpha = a_0, a_1 a_2 \ldots$, cu $a_0, a_1, a_2, \ldots \in \mathbb{N}$ (în cele ce urmează prin diferite exemplificări se va deduce cu claritate modalitatea generală de reprezentare a numerelor raționale sub forma de fracții zecimale).

În cele ce urmează vom presupune că fracția α este subunitară (dacă ea este supraunitară, împărțind pe p la q putem scrie p=cq+r, cu $c \in \mathbb{Z}$ şi $0 \le r < q$ şi atunci $\alpha = \frac{p}{q} = c + \frac{r}{q}$, astfel că se continuă studiul lui α cu $\frac{r}{q}$ care este subunitară; convenim în acest caz să scriem $\alpha = \frac{p}{q} = c\frac{r}{q}$. De exemplu $\frac{35}{21} = 1\frac{2}{3}$).

În cazul în care $0 < \alpha < 1$, $a_0=0$ astfel că prin împărțiri repetate vom scrie $\alpha = 0, a_1 a_2 \ldots$, cu $a_i \in \mathbb{N}$.(după cum se va vedea în continuare şirul $a_1, a_2, \ldots$ poate fi finit sau infinit; (în cazul infinit anumite grupuri de cifre se vor repeta periodic).

Iată câteva exemplificări:

E_1: $\alpha = \frac{7}{20} = 0,35$

E_2: $\alpha = \frac{2}{3} = 0,666\ldots$ (se repetă cifra 6; convenim să scriem $\alpha = 0,(6)$)

E_3: $\alpha = \frac{8}{21} = 0,380952380952\ldots$(se repetă grupul de cifre 380952 şi vom scrie $\alpha = 0,(380952)$)

E_4: $\alpha = \frac{1}{7} = 0,142857142857\ldots = 0,(142857)$

E_5: $\alpha = \frac{5}{24} = 0,208333\ldots$ (se repetă 3 caz în care vom scrie $\alpha = 0,208(3)$)

E_6: $\alpha = \frac{7}{22} = 0,31818\ldots$(se repetă 18 caz în care vom scrie $\alpha = 0,3(18)$).

Să facem acum câteva observații:

1. În exemplul 1 împărțirea se termină cu a doua zecimală.

2. În exemplele 2 şi 3 împărțirea se continuă indefinit, grupurile de cifre 6 şi 380952 repetându-se de o infinitate de ori. În aceste cazuri convenim să spunem că avem de a face cu *fracţii periodice simple*.

În cazul exemplului 6, fracția zecimală obținută este tot periodică, cu perioada 18, dar observăm că perioada nu începe imediat după virgulă (ca în exemplul 2) ci este precedată de o parte care nu se repetă (cifra 3). Convenim să spunem că avem de a face cu o *fracție periodică mixtă*.

În cele ce urmează vom proba că în general dacă avem o fracție subunitară, atunci şirul $a_1, a_2, \ldots$ este sau finit sau periodic.

Să urmărim exemplul 4: resturile parțiale trebuie să fie mai mici decât 7.

În cazul exemplului 3 sunt posibile a priori 20 de resturi, deci după cel mult 20 de împărțiri parțiale trebuie să întâlnim un rest care a mai fost obținut şi ştim că de îndată ce restul se repetă şi cifrele încep să se repete.

În general, dacă q este câtul, resturile parțiale fiind mai mici decât q, după *cel mult q* împărțiri parțiale resturile parțiale şi deci cifrele câtului încep să se repete. Am subliniat *cel mult q* împărțiri, deoarece exemplele ne arată că repetarea resturilor parțiale poate începe şi înainte de a fi trecut prin toate resturile posibile a priori.

Să adâncim acum chestiunea :

Observația de bază este următoarea: fiind dată fracția subunitară $\frac{b}{a}$, pentru a găsi primele n cifre ale fracției zecimale în care se transformă ea, facem împărțirea *întreagă* 10^nb:a.

Exemplu. Pentru a găsi primele 4 zecimale ale fracției $\frac{8}{21}$, facem împărțirea.

80 000:21= 3809.
170
200
11

Să considerăm acum o fracție cu numărătorul 1, de exemplu $\frac{1}{21}$ şi să facem împărțirile întregi 10:21;100:21; 1000:21, etc. Resturile acestor împărțiri reoroduc tocmai resturile parțiale din împărțirea

10 : 21=0,47619….
100
84
160
147
130
126
40
21

$$\begin{array}{r} \overline{190} \\ \underline{189} \\ 1 \end{array}$$

$$\begin{array}{llll} 10:21=0 & 100:21=4 & 1000:21=47 & 10\,000:21=476 \\ \underline{10} & \underline{16} & \underline{13} & \underline{4} \end{array}$$

$$\begin{array}{rrrr} 100\ 000: & 21=4\ 761 & 1\ \underline{000\ 000}: & 21=47619 \\ 19 & & 1 & \end{array} \quad (1)$$

Pentru a şti în ce fel se transformă fracţia $\frac{1}{a}$, trebuie deci să urmărim resturile obţinute prin împărţirea lui 10, 10^2, 10^3,…prin a. Este o chestiune deja studiată .

1). Să începem cu cazul *a este prim cu 10* (adică a descompus în factori primi nu are nici pe 2 nici pe 5 ca factori)

Ştim din cele expuse mai înainte că, în acest caz, resturile încep să se repete după ce întâlnim restul 1, până acolo resturile fiind toate diferite. Ştim că dacă $10^d \equiv 1$ (a), d este un divizor al lui φ(a). Ştim că, dacă $a=p^\alpha q^\beta r^\gamma$…, cel mai mic exponent n, astfel ca să avem $b^n \equiv 1$ (a) oricare ar fi b prim cu a, este c. m. m. m. c al numerelor $\varphi(p^\alpha)$, $\varphi(q^\beta)$, $\varphi(r^\gamma)$,…(vezi Corolarul 6.2.).

Rezultă că: dacă a este prim cu 10, primul rest care se repetă în împărţirea 1:a este 1 (adică numărul cu care am început), deci *fracţia zecimală este periodică simplă.*

De exemplu: $\frac{1}{21}$, $21=3\cdot7$; φ(3)=2; φ(7)=6; c.m.m.m.c. al numerelor φ(3) şi φ(7) este 6. Fracţia $\frac{1}{21}$ este periodică simplă şi perioada ei este un divizor al lui 6.

Dacă numărătorul nu este 1, ci un alt număr prim cu a, rezultatele enunţate se menţin. De exemplu, în împărţirea 8:21 obţinem ca resturile împărţirilor întregi succesive 80:21; $8\cdot10^2$:21; $8\cdot10^3$:21… Aceste resturi se pot obţine dacă înmulţim resturile (2) cu 8 (21).

$8\cdot10=80\equiv17$ (21); $8\cdot16=128\equiv2$ (21); $8\cdot13=104\equiv20$ (21)

$8\cdot4=32\equiv11$ (21); $8\cdot19=152\equiv5$ (21); $8\cdot1=8\equiv8$ (21).

Dacă resturile şirului (1) sunt toate diferite între ele, prin înmulţirea lor cu 8 obţinem tot resturi diferite (dacă $8r_1$ ar fi congruent cu $8r_2$, atunci $8r_1-8r_2\equiv0$ (21); $8(r_1-r_2)\equiv0$ (21), 8 este prim cu 21 pentru că fracţia a fost reductibilă; $r_2-r_1<21$, deci nu putem avea $8(r_2-r_1)$= multiplu de 21.

Rezultă că fracţia $\frac{8}{21}$ este tot periodocă simplă, iar numărul cifrelor perioadei este acelaşi ca şi la fracţia $\frac{1}{21}$.

Fie acum cazul $a=2^\alpha\cdot5^\beta$, adică a are numai factori primi ai lui 10.

(De exemplu, $a=40=2^3\cdot 5$ sau $a=25=5^2$, etc). În acest caz, 10 ridicat la puterea α, dacă $\alpha>\beta$, sau la puterea β, dacă $\beta>\alpha$ se divide cu a (dacă $a=40$, $10^3=2^3\cdot 5^3$ se divide cu $2^3\cdot 5$; dacă $a=25$, $10^2=2^2\cdot 5^2$ se divide cu 5^2).

Rezultă că, în acest caz, fracția zecimală rezultând din $\frac{1}{a}$ are un număr finit de zecimale, egal cu cel mai mare dintre numerele α şi β.

De exemplu : $20=2^2\cdot 5$; $7:20=0,35$.

În general : $\frac{b}{2^\alpha\cdot 5^\beta}=\frac{b\cdot 5^{\alpha-\beta}}{10^\alpha}$ (dacă $\alpha>\beta$) sau $=\frac{b\cdot 5^{\beta-\alpha}}{10^\beta}$ (dacă $\alpha<\beta$), însă împărțirea unui număr cu 10^α se face despărțind prin virgulă α cifre.

$3^0\cdot a=2^\alpha\cdot 5^\beta p^m\cdot q^n\ldots$

În acest caz, fracția $\frac{b}{a}$ poate fi scrisă $\frac{b}{a}=\frac{1}{10^\alpha}\cdot\frac{b\cdot 5^{\alpha-\beta}}{p^m q^n\ldots}$ (dacă $\alpha>\beta$).

Fracția $\frac{b\cdot 5^{\alpha-\beta}}{p^m q^n\ldots}$ se transformă într-o fracție periodică simplă. Dacă ea este mai mare decât 1 – ceea ce se poate întâmpla din cauza înmulțirii cu $5^{\alpha-\beta}$ - ea se transformă tot într-o fracție periodică simplă, având însă şi întregi. Această fracție înmulțită cu $\frac{1}{10^\alpha}$ (adică mutând virgula cu α cifre spre stânga), ne dă fracția $\frac{b}{a}$, care va avea ca parte neperiodică cele α cifre, iar partea periodică aceeaşi ca şi a fracției $\frac{b\cdot 5^{\alpha-\beta}}{p^m q^n\ldots}$.

Dacă $\beta>\alpha$ procedăm analog.

Exemplu $\frac{7}{22}=\frac{7}{2\cdot 11}=\frac{1}{10}\cdot\frac{5\cdot 7}{11}$; $\frac{35}{11}=3,1818...$, deci $\frac{7}{22}=3,1818...=0,3(18)$.

Dar $\frac{1}{22}=\frac{1}{2\cdot 11}=\frac{1}{10}\cdot\frac{5}{11}$; $\frac{5}{11}=0,4545.....$ Deci $\frac{1}{22}=0,04545....=0,0(45)$ partea neperiodică este 0.

Rezumând cele de mai sus obținem:

<u>TEOREMA 5.1.</u> Orice fracție se transformă într-o fracție zecimală cu un număr finit de zecimale sau într-o fracție zecimală cu un număr înfinit de zecimale, în care caz zecimalele admit o perioadă ce se repetă.

Reciproc, să vedem cum rescriem o fracție zecimală α (simplă, periodică sau periodică mixtă) sub forma $\frac{p}{q}$ cu $p, q\in\mathbb{N}$.

<u>Cazul 1.</u> Dacă $\alpha=a_0, a_1a_2\ldots a_n$, atunci în mod evident $\alpha=\frac{\overline{a_0a_1\ldots a_k}}{10^k}$. De exemplu:

$$\alpha=1,7=\frac{17}{10},\ \alpha=0,3=\frac{3}{10}$$

Cazul 2. Să presupunem acum că $\alpha = a_0, (\overline{a_1 \ldots a_n})$. Atunci:

$$\alpha = a_0 + \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n}\right) + \left(\frac{a_1}{10^{n+1}} + \frac{a_2}{10^{n+2}} + \ldots + \frac{a_n}{10^{2n}}\right) + \ldots =$$

$$= a_0 + \frac{a_1}{10}\left(1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + \ldots\right) + \frac{a_2}{10^2}\left(1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + \ldots\right) + \ldots +$$

$$+ \frac{a_n}{10^n}\left(1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + \ldots\right)$$

Însă $1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + \ldots = \frac{1}{1 - \frac{1}{10^n}} = \frac{10^n}{10^n - 1}$ astfel că

$$\alpha = a_0 + \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_n}{10^n}\right)\frac{10^n}{10^n - 1} =$$

$$= a_0 + \frac{a_n + a_{n-1}10 + \ldots + 10^{n-1}}{10^n - 1} = a_0 + \frac{\overline{a_1 a_2 \ldots a_n}}{\underbrace{99\ldots9}_{n \text{ ori}}}.$$

De exemplu $\alpha = 3,(6) = 3 + \frac{6}{9} = \frac{27+6}{9} = \frac{33}{9} = \frac{11}{3}$ iar dacă $\alpha = 2,(154)$, atunci $\alpha = 2 + \frac{154}{999} = \frac{1998+154}{999} = \frac{2152}{999}$.

Cazul 3. Să presupunem că α este o fracție zecimală periodică mixtă : $\alpha = a_0, a_1a_2\ldots a_k(a_{k+1}a_{k+2}\ldots a_{k+n})$. Atunci $\alpha = a_0, a_1a_2\ldots a_k + 0,00\ldots0(a_{k+1}a_{k+2}\ldots a_{k+n}) =$

$$= \frac{\overline{a_0 a_1 \ldots a_k}}{10^k} + \frac{0,(a_{k+1}\ldots a_{k+n})}{10^k} = \frac{\overline{a_0 a_1 \ldots a_k}}{10^k} + \frac{\overline{a_{k+1}\ldots a_{k+n}}}{\underbrace{99\ldots9}_{n \text{ ori}}\underbrace{00\ldots0}_{k \text{ ori}}}.$$

De exemplu dacă $\alpha = 3,7(2) = \frac{37}{10} + \frac{2}{90} = \frac{37\cdot9+2}{90} = \frac{333+2}{90} = \frac{335}{90} = \frac{67}{18}$ iar dacă $\alpha = 2,15(172) = \frac{215}{100} + \frac{172}{99900} = \frac{215\cdot999+172}{99900} = \frac{214957}{99900}$.

Rezumând cele trei cazuri de mai sus obținem:

TEOREMA 5.2. i) Dacă $\alpha = a_0, a_1a_2\ldots a_k$, atunci $\alpha = \frac{\overline{a_0 a_1 \ldots a_k}}{10^k}$

ii) Dacă $\alpha = a_0, (\overline{a_1 \ldots a_n})$**, atunci** $\alpha = a_0 + \frac{a_n + a_{n-1}10 + \ldots + 10^{n-1}}{10^n - 1} = a_0 + \frac{\overline{a_1 a_2 \ldots a_n}}{\underbrace{99\ldots9}_{n \text{ ori}}}$

iii) Dacă $\alpha = a_0, a_1\ldots a_k(a_{k+1}\ldots a_{k+n})$, atunci

$$\alpha = \frac{\overline{a_0 a_1 \ldots a_k}}{10^k} + \frac{\overline{a_{k+1}\ldots a_{k+n}}}{\underbrace{99\ldots9}_{n \text{ ori}}\underbrace{00\ldots0}_{k \text{ ori}}}.$$

Observație Acest paragraf a fost redactat în cea mai mare parte după lucrarea [8].

§6.Teoremele lui Euler, Fermat şi Wilson

LEMA 6.1. Dacă G este un grup (multiplicativ) finit cu n elemente (n≥2), atunci $x^n=1$, pentru orice $x\in G$.

Demonstraţie Fie $x\in G$, iar $k=o(x)$ (ordinul lui x). Atunci $x^k=1$ şi conform Teoremei lui Lagrange $k|n$, adică $n=k\cdot p$ cu $p\in\mathbb{N}$. Deducem imediat că $x^n=x^{kp}=(x^k)^p=1^p=1$. ■

Observaţie În cazul că G este comutativ există o demonstraţie elementară ce evită Teorema lui Lagrange. Pentru aceasta se alege $G=\{x_1, x_2,\ldots,x_n\}$ şi $x\in G$. Cum $\{xx_1, xx_2,\ldots,xx_n\}=G=\{x_1,\ldots,x_n\}$, deducem că $(xx_1)\ldots(xx_n)=x_1\ldots x_n \Leftrightarrow x^n(x_1\ldots x_n) = x_1\ldots x_n \Leftrightarrow x^n=1$. ■

COROLAR 6.2. (Euler) Dacă $n \geq 2$ este un număr natural iar $a\in\mathbb{Z}$ a.î. $(a, n)=1$, atunci $a^{\varphi(n)} \equiv 1(n)$ (φ fiind indicatorul lui Euler).

Demonstraţie Am văzut mai înainte că $(\mathbb{Z}_n, \cdot)$ este un monoid cu $\varphi(n)$ elemente inversabile. Astfel, dacă aplicăm Lema 6.1. grupului $G=U(\mathbb{Z}_n, \cdot)$ (ce are $\varphi(n)$ elemente) pentru $\hat{a} \in G$ obţinem că :

$$\hat{a}^{\varphi(n)} = \hat{1} \Leftrightarrow \overset{\wedge}{a^{\varphi(n)}} = \hat{1} \Leftrightarrow n \mid a^{\varphi(n)} - 1 \Leftrightarrow a^{\varphi(n)} \equiv 1(n). \quad \blacksquare$$

COROLAR 6.3. (Mica teoremă a lui Fermat) Dacă $p\geq 2$ este un număr prim, iar $a\in\mathbb{Z}$ a.î. $p\nmid a$, atunci $a^{p-1} \equiv 1(p)$.

Demonstraţie Cum p este un număr prim, $\varphi(p)=p-1$ şi acum totul rezultă din Corolarul 6.2. ■

LEMA 6.4. Fie G un grup (multiplicativ) finit comutativ iar $\prod_{x\in G} x$ produsul tuturor elementelor din G. Atunci $\prod_{x\in G} x = \prod_{\substack{x\in G \\ o(x)\leq 2}} x$.

Demonstraţie Vom scrie $\prod_{x\in G} x = (\prod_{\substack{x\in G \\ o(x)\leq 2}} x)(\prod_{\substack{x\in G \\ o(x)>2}} x)$. Însă în cadrul produsului $\prod_{\substack{x\in G \\ o(x)>2}} x$ vom grupa fiecare element x cu x^{-1} (avem $x\neq x^{-1}$ căci dacă $x=x^{-1}$

atunci $x^2=1$ şi deci o(x)=2, absurd) şi astfel $\prod_{\substack{x\in G\\ o(x)>2}} x=1$, de unde concluzia că

$\prod_{x\in G} x = \prod_{\substack{x\in G\\ o(x)\le 2}} x$. ■

COROLAR 6.5. (Wilson) Dacă p≥2 este un număr prim, atunci (p-1)!+1≡0(p).

Demonstraţie Cum p este prim $(\mathbb{Z}_p^*, \cdot)$ este grup cu p-1 elemente şi conform Lemei 5.4., $\prod_{\hat{x}\in Z_p^*} \hat{x} = \prod_{\substack{\hat{x}\in Z_p^*\\ o(\hat{x})\le 2}} \hat{x}$. Rămăne să punem în evidenţă elementele

$\hat{x} \in \mathbb{Z}_p^*$ cu proprietatea că $o(\hat{x}) = 2 \Leftrightarrow \hat{x}^2 = \hat{1} \Leftrightarrow \hat{x}^2 = \hat{1} \Leftrightarrow p|x^2-1=(x-1)(x+1)$

$\Leftrightarrow$ p|x-1 sau p|x+1 de unde deducem că $\hat{x} = -\hat{1} = \widehat{p-1}$ sau $\hat{x} = \hat{1}$ astfel că

$\hat{1}\cdot\hat{2}\ldots\widehat{p-1} = -\hat{1} \Leftrightarrow \widehat{(p-1)!} + \hat{1} = \hat{0} \Leftrightarrow (p-1)!+1\equiv 0(p)$. ■

Vom prezenta în continuare diferite variante de generalizare a Teoremei lui Wilson.

LEMA 6.6. Fie p≥2 un număr prim, iar n≥2 un număr natural. Atunci :

i) Dacă p=2 şi n>2 în grupul $U(\mathbb{Z}_2^n,\cdot)$ numai elementele $\hat{1}, -\hat{1}, \widehat{2^{n-1}+1}, \widehat{2^{n-1}-1}$ au ordinul cel mult 2.

ii) Dacă p>2 atunci în grupul $U(\mathbb{Z}_p^n,\cdot)$ numai elementele $\hat{1}, -\hat{1}$ au ordinul cel mult 2.

Demonstraţie Avem că $U(Z_{p^n}^*,\cdot)=\{\hat{a} \in Z_{p^n}^*, (a,p)=1\}$. Să determinăm în acest grup elementele $\hat{a} \in U(Z_{p^n}^*,\cdot)$ a.î $\hat{a}^2=1$, adică acele numere naturale a a.î. $1\le a<p^n$, cu (a, p)=1 şi $p^n \mid a^2-1$ (∗).

Evident a=1 verifică (∗). Dacă a>1, atunci putem scrie $a-1=p^k u$ şi $a+1=p^t v$ cu k, t ≥ 0, (p, u)=(p, v)=1, iar k+t≥n.

Dacă k=0 $\Rightarrow$ t ≥ n $\Rightarrow$ p^n | a+1 şi cum a < p^n $\Rightarrow$ a+1=p^n $\Rightarrow$ a= p^n-1 şi astfel obţinem şi elementul $\hat{a} = \overset{\wedge}{p^n - 1} = -\hat{1}$ ce verifică de asemenea (∗).

Dacă t=0 $\Rightarrow$ k >n $\Rightarrow$ p^n |a-1 şi cum a < p^n $\Rightarrow$ a-1=0 $\Rightarrow$ a=1, contradicţie.

Dacă k≠0, t≠0 $\Rightarrow$ 2=p^tv-p^ku $\Rightarrow$ p|2, deci dacă p≥2, obţinem o contradicţie.

În concluzie : dacă p >2, atunci în $U(Z^*_{p^n})$ avem numai elementele $\hat{1}$ şi $-\hat{1} = \overset{\wedge}{p^n - 1}$ ce au ordinul cel mult 2, obţinând astfel concluzia de la ii).

Dacă p=2, atunci din 2=2^tv-2^ku $\Rightarrow$ t=1 sau k=1. Dacă t=1 $\Rightarrow$ k ≥ n-1$\Rightarrow$ a-1=2^ku ≥ 2^{n-1}u şi cum 1<a<2^n $\Rightarrow$ u=2 şi k=n-1. Deci, în acest caz, dacă a verifică (∗)$\Rightarrow$a=2^{n-1}+1.

Dacă k=1$\Rightarrow$ t ≥ n-1$\Rightarrow$ a+1=2^tv ≥ 2^{n-1}v şi cum 1<a<2^n $\Rightarrow$ v=1 sau v=2 (cazul v=2 este exclus căci (v, 2)=1)

Dacă v=1 $\Rightarrow$ t = n-1 sau t = n. În cazul t=n-1$\Rightarrow$a=2^{n-1}-1, iar dacă t=n $\Rightarrow$a=2^n-1.

În concluzie : dacă p=2 şi n>2 în $U(Z^*_{2^n})$ numai elemente $-\hat{1}, \hat{1}, \overset{\wedge}{2^{n-1}+1}, \overset{\wedge}{2^{n-1}-1}$ au ordinul cel mult 2, obţinând astfel concluzia de la i).

■

<u>COROLAR 6.7.</u> (O generalizare a teoremei lui Wilson) Dacă p este un număr prim şi n un număr natural, atunci:

a) Dacă p>2 şi n ≥2 atunci $p^n \mid \left(\prod_{\substack{1\le a<p^n \\ (a,p)=1}} a\right)+1$

b) Dacă p=2 şi n >2 atunci : $2^n \mid \left(\prod_{\substack{1\le a<2^n \\ (a,2)=1}} a\right)-1$

c) Dacă p=2 şi n=2 atunci : $2^2 \mid \left(\prod_{\substack{1\le a<2^2 \\ (a,2)=1}} a\right)+1$

<u>*Demonstraţie*</u> Totul rezultă imediat din Lema 5.4 ţinând cont de cele stabilite în Lema 6.6. ■

§7.Teorema chinezească a resturilor

Fie $m_1, m_2, \ldots, m_t \in \mathbb{N}$ a.î. $(m_i, m_j)=1$ pentru orice $i \neq j$, $m=m_1m_2\ldots m_t$, iar $b_1, b_2, \ldots, b_t \in \mathbb{Z}$.

TEOREMA 7.1. (Teorema chinezească a resturilor)
Sistemul

$$(S)\begin{cases} x \equiv b_1 \ (m_1) \\ \ldots\ldots\ldots \\ x \equiv b_t \ (m_t) \end{cases}$$

are soluție în $\mathbb{Z}$ şi oricare două soluții diferă printr-un multiplu de m.

Demonstrație Dacă $n_i=\frac{m}{m_i}$, atunci $(m_i, n_i)=1$ pentru orice $1 \leq i \leq t$. Astfel există $r_i, s_i \in \mathbb{Z}$ a.î. $r_i m_i+s_i n_i=1$ pentru orice $1 \leq i \leq t$.

Dacă notăm $e_i=s_i n_i$, atunci $e_i \equiv 1(m_i)$ şi $e_i \equiv 0(m_j)$ pentru $1 \leq i, j \leq t$, $i \neq j$.

Dacă vom considera $x_0=\sum_{i=1}^{t} b_i e_i$, atunci vom avea $x_0 \equiv b_i e_i \ (m_i)$ şi astfel $x_0 \equiv b_i (m_i)$ pentru orice $1 \leq i \leq t$, de unde concluzia că x_0 soluție a lui (S).

Să presupunem că x_1 este o altă soluție a lui (S). Atunci $x_1-x_0 \equiv 0 \ (m_i)$ pentru $1 \leq i \leq t$, adică $m_i \mid x_1-x_0$ pentru orice $1 \leq i \leq t$, şi cum $(m_i, m_j)=1$ pentru $i \neq j$, deducem că $m=m_1m_2\ldots m_t \mid x_0-x_1$, adică $x_0 \equiv x_1(m)$. ■

Să interpretăm acum teorema chinezească a resturilor din punct de vedere al teoriei inelelor.

Fie pentru aceasta $(A_i)_{i\in I}$ o familie nevidă de inele (unitare).Vom considera un nou inel notat $\prod_{i\in I} A_i$ şi având mulțimea subiacentă $\prod_{i\in I} A_i = \{(x_i)_{i\in I} \mid x_i \in A_i \text{ pentru orice } i \in I\}$, iar pentru $x,y \in \prod_{i\in I} A_i$, $x=(x_i)_{i\in I}$ şi $y=(y_i)_{i\in I}$, $x+y=(x_i+y_i)_{i\in I}$, iar $x \cdot y=(x_i \cdot y_i)_{i\in I}$.

Se verifică imediat că $(\prod_{i\in I} A_i, +, \cdot)$ devine inel unitar în care elementul nul este $0=(x_i)_{i\in I}$ cu $x_i=0$ pentru orice $i \in I$, iar pentru $x=(x_i)_{i\in I} \in A$, $-x=(-x_i)_{i\in I}$; elementul unitate este $1=(x_i)_{i\in I}$ cu $x_i=1$ pentru orice $i \in I$, iar dacă $x=(x_i)_{i\in I} \in$

$\in \prod_{i\in I} A_i$, atunci $x\in U(\prod_{i\in I} A_i)$ dacă şi numai dacă $x_i\in U(A_i)$ pentru orice $i\in I$, altfel zis $U(\prod_{i\in I} A_i)=\prod_{i\in I} U(A_i)$.

Dacă I este finită notăm $\prod_{i\in I} A_i = \underset{i\in I}{X} A_i$.

Fie acum $m_1, m_2, \ldots, m_t\in\mathbb{N}^*$ a.î. $(m_i, m_j)=1$ pentru orice $i\neq j$, $1\leq i, j\leq t$ şi $m=m_1m_2\ldots m_t$.

TEOREMA 7.2. Avem următorul izomorfism de inele :

$$Z_{m_1}\times Z_{m_2}\times\ldots\times Z_{m_t}\approx Z_m.$$

Demonstraţie. Pentru fiecare $1\leq i\leq t$ fie $\pi_i: \mathbb{Z}\to Z_{m_i}$ morfismul surjectiv canonic de inele ce duce fiecare element $x\in\mathbb{Z}$ în clasa sa de echivalenţă modulo m_i.

Definim $f : Z_m\to Z_{m_1}\times Z_{m_2}\times\ldots\times Z_{m_t}$ prin $f(x)=(\pi_1(x),\ldots,\pi_t(x))$ pentru orice $x\in\mathbb{Z}$.

Dacă $x, y\in\mathbb{Z}$ şi $f(x)=f(y)$ atunci $x\equiv y(m) \Leftrightarrow x\equiv y(m_i)$ pentru orice $1\leq i\leq t$ (căci $(m_i, m_j)=1$ pentru $1\leq i\neq j\leq t$) $\Leftrightarrow \pi_i(x)=\pi_i(y)$ pentru orice $1\leq i\leq t$. Deducem astfel că f este bine definită şi că funcţia f este o injecţie. Se verifică imediat că f este morfism de inele unitare .

Surjectivitatea lui f rezultă fie din teorema chinezească a resturilor, fie observând că $|Z_{m_1}\times Z_{m_2}\times\ldots\times Z_{m_t}|=|Z_m| = m = m_1\ldots m_t$.

Deci f este un izomorfism de inele unitare. ■

COROLAR 7.3. Cu notaţiile de la teorema precedentă avem următorul izomorfism de grupuri multiplcative :

$$U(Z_m)\approx U(Z_{m_1})\times\ldots\times U(Z_{m_t}).$$

COROLAR 7.4. Fie $\varphi:\mathbb{N}\to\mathbb{N}$ indicatorul lui Euler.

i) Dacă $m_1, m_2, \ldots, m_t\in\mathbb{N}^*$ a.î. $(m_i, m_j)=1$ pentru $i\neq j$, atunci $\varphi(m_1\ldots m_t)=\varphi(m_1)\ldots\varphi(m_t)$

ii) Dacă $p\geq 2$ este număr prim şi $n\in\mathbb{N}^*$, atunci $\varphi(p^n) = p^n - p^{n-1} = p^n(1-1/p)$

iii) Dacă $n=p_1^{k_1}\dots p_t^{k_t}$ este descompunerea în factori primi a lui n, atunci $\varphi(n) = n\,(1-1/p_1)\dots(1-1/p_t)$.

Demonstraţie. i) Am văzut că $|U(Z_m)|=\varphi(n)$ pentru orice $n\in\mathbb{N}$, $n \geq 2$. Dacă ţinem cont de Corolarul 7.3. deducem că

$$\left| U(Z_m) \right| = \left| U(Z_{m_1})\times\dots\times U(Z_{m_t}) \right| = \left| U(Z_{m_1}) \right| \dots \left| U(Z_{m_t}) \right| \Leftrightarrow$$

$$\varphi(m)=\varphi(m_1)\dots\varphi(m_t)$$

ii) Prin calcul direct se deduce că între 1 şi p^n există $p^n - p^{n-1}$ numere naturale mai mici strict decât p^n şi prime cu p^n (adică cu p), de unde egalitatea $\varphi(p^n)=p^n-p^{n-1}$

iii)Ţinând cont de i) şi ii) deducem că

$$\varphi(n) = \varphi(p_1^{k_1})\dots\varphi(p_t^{k_t}) = (p_1^{k_1} - p_1^{k_1-1})\dots(p_t^{k_t} - p_t^{k_t-1}) =$$

$$= p_1^{k_1}\dots p_t^{k_t}(1-1/p_1)\dots(1-1/p_t) = n(1-1/p_1)\dots(1-1/p_t).$$

De exemplu , $\varphi(12)=\varphi(2^3\cdot 3)=12(1-1/2)(1-1/3)=12\cdot(1/2)(2/3)=4$. ■

§8. Rădăcini primitive modulo un număr prim

Dacă $n=p_1^{k_1}\dots p_s^{k_s}$ este descompunerea în factori primi a lui n, conform Corolarului 6.3., $U(Z_n)\approx U(Z_{p_1^{k_1}})\times\dots\times U(Z_{p_s^{k_s}})$ astfel, pentru a determina structura grupului multiplicativ $U(\mathbb{Z}_n)$ este suficient să studiem structura grupurilor de forma $U(\mathbb{Z}_p^n)$ cu p prim şi $n\in\mathbb{N}$.

Vom începe cu cazul cel mai simplu şi anume cu $U(\mathbb{Z}_p)$ cu p prim. Cum $\mathbb{Z}_p$ este corp, $U(\mathbb{Z}_p)=\mathbb{Z}_p^*$. Dacă $f=a_0+a_1X+\dots+a_nX^n\in\mathbb{Z}[X]$, vom nota $\hat{f} = \hat{a}_0 + \hat{a}_1 X + \dots + \hat{a}_n X^n \in \mathbb{Z}_p[X]$.

LEMA 8.1. Fie K un corp comutativ şi $f\in K[X]$ cu grad(f)=n. Atunci f are cel mult n rădăcini distincte.

Demonstraţie Facem inducţie matematică după n. Cum pentru n=1 totul este clar, să presupunem că afirmaţia din enunţ este adevărată pentru orice polinom din K[x] de grad ≤ n-1.

Dacă f nu are rădăcini în K totul este clar.

Dacă există $\alpha\in k$ a.î. $f(\alpha)=0$, atunci $f(x)=q(x)(x-\alpha)$ şi grad (q)=n-1.

Dacă β este o altă rădăcină a lui f, $\beta\neq\alpha$, atunci $0=f(\beta)=(\beta-\alpha)q(\beta)$ ceea ce implică $q(\beta)=0$. Cum prin ipoteza de inducţie q are cel mult n-1 rădăcini distincte, deducem că f are cel mult n rădăcini distincte.■

COROLAR 8.2. Fie K un corp comutativ f, g∈K[X] a.î. grad(f)=grad(g)=n. Dacă avem n+1 elemente distincte $\alpha_1,\alpha_2,\ldots,\alpha_{n+1}$, a.î. $f(\alpha_i)=g(\alpha_i)$ pentru orice $1\le i\le n+1$ atunci f=g.

Demonstrație Considerând h=f-g, atunci grad(h)≤n şi cum h are n+1 rădăcini distincte $\alpha_1,\alpha_2,\ldots,\alpha_{n+1}$, deducem că h=0, adică f=g. ■

COROLAR 8.3. Dacă p≥2 este un număr prim, atunci orice x∈ℤ, avem: $x^{p-1}-1\equiv(x-1)(x-2)\ldots(x-p+1)\ (p)$.

Demonstrație Cum p este prim, $\mathbb{Z}_p$ este corp comutativ. Considerând $f=(x^{p-1}-\hat{1})-(x-\hat{1})(x-\hat{2})\ldots(x-(\widehat{p-1}))\in Z_p[X]$ avem că grad(f)≤p-2 şi $f(\hat{x})=\hat{0}$ pentru $\hat{x}=\hat{1},\hat{2},\ldots,\widehat{p-1}$ (ținând cont şi de mica teoremă a lui Fermat, adică de Corolarul 6.3.). Conform Corolarului 8.2., f=0. ■

Observație Dacă în corolarul 8.3. considerăm x=0 obținem că (p-1)!≡-1(p), adică teorema lui Wilson (Corolarul 6.5.).

PROPOZIȚIA 8.4. Fie p≥2 un număr prim şi d|p-1. Atunci congruența $x^d\equiv 1(p)$ are exact d soluții.

Demonstrație Dacă p-1=dd′, atunci:

$$\frac{x^{p-1}-1}{x^d-1}=\frac{(x^d)^{d'}-1}{x^d-1}=(x^d)^{d'-1}+(x^d)^{d'-2}+\ldots+x^d+1=g(x),\text{ adică}$$

$x^{p-1}-1=(x^d-1)g(x)$ şi astfel $x^{p-1}-\hat{1}=(x^d-\hat{1})g(x)$.

Cum $x^{p-1}-\hat{1}$ are exact p-1 rădăcini (şi anume $\hat{1},\hat{2},\ldots,\widehat{p-1}$ -conform micii teoreme a lui Fermat), ținând cont de Lema 8.1. deducem că $x^d-\hat{1}$ are exact d rădăcini în $\mathbb{Z}_p$ şi astfel congruența $x^d\equiv 1(p)$ are exact d soluții în $\mathbb{Z}_p$.■

TEOREMA 8.5. Dacă p este un număr prim, atunci $U(\mathbb{Z}_p)$ este un grup ciclic.

Demonstrație

Soluția 1: Evident | U($\mathbb{Z}_p$) | = | $\mathbb{Z}_p^*$ | = p-1 iar pentru d | p-1, fie ψ(d) numărul elementelor din $\mathbb{Z}_p^*$ de ordin d. Conform Propoziției 8.4. elementele din $\mathbb{Z}_p^*$ ce satisfac congruența $x^d \equiv 1(p)$ formează un grup de ordin d. Însă $\sum_{c|d} \psi(c) = d$, de unde se deduce că ψ(d) = φ(d) (φ fiind indicatorul lui Euler). În particular, ψ(p-1) = φ(p-1)>1 (dacă p≥ 3). Deducem că în $\mathbb{Z}_p^*$, φ(p-1) elemente au ordinul p-1 şi astfel oricare dintre aceştia generează pe $\mathbb{Z}_p^*$, adică $\mathbb{Z}_p^*$ este grup multiplicativ ciclic.

Soluția 2: Fie $p-1 = q_1^{l_1} q_2^{l_2} \dots q_t^{l_t}$ descompunerea în factori primi a lui p-1 şi să considerăm congruențele:

(1) $x^{q_i^{l_i-1}} \equiv 1(p)$

(2) $x^{q_i^{l_i}} \equiv 1(p)$ cu $1 \le i \le t$

În mod evident orice soluție a congruentei (1) este soluție şi a congruenței (2). Mai mult, congruența (2) are mai multe soluții decât congruența (1). Pentru fiecare $1 \le i \le t$ fie g_i o soluție a congruentei (2) ce nu este soluție a congruenței (1) iar $g = g_1 g_2 \dots g_t$.

Evident, $\hat{q_i}$ genereaza un subgrup al lui $\mathbb{Z}_p^*$ de ordin $q_i^{l_i}$, $1 \le i \le t$. Deducem ca $\hat{g}$ genereaza un subgrup al lui $\mathbb{Z}_p^*$ de ordin $p-1 = q_1^{l_1} q_2^{l_2} \dots q_t^{l_t}$. Atunci $< \hat{g} > = \mathbb{Z}_p^*$. ■

DEFINITIA 8.6. Fie p≥2 un numar prim. Un element a∈Z se zice *rădăcină primitivă* modulo p dacă $\hat{a}$ generează $\mathbb{Z}_p^*$.

De exemplu, 2 este rădăcină primitivă modulo 5 (se verifică imediat că 4=5-1 este cel mai mic număr natural n pentru care $2^n \equiv 1(5)$), pe când 2 nu este rădăcină primitivă modulo 7 (de ex. $2^3 \equiv 1(7)$).

Noțiunea de rădăcină primitivă se poate generaliza astfel:

DEFINIȚIA 8.7. Fie n∈ℕ. Un element a∈ℤ se zice *rădăcină primitivă modulo n* dacă $\hat{a}$ în $\mathbb{Z}_n$ generează U($\mathbb{Z}_n$). (echivalent cu a spune că φ(n) este cel mai mic număr natural pentru care $a^{\varphi(n)} \equiv 1(n)$).

Observație În general nu rezultă că U($\mathbb{Z}_n$)este ciclic.

De exemplu, elementele lui $U(\mathbb{Z}_8)$ sunt $\hat{1}, \hat{3}, \hat{5}, \hat{7}$ iar $\hat{1}^2=\hat{1}, \hat{3}^2=\hat{1}, \hat{5}^2=\hat{1}, \hat{7}^2=\hat{1}$ neexistând deci în $U(\mathbb{Z}_8)$ elemente de ordin $4=\varphi(8)$.

Rezultă că nu orice întreg posedă rădăcini primitive.

LEMA 8.8. Dacă p este un număr natural prim şi $1\le k<p$ atunci $p \mid C_p^k$.

Demonstraţie Avem $C_p^k = \frac{p!}{k!(p-k)!} \in \mathbb{N}$ şi cum $\frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!}$ iar p nu divide nici pe k! şi nici pe (p-k)!, deducem că dacă notăm $q = \frac{(p-1)!}{k!(p-k)!}$, atunci $q\in\mathbb{N}$ şi cum $C_p^k = p \cdot q$,atunci $p \mid C_p^k$.■

Observaţie Utilizând Lema 8.8. putem prezenta o nouă demonstraţie a micii teoreme a lui Fermat : Dacă p este un număr prim şi $a\in\mathbb{Z}$ a.î. $p\nmid a$, atunci $p|a^{p-1}-1$.

Într-adevăr, să notăm $s_a=a^p-a$. Cum $s_{a+1} = (a+1)^p-(a+1)=$

$$= a^p + C_p^1 a^{p-1} + ... + C_p^{p-1} a + 1 - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} C_p^k a^{p-k} =$$

$$= s_a + \sum_{k=1}^{p-1} C_p^k a^{p-k}$$

Ţinând cont de Lema 8.8. deducem că $s_{a+1}\equiv s_a(p)$.

Astfel $s_a\equiv s_{a-1}\equiv s_{a-2}\equiv\ldots\equiv s_1(p)$ şi cum $s_1=1^a-1=0$ deducem că $s_a\equiv 0(p)$, adică $p|a^p-a=a(a^{p-1}-1)$ şi cum $p\nmid a$ obţinem că $p \mid a^{p-1}-1$.

LEMA 8.9. Dacă $n\ge 1$ este un număr natural, $p\ge 2$ un număr prim şi $a, b\in\mathbb{Z}$ a.î. $a\equiv b(p^n)$, atunci $a^p \equiv b^p(p^{n+1})$.

Demonstraţie Putem scrie $a=b+cp^n$, cu $c\in\mathbb{Z}$.

Atunci $a^p=(b+cp^n)^p = b^p + C_p^1 b^{p-1} c\, p^n + x$ (cu $x\in\mathbb{Z}$ şi $p^{n+2} \mid x$) astfel că $a^p = b^p + b^{p-1} c\, p^{n+1} + x$, de unde $a^p \equiv b^p(p^{n+1})$.■

COROLAR 8.10. Dacă p este un număr prim, $p\ge 3$, $n\in\mathbb{N}$, $n\ge 2$, atunci $(1+ap)^{p^{n-2}} \equiv 1 + a\, p^{n-1}(p^n)$ pentru orice $a\in\mathbb{Z}$.

Demonstraţie Facem inducţie după n, pentru n=2 afirmaţia fiind trivială

Să presupunem acum că afirmaţia din enunţ este adevărată pentru n şi să arătăm că este adevărată pentru n+1.

Conform Lemei 8.9. avem: $(1+ap)^{p^{n-1}} \equiv (1+a\,p^{n-1})^{p}\,(p^{n+1})$.

Dezvoltând cu ajutorul binomului lui Newton obţinem $(1+a\,p^{n-1})^{p} = 1 + C_p^1 a\,p^{n-1} + \beta$, unde β este o sumă de p-2 termeni. Utilizând din nou Lema 7.9. se verifică imediat că toţi termenii lui β sunt divizibili prin $p^{1+2(n-1)}$, exceptând eventual ultimul termen $a^p p^{p(n-1)}$. Cum n≥2, 1+2(n-1)≥n+1 şi cum p(n-1) ≥ n+1, adică $p^{n+1}|\beta$ şi astfel $(1+ap)^{p^{n-2}} \equiv 1 + a\,p^{n}\,(p^{n+1})$ adică c.c.t.d.■

Observaţie Fie a, n∈ℤ a.î. (a, n)=1. Vom spune că a are *ordinul* k modulo n dacă este cel mai mic număr natural pentru care $a^k \equiv 1(n)$. Acest lucru este echivalent cu a spune că $\hat{a}$ din $\mathbb{Z}_n$ are ordinul k în grupul $U(\mathbb{Z}_n)$.

COROLARUL 8.11. Dacă p ≠2 este un număr prim a.î. p∤a, atunci ordinul lui 1+ap modulo p^n este egal cu p^{n-1} (n∈ℕ, n ≥2).

Demonstraţie Conform Corolarului 8.10., $(1+ap)^{p^{n-2}} \equiv 1 + a\,p^{n}\,(p^{n+1})$, de unde deducem că $(1+ap)^{p^{n-2}} \equiv 1 + a\,p^{n-1}\,(p^{n})$ adică p^{n-2} nu este de ordinul lui 1+ap, rezultând astfel că ordinul lui 1+ap modulo p^n este egal cu p^{n-1}.■

TEOREMA 8.12. Fie p≥3 un număr prim şi n∈ℕ*. Atunci $U(\mathbb{Z}_{p^n})$ este grup ciclic (adică există în acest grup rădăcini primitive modulo p^n).

Demonstraţie Conform Teoremei 8.5. există o rădăcină primitivă modulo p. Dacă g∈ℤ este o astfel de rădăcină, atunci în mod evident şi g+p este. Dacă $g^{p-1} \equiv 0(p^2)$, atunci $(g+p)^{p-1} \equiv g^{p-1}+(p-1)g^{p-2}p \equiv 1+(p-1)g^{p-2}p\ (p^2)$. Cum p^2 nu divide $(p-1)g^{p-2}$ p putem presupune pentru început că g este o rădăcinină primitivă modulo p şi că $g^{p-1} \not\equiv 1(p^2)$.

Să arătăm că un astfel de g poate fi rădăcină primitivă modulo p^n iar pentru aceasta este suficient să demonstrăm că dacă $g^m \equiv 1(p^n)$, atunci $\varphi(p^n)|m$.

Avem că $g^{p-1}=1+ap$, unde p∤a. Conform Corolarului 8.11., p^{m-1} este de ordinul lui 1+ap modulo p^m. Deoarece $(1+ap)^m \equiv 1(p^n)$ atunci $p^{n-1} \mid m$;

Fie $m=p^{n-1}\,m'$. Atunci $g^{m'} \equiv 1(p)$. Deoarece g este o rădăcină primitivă modulo p, $p-1|m'$ şi astfel $p^{n-1}(p-1)=\varphi(p^n)|m$.■

Pentru cazul p=2 vom demonstra:

<u>TEOREMA 8.13.</u> Numărul 2^n are rădăcini primitive pentru n=1 sau 2 iar pentru n≥3 nu are. Dacă n≥3, atunci $\{(-1)^a 5^b | a=0,\ 1$ şi $0 \le b < 2^{n-2}\}$ constituie un sistem redus de resturi modulo 2^n. Rezultă că pentru n≥3 $U(\mathbb{Z}_{2^n})$ este produsul direct a două grupuri ciclice (unul de ordin 2 iar celălalt de ordin 2^{n-2}).

<u>Demonstrație</u> Numărul 1 este rădăcină primitivă modulo 2 iar 3 este rădăcină primitivă modulo $2^2=4$, deci putem presupune n ≥ 3.

Intenționăm să demonstrăm că :

(1) $5^{2^{n-1}} \equiv 1 + 2^{n-1} \ (2^n)$

Evident, pentru n=3 (1) este adevărată .

Să presupunem că (1) este adevărată pentru n şi să demonstrăm pentru n+1.

La început să notăm că : $(1+2^{n-1})^2=1+2^n+2^{2n-2}$ şi că 2n-2 ≥ n+1 pentru n ≥ 3.

Aplicând Lema 8.9. congruenței (1) obținem (2) $5^{2^{n-1}} \equiv 1 + 2^n \ (2^{n+1})$ şi astfel (1) este probată prin inducție.

Din (2) se vede că $5^{2^{n-2}} \equiv 1 \ (2^n)$ pe când din (1) avem că $5^{2^{n-3}} \not\equiv 1 (2^n)$.

Atunci 5 are ordinul 2^{n-2} modulo 2^n.

Să considerăm mulțimea $\{(-1)^a 5^b | a=0,1$ şi $0 \le b < 2^{n-2}\}$ formată din 2^{n-1} numere şi să probăm că acestea nu sunt congruente modulo 2^n (deoarece $\varphi(2^n)=2^{n-1}$ deducem că mulțimea de mai sus conține un sistem redus de resturi modulo 2^n).

Dacă prin absurd $(-1)^a 5^b \equiv (-1)^{a'} 5^{b'} \ (2^n)$, n≥3, atunci $(-1)^a \equiv (-1)^{a'}$ (4), adică a≡a′ (2), deci a=a′. Atunci $5^b \equiv 5^{b'} (2^n)$ şi astfel $5^{b-b'} \equiv 1 \ (2^n)$, de unde b≡b′(2^n), deci b=b′.

În final să notăm că $(-1)^a 5^b$ ridicat la puterea 2^{n-2} este congruent cu 1 modulo 2^n, astfel că 2^n nu are rădăcini primitive modulo 2^n, dacă n ≥ 3. ■

Din Teoremele 8.12. şi 8.13. deducem următoarea descriere completă a grupurilor U($\mathbb{Z}_n$) pentru n arbitrar:

<u>TEOREMA 8.14</u>. Fie $n = 2^a p_1^{a_1} \dots p_n^{a_n}$ descompunerea lui n în factori primi distincți. Atunci:

$$U(Z_n) \approx U(Z_{2^a}) \times U(Z_{p_1^{q1}}) \times \dots \times U(Z_{p_n^{a_n}}).$$

Grupurile $U(Z_{p_i^{a_i}})$ sunt grupuri ciclice de ordin $p_i^{a_i-1}(p_i-1)$, $1\le i\le n$ iar $U(\mathbb{Z}_2^n)$ este grup ciclic de ordin 1 şi 2 pentru a=1, respectiv a=2. Dacă a≥3, atunci $U(\mathbb{Z}_2^a)$ este produsul direct a două grupuri ciclice de ordine 2 şi respectiv 2^{n-2}.

Putem acum răspunde la întrebarea: care numere întregi posedă rădăcini primitive?

<u>TEOREMA 8.15</u>. Numărul n∈ℕ posedă rădăcini primitive dacă şi numai dacă n este de forma 2, 4, p^a sau $2p^a$ cu a∈ℕ iar p≥3 un număr prim.

<u>Demonstraţie</u> Conform Teoremei 8.13., putem presupune că $n \neq 2^k$ cu $k \ge 3$. Dacă n nu este de forma din enunt, este uşor de a vedea că n se poate atunci scrie ca produs m_1m_2 cu $(m_1, m_2)=1$ şi $m_1, m_2 >2$.

Atunci $\varphi(m_1)$ şi $\varphi(m_2)$ sunt simultan pare iar $U(Z_n) \approx U(Z_{m_1}) \times U(Z_{m_2})$. Însă $U(Z_{m_1})$ şi $U(Z_{m_2})$ au elemente de ordin 2 iar acest lucru ne arată că $U(\mathbb{Z}_n)$ nu este ciclic. (deoarece conţine cel mult un element de ordin 2).

Atunci n nu posedă rădăcini primitive.

Reciproc, am văzut că 2, 4, şi p^a posedă rădăcini primitive. Deoarece $U(Z_{2p^a}) \approx U(Z_2) \times U(Z_{p^a})$ deducem că $U(Z_{2p^a})$ este ciclic, adică $2p^a$ posedă rădăcini primitive şi cu aceasta teorema este demonstrată .■

CAPITOLUL 7:

<u>MULŢIMEA NUMERELOR PRIME</u>

§ 1 Teoreme referitoare la infinitatea numerelor prime

Reamintim că un număr n∈ℕ, n≥2 se zice *<u>prim</u>* dacă singurii săi divizori naturali sunt 1 şi n. Numărul natural 2 este singurul număr prim par iar pentru n≥3 dacă n este prim atunci cu necesitate n este impar (condiţie insuficientă după cum se poate dovedi facil în cazul lui 9 care este impar dar nu este prim).

S-a pus de foarte mult timp întrebarea câte numere prime există ? În cadrul acestui paragraf vom prezenta anumite rezultate ce răspund într-un fel la această întrebare. Vom nota prin **P** mulţimea numerelor prime.

TEOREMA 1.1.(Euclid) Mulțimea P este infinită.

Demonstrație Să presupunem prin absurd că mulțimea **P** este finită, $\mathbf{P}=\{p_1, p_2, \dots p_n\}$ (unde în mod evident $p_1=2$, $p_2=3$, $p_3=5$, etc.).

Vom considera $p=p_1p_2\dots p_n+1$ şi să observăm că $p>1$ iar $p_i \nmid p$ pentru $1\le i\le n$. Ținând cont de teorema fundamentală a aritmeticii (teorema – de la cap.6), va exista un număr prim $q>1$ care să dividă pe p. Cum toate numerele prime sunt presupuse a fi doar $p_1,\dots, p_n$ deducem că $q=p_i$ cu $1\le i\le n$, ceea ce este absurd căci $p_i \nmid p$ pentru orice $1\le i\le n$. Deci **P** este mulțime infinită. ■

Observație În continuare pentru fiecare număr natural $n\ge 1$ vom nota prin p_n al n-ulea număr prim, astfel că $\mathbf{P}=\{p_1, p_2, \dots, p_n, \dots\}$ (evident $p_1=2$, $p_2=3$, $p_3=5$, etc).

O altă întrebare firească legată de mulțimea numerelor prime a fost dacă anumite submulțimi infinite ale lui $\mathbb{N}$ conțin sau nu o infinitate de numere prime. În acest sens merită amintit un rezultat celebru al lui Dirichlet :

TEOREMA 1.2. (Dirichlet) Dacă $a, b\in\mathbb{N}^*$ iar $(a, b)=1$, atunci mulțimea $\{an+b \mid n\in\mathbb{N}\}$ conține o infinitate de numere prime.

În cadrul acestei lucrări nu vom prezenta o demonstrație a Teoremei 1.2. (cititorul poate consulta în acest sens lucrările [21] şi [23]).

Totuşi pentru anumite valori particulare ale lui a şi b vom prezenta în cadrul acestei lucrări demonstrații complete.

Iată la început două exemple:

TEOREMA 1.3. Există o infinitate de numere prime de forma 4n-1 cu $n\in\mathbb{N}^*$.

Demonstrație Să presupunem prin reducere la absurd că mulțimea $\{4n-1 \mid n\in\mathbb{N}^*\}$ conține numai un număr finit de numere prime, fie acestea $q_1,\dots, q_t$ şi să considerăm numărul $q=4q_1q_2\dots q_t-1$.

Numărul q trebuie să aibă un factor prim de forma 4k-1 (căci dacă toți factorii primi ai lui q ar fi de forma 4k+1 atunci şi q ar trebui să fie de forma 4k+1. Deci ar trebui ca q_i să dividă pe q, ceea ce este absurd.), de unde concluzia din enunț. ■

TEOREMA 1.4. Există o infinitate de numere prime de forma 6n-1, $n\in\mathbb{N}^*$.

Demonstrație Să presupunem prin absurd că există doar un număr finit de numere prime de forma 6n-1 și anume $q_1, q_2,\ldots,q_k$. Să considerăm numărul $q=6q_1q_2\ldots q_k-1$. Cum un număr prim este de forma 6t-1 sau 6t+1, deducem că q trebuie să conțină un factor prim de forma 6t-1 (căci în caz contrar ar trebui ca q să fie de forma 6k+1. Deci ar trebui ca un q_i să dividă pe q, ceea ce este absurd.), de unde concluzia din enunț. ■

§2. Ciurul lui Eratostene

Fiind dat un număr natural $n\geq 2$, pentru a stabili dacă el este prim sau nu este suficient să verificăm dacă el este divizibil doar prin acele numere prime $p\leq\sqrt{n}$.

Într-adevăr, să presupunem că n este compus și că toate numerele prime ce-l divid verifică inegalitățile $\sqrt{n}<p\leq n$. Dacă un anumit număr prim p_0 divide pe n, atunci putem scrie $p=p_0n_0$ pentru un $n_0\geq 2$.

Atunci $n_0=\frac{n}{p_0}<\frac{n}{\sqrt{n}}=\sqrt{n}$ și $n_0 \mid n$. Numărul n_0 va avea cel puțin un factor prim (care va fi mai mic decât $\sqrt{n}$) - absurd !.

Obținem astfel un criteriu simplu de a determina dacă un număr natural este prim sau nu : *Dacă un număr natural n nu este divizibil prin nici un număr prim* $p\leq\sqrt{n}$ *atunci numărul n este prim.*

Acest criteriu stă la baza „ciurului” prin care Eratostene a stabilit care numere dintr-o mulțime finită de numere naturale sunt prime.

Mai precis, el a scris de exemplu toate numerele de la 2 la n în ordine crescătoare. A tăiat toți multiplii proprii ai lui 2, apoi toți multiplii proprii ai lui 3, pe urmă pe cei ai lui 5.

Se observă că cel mai mic număr natural superior lui 5 care nu a fost tăiat este 7 şi se taie atunci şi toți multiplii lui 7.

Se continuă în felul acesta procedeul de tăiere până se ajunge la etapa când cel mai mic număr natural din şirul 2, 3, …,n care nu a fost tăiat este $\geq\sqrt{n}$. Atunci procedeul se opreşte deoarece conform criteriului enunțat mai înainte toate numerele netăiate din şirul 2, 3, …,n sunt numere prime $p\leq n$.

De exemplu numărul 223 nu se divide cu 2, 3, 5, 7, 11 şi 13. Este inutil să verificăm dacă se mai divide cu 17 căci $17^2=289>223$, rezultând astfel că 223 este prim. Procedeul descris mai sus poartă numele de *ciurul lui Eratostene*.

Pe această cale se poate obţine următorul şir de numere prime mai mici decât 100 : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 51, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

În anul 1909 au fost editate tabele cu numerele prime $<10.000.000$, în care se dau cei mai mici divizori primi pentru fiecare număr natural $\leq 10.170.600$ care nu se divid la 2, 3, 5 sau 7.

În anul 1951 au fost publicate tabele de numere prime până la 11.000.000.

Jacob Philipp Kulik (1793-1863) a întocmit tabele de numere prime până la 100.000.000 (manuscrisul se păstrează la Academia Austriacă de Ştiinţe din Viena). În finalul lucrării, în cadrul Anexei 1 prezentăm numerele prime de la 1 la 10.000.

C. L. Baker şi J. F. Gruenberger au întocmit în anul 1959 un microfilm care conţine toate numerele prime mai mici decât $p_{6000000}=104.\,395.\,301$.

§3 Teorema Bertrand-Cebîşev

În cadrul acestui paragraf vom demonstra următorul rezultat:

TEOREMA 3.1. Dacă $n\in\mathbb{N}$, $n\geq 4$, atunci între n şi 2(n-1) se află cel puţin un număr natural prim.

Acest rezultat a fost formulat încă din anul 1845 de către J. Bertrand însă cel care a prezentat primul o soluţie a acestuia a fost P. L. Cebîşev în anul 1850.

În cele ce urmează vom prezenta o soluţie a lui P. Erdös (adaptată de L. Kalmar).

Această soluţie se bazează pe demonstrarea câtorva leme:

LEMA 3.2. Dacă $n\in\mathbb{N}$, $n>1$, atunci

$$C_{2n}^{n} > \frac{4^n}{2\sqrt{n}} \quad \textbf{(1).}$$

Demonstraţie Facem inducţie după n. Pentru n=2, (1) este adevărată deoarece $C_4^2 = 6 > \frac{4^2}{2\sqrt{2}} = \frac{8}{\sqrt{2}} \Leftrightarrow 6\sqrt{2} > 8 \Leftrightarrow 3\sqrt{2} > 4 \Leftrightarrow 18 > 16$ ceea ce este evident.

Cum $C_{2n+2}^{n+1} = 2 \cdot \frac{2n+1}{n+1} \cdot C_{2n}^{n}$, pentru a proba (1) pentru n+1, este suficient să demonstrăm că

$$2 \cdot \frac{2n+1}{n+1} \cdot \frac{4^n}{2\sqrt{n}} > \frac{4^{n+1}}{2\sqrt{n+1}} \Leftrightarrow \frac{2n+1}{n+1} \cdot \frac{1}{\sqrt{n}} > \frac{2}{\sqrt{n+1}} \Leftrightarrow 2n+1 > \sqrt{4n(n+1)} \Leftrightarrow$$

$\Leftrightarrow 4n^2+4n+1>4n^2+4n \Leftrightarrow 1>0$ ceea ce este evident . ■

<u>LEMA 3.3.</u> Dacă definim $P_1=1$ iar pentru $n\geq 2$, $P_n = \prod_{\substack{p \text{ prim} \\ p\leq n}} p$, atunci $P_n<4^n$, pentru orice $n\in\mathbb{N}^*$.

<u>Demonstrație</u> Facem din nou inducție după n. Pentru n =1, 2 totul este clar. Presupunem lema adevărată pentru toate numerele <n şi să o demonstrăm pentru n.

Dacă n este par, atunci $P_n=P_{n-1}$ şi totul este clar. Dacă n este impar, n=2k+1 ($k\in\mathbb{N}^*$), atunci orice număr prim p a.î. $k+2\leq p\leq 2k+1$ este un divizor al lui $C_{2k+1}^{k} = \frac{(2k+1)\ 2k\ (2k-1)....(k+2)}{1\cdot 2.....\cdot k}$.

Din $(1+1)^{2k+1} > C_{2k+1}^{k} + C_{2k+1}^{k+1} = 2C_{2k+1}^{k}$ deducem că $C_{2k+1}^{k} < 4^k$. (2)

Produsul tuturor numerelor prime p a.î. $k+2\leq p\leq 2k+1$ divizând C_{2k+1}^{k} este inferior lui 4^k (ținând cont de (2)) . Scriind că $P_n=P_{2k+1}=P_{k+1}\cdot \prod_{\substack{p \text{ prim} \\ k+2\leq p\leq n}} p$ şi ținând cont de ipoteza de inducție $P_{k+1}<4^{k+1}$ şi de (2) deducem că $P_n<4^{k+1}\cdot 4^k=4^{2k+1}=4^n$ şi astfel Lema 3.3. este demonstrată. ■

<u>LEMA 3.4.</u> Dacă p este un număr prim ce divide C_{2n}^{n} a.î. $p \geq \sqrt{2n}$, atunci p apare cu exponentul 1 în descompunerea lui C_{2n}^{n} în factori primi.

<u>Demonstrație</u> Exponentul lui p în $C_{2n}^{n} = \frac{(2n)\ !}{(n\ !)^2}$ va fi

$$\alpha = \sum_{k\geq 1}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right).$$

Dacă $p\geq\sqrt{2n}$ (avem $p=\sqrt{2n}$ $\Leftrightarrow n=2$ în care caz lema este adevărată căci $C_4^2=2\cdot 3$), atunci pentru $n\geq 3$ avem $p\geq\sqrt{2n}$, de unde deducem imediat că $\alpha=\left[\frac{2n}{p}\right]-2\cdot\left[\frac{n}{p}\right]<2$, de unde $\alpha=1$ şi astfel lema este demonstrată. ■

<u>LEMA 3.5.</u> Dacă p este un număr prim, $r\in\mathbb{N}^*$ a.î. $p^r|C_{2n}^n$, atunci $p^r\leq 2n$ şi $C_{2n}^n\leq(2n)^{\pi(2n)}$ (unde pentru $x\in\mathbb{R}_+$ prin $\pi(x)$ desemnăm numărul numerelor prime $q\leq x$).

<u>Demonstraţie</u> Din $p^r|C_{2n}^n$, deducem că exponentul lui p în descompunerea lui C_{2n}^n în factori primi (care este $\alpha=\sum_{k\geq 1}\left(\left[\frac{2n}{p^k}\right]-2\cdot\left[\frac{n}{p^k}\right]\right)$) verifică inegalitatea $\alpha\geq r$. Dacă am avea $p^r>2n$, pentru $k\geq r$ am avea $\left[\frac{2n}{p^k}\right]-2\cdot\left[\frac{n}{p^k}\right]=0$ şi atunci $\alpha=\sum_{k=1}^{r-1}\left(\left[\frac{2n}{p^k}\right]-2\cdot\left[\frac{n}{p^k}\right]\right)$. Cum pentru orice $x\in\mathbb{R}$ avem $[2x]-2\cdot[x]\leq 1$ ar trebui să avem $\alpha\leq r-1$ ceea ce contrazice faptul că $\alpha\geq r$. Deci $p^r\leq 2n$. Ţinând cont şi de lucrul acesta, pentru a demonstra partea a doua a lemei ţinem cont de faptul că în descompunerea în factori primi a lui C_{2n}^n nu pot să apară decât numere prime $q\leq 2n$, de unde deducem că $C_{2n}^n\leq(2n)^{\pi(2n)}$.

■

<u>LEMA 3.6.</u> Dacă $n\in\mathbb{N}$, $n>2$, atunci nici un număr prim p a.î. $\frac{2}{3}\cdot n<p\leq n$ nu poate să dividă C_{2n}^n.

<u>Demonstraţie</u> Dacă $\frac{2}{3}n<p\leq n$, atunci $\frac{2n}{p}<3$ şi $\frac{n}{p}\geq 1$, deci $\left[\frac{2n}{p}\right]\leq 2$ şi $\left[\frac{n}{p}\right]\geq 1$, de unde deducem că $\left[\frac{2n}{p}\right]-2\cdot\left[\frac{n}{p}\right]\leq 2-2\times 1=0$. Cum pentru orice $x\in\mathbb{R}$, $[2x]-2\cdot[x]\geq 0$, deducem că $\left[\frac{2n}{p}\right]-2\cdot\left[\frac{n}{p}\right]=0$.

Pentru k>1, avem $p^k > \frac{4}{9}n^2$ şi atunci $\frac{2n}{p^k} < \frac{9}{2n} < 1$ pentru n>1, deci $\left[\frac{2n}{p^k}\right] - 2\cdot\left[\frac{n}{p^k}\right] = 0$ pentru k>1şi n >4. Rezultă astfel că pentru n>4, $p \nmid C_{2n}^n$.

Pentru n=3 sau n=4, cu necesitate p=3 şi din nou lema este adevărată căci $C_6^3 = 20$ iar $C_8^4 = 70$ ce nu se divid prin 3. ■

<u>LEMA 3.7.</u> Un număr prim p a.î. n<p<2n apare în descompunerea lui C_{2n}^n în factori primi cu exponentul 1 (n≥2).

<u>Demonstraţie</u> Dacă n<p<2n, atunci $1 < \frac{2n}{p} < 2$ şi $\frac{n}{p} < 1$, deci $\left[\frac{2n}{p}\right] = 1$ şi $\left[\frac{n}{p}\right] = 0$. Pentru k≥2, avem $\frac{2n}{p^k} \le \frac{2n}{p^2} < \frac{2}{n}$, deci pentru n>1 avem $\frac{2n}{p^k} < 1$ şi $\left[\frac{2n}{p^k}\right] = 0$ ca şi $\left[\frac{n}{p^k}\right] = 0$.

Deci exponentul α al lui p în C_{2n}^n este 1. ■

<u>LEMA 3.8.</u> Dacă n∈ℕ, n≥14, atunci π(n) $\le \frac{n}{2} - 1$.

<u>Demonstraţie</u> Se verifică imediat că π(14)=6= $\frac{14}{2} - 1$, adică lema este adevărată pentru n=14.

În şirul 1, 2, …,n numerele 4, 6, …, $2\cdot\left[\frac{n}{2}\right]$ (în număr de $\left[\frac{n}{2}\right] - 1$) sunt compuse. Pe de altă parte, pentru n≥15, şirul 1, 2, …,n conţine şi numerele impare compuse 1, 9 şi 15, de unde deducem că

π(n) $\le n - \left(\left[\frac{n}{2}\right] - 1 + 3\right) = n - \left[\frac{n}{2}\right] - 2 < \frac{n}{2} - 1$. (căci $\left[\frac{n}{2}\right] > \frac{n}{2} - 1$) şi astfel lema este probată (observând că pentru n≥15 avem chiar $\pi(n) < \frac{n}{2} - 1$). ■

LEMA 3.9. **Fie** $R_n = \prod_{\substack{p\ prim \\ n<p<2n}} p$ **(sau R_n=1 dacă nu există astfel de numere prime). Atunci, pentru n≥98 avem** $R_n > \frac{\sqrt[3]{4^n}}{2\sqrt{n}\cdot(2n)^{\sqrt{n}/2}}$ **(3).**

Demonstraţie După felul în care am definit pe R_n deducem că $R_n \mid C_{2n}^n$, deci putem scrie $C_{2n}^n = R_n \cdot Q_n$, cu $Q_n \in \mathbb{N}^*$.

Conform Lemei 3.7., dacă p este un număr prim a.î. $n<p<2n$, atunci $p \nmid Q_n$ şi prin urmare dacă p este prim şi $p \mid Q_n$, cu necesitate $p \le n$. Conform Lemei 3.6. avem chiar mai mult, $p \le \frac{2}{3}n$, astfel că produsul divizorilor primi ai lui Q_n va fi cel mult egal cu $P_{\left[\frac{2n}{3}\right]}$ iar conform Lemei 3.3. acest produs va fi $< 4^{\left[\frac{2n}{3}\right]} \le 4^{\frac{2n}{3}}$.

Conform Lemei 3.4., cum $Q_n \mid C_{2n}^n$ se vede că exponentul unui număr prim p din descompunerea lui Q_n nu va fi >1 decât dacă $p < 2\sqrt{n}$.

Numărul acestor numere prime va fi conform Lemei 3.8. (înlocuind în aceasta pe n prin $\left[\sqrt{2n}\right]$, lucru posibil deoarece $n \ge 98 \Rightarrow \sqrt{2n} \ge 14$, de unde şi $\left[\sqrt{2n}\right] \ge 14$) inferior lui $\frac{\sqrt{2n}}{2}$.

Conform Lemei 3.5., produsul puterilor acestor numere prime (care divid Q_n, deci şi pe C_{2n}^n) va fi cel mult egal cu $(2n)^{\sqrt{2n}/2}$, de unde deducem în final că $Q_n < 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{2n}/2}$. (4)

Astfel, cum $R_n = \frac{C_{2n}^n}{Q_n}$ deducem, ţinând cont de Lema 3.2. şi inegalitatea (4) că $R_n > \frac{4^n}{2\sqrt{n}} \cdot \frac{1}{4^{\frac{2n}{3}}(2n)^{\frac{\sqrt{2n}}{2}}} = \frac{\sqrt[3]{4^n}}{2\sqrt{n}\cdot(2n)^{\sqrt{n}/2}}$ adică exact inegalitatea (3). ■

LEMA 3.10. **Dacă $k \in \mathbb{N}$, $k \ge 8$, atunci $2^k > 18(k+1)$.**

Demonstraţie Cum $2^8=256 >18\cdot 9$ iar dacă $2^k>18(k+1)$, atunci $2^{k+1}=2\cdot 2^k>2(18(k+1))=36k+36>18k+36=18(k+2)$, deducem conform principiului inducţiei matematice că lema este adevărată pentru orice $k \geq 8$. ■

LEMA 3.11. Dacă $x\in\mathbb{R}$, $x\geq 8$, atunci $2^x>18x$.

Demonstraţie Pentru $x\in\mathbb{R}$, $x\geq 8$ avem $[x]\geq 8$ şi conform Lemei 3.10. avem $2^x\geq 2^{[x]}\geq 18([x]+1) >18x$.■

LEMA 3.12. Dacă $k\in\mathbb{N}$, $k\geq 6$, atunci $2^k>6(k+1)$.

Demonstraţie Se face inducţie matematică după k (sau, dacă ţinem cont de Lema 3.10. mai avem de demonstrat inegalităţile pentru $k=6$ şi $k=7$ care sunt adevărate deoarece $2^6>64 > 6\cdot 7$ şi $2^7>128>6\cdot 8$) .■

LEMA 3.13. Dacă $x\in\mathbb{R}$, $x\geq 6$, atunci $2^x>6x$.

Demonstraţie Analog ca în cazul Lemei 3.11. ■

LEMA 3.14. Dacă $n\in\mathbb{N}$, $n\geq 648$, atunci $R_n>2n$.

Demonstraţie Ţinând cont de Lema 3.9. este suficient să demonstrăm că pentru $n\geq 648$ avem $\sqrt[3]{4^n} > 4n\sqrt{n}\ (2n)^{\sqrt{n}/2}$. Cum pentru $n\geq 648$, $\frac{\sqrt{2n}}{6}\geq 6$, conform Lemei 3.13. avem $2^{\frac{\sqrt{2n}}{6}} > \sqrt{2n}$, de unde ridicând ambii membrii la puterea $\sqrt{2n}$ deducem că $\sqrt[3]{2^n} > (2n)^{\sqrt{n}/2}$.

De asemenea, din $n\geq 648$, deducem că $\frac{2n}{9} > 8$ şi atunci conform Lemei 3.11. avem $2^{\frac{2n}{9}} > 4n$, de unde $2^{\frac{n}{3}} > 4n\sqrt{4n} > 4n\sqrt{n}$.

Deci pentru $n\geq 648$, $2^{\frac{n}{3}} > (2n)^{\sqrt{n}/2}$ şi $2^{\frac{n}{3}} > 4n\sqrt{n}$ de unde $\sqrt[3]{4^n} > 4n\sqrt{n}\ (2n)^{\sqrt{n}/2}$ şi cu aceasta lema este demonstrată. ■

LEMA 3.15. Dacă $n\geq 6$, atunci între n şi 2n se află cel puţin două numere prime distincte.

Demonstraţie Dacă $n \geq 648$, atunci conform definirii lui R_n, dacă în intervalul $(n, 2n)$ nu ar exista nici un număr prim, sau numai unul, atunci $R_n \leq 2n$, ceea ce ar fi în contradicţie cu Lema 3.14.

Dacă $n=6$, lema este adevărată căci între 6 şi 12 se află numerele prime 7 şi 11.

Mai avem de demonstrat Lema 3.15. pentru $7 \leq n \leq 647$. Acest lucru poate fi făcut fie direct (utilizând un tabel de numere prime ≤ 1000), fie construind un şir de numere prime $q_0, q_1, \ldots q_m$ a.î. $q_0=7$, $q_k < 2q_{k-2}$, $2 \leq k \leq m$ şi $q_{m-1} > a=647$.

O dată construit un astfel de şir (cum ar fi de exemplu şirul 7, 11, 13, 19, 23, 37, 43, 73, 83, 139, 163, 277, 317, 547, 631, 653, 1259 pentru $m=16$), să vedem cum rezultă Lema 3.15. pentru $7 \leq n \leq a=647$.

Primul termen al şirului $q_0, q_1, \ldots q_m$ nu depăşeşte pe n decât dacă $q_m > q_{m-1} > a \geq n$, deci $q_m > n$.

Există deci un indice maximal $k<m-1$ a.î. $q_k<n$. Atunci $k+2 \leq m$, $n<q_{k+1}$ şi cum $q_{k+2}<2q_k \leq 2n$, între n şi 2n există cel puţin numerele prime q_{k+1} şi q_{k+2} şi cu aceasta lema este complet demonstrată. ■

TEOREMA 3.16. (Cebîşev) Dacă $n \in \mathbb{N}$, $n \geq 4$, atunci între n şi 2(n-1) avem cel puţin un număr prim.

Demonstraţie Pentru $n=4$ şi $n=5$ teorema este adevărată în mod evident deoarece între 4 şi 6 se află 5 iar între 5 şi 8 se află 7. Pentru $n \geq 6$, conform Lemei 3.15. între n şi 2n se află cel puţin două numere prime distincte p şi q cu $p<q$. Dacă cel mai mare dinte acestea este $q=2n-1$, celălalt trebuie să fie $<2n-2$ căci $2(n-1)$ este par şi compus pentru $n \geq 6$. Deci $n<p<2(n-1)$. Dacă $q<2n-1$, cum $p<q$, din $p<q$ deducem că $n<p<2n-2$ şi cu aceasta Teorema lui Cebîşev este complet demonstrată. ■

În continuare vom prezenta câteva corolare la Teorema lui Cebîşev:

COROLARUL 3.17. Dacă $n \in \mathbb{N}$, $n \geq 2$, atunci între n şi 2n se află cel puţin un număr prim.

Demonstraţie Dacă $n \geq 4$ totul rezultă din teorema lui Cebîşev. Dacă $n=2$ între 2 şi 4 se află 3 iar dacă $n=3$ atunci între 3 şi 6 se află 5. Astfel Corolarul este demonstrat pentru orice $n \geq 2$. ■

Observaţie În anul 1892 J. J. Sylvester a demonstrat următoarea generalizare a Corolarului 3.17.:

Dacă n, k $\in\mathbb{N}$, n>k, atunci în şirul n, n+1, …n+k-1 se află cel puţin un număr admiţând un divizor prim > k.

Corolarul 3. 17. Se deduce acum din acest rezultat pentru n=k+1.

Această generalizare a mai fost demonstrată şi de I. Schur în 1929 ca şi de P. Erdös în 1934.

<u>COROLARUL 3.18.</u> Dacă k$\in\mathbb{N}$, k>1, atunci $p_k<2^k$ (unde p_k este al k-lea număr prim).

<u>Demonstraţie</u> Facem inducţie după k. Pentru k=2 avem $p_2=3<2^2$. Dacă $p_k<2^k$, conform Corolarului 3.17. există cel puţin un număr prim p a.î. $2^k<p<2\cdot 2^k=2^{k+1}$ şi astfel corolarul este demonstrat. ■

<u>COROLARUL 3.19.</u> Dacă n$\in\mathbb{N}$, n≥2, atunci în descompunerea lui n! în factori primi găsim cel puţin un număr prim cu exponentul egal cu 1.

<u>Demonstraţie</u> Corolarul este în mod evident adevărat pentru n=2 şi n=3. (2!=2, 3!=2·3) .

Fie acum n≥4. Dacă n este par, n=2k, atunci k≥2 şi conform Corolarului 3.17. între k şi 2k=n găsim cel puţin un număr prim p a.î. k<p<2k=n.

Vrem să demonstrăm că p apare cu exponentul 1 în descompunerea în factori primi a lui n!. Într-adevăr, următorul număr din n! ce ar fi multiplu de p este 2p însă din k<p $\Rightarrow$2k<2p $\Leftrightarrow$2p>n.

Dacă n este impar, n=2k+1$\Rightarrow$k≥2 şi din nou conform Corolarului 3.17. între k şi 2k găsim cel puţin un număr prim p (k<p<2k). Avem deci p<2k<n şi 2p>2k $\Rightarrow$2p>2k+1=n şi din nou ajungem la concluzia că p apare în descompunerea lui n! cu exponentul 1. ■

<u>Observaţie</u> De fapt, Corolarele 3.17. şi 3. 19. sunt echivalente.

Într-adevăr, mai înainte am văzut cum Corolarul 3.17. implică Corolarul 3.19..

Reciproc, să admitem că ceea ce afirmă Corolarul 3.19. este adevărat (adică pentru orice număr natural n≥1 în n! există cel puţin un număr prim cu exponentul 1) şi să demonstrăm Corolarul 3.17. (adică pentru orice n≥2, între n şi 2n se află cel puţin un număr prim).

Într-adevăr, fie p numărul prim ce apare în descompunerea în factori primi a lui (2n)! cu exponentul 1. Avem $p<2n<2p$ căci dacă am avea $2p\leq 2n$, atunci în $(2n)!=1\cdot 2\cdot\ldots\cdot(n-1)\cdot n\cdot(n+1)\cdot\ldots\cdot(2n)$ apar şi p şi 2p şi astfel exponentul lui p în (2n)! ar fi cel puţin 2. În concluzie, $2n<2p$, adică $n<p$ şi cum $n<2p$ deducem că $n<p<2n$. ■

Deducem imediat:

COROLARUL 3.20. Dacă $n\in\mathbb{N}$, $n\geq 2$ atunci n! nu poate fi puterea unui număr natural cu exponentul >1.

COROLARUL 3.21. Pentru orice $k\in\mathbb{N}$, $k\geq 4$, avem inegalitatea $p_{k+2}<2p_k$.

Demonstraţie Pentru $k\geq 4$ avem $p_k>p_3=5$ şi atunci conform Lemei 3.15. între p_k şi $2p_k$ există cel puţin două numere prime distincte. Cum cele mai mici dintre aceste numere vor fi p_{k+1} şi p_{k+2} avem $p_{k+2}<2p_k$. ■

COROLARUL 3.22. Pentru orice $k\in\mathbb{N}$, $k\geq 2$ avem $p_{k+2}<p_{k+1}+p_k$.

Demonstraţie Pentru k=2, 3 se verifică imediat prin calcul iar pentru $k\geq 4$ totul rezultă din corolarul precedent. ■

COROLARUL 3.23. Dacă $n, k\in\mathbb{N}$, $n\geq 2$, atunci

$$\frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{n+k}\notin\mathbb{N}.$$

Demonstraţie Dacă $x=\frac{1}{n}+\frac{1}{n+1}+\ldots+\frac{1}{n+k}\in\mathbb{N}$, atunci $x\geq 1$ şi cum $x<\frac{k+1}{n}$, cu necesitate $k+1>n$ şi deci $k\geq n$. Fie p cel mai mare număr prim $\leq n+k$. Atunci $2p>n+k$. Conform Corolarului 3.17., între p şi 2p găsim cel puţin un număr prim q, iar dacă am avea $2p\leq n+k$, atunci $p<q<n+k$, în contradicţie cu alegerea lui p. Deci $n+k<2p$.

Cum $k \geq n$, atunci $n+k \geq 2n$ şi din nou conform Corolarului 3.17, între n şi 2n există un număr prim r. Cum $r < 2n \leq n+k$, ținând cont de felul în care l-am ales pe p deducem că $r \leq p$.

De asemenea, deoarece $n < r$, avem $n < p \leq n+k < 2p$.

Deducem de aici că printre termenii sumei $x = \frac{1}{n} + \frac{1}{n+1} + ... + \frac{1}{n+k}$ există numai unul al cărui numitor să fie divizibil prin p. Punând pe x sub formă de fracție (cu numitorul $n \cdot (n+1) \cdot ... \cdot (n+k)$) se observă că printre termenii ce dau numărătorul lui x există unul ce nu se divide prin p.

Atunci, dacă scriem $x = \frac{m}{t}$ (cu $t = n \cdot (n+1) \cdot ... \cdot (n+k)$), $p \mid t$ şi $p \nmid m$, de unde concluzia că $x \notin \mathbb{N}$.■

§4 Inegalitățile lui Cebîşev

Reamintim că pentru $x \in \mathbb{R}_+$, prin $\pi(x)$ am notat numărul numerelor prime $p \leq x$. Astfel, $\pi(1)=0$, $\pi(2)=1$, $\pi(3)=\pi(4)=2$, $\pi(5)=\pi(6)=3$, $\pi(100)=25$, $\pi(1000)=168$, etc.

În anul 1958, D. H. Lehmer a calculat $\pi(10^8)$ şi $\pi(10^9)$ arătând că $\pi(10^8)=5761455$ şi $\pi(10^9)=50847534$.

Evident, $\pi(p_n)=n$ pentru orice $n \geq 1$.

Reamintim că în cadrul Lemei 3.9. am definit pentru $n \geq 1$, $R_n = \prod_{\substack{p \text{ prim} \\ n < p \leq 2n}} p$.

Există $\pi(2n)-\pi(n)$ numere prime p a.î. $n < p \leq 2n$ şi cum toate aceste numere prime sunt $\leq 2n$ deducem că $R_n \leq (2n)^{\pi(2n)-\pi(n)}$. Ținând cont de Lema 3.9., deducem că pentru $n \geq 98$ avem inegalitatea $(2n)^{\pi(2n)-\pi(n)} > \frac{4^{n/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}$, de unde, logaritmând în baza 10 deducem inegalitatea

$$(1) \quad \pi(2n)-\pi(n) > \frac{n}{3\lg(2n)}\left[\lg 4 - \frac{3\lg(4n)}{2n} - \frac{3\lg(2n)}{\sqrt{2n}}\right].$$

Cum $\lim_{x\to\infty} \frac{\lg x}{\sqrt{x}} = \lim_{x\to\infty} \frac{\lg x}{x} = 0$, din (1) deducem că $\lim_{x\to\infty} [\pi(2n) - \pi(n)] = \infty$.

De aici deducem următorul

<u>COROLAR 4.1.</u> Pentru orice număr natural k există un număr natural m_k a.î. pentru orice $n \geq m_k$, există cel puțin k numere prime între n şi 2n.

Fie acum $p_1,\ldots p_r$ numerele prime ce intră în descompunerea în factori primi a lui C_{2n}^n (evident $p_1, p_2, \ldots p_r \leq 2n$). Fiecare număr p_i apare la puterea $\left(\left[\frac{2n}{p_i}\right]-2\left[\frac{n}{p_i}\right]\right)+\ldots.+\left(\left[\frac{2n}{p_i^{q_i}}\right]-2\left[\frac{n}{p_i^{q_i}}\right]\right)$, unde q_i este cel mai mare număr natural pentru care $p_i^{q_i} \leq 2n$.

Cum pentru orice $a \geq 0$, $[a]-2\left[\frac{a}{2}\right]=0$ sau 1, deducem că suma $\sum_{k=1}^{q_i}\left(\left[\frac{2n}{p_i^k}\right]-2\left[\frac{n}{p_i^k}\right]\right) \leq \underbrace{1+\ldots+1}_{q_i}=q_i$, astfel că fiecare p_i apare în descompunerea lui C_{2n}^n la o putere $\leq q_i$, deci $C_{2n}^n \leq p_1^{q_1}.....p_r^{q_r} \leq \underbrace{(2n)...(2n)}_{r\ ori}=(2n)^r$.

Cum $r=\pi(2n)$ deducem că $C_{2n}^n \leq (2n)^{\pi(2n)}$ (este de fapt o re-demonstrare a inegalității din cadrul Lemei 3.5. !).

Pe de altă parte, $C_{2n}^n=\frac{(2n)\cdot(2n-1)...(n+1)}{1\cdot 2\cdot.....\cdot n}$ se divide prin produsul tuturor numerelor prime $p_{s+1}, p_{s+2},\ldots p_r$ mai mari decât n şi mai mici decât 2n (am notat prin $p_1,\ldots p_s$ toate numerele prime mai mici decât n).

Astfel, $C_{2n}^n \geq p_{s+1}p_{s+2}...p_r > \underbrace{n\cdot n\cdot....\cdot n}_{r-s\ ori}=n^{\text{ r-s}}$.

Cum $r=\pi(2n)$ şi $s=\pi(n)$, deducem că

(2) $n^{\pi(2n)-\pi(n)} < C_{2n}^n < (2n)^{\pi(2n)}$.

De asemenea, pentru orice număr natural $n \geq 1$, avem

(3) $2^n < C_{2n}^n < 4^n$.

Comparând (1) cu (2) deducem că $2^n < (2n)^{\pi(2n)}$, de unde prin logaritmare în baza 10 deducem:

(4) $\pi(2n) > \frac{\lg 2}{2}\cdot\frac{2n}{\lg(2n)}=0{,}15051...\cdot\frac{2n}{\lg(2n)}$

Cum pentru n≥1 avem $\frac{2n}{2n+1} \geq \frac{2}{3}$ deducem că

$\pi(2n+1)\lg(2n+1) > \pi(2n)\lg(2n) > 0{,}15051...2n > \frac{2}{3} \cdot 0{,}15051...(2n+1) =$

$= 0{,}10034... \cdot (2n+1)$

sau $\pi(2n+1) > 0{,}10034.... \cdot \frac{2n+1}{\lg(2n+1)}$.

Obţinem astfel următorul rezultat:

<u>PROPOZIŢIA 4.2.</u> Pentru orice număr natural n>1, avem inegalitatea $\pi(n) > 0{,}1 \cdot \frac{n}{\lg n}$.

Tot din combinaţia inegalităţilor (2) şi (3) deducem că $n^{\pi(2n)-\pi(n)} < 2^{2n}$ pentru orice n>1, de unde prin logaritmare deducem că $[\pi(2n)-\pi(n)]\lg n < 2n \lg 2$, adică $\pi(2n)-\pi(n) < 2\lg 2 \cdot \frac{n}{\lg n} = 0{,}60206.... \cdot \frac{n}{\lg n}$.

Fie acum x≥0 un număr real. Dacă notăm $\left[\frac{x}{2}\right] = n$, atunci în mod evident x=2n sau 2n+1 şi vom avea

$$\pi(x) - \pi\left(\frac{x}{2}\right) \leq \pi(2n) - \pi(n) + 1 < 0.60206... \frac{n}{\lg n} + 1 < 1{,}60206.... \cdot \frac{n}{\lg n}$$

(deoarece $\frac{n}{\lg n} > 1$).

Se verifică imediat că pentru n≥3, din n<x rezultă $\frac{n}{\lg n} < \frac{x}{\lg x}$, deci pentru $\left[\frac{x}{2}\right] \geq 3$ avem $\pi(x) - \pi\left(\frac{x}{2}\right) < 1{,}60206..... \frac{x}{\lg x}$.

(Este uşor de verificat că ultima inegalitate este valabilă şi pentru $\left[\frac{x}{2}\right] < 3$; într-adevăr, dacă $\left[\frac{x}{2}\right] < 3$, diferenţa $\pi(x) - \pi\left(\frac{x}{2}\right)$ evident poate fi egală cu 2

(pentru $2{,}5 \le \frac{x}{2} < 3$), cu unu sau cu zero; în toate aceste cazuri, produsul $1{,}60206... \cdot \frac{x}{\lg x}$ va lua valoarea cea mai mare).

Astfel, pentru orice $x \in \mathbb{R}_+$

(5) $\pi(x) - \pi\left(\frac{x}{2}\right) < 1{,}60206... \cdot \frac{x}{\lg x}$.

Din (5) deducem mai departe că

$$\pi(x)\lg x - \pi\left(\frac{x}{2}\right)\lg\frac{x}{2} = \left[\pi(x) - \pi\left(\frac{x}{2}\right)\right]\lg x + \pi\left(\frac{x}{2}\right)\left(\lg x - \lg\frac{x}{2}\right) <$$

$$< (\lg x) \cdot 1{,}60206... \cdot \frac{x}{\lg x} + \lg 2 \cdot \pi\left(\frac{x}{2}\right) < \left(1{,}60206.... + \frac{\lg 2}{2}\right)x \approx 1{,}75257 \cdot x$$

(am folosit faptul evident: $\pi\left(\frac{x}{2}\right) < \frac{x}{2}$).

Deci $\pi(x)\lg x - \pi\left(\frac{x}{2}\right)\lg\frac{x}{2} < 1{,}75257 \cdot x$.

Fie acum $n \in \mathbb{N}$, $n>1$. Conform ultimei inegalități avem

$$\pi(n)\lg n - \pi\left(\frac{n}{2}\right)\lg\left(\frac{n}{2}\right) < 1{,}75257... \cdot n$$

$$\pi\left(\frac{n}{2}\right)\lg\left(\frac{n}{2}\right) - \pi\left(\frac{n}{4}\right)\lg\left(\frac{n}{4}\right) < 1{,}75257... \cdot \frac{n}{2}$$

. . . . . .

$$\pi\left(\frac{n}{2^{k-1}}\right)\lg\left(\frac{n}{2^{k-1}}\right) - \pi\left(\frac{n}{2^k}\right)\lg\left(\frac{n}{2^k}\right) < 1{,}75257... \cdot \frac{n}{2^{k-1}}$$

(vom alege pe k a.î. $2^k > n$).

Adunând aceste inegalități deducem că :

$$\pi(n)\lg n - \pi\left(\frac{n}{2^k}\right)\lg\frac{n}{2^k} < 1{,}75257...\left(n + \frac{n}{2} + ... + \frac{n}{2^{k-1}}\right) = 1{,}75257... \cdot \frac{n - \frac{n}{2^k}}{1 - \frac{1}{2}} <$$

$$< 3{,}50514... \cdot n < 4n$$

Cum pentru 2^k>n, $\frac{n}{2^k}<1$ şi deci $\pi\left(\frac{n}{2^k}\right)=0$, deducem că $\pi(n)<4\cdot\frac{n}{\lg n}$.

Am obţinut astfel:

PROPOZIŢIA 4.3. Dacă n>1, $\pi(n)<4\cdot\frac{n}{\lg n}$**.**

Din Propoziţiile 4.2. şi 4.3. deducem:

PROPOZIŢIA 4.4. Pentru orice număr natural n>1, avem dubla inegalitate $0{,}1\cdot\frac{n}{\lg n}<\pi(n)<4\cdot\frac{n}{\lg n}$**.**

Observaţii 1. Dacă trecem la logaritmi naturali, Propoziţia 4.4 capătă o formulare mai elegantă $0{,}92\cdot\frac{n}{\lg n}<\pi(n)<1{,}11\cdot\frac{n}{\lg n}$, astfel că variaţia funcţiei π(n) este redată cu o mai mare exactitate de funcţia $\frac{n}{\lg n}$ (factorii numerici 0,92 şi 1,11 diferă puţin de 1). Aceste rezultate aparţin de asemenea lui Cebîşev.

2. Cebîşev a demonstrat de asemenea că dacă raportul $\pi(n):\frac{n}{\lg n}$ tinde (pentru $n\to\infty$) la o limită l, atunci $l=1$. Faptul că limita raportului π(n): $\frac{n}{\lg n}$ există pentru $n\to\infty$ (şi deci este egală cu 1) a fost demonstrată pentru prima dată de J. Hadamard (la aproximativ 50 de ani de la lucrările remarcabile ale lui P. L. Cebîşev) utilizând un aparat matematic complicat, specific matematicilor superioare (o demonstraţie elementară a fost totuşi dată ceva mai târziu de matematicianul danez A. Selberg; recomandăm cititorului lucrarea [21]).

Obţinem deci $\pi(n)\approx\frac{n}{\lg n}$ pentru n>1.

TEOREMA 4.5. (Cebîşev) Pentru x∈ℝ, x≥2 avem dubla inegalitate

$$\frac{\lg 2}{4}\cdot\frac{x}{\lg x}<\pi(x)<9\lg 2\cdot\frac{x}{\lg x}.$$

Demonstraţie Pentru prima inegalitate ţinem cont de două inegalităţi stabilite mai înainte şi anume

$$n^{\pi(2n)-\pi(n)}<C_{2n}^{n}<(2n)^{\pi(2n)}\quad\text{şi}$$

$2^n < C_{2n}^n < 4^n$ pentru n∈ℕ, n≥2, de unde deducem că $\pi(2n)-\pi(n) \le 2\lg 2 \cdot \frac{n}{\lg n}$ şi $\pi(2n) \ge \lg 2 \cdot \frac{n}{\lg(2n)}$.

Pentru x∈ℝ, x≥2, alegem acum n∈ℕ a.î. $n \le \frac{x}{2} < n+1$, astfel că $\pi(x) \ge \pi(2n) \ge \lg 2 \cdot \frac{n}{\lg(2n)} \ge \lg 2 \cdot \frac{n}{\lg x} \ge \frac{\lg 2}{4} \cdot \frac{(2n+2)}{\lg x} > \frac{\lg 2}{4} \cdot \frac{x}{\lg x}$.

Să stabilim acum a doua inegalitate.

Pentru un număr real oarecare y≥4, alegem n∈ℕ a.î. $n-1 < \frac{y}{2} \le n$. Astfel,

$$\pi(y)-\pi\left(\frac{y}{2}\right) \le \pi(2n)-\pi(n)+1 \le \frac{2n\lg 2}{\lg n}+1 \le \frac{(y+2)\lg 2}{\lg\left(y/2\right)}+1 \le$$

$$\le \frac{2(y+2)\lg 2}{\lg y}+1 \le \frac{3y\lg 2}{\lg y}+1 < \frac{4y\lg 2}{\lg y}$$

Am demonstrat astfel că pentru y∈ℝ, y≥4, avem $\pi(y)-\pi\left(\frac{y}{2}\right) < (4\lg 2)\frac{y}{\lg y}$.

Evident că pentru 2≤y<4 avem $\pi(y)-\pi\left(\frac{y}{2}\right) \le 2$ şi cum funcția $y \to \frac{y}{\lg y}$ îşi atinge valoarea minimă în y=e, deducem că $\pi(y)-\pi\left(\frac{y}{2}\right) \le \frac{\left(2/e\right)^y}{\lg y}$ pentru 2≤y≤4.

Cum însă $\frac{2}{e} < 4\lg 2$, deducem că $\pi(y)-\pi\left(\frac{y}{2}\right) < (4\lg 2)\frac{y}{\lg y}$ pentru orice y≥2.

Astfel, pentru y≥2, avem:

$$\pi(y)\lg y-\pi\left(\frac{y}{2}\right)\lg\left(\frac{y}{2}\right)=\left[\pi(y)-\pi\left(\frac{y}{2}\right)\right]\lg y+\pi\left(\frac{y}{2}\right)\lg 2 < 4y\lg 2+\frac{y}{2}\lg 2$$

$$=\frac{9}{2}\lg 2 .$$

Fie acum $x\in\mathbb{R}$, $x\geq 2$ şi $r\in\mathbb{N}$ a.î. $2^{r+1}\leq x<2^{r+2}$.

Înlocuind în ultima egalitate pe rând pe y cu x, $\frac{x}{2}$, $\frac{x}{2^2}$,....,$\frac{x}{2^r}$ obţinem r+1 inegalităţi ; adunând membru cu membru aceste inegalităţi şi ţinând cont de faptul că $\pi\left(\frac{x}{2^{r+1}}\right)=0$ obţinem în final că $\pi(x)\lg x<\frac{9}{2}\left(x+\frac{x}{2}+...+\frac{x}{2^r}\right)\lg 2<(9\lg 2)x$, adică a doua inegalitate din enunţ.

■

Observaţie În cartea lui **G.Tenenbaum : Introduction à la théorie analitique des nombres (Université de Nancy, 1991, p. 22)** se demonstrează că pentru $x\geq 52$ avem $\frac{x}{\lg x}\cdot\left(1+\frac{1}{2\lg x}\right)<\pi(x)<\frac{x}{\lg x}\cdot\left(1+\frac{3}{2\lg x}\right)$.

TEOREMA 4.6. Pentru $n\in\mathbb{N}$, $n\geq 2$ avem $\frac{n\lg n}{9\lg 2}<p_n<\frac{8n\lg n}{\lg 2}$.

Demonstraţie Ţinând cont de Teorema 4.5., pentru $n\in\mathbb{N}$, $n\geq 1$ avem : $n=\pi(p_n)<(9\lg 2)\frac{p_n}{\lg p_n}$, de unde deducem prima inegalitate din enunţ. Cum funcţia $f:(0,+\infty)\to\mathbb{R}$, $f(x)=\frac{\lg x}{\sqrt{x}}$ pentru $x>0$, este descrescătoare pentru $x>e^2$ iar $f(e^9)<\frac{\lg 2}{4}$ deducem că pentru $x\geq e^9$ avem $\frac{\lg x}{\sqrt{x}}<\frac{\lg 2}{4}$. Deci, dacă $p_n\geq e^9$ avem $\frac{\lg p_n}{\sqrt{p_n}}<\frac{\lg 2}{4}$.

Pe de altă parte, pentru $n\geq 1$, avem $n=\pi(p_n)>\frac{\lg 2}{4}\cdot\frac{p_n}{\lg p_n}$. Combinând cele două inegalităţi obţinem că dacă $p_n\geq e^9$, atunci $\frac{\lg p_n}{\sqrt{p_n}}<\frac{\lg 2}{4}<\frac{n\lg p_n}{p_n}$, ceea ce implică printre altele că $\sqrt{p_n}<n$ şi că $\lg p_n<2\lg n$.

Deducem că pentru $p_n \geq e^9$, $\frac{\lg 2}{4} p_n < n \cdot \lg p_n < 2n \cdot \lg n$ şi astfel membrul drept al inegalităţii din enunţ este verificat pentru $p_n \geq e^9$. Pentru $2 \leq p_n < e^9$ inegalitatea din enunţ se verifică prin calcul direct. ■

Observaţie În lucrarea lui **B. Rosser : The n-th Prime is Greater than n lg(n)** din **Proc. London Math. Soc., vol. 49, 1939, pp. 21- 44** se demonstrează că dacă $n \geq 4$, atunci $n \lg n + n \lg(\lg n) - 10n < p_n < n \lg n + n \lg(\lg n) + 8n$.

Într-o lucrare mai recentă a lui **B. Rosser** şi **L. Schoenfeld**: **Aproximate formulas for some functions of prime numbers** din **Ilinois J. Math vol. 6, 1962, pp. 64-89** se demonstrează următoarele:

1) Pentru orice $n \in \mathbb{N}$, $n \geq 2$ avem $p_n > n\left(\ln n + \ln\ln n - \frac{3}{2}\right)$

2) Pentru orice $n \in \mathbb{N}$, $n \geq 20$ avem $p_n < n\left(\ln n + \ln\ln n - \frac{1}{2}\right)$.

TEOREMA 4.7. Pentru orice $x \in \mathbb{R}$, $x \geq 3$, există două constante reale pozitive $c_1, c_2 > 0$, a.î. $c_1 \lg(\lg x) < \sum_{\substack{p \text{ prim} \\ p \leq x}} \frac{1}{p} < c_2 \lg(\lg x)$.

Demonstraţie Fie $x \in \mathbb{R}$, $x \geq 3$. Cum $\pi(n) - \pi(n-1) = \begin{cases} 1 & \text{pentru } n \text{ prim} \\ 0 & \text{in rest} \end{cases}$

avem:

$$\sum_{\substack{p \text{ prim} \\ p \leq x}} \frac{1}{p} = \sum_{2 \leq n \leq x} \frac{\pi(n) - \pi(n-1)}{n} = \sum_{2 \leq n \leq x} \pi(n) \cdot \left(\frac{1}{n} - \frac{1}{n+1}\right) + \frac{\pi(x)}{[x]+1} =$$

$$= \sum_{2 \leq n \leq x} \frac{\pi(n)}{n(n+1)} + \frac{\pi(x)}{[x]+1}$$

Conform inegalităţilor lui Cebîşev (Teorema 4.5.) deducem că pentru $x \geq 2$ avem $\frac{\lg 2}{4 \lg n} < \frac{\pi(n)}{n} < \frac{9 \lg 2}{\lg n}$, de unde deducem că

$$\frac{\lg 2}{4} \sum_{2 \leq n \leq x} \frac{1}{(n+1)\lg n} < \sum_{2 \leq n \leq x} \frac{\pi(n)}{n(n+1)} < 9 \lg 2 \sum_{2 \leq n \leq x} \frac{1}{(n+1)\lg n}.$$

Prin inducţie matematică se probează că pentru orice $k \in \mathbb{N}$, $k \geq 1$ avem :

$\lg k < \sum_{n=1}^{k} \frac{1}{n} \le \lg k + 1$. De asemenea, pentru orice $x \in \mathbb{R}$, $x \ge 1$ avem

$$\left| \sum_{\substack{n \in N - \{0\} \\ n \le x}} \frac{1}{n} - \lg x \right| \le 1.$$

Din cele de mai înainte deducem existența unei constante c > 0 a.î.

$\left| \sum_{2 \le n \le x} \frac{1}{(n+1)\lg n} - \lg(\lg x) \right| < c$. Evaluând acum $\frac{\pi(n)}{[x]+1}$ obținem constantele c_1 şi c_2 din enunț. ■

Observație Dacă pentru două funcții reale f şi g scriem f ~ g dacă $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$, atunci vom menționa următoarele rezultate :

1. $\pi(x) \sim \frac{x}{\lg x}$. Acest rezultat cunoscut şi sub numele de *Teorema elementului prim sau Legea de repartiție a numerelor prime* a fost intuit de Legendre şi Gauss în secolul al 18-lea şi demonstrat în 1896, independent de J. Hadamard (1865-1963) şi G. J. de la Vallée-Poussin cu metode specifice analizei complexe.

Pentru o demonstrație elementară a Teoremei numărului prim cititorul este rugat să consulte **P. Erdös : „ On a New Method in Elementary Number Theory which leads to an Elementary Proof of the Prime Number Theorem'', Proc. Nat. Acad. Sci. , Washington , vol 35, 1949, pp. 347-383** sau **A. Selberg : „ An Elementary Proof of the Prime Number Theorem'', Ann. Math. Vol 50, 1949, pp. 303-313.**

2. La 15 ani Gauss a conjecturat că $\pi(x) \sim L_i(x) = \int_2^x \frac{1}{\lg t}\, dt$.

Deoarece $\int_2^x \frac{1}{\lg t}\, dt = \frac{x}{2} - \frac{2}{\lg 2} + \int_2^x \frac{1}{(\lg t)^2}\, dt$ şi

$$0 < \int_2^x \frac{1}{(\lg t)^2}\, dt = \int_2^{\sqrt{x}} \frac{1}{(\lg t)^2}\, dt + \int_{\sqrt{x}}^x \frac{1}{(\lg t)^2}\, dt <$$

$$< \frac{\sqrt{x} - 2}{(\lg 2)^2} + \frac{x - \sqrt{x}}{\frac{1}{4} \cdot (\lg x)^2} < \frac{\sqrt{x}}{(\lg 2)^2} + \frac{4x}{(\lg x)^2}$$, deducem că

$$0 < \frac{\int_2^x \frac{1}{(\lg t)^2}\,dt}{\frac{x}{\lg x}} < \frac{\lg x}{\sqrt{x}(\lg 2)^2} + \frac{4}{\lg x}$$, de unde acum se deduce facil că $\frac{x}{\lg x} \sim L_i(x)$.

TEOREMA 4.8. Seria $\sum_{n\geq 1}\frac{1}{p_n}$ este divergentă.

Demonstrație Fie $p_1, p_2, \ldots, p_{l(n)}$ toate numerele prime $\leq n$ şi să definim $\lambda(n) = \prod_{i=1}^{l(n)}\left(1-\frac{1}{p_i}\right)^{-1}$. Deoarece $\left(1-\frac{1}{p_i}\right)^{-1} = \sum_{a_i=0}^{\infty}\frac{1}{p_i^{a_i}}$, atunci $\lambda(n) = \sum\left(p_1^{a_1}\ldots p_l^{a_l}\right)^{-1}$ (unde sumarea se face după toate l-upurile de numere naturale $(a_1, \ldots, a_l)$). În particular $1+\frac{1}{2}+\ldots.+\frac{1}{n} < \lambda(n)$ şi astfel $\lambda(n)\to\infty$ pentru $n\to\infty$. Avem :

$$\lg\lambda(n) = -\sum_{i=1}^{l}\lg\left(1-\frac{1}{p_i}\right) =$$

$$= \sum_{i=1}^{l}\sum_{m=1}^{\infty}\left(m\ p_i^m\right)^{-1} = p_1^{-1}+p_2^{-1}+\ldots.+p_l^{-1}+\sum_{i=1}^{l}\sum_{m=2}^{\infty}\left(m\ p_i^m\right)^{-1}.$$

Însă $\sum_{m=2}^{\infty}\left(m\ p_i^m\right)^{-1} < \sum_{m=2}^{\infty}p_i^{-m} = p_i^{-2}\left(1-p_i^{-1}\right)^{-1} \leq 2p_i^{-2}$ astfel că

$$\lg\lambda(n) < p_1^{-1}+\ldots+p_l^{-1}+2\ \left(p_1^{-2}+\ldots+p_l^{-2}\right).$$

Este însă cunoscut faptul că $\sum_{n\geq 1}\frac{1}{n^2} = \frac{\pi^2}{6}$. Atunci $\sum_{i\geq 1}p_i^{-2}$ este convergentă, astfel că dacă presupunem că $\sum_{n\geq 1}\frac{1}{p_n}$ este convergentă, atunci trebuie să existe o constantă M a.î. $\lg(\lambda(n)) < M \Leftrightarrow \lambda(n) < e^M$, ceea ce este imposibil (deoarece am stabilit că $\lambda(n)\to\infty$ pentru $n\to\infty$), de unde deducem că $\sum_{n\geq 1}\frac{1}{p_n}$ este divergentă. ■

§5 Teorema lui Scherk

Rezultatul pe care îl prezentăm în continuare este datorat lui H. F. Scherk şi prezintă un fel de recurență „slabă'' pentru şirul $(p_k)_{k\geq 1}$ al numerelor prime.

Mai precis, vom demonstra :

TEOREMA 5.1. (H. F. Scherk) Pentru orice număr natural n≥1 există o alegere convenabilă a semnelor + sau – a.î. :

(1) $p_{2n} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-2} + p_{2n-1}$ **şi**

(2) $p_{2n+1} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-1} + 2p_{2n}$ **.**

Observaţie Formulele (1) şi (2) au fost enunțate de Scherk în anul 1830 iar S. S. Pillai a fost primul care a prezentat o demonstrație a lor în anul 1928.

În cele ce urmează vom prezenta o soluție dată de W. Sierpinski în anul 1952.

Vom spune că un şir $(q_n)_{n\geq 1}$ de numere naturale impare are proprietate (P) dacă el este strict crescător, $q_1=2$, $q_2=3$, $q_3=5$, $q_4=7$, $q_5=11$, $q_6=13$, $q_7=17$ şi $q_{n+1} < 2q_n$, pentru orice $n\in\mathbb{N}^*$.

Ținând cont de relațiile de la Teorema lui Cebîşev deducem imediat că şirul $(p_n)_{n\geq 1}$ al numerelor prime este un exemplu de şir cu proprietatea (P). Astfel, pentru probarea formulelor (1) şi (2) ale lui Scherk, este suficient să le probăm pe acestea pentru un şir $(q_n)_{n\geq 1}$ ce are proprietatea (P).

LEMA 5.2. Dacă $(q_n)_{n\geq 1}$ este un şir cu proprietatea (P), atunci pentru orice număr natural impar $m \leq q_{2n+1}$ (n ≥3), există o alegere convenabilă a semnelor „+'' sau „–" a.î. $m = \pm q_1 \pm q_2 \pm .... \pm q_{2n-1} + q_{2n}$ **.**

Demonstraţie Vom demonstra această lemă făcând inducție matematică după n≥3. Dacă n=3, atunci $q_7=17$ iar numerele impare $m \leq 17$ sunt 1, 3, 5, 7, 9, 11, 13, 15, 17.

Deoarece prin calcul direct se verifică egalitățile :

$$1 = -q_1 + q_2 + q_3 - q_4 - q_5 + q_6$$
$$3 = q_1 - q_2 - q_3 + q_4 - q_5 + q_6$$
$$5 = q_1 + q_2 + q_3 - q_4 - q_5 + q_6$$
$$7 = -q_1 - q_2 - q_3 - q_4 + q_5 + q_6$$
$$9 = q_1 + q_2 - q_3 + q_4 - q_5 + q_6$$
$$11 = q_1 - q_2 - q_3 - q_4 + q_5 + q_6$$
$$13 = q_1 - q_2 + q_3 + q_4 - q_5 + q_6$$
$$15 = -q_1 + q_2 + q_3 + q_4 - q_5 + q_6$$
$$17 = q_1 + q_2 - q_3 - q_4 + q_5 + q_6$$

deducem că lema este adevărată pentru n=3.

Să observăm că pentru n=2 lema este falsă căci atunci $q_2=11$ iar 5 de exemplu nu se poate scrie sub forma $\pm 2 \pm 3 \pm 5 + 7$ pentru nici o alegere a lui „+'' sau „-''.

Să presupunem acum că lema este adevărată pentru n≥3, şi fie 2k-1 un număr impar a.î. $2k-1 \le q_{2n+3}$.

Cum şirul $(q_n)_{n\ge 1}$ are proprietatea (P) deducem că $q_{2n+3} < 2q_{2n+2}$ şi prin urmare deducem că $-q_{2n+2} < 2k-1-q_{2n+2} < q_{2n+2}$ astfel că pentru o alegere convenabilă a semnelor „+" sau „–" avem $0 \le \pm(2k-1-q_{2n+2}) < q_{2n+2}$.

Cum din $q_{2n+2} < 2q_{2n+1}$ deducem că $-q_{2n+1} \le \pm(2k-1-q_{2n+2}) - q_{2n+1} < q_{2n+1}$ şi astfel pentru o nouă alegere convenabilă a semnelor „+" sau „–" avem

$$0 \le \pm\left[\pm(2k-1-q_{2n+2}) - q_{2n+1}\right] \le q_{2n+1}.$$

Cum q_{2n+2} şi q_{2n+1}sunt numere impare, deducem că şi numărul $m = \pm\left[\pm(2k-1-q_{2n+2}) - q_{2n+1}\right]$ este impar şi cum $m \le q_{2n+1}$, conform ipotezei de inducție găsim o alegere convenabilă a semnelor „+" sau „–" a.î.
$m = \pm\left[\pm(2k-1-q_{2n+2}) - q_{2n+1}\right] = \pm q_1 \pm q_2 \pm .... \pm q_{2n-1} \pm q_{2n}$, de unde deducem că la o alegere convenabilă a semnelor „+" sau „–" avem

$$2k-1 = \pm q_1 \pm q_2 \pm .... \pm q_{2n+1} \pm q_{2n+2}$$

şi astfel Lema 5.2. este demonstrată. ■

<u>COROLAR 5.3.</u> Pentru o alegere convenabilă a semnelor „+" sau „–" avem egalitatea $q_{2n+1} = \pm q_1 \pm q_2 \pm ..... \pm q_{2n-1} + q_{2n}$.

Pentru n=1 şi n=2 se verifică imediat relaţiile $q_3=q_1+q_2$ şi $q_5=q_1-q_2+q_3+q_4$.

Să demonstrăm acum formulele (1) şi (2) din Teorema lui Scherk.

Într-adevăr, pentru n≥3, numărul $q_{2n+1}-q_{2n}-1$ este impar şi $<q_{2n+1}$ şi deci conform lemei anterioare, la o alegere convenabilă a semnelor „+" sau „–" avem egalitatea $q_{2n+1}-q_{2n}-1=\pm q_1\pm q_2\pm\ldots\pm q_{2n-1}+q_{2n}$, de unde $q_{2n+1}=1\pm q_1\pm\ldots\pm q_{2n-1}+2q_{2n}$ şi astfel formula (2) rezultă imediat considerând pentru n≥1, $q_n=p_n$.

Pentru n=1 sau n=2, prin calcul direct se verifică egalităţile $q_3=1-q_1+2q_2$ şi $q_5=1-q_1+q_2-q_3+2q_4$, astfel că formulele (2) sunt valabile pentru orice $n\in\mathbb{N}^*$.

Pentru a proba formulele (1) să observăm că $q_{2n+2}<2q_{2n+1}$ şi $q_{2n+2}-q_{2n+1}-1$ este impar şi $<q_{2n+1}$, deci conform lemei putem alege convenabil semnele „+" sau „–" a.î. $q_{2n+2}-q_{2n+1}-1=\pm q_1\pm\ldots\pm q_{2n-1}+q_{2n}$, de unde $q_{2n+2}=1\pm q_1\pm\ldots\pm q_{2n-1}+q_{2n}+q_{2n+1}$ deci (luând în loc de n+1 pe n) $q_{2n}=1\pm q_1\pm\ldots\pm q_{2n-3}+q_{2n-2}+q_{2n-1}$ şi astfel şi (1) sunt verificate pentru n≥3.

Pentru n=0, 1 sau 2, cum $q_2=1+q_1$, $q_4=1-q_1+q_2+q_3$ iar $q_6=1+q_1-q_2-q_3+q_4+q_5$ deducem că formulele (1) sunt valabile pentru orice $n\in\mathbb{N}^*$. (luând din nou $q_n=p_n$). ■

§6 Există funcţii care definesc numerele prime ?

În cele ce urmează dorim să clarificăm existenţa unor funcţii (calculabile) $f:\mathbb{N}^*\to\mathbb{N}^*$ care să satisfacă una din următoarele condiţii :

a) $f(n)=p_n$, pentru orice n≥1 (unde reamintim că p_n este al n-ulea număr prim).

b) Pentru orice $n\in\mathbb{N}^*$, f(n) este număr prim iar f este funcţie injectivă.

1. Funcţii satisfăcând condiţia a)

Hardy şi Wright şi-au pus următoarele probleme :

1) Există o formulă care să ne dea al n-ulea număr prim p_n ?

2) Există o formulă care să ne dea expresia fiecărui număr prim în funcţie de numerele prime precedente ?

În cele ce urmează vom prezenta o formulă pentru calculul lui p_n.

Reamintim că pentru orice număr real strict pozitiv x prin $\pi(x)$ am notat numărul numerelor prime p a.î. $p \le x$.

La început vom prezenta o formulă pentru $\pi(m)$ dată de Willans în anul 1964.

Pentru aceasta, pentru fiecare număr natural $j \ge 1$ fie

$$F(j)=\left[\cos^2 \pi \frac{(j-1)\,!\,+1}{j}\right].$$

Astfel, pentru orice număr natural $j>1$, $F(j)=1$ pentru j prim iar $F(j)=0$ în caz contrar (evident $F(1)=1$). Deducem că $\pi(m)=-1+\sum_{j=1}^{m}F(j)$.

Willans a dat formula $\pi(m)=\sum_{j=1}^{m}H(j)$, m=2, 3, ….. unde

$$H(j)=\frac{\sin^2 \frac{((j-1)\,!)^2}{j}}{\sin^2 \frac{\pi}{j}}.$$

Mináč a dat o altă expresie pentru $\pi(m)$ în care nu mai intervine sinusul sau cosinusul şi anume

$$\pi(m)=\sum_{j=2}^{m}\left[\frac{(j-1)\,!+1}{j}-\left[\frac{(j-1)\,!}{j}\right]\right].$$

Iată o demonstraţie simplă pentru formula lui Mináč. Începem cu observaţia că pentru $n\ne 4$, care nu este prim, n divide (n-1)!. Într-adevăr, fie n este de forma $n=ab$ cu $2 \le a, b \le n-1$, şi $a \ne b$, fie $n=p^2\ne 4$.

În primul caz, n divide (n-1)! în timp ce în al doilea caz $2<p\le n-1=$ $=p^2-1$, şi atunci $2p\le p^2-1$ şi n divide $2p^2=p\cdot 2p$ care la rândul său divide pe (n-1)!.

Conform Teoremei lui Wilson pentru fiecare număr prim j putem scrie $(j-1)!+1=kj$, $(k\in\mathbb{N}^*)$, deci

$$\left[\frac{(j-1)\,!\,+1}{j}-\left[\frac{(j-1)\,!}{j}\right]\right]=\left[k-\left[k-\frac{1}{j}\right]\right]=1\ .$$

Dacă j nu este număr prim, atunci după remarca precedentă $(j-1)!=kj$ $(k\in\mathbb{N}^*)$ şi astfel $\left[\frac{(j-1)\,!\,+1}{j}-\left[\frac{(j-1)\,!}{j}\right]\right]=\left[k+\frac{1}{j}-k\right]=0$.

În fine, dacă j=4, atunci $\left[\frac{3\ !\ +1}{4}-\left[\frac{3\ !}{4}\right]\right]=0$ şi astfel formula lui Mináč este demonstrată.

Utilizând cele de mai sus se obține formula lui Willans pentru p_n :

$$p_n=1+\sum_{m=1}^{n}\left[\left[\frac{n}{\sum_{j=1}^{m}F(j)}\right]^{\frac{1}{n}}\right], \text{ sau } p_n=1+\sum_{m=1}^{n}\left[\left[\frac{n}{1+\pi(m)}\right]^{\frac{1}{n}}\right].$$

O altă formulă pentru cel mai mic număr prim superior unui număr natural dat m≥2, a fost dată de Ernvall în 1975 : Fie $d=\left((m\ !)^{m\ !}-1,\ (2m)\ !\right)$, $t=\frac{d^d}{\left(d^d,d\ !\right)}$ iar a unicul număr natural pentru care d^a divide t iar d^{a+1} nu divide t.

Atunci cel mai mic număr prim p superior lui m este $p=\frac{d}{\left(\frac{t}{d^a},d\right)}$.

Dacă vom lua $m=p_{n-1}$ obținem din nou o formulă pentru p_n.

Reamintim cum se defineşte funcția lui Möbius : $\mu(1)=1$, $\mu(n)=(-1)^r$ dacă n este un produs de r numere prime distincte iar $\mu(n)=0$ dacă n are ca factor un pătrat.

Cu ajutorul acestei funcții, în 1971 Ghandi a arătat că dacă notăm $P_{n-1}=p_1p_2\ldots p_{n-1}$, atunci $P_n=\left[1-\frac{1}{\log 2}\log\left(-\frac{1}{2}+\sum_{d\mid P_{n-1}}\frac{\mu(d)}{2^d-1}\right)\right]$ sau, analog, P_n este singurul număr natural pentru care $1<2^{P_n}\left(-\frac{1}{2}+\sum_{d\mid P_{n-1}}\frac{\mu(d)}{2^d-1}\right)<2$.

Iată o demonstrație a formulei lui Ghandi prezentată în 1972 de Vanden Eynden :

Să notăm $Q=P_{n-1}p_n=p$ şi $S=\sum_{d\mid Q}\frac{\mu(d)}{2^d-1}$. Atunci

$\left(2^Q-1\right)S=\sum_{d\mid Q}\mu(d)\cdot\frac{2^Q-1}{2^d-1}=\sum_{d\mid Q}\mu(d)\left(1+2^d+2^{2d}+\ldots+2^{Q-d}\right)$. Dacă $0\le t<Q$ termenul $r(d)\cdot 2^t$ apare exact atunci când $d\mid(t, Q)$. Deci coeficientul lui 2^t în sumă este $\sum_{d\mid(t,Q)}\mu(d)$; în particular, pentru t=0, coeficientul este egal cu $\sum_{d\mid Q}\mu(d)$.

Reamintim că $\sum_{d\mid m}\mu(d)=\begin{cases}1 & daca\ m=1\\ 0 & daca\ m>1\end{cases}$. Dacă scriem $\sum_{0<t<Q}{}'$ pentru suma extinsă la toate valorile lui t a.î. $0<t<Q$ şi $(t, Q)=1$, atunci $(2^Q-1)\ S=\sum_{0<t<Q}{}'2^t$; cel mai mare indice în această sumă este t=Q-1. Rezultă că

$$2\left(2^Q-1\right)\left(-\frac{1}{2}+S\right)=-\left(2^Q-1\right)+\sum_{0<t<Q}{}'2^{t+1}=1+\sum_{0<t<Q-1}{}'2^{t+1}.$$

Dacă $2\le j<p_n=p$, există un număr prim q a.î. $q<p_n<p$ (deci q|Q) şi q|Q-j. Fiecare indice t din suma considerată mai înainte satisface deci condiția $0<t\le Q-p$.

Atunci $\frac{2^{Q-p+1}}{2\cdot 2^Q}<-\frac{1}{2}+S=\frac{1+\sum_{0<t\le Q-p}{}'2^{t+1}}{2\cdot\left(2^Q-1\right)}<\frac{2^{Q-p+2}}{2\cdot 2^Q}$. Înmulțind cu 2^p deducem că $1<2^p\left(-\frac{1}{2}+S\right)<2$.■

2. Funcții satisfăcând condiția b)

Numărul $f(n)=\left\lfloor\theta^{3^n}\right\rfloor$ este prim pentru orice $n\ge 1$, (aici $\theta\approx 1{,}3064\ldots$ - vezi –**W. H. Mills : Prime- representing function, Bull. Amer. Math. Soc.,53 , pp 604) .**

De asemenea, $g(n)=\left[2^{2^{\cdot^{\cdot^{\cdot^{\omega}}}}}\right]$ (cu un şir de n exponenți) este un număr prim pentru orice număr natural $n\ge 1$ (aici $\omega\approx 1{,}9287800\ldots$-vezi – **E. M. Wright: A prime –representing function, Amer. Math. Monthly, 58, 1951, pp.616-618).**

Din păcate, numerele θ şi ω se cunosc doar cu aproximație iar valorile lui f(n) şi g(n) cresc foarte repede, aşa că cele două funcții nu sunt prea utile

rămânând doar ca nişte curiozităţi (de ex, g(1)=3, g(2)=13, g(3)=16381, g(4) are deja mai mult de 5000 de cifre !).

Tentaţia de a găsi o funcţie polinomială cu coeficienţi din $\mathbb{Z}$ a.î. valorile sale să fie numere prime este sortită eşecului deoarece dacă $f\in\mathbb{Z}[X]$ este neconstant, atunci există o infinitate de întregi n cu proprietatea că |f(n)| nu este număr prim.

Într-adevăr, deoarece f este neconstant problema este trivială dacă toate valorile lui f sunt numere compuse. Să presupunem deci că există $n_0\geq 0$ un număr natural a.î. $|f(n_0)|=p$ este număr prim. Cum f nu este constant deducem că $\lim_{x\to\infty}|f(x)|=+\infty$, deci există $n_1>n_0$ a.î. dacă $n\geq n_1\Rightarrow|f(n)|>p$. Astfel pentru orice întreg h pentru care $n_0+ph\geq n_1$ avem $f(n_0+ph)=f(n_0)+Mp=Mp$. Dacă $|f(n_0+ph)|>p$, atunci $|f(n_0+ph)|$ este număr compus.

Cum dacă $f\in\mathbb{C}[X_1,\ldots X_m]$ ($m\geq 2$) are proprietatea că ia valori numere prime pentru orice $X_1, ..X_n$ naturale, atunci cu necesitate f este constant, deducem că şi tentaţia de a găsi o funcţie polinomială neconstantă de mai multe nedeterminate care să ia valori numere prime pentru oricare valori naturale ale nedeterminatelor este sortită eşecului.

Dacă $f(x)=x^2+x+41$ (faimosul polinom al lui Euler) atunci pentru k=0, 1, .., 39 f(k) este prim : 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601 (pentru $k=40\Rightarrow f(40)=1681=41^2$).

Dacă vom considera $f(x)=x^2+x+q$, (q prim) atunci sunt echivalente :

1) x^2+x+q este prim pentru x=0, 1, …, q-2

2) q=2, 3, 5, 11, 17, sau 41.

Frobenius (1912) şi Hendy (1974) au demonstrat că :

i) Singurele polinoame $f(x)=2x^2+p$ (cu p prim) a.î. f(k) este prim pentru x=0, 1, .., p-1 sunt pentru p=3, 5, 11, 29.

ii) Singurele polinoame de forma $f(x)=2x^2+2x+\frac{p+1}{2}$ (cu p prim, $p\equiv 1 \pmod 4$) a.î. f(x) este prim pentru x=0, 1, …, $\frac{p-3}{2}$ sunt cele pentru p=5, 13, 37.

§7. Numere prime gemene

Dacă p şi p+2 sunt simultan numere prime, vom spune despre ele că sunt *gemene*. Exemple : (3, 5), (5, 7), (11, 13), (17, 19), etc.

În 1949, **Clément [Clement, P. A. : Congruences for sets of primes, Amer. Math. Monthly, 56, 1949, 23-25**] a prezentat următorul rezultat legat de numerele gemene :

Pentru $n \geq 2$, n şi n+2 sunt simultan prime $\Leftrightarrow 4[(n-1)!+1]+n \equiv 0 \pmod{n(n+2)}$. (din păcate din punct de vedere practic acest rezultat nu are nici o utilitate).

Problema principală este de a decide dacă există sau nu o infinitate de numere gemene.

Dacă notăm pentru $x > 1$ prin $\pi_2(x)$=numărul numerelor prime p a.î. p+2 este prim şi $p+2 \leq x$, atunci Brun a demonstrat în 1920 că există un număr natural x_0 (efectiv calculabil) a.î. pentru orice $x \geq x_0$ să avem $\pi_2(x) < \frac{100x}{(\lg x)^2}$.

Într-un alt articol celebru din 1919 (**La serie** $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+....$ **, ou les denominateurs sont nombres premiers jumeaux est convergente ou finie** din **Bull. Sc. Math., vol.43, pp. 100-104** şi **124-128**) tot Brun a demonstrat că seria $B = \sum\left(\frac{1}{p}+\frac{1}{p+2}\right)$ (unde suma este extinsă după perechile de numere gemene (p, p+2)) este convergentă sau mulţimea acestor numere gemene este finită. Numărul B poartă numele de *constanta lui Brun* iar Shanks şi Wrench (în 1974) iar Brent (în 1976) au arătat că $B \simeq 1{,}90216054\ldots$

Cele mai mari numere prime gemene cunoscute sunt $1706595 \cdot 2^{11235} \pm 1$ şi $571305 \cdot 2^{7701} \pm 1$. ([26]) .

De aici rezultă că mulţimea numerelor prime gemene, dacă este infinită, (lucru neprobat până acum), atunci ele se apropie foarte mult unele de altele.

CAPITOLUL 8:
FUNCŢII ARITMETICE

§1. Generalităţi. Operaţii cu funcţii aritmetice

DEFINITIA 1.1. **Numim *funcţie aritmetică* orice funcţie f:$\mathbb{N}\to\mathbb{C}$.**

În cadrul acestui capitol vom prezenta mai multe exemple de astfel de funcţii.

Fie **A**={f:$\mathbb{N}\to\mathbb{C}$} mulţimea funcţiilor aritmetice. Pentru f, g$\in$**A** definim f+g, fg, f∗g:$\mathbb{N}\to\mathbb{C}$ astfel: (f+g)(n)=f(n)+g(n), (fg)(n)=f(n)·g(n) şi (f∗g)(n)= $\sum_{d|n} f(d)g(n/d)$ pentru orice n$\in\mathbb{N}$.

Observaţie f∗g poartă numele de „ *produsul Dirichlet de convoluţie*" al lui f şi g.

PROPOZITIA 1.2. **(A , + , ∗) este inel comutativ unitar**.

Demonstraţie Faptul că (**A**, +) , este grup abelian este imediat. Să probăm că (**A** , ∗) este monoid comutativ. Într-adevăr, dacă f, g, h$\in$**A**, atunci:

$$(f*(g*h))(n)=\sum_{d/n} f(d)\sum_{e/\frac{n}{d}} g(e)h(n/de)=$$

$$=\sum_{D|n}\Big(\sum_{e|D} f(D/e)g(e)h(n/D)\Big)=((f*g)*h)(n)$$

(D=de), pentru orice n$\in\mathbb{N}$, adică „∗" este asociativă. (am ţinut cont de faptul că atunci când d parcurge divizorii lui d, acelaşi lucru îl face şi n/d). Cu acelaşi argument rezultă şi comutativitatea produsului de convoluţie.

Elementul neutru pentru ∗ este δ :$\mathbb{N}\to\mathbb{C}$, $\delta(n)=\begin{cases}1 & pentru\ n=1\\ 0 & pentru\ n\neq 1\end{cases}$

deoarece se verifică imediat că f∗δ=δ∗f =f, pentru orice f$\in$**A**.

Pentru a încheia, să mai probăm că dacă f, g, h$\in$**A**, atunci

f∗(g+h)=(f∗g)+(f∗h). Într-adevăr, dacă n$\in\mathbb{N}$, atunci:

$$(f*(g+h))(n)=\sum_{d/n} f(d)(g(n/d)+h(n/d))=\sum_{d/n} f(d)g(n/d)+$$

$$+\sum_{d/n} f(d)h(n/d) = (f*g)(n)+(f*h)(n) = (f*g+f*h)(n)\ .\ \blacksquare$$

PROPOZIŢIA 1.3. $\mathbf{f\in U(A) \Leftrightarrow f(1)\neq 0.}$

Demonstraţie: Dacă $f\in\mathbf{U(A)}$, atunci există $g \overset{not}{=} f^{-1}\in\mathbf{A}$ a.î. $f*f^{-1}=f^{-1}*f=\delta$. Deci $1=\delta(1)=f(1)f^{-1}(1)$, adică $f(1)\neq 0$. Reciproc, dacă $f(1)\neq 0$, dacă definim inductiv

$$g(n)=\begin{cases} \dfrac{1}{f(1)} & \text{dacă } n=1 \\ -\dfrac{1}{f(1)}\displaystyle\sum_{\substack{d/n \\ d>1}} f(d)g(n/d) & \text{dacă } n>1, \end{cases}$$

se verifică imediat că $g=f^{-1}$. $\blacksquare$

Iată câteva exemple de funcţii aritmetice:

1. **Funcţia φ a lui Euler** definită în §4 de la Capitolul 6.

2. Pentru $k\in\mathbb{N}$ definim $\sigma_k:\mathbb{N}\to\mathbb{C}$ astfel $\sigma_k=\sum_{d/n} d^k$ iar $\xi_k(n)=n^k$.

În particular σ_1 se va nota cu σ (deci $\sigma(n)$=*suma divizorilor lui n*), σ_0 cu τ (deci $\tau(n)$=*numărul divizorilor lui n*) iar $\xi_0=\xi$ (ξ poartă numele de *funcţia zeta* şi deci $\xi(n)=1$ pentru orice $n\in\mathbb{N}$).

Dacă $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ este descompunerea canonică a lui n în produs de numere prime, atunci $\sigma(n)$ va fi suma produselor de forma $p_1^{\beta_1}\ldots p_k^{\beta_k}$ cu $\beta_i\le\alpha_i$, $1\le i\le k$ adică

$$\sigma(n)=\left(1+p_1+\ldots+p_1^{\alpha_1}\right)\left(1+p_2+\ldots+p_2^{\alpha_2}\right)\ldots\left(1+p_k+\ldots+p_k^{\alpha_k}\right)=$$
$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

3. Funcţia $\tau:\mathbb{N}\to\mathbb{N}$, $\tau(n)$=numărul divizorilor naturali ai lui n ($n\in\mathbb{N}$).

Se verifică imediat că dacă $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ atunci $\tau(n)=(\alpha_1+1)\ldots(\alpha_k+1)$.

Observaţie Conform Propoziţiei 1.3. funcţia zeta ξ are inversă în inelul **A**; ξ^{-1} se notează cu μ şi poartă numele de *funcţia lui Möbius*.

Deoarece $\mu*\xi=\delta$, deducem că:

$$\sum_{d|n}\mu(d)=\begin{cases}1 & daca\ \ n=1\\ 0 & daca\ \ n\neq 1\end{cases}$$

În particular, dacă p este un număr prim iar $\alpha \geq 2$ atunci $\sum_{j=0}^{\mu} \mu(p^{\alpha})=0$.

Astfel $\mu(1)=1$, $\mu(p)=-1$, iar $\mu(p^{\alpha})=0$, pentru orice $\alpha \geq 2$.

Observaţie Dacă f, $g\in\mathbf{A}$ şi $f=g*\xi$, atunci $g=f*\mu$. Acest fapt este cunoscut sub numele de *formula clasică de inversare a lui Möbius*.

Dacă scriem explicit obţinem:

PROPOZIŢIA 1.4. Dacă f şi g sunt funcţii aritmetice atunci $f(n)=\sum_{d/n} g(d)$ **pentru orice** $n\in\mathbb{N}$ $\Leftrightarrow g(n)=\sum_{d/n} f(d)\mu(n/d)$ **pentru orice** $n\in\mathbb{N}$.

Ca un exemplu avem că: $\sigma_k(n)=\sum_{d/n} d^k$ pentru orice $n\in\mathbb{N}$ astfel că $n^k=\sum_{d/n} \sigma_k(d)\mu(n/d)$ pentru orice $n\in\mathbb{N}$.

LEMA 1.5. Pentru $n\in\mathbb{N}$ **şi** $d|n$ **, fie** $S_d=\{xn/d : 1\leq x\leq d, x\in\mathbb{N}, (x, d)=1\}$ **Atunci pentru** $d|n, e|n, d\neq e$, $S_d\cap S_e=\varnothing$ **iar** $\bigcup_{d/n} S_d=\{1,2,\ldots\ldots,n\}$.

Demonstraţie: Presupunând că $S_d\cap S_e\neq\varnothing$, există $x, y\in\mathbb{N}^*$ a.î. $1\leq x\leq d$, $1\leq y\leq e$, $(x, d)=(y, e)=1$ şi $xn/d=yn/e \Leftrightarrow xe=yd$.

Cum $(x, d)=1$, $x|y$ şi analog $y|x$, deci $x=y$, adică $d=e$ - absurd !.

Cum pentru $d|n$, $1\leq m\leq n$ şi $(m, n)=n/d$, dacă $m=xn/d$, atunci $(x, d)=1$ şi $1\leq x\leq dm/n\leq d$, deducem că $m\in S_d$ adică $\{1,2,\ldots, n\}\subseteq \bigcup_{d/n} S_d$ şi cum incluziunea inversă este imediată deducem egalitatea cerută. ■

COROLAR 1.6. Cum S_d **are** $\varphi(d)$ **elemente, deducem că** $n=\sum_{d/n} \varphi(d)$, **pentru orice** $n\in\mathbb{N}$.

Conform Propoziţiei 1.4. deducem că $\varphi(n)=\sum_{d/n} d\mu(n/d)$ pentru orice $n\in\mathbb{N}$. În particular, dacă p este prim şi $\alpha\geq 1$ natural,

$$\varphi(p^{\alpha})=\sum_{j=0}^{q} p^j\mu(p^{\alpha-j})=p^{\alpha}-p^{\alpha-1}=p^{\alpha}(1-\frac{1}{p}).$$

§2. Funcţii multiplicative

DEFINIŢIA 2.1. O funcţie aritmetică f se zice *funcţie multiplicativă* dacă f≠0 şi f(m·n)=f(m)f(n), pentru orice m, n∈ℕ cu (m, n)=1.

Observaţie Dacă f este multiplicativă atunci din f≠0 există un n∈ℕ a.î. f(n)≠0 şi cum f(n)=f(1·n)=f(1)·f(n) deducem că f(1)=1, adică în inelul **A**, f este inversabilă.

Dacă n∈ℕ iar $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ este descompunerea în factori primi a lui n, atunci $f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$, astfel că o funcţie multiplicativă este complet determinată de valorile ei pe mulţimile de forma p^{α} cu p prim şi α∈ℕ.

Să notăm cu **M** familia funcţiilor aritmetice multiplicative.

PROPOZIŢIA 2.2. Dacă $f \in M$ atunci şi $f^{-1} \in M$.

Demonstraţie Fie m, n∈ℕ cu (m, n)=1. Dacă m=n=1 atunci $f^{-1}(mn) = f^{-1}(m) f^{-1}(n)$.

Presupunem acum că mn ≠1 şi că $f^{-1}(m_1 n_1)=f^{-1}(m_1)f^{-1}(n_1)$ pentru orice pereche (m_1, n_1) de numere naturale cu $m_1n_1 < mn$ şi $(m_1, n_1) =1$.

Cum dacă m=1 sau n=1 din nou $f^{-1}(mn)=f^{-1}(n)\, f^{-1}(m)$, rămâne să analizăm cazul m≠1 şi n≠1.

Conform Propoziţiei 1.4. avem: $f^{-1}(mn) = -\sum_{\substack{d/mn \\ d>1}} f(d) f^{-1}(mn/d)$.

Deoarece (m, n)=1 orice divizor d al lui mn se scrie unic sub forma $d = d_1d_2$, unde $d_1|m$ şi $d_2|n$. Atunci $(d_1, d_2)=1$ şi $(m/d_1, n/d_2)=1$.

Astfel că:

$$f^{-1}(mn) = -\sum_{\substack{d_1|m \\ d_2|n \\ d_1d_2>1}} f(d_1d_2) f^{-1}(mn/d_1d_2) = (deoarece\ \ (m/d_1)(n/d_2) < mn) =$$

$$= -\sum_{\substack{d_1|m \\ d_2|n \\ d_1d_2>1}} f(d_1) f(d_2) f^{-1}(m/d_1) f^{-1}(n/d_2) = -f^{-1}(m) \sum_{\substack{d_2|n \\ d_2>1}} f(d_2) f^{-1}(n/d_2) -$$

$$-f^{-1}(n) \sum_{\substack{d_1|m \\ d_1>1}} f(d_1) f^{-1}(m/d_1) - \left(-\sum_{\substack{d_1|m \\ d_1>1}} f(d_1) f^{-1}(m/d_1)\right) \cdot$$

$$\cdot(-\sum_{\substack{d_2|n\\ d_2>1}} f(d_2)f^{-1}(n/d_2)) =$$

$$= f^{-1}(m)f^{-1}(n) + f^{-1}(m)f^{-1}(n) - f^{-1}(m)f^{-1}(n) = f^{-1}(m)f^{-1}(n)$$ şi totul este clar. ■

Observaţie Cum funcţia zeta ξ este multiplicativă, inversa sa care este funcţia lui Möbius μ este multiplicativă. Astfel :

$$\mu(n)=\begin{cases} 1 & \text{dacă } n=1 \\ (-1)^t & \text{dacă n este produs de t primi distincţi} \\ 0 & \text{în rest} \end{cases}$$

Avem în felul acesta o altă definire a funcţiei lui Möbius.

PROPOZIŢIA 2.3. Dacă f, g∈M atunci f*g∈M.

Demonstraţie (f∗g)(1)=f(1)g(1)=1 iar dacă (m, n)=1, atunci :

$$(f*g)(mn) = \sum_{d|mn} f(d)g(mn/d) = \sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2)g(m/d_1)g(n/d_2) =$$

$$= (\sum_{d_1|m} f(d_1)g(m/d_1))\cdot(\sum_{d_2|n} f(d_2)g(n/d_2)) = [(f*g)(m)][(f*g)(n)].$$ ■

Observaţii1. Deoarece ξ_k este multiplicativă şi $\sigma_k = \xi_k * \xi$ deducem că şi σ_k este multiplicativă. Astfel dacă k≥1, p este număr prim iar $\alpha\geq 1$ atunci

$$\sigma_k(p^\alpha) = \sum_{j=0}^{\alpha} p^{jk} = \frac{p^{(\alpha+1)k}-1}{p^k-1}$$ iar dacă $n = p_1^{\alpha_1}...p_t^{\alpha_t}$ atunci

$$\sigma_k(n) = \prod_{i=1}^{t} \frac{p_i^{(\alpha_i+1)k}-1}{p_i^k-1}.$$

În particular, $\sigma(n) = \prod_{i=1}^{t} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$.

Deoarece $\tau(p^\alpha) = \alpha+1$, $\tau(n) = \prod_{i=1}^{t} (\alpha_i+1)$.

2. Cum funcţia lui Euler φ este multiplicativă şi $\varphi=\xi_1*\mu$ atunci pentru orice $n\in\mathbb{N}$: $\varphi(n) = n\prod_{\substack{p|n\\ p\ prim}} (1-\frac{1}{p})$.

3. Funcţia φ a lui Euler este o funcţie calculabilă (adică pentru orice n, $\varphi(n)$ este cardinalul unei mulţimi şi anume a mulţimii $\{x: 1\leq x\leq n$ şi $(x, n)=1\}$).

Funcţiile calculabile pot fi câte o dată evaluate ţinând cont de *principiul includerii şi excluderii*:

Dacă $A_1,\ldots,A_t$ sunt submulţimi ale unei mulţimi finite S, atunci

$$|S-(A_1\cup\ldots\cup A_t)|=|S|+\sum_{j=1}^{t}(-1)^j\cdot\sum_{1\le i_1\le\ldots\le i_j\le t}\left|A_{i_1}\cap\ldots\cap A_{i_j}\right|$$

§3.Funcţia Jordan J_k

Funcţia Jordan J_K reprezintă o generalizare a funcţiei Euler φ şi se defineşte astfel:

DEFINIŢIA 3.1. Pentru $n\in\mathbb{N}$, $J_k(n)$=numărul k-uplurilor ordonate de numere naturale $(x_1,\ldots,x_k)$ a.î. $1\le x_i\le n$, $1\le i\le k$ şi $(x_1, x_2,\ldots,x_k, n)=1$.

Observaţie Evident $J_1=\varphi$.

Fie $n=p_1^{\alpha_1}\ldots p_t^{\alpha_t}$ descompunerea în factori primi a lui n, S=mulţimea k-uplurilor $(x_1,\ldots, x_k)$ a.î. $1\le x_i\le n$, $1\le i\le k$, iar A_i =mulţimea acelor k-upluri din S pentru care $p_i\mid(x_1,\ldots, x_k)$, $1\le i\le t$, atunci: $J_k(n)=|S-(A_1\cup\ldots\cup A_t)|$ iar $\left|A_{i_1}\cap\ldots\cap A_{i_j}\right|=(n/p_{i_1}\ldots p_{i_j})$ .Astfel:

$$J_K(n)=n^k+\sum_{j=1}^{t}(-1)^j\sum_{1\le i_1<i_2<\ldots<i_j\le t}\left(\frac{n}{p_{i_1}\cdots p_{i_j}}\right)^k=\sum_{d\mid n}\left(\frac{n}{d}\right)^k\mu(d)=\sum_{d\mid n}d^k\mu(n/d)$$

Deducem astfel că $J_k=\xi_k*\mu$ şi astfel rezultă că J_k este funcţie multiplicativă.

Dacă p este prim şi $\alpha\ge1$, atunci $J_K(p^\alpha)=p^{\alpha k}-p^{(\alpha-1)k}=p^{\alpha k}(1-\frac{1}{p^k})$, astfel că $J_k(n)=n^k\prod_{p\mid n}(1-\frac{1}{p^k})$.

§4.Funcţia von Sterneck H_k

Iată acum o altă generalizare a funcţiei lui Euler (numită funcţia *von Sterneck*).

DEFINIŢIA 4.1. Pentru $n, k\in\mathbb{N}$ definim

$H_k(n)=\sum_{[e_1,\ldots,e_k]=n}\varphi(e_1)\ldots\varphi(e_k)$, *suma făcându-se după toate k-uplurile $(e_1,\ldots,e_k)$ de numere naturale a.î. $1\le e_i\le n$, $1\le i\le k$ şi $[e_1,\ldots,e_k]=n$.*

Observaţie În mod evident $\varphi=H_1$ iar $H_k(1)=1$.

Presupunem acum că (m, n)=1 şi că $[e_1,\ldots, e_k]=mn$. Pentru i=1,…, k, e_i poate fi descompus în mod unic sub forma $e_i=c_id_i$, unde $c_i|m$ şi $d_i|n$, iar $[c_1,\ldots,c_k]=m$ şi $[d_1,\ldots, d_k]=n$. Astfel:

$$H_k(mn)=\sum_{[e_1,\ldots,e_k]=mn}\varphi(e_1)\ldots\varphi(e_k)=\sum_{\substack{[c_1,\ldots,c_k]=m\\ [d_1,\ldots,d_k]=n}}\varphi(c_1)\ldots\varphi(c_k)\varphi(d_1)\ldots\varphi(d_k)=$$

$$=\sum_{[c_1,\ldots,c_k]=m}\varphi(c_1)\ldots\varphi(c_k)\sum_{[d_1,\ldots,d_k]=n}\varphi(d_1)\ldots\varphi(d_k)=H_k(m)H_k(n)$$

adică H_k este funcţie multiplicativă .

PROPOZIŢIA 4.2. Pentru orice k, $H_k=J_k$.

Demonstraţie Facem inducţie matematică după k.

Am văzut mai înainte că $H_1=\varphi=J_1$.

Fie k>1 şi presupunem că $H_{k-1}=J_{k-1}$.

Cum H_k şi J_k sunt funcţii multiplicative, a demonstra că $H_k=J_k$ este suficient să demonstrăm că $H_k(p^\alpha)=J_k(p^\alpha)$ unde p este prim, iar $\alpha\geq 1$. Conform ipotezei de inducţie avem că $H_{k-1}(p^\alpha)=J_{k-1}(p^\alpha)$ iar

$$H_k(p^\alpha)=\sum_{\max(\beta_1,\ldots,\beta_i)=\alpha}\varphi(p^{\beta_1})\ldots\varphi(p^{\beta_i})=$$

$$=\sum_{\max(\beta_1,\ldots,\beta_i)=\alpha}\varphi(p^{\beta_1})\ldots\varphi(p^{\beta_{i-1}})\varphi(p^{\beta_i})+\ldots\sum_{\max(\beta_1,\ldots,\beta_i)\leq\alpha}\varphi(p^{\beta_1})\ldots\varphi(p^{\beta_{i-1}})\varphi(p^\alpha)=$$

$$=H_{k-1}\left(p^\alpha\right)\sum_{d\mid p^\alpha}\varphi(d)+\left(\sum_{d\mid p^\alpha}\varphi(d)\right)^{k-1}\varphi(p^\alpha)=$$

$$=p^{\alpha-1}H_{k-1}(p^\alpha)+p^{\alpha(k-1)}\varphi(p^\alpha)=$$

$$=p^{\alpha-1}J_{k-1}(p^\alpha)+p^{\alpha(k-1)}\varphi(p^\alpha)=p^{\alpha-1}p^{\alpha(k-1)}(1-\frac{1}{p^{k-1}})+p^{\alpha(k-1)}p^\alpha(1-\frac{1}{p})=$$

$$=p^{\alpha k}[\frac{1}{p}(1-\frac{1}{p^{k-1}})+(1-\frac{1}{p})]=p^{\alpha k}(1-\frac{1}{p^k})=J_k(p^\alpha).\ \blacksquare$$

§5.Funcţii complet multiplicative

DEFINIŢIA 5.1. **O funcţie $f\in A$ se zice *complet multiplicativă* dacă există $n\in\mathbb{N}$ a.î. $f(n)\neq 0$ iar $f(mn)=f(m)f(n)$, pentru orice $m, n\in\mathbb{N}$. (dacă notăm prin $\mathbf{M}^c$ clasa acestor funcţii, atunci în mod evident $\mathbf{M}^c\subseteq\mathbf{M}\subseteq\mathbf{A}$)**

PROPOZIŢIA 5.2. Dacă $f\in\mathbf{M}$, atunci $f\in\mathbf{M}^c \Leftrightarrow f^{-1}=\mu f$.

Demonstraţie Dacă $f\in\mathbf{M}^c$, atunci pentru orice $n\in\mathbb{N}$:

$$(\mu f * f) = \sum_{d|n}\mu(d)f(d)f(n/d) = f(n)\sum_{d|n}\mu(d) = \begin{cases} f(1)=1 & daca\ \ n=1 \\ 0 & daca\ \ n\neq 1 \end{cases},$$

adică $\mu f * f = \delta \Leftrightarrow f^{-1}=\mu f$.

Invers, să presupunem că $f^{-1}=\mu f$. Pentru a proba că $f\in\mathbf{M}^c$ este suficient să probăm că dacă p este prim şi $\alpha \geq 1$, atunci $f(p^\alpha)=(f(p))^\alpha$. Acest lucru îl vom face prin inducţie matematică după α ; evident, pentru $\alpha=1$ totul este clar. Să presupunem că $\alpha\geq 2$ şi că $f(p^{\alpha-1})=(f(p))^{\alpha-1}$.

Deoarece pentru oricare $\beta\geq 2$, $f^{-1}(p^\beta)=\mu(p^\beta)f(p^\beta)=0$, deducem că:
$0=(f^{-1}*f)(p^\alpha) = f(p^\alpha) + f^{-1}(p)\, f(p^{\alpha-1}) = f(p^\alpha) + f^{-1}(p)\,(f(p))^{-1}$. Deoarece $f^{-1}(p)=-f(\beta)$ $\Rightarrow f(p^\alpha)=(f(p))^\alpha$. ■

COROLAR 5.3. Dacă $f\in\mathbf{M}$, atunci $f\in\mathbf{M}^c \Leftrightarrow f^{-1}(p^\alpha)=0$, pentru orice p prim şi $\alpha\geq 2$.

PROPOZIŢIA 5.4. Fie $f\in\mathbf{M}$. Atunci $f\in\mathbf{M}^c \Leftrightarrow f(g*h)=(fg)*(fh)$, pentru orice $g, h\in\mathbf{A}$.

Demonstraţie Dacă $f\in\mathbf{M}^c$, atunci pentru orice $g, h\in\mathbf{A}$ avem

$$(f(g*h))(n) = f(n)\sum_{d|n}g(d)h(n/d) = \sum_{d|n}f(d)g(d)f(n/d)h(n/d) = (fg*fh)(n).$$

Invers, să presupunem că $f(g*h)=(fg)*(fh)$, pentru orice $g, h\in\mathbf{A}$. În particular, pentru $g=\xi$ şi $h=\mu$ avem $\delta=f\delta=f(\xi*\mu)=f\xi*f\mu=f*f\mu$, adică $f^{-1}=\mu f$, adică $f\in\mathbf{M}^c$ (conform Propoziţiei 5.4.).■

PROPOZIŢIA 5.5. Dacă $f\in\mathbf{M}$, atunci există $g, h\in\mathbf{M}^c$ a.î. $f=g*h \Leftrightarrow f^{-1}(p^\alpha)=0$, pentru orice p prim şi orice $\alpha\geq 3$.

Demonstraţie Să presupunem că $f=g*h$ cu $g, h\in\mathbf{M}^c$ şi fie p prim iar $\alpha\geq 3$. Atunci

$$f^{-1}\left(p^{\alpha}\right)=\left(g^{-1}*h^{-1}\right)\left(p^{\alpha}\right)=$$

$$=\sum_{j=0}^{\alpha}g^{-1}\left(p^{j}\right)\cdot h^{-1}\left(p^{\alpha-j}\right)=g^{-1}(1)\cdot h^{-1}\left(p^{\alpha}\right)+g^{-1}(p)\cdot h^{-1}\left(p^{\alpha-1}\right)$$

(căci $g\in\mathbf{M}^{c}$) =0 (căci $h\in\mathbf{M}^{c}$ şi $\alpha\geq 3$).

Invers, fie $f\in\mathbf{M}$ a.î. $f^{-1}(p^{\alpha})=0$ pentru orice p prim şi $\alpha\geq 3$.

Alegem $g\in\mathbf{M}^{c}$ a.î. pentru orice p prim, g(p) este o rădăcină a ecuaţiei :

$$X^2+f^{-1}(p)X+f^{-1}(p^2)=0.$$

Dacă alegem $h=g^{-1}*f$, atunci $h\in\mathbf{M}$ şi pentru orice p prim şi $\alpha\geq 2$, avem: $h^{-1}(p^{\alpha})=(g*f^{-1})(p^{\alpha})+g(p^{\alpha-1})f^{-1}(p)+g(p^{\alpha-2})f^{-1}(p^2)=g(p^{\alpha-2})[(g(p))^2+f^{-1}(p)g(p)+f^{-1}(p^2)]=0$.

Conform Propoziţiei 5.4., $h\in\mathbf{M}^{c}$ si astfel $f=g*h$. ■

<u>TEOREMA 5.6.</u> Pentru $f\in\mathbf{M}$, următoarele condiţii sunt echivalente:

(1) Există $g, h\in\mathbf{M}^{c}$ a.î. $f=g*h$;

(2) Există $F\in\mathbf{M}$ a.î. pentru orice m, n : $f(mn)=\sum_{d\mid(m,n)}f(m/d)f(n/d)F(d)$**.**

(3) Există $B\in\mathbf{M}^{c}$ a.î. pentru orice m, n: $f(m)f(n)=\sum_{d\mid(m,n)}f(mn/d^2)B(d)$**.**

(4) Pentru orice p prim şi $\alpha\geq 1$: $f(p^{\alpha+1})=f(p)f(p^{\alpha})+f(p^{\alpha-1})[f(p^2)-(f(p))^2]$.

<u>Demonstraţie</u> Vom demonsra că (1)⇒(4), (4)⇒(1), (2)⇒(4), (4)⇒(2), adică (1)⇔(2)⇔(4), iar apoi (2)⇒(3) şi (3)⇒(4)

(1)⇒(4). Presupunem că $f=g*h$ cu $g, h\in\mathbf{M}^{c}$.

Dacă $g(p)=M$ şi $h(p)=N$, atunci $f(p)=M+N$ şi $f(p^2)=M^2+MN+N^2$. Dacă $\alpha\geq 1$ atunci partea dreaptă a egalităţii din (4) este egală cu :

$$(M+N)\sum_{i=0}^{\alpha}M^{i}N^{\alpha-1}-MN\sum_{i=0}^{\alpha-1}M^{i}N^{\alpha+1-i}=$$

$$=\sum_{i=0}^{\alpha}M^{i+1}N^{\varepsilon-i}+\sum_{i=0}^{\alpha}M^{i}N^{\alpha+1-i}-\sum_{i=0}^{\alpha-1}M^{i+1}N^{\alpha-1}=$$

$$=M^{\alpha+1}+\sum_{i=0}^{\alpha}M^{i}N^{\alpha+1-i}=\sum_{i=0}^{\alpha+1}M^{i}N^{\alpha+1-i}=f(p^{\alpha+1})$$

(4)⇒(1). Pentru fiecare p prim, fie M şi N soluţiile ecuaţiei:

$$X^2-f(p)X+(f(p))^2-f(p^2)=0$$ (evident M şi N sunt funcţii de p)

Fie $g, h\in\mathbf{M}^{c}$ a.î. pentru orice p prim $g(p)=M$ şi $h(p)=N$.

Atunci $f(p)=M+N=(g*h)(p)$ iar pentru $\alpha\geq 2$:

$$(g*h)(p^\alpha)=\sum_{i=0}^{\alpha} M^i N^{\alpha-1}=(M+N)\sum_{i=0}^{\alpha-1} M^i N^{\alpha-1-i}-MN\sum_{i=0}^{\alpha-2} M^i N^{\alpha-2-i}=$$

$$=f(p)f(p^{\alpha-1})+f(p^{\alpha-2})[f(p^2)-(f(p))^2]=f(p^\alpha).$$

Cum f∈**M** deducem că f=g∗h.

(2)⇒(4). Fie p un număr prim şi α≥1. Punem în ecuaţia din (2) m=p^α şi n=p. Atunci f($p^{\alpha+1}$)=f(p)f(p^α)+f($p^{\alpha-1}$)F(p). Dacă particularizăm α=1 obţinem F(p)=f(p^2)-f(p))^2.

(4)⇒(2). Dacă (mn, m′n′)=1 atunci ((m, n), (m′, n′))=1 şi (mm′, nn′) = (m, n)(m′, n′).

Astfel, pentru a proba (2) este suficient să arătăm că există f∈**M** a.î. pentru orice p prim şi α, β≥1, $f(p^{\alpha+\beta})=\sum_{i=0}^{\min(\alpha,\beta)} f(p^{\alpha-i})f(p^{\beta-i})F(p^i)$ (de fapt este cazul în care F=μB′ cu B′∈$\mathbf{M}^c$ a.î. B′(p)=f(p^2)-(f(p))^2 pentru orice p prim).

Fără a reduce din generalitate, să presupunem că β≤α şi să facem inductie după β.

Dacă β=1 totul este clar. Presupunem că β>1 şi că (2) este adevărată pentru β-1 şi orice α≥β-1.

Cum F=μB′, F(p^2)=F(p^3)=…=0 iar f ($p^{\alpha+\beta}$) =f ($p^{\alpha+1+\beta-1}$)=f ($p^{\alpha+1}$) f ($p^{\beta-2}$) F(p)=[f(p) f(p^α)-f($p^{\alpha-1}$) B′(p)] f ($p^{\beta-1}$)-f (p^α) f ($p^{\beta-2}$) B′(p) = f (p^α) [f (p) f ($p^{\beta-1}$) – - f ($p^{\beta-2}$) B′(p)]-f ($p^{\alpha-1}$) f ($p^{\beta-1}$) B′(p)=f (p^α) f (p^β) + f ($p^{\alpha-1}$) f ($p^{\beta-1}$) F(p)

(2)⇒(3). Pentru orice m, n avem:

$$\sum_{d\mid(m,n)} f(mn/d^2)\ B'(d)=$$

$$=\sum_{d\mid(m,n)}\ \sum_{D\mid(\frac{m}{d},\frac{n}{d})} f(\frac{m/d}{D})\ f(\frac{n/d}{D})\ \mu(D)\ B'(D)\ B'(d)=$$

$$=\sum_{d\mid(m,n)}\ \sum_{\substack{e\mid(m,n)\\ d\mid e}} f(m/e)\ f(n/e)\ \mu(e/d)\ B'(e)=$$

$$=\sum_{e\mid(m,n)} f(m/e)\ f(n/e)\ B'(e)\ \sum_{d\mid e}\mu(e/d)=f(m)f(n)$$

Astfel funcţia B′∈$\mathbf{M}^c$ serveşte pe post de B cerut în (3).

(3)⇒(4). Dacă p este prim şi alegem m=n=p, atunci obţinem B(p)=(f(p))^2-f(p^2), adică B=B′. Fie α≥1. Dacă alegem m=p^α şi n=p obţinem (4).■

Observaţie Funcţia f∈**A** ce satisface una din condiţiile teoremei de mai sus poartă numele de *funcţie multiplicată specială* (După cum am observat înainte σ_k este o astfel de funcţie. Pentru σ_k avem că B=ξ_k ; într-adevăr, dacă p este prim, atunci $B(p)=(\sigma_k(p))^2-\sigma_k(p^2)=(1+p^k)^2-(1+p^k+p^{2k})=p^k=\xi_k(p)$. Deci pentru orice m, n avem: $\sigma_k(mn)=\sum_{d|(m,n)}\sigma_k(m/d)\sigma_k(n/d)\mu(d)d^k$ [S.Ramanujan pentru k=0, în 1916] şi $\sigma_k(m)\sigma_k(n)=\sum_{d|(m,n)}d^k\sigma_k(mn/d^2)$. [Busche-1906].

CAPITOLUL 9:
RESTURI PĂTRATICE

§1.Generalităţi.Simbolul lui Legendre

Fie m∈ℕ, m >1 un număr natural fixat.

DEFINIŢIA 1.1. **Un număr a∈ℤ cu (m, a)=1 se zice *rest pătratic modulo m* dacă ecuaţia $x^2\equiv a\ (m)$ are soluţie.**

În caz contrar a se zice *non-rest pătratic modulo m*.

În mod evident, dacă a, b∈ℤ şi a≡b(m), atunci a este rest pătratic modulo m ⇔ b este rest pătratic modulo m.

Datorită acestei observaţii este mai comod să lucrăm în $\mathbb{Z}_p$ decât în ℤ, distincţia făcându-se în contextul în care se lucrează (notăm deseori elementele lui $\mathbb{Z}_p$ prin 0, 1,…, p-1).

Observaţii:

1. Fie p un număr prim; dacă p=2 şi a∈ℤ este impar, a=2k+1 cu k∈ℤ, atunci ecuaţia $x^2\equiv a\ (\mathrm{mod}\ 2)$ are soluţie pentru x=1 sau x=a. Deci orice număr impar este rest pătratic modulo 2.

2. Dacă p este impar (deci p≥3), atunci a∈ℤ este rest pătratic modulo p ⇔ restul împărţirii lui a la p este din $\mathbb{Z}^{*2}$ (sau $\mathbb{Z}_p^{*2}$). Aici $\mathbb{Z}^{*2}=\{x^2 \mid x\in\mathbb{Z}^*\}$ şi analog $\mathbb{Z}_p^{*2}$.

Într-adevăr, dacă a∈ℤ este rest pătratic modulo p, atunci există x∈ℤ a.î. $x^2\equiv a(p)$ ⇔există c∈ℤ a.î. $a-x^2=cp$ ⇔ $a=cp+x^2$.

Reciproc, dacă putem scrie $a=cp+r^2$, cu $0\le r^2<p$, atunci ecuaţia $x^2\equiv a\ (p)$ are soluţie pe x=r.

În cele ce urmează prin p vom desemna un număr prim impar ($p\geq 3$).

Cum $\frac{p-1}{2}\in\mathbb{N}$, funcția $\sigma:\mathbb{Z}_p^*\to\mathbb{Z}_p^*$, $\sigma(x)=x^{\frac{p-1}{2}}$ este morfism de grupuri multiplicative. Cum $\sigma(x)^2=x^{p-1}=1$ deducem că $\sigma(x)=\pm 1$ (în $\mathbb{Z}_p^*$) (deci $\sigma:\mathbb{Z}_p^*\to\{\pm 1\}$)

Mai mult :

1. $\sigma(x)=-1$ pentru un anumit $x\in\mathbb{Z}_p^*$ (căci în caz contrar polinomul $X^{(p-1)/2}-1$ ar avea mai multe rădăcini decât gradul său).

2. Dacă $x=t^2\in\mathbb{Z}_p^{*2}$, atunci $\sigma(x)=x^{(p-1)/2}=(t^2)^{(p-1)/2}=t^{p-1}=1$ (reamintim că am notat $\mathbb{Z}_p^{*2}=\{a^2|a\in\mathbb{Z}_p^*\}$).

Din cele de mai sus deducem că: $\mathbb{Z}_p^{*2}\subseteq\ker\sigma\subseteq\mathbb{Z}_p^*$ și cum $[\mathbb{Z}_p^*:\ker\sigma]=|\mathbb{Z}_p^*/\ker\sigma|=|\mathrm{Im}\,\sigma|=2$ deducem că $2=[\mathbb{Z}_p^*:\mathbb{Z}_p^{*2}]=[\mathbb{Z}_p^*:\ker\sigma][\ker\sigma:\mathbb{Z}_p^{*2}]$, de unde $[\ker\sigma:\mathbb{Z}_p^{*2}]=1$, adică $\ker\sigma=\mathbb{Z}_p^{*2}$.

<u>DEFINIȚIA 1.2</u>. Numim *<u>simbolul lui Legendre</u>* morfismul de grupuri multiplicative $\sigma\overset{not}{=}\left(\frac{-}{p}\right):\mathbb{Z}_p^*\to\{\pm 1\}$.

Deci $\left(\frac{a}{p}\right)=\sigma(a)=a^{(p-1)/2}$, pentru orice $a\in\mathbb{Z}_p^*$ (evident $p\nmid a$, căci $a\in\mathbb{Z}_p^*$).

Mai mult :

(1) $$\left(\frac{a}{p}\right)=\begin{cases}1 & daca\ a\ este\ rest\ patratic\ \mathrm{mod}\,ulo\ p\\ -1 & daca\ a\ nu\ este\ rest\ patratic\ \mathrm{mod}\,ulo\ p\end{cases}$$

În particular:

(2) $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$ și $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ pentru orice $a, b\in\mathbb{Z}_p^*$.

<u>LEMA 1.3.(Gauss)</u> Fie $\mathbb{Z}_p^*=X\cup Y$, unde $X=\{\hat{1},\ \hat{2},\ ...,\ \widehat{\frac{p-1}{2}}\}$ iar $Y=\{\widehat{\frac{p+1}{2}},...,\ \widehat{p-1}\}$ (evident $X\cap Y=\varnothing$).

Pentru $\hat{a} \in \mathbb{Z}_p^*$, **fie** $\hat{a}\,X=\{\hat{a}\cdot\hat{x} \mid x\in X\}$. **Atunci** $\left(\frac{a}{p}\right)=(-1)^g$, **unde** $g=|\hat{a}\,X\cap Y|$

Demonstraţie Să observăm la început că funcţia $m_a:\mathbb{Z}_p^*\to\mathbb{Z}_p^*$, $m_a(\hat{x})=a\hat{x}$, pentru $x\in\mathbb{Z}_p^*$, permută doar elementele lui $\mathbb{Z}_p^*$.

Astfel, dacă notăm

$X'=\hat{a}X\cap X=\{\hat{x}_1,...,\hat{x}_k\}$, $Y'=\hat{a}X\cap Y=\{\hat{y}_1,...,\hat{y}_g\}$,atunci $X'\cup Y'=aX$, iar $X'\cap Y'=\varnothing$, deci $g+k=(p-1)/2$.

Fie $Z=\{\hat{x}_1,...,\hat{x}_k,\hat{p-y}_1,...,\hat{p-y}_g\}\subseteq X$. Să observăm că elementele lui Z sunt distincte două câte două (ca elemente ale lui $\mathbb{Z}_p$).

Într-adevăr, dacă există i, j a.î. $x_i=p-y_j\Rightarrow x_i+y_j=0$ (în $\mathbb{Z}_p$). Însă $x_i=ar$, $y_j=as$ cu $1\le r, s\le(p-1)/2$, deci $a(r+s)=0$ şi cum $a\neq0$ deducem că $r+s=0$ ceea ce este imposibil deoarece $2\le r+s<p-1$. Deducem atunci că $Z=X$ (căci $Z\subseteq X$ şi $|Z|=|X|$), deci (în $\mathbb{Z}_p$) avem : $1\cdot2\dots\frac{p-1}{2}=x_1\dots x_k(p-y_1)\dots(p-y_g)=(-1)^g x_1\dots x_k y_1\dots y_g=$ $=(-1)^g a\,2a\dots\frac{p-1}{2}a$ (căci $X'\cup Y'=aX$!) $=(-1)^g a^{(p-1)/2}\cdot1\cdot2\dots\frac{p-1}{2}$, de unde $(-1)^g a^{(p-1)/2}=1$, de unde :

$$(-1)^g=a^{(p-1)/2}=\left(\frac{a}{p}\right).\ \blacksquare$$

COROLAR 1.4. **Pentru orice număr prim p impar (deci p≥3) avem:**

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

Demonstraţie Să observăm la început că $(p^2-1)/8\in\mathbb{N}$. Într-adevăr, dacă $p=8m+r$ (r=1, 3, 5, 7), atunci : $\frac{p^2-1}{8}=\frac{(8m+r)^2-1}{8}=2n+\frac{r^2-1}{8}$ $(n\in\mathbb{N})$ şi cum $(r^2-1)/8\in\mathbb{N}$ pentru r =1, 3, 5, 7 totul este clar.

Pentru $1\le x<(p-1)/2$, $2x<p-1$. Atunci g din lema 1.3. a lui Gauss (pentru a=2) este numărul elementelor de forma 2x, $1\le x<(p-1)/2$ ce verifică condiţia $2x\in Y\Leftrightarrow x>(p-1)/4$, adică : $g=\frac{p-1}{2}-[\frac{p-1}{4}]$ .Considerând $p=8m+r$, (r =1, 3, 5, 7), avem:

$$g = 4m + \frac{r-1}{2} - [2m + \frac{r-1}{4}] = 4m + \frac{r-1}{2} - 2m - [\frac{r-1}{4}] = 2m + \frac{r-1}{2} - [\frac{r-1}{4}],$$

care ne duce la concluzia că g este par pentru r=1, 7 şi impar pentru r=3, 5, adică g şi $(p^2-1)/8$ au aceeaşi paritate, de unde $\left(\frac{2}{p}\right) = (-1)^g = (-1)^{(p^2-1)/8}$ ■

§2. Legea reciprocității pătratice

În vederea demonstrării legii reciprocității pătratice, să stabilim la început următoarea lemă:

LEMA 2.1. Dacă p şi q sunt două numere prime impare (p, q≥3), distincte, atunci :

$$\sum_{j=1}^{(p-1)/2} \left[\frac{jq}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Demonstrație Notând $s(p,\ q) = \sum_{j=1}^{(p-1)/2} \left[\frac{jq}{p}\right]$, egalitatea din enunț devine : s(p, q)+s(q, p)=(p-1)(q-1)/4.

Este uşor de observat că pentru orice j=1, 2,…, $\frac{p-1}{2}$, $\left[\frac{jq}{p}\right]$ este numărul de numere naturale din intervalul (0, jq/p).

Deci pentru fiecare j ca mai sus, [jq/p] este numărul acelor puncte laticiale din plan situate pe dreapta x=j (delimitate strict superior de dreapta y=qx/p şi inferior de y=0)

Astfel s(p, q) reprezintă numărul punctelor laticiale din interiorul dreptunghiului OABC (deci nesituate pe conturul lui OABC !) situate sub dreapta de ecuație y=(q/p)x. (vezi Fig.1)

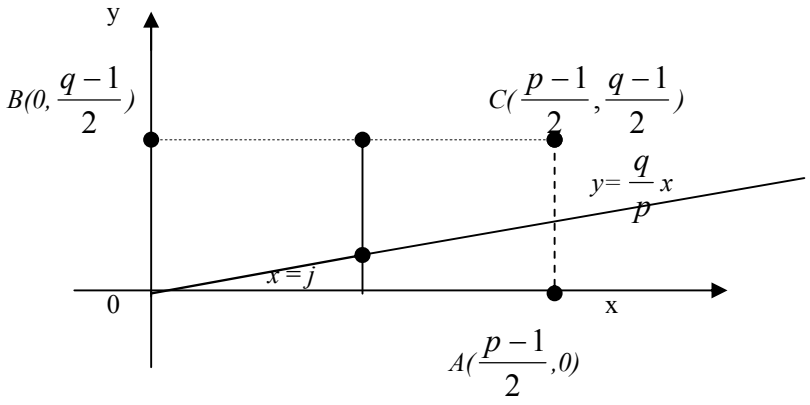


Fig. 1

Analog, s(q, p) reprezintă numărul punctelor laticiale din interiorul dreptunghiului OABC situate deasupra dreptei de ecuatie y=(q/p)x astfel că s(p, q)+s(q, p)=numărul de puncte laticiale din interiorul dreptunghiului OABC $= \frac{p-1}{2} \cdot \frac{q-1}{2}$ şi astfel lema este probată. ■

TEOREMA 2.2. (Legea reciprocităţii pătratice) Dacă p şi q sunt două numere prime impare distincte, atunci :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Demonstraţie Revenim la notaţiile din Lema 1.3. a lui Gauss (numai că de data aceasta elementele x_i şi y_i vor fi privite ca numere întregi, deci nu ca elemente din $\mathbb{Z}_p$).

Fie $\alpha = \sum_{j=1}^{k} x_j, \quad \beta = \sum_{j=1}^{g} y_j$

Avem $\sum_{x \in X} x = 1 + 2 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8}$.

Analog ca în demonstraţia lemei lui Gauss vom avea :

$\sum_{z\in Z} z = \sum_{j=1}^{k} x_j + \sum_{j=1}^{g} (p - y_j) = \alpha - \beta + p \cdot g$ şi cum X=Z deducem că $\frac{p^2-1}{8} = \alpha - \beta + p \cdot q$

Acum, pentru j=1, 2,…, (p-1)/2, fie t_j restul împărțirii prin p a lui jq. Evident câtul este [jq/p], deci jq =[jq/p]+t_j.

Făcând j=1, 2,…, (p-1)/2 şi sumând obținem :

$$\frac{q(p^2-1)}{8} = p\ s(p,q) + \sum_{j=1}^{(p-1)/2} t_j = p\ s(p,q) + \sum_{j=1}^{k} x_j + \sum_{j=1}^{g} y_j \text{ sau}$$

$$\frac{q(p^2-1)}{8} = p\ s(p,q) + \alpha + \beta .$$

Cum $\frac{p^2-1}{8} = \alpha - \beta + p \cdot q$ deducem că

$$\frac{(q-1)(p^2-1)}{8} = p[s(p,q) - g] + 2\beta$$

Deoarece p si q sunt primi impari şi (p^2-1)/8∈ℕ, deducem că s(p, q)-g≡0(mod 2), astfel că $\left(\frac{q}{p}\right) = (-1)^g = (-1)^{s(p,q)}$. Schimbând rolul lui p cu q deducem că $\left(\frac{p}{q}\right) = (-1)^{s(q,p)}$, de unde

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s(p,q)+s(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} .\ \blacksquare$$

Aplicație. Fie p=1009 şi a=45=3^2·5. Avem:

$$\left(\frac{45}{1009}\right) = \left(\frac{3^2}{1009}\right)\left(\frac{5}{1009}\right) = \left(\frac{5}{1009}\right) = \left(\frac{1009}{5}\right)(-1)^{\frac{1009-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{1009}{5}\right) = \left(\frac{9}{5}\right) = 1 ,$$

deci 45 este rest pătratic modulo 1009 (adică 45 este pătrat în $\mathbb{Z}^*_{1009}$).

§3.Alte cazuri particulare ale teoremei lui Dirichlet

După cum am văzut, pentru orice număr prim p, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ (conform Corolarului 1.4.)

De aici deducem că 2 este rest pătratic modulo p pentru p de forma $8k\pm1$ şi non-rest pătratic pentru p de forma $8k\pm3$ (cu $k\in\mathbb{N}^*$).

PROPOZITIA 3.1. Există o infinitate de numere prime de forma 8n-1, $n\in\mathbb{N}^*$.

Demonstraţie Fie $n\in\mathbb{N}$, $n\geq2$; atunci numărul $N=2(n!)^2-1>1$ are cel putin un divizor prim p impar care nu este de forma 8k+1 (căci N este de forma 8k-1 iar dacă toţi divizorii primi impari ai lui N ar fi de forma 8k+1, atunci şi N ar trebui să fie de aceeaşi formă)

Atunci $p|N \Leftrightarrow 2(n!)^2\equiv1^2(p)$, de unde deducem că $\left(\frac{2(n!)^2}{p}\right)=1$.

Însă $\left(\frac{2(n!)^2}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{n!}{p}\right)^2=\left(\frac{2}{p}\right)$, deci $\left(\frac{2}{p}\right)=1$, adică p trebuie să fie de forma $8k\pm1$. Cum p nu este de forma 8k+1 rămâne doar că p prim trebuie să fie de forma 8k-1.

Cum $p \mid N$ deducem că $p>n$. Am probat deci că pentru orice $n\in\mathbb{N}$, $n>1$, există un prim $p>n$ de forma 8k-1.

Să presupunem acum că avem un număr finit de numere prime de forma 8k-1 şi anume $q_1, q_2,\ldots, q_t$.

Considerând numărul $n=8q_1\ldots q_t-1$ conform celor de mai înainte există un număr prim de forma 8k-1 (adică un q_i) a.î. $q_i>n$, ceea ce este absurd. ■

PROPOZITIA 3.2. Există o infinitate de numere prime de forma 8n+3, $n\in\mathbb{N}^*$.

Demonstraţie Fie $n>1$ şi $a=p_2 p_3\ldots p_n$ (unde p_n este al n-lea număr prim).

Cum a este impar, a^2 va fi de forma 8t+1 iar $N=a^2+2$ va fi de forma 8t+3. Dacă orice divizor prim al lui N este de forma $8t\pm1$, N însuşi este de această formă –absurd !. Deci N are cel puţin un divizor prim impar p ce nu este de forma 8t+3 sau 8t+5.

Cum p|N=a^2 +2 deducem că $a^2 \equiv -2\ (p)$ şi deci $\left(\frac{-2}{p}\right)=1$.

Însă , $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$.

Dacă p=8t+5 atunci $\left(\frac{-2}{p}\right)=-1$ absurd, de unde concluzia că p este de forma 8t+3. Însă din p|a^2 +2 deducem p> p_n şi astfel avem o infinitate de numere prime de forma 8t+3. ■

<u>PROPOZIŢIA 3.3</u>. Există o infinitate de numere prime de forma 8n+5, cu n∈ℕ*.

<u>Demonstraţie</u> Fie n>1 natural şi a=$p_2\ p_3 \ldots p_n$.

Cum a este impar, N=a^2 +4 este de forma 8t+5.

Dacă toţi divizorii lui N ar fi de forma 8t±1, atunci şi N ar fi de aceeaşi formă ceea ce este imposibil.

Atunci N ar trebui să aibă un divizor prim p de forma 8t+3 sau 8t+5.

Dacă p=8t+3 atunci din p|N=a^2 +4⇒ a^2≡-4(p), deci $\left(\frac{-4}{p}\right)=1$ şi astfel :

$\left(\frac{-4}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2=(-1)^{\frac{p-1}{2}}$ şi cum p=8t+3 ⇒ $\left(\frac{-4}{p}\right)=-1$ -contradicţie.

Deci p este de forma 8t+5 şi astfel din p|a^2 +4 şi a=$p_2\ p_3 \ldots p_n$ deducem că p>p_n, de unde rezultă imediat că avem o infinitate de numere prime de forma 8n+5.■

<u>Observaţie</u>: Din legea reciprocităţii pătratice deducem :

<u>COROLAR 3.4</u>. Există o infinitate de numere prime de forma 5n-1, cu n∈ℕ*.

<u>Demonstraţie</u> Fie n∈ℕ*, n>1 iar N=5(n!)^2-1.

Cum N>1 şi este impar, atunci N, cum nu este de forma 5t+1, va avea cel puţin un divizor prim p (p≠5) ce este de forma 5t+1. Evident p>n.

Cum p|N ⇒ $5(n!)^2 \equiv 1 (\text{mod } p)$, adică $\left(\frac{5}{p}\right)=1$. Atunci şi $\left(\frac{p}{5}\right)=1$.

Avem că p≠5 poate să fie de forma 5k ±1 sau 5k±2.

Dacă p=5k±2, atunci $\left(\frac{p}{5}\right)=\left(\frac{\pm 5}{5}\right)=\left(\frac{\pm 1}{5}\right)\left(\frac{2}{p}\right)$ şi cum $\left(\frac{\pm 1}{5}\right)=1$, $\left(\frac{2}{p}\right)=-1$, deducem că $\left(\frac{p}{5}\right)=-1$ -contradicție.

Cum am văzut că p nu poate fi de forma 5k+1 deducem că p trebuie să fie de formă 5k-1.

De aici corolarul rezultă imediat. ■

Observaţie Din demonstrația Corolarului 3.3. deducem că numărul prim p este de forma p=5k-1 ($k\in\mathbb{N}$). Evident k=2t, deci p=10t-1.

De aici rezultă:

COROLAR 3.5. Există o infinitate de numere prime de forma 10n-1, $n\in\mathbb{N}^*$. ■

CAPITOLUL 10:
FRACŢII CONTINUE

§1.Mulţimea numerelor iraţionale I

Complementara în $\mathbb{R}$ a lui $\mathbb{Q}$ o vom numi *mulţimea numerelor iraţionale* şi o vom nota cu **I** (deci $\mathbf{I}=\mathbb{R}\setminus\mathbb{Q}$). (vezi Definiția 2.6. de la Capitolul 4).

Să demonstrăm de exemplu că $\sqrt{2}\in\mathbf{I}$. Dacă presupunem prin absurd că $\sqrt{2}\in\mathbb{Q}$, atunci putem scrie $\sqrt{2}=m/n$, cu m, $n\in\mathbb{N}^*$ şi (m, n)=1. Deducem imediat că $2n^2=m^2$, adică m^2 este număr par, deci m este par, adică $m=2m_1$, cu $m_1\in\mathbb{N}^*$. Înlocuind deducem $n^2=2m_1^2$, adică $n=2n_1$, cu $n_1\in\mathbb{N}^*$.Contradicția constă în aceea că 2|m şi 2|n, contrar presupunerii că (m, n)=1.

Observaţie Mai general se demonstrează , analog, că dacă $x\in\mathbb{Q}$, $n\in\mathbb{N}^*$, $n\geq 2$ şi $x\neq d^n$, pentru orice $d\in\mathbb{Q}$, atunci $\sqrt[n]{x}\in\mathbf{I}$. Deci $\sqrt[3]{2/3}\in\mathbf{I}$, $\sqrt[5]{2^4}\in\mathbf{I}$.

Să mai demonstrăm de exemplu că $\log_2 3\in\mathbf{I}$. Într-adevăr, dacă prin absurd $\log_2 3\in\mathbb{Q}$, atunci există m, $n\in\mathbb{N}^*$ a.î. (m, n)=1 şi $\log_2 3=m/n \Leftrightarrow 2^{m/n}=3 \Leftrightarrow 2^m=3^n$, ceea ce este absurd deoarece (2, 3)=1. (mai general deducem că dacă m, $n\in\mathbb{N}^*$, (m, n)=1, atunci $\log_m n\in\mathbf{I}$).

LEMA 1.1. Dacă $x\in\mathbb{Q}$, $y\in\mathbf{I}$, atunci $x+y\in\mathbf{I}$, iar dacă $x\neq 0$ atunci $xy\in\mathbf{I}$.

Demonstraţie Am văzut că $(\mathbb{Q}, +, \cdot)$ este corp.

Notând $z=x+y$, dacă prin absurd $z\in\mathbb{Q}$, am deduce că $y=z-x\in\mathbb{Q}$, ceea ce este absurd. Analog pentru partea a doua. ■

De exemplu, $1\pm\sqrt{2}\in\mathbf{I}$, $\frac{1\pm\sqrt{5}}{2}\in\mathbf{I}$.

LEMA 1.2. Operaţiile de adunare şi înmulţire nu sunt operaţii interne pe I.

Demonstraţie Fie $x=1+\sqrt{2}$ şi $y=1-\sqrt{2}$. Cum $1\in\mathbb{Q}$ iar $\sqrt{2}\in\mathbf{I}$, conform lemei precedente deducem că $x, y\in\mathbf{I}$. Cum $x+y=2$ iar $xy=-1$, deducem că $x+y, xy\in\mathbb{Q}$. ■

Observaţie Cu toate acestea este posibil ca pentru $x, y\in\mathbf{I}$ să avem $x+y\in\mathbf{I}$ sau $xy\in\mathbf{I}$ (chiar simultan !).

De exemplu, dacă $x=\sqrt{2}$, $y=\sqrt{3}$, atunci $x, y\in\mathbf{I}$ şi $xy=\sqrt{6}\in\mathbf{I}$. Să demonstrăm că şi $x+y\in\mathbf{I}$. Fie pentru aceasta $z=x+y=\sqrt{2}+\sqrt{3}$. Dacă prin absurd $z\in\mathbb{Q}$, atunci $z^2=5+2\sqrt{6}$, de unde am deduce că $\sqrt{6}=(z^2-5)/2\in\mathbb{Q}$, absurd ! .

Să prezentăm acum câteva rezultate importante legate de numerele iraţionale.

Ştim că $e=\lim\limits_{n\to\infty}(1+\frac{1}{n})^n=\lim\limits_{n\to\infty}(1+\frac{1}{1!}+\frac{1}{2!}+...+\frac{1}{n!})$.

TEOREMA 1.3. $e\in\mathbf{I}$.

Demonstraţie Să presupunem prin absurd că $e\in\mathbb{Q}$, adică $e=a/b$, cu $a, b\in\mathbb{N}^*$. Pentru orice $k\in\mathbb{N}$, $k\geq b$, cum $b \mid k!$ deducem că numărul :

$$c=k!(\frac{a}{b}-1-\frac{1}{1!}-\frac{1}{2!}-...-\frac{1}{k!})\in\mathbb{Z}.$$

Însă

$$0<c=\frac{1}{k+1}+\frac{1}{(k+1)(k+2)}+...<\frac{1}{k+1}+\frac{1}{(k+1)^2}+...=\frac{1}{k+1}\cdot\frac{1}{1-\frac{1}{k+1}}=\frac{1}{k}<1$$

Contradicţia provine din aceea că $c\in(0, 1)$, iar mai înainte am dedus că $c\in\mathbb{Z}$. În concluzie $e\in\mathbf{I}$. ■

Pentru a demonstra că şi alte numere importante sunt iraţionale se utilizează un mic „ truc ”, considerând o anumită funcţie (de obicei polinomială).

Pentru $n\in\mathbb{N}^*$, fie $f(x)\overset{def}{=}\frac{x^n(1-x)^n}{n!}=\frac{1}{n!}\sum_{m=n}^{2n}c_m x^m$, unde $c_m\in\mathbb{Z}$, pentru $n\le m\le 2n$.

Pentru $0<x<1$ avem $0<f(x)<\frac{1}{n!}$.

Este clar că $f(0)=0$ şi că $f^{(m)}(0)=0$ dacă $m < n$ sau $m >2n$, iar dacă $n \le m \le 2n$ avem $f^{(m)}(0)=\frac{m!}{n!}c_m\in\mathbb{Z}$.

Deducem ca o concluzie că f, ca şi toate derivatele sale iau valori întregi în x=0 şi cum f(1-x)=f(x) aceeaşi concluzie este valabilă şi în x=1.

Ca un corolar la acest mic truc să demonstrăm:

<u>TEOREMA 1.4.</u> Dacă $y\in\mathbb{Q}^*$, $e^y\in$ I.

<u>Demonstraţie</u> Fie $y=h/k\in\mathbb{Q}^*$ şi să presupunem prin absurd că $e^y\in\mathbb{Q}$.

Atunci $e^h=e^{ky}\in\mathbb{Q}$ şi să punem $e^h=a/b$, cu $a, b\in\mathbb{N}^*$.

Considerăm (pentru n suficient de mare după cum se va vedea în final) funcţia : $f(x)=\frac{x^n(1-x)^n}{n!}$ şi

$F(x)\overset{def}{=}h^{2n}f(x)-h^{2n-1}f'(x)+\ldots-hf^{(2n-1)}(x)+f^{(2n)}(x)$, pentru orice $x\in\mathbb{R}$.

Ţinând cont de cele de mai sus deducem că $F(0), F(1)\in\mathbb{Z}$.

De asemenea $\left[e^{hx}F(x)\right]'=e^{hx}\left[hF(x)+F'(x)\right]=h^{2n+1}e^{hx}f(x)$, oricare ar fi $x\in\mathbb{R}$.

Deducem că : $b\int_0^1 h^{2n+1}e^{hx}f(x)\,dx=be^{hx}F(x)\Big|_0^1=aF(1)-bF(0)\in\mathbb{Z}$.

Cum însă $0<f(x)<1/n!$, deducem că $0<b\int_0^1 h^{2n+1}e^{hx}f(x)\,dx<\frac{bh^{2n}e^h}{n!}<1$ pentru n suficient de mare (căci $\frac{b(h^2e)^n}{n!}\to 0$ pentru $n\to\infty$) ceea ce e contradictoriu !.

Deci $e^y\in$ **I.** ■

Considerând o funcție f asemănătoare celei pentru care am demonstrat că $e^y \in \mathbf{I}$ pentru $y \in \mathbb{Q}^*$ putem demonstra:

TEOREMA 1.5. $\pi \in \mathbf{I}$.

Demonstrație Să demonstrăm la început că dacă $n \in \mathbb{N}$, $g \in \mathbb{Z}[X]$, atunci $f(x)=x^n g(x)$ are toate derivatele sale în 0 întregi divizibili prin n!.

Într-adevăr, orice termen al lui g(x) este de forma cx^j cu c, $j \in \mathbb{Z}$, $c \neq 0$, $j \geq 0$ iar termenul corespunzător în f(x) este cx^{j+n}. Astfel dacă vom demonstra lucrul acesta pentru un singur termen al lui f, atunci el va rezulta în general pentru f.

Pentru x=0 este usor de văzut că cx^{n+j} şi derivatele sale sunt zero, cu o singură excepție şi anume la derivata sa de ordin j+n care este egală cu c[(j+n)!] şi cum $j \geq 0$ deducem că n! | c[(j+n)!]. Să revenim acum şi să demonstrăm că $\pi \in \mathbf{I}$.

Presupunem prin absurd că $\pi = a/b \in \mathbb{Q}$ (cu a, $b \in \mathbb{N}^*$) şi să considerăm polinomul

$$f(x) = \frac{x^n (a-bx)^n}{n!} = \frac{b^n x^n (\pi - x)^n}{n!}$$ (n va fi pus în evidență ceva mai târziu).

Considerăm $g(x)=(a-bx)^n$; conform celor remarcate la început putem trage concluzia că $x^n (a-bx)^n$ şi toate derivatele sale calculate în 0 sunt întregi divizibili prin n!. Prin urmare, împărțind prin n! deducem că f(x) şi toate derivatele sale calculate în x=0 sunt întregi, deci $f^{(j)}(0) \in \mathbb{Z}$, pentru orice j=1, 2, …(cu $f^{(0)} = f$). Cum $f(\pi-x)=f(x)$ deducem că $(-1)^j f^{(j)}(\pi-x) = f^{(j)}(x)$, pentru orice $j \geq 1$. Considerând x=0 deducem că $f^{(j)}(\pi) \in \mathbb{Z}$, pentru orice j=1, 2,….

Fie $F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - f^{(6)}(x) + \ldots + (-1)^n f^{(2n)}(x)$.

Deducem că $F^{(2)}(x) = f^{(2)}(x) - f^{(4)}(x) + f^{(6)}(x) - f^{(8)}(x) + \ldots + (-1)^{n-1} f^{(2n)}(x)$ (căci $f^{(2n+2)}(x) = 0$, f fiind polinom de grad 2n).

Deducem că $F(x) + F^{(2)}(x) = f(x)$ iar de aici că $F(0), F(\pi) \in \mathbb{Z}$.

Cum $(F'(x) \sin x - F(x) \cos x)' = F''(x) \sin x + F(x) \sin x = f(x) \sin x$, deducem că : $\int_0^{\pi} f(x) \sin x = (F'(x)\sin x - F(x)\cos x)\Big|_0^{\pi} = F(\pi) - F(0) \in \mathbb{Z}$.

Vom demonstra însă că pentru n suficient de mare avem $0 < \int_0^{\pi} f(x) \sin x \, dx < 1$ şi atunci contradicția va fi clară.

Cum pentru $x\in[0,\pi]$, $f(x)<\frac{\pi^n a^n}{n!}$ deducem că $f(x)\sin x<\frac{\pi^n a^n}{n!}$ şi astfel $0<\int_0^{\pi} f(x)\sin x\,dx<\frac{\pi^n a^n}{n!}\pi<1$ pentru orice $n>n_0$ căci $\frac{(\pi a)^n}{n!}\pi\to 0$ pentru $n\to\infty$. ■

În legătură cu felul în care funcţiile trigonometrice generează numere iraţionale prezentăm:

<u>TEOREMA 1.6.</u> Fie θ un multiplu raţional de π (adică $\theta=r\cdot\pi$, cu $r\in\mathbb{Q}$). Atunci sin θ, cos θ, tg $\theta\in$I, cu excepţia cazurilor când tg θ nu este definit iar cos θ, sin $\theta\in\{0,\pm1/2,\pm1\}$, tg $\theta\in\{0,\pm1\}$.

<u>Demonstraţie</u> Pentru orice număr natural n vom proba prin inducţie matematică existenţa unui polinom $f_n\in\mathbb{Z}[X]$ de grad n cu coeficientul dominant 1 a.î. $2\cos n\theta=f_n(2\cos\theta)$, pentru orice $\theta\in\mathbb{R}$.

Cum $2\cdot\cos 2\theta=(2\cos\theta)^2-2$ deducem că $f_1(x)=x$ şi $f_2(x)=x^2-2$.

Cum $2\cdot\cos(n+1)\theta=(2\cos\theta)(2\cos n\theta)-2\cos(n-1)\theta$ deducem că $f_{n+1}(x)=xf_n(x)-f_{n-1}(x)$ si astfel prin inducţie matematică existenţa polinomului f_n este asigurată.

Fie acum $n\in\mathbb{N}^*$ a.î. $n\cdot r\in\mathbb{Z}$. Dacă $\theta=r\cdot\pi$ rezultă că $f_n(2\cos\theta)=2\cos n\theta=$ $=2\cos nr\theta=\pm2$ („+” dacă nr este par şi „-” dacă nr este impar). Astfel $2\cos\theta$ este soluţie a ecuaţiei $f_n(x)\pm2=0$.

Eliminând cazul $\cos\theta=0$, cum $2\cos\theta$ este rădăcina unei ecuaţii de forma $f_n(x)\pm2=0$ cu coeficientul dominant 1, dacă $2\cos\theta\in\mathbb{Q}$, cu necesitate $2\cdot\cos\theta\in\mathbb{Z}^*$. Cum $-1\le\cos\theta\le 1$ deducem că $2\cos\theta=\pm1,\pm2$, adică $\cos\theta\in\{\pm1,\pm1/2\}$.

Astfel, în cazul lui cos θ teorema este demonstrată .

În cazul lui sin θ, dacă θ este multiplu raţional de π, la fel este şi $\pi/2-\theta$ şi din identitatea $\sin\theta=\cos(\pi/2-\theta)$ deducem concluzia teoremei pentru sin θ.

În final din identitatea $\cos 2\theta=(1-\mathrm{tg}^2\theta)/(1+\mathrm{tg}^2\theta)$ deducem că dacă $\mathrm{tg}\theta\in\mathbb{Q}$ atunci şi $\cos 2\theta\in\mathbb{Q}$. Ţinând cont de cele stabilite în cazul lui cos θ deducem că $\cos 2\theta=0,\pm1/2,\pm1$.

Dacă $\cos 2\theta=0$, atunci $\mathrm{tg}\,\theta=\pm1$; dacă $\cos 2\theta=1$ atunci $\mathrm{tg}\,\theta=0$ iar dacă $\cos 2\theta=-1$, atunci tg θ nu este definită.

Dacă cos 2θ = ±1/2 atunci tg $\theta \in \{ \pm \sqrt{3},\ \pm 1/\sqrt{3} \}$ şi cu aceasta teorema este demonstrată. ■

TEOREMA 1.7. e nu este irațional pătratic.

Demonstrație Presupunem prin absurd că există a, b, c∈ℤ, nu toate nule, a.î. $ae^2+be+c=0$ (vezi Definiția 3.10.).

Cum e∈**I** avem a≠0 şi c≠0. Să presupunem de exemplu că a>0.
Atunci $ae + b + ce^{-1} = 0$, a>0, c≠0.

Reamintim că $\frac{1}{e} = \sum_{k\geq 0} \frac{(-1)^n}{k!}$.

Să notăm $B_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$; avem că $B_n \in \mathbb{Z}$, n=1, 2, … şi să mai considerăm şi

$$b_n = n! \sum_{k\geq n+1} \frac{(-1)^{n-k-1}}{k!} = \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} - \ldots$$

Avem că $0 < \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} < b_n < \frac{1}{n+1}$.

Astfel: $n!(ae + b + ce^{-1}) = (aA_n + bn! + cB_n) + (aa_n + (-1)^{n+1} cb_n) = C_n + c_n = 0$ (⋆)
unde $C_n = (aA_n + bn! + cB_n) \in \mathbb{Z}$ şi $c_n = aa_n + (-1)^{n+1} cb_n$, n≥1 .

Alegem acum n a.î. $n \geq 2a + |c|$ şi $(-1)^{n+1} c > 0$.

Cum a>0 avem că $0 < c_n = aa_n + (-1)^{n+1} cb_n < \frac{2a + |c|}{n+1} < 1$, ceea ce contrazice (⋆). ■

§2.Numere algebrice şi numere transcendente

DEFINIȚIA 2.1. Un număr α∈ℂ se zice *algebric* dacă există f∈ℚ[X], f≠0 a.î. f(α)=0. Un număr ce nu este algebric se zice *transcendent.*

Evident, orice număr rațional este algebric .

De asemenea, $i=\sqrt{-1}$ este algebric (fiind soluție a ecuației algebrice $X^2+1=0$).

Dacă un număr algebric α este rădăcina unui polinom nenul $f \in \mathbb{Q}[X]$ de grad minim, vom spune că α este de grad n (astfel un număr raţional este algebric de grad 1).

TEOREMA 2.2. Mulţimea numerelor algebrice este numărabilă.

Demonstraţie Cunoaştem că orice număr algebric α este soluţie a unei ecuaţii: $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0 = 0$ cu $a_i \in \mathbb{Z}$, $0 \le i \le n$, nu toţi nuli. Dacă notăm $N = n + |a_0| + \ldots + |a_n|$, atunci cu necesitate $N \ge 1$. Pentru fiecare n fixat există numai un număr finit de ecuaţii algebrice de forma celei de mai sus şi fiecare dintre acestea au numai un număr finit de soluţii.

În concluzie, numărul numerelor algebrice corespunzătoare lui N este finit; fie E_N mulţimea acestora. Cum mulţimea E a numerelor algebrice este o submulţime a mulţimii $\bigcup_{N \ge 2} E_N$ (care este numărabilă), deducem că E este numărabilă.■

Ca un corolar deducem imediat:

TEOREMA 2.3. Atât în $\mathbb{C}$ cât şi în $\mathbb{R}$, mulţimea numerelor transcendente este numărabilă.

TEOREMA 2.4. (Criteriul lui Liouville) Fie $f \in \mathbb{Z}[X]$ ireductibil de gradul $r \ge 2$, $\alpha \in \mathbb{R}$ o rădăcină a lui f şi p, $q \in \mathbb{Z}$ cu $q \in \mathbb{N}^*$. Atunci există un număr real $c > 0$ ce nu depinde de p şi q a.î. $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^r}$.

Demonstraţie Fie $f = a_0 + a_1X + \ldots + a_rX^r \in \mathbb{Z}[X]$ polinomul minimal al lui α . Putem presupune că $\left|\alpha - \frac{p}{q}\right| < 1$ (căci în caz contrar putem lua $c = 1$).

Atunci fie $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ toate rădăcinile lui f (conform Teoremei 2.3. acestea sunt în $\mathbb{C}$).

Avem :

$$\left|f\left(\frac{p}{q}\right)\right| = |a_r| \left|\alpha - \frac{p}{q}\right| \left|\prod_{i=2}^{r}\left(\alpha_i - \frac{p}{q}\right)\right| \le |a_r| \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{r}\left(|\alpha| + 1 + |\alpha_i|\right) = c' \left|\alpha - \frac{p}{q}\right|$$

unde $c' > 0$ este o constantă ce nu depinde de p şi q.

Pe de altă parte, $\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^r}$ şi astfel teorema este demonstrată. ■

Observaţie Criteriul precedent exprimă faptul că, într-un anumit mod, numerele algebrice nu pot fi suficient de bine aproximate prin numere raţionale.

COROLARUL 2.5. Numărul $\alpha = \sum_{n \geq 1} \frac{1}{3^{n!}}$ este transcendent (adică nu este algebric).

Demonstraţie Să arătăm la început că $\alpha \notin \mathbb{Q}$. Dacă prin absurd $\alpha = \frac{p}{q} \in \mathbb{Q}$ cu p, q∈ℕ*, atunci considerând un număr întreg k≥1 şi înmulţind relaţia $\alpha = \frac{p}{q}$ cu $3^{k!}q$ obţinem o relaţie de forma $a=b+q\sum_{n \geq k+1} \frac{1}{3^{n!-k!}}$ cu a, b ∈ℤ. Este suficient să arătăm că numărul $d = q\sum_{n \geq k+1} 3^{-n!+k!} \notin \mathbb{Z}$ pentru k suficient de mare. Un astfel de k există deoarece d este restul unei serii convergente ; deci $\alpha \notin \mathbb{Z}$.

Să presupunem acum că α ar fi algebric. Atunci polinomul minimal al său ar avea gradul r ≥2. Fie c constanta din Criteriul lui Liouville de mai sus asociată lui α. Considerăm k≥1 întreg şi $s = \sum_{n=1}^{k} 3^{-n!}$. Atunci avem $|\alpha - s| = \sum_{n \geq k+1} 3^{-n!}$. Luând k suficient de mare, obţinem inegalitatea $3^{r\,k!} \sum_{n \geq k+1} 3^{-n!} < c$ ceea ce contrazice Criteriul lui Liouville, absurd!. ■

În continuare vom mai prezenta si alte exemple.

TEOREMA 2.6. (Hermite) Numărul e este transcendent.

Demonstraţie Fie $I(t) = \int_0^t e^{t-x} f(x)\, dx$, definită pentru t≥0, unde f∈ℝ[X] este un polinom de grad m.

Integrând prin părți obținem: $I(t) = e^t \sum_{j=1}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t)$.

Se observă că dacă prin $\bar{f}$ desemnăm polinomul ce se obține înlocuind coeficienții lui f cu valorile lor absolute, atunci :

$$\left| I(t) \right| \le \int_0^t \left| e^{t-x} f(x) \right| dx \le te^t \bar{f}(t).$$

Să presupunem acum prin absurd că e este algebric. Atunci există $a_0,a_1,\ldots,a_n \in \mathbb{Z}$ cu $a_0 \neq 0$ a.î. $a_0+a_1e+\ldots+a_ne^n=0$.

Fie $f(x)=x^{p-1}(x-1)^p\ldots(x-n)^p$ unde p este un număr prim (care va fi convenabil ales).

Atunci gradul lui f este (n+1)p-1.

Fie $J=a_0I(0) + a_1I(1) +\ldots+a_nI(n)$. Avem $J = -\sum_{j=0}^{m}\sum_{k=0}^{n} a_k f^{(j)}(k)$.

Însă pentru $1\le k \le n$ avem $f^{(j)}(k) = 0$ pentru $j<p$ şi $f^{(j)}(k) = C_p^j\, p!\, g^{(j-p)}(k)$ pentru $j\ge p$, unde $g(x) = f(x)/(x-k)^p$.

Atunci pentru orice j, $f^{(j)}(k)$ este un întreg divizibil prin p!.

Mai mult, avem că $f^{(j)}(0)=0$, pentru $j<p-1$ şi $f^{(j)}(0) = C_{p-1}^j (p-1)!\cdot h^{(j-p+1)}(0)$ pentru $j\ge p-1$, unde $h(x)=f(x)/x^{p-1}$. Evident $h^{(j)}(0)$ este un număr întreg divizibil prin p pentru $j>0$ şi $h(0)=(-1)^{np}(n!)^p$. Atunci pentru $j\neq p-1$, $f^{(j)}(0)$ este un întreg divizibil prin p! şi $f^{(p-1)}(0)$ este întreg divizibil prin (p-1)!, însă nu prin p pentru $p>n$. Rezultă că J este un întreg nenul divizibil prin (p-1)!, deci $|J| \ge (p-1)!$.

Pe de altă parte, ținând cont de faptul că $\bar{f}(k)\le(2n)^m$ şi $m\le 2np$ deducem că $|J| \le |a_1|e\bar{f}(1)+\ldots+|a_n|ne^n\bar{f}(n) \le e^p$ pentru un anumit c ce nu depinde de p.

Alegând p prim suficient de mare (a.î. $(p-1)!>c^p$) ajungem la o contradicție evidentă, de unde rezultă că presupunerea că e este algebric este falsă, rezultând deci că e nu este algebric, adică este transcendent. ■

COROLAR 2.7. $e\in I$.

Observație Deşi iraționalitatea lui e rezultă din aceea că e este transcendent trebuie reținută şi demonstrația precedentă pentru faptul că e este irațional, fie şi numai pentru frumusețea metodei folosite.

TEOREMA 2.8. (Lindemann) π este transcendent.

Demonstrație Să stabilim la început așa- zisa „identitate a lui Hermite":

Fie $f\in\mathbb{R}[X]$ de grad n și $F(x)=f(x)+f'(x)+\ldots+f^{(n)}(x)$.

Atunci $e^x\int_0^x f(t)e^{-t}dt = F(0)e^x - F(x)$, pentru orice $x\in\mathbb{R}$.

Într-adevăr, integrând prin părți obținem relația:

$$\int_0^x f(t)e^{-t}dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t}dt$$

Repetând de n+1 ori integrarea prin părți obținem egalitatea:

$$\int_0^x f(t)e^{-t}dt = F(0) - F(x)e^{-x}$$

din care rezultă acum identitatea lui Hermite.

Să revenim acum la demonstrarea transcendenței lui π.

Pe lângă identitatea lui Hermite vom mai folosi și ecuatia $e^{\pi i}+1=0$.

Să presupunem prin absurd că π este algebric. Atunci $\gamma=\pi i$ este de asemenea algebric; fie n=gradul lui γ și $\gamma=\gamma_1, \gamma_2\ldots\gamma_n$ conjugații lui γ.

Cum $e^{\gamma}+1=0$, avem $\prod_{i=1}^{n}(1+e^{\gamma_i}) = 0$ de unde deducem că :

$$\prod_{i=1}^{n}(1+e^{\gamma_i}) = \sum_{\varepsilon_1=0}^{1}\ldots\sum_{\varepsilon_n=0}^{1} e^{\varepsilon_1\gamma_1+\ldots+\varepsilon_k\gamma_k} = 0 \qquad (1)$$

Presupunem că în relația de mai sus sunt exact m exponenți nenuli și $a=2^n$-m care sunt zero ($a\geq 1$). Atunci, dacă $\alpha_1, \ldots, \alpha_m$ sunt exponenții nenuli putem pune relația (1) de mai sus sub forma $a + e^{\alpha_1} + \ldots + e^{\alpha_m} = 0$, $a\geq 1$. (2)

Vom arăta că numerele $\alpha_1,\ldots, \alpha_m$ formează mulțimea rădăcinilor unui polinom $\psi\in\mathbb{Z}[X]$ de grad m.

Pentru aceasta să observăm că polinomul:

$$\varphi(x) = \prod_{\varepsilon_1=0}^{1}\ldots\prod_{\varepsilon_n=0}^{1}[x-(\varepsilon_1\gamma_1+\ldots+\varepsilon_n\gamma_n)]$$

considerat ca polinom în $\gamma_1,\ldots, \gamma_n$ cu coeficienți în $\mathbb{Z}[X]$ este simetric în $\gamma_1,\ldots, \gamma_n$, deci $\varphi(x)\in\mathbb{Q}[X]$.

Atunci rădăcinile polinomului $\varphi(x)$ (de grad 2^n) sunt $\alpha_1,\ldots\alpha_m$ și 0 (cu multiplicitate a).

Deci polinomul $x^{-a}\varphi(x)\in\mathbb{Q}[X]$ (de grad m) are drept rădăcini pe $\alpha_1,\ldots,\alpha_m$.

Dacă $r\in\mathbb{N}$ este c.m.m.m.c al numitorilor coeficienților acestui polinom atunci $\psi(x)=(\gamma/x^a)\varphi(x)=b_mx^m+\ \ldots+b_1x+b_0\in\mathbb{Z}[X]$ $(b_m>0,\ b_0\neq 0)$ are exact rădăcinile $\alpha_1,\ldots,\ \alpha_m$.

În identitatea lui Hermite vom considera succesiv $x=\alpha_1,\ldots,\ \alpha_m$.

Dacă adunăm şi ținem cont de (2) obținem :

$$-aF(0)-\sum_{k=1}^{m}F(\alpha_k)=\sum_{k=1}^{m}e^{\alpha_k}\int_0^{\alpha_k}f(t)e^{-t}dt \qquad (3)$$

De aici demonstrația transcendenței lui π merge ca şi în cazul transcendenței lui e.

Pentru aceasta în (3) vom considera:

$$f(x)=\frac{1}{(n-1)!}b_m^{mn-1}x^{n-1}\psi^n(x)=\frac{1}{(n-1)!}b_m^{(m+1)n-1}x^{n-1}(x-\alpha_1)^n\ldots(x-\alpha_m)^n \quad (4)$$

unde n este un număr natural ce va fi ales suficient de mare. Vom demonstra că alegând pe f ca mai sus, din (3) vom ajunge la o contradicție.

Obținem imediat relațiile:

$$\begin{cases} f^{(l)}(0)=0,\ l=0,\ 1,\ldots,\ n-2 \\ f^{(n-1)}(0)=b_m^{mn-1}b_0^n \\ F(0)=\sum_{l=n-1}^{(m+1)n-1}f^{(l)}(0)=b_m^{mn-1}b_0^n+nA \quad (A\in\mathbb{Z}) \end{cases} \qquad (5)$$

Cum α_k este o rădăcină a lui f(x) de multiplicitate n obținem că $f^{(l)}(\alpha_k)=0$, $l=0,\ 1,\ldots,n-1,\ k=1,\ 2,\ldots,\ m$. (6)

Analog ca în cazul lui e derivata de ordin l a lui $x^{n-1}\psi^n(x)$ are coeficienți divizibili prin n!. Deci pentru l > n coeficienții lui $f^{(l)}(x)$ sunt întregi şi divizibili prin $b_m^{mn-1}n$.

Atunci din (6) deducem că

$$F(\alpha_k)=\sum_{l=n-1}^{(m+1)n-1}f^{(l)}(\alpha_k)=nb_m^{mn-1}\Phi(\alpha_k)\ \ (7),\ k=1,\ldots,m \text{ cu } \Phi(z)\in\mathbb{Z}[z].$$

Numerele $\beta_k=b_m\alpha_k$, $k=1,\ldots,m$ sunt întregi algebrici ce formează mulțimea rădăcinilor unui polinom de grad m din $\mathbb{Z}[X]$ cu coeficientul dominant 1.

Mai mult, $b_m^{mn-1}\Phi(\alpha_k)=H(\beta_k)$, $H\in\mathbb{Z}[X]$.

Atunci $\sum_{k=1}^{m}b_m^{mn-1}\Phi(\alpha_k)=\sum_{k=1}^{m}H(\beta_k)=B$, $B\in\mathbb{Z}$. (8)

Din (5), (7), (8) deducem că :

$$aF(0)+\sum_{k=1}^{m}F(\alpha_k)=ab_0b_m^{mn-1}+n(aA+B) \qquad (9)$$

Fie acum $n\in\mathbb{N}^*$ a.î. $(n, b_0b_m)=1$ şi $n>1$. Membrul drept al lui (9) este un întreg nedivizibil cu n şi deci nenul, de unde :

$$\left|\ aF(0)+\sum_{k=1}^{m}F(\alpha_k)\ \right|\geq 1\,. \qquad (10)$$

Să căutăm acum o majorare a membrului drept din (3).

Să presupunem că toate punnctele $\alpha_1,\ldots,\alpha_m$ sunt conținute în cercul $|x|\leq R$ şi să notăm $\max\limits_{|x|\leq R}\left|b_m^m\psi(x)\right|=c$, cu c nedepinzând de n.

Atunci $\max\limits_{|x|\leq R}\left|f(x)\right|\leq\dfrac{R^{n-1}c^n}{(n-1)!}$.

Există deci n_0 a.î. pentru orice $n\geq n_0$ ce satisface (10) să avem inegalitatea:

$$\left|\sum_{k=1}^{m}e^{\alpha_k}\int_0^{\alpha_k}f(x)e^{-x}dx\right|\leq\sum_{k=1}^{m}\left|\int_0^{\alpha_k}\left|f(x)\right|\cdot e^{\alpha_k-x}dx\right|\leq\frac{R^{n-1}e^R}{(n-1)!}c^n\sum_{k=1}^{m}\left|\int_0^{\alpha_k}dx\right|\leq me^R\,\frac{(Rc)^n}{(n-1)!}<$$

<1 (11)

Din (10), (11) şi (3) deducem că $1<1$ -absurd! . ■

§3. Fracţii continue

Vrând să construiască un planetariu cu roți dințate, Cristian Huyghens (matematician, fizician şi astronom, 1629-1695) a avut de rezolvat problema : care raport între numărul de dinți a doua roți care se angrenează (egal cu raportul duratelor lor de rotație) este mai apropiat de raportul α dintre duratele de rotație ale planetelor respective. Din motive tehnice, numărul de dinți de pe o roată nu putea să fie prea mare.

O problemă similară a apărut la alcătuirea calendarului: Ce numar p de ani bisecți (de 366 zile) trebuie pus într-un ciclu de q ani pentru ca durata medie

a anului calendaristic, $A_c = \frac{q \cdot 365 + p}{q} = (365 + \frac{p}{q})$ zile, să fie cât mai aproape de durata reală A=365,24219878…..zile ?

Calendarul iulian a ales q=4, p=1. Calendarul gregorian, după care trăim introdus la sfârşitul secolului XVI, l-a aproximat mai bine pe A, alegând q=400 şi p=97 ; anii bisecți sunt acei multipli de 4 care nu sunt multipli de 100, excepție facând multiplii de 400. Anul nostru calendaristic durează deci 365+97/400= =365,2425 zile. Alte alegeri, ca p=8, q=33, sau p=31, q=128, ar fi dus la 365,24(24) sau 365,24218…, dar nu era comod să avem un ciclu de 33 sau 128 de ani.

Asemenea probleme de aproximare cu numere raționale apar în numeroase domenii. O soluție este dată de *fracțiile continue*. După cum vom vedea, fracțiile continue pot fi folosite cu succes şi la rezolvarea unor probleme care, cel putin aparent, nu au legatură cu aproximarea numerelor.

Fie $\alpha \in \mathbb{Q}$. Atunci putem scrie $\alpha = \frac{p}{q}$, cu $p \in \mathbb{Z}$ şi $q \in \mathbb{N}^*$.

Făcând mai multe împărțiri cu rest găsim că pentru un anumit $k \in \mathbb{N}$ avem:

$p = a_0 q + q_1 \quad , 0 < q_1 < q$
$q = a_1 q_1 + q_2 \quad , 0 < q_2 < q_1$
$q_1 = a_2 q_2 + q_3 \quad , 0 < q_3 < q_2$

$q_{k-2} = a_{k-1} q_{k-1} + q_k \quad , 0 < q_k < q_{k-1}$

$q_{k-1} = a_k q_k$, unde $a_0 \in \mathbb{Z}$ iar $a_1, \ldots, a_k \in \mathbb{N}^*$. Conform algoritmului lui Euclid, ultimul rest nenul $q_k$este cel mai mare divizor comun al lui p şi q.

Să observăm că numerele a_0, a_1,…depind numai de α, nu şi de reprezentarea p/q: $a_0 = [\alpha]$, $a_1 = \left[\frac{q}{q_1}\right] = \left[\frac{1}{\alpha - a_0}\right]$, etc.

Cunoscând câturile a_0, a_1,…, a_n putem scrie:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}$$

Convenim să scriem asemenea fracții etajate sub forma :

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + - - - + \frac{1|}{|a_k} \qquad (1)$$

În fracția de mai sus, $a_0 \in \mathbb{Z}$ iar $a_1,\ldots, a_k \in \mathbb{N}^*$.

Scrierea lui α sub forma (1) nu mai este aşa de simplă dacă α este irațional ;

Procedând analog ca mai sus obținem $a_0=[\alpha]\in\mathbb{Z}$. Evident $\alpha_1= \dfrac{1}{\alpha - a_0} > 1$ şi din nou dacă $a_1=[\alpha_1]\in\mathbb{N}^*$ atunci $\alpha_2= \dfrac{1}{\alpha_1 - a_1} > 1$.

Putem scrie că $\alpha = a_0 + \dfrac{1|}{|a_1} + \dfrac{1|}{|a_2}$. Continuând procedeul obținem scrieri intermediare de forma :

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_n} + \frac{1|}{|\alpha_{n+1}} \qquad (2)$$

Să observăm că procesul de scriere a lui α sub forma (2) poate continua atâta timp cât $\alpha_{n+1}\notin\mathbb{N}$. După cum am văzut, dacă $\alpha\in\mathbb{Q}$, pentru un anumit $k\in\mathbb{N}$, $\alpha_k\in\mathbb{N}$.

Dacă însă $\alpha\notin\mathbb{Q}$, acest proces se poate continua oricât de mult, deoarece fiecare $\alpha_k\notin\mathbb{Q}$. Se obține astfel o fracție etajată infinită:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots. + \frac{1|}{|a_n} + \ldots \qquad (3)$$

Semnul egal de mai sus este pus convențional : nu ştim deocamdată ce reprezintă membrul drept. Să comprimăm şi mai mult scrierea fracțiilor etajate (1), (2), (3), notându-le $[a_0;a_1, a_2,\ldots,a_n]$ pentru (1), $[a_0;a_1, a_2,\ldots,a_n,\alpha_{n+1}]$ pentru (2), şi $[a_0;a_1, a_2,\ldots]$ pentru (3).

Vom prezenta în continuare câteva proprietăți ale fracțiilor continue.

Pentru o fracție continuă $[a_0;a_1, a_2,\ldots,a_n,\ldots]$ (unde $a_0\in\mathbb{Z}$ iar $a_n\in\mathbb{N}^*$ pentru $n\geq 1$) să notăm :

$$\pi_n = \frac{p_n}{q_n} = [a_0;a_1, a_2,\ldots,a_n]$$

Numerele π_n sunt, evident, raționale şi se numesc <u>*redusele*</u> fracției continue.

<u>*Observație*</u> Fracția continuă $[a_0;a_1, a_2,\ldots,a_m,1]$ se poate scrie mai scurt $[a_0;a_1, a_2,\ldots,a_m+1]$. Cu convenția $a_k\geq 2$, scrierea $[a_0;a_1, a_2,\ldots,a_k]$ a numerelor raționale neîntregi este unică.

Fie $\frac{p}{q}=[a_0;a_1,\ a_2,\ldots,a_n]$ şi $\frac{p'}{q'}=[a_1;a_2,\ a_3,\ldots,a_n]$. Se vede că legătura dintre cele două numere este $\frac{p}{q}=a_0+\frac{p'}{q'}$. Dacă $\frac{p'}{q'}$ este o fracţie ireductibilă, atunci şi $\frac{p'a_0+q'}{p'}$ este ireductibilă, deci putem afirma că, dacă şi p/q este o fracţie ireductibilă, atunci $p=p'a_0+q$ şi $q=p'$. (4)

Această observaţie arată că maniera naturală de a calcula valoarea unei fracţii continue finite este exact inversul algoritmului de dezvoltare în fracţie continuă. Într-adevăr, dacă $\alpha=[a_0;a_1,\ a_2,\ldots,a_n]$, atunci $\alpha_n=a_n/1$ este o fracţie ireductibilă, deci formulele (4) permit calculul lui $\alpha_{n-1}=[a_{n-1};\alpha_n]$, apoi al lui $\alpha_{n-2}=[a_{n-2};\alpha_{n-1}]$, etc. Această modalitate de calcul poate deveni laborioasă pentru n destul de mare şi nu sugerează nimic despre calculul „valorii" unei fracţii continue infinite.

PROPOZIŢIA 3.1. Numărătorii şi numitorii reduselor verifică relaţile :

$$\mathbf{p_0=a_0,\ p_1=a_0a_1+1,\ldots,\ p_{n+1}=a_{n+1}p_n+p_{n-1}\ (n=1,2,\ldots)} \qquad \mathbf{(5)}$$
$$\mathbf{q_0=1,\ q_1=a_1,\ldots,\ q_{n+1}=a_{n+1}q_n+q_{n-1}\ (n=1,2,\ldots)}$$

Demonstraţie Avem : $\frac{p_0}{q_0}=a_0=\frac{a_0}{1};\ \frac{p_1}{q_1}=a_0+\frac{1}{a_1}=\frac{a_1a_0+1}{a_1}$ şi

$\frac{p_2}{q_2}=[a_0;a_1,a_2]=a_0+\frac{a_2}{a_2a_1+1}=\frac{a_2(a_1a_0+1)+a_0}{a_2a_1+1}=\frac{a_2p_1+p_0}{a_2q_1+q_0}$, deci relaţiile (5) se verifică pentru n=1. Presupunem că ele sunt adevărate pentru n=k-1 şi arătăm că sunt adevărate şi pentru n=k. Avem:

$$\frac{p_{k+1}}{q_{k+1}}=[a_0;a_1,\ldots\ldots,a_{k+1}]=[a_0;\alpha_1],\ \text{unde}\ \ \alpha_1=[a_1;a_2\ldots\ldots,a_{k+1}].$$

Fie $\frac{p_0'}{q_0'},\ \frac{p_1'}{q_1'},\ldots,\ \frac{p_k'}{q_k'}=\alpha_1$ redusele fracţiei α_1. Conform ipotezei de inducţie,

$$p_k'=a_{k+1}p_{k-1}'+p_{k-2}'$$
$$q_k'=a_{k+1}q_{k-1}'+q_{k-2}'$$

Pe de altă parte, din (4), avem

$$p_{k+1}=p_k'a_0+q_k'\ ,\ \ q_{k+1}=p_k'$$
$$p_k=p_{k-1}'a_0+q_{k-1}'\ ,\ q_k=p_{k-1}'$$
$$p_{k-1}=p_{k-2}'a_0+q_{k-2}'\ ,\ q_{k-1}=p_{k-2}'$$

şi deci,

$$q_{k+1} = p'_k = a_{k+1}p'_{k-1} + p'_{k-2} = a_{k+1}q_k + q_{k-1}.$$

$$p_{k+1} = a_0 p'_k + q'_k = a_0(a_{k+1}p'_{k-1} + p'_{k-2}) + a_{k+1}q'_{k-1} + q'_{k-2} =$$

$$= a_{k+1}(a_0 p'_{k-1} + q'_{k-1}) + a_0 p'_{k-2} + q'_{k-2} = a_{k+1}p_k + p_{k-1}$$

Folosind principiul inducţiei complete, propoziţia este demonstrată.■

În demonstraţie nu am folosit faptul că a_{n+1} este natural, prin urmare, aplicând relaţiile (5) cu α_{n+1} în loc de a_{n+1}, obţinem :

PROPOZIŢIA 3.2. Dacă $\alpha=[a_0 ; a_1,\ldots,a_n , \alpha_{n+1}]$ atunci

$$\alpha = \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}}. \qquad (6)$$

Relaţiile de recurenţă (5) permit calculul uşor al şirului reduselor unei fracţii continue. Este comod să punem $p_{-1}=1$ şi $q_{-1}=0$; relaţiile (5) sunt valabile atunci şi pentru n=0. Redusele se obţin completând de la stânga la dreapta tabelul:

a		a_0	a_1	a_2 . . . a_{n+1}
p	1	$p_0=a_0$	p_1	p . . . $a_{n+1}p_n+p_{n-1}$
q	0	$q_0=1$	q_1	q_2 . . . $a_{n+1}q_n+q_{n-1}$

Exemplu Fie $\alpha = \frac{\sqrt{5}+1}{2}$. Avem $a_0=1$,

$\alpha - a_0 = \frac{\sqrt{5}-1}{2}$, $\alpha_1 = \frac{2}{\sqrt{5}-1} = \frac{2(\sqrt{5}+1)}{4} = \frac{\sqrt{5}+1}{2} = \alpha$, deci $a_1=a_0$ şi $\alpha_1=\alpha$.

Este uşor de văzut că $\alpha_n=\alpha$ şi $a_n=a_0=1$, pentru fiecare n natural. Fracţia continuă ataşată este, deci [1;1,1,1…]. Să calculăm câteva reduse:

a		1	1	1	1	1	1	1	. . .
p	1	1	2	3	5	8	13	21	. . .
q	0	1	1	2	3	5	8	13	. . .

PROPOZIŢIA 3.3. Au loc relaţiile :

$$\begin{cases} q_n p_{n-1} - p_n q_{n-1} = (-1)^n, n \geq 0, & (7) \\ q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n, n \geq 1, & (8) \\ \pi_{n-1} - \pi_n = \dfrac{(-1)^n}{q_n q_{n-1}}, n \geq 1 & (9) \\ \pi_{n-2} - \pi_n = \dfrac{(-1)^{n-1}}{q_n q_{n-2}} a_n, n \geq 2, & (10) \end{cases}$$

Demonstraţie Deoarece $q_0=1$, $p_0=a_0$, $q_{-1}=0$, $p_{-1}=1$ avem $q_0 p_{-1} - p_0 q_{-1} = (-1)^0$, deci relaţia (7) este adevărată pentru n=0. Presupunem că pentru un n avem $q_n p_{n-1} - p_n q_{n-1}=(-1)^n$.

Folosind (5), avem

$q_{n+1} p_n - p_{n+1} q_n=(a_{n+1}q_n+q_{n-1})p_n - (a_{n+1}p_n + p_{n-1})q_n = -(q_n p_{n-1} - p_n q_{n-1})=(-1)^{n+1}$,

Deci am demonstrat prin inducţie relaţia (7).

Folosind întâi (5), apoi (7), avem :

$q_n p_{n-2} - p_n q_{n-2}=(a_n q_{n-1}+q_{n-2})p_{n-2} - (a_n p_{n-1} + p_{n-2})q_{n-2} = a_n(q_{n-1}p_{n-2} - p_{n-1}q_{n-2})=(-1)^{n-1}a_n$

adică relaţiile (8). Relaţiile (9) şi (10) sunt simple transcrieri ale lui (7) şi (8) şi astfel propoziţia este demonstrată.■

O consecinţă imediată a relaţiilor (9) şi (10) o constituie:

PROPOZIŢIA 3.4. Au loc inegalităţile :

$$\pi_0 < \pi_2 < \pi_4 < \ldots < \pi_5 < \pi_3 < \pi_1$$

Fie $\alpha=[a_0;a_1,\ldots,a_n, \alpha_{n+1}]$ un număr real oarecare. Folosind (6), avem

$$\alpha - \pi_n = \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(q_n\alpha_{n+1} + q_{n-1})} = \frac{(-1)^n}{q_n(q_n\alpha_{n+1} + q_{n-1})}$$

Egalitatea obţinută arată că redusele de ordin par sunt mai mici decât α, iar cele de ordin impar sunt mai mari decât α. Întrucât $\alpha_{n+1} \geq a_{n+1}$ avem şi

$$|\alpha - \pi_n| = \frac{1}{q_n(q_n\alpha_{n+1} + q_{n-1})} \leq \frac{1}{q_n(q_n a_{n+1} + q_{n-1})} = \frac{1}{q_n q_{n+1}}$$

Egalitatea din mijloc este posibilă numai dacă $a_{n+1}=\alpha_{n+1}$, deci dacă α este raţional şi $\alpha=\pi_{n+1}$. Pe de altă parte $a_{n+1}+1>\alpha_{n+1}$, deci:

$$|\alpha - \pi_n| = \frac{1}{q_n(q_n\alpha_{n+1} + q_{n-1})} > \frac{1}{q_n[q_n + (q_n a_{n+1} + q_{n-1})]} = \frac{1}{q_n(q_n + q_{n+1})}$$

Rezumând cele de mai sus, am demonstrat :

PROPOZITIA 3.5. **Dacă $\alpha=[a_0 ; a_1, \ldots, a_n, \alpha_{n+1}]$, atunci**

$$\frac{1}{q_n(q_n+q_{n+1})} < \left|\alpha - \frac{p_n}{q_n}\right| \le \frac{1}{q_n q_{n+1}}, \qquad (11)$$

egalitatea din dreapta având loc numai dacă $\alpha=\frac{p_{n+1}}{q_{n+1}}$ **.**

Suntem în măsură să dăm sens egalității din (3). Din (5) este uşor de dedus că, pentru fracții continue infinite, $q_{n+1}>q_n$, începând cu n=1 şi deci $q_n \ge n$. Pornind de la un număr irațional α, şirul $(\pi_n)_{n\ge1}$ aproximează din ce în ce mai bine numărul α. În limbajul analizei matematice, $\lim_{n\to\infty} \pi_n = \alpha$. Dacă pornim de la o fracție continuă infinită, Propoziția 3.4., împreună cu (9), garantează că şirul $(\pi_n)_{n\ge1}$ converge. Lăsăm în seama cititorului să arate că fracția continuă ataşată acestui număr este tocmai fracția continuă de la care am plecat. Ideea demonstrației este următoarea :

Dacă

$$[a_0;a_1,\ldots, a_{2n}]<\beta=[b_0;\beta_1]<[a_0;a_1,\ldots, a_{2n},a_{2n+1}],$$

atunci:

$$b_0=a_0 \text{ şi } [a_1;a_2,\ldots, a_{2n+1}]<\beta_1=[b_1;\beta_2]<[a_1;a_2,\ldots, a_{2n}]$$

Să mai demonstrăm o proprietate a reduselor:

PROPOZITIA 3.6. **Fie $a_0\ge1$, $\frac{p_{n-1}}{q_{n-1}}=[a_0;a_1,\ldots, a_{n-1}]$**

şi $\frac{p_n}{q_n}=[a_0;a_1,\ldots, a_n]$.

Atunci $[a_n;a_{n-1},\ldots, a_0]=\frac{p_n}{p_{n-1}}$ şi $[a_n;a_{n-1},\ldots, a_1]=\frac{q_n}{q_{n-1}}$.

Demonstrație Procedăm prin inducție după n.

Pentru n=1, $[a_0;a_1]=\frac{a_0a_1+1}{a_1}=\frac{p_1}{q_1}$, $\frac{a_0}{1}=\frac{p_0}{q_0}$

Avem $[a_1;a_0]=\frac{a_0a_1+1}{a_0}=\frac{p_1}{p_0}$, $a_1=\frac{q_1}{q_1}$

Presupunem afirmația adevărată pentru n. Atunci :

$$[a_{n+1};a_n,\ldots,a_1]=a_{n+1}+\frac{1}{[a_n;a_{n-1},\ldots,a_1]}=a_{n+1}+\frac{q_{n-1}}{q_n}=\frac{a_{n+1}q_n+q_{n-1}}{q_n}$$

Tot cu ajutorul lui (5), avem şi

$$[a_{n+1}; a_n, ..., a_0] = a_{n+1} + \frac{1}{[a_n; a_{n-1}, ..., a_0]} = a_{n+1} + \frac{p_{n-1}}{p_n} = \frac{p_{n+1}}{p_n}$$

ceea ce trebuia demonstrat. ■

Vom prezenta în continuare câteva chestiuni legate de aproximarea numerelor reale.

Fie α un număr real. Problema aproximării lui cu numere raționale are următoarea interpretare geometrică. În planul xOy considerăm dreapta (d) de ecuație y=αx şi rețeua de puncte ,,laticiale" din semiplanul drept, adică mulțimea punctelor de coordonate întregi (q, p) cu q>0 (vezi Fig. 2). Căutăm puncte P(q, p) pentru care p/q este aproape de α, adică puncte P(q, p) situate ,,aproape" de dreapta (d). Această apropiere o putem măsura prin abaterea $\left|\alpha - \frac{p}{q}\right|$ dintre pantele dreptelor (d) şi OP (de ecuație y=$\frac{p}{q}$ x), fie prin distanța de la P la dreapta (d) sau, ceea ce este echivalent, prin lungimea |qα-p| a segmentului PQ, unde Q este punctul de pe dreapta (d) care are abscisă cu P.

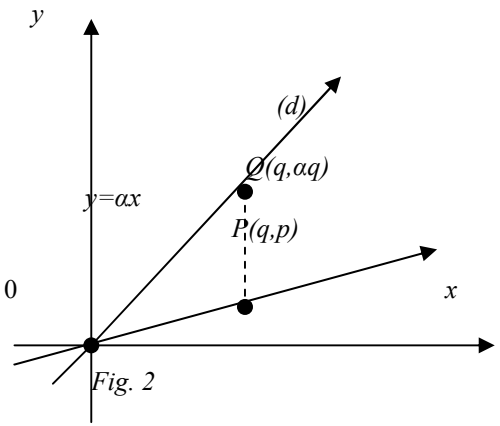


Fig. 2

Vom spune că $\frac{p}{q}$ este o „*cea mai bună aproximare de speţa întâi*“ a lui α dacă pentru orice altă fracţie $\frac{p'}{q'}$, cu $0<q'\le q$ avem $\left|\alpha-\frac{p}{q}\right|<\left|\alpha-\frac{p'}{q'}\right|$.

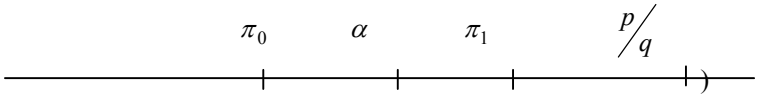
Numărul $\frac{p}{q}$ se numeşte o „*cea mai bună aproximare de speţa a doua*“ a lui α dacă $|q\alpha-p|<|q'\alpha-p'|$, pentru orice $(q',p')\neq(q,p)$ pentru care $q'\le q$. Se vede imediat că orice „cea mai bună aproximare de speţa a doua ” este şi o „cea mai bună aproximare de speţa întâi ”. Ne ocupăm aici numai de cele mai bune aproximări de speţa a doua şi le vom numi pe scurt cele mai bune aproximări.

PROPOZIŢIA 3.7. Orice cea mai bună aproximare a lui α este o redusă a fracţiei continue a lui α.

Demonstraţie Fie $\frac{p}{q}$ o cea mai bună aproximare a lui $\alpha=[a_0;a_1,\ldots,a_n,\ldots]$.

Dacă $\frac{p}{q}<a_0\ (=\pi_0)$, atunci : $|1\cdot\alpha-a_0|=\left|\alpha-\frac{p_n}{q_n}\right|\le|q\alpha-p|$, deci $\frac{p}{q}$ n-ar fi o cea mai bună aproximare. Dacă $\frac{p}{q}>\frac{p_1}{q_1}\ (=\pi_1)$ atunci :

$$\left|\alpha-\frac{p}{q}\right|>\left|\frac{p}{q}-\frac{p_1}{q_1}\right|\ge\frac{1}{qq_1},$$ (căci avem următoarea ordonare



deci

$$|q\alpha-p|>\frac{1}{q_1}.$$

Pe de altă parte, din (11), $\frac{1}{q_1}=\frac{1}{a_1}\ge|1\cdot\alpha-a_0|$ şi, din nou, p/q n-ar fi o cea mai bună aproximare. Am stabilit deci că $\pi_0\le p/q\le\pi_1$

Presupunem că p/q nu coincide cu nici o redusă a lui α. Atunci p/q este cuprins între două reduse π_{n-1} şi π_{n+1}, cu rangurile de aceeaşi paritate. Avem

$$\left|\frac{p}{q}-\frac{p_{n-1}}{q_{n-1}}\right|\geq\frac{1}{qq_{n-1}} \text{ şi } \left|\frac{p}{q}-\frac{p_{n-1}}{q_{n-1}}\right|<\left|\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right|=\frac{1}{q_nq_{n-1}}$$

de unde deducem $q_n<q$. Pe de altă parte,

$$\left|\alpha-\frac{p}{q}\right|\geq\left|\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}\right|\geq\frac{1}{q_nq_{n-1}},$$

deci

$$\left|q\alpha-p\right|\geq\frac{1}{q_{n+1}}$$

şi din (11),

$$\frac{1}{q_{n+1}}\geq\left|q_n\alpha-p_n\right|$$

adică $q_n<q$ şi $\left|q_n\alpha-p_n\right|\leq\left|q\alpha-p\right|$, în contradicție cu faptul că p/q este o cea mai bună aproximare şi astfel propoziția este demonstrată. ■

Observație. Dacă α este rațional şi p/q nu este o redusă a lui α, atunci găsim redusa $\frac{p_n}{q_n}$, cu $\left|q_n\alpha-p_n\right|\leq\left|q\alpha-p\right|$ şi $q_n<q$.

Este adevărată şi reciproca:

PROPOZIȚIA 3.8. Orice redusă este o cea mai bună aproximare, cu excepția eventuală a redusei $\pi_0=\frac{p_0}{q_0}$.

Observație Dacă $\alpha = [a_0 ; 2]$, atunci $\pi_0=\frac{a_0}{1}$ nu este o cea mai bună aproximare, căci $|1\cdot\alpha-a_0|=1/2=|1\cdot\alpha-a_0-1|$. În schimb,$\pi_1=\alpha$ este, evident, o cea mai bună aproximare.

Demonstrație Examinăm numai cazul $\alpha\neq[a_0 ; 2]$. Fie $\frac{p_m}{q_m}$ o redusă a lui α, cu $m\geq1$. Considerăm numerele $| y\alpha-x |$, unde $y\in\mathbb{N}^*$, $y \leq q_m$, iar x este $[y\alpha]$ sau $[y\alpha]+1$. Fie $| y_0\alpha-x_0 |$ cel mai mic dintre ele. Dacă minimul este atins de mai multe valori y, am notat cu y_0 cea mai mică dintre ele; x_0 este atunci unic determinat, deoarece, dacă $| y_0\alpha-x_0 |=| y_0\alpha-x_0-1|$, atunci $y_0\alpha-x_0 = x_0+1-y_0\alpha$, deci $\alpha=\frac{2x_0+1}{2y_0}$ este rațional.

Fie $\alpha=[a_0 ; a_1,\ldots,a_n]$, cu $a_n \geq 2$, fracția continuă a lui α. Avem $n \geq 1$ şi deoarece cazul $[a_0 ; 2]$ l-am exclus, rezultă fie $a_n>2$, fie $a_n=2$ şi $n >1$. Avem

$2y_0=q_n=a_nq_{n-1}+q_{n-2}$ şi $2x_0+1=p_n=a_n p_{n-1}+p_{n-2}$

de unde $q_{n-1}<y_0$, dar $|\ q_{n-1}\ \alpha-p_{n-1}|\ =\ \frac{1}{q_n}=\frac{1}{2y_0}\le\frac{1}{2}\ =\ |\ y_0\ \alpha-p_0\ |$, ceea ce ar contrazice alegerea lui y_0. Numărul $\frac{x_0}{y_0}$ este deci o cea mai bună aproximare a lui α şi, conform teoremei precedente, $\frac{x_0}{y_0}=\frac{p_k}{q_k}$. Cum şirul $q_1, q_2,\ldots$ este strict crescător, avem $k \le m$ (căci $q_k \le q_m$). Dacă k=m, am terminat, dacă, însă, k<m, atunci, folosind (11), avem:

$$\left|q_k\alpha-p_k\right|>\frac{1}{q_k+q_{k+1}}\ge\frac{1}{q_{m-1}+q_m}\ge\frac{1}{q_{m-1}+a_{m+1}q_m}=\frac{1}{q_{m+1}}\ge\left|q_m\alpha-p_m\right|$$

ceea ce ar contrazice definiția lui y_0.

În prima parte a demonstrației am arătat că, exceptând numerele $\alpha=[a_0;\ 2]$, luând un $q\in\mathbb{N}^*$ (în locul lui q_m), există o cea mai bună aproximare $\frac{x_0}{y_0}$ (deci o redusă a lui α) cu $y_0\le q$. În cazul q=1, această cea mai bună aproximare este π_0 sau $\frac{a_0+1}{1}$ şi deci, π_0 este o cea mai bună aproximare a lui α, exceptând cazul când când $q_1=1$, deci $\alpha=[a_0;\ 1,\ldots]$. ■

În continuare ne vom ocupa de dezvoltarea în fracții continue periodice a numerelor iraționale pătratice.

<u>DEFINIȚIA 3.9.</u> Fracția continuă infinită $[a_0;a_1,\ldots]$ se zice *<u>periodică</u>* dacă există $h\in\mathbb{N}^*$ şi $k\in\mathbb{N}$ cu $a_n=a_{n+h+1}$ pentru fiecare $n\ge k$. Convenim să notăm o asemenea fracție continuă cu $[a_0;a_1,\ldots,\overline{a_{k-1},a_k,a_{k+1},\ldots,a_{k+h}}]$.

Pentru asemenea fracții continue putem calcula valoarea mai simplu decât ca limită a şirului de reduse.

<u>Exemplu</u> Fie $\alpha=[1;\overline{2}]=[1;2,2,2,2\ldots]$.Avem $\alpha=[1;\alpha_1]$, unde $\alpha_1=[2;2,2,2,2\ldots]=[\ \overline{[2]}\ ]$.De asemenea $\alpha_1=[2;\alpha_2]$, unde $\alpha_2=\alpha_1$, deci $\alpha_1=2+1/\alpha_1$, adică $\alpha_1^2-2\alpha_1-1=0$, de unde $\alpha_1=1+\sqrt{2}$. Revenind la α, obținem $\alpha=1+1/\alpha_1=\sqrt{2}$.

În general, dacă $\alpha = [a_0; a_1, ..., a_{k-1}, \overline{a_k, ..., a_{k+h}}]$, atunci $\alpha_k = [\overline{a_k; a_{k+1} ..., a_{k+h}}] = \alpha_{k+h+1}$ şi, conform lui (6),

$$\alpha = \frac{p_{k-1}\alpha_n + p_{k-2}}{q_{k-1}\alpha_n + q_{k-2}} = \frac{p_{k+h}\alpha_k + p_{k+h-1}}{q_{k+h}\alpha_k + q_{k+h-1}}$$

Din a doua egalitate urmează că α_k este rădăcina unei ecuații de gradul doi cu coeficienți întregi :

$$A\alpha_k^2 + B\alpha_k + C = 0$$

iar prima egalitate ne dă

$$\alpha_k = \frac{-q_{k-2}\alpha + p_{k-2}}{q_{k-1}\alpha - q_{k-2}}$$

de unde :

$$A(p_{k-2} - \alpha\, q_{k-2})^2 + B(p_{k-2} - \alpha\, q_{k-2})(\alpha\, q_{k-1} - p_{k-1}) + C(\alpha\, q_{k-1} - p_{k-1})^2 = 0$$

deci şi α este rădăcina a unei ecuații de gradul doi cu coeficienți întregi.

<u>DEFINITIA 3.10.</u> Numerele iraționale, rădăcini ale unei ecuații de gradul doi cu coeficienți întregi (nu toți nuli), se numesc *<u>iraționale pătratice</u>*. În anul 1770, Joseph Louis de Lagrange (1736-1813) a demonstrat următorul rezultat:

<u>PROPOZIȚIA 3.11.(Lagrange)</u> Un număr irațional este pătratic dacă şi numai dacă fracția sa continuă este periodică.

<u>Demonstrație</u> Am arătat deja că orice fracție continuă periodică este un irațional pătratic. Să presupunem acum că α este rădăcină a ecuației cu coeficienți întregi $Ax^2+Bx+C=0$, unde $A \neq 0$ şi $0 < B^2-4AC$ nu este pătrat perfect.

Fie $\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n]$. Cu relația(6), avem

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$$

şi, deci,

$$A(p_{n-1}\,\alpha_n + p_{n-2})^2 + B(q_{n-1}\alpha_n + q_{n-2})(p_{n-1}\,\alpha_n + p_{n-1}) + C(q_{n-1}\alpha_n + q_{n-2})^2 = 0$$

adică α_n este rădăcina ecuației $A_n x^2 + B_n x + C_n = 0$, unde:

$$A_n = Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2 \qquad (12)$$

$$B_n = 2Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + q_{n-1}p_{n-2}) + 2Cq_{n-1}q_{n-2} \qquad (13)$$

$$C_n = Ap_{n-2}^2 + Bp_{n-2}q_{n-2} + Cq_{n-2}^2 \qquad (14)$$

Să observăm întâi că $C_n = A_{n-1}$. Din (7) deducem că $p_{n-1}q_{n-2} + q_{n-1}p_{n-2}$ este impar şi deci B şi B_n au aceeași paritate. Prin calcul direct se verifică şi că

$B_n^2-4A_nC_n=(B^2-4AC)(p_{n-1}q_{n-2}+q_{n-1}p_{n-2})^2=B^2-4AC.$ (15)

Folosind însă faptul că $A\alpha^2+B\alpha+C=0$, relația (12) se scrie:

$$A_n = Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2 - q_{n-1}^2(A\alpha^2 + B\alpha + C) =$$
$$= A(p_{n-1}^2 - q_{n-1}^2) + B(p_{n-1} - \alpha\ q_{n-1})q_{n-1} =$$
$$= (p_{n-1} - \alpha\ q_{n-1})(A(p_{n-1} + \alpha\ q_{n-1}) + Bq_{n-1})$$

Cu ajutorul lui (11), vom avea

$$|A_n| \le \frac{1}{q_n}|A(p_{n-1} + \alpha\ q_{n-1}) + Bq_{n-1}\ | \le \frac{1}{q_{n-1}}\left|A(p_{n-1} + \alpha\ q_{n-1}) + Bq_{n-1}\right| \le$$
$$\le |A|\left|\frac{p_{n-1}}{q_{n-1}} + \alpha\right| + |B| \le |A|\left(\left|\frac{p_{n-1}}{q_{n-1}} - \alpha\right| + 2|\alpha|\right) + |B| \le |A|\left(1 + 2|\alpha|\right) + |B|$$

Vedem de aici că şirul de întregi A_n ia un număr finit de valori şi deci $C_n(=A_{n-1})$ ia un număr finit de valori; în fine, din cauza lui (15), α_n ia un număr finit de valori. Rezultă că pentru anumiți k, h, vom avea $\alpha_k=\alpha_{k+h+1}$.

Este uşor de dedus de aici că $a_k= a_{k+h+1}$, $a_{k+1}= a_{k+1+h+1}$ şi prin inducție, $a_n=a_{n+h+1}$ pentru $n \ge k$, deci fracția continuă a lui α este periodică. ■

Cele mai simple fracții continue periodice sunt cele *pur periodice*.(adică cele pentru care $a_0=a_{n+1}$). Fie deci $\alpha=[\overline{a_0; a_1,.., a_n}]$ o fracție continuă pur periodică. Avem $a_0=a_{n+1}\ge 1$ şi $\alpha=[a_0;a_1,\ldots,a_n,\alpha]$, deci, folosind (6), $\alpha=\dfrac{p_n\alpha\ + p_{n-1}}{q_n\alpha\ + q_{n-1}}$, adică:

$$q_n\,\alpha^2 + (q_{n-1}- p_n)\alpha - p_{n-1} = 0.$$

Pentru trinomul $f(x) = q_nx^2 +(q_{n-1}-p_n)x-p_{n-1}$, avem

$$f(-1) = q_n - q_{n-1} + p_n - p_{n-1} > 0,\ f(0) = - p_{n-1} < 0.$$

Cum, evident, $\alpha > a_0 \ge 0$, deducem că cealaltă rădăcină a trinomului este cuprinsă între –1 şi 0. Evident α este de forma $\dfrac{P+\sqrt{D}}{Q}$, iar cealaltă rădăcină este $\dfrac{P-\sqrt{D}}{Q}$. Pentru un irațional pătratic $\alpha=\dfrac{P+\sqrt{D}}{Q}$, vom nota $\widetilde{\alpha} = \dfrac{P-\sqrt{D}}{Q}$ şi îl vom numi pe $\widetilde{\alpha}$ *conjugatul lui* α.

DEFINITIE 3.12. Numărul irațional pătratic α se numeşte redus dacă $\alpha > 1$, iar $\widetilde{\alpha} \in (-1, 0)$.

Teorema care urmează a fost demonstrată în 1828 de Evariste Galois (1811-1832), pe atunci elev.

PROPOZIŢIA 3.13. (E. Galois) Fracția continuă a lui α este pur periodică dacă şi numai dacă este un irațional pătratic redus.

Demonstrație Am văzut mai sus că orice fracție continuă pur periodică este un irațional pătratic redus (vom prescurta în continuare i.p.r). Fie α un i.p.r. Avem $\alpha_1 = \frac{1}{\alpha - a_0} > 1$ şi $\widetilde{\alpha}_1 = \frac{1}{\widetilde{\alpha} - a_0} \in (-1,0)$, căci $a_0 \geq 1$. Prin inducție, rezultă că α_n este i.p.r. pentru fiecare n. Ştim că fracția continuă a lui α este periodică. Dacă nu este pur periodică, atunci $\alpha = [a_0; a_1, ..., a_{k-1}, \overline{a_k, ..., a_{k+h}}]$, unde $a_{k-1} \neq a_{k+h}$.

Am văzut însă că $\alpha_{k-1} = [a_{k-1}; \alpha_k]$ este i.p.r. şi la fel este

$$\alpha_{k+1} = [a_{k+h}; \alpha_{k+h+1}] = [a_{k+h}; \alpha_k].$$

Avem deci $\widetilde{\alpha}_{k-1} = \left(a_{k-1} + \frac{1}{\alpha_k}\right)^{\sim} = a_{k-1} + \frac{1}{\widetilde{\alpha}_k} \in (-1, 0)$,

$$\widetilde{\alpha}_{k+1} = a_{k+h} + \frac{1}{\widetilde{\alpha}_k} \in (-1, 0).$$

Deducem de aici că $a_{k-1} \in \left(-1 - \frac{1}{\widetilde{\alpha}_k}, -\frac{1}{\widetilde{\alpha}_k}\right)$ şi $a_{k+h} \in \left(-1 - \frac{1}{\widetilde{\alpha}_k}, -\frac{1}{\widetilde{\alpha}_k}\right)$ deci $a_{k-1} = a_{k+h} = [-\frac{1}{\widetilde{\alpha}_k}]$.

Am ajuns la o contradicție, deci $\alpha = [\overline{a_0; a_1, ..., a_h}]$. ■

Ce se întâmplă dacă „răsturnăm " perioada unui i.p.r.?

PROPOZIŢIA 3.14. Fie $\alpha = [\overline{a_0; a_1, ..., a_n}]$ şi $\beta = [\overline{a_n; a_{n-1}, ..., a_0}]$. Atunci $\alpha = -\frac{1}{\widetilde{\beta}}$.

Demonstrație Întrucât $\alpha = [a_0; a_1, ..., a_n, \alpha]$, folosind (6), avem, după cum am mai văzut,

$$q_n\alpha^2 + (q_{n-1} - p_n)\alpha - p_{n-1} = 0. \qquad (16)$$

Cum $\beta = [a_n; a_{n-1},..., a_0, \beta]$, cu ajutorul propoziției 6 se deduce, analog,

$$p_{n-1}\beta^2 + (q_{n-1}-p_n)\beta - q_n = 0,$$

de unde $p_{n-1}\widetilde{\beta}^2 + (q_{n-1} - p_n)\widetilde{\beta} - q_n = 0$,

$$-\widetilde{\beta}^2\left(q_n(-\frac{1}{\widetilde{\beta}})^2 + (q_{n-1} - p_n)(-\frac{1}{\widetilde{\beta}}) - p_{n-1}\right) = 0$$

și, deoarece ecuația (16) are o singură rădăcină pozitivă, $\alpha = -\frac{1}{\widetilde{\beta}}$. ■

Cele mai simple iraționale pătratice sunt cele de forma $\sqrt{D}$, unde $D \in \mathbb{Q}_+$ și $\sqrt{D} \notin \mathbb{Q}$. Fracțiile lor continue, în cazul D>1, au proprietăți remarcabile:

<u>PROPOZITIA 3.15.</u> Fie $D \in \mathbb{Q}$, D>1, $\sqrt{D} \notin \mathbb{Q}$. Atunci

$$\sqrt{D} = [a_0; \overline{a_1,..., a_n, 2a_0}]$$

În plus, partea $a_1, a_2, \ldots, a_n$ a perioadei este simetrică, adică $a_k = a_{n+1-k}$, pentru $1 \le k \le n$.

<u>Demonstrație</u> Avem $a_0 = [\sqrt{D}]$ deci $\alpha = a_0 + \sqrt{D} > 1$ și $\widetilde{\alpha} = a_0 - \sqrt{D} \in (-1,0)$, deci α este i.p.r. și $[\alpha] = 2a_0$, deci $\alpha = [\overline{2a_0; a_1,..., a_n}]$. Deducem de aici că :

$\sqrt{D} = [a_0; \overline{a_1,..., a_n, 2a_0}]$ și, încă, $-a_0 + \sqrt{D} = [0; \overline{a_1,..., a_n, 2a_0}]$,

de unde $\beta \overset{not}{=} \frac{1}{-a_0 + \sqrt{D}} = [\overline{a_1; a_2,..., a_n, 2a_0}]$

Folosind propoziția 11, vom avea:

$$-\frac{1}{\widetilde{\beta}} = [\overline{2a_0; a_n,..., a_1}] = a_0 + \sqrt{D} = \alpha = [\overline{2a_0; a_1,..., a_n}]$$

de unde rezultă $a_{n+1-k} = a_k$.

Putem demonstra și reciproca:

Dacă $\alpha = [a_0; \overline{a_1,..., a_n, 2a_0}]$, $(a_0 \ge 1)$, unde $a_k = a_{n+1-k}$, atunci $\alpha + a_0 = [\overline{2a_0; a_1,..., a_n}]$ și $\frac{1}{\alpha - a_0} = [\overline{a_1; a_2,..., a_n, 2a_0}] = [\overline{a_n; a_{n-1},..., a_1, 2a_0}]$ și, din Propoziția 11, vom avea $\alpha + a_0 = (-\alpha + a_0)\tilde{}$, deci $\alpha = -\widetilde{\alpha}$, adică în scrierea $\alpha = \frac{P + \sqrt{\Delta}}{Q}$, avem $\frac{P + \sqrt{\Delta}}{Q} = \frac{-P + \sqrt{\Delta}}{Q}$, de unde P=0, deci $\alpha = \sqrt{\frac{\Delta}{Q^2}}$. ■

Pe noi ne interesează informația pe care ne-o dă Propoziția 3.15 despre fracția continuă a lui $\sqrt{D}$ în cazul $D\in\mathbb{N}$, cu $\sqrt{D}\notin\mathbb{Q}$.

Exemple 1. Să dezvoltăm în fracție continuă numărul $\alpha=\sqrt{5}$.

Avem $a_0=2$, $\alpha_1=1/\sqrt{5}-2=\sqrt{5}+2$,

$a_1=4$, $\alpha_2=1/\alpha_1-a_1=1/\sqrt{5}-2=\sqrt{5}+2=\alpha_1$,

deci $\sqrt{5}=[2;4]$.

2. Să găsim fracția continuă a lui $\sqrt{7}$.

$a_0=2$, $\alpha_1=1/(\sqrt{7}-2)=(\sqrt{7}+2)/3$

$a_1=4$, $\alpha_2=3/(\sqrt{7}-1)=3(\sqrt{7}+1)/6=(\sqrt{7}+1)/2$

$a_2=1$, $\alpha_3=2/(\sqrt{7}-1)=2(\sqrt{7}+1)/6=(\sqrt{7}+1)/3$

$a_3=1$, $\alpha_4=3/(\sqrt{7}-2)=3(\sqrt{7}+2)/3=\sqrt{7}+2$

$a_4=4$, $\alpha_5=1/(\sqrt{7}-2)=\alpha_1$,

deci $\sqrt{7}=[2;\overline{1,1,4}]$.

Acest şir poate fi destul de lung:

$\sqrt{991}=[31;\overline{2,12,10,2,2,2,1,1,2,6,1,1,1,1,3,1,8,4,1,2,1,2,3,1,4,1,20,6,4,31,4,6,20,1,4,1,3,2,1,4,8,1,3,1,1,1,1,2,1,1,2,2,2,10,12,2,62}]$

În continuare vom pune în evidență un algoritm de dezvoltare a lui $\alpha=\sqrt{D}$ în fracție continuă (cu $D\in\mathbb{N}^*$ a.î. $\alpha\notin\mathbb{Q}$).

Avem $a_0=[\sqrt{D}]$, deci $\sqrt{D}=a_0+\frac{1}{\alpha_1}$, deci

$\alpha_1=\frac{1}{\sqrt{D}-a_0}=\frac{\sqrt{D}+a_0}{D-a_0^2}=\frac{\sqrt{D}+b_1}{c_1}$, unde $b_1=a_0$ şi $c_1=D-a_0^2>0$ (deoarece $a_0=[\sqrt{D}]$).

Avem $D-b_0^2=c_1$. Continuând obținem: $a_1=[\alpha_1]$ şi $\alpha_1=a_1+\frac{1}{\alpha_1}$, deci

$\alpha_2=\frac{1}{\alpha_1-a_1}=$

$$= \frac{1}{\frac{\sqrt{D}+b_1}{c_1}-a_1} = \frac{c_1}{\sqrt{D}+b_1-a_1c_1} = \frac{c_1(\sqrt{D}+a_1c_1-b_1)}{D-(a_1c_1-b_1)^2} = \frac{c_1(\sqrt{D}+a_1c_1-b_1)}{D-b_1^2-a_1^2c_1^2+2a_1b_1c_1} =$$

$$= \frac{\sqrt{D}+a_1c_1-b_1}{1-a_1^2c_1+2a_1b_1} = \frac{\sqrt{D}+b_2}{c_2}$$

unde $b_2=a_1c_1-b_1$ şi $c_2=1-a_1^2c_1+2a_1b_1$.

Pentru $n\in\mathbb{N}$, $n\geq 2$, fie $b_{n+1}=a_nc_n-b_1$ şi $c_{n+1}=c_{n-1}-a_1^2c_n+2a_nb_n$ şi să arătăm că pentru $n\geq 2$:

(1) $D-b_n^2=c_{n-1}c_n$.

Vom proba (1) prin inducţie matematică relativ la $n\geq 2$.

Pentru $n=2$ avem $D-b_2^2=D-(a_1c_1-b_1)^2=D-b_1^2-a_1^2c_1^2+2a_1b_1c_1=$
$=c_1-a_1^2c_1^2+2a_1b_1c_1=c_1(1-a_1^2c_1+2a_1b_1)=c_1c_2$.

Să presupunem că pentru $n\geq 2$ avem $D-b_n^2=c_{n-1}c_n$. Atunci:
$D-b_{n+1}^2=D-(a_nc_n-b_n)^2=D-b_n^2-a_n^2c_n^2+2a_nb_nc_n=c_{n-1}c_n-a_n^2c_n^2+2a_nb_nc_n=c_n(c_{n-1}-a_n^2c_n+$
$+2a_nb_n)=c_nc_{n+1}$ şi astfel (1) este adevărată pentru orice $n\geq 2$.

Să arătăm acum că pentru orice $n\geq 1$:

(2) $\alpha_n=\frac{\sqrt{D}+b_n}{c_n}$

După calculele de la început avem că (2) se verifică pentru n=1, 2.

Dacă presupunem că (2) este verificată pentru n, atunci:

$$\alpha_{n+1} = \frac{1}{\alpha_n-a_n} = \frac{1}{\frac{\sqrt{D}+b_n}{c_n}-a_n} = \frac{c_n}{\sqrt{D}+b_n-a_nc_n} = \frac{c_n(\sqrt{D}+a_nc_n-b_n)}{D-(a_nc_n-b_n)^2} =$$

$$= \frac{c_n(\sqrt{D}+b_{n+1})}{c_nc_{n+1}} = \frac{\sqrt{D}+b_{n+1}}{c_{n+1}}$$

(am ţinut cont şi de (1)), astfel că (2) este adevărată pentru orice $n\in\mathbb{N}$.

În mod evident $c_1\in\mathbb{N}$. Atunci $b_1=a_0=[\sqrt{D}]<\sqrt{D}$ şi astfel $0<\sqrt{D}-b_1<1$, deci $0<(\sqrt{D}-b_1)/c_1<1$. Cum $\alpha_1>1$ deducem că $(\sqrt{D}+b_1)/c_1>1$.

Astfel $0<(\sqrt{D}-b_1)/c_1<1<(\sqrt{D}+b_1)/c_1$.

Să arătăm acum că pentru orice $n\in\mathbb{N}$:

(3) $\quad 0 < (\sqrt{D} - b_n)/c_n < 1 < (\sqrt{D} + b_n)/c_n$.

(pentru n=1 (3) este adevărată datorită celor stabilite mai sus). Să presupunem că (3) este adevărată pentru un anumit n şi să o probăm pentru n+1.

Conform cu (2) avem $\frac{\sqrt{D}+b_{n+1}}{c_{n+1}} = \alpha_{n+1} > 1$ astfel că :

$$\frac{\sqrt{D}-b_{n+1}}{c_{n+1}} = \frac{D-b_{n+1}^2}{c_{n+1}(\sqrt{D}+b_{n+1})} = \frac{c_n}{\sqrt{D}+b_{n+1}} = \frac{c_n}{\sqrt{D}+a_n c_n - b_n} = \frac{1}{\frac{\sqrt{D}-b_n}{c_n}+a_n}$$

de unde deducem că $0 < \frac{\sqrt{D}-b_{n+1}}{c_{n+1}} < 1$. (ținând cont şi de ipoteza de inducție)

Astfel (3) este adevărată pentru orice $n\in\mathbb{N}$.

Dacă $c_n<0$ pentru un anumit $n\in\mathbb{N}$, atunci din (3) deducem că $\sqrt{D} - b_n<0$ şi $\sqrt{D} + b_n<0$, deci $2\sqrt{D}<0$ – absurd!.

Deci $c_n>0$ pentru orice $n\in\mathbb{N}^*$.

În consecință $\sqrt{D} - b_n < c_n < \sqrt{D} + b_n$, deci $\sqrt{D} - b_n < \sqrt{D} + b_n$ şi astfel $b_n>0$ pentru orice $n\in\mathbb{N}^*$.

Din (3) deducem că $b_n<\sqrt{D}$ şi astfel $c_n<\sqrt{D}+b_n<2\sqrt{D}$. Din observația de mai înainte deducem că numărul perechilor (b_n, c_n) este mai mic decât 2D.

Astfel, printre termenii şirului $\alpha_n=\frac{\sqrt{D}+b_n}{c_n}$ numai un număr finit dintre ei sunt diferiți, fiecare dintre aceştia fiind mai mici decât 2D. Astfel cel puțin doi termeni ai şirului $(\alpha_n)_{n\geq 1}$ sunt egali.

Deci există k, $s\in\mathbb{N}$ a.î. k, s<2D şi (4) $\alpha_k=\alpha_{k+s}$. Deoarece $\alpha_{n+1} = \frac{1}{\alpha_n - [\alpha_n]}$ pentru n≥1, din (4) deducem că $\alpha_{k+1}=\alpha_{k+s+1}$ şi mai general, $\alpha_n=\alpha_{n+s}$ pentru n≥k .

Astfel şirurile $(\alpha_n)_{n\geq 1}$ şi $(a_n)_{n\geq 1}$ sunt periodice (căci $a_n=[\alpha_n]$ pentru n≥1).

Fie (5) $\alpha_n' = \frac{\sqrt{D}-b_n}{c_n}$ pentru n≥1; ținând cont de (1) deducem imediat că $a_n = [\frac{1}{x'_{n+1}}]$ pentru orice n≥1.

Mai mult, cum $\alpha_k=\alpha_{k+s}$ deducem că $\alpha'_n=\alpha'_{n+k}$ şi deci pentru k>1 avem $a_{k-1}=[\frac{1}{x'_k}]=[\frac{1}{x'_{k+s}}]=a_{k+s-1}$. Ţinând cont de relaţiile $\alpha_n=a_n+\frac{1}{\alpha_{n+1}}$ şi $\alpha_k=\alpha_{k+s}$ deducem că $\alpha_{k-1}=\alpha_{k+s-1}$. Repetând raţionamentul anterior pentru k>2 obţinem că $\alpha_{k-2}=\alpha_{k+s-2}$. Astfel $\alpha_{n+s}=\alpha_n$ şi $a_{n+s}=a_n$ pentru orice $n\in\mathbb{N}^*$.

Deducem imediat formulele:

$$\alpha_1=a_1+\frac{1}{|a_2|}+\ldots+\frac{1}{|a_s|}+\frac{1}{|\alpha_1|} \quad \text{şi} \quad \frac{1}{\alpha'_1}=a_s+\frac{1}{|a_{s-1}|}+\ldots+\frac{1}{|a_1|}+\frac{1}{\left|(\frac{1}{x'_1})\right|}.$$

Deoarece $\alpha_1>1$ şi $\frac{1}{\alpha'_1}>1$ aceste ultime relatii ne dau :

$a_s=2a_0=2[\sqrt{D}]$, $a_1=a_{s-1}$, $a_2=a_{s-2}$, …, $a_{s-1}=a_1$. (adică şirul a_1, a_2, …, a_{s-1} este simetric)

Ţinând cont că dacă $x\in\mathbb{R}$ şi $k\in\mathbb{N}^*$, atunci [x/k]=[[x]/k] avem (conform cu relaţiile (1)) : $a_n=[\alpha_n]=[\frac{\sqrt{D}+b_n}{c_n}]=[\frac{[\sqrt{D}]+b_n}{c_n}]=[\frac{a_0+b_n}{c_n}]$, adică $a_n=[\frac{a_0+b_n}{c_n}]$ pentru orice $n\geq 1$.

Rezumând cele expuse mai înainte obţinem următorul algoritm de dezvoltare a lui $\sqrt{D}$ (cu $D\in\mathbb{N}^*$ a.î. $\sqrt{D}\notin\mathbb{Q}$) în fracţie continuă.

Alegem $a_0=[\sqrt{D}]$, $b_0=1$, $c_0=1$ şi apoi construim sirurile $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ şi $(c_n)_{n\geq 0}$ cu ajutorul recurenţelor :

$$(6) \qquad \begin{cases} a_n=[\frac{a_0+b_{n-1}}{c_{n-1}}] \\ b_n=a_{n-1}c_{n-1}-b_{n-1} \qquad \text{pentru } n\geq 1 \\ c_n=\frac{D-b_n^2}{c_{n-1}} \end{cases}$$

Construim apoi şirul (b_2, c_2), (b_3, c_3) şi găsim cel mai mic indice s pentru care $b_{s+1}=b_1$ şi $c_{s+1}=c_1$. Atunci $\sqrt{D}=[a_0;\overline{a_1,\ldots,a_s}]$.

Observaţie Conform unei teoreme a lui T. Muir (vezi **O. Perron: Die Lehre von den Kettenbrüchen 1, Stuttgart 1954)**, dacă numărul s de termeni ai perioadei este par, atunci k=s/2 este cel mai mic indice pentru care $b_{k+1}=b_k$, pe

când dacă s este impar atunci k=(s-1)/2 este cel mai mic indice pentru care $c_{k+1}=c_k$.

Practic se procedează astfel:

Pentru $\alpha=\sqrt{D}$ (cu $D\in\mathbb{N}^*$ a.î. $\sqrt{D}\notin\mathbb{Q}$) alegem $a_0=[\sqrt{D}]$, $b_0=0$, $c_0=1$ şi apoi construim prin recurenţă şirurile $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ şi $(c_n)_{n\geq 0}$ cu ajutorul formulelor:

(7) $b_n=a_{n-1}c_{n-1}-b_{n-1}$, $c_n=\frac{D-b_n^2}{c_{n-1}}$, $a_{n-1}=[\frac{a_0+b_{n-1}}{c_{n-1}}]$, pentru $n\geq 1$.

Calculele se continuă până când $b_{n+1}=b_n$ sau până când $c_{n+1}=c_n$.

Dacă $b_{n+1}=b_n$, atunci $\sqrt{D}=[a_0; a_1,\ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_1, 2a_0]$ (adică lungimea perioadei minime este pară).

Dacă $c_{n+1}=c_n$, atunci $\sqrt{D}=[a_0;\overline{a_1,\ldots,a_n,a_n,\ldots,a_1,2a_0}]$ (adică lungimea perioadei minime este impară).

Numerele $b_n, c_n\in\mathbb{N}$ sunt cele din scrierea lui $\alpha_n=\frac{\sqrt{D}+b_n}{c_n}$.

Exemple 1. Fie D=1009 şi $\alpha=\sqrt{1009}$.

Avem $a_0=[\sqrt{D}]=[\sqrt{1009}]=31$, $b_0=0$, $c_0=1$.

Conform recurenţelor (6) sau (7) avem:

$b_1=a_0c_0-b_0=a_0=31$, $c_1=\frac{1009-b_1^2}{c_0}=\frac{1009-31^2}{1}=\frac{1009-961}{1}=48$,

$a_1=\left[\frac{a_0+b_1}{c_1}\right]=\left[\frac{31+31}{48}\right]=1$. Apoi:

$b_2=a_1c_1-b_1=17$, $c_2=\frac{1009-b_2^2}{c_2}=15$, $a_2=\left[\frac{a_0+b_2}{c_2}\right]=\left[\frac{31+17}{15}\right]=3$

Aplicând din nou recurenţele (6) şi (7) găsim

$b_3=a_2c_2-b_2=28$, $c_3=\frac{1009-b_3^2}{c_2}=1=c_2$.

Conform algoritmului descris mai înainte avem $\sqrt{1009}=[31;\overline{1,3,3,1,62}]$, iar $\alpha_3=\frac{28+\sqrt{1009}}{15}$.

2. Fie $a\in\mathbb{N}$, $a\geq 3$, $D=a^2-2$ şi $\alpha=\sqrt{D}=\sqrt{a^2-2}$.

Cum $(a-1)^2=a^2-2a+1<a^2-2<a^2$, deducem că $a_0=[\sqrt{a^2-2}\,]=a-1$.

Deci, $b_1=a_0=a-1$,

$c_1=D-a_0^2=a^2-2-(a-1)^2=2a-3$,

$$a_1=\left[\frac{a_0+b_1}{c_1}\right]=\left[\frac{2a-2}{2a-3}\right]=\left[1+\frac{1}{2a-3}\right]=1$$

Continuăm $b_2=a_1c_1-b_1=2a-3-(a-1)=a-2$,

$$c_2=\frac{D-b_2^2}{c_1}=\frac{a^2-2-(a-2)^2}{2a-3}=\frac{4a-6}{2a-3}=2$$

$$a_2=\left[\frac{a_0+b_2}{c_2}\right]=\left[\frac{a-1+a-2}{2}\right]=\left[a-\frac{3}{2}\right]=a-2$$

Apoi

$b_3=a_2c_2-b_2=(a-2)^2-(a-2)=a-2$;

$$c_3=\frac{D-b_3^2}{c_2}=\frac{a^2-2-(a-2)^2}{2}=\frac{4a-6}{2}=2a-3$$

$$a_3=\left[\frac{a_0+b_3}{c_3}\right]=\left[\frac{a-1+a-2}{2a-3}\right]=1$$

$b_4=a_3c_3-b_3=2a-3-(a-2)=a-1$,

$$c_4=\frac{D-b_4^2}{c_3}=\frac{a^2-2-(a-1)^2}{2a-3}=1$$

$$a_4=\left[\frac{a_0+b_4}{c_4}\right]=\left[\frac{a-1+a-1}{1}\right]=2a-2.$$

În sfârşit,

$$b_5=a_4c_4-b_4=2a-2-(a-1)=a-1=b_1,\ c_5=\frac{D-b_5^2}{c_4}=\frac{a^2-2-(a-1)^2}{1}=2a-3=c_1$$

Din cele expuse mai înainte avem $s=4$ astfel că:

$$\sqrt{a^2-2}=\left[a-1;\overline{1,a-2,1,2a-2}\right].$$

Analog se obţine $\sqrt{a^2+1}=\left[a;\overline{2a}\right]$ şi $\sqrt{a^2+2}=\left[a;\overline{a,2a}\right]$ pentru orice $a\in\mathbb{N}$.

Observaţie. Acest paragraf a fost redactat în cea mai mare parte după lucrarea [10].

CAPITOLUL 11:
TEOREME DE REPREZENTARE PENTRU NUMERE ÎNTREGI

§1 Reprezentarea unui număr natural ca sumă de două pătrate de numere întregi.

Pentru un număr natural n, prin d(n) vom nota numărul divizorilor lui n iar prin $d_a(n)$ numărul divizorilor d ai lui n cu proprietatea că $d \equiv a \ (4)$. Astfel, $d_1(n)$ reprezintă numărul divizorilor de forma 4k+1 ai lui n iar $d_3(n)$ numărul divizorilor de forma 4k+3 ai lui n $(k \in \mathbb{N})$.

Conform teoremei fundamentale a aritmeticii pe n îl putem scrie sub forma $n = 2^k \cdot n_1 \cdot n_2$ cu $k \in \mathbb{N}$, $n_1 = \prod_{\substack{p \ prim \\ p \equiv 1 \ (4)}} p^r$ iar $n_2 = \prod_{\substack{q \ prim \\ q \equiv 3 \ (4)}} q^s$.

În cadrul acestui paragraf vom da răspuns la următoarele chestiuni :

P_1. Pentru care numere naturale n există $x, y \in \mathbb{Z}$ a.î. $n = x^2 + y^2$ $(\star)$.

P_2. În caz că pentru n fixat ecuaţia $(\star)$ are cel puţin o soluţie atunci să se determine numărul tuturor soluţiilor sale.

Observaţie

Dacă ecuaţia $(\star)$ are o soluţie (x, y) în $\mathbb{N} \times \mathbb{N}$, atunci în $\mathbb{Z} \times \mathbb{Z}$ ecuaţia $(\star)$ va avea soluţiile $(\pm x, \pm y)$.

Astfel :

i) Dacă x=y=0 atunci cu necesitate n=0 şi ecuaţia $(\star)$ are o unică soluţie: (0, 0).

ii) Dacă $x \neq 0$ şi y=0 atunci soluţia (x, 0) din $\mathbb{N} \times \mathbb{N}$ generează patru soluţii în $\mathbb{Z} \times \mathbb{Z}$ şi anume: (x, 0), (0, x), (-x, 0) şi (0, -x).

iii) Dacă x=0 şi $y \neq 0$ atunci soluţia (0, y) din $\mathbb{N} \times \mathbb{N}$ generează de asemenea patru soluţii în $\mathbb{Z} \times \mathbb{Z}$ şi anume: (0, y), (y, 0), (0, -y), (-y, 0).

iv) Dacă $x \neq 0$, $y \neq 0$ şi $x \neq y$ atunci soluţia (x, y) din $\mathbb{N} \times \mathbb{N}$ generează opt soluţii în $\mathbb{Z} \times \mathbb{Z}$ şi anume: (x, y), (y, x), (-x, y), (y, -x), (x, -y), (-y, x), (-x, -y), şi (–y, -x).

v) Dacă $x\neq 0$, $y\neq 0$ şi $x=y$ atunci soluţia (x, x) din $\mathbb{N}\times\mathbb{N}$ generează patru soluţii în $\mathbb{Z}\times\mathbb{Z}$ şi anume: (x, x), (-x, x), (x, -x) şi (–x, -x).

Această observaţie ne arată că atunci când vorbim despre numărul de soluţii pentru ecuaţia $(\star)$, trebuie să specificăm neapărat următoarele:

a) Dacă este vorba de numărul de soluţii din $\mathbb{N}\times\mathbb{N}$ sau din $\mathbb{Z}\times\mathbb{Z}$.

b) Ce înţelegem prin soluţii distincte ? (altfel spus, dacă soluţiile (x, y) şi (y, x) pentru $x\neq y$ sunt considerate distincte sau nu) .

Pentru a nu crea confuzii în cadrul acestei lucrări vom ţine cont de ordinea termenilor în cadrul soluţiei (x, y) (pentru $x\neq y$) urmând ca atunci când nu ţinem cont de lucrul acesta să-l menţionăm expres.

Exemple 1. Ecuaţia $x^2+y^2=1$ are două soluţii în $\mathbb{N}\times\mathbb{N}$: (1, 0) şi (0, 1) pe când în $\mathbb{Z}\times\mathbb{Z}$ are patru soluţii: (1, 0), (0, 1), (-1, 0) şi (0, -1).

Dacă nu ţinem cont de ordinea termenilor concluzionăm că ecuaţia $x^2+y^2=1$ are o unică soluţie în $\mathbb{N}\times\mathbb{N}$ (pe (1, 0)) pe când în $\mathbb{Z}\times\mathbb{Z}$ are două soluţii (pe (1, 0) şi (-1, 0)).

2. Ecuaţia $x^2+y^2=2$ are în $\mathbb{N}\times\mathbb{N}$ o soluţie unică şi anume pe (1, 1), pe când în $\mathbb{Z}\times\mathbb{Z}$ are patru soluţii şi anume : (1, 1), (1, -1), (-1, 1) şi (-1, -1).

Dacă nu ţinem cont de ordinea termenilor concluzionăm că ecuaţia $x^2+y^2=2$ are în $\mathbb{Z}\times\mathbb{Z}$ trei soluţii şi anume : (1, 1), (-1, 1) şi (-1, -1).

3. Ecuaţia $x^2+y^2=5$ are în $\mathbb{N}\times\mathbb{N}$ două soluţii: (1, 2) şi (2, 1) pe când în $\mathbb{Z}\times\mathbb{Z}$ are opt soluţii: (1, 2), (1, -2), (-1, 2), (-1, -2), (2, 1), (-2, 1), (2, -1), (-2, -1)

Dacă nu ţinem cont de ordinea termenilor concluzionăm că ecuaţia $x^2+y^2=5$ are o unică soluţie în $\mathbb{N}\times\mathbb{N}$ (pe (1, 2)) pe când în $\mathbb{Z}\times\mathbb{Z}$ are patru soluţii: (1, 2), (-1, 2), (1, -2), şi (–1, -2).

LEMA 1.1. Dacă p este un număr prim de forma 4k+1, atunci $\left[\left(\frac{p-1}{2}\right)!\right]^2+1\equiv 0\ (p)$.

Demonstraţie Scriind că

$$(p-1)!=\left(1\cdot 2\cdot\ldots\cdot\frac{p-1}{2}\right)\cdot\left[\frac{p+1}{2}\cdot\ldots\cdot(p-1)\right]=$$

$$=\left(\frac{p-1}{2}\right)!\left[(p-1)\cdot(p-2)\cdot\ldots\cdot\left(p-\frac{p-1}{2}\right)\right]$$

deducem imediat egalităţile modulo p :

$$(p-1)\,!=\left(\frac{p-1}{2}\right)\,!\,(-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)\,!=\left[\left(\frac{p-1}{2}\right)\,!\right]^2 .$$

Conform teoremei lui Wilson $(p-1)\,!+1\equiv 0\ (p)$ astfel că $\left[\left(\frac{p-1}{2}\right)\,!\right]^2+1\equiv 0\ (p)$. ■

<u>LEMA 1.2.</u> Dacă p∈ℕ este un număr prim iar a∈ℤ a.î. p∤a, atunci există numerele naturale nenule x, y $<\sqrt{p}$ a.î. la o alegere convenabilă a semnelor + sau – să avem ax ± y ≡ 0 (p) .

<u>Demonstraţie</u> Dacă $m=[\sqrt{p}\,]$, atunci $(m+1)^2>p$ şi considerăm mulţimea $X=\{ax-y\ |0\le x,\ y\le m\}$. Cum $|X|=(m+1)^2>p$, rezultă că există două perechi diferite $(x_1,\ y_1)$, $(x_2,\ y_2)\in X$ cu $x_1\ge x_2$ şi $p|(ax_1-y_1)-(ax_2-y_2)=$ $=a(x_1-x_2)-(y_1-y_2)$.

Egalitatea $x_1=x_2$ este imposibilă, căci în caz contrar ar rezulta că $p|y_1-y_2$ (lucru imposibil căci $0\le y_1,\ y_2\le m\le\sqrt{p}<p$). De asemenea, egalitatea $y_1=y_2$ este imposibilă, căci în caz contrar ar rezulta $p|a(x_1-x_2)$, deci $p|x_1-x_2$ – imposibil (căci $0\le x_1,\ x_2\le m\le\sqrt{p}<p$).

Deci $x=x_1-x_2\in\mathbb{N}^*$ (dacă $x<0$, atunci notăm $x=x_2-x_1$) şi cum $y_1-y_2\in\mathbb{Z}^*$, există o alegere convenabilă a semnelor + sau – a.î. $y=\pm(y_1-y_2)\in\mathbb{N}^*$.

Cum $x=x_1-x_2\le x_1\le m<\sqrt{p}$, deducem că $0<x,\ y<\sqrt{p}$ şi astfel numărul $ax\pm b$ (care la o alegere convenabilă a semnelor + şi – este egal cu $a(x_1-x_2)-(y_1-y_2)$) se divide prin p. ■

<u>TEOREMA 1.3. (Fermat)</u> Orice număr prim p de forma 4k+1 se poate scrie ca suma pătratelor a două numere naturale.

<u>Demonstraţie</u> Considerăm $a=\left(\frac{p-1}{2}\right)\,!$. Evident, $a\in\mathbb{N}^*$ şi $(a,\ p)=1$.

Conform Lemei 1.2., există o alegere convenabilă a semnelor + şi – a.î. $ax\pm y\equiv 0(p)$. Atunci $a^2x^2-y^2=(ax+y)(ax-y)\equiv 0(p)$ şi conform Lemei 1.1. $a^2+1\equiv 0(p)$, de unde deducem că $a^2x^2+x^2\equiv 0(p)$ iar de aici că $(a^2x^2+x^2)-(a^2x^2-y^2)=x^2+y^2\equiv 0(p)$, adică putem scrie $x^2+y^2=kp$ cu $k\in\mathbb{N}^*$.

Cum x, y $<\sqrt{p}$ deducem că $x^2+y^2 < 2p$, adică $kp < 2p$, deci $k < 2$, adică $k=1$ (căci $x, y \in \mathbb{N}^*$). Deducem că $p=x^2+y^2$ şi astfel Teorema lui Fermat este complet demonstrată.■

COROLAR 1.4. Dacă $n \in \mathbb{N}^*$ conține în descompunerea sa în factori primi numai numere prime de forma 4k+1, atunci n se poate scrie sub forma $n=x^2+y^2$ cu $x, y \in \mathbb{N}$.

Demonstrație Totul rezultă din Teorema 1.3. şi din aceea că un produs finit de expresii de forma x^2+y^2 este de aceiaşi formă (conform identității $(x^2+y^2)(z^2+t^2)=(xz+yt)^2+(xt-yz)^2$). ■

Vom demonstra acum că scrierea unui număr natural ca sumă de două pătrate de numere naturale este unică, dacă nu ținem cont de ordinea termenilor.

În fapt, vom demonstra o propoziție mai generală :

PROPOZIȚIA 1.5. Fie $a, b \in \mathbb{N}$. Dacă un număr natural prim p se scrie sub forma $p=ax^2+by^2$ cu $x, y \in \mathbb{N}$ atunci această scriere este unică (cu convenția ca în cazul în care $a=b=1$ să nu ținem cont de ordinea termenilor).

Demonstrație Să presupunem că p are două descompuneri: $p=ax^2+by^2= ax_1^2 + by_1^2$ cu $x, y, x_1, y_1 \in \mathbb{N}$.

Atunci $p^2=(axx_1+byy_1)^2+ab(xy_1-yx_1)^2=(axx_1-byy_1)^2+ab(xy_1+yx_1)^2$ şi cum $(axx_1+byy_1)(xy_1+yx_1)=(ax^2+by^2)x_1y_1+\left(ax_1^2 + by_1^2\right)xy=p(x_1y_1+xy)$ deducem că $p \mid axx_1+byy_1$ sau $p \mid xy_1+yx_1$.

Dacă $p \mid axx_1+byy_1$, atunci din prima reprezentare a lui p deducem că $xy_1-yx_1=0$ şi deci $xy_1=yx_1$, $p=axx_1+byy_1$, $px=(ax^2+by^2)x_1=px_1$, de unde $x=x_1$ şi atunci $y=y_1$.

Dacă $p \mid xy_1+yx_1$, atunci din a doua reprezentare a lui p deducem că $axx_1-byy_1=0$ şi $p^2=ab(xy_1+yx_1)^2$, de unde $a=b=1$.

Vom avea deci $p=xy_1+yx_1$ şi $xx_1-yy_1=0$, de unde $px=(x^2+y^2)y_1=py_1$, adică $x=y_1$ şi din $p=x^2+y^2= x_1^2 + y_1^2$, deducem că $y=x_1$ (astfel că în acest caz descompunerile se pot deosebi doar prin ordinea termenilor). ■

Observații 1. Din propoziția de mai înainte deducem că dacă numărul natural n poate fi reprezentat în cel puțin două moduri diferite ca sumă de două

pătrate de numere naturale (cu condiția să nu considerăm diferite descompunerile ce se deosebesc numai prin ordinea termenilor), atunci cu necesitate n nu este prim.

De exemplu, din egalitățile $2501=1^2+50^2=10^2+49^2$ deducem că numărul 2501 nu este prim.

2. Dacă numărul n are doar o singură descompunere într-o sumă de două pătrate de numere naturale, nu rezultă cu necesitate că n este prim.

De exemplu, se demonstrează cu uşurință că numerele 10, 18 şi 45 au descompuneri unice sub forma $10=1^2+3^2$, $18=3^2+3^2$, $45=3^2+6^2$ şi totuşi ele nu sunt numere prime (se subânțelege că nu am ținut cont de ordinea termenilor).

Putem acum răspunde la chestiunea P_1 formulată la începutul paragrafului :

<u>TEOREMA 1.6. (Fermat-Euler)</u> Un număr natural n (scris sub forma $n=2^k n_1 n_2$ ca la începutul paragrafului) se poate scrie sub forma $n=x^2+y^2$ cu $x, y\in\mathbb{N}$ dacă şi numai dacă toți exponenții s din scrierea lui n_2 sunt numere pare.

<u>Demonstrație</u> Revenim la scrierea lui n sub forma $n=2^k n_1 n_2$ cu $k\in\mathbb{N}$, $n_1 = \prod_{\substack{p\ prim\\ p\equiv 1\ (4)}} p^r$ şi $n_2 = \prod_{\substack{q\ prim\\ q\equiv 3\ (4)}} q^s$.

Cum $2=1^2+1^2$ iar conform Teoremei 1.3. fiecare factor prim $p\equiv 1(4)$ din scrierea lui n_1 se scrie sub forma x^2+y^2 cu $x, y\in\mathbb{N}$ deducem imediat că n_1 se poate scrie sub aceiaşi formă şi aceiaşi proprietate o va avea şi $2^k n_1$ (adică $2^k n_1=z^2+t^2$ cu $z, t\in\mathbb{N}$).

Dacă presupunem că fiecare exponent s din scrierea lui n_2 este par, atunci în mod evident $n_2=m^2$ cu $m\in\mathbb{N}$ şi atunci $n=2^k n_1 n_2= =(z^2+t^2)m^2=(zm)^2+(tm)^2$.

Reciproc, fie $n\in\mathbb{N}$ ce se poate scrie sub forma $n=x^2+y^2$ cu $x, y\in\mathbb{N}$ şi să demonstrăm că dacă q^s este cea mai mare putere a unui număr prim $q\equiv 3(4)$ ce intră în descompunerea în factori primi a lui n (de fapt a lui n_2) atunci cu necesitate s este par. Presupunem prin absurd că s este impar. Dacă $d=(x, y)$, atunci $d^2|n$ şi dacă notăm $x_1 = \frac{x}{d}$ şi $y_1 = \frac{y}{d}$, $n_1 = \frac{n}{d^2}$ obținem că $n_1 = x_1^2 + y_1^2$ cu $(x_1, y_1)=1$.

Conform presupunerii s este impar iar d^2 (prin care am împărțit egalitatea $n=x^2+y^2$) conține eventual o putere pară a lui q, deducem că $q|n_1$ şi că q nu divide simultan pe x_1 şi y_1 (să zicem că $q\nmid y_1$).

Privind acum egalitatea $n_1 = x_1^2 + y_1^2$ în $\mathbb{Z}_q$ deducem că $0 = x_1^2 + y_1^2$ şi cum am presupus că $q\nmid y_1$ deducem că $0 = x_1^2 \cdot \left(y_1^{-1}\right)^2 + 1 \Leftrightarrow \left(x_1 \cdot y_1^{-1}\right)^2 = -1$ de unde $\left(\frac{-1}{q}\right) = \left(\frac{\left(x_1 \cdot y_1^{-1}\right)^2}{q}\right) = 1$.

Însă în cadrul Capitolului 9 am stabilit că $\left(\frac{-1}{q}\right) = (-1)^{q-1/2}$ şi cum $q\equiv 3(4)$ deducem că $\frac{q-1}{2}$ este impar, astfel că $\left(\frac{-1}{q}\right) = -1$, absurd.

Deci s este par. Raționând inductiv deducem că toți exponenții s din descompunerea lui n_2 sunt pari şi cu aceasta teorema este demonstrată. ■

Pentru a răspunde la chestiunea P_2 de la începutul paragrafului avem nevoie să reamintim anumite chestiuni legate de aritmetica întregilor lui Gauss. $\mathbb{Z}[i]=\{a+bi \mid a, b\in\mathbb{Z}\}$.

Se cunoaşte faptul că ($\mathbb{Z}[i]$, +, ·) este un inel comutativ în care $U(\mathbb{Z}[i], +, \cdot) =\{\pm 1, \pm i\}$, precum şi faptul că elementele prime din $\mathbb{Z}[i]$ sunt (până la o multiplicare cu ± 1 sau $\pm i$) următoarele :

1) $1\pm i$

2) Numerele prime p din $\mathbb{Z}$ cu $p\equiv 3(4)$

3) Numerele de forma a+bi cu a, b $\in\mathbb{N}^*$ şi $a^2+b^2=p$, unde p este un număr natural prim şi $p\equiv 1(4)$.

Reamintim că descompunerea numerelor din $\mathbb{Z}[i]$ în factori primi este unică (în ipoteza că nu se ține seama de multiplicările cu ± 1, $\pm i$, şi de ordinea factorilor).

Pentru $z=a+bi\in\mathbb{Z}[i]$ definim *norma* lui z prin $N(z)=a^2+b^2$. Evident, dacă $N(z)=p$ cu p prim, $p\equiv 1(4)$, atunci $a\neq b$ (căci în caz contrar $p=2a^2\equiv 0(2)$).

Fie acum $n\in\mathbb{N}$ pe care îl scriem sub forma $n=2^k n_1 n_2$ cu $k\in\mathbb{N}$, $n_1 = \prod_{\substack{p\ prim\\ p\equiv 1\ (4)}} p^r$ iar $n_2 = \prod_{\substack{q\ prim\\ q\equiv 3\ (4)}} q^s$. Atunci descompunerea lui n în factori primi în $\mathbb{Z}[i]$ va fi : $n = \left[(1+i)(1-i)\right]^k \cdot \prod_{\substack{a^2+b^2=p\\ p\ prim\\ p\equiv 1\ (4)}} \left[(a+bi)(a-bi)\right]^r \cdot \prod_{\substack{q\ prim\\ q\equiv 3\ (4)}} q^s$ (unde r şi s variază o dată cu p şi q).

Ţinând cont de unicitatea descompunerii lui n de mai înainte deducem că fiecărei reprezentări a lui n sub forma $n=u^2+v^2=(u+iv)(u-iv)$ (cu $u, v\in\mathbb{Z}$) îi corespund pentru u+iv şi u-iv descompuneri de forma :

$$(\star)\quad u+iv = i^t\cdot(1+i)^{k_1}(1-i)^{k_2}\prod\left[(a+bi)^{r_1}(a-bi)^{r_2}\right]\cdot\prod q^{s_1}$$

$$(\star\star)\quad u-iv = i^{-t}\cdot(1+i)^{k_2}(1-i)^{k_1}\prod\left[(a+bi)^{r_2}(a-bi)^{r_1}\right]\cdot\prod q^{s_2}$$

cu $t\in\{0, 1, 2, 3\}$, $k_1+k_2=k$, $r_1+r_2=r$ şi $s_1+s_2=s$.

Observăm că factorii primi asociaţi lui u+iv determină în mod unic factorii primi ai lui u-iv (şi reciproc).

De asemenea, fiecare pereche de numere complex conjugate (u+iv, u-iv) cu $u, v\in\mathbb{Z}$ dată de relaţiile $(\star)$ şi $(\star\star)$ de mai sus verifică egalitatea $n=u^2+v^2$.

Observăm de asemenea că schimbarea $i\to -i$ nu afectează factorii reali q astfel că $s_1=s_2$ iar $s=2s_1$ (ţinând cont de Teorema 1.6.).

Pentru alegerea lui t avem 4 posibilităţi (căci $t\in\{0, 1, 2, 3\}$). Pentru k_1 avem k+1 posibilităţi de alegere (căci $k_1\in\{0, 1, \dots, k\}$) iar pentru k_1 ales, k_2 se determină din $k_2=k-k_1$.

Analog, pentru r_1 avem r+1 posibilităţi de alegere (căci $r_1\in\{0, 1, .., r\}$) iar $r_2=r-r_1$.

Astfel, avem un număr total de $4(k+1)\prod(r+1)$ posibilităţi de a asocia lui u+iv factorii primi Gauss din descompunerea lui n în factori primi (în $\mathbb{Z}[i]$) (unde produsul $\prod(r+1)$ se face după toţi primii $p\equiv 1(4)$ a.î. $p^r|n$).

Să vedem câte dintre aceste asocieri sunt diferite.

Ţinând cont de egalitatea $1+i=i\cdot(1-i)$, dacă avem un factor $(1+i)^{k_1}(1-i)^{k_2}$ atunci acesta devine

$i^{k_1}(1-i)^{k_1}(1-i)^{k_2} = i^{k_1}(1-i)^{k_1+k_2} = i^{k_1}(1-i)^{k}$ astfel că numărul căutat este de fapt $4\prod_{\substack{p\ prim\\ p^r \mid n}}(1+r) = d(n_1)$ (căci $n_1 = \prod_{\substack{p\ prim\\ p\equiv 1\ (4)}} p^r$).

Din cele de mai înainte deducem că numărul total de soluții întregi ale ecuației $x^2+y^2=n$ este $4d(n_1)$.

Să arătăm acum că $d(n_1)=d_1(n)-d_3(n)$.

Pentru aceasta să observăm că numărul divizorilor impari ai lui n este egal cu numărul termenilor sumei

$$\sum_{\substack{0\le m_i\le r_i\\ 0\le k_j\le s_j}} p_1^{m_1}\cdot p_2^{m_2}\cdot\ldots\cdot p_n^{m_n}\cdot q_1^{k_1}\cdot\ldots\cdot q_t^{k_t} =$$

$$= \prod_{\substack{p^r \mid n\\ p\ prim\\ p\equiv 1\ (4)}}\left(1+p+..+p^r\right)\cdot \prod_{\substack{q^s \mid n\\ q\ prim\\ q\equiv 3\ (4)}}\left(1+q+\ldots+q^s\right) \qquad (\star\star\star)$$

Dacă $d \mid n$, atunci este clar că avem $d\equiv 1(4)$ dacă şi numai dacă în $(\star\star\star)$ $\sum_{j=1}^{t} k_j$ este par, în caz contrar având $d\equiv 3(4)$.

Dacă înlocuim pe q cu –1 atunci produsul $\prod_{\substack{q^s \mid n\\ q\ prim\\ q\equiv 3\ (4)}}\left(1+q+\ldots+q^s\right)$ este zero chiar dacă un singur exponent s este impar ; dacă toți acești exponenți s sunt pari atunci $\prod_{\substack{q^s \mid n\\ q\ prim\\ q\equiv 3\ (4)}}\left(1+q+\ldots+q^s\right)=1$ şi astfel membrul drept din $(\star\star\star)$ devine $\prod_{\substack{p^r \mid n\\ p\equiv 1\ (4)}}\left(1+p+\ldots+p^r\right)$ astfel că termenii dezvoltării acestui produs sunt exact toți divizorii lui n_1. Pentru a obține $d(n_1)$ fiecare termen trebuie să fie numărat ca 1. Acest lucru este uşor de realizat dacă în $(\star\star\star)$ înlocuim în partea dreaptă şi pe p cu 1, obținând $\prod_{\substack{p^r \mid n\\ p\ prim\\ p\equiv 1\ (4)}}(1+r)$. Dacă privim acum membrul stâng al egalității $(\star\star\star)$ după ce în partea dreaptă am înlocuit fiecare p cu 1 şi fiecare q cu –1

este clar că fiecare d|n, d≡1(4) este numărat ca +1 şi fiecare d|n, d≡3(4) este numărat ca –1.

Astfel membrul stâng din $(\star\star\star)$ devine $d_1(n)-d_3(n)$ iar membrul drept $d(n_1)$, de unde egalitatea $d(n_1)=d_1(n)-d_3(n)$.

Sumând cele expuse până aici obţinem următorul rezultat ce include şi Teorema 1.6. (Fermat –Euler) :

<u>TEOREMA 1.7.</u> Fie $n\in\mathbb{N}^*$ iar $n=2^k n_1 n_2$ (cu $k\in\mathbb{N}$, $n_1=\prod_{\substack{p\mid n\\ p\ prim\\ p\equiv 1\ (4)}} p^r$ şi $n_2=\prod_{\substack{q\mid n\\ q\ prim\\ q\equiv 3\ (4)}} q^s$) descompunerea lui n în factori primi.

Atunci ecuaţia $x^2+y^2=n$ are soluţie în $\mathbb{Z}$ dacă şi numai dacă toţi exponenţii s din descompunerea lui n_2 sunt pari.

Numărul soluţiilor din $\mathbb{Z}\times\mathbb{Z}$ ale ecuaţiei $x^2+y^2=n$ este egal cu $4(d_1(n)-d_3(n))$ unde $d_a(n)$ este numărul divizorilor d ai lui n cu proprietatea că $d\equiv a(4)$, $a=1, 3$.

<u>Exemple</u> 1. Dacă n=1, atunci $d_1(1)=1$ şi $d_2(1)=0$, astfel că în $\mathbb{Z}\times\mathbb{Z}$ ecuaţia $x^2+y^2=1$ va avea 4(1-0)=4 soluţii.

2. Dacă n=2, atunci $d_1(2)=1$ şi $d_2(2)=0$, astfel că în $\mathbb{Z}\times\mathbb{Z}$ ecuaţia $x^2+y^2=2$ va avea 4(1-0)=4 soluţii.

3. Dacă n=5, atunci $d_1(5)=2$ şi $d_2(5)=0$, astfel că în $\mathbb{Z}\times\mathbb{Z}$ ecuaţia $x^2+y^2=5$ va avea 4(2-0)=8 soluţii. (Se confirmă astfel cele stabilite la exemplele 1)-3) de la începutul paragrafului 1).

4. Am văzut mai înainte (Teorema 1.3.) că dacă p este un număr prim de forma 4k+1, atunci există x, $y\in\mathbb{N}^*$ a.î. $p=x^2+y^2$.(cum $d_1(p)=2$ iar $d_2(p)=0$, conform teoremei 1.7. ecuaţia $x^2+y^2=p$ va avea în $\mathbb{Z}\times\mathbb{Z}$ 4(2-0)=8 soluţii. Se reconfirmă concluzia de la observaţia de la începutul paragrafului 1, cazul iv)).

În continuare vom prezenta o metodă de găsire a numerelor x, y atunci când se dă p (metodă dată de Lagrange în anul 1808, după ce, tot el demonstrase în 1785 că lungimea perioadei pentru funcţia continuă a lui $\sqrt{p}$ este impară pentru numerele prime p de forma 4k+1).

Pentru aceasta să ne reamintim că la capitolul de fracții continue a fost prezentat următorul algoritm de dezvoltare în fracție continuă a unui irațional pătratic $\alpha=\sqrt{D}$:

Punem $a_0=\left[\sqrt{D}\right]$, $b_0=0$, $c_0=1$ şi apoi construim prin recurență

$$a_{n+1}=\left[\frac{a_0+b_{n+1}}{c_{n+1}}\right],\quad b_{n+1}=a_nc_n-b_n \text{ şi } c_{n+1}=\frac{D-b_{n+1}^2}{c_n}.$$

Calculul se continuă până când $b_{n+1}=b_n$ sau $c_{n+1}=c_n$.

i) Dacă $b_{n+1}=b_n$, atunci $\sqrt{D}=\left[a_0;\overline{a_1,...,a_{n-1},a_n,a_{n-1},...,a_1,2a_0}\right]$ (adică lungimea perioadei minime este pară).

ii) Dacă $c_{n+1}=c_n$, atunci $\sqrt{D}=\left[a_0;\overline{a_1,...,a_n,a_n,...,a_1,2a_0}\right]$ (adică lungimea perioadei minime este impară).

Numerele b_n şi c_n de mai sus sunt cele din scrierea lui $\alpha_n=\dfrac{b_n+\sqrt{D}}{c_n}$.

Să trecem acum la rezolvarea ecuației $x^2+y^2=p$, cu p un număr prim de forma 4k+1 (de exemplu în $\mathbb{N}\times\mathbb{N}$).

După cum am amintit mai sus, lungimea perioadei minime pentru fracția continuă a lui $\sqrt{p}$ este impară .

Deci $\sqrt{p}=\left[a_0;\overline{a_1,...,a_n,a_n,...,a_1,2a_0}\right]$.

Numărul $\alpha_{n+1}=\left[\overline{a_n;a_{n-1},...,a_1,2a_0,a_1,...,a_n}\right]$ are perioada simetrică, deci - ținând cont de Propoziția 3.14. de la Capitolul 10 - deducem că $\alpha_{n+1}\cdot\widetilde{\alpha}_{n+1}=-1$ (notațiile sunt cele de la Capitolul 10).

Pe de altă parte, $\alpha_{n+1}=\dfrac{b_{n+1}+\sqrt{p}}{c_{n+1}}$, $\widetilde{\alpha}_{n+1}=\dfrac{b_{n+1}-\sqrt{p}}{c_{n+1}}$ astfel că obținem

$$\frac{b_{n+1}+\sqrt{p}}{c_{n+1}}\cdot\frac{b_{n+1}-\sqrt{p}}{c_{n+1}}=-1\Leftrightarrow b_{n+1}^2+c_{n+1}^2=p$$

şi astfel (b_{n+1} , c_{n+1}) este singura soluție din $\mathbb{N}\times\mathbb{N}$ a ecuației $x^2+y^2=p$ (evident dacă nu ținem cont de ordinea termenilor).

Exemplu Să se rezolve ecuația $x^2+y^2=1009$ în $\mathbb{N}\times\mathbb{N}$.

Evident, numărul p =1009 este prim de forma 4k+1.

Avem a_0=31, b_0=0, c_0=1 şi apoi $b_1 = a_0c_0 - b_0 = 31$,

$c_1 = \frac{1009 - b_1^2}{c_0}$=48, $a_1 = \left[\frac{31+31}{48}\right] = 1$,

$b_2 = a_1c_1 - b_1 = 17,\ \ c_2 = \frac{1009 - b_2^2}{c_1} = 15,\ \ a_2 = \left[\frac{31+17}{15}\right] = 3,$

$b_3 = a_2c_2 - b_2 = 28,\ \ c_3 = \frac{1009 - 28^2}{15} = 15 = c_2$.

Prin urmare suntem în cazul ii) astfel că $\sqrt{1009} = \left[31;\overline{1,3,3,1,6,2}\right]$ şi $\alpha_3 = \frac{28+\sqrt{1009}}{15}$ aşa încât $28^2+15^2=1009$, deci în acest caz soluţia ecuaţiei $x^2+y^2=1009$ din $\mathbb{N}\times\mathbb{N}$ este (15, 28) (dacă nu ţinem cont de ordinea termenilor).

§2 Reprezentarea numerelor naturale ca sumă de patru pătrate de numere întregi.

Scopul acestui paragraf este acela de a demonstra că orice număr natural poate fi scris ca sumă a patru pătrate de numere întregi.

Ţinând cont de identitea lui Euler, potrivit căreia dacă $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$, atunci

$$\left(x_1^2+x_2^2+x_3^2+x_4^2\right)\left(y_1^2+y_2^2+y_3^2+y_4^2\right) = \left(x_1y_1+x_2y_2+x_3y_3+x_4y_4\right)^2 +$$
$$+\left(x_1y_2-x_2y_1+x_3y_4-x_4y_3\right)^2+\left(x_1y_3-x_3y_1+x_4y_2-x_2y_4\right)^2 +$$
$$+\left(x_1y_4-x_4y_1+x_2y_3-x_3y_2\right)^2$$

pentru a demonstra că un număr natural se scrie ca sumă de patru pătrate de numere naturale, este suficient să probăm lucrul acesta pentru numere prime.

TEOREMA 2.1. (Lagrange) Fie p este un număr prim; atunci:

(1) Există m şi $x_1, x_2, x_3, x_4 \in \mathbb{N}$ a.î. $m \cdot p = x_1^2+x_2^2+x_3^2+x_4^2$ **$(1 \le m < p)$**

(2) Dacă m este cel mai mic număr natural ce verifică (1), atunci m=1.

Demonstraţie Pentru a proba (1), să considerăm mulţimile :

$$X = \left\{ x^2 \,\middle|\, x = 0,\ 1,\ 2,..., \frac{p-1}{2} \right\} \quad \text{şi}$$

$$Y=\left\{-x^2-1 \;\middle|\; x=0,\ 1,\ 2,...,\frac{p-1}{2}\right\}.$$

Să observăm că elementele lui X şi Y nu sunt congruente două câte două modulo p (separat).

Într-adevăr, dacă există $x_1,x_2\in\left\{0,\ 1,...,\frac{p-1}{2}\right\}$ a.î. $x_1^2\equiv x_2^2\pmod p$ cu $x_1>x_2\Rightarrow p|(x_1-x_2)(x_1+x_2)$ ceea ce este imposibil deoarece $1\le x_1+x_2\le p-1$.

Analog se arată că elementele lui Y nu sunt congruente două câte două modulo p. Dacă notăm prin | X | numărul de elemente ale lui X modulo p, atunci cum $|X|+|Y|=\frac{p+1}{2}+\frac{p+1}{2}=p+1>p$, deducem că există x, $y\in\left\{1,\ 2,...,\frac{p-1}{2}\right\}$ a.î. $x^2\equiv -y^2-1 \pmod p$, altfel zis există $m\in\mathbb{N}$ a.î. $mp=x^2+y^2+1$.

Clar

$$1\le m=\frac{1}{p}\left(x^2+y^2+1\right)\le\frac{1}{p}\left[2\left(\frac{p-1}{2}\right)^2+1\right]=\frac{p-1}{p}\cdot\frac{p-1}{2}+\frac{1}{p}<\frac{p-1}{2}+\frac{1}{p}<p.$$

Pentru a proba (2) să observăm că dacă m este par, atunci sau toate x_i-urile sunt impare sau două .

Dacă toate x_i-urile sunt impare, atunci egalitatea de la (1) se mai scrie sub forma: $\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2=\frac{m}{2}\cdot p$ iar cum $x_1\pm x_2$ şi $x_3\pm x_4$ sunt numere pare se contrazice minimalitatea lui m.

Dacă numai x_1 şi x_2 sunt pare iar x_3 şi x_4 sunt impare, din nou se contrazice minimalitatea lui m (căci din nou $x_1\pm x_2$ şi $x_3\pm x_4$ sunt numere pare).

Analog dacă x_i-urile sunt pare.

Deci m trebuie să fie impar.

Dacă m=1 nu avem ce demonstra.

Să presupunem deci că $3\le m<p$.

Alegem y_1, y_2, y_3, y_4 a.î. $x_i\equiv y_i\ (m)$, $-\frac{m-1}{2}\le y_i\le\frac{m-1}{2}$, i=1, 2, 3, 4 şi în mod evident $y_1^2+y_2^2+y_3^2+y_4^2\equiv 0\ (m)$, deci $mn=y_1^2+y_2^2+y_3^2+y_4^2$ pentru un anumit n. Mai mult, $0\le n\le\frac{4}{m}\cdot\left(\frac{m-1}{2}\right)^2<m$.

Evident, $n \neq 0$ (căci în caz contrar ar rezulta $y_j = 0$ pentru orice j=1, 2, 3, 4, ceea ce ar implica $x_j \equiv 0(m)$, j=1, 2, 3, 4, şi deci $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0 \ \left(m^2\right)$, de unde p≡0(m), ceea ce este imposibil deoarece 3≤m<p).

Deci n≥1 şi deducem imediat că

$m^2 np = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) = z_1^2 + z_2^2 + z_3^2 + z_4^2$, unde

$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, $z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$

$z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4$, $z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2$

Cum $x_i \equiv y_i$ (m), $\left(-\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2}\right)$, i=1, 2, 3, 4, deducem că $m|z_j$, j=2, 3, 4 şi din egalitatea de mai sus rezultă că $m|z_1$.

Avem deci că $np = \left(\frac{z_1}{m}\right)^2 + \left(\frac{z_2}{m}\right)^2 + \left(\frac{z_3}{m}\right)^2 + \left(\frac{z_4}{m}\right)^2$, ceea ce din nou contrazice minimalitatea lui m.(căci n<m).

În concluzie m=1 şi totul este acum clar. ■

§3. Alte teoreme de reprezentare a numerelor întregi

TEOREMA 3.1. (Erdös-Suranyi)

Orice număr $k \in \mathbb{Z}$ se poate scrie într-o infinitate de moduri sub forma $k = \pm 1^2 \pm 2^2 \pm \ldots \pm m^2$ cu $m \in \mathbb{N}$.

Demonstraţie Facem inducţie matematică observând că este suficient să presupunem $k \in \mathbb{N}$.

Observăm că
$0 = 1^2 + 2^2 - 3^2 + 4^2 - 5^2 - 6^2 + 7^2$
$1 = 1^2$
$2 = -1^2 - 2^2 - 3^2 + 4^2$
$3 = -1^2 + 2^2$
$4 = -1^2 - 2^2 + 3^2$

Să presupunem acum că pentru un $k \in \mathbb{N}$ avem $k = \pm 1^2 \pm 2^2 \pm \ldots \pm m^2$.

Cum $(m+1)^2 - (m+2)^2 - (m+3)^2 + (m+4)^2 = 4$, avem
$k+4 = \pm 1^2 \pm 2^2 \pm \ldots \pm m^2 + (m+1)^2 - (m+2)^2 - (m+3)^2 + (m+4)^2$ şi astfel teorema este demonstrată.

Infinitatea descompunerii rezultă din identitatea

$(m+1)^2 - (m+2)^2 - (m+3)^2 + (m+4)^2 - (m+5)^2 + (m+6)^2 + (m+7)^2 - (m+8)^2 = 0$ şi astfel în descompunerea lui k înlocuim pe m cu m+8 ş.a.m.d. ■

În legătură cu alte tipuri de reprezentări ale numerelor întregi recomandăm cititorului lucrarea lui **Emil Grosswald : „Representations of Integers as Sums of Squares", Springer-Verlag, 1985.**

Printre alte rezultate, în cartea respectivă se prezintă şi următoarele:

<u>TEOREMA 3.2.</u> Un număr natural n se poate scrie sub forma $n=x^2+y^2+z^2$, cu x, y, z$\in\mathbb{Z}$ dacă şi numai dacă n nu este de forma $4^k(8m+7)$ cu k, m$\in\mathbb{N}$.

<u>TEOREMA 3.3.</u> Numărul soluţiilor întregi (x, y, z) ale ecuaţiei $x^2+y^2+z^2=n$ este dat de $\frac{16}{\pi}\sqrt{n}\cdot L(1,\chi)\ q(n)\ P(n)$, unde $n=4^a n_1$, ($4\nmid n_1$),

$$q(n)=\begin{cases} 0 \ \ daca \ \ n_1\equiv 7 \ \ (8) \\ 2^{-a} \ \ daca \ \ n_1\equiv 3 \ \ (8) \\ 3\cdot 2^{-a-1} \ \ daca \ \ n_1\equiv 1,\ 2,\ 5 \ \ sau \ \ 6 \ \ (8) \end{cases}$$

$$P(n)=\prod_{\substack{p \ prim\geq 3 \\ p^{2b}\mid n}}\left(1+\sum_{j=1}^{b-1}p^{-j}+p^{-b}\left\{1-\left(\frac{\left(-n/p^{2b}\right)}{p}\right)\cdot\frac{1}{p}\right\}^{-1}\right)$$

(P(n)=1 dacă n nu conţine pătrate), iar $L(s,\chi)=\sum_{m=1}^{\infty}\chi(m)\ m^{-s}$, cu $\chi(m)=\left(\frac{-4n}{m}\right)$ (simbolul lui Jacobi !).

Demonstraţiile acestor teoreme fiind destul de laborioase am renunţat la prezentarea lor în detaliu limitându-ne doar la a le semnala. (cititorul interesat le poate găsi în cartea citată mai sus).

<u>TEOREMA 3.4. (H.E.Richert)</u> Orice număr natural n>6 se poate scrie ca sumă de diferite numere prime.

Demonstrație Pentru a demonstra teorema lui Richert avem nevoie de două rezultate preliminare:

Lema 1. Fie $m_1, m_2,\ldots$ un şir infinit crescător de numere naturale a.î. pentru un $k\in\mathbb{N}$, (1) $m_{i+1}\le 2m_i$ pentru orice $i>k$.

Presupunem că există $a\in\mathbb{N}$ şi r, $s_{r-1}\in\mathbb{N}$ a.î. $s_{r-1}\ge m_{k+r}$ a.î. fiecare dintre numerele :

(2) $a+1, a+2, \ldots, a+s_{r-1}$ este suma diferitelor numere din şirul $m_1, m_2, \ldots, m_{k+r-1}$.

Atunci fiecare dintre numerele:

(3) $a+1, a+2, \ldots, a+s_r$ este suma diferitelor numere din şirul $m_1, m_2, \ldots, m_{k+r}$ şi mai mult, $s_r\ge m_{k+r+1}$.

Într-adevăr, fie n un număr din şirul (3). Dacă $n\le a+s_{r-1}$ nu mai avem ce demonstra deoarece conform ipotezei n este sumă de diferiți termeni ai şirului $m_1, m_2, \ldots, m_{k+r-1}$.

Să presupunem că $n>a+s_{r-1}$.Cum $s_{r-1}\ge m_{k+r}$, avem $n\ge a+1+m_{k+r}$, deci $n-m_{k+r}\ge a+1$, adică numărul $n-m_{k+r}$ este un termen al şirului (2) şi în consecință se va scrie ca sumă de termeni din şirul $m_1, m_2, \ldots, m_{k+r-1}$. Rezultă că şi n este atunci sumă de diferiți termeni din şirul $m_1, m_2, \ldots, m_{k+r}$. Mai mult, ținând cont de (1) deducem că $m_{r+k+1}\le 2m_{k+r}$ şi astfel $s_r=s_{r-1}+m_{k+r}\ge 2m_{k+1}\ge m_{k+r+1}$. Astfel Lema 1 este probată.

Lema 2. Fie $m_1, m_2,\ldots$ un şir infinit de numere naturale a.î. (1) are loc pentru un număr natural k, şi există s_0, $a\in\mathbb{N}$ a.î. $s_0\ge m_{k+1}$ a.î. fiecare dintre numerele

(4) $a+1, a+2, \ldots, a+s_0$ este sumă de diferiți termeni din şirul $m_1, m_2, \ldots, m_k$.

Atunci orice număr natural >a se scrie ca sumă de termeni ai şirului $m_1, m_2,\ldots$

Într-adevăr, conform Lemei 1 (cu r=1, 2, …, t, $t\in\mathbb{N}$) fiecare dintre numerele

(5) $a+1, a+2, \ldots, a+s_t$ se scrie ca sumă de termeni din şirul $m_1, m_2, \ldots, m_{k+t}$. Cum însă $s_r>s_{r-1}$, r=1, 2, …t, observăm că pentru orice număr natural n există un număr natural t a.î. $n\le a+s_t$.

În consecință orice număr natural n>a este unul dintre termenii şirului (5) cu t convenabil ales şi astfel va fi sumă de diferiți termeni din şirul $m_1, m_2, \ldots$

Cu aceasta Lema 2 este şi ea probată.

Să revenim acum la demonstrația teoremei.

Fie $m_i=p_i$ cu i=1, 2, …(p_i-fiind al i-ulea număr prim). Conform Corolarului 3.21. de la Capitolul 7, numerele m_i verifică condițiile Lemei 2 (cu a=6, s_0=13, k=5). Aceasta deoarece $13=p_6$ şi fiecare dintre numerele 7, 8, …, 19

se scriu ca sumă de diferite numere prime, $\leq p_5=11$ după cum urmează: 7=2+5, 8=3+5, 9=2+7, 10=3+7, 11=11, 12=5+7, 13=2+11, 14=3+11, 15=3+5+7, 16=5+11, 17=2+3+5+7, 18=7+11, 19=3+5+11.

Teorema rezultă acum ca o consecință imediată a Lemei 2. ■

COROLARUL 3. 5. Orice număr natural $n\geq 10$ se poate scrie ca sumă de diferite numere prime impare.

Demonstrație Într-adevăr, dacă alegem $m_i=p_{i+1}$ atunci condițiile Lemei 2 de la demonstrația Teoremei 3.4. sunt satisfăcute (cu a=9, $s_0=19$, k=6), deoarece $19=p_8=m_7$, deci $s_0=m_{6+1}$ şi mai mult, fiecare dintre numerele 10, 11, …, 28 se scriu ca sumă de diferite numere prime impare, $\leq m_6=19$ după cum urmează: 10=3+7, 11=11, 12=5+7, 13=13, 14=3+11, 15=3+5+7, 16=5+11, 17=17, 18=5+13, 19=3+5+11, 20=7+13, 21=3+5+13, 22=5+17, 23=3+7+13, 24=11+13, 25=5+7+13, 26=3+5+7+11, 28=3+5+7+13.

Observație: În lucrarea **A. Macowski, Partitions into unequal primes** din **Bull. Acad. Sci. Sér. Sci. Math. Astr. Phys., 8(1960), pp. 125-126** se demonstrează următoarele rezultate :

TEOREMA 3.6. Orice număr natural $n>55$ se poate scrie ca sumă de diferite numere prime de forma 4k-1.

TEOREMA 3.7. Orice număr natural $n>121$ se poate scrie ca sumă de numere prime de forma 4k+1.

TEOREMA 3.8. Orice număr natural $n>161$ se poate scrie ca sumă de numere prime de forma 6k-1.

TEOREMA 3.9. Orice număr natural $n>205$ se poate scrie ca sumă de numere prime de forma 6k+1.

Să mai amintim şi un rezultat al lui L. Schnirelman:

TEOREMA 3.10. (Schnirelman) Există un număr natural s a.î. orice număr natural mai mare sau egal cu 2 se scrie ca suma a cel mult s numere prime (nu neapărat distincte).

Cititorul poate găsi demonstrația acestei teoreme în lucrarea [21, pp.107] (preluată după articolul original al lui **Schnirelman: Uber additive Eigeenschaften von Zahlen** din **Math. Ann. 107, 1933, pp. 649-690).**

În lucrarea lui **Vinogradov: Representation of an odd number as a sum of three primes** din **Comptes Rendus (Doklady) de l'Academie de Sciences de l' URSS , nr 15, 1937, pp. 191-294,** se demonstrează (din păcate neelementar):

TEOREMA3.11. (Vinogradov) Orice număr natural impar suficient de mare se scrie ca sumă a cel mult trei numere prime.

Din Teoremele lui Schnirelman şi Vinogradov deducem imediat:

COROLARUL 3.12. Există $n_0 \in \mathbb{N}$, $n_0 \geq 2$, a.î. orice număr natural n, $n \geq n_0$ se scrie ca suma a cel mult patru numere prime.

Observații **1.** Shapiro **şi** Warga **în lucrarea:** On representation of large integers as sums of primes **din** Comm. Pure Appl. Math, 3, 1950, p. 153 **demonstrează elementar un rezultat mai slab:** orice număr natural suficient de mare se scrie ca suma a cel mult 20 de numere prime.

2. Rafinând procedeul lui Schnirelman, **Yin Wen-Lin**, în lucrarea **Note on the representation of large integers as sums of primes** din **Bull. Acad. Polon. Sci. cl III, 4, 1956, pp. 793-795** demonstrează elementar că **orice număr natural suficient de mare se scrie ca suma a cel mult 18 de numere prime.**

3. Să reamintim aici şi o conjectură a lui Goldbach: **orice număr natural par mai mare sau egal cu 4 se scrie ca suma a două numere prime.**

Dacă această conjectură ar fi adevărată (lucru neprobat până acum) atunci ar rezulta că **orice număr natural mai mare sau egal cu 2 se scrie ca suma a cel mult 3 numere prime.**

CAPITOLUL 12:
ECUAŢII DIO PHANTICE

În cele ce urmează prin *ecuaţie diophantică* înţelegem o ecuaţie de forma $f(x_1,\ldots,x_n)=0$ cu $f\in\mathbb{Z}[X_1,\ldots,X_n]$.

A rezolva o astfel de ecuaţie diophantică revine la a găsi toate n-uplurile $(a_1,\ldots,a_n)\in\mathbb{Z}^n$ pentru care $f(a_1,\ldots,a_n)=0$.

Observaţie Denumirea de *ecuaţii diophantice* provine de la numele matematicianului grec Diophante (aprox. secolul III era noastră).

§1.Ecuaţia ax+by+c=0, a, b, c∈ℤ (1)

LEMA 1.1. Ecuaţia (1) are soluţie în ℤ dacă şi numai dacă d=(a, b) | c.

Demonstraţie În mod evident, dacă x, y∈ℤ a.î. ax+by+c=0, atunci cum c = -ax-by deducem că d | c ⇔ c=dt cu t∈ℤ.

Reciproc, să presupunem că d|c. Atunci din algoritmul lui Euclid deducem că există $x_1, y_1\in\mathbb{Z}$ a.î. $d=ax_1+by_1$.

Atunci $c = dt =(ax_1 + by_1)t = a(x_1t) + b(y_1t) \Leftrightarrow a(x_1t) + b(y_1t)-c = 0\Leftrightarrow$ $\Leftrightarrow a(-x_1t)+b(-y_1t)+c=0$, adică $(-x_1t, -y_1t)$ este soluţie a ecuaţiei ax + by + c = 0.■

LEMA 1.2. Dacă (a, b) =1 iar (x_0, y_0) este soluţie particulară a ecuaţiei (1), atunci soluţia generală din ℤ a acestei ecuaţii este dată de $x=x_0-kb$ şi $y=y_0+ka$, cu k∈ℤ.

Demonstraţie Dacă $x=x_0-kb$ şi $y=y_0+ka$ (cu $(x_0, y_0)\in\mathbb{Z}^2$ soluţie particulară a lui (1) şi k∈ℤ), atunci $ax+by+c=a(x_0-kb)+b(y_0+ka)+c= =ax_0+by_0+c-abk+abk=0$.

Fie acum $(x, y)\in\mathbb{Z}^2$ a.î. ax+by+c=0.

Atunci $ax_0+by_0=ax+by \Leftrightarrow a(x_0-x)=b(y-y_0)$. Cum (a, b)=1 deducem că $a|y-y_0$, adică $y-y_0=ka$ (cu k∈ℤ) ⇔ $y=y_0+ka$. Deducem imediat că $a(x_0-x)=bka$, de unde $x=x_0-kb$. ■

COROLAR 1.3. Fie a, b, c∈ℤ a.î. d=(a, b)|c, a=da′, b=db′, c=dc′.

Dacă $(x_0, y_0)\in\mathbb{Z}^2$ este o soluţie particulară a ecuaţiei $a'x+b'y+c'=0$, atunci soluţia generală a ecuaţiei (1) este dată de $x=x_0-kb'$, $y=y_0+ka'$ cu k∈ℤ.

Observaţie Ţinând cont de Lema 1.2. şi Corolarul 1.3. deducem că atunci când suntem puşi în situaţia de a rezolva o ecuaţie diophantică de forma (1) (în cazul în care d=(a, b)≠c) este recomandabil să împărţim ambii membrii ai ecuaţiei prin d, transformând-o astfel în ecuaţia echivalentă a′x+b′y+c′=0 (cu a′=a/d, b′=b/d, c′=c/d). Cum (a′, b′)=1, forma generală a soluţiilor ecuaţiei a′x+b′y+c′=0 este dată de Lema 1.2.

Să prezentăm acum un procedeu de a găsi o soluţie particulară (x_0, y_0) a ecuaţiei (1) (cu a, b, c∈ℤ, (a, b)=1). Pentru aceasta vom dezvolta numărul raţional α=a/b în fracţie continuă. Păstrând notaţiile de la Capitolul 10 (de Fracţii continue), observăm că ultima redusă p_n/q_n a lui α este chiar $p_n/q_n=a/b=\alpha$.

Ţinând cont de Propoziţia 3.3. de la Capitolul 10 putem scrie:

$$\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^{n-1}}{q_nq_{n-1}} \Leftrightarrow \frac{a}{b}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^{n-1}}{q_nq_{n-1}} \Leftrightarrow aq_{n-1}-bp_{n-1}+(-1)^{n-1}=0$$

de unde (prin înmulţire a ambilor membrii ai ultimei egalităţi cu $(-1)^n$ c)

$$a[(-1)^n c\ q_{n-1}] + b[(-1)^{n+1} c\ p_{n-1}] + c = 0.$$

Deducem că $x_0=(-1)^n c\ q_{n-1}$ şi $y_0=(-1)^{n+1} c\ p_{n-1}$ este o soluţie particulară a ecuaţiei (1).

Conform Lemei 1.2. soluţia generală a ecuaţiei (1) va fi atunci

$x=(-1)^n c\ q_{n-1}-bk$ şi $y=(-1)^{n+1} c\ p_{n-1}+ak$ cu $k\in\mathbb{Z}$.

Exemplu Să se rezolve ecuaţia diofantică (∗) $317x + 182y + 94 = 0$

Avem a=317, b=182, c=94 şi se observă că (a, b)=1, astfel că ecuaţia (∗) are soluţie în $\mathbb{Z}^2$ (conform Lemei 1.2.).

Pentru a găsi soluţia generală a ecuaţiei (∗) să găsim o soluţie particulară $(x_0, y_0)\in\mathbb{Z}^2$ a ecuaţiei (∗).

Prin calcul direct găsim următoarea dezvoltare în fracţie continuă a lui $\alpha=\frac{317}{182}:\frac{317}{182}=[1;1, 2, 1, 6, 1, 5]$.

Redusele $\alpha=\frac{317}{182}$ se obţin completând de la stânga la dreapta tabelul:

	1	1	2	1	6	1	5
α	(a_0)	(a_1)	(a_2)	(a_3)	(a_4)	(a_5)	(a_6)
p	1	1	2	5	7	47	54	317
q	0	1	1	3	4	27	31	182

Deducem că $\alpha = \frac{p_6}{q_6} = \frac{317}{182}$, adică n=6.

O soluție particulară va fi $x_0 = (-1)^n \cdot q_{n-1} = (-1)^6 \cdot 94 \cdot q_5 = 94 \cdot 31 = 2914$, $y_0 = (-1)^{n+1} \cdot p_{n-1} = (-1)^7 \cdot 94 \cdot p_5 = -94 \cdot 54 = -5076$

Astfel, soluția generală a ecuației (∗) va fi x=2914-182k, y=-5076+317k, cu $k \in \mathbb{Z}$.

§2.Ecuația $x^2 + y^2 = z^2$ (2)

În primul rând trebuie observat că dacă tripletul (x, y, z) de numere întregi verifică ecuația (2), atunci aceeaşi ecuație va fi satisfăcută de orice triplet de forma (λx, λy, λz), unde $\lambda \in \mathbb{Z}$ şi reciproc.

De aceea, pentru a găsi toate soluțiile ecuației (2) (constând din numere diferite de zero) este suficient să găsim (soluțiile (x, y, z) pentru care numerele x, y, z sunt relativ prime (adică nu au nici un divizor prim diferit de 1)).

Este clar că dacă într-o soluție (x, y, z) a ecuației (2) două dintre numerele x, y, z au un divizor comun $\lambda = \pm 1$, atunci şi cel de al treilea număr se divide cu λ.

De aceea ne putem restrânge la soluțiile ce constau din numere relativ prime două câte două, pe care le vom numi *soluții primitive*.

Dacă (x, y, z) este o soluție a lui (2), atunci în mod evident şi (y, x, z) este soluție.

Pe de altă parte, dacă (x, y, z) este soluție, atunci x sau y este par (căci dacă x şi y ar fi impare atunci x^2+y^2 ar fi de forma 4k+2, pe când pătratul unui număr întreg nu poate fi decât de forma 4k sau 4k+1).

În plus, este evident că dacă (x, y, z) este soluție, atunci şi (±x, ±y, ±z) vor fi soluții.

LEMA 2.1. **Orice soluție particulară (x, y, z) de numere naturale (cu n par) a ecuației (2) este de forma $x=2mn$, $y=m^2-n^2$, $z=m^2+n^2$ cu $m, n\in\mathbb{N}$ şi $n<m$, $(n, m)=1$ iar m, n au parități diferite** .

Demonstrație Identitatea $(2mn)^2+(m^2-n^2)^2=(m^2+n^2)^2$ arată că numerele de forma din enunț sunt soluții ale ecuației (2) cu x par. Dacă x, y, z au un divizor comun $\lambda \geq 2$, atunci λ divide şi numerele $2m^2=(m^2+n^2)^2+(m^2-n^2)^2$ şi $2n^2=(m^2+n^2)^2-(m^2-n^2)^2$.

Rezultă că $\lambda=2$ (căci $(m, n)=1$). Însă atunci m^2 şi n^2 sunt simultan pare sau impare, ceea ce este imposibil căci prin ipoteză m şi n au parități diferite. Deci soluția din enunț este primitivă.

Reciproc, fie (x, y, z) o soluție primitivă a lui (2) cu $x, y, z\in\mathbb{N}$ iar $x=2a$.

Atunci y şi z sunt impare, deci numerele z+y şi z-y sunt pare (fie $z+y=2b$, $z-y=2c$).

Orice divizor comun al lui b şi c divide pe $z=b+c$ şi pe $y=b-c$, de aceea $\lambda=\pm1$, astfel că $(b, c)=1$.

Pe de altă parte $4a^2 = x^2 = z^2 - y^2 = 4bc$, de unde $a^2 = bc$, adică $b = m^2$ şi $c= n^2$ $(m, n\in\mathbb{N})$ iar de aici $a^2=m^2n^2\Leftrightarrow a=mn$, deci $x=2a=2mn$, $y=b-c=m^2-n^2$ iar $z=b+c=m^2+n^2$ (se observă că $n<m$). ■

COROLAR 2.2. **Soluția generală a ecuației (2) este $x= 2r\cdot mn$, $y=r(m^2-n^2)$, $z=r(m^2+n^2)$ cu $r, m, n\in\mathbb{Z}$.**

§3. Ecuația $x^4+y^4=z^4$ (3).

În cadrul acestui paragraf vom demonstra un rezultat ceva mai general şi anume:

LEMA 3.1. **Ecuația $x^4+y^4=z^2$ (4) nu are soluții în $\mathbb{Z}^*$.**

Demonstrație Să presupunem că ar exista o soluție în $\mathbb{Z}^*$ a ecuației (4). Putem presupune în mod evident că această soluție constă din numere din $\mathbb{N}^*$.

Cum orice mulțime nevidă de numere naturale are un cel mai mic element, atunci printre soluțiile ecuației (4) există una (x, y, z) cu z minim.(vezi Teorema 4.5. de la Capitolul 1).

Analog ca în cazul ecuației (2) se arată că x sau y trebuie să fie par ; să presupunem că x este par.

Cum $(x^2)^2+(y^2)^2=z^2$ iar x^2, y^2 şi z sunt naturale (şi pot fi presupuse relativ prime), atunci conform celor stabilite la §2. există numerele naturale m, n, $m>n$, relativ prime şi de paritate diferită a.î. $x^2=2mn$, $y^2=m^2-n^2$ şi $z^2=m^2+n^2$.

Dacă m=2k şi n=2k+1$\Rightarrow y^2=4(k^2-l^2-l-1)+3$, ceea ce nu se poate (căci y^2 trebuie să fie de forma 4k sau 4k+1).

Rezultă că m este impar iar n este par.

Fie n=2q; atunci $x^2=4mn$ aşa că $mq=(x/2)^2$. Cum (m, n)=1 deducem că $m=z_1^2$,$q=t^2$ cu $(z_1,t)=1$ şi naturale.

În particular, observăm că $y^2=(z_1^2)^2-(2t^2)^2 \Leftrightarrow (2t^2)^2+y^2=(z_1^2)^2$.

Aplicând din nou cele stabilite la §2 deducem că există a, $b\in\mathbb{N}^*$, a>b, (a,b)=1 şi de parităţi diferite a.î.

$$2t^2=2ab \Leftrightarrow t^2=ab$$
$$y^2=a^2-b^2$$
$$z_1^2=a^2+b^2.$$

Cum (a, b)=1 iar $t^2=ab$ deducem că $a=x_1^2$, $b=y_1^2$ şi atunci $x_1^4+y_1^4=z_1^2$.

Deducem că (x_1, y_1, z_1) este o soluţie a lui (4) şi conform alegerii lui z ar trebui ca $z_1 \geq z \Leftrightarrow z_1^2 \geq z \Leftrightarrow m \geq m^2+n^2$, ceea ce este absurd. ■

<u>COROLARUL 3.2.</u> Ecuaţia (3) nu poate avea soluţii (x, y, z) cu x, y, $z\in\mathbb{Z}^*$.

<u>Observaţie</u> Ecuaţia (3) este legată de ceea ce în teoria numerelor a fost cunoscută sub numele de Marea teoremă a lui Fermat (deşi corect ar fi fost să fie numită ,,Marea Conjectură a lui Fermat"!):

Dacă $n \geq 3$ atunci ecuatia $x^n+y^n=z^n$ nu poate avea soluţie nenulă în $\mathbb{Z}$ (în sensul că $xyz \neq 0$). (Evident, este suficient să presupunem că n este prim).

Pentru n=4 am văzut mai sus că ecuaţia lui Fermat $x^4+y^4=z^4$ nu are soluţii în $\mathbb{Z}^*$ (Corolarul 3.2.).

Printre hârtiile lui Fermat a fost găsită demonstraţia teoremei numai pentru cazul n=4 (interesant este că aceasta este singura demonstraţie a unui rezultat de teoria numerelor care s-a păstrat de la Fermat !).

În ce priveşte cazul general, n>4, Fermat a notat (pe marginea unei pagini din ,,Aritmetica" lui Diophant) că a găsit ,,o demonstraţie cu adevărat minunată" a acestui fapt, dar ,,această margine este prea îngustă pentru a o cuprinde".

Cu toate eforturile multor matematicieni, această demonstraţie nu a fost găsită şi este îndoielnic că ea ar fi existat în general!.

Mai mult, numai pentru n=4 s-a reuşit să se dea o soluţie elementară.

Astfel se explică de ce specialiştii în teoria numerelor au fost convinşi de imposibilitatea demonstrării Marii teoreme a lui Fermat prin procedee elementare.

Paradoxul constă totuşi în aceea că în toate cazurile în care Fermat a afirmat categoric că a demonstrat o afirmație sau alta, ulterior s-a reuşit a se demonstra această afirmație.

Cel care a reuşit să demonstreze conjectura lui Fermat este matematicianul englez Andrew Wiles de la Universitatea din Princeton (S.U.A). De fapt acesta a demonstrat o altă conjectură (aşa zisa conjectură a lui Taniyama-Weil) din care conjectura lui Fermat rezultă ca un corolar.

Din păcate demonstrația lui Wiles este destul de dificilă, ea neavând un caracter elementar, limitând astfel accesul la înțelegerea ei pentru un foarte mare număr de matematicieni.

Celor care posedă cunoştințe solide de aritmetica geometriei algebrice le recomandăm lucrarea lui A.Wiles din care rezultă conjectura lui Fermat (dacă $x, y, z \in \mathbb{Z}$, $p \geq 3$ este număr prim a.î. $x^p+y^p=z^p$, atunci $xyz=0$):

A.Wiles: Modular Elliptic Curves and Fermat's Last Theorem, Annals of Math, vol. 141, pp. 443-551, 1995.

§4 Ecuații de tip Pell: $x^2-Dy^2=\pm 1$ ($D \in \mathbb{N}$) (5)

Ca şi în paragrafele precedente, pentru a rezolva ecuația (5) în $\mathbb{Z}$ este suficient să găsim soluțiile sale $x, y \in \mathbb{N}^*$.

Dacă $D=n^2$ cu $n \in \mathbb{N}^*$, atunci $(x-ny)(x+ny)=1$ şi se arată imediat că această ecuație nu are soluții $x, y \in \mathbb{N}^*$.

Rămâne deci să ne ocupăm doar de cazul $D \in \mathbb{N}^*$ şi $\sqrt{D} \in \mathbf{I}$.

În Capitolul 10 (Propoziția 3.15) am văzut că fracția continuă a lui $\sqrt{D}$ este de forma $\sqrt{D} = [a_0; a_1, ..., a_n, 2a_0]$, adică $\sqrt{D} = [a_0; a_1, ..., a_n, a_0 + \sqrt{D}]$, de unde $\sqrt{D} = \dfrac{p_n\left(a_0 + \sqrt{D}\right) + p_{n-1}}{q_n\left(a_0 + \sqrt{D}\right) + q_{n-1}}$ iar de aici,

$$Dq_n + \sqrt{D}(q_n a_0 + q_{n-1}) = (p_n a_0 + p_{n-1}) + p_n\sqrt{D}\,.$$

Cum $\sqrt{D} \in \mathbf{I}$, deducem că $Dq_n=p_n a_0 + p_{n-1}$ şi $p_n=q_n a_0 + q_{n-1}$.

Atunci $p_n^2 - Dq_n^2 = (q_n a_0 + q_{n-1})p_n - (p_n a_0 + p_{n-1})q_n = -(q_n p_{n-1} - p_n q_{n-1}) =$ $= (-1)^{n+1}$, adică $p_n^2 - Dq_n^2 = (-1)^{n+1}$.

Această ultimă egalitate ne sugerează :

LEMA 4.1. Toate soluțiile ecuației (5) sunt date de reduse ale lui $\sqrt{D}$.

Demonstrație Egalitatea $p_n^2 - Dq_n^2 = (-1)^{n+1}$ rămâne adevărată și dacă în locul lui n punem k(n+1)-1 (deoarece nu este nevoie să considerăm cea mai scurtă perioadă) :

$(\star)$ $p_{k(n+1)-1}^2 - Dq_{k(n+1)-1}^2 = (-1)^{k(n+1)}$, ceea ce ne arată că o infinitate de reduse ale lui $\sqrt{D}$ ne dau soluții pentru ecuația $x^2-Dy^2=\pm 1$.

Fie acum $p, q\in\mathbb{N}^*$ a.î. $|p^2-Dq^2|=1$. Vrem să demonstrăm că p/q este o redusă a lui $\sqrt{D}$.

Să presupunem prin absurd că p/q nu este o redusă a lui $\sqrt{D}$.

Atunci conform observației de la Propoziția 3.7. de la Capitolul 10, există o redusă p_k/q_k a lui $\sqrt{D}$ cu :

$$|q_k\sqrt{D}-p_k|<|q\sqrt{D}-p| \text{ și } q_k<q.$$

Avem $|q_k\sqrt{D}+p_k|\le 2q_k\sqrt{D}+|p_k-Dq_k|\le 2(q-1)\sqrt{D}+|q\sqrt{D}-p|=2q\sqrt{D}-$ $-(2\sqrt{D}-|q\sqrt{D}-p|)<2q\sqrt{D}-|q\sqrt{D}-p|\le|q\sqrt{D}+p|$, de unde rezultă că:

$0< \left| p_k^2 - Dq_k^2\right| = |q_k\sqrt{D}-p_k|\cdot|q_k\sqrt{D}+p_k|<|q^2D-p^2|=1$, ceea ce este absurd.

Rezultă deci că toate soluțiile ecuației $x^2-Dy^2=\pm 1$ sunt date de reduse ale lui $\sqrt{D}$.

Fie acum $p_k^2 - Dq_k^2 = \pm 1$ o astfel de soluție.

Avem $\sqrt{D}=[a_0;a_1,\ldots, a_k, \alpha_{k+1}]$.

Știm că α_{k+1} este un irațional pătratic redus care satisface ecuația:

$$A_{k+1}x^2 + B_{k+1}x + C_{k+1}=0, \text{ unde } A_{k+1}= p_k^2 - Dq_k^2 = \pm 1 .$$

În plus, $B_{k+1}^2-4A_{k+1}C_{k+1}=4D$ și B_{k+1} este par.

Rezultă $\alpha_{k+1}=\frac{B_{k+1}}{2}+\sqrt{D}$ și cum α_{k+1} este irațional pătratic redus avem $\alpha_{k+1}=a_0+\sqrt{D}$ și deci $\overline{[2a_0;a_1,...,a_k]}$ este o perioadă a lui $\sqrt{D}$, deci toate soluțiile ecuației (5) sunt de forma $(\star)$.■

Observație Este de reținut algoritmul de găsire a soluției $x_0^2 - Dy_0^2 = 1$, cu cele mai mici x_0 și y_0 naturale nenule:

$$\frac{x_0}{y_0} = \begin{cases} [a_0;a_1,\ldots,a_n] \text{ dacă perioada minimă are lungimea pară} \\ [a_0;a_1,\ldots,a_n,2a_0,a_1,\ldots,a_n] \text{ dacă n este par (adică perioada este impară).} \end{cases}$$

Să remarcăm şi faptul că dacă lungimea perioadei lui $\sqrt{D}$ este pară, atunci ecuaţia $x^2-Dy^2=-1$ nu are soluţii.

Exemple : a) Ecuaţia $x^2-7y^2=1$.

Avem: $\sqrt{7} = [2;\overline{1,1,1,4}]$, $\frac{p_3}{q_3}=[2;1,1,1]=8/3$, deci $x_0=8$ şi $y_0=3$.

b) Ecuaţia $x^2-13y^2=-1$.

Avem: $\sqrt{13} = [3;\overline{1,1,1,1,6}]$, $\frac{p_4}{q_4}=18/5$, deci $x_0=18$ şi $y_0=5$.

Să mai notăm faptul că ecuaţiile de forma $x^2-Dy^2=m$ cu D, $m\in\mathbb{Z}$ sunt cunoscute sub numele de *ecuaţii de tip Pell* (deşi Pell nu s-a ocupat de studiul unor astfel de ecuaţii, această greşeală de denumire datorându-se lui Euler).

§5. Ecuaţii de tipul $ax^2 + by^2 + cz^2=0$, cu a, b, $c\in\mathbb{Z}$.(6)

În cadrul acestui paragraf ne vom ocupa de rezolvarea ecuaţiei diophantice (6), unde a, b, $c\in\mathbb{Z}$ sunt libere de pătrate (adică nu conţin în descompunerea lor factori de forma d^2 cu d prim), iar (a, b)=(b, c)=(c, a)=1.

În mod evident, dacă a, b, c ≥ 0 sau a, b, c ≤ 0 atunci ecuaţia (6) are soluţie trivială x=y=z=0. Prin urmare vom presupune că a, b, c nu sunt simultan negative sau pozitive.

Dacă m, $n\in\mathbb{Z}$, vom scrie m **R** n dacă există $x\in\mathbb{Z}$ a.î. $x^2\equiv m(n)$, (adică m este rest pătratic modulo n).

TEOREMA 5.1. (Legendre) Fie a, b, $c\in\mathbb{Z}$, libere de pătrate, oricare două relativ prime, neavând toate acelaşi semn.

În aceste condiţii ecuaţia $ax^2+by^2=z^2$ (7) are o soluţie netrivială dacă şi numai dacă următoarele condiţii sunt îndeplinite:

(i) -ab R c

(ii) –ac R b

(iii) **$-bc$ R a**

Este preferabil să demonstrăm teorema lui Lagrange sub următoarea formă echivalentă :

<u>TEOREMA 5.2.</u> Fie a, b numere naturale libere de pătrate. Atunci ecuaţia $ax^2+by^2+cz^2=0$ are o soluţie netrivială întreagă dacă şi numai dacă următoarele condiţii sunt îndeplinite :

(i) **a R b**

(ii) **b R a**

(iii) **$-(ab/d^2)$ R d , unde d=(a, b)**

Într-adevăr, să presupunem că Teorema 5.2. este adevărată şi să considerăm ecuaţia $ax^2+by^2+cz^2=0$ cu a, b, c ca în enunţul Teoremei 5.1. (să presupunem că a, b>0, iar c<0). Atunci $-acx^2-bcy^2-z^2=0$ satisface condiţiile din Teorema 5.2. Dacă (x, y, z) este o soluţie netrivială, atunci, deoarece c este liber de pătrate, c/z. Punând $z=cz'$ şi simplificând ajungem la o soluţie netrivială pentru (5). Lăsăm ca exerciţiu probarea faptului că Teorema 5.1. implică Teorema 5.2..

Să trecem acum la demonstrarea Teoremei 5.2..

Dacă a=1 totul este clar. Să presupunem că a>b (căci dacă b>a schimbăm pe x cu y, iar dacă a=b atunci -1 este pătrat modulo b, şi se verifică imediat că există r, $s\in\mathbb{Z}$ a.î. $b=r^2+s^2$; în aceste condiţii o soluţie a ecuaţiei (6) va fi $x = r$, $y = s$, $z = r^2+s^2$).

Să construim acum o nouă formă $Ax^2+by^2=z^2$ satisfăcând aceleaşi condiţii ca în enunţul Teoremei 5.2., $0<A<a$ şi a.î. dacă forma astfel construită are o soluţie netrivială, atunci acea soluţie verifică şi forma din enunţul Teoremei 5.2.. Astfel după un număr de paşi, schimbând de fiecare dată pe A cu b dacă A<b ajungem la unul din cazurile a=1 sau a=b care au fost deja discutate.

Iată cum ajungem la aceste cazuri .

Conform cu (ii), există T, $c\in\mathbb{Z}$ a.î. (8) $c^2-b=aT=aAm^2$, cu A, $m\in\mathbb{Z}$, A liber de pătrate, iar $|c|\le a$.

Să arătăm că $0<A<a$.

Într-adevăr, din (8) deducem că $0\le c^2=aAm^2+b<a(Am^2+1)$, adică $A\ge 0$.

Cum b este liber de pătrate deducem că A>0. Mai mult, din (8) deducem că $aAm^2<c^2\le a^2/4$ astfel că $A\le Am^2<a/4<a$. Să arătăm acum că A **R** b.

Fie $b=b_1d$, $a=a_1d$, cu $(a_1, b_1)=1$ şi să observăm că $(a_1, d)=(b_1, d)=1$ deoarece a şi b sunt libere de pătrate. Atunci (8) devine:

(9) $c^2-b_1d=a_1dAm^2$ şi cum d este liber de pătrate deducem că d/c.

Punând $c=c_1d$ şi simplificând obţinem :

(10) $d\,c_1^2 - b_1 = a_1 A m^2$.

Atunci $Aa_1m^2 \equiv -b_1\ (d)$ sau $Aa_1{}^2m^2 \equiv -a_1b_1\ (d)$.

Însă (m, d)=1 deoarece din (10) deducem că în caz contrar un factor comun al lui m şi d ar divide b_1 şi d şi astfel b nu ar mai fi liber de pătrate.

Utilizând (iii) şi faptul că m este o unitate modulo d deducem că A **R** d.

Mai mult, $c^2 \equiv aAm^2 (b_1)$ iar deoarece a **R** b avem că a **R** b_1. De asemenea $(a, b_1)=1$ deoarece în caz contrar un factor comun ar divide d şi b_1, contrazicând faptul că $b=b_1d$ este liber de pătrate.

Similar $(m, b_1)=1$, ceea ce arată că A **R** b_1. Atunci A **R** db_1 sau A **R** b.

Vom scrie acum $A=rA_1$, $b=rb_2$, $(A_1, b_2)=1$ şi trebuie să demonstrăm că $-A_1b_2$ **R** r .

Din (8) deducem că : $c^2 - rb_2 = arA_1m^2$ (11).

Cum r este liber de pătrate deducem că r | c. Dacă $c=rc_1$ atunci $aA_1m^2 \equiv -b_2\ (r)$. Cum a **R** b avem a **R** r. Scriind acum că $-aA_1b_2m^2 \equiv b_2^2\ (r)$ şi observând că (a, r)=(m, r)=1, concluzionăm că $-A_1b_2$ **R** r.

Să presupunem acum că $AX^2+bY^2=Z^2$ are o soluție netrivială.

Atunci $AX^2=Z^2-bY^2$ (12).

Din (12) şi (6) prin multiplicare obținem :

$$A(Axm)^2=(Z^2-bY^2)(c^2-b)=(Zc+bY)^2-b(cY+Z)^2.$$

Atunci (6) are soluția : $x=AXm$

$y=cY+Z$

$z=Zc+bY$ ceea ce completează demonstrația (căci $X\neq 0$ şi $m\neq 0$ deoarece b este liber de pătrate). ■

<u>COROLAR 5.3.</u> Fie a, b, c$\in\mathbb{Z}$ libere de pătrate, cu (a,b)=(a, c)= =(b, c)=1 şi nu au toate acelaşi semn.

Dacă pentru un număr prim p≥2 congruența $ax^2+by^2+cz^2\equiv 0(p^m)$ are soluție $(x, y, z)\in\mathbb{Z}^3$, pentru orice $m\in\mathbb{N}^*$ a.î. nici o componentă a sa nu se divide prin p, atunci $ax^2+by^2+cz^2=0$ are soluție netrivială întreagă (x, y, z).

<u>Demonstrație</u> Fie m=2 şi să presupunem că p|a. Atunci dacă (x, y, z) este o soluție ca în corolar, să arătăm că p∤yz.

Dacă p|y, atunci $p|cz^2$ care implică (deoarece (a, c)=1) că p|z. Atunci $p^2|ax^2$ şi cum p∤x obținem contradicția $p^2|a$. Similar p∤z. Atunci $by^2+cz^2\equiv 0(p)$, de unde deducem că –bc **R** p, ceea ce implică –bc **R** a.

Similar –ab R **c şi –ac** R **b iar acum corolarul rezultă din teorema lui Legendre (pusă sub prima formă).**

Observaţii 1. Acest corolar confirmă *principiul lui Hasse* conform căruia rezolubilitatea locală implică rezolubilitatea globală (aici rezolubilitatea locală înseamnă că ecuaţia considerată are soluţie netrivială modulo p^m pentru orice p prim şi m natural nenul, iar rezolubilitatea globală înseamnă că ecuaţia are o soluţie întreagă).

2. Pentru forme pătratice acest principiu funcţionează însă este fals dacă ecuaţia are grad mai mare.

De exemplu : ecuaţia $x^4-17y^4=2z^4$ are soluţie netrivială modulo p^m pentru orice p prim şi $m\in\mathbb{N}$ şi o soluţie reală, însă nu are soluţie netrivială întreagă [vezi **H. Reichardt: Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen, J. Reine Angew und Math., 184(1942) pp. 12-18]**. ■

§6 Rezolvarea în numere întregi a sistemelor de ecuaţii liniare

În cadrul acestui paragraf vom prezenta condiţii necesare şi suficiente ca un sistem de m ecuaţii liniare cu n necunoscute cu coeficienţi din $\mathbb{Z}$ să aibă soluţie întreagă precum şi modul de aflare a soluţiei generale în caz de compatibilitate.

DEFINIŢIA 6.1. O matrice $U\in M_n(\mathbb{Z})$ ($n\geq 2$) se zice unimodulară dacă $\det(U)=\pm 1$.

În mod evident U este unimodulară dacă şi numai dacă U este inversabilă în $M_n(\mathbb{Z})$. Grupul unităţilor monoidului $(M_n(\mathbb{Z}),\cdot)$ se notează prin $GL_n(\mathbb{Z})$ şi poartă numele de *grupul general liniar de ordin n al lui $\mathbb{Z}$.*.

Pentru $n\geq 1$, $i, j\in\mathbb{N}$, $i\neq j$, $1\leq i, j\leq n$ şi $\lambda\in\mathbb{Z}$ vom nota prin $T_{ij}(\lambda)$ maticea din $M_n(\mathbb{Z})$ ce are 1 pe diagonala principală , λ pe poziţia (i, j) şi 0 în rest.

Reamintim că pentru $m, n\in\mathbb{N}$, $m, n\geq 2$, matricea unitate I_n este matricea din $M_n(\mathbb{Z})$ ce are 1 pe diagonala principală şi 0 în rest, iar matricea nulă $O_{m,n}$ este matricea din $M_{m,n}(\mathbb{Z})$ ce are 0 pe toate poziţiile.

De asemenea, pentru $1\leq i\leq n$ vom nota prin D_i matricea ce diferă de matricea unitate I_n doar pe poziţia (i, i), unde D_i are –1.

În mod evident $\det(T_{ij}(\lambda))=1$ şi $\det(D_i)=-1$, de unde deducem că $T_{i,j}$, $D_i\in GL_n(\mathbb{Z})$.

DEFINIŢIA 6.2. **Matricele de forma $T_{ij}(\lambda)$ şi D_i cu $\lambda \in \mathbb{Z}$, $1 \le i, j \le n$ definite anterior se numesc elementare. Înmulţirea la stânga sau la dreapta a unei matrici A cu o matrice elementară poartă numele de transformare elementară.**

Din felul în care se înmulţesc două matrice, următorul rezultat este imediat:

TEOREMA 6.3. **Fie $m, n \in \mathbb{N}$, $m, n \ge 2$ şi $A \in M_{m,n}(\mathbb{Z})$.**

1) Dacă $T_{ij}(\lambda)$ este o matrice elementară din $M_m(\mathbb{Z})$ atunci matricea $T_{ij}(\lambda)A$ se obţine din A adunând la elementele liniei i pe cele ale coloanei j înmulţite cu λ.

2) Dacă $T_{ij}(\lambda)$ este o matrice elementară de ordinul n atunci matricea $AT_{ij}(\lambda)$ se obţine din A, adunând la elementele coloanei j pe cele ale coloanei i înmulţite cu λ.

3) Dacă D_i este o matrice elementară de ordin m atunci matricea $D_i A$ se obţine din A înmulţind elementele liniei i cu –1.

4) Dacă D_i este o matrice elementară de ordin n, atunci matricea AD_i se obţine din A înmulţind elementele coloanei i cu –1.

Exemple Fie m=3 şi n=4 şi $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}$.

1) Dacă $T_{23}(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z})$, atunci

$$T_{23}(\lambda)\, A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} + \lambda\, a_{31} & a_{22} + \lambda\, a_{32} & a_{23} + \lambda\, a_{33} & a_{24} + \lambda\, a_{34} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}.$$

2) Dacă $T_{12}(\lambda) = \begin{pmatrix} 1 & \lambda & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in M_4(\mathbb{Z})$, atunci

$$AT_{12}(\lambda) = \begin{pmatrix} a_{11} & a_{12}+\lambda & a_{11} & a_{13} & a_{14} \\ a_{21} & a_{22}+\lambda & a_{21} & a_{23} & a_{24} \\ a_{31} & a_{32}+\lambda & a_{31} & a_{33} & a_{34} \end{pmatrix}.$$

3) Dacă $D_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z})$, atunci

$$D_2A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ -a_{21} & -a_{22} & -a_{23} & -a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}.$$

4) Dacă $D_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \in M_4(\mathbb{Z})$, atunci

$$AD_4 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & -a_{14} \\ a_{21} & a_{22} & a_{23} & -a_{24} \\ a_{31} & a_{32} & a_{33} & -a_{34} \end{pmatrix}.$$

<u>DEFINIȚIA 6.4.</u> Fie $n \in \mathbb{N}$, $n \geq 2$ şi $1 \leq i, j \leq n$. Matricea $P_{ij} \in M_n(\mathbb{Z})$ ce se obține din I_n punând pe pozițiile (i, i) şi (j, j) în loc de 1 pe 0 şi care în plus pe pozițiile (i, j) şi (j, i) are 1 poartă numele de <u>matrice de transpoziție.</u>

Exemplu Dacă n=4, atunci $P_{23}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

OBSERVAŢIA 6.5. Ţinând cont de Lema 6.3. deducem că:

Pentru orice $n\in\mathbb{N}$, $n\geq 2$ şi $1\leq i,\ j\leq n$ avem egalitatea:
$P_{ij}=D_i T_{ij}(1)\ T_{ij}(-1)\ T_{ji}(1)$.

În particular, $\det(P_{ij})=-1$, deci $P_{ij}\in GL_n(\mathbb{Z})$.

De asemenea avem următorul rezultat:

LEMA 6.6. Fie $m, n\in\mathbb{N}$, $m, n\geq 2$ şi $A\in M_{m,n}(\mathbb{Z})$.

1) Dacă P_{ij} are ordinul m, atunci matricea $P_{ij}A$ se obţine din A permutând linia i cu linia j.

2) Dacă P_{ij} are ordinul n, atunci matricea AP_{ij} se obţine din A permutând coloana i cu coloana j.

DEFINIŢIA 6.7. Fie $m, n\in\mathbb{N}$, $m, n\geq 2$ şi $A, B\in M_{m,n}(\mathbb{Z})$. Vom spune că A este aritmetic echivalentă cu B, şi vom scrie $A\sim B$, dacă există $U\in GL_m(\mathbb{Z})$ şi $V\in GL_n(\mathbb{Z})$ a.î. $UAV=B$.

Se verifică imediat că relaţia $\sim$ este o echivalenţă pe $M_{m,n}(\mathbb{Z})$.

LEMA 6.8. Oricare ar fi $A\in M_{m,n}(\mathbb{Z})$ există $0\leq r\leq\min\{m, n\}$ şi $d_1, \ldots, d_r\in\mathbb{N}^*$ a. î. $A\sim$ $\begin{pmatrix} d_1 & & & & & 0 \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ 0 & & & & & 0 \end{pmatrix}$ **$\in M_{m,n}(\mathbb{Z})$.**

Demonstraţie Pentru fiecare matrice $A=(a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}\in M_{m,n}(\mathbb{Z})$ definim:

$$m(A)=\begin{cases}0 \ \ daca \ \ \det(A)=0\\ \min\left\{\,|a_{ij}| \ \ cu \ \ a_{ij}\neq 0\right\} \ daca \ \ \det(A)\neq 0.\end{cases}$$

Vom face inducție matematică după m(A). Lema este în mod evident adevărată dacă $A=O_{m,n}$. Să presupunem că $A\neq O_{m,n}$ şi că lema este adevărată pentru toate matricele $B\in M_{m,n}(\mathbb{Z})$ cu $m(B)<m(A)$ ca şi pentru matricele din $M_{m-1,n-1}(\mathbb{Z})$.

Există atunci $1\leq i_0\leq m$ şi $1\leq j_0\leq n$ a.î. $m(A)=|a_{i_0j_0}|$. Prin diferite permutări de linii şi coloane ale lui A putem presupune că $i_0=j_0=1$ (adică $A\sim P_{1i_0}AP_{1j_0}$). Astfel, putem presupune că $m(A)=a_{11}$ şi chiar mai mult că $a_{11}>0$ (căci dacă $a_{11}<0$, atunci în loc de A putem lua D_1A).

<u>Cazul 1.</u> Presupunem că $a_{11}|a_{1j}$ pentru $2\leq j\leq n$ şi $a_{11}|a_{i1}$ pentru $2\leq i\leq m$, adică există $q_{1j}, q_{i1}\in\mathbb{Z}$ a.î. $a_{1j}=a_{11}\cdot q_{1j}$ cu $2\leq j\leq n$ şi $a_{i1}=a_{11}\cdot q_{i1}$ cu $2\leq i\leq m$.

Adunând la coloanele 2, 3, …, n coloana 1 a lui A înmulțită respectiv cu $-q_{12}$, $-q_{13}$, …., $-q_{1n}$ şi procedând analog pentru linii, obținem:

$$A\sim\begin{pmatrix}a_{11}&0\\0&A'\end{pmatrix},\ \text{cu } A'\in M_{m-1,n-1}(\mathbb{Z}).$$

Aplicând ipoteza de inducție lui A′ deducem că există $U'\in GL_{m-1}(\mathbb{Z})$ şi $V'\in GL_{n-1}(\mathbb{Z})$ a.î. $U'A'V'=\begin{pmatrix}d_2&&&&&0\\&\ddots&&&&\\&&d_r&&&\\&&&0&&\\&&&&\ddots&\\0&&&&&0\end{pmatrix}\in M_{m-1,n-1}(\mathbb{Z})$,

unde $d_i\in\mathbb{N}^*$ pentru $2\leq i\leq r$.

Alegând $U=\begin{pmatrix}1 & 0\\ 0 & U'\end{pmatrix}$, $V=\begin{pmatrix}1 & 0\\ 0 & V'\end{pmatrix}$, $d_1=a_{11}$ avem $U\in GL_m(\mathbb{Z})$, $V\in GL_n(\mathbb{Z})$ şi $A\sim U\begin{pmatrix}a_{11} & 0\\ 0 & A'\end{pmatrix}V=\begin{pmatrix} d_1 & & & & & & 0\\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0\end{pmatrix}$

cu $A\in M_{m,n}(\mathbb{Z})$.

Cazul 2. Să presupunem că există în prima linie (sau prima coloană) a lui A un element (să zicem a_{1j_0}, cu $2\le j_0\le n$) ce nu divide pe a_{11}. Împărţind pe a_{1j_0} la a_{11} putem scrie $a_{1j_0}=a_{11}\cdot q_{1j_0}+r_{1j_0}$ cu $0<r_{1j_0}<a_{11}$.

Adunând la coloana j_0 a matricii A coloana întâi înmulţită cu $-q_{1j_0}$ se obţine o matrice B~A care are în poziţia $(1, j_0)$ elementul r_{1j_0}.

Cum $m(B)\le r_{1j_0}<a_{11}=m(A)$, conform ipotezei de inducţie B este echivalentă cu o matrice de forma celei din enunţ şi atunci şi A va avea aceleaşi proprietate.■

OBSERVAŢIA 6.9. Analizând demonstraţia Lemei 6.8. se observă că matricea diagonală cu care A este echivalentă se obţine aplicând asupra lui A un număr finit de transformări elementare.

LEMA6.10. Orice matrice unimodulară $U\in GL_n(\mathbb{Z})$, este egală cu produsul unui număr finit de matrice elementare.

Demonstraţie. Conform Observaţiei 6.9. există matricele elementare $R_1, \ldots, R_s, Q_1, \ldots, Q_t$ a.î.

$R_1 \ldots R_s U Q_1 \ldots Q_t = D = \begin{pmatrix} d_1 & & & & & & 0 \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix} \in M_m(\mathbb{Z})$.

Cum $1=|\det(U)|=\det(D)$, rezultă că $\det(D)\neq 0$, deci r=n.

Din $d_i\in\mathbb{N}^*$, $1\leq i\leq n$ şi $d_1\ldots d_n=1$ deducem că $d_1=d_2=\ldots=d_n=1$, adică $D=I_n$ şi atunci $U=R_1^{-1} \ldots R_s^{-1}Q_t^{-1} \ldots Q_1^{-1}$. Din $T_{ij}^{-1}(\lambda)=T_{ij}(-\lambda)$ şi $D_i^{-1}=D_i$ rezultă că şi matricile R_i^{-1} şi Q_j^{-1} sunt elementare, deci U este produs finit de matrici elementare. ■

<u>LEMA6.11.</u> Pentru orice a, b$\in\mathbb{Z}$ avem $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} (a,b) & 0 \\ 0 & [a,b] \end{pmatrix}$.

<u>Demonstraţie</u> Fie d=(a, b) şi a_1, $b_1\in\mathbb{Z}$ pentru care $a=da_1$ şi $b=db_1$. Conform Corolarului 2.7. de la Capitolul 6, există h, $k\in\mathbb{Z}$ a.î. d=ha+kb, de unde $1=ha_1+kb_1$.

Alegând $U=\begin{pmatrix} 1 & 1 \\ -kb_1 & ha_1 \end{pmatrix}$ şi $V=\begin{pmatrix} h & -b_1 \\ k & a_1 \end{pmatrix}$ avem că

$\det(U)=\det(V)= ha_1+kb_1=1$, adică $U, V\in GL_2(\mathbb{Z})$ şi cum ab=(a, b) [a, b] obţinem că :

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim U \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} V = \begin{pmatrix} (a,b) & 0 \\ 0 & [a,b] \end{pmatrix}. \blacksquare$$

În cele ce urmează vom prezenta un rezultat important (cunoscut sub numele de *<u>Teorema factorilor invarianţi</u>*).

<u>TEOREMA 6.12.</u> Fie m, n $\in\mathbb{N}$, m, n$\geq$2 şi A$\in$M $_{m,\ n}$ ($\mathbb{Z}$). Atunci există $f_1, \ldots, f_r \in \mathbb{N}^*$ cu r$\leq$min {m, n} unic determinaţi a.î. $f_1 | f_2 | \ldots | f_r$ şi

$$A \sim \begin{pmatrix} f_1 & & & & 0 \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ & & & & \ddots \\ 0 & & & & 0 \end{pmatrix} \in \mathbf{M}_{m,n}(\mathbb{Z}).$$

<u>Demonstraţie</u> . Conform Lemei 6.10. avem

$$A \sim \begin{pmatrix} d_1 & & & & 0 \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \\ 0 & & & & 0 \end{pmatrix} = D \text{ cu } d_i \in \mathbb{N}^* \ 1 \leq i \leq r \leq \min\{m, n\}$$

iar $D \in M_{m,n}(\mathbb{Z})$.

Făcând la nevoie permutări de linii sau coloane putem presupune că $d_1 \leq d_2 \leq \ldots \leq d_r$.

Dacă pentru i<j, d_i nu divide d_j, atunci conform Lemei 6.11. există matricile unimodulare $U=\begin{pmatrix} x & y \\ z & w \end{pmatrix}$, $V=\begin{pmatrix} p & q \\ s & t \end{pmatrix}$ a.î.

$$U\begin{pmatrix} d_i & 0 \\ 0 & d_j \end{pmatrix}V=\begin{pmatrix} (d_i, d_j) & 0 \\ 0 & [d_i, d_j] \end{pmatrix}.$$

Considerăm acum matricele U′ de ordin m ce se obţine din I_m punând pe poziţia (i, i) pe x, pe poziţia (j, j) pe w, pe poziţia (i, j) pe y iar pe poziţia (j, i)

pe z şi matricea V' de ordin n ce se obţine din I_n punând pe poziţia (i, i) pe p, pe poziţia (j, j) pe t, pe poziţia (i, j) pe q iar pe poziţia (j, i) pe s.

În mod evident, $U' \in GL_m(\mathbb{Z})$, $V' \in GL_n(\mathbb{Z})$ iar matricea $U'DV'$ se obţine din D înlocuind pe d_i cu (d_i, d_j) iar pe d_j cu $[d_i, d_j]$.

Dacă $d_1 | d_j$, $2 \le j \le r$ atunci se defineşte $f_1 = d_1$. Dacă există $j \ge 2$ a.î. $d_1 \nmid d_j$ atunci d_1 se înlocuieşte cu (d_1, d_2), iar d_j cu $[d_1, d_j]$ şi observăm că în acest caz $(d_1, d_2) < d_1$ şi $(d_1, d_2) \mid [d_1, d_2]$. După un număr finit de paşi se ajunge la

$$A \sim \begin{pmatrix} d_1' & & & & & & 0 \\ & d_2' & & & & & \\ & & \ddots & & & & \\ & & & d_r' & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix}$$

cu $d_1' \mid d_j'$ cu $2 \le j \le r$ şi se ia $f_1 = d_1'$. Dacă $d_2' \mid d_j'$, $3 \le j \le r$ atunci vom lua $f_2 = d_2'$. În caz contrar, se aplică procedeul de mai înainte ş.a.m.d.. Astfel, după un număr finit de paşi se obţine o matrice de forma celei din enunţ echivalentă cu A.

Să arătăm acum unicitatea numerelor r, $f_1, f_2, \ldots, f_r$.

Pentru matricea A prin $\Delta_i(A)$ vom nota cel mai mare divizor comun al minorilor de ordin i al matricei A.

Atunci dacă $A \sim B$ în mod evident $\Delta_i(A) = \Delta_i(B)$, i=1, 2, …, n iar pentru

matricea $D = \begin{pmatrix} f_1 & & & & & 0 \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$ cu $f_1 | f_2 | \ldots | f_r$, avem

$\Delta_1(D) = f_1$, $\Delta_2(D) = f_1 f_2$, ……..,$\Delta_r(D) = f_1 f_2 \ldots f_r$ iar $\Delta_i(D) = 0$, pentru $r \le i \le \min\{m, n\}$.

Cu aceasta teorema este complet demonstrată. ■

DEFINIŢIA 6.13. **Dacă $A\in M_{m,n}(\mathbb{Z})$, atunci matricea unic determinată**

$$B=\begin{pmatrix} f_1 & & & & 0 \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ 0 & & & & 0 \end{pmatrix} \in M_{m,n}(\mathbb{Z}),$$ **cu** $f_1|f_2|\ldots|f_r$ **a.î. A~B se numeşte forma diagonal canonică a lui A. Numerele $f_1, \ldots, f_r > 1$ se zic factorii invarianţi ai lui A.**

Exemplul[14] Să găsim forma diagonal canonică a matricei

$$A=\begin{pmatrix} 6 & 2 & -12 & 8 \\ -6 & 0 & 12 & -6 \\ 12 & 2 & -24 & 14 \end{pmatrix}.$$

Înmulţind pe rând la dreapta matricea A cu matricile P_{12}, $T_{12}(-3)$, $T_{13}(6)$, $T_{14}(-4)$ de ordin 4 şi apoi la stânga cu matricea $T_{31}(-1)$ de ordin 3, se obţine matricea $B=T_{31}(-1)\ A\ P_{12}\ T_{12}(-3)\ T_{13}(6)\ T_{14}(-4)=\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -6 & 12 & -6 \\ 0 & 6 & -12 & 6 \end{pmatrix}$.

Înmulţind la stânga matricea B cu matricea D_2 de ordin 3, apoi pe rând la dreapta cu matricile $T_{23}(2)$, $T_{24}(-1)$ de ordin 4 şi în sfârşit la stânga cu matricea $T_{32}(-1)$ de ordin 3 se obţine matricea $D=T_{32}(-1)\ D_2\ B\ T_{23}(2)\ T_{24}(-1)=\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

ce reprezintă forma diagonal canonică a matricei A, 2 şi 6 fiind factorii invarianţi ai acesteia.

Fie $U=T_{32}(-1)\, D_2\, T_{31}(-1)=\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$ şi

$V=P_{12}\, T_{12}(-3)\, T_{13}(6)\, T_{14}(-4)\, T_{23}(2)\, T_{24}(-1)=\begin{pmatrix} 0 & 1 & 2 & -1 \\ 1 & -3 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Avem $U\in GL_3(\mathbb{Z})$, $V\in GL_4(\mathbb{Z})$ şi $UAV=\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Cu ajutorul celor stabilite anterior vom studia în continuare sistemele liniare de m ecuații cu n necunoscute:

$$(S)\quad \begin{cases} a_{11}X_1 + \ldots + a_{1n}X_n = b_1 \\ a_{21}X_1 + \ldots + a_{2n}X_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}X_1 + \ldots + a_{mn}X_n = b_m \end{cases}$$

cu coeficienții a_{ij} , $b_j \in \mathbb{Z}$, $1\le i\le m$, $1\le j\le n$.

Prin <u>*soluție întreagă a lui (S)*</u> înțelegem un n-uplu $(\lambda_1, \ldots \lambda_n)\in \mathbb{Z}^n$ a.î. $\sum_{j=1}^{n} a_{ij}\lambda_j = b_i$ pentru orice $1\le i\le m$.

Dacă notăm $A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$, $\mathbf{b}=\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ şi $X=\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ atunci sistemul (S) se scrie matricial sub forma $AX=\mathbf{b}$.

DEFINIŢIA 6.14. **Dacă** $U\in GL_n(\mathbb{Z})$, $U=\left(u_{ij}\right)_{\substack{1\le i\le m\\ 1\le j\le n}}$ **atunci transformarea** $X_i=\sum_{j=1}^{n}u_{ij}Y_j$, $1\le i\le n$ **(sau matriceal X=UY) se numeşte substituţie întreagă unimodulară , unde** $Y=\begin{pmatrix}Y_1\\ \vdots\\ Y_n\end{pmatrix}$.

PROPOZIŢIA 6.15. **Fie** $U\in GL_n(\mathbb{Z})$, $U=\left(u_{ij}\right)_{\substack{1\le i\le m\\ 1\le j\le n}}$ **şi numerele reale** α_i, β_i **cu** $1\le i\le n$ **a.î.** $\beta_i=\sum_{j=1}^{n}u_{ij}\alpha_j$, $1\le i\le n$.

Atunci $\beta_i\in\mathbb{Z}$ **pentru** $1\le i\le n$ **dacă şi numai dacă** $\alpha_j\in\mathbb{Z}$ **pentru** $1\le j\le n$. **Mai mult,** $(\beta_1,\ldots\beta_n)$ **este soluţie întreagă a sistemului (S) dacă şi numai dacă** $(\alpha_1,\ldots\alpha_n)$ **este soluţie întreagă a sistemului (AU)Y=b.**

Demonstraţie O implicaţie este evidentă.

Să presupunem acum că $\beta_i\in\mathbb{Z}$ pentru $1\le i\le n$ şi fie $V\in GL_n(\mathbb{Z})$ a.î. $VU=UV=I_n$. Atunci $\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=VU\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=V\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}=\begin{pmatrix}\sum_{i=1}^{n}v_{1i}\beta_i\\ \vdots\\ \sum_{i=1}^{n}v_{ni}\beta_i\end{pmatrix}$ de unde deducem că $\alpha_i\in\mathbb{Z}$ pentru $1\le i\le n$. Ultima afirmaţie este evidentă. ■

LEMA 6.16. **Dacă** $a_1,\ldots a_n\in\mathbb{Z}$, **atunci există** $U\in GL_n(\mathbb{Z})$ **a.î.** $(a_1,\ldots,a_n)\,U=(d,0,\ldots,0)$, **unde** $d=(a_1,a_2,\ldots a_n)$.

Demonstraţie Facem inducţie matematică după n şi să arătăm la început că lema este adevărată pentru n=2.

Dacă $d=(a_1,a_2)$, atunci $a_1=da_1'$ şi $a_2=da_2'$ cu $a_1',a_2'\in\mathbb{Z}$ iar $(a_1',a_2')=1$, de unde deducem că există $h,k\in\mathbb{Z}$ a.î. $ha_1'+ka_2'=1$ şi fie $U=\begin{pmatrix}h & -a_2'\\ k & a_1'\end{pmatrix}$. (cum $\det(U)=ha_1'+ka_2'=1$ deducem că $U\in GL_2(\mathbb{Z})$).

Avem că (a_1, a_2) U= $(ha_1 + ka_2 , -a_1a_2' + a_2a_1') = (d, 0)$.

Fie n>2 şi să presupunem că lema este adevărată pentru n-1. Atunci există $V_1 \in GL_{n-1}(\mathbb{Z})$ a.î. $(a_2, \ldots, a_n) V_1 = (d_1, 0, \ldots 0)$, unde $d_1=(a_2 , a_3, \ldots a_n)$ astfel că dacă notăm $V=\begin{pmatrix} 1 & 0 \\ 0 & V_1 \end{pmatrix} \in GL_n(\mathbb{Z})$ avem

$$(a_1, \ldots, a_n) V=(a_1, d_1, 0, \ldots 0).$$

Conform cazului n=2 există $W_1 \in GL_2(\mathbb{Z})$ a.î. $(a_1, d_1)W_1=(d_1, 0)$, unde $d=(a_1, d_1)$.

Dacă alegem $W=\begin{pmatrix} W_1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in GL_n(\mathbb{Z})$ atunci $W \in GL_n(\mathbb{Z})$ şi

$(a_1, \ldots, a_n) U=(d, 0, \ldots 0)$, unde U=VW (se observă că $d=(a_1, \ldots, a_n)$).■

Să considerăm acum ecuaţia

$(\star)$ $a_1X_1+\ldots.+a_nX_n=b$, cu $a_1, \ldots, a_n, b \in \mathbb{Z}$.

Pentru n=2 am arătat în §1 de la Capitolul 12, în ce condiţii această ecuaţie are soluţii întregi şi felul în care acestea se găsesc. În cele ce urmează vom face acelaşi lucru cu ecuaţia $(\star)$ pentru $n \geq 2$ (prezentând deci o generalizare a Lemelor 1.1 şi 1.2 de la Capitolul 12).

<u>TEOREMA 6.17.</u> Ecuaţia $(\star)$ cu coeficienţi întregi admite soluţii întregi dacă şi numai dacă $d \mid (a_1, \ldots, a_n)$. Dacă $U \in GL_n(\mathbb{Z})$, $U=\left(u_{ij}\right)_{1 \leq i, j \leq n}$ este a.î. $(a_1, \ldots, a_n)U=(d, 0, \ldots 0)$, (conform Lemei 6.16.) atunci $\left(x_1^0, \ldots, x_n^0\right)$ cu $x_i^0 = u_{i1} \cdot \frac{b}{d}$, $1 \leq i \leq n$ este soluţie întreagă particulară a ecuaţiei $(\star)$. Soluţia generală din $\mathbb{Z}$ a ecuaţiei $(\star)$ va fi de forma $(x_1, \ldots x_n)$ cu $x_i = x_i^0 + \sum_{j=2}^{n} u_{ij} t_j$, $t_j \in \mathbb{Z}$, $1 \leq i \leq n$.

<u>Demonstraţie</u> Dacă $U \in GL_n(\mathbb{Z})$ ca în enunţ, atunci făcând substituţia întreagă unimodulară X=UY obţinem $(d, 0, \ldots, 0)Y=b$. Atunci deducem că această ultimă ecuaţie are soluţie întreagă dacă şi numai dacă $d \mid b$ iar o soluţie

întreagă particulară a acesteia este $\left(\frac{b}{d},0,....0\right)$, soluția generală fiind de forma $\left(\frac{b}{d},t_2,...t_n\right)$ cu $t_j\in\mathbb{Z}$, $2\le j\le n$ arbitrare. Conform Propoziției 6.15. obținem că

$$\begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix} = U\begin{pmatrix} b/d \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} u_{11}b/d \\ \vdots \\ u_{n1}b/d \end{pmatrix}$$ este soluția întreagă particulară a

ecuației $(\star)$ iar dacă $(x_1, \ldots x_n)$ este soluția întreagă oarecare a lui $(\star)$, atunci

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = U\begin{pmatrix} b/d \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} \frac{u_{11}b}{d}+\sum_{j=2}^{n}u_{1j}t_j \\ \vdots \\ \frac{u_{n1}b}{d}+\sum_{j=2}^{n}u_{nj}t_j \end{pmatrix}$$ adică $x_i = x_i^0 + \sum_{j=2}^{n} u_{ij}t_j$, $1\le j\le n$. ■

OBSERVAŢII 1. Când $d|b$, descrierea soluțiilor întregi ale ecuației $(\star)$ din enunțul teoremei precedente se face cu ajutorul matricei unimodulare U. Calculul lui U se face folosind de n-1 ori algoritmul lui Euclid extins.

Într-adevăr, într-o primă etapă cu ajutorul acestui algoritm determinăm succesiv :

$d_1=(a_{n-1}, a_n)$, $h_1a_{n-1}+k_1a_n=d_1$
$d_2=(a_{n-2}, d_1)$, $h_2a_{n-2}+k_2d_1=d_2$
……..
$d=d_{n-1}=(a_2, d_{n-2})$, $h_{n-1}a_{n-1}+k_1d_{n-2}=d_{n-1}=d$

şi atunci avem

$$U=\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \begin{vmatrix} h_1 & -a_n \\ k_1 & -a'_{n-1} \end{vmatrix} \end{pmatrix} \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \begin{vmatrix} h_2 & -d'_1 \\ k_2 & a'_{n-1} \end{vmatrix} \\ & & & 1 \end{pmatrix} \cdots\cdots$$

$$\cdots \begin{pmatrix} \begin{vmatrix} h_{n-1} & -d'_{n-1} \\ k_{n-1} & a'_1 \end{vmatrix} & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \quad \text{unde} \quad a_n = d_1 a'_n, \quad a_{n-1} = d_1 a'_{n-1},$$

$d_1 = d_2 d'_1$, $a_{n-2} = d_2 a'_{n-2}$, etc.

2. Când n=2 obținem rezultatele de la §1, Capitolul 12.

<u>LEMA 6.18.</u> Fie n≥2 şi A=(a_{ij})∈$\mathbf{M_n(\mathbb{Z})}$ a.î. Δ=det (A) > 0. Atunci există U∈$\mathbf{GL_n(\mathbb{Z})}$ a.î.

AU=$\begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ c_{12} & c_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}$ **unde $c_{i\,i}$ >0, 1≤i≤n şi 0≤$c_{i\,1}$, $c_{i\,2}$, …, $c_{i,\,i-1}$< $c_{i\,i}$, 1≤i≤n.**

<u>Demonstraţie</u> Fie $c_{11}=(a_{11}, a_{12}, \ldots a_{1n})$. Conform Lemei 6.16. există $U_1 \in GL_n(\mathbb{Z})$ a.î. $(a_{11}, a_{12}, \ldots, a_{1n})\, U_1 = (c_{11}, 0, \ldots, 0)$

şi deci $AU_1=\begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ .... & .... & .... & .... \\ a'_{n1} & a'_{n2} & \cdots & a'_{nn} \end{pmatrix}$ unde $a'_{ij} \in \mathbb{Z}$. Aplicând din nou aceiaşi lemă găsim $V \in GL_{n-1}(\mathbb{Z})$ a.î. $(a'_{22}, a'_{23}, \ldots, a'_{2n})\ V = (c_{22}, 0, \ldots, 0)$ unde $c_{22}=(a'_{22}, a'_{23}, \ldots, a'_{2n})$. Punând $U_2=\begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix}$ avem $U_2 \in GL_n(\mathbb{Z})$ şi se obține

$$AU_1U_2=\begin{pmatrix} c_{11} & 0 & 0 & .... & 0 \\ a''_{21} & c_{22} & 0 & .... & 0 \\ a''_{31} & a''_{32} & a''_{33} & .... & a''_{3n} \\ ... & .... & .... & .... & .... \\ a''_{n1} & a''_{n2} & a''_{n3} & .... & a''_{nn} \end{pmatrix}.$$

Dacă $0 \le a''_{21} < c_{22}$ luăm $c_{21}=a''_{21}$, în caz contrar scriem $a''_{21} = c_{22}q_{21} + r_{21}$ cu $0 \le r_{21} < c_{22}$. Atunci

$$AU_1U_2T_{21}(-q_{21})=\begin{pmatrix} c_{11} & 0 & .... & 0 \\ r_{21} & c_{22} & .... & 0 \\ .... & .... & .... & .... \end{pmatrix}$$ şi alegem $c_{21}=r_{21}$. Continuând se găseşte matricea $U=U_1U_2\ldots..\in GL_n(\mathbb{Z})$ a.î. matricea AU este de forma celei din enunț. ■

<u>TEOREMA 6.19</u>. Fie un sistem de de n ecuații liniare cu n necnoscute (S_1) $\sum_{j=1}^{n} a_{ij}X_j = b_i$, $1 \le i \le n$ a.î. $a_{ij}, b_i \in \mathbb{Z}$ şi det (A) > 0 (A fiind matricea $A=\left(a_{ij}\right)_{1 \le i,j \le n}$).

Atunci sistemul (S_1) admite soluție întreagă dacă şi numai dacă congruențele (C) $\sum_{j=1}^{n} a_{ij}X_j \equiv b_i \ (m)$, $1 \le i \le n$ au soluție întreagă pentru orice $m \in \mathbb{Z}$ a.î. $0 < m \le \Delta$.

Demonstraţie. Implicația de la stînga la dreapta este evidentă.

Să presupunem acum că (C) are soluție pentru orice $0<m\leq\Delta$. Scriem pe (C) sub formă matricială astfel $AX\equiv b$ (m), $0<m\leq\Delta$.

Dacă $X=UY$ este o substituție întreagă unimodulară , atunci $(AU)Y\equiv b$ (m), $0<m\leq\Delta$. Alegând $U\in GL_n(\mathbb{Z})$ dată de Lema 6.16. sistemul (S_1) devine $\begin{cases} c_{11}Y_1 = b_1 \\ c_{21}Y_1 + c_{22}Y_2 = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ c_{n1}Y_1 + c_{n2}Y_2 + \ldots + c_{nn}Y_n = b_n . \end{cases}$

Evident $\Delta=c_{11}c_{22}\ldots c_{n\,n}$, deci $0<c_{11}c_{22}\ldots c_{ii}\leq\Delta$, $1\leq i\leq n$.

Cum $0<c_{11}\leq\Delta$, congruența $c_{11}Y_1=b_1$ (c_{11}) are soluție, deci există h, $k\in\mathbb{Z}$ a.î. $c_{11}h=b_1+kc_{11}$, de unde $c_{11}\alpha_1=b_1$ cu $\alpha_1=h-k$.

Adunând ecuația $c_{11}Y_1=b_1$ (înmulțită cu $-c_{21}$) cu ecuația $c_{12}Y_1+c_{22}Y_2=$ $=b_2$ (înmulțită cu c_{11}) se obține $c_{11}c_{22}Y_2 =- c_{21}b_1+c_{11}b_2$.

Conform ipotezei, congruența $c_{11}c_{22}Y_2 \equiv c_{21}b_1+c_{11}b_2$ $(c_{11}c_{22})$ are soluție, deci există h', $k' \in\mathbb{Z}$ a.î. $c_{11}c_{22}\,h' = - c_{21}c_{11}\alpha_1+c_{11}b_2 +k'c_{11}c_{22}$.

Simplificând cu $c_{11}\neq0$, obținem $c_{21}\alpha_1+c_{22}\alpha_2 =b_2$, unde $\alpha_2=h'-k'\in\mathbb{Z}$.

Analog, din primele trei ecuații în Y_1, Y_2, Y_3 obținem

$c_{11}c_{22}\,c_{33}Y_3 =c_{11}c_{22}b_3 - c_{31}\,c_{22}b_1 - c_{11}c_{22}b_1-c_{11}\,c_{32}b_2 +c_{21}c_{32}b_1$.

Înlocuind $b_1= c_{11}\alpha_1$, $b_2 =c_{21}\alpha_1+c_{22}\alpha_2$ şi pornind de la condiția ca această ultimă ecuație să fie solubilă modulo $c_{11}\,c_{22}c_{33}$, găsim $\alpha_3\in\mathbb{Z}$ a.î.

$$c_{31}\alpha_1+c_{32}\alpha_2 +c_{33}\alpha_3=b_3 .$$

Continuând în acelaşi mod găsim o soluție întreagă $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a sistemului $AUY=b$ şi atunci $(\beta_1, \beta_2, \ldots, \beta_n)$, unde $\beta_i = \sum_{j=1}^{n} u_{ij}\alpha_j$, $1\leq i\leq n$ este o soluție întreagă a sistemului (S_1) $AX=b$. ■

Observaţie Cum $\mathbb{Z}_m$-urile sunt finite rezultă din teorema de mai sus că putem stabili printr-un număr finit de încercări dacă sistemul (S_1) are sau nu soluții întregi.

Teorema următoare soluționează cazul sistemelor omogene.

TEOREMA 6.20. Sistemul de ecuaţii liniare

(S_2) $\sum_{j=1}^{n} a_{ij} X_j = 0$, **$1 \le i \le m$ cu $a_{ij} \in \mathbb{Z}$, ($m<n$) admite o soluţie întreagă netrivială ($x_1, \ldots x_n$) ce satisface condiţia** $|x_j| \le (a_1 a_2 \ldots a_m)^{1/n-m}$, **$1 \le j \le n$, unde** $a_i = \sum_{j=1}^{n} |a_{ij}|$, **$1 \le i \le m$.**

Demonstraţie Fie $L_i(X_1, \ldots X_n) = \sum_{j=1}^{n} a_{ij} X_j$, $1 \le i \le m$, $b_i = \sum_{a_{ij}>0} a_{ij}$, $-c_i = \sum_{a_{ij}<0} a_{ij}$, $1 \le i \le m$.

Atunci $a_i = b_i + c_i$ cu $1 \le i \le m$ şi fie $a \in \mathbb{N}$. Dacă $0 \le \alpha_j \le a$ cu $1 \le j \le n$, atunci

$$-c_i a \le L_i(\alpha_1, \ldots, \alpha_n) \le b_i a, \quad 1 \le i \le m,$$

deci $L_i(\alpha_1, \ldots \alpha_n)$ ia cel mult $a_i a + 1$ valori întregi.

Alegând $a = \left\lfloor (a_1 \ldots a_m)^{1/m-n} \right\rfloor$ (partea întreagă!) atunci

$a > (a_1 a_2 \ldots a_m)^{1/n-m} - 1$, de unde

$$(a+1)^n > (a+1)^m a_1 \ldots a_m > (a_1 a + 1) \ldots (a_m a + 1).$$

Deducem că există $(\alpha'_1, \ldots, \alpha'_n) \ne (\alpha''_1, \ldots, \alpha''_n)$ cu $0 \le \alpha'_i, \alpha''_i \le a$ a.î. $L_i(\alpha'_1, \ldots \alpha'_n) = L_i(\alpha''_1, \ldots \alpha''_n)$, $1 \le i \le n$.

Alegând $x_i = \alpha'_i - \alpha''_i$, $1 \le i \le n$, avem că $L_i(x_1, \ldots x_n) = 0$, $1 \le i \le m$ şi $|x_j| \le (a_1 a_2 \ldots a_m)^{1/n-m}$, $1 \le j \le m$. Mai mult, $(x_1, \ldots x_n) \ne (0, \ldots 0)$ şi astfel teorema este demonstrată. ■

Cu ajutorul formei diagonal canonice a matricelor din $M_{m,n}(\mathbb{Z})$ putem acum soluţiona problema existenţei şi descrierii soluţiilor întregi ale unui sistem de m ecuaţii liniare cu n necunoscute cu coeficienţi întregi.

TEOREMA 6.21. **Fie sistemul de m ecuații liniare în n necunoscute cu coeficienți întregi (S)** $\sum_{j=1}^{n} a_{ij} X_j = b_i$ **, 1≤i≤n .**

Dacă $A=\left(a_{ij}\right)_{\substack{1\le i\le m\\ 1\le j\le n}} \in \mathbf{M}_{m,n}(\mathbb{Z})$ **şi** $U\in \mathbf{GL}_m(\mathbb{Z})$, $V\in \mathbf{GL}_n(\mathbb{Z})$, $U=(u_{ij})$, $V=(v_{ij})$ **sunt a.î.** $UAV=\begin{pmatrix} f_1 & & & & 0 \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ 0 & & & & 0 \end{pmatrix}$ **(vezi Teorema 6.12.), atunci condiția necesară şi suficientă ca (S) să aibă soluții întregi este ca** $f_k \left| \sum_{j=1}^{m} u_{kj} b_j \right.$ **, 1≤k≤r şi** $\sum_{j=1}^{m} u_{ij} b_j = 0$ **, r<j≤min {m, n}.**

În aceste condiții $\left(x_1^0,\ldots x_n^0\right)$, **unde** $x_i^0 = \sum_{k,j=1}^{r,m} \frac{v_{ik} u_{kj} b_j}{f_k}$ **, 1≤i≤n, este o soluție întreagă a sistemului (S). Mai mult, un sistem** $(x_1, \ldots x_n)$ **de numere întregi este soluție a lui (S) dacă şi numai dacă**

$$x_i = x_i^0 + \sum_{k=r+1}^{n} v_{ik} t_k \text{ , } t_k\in\mathbb{Z}, 1\le i\le n.$$

Demonstrație Scriem sistemul (S) sub formă matricială AX=**b**. Cum $UAV V^{-1}X=Ub$, notând $Y=V^{-1}X$ avem (S′) DY=UL unde

$$D=\begin{pmatrix} f_1 & & & & 0 \\ & \ddots & & & \\ & & f_r & & \\ & & & 0 & \\ 0 & & & & 0 \end{pmatrix}.$$

Deducem că $f_k Y_k = \sum_{j=1}^{m} u_{jk} b_j$, $1 \le k \le r$ şi $0 = \sum u_{kj} b_j$, $r < k \le$

$\le \min\{m, n\}$. Este clar că DY=Ub admite soluție întreagă dacă şi numai dacă $f_k \left| \sum_{j=1}^{m} u_{kj} b_j \right.$, $1 \le k \le r$ şi o soluție particulară a sistemului (S′) este:

$$\left(\sum_{j=1}^{m} \frac{u_{1j} b_j}{f_1}, \ldots, \sum_{j=1}^{m} \frac{u_{rj} b_j}{f_r}, 0, \ldots, 0 \right)$$

iar soluția generală a sistemului (S′) este :

$$\left(\sum_{j=1}^{m} \frac{u_{1j} b_j}{f_1}, \ldots, \sum_{j=1}^{m} \frac{u_{rj} b_j}{f_r}, t_{r+1}, \ldots, t_n \right)$$ cu $t_{r+1}, \ldots, t_n$ arbitrari din $\mathbb{Z}$.

Cum X=VY deducem că soluțiile sistemului (S) sunt cele din enunț. ■

Exemplu Să considerăm sistemul :

$$(\star) \begin{cases} 6X_1 + 2X_2 - 12X_3 + 8X_4 = 10 \\ -6X_1 + \quad 12X_3 - 6X_4 = 18 \\ 12X_1 + 2X_2 - 24X_3 + 14X_4 = -8. \end{cases}$$

Avem $A = \begin{pmatrix} 6 & 2 & -12 & 8 \\ -6 & 0 & 12 & -6 \\ 12 & 2 & -24 & 14 \end{pmatrix}$.

După exemplul de la Teorema 6.12. avem că $UAV = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$,

unde $U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$, $V = \begin{pmatrix} 0 & 1 & 2 & -1 \\ 1 & -3 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Avem r=2, $f_1=2$, $f_2=6$.

Din $\sum_{j=1}^{4} u_{1j} b_j = 10$ şi $2 \mid 10$, unde $2=f_1$

$\sum_{j=1}^{3} u_{2j} b_j = -18$ şi $6 \mid -18$, unde $6=f_2$

$\sum_{j=1}^{3} u_{3j} b_j = 0$

rezultă că sistemul $(\star)$ are soluție în numere întregi (conform Teoremei 6.21.). Urmând algoritmul dat de Teorema 6.21., deducem că o soluție particulară a lui $(\star)$ este $\left(x_1^0, x_2^0, x_3^0, x_4^0\right)=(-3, 14, 0, 0)$ iar soluția generală este:

$x_1= -3+2t_3 - t_4$

$x_2=14 - t_4$

$x_3=t_3$

$x_4=t_4$, cu $t_3, t_4 \in \mathbb{Z}$ arbitrare.

Observație Acest paragraf a fost redactat în cea mai mare parte după lucrarea [14].

CAPITOLUL 13:
PUNCTE LATICIALE ÎN PLAN ŞI SPAȚIU

§1.Puncte laticiale în plan

Să considerăm planul euclidian $\mathcal{E}$ raportat la un sistem ortogonal de axe de coordonate.

DEFINIȚIA 1.1. Un punct M de coordonate (a, b) din planul euclidian $\mathcal{E}$ se zice *punct laticial* dacă a, b$\in\mathbb{Z}$.

TEOREMA 1.2. (Steinhaus-Sierpinski) Pentru fiecare număr n$\in\mathbb{N}^*$ există în planul euclidian $\mathcal{E}$ un cerc ce conține în interiorul său exact n puncte laticiale.

Demonstraţie Să considerăm în $\mathcal{E}$ punctul C de coordonate ($\sqrt{2}$, 1/3) şi să demonstrăm că dacă M(a, b) şi N(c, d) sunt două puncte laticiale din $\mathcal{E}$ ce au aceeaşi distanţă la punctul C, atunci M≡N.

Într-adevăr, dacă CM≡CN, atunci:

$(a-\sqrt{2})^2 + (b-\frac{1}{3})^2 = (c-\sqrt{2})^2 + (d-\frac{1}{3})^2 \Leftrightarrow 2(c-a)\sqrt{2} = c^2 + d^2 - a^2 - b^2 + \frac{2}{3}(b-d)$,

de unde a=c şi $c^2 + d^2 - a^2 - b^2 + \frac{2}{3}(b-d) = 0 \Leftrightarrow (d-b)(d+b-\frac{2}{3})=0$ şi cum b, d∈ℤ,

$d + b - \frac{1}{3} \neq 0$, ceea ce implică b=d, adică M≡N. ■

Ţinând cont de observaţia de mai înainte, punctele laticiale din $\mathcal{E}$ pot fi ordonate în funcţie de distanţele lor la C($\sqrt{2}$, 1/3).

Fie deci M_1 punctul laticial a cărui distanţă d_1 la C este cea mai mică, M_2 următorul (adică acel punct pentru care distanţa d_2 de la M_2 la C este cel mai apropiat număr natural faţă de d_1) ş.a.m.d.

Obţinem astfel şirul M_1, M_2,… de puncte laticiale cu proprietatea că dacă notăm prin d_i distanţa de la M_i la C, i=1, 2,… , atunci $d_1<d_2<d_3<\ldots$.

Atunci cercul cu centru în punctul C şi de rază d_{n+1} conţine în interiorul său doar punctele laticiale M_1, M_2, …, M_n ce sunt în număr de n şi astfel teorema este demonstrată. ■

Observaţie Există un rezultat datorat lui Hugo Steinhaus potrivit căruia pentru fiecare număr natural n∈ℕ există un cerc de arie n ce conţine în interiorul său exact n puncte laticiale.

TEOREMA 1.3. (A. Schinzel) Pentru orice număr natural n∈ℕ există în $\mathcal{E}$ un cerc ce conţine pe circumferinţa sa exact n puncte laticiale.

Demonstraţie Dacă n este par, adică n=2k cu k∈ℕ, vom demonstra că cercul de centru (1/2, 0) şi rază $\frac{1}{2}\cdot 5^{(k-1)/2}$ conţine pe circumferinţa sa exact n puncte laticiale, pe când atunci când n este impar, adică n=2k+1 cu k∈ℕ, cercul

de centru (1/3, 0) şi rază $\frac{1}{3}\cdot 5^k$ conține pe circumferința sa exact n puncte laticiale.

Pentru aceasta vom apela la Teorema 1.7. de la Capitolul 11 potrivit căreia numărul total de perechi (x, y) din $\mathbb{Z}\times\mathbb{Z}$ pentru care $x^2+y^2=n$ este egal cu $4(d_1(n)-d_2(n))$, unde $d_1(n)$ este numărul divizorilor lui n de forma 4t+1 iar $d_2(n)$ este numărul divizorilor primi de forma 4t+3. (atunci când numărăm perechile (x, y) facem distincție între (x, y) şi (y, x) pentru $x\neq y$).

Cazul 1 : n=2k cu $k\in\mathbb{N}$. Să considerăm ecuația (1) $x^2 + y^2 = 5^{k-1}$. Toți divizorii lui 5^{k-1} sunt puteri ale lui 5, deci toți aceşti divizori sunt de forma 4t+1. Cum numărul acestor divizori este k deducem că $d_1(5^{k-1})=k$ iar cum $d_2(5^{k-1})=0$ atunci numărul perechilor $(x, y)\in\mathbb{Z}\times\mathbb{Z}$ pentru care $x^2 + y^2=5^{k-1}$ este 4(k-0)=4k.

Cum 5^{k-1} este impar trebuie ca x sau y să fie impar.

Cercul de circumferință $C_1(1/2, 0)$ şi rază $\frac{1}{2}\cdot 5^{(k-1)/2}$ are ecuația:

$$(\alpha-\frac{1}{2})^2+\beta^2=\frac{1}{4}\cdot 5^{k-1}\Leftrightarrow(2\alpha-1)^2+4\beta^2=5^{k-1}\Leftrightarrow(2\alpha-1)^2+(2\beta)^2=5^{k-1}. \quad (2)$$

Deci un punct $M(\alpha, \beta)$ se află pe circumferința cercului C_1 dacă şi numai dacă coordonatele sale (α, β) verifică (2).

Se observă că dacă $M(\alpha, \beta)$ se află pe cercul C nu rezultă că şi $M(\beta, \alpha)$ se află pe C_1.

Astfel, numărul punctelor $M(\alpha, \beta)$ de pe cercul C_1 cu $(\alpha, \beta)\in\mathbb{Z}$ este egal cu numărul perechilor ordonate $(\alpha, \beta)\in\mathbb{Z}$ ce verifică ecuația (2).

Se observă că ecuația (2) este de tipul (1), astfel că numărul soluțiilor $(\alpha, \beta)\in\mathbb{Z}$ ale lui (2) este egal cu numărul soluțiilor ordonate $(x, y)\in\mathbb{Z}$ ce verifică (1), adică cu 4k/2=2k=n.

Cazul 2: n=2k+1. Analog ca în cazul 1, dacă vom considera ecuația (3) $x^2+y^2=5^{2k}$, numărul perechilor $(x, y)\in\mathbb{Z}$ ce verifică (3) este egal cu :

$$4[d_1(5^{2k})-d_2(5^{2k})] =4[(2k+1)-0]=8k+4.$$

Să observăm acum că punctul $M(\alpha, \beta)$ se află pe circumferința cercului $C_2(1/3, 0)$ şi rază $\frac{1}{3}\cdot 5^k \Leftrightarrow (\alpha-\frac{1}{3})^2+\beta^2=\frac{1}{9}\cdot 5^{2k}\Leftrightarrow$ (4) $(3\alpha-1)^2+\beta^2=5^{2k}$.

Astfel numărul de puncte laticiale $M(\alpha, \beta)$ de pe C_2 este egal cu numărul soluțiilor ordonate $(x, y)\in\mathbb{Z}$ ale ecuației (3) cu $x=3\alpha-1$ si $y=3\beta$. Pentru a determina numărul acesta, să împărțim cele 8k+4 soluții din $\mathbb{Z}$ ale lui (3) în 8 familii:

(x, y), (x,-y), (-x, y), (-x,-y), (y, x), (y, -x) (-y, x), (-y, -x).

Dacă de exemplu x=0 atunci familia se reduce la 4 soluții: (0, y), (0,-y), (y, 0), (-y, 0). De asemenea, dacă x=y există numai 4 soluții în familia de mai sus: (x, x), (-x, x), (x, -x), (-x, -x). (cum 5^{2k} este impar această posibilitate este exclusă).

Soluțiile lui (3) cu o componentă nulă sunt: $(0, 5^k)$, $(0, -5^k)$, $(5^k, 0)$ și $(-5^k,0)$.

În consecință, familia celor 8k+4 soluții se împarte în k familii de 8 soluții și o familie de 4 soluții.

Observăm de asemenea că ecuația (4) este de tipul (3) (cu $x \equiv -1(3)$ și $y \equiv 0(3)$) și că $5^{2k} = 25^k \equiv 1^k \equiv 1(3)$. Deoarece pătratul unui număr întreg este congruent cu 0 sau 1 modulo 3, dacă $(x, y)\in\mathbb{Z}$ și $x^2+y^2=5^{2k}$ atunci trebuie ca unul dintre x^2 sau y^2 să fie congruent cu 1 iar celălalt cu 0 modulo 3.

Fie x și –x termenii din familia celor 8 soluții ce sunt divizibili prin 3. În acest caz y sau –y este congruent cu –1 modulo 3. Să presupunem că $y \equiv -1(3)$. Atunci numai cele 2 soluții (y, x) și (y, -x) au primul termen congruent cu –1 modulo 3 și pe al doilea congruent cu 0 modulo 3 (observăm că în familia celor 4 soluții, $(-5^k, 0)$ sau $(5^k, 0)$ este de tipul de mai înainte).

În concluzie, fiecare din cele k familii de 8 soluții (x, y) ale lui (3) conțin exact 2 soluții ale lui (4) și o singură familie din cele 4 soluții ale lui (3) conține o singură soluție a lui (4). Obținem în total 2k+1=n soluții pentru (4), astfel că pe cercul C_2 se află exact 2k+1=n puncte laticiale. ■

<u>TEOREMA 1.4.(G. Browkin)</u> Pentru orice număr natural $n\in\mathbb{N}$, există în $\mathcal{E}$ un pătrat ce conține în interiorul său exact n puncte laticiale.

<u>Demonstrație</u> Vom încerca să „ordonăm” punctele laticiale din $\mathcal{E}$ într-un șir $P_1, P_2,\ldots$ Pentru aceasta vom utiliza funcția $f : \mathbb{Z}\times\mathbb{Z}\to\mathbb{R}_+$,

$f(x, y)=\left| x + y\sqrt{3} - \frac{1}{3} \right| + \left| x\sqrt{3} - y - \frac{1}{\sqrt{3}} \right|$, pentru orice $(x, y)\in\mathbb{Z}\times\mathbb{Z}$.

Să arătăm la început că dacă $(a, b), (c, d)\in\mathbb{Z}\times\mathbb{Z}$ și $f(a, b)=f(c, d)$, atunci $(a, b)=(c, d)$, adică a=c și b=d.

Într-adevăr, egalitatea f(a, b)=f(c, d) este echivalentă cu :

$$p(a + b\sqrt{3} - \frac{1}{3}) + q(a\sqrt{3} - b - \frac{1}{\sqrt{3}}) = r(c + d\sqrt{3} - \frac{1}{3}) + s(c\sqrt{3} - d - \frac{1}{\sqrt{3}})$$

cu $p, q, r, s\in\{\pm1\}$.

Ţinând cont că $\sqrt{3}$ este număr iraţional şi că o egalitate de forma $x+y\sqrt{3}=x'+y'\sqrt{3}$ cu $(x, y), (x' y')\in\mathbb{Z}\times\mathbb{Z}$ implică $x=x'$ şi $y=y'$, din (1) deducem că :

$$\begin{cases} pa-qb-rc+sd+\dfrac{r-p}{3}=0 \quad \text{şi} \\ rd+sc-pb-qa+\dfrac{q-s}{3}=0 \end{cases} \qquad (2)$$

Din (2) deducem cu necesitate că $\dfrac{r-p}{3}, \dfrac{q-s}{3}\in\mathbb{Z}$, lucru posibil doar pentru r = p şi q = s, astfel că (2) capătă forma echivalentă:

$$(3) \qquad \begin{cases} p(a-c)+q(d-b)=0 \\ p(d-b)+q(c-a)=0 \end{cases}$$

Multiplicând prima egalitate din (3) cu p şi pe a doua cu q şi scăzându-le, obţinem egalitatea $(a-c)(p^2+q^2)=0 \Leftrightarrow 2(a-c)=0 \Leftrightarrow a=c$. Deducem atunci şi că b=d.

Să vedem ce interpretare geometrică are f.

Pentru aceasta considerăm în $\mathcal{E}$ dreptele d şi d' de ecuaţii:

$(d): x+y\sqrt{3}-\dfrac{1}{3}=0$

$(d'): x\sqrt{3}-y-\dfrac{1}{\sqrt{3}}=0$

Evident, $d \perp d'$ şi $(d)\cap(d')=\{(1/3, 0)\}$.

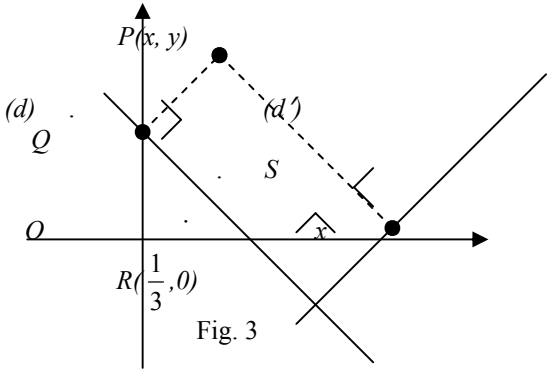


Fig. 3

Ținând cont de formula ce dă distanța unui punct P(x, y) la (d) și respectiv (d'), deducem imediat că f(x, y)=2PQ+2PS, adică f(x, y) este perimetrul dreptunghiului PQRS din figura 3 de mai sus.

Găsim atunci un punct laticial $P_1(x_1, y_1)$ în apropierea lui R pentru care $f(x_1, y_1)$ este cea mai mică valoare a lui f(x, y) (când $x, y \in \mathbb{Z}$). Conform celor stabilite la început punctul P_1 este unic.

În felul acesta putem ordona punctele laticiale într-un șir $P_1, P_2, \ldots$ (scriind că $P_i(x_i, y_i) < P_{i+1}(x_{i+1}, y_{i+1}) \Leftrightarrow f_i(x_i, y_i) < f_{i+1}(x_{i+1}, y_{i+1})$).

Dacă $P_n(x_n, y_n)$ este a n-lea punct laticial în această ordonare, să notăm $a_n=f(x_n, y_n)$, iar $h(x, y)=x(1+\sqrt{3})+y(\sqrt{3}-1)-\frac{1}{3}-\frac{1}{\sqrt{3}}$

$$g(x, y)=x(1-\sqrt{3})+y(1+\sqrt{3})-\frac{1}{3}+\frac{1}{\sqrt{3}}$$

Să considerăm acum cele 4 drepte : $h(x, y) = \pm a_{n+1}$ și $g(x, y) = \pm a_{n+1}$; se verifică imediat că cele 4 drepte formează un pătrat.

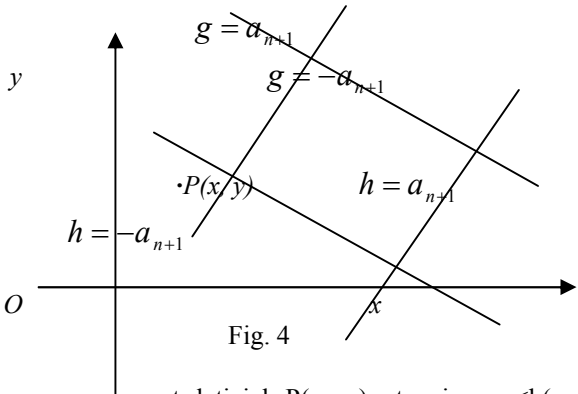


Fig. 4

Dacă avem un punct laticial P(x, y) atunci $-a_{n+1}<h(x, y)<a_{n+1} \Leftrightarrow |h(x, y)|<a_{n+1}$, adică P se găsește între dreptele de ecuație $h(x, y)=a_{n+1}$ și $h(x, y)= -a_{n+1}$ și reciproc.

Similar, se deduce că punctul P(x,y) se află între dreptele de ecuații $g(x, y)=a_{n+1}$ și $g(x, y)=-a_{n+1} \Leftrightarrow |g(x, y)|<a_{n+1}$.

Astfel punctul P(x, y) se află în interiorul pătratului din figura 4 $\Leftrightarrow |h(x, y)|<a_{n+1}$ și $|g(x, y)|<a_{n+1}$.

Însă se verifică imediat că pentru numerele reale a, b, c:

$|a|<c$ și $|b|<c \Leftrightarrow \left|\frac{a+b}{2}\right|+\left|\frac{a-b}{2}\right|<c$ și astfel :

$$\begin{cases} |h(x, y)|<a_{n+1} \\ \text{și} \\ \left|\frac{h(x, y)+g(x, y)}{2}\right|+\left|\frac{h(x, y)-g(x, y)}{2}\right|<a_{n+1} \Leftrightarrow f(x, y)<a_{n+1}, \\ |g(x, y)|<a_{n+1} \end{cases}$$

adică punctul laticial P(x, y) se află în interiorul pătratului din Fig. 4 dacă și numai dacă $f(x, y)<a_{n+1}$.

Atunci în interiorul pătratului din figură sunt exact punctele laticiale $P_1, P_2, \ldots, P_n$, ce sunt în număr de n. ■

<u>TEOREMA 1.5. (Pick)</u> Fie P un poligon convex în plan care conține m puncte laticiale în interiorul său, k puncte laticiale pe laturi sau vârfuri și vârfurile sale sunt puncte laticiale.

Atunci Aria(P)=m+ $\frac{k}{2}$ **-1.**

Demonstrație Să demonstrăm formula la început pentru cazul m=0, k=3 (aceasta exprimă faptul că P este un triunghi cu vârfurile în nodurile rețelei şi care nu mai conține alte noduri pe laturi sau în interior). Atunci S=1/2 (vezi figura 5)

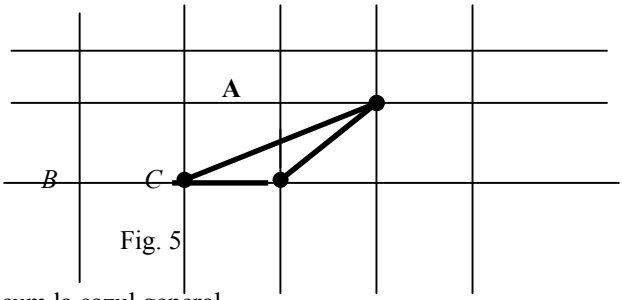


Fig. 5

Să trecem acum la cazul general.

Descompunem poligonul P în triunghiuri cu vârfurile în puncte laticiale şi care nu mai conțin puncte laticiale pe laturi sau în interior.

Vom calcula numărul n de triunghiuri de mai sus în două moduri exprimând în două moduri suma unghiurilor lor.

Pe de altă parte suma unghiurilor lor este $180^\circ \cdot$ n iar pe de altă parte suma unghiurilor lor este egală cu suma unghiurilor poligonului şi a unghiurilor din jurul punctelor interioare, adică $180^\circ \cdot (k-2) + 360^\circ \cdot m$.

Deci $180^\circ \cdot n = 180^\circ \cdot (k-2) + 360^\circ \cdot m$, de unde n=2m+k-2 şi cum S=n/2 deducem că S= m+ $\frac{k}{2}$ -1. ■

Observații 1. Teorema lui Pick este valabilă şi pentru poligoane oarecare (nu neapărat convexe), însă demonstrația ei este diferită de cazul convex.

Pentru aceasta vom considera două poligoane Q_1 şi Q_2 care au toate vârfurile în puncte laticiale şi care sunt adiacente prin una din laturile comune AB (vezi figura 6).

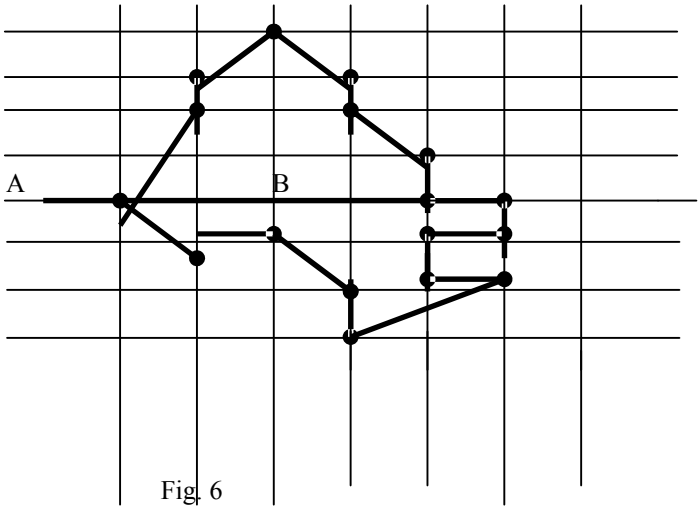


Fig. 6

Să presupunem cunoscut că formula $S= m+\frac{k}{2}-1$ este adevărată pentru amândouă aceste poligoane ; vom demonstra că în acest caz, formula va fi adevărată şi pentru poligonul mai mare Q, obţinut prin reuniunea lui Q_1 şi Q_2.

Într-adevăr, fie S_1, m_1 şi k_1 – aria, numărul punctelor laticiale din interiorul poligonului şi numărul punctelor laticiale de pe frontiera lui Q_1, iar S_2, m_2 şi k_2-numerele corespunzătoare pentru poligonul Q_2.

Conform ipotezei avem $S_1=m_1+\frac{k_1}{2}-1$ şi $S_2=m_2+\frac{k_2}{2}-1$.

Vom nota cu k' numărul nodurilor reţelei de pătrate situate pe segmentul AB, care conţine punctele A şi B. Pentru poligonul Q, aria sa S, numărul m de puncte laticiale din interiorul său şi numărul k de puncte laticiale de pe frontiera sa vor fi exprimate cu ajutorul lui m_1, m_2, k_1, k_2 şi k' astfel: $S=S_1+S_2$, $m=m_1+m_2+(k'-2)$ (la punctele laticiale interioare se vor adăuga toate punctele laticiale situate pe AB cu excepţia lui A şi B) şi $k=(k_1-k')+(k_2-k')+2$ (în ultimul termen +2 figurează nodurile A şi B). Deci:

$$S=S_1+S_2= m_1+\frac{k_1}{2}-1+ m_2+\frac{k_2}{2}-1=(m_1+m_2+k'-2)+\frac{k_1+k_2-2k'+2}{2}-1=m+\frac{k}{2}-1.$$

Formula de demonstrat la modul general se poate stabili acum inductiv.

2. Merită să mai amintim şi un rezultat datorat lui Hermann Minkowski legat de punctele laticiale:

Dacă un poligon convex simetric față de centrul său (care este un punct laticial) nu mai conține în interiorul său alte puncte laticiale, atunci aria sa este < 4 (ca unitate de arie se consideră aria unui pătrat al rețelei).

Nu vom prezenta aici demonstrația teoremei lui Minkowski deoarece ea este destul de laborioasă, dar în esență este asemănătoare cu cea a teoremei lui Pick. (indicăm cititorului lucrarea [13]).

Pentru un număr natural n fie $\tau(n)$=numărul de reprezentări ale lui n ca sumă de două pătrate de numere naturale (două reprezentări fiind considerate diferite dacă diferă ordinea termenilor)- vezi Teorema 1.7. de la Capitolul 11.

De exemplu : $\tau(1)=4$, $\tau(2)=4$, $\tau(3)=0$, $\tau(5)=8$, $\tau(6)=0$, $\tau(7)=0$, $\tau(8)=4$, $\tau(9)=4$, $\tau(10)=8$.

După cum am văzut mai înainte orice număr prim de forma 4k+1are o unică reprezentare ca sumă de două pătrate de numere naturale (dacă nu ținem cont de ordinea termenilor ; vezi Propoziția 1.5. de la Capitolul 11). De aici deducem că dacă p este prim de forma 4k+1, atunci $\tau(p)=8$ (căci dacă (a, b) este o soluție, atunci sunt soluții şi (b, a) ca şi (±a, ±b), (±b, ±a)).

Observăm că dacă $n=x^2+y^2$ atunci $|x|, |y| \le \sqrt{n}$, deducem imediat că $\tau(n) \le 4\sqrt{n}$.

Pentru $n \in \mathbb{N}^*$, fie $T(n)=\tau(1)+\tau(2)+\ldots+\tau(n)$. Atunci T(n) este numărul de soluții din $\mathbb{Z}$ ale inegalităților: $0< x^2+y^2 \le n$.

<u>LEMA 1.6</u>. Pentru orice $n \in \mathbb{N}^*$, $T(n)=4\sum_{k=0}^{[\sqrt{n}]}[\sqrt{n-k^2}]$.

<u>Demonstrație</u> Dacă x=0, atunci $y^2 \le n \Leftrightarrow |y| \le \sqrt{n}$, deci numărul numerelor y pentru care $0 < x^2+y^2 \le n$ este $2[\sqrt{n}]$.

Dacă $x=k\neq 0$, atunci $k^2 \le n$, deci $|k| \le \sqrt{n}$ iar $y^2 \le n-k^2$, adică $|y| \le \sqrt{n-k^2}$ (deci numărul y-cilor este $1+2[\sqrt{n-k^2}]$; am adunat şi pe 1 deoarece y=0 trebuie considerat).

Deoarece $k \in \{\pm 1, \pm 2, \ldots, \pm[\sqrt{n}]\}$ iar semnele ± nu influențează valoarea lui k^2, obținem că:

$$T(n)=2[\sqrt{n}]+2\sum_{k=1}^{[\sqrt{n}]}[1+2\sqrt{n-k^2}]=4[\sqrt{n}]+4\sum_{k=1}^{[\sqrt{n}]}[\sqrt{n-k^2}]=4\sum_{k=0}^{[\sqrt{n}]}[\sqrt{n-k^2}].$$

Astfel, de exemplu pentru n=100, avem:

T(100)=

$$= 4([\sqrt{100}]) + [\sqrt{99}] + [\sqrt{96}] + [\sqrt{91}] + [\sqrt{84}] + [\sqrt{75}] + [\sqrt{64}] + [\sqrt{51}] + [\sqrt{36}] +$$
$$+ [\sqrt{19}]) = 4(10 + 9 + 9 + 9 + 9 + 8 + 8 + 7 + 6 + 4) = 316$$

Interpretare geometrică pentru T(n)

Pentru $n \in \mathbb{N}$, 1+T(n) reprezintă numărul de perechi din $\mathbb{Z}^2$ ce satisface inegalitatea $x^2+y^2 \leq n$.

Astfel 1+T(n) reprezintă numărul punctelor laticiale din interiorul cercului C_n de centru (0, 0) şi rază $\sqrt{n}$ (eventual de pe circumferință).

În continuare, la fiecare punct laticial vom asocia un pătrat ce are centrul în punctul respectiv, laturile paralele cu axele de coordonate şi aria 1 (vezi Fig.7).

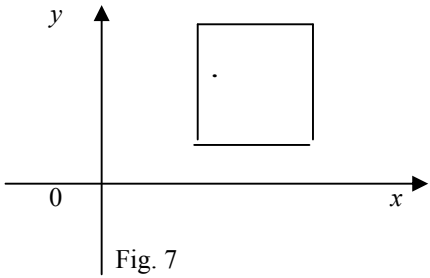


Fig. 7

Dacă notăm cu P aria acoperită de pătratele asociate punctelor laticiale care nu sunt în afara cercului C_n este egală cu numărul acestora, adică P=1+T(n).

Cercul C_{1n} de centru (0, 0) şi rază $\sqrt{n} + \frac{1}{\sqrt{2}}$ conține în interior sau pe circumferință toate punctele acoperite de pătratele asociate punctelor laticiale din C_n (aceasta deoarece în mod evident $\frac{1}{\sqrt{2}}$ este cea mai mare distanță posibilă a unui punct din interiorul pătratului de arie 1 la centrul pătratului).

Atunci P ≤ aria $(C_{1n}) \Leftrightarrow P \leq \pi (\sqrt{n} + \frac{1}{\sqrt{2}})^2$.

Pe de altă parte, dacă notăm cu C_{2n} cercul de centru (0, 0) şi rază $\sqrt{n} - \frac{1}{\sqrt{2}}$, atunci din aria $(C_{2n}) \le P$ deducem că $\pi (\sqrt{n} - \frac{1}{\sqrt{2}})^2 \le P$.

Înlocuind P=1+T(n) deducem că $\pi (\sqrt{n} - \frac{1}{\sqrt{2}})^2 - 1 < T(n) < \pi (\sqrt{n} - \frac{1}{\sqrt{2}})^2 - 1$.

Cum $\pi\sqrt{2} < 5$ şi $0 < \frac{1}{2}\pi - 1 < 1 \le \sqrt{n}$ deducem că:

$$\pi (\sqrt{n} + \frac{1}{\sqrt{2}})^2 - 1 = \pi n + \pi\sqrt{2}\sqrt{n} + \frac{1}{2}\pi - 1 < \pi n + 6\sqrt{n}$$

şi $$\pi (\sqrt{n} - \frac{1}{\sqrt{2}})^2 - 1 = \pi n - \pi\sqrt{2}\sqrt{n} + \frac{1}{2}\pi - 1 > \pi n - 6\sqrt{n}$$

de unde $\pi n - 6\sqrt{n} < T(n) < \pi n + 6\sqrt{n} \Leftrightarrow \left| \frac{T(n)}{n} - \pi \right| < \frac{6}{\sqrt{n}}$ iar de aici deducem :

PROPOZIŢIA 1.7. $\lim_{n \to \infty} \frac{T(n)}{n} = \pi$.

După cum am văzut T(100)=316, deci T(100)/100=3,16. Analog T(400)=1256, deci T(400)/400=3,14 iar T(1000)/1000=3,148.

Avem astfel posibilitatea de a aproxima pe π considerând valori din ce în ce mai mari pentru n.

§2. Puncte laticiale în spaţiu

Considerăm spaţiul $\mathbb{R}^3$ raportat la un sistem ortogonal de axe 0xyz.

DEFINIŢIA 2.1. Un punct $M(x, y, z) \in \mathbb{R}^3$ se zice punct laticial, dacă $(x, y, z) \in \mathbb{Z}^3$.

Multe rezultate legate de puncte laticiale din plan au extinderi aproape imediate la puncte laticiale din spaţiu.

LEMA 2.2. Dacă p, q, r$\in\mathbb{Q}$ şi $p\sqrt{2} + q\sqrt{3} + r\sqrt{5} \in \mathbb{Q}$, atunci p=q=r=0.

Demonstrație Fie $p\sqrt{2}+q\sqrt{3}+r\sqrt{5}=k\in\mathbb{Q}$. Atunci $p\sqrt{2}+q\sqrt{3}=k-r\sqrt{5}$, de unde $2p^2+2pq\sqrt{6}+3q^2=k^2-2kr\sqrt{5}+5r^2$. Deducem că $2pq\sqrt{6}+2kr\sqrt{5}=k^2+5r^2-2p^2-3q^2\in\mathbb{Q}$, de unde $2pq=2kr=k^2+5r^2-2p^2-3q^2=0$ iar de aici p = q = r = 0. ■

TEOREMA 2.3. Pentru orice număr natural $n\in\mathbb{N}^*$ există în spațiu o sferă ce conține în interiorul său exact n puncte laticiale.

Demonstrație Să arătăm la început că sfera de centru $(\sqrt{2},\sqrt{3},\sqrt{5})$ are cel mult un punct laticial pe suprafața ei.

Într-adevăr, să presupunem că pe suprafața sferei cu centrul în punctul de coordonate $(\sqrt{2},\sqrt{3},\sqrt{5})$ există două puncte laticiale de coordonate (a, b, c) respectiv (d, e, f).

Scriind că

$$(a-\sqrt{2})^2+(b-\sqrt{3})^2+(c-\sqrt{5})^2=(d-\sqrt{2})^2+(e-\sqrt{3})^2+(f-\sqrt{5})^2$$

obținem $2\sqrt{2}(d-a)+2\sqrt{3}(e-b)+2\sqrt{5}(f-c)=d^2+e^2+f^2-a^2-b^2-c^2\in\mathbb{Q}$ și atunci conform Lemei 2.2., d-a = e-b = f-c = 0 $\Leftrightarrow$ a = d, b = e, c = f.

Analog ca în cazul plan (teorema 1.2.) putem ordona punctele laticiale din spațiu într-un șir crescător M_1, M_2, … în funcție de distanțele d_1, d_2, … ale acestora la punctul de coordonate $(\sqrt{2},\sqrt{3},\sqrt{5})$. Astfel, sfera cu centrul în punctul de coordonate $(\sqrt{2},\sqrt{3},\sqrt{5})$ și rază d_{n+1} conține în interiorul său exact n puncte laticiale din spațiu și anume pe M_1, M_2, …, M_n . ■

TEOREMA 2.4. (T. Kulikowski) Pentru orice număr natural $n\in\mathbb{N}^*$ există în spațiu o sferă ce conține pe suprafața sa exact n puncte laticiale.

Demonstrație Conform Teoremei 1.3. există un cerc în planul 0xy de ecuație $(x-a)^2+(y-b)^2=c$ (cu a, b, $c\in\mathbb{Q}$, c>0) ce trece prin exact n puncte laticiale de coordonate (x, y). Identificând punctele laticiale de coordonate (x, y) din planul 0xy cu punctele de coordonate (x, y, 0) din spațiul 0xyz putem trage concluzia că cercul $(x-a)^2+(y-b)^2=c$ conține exact n puncte laticiale (x, y, 0) din spațiu.

Să considerăm acum sfera cu centrul în punctul de coordonate $(a, b, \sqrt{2})$ și de rază $\sqrt{c+2}$ a cărei ecuație în sistemul de axe 0xyz este :

(1) $(x-a)^2+(y-b)^2+\left(z-\sqrt{2}\right)^2=c+2 \quad \Leftrightarrow$

(2) $(x-a)^2+(y-b)^2+z^2-2z\sqrt{2}=c$

Conform Teoremei lui Schinzel a, b, c$\in\mathbb{Q}$ (putem avea de exemplu a=$\frac{1}{2}$ sau $\frac{1}{3}$ şi b=0 iar c pătratul unui număr întreg).

Astfel, dacă (x, y, z)$\in\mathbb{Z}^3$ verifică ecuația (2), atunci cu necesitate z=0 şi atunci obținem $(x-a)^2+(y-b)^2=c$ ce are numai n soluții.

Cele n puncte laticiale de pe sfera de ecuație (1) sunt cele ce se obțin intersectând suprafața sferică cu planul de ecuație z=0 (obținând astfel cercul de ecuație (2) ce trece prin exact n puncte laticiale).

În concluzie, sfera de centru (a, b, $\sqrt{2}$) şi rază $\sqrt{c+2}$ trece prin exact n puncte laticiale din spațiu de forma (x, y, 0). ■