Despre autori

Dumitru Buşneag

Este absolvent al Facultăţii de Matematică a Universităţii din Bucureşti, promoţia 1974.

In perioada 1974-1980 a funcţionat ca profesor de matematică în învăţământul preuniversitar (la Liceul de Industrie alimentară şi Colegiul Naţional ≪ Carol I ≫ din Craiova).

Din anul 1980 devine Asistent universitar la Facultatea de Matematică-Informatică a Universităţii din Craiova.

In anul 1985 îşi susţine teza de doctorat intitulată *Contribuţii la studiul algebrelor Hilbert* în cadrul Institutului Central de Matematică din Bucureşti sub coordonarea domnului Dr. Doc. Nicolae Popescu-Membru corespondent al Academiei Române.

Din anul 1995 ocupă funcţia didactică de Profesor la Catedra de algebră şi geometrie a Facultăţii de Matematică-Informatică a Universităţii din Craiova.

Din anul 1978 este membru al Comisiei Centrale a MEdC pentru concursurile de matematică ale elevilor, iar din anul 2000 Preşedinte al Comisiei de organizare al Concursului interjudeţean de matematică ≪ Gheorghe Ţiţeica ≫ pentru echipaje de elevi, concurs ajuns la a XXIX-a ediţie.

Florentina Chirteş

Este absolventă a Facultăţii de Matematică-Informatică a Universităţii din Craiova, promoţia 1997.

In anul universitar 1997-1998 urmează Studiile aprofundate de algebră şi geometrie la Facultatea de Matematică-Informatică a Universităţii din Craiova.

In anul 1999 devine Preparator universitar, în anul 2003 Asistent iar din 2007 Lector la Catedra de algebră şi geometrie a Facultăţii de Matematică-Informatică a Universităţii din Craiova.

Din 2000 face parte din Comitetul de organizare al Concursului interjudeţean de matematică ≪ Gheorghe Ţiţeica ≫ pentru echipaje de elevi.

In anul 2007, pe 26 ianuarie şi-a susţinut teza de doctorat intitulată *Contribution to the study of LM_n-algebras* în cadrul Facultăţii de Matematică şi Informatică a Universităţii din Bucureşti sub coordonarea domnului Prof. univ. dr. Sergiu Rudeanu.

Dana Piciu

Este absolventă a Facultăţii de Matematică-Informatică a Universităţii din Craiova, promoţia 1997.

In perioada 1997-1999 a funcţionat ca profesoară de matematică în învăţământul preuniversitar iar în anul universitar 1997-1998 urmează Studiile aprofundate de algebră şi geometrie la Facultatea de Matematică-Informatică a Universităţii din Craiova.

In anul 1999 devine Preparator universitar la Facultatea de Matematică-Informatică a Universităţii din Craiova.

In anul 2004 îşi susţine teza de doctorat intitulată *Localizations of MV and BL-algebras* în cadrul Facultăţii de Matematicăşi Informatică a Universităţii din Bucureşti sub coordonarea domnului Prof. univ. dr. George Georgescu.

Din anul 2005 ocupă funcţia didactică de Lector la Catedra de algebră şi geometrie a Facultăţii de Matematică-Informatică a Universităţii din Craiova.

Din 2000 face parte din Comitetul de organizare al Concursului interjudeţean de matematică $\ll$ Gheorghe Ţiţeica $\gg$ pentru echipaje de elevi.

Prefaţă

Această lucrare este în esenţă o ediţie revizuită şi îmbunătăţită a lucrării [6] elaborată de aceeaşi autori şi acoperă atât programa analitică a cursului de *Teoria elementară a numerelor* ţinut de autori studenţilor de la Facultatea de Matematică-Informatică a Universităţii din Craiova, cât şi programa tradiţionalelor concursuri de matematică ale elevilor din învăţământul preuniversitar.

Lucrarea este structurată pe 9 capitole şi în cea mai mare parte are un caracter elementar, fapt ce o face accesibilă unor categorii destul de numeroase de cititori: elevi, studenţi, profesori precum şi tuturor celor ce iubesc matematicile elementare.

Tehnoredactarea şi corectura sunt efectuate de autori.

Craiova, 11 mai 2007 Autorii

Cuprins

Capitolul 1

Elemente de aritmetică

1.1 Divizibilitate pe N

Definiţia 1.1.1. Fie $a, b \in \mathbf{N}, b \neq 0$.Vom spune că b *divide* a şi vom scrie $b|a$, dacă există $c \in \mathbf{N}$ astfel încât $a = bc$ (nu definim divizibilitatea prin 0!). In acest caz vom spune că b este un *divizor* al lui a (sau că a este *multiplu* de b).

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

Definiţia 1.1.2. Un număr $p \in \mathbf{N}, p \geq 2$ 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). Astfel, singurul număr prim par este 2. Reamintim că în [6], Corolarul 4.9 am demonstrat teorema împărţirii cu rest în $\mathbf{N}$: dacă $a, b \in \mathbf{N}, b \geq 1$, atunci există şi sunt unici $c, r \in \mathbf{N}$ astfel încât $a = bc + r$, iar $0 \leq r < b$; numărul c se numeşte *câtul* împărţirii lui b la a, iar r *restul* acestei împărţiri (evident $b|a$ dacă şi numai dacă $r = 0$).

Teorema 1.1.3. *Fiind date două numere $a, b \in \boldsymbol{N}$, există $d \in \boldsymbol{N}$ (vom nota $d = (a, b)$) astfel încât $d|a, d|b$, iar dacă mai avem $d' \in \boldsymbol{N}$ astfel încât $d'|a$ şi $d'|b$, atunci $d'|d$ (adică în mulţimea parţial ordonată $(N, |)$ pentru orice două elemente a şi b există $a \wedge b$).*

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

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

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

Dacă $r_2 = 0$, atunci $d = r_1$. Intr-adevăr, din $b = r_1c_2$ deducem că $d|b$, iar din $a = bc_1 + r_1$ deducem că $d|a$. Dacă mai avem $d' \in \mathbf{N}$ astfel încât $d'|a$ 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 $r_1 = r_2c_3 + r_3$, cu $0 \leq r_3 < r_2$, şi algoritmul descris până acum continuă, obţinându-se un şir descrescător de numere naturale $r_1, r_2, ...$ astfel încât $r_{j-2} = r_{j-1}c_j (j \geq 3)$. Conform Corolarului 4.6. de la Capitolul 1, §4 din lucrarea [6], şirul $r_1, r_2, r_3, ...$ este staţionar.

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 :

$$\begin{aligned} 49 &= 1 \cdot 35 + 14 \quad (c_1 = 1, r_1 = 14) \\ 35 &= 2 \cdot 14 + 7 \quad (c_2 = 2, r_2 = 7) \\ 14 &= 2 \cdot 7 \quad (c_3 = 2, r_3 = 0) \end{aligned}$$

de unde deducem că $(49, 35) = 7$.

Dacă $a = 187$ şi $b = 35$ avem:

$$\begin{aligned} 187 &= 5 \cdot 35 + 12 \quad (c_1 = 5, r_1 = 12) \\ 35 &= 2 \cdot 12 + 11 \quad (c_2 = 2, r_2 = 11) \\ 12 &= 1 \cdot 11 + 1 \quad (c_3 = 1, r_3 = 1) \end{aligned}$$

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 $a, b \in \mathbf{N}$ 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 $a_1, a_2, ..., a_n (n \geq 2)$ există $d \in \mathbf{N}$ astfel încât $d|a_i$ pentru orice $1 \leq i \leq n$ şi dacă mai avem $d' \in \mathbf{N}$ astfel încât $d'|a_i$ pentru orice $1 \leq i \leq n$, atunci $d'|d$. Numărul d se notează prin $d = (a_1, a_2, ..., a_n)$ şi poartă numele de *cel mai mare divizor comun* al numerelor $a_1, a_2, ..., a_n$.

1.2 Divizibilitate pe Z

Definiţia 1.2.1. Dacă $a, b \in \mathbf{Z}, b \neq 0$, vom spune că b *divide* a (vom scrie $b|a$) dacă există $c \in \mathbf{Z}$ astfel încât $a = bc$ (ca şi în cazul lui $\mathbf{N}$ nu vom defini, nici în cazul lui $\mathbf{Z}$, divizibilitatea prin 0).

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

Numerele prime în $\mathbf{Z}$ 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 $\mathbf{Z}$ sunt numerele de forma $\pm p$, cu $p \geq 2$ număr prim în $\mathbf{N}$.

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

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

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

3) Dacă $a|b$ şi $b|c$, atunci $a|c$.

Teorema 1.2.2. *(Teorema împărţirii cu rest în $\boldsymbol{Z}$) Dacă $a, b \in \boldsymbol{Z}, b > 0$, atunci există $c, r \in \boldsymbol{Z}$ astfel încât $a = cb + r$, cu $0 \leq r < b$.*

Demonstraţie. Fie $P = \{a - xb : x \in \mathbf{Z}\}$; evident în P avem şi numere naturale. Fie $r = a - cb$ cel mai mic număr natural din P (cu $c \in \mathbf{Z}$)(un astfel de număr există conform Teoremei 4.5 din [6]). Avem $0 \leq r < b$ căci dacă $r = a - cb \geq b$ atunci $0 \leq a - (c+1)b < r$, ceea ce contrazice minimalitatea lui r. ■

Observaţii.

1. Putem formula teorema împărţirii cu rest din $\mathbf{Z}$ şi sub forma: Dacă $a, b \in \mathbf{Z}, b \neq 0$, atunci există $c, r \in \mathbf{Z}$ astfel încât $a = cb + r$, 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 $c', r' \in \mathbf{Z}$ astfel încât $a = c'b + r'$, 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 $b|r' - r$ implică $r' - r = 0 \Leftrightarrow r' = r$ şi cum $(c - c')b = r' - r = 0$, deducem imediat că $c = c'$.

Definiţia 1.2.3. Numim *ideal* al inelului $(\mathbf{Z}, +, \cdot)$ orice submulţime nevidă $\underline{a} \in \mathbf{Z}$ astfel încât

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

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

Propoziţia 1.2.4. *Fie $\underline{a} \in \boldsymbol{Z}$ un ideal. Atunci există $d \in \boldsymbol{N}$ astfel încât $\underline{a} = d\boldsymbol{Z}$.*

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 $x \in \mathbf{N}^*$, iar dacă $x < 0$, cum $\underline{a}$ este un ideal, $-x \in \underline{a}$, şi atunci $-x \in \mathbf{N}^*$.

In concluzie, $\underline{a} \cap \mathbf{N}^* \neq \emptyset$. Conform Teoremei 4.5 din [6], putem alege $d \in \underline{a} \cap \mathbf{N}^*$ ca fiind cel mai mic element din $\underline{a} \cap \mathbf{N}^*$ şi să demonstrăm că $\underline{a} = d\mathbf{Z}$. Cum $d \in \underline{a}$ şi $\underline{a}$ este ideal al inelului $\mathbf{Z}$, incluziunea $dZ \in \underline{a}$ este imediată. Fie acum $a \in \underline{a}$. Conform Teoremei 1.2.2 putem scrie $a = cd + r$, cu $c, r \in \mathbf{Z}$ şi $0 \leq r < d$ (căci $d \in \mathbf{N}^*$). 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 $a = cd \in d\mathbf{Z}$, de unde şi incluziunea inversă $\underline{a} \in d\mathbf{Z}$, care ne asigură egalitatea $\underline{a} = d\mathbf{Z}$.

Propoziţia 1.2.5. *Fie $a_1, a_2, ..., a_n \in \boldsymbol{Z}$. Dacă notăm prin $< a_1, a_2, ..., a_n >$ idealul generat de $\{a_1, a_2, ..., a_n\}$, atunci $< a_1, a_2, ..., a_n >= \{k_1a_1 + ... + k_na_n : k_i \in \boldsymbol{Z}, 1 \leq i \leq n\}$.*

Demonstraţie. Dacă notăm $\underline{a} = \{k_1a_1 + ... + k_na_n : k_i \in \mathbf{Z}, 1 \leq i \leq n\}$, se arată imediat că $\underline{a}$ este ideal al lui $\mathbf{Z}$ ce conţine $\{a_1, a_2, ..., a_n\}$. Cum $< a_1, a_2, ..., a_n >$ este cel mic ideal al lui $\mathbf{Z}$ ce include $\{a_1, a_2, ..., a_n\}$, deducem că $< a_1, a_2, ..., a_n > \subseteq \underline{a}$.

Pentru incluziunea inversă ţinem cont de faptul că:

$$< a_1, a_2, ..., a_n >= \bigcap_{\substack{\underline{b} \subseteq \mathbf{Z} \text{ ideal}, \\ \{a_1, a_2, ..., a_n\} \subseteq \underline{b}}} \underline{b}$$

şi fie deci $\underline{b} \in \mathbf{Z}$ un ideal astfel încât $\{a_1, a_2, ..., a_n\} \in \underline{b}$. Atunci pentru orice $k_1, .., k_n \in \mathbf{Z}$ avem $k_1a_1 + ... + k_na_n \in \underline{b}$, adică $\underline{a} \subseteq \underline{b}$ şi cum $\underline{b}$ este oarecare, deducem că $\underline{a} \subseteq \bigcap \underline{b} =< a_1, a_2, ..., a_n >$, de unde egalitatea dorită. ■

Fiind date $a_1, a_2, ..., a_n \in \mathbf{Z}$, prin *cel mai mare divizor comun al numerelor* $a_1, a_2, ..., a_n$ înţelegem acel număr $d \in \mathbf{Z}$ astfel încât $d|a_i$ 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 $a_1, a_2, ..., a_n$ acel număr natural d cu proprietăţile de mai înainte şi vom nota $d = (a_1, a_2, ..., a_n)$ (vezi şi §1 pentru cazul numerelor naturale).

Teorema 1.2.6. *Fiind date n numere întregi* $a_1, a_2, ..., a_n (n \geq 2)$*, dacă notăm prin d numărul natural a cărui existenţă este asigurată de Propoziţia 1.2.4 pentru idealul* $\underline{a} =< a_1, a_2, ..., a_n >$*, atunci* $d = (a_1, a_2, ..., a_n)$.

Demonsraţie. Intr-adevăr, cum fiecare $a_i \in < a_1, a_2, ..., a_n >= d\mathbf{Z}$ deducem că $a_i \in d\mathbf{Z}$, adică $d|a_i$ pentru $1 \leq i \leq n$.

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

Corolar 1.2.7. *Fiind date n numere întregi* $a_1, a_2, ..., a_n (n \geq 2)$*,* $d = (a_1, a_2, ..., a_n)$ *dacă şi numai dacă există* $k_1, ..., k_n \in \boldsymbol{Z}$ *astfel încât* $d = k_1a_1 + ... + k_na_n$.

1.3 Teorema fundamentală a aritmeticii

Fie $a \in \mathbf{Z}^*$ şi $p \in \mathbf{N}$, $p \geq 2$, un număr prim. In mod evident, există $k \in \mathbf{N}$ astfel încât $p^k|a$ şi $p^{k+1} \nmid a$ (altfel zis, k este cel mai mare număr natural cu proprietatea $p^k|a$). 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 1.3.1. *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 adevarată, atunci $A \neq \emptyset$. Conform Teoremei 4.5 din [6] mulţimea A va conţine un element minimal x. In 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 1.3.2. *Pentru orice $n \in \boldsymbol{Z}^*$ există numerele întregi prime $p_1, ..., p_m$ astfel încât $n = p_1^{k_1}...p_m^{k_m}$ cu $k, ..., k_m \in \boldsymbol{N}$.*

Putem folosi şi notaţia: $n = (-1)^{\varepsilon(n)} \prod_{\substack{p \text{ prim}, \\ p \geq 2}} p^{e(p)}$, 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 1.3.3. *Dacă $a, b, c \in \boldsymbol{Z}^*$ astfel încât $(a, b) = 1$ şi $a|bc$, atunci $a|c$.*

Demonstraţie. Intr-adevăr, cum $(a, b) = 1$ conform Corolarului 1.2.7 există $r, s \in \mathbf{Z}$ astfel încât $ra + sb = 1$, de unde $c = rac + sbc$. Cum $a|bc$ deducem că $a|rac + sbc = c$, adică $a|c$. ■

Observaţie.

Dacă $(a, b) \neq 1$, atunci lema de mai înainte nu mai este adevarătă tot timpul căci, de exemplu, $6 \mid 3 \cdot 8 = 24$, dar $6 \nmid 13$ şi $6 \nmid 18$.

Corolar 1.3.4. *Dacă $p, a, b \in \boldsymbol{Z}$ astfel încât p este prim şi $p|ab$, atunci $p|a$ sau $p|b$.*

Demonstraţie. Intr-adevăr, singurii divizori ai lui $p \in \mathbf{Z}$ sunt $\pm 1, \pm p$.

Atunci $(p, b) = 1$ sau $p|b$. Dacă $p|b$ totul este în regulă, iar dacă $(p, b) = 1$, atunci se aplică Lema 1.3.5. ■

Observaţie.

Putem utiliza corolarul de mai înainte şi sub forma: dacă $p, a, b \in \mathbf{Z}$ astfel încât p este prim iar $p \nmid a, p \nmid b$, atunci $p \nmid ab$.

Corolar 1.3.5. *Presupunem că $p, a, b \in \boldsymbol{Z}$ 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 $p \nmid c$ şi $p \nmid d$. Atunci $ab = p^{\alpha+\beta}cd$ şi cum $p \nmid cd$, deducem că $o_p(ab) = \alpha + \beta = o_p(a) + o_p(b)$. ■

Teorema 1.3.6. *(Teorema fundamentală a aritmeticii) Pentru orice număr întreg nenul n, există o descompunere a lui în factori primi $n = (-1)^{\varepsilon(n)} \prod_{\substack{p \text{ prim}, \\ p \geq 2}} p^{e(p)}$ 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 1.3.2. Să probăm acum unicitatea acestei scrieri. Aplicând pentru un q prim o_q în ambii membrii ai egalităţii $n = (-1)^{\varepsilon(n)} \prod_{\substack{p \text{ prim}, \\ p \geq 2}} p^{e(p)}$ obţinem: $o_q(n) = \varepsilon(n)o_q(-1) + \sum_p e(p)o_q(p)$. Insă $o_q(-1) = 0$ iar $o_q(p) = \begin{cases} 1, \text{ dacă } p = q \\ 0, \text{ dacă } p \neq q \end{cases}$ de unde deducem că $e(q) = o_q(n)$ şi astfel teorema este demonstrată. ■

Corolar 1.3.7. *Pentru orice n există şi sunt unice numerele prime distincte*

$p_1, p_2, ..., p_m$ *şi numerele naturale* $k_1, k_2, ..., k_m$ *astfel încât* $n = p_1^{k_1}...p_m^{k_m}$ *(spunem că această scriere a lui n este descompunerea lui n în factori primi).*

Corolar 1.3.8. *Fie* $a, b, c, n \in \boldsymbol{N}^*$ *astfel încât* $(a, b) = 1$ *şi* $ab = c^n$. *Atunci există* $x, y \in \boldsymbol{N}^*$ *astfel încât* $a = x^n$ *şi* $b = y^n$.

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

Insă, conform Teoremei 1.3.6, descompunerea unui număr natural în produs de puteri de numere prime distincte este unică (abstracţie facând de ordinea factorilor). Astfel, dacă $c = p_1^{n_1}...p_s^{n_s} q_1^{m_1}...q_t^{m_t}$, atunci $c^n = p_1^{nn_1}...p_s^{nn_s} q_1^{nm_1}...q_t^{nm_t}$, 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 $x = p_1^{n_1}...p_s^{n_s}$ şi $y = q_1^{m_1}...q_t^{m_t}$. ■

Teorema 1.3.9. *(Legendre) Dacă* $n \in \boldsymbol{N}$ *iar* p *este un număr prim, atunci exponentul lui* p *în* $n!$ *este dat de* $\sum_{k \in \boldsymbol{N}^*} [\frac{n}{p^k}]$.

Demonstraţie. In 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 dintre $1, 2, ..., n$ care se divid cu p dar nu cu p^2, k_2 este numărul numerelor 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 $t_i = [\frac{n}{p^i}]$.

Numerele dintre $1, 2, ..., n$ care se divid cu p^{i+1} se află toate printre numerele dintre $1, 2, ..., n$ care se divid cu p^i. Dacă din numerele dintre $1, 2, ..., n$ care se divid cu p^i (ce sunt în număr de t_i) extragem toate numerele $1, 2, ..., n$ care se divid cu p^{i+1} (ce sunt în număr de $t_{i+1} = [\frac{n}{p^{i+1}}]$) obţinem numai numerele 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 $e_p = 1 \cdot (t_1 - t_2) + 2 \cdot (t_2 - t_3) + ... = t_1 + t_2 + ... = [\frac{n}{p}] + [\frac{n}{p^2}] + ...$ (această sumă este finită deoarece va exista un $k \in \mathbf{N}^*$ astfel încât $p^k \leq n < p^{k+1}$ şi atunci $[\frac{n}{p^s}] = 0$ pentru orice $s \geq k + 1$). ■

Observaţie. Dacă $p > n$ atunci $e_p = 0$.

1.4 Congruenţe pe Z

Definiţia 1.4.1. Fie $n \in \mathbf{N}, n \geq 2$ un număr fixat. Vom spune că $a, b \in \mathbf{Z}$ sunt *congruente modulo n* dacă $n | a - b$; în acest caz scriem $a \equiv b (mod\ n)$.

Propoziţia 1.4.2. *Relaţia de congruenţă modulo n este o echivalenţă pe* $\boldsymbol{Z}$ *compatibilă cu operaţiile de adunare şi înmulţire de pe* $\boldsymbol{Z}$ *(adică este o congruenţă pe inelul* $(\boldsymbol{Z}, +, \cdot)$*).*

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

Corolar 1.4.3. *Fie $a_i, b_i \in \boldsymbol{Z}$ astfel încât $a_i \equiv b_i(mod\ n)$ pentru orice $i = 1, 2, ..., k$. Atunci: $\sum_{i=1}^{k} a_i = \sum_{i=1}^{k} b_i(mod\ n)$ şi $\prod_{i=1}^{k} a_i = \prod_{i=1}^{k} b_i(mod\ n)$. In particular, dacă $a, b \in \boldsymbol{Z}$ astfel încât $a \equiv b(mod\ n)$ şi $k \in \boldsymbol{N}^*$, atunci $a^k \equiv b^k(mod\ n)$.*

Pentru $x \in \mathbf{Z}$ vom nota prin $\widehat{x}$ clasa de echivalenţă a lui x *modulo* n. Deoarece resturile împărţirii unui număr oarecare din $\mathbf{Z}$ prin n sunt $0, 1, ..., n-1$, deducem imediat că dacă notăm mulţimea claselor de echivalenţă *modulo* n prin $\mathbf{Z}_n$, atunci $\mathbf{Z}_n = \{\widehat{0}, \widehat{1}, ..., \widehat{n-1}\}$, iar pentru $k \in \{0, 1, ..., n-1\}$ avem $\widehat{k} = \{k + nt : t \in \mathbf{Z}\}$. Pe mulţimea $\mathbf{Z}_n$ se definesc operaţiile de adunare şi înmulţire astfel: $\widehat{x} + \widehat{y} = \widehat{x+y}$ şi $\widehat{x} \cdot \widehat{y} = \widehat{x \cdot y}$ (ţinând cont de Propoziţia 1.4.2 deducem că acestea sunt bine definite).

Propoziţia 1.4.4. *$(\boldsymbol{Z}_n, +, \cdot)$ este inel comutativ în care unităţile sale sunt*

$$U(\mathbf{Z}_n, +, \cdot) = \{\widehat{x} \in \mathbf{Z}_n : (x, n) = 1\}.$$

Demonstraţie. Cum verificarea anumitor axiome nu ridică probleme deosebite, vom reaminti doar că elementul neutru din $\mathbf{Z}_n$ faţă de adunare este $\widehat{0}$,$-\widehat{x} = \widehat{n-x}$ iar elementul neutru faţă de înmulţire este $\widehat{1}$. Dacă $\widehat{x} \in U(\mathbf{Z}_n)$, atunci există $\widehat{y} \in \mathbf{Z}_n$ astfel încât $\widehat{x} \cdot \widehat{y} = \widehat{1} \Leftrightarrow \widehat{x \cdot y} = \widehat{1} \Leftrightarrow n|xy - 1$, de unde deducem că $(x, n) = 1$.

Reciproc, dacă $x \in \{0, 1, .., n-1\}$ şi $(x, n) = 1$, atunci, conform Corolarului 1.2.7 există $r, s \in \mathbf{Z}$ astfel încât $r \cdot n + s \cdot x = 1$, de unde deducem că $\widehat{s}\widehat{x} = \widehat{1} \Leftrightarrow \widehat{x}^{-1} = \widehat{s}$, deci $x \in U(\mathbf{Z}_n)$. ■

De exemplu: $U(\mathbf{Z}_{12}) = \{\widehat{1}, \widehat{5}, \widehat{7}, \widehat{11}\}$.

Pentru un număr natural $n \geq 1$ definim $\varphi(1) = 1$ iar pentru $n \geq 2$, $\varphi(n)$ =numărul numerelor naturale $m < n$ astfel încât $(m, n) = 1$. Astfel, $\varphi(1) = \varphi(2) = 1, \varphi(3) = 2$, etc., iar $|U(\mathbf{Z}_n)| = \varphi(n)$.

Funcţia $\varphi : \mathbf{N}^* \to \mathbf{N}$ definită mai sus poartă numele de *indicatorul lui Euler*. Ea a fost studiată de Euler încă din anul 1760. Notarea funcţiei lui Euler prin φ a fost făcută de Gauss în anul 1801.

Corolar 1.4.5. *$(\boldsymbol{Z}_n, +, \cdot)$ este corp $\Leftrightarrow$ n este prim.*

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

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

Propoziţia 1.4.6. *Ecuaţia $\widehat{a}\widehat{x} = \widehat{b}$ are soluţie în $\boldsymbol{Z}_n$ dacă şi numai dacă $d|b$; dacă $d|b$ atunci ecuaţia $\widehat{a}\widehat{x} = \widehat{b}$ are exact d soluţii în $\boldsymbol{Z}_n$.*

Demonstraţie. Dacă $\widehat{x}_0 \in \mathbf{Z}_n$ este o soluţie a ecuaţiei $\widehat{a}\widehat{x} = \widehat{b}$, 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 1.2.7, există $x_0', y_0' \in \mathbf{Z}$ astfel încât $d = ax_0' - ny_0'$. Dacă $c = \frac{b}{d}$, atunci $a(x_0'c) - n(y_0'c) = b$, adică $\widehat{a}(\widehat{x_0'c}) = \widehat{b}$, deci $\widehat{x_0'c}$ este o soluţie a ecuaţiei $\widehat{a}\widehat{x} = \widehat{b}$.

Să presupunem acum că $\widehat{x}_0$ şi $\widehat{x}_1$ sunt două soluţii ale ecuaţiei $\widehat{a}\widehat{x} = \widehat{b}$. Atunci $n|ax_0 - b$ şi $n|ax_1 - b$, de unde $n|a(x_1 - x_0)$. Dacă notam $n' = \frac{n}{d}$ şi $a' = \frac{a}{d}$, atunci $(a', n') = 1$ şi obţinem că $n'|x_1 - x_0$, adică $x_1 = x_0 + kn'$, cu $k \in \mathbf{Z}$.

Pe de altă parte se verifică imediat că $\widehat{x_0 + kn'}$ este soluţie a ecuaţiei $\widehat{a}\widehat{x} = \widehat{b}$ cu $k \in \{0, 1, ..., d-1\}$. Cum nu e posibil să avem $\widehat{x_0 + k} = \widehat{x_0 + k'}$ pentru $k, k' \in \{0, 1, ..., d-1\}$ şi $k \neq k'$ (căci ar trebui ca $n|n'(k-k') \Leftrightarrow d|k-k'$-absurd!), deducem că dacă $\widehat{x}_0 \in \mathbf{Z}_n$ este o soluţie a ecuaţiei $\widehat{a}\widehat{x} = \widehat{b}$, atunci această ecuaţie are d soluţii şi anume: $\widehat{x}_0, \widehat{x_0 + n'}, ..., \widehat{x_0 + (d-1)n'}$.

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

Corolar 1.4.7. *Dacă n este număr prim, atunci ecuaţia $\widehat{a}\widehat{x} = \widehat{b}$ are soluţie unică în $\mathbf{Z}_n$ dacă şi numai dacă $(a, n) = 1$ (adică, dacă şi numai dacă $n \nmid a$).*

1.5 Fracţii periodice

Fiind dată fracţia $\alpha = \frac{p}{q} \in \mathbf{Q}$, (cu $q \in \mathbf{N}^*$), prin împărţirea lui p la q putem scrie pe α sub forma de *fracţie zecimală*: $\alpha = a_0, a_1a_2, ...$ cu $a_0, a_1, a_2, ... \in \mathbf{N}$ (în cele ce urmează prin diferite exemplificări se va deduce cu claritate modalitatea generală de reprezentare a numerelor raţionale sub forma de fracţii zecimale). In cele ce urmează vom presupune că fracţia α este subunitară (dacă ea este supraunitară, împărţind pe p la q putem scrie $p = cq + r$, cu $c \in \mathbf{Z}$ şi $0 \leq r < q$ 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 $\frac{35}{21} = 1\frac{2}{3}$).

In cazul în care $0 < \alpha < 1, a_0 = 0$ astfel că prin împărţiri repetate vom scrie $\alpha = 0, a_1a_2...$, cu $a_i \in \mathbf{N}$(după cum se va vedea în continuare şirul $a_1, a_2, ...$ 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: $\alpha = \frac{2}{3} = 0,666...$ (se repetă cifra 6; convenim să scriem $\alpha = 0,(6)$);

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

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

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

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

Să facem acum câteva observaţii:

1. In exemplul 1 împărţirea se termină cu două zecimale.

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

In cazul exemplului 6, fracţia zecimală obţinută 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 *fracţie periodică mixtă*.

In cele ce urmează vom proba că în general dacă avem o fracţie subunitară, atunci şirul $a_1, a_2, ...$ este sau finit sau periodic.

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

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

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

Să adâncim acum chestiunea:

Observaţia de bază este urmatoarea: fiind dată fracţia subunitară $\frac{b}{a}$, pentru a găsi primele n cifre ale fracţiei zecimale în care se transformă ea, facem împărţirea *întreagă* $10^n b : a$.

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

$$\begin{array}{l} \underline{80000} : 21 = 3809 \\ \underline{170} \\ \quad \underline{200} \\ \quad\quad 11 \end{array}$$

Să considerăm acum o fracţie cu numărătorul 1, de exemplu $\frac{1}{21}$ şi să facem împărţirile întregi $10 : 21$; $100 : 21$; $1000 : 21$, etc. Resturile acestor împărţiri reoproduc tocmai resturile parţiale din împărţirea

$\underline{10} : 21 = 0,47619...$

100

$\underline{84}$

160

$\underline{147}$

130

$\underline{126}$

40

$\underline{21}$

190

$\underline{189}$

1

$\underline{10} : 21 = 0$ $\quad \underline{100} : 21 = 4$ $\quad \underline{1000} : 21 = 47$ $\quad \underline{10000} : 21 = 476$

10 $\qquad$ 16 $\qquad$ 13 $\qquad$ 4

$\underline{100000} : 21 = 4761$ $\quad \underline{1000000} : 21 = 47619$

19 $\qquad$ 1

Pentru a şti în ce fel se transformă fracţia $\frac{1}{a}$, trebuie deci să urmărim resturile obţinute prin împărţirea lui $10, 102, 103, ...$ 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, pâna acolo resturile fiind toate diferite. Ştim că dacă $10^d \equiv 1(\text{mod } a)$, d este un divizor al lui $\varphi(a)$. Ştim că, dacă $a = p^\alpha q^\beta r^\gamma ...$, cel mai mic exponent n, astfel ca să avem $b^n \equiv 1(\text{mod } a)$ oricare ar fi b prim cu a, este c. m. m. m. c al numerelor $\varphi(p^\alpha), \varphi(q^\beta), \varphi(r^\gamma), ...$

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: $\frac{1}{21}, 21 = 3 \cdot 7; \varphi(3) = 2; \varphi(7) = 6;$ c.m.m.m.c. al numerelor $\varphi(3)$ şi $\varphi(7)$ 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 $80 : 21; 8 \cdot 10^2 : 21; 8 \cdot 10^3 : 21...$ Aceste resturi se pot obţine dacă înmulţim resturile (2) cu 8 (mod 21):

$$\begin{aligned} 8 \cdot 10 &= 80 \equiv 17(\text{mod } 21); 8 \cdot 16 = 128 \equiv 2(\text{mod } 21); 8 \cdot 13 = 104 \equiv 20(\text{mod } 21) \\ 8 \cdot 4 &= 32 \equiv 11(\text{mod } 21); 8 \cdot 19 = 152 \equiv 5(\text{mod}21); 8 \cdot 1 = 8 \equiv 8(\text{mod } 21). \end{aligned}$$

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 $8r_1 - 8r_2 \equiv 0(\text{mod } 21); 8(r_1 - r_2) \equiv 0(\text{mod } 21)$, 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 periodică simplă, iar numărul cifrelor perioadei este acelaşi ca şi la fracţia $\frac{1}{21}$.

Fie acum cazul $a = 2^\alpha \cdot 5^\beta$, adică a are numai factori primi ai lui 10. (De exemplu, $a = 40 = 2^3 \cdot 5$ sau $a = 25 = 5^2$, etc). In 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, fracţia zecimală rezultând din $\frac{1}{a}$ are un număr finit de zecimale, egal cu cel mai mare dintre numerele α şi β.

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

In 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 împărţirea unui număr cu 10^α se face despărţind prin virgulă α cifre.

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

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

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

Dacă $\beta > \alpha$ procedăm analog.

Exemplu. $\frac{7}{22} = \frac{7}{2 \cdot} = \frac{1}{10} \cdot \frac{5 \cdot 7}{11}$; $\frac{35}{11} = 3,1818...$, deci $\frac{7}{22} = 0,31818... = 0,3(18)$. 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 obţinem:

Teorema 1.5.1. *Orice fracţie se transformă într-o fracţie zecimală cu un număr finit de zecimale sau într-o fracţie zecimală cu un număr înfinit de zecimale, în care caz zecimalele admit o perioadă ce se repetă.*

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

Cazul 1. Dacă $\alpha = a_0, a_1 a_2 ... a_n$, atunci în mod evident $\alpha = \frac{\overline{a_0 a_1 a_2 ... a_n}}{10^k}$. De exemplu:

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

Cazul 2. Să presupunem acum că $\alpha = a_0, (\overline{a_1 a_2 ... a_n})$. Atunci:

$$\begin{aligned}\alpha &= a_0 + (\frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n}) + (\frac{a_1}{10^{n+1}} + \frac{a_2}{10^{n+2}} + ... + \frac{a_n}{10^{2n}}) + ... \\ &= a_0 + \frac{a_1}{10}(1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + ...) + \frac{a_2}{10^2}(1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + ...) + ... + \\ &+ \frac{a_n}{10^n}(1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + ...).\end{aligned}$$

Insă $1 + \frac{1}{10^n} + \frac{1}{10^{2n}} + ... = \frac{10^n}{10^n - 1}$ astfel că:

$$\begin{aligned}\alpha &= a_0 + (\frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_n}{10^n})\frac{10^n}{10^n - 1} \\ &= a_0 + \frac{a_n + a_{n-1}10 + ... + 10^{n-1}}{10^n - 1} = a_0 + \frac{\overline{a_1 a_2 ... a_n}}{\underbrace{99...9}_{n \text{ ori}}}.\end{aligned}$$

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 fracţie zecimală periodică mixtă: $\alpha = a_0, a_1 a_2 ... a_k(a_{k+1} a_{k+2} ... a_{k+n})$.

Atunci $\alpha = a_0, a_1 a_2 ... a_k + 0, 00...0(a_{k+1} a_{k+2} ... a_{k+n}) = \frac{\overline{a_1 a_2 ... a_n}}{10^k} + \frac{0, (a_{k+1} ... a_{k+n})}{10^k} = \frac{\overline{a_1 a_2 ... a_n}}{10^k} + \frac{\overline{a_{k+1} ... a_{k+n}}}{\underbrace{99...9}_{n \text{ ori}}\underbrace{00...0}_{k \text{ ori}}}$

De exemplu, dacă $\alpha = 3, 7(2) = \frac{37}{10} + \frac{2}{90} = \frac{37 \cdot 9 + 2}{90} = \frac{333+2}{90} = \frac{335}{90} = \frac{67}{18}$ iar dacă $\alpha = 2, 15(172) = \frac{215}{100} + \frac{172}{99900} = \frac{215 \cdot 999 + 172}{99900} = \frac{214957}{99900}$.

Rezumând cele trei cazuri de mai sus obţinem:

Teorema 1.5.2. *(i) Dacă* $\alpha = a_0, a_1 a_2 ... a_n$, *atunci* $\alpha = \frac{\overline{a_0 a_1 a_2 ... a_n}}{10^k}$.

(ii) Dacă $\alpha = a_0, (\overline{a_1 a_2 ... a_n})$, *atunci* $a_0 + \frac{a_n + a_{n-1}10 + ... + 10^{n-1}}{10^n - 1} = a_0 + \frac{\overline{a_1 a_2 ... a_n}}{\underbrace{99...9}_{n \ ori}}$.

(iii) Dacă $\alpha = a_0, a_1 a_2 ... a_k(a_{k+1} a_{k+2} ... a_{k+n})$, *atunci* $\frac{\overline{a_1 a_2 ... a_n}}{10^k} + \frac{\overline{a_{k+1} ... a_{k+n}}}{\underbrace{99...9}_{n \ ori}\underbrace{00...0}_{k \ ori}}$.

Observaţie. Acest paragraf a fost redactat în cea mai mare parte după lucrarea [20].

1.6 Teoremele lui Euler, Fermat şi Wilson

Lema 1.6.1. *Dacă G este un grup (multiplicativ) finit cu n elemente ($n \geq 2$), 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 $p \in \mathbf{N}$. Deducem imediat că $x^n = x^{kp} = (x^k)^p = 1^p = 1$. ■

Observaţie. Dacă G este comutativ există o demonstraţie elementară ce evită Teorema lui Lagrange. Pentru aceasta se alege $G = \{x_1, x_2, ..., x_n\}$ şi $x \in G$. Cum

$\{xx_1, xx_2, ..., xx_n\} = G = \{x_1, ..., x_n\}$, deducem că $(xx_1)...(xx_n) = x_1...x_n \Leftrightarrow x^n(x_1...x_n) = x_1...x_n \Leftrightarrow x^n = 1$. ■

Corolar 1.6.2. *(Euler) Dacă $n \geq 2$ este un număr natural iar $a \in \boldsymbol{Z}$ astfel încât $(a, n) = 1$, atunci $a^{\varphi(n)} \equiv 1(mod\ n)$ (φ fiind indicatorul lui Euler).*

Demonstraţie. Am vazut mai înainte că $(\mathbf{Z}_n, \cdot)$ este un monoid cu $\varphi(n)$ elemente inversabile. Astfel, dacă aplicăm Lema 1.6.1 grupului $G = U(\mathbf{Z}_n, \cdot)$ (ce are $\varphi(n)$ elemente) pentru $\widehat{a} \in G$ obţinem că:

$$\widehat{a}^{\varphi(n)} = \widehat{1} \Leftrightarrow \widehat{a^{\varphi(n)}} = \widehat{1} \Leftrightarrow n \mid a^{\varphi(n)} - 1 \Leftrightarrow a^{\varphi(n)} \equiv 1(\text{mod } n).\ \blacksquare$$

Corolar 1.6.3. *(Mica teorema a lui Fermat) Dacă $p \geq 2$ este un număr prim, iar $a \in \boldsymbol{Z}$ astfel încât $p \nmid a$, atunci $a^{p-1} \equiv 1(mod\ p)$.*

Demonstraţie. Cum p este un număr prim, $\varphi(p) = p - 1$ şi acum totul rezultă din Corolarul 1.6.2. ■

Lema 1.6.4. *Fie G un grup (multiplicativ) finit comutativ iar $\prod\limits_{x \in G} x$ produsul tuturor elementelor din G. Atunci $\prod\limits_{x \in G} x = \prod\limits_{\substack{x \in G, \\ o(x) \leq 2}} x$.*

Demonstraţie. Vom scrie $\prod\limits_{x \in G} x = \prod\limits_{\substack{x \in G, \\ o(x) \leq 2}} x \cdot \prod\limits_{\substack{x \in G, \\ o(x) > 2}} x$. Insă în cadrul produsului $\prod\limits_{\substack{x \in G, \\ o(x) > 2}} x$ 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 $\prod\limits_{\substack{x \in G, \\ o(x) > 2}} x = 1$, de unde concluzia că $\prod\limits_{x \in G} x = \prod\limits_{\substack{x \in G, \\ o(x) \leq 2}} x$. ■

Corolar 1.6.5. *(Wilson) Dacă $p \geq 2$ este un număr prim, atunci $(p-1)! + 1 \equiv 0(mod\ p)$.*

Demonstraţie. Cum p este prim $(\mathbf{Z}_p^*, \cdot)$ este grup cu $p - 1$ elemente, conform Lemei 1.6.4, $\prod\limits_{\widehat{x} \in \mathbf{Z}_p^*} \widehat{x} = \prod\limits_{\substack{\widehat{x} \in \mathbf{Z}_p^*, \\ o(\widehat{x}) \leq 2}} \widehat{x}$. Rămâne să punem în evidenţă elementele $\widehat{x} \in \mathbf{Z}_p^*$ cu proprietatea că $o(\widehat{x}) = 2 \Leftrightarrow \widehat{x}^2 = \widehat{1} \Leftrightarrow \widehat{x^2} = \widehat{1} \Leftrightarrow p|x^2 - 1 = (x-1)(x+1) \Leftrightarrow p|x-1$ sau $p|x+1$ de unde deducem că $\widehat{x} = -\widehat{1} = \widehat{p-1}$ sau $\widehat{x} = \widehat{1}$, astfel că $\widehat{1} \cdot \widehat{2} \cdot ... \widehat{p-1} = -\widehat{1} \Leftrightarrow \widehat{(p-1)!} + 1 = \widehat{0} \Leftrightarrow (p-1)! + 1 \equiv 0(\text{mod } p)$. ■

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

Lema 1.6.6. *Fie $p \geq 2$ un număr prim, iar $n \geq 2$ un număr natural. Atunci*:

(i) *Dacă $p = 2$ şi $n > 2$ în grupul $U(\boldsymbol{Z}_{2^n}, \cdot)$ numai elementele $\widehat{1}, -\widehat{1}, \widehat{2^{n-1}+1}$, $\widehat{2^{n-1}-1}$ au ordinul cel mult 2;*

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

Demonstraţie. Avem că $U(\mathbf{Z}_{p^n}^*, \cdot) = \{\widehat{a} \in \mathbf{Z}_{p^n}^* : (a, p) = 1\}$. Să determinăm în acest grup elementele $\widehat{a} \in U(\mathbf{Z}_{p^n}^*, \cdot)$ astfel încât $\widehat{a}^2 = 1$, adică acele numere naturale a astfel încât $1 \leq a < p^n$, 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 $k, t \geq 0, (p, u) = (p, v) = 1$, iar $k + t \geq n$.

Dacă $k = 0$ atunci $t \geq n$, deci $p^n \mid a + 1$ şi cum $a < p^n$ rezultă că $a + 1 = p^n$, de unde $a = p^n - 1$ şi astfel obţinem elementul $\widehat{a} = \widehat{p^n - 1} = -\widehat{1}$ ce verifică de asemenea $(*)$.

Dacă $t = 0$ atunci $k > n$, deci $p^n \mid a - 1$ şi cum $a < p^n$ rezultă că $a - 1 = 0$ de unde $a = 1$, contradicţie.

Dacă $k \neq 0, t \neq 0$ atunci $2 = p^t v - p^k u$, adică $p \mid 2$, deci dacă $p \geq 2$, obţinem o contradicţie.

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

Dacă $p = 2$, atunci din $2 = 2^t v - 2^k u$ rezultă că $t = 1$ sau $k = 1$. Dacă $t = 1$ atunci $k \geq n - 1$, deci $a - 1 = 2^k u \geq 2^{n-1} u$ şi cum $1 < a < 2^n$ avem că $u = 2$ şi $k = n - 1$. Deci, în acest caz, dacă a verifică $(*)$ atunci $a = 2^{n-1} + 1$.

Dacă $k = 1$ atunci $t \geq n - 1$, deci $a + 1 = 2^t v \geq 2^{n-1} v$ şi cum $1 < a < 2^n$ rezultă că $v = 1$ sau $v = 2$ (cazul $v = 2$ este exclus căci $(v, 2) = 1$).

Dacă $v = 1$ atunci $t = n - 1$ sau $t = n$. In cazul $t = n - 1$ rezultă $a = 2^{n-1} - 1$, iar dacă $t = n$ atunci $a = 2^n - 1$.

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

Corolar 1.6.7. *(O generalizare a teoremei lui Wilson) Dacă p este un număr prim şi n un număr natural, atunci*:

(i) Dacă $p > 2$ şi $n \geq 2$ atunci $p^n \mid \prod_{\substack{1 \leq a < p^n, \\ (a,p)=1}} a + 1$;

(ii) Dacă $p = 2$ şi $n > 2$ atunci $2^n \mid \prod_{\substack{1 \leq a < 2^n, \\ (a,2)=1}} a - 1$;

(iii) Dacă $p = 2$ şi $n = 2$ atunci $2^2 \mid \prod_{\substack{1 \leq a < 2^2, \\ (a,2)=1}} a + 1$.

Demonstraţie. Totul rezultă imediat din Lema 1.6.4 ţinând cont de cele stabilite în Lema 1.6.6. ■

1.7 Teorema chinezească a resturilor

In cadrul acestui paragraf vom prezenta sub altă formă aşa zisă teoremă chinezească a resturilor (vezi şi [7]). Fie $m_1, m_2, ..., m_t \in \mathbf{N}$ astfel încât $(m_i, m_j) = 1$ pentru orice $i \neq j, m = m_1 m_2 ... m_t$, iar $b_1, b_2, ..., b_t \in \mathbf{Z}$.

Teorema 1.7.1. *(Teorema chinezească a resturilor)*

Sistemul

$$(S) \begin{cases} x = b_1 (\mod m_1) \\ ..... \\ x = b_t (\mod m_t) \end{cases}$$

are soluţie în $\boldsymbol{Z}$ şi oricare două soluţii diferă printr-un multiplu de m.

Demonstraţie. Dacă $n_i = \frac{m}{m_i}$, atunci $(m_i, n_i) = 1$ pentru orice $1 \leq i \leq t$. Astfel există $r_i, s_i \in \mathbf{Z}$ astfel încât $r_i m_i + s_i n_i = 1$ pentru orice $1 \leq i \leq t$.

Dacă notăm $e_i = s_i n_i$, atunci $e_i \equiv 1 (\mod m_i)$ şi $e_i \equiv 0 (\mod m_j)$ 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 $x_0 \equiv b_i e_i (\mod m_i)$ şi astfel $x_0 \equiv b_i (\mod m_i)$ pentru orice $1 \leq i \leq t$, de unde concluzia că x_0 este soluţie a sistemului (S).

Să presupunem că x_1 este o altă soluţie a lui (S). Atunci $x_1 - x_0 \equiv 0 (\mod m_i)$ 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 $m = m_1 m_2 ... m_t \mid x_0 - x_1$, adică $x_0 \equiv x_1 (\mod m)$. ■

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 $\prod_{i \in I} A_i$, având mulţimea subiacentă $\prod_{i \in I} A_i = \{(x_i)_{i \in I} : x_i \in A_i$ pentru orice $i \in I\}$, iar pentru $x, y \in \prod_{i \in I} A_i, x = (x_i)_{i \in I}$ şi $y = (y_i)_{i \in I}$ definim $x + y = (x_i + y_i)_{i \in I}$ şi $x \cdot y = (x_i \cdot y_i)_{i \in I}$.

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 $x = (x_i)_{i \in I}, -x = (-x_i)_{i \in I}$; elementul unitate este $1 = (x_i)_{i \in I}$ cu $x_i = 1$ pentru orice $i \in I$, iar dacă $x = (x_i)_{i \in I} \in \prod_{i \in I} A_i$, 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 $m_1, m_2, ..., m_t \in \mathbf{N}^*$ astfel încât $(m_i, m_j) = 1$ pentru orice $i \neq j, 1 \leq i, j \leq t$ şi $m = m_1 m_2 ... m_t$.

Teorema 1.7.2. *Avem următorul izomorfism de inele:*

$$\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_t} \approx \mathbf{Z}_m.$$

Demonstraţie. Pentru fiecare $1 \leq i \leq t$, fie $\pi_i : \mathbf{Z} \longrightarrow \mathbf{Z}_{m_i}$ morfismul surjectiv canonic de inele ce duce fiecare element $x \in \mathbf{Z}$ în clasa sa de echivalenţă modulo m_i.

Definim $f : \mathbf{Z}_m \longrightarrow \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_t}$ prin $f(x) = (\pi_1(x), ..., \pi_t(x))$ pentru orice $x \in \mathbf{Z}$.

Dacă $x, y \in \mathbf{Z}$ şi $f(x) = f(y)$ atunci $x \equiv y (\text{mod } m) \Leftrightarrow x \equiv y (\text{mod } m_i)$ 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 $|\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_t}| = |Z_m| = m = m_1...m_t$.

Deci f este un izomorfism de inele unitare. ■

Corolar 1.7.3. *Cu notaţiile de la teorema precedentă avem următorul izomorfism de grupuri multiplcative*:

$$U(\mathbf{Z}_m) \approx U(\mathbf{Z}_{m_1}) \times U(\mathbf{Z}_{m_2}) \times ... \times U(\mathbf{Z}_{m_t}).$$

Corolar 1.7.4. *Fie $\varphi : \boldsymbol{N} \longrightarrow \boldsymbol{N}$ indicatorul lui Euler.*

(i) Dacă $m_1, m_2, ..., m_t \in \boldsymbol{N}^*$ astfel încât $(m_i, m_j) = 1$ pentru $i \neq j$, atunci $\varphi(m_1...m_t) = \varphi(m_1)...\varphi(m_t)$;

(ii) Dacă $p \geq 2$ este număr prim şi $n \in \boldsymbol{N}^*$, atunci $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$;

(iii) Dacă $n = p_1^{k_1}...p_t^{k_t}$ este descompunerea în factori primi a lui n, atunci $\varphi(n) = n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_t})$.

Demonstraţie. (i). Am văzut că $|U(\mathbf{Z}_m)| = \varphi(n)$ pentru orice $n \in \mathbf{N}, n \geq 2$. Dacă ţinem cont de Corolarul 1.7.3 deducem că:

$$|U(\mathbf{Z}_m)| = |U(\mathbf{Z}_{m_1}) \times ... \times U(\mathbf{Z}_{m_t})| = |U(\mathbf{Z}_{m_1})|...|U(\mathbf{Z}_{m_t})| \Leftrightarrow \varphi(m) = \varphi(m_1)...\varphi(m_t).$$

(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:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1}...p_t^{k_t}) = (p_1^{k_1} - p_1^{k_1-1})...(p_t^{k_t} - p_t^{k_t-1}) = p_1^{k_1}...p_t^{k_t}(1 - \frac{1}{p_1})...(1 - \frac{1}{p_t}) \\ &= n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_t}). \ \blacksquare \end{aligned}$$

De exemplu, $\varphi(12) = \varphi(2^3 \cdot 3) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$.

1.8 Rădăcini primitive modulo un număr prim

Fie $n \in \mathbf{N}^*, a \in \mathbf{Z}, (a, n) = 1$. Conform Teoremei lui Euler (Corolarul 1.6.2) ştim că $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.

Definiţia 1.8.1. Cel mai mic număr natural nenul pentru care $a^m \equiv (\text{mod } n)$ se numeşte *gaussian* sau *ordin* al lui a şi se notează prin $\gamma_n(a)$. De fapt, $\gamma_n(a) = ord(\widehat{a})$ în $(U(\mathbf{Z}_n), \cdot)$.

Observaţie.

1. Dacă $a^m \equiv 1(\text{mod } p)$, atunci $\gamma_n(a) \mid m$;

2. $\gamma_n(a) \mid \varphi(n)$;

3. Dacă $a^r \equiv a^s(\text{mod } n)$, atunci $r \equiv s(\text{mod } \gamma_n(a))$.

Dacă $n = p_1^{k_1}...p_s^{k_s}$ este descompunerea în factori primi a lui n, conform Corolarului 1.7.3, $U(\mathbf{Z}_m) \approx U(\mathbf{Z}_{p_1^{k_1}}) \times ... \times U(\mathbf{Z}_{p_s^{k_s}})$ astfel, pentru a determina structura grupului multiplicativ $U(\mathbf{Z}_n)$ este suficient să studiem structura grupurilor de forma $U(\mathbf{Z}_{p^n})$ cu p prim şi $n \in \mathbf{N}$.

Vom începe cu cazul cel mai simplu şi anume cu $U(\mathbf{Z}_p)$ cu p prim. Cum $\mathbf{Z}_p$ este corp, $U(\mathbf{Z}_p) = \mathbf{Z}_p^*$. Dacă $f = a_0+a_1X+...+a_nX^n \in \mathbf{Z}[X]$, vom nota $\widehat{f} = \widehat{a}_0+\widehat{a}_1X+...+\widehat{a}_nX^n \in \mathbf{Z}_p[X]$.

Lema 1.8.2. *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 $\leq n - 1$.

Dacă f nu are rădăcini în K totul este clar.

Dacă există $\alpha \in K$ astfel încât $f(\alpha) = 0$, 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 1.8.3. *Fie K un corp comutativ $f, g \in K[X]$ astfel încât grad(f)=grad(g)=n. Dacă avem n+1 elemente distincte $\alpha_1, \alpha_2, ..., \alpha_{n+1}$ astfel încât $f(\alpha_i)=g(\alpha_i)$ pentru orice $1 \leq i \leq n + 1$, atunci f=g.*

Demonstraţie. Considerând $h = f - g$, atunci $grad(h) \leq n$ şi cum h are $n + 1$ rădăcini distincte $\alpha_1, \alpha_2, ..., \alpha_{n+1}$, deducem că $h = 0$, adică $f = g$. ■

Corolar 1.8.4. *Dacă $p \geq 2$ este un număr prim, atunci orice $x \in \mathbf{Z}$, avem: $x^{p-1} - 1 \equiv (x - 1)(x - 2)...(x - p + 1)(mod\ p)$.*

Demonstraţie. Cum p este prim, $\mathbf{Z}_p$ este corp comutativ. Considerând $f = (X^{p-1} - \widehat{1}) - (X - \widehat{1})(X - \widehat{2})...(X - \widehat{p-1}) \in \mathbf{Z}_p[X]$ avem că grad$(f) \leq p - 2$ şi $f(\widehat{x}) = \widehat{0}$ pentru $\widehat{x} = \widehat{1}, \widehat{2}, ..., \widehat{p-1}$ (ţinând cont şi de mica teoremă a lui Fermat, adică de Corolarul 1.6.3). Conform Corolarului 1.8.2, $f = 0$. ■

Observaţie. Dacă în Corolarul 1.8.3 considerăm $x = 0$ obţinem că $(p - 1)! \equiv -1(\text{mod } p)$, adică teorema lui Wilson (Corolarul 1.6.5).

Propoziţia 1.8.5. *Fie $p \geq 2$ un număr prim şi $d|p - 1$. Atunci congruenţa $x^d \equiv 1(mod\ p)$ are exact d soluţii.*

Demonstraţie. Dacă $p-1=dd'$, atunci: $\frac{x^{p-1}-1}{x^d-1}=\frac{(x^d)^{d'}-1}{x^d-1}=(x^d)^{d'-1}+(x^d)^{d'-2}+...+x^d+1=g(x)$, adica $x^{p-1}-1=(x^d-1)g(x)$ şi astfel $x^{p-1}-\widehat{1}=(x^d-\widehat{1})\widehat{g}(x)$.

Cum $x^{p-1}-\widehat{1}$ are exact $p-1$ rădăcini (şi anume $\widehat{1},\widehat{2},...,\widehat{p-1}$-conform micii teoreme a lui Fermat), ţinând cont de Lema 1.8.1 deducem că $x^d-\widehat{1}$ are exact d rădăcini în $\mathbf{Z}_p$ şi astfel congruenţa $x^d\equiv 1(\text{mod } p)$ are exact d soluţii în $\mathbf{Z}_p$. ■

Teorema 1.8.6. *Dacă p este un număr prim, atunci $U(\boldsymbol{Z}_p)$ este un grup ciclic.*

Demonstraţie.

Soluţia 1: Evident $|U(\mathbf{Z}_p)|=|\mathbf{Z}_p^*|=p-1$ iar pentru $d|p-1$, fie $\psi(d)$ numărul elementelor din $\mathbf{Z}_p^*$ de ordin d. Conform Propoziţiei 1.8.4 elementele din $\mathbf{Z}_p^*$ ce satisfac congruenţa $x^d\equiv 1(\text{mod } p)$ formează un grup de ordin d. Insă $\sum\limits_{c|d}\psi(c)=d$, de unde se deduce că $\psi(d)=\varphi(d)$ (φ fiind indicatorul lui Euler). In particular, $\psi(p-1)=\varphi(p-1)>1$ (dacă $p\geq 3$). Deducem că în $\mathbf{Z}_p^*$, $\varphi(p-1)$ elemente au ordinul $p-1$ şi astfel oricare dintre aceştia generează pe $\mathbf{Z}_p^*$, adică $\mathbf{Z}_p^*$ este grup multiplicativ ciclic.

Soluţia 2: Fie $p-1=q_1^{l_1}...q_t^{l_t}$ descompunerea în factori primi a lui $p-1$ şi să considerăm congruenţele:

(1) $x^{q_i^{l_i-1}}\equiv 1(p)$

(2) $x^{q_i^{l_i}}\equiv 1(p)$, cu $1\leq i\leq t$.

In mod evident orice soluţie a congruenţei (1) este soluţie şi a congruenţei (2). Mai mult, congruenţa (2) are mai multe soluţii decât congruenţa (1). Pentru fiecare $1\leq i\leq t$ fie g_i o soluţie a congruenţei (2) ce nu este soluţie a congruenţei (1) iar $g=g_1g_2...g_t$.

Evident, $\widehat{q}_i$ generează un subgrup al lui $\mathbf{Z}_p^*$ de ordin $q_i^{l_i}, 1\leq i\leq t$. Deducem că $\widehat{g}$ generează un subgrup al lui $\mathbf{Z}_p^*$ de ordin $p-1=q_1^{l_1}...q_t^{l_t}$. Atunci $<\widehat{g}>=\mathbf{Z}_p^*$. ■

Definiţia 1.8.7. Fie $p\geq 2$ un număr prim. Un element $a\in\mathbf{Z}$ se zice *rădăcină primitivă modulo p* dacă $\widehat{a}$ generează $\mathbf{Z}_p^*$.

De exemplu, 2 este rădăcină primitivă modulo 5 (se verifică imediat că 4=5-1 este cel mai mic număr natural n pentru care $2^n\equiv 1(\text{mod } 5)$), pe când 2 nu este rădăcină primitivă modulo 7 (de exemplu, $2^3\equiv 1(\text{mod } 7)$).

Noţiunea de rădăcină primitivă se poate generaliza astfel:

Definiţia 1.8.8. Fie $n\in\mathbf{N}$. Un element $a\in\mathbf{Z}$ se zice *rădăcină primitivă modulo n* dacă în $\mathbf{Z}_n$ generează $U(\mathbf{Z}_n)$(echivalent cu a spune că $\varphi(n)$ este cel mai mic număr natural pentru care $a^{\varphi(n)}\equiv 1(\text{mod } n)$, adică $\gamma_n(a)=\varphi(n)$).

Observaţie. In general nu rezultă că $U(\mathbf{Z}_n)$ este ciclic.

De exemplu, elementele lui $U(\mathbf{Z}_8)$ sunt $\widehat{1},\widehat{3},\widehat{5},\widehat{7}$ iar $\widehat{1}^2=\widehat{1},\widehat{3}^2=\widehat{1},\widehat{5}^2=\widehat{1},\widehat{7}^2=\widehat{1}$, neexistând deci în $U(\mathbf{Z}_8)$ elemente de ordin $4=\varphi(8)$.

Rezultă că nu orice întreg posedă rădăcini primitive.

Lema 1.8.9. *Dacă p este un număr natural prim şi $1\leq k<p$ atunci $p\mid C_p^k$.*

Demonstraţie. Avem $C_p^k=\frac{p!}{k!(p-k)!}\in\mathbf{N}$ 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

$q \in \mathbf{N}$ şi cum $C_p^k = p \cdot q$, rezultă că $p \mid C_p^k$. ■

Observaţie. Utilizând Lema 1.8.9 putem prezenta o nouă demonstraţie a micii teoreme a lui Fermat: Dacă p este un număr prim şi $a \in \mathbf{Z}$ astfel încât $p \nmid a$, atunci $p|a^{p-1} - 1$. Intr-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 1.8.9 deducem că $s_{a+1} \equiv s_a (\text{mod } p)$. Astfel, $s_a \equiv s_{a-1} \equiv s_{a-2} \equiv ... \equiv s_1 (\text{mod } p)$ şi cum $s_1 = 1^a - 1 = 0$ deducem că $s_a \equiv 0 (\text{mod } p)$, adică $p|a^p - a = a(a^{p-1} - 1)$ şi cum $p \nmid a$ obţinem că $p \mid a^{p-1} - 1$.

Lema 1.8.10. *Dacă $n \geq 1$ este un număr natural, $p \geq 2$ un număr prim şi $a, b \in \boldsymbol{Z}$ astfel încât $a \equiv b (mod\ p^n)$, atunci $a^p \equiv b^p (mod\ p^{n+1})$.*

Demonstraţie. Putem scrie $a = b + cp^n$, cu $c \in \mathbf{Z}$. Atunci $a^p = (b + cp^n)^p = b^p + C_p^1 b^{p-1} cp^n + x$ (cu $x \in \mathbf{Z}$ şi $p^{n+2} \mid x$) astfel că $a^p = b^p + b^{p-1} cp^{n+1} + x$, de unde $a^p \equiv b^p (\text{mod } p^{n+1})$. ■

Corolar 1.8.11. *Dacă p este un număr prim, $p \geq 3, n \in \boldsymbol{N}, n \geq 2$, atunci $(1 + ap)^{p^{n-2}} \equiv 1 + ap^{n-1} (mod\ p^n)$ pentru orice $a \in \boldsymbol{Z}$.*

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 1.8.10 avem: $(1 + ap)^{p^{n-1}} \equiv (1 + ap^{n-1})^p (\text{mod } p^{n+1})$. Dezvoltând cu ajutorul binomului lui Newton obţinem $(1 + ap^{p-1})^p = 1 + C_p^1 ap^{n-1} + \beta$, unde β este o sumă de $p-2$ termeni. Utilizând din nou Lema 1.7.9 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 $n \geq 2, 1 + 2(n-1) \geq n+1$ şi cum $p(n-1) \geq n+1$, adică $p^{n+1} \mid \beta$ şi astfel $(1 + ap)^{p^{n-1}} \equiv 1 + ap^{n-1} (\text{mod } p^n)$, adică c.c.t.d. ■

Observaţie. Fie $a, n \in \mathbf{Z}$ astfel încât $(a, n) = 1$. Vom spune că a are *ordinul k modulo n* dacă este cel mai mic număr natural pentru care $a^k \equiv 1 (\text{mod } n)$. Acest lucru este echivalent cu a spune că $\widehat{a}$ din $\mathbf{Z}_n$ are ordinul k în grupul $U(\mathbf{Z}_n)$.

Corolar 1.8.12. *Dacă $p \neq 2$ este un număr prim astfel încât $p \nmid a$, atunci ordinul lui $1 + ap$ modulo p^n este egal cu p^{n-1} ($n \in \boldsymbol{N}, n \geq 2$).*

Demonstraţie. Conform Corolarului 1.8.11, $(1 + ap)^{p^{n-2}} \equiv 1 + ap^n (\text{mod } p^{n+1})$, de unde deducem că $(1 + ap)^{p^{n-2}} \equiv 1 + ap^{n-1} (\text{mod } p^n)$ 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 1.8.13. *Fie $p \geq 3$ un număr prim şi $n \in \boldsymbol{N}^*$. Atunci $U(\boldsymbol{Z}_{p^n})$ este grup ciclic (adică există în acest grup rădăcini primitive modulo p^n).*

Demonstraţie. Conform Teoremei 1.8.56. există o rădăcină primitivă modulo p. Dacă $g \in \mathbf{Z}$ este o astfel de rădăcină, atunci în mod evident şi $g + p$ este. Dacă $g^{p-1} \equiv 0 (\text{mod } p^2)$, atunci $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p (\text{mod } p^2)$. Cum p^2 nu divide $(p-1)g^{p-2}p$ putem presupune pentru început că g este o rădăcină primitivă modulo p şi că $g^{p-1} \equiv 1 (\text{mod } p^2)$.

Să arătăm că un astfel de g poate fi rădăcină primitivă modulo p^n iar pentru aceasta este suficient să demonstrăm că dacă $g^m \equiv 1 (\text{mod } p^n)$, atunci $\varphi(p^n) \mid m$.

Avem că $g^{p-1} = 1 + ap$, unde $p \nmid a$. Conform Corolarului 1.8.11, p^{m-1} este de ordinul lui $1 + ap$ modulo p^m. Deoarece $(1 + ap)^m \equiv 1(\text{mod } p^n)$ atunci $p^{n-1} \mid m$. Fie $m = p^{n-1}m'$. Atunci $g^{m'} \equiv 1(\text{mod } p)$. Deoarece g este o rădăcină primitivă modulo p, $p - 1 \mid m'$ şi astfel $p^{n-1}(p-1) = \varphi(p^n) \mid m$. ■

Pentru cazul $p = 2$ vom demonstra:

Teorema 1.8.14. *Numărul 2^n are rădăcini primitive pentru $n = 1$ sau 2 iar pentru $n \geq 3$ nu are. Dacă $n \geq 3$, atunci $\{(-1)^a 5^b : a = 0, 1$ şi $0 \leq b < 2^{n-2}\}$ constituie un sistem redus de resturi modulo 2^n. Rezultă că pentru $n \geq 3, U(\boldsymbol{Z}_{2^n})$ este produsul direct a două grupuri ciclice (unul de ordin 2 iar celălalt de ordin 2^{n-2}).*

Demonstraţie. Numărul 1 este rădăcină primitivă modulo 2 iar 3 este rădăcină primitivă modulo $2^2 = 4$, deci putem presupune $n \geq 3$.

Intenţionăm să demonstrăm că:

(1) $5^{2^{n-1}} \equiv 1 + 2^{n-1}(\text{mod } 2^n)$.

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 $2n - 2 \geq n + 1$ pentru $n \geq 3$.

Aplicând Lema 1.8.10 congruenţei (1) obţinem

(2) $5^{2^{n-1}} \equiv 1 + 2^n(\text{mod } 2^{n+1})$

şi astfel (1) este probată prin inducţie.

Din (2) se vede că $5^{2^{n-2}} \equiv 1(\text{mod } 2^n)$ pe când din (1) avem că $5^{2^{n-3}} \equiv 1(\text{mod } 2^n)$. Atunci 5 are ordinul 2^{n-2} modulo 2^n.

Să considerăm mulţimea $\{(-1)^a 5^b : a = 0, 1$ şi $0 \leq b < 2^{n-2}\}$ 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 mulţimea de mai sus conţine un sistem redus de resturi modulo 2^n).

Dacă prin absurd, $(-1)^a 5^b \equiv (-1)^{a'} 5^{b'}(\text{mod } 2^n), n \geq 3$, atunci $(-1)^a \equiv (-1)^{a'}(\text{mod } 4)$, adică $a \equiv a'(\text{mod } 2)$, deci $a = a'$. Atunci $5^b \equiv 5^{b'}(\text{mod } 2^n)$ şi astfel $5^{b-b'} \equiv 1(\text{mod } 2^n)$, de unde $b \equiv b'(\text{mod } 2^n)$, deci $b = b'$.

In 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 $n \geq 3$. ■

Din Teoremele 1.8.13 şi 1.8.14 deducem următoarea descriere completă a grupurilor $U(\mathbf{Z}_n)$ pentru n arbitrar:

Teorema 1.8.15. *Fie $n = 2^a p_1^{a_1} ... p_n^{a_n}$ descompunerea lui n în factori primi distincţi. Atunci:*

$$U(\mathbf{Z}_n) \approx U(\mathbf{Z}_{2^a}) \times U(\mathbf{Z}_{p_1^{a_1}}) \times ... \times U(\mathbf{Z}_{p_n^{a_n}})$$

Grupurile $U(\boldsymbol{Z}_{p_i^{a_i}})$ sunt grupuri ciclice de ordin $p_i^{a_i-1}(p_i - 1), 1 \leq i \leq n$ iar $U(\boldsymbol{Z}_{2^a})$ este grup ciclic de ordin 1 şi 2 pentru $a = 1$, respectiv $a = 2$. Dacă $a \geq 3$, atunci $U(\boldsymbol{Z}_{2^a})$ 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?

Teorema 1.8.16. *Numărul $n \in \boldsymbol{N}$ posedă rădăcini primitive dacă şi numai dacă n este de forma 2, 4, p^a sau $2p^a$ cu $a \in \boldsymbol{N}$ iar $p \geq 3$ un număr prim.*

Demonstraţie. Conform Teoremei 1.8.14, putem presupune că $n \neq 2^k$ cu $k \geq 3$. Dacă n nu este de forma din enunţ, este uşor de văzut că n se poate atunci scrie ca produs $m_1 m_2$ cu $(m_1, m_2) = 1$ şi $m_1, m_2 > 2$.

Atunci $\varphi(m_1)$ şi $\varphi(m_2)$ sunt simultan pare iar $U(\mathbf{Z}_n) \approx U(\mathbf{Z}_{m_1}) \times U(\mathbf{Z}_{m_2})$. Insă $U(\mathbf{Z}_{m_1})$ şi $U\mathbf{Z}_{m_2})$ au elemente de ordin 2 iar acest lucru ne arată că $U(\mathbf{Z}_n)$ 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 $U(\mathbf{Z}_{2p^a}) \approx U(\mathbf{Z}_2) \times U(\mathbf{Z}_{p^a})$ deducem că $U(\mathbf{Z}_{2p^a})$ este ciclic, adică $2p^a$ posedă rădăcini primitive şi cu aceasta teorema este demonstrată. ■

1.9 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 larga răspândire în Europa). In cele ce urmează vom fundamenta ceea ce înseamnă *scrierea numerelor naturale în baza u*, unde $u \in \mathbf{N}, u \geq 2$.

Lema 1.9.1. *Fie u un număr natural > 1. Oricare ar fi numărul natural $a > 0$, există numerele naturale n, $q_0, q_1, ..., q_{n-1}, a_0, a_1, ..., a_n$ astfel încât:*

$$\begin{aligned} a &= uq_0 + a_0,\ 0 \leq a_0 < u \\ q_0 &= uq_1 + a_1,\ 0 \leq a_1 < u \\ ..... &\ ... \ ..... \\ q_{n-2} &= uq_{n-1} + a_{n-1},\ 0 \leq a_{n-1} < u \\ q_{n-1} &= a_n,\ 0 \leq a_n < u. \end{aligned}$$

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

Cum $a \geq u$, avem $q_0 > 0$. Există $q_1, a_1 \in \mathbf{N}$ 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 $a > q_0 > q_1 > ... > q_{i-1} > q_i > ... \geq 0$.

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 1.9.2. *Fie* $u,\ a_0, a_1, ..., a_n \in \boldsymbol{N}$ *astfel încât* $u > 1, 0 \leq a_i < u$ *pentru* $0 \leq i < n$ *şi* $0 < a_n < u$. *Atunci:*

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

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

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

de unde rezultă lema. ■

Teorema 1.9.3. *Fie* u *un număr natural* > 1. *Oricare ar fi numărul* $a > 0$, *există numerele naturale* $n,\ a_n, a_{n-1}, ..., a_0$ *unic determinate astfel încât:* $a = a_n u^n + a_{n-1}u^{n-1} + ... + a_1 u + a_0$, *unde* $0 < a_0 < u$ *şi* $0 \leq a_i < u$ *pentru orice* $0 \leq i \leq n-1$.

Demonstraţie. Conform Lemei 1.9.1, există $n, q_0, ..., q_{n-1}$ şi $a_0, a_1, ..., a_n$ astfel încât:

$$\begin{aligned}
a &= uq_0 + a_0,\ 0 \leq a_0 < u \\
q_0 &= uq_1 + a_1,\ 0 \leq a_1 < u \\
&\cdots\cdots \quad \cdots\cdots \\
q_{n-2} &= uq_{n-1} + a_{n-1},\ 0 \leq a_{n-1} < u \\
q_{n-1} &= a_n,\ 0 \leq a_n < u.
\end{aligned}$$

Inmulţim aceste egalităţi respectiv cu $1, u, u^2, ..., u^n$. Adunând apoi termen cu termen egalităţile ce se obţin, rezultă: $a = a_n u^n + a_{n-1}u^{n-1} + ... + a_1 u + a_0$.

Rămâne să dovedim unicitatea numerelor $n, a_0, a_1, ..., a_n$. Fie de asemenea numerele naturale $n', a_0', a_1', ..., a_n'$ astfel încât $a = a_{n'}' u^{n'} + a_{n'-1}' u^{n'-1} + ... + a_1' u + a_0'$ cu $0 < a_{n'}' < u$ şi $0 \leq a_i' < u$ pentru $0 \leq i < n'$.

Dacă $n < n'$, atunci $n + 1 \leq n'$ şi din Lema 1.9.2 rezultă:

$a = \sum_{i=0}^{n} a_i u^i < u^{n+1} \leq u^{n'} \leq \sum_{i=0}^{n'} a_i' u^i = a$, deci $a < a$-contradicţie.

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

Să demonstrăm acum că $a_i = a_i', 0 \leq i \leq n$. Dacă $n = 0$, atunci $a_0 = a = a_0'$.

Presupunem că $n > 0$ şi că afirmaţia este adevărată pentru $n - 1$. Din egalităţile: $a = u(a_n u^{n-1} + a_{n-1}u^{n-2} + ... + a_1) + a_0 = u(a_{n'}' u^{n'-1} + a_{n'-1}' u^{n'-2} + ... + a_1') + a_0'$, unde $0 \leq a_0 < u$ şi $0 \leq a_0' < u$ rezultă, folosind unicitatea câtului împărţirii lui a prin u, că $a_0 = a_0'$ şi $a_n u^{n-1} + a_{n-1}u^{n-2} + ... + a_1 = a_{n'}' u^{n'-1} + a_{n'-1}' u^{n'-2} + ... + a_1'$. 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 $a_n a_{n-1}...a_1 a_0$, unde $a_i < u, 0 \leq i \leq n, a_n \neq 0$ şi $a = \sum_{i=0}^{n} a_i u^i$.

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

Din Teorema 1.9.3 rezultă că se stabileşte astfel o corespondentă biunivocă între numerele naturale > 0 şi secvenţele finite $a_n a_{n-1}...a_1 a_0$ 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 $a_n a_{n-1}...a_1 a_{0(u)}$ sau $\overline{a_n a_{n-1}...a_1 a_{0(u)}}$.

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 noteaza 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: $7 \cdot 10^4 + 5 \cdot 10^3 + 0 \cdot 10^2 + 3 \cdot 10 + 8$.

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

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

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 doua numere reprezentate în aceeaşi bază.

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

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

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

Teorema 1.9.4. *Fie a şi b două numere naturale, $a = a_m a_{m-1}...a_1 a_{0(u)}$ şi $b = b_n b_{n-1}...b_1 b_{0(u)}$. 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 1.9.2. rezultă $a < u^{m+n} \leq u^n \leq b$, deci $a < b$. Dacă $m = n$ şi $a_p < b_p$, unde $p = max\{i | a_i \neq b_i\}$, atunci $b - a = (b_p - a_p)u^p + (b_{p-1}u^{p-1} + ... + b_0) - (a_{p-1}u^{p-1} + ... + a_0) > (b_p - a_p)u^p + (b_{p-1}u^{p-1} + ... + b_0) - u^p \geq u^p + (b_{p-1}u^{p-1} + ... + b_0) - u^p \geq 0$, de unde $b - a > 0$, deci $a < b$.

Reciproc, presupunem că $a < b$. Atunci $m \leq n$, 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 parţi a demonstraţiei, $b < a$. Teorema este astfel 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 arata cum se face adunarea şi înmulţirea numerelor naturale reprezentate într-o bază u. In particular, dacă $u = 10$, se regăsesc cunoscutele procedee de adunare şi înmulţire a numerelor naturale.

Fie a şi b două numere naturale, $a = a_m a_{m-1}...a_1 a_{0(u)}$, $b = b_n b_{n-1}...b_1 b_{0(u)}$. Trebuie să găsim cifrele $c_0, c_1, ...$ ale numărului $a+b$ în baza u. Putem scrie $a = a_0+a_1u+a_2u^2+...$ şi $b = b_0 + b_1u + b_2u^2 + ...$ Cum $a_0 < u$ şi $b_0 < u$, rezultă că $a_0 + b_0 < 2u$, deci $a_0 + b_0 = u\varepsilon_1 + c_0, 0 \leq c_0 < u, \varepsilon_1 = 0$ 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 $u \leq a_0 + b_0 < 2u$. Rezultă $a+b = c_0+(a_1+b_1+\varepsilon_1)u+(a_2+b_2)u^2+....$ Evident, $a_1+b_1+\varepsilon_1 < 2u$, de unde $a_1+b_1+\varepsilon_1 = u\varepsilon_2+c_1, 0 \leq c_1 < u$, unde $\varepsilon_2 = 0$ sau $\varepsilon_2 = 1$. Avem $a+b = c_0+c_1u+(a_2+b_2+\varepsilon_2)u^2+...$, s.a.m.d.

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

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

$\varepsilon_i = 1 \Leftrightarrow a_{i-1} + b_{i-1} + \varepsilon_{i-1} \geq u$ 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 $a_n + b_n + \varepsilon_n \geq u$, cifra de rang $m+1$ fiind în acest caz $c_{m+1} = 1$.

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

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. In 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

Cititorul poate singur acum să redacteze un algoritm al adunării numerelor naturale în baza u, luând ca motivaţie teoretică a acestuia consideraţiile de mai sus. Observăm că în acest algoritm apare variabila ε care are valoarea iniţială $\varepsilon_0 = 0$ iar valorile $\varepsilon_i, i \geq 1$, 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 unităţii de la cifrele de rang i la cele de rang $i + 1, i = 0, 1, ...$

In calculul cu "creionul şi hârtia" al sumei a două numere naturale, operaţiile din

algoritmul adunării în baza u se sistematizează astfel:

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

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

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

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

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.

In continuare se va arăta că înmulţirea a două numere naturale în baza u se reduce la urmatoarele tipuri de operaţii:

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

2) înmulţirea unui număr natural a cu o cifră a sistemului de numeraţie (deci cu un număr natural $j, 0 \leq j < u$);

3) adunarea în baza u.

Fie $a = a_m a_{m-1}...a_1 a_{0(u)} = a_m u^m + a_{m-1} u^{m-1} + ... + a_1 u + a_0$. Atunci $au^j = a_m u^{m+j} + a_{m-1} u^{m-1+j} + ... + a_1 u^{1+j} + a_0 u^j = a_m a_{m-1}...a_1 a_0 \underbrace{00..0}_{j}{}_{(u)}$ şi acum este clar cum se face în baza u o înmulţire de tipul 1).

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

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

câtul $q(i,j)$ şi restul $r(i,j)$ împărţirii numărului ij prin u depinzând de i şi j.

Fie acum a un număr natural dat în baza u, $a = a_m a_{m-1}...a_1 a_{0(u)} = \sum_{i=0}^{m} a_i u^i$ şi j o cifră a sistemului de numeraţie de bază u, deci $0 \leq j < u$. Avem:

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

deci efectuarea produsului aj în baza u revine la a face suma în baza u a numerelor a' şi a'' reprezentate în baza u:

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

$a'' = q(a_0, j) + q(a_1, j)u^2 + ...$

Aşadar, s-a lămurit cum se face în baza u şi o înmulţire de tipul 2).

In sfârşit, dacă $b = b_n b_{n-1}...b_1 b_{0(u)} = \sum_{j=0}^{n} b_j u^j$, 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 $ab_j u^j = (ab_j)u^j$. Aşadar ab_j este o operaţie de tipul 2) şi în sfârşit $(ab_j)u^j$ e o operaţie de tipul 1).

Cititorul se poate convinge usor că regula de înmulţire a numerelor naturale în baza zece se motivează din punct de vedere teoretic prin consideraţiile de mai sus, luând $u = 10$. Un instrument important al înmulţirii numerelor în baza zece este tabla înmulţirii numerelor < 10. Pe de altă parte, se observă că în regula de înmulţire a numerelor în baza u trebuie să cunoaştem numerele $q(i, j)$ şi $r(i, j), 0 \leq i, j < u$, din relaţia $(*)$. Din relaţia (ast) rezultă că $q(i, j)$ şi $r(i, j)$ sunt cifrele numărului $ij, 0 \leq i, j < u$, reprezentat în baza u (dacă $ij < u$, avem $q(i, j) = 0$). Aşadar, procedeul de înmulţire expus uzează de tabla înmulţirii numerelor naturale $< u$, cu rezultatele reprezentate în baza u.

In tabelele 2 şi 3 sunt date tablele înmulţirii 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 înmulţirii în baza 5

·	0	1
0	0	0
1	0	11

Tabelul 3: Tabla înmulţirii în baza 2

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

Să ne ocupăm acum de problema (III).

Trebuie observat că numărul natural a ce urmeaza 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 numeraţie 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 $u = 10$), execuţia algoritmului sistemelor de numeraţie putând fi astfel încredinţată 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 înţeles.

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

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

Pentru a trece pe $a = a_n a_{n-1}...a_1 a_{0(v)}$ din baza v în baza u cu metoda 2) se reprezintă mai întâi $a_0, a_1, ..., a_n$ şi v în baza u cu ajutorul algoritmului sistemelor de numeraţie. Se introduce $a_0, a_1, ..., a_n$ şi v astfel reprezentaţi în expresia $a_n v^n + a_{n-1} v^{n-1} + ... + a_1 v + a_0$ şi se face calculul acesteia folosind algoritmului adunării şi algoritmul înmulţirii în baza u. Se obţine, în final, reprezentarea lui a în calculator. Numerele sunt date de regulă în baza $u = 2$; efectuarea calculelor în baza $u = 2$ poate fi încredinţată calculatorului.

Metoda 3) este evident o combinaţie a primelor două. Astfel, dacă dorim să trecem un număr a dintr-o bază $v \neq 2$, într-o bază $u \neq 2$, 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 încredinţate calculatorului. Când $v \neq 10$ şi $u \neq 10$, 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 obişnuiţi.

Observaţii.

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

$$b = c_{r-1} u^{r-1} + ... + c_1 u + c_0, 0 \leq c_i < u, 0 \leq i < r. \quad (**)$$

De aici, rezultă că pentru a reprezenta numărul $a = a_n a_{n-1}...a_1 a_{0(v)} = a_n v^n + a_{n-1} v^{n-1} + ... + a_1 v + a_0$ în baza u, unde $v = u^r$ cu $r > 1$, fiecare cifră a_i se scrie ca în $(**)$, anume $a_i = c_{ir-1} u^{r-1} + ... + c_{i1} u + c_{i0}$ şi se înlocuieşte fiecare a_i cu secvenţa, $c_{ir-1}...c_{i1} c_{i0}$, deci obţinem secvenţa $c_{nr-1}...c_{n1} c_{n0} c_{n-1,r-1}...c_{n-1,1} c_{n-1,0}...c_{01} c_{00}$.

Inlăturând cifrele egale cu 0 de la începutul secvenţei de mai sus se obţine repreprezentarea lui a în baza u.

Astfel, pentru a reprezenta numărul $a = 375_{(8)}$ în baza $u = 2$ (deci $v = u$), scriem

mai întâi:

$$\begin{aligned} a_0 &= 5 = 1 \cdot 2^2 + 0 \cdot 2 + 1 \cdot 1 = c_{02} \cdot 2^2 + c_{01} \cdot 2 + c_{00}, \\ a_1 &= 7 = 1 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 1 = c_{12} \cdot 2^2 + c_{11} \cdot 2 + c_{10}, \\ a_3 &= 3 = 0 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 1 = c_{22} \cdot 2^2 + c_{21} \cdot 2 + c_{20}, \end{aligned}$$

aşadar secvenţa 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 observaţia 1. In acest caz, pentru a trece în baza u numărul $a = a_n a_{n-1} ... a_1 a_{0(v)}$ 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 obţine astfel reprezentarea lui a în baza u.

Astfel, dacă $u = 8$ şi $v = 2$, deci $v^3 = u$, numărul $a = 11111101_{(2)}$ 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 obţinute 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 metoda 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 dupa cum urmează:

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

In 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 [20].

Capitolul 2

Mulţimea numerelor prime

2.1 Teoreme referitoare la infinitatea numerelor prime

Reamintim că un număr $n \in \mathbf{N}, n \geq 2$ se zice *prim* dacă singurii săi divizori naturali sunt 1 şi n. Numărul natural 2 este singurul număr prim par iar pentru $n \geq 3$ 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? In cadrul acestui paragraf vom prezenta anumite rezultate ce răspund într-un fel la această întrebare.

Vom nota prin $\mathcal{P}$ mulţimea numerelor prime.

Teorema 2.1.1. (*Euclid*) *Mulţimea $\mathcal{P}$ este infinită. Demonstraţie.* Să presupunem prin absurd că mulţimea $\mathcal{P}$ este finită, $\mathcal{P} = \{p_1, p_2, ..., p_n\}$ (unde în mod evident $p_1 = 2, p_2 = 3, p_3 = 5$, etc.). Vom considera $p = p_1 p_2 ... p_n + 1$ şi să observăm că $p > 1$ iar $p_i \nmid p$ pentru $1 \leq i \leq n$. Ţinând cont de teorema fundamentală a aritmeticii va există un număr prim $q > 1$ care să dividă pe p. Cum toate numerele prime sunt presupuse a fi doar $p_1, .., p_n$ deducem că $q = p_i$ pentru un $i \in \{1, ..., n\}$, ceea ce este absurd căci $p_i \nmid p$ pentru orice $1 \leq i \leq n$. Deci $\mathcal{P}$ este mulţime infinită. ■

Observaţie. In continuare pentru fiecare număr natural $n \leq 1$ vom nota prin p_n al n-ulea număr prim, astfel că $\mathcal{P} = \{p_1, p_2, .., p_n, ...\}$ (evident $p_1 = 2, p_2 = 3, p_3 = 5$, etc).

O altă întrebare firească legată de mulţimea numerelor prime a fost dacă anumite submulţimi infinite ale lui $\mathbf{N}$ conţin sau nu o infinitate de numere prime. In acest sens merită amintit un rezultat celebru al lui Dirichlet :

Teorema 2.1.2. *(Dirichlet) Dacă $a, b \in \boldsymbol{N}^*$ iar $(a, b) = 1$, atunci mulţimea $\{an+b : n \in \boldsymbol{N}\}$ conţine o infinitate de numere prime.*

In cadrul acestei lucrări nu vom prezenta o demonstraţie completă a Teoremei 2.1.2 Totuşi, pentru anumite valori particulare ale lui a şi b vom prezenta în cadrul acestei lucrări demonstraţii complete.

Iată la început două exemple:

Teorema 2.1.3. *Există o infinitate de numere prime de forma* $4n-1$ *cu* $n \in \boldsymbol{N}^*$.

Demonstraţie. Să presupunem prin reducere la absurd că mulţimea $\{4n-1 : n \in \mathbf{N}^*\}$ conţine numai un număr finit de numere prime, fie acestea $q_1, .., q_t$ şi să considerăm numărul $q = 4q_1q_2..q_t - 1$. Numărul q trebuie să aibă un factor prim de forma $4k-1$ (căci dacă toţi 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 enunţ. ■

Teorema 2.1.4. *Există o infinitate de numere prime de forma* $6n-1$ *cu* $n \in \boldsymbol{N}^*$.

Demonstraţie. Să presupunem prin absurd că există doar un număr finit de numere prime de forma $6n-1$ şi anume $q_1, q_2, ..., q_k$ şi să considerăm numărul $q = 6q_1q_2...q_k - 1$. Cum un număr prim este de forma $6t-1$ sau $6t+1$, deducem că q trebuie să conţină 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 enunţ.■

Teorema 2.1.5. *(A. Rotkiewicz). Fie* p *un număr prim fixat. Există o infinitate de numere prime de forma* $pn+1$, *cu* $n \in \boldsymbol{N}$.

Demonstraţie. Să presupunem că există un număr finit $p_1, p_2, ..., p_t$ de numere prime de forma din enumt şi să considerăm $a = p \cdot p_1p_2...p_t$ (in caz că există numere prime de forma $pn+1$) sau $a = p$ în caz contrar.

Considerăm de asemenea numărul $N = a^{p-1} + a^{p-2} + ... + a + 1 > 1$ şi fie q un divizor al lui N. Atunci $q \mid N(a-1) = a^p - 1$, deci $a^p \equiv 1 (\text{mod } q)$. Atunci $\gamma_q(a) = 1$ sau $\gamma_q(a) = p$. Dacă $\gamma_q(a) = 1$, atunci $a \equiv 1(\text{mod } q)$ şi $0 \equiv N = a^{p-1} + ... + a + 1 \equiv p(\text{mod } q), q \mid p, q = p, p \mid N$. Cum $p \mid a$ şi $p \mid N$, atunci $p \mid N - a^{p-1} - a^{p-2} - ... - a = 1$, contradicţie.

Deci $\gamma_q(a) = p$ şi $p \mid \varphi(q) = q-1$, adică $q - 1 = ps$ cu $s \in \mathbf{N}$, deci $q = ps + 1$. Cum am presupus că $p_1, ..., p_t$ sunt toate numerele prime de forma $pn+1$, deducem că $q = p_i$ cu $1 \leq i \leq t$. Atunci $q \mid a$ şi $q \mid N$ şi din nou obţinem contradicţia că $q \mid 1$.

Deci pentru un număr prim p fixat există o infinitate de numere prime de forma $pn+1$. ■

2.2 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 $p \leq \sqrt{n}$. Intr-adevăr, să presupunem că n este compus şi că toate numerele prime ce-l divid verifică inegalităţile $\sqrt{n} < p < n$. Dacă un anumit număr prim p_0 divide pe n, atunci putem scrie $p = p_0n_0$ pentru un $n_0 \geq 2$. Atunci $n_0 = \frac{n}{p_0} < \frac{n}{p_0} = \sqrt{n}$ şi $n_0 \mid n$. Numărul n_0 va avea cel putin un factor prim (care va fi mai mic decât $\sqrt{n}$)- absurd!

Obţinem 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 mulţime 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 toţi multiplii proprii ai lui 2, apoi toţi 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 toţi 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 opreste deoarece conform criteriului enunţat 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 : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 51, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

In 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.

In 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). In 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 $p_{6000000} = 104.395.301$.

2.3 Teorema Bertrand-Cebîşev

In cadrul acestui paragraf vom demonstra următorul rezultat:

Teorema 2.3.1. *Dacă $n \in \boldsymbol{N}, n \geq 4$, 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 catre J. Bertrand însă cel care a prezentat primul o soluţie a acestuia a fost P. L. Cebîşev în anul 1850. In cele ce urmează vom prezenta o soluţie a lui P. Erdös (adaptată de L. Kalmar). Această soluţie se bazează pe demonstrarea câtorva leme:

Lema 2.3.2. *Dacă $n \in \boldsymbol{N}, n > 1$, atunci*

$$C_{2n}^n > \frac{4^n}{2\sqrt{n}} \quad (1).$$

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 $2 \cdot \frac{2n+1}{n+1} \cdot \frac{4^n}{2\sqrt{n}} > \frac{4^{n+1}}{2\sqrt{n+1}} \Leftrightarrow \frac{2n+1}{n+1} \cdot \frac{1}{\sqrt{n}} > \frac{2}{\sqrt{n+1}} \Leftrightarrow 2n+1 > \sqrt{4n(n+1)} \Leftrightarrow 4n^2+4n+1 > 4n^2+4n \Leftrightarrow 1 > 0$ ceea ce este evident. ■

Lema 2.3.3. *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* $n \in \boldsymbol{N}^*$.

Demonstraţie. Facem din nou inducţie 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, $n = 2k+1$ ($k \in \mathbf{N}^*$), atunci orice număr prim p astfel încât $k+2 \leq p \leq 2k+1$ este un divizor al lui $C_{2k+1}^{k} = \frac{(2k+1)2k(2k-1)...(k+2)}{1 \cdot 2 \cdot ... \cdot k}$. 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 astfel încât $k+2 \leq p \leq 2k+1$ divizând C_{2k+1}^{k} este inferior lui 4^k (ţinând 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 ţinând cont de ipoteza de inducţie, $P_{k+1} < 4^{k+1}$ şi de (2) deducem că $P_n < 4^{k+1} \cdot 4^k = 4^{2k+1} = 4^n$ şi astfel Lema 2.3.3 este demonstrată. ■

Lema 2.3.4. *Daca p este un număr prim ce divide* C_{2n}^{n} *astfel încât* $p \geq \sqrt{2n}$*, atunci p apare cu exponentul* 1 *în descompunerea lui* C_{2n}^{n} *în factori primi.*

Demonstraţie. Exponentul lui p în $C_{2n}^{n} = \frac{(2n)!}{(n!)^2}$ va fi $\alpha = \sum_{k \geq 1} ([\frac{2n}{p^k}] - 2[\frac{n}{p^k}])$.

Daca $p \geq \sqrt{2n}$ (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 $\alpha = [\frac{2n}{p}] - 2[\frac{n}{p}] < 2$, de unde $\alpha = 1$ şi astfel lema este demonstrată. ■

Pentru un număr real pozitiv x, prin $\pi(x)$ desemnăm numărul numerelor prime q astfel încât $q \leq x$.

Lema 2.3.5. *Dacă p este un număr prim,* $r \in \boldsymbol{N}^*$ *astfel încât* $p^r | C_{2n}^{n}$*, atunci* $p^r \leq 2n$ *şi* $C_{2n}^{n} \leq (2n)^{\pi(2n)}$.

Demonstraţie. Din $p^r | C_{2n}^{n}$, deducem că exponentul lui p în descompunerea lui C_{2n}^{n} în factori primi (care este $\alpha = \sum_{k \geq 1} ([\frac{2n}{p^k}] - 2[\frac{n}{p^k}])$) verifică inegalitatea $\alpha \geq r$.

Dacă am avea $p^r > 2n$, pentru $k \geq r$ am avea $[\frac{2n}{p^k}] - 2[\frac{n}{p^k}] = 0$ şi atunci $\alpha = \sum_{k=1}^{r-1} ([\frac{2n}{p^k}] - 2[\frac{n}{p^k}])$. Cum pentru orice $x \in \mathbf{R}$ avem $[2x] - 2[x] \leq 1$ 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 $C_{2n}^{n} \leq (2n)^{\pi(2n)}$. ■

Lema 2.3.6. *Dacă $n \in \boldsymbol{N}, n > 2$, atunci nici un număr prim p astfel încât $\frac{2}{3}n < p \leq n$ nu poate să dividă C_{2n}^n.*

Demonstraţie. Dacă $\frac{2}{3}n < p \leq n$, atunci $\frac{2n}{p} < 3$ şi $\frac{n}{p} \geq 1$, deci $[\frac{2n}{p}] \leq 2$ şi $[\frac{n}{p}] \geq 1$, de unde deducem că $[\frac{2n}{p}] - 2[\frac{n}{p}] \leq 2 - 2 \cdot 1 = 0$. Cum pentru orice $x \in \mathbf{R}, [2x] - 2[x] \geq 0$, deducem că $[\frac{2n}{p}] - 2[\frac{n}{p}] = 0$.

Pentru $k > 1$, avem $p^k > \frac{4}{9}n^2$ şi atunci $\frac{2n}{p^k} < \frac{9}{2n} < 1$ pentru $n > 4$, deci $[\frac{2n}{p^k}] - 2[\frac{n}{p^k}] = 0$ pentru $k > 1$ şi $n > 4$. 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. ■

Lema 2.3.7. *Un număr prim p astfel încât $n < p < 2n$ apare în descompunerea lui C_{2n}^n în factori primi cu exponentul 1 ($n \geq 2$).*

Demonstraţie. Dacă $n < p < 2n$, atunci $1 < \frac{2n}{p} < 2$ şi $\frac{n}{p} < 1$, deci $[\frac{2n}{p}] = 1$ şi $[\frac{n}{p}] = 0$. Pentru $k \geq 2$, avem $\frac{2n}{p^k} \leq \frac{2n}{p^2} < \frac{2}{n}$, deci pentru $n > 1$ avem $\frac{2n}{p^k} < 1$ şi $[\frac{2n}{p^k}] = 0$ ca şi $[\frac{n}{p^k}] = 0$.

Deci exponentul α al lui p în C_{2n}^n este 1. ■

Lema 2.3.8. *Dacă $n \in \boldsymbol{N}, n \geq 14$, atunci $\pi(n) \leq \frac{n}{2} - 1$.*

Demonstraţie. Se verifică imediat că $\pi(14) = 6 = \frac{14}{2} - 1$, adică lema este adevarată pentru $n = 14$.

In şirul $1, 2, ..., n$ numerele $4, 6, ..., 2 \cdot [\frac{n}{2}]$ (în număr de $[\frac{n}{2}] - 1$) sunt compuse. Pe de alta parte, pentru $n \geq 15$, şirul $1, 2, ..., n$ conţine şi numerele impare compuse $1, 9$ şi 15, de unde deducem că $\pi(n) \leq n - ([\frac{n}{2}] - 1 + 3) = n - [\frac{n}{2}] - 2 < \frac{n}{2} - 1$ (căci $[\frac{n}{2}] > \frac{n}{2} - 1$) şi astfel lema este probată (observând că pentru $n \geq 15$ avem chiar $\pi(n) < \frac{n}{2} - 1$). ■

Lema 2.3.9. *Fie $R_n = \prod_{\substack{p \text{ prim}, \\ n < p < 2n}} p$ (sau $R_n = 1$ dacă nu există astfel de numere prime). Atunci, pentru $n \geq 98$ avem $R_n > \frac{\sqrt[3]{4^n}}{2\sqrt{n} \cdot (2n)^{\sqrt{\frac{n}{2}}}}$ (3) .*

Demonstraţie. După felul în care am definit pe R_n deducem că $R_n | C_{2n}^n$, deci putem scrie $C_{2n}^n = R_n \cdot Q_n$, cu $Q_n \in \mathbf{N}^*$. Conform Lemei 2.3.7, dacă p este un număr prim astfel încât $n < p < 2n$, atunci $p \nmid Q_n$ şi prin urmare dacă p este prim şi $p | Q_n$, cu necesitate $p \leq n$. Conform Lemei 2.3.6 avem chiar mai mult, $p \leq \frac{2}{3}n$, astfel că produsul divizorilor primi ai lui Q_n va fi cel mult egal cu $P_{[\frac{2n}{3}]}$ iar conform Lemei 2.3.3 acest produs va fi $< 4^{[\frac{2n}{3}]} \leq 4^{\frac{2n}{3}}$.

Conform Lemei 2.3.4, cum $Q_n | C_{2n}^n$ se vede că exponentul unui număr prim p din descompunerea lui Q_n nu va fi > 1 decât dacă $p < \sqrt{2n}$.

Numărul acestor numere prime va fi conform Lemei 2.3.8 (înlocuind în aceasta pe n prin $[\sqrt{2n}]$, lucru posibil deoarece $n \geq 98 \Rightarrow \sqrt{2n} \geq 14$, de unde şi $[\sqrt{2n}] \geq 14$) inferior lui $\frac{\sqrt{2n}}{2}$.

Conform Lemei 2.3.5, produsul puterilor acestor numere prime (care divid Q_n, deci şi pe C_{2n}^n) va fi cel mult egal cu $(2n)^{\frac{\sqrt{2n}}{2}}$, de unde deducem în final că $Q_n < 4^{\frac{2n}{3}} \cdot (2n)^{\frac{\sqrt{2n}}{2}}$. (4)

Astfel, cum $R_n = \frac{C_{2n}^n}{Q_n}$ deducem, tinând cont de Lema 2.3.2 şi inegalitatea (4) că $R_n > \frac{4^n}{2\sqrt{n}} \cdot \frac{1}{4^{\frac{2n}{3}} \cdot (2n)^{\frac{\sqrt{2n}}{2}}} = \frac{\sqrt[3]{4^n}}{2\sqrt{n} \cdot (2n)^{\sqrt{\frac{n}{2}}}}$ adică exact inegalitatea (3). ■

Lema 2.3.10. *Dacă $k \in \boldsymbol{N}, k \geq 8$, atunci $2^k > 18(k+1)$.*

Demonstraţie. Cum $2^8 = 256 > 18 \cdot 9$ iar dacă $2^k > 18(k+1)$, atunci $2^{k+1} = 2 \cdot 2^k > 2 \cdot 18(k+1) = 36k + 36 > 18k + 36 = 18(k+2)$, deducem conform principiului induţiei matematice că lema este adevărată pentru orice $k \geq 8$. ■

Lema 2.3.11. *Dacă $x \in \boldsymbol{R}, x \geq 8$, atunci $2^x > 18x$.*

Demonstraţie. Pentru $x \in \mathbf{R}, x \geq 8$ avem $[x] \geq 8$ şi conform Lemei 2.3.10. avem $2^x \geq 2^{[x]} \geq 18([x]+1) > 18x$. ■

Lema 2.3.12. *Dacă $k \in \boldsymbol{N}, k \geq 6$, atunci $2^k > 6(k+1)$.*

Demonstraţie. Se face induţie matematică după k (sau, dacă ţinem cont de Lema 2.3.10 mai avem de demonstrat inegalităţile pentru $k = 6$ şi $k = 7$ care sunt adevarate deoarece $2^6 > 64 > 6 \cdot 7$ şi $2^7 > 128 > 6 \cdot 8$). ■

Lema 2.3.13. *Dacă $x \in \boldsymbol{R}, x \geq 6$, atunci $2^x > 6x$.*

Demonstraţie. Ca în cazul Lemei 2.3.11. ■

Lema 2.3.14. *Dacă $n \in \boldsymbol{N}, n \geq 648$, atunci $R_n > 2n$.*

Demonstraţie. Ţinând cont de Lema 2.3.9 este suficient să demonstrăm că pentru $n \geq 648$ avem $\sqrt[3]{4^n} > 4n\sqrt{n} \cdot (2n)^{\frac{\sqrt{n}}{2}}$. Cum pentru $n \geq 648$, $\frac{\sqrt{2n}}{6} \geq 6$, conform Lemei 2.3.13 avem $2^{\frac{\sqrt{2n}}{6}} > \sqrt{2n}$, de unde ridicând ambii membrii la puterea $\sqrt{2n}$ deducem că $\sqrt[3]{2^n} > (2n)^{\frac{\sqrt{n}}{2}}$.

De asemenea, din $n \geq 648$, deducem că $\frac{2n}{9} > 8$ şi atunci conform Lemei 2.3.11 avem $2^{\frac{2n}{9}} > 4n$, de unde $2^{\frac{n}{3}} > 4n\sqrt{4n} > 4n\sqrt{n}$.

Deci, pentru $n \geq 648, 2^{\frac{n}{3}} > (2n)^{\frac{\sqrt{n}}{2}}$ şi $2^{\frac{n}{3}} > 4n\sqrt{n}$ de unde $\sqrt[3]{4^n} > 4n\sqrt{n} \cdot (2n)^{\frac{\sqrt{n}}{2}}$ şi cu aceasta lema este demonstrată. ■

Lema 2.3.15. *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 2.3.14.

Dacă $n = 6$, lema este adevărată căci între 6 şi 12 se afla numerele prime 7 şi 11.

Mai avem de demonstrat Lema 2.3.15 pentru $7 \leq n \leq 647$. Acest lucru poate fi facut fie direct (utilizând un tabel de numere prime ≤ 1000), fie construind un şir de

numere prime $q_0, q_1, ..., q_m$ astfel încât $q_0 = 7, q_k < 2q_k - 2, 2 \leq k \leq m$ 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 2.3.15. pentru $7 \leq n \leq a = 647$.

Primul termen al şirului $q_0, q_1, ..., q_m$ nu depăşeşte pe n decât dacă $q_m > q_{m-1} > a \geq n$, deci $q_m > n$.

Există deci un indice maximal $k < m-1$ astfel încât $q_k < n$. 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 2.3.16. (*Cebîşev*) *Dacă $n \in \boldsymbol{N}, n \geq 4$, 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 2.3.15 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. ■

In continuare vom prezenta câteva corolare la Teorema lui Cebîşev.

Corolar 2.3.17. *Dacă $n \in \boldsymbol{N}, n \geq 2$, 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. In anul 1892 J. J. Sylvester a demonstrat urmatoarea generalizare a Corolarului 2.3.17: *Dacă $n, k \in \boldsymbol{N}, n > k$, atunci în şirul n, n+1,...,n+k-1 se află cel puţin un număr admiţând un divizor prim $> k$.*

Corolarul 2.3.17 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.

Corolar 2.3.18. *Dacă $k \in \boldsymbol{N}, k > 1$, atunci $p_k < 2^k$.*

Demonstraţie. Facem induţie după k. Pentru $k = 2$ avem $p_2 = 3 < 2^2$. Dacă $p_k < 2^k$, conform Corolarului 2.3.17 există cel puţin un număr prim p astfel încât $2^k < p < 2 \cdot 2^k = 2^{k+1}$ şi astfel corolarul este demonstrat. ■

Corolar 2.3.19. *Dacă $n \in \boldsymbol{N}, n \geq 2$, atunci în descompunerea lui n! în factori primi găsim cel puţin un număr prim cu exponentul egal cu 1.*

Demonstraţie. Corolarul este în mod evident adevărat pentru $n = 2$ şi $n = 3 (2! = 2, 3! = 2 \cdot 3)$.

Fie acum $n \geq 4$. Dacă n este par, $n = 2k$, atunci $k \geq 2$ şi conform Corolarului 2.3.17 între k şi $2k = n$ găsim cel puţin un număr prim p astfel încât $k < p < 2k = n$.

Vrem să demonstrăm că p apare cu exponentul 1 în descompunerea în factori primi a lui $n!$. Intr-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, $n = 2k + 1 \Rightarrow k \geq 2$ şi din nou conform Corolarului 2.3.17 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. ■

Observaţie. De fapt, Corolarele 2.3.17 şi 2.3.19 sunt echivalente.

Intr-adevăr, mai înainte am văzut cum Corolarul 2.3.17 implică Corolarul 2.3.19 Reciproc, să admitem că ceea ce afirmă Corolarul 2.3.19 este adevărat (adică pentru orice număr natural $n \geq 1$ în $n!$ există cel puţin un număr prim cu exponentul 1) şi să demonstrăm Corolarul 2.3.17 (adică pentru orice $n \geq 2$, între n şi $2n$ se află cel puţin un număr prim). Intr-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 $(2n)! = 1 \cdot 2 \cdot ... \cdot (n-1) \cdot n(n+1) \cdot ... \cdot (2n)$ apar şi p şi $2p$ şi astfel exponentul lui p în $(2n)!$ ar fi cel puţin 2. In concluzie, $2n < 2p$, adică $n < p$ şi cum $n < 2p$ deducem că $n < p < 2n$. ■

Deducem imediat:

Corolar 2.3.20. *Dacă $n \in \boldsymbol{N}, n \geq 2$ atunci $n!$ nu poate fi puterea unui număr natural cu exponentul > 1.*

Corolar 2.3.21. *Pentru orice $k \in \boldsymbol{N}, k \geq 4$, avem inegalitatea $p_{k+2} < 2p_k$.*

Demonstraţie. Pentru $k \geq 4$ avem $p_k > p_3 = 5$ şi atunci conform Lemei 2.3.15 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 $p_{k+2} < 2p_k$. ■

Corolar 2.3.22. *Pentru orice $k \in \boldsymbol{N}, k \geq 2$ 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. ■

Corolar 2.3.23. *Dacă $n, k \in \boldsymbol{N}, n \geq 2$, atunci*

$$\frac{1}{n} + \frac{1}{n+1} + ... + \frac{1}{n+k} \notin \mathbf{N}.$$

Demonstraţie. Dacă $x = \frac{1}{n} + \frac{1}{n+1} + ... + \frac{1}{n+k} \in \mathbf{N}$, 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 2.3.17, 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 2.3.17, între n şi $2n$ există un număr prim r. Cum $r < 2n \leq n + k$, ţinând cont de felul în care l-am ales pe p deducem că $r \geq p$. De asemenea, deoarece $n < r$, avem $n < p \leq n + k < 2p$.

Deducem de aici ca 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 fracţie

(cu numitorul $n(n+1)...(n+k)$) 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 $t = n(n+1)...(n+k)$), $p|t$ şi $p \nmid m$, de unde concluzia că $x \notin \mathbf{N}$. ■

2.4 Inegalităţile lui Cebîşev

Reamintim că pentru $x \in \mathbf{R}_+$, 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.

In anul 1958, D. H. Lehmer a calculat $\pi(10^8)$ şi $\pi(10^9)$ aratând 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 2.3.9 am definit pentru $n \geq 1, R_n = \prod_{\substack{p \text{ prim}, \\ n < p < 2n}} p$.

Există $\pi(2n) - \pi(n)$ numere prime p astfel încât $n < p \leq 2n$ şi cum toate aceste numere prime sunt $\leq 2n$ deducem că $R_n \leq (2n)^{\pi(2n)-\pi(n)}$. Ţinând cont de Lema 2.3.9, deducem că pentru $n \geq 98$ avem inegalitatea $(2n)^{\pi(2n)-\pi(n)} > \frac{\sqrt[3]{4^n}}{2\sqrt{n} \cdot (2n)^{\sqrt{\frac{n}{2}}}}$, de unde, logaritmând în baza 10 deducem inegalitatea

(1) $\pi(2n) - \pi(n) > \frac{n}{3\lg(2n)}[\lg(4) - \frac{3\lg(4n)}{2n} - \frac{3\lg(2n)}{\sqrt{2n}}]$.

Cum $\lim\limits_{x\to\infty} \frac{\lg(x)}{\sqrt{x}} = \lim\limits_{x\to\infty} \frac{\lg(x)}{x} = 0$, din (1) deducem că $\lim\limits_{x\to\infty} [\pi(2n) - \pi(n)] = \infty$.

De aici deducem:

Corolar 2.4.1. *Pentru orice număr natural k există un număr natural m_k astfel încât pentru orice $n \geq m_k$, există cel putin k numere prime între n şi $2n$.*

Fie acum $p_1, ..., p_r$ numerele prime ce intră în descompunerea în factori primi a lui C_{2n}^n (evident $p_1, p_2, ..., p_r \leq 2n$). Fiecare număr p_i apare la puterea $([\frac{2n}{p_i}] - 2[\frac{n}{p_i}]) + ... + ([\frac{2n}{p_i^{q_i}}] - 2[\frac{n}{p_i^{q_i}}])$, unde q_i este cel mai mare număr natural pentru care $p_i^{q_i} \leq 2n$.

Cum pentru orice $a \geq 0$, $[2a] - 2[a] = 0$ sau 1, deducem că suma $\sum\limits_{k=1} ([\frac{2n}{p_i^k}] - 2[\frac{n}{p_i^k}]) \leq \underbrace{1 + ... + 1}_{q_i} = q_i$, astfel că fiecare p_i apare în descompunerea lui C_{2n}^n la o putere $\leq q_i$, deci $C_{2n}^n \leq p_1^{q_1}...p_r^{q_r} \leq (2n)...(2n) = (2n)^r$.

Cum $r = \pi(2n)$ deducem că $C_{2n}^n \leq (2n)^{\pi(2n)}$ (este de fapt o redemonstrare a inegalităţii din cadrul Lemei 2.3.5!).

Pe de alta parte, $C_{2n}^n = \frac{2n(2n-1)...(n+1)}{1 \cdot 2 \cdot ... \cdot n}$ se divide prin produsul tuturor numerelor prime $p_{s+1}, p_{s+2}, ..., p_r$ mai mari decât n şi mai mici decât $2n$ (am notat prin $p_1, ...p_s$ toate numerele prime mai mici decât n).

Astfel, $C_{2n}^n \geq p_{s+1}p_{s+2}...p_r > \underbrace{n \cdot n \cdot ... \cdot n}_{r-s \text{ ori}} = n^{r-s}$.

Cum $r = \pi(2n)$ şi $s = \pi(n)$, deducem că

$$(2) \quad n^{\pi(2n)-\pi(n)} < C_{2n}^n < (2n)^{\pi(2n)}.$$

De asemenea, pentru orice număr natural $n \geq 1$, avem

$$(3) \quad 2^n < C_{2n}^n < 4^n.$$

Comparând (2) cu (3) deducem că $2^n < 2^{\pi(2n)}$, de unde prin logaritmare în baza 10 deducem:

$$(4) \quad \pi(2n) > \frac{\lg 2}{2} \cdot \frac{2n}{\lg(2n)} = 0,15051... \cdot \frac{2n}{\lg(2n)}.$$

Cum pentru $n \geq 1$ avem $\frac{2n}{2n+1} \geq \frac{2}{3}$ deducem că:

$\pi(2n+1)\lg(2n+1) > \pi(2n)\lg(2n) > 0,15051... \cdot 2n > \frac{2}{3} \cdot 0,15051... \cdot (2n+1) = 0,10034... \cdot (2n+1)$ sau $\pi(2n+1) > 0,10034... \cdot \frac{2n+1}{\lg(2n+1)}$.

Obţinem astfel următorul rezultat:

Propoziţia 2.4.2. *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 $\pi(2n) - \pi(n) < 2\lg 2 \cdot \frac{n}{\lg n}$.

Fie acum $x \geq 0$ un număr real. Dacă notăm $[\frac{x}{2}] = n$, atunci în mod evident $x = 2n$ sau $2n+1$ şi vom avea

$\pi(x) - \pi(\frac{x}{2}) \leq \pi(2n) - \pi(n) + 1 < 0,60206... \cdot \frac{n}{\lg n} + 1 < 1,60206... \cdot \frac{n}{\lg n}$ (deoarece $\frac{n}{\lg n} > 1$).

Se verifică imediat că pentru $n \geq 3$, din $n < x$ rezultă $\frac{n}{\lg n} < \frac{x}{\lg x}$, deci pentru $[\frac{x}{2}] \geq 3$ avem $\pi(x) - \pi(\frac{x}{2}) < 1,60206... \cdot \frac{x}{\lg x}$.

Este uşor de verificat că ultima inegalitate este valabilă şi pentru $[\frac{x}{2}] < 3$; într-adevăr, dacă $[\frac{x}{2}] < 3$, diferenţa $\pi(x) - \pi(\frac{x}{2})$ evident poate fi egală cu 2 (pentru $2,5 \leq \frac{x}{2} < 3$), 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 $x \in \mathbf{R}_+$:

$$(5) \quad \pi(x) - \pi(\frac{x}{2}) < 1,60206... \cdot \frac{x}{\lg x}.$$

Din (5) deducem mai departe că

$\pi(x)\lg x - \pi(\frac{x}{2})\lg\frac{x}{2} = [\pi(x) - \pi(\frac{x}{2})]\lg x + \pi(\frac{x}{2})[\lg x - \lg\frac{x}{2}] < \lg x \cdot 1,60206... \cdot \frac{x}{\lg x} + \lg 2 \cdot \pi(\frac{x}{2}) < (1,60206... + \frac{\lg 2}{2}) \cdot x \approx 1,75257... \cdot x$ (am folosit faptul evident: $\pi(\frac{x}{2}) < \frac{x}{2}$).

Deci $\pi(x)\lg x - \pi(\frac{x}{2})\lg\frac{x}{2} < 1,75257... \cdot x$.

Fie acum $n \in \mathbf{N}, n > 1$. Conform ultimei inegalităţi avem:

$$\pi(n)\lg n - \pi(\frac{n}{2})\lg\frac{n}{2} < 1,75257... \cdot n$$
$$\pi(\frac{n}{2})\lg\frac{n}{2} - \pi(\frac{n}{4})\lg\frac{n}{4} < 1,75257... \cdot \frac{n}{2}$$
$$.....$$
$$\pi(\frac{n}{2^{k-1}})\lg\frac{n}{2^{k-1}} - \pi(\frac{n}{2^k})\lg\frac{n}{2^k} < 1,75257... \cdot \frac{n}{2^{k-1}}$$

(vom alege pe k astfel încât $2^k > n$).

Adunând aceste inegalităţi deducem că :

$$\begin{aligned}\pi(n)\lg n - \pi(\frac{n}{2^k})\lg\frac{n}{2^k} &< 1,75257... \cdot (n + \frac{n}{2} + ... + \frac{n}{2^{k-1}}) = 1,75257... \cdot \frac{n - \frac{n}{2^k}}{1 - \frac{1}{2}} \\ &< 3,50514... \cdot n < 4n.\end{aligned}$$

Cum pentru $2^k > n$, $\frac{n}{2^k} < 1$, şi deci $\pi(\frac{n}{2^k}) = 0$, deducem că $\pi(n) < 4 \cdot \frac{n}{\lg n}$.

Am obţinut astfel:

Propoziţia 2.4.3. *Dacă* $n > 1, \pi(n) < 4 \cdot \frac{n}{\lg n}$.

Din Propoziţiile 2.4.2 şi 2.4.3 deducem:

Propoziţia 2.4.4. *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 2.4.4 capătă o formulare mai elegantă $0,92 \cdot \frac{n}{\ln n} < \pi(n) < 1,11 \cdot \frac{n}{\ln n}$, astfel că variaţia funcţiei $\pi(n)$ este redată cu o mai mare exactitate de funcţia $\frac{n}{\ln n}$ (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 $\pi(n) : \frac{n}{\lg n}$ există pentru $n \to \infty$ (şi deci este egală cu 1) a fost demonstrat 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; pentru detalii recomandăm cititorului lucrarea [36]).

Obţinem deci $\pi(n) \approx \frac{n}{\lg n}$ pentru $n > 1$.

Teorema 2.4.5. *(Cebîşev) Pentru* $x \in \boldsymbol{R}, x \geq 2$ *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:

$$n^{\pi(2n)-\pi(n)} < C_{2n}^n < (2n)^{\pi(2n)} \text{ şi } 2^n < C_{2n}^n < 4^n$$

pentru $n \in \mathbf{N}, n \geq 2$, de unde deducem că $\pi(2n) - \pi(n) \leq 2\lg 2 \cdot \frac{n}{\lg n}$ şi $\pi(2n) \geq \lg 2 \cdot \frac{n}{\lg n}$.

Pentru $x \in \mathbf{R}, x \geq 2$, alegem acum $n \in \mathbf{N}$ astfel încât $n \leq \frac{x}{2} < n+1$, astfel că $\pi(x) \geq \pi(2n) \geq \lg 2 \cdot \frac{n}{\lg(2n)} \geq \lg 2 \cdot \frac{n}{\lg x} \geq \frac{\lg 2}{4} \cdot \frac{2n+2}{\lg x} > \frac{\lg 2}{4} \cdot \frac{x}{\lg x}$.

Să stabilim acum a doua inegalitate.

Pentru un număr real oarecare $y \geq 4$, alegem $n \in \mathbf{N}$ astfel încât $n - 1 < \frac{y}{2} \leq n$.

Astfel,

$$\begin{aligned} \pi(y) - \pi(\frac{y}{2}) &\leq \pi(2n) - \pi(n) + 1 \leq \frac{2n\lg 2}{\lg n} + 1 \leq \frac{(y+2)\lg 2}{\lg \frac{y}{2}} + 1 \\ &\leq \frac{2(y+2)\lg 2}{\lg y} + 1 \leq \frac{3y\lg 2}{\lg y} + 1 < \frac{4y\lg 2}{\lg y}. \end{aligned}$$

Am demonstrat astfel că pentru $y \in \mathbf{R}, y \geq 4$, avem $\pi(y) - \pi(\frac{y}{2}) < 4\lg 2 \cdot \frac{y}{\lg y}$.

Evident că pentru $2 \leq y < 4$ avem $\pi(y) - \pi(\frac{y}{2}) \leq 2$ şi cum funcţia $y \to \frac{y}{\lg y}$ îşi atinge valoarea minimă în $y = e$, deducem că $\pi(y) - \pi(\frac{y}{2}) \leq \frac{\frac{2}{e}^y}{\lg y}$ pentru $2 \leq y \leq 4$.

Cum însă $\frac{2}{e} < 4\lg 2$, deducem că $\pi(y) - \pi(\frac{y}{2}) < 4\lg 2 \cdot \frac{y}{\lg y}$ pentru orice $y \geq 2$.

Astfel, pentru $y \geq 2$, avem:

$$\pi(y)\lg y - \pi(\frac{y}{2})\lg\frac{y}{2} = [\pi(y) - \pi(\frac{y}{2})]\lg y + \pi(\frac{y}{2})\lg 2 < 4y\lg 2 + \frac{y}{2}\lg 2 = \frac{9}{2}\lg 2.$$

Fie acum $x \in \mathbf{R}, x \geq 2$ şi $r \in \mathbf{N}$ astfel încât $2^{r+1} \geq x < 2^{r+2}$. Inlocuind 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 $\pi(\frac{x}{2^{r+1}}) = 0$ obţinem în final că $\pi(x)\lg x < \frac{9}{2}(x + \frac{x}{2} + ... + \frac{x}{2^r}\lg 2 < (9\lg 2)x$, adică a doua inegalitate din enunţ . ■

Observaţie. In 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 $\frac{x}{\lg x} \cdot (1 + \frac{1}{2\lg x}) < \pi(x) < \frac{x}{\lg x} \cdot (1 + \frac{3}{2\lg x})$.

Teorema 2.4.6. *Pentru $n \in \boldsymbol{N}, n \geq 2$ avem $\frac{n\lg n}{9\lg 2} < p_n < \frac{8n\lg n}{\lg 2}$.*

Demonstraţie. Ţinând cont de Teorema 2.4.5, pentru $n \in \mathbf{N}, n \geq 1$ avem $n = \pi(p_n) < (9\lg 2) \cdot \frac{p_n}{\lg p_n}$, de unde deducem prima inegalitate din enunţ.

Cum funcţia $f : (0, +) \to \mathbf{R}, f(x) = \frac{\lg x}{\sqrt{x}}$ 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 $p_n \geq e^9$, $\frac{\lg 2}{4} \cdot p_n, n \cdot \lg p_n < 2n \cdot \lg n$ 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. In 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 $n \lg n + n \lg(\lg n) - 10n < p_n < n \lg n + n \lg(\lg n) + 8n$.

Intr-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 demonstreză următoarele:

1) Pentru orice $n \in \mathbf{N}, n \geq 2$ avem $p_n > n(\ln n + \ln(\ln n) - \frac{3}{2})$;

2) Pentru orice $n \in \mathbf{N}, n \geq 20$ avem $p_n < n(\ln n + \ln(\ln n) - \frac{1}{2})$.

Teorema 2.4.7. *Pentru orice $x \in \boldsymbol{R}, x \geq 3$, există două constante reale pozitive $c_1, c_2 > 0$, astfel încât*:

$$c_1 \lg(\lg x) < \sum_{\substack{p \text{ prim}, \\ p \leq x}} \frac{1}{p} < c_2 \lg(\lg x).$$

Demonstraţie. Fie $x \in \mathbf{R}, x \geq 3$. Cum $\pi(n) - \pi(n-1) = \begin{cases} 1, & \text{dacă } n \text{ prim} \\ 0, & \text{în rest} \end{cases}$ avem:

$$\begin{aligned} \sum_{\substack{p \text{ prim}, \\ p \leq x}} \frac{1}{p} &= \sum_{2 \leq n \leq x} \frac{\pi(n) - \pi(n-1)}{n} = \sum_{2 \leq n \leq x} \pi(n) \cdot (\frac{1}{n} - \frac{1}{n+1}) + \frac{\pi(x)}{[x]+1} \\ &= \sum_{2 \leq n \leq x} \frac{\pi(n)}{n(n+1)}) + \frac{\pi(x)}{[x]+1}. \end{aligned}$$

Conform inegalităţilor lui Cebîşev (Teorema 2.4.5) 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

$$\frac{\lg 2}{4} \sum_{2 \leq n \leq x} \frac{1}{(n+1) \lg n} < \sum_{2 \leq n \leq x} \frac{\pi(n)}{n(n+1)} < 9 \lg 2 \cdot \sum_{2 \leq n \leq x} \frac{1}{(n+1) \lg n}.$$

Prin induţie matematică se probează că pentru orice $k \in \mathbf{N}, k \geq 1$ avem $\lg k < \sum_{n=1}^{k} \frac{1}{n} \leq \lg k + 1$.

De asemenea, pentru orice $x \in \mathbf{R}, x \geq 1$ avem $|\sum_{\substack{n \in \mathbf{N}^*, \\ n \leq x}} \frac{1}{n} - \lg x| \leq 1$.

Din cele de mai înainte deducem existenţa unei constante $c > 0$ astfel încât $|\sum_{2 \leq n \leq x} \frac{1}{(n+1) \lg n}) - \lg(\lg x)| < c$. Evaluând acum $\frac{\pi(n)}{[x]+1}$ obţinem constantele c_1 şi c_2 din enunţ. ■

Observaţie. Dacă pentru două funcţii reale f şi g scriem $f \sim g$ dacă $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$, atunci vom menţiona următoarele rezultate:

1. $\pi(x) \sim \frac{x}{\lg x}$. Acest rezultat cunoscut şi sub numele de *Teorema elementului prim* sau *Legea de repartiţie 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 demonstraţie 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 $\pi(x) \sim L_i(x) = \int\limits_2^x \frac{1}{\lg t} dt$.

Deoarece $\int\limits_2^x \frac{1}{\lg t} dt = \frac{x}{2} - \frac{2}{\lg 2} + \int\limits_2^x \frac{1}{(\lg t)^2} dt$ şi $0 < \int\limits_2^x \frac{1}{(\lg t)^2} dt = \int\limits_2^{\sqrt{x}} \frac{1}{(\lg t)^2} dt + \int\limits_{\sqrt{x}}^x \frac{1}{(\lg t)^2} dt < \frac{\sqrt{x}-2}{(\lg 2)^2} + \frac{x-\sqrt{x}}{\frac{1}{4}\cdot(\lg 2)^2} < \frac{\sqrt{x}}{(\lg 2)^2} + \frac{4x}{(\lg 2)^2}$, deducem că $0 < \frac{\int\limits_2^x \frac{1}{(\lg t)^2} dt}{\frac{x}{\lg x}} < \frac{\lg x}{\sqrt{x}(\lg 2)^2} + \frac{4}{\lg x}$, de unde acum se deduce facil că $\frac{x}{\lg x} \sim L_i(x)$.

Teorema 2.4.8. *Seria* $\sum\limits_{n\geq 1} \frac{1}{p_n}$ *este divergentă.*

Demonstraţie. Fie $p_1, p_2, ..., p_{l(n)}$ toate numerele prime mai mici decât n şi să definim $\lambda(n) = \prod\limits_{i=1}^{l(n)} (1-\frac{1}{p_i})^{-1}$. Deoarece $(1-\frac{1}{p_i})^{-1} = \sum\limits_{a_i=0}^{\infty} \frac{1}{p_i^{a_i}}$, atunci $\lambda(n) = \sum (p_1^{a_1} ... p_i^{a_i})^{-1}$ (unde sumarea se face dupa toate l-upurile de numere naturale $(a_1, ..., a_l)$). In particular $1 + \frac{1}{2} + ... + \frac{1}{n} < \lambda(n)$ şi astfel $\lambda(n) \to \infty$ pentru $n \to \infty$. Avem:

$$\lg \lambda(n) = -\sum_{i=1}^{l} \lg(1 - \frac{1}{p_i}) = \sum_{i=1}^{l} \sum_{m=1}^{\infty} (mp_i^m)^{-1} = p_1^{-1} + ... + p_l^{-1} + \sum_{i=1}^{l} \sum_{m=2}^{\infty} (mp_i^m)^{-1}.$$

Insă $\sum\limits_{m=2}^{\infty} (mp_i^m)^{-1} < \sum\limits_{m=2}^{\infty} p_i^{-m} = p_i^{-2}(1 - p_i^{-1})^{-1} \leq 2p_i^{-2}$ astfel că $\lg \lambda(n) < p_1^{-1} + ... + p_l^{-1} + 2(p_1^{-2} + ... + p_l^{-2})$.

Este însă cunoscut faptul că $\sum\limits_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$. Atunci $\sum\limits_{i\geq 1} p_i^{-2}$ este convergentă, astfel că dacă presupunem că $\sum\limits_{n\geq 1} \frac{1}{p_n}$ este convergentă, atunci trebuie să existe o constantă M astfel încât $\lg \lambda(n) < M \Leftrightarrow \lambda(n) < e^M$, ceea ce este imposibil (deoarece am stabilit că $\lambda(n) \to \infty$ pentru $n \to \infty$), de unde deducem că $\sum\limits_{n\geq 1} \frac{1}{p_n}$ este divergentă. ■

2.5 Teorema lui Scherk

Rezultatul pe care îl prezentăm în continuare este datorat lui H. F. Scherk şi prezintă un fel de recurenţă ,,slabă" pentru şirul $(p_k)_{k\geq 1}$ al numerelor prime.

Mai precis, vom demonstra:

Teorema 2.5.1. *(H. F. Scherk) Pentru orice număr natural $n \geq 1$ există o alegere convenabilă a semnelor + sau - astfel încât*:

$$(1) \quad p_{2n} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-2} + p_{2n-1} \text{ şi}$$
$$(2) \quad p_{2n+1} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-1} + 2p_{2n}.$$

Observaţie.

Formulele (1) şi (2) au fost enunţate de Scherk în anul 1830 iar S. S. Pillai a fost primul care a prezentat o demonstraţie a lor în anul 1928.

In cele ce urmează vom prezenta o soluţie 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 $n \in \mathbf{N}^*$.

Ţinând cont de relaţiile 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 2.5.2. *Dacă $(q_n)_{n\geq 1}$ este un şir cu proprietatea (P), atunci pentru orice număr natural impar $m \leq q_{2n+1} (n \geq 3)$, există o alegere convenabila a semnelor ,,+" sau ,,-" astfel încât $m = \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} + q_{2n}$.*

Demonstraţie. Vom demonstra această lemă făcând inducţie matematică după $n \geq 3$. 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 egalităţile:

$$\begin{aligned}
1 &= -q_1 + q_2 + q_3 - q_4 - q_5 + q_6 \\
3 &= q_1 - q_2 - q_3 + q_4 - q_5 + q_6 \\
5 &= q_1 + q_2 + q_3 - q_4 - q_5 + q_6 \\
7 &= -q_1 - q_2 - q_3 - q_4 + q_5 + q_6 \\
9 &= q_1 + q_2 - q_3 + q_4 - q_5 + q_6
\end{aligned}$$

$$\begin{aligned}
11 &= q_1 - q_2 - q_3 - q_4 + q_5 + q_6 \\
13 &= q_1 - q_2 + q_3 + q_4 - q_5 + q_6 \\
15 &= -q_1 + q_2 + q_3 + q_4 - q_5 + q_6 \\
17 &= q_1 + q_2 - q_3 - q_4 + q_5 + q_6
\end{aligned}$$

deducem că lema este adevarată 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 adevarată pentru $n \geq 3$, şi fie $2k - 1$ un număr impar astfel încât $2k - 1 \leq q_{2n+3}$.

Cum şirul $(q_n)_{n\geq 1}$ 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 $0 \leq \pm(2k - 1 - q_{2n+2}) < q_{2n+2}$.

Cum din $q_{2n+2} < 2q_{2n+1}$ deducem că $-q_{2n+1} \leq \pm(2k - 1 - q_{2n+2}) - q_{2n+1} < q_{2n+1}$ şi astfel pentru o nouă alegere convenabilă a semnelor ,,+" sau ,,-" avem $0 \leq \pm[\pm(2k - 1 - q_{2n+2}) - q_{2n+1}] < q_{2n+1}$. Cum q_{2n+2} şi q_{2n+1} sunt numere impare, deducem că şi numărul $m = \pm[\pm(2k - 1 - q_{2n+2}) - q_{2n+1}]$ este impar şi cum $m \leq q_{2n+1}$, conform ipotezei de induţie găsim o alegere convenabilă a semnelor ,,+" sau ,,-" astfel încât $m = \pm[\pm(2k-1-q_{2n+2})-q_{2n+1}] = \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} \pm q_{2n}$, 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 2.5.2. este demonstrată. ■

Corolar 2.5.3. *Pentru o alegere convenabilă a semnelor ,,+" sau ,,-" avem egalitatea* $q_{2n-1} = \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} + q_{2n}$.

Demonstraţie. 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.

Intr-adevăr, pentru $n \geq 3$, 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 $q_{2n+1} - q_{2n} - 1 = \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} + q_{2n}$, de unde $q_{2n+1} = 1 \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} + 2q_{2n}$ şi astfel formula (2) rezultă imediat considerând pentru $n \geq 1, q_n = p_n$.

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 $n \in \mathbf{N}^*$.

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 ,,-" astfel încât $q_{2n+2} - q_{2n+1} - 1 = \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} + q_{2n}$, de unde $q_{2n+2} = 1 \pm q_1 \pm q_2 \pm ... \pm q_{2n-1} + q_{2n} + q_{2n+1}$ deci (luând în loc de $n+1$ pe n) $q_{2n} = 1 \pm q_1 \pm q_2 \pm ... \pm q_{2n-3} + q_{2n-2} + q_{2n-1}$ şi astfel şi (1) sunt verificate pentru $n \geq 3$.

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 $n \in \mathbf{N}^*$(luând din nou $q_n = p_n$). ■

2.6 Există funcţii care definesc numerele prime?

In continuare dorim să clarificăm existenţa unor funcţii (calculabile) $f : \mathbf{N}^* \to \mathbf{N}^*$ 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 $n \in \mathbf{N}^*$, $f(n)$ este număr prim iar f este functie 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?

In 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 astfel încât $p \leq x$.

La început vom prezenta o formulă pentru $\pi(m)$ dată de Willans în anul 1964.

Pentru aceasta, pentru fiecare număr natural $j \geq 1$ fie

$$F(j) = [cos^2 \pi \frac{(j-1)! + 1}{j}].$$

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

$$H(j) = \frac{\frac{sin^2((j-1)!)^2}{j}}{sin^2 \frac{\pi}{j}}.$$

Mináč a dat o altă expresie pentru $\pi(m)$ în care nu mai intervine sinusul sau cosinusul şi anume

$$\pi(m) = \sum_{j=2}^{m} [\frac{(j-1)! + 1}{j} - [\frac{(j-1)!}{j}]].$$

Iată o demonstraţie simplă pentru formula lui Mináč. Incepem cu observaţia că pentru $n \neq 4$, care nu este prim, n divide $(n-1)!$. Intr-adevăr, fie n este de forma $n = ab$ cu $2 \leq a, b \leq n-1$ şi $a \neq b$; fie $n = p^2 \neq 4$. In primul caz, n divide $(n-1)!$ în timp ce în al doilea caz $2 < p \leq n - 1 = p^2 - 1$, şi atunci $2p \leq p^2 - 1$ 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 $(j-1)!+1 = kj, (k \in \mathbf{N}^*)$, deci

$$[\frac{(j-1)! + 1}{j} - [\frac{(j-1)!}{j}]] = [k - [k - \frac{1}{j}]] = 1.$$

Dacă j nu este număr prim, atunci după remarca precedentă $(j-1)! = kj (k \in \mathbf{N}^*)$ şi astfel $[\frac{(j-1)! + 1}{j} - [\frac{(j-1)!}{j}]] = [k + \frac{1}{j} - k] = 0$.

In fine, dacă $j = 4$, atunci $[\frac{3! + 1}{4} - [\frac{3!}{4}]] = 0$ şi astfel formula lui Mináč este demonstrată.

Utilizând cele de mai sus se obţine formula lui Willans pentru p_n:

$$p_n = 1 + \sum_{m=1}^{n} [[\frac{n}{\sum_{j=1}^{m} F(j)}]^{\frac{1}{n}}] \text{ sau } p_n = 1 + \sum_{m=1}^{n} [[\frac{n}{1+\pi(m)}]^{\frac{1}{n}}].$$

O altă formulă pentru cel mai mic număr prim superior unui număr natural dat $m \geq 2$, a fost dată de Ernvall în 1975: Fie $d = ((m!)^{m!} - 1, (2m)!), t = \frac{d^d}{(d^d, d!)}$ 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 $p = \frac{d}{(\frac{t}{d^a}, d)}$.

Dacă vom lua $m = p_{n-1}$ obţinem din nou o formulă pentru p_n.

Reamintim cum se defineste functia 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 funcţii, în 1971 Ghandi a arătat că dacă notăm $P_{n-1} = p_1 p_2 ... p_{n-1}$, atunci $P_n = [1 - \frac{1}{\log 2} \cdot \log(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1})]$ sau, analog, P_n este singurul număr natural pentru care $1 < 2^{P_n}(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1}) < 2$.

Iată o demonstraţie a formulei lui Ghandi prezentată în 1972 de Vanden Eynden:

Să notăm $Q = P_{n-1} p_n = p$ şi $S = \sum_{d|Q} \frac{\mu(d)}{2^d - 1}$. Atunci

$$(2^Q - 1)S = \sum_{d|Q} \mu(d) \frac{2^Q - 1}{2^d - 1} = \sum_{d|Q} \mu(d)(1 + 2^d + 2^{2d} + ... + 2^{Q-d}).$$

Dacă $0 \leq t < Q$ termenul $r(d) \cdot 2^t$ apare exact atunci când $d|(t, Q)$. Deci coeficientul lui 2^t în sumă este $\sum_{d|(t,Q)} \mu(d)$; în particular, pentru $t = 0$, coeficientul este egal cu $\sum_{d|Q} \mu(d)$.

Reamintim că $\sum_{d|Q} \mu(d) = \begin{cases} 1, & \text{dacă } m = 1 \\ 0, & \text{dacă } m > 1 \end{cases}$.

Dacă scriem $\sum_{0<t<Q}'$ pentru suma extinsă la toate valorile lui t astfel încât $0 < t < Q$ 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 $2(2^Q - 1)(-\frac{1}{2} + S) = -2(2^Q - 1) + \sum_{0<t<Q}' 2^{t+1} = 1 + \sum_{0<t<Q}' 2^{t+1}$.

Dacă $2 \leq j < p_n = p$, există un număr prim q astfel încât $q < p_n < p$ (deci $q|Q$) şi $q|Q - j$. Fiecare indice t din suma considerată mai înainte satisface deci condiţia $0 < t \leq Q - p$.

Atunci $\frac{2^{Q-p+1}}{2 \cdot 2^Q} < -\frac{1}{2} + S = \frac{1 + \sum_{0<t\leq Q-p}' 2^{t+1}}{2(2^Q - 1)} < \frac{2^{Q-p+2}}{2 \cdot 2^Q}$. Inmulţind cu 2^p deducem că $1 < 2^p(-\frac{1}{2} + S) < 2$. ■

2. Funcţii satisfăcând condiţia b)

Numărul $f(n) = [\theta^{3^n}]$ este prim pentru orice $n \geq 1$, (aici $\theta \approx 1,3064...$ -vezi -**W. H. Mills : Prime- representing function, Bull. Amer. Math. Soc.,53 , p 604**).

De asemenea, $g(n) = [2^{2^{\cdots^{\omega}}}]$ (cu un şir de n exponenţi) este un număr prim pentru orice număr natural $n \geq 1$ (aici $\omega \approx 1,9287800...$-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 aproximaţie iar valorile lui $f(n)$ şi $g(n)$ cresc foarte repede, aşa că cele doua funcţii nu sunt prea utile ramânând 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 $\mathbf{Z}$ astfel încât valorile sale să fie numere prime este sortită eşecului deoarece dacă $f \in \mathbf{Z}[X]$ este neconstant, atunci există o infinitate de întregi n cu proprietatea că $|f(n)|$ nu este număr prim.

Intr-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 astfel încât $|f(n_0)| = p$ este număr prim. Cum f nu este constant deducem că $\lim\limits_{x\to\infty} |f(x)| = +\infty$, deci există $n_1 > n_0$ astfel încât 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 $f \in \mathbf{C}[X_1, ..., X_m](m \geq 2)$ 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) astfel încât $f(k)$ 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, $p \equiv 1 (\text{mod } 4)$) astfel încât $f(x)$ este prim pentru $x = 0, 1, ..., \frac{p-3}{2}$ sunt cele pentru $p = 5, 13, 37$.

2.7 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.

In 1949, **Clément [Clément, P. A. : Congruences for sets of primes, Amer. Math. Monthly, 56, 1949, 23-25]** a prezentat următorul rezultat legat de numerele prime gemene: Pentru $n \geq 2$, n şi $n+2$ sunt simultan prime dacă şi numai dacă $4[(n-1)!+1]+n \equiv 0(\text{mod } n(n+2))$ (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 prime gemene.

Dacă notăm pentru $x > 1$ prin $\pi_2(x)$=numărul numerelor prime p astfel încât $p+2$ este prim şi $p+2 \leq x$, atunci Brun a demonstrat în 1920 că există un număr natural x_0 (efectiv calculabil) astfel încât pentru orice $x \geq x_0$ să avem $\pi_2(x) < \frac{100x}{(\lg x)^2}$.

Intr-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, Bull. Sc. Math., vol.43, pp. 100-104** şi **124-128**) tot Brun a demonstrat că seria $B = \sum(\frac{1}{p}+\frac{1}{p+2})$ (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 $B \approx 1,90216054....$

Printre cele mai mari numere prime gemene cunoscute amintim $1706595 \cdot 2^{11235} \pm 1$ şi $571305 \cdot 2^{7701} \pm 1$ ([38]) ca şi $665551035 \cdot 2^{80025} \pm 1$ (David Underbakke).

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 3

Funcţii aritmetice

3.1 Generalităţi. Operaţii cu funcţii aritmetice

Definiţia 3.1.1. Numim *funcţie aritmetică* orice funcţie $f : \mathbf{N}^* \to \mathbf{C}$.

In cadrul acestui capitol vom prezenta mai multe exemple de astfel de funcţii.

Fie $\mathbf{A} = \{f : \mathbf{N}^* \longrightarrow \mathbf{C}\}$ mulţimea funcţiilor aritmetice.

Pentru $f, g \in \mathbf{A}$ definim $f + g, fg, f * g : \mathbf{N}^* \to \mathbf{C}$ astfel:

$$\begin{aligned} (f+g)(n) &= f(n) + g(n), \\ (fg)(n) &= f(n) \cdot g(n) \text{ şi} \\ (f*g)(n) &= \sum_{d|n} f(d)g(\frac{n}{d}) \text{ pentru orice } n \in \mathbf{N}^*. \end{aligned}$$

Observaţie. $f * g$ poartă numele de *produsul Dirichlet de convoluţie* al lui f şi g.

Propoziţia 3.1.2. $(\mathbf{A}, +, *)$ *este inel comutativ unitar.*

Demonstraţie. Faptul că $(\mathbf{A}, +)$ este grup abelian este imediat. Să probăm că $(\mathbf{A}, *)$ este monoid comutativ. Intr-adevăr, dacă $f, g, h \in \mathbf{A}$, atunci:

$(f * (g * h))(n) = \sum_{d|n} f(d) \sum_{e|\frac{n}{d}} g(e)h(\frac{n}{de}) = \sum_{D|n} (\sum_{e|D} f(\frac{D}{e})g(e)h(\frac{n}{D}) = ((f * g) * h)(n)$

$(D = de)$, pentru orice $n \in \mathbf{N}^*$, adică „$*$" este asociativă (am ţinut cont de faptul că atunci când d parcurge divizorii lui n, acelaşi lucru îl face şi $\frac{n}{d}$). Cu acelaşi argument rezultă şi comutativitatea produsului de convoluţie.

Elementul neutru pentru $*$ este $\delta : \mathbf{N}^* \longrightarrow \mathbf{C}, \delta(n) = \begin{cases} 1, \text{ dacă } n = 1 \\ 0, \text{ dacă } n \neq 1. \end{cases}$, deoarece se verifică imediat că $f * \delta = \delta * f = f$, pentru orice $f \in \mathbf{A}$.

Pentru a încheia, să mai probăm că dacă $f, g, h \in \mathbf{A}$, atunci $f * (g + h) = (f * g) + (f * h)$. Intr-adevăr, dacă $n \in \mathbf{N}^*$, atunci: $f * (g + h))(n) = \sum_{d|n} f(d)g(\frac{n}{d}) + h(\frac{n}{d}) = \sum_{d|n} f(d)g(\frac{n}{d}) + \sum_{d|n} f(d)h(\frac{n}{d}) = (f * g)(n) + (f * h)(n) = (f * g + f * h)(n)$. ■

Propoziţia 3.1.3. $f \in U(\mathbf{A}) \Leftrightarrow f(1) \neq 0$.

Demonstraţie. Dacă $f \in U(\mathbf{A})$, atunci există $g = f^{-1} \in \mathbf{A}$ astfel încât $f * f^{-1} = f^{-1} * f = \delta$. Deci $1 = \delta(1) = f(1)f^{-1}(1)$, adică $f(1) \neq 0$.

Reciproc, dacă $f(1) \neq 0$, definim inductiv

$$g(n) = \begin{cases} \frac{1}{f(1)}, \text{ dacă } n = 1 \\ -\frac{1}{f(1)} \sum\limits_{d|n, d>1} f(d)g(\frac{n}{d}), \text{ dacă } n > 1. \end{cases}$$

Se verifică imediat că $g = f^{-1}$. ■

Iată câteva exemple de funcţii aritmetice:

1. *Funcţia φ a lui Euler* definită în paragraful §4 de la Capitolul 1.

2. Pentru $k \in \mathbf{N}$ definim $\sigma_k : \mathbf{N}^* \to \mathbf{C}$ astfel $\sigma_k(n) = \sum\limits_{d|n} d^k$ iar $\xi_k(n) = n^k$.

In 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 $n \in \mathbf{N}^*$).

Dacă $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ este descompunerea canonică a lui n în produs de numere prime, atunci $\sigma(n)$ va fi suma produselor de forma $p_1^{\beta_1}...p_k^{\beta_k}$ cu $\beta_i \leq \alpha_i, 1 \leq i \leq k$, adică

$$\begin{aligned} \sigma(n) &= (1 + p_1 + ... + p_1^{\alpha_1})(1 + p_2 + ... + p_2^{\alpha_2})...(1 + p_k + ... + p_k^{\alpha_k}) \\ &= \frac{p_1^{\alpha_1+1}}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1}}{p_2 - 1} \cdot ... \cdot \frac{p_k^{\alpha_k+1}}{p_k - 1}. \end{aligned}$$

3. Funcţia $\tau : \mathbf{N}^* \to \mathbf{N}^*, \tau(n)$ =numărul divizorilor naturali ai lui n ($n \in \mathbf{N}^*$). Se verifică imediat că dacă $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ atunci $\tau(n) = (1 + \alpha_1)...(1 + \alpha_k)$.

Observaţie. Conform Propoziţiei 3.1.3 funcţia zeta ξ are inversă în inelul $\mathbf{A}$; ξ^{-1} se notează cu μ şi poartă numele de *funcţia lui Möbius*. Deoarece $\mu * \xi = \delta$, deducem că $\sum\limits_{d|n} \mu(d) = \begin{cases} 1, \text{ dacă } n = 1 \\ 0, \text{ dacă } n \neq 1. \end{cases}$

In particular, dacă p este un numar prim iar $\alpha \geq 2$ atunci $\sum\limits_{j=0}^{\alpha} \mu(p^j) = 0$. 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 3.1.4. *Dacă f şi g sunt funcţii aritmetice atunci $f(n) = \sum\limits_{d|n} g(d)$ pentru orice $n \in \boldsymbol{N}^* \Leftrightarrow g(n) = \sum\limits_{d|n} f(d)\mu(\frac{n}{d})$ pentru orice $n \in \boldsymbol{N}^*$.*

Ca un exemplu avem că: $\sigma_k(n) = \sum\limits_{d|n} d^k$ pentru orice $n \in \mathbf{N}^*$ astfel că $n^k = \sum\limits_{d|n} \sigma_k(d)\mu(\frac{n}{d})$ pentru orice $n \in \mathbf{N}^*$.

Lema 3.1.5. *Pentru $n \in \boldsymbol{N}^*$ şi $d|n$, fie $S_d = \{\frac{xn}{d} : 1 \leq x \leq d, x \in \boldsymbol{N}^*, (x, d) = 1\}$. Atunci pentru $d|n, e|n, d \neq e, S_d \cap S_e = \emptyset$ iar $\bigcup\limits_{d|n} S_d = \{1, 2, ..., n\}$.*

Demonstraţie. Presupunând că $S_d \cap S_e = \emptyset$, există $x, y \in \mathbf{N}^*$ astfel încât $1 \leq x \leq d, 1 \leq y \leq e, (x,d) = (y,e) = 1$ şi $\frac{xn}{d} = \frac{yn}{e} \Leftrightarrow xe = yd$.

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 $(m,n) = \frac{n}{d}$, dacă $m = \frac{xn}{d}$, atunci $(x,d) = 1$ şi $1 \leq x \leq \frac{dm}{n} \leq d$, deducem că $m \in S_d$ adică $\{1,2,...,n\} \subseteq \bigcup_{d|n} S_d$ şi cum incluziunea inversă este imediată deducem egalitatea cerută. ■

Corolar 3.1.6. *Cum S_d are $\varphi(d)$ elemente, deducem că $n = \sum_{d|n} \varphi(d)$, pentru orice $n \in \boldsymbol{N}^*$.*

Conform Propozitiei 3.1.4 deducem că $\varphi(n) = \sum_{d|n} d\mu(\frac{n}{d})$ pentru orice $n \in \mathbf{N}^*$. In particular, dacă p este prim şi $\alpha \geq 1$ natural,

$$\varphi(p^\alpha) = \sum_{j=0}^{\alpha} p^j \mu(p^{\alpha-j}) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p}).$$

3.2 Funcţii multiplicative

Definiţia 3.2.1. O funcţie aritmetică f se zice *funcţie multiplicativă* dacă $f \neq 0$ şi $f(mn) = f(m)f(n)$, pentru orice $m, n \in \mathbf{N}^*$ cu $(m,n) = 1$.

Observaţie. Dacă f este multiplicătivă atunci din $f \neq 0$ există un $n \in \mathbf{N}^*$ astfel încât $f(n) \neq 0$ şi cum $f(n) = f(1 \cdot n) = f(1) \cdot f(n)$ deducem că $f(1) = 1$, adică în inelul $\mathbf{A}$, f este inversabilă. Dacă $n \in \mathbf{N}$ iar $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ este descompunerea în factori primi a lui n, atunci $f(n) = f(p_1^{\alpha_1})...f(p_k^{\alpha_k}) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$, astfel că o funcţie multiplicativă este complet determinată de valorile ei pe mulţimile de forma p^α cu p prim şi $\alpha \in \mathbf{N}$. Să notăm cu $\mathbf{M}$ familia funcţiilor aritmetice multiplicative.

Propoziţia 3.2.2. *Dacă $f \in \boldsymbol{M}$, atunci şi $f^{-1} \in \boldsymbol{M}$.*

Demonstraţie. Fie $m, n \in \mathbf{N}$ cu $(m,n) = 1$. Dacă $m = n = 1$ atunci $f^{-1}(mn) = f^{-1}(m)f^{-1}(n)$.

Presupunem acum că $mn \neq 1$ şi că $f^{-1}(m_1n_1) = f^{-1}(m_1)f^{-1}(n_1)$ 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 $m \neq 1$ şi $n \neq 1$.

Conform Propoziţiei 3.1.3 avem $f^{-1}(mn) = -\sum_{\substack{d \mid mn, \\ d > 1}} f(d)f^{-1}(\frac{mn}{d})$.

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 $(\frac{m}{d_1}, \frac{n}{d_2}) = 1$.

Astfel că:

$$f^{-1}(mn) = -\sum_{\substack{d_1 \mid m, d_2 \mid n,\\ d_1 d_2 > 1}} f(d_1 d_2) f^{-1}(\frac{mn}{d_1 d_2}) = (\text{ deoarece } \frac{m}{d_1} \cdot \frac{n}{d_2} < mn) =$$

$$-\sum_{\substack{d_1 \mid m, d_2 \mid n,\\ d_1 d_2 > 1}} f(d_1) f(d_2) \cdot f^{-1}(\frac{m}{d_1}) f^{-1}(\frac{n}{d_2}) = -f^{-1}(m) \sum_{\substack{d_2 \mid n,\\ d_2 > 1}} f(d_2) f^{-1}(\frac{n}{d_2})$$

$$-f^{-1}(n) \sum_{\substack{d_1 \mid m,\\ d_1 > 1}} f(d_1) f^{-1}(\frac{m}{d_1}) - (\sum_{\substack{d_1 \mid m,\\ d_1 > 1}} f(d_1) f^{-1}(\frac{m}{d_1})) \cdot (-\sum_{\substack{d_2 \mid n,\\ d_2 > 1}} f(d_2) f^{-1}(\frac{n}{d_2})$$

$$= f^{-1}(m) f^{-1}(n) + f^{-1}(m) f^{-1}(n) - f^{-1}(m) f^{-1}(n) = f^{-1}(m) f^{-1}(n) \text{ şi totul}$$

este clar. ■

Observaţie. Cum funcţia zeta ξ este multiplicativă, inversa sa, care este funcţia lui *Möbius*, μ este multiplicativă. Astfel:

$$\mu(n) = \begin{cases} 1, \text{ dacă } n = 1, \\ (-1)^t, \text{dacă } n \text{ este produs de } t \text{ primi distincţi}, \\ 0, \text{ în rest .} \end{cases}$$

Avem în felul acesta o altă definire a funcţiei lui *Möbius*.

Propoziţia 3.2.3. *Dacă $f, g \in \boldsymbol{M}$, atunci $f * g \in \boldsymbol{M}$.*

Demonstraţie. $(f * g)(1) = f(1)g(1) = 1$ iar dacă $(m, n) = 1$, atunci:

$$(f * g)(mn) = \sum_{d \mid mn} f(d) g(\frac{mn}{d}) = \sum_{\substack{d_1 \mid m,\\ d_2 \mid n}} f(d_1) f(d_2) g(\frac{m}{d_1}) g(\frac{n}{d_2})$$

$$= (\sum_{d_1 \mid m} f(d_1) g(\frac{m}{d_2})) \cdot (\sum_{d_2 \mid n} f(d_2) g(\frac{n}{d_2})) = [(f * g)(m)][(f * g)(n)]. \blacksquare$$

Observaţii.

1. Deoarece ξ_k este multiplicativă şi $\sigma_k = \xi_k * \xi$ deducem că şi σ_k este multiplicativă. Astfel, dacă $k \geq 1, p$ 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 $\sigma_k(n) = \prod_{i=1}^{t} \frac{p_i^{(\alpha_i+1)k} - 1}{p_i^k - 1}$.

In particular, $\sigma(n) = \prod_{i=1}^{t} \frac{p_i^{\alpha_i+1} - 1}{p_i^k - 1}$.

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

$n \in \mathbf{N}^*$: $\varphi(n) = n \prod_{\substack{p \mid n, \\ p \text{ prim}}} (1 - \frac{1}{p})$.

3. Funcţia φ a lui Euler este o funcţie calculabilă (adică pentru orice $n, \varphi(n)$ este cardinalul unei mulţimi şi anume a mulţimii $\{x : 1 \leq x \leq n \text{ şi } (x, n) = 1\}$).

Funcţiile calculabile pot fi câte o dată evaluate ţinând cont de principiul includerii şi excluderii.

3.3 Funcţia Jordan J_k

Funcţia Jordan J_k reprezintă o generalizare a funcţiei φ a lui Euler şi se defineşte astfel:

Definiţia 3.3.1. Pentru $n \in \mathbf{N}^*, J_k(n)$=*numarul k-uplurilor ordonate de numere naturale* $(x_1, ..., x_k)$ astfel încât $1 \leq x_i \leq n, 1 \leq i \leq k$ şi $(x_1, x_2, ..., x_k, n) = 1$.

Observaţie. Evident $J_1 = \varphi$. Fie $n = p_1^{\alpha_1}...p_t^{\alpha_t}$ descompunerea în factori primi a lui n, S=mulţimea k-uplurilor $(x_1, ..., x_k)$ astfel încât $1 \leq x_i \leq n, 1 \leq i \leq k$, iar A_i =multimea acelor k-upluri din S pentru care $p_i|(x_1, ..., x_k), 1 \leq i \leq t$, atunci: $J_k(n) = |S - (A_1 \cup ... \cup A_t)|$ iar $|A_{i_1} \cap ... \cap A_{i_j}| = \frac{n}{p_{i_1}...p_{i_j}}$.

Astfel:

$J_k(n) = n^k + \sum_{j=1}^{t} (-1)^j \sum_{1 \leq i_1 < ... < i_j \leq t} (\frac{n}{p_{i_1}...p_{i_j}})^k = \sum_{d|n} (\frac{n}{d})^k \mu(d) = \sum_{d|n} d^k \mu(\frac{n}{d})$.

Deducem astfel că $J_k = \xi_k * \mu$ şi astfel rezultă că J_k este funcţie multiplicativă.

Dacă p este prim şi $\alpha \geq 1$, atunci $J_k(p^\alpha) = p^{\alpha k} - p^{(\alpha-1)k} = p^{\alpha k}(1 - \frac{1}{p^k})$, astfel că $J_k(n) = n^k \prod_{p|n} (1 - \frac{1}{p^k})$.

3.4 Funcţia von Sterneck H_k

Iată acum o altă generalizare a funcţiei lui Euler (numită funcţia *von Sterneck*).

Definiţia 3.4.1. Pentru $n, k \in N^*$ definim $H_k(n) = \sum_{[e_1,...,e_k]=n} \varphi(e_1)...\varphi(e_k)$, suma făcându-se după toate k-uplurile $(e_1, ..., e_k)$ de numere naturale astfel încât $1 \leq e_i \leq n, 1 \leq i \leq k$ şi $[e_1, ..., e_k] = n$.

Observaţie. In mod evident $\varphi = H_1$ iar $H_k(1) = 1$.

Presupunem acum că $(m, n) = 1$ şi că $[e_1, ..., e_k] = mn$. Pentru $i = 1, ..., k, e_i$ poate fi descompus în mod unic sub forma $e_i = c_i d_i$, unde $c_i \mid m$ şi $d_i \mid n$, iar $[c_1, ..., c_k] = m$ şi $[d_1, ..., d_k] = n$. Astfel:

$$H_k(mn) = \sum_{[e_1,...,e_k]=mn} \varphi(e_1)...\varphi(e_k) = \sum_{\substack{[c_1,...,c_k]=m, \\ [d_1,...,d_k]=n}} (\varphi(c_1)...\varphi(c_k))(\varphi(d_1)...\varphi(d_k))$$

$$= \sum_{[c_1,...,c_k]=m} \varphi(c_1)...\varphi(c_k) \sum_{[d_1,...,d_k]=n} \varphi(d_1)...\varphi(d_k) = H_k(m)H_k(n),$$

adică H_k este funcţie multiplicativă.

Propoziţia 3.4.2. Pentru orice $k \geq 1$, $H_k = J_k$.

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

$$H_k(p^\alpha) = \sum_{max(\beta_1,\ldots,\beta_i)=\alpha} \varphi(p^{\beta_1})\ldots\varphi(p^{\beta_i}) = \sum_{max(\beta_1,\ldots,\beta_i)=\alpha} \varphi(p^{\beta_1})\ldots\varphi(p^{\beta_{i-1}})\varphi(p^{\beta_i}) +$$

$$\sum_{max(\beta_1,\ldots,\beta_i)\leq\alpha} \varphi(p^{\beta_1})\ldots\varphi(p^{\beta_{i-1}})\varphi(p^\alpha) = H_{k-1}(p^\alpha)\sum_{d|p^\alpha}\varphi(d) + (\sum_{d|p^\alpha}\varphi(d))^{k-1}\varphi(p^\alpha) =$$

$$p^{\alpha-1}H_{k-1}(p^\alpha) + p^{\alpha(k-1)}\varphi(p^\alpha) = p^{\alpha-1}J_{k-1}(p^\alpha) + p^{\alpha(k-1)}\varphi(p^\alpha) = p^{\alpha-1}p^{\alpha(k-1)}(1 -$$

$$\frac{1}{p^{k-1}}) + p^{\alpha(k-1)}p^\alpha(1-\frac{1}{p}) = p^{\alpha k}[\frac{1}{p}(1-\frac{1}{p^{k-1}}) + (1-\frac{1}{p})] = p^{\alpha k}(1-\frac{1}{p^k}) = J_k(p^\alpha).\blacksquare$$

3.5 Funcţii complet multiplicative

Definiţia 3.5.1. O funcţie $f \in \mathbf{A}$ se zice *complet multiplicativă* dacă există $n \in \mathbf{N}^*$ astfel încât $f(n) \neq 0$ iar $f(mn) = f(m)f(n)$, pentru orice $m, n \in \mathbf{N}$(dacă notăm prin $\mathbf{M}^c$ clasa acestor funcţii, atunci în mod evident $\mathbf{M}^c \subseteq \mathbf{M} \subseteq \mathbf{A}$).

Avem, de exemplu, $\mu(2) = -1, \mu(6) = 1, \mu(2\cdot 6) = \mu(2^2\cdot 3) = 0$, deci $\mu(2\cdot 6) \neq \mu(2)\cdot\mu(6)$, adică μ nu este complet multiplicativă.

Propoziţia 3.5.2. *Dacă $f \in \boldsymbol{M}$, atunci $f \in \boldsymbol{M}^c \Leftrightarrow f^{-1} = \mu f$.*

Demonstraţie. Dacă $f \in \mathbf{M}^c$, atunci pentru orice $n \in \mathbf{N}$:

$$(\mu * f)(n) = \sum_{d|n}\mu(d)f(d)f(\frac{n}{d}) = f(n)\sum_{d|n}\mu(d) = \begin{cases} f(1), \text{ dacă } n = 1 \\ 0, \text{ dacă } n \neq 1, \end{cases}$$

adică $\mu * f = \delta \Leftrightarrow f^{-1} = \mu f$.

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 $a \geq 1$, 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 $0 = (f^{-1} * f)(p^\alpha) = f(p^\alpha) + f^{-1}(p)f(p^{\alpha-1}) = f(p^\alpha) + f^{-1}(p)(f(p))^{\alpha-1}$. Deoarece $f^{-1}(p) = -f(p) \Rightarrow f(p^\alpha) = (f(p))^\alpha$. ■

Corolar 3.5.3. *Dacă $f \in \boldsymbol{M}$, atunci $f \in \boldsymbol{M}^c \Leftrightarrow f^{-1}(p^\alpha) = 0$, pentru orice p prim şi $\alpha \geq 2$.*

Propoziţia 3.5.4. *Fie $f \in \boldsymbol{M}$. Atunci $f \in \boldsymbol{M}^c \Leftrightarrow f(g*h) = (fg)*(fh)$, pentru orice $g, h \in \boldsymbol{A}$.*

Demonstraţie. Dacă $f \in \mathbf{M}^c$, atunci pentru orice $g, h \in \mathbf{A}$ avem$(f(g*h))(n) = f(n)\sum_{d|n} g(d)h(\frac{n}{d}) = \sum_{d|n} f(d)g(d)f(\frac{n}{d})h(\frac{n}{d}) = (fg * fh)(n)$.

Invers, să presupunem că $f(g*h) = (fg)*(fh)$, pentru orice $g, h \in \mathbf{A}$. In 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 3.5.2). ■

Propoziţia 3.5.5. *Dacă $f \in \boldsymbol{M}$, atunci există $g, h \in \boldsymbol{M}^c$ astfel încât $f = g * h \Leftrightarrow f^{-1}(p^\alpha) = 0$, 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 $f^{-1}(p^\alpha) = (g^{-1} * h^{-1})(p^\alpha) = \prod_{j=0}^{\alpha} g^{-1}(p^j)h^{-1}(p^{\alpha-j}) = g^{-1}(1)h^{-1}(p^\alpha) + g^{-1}(p)h^{-1}(p^{\alpha-1}) = 0$ (căci $g, h \in \mathbf{M}^c$ şi $\alpha \geq 3$).

Invers, fie $f \in \mathbf{M}$ astfel încât $f^{-1}(p^\alpha) = 0$ pentru orice p prim şi $\alpha \geq 3$. Alegem $g \in \mathbf{M}^c$ astfel încât 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 3.5.4, $h \in \mathbf{M}^c$ şi astfel $f = g * h$. ■

Teorema 3.5.6. *Pentru $f \in \boldsymbol{M}$, următoarele condiţii sunt echivalente*:

(1) *Există $g, h \in \mathbf{M}^c$ astfel încât $f = g * h$;*

(2) *Există $F \in \mathbf{M}$ astfel încât pentru orice m, n: $f(mn) = \sum_{d|(m,n)} f(\frac{m}{d})f(\frac{n}{d})F(d)$;*

(3) *Există $B \in \mathbf{M}^c$ astfel încât pentru orice m, n: $f(m)f(n) = \sum_{d|(m,n)} f(\frac{mn}{d^2})B(d)$;*

(4) *Pentru orice p prim şi $\alpha \geq 1$: $f(p^{\alpha+1}) = f(p)f(p^\alpha) + f(p^{\alpha-1})[f(p^2) - (f(p))^2]$.*

Demonstraţie. Vom demonstra că (1) $\Rightarrow$ (4), (4) $\Rightarrow$ (1), (2) $\Rightarrow$ (4), (4) $\Rightarrow$ (2), adică (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4), iar apoi (2) $\Rightarrow$ (3) şi (3) $\Rightarrow$ (4).

(1) $\Rightarrow$ (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:

$$(M+N)\sum_{i=0}^{\alpha} M^i N^{\alpha-1} - MN\sum_{i=0}^{\alpha-1} M^i N^{\alpha+1-i} = \sum_{i=0}^{\alpha} M^{i+1}N^{\alpha-i} + \sum_{i=0}^{\alpha} M^i N^{\alpha+1-i} -$$
$$\sum_{i=0}^{\alpha-1} M^{i+1}N^{\alpha-1} = M^{\alpha+1} + \sum_{i=0}^{\alpha} M^i N^{\alpha+1-i} = \sum_{i=0}^{\alpha+1} M^i N^{\alpha+1-i} = f(p^{\alpha+1}).$$

(4) $\Rightarrow$ (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 $g, h \in \mathbf{M}^c$ astfel încât 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 $f \in \mathbf{M}$ deducem că $f = g * h$.

(2) $\Rightarrow$ (4). Fie p un număr prim şi $\alpha \geq 1$. Punem în ecuaţia din (2) $m = p^\alpha$ şi $n = p$. Atunci $f(p^{\alpha+1}) = f(p)f(p^\alpha) + f(p^{\alpha-1})F(p)$. Dacă particularizăm $\alpha = 1$ obţinem

$F(p) = f(p^2) - f(p))^2$.

(4) $\Rightarrow$ (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 $f \in \mathbf{M}$ astfel încât pentru orice p prim şi $\alpha, \beta \geq 1$, $f(p^{\alpha+\beta}) = \sum_{i=0}^{min(\alpha,\beta)} f(p^{\alpha-i}) f(p^{\beta-i}) F(p^i)$(de fapt este cazul în care $F = \mu B'$ cu $B' \in \mathbf{M}^c$ astfel încât $B'(p) = f(p^2) - (f(p))^2$ pentru orice p prim).

Fără a reduce din generalitate, să presupunem că $\beta \leq \alpha$ şi să facem inducţie după β.

Dacă $\beta = 1$ totul este clar. Presupunem că $\beta > 1$ şi că (2) este adevărată pentru $\beta - 1$ şi orice $\alpha \geq \beta - 1$.

Cum $F = \mu B', F(p^2) = F(p^3) = ... = 0$ iar $f(p^{\alpha+\beta}) = f(p^{\alpha+1+\beta-1}) = f(p^{\alpha+1})$ $f(p^{\beta-2})F(p) = [f(p)f(p^\alpha) - f(p^{\alpha-1})B'(p)]f(p^{\beta-1}) - f(p^\alpha)f(p^{\beta-2})B'(p) = f(p^\alpha)[f(p)$ $f(p^{\beta-1}) - f(p^{\beta-2})B'(p)] - f(p^{\alpha-1})f(p^{\beta-1})B'(p) = f(p^\alpha)f(p^\beta) + f(p^{\alpha-1})f(p^{\beta-1})F(p)$.

(2) $\Rightarrow$ (3). Pentru orice m, n avem:

$$\sum_{d|(m,n)} f(\frac{mn}{d^2})B'(d) = \sum_{d|(m,n)} \sum_{D|(\frac{m}{d},\frac{n}{d})} f(\frac{m/d}{D}) f(\frac{n/d}{D}) \mu(D) B'(D) B'(d) =$$

$$\sum_{d|(m,n)} \sum_{\substack{e \mid (m,n), \\ d \mid e}} f(\frac{m}{e}) f(\frac{n}{e}) \mu(\frac{e}{d}) B'(e) = \sum_{e|(m,n)} f(\frac{m}{e}) f(\frac{n}{e}) B'(e) \sum_{d|e} \mu(\frac{e}{d})$$

$$= f(m)f(n).$$

Astfel, funcţia $B' \in \mathbf{M}^c$ serveşte pe post de B cerut în (3).

(3) $\Rightarrow$ (4). Dacă p este prim şi alegem $m = n = p$, atunci obţinem $B(p) = (f(p))^2 - f(p^2)$, adică $B = B'$. Fie $\alpha \geq 1$. Dacă alegem $m = p^\alpha$ şi $n = p$ obţinem (4). ■

Observaţie. Funcţia $f \in \mathbf{A}$ 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 $B = \xi_k$; 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: $\sigma_k(mn) = \sum_{d|(m,n)} \sigma_k(\frac{m}{d})\sigma_k(\frac{n}{d})\mu(d)d^k$ [S.Ramanujan pentru $k = 0$, în 1916] şi $\sigma_k(m)\sigma_k(n) = \sum_{d|(m,n)} d^k \sigma_k(\frac{mn}{d^2})$[Busche-1906].

Capitolul 4

Resturi pătratice

4.1 Generalităţi. Simbolul lui Legendre

Fie $m \in \mathbf{N}, m > 1$ un număr natural fixat.

Definiţia 4.1.1. Un număr $a \in \mathbf{Z}$ cu $(m, a) = 1$ se zice *rest pătratic modulo m* dacă ecuaţia $x^2 \equiv a(\text{mod } m)$ are soluţie. In caz contrar a se zice *non-rest pătratic modulo m.*

In mod evident, dacă $a, b \in \mathbf{Z}$ şi $a \equiv b(\text{mod } m)$, atunci a este rest pătratic modulo $m \Leftrightarrow b$ este rest pătratic modulo m.

Datorită acestei observaţii este mai comod să lucrăm în $\mathbf{Z}_p$ decât în $\mathbf{Z}$, distincţia facându-se în contextul în care se lucrează (notăm deseori elementele lui $\mathbf{Z}_p$ prin $0, 1, ..., p-1$).

Observaţii.

1. Fie p un număr prim; dacă $p = 2$ şi $a \in \mathbf{Z}$ este impar, $a = 2k+1$ cu $k \in \mathbf{Z}$, atunci ecuaţia $x^2 \equiv a(\text{mod } 2)$ are soluţie pentru $x = 1$ sau $x = a$. Deci orice număr impar este rest pătratic modulo 2.

2. Dacă p este impar (deci $p \geq 3$), atunci $a \in \mathbf{Z}$ este rest pătratic modulo $p \Leftrightarrow$ restul împăţirii lui a la p este din $\mathbf{Z}^{*2}$ (sau $\mathbf{Z}_p^{*2}$). Aici $\mathbf{Z}^{*2} = \{x^2 | x \in \mathbf{Z}^*\}$ şi analog $\mathbf{Z}_p^{*2}$.

Intr-adevăr, dacă $a \in \mathbf{Z}$ este rest pătratic modulo p, atunci există $x \in \mathbf{Z}$ astfel încât $x^2 \equiv a(\text{mod } p) \Leftrightarrow$ există $c \in \mathbf{Z}$ astfel încât $a - x^2 = cp \Leftrightarrow a = cp + x^2$.

Reciproc, dacă putem scrie $a = cp + r^2$, cu $0 \leq r^2 < p$, atunci ecuaţia $x^2 \equiv a(\text{mod } p)$ are soluţie pe $x = r$.

In cele ce urmează prin p vom desemna un număr prim impar ($p \geq 3$).

Cum $\frac{p-1}{2} \in \mathbf{N}$, funcţia $\sigma : \mathbf{Z}_p^* \to \mathbf{Z}_p^*$, este morfism de grupuri multiplicative. Cum $\sigma(x)^2 = x^{p-1} = 1$ deducem că $\sigma(x) = \pm 1$ (în $\mathbf{Z}_p^*$) (deci $\sigma : \mathbf{Z}_p^* \to \{\pm 1\}$).

Mai mult

1. $\sigma(x) = -1$ pentru un anumit $x \in \mathbf{Z}_p^*$ (căci în caz contrar polinomul $X^{\frac{p-1}{2}} - 1$ ar avea mai multe rădăcini decât gradul său).

2. Dacă $x = t^2 \in \mathbf{Z}_p^{*2}$, atunci $\sigma(x) = x^{\frac{p-1}{2}} = (t^2)^{\frac{p-1}{2}} = t^{p-1} = 1$ (reamintim că am notat $\mathbf{Z}_p^{*2} = \{a^2 | a \in \mathbf{Z}_p^*\}$).

Din cele de mai sus deducem că: $\mathbf{Z}_p^{*2} \subseteq ker\sigma \subseteq \mathbf{Z}_p^*$ şi cum $[\mathbf{Z}_p^* : \ker \sigma] = |\mathbf{Z}_p^*/\ker \sigma| = |Im\sigma| = 2$ deducem că $2 = [\mathbf{Z}_p^* : \mathbf{Z}_p^{*2}] = [\mathbf{Z}_p^* : \ker \sigma][\ker \sigma : \mathbf{Z}_p^{*2}]$, de unde $[\ker \sigma : \mathbf{Z}_p^{*2}] = 1$, adică $\ker \sigma = \mathbf{Z}_p^{*2}$.

Definiţia 4.1.2. Numim *simbolul lui Legendre* morfismul de grupuri multiplicative $\sigma = (\frac{\cdot}{p}) : \mathbf{Z}_p^* \to \{\pm 1\}$.

Deci $(\frac{a}{p}) = \sigma(a) = a^{\frac{p-1}{2}}$, pentru orice $a \in \mathbf{Z}_p^*$ (evident $p \nmid a$, căci $a \in \mathbf{Z}_p^*$).

Mai mult

(1) $(\frac{a}{p}) = \begin{cases} 1, & \text{dacă } a \text{ este rest pătratic modulo } p \\ -1, & \text{dacă } a \text{ nu este rest pătratic modulo } p \end{cases}$

In particular

(2) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ şi $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ pentru orice $a, b \in \mathbf{Z}_p^*$.

Lema 4.1.3. *(Gauss) Fie $\mathbf{Z}_p^* = X \cup Y$, unde $X = \{\widehat{1}, \widehat{2}, ..., \widehat{\frac{p-1}{2}}\}$ iar $Y = \{\widehat{\frac{p+1}{2}}, ..., \widehat{p-1}\}$ (evident $X \cap Y = \emptyset$). Pentru $\widehat{a} \in \mathbf{Z}_p^*$, fie $\widehat{a}X = \{\widehat{a} \cdot \widehat{x} | x \in X\}$. Atunci $(\frac{a}{p}) = (-1)^g$, unde $g = |\widehat{a}X \cap Y|$.*

Demonstraţie. Să observăm la început că funcţia $m_a : \mathbf{Z}_p^* \to \mathbf{Z}_p^*, m_a(\widehat{x}) = a\widehat{x}$, pentru $x \in \mathbf{Z}_p^*$, permută doar elementele lui $\mathbf{Z}_p^*$.

Astfel, dacă notăm $X' = \widehat{a}X \cap X = \{\widehat{x_1}, ..., \widehat{x_k}\}, Y' = \widehat{a}X \cap Y = \{\widehat{y_1}, ..., \widehat{y_g}\}$, atunci $X' \cup Y' = \widehat{a}X$ iar $X' \cap Y' = \emptyset$, deci $g + k = \frac{p-1}{2}$.

Fie $Z = \{\widehat{x_1}, ..., \widehat{x_k}, \widehat{p - y_1}, ..., \widehat{p - y_g}\} \subseteq X$. Să observăm că elementele lui Z sunt distincte două câte două (ca elemente ale lui $\mathbf{Z}_p$).

Intr-adevăr, dacă există i, j astfel încât $x_i = p - y_j \Rightarrow x_i + y_j = 0$ (în $\mathbf{Z}_p$). Insă $x_i = ar, y_j = as$ cu $1 \leq r, s \leq \frac{p-1}{2}$, deci $a(r + s) = 0$ şi cum $a \neq 0$ deducem că $r + s = 0$ ceea ce este imposibil deoarece $2 \leq r + s < p - 1$. Deducem atunci că $Z = X$ (căci $Z \subseteq X$ şi $|Z| = |X|$), deci (în $\mathbf{Z}_p$) avem : $1 \cdot 2 ... \frac{p-1}{2} = x_1 ... x_k (p - y_1) ... (p - y_g) = (-1)^g x_1 ... x_k y_1 ... y_g = (-1)^g a \cdot 2a \cdot .... \frac{p-1}{2} a$ (căci $X' \cup Y' = \widehat{a}X!$) $= (-1)^g a^{\frac{p-1}{2}} \cdot 1 \cdot 2 ... \frac{p-1}{2}$, de unde $(-1)^g a^{\frac{p-1}{2}} = 1$, de unde

$$(-1)^g = a^{\frac{p-1}{2}} = (\frac{a}{p}). \ \blacksquare$$

Corolar 4.1.4. *Pentru orice număr prim p impar (deci $p \geq 3$) avem*

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

Demonstraţie. Să observăm la început că $\frac{p^2-1}{8} \in \mathbf{N}$. Intr-adevăr, dacă $p = 8m + r (r = 1, 3, 5, 7)$, atunci: $\frac{p^2-1}{8} = \frac{(8m+r)^2-1}{8} = 2n + \frac{r^2-1}{8} (n \in \mathbf{N})$ şi cum $\frac{r^2-1}{8} \in \mathbf{N}$ pentru $r = 1, 3, 5, 7$ totul este clar.

Pentru $1 \leq x < \frac{p-1}{2}$ avem că $2x < p-1$. Atunci g din Lema 4.1.3 a lui Gauss (pentru $a=2$) este numărul elementelor de forma $2x, 1 \leq x < \frac{p-1}{2}$ ce verifică condiţia $2x \in Y \Leftrightarrow x > \frac{p-1}{4}$, adică $g = \frac{p-1}{2} - [\frac{p-1}{4}]$. Considerând $p = 8m+r, (r = 1,3,5,7)$, avem $g = 4m + \frac{r-1}{2} - [2m + \frac{r-1}{2}] = 4m + \frac{r-1}{2} - 2m - [\frac{r-1}{4}] = 2m + \frac{r-1}{2} - [\frac{r-1}{4}]$, care ne duce la concluzia că g este par pentru $r = 1,7$ şi impar pentru $r = 3,5$, adică g şi $\frac{p^2-1}{8}$ au aceeaşi paritate, de unde $(\frac{2}{p}) = (-1)^g = (-1)^{\frac{p^2-1}{8}}$. ■

4.2 Legea reciprocităţii pătratice

In vederea demonstrării legii reciprocităţii pătratice, să stabilim la început urmatoarea lemă:

Lema 4.2.1. *Dacă p şi q sunt două numere prime impare ($p, q \geq 3$), distincte, atunci*

$$\sum_{j=1}^{\frac{p-1}{2}} [\frac{jq}{p}] + \sum_{j=1}^{\frac{q-1}{2}} [\frac{jp}{q}] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Demonstraţie. Notând $s(p,q) = \sum_{j=1}^{\frac{p-1}{2}} [\frac{jq}{p}]$, egalitatea din enunţ devine : $s(p,q) + s(q,p) = \frac{(p-1)(q-1)}{4}$.

Este uşor de observat că pentru orice $j = 1, 2, ..., \frac{p-1}{2}, [\frac{jq}{p}]$ este numărul de numere naturale din intervalul $(0, \frac{jq}{p})$.

Deci pentru fiecare j ca mai sus, $[\frac{jq}{p}]$ este numărul acelor puncte laticiale din plan situate pe dreapta $x = j$ (delimitate strict superior de dreapta $y = \frac{qx}{p}$ 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 ecuaţie $y = \frac{q}{p}x$ (vezi Fig.1).

Analog, $s(q,p)$ reprezintă numărul punctelor laticiale din interiorul dreptunghiului $OABC$ situate deasupra dreptei de ecuaţie $y = \frac{q}{p}x$ astfel că $s(p,q) + s(q,p)$=numă- rul de puncte laticiale din interiorul dreptunghiului $OABC = \frac{p-1}{2} \cdot \frac{q-1}{2}$ şi astfel lema este probată. ■

Teorema 4.2.2. *(Legea reciprocităţii pătratice) Dacă p şi q sunt doua numere prime impare distincte, atunci*

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

.

Demonstraţie. Revenim la notaţiile din Lema 4.1.3 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 $\mathbf{Z}_p$).

Fie $\alpha = \sum_{j=1}^{k} x_j, \beta = \sum_{j=1}^{g} y_j$.

Avem $\sum_{x \in X} x = 1 + 2 + ... + \frac{p-1}{2} = \frac{p^2-1}{8}$.

Analog ca în demonstraţia lemei lui Gauss vom avea:

$\sum_{z \in Z} z = \sum_{j=1}^{k} x_j + \sum_{j=1}^{g} (p - y_j) = \alpha - \beta + pg$ şi cum $X = Z$ deducem că $\frac{p^2-1}{8} = \alpha - \beta + pg$.

Acum, pentru $j = 1, 2, ..., \frac{p-1}{2}$, fie t_j restul împărţirii prin p a lui jq. Evident câtul este $[\frac{jq}{p}]$, deci $jq = [\frac{jq}{p}] \cdot p + t_j$. Făcând $j = 1, 2, ..., \frac{p-1}{2}$ şi sumând obţinem:

$$\frac{q(p^2-1)}{8} = p \cdot s(p,q) + \sum_{j=1}^{\frac{p-1}{2}} t_j = p \cdot s(p,q) + \sum_{j=1}^{k} x_j + \sum_{j=1}^{g} y_j$$

sau $\frac{q(p^2-1)}{8} = p \cdot s(p,q) + \alpha + \beta$.

Cum $\frac{p^2-1}{8} = \alpha - \beta + p \cdot g$ deducem că $\frac{(q-1)(p^2-1)}{8} = p[s(p,q) - g] + 2\beta$.

Deoarece p şi q sunt primi impari şi $\frac{p^2-1}{8} \in \mathbf{N}$, deducem că $s(p,q) - g \equiv 0 (\mathrm{mod}\ 2)$, astfel că $(\frac{q}{p}) = (-1)^g = (-1)^{s(p,q)}$.

Schimbând rolul lui p cu q deducem că $(\frac{p}{q}) = (-1)^{s(q,p)}$, de unde

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{s(p,q)+s(q,p)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \ \blacksquare$$

Legea reciprocităţii pătratice a fost intuită de Euler, formulată de Legendre şi desăvârşită de Gauss.

Aplicaţie. Fie $p = 1009$ şi $a = 45 = 3^2 \cdot 5$. Avem

$(\frac{45}{1009}) = (\frac{3^2}{1009})(\frac{5}{1009}) = (\frac{5}{1009}) = (\frac{1009}{5})(-1)^{\frac{1009-1}{2} \cdot \frac{5-1}{2}} = (\frac{1009}{5}) = (\frac{9}{5}) = 1$, deci 45 este rest pătratic modulo 1009 (adică 45 este pătrat în $\mathbf{Z}_{1009}^*$).

4.3 Alte cazuri particulare ale teoremei lui Dirichlet

După cum am văzut, pentru orice număr prim p, $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ (conform Corolarului 4.1.4). De aici deducem că 2 este rest pătratic modulo p pentru p de forma $8k \pm 1$ şi non-rest pătratic pentru p de forma $8k \pm 3$ (cu $k \in \mathbf{N}^*$).

Propoziţia 4.3.1. *Există o infinitate de numere prime de forma 8n-1, $n \in \boldsymbol{N}^*$.*

Demonstraţie. Fie $n \in \mathbf{N}, n \geq 2$; atunci numărul $N = 2(n!)^2 - 1 > 1$ are cel puţin 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 $p \mid N \Leftrightarrow 2(n!)^2 \equiv 1^2 (\mathrm{mod}\ p)$, de unde deducem că $(\frac{2(n!)^2}{p}) = 1$.

Insă $(\frac{2(n!)^2}{p}) = (\frac{2}{p})(\frac{n!}{p})^2 = (\frac{2}{p})$, deci $(\frac{2}{p}) = 1$, adică p trebuie să fie de forma $8k \pm 1$. Cum p nu este de forma $8k+1$ ramâne 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 $n \in \mathbf{N}, n > 1$, 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 $q_1, q_2, ..., q_t$.

Considerând numărul $n = 8q_1...q_t - 1$, conform celor de mai înainte există un număr prim de forma $8k - 1$ (adică un q_i) astfel încât $q_i > n$, ceea ce este absurd. ■

Propoziţia 4.3.2. *Există o infinitate de numere prime de forma* $8n + 3, n \in \boldsymbol{N}^*$.

Demonstraţie. Fie $n > 1$ şi $a = p_2p_3...p_n$ (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 $8t \pm 1, N$ 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 $p \mid N = a^2 + 2$ deducem că $a^2 \equiv -2(p)$ şi deci $(\frac{-2}{p}) = 1$.

Insă, $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$.

Dacă $p = 8t + 5$ atunci $(\frac{-2}{p}) = -1$ absurd, de unde concluzia că p este de forma $8t + 3$. Insă din $p \mid a^2 + 2$ deducem că $p > p_n$ şi astfel avem o infinitate de numere prime de forma $8t + 3$. ■

Propoziţia 4.3.3. *Există o infinitate de numere prime de forma* $8n+5$*, cu* $n \in \boldsymbol{N}^*$.

Demonstraţie. Fie $n > 1$ natural şi $a = p_2p_3...p_n$. Cum a este impar, $N = a^2 + 4$ este de forma $8t + 5$.

Dacă toti divizorii lui N ar fi de forma $8t \pm 1$, 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 $p \mid N = a^2 + 4 \Rightarrow a^2 \equiv -4(\text{mod } p)$, deci $(\frac{-4}{p}) = 1$ şi astfel $(\frac{-4}{p}) = (\frac{-1}{p})(\frac{2}{p})^2 = (-1)^{\frac{p-1}{2}}$ şi cum $p = 8t + 3 \Rightarrow (\frac{-4}{p}) = -1$, contradicţie!

Deci p este de forma $8t+5$ şi astfel din $p|a^2+4$ şi $a = p_2p_3...p_n$ deducem că $p > p_n$, de unde rezultă imediat că avem o infinitate de numere prime de forma $8n + 5$. ■

Observaţie. Din legea reciprocităţii pătratice deducem

Corolar 4.3.4. *Există o infinitate de numere prime de forma* $5n - 1$*, cu* $n \in \boldsymbol{N}^*$.

Demonstraţie. Fie $n \in \mathbf{N}^*, n > 1$ 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 $p(p \neq 5)$ ce este de forma $5t + 1$. Evident $p > n$.

Cum $p \mid N \Rightarrow 5(n!)^2 \equiv 1(\text{mod } p)$, adică $(\frac{5}{p}) = 1$. Atunci şi $(\frac{p}{5}) = 1$.

Avem că $p \neq 5$ poate să fie de forma $5k \pm 1$ sau $5k \pm 2$.

Dacă $p = 5k \pm 2$, atunci $(\frac{p}{5}) = (\frac{\pm 2}{5}) = (\frac{\pm 1}{5})(\frac{2}{5})$ şi cum $(\frac{\pm 1}{5}) = 1, (\frac{2}{5}) = -1$, deducem că $(\frac{p}{5}) = -1$, contradicţie!

Cum am văzut că p nu poate fi de forma $5k + 1$ deducem că p trebuie să fie de forma $5k - 1$. De aici corolarul rezultă imediat. ■

Observaţie. Din demonstraţia Corolarului 4.3.3 deducem că numărul prim p este de forma $p = 5k - 1(k \in \mathbf{N})$. Evident $k = 2t$, deci $p = 10t - 1$.

De aici rezultă

Corolar 4.3.5. *Există o infinitate de numere prime de forma* $10n-1, n \in \boldsymbol{N}^*$.

Capitolul 5

Fracţii continue

5.1 Fracţii continue. Proprietăţi elementare

Vrând să construiască un planetariu cu roţi dinţate, Cristian Huyghens (matematician, fizician şi astronom, 1629-1695) a avut de rezolvat problema: care raport între numărul de dinţi a două roţi care se angrenează (egal cu raportul duratelor lor de rotaţie) este mai apropiat de raportul α dintre duratele de rotaţie ale planetelor respective. Din motive tehnice, numărul de dinţi de pe o roata nu putea să fie prea mare.

O problemă similară a apărut la alcătuirea calendarului: ce număr p de ani bisecţi (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 reala $A = 365,24219878...$ 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 bisecţi sunt acei multipli de 4 care nu sunt multipli de 100, excepţie făcând multiplii de 400. Anul nostru calendaristic durează deci $365 + \frac{97}{400} = 365,2425$ 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 raţionale apar în numeroase domenii. O soluţie este dată de *fracţiile continue*. După cum vom vedea, fracţiile continue pot fi folosite cu succes şi la rezolvarea unor probleme care, cel puţin aparent, nu au legatură cu aproximarea numerelor.

Fie $\alpha \in \mathbf{Q}$. Atunci putem scrie $\alpha = \frac{p}{q}$, cu $p \in \mathbf{Z}$ şi $q \in \mathbf{N}^*$.

Făcând mai multe împărţiri cu rest găsim că pentru un anumit $k \in \mathbf{N}$ avem:

$$\begin{aligned} p &= a_0 q + q_1, 0 < q_1 < q \\ q &= a_1 q_1 + q_2, 0 < q_2 < q_1 \\ q_1 &= a_2 q_2 + q_3, 0 < q_3 < q_2 \\ ..... &... ..... \\ q_{k-2} &= a_{k-1} q_{k-1} + q_k, 0 < q_k < q_{k-1} \\ q_{k-1} &= a_k q_k, \end{aligned}$$

unde $a_0 \in \mathbf{Z}$ iar $a_1, ..., a_k \in \mathbf{N}^*$. 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 $\frac{p}{q}$: $a_0 = [\alpha], a_1 = [\frac{p}{q_1}] = [\frac{1}{\alpha - a_0}]$, 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 fracţii etajate sub forma:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_k}. \tag{1}$$

In fracţia de mai sus, $a_0 \in \mathbf{Z}$ iar $a_1, ..., a_k \in \mathbf{N}$.

Scrierea lui α sub forma (1) nu mai este aşa de simplă dacă α este iraţional;

Procedând ca mai sus obţinem $a_0 = [\alpha] \in \mathbf{Z}$. Evident $\alpha_1 = \frac{1}{\alpha - a_0} > 1$ şi din nou dacă $a_1 = [\alpha_1] \in \mathbf{N}^*$, atunci $\alpha_2 = \frac{1}{\alpha_1 - a_1} > 1$.

Putem scrie că $\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|\alpha_2}$. Continuând procedeul obţinem scrieri intermediare de forma

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_n} + \frac{1|}{|\alpha_{n+1}}. \tag{2}$$

Să observăm că procesul de scriere al lui α sub forma (2) poate continua atâta timp cât $\alpha_n \notin \mathbf{N}$. După cum am văzut, dacă $\alpha \in \mathbf{Q}$, pentru un anumit $k \in \mathbf{N}$, $\alpha_k \in \mathbf{N}$.

Dacă însă $\alpha \notin \mathbf{Q}$, acest proces poate continua oricât de mult, deoarece fiecare $\alpha_k \notin \mathbf{Q}$. Se obţine astfel o fracţie etajată infinită:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_n} + ... \tag{3}$$ Semnul egal de mai sus este pus convenţional: nu ştim deocamdată ce reprezintă membrul drept. Să comprimăm şi mai mult scrierea fracţiilor etajate (1), (2), (3), notându-le $[a_0; a_1, a_2, ..., a_n]$ pentru (1), $[a_0; a_1, a_2, ..., a_n, \alpha_{n+1}]$ pentru (2), şi $[a_0; a_1, a_2, ...]$ pentru (3).

Vom prezenta în continuare câteva proprietăţi ale fracţiilor continue.

Pentru o fracţie continuă $[a_0; a_1, a_2, ..., a_n, ...]$ (unde $a_0 \in \mathbf{Z}$ iar $a_n \in \mathbf{N}^*$ pentru $n \geq 1$) să notăm

$$\pi_n = \frac{p_n}{q_n} = [a_0; a_1, a_2, ..., a_n].$$

Numerele π_n sunt, evident, raţionale şi se numesc *redusele* fracţiei continue.

Observaţie. Fracţia continuă $[a_0; a_1, a_2, ..., a_m, 1]$ se poate scrie mai scurt $[a_0; a_1, a_2, ..., a_m + 1]$. Cu convenţia $a_k \geq 2$, scrierea $[a_0; a_1, a_2, ..., a_k]$ a numerelor raţionale neîntregi este unică.

Fie $\frac{p}{q} = [a_0; a_1, a_2, ..., a_n]$ şi $\frac{p'}{q'} = [a_1; a_2, a_3, ..., a_n]$. Se vede că legătura dintre cele două numere este $\frac{p}{q} = a_0 + \frac{q'}{p'}$. Dacă $\frac{p'}{q'}$ este o fracţie ireductibilă, atunci şi $\frac{p'a_0 + q'}{p'}$ este ireductibilă, deci putem afirma că, dacă şi $\frac{p}{q}$ 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. Intr-adevăr, dacă $\alpha = [a_0; a_1, a_2, ..., a_n]$, atunci $\alpha_n = \frac{a_n}{1}$ 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 5.1.1. *Numărătorii şi numitorii reduselor verifică relaţile*:

$$\begin{aligned} p_0 &= a_0, p_1 = a_0a_1 + 1, ..., p_{n+1} = a_{n+1}p_n + p_{n-1} (n = 1, 2, ...) \\ q_0 &= 1, q_1 = a_1, ..., q_{n+1} = a_{n+1}q_n + q_{n-1} (n = 1, 2, ...). \end{aligned} \tag{5}$$

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 $n \leq k - 1$ şi arătăm că sunt adevărate şi pentru $n = k$. Avem

$\frac{p_{k+1}}{q_{k+1}} = [a_0; a_1, ..., a_{k+1}] = [a_0; \alpha_1]$, unde $\alpha_1 = [a_1; a_2, ..., a_{k+1}]$.

Fie $\frac{p'_0}{q'_0}, \frac{p'_1}{q'_1}, ..., \frac{p'_k}{q'_k} = \alpha_1$ redusele fracţiei α_1. Conform ipotezei de inducţie,

$$\begin{aligned} p'_k &= a_kp'_{k-1} + p'_{k-2} \\ q'_k &= a_kq'_{k-1} + q'_{k-2}. \end{aligned}$$

Pe de alta parte, din (4), avem

$$\begin{aligned} p_{k+1} &= a_0p'_k + q'_k, q_{k+1} = p'_k \\ p_k &= a_0p'_{k-1} + q'_{k-1}, q_k = p'_{k-1} \\ p_{k-1} &= a_0p'_{k-2} + q'_{k-2}, q_{k-1} = p'_{k-2}, \end{aligned}$$

şi deci,

$$\begin{aligned} q_{k+1} &= p'_k = a_{k+1}p'_{k-1} + p'_{k-2} = a_{k+1}q_k + q_{k-1}, \\ p_{k+1} &= a_0p'_k + q'_k = a_0(a_{k+1}p'_{k-1} + p'_{k-2}) + a_{k+1}q'_{k-1} + q'_{k-2} \\ &= a_{k+1}(a_0p'_{k-1} + q'_{k-1}) + a_0p'_{k-2} + q'_{k-2} = a_{k+1}p_k + p_{k-1}. \end{aligned}$$

Folosind principiul inducţiei complete, propoziţia este demonstrată. ■

In 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 5.1.2. *Dacă* $\alpha = [a_0; a_1, ..., a_n, \alpha_{n+1}]$ *atunci*

$$\alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}. \tag{6}$$

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_2	...	$a_{n+1}p_n + p_{n-1}$
q	0	q_0	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	...
p	1	1	2	3	5	8	13	21	...
q	0	1	1	2	3	5	8	13	...

Propoziţia 5.1.3. *Au loc relaţiile*

$$\begin{cases} q_np_{n-1} - p_nq_{n-1} = (-1)^n, n \geq 0 & (7) \\ q_np_{n-2} - p_nq_{n-2} = (-1)^{n-1}a_n, n \geq 1 & (8) \\ \pi_{n-1} - \pi_n = \frac{(-1)^n}{q_nq_{n-1}}, n \geq 1 & (9) \\ \pi_{n-2} - \pi_n = \frac{(-1)^{n-1}}{q_nq_{n-2}}, n \geq 2 & (10) \end{cases}$$

Demonstraţie. Deoarece $q_0 = 1, p_0 = a_0, q_{-1} = 0, p_{-1} = 1$ avem $q_0p_{-1} - p_0q_{-1} = (-1)^0$, deci relaţia (7) este adevărată pentru $n = 0$. Presupunem că pentru un n avem $q_np_{n-1} - p_nq_{n-1} = (-1)^n$.

Folosind (5), avem $q_{n+1}p_n - p_{n+1}q_n = (a_{n+1}q_n + q_{n-1})p_n - (a_{n+1}p_n + p_{n-1})q_n = -(q_np_{n-1} - p_nq_{n-1}) = (-1)^{n+1}$.

Deci am demonstrat prin induţie relaţia (7).

Folosind întâi (5), apoi (7), avem : $q_np_{n-2} - p_nq_{n-2} = (a_nq_{n-1} + q_{n-2})p_{n-2} - (a_np_{n-1} + p_{n-2})q_{n-2} = a_n(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = (-1)^{n-1}a_n$ 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 5.1.4. *Au loc inegalităţile*

$$\pi_0 < \pi_2 < \pi_4 < ... < \pi_5 < \pi_3 < \pi_1.$$

Fie $\alpha = [a_0; a_1, ..., a_n, a_{n+1}]$ un număr real oarecare. Folosind (6), avem:

$$\alpha - \pi_n = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(q_n\alpha_{n+1} + q_{n-1})} = \frac{(-1)^n}{q_n(q_n\alpha_{n+1} + q_{n-1})}.$$

Egalitatea obţinută arată că redusele de ordin par sunt mai mici decât α, iar cele de ordin impar sunt mai mari decât α. Intru-cât $\alpha_{n+1} \geq a_{n+1}$ 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:

Propoziţia 5.1.5. *Dacă* $\alpha = [a_0; a_1, ..., a_n, \alpha_{n+1}]$, *atunci*

$$\frac{1}{q_n(q_n + q_{n-1})} < |\alpha - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}} \qquad (11)$$

egalitatea din dreapta având loc numai dacă $\alpha = \frac{p_{n+1}}{q_{n+1}}$.

Suntem în măsură să dăm sens egalităţii din (3). Din (5) este uşor de dedus că, pentru fracţii continue infinite, $q_{n+1} > q_n$, începând cu $n = 1$ şi deci $q_n \geq n$.

Pornind de la un număr iraţional α, şirul $(\pi_n)_{n\geq 1}$ aproximează din ce în ce mai bine numărul α. In limbajul analizei matematice asta înseamnă că $\lim\limits_{n\to\infty} \pi_n = \alpha$. Dacă pornim de la o fracţie continuă infinită, Propoziţia 5.1.4, împreună cu (9), garantează că şirul $(\pi_n)_{n\geq 1}$ converge. Lăsăm în seama cititorului să arate că fracţia continuă ataşată acestui număr este tocmai fracţia continuă de la care am plecat. Ideea demonstraţiei este următoarea:

Dacă

$$[a_0; a_1, ..., a_{2n}] < \beta = [b_0; \beta_1] < [a_0; a_1, ..., a_{2n}, a_{2n+1}],$$

atunci

$$b_0 = a_0 \text{ şi } [a_1; a_2, ..., a_{2n+1}] < \beta_1 = [b_1; \beta_2] < [a_1; a_2, ..., a_{2n}].$$

Să mai demonstrăm o proprietate a reduselor:

Propoziţia 5.1.6. *Fie* $a_0 \geq 1, \frac{p_{n-1}}{q_{n-1}} = [a_0; a_1, ..., a_{n-1}]$ *şi* $\frac{p_n}{q_n} = [a_0; a_1, ..., a_n]$.
Atunci $[a_n; a_{n-1}, ..., a_0] = \frac{p_n}{p_{n-1}}$ *şi* $[a_n; a_{n-1}, ..., a_1] = \frac{q_n}{q_{n-1}}$.

Demonstraţie. Procedăm prin induţie după n.

Pentru $n = 1, [a_0; a_1] = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}, \frac{a_0}{1} = \frac{p_0}{q_0}$.

Avem $[a_1; a_0] = \frac{a_0 a_1 + 1}{a_0} = \frac{p_1}{p_0}, a_1 = \frac{q_1}{q_0}$.

Presupunem afirmaţia adevarată pentru n. Atunci:

$$[a_{n+1}; a_n, ..., a_1] = a_{n+1} + \frac{1}{[a_n; a_{n-1}, ..., a_1]} = a_{n+1} + \frac{q_{n-1}}{q_n} = \frac{a_{n+1}q_n + q_{n-1}}{q_n} = \frac{q_{n+1}}{q_n}.$$

Tot cu ajutorul lui (5), avem şi

$$[a_{n+1}; a_n, ..., a_0] = a_{n+1} + \frac{1}{[a_n; a_{n-1}, ..., a_0]} = a_{n+1} + \frac{p_{n-1}}{p_n} = \frac{a_{n+1}p_n + p_{n-1}}{p_n} = \frac{p_{n+1}}{p_n}.$$

ceea ce trebuia demonstrat. ■

5.2 Aproximări ale numerelor reale prin numere raţionale

Vom prezenta în continuăre câteva chestiuni legate de aproximarea numerelor reale.

Fie α un număr real. Problema aproximării lui cu numere raţionale are următoarea interpretare geometrică. In planul xOy considerăm dreapta (d) de ecuaţie $y = \alpha x$ şi reţeaua de puncte ,,laticiale" din semiplanul drept, adică mulţimea punctelor de coordonate întregi (q, p) cu $q > 0$ (vezi Fig. 2). Căutăm puncte $P(q, p)$ pentru care $\frac{p}{q}$ este aproape de α, adica puncte $P(q, p)$ situate ,,aproape" de dreapta (d). Această apropiere o putem măsura prin abaterea dintre pantele dreptelor (d) şi OP (de ecuaţie $y = \frac{p}{q}x$), fie prin distanţa de la P la dreapta (d) sau, ceea ce este echivalent, prin lungimea $|q\alpha - p|$ a segmentului PQ, unde Q este punctul de pe dreapta (d) care are abscisa egală cu P.

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 $0 < q' \leq q$ avem $|\alpha - \frac{p}{q}| < |\alpha - \frac{p'}{q'}|$. 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 $q' \leq q$. 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 5.2.1. *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 $\alpha = [a_0; a_1, ..., a_n, ...]$.

Dacă $\frac{p}{q} < a_0 (= \pi_0)$, atunci $|1 \cdot \alpha - a_0| = |\alpha - \frac{p_0}{q_0}| < |\alpha - \frac{p}{q}|$, deci $\frac{p}{q}$ n-ar fi o cea mai bună aproximare.

Dacă $\frac{p}{q} > \frac{p_1}{q_1} (= \pi_1)$ atunci $|\alpha - \frac{p}{q}| > |\frac{p}{q} - \frac{p_1}{q_1}| \geq \frac{1}{qq_1}$ (căci avem următoarea ordonare deci $|q\alpha - p| > \frac{1}{q_1}$.

Pe de altă parte, din (11), $\frac{1}{q_1} = \frac{1}{a_1} \geq |1 \cdot \alpha - a_0|$ şi, din nou, $\frac{p}{q}$ nu ar fi o cea mai bună aproximare. Am stabilit deci că $\pi_0 \leq p/q \leq \pi_1$.

Presupunem că $\frac{p}{q}$ nu coincide cu nici o redusă a lui α. Atunci $\frac{p}{q}$ este cuprins între două reduse π_{n-1} şi π_{n+1}, cu rangurile de aceeaşi paritate. Avem

$$|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}| \geq \frac{1}{qq_{n-1}} \text{ şi } |\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}| < |\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}}$$

de unde deducem $q_n < q$. Pe de alta parte,

$$|\alpha - \frac{p}{q}| \geq |\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| \geq \frac{1}{q_n q_{n-1}}$$

deci $|q\alpha - p| \geq \frac{1}{q_{n-1}}$ şi din (11), $\frac{1}{q_{n+1}} \geq |q_n\alpha - p_n|$ adică $q_n < q$ şi $|q_n\alpha - p_n| \leq |q\alpha - p|$, în contradicţie cu faptul că $\frac{p}{q}$ este o cea mai bună aproximare şi astfel propoziţia este demonstrată. ■

Observaţie. Dacă α este raţional şi $\frac{p}{q}$ nu este o redusă a lui α, atunci găsim redusa $\frac{p_n}{q_n}$, cu $|q_n\alpha - p_n| \leq |q\alpha - p|$ şi $q_n < q$.

Este adevărată şi reciproca:

Propoziţia 5.2.2. *Orice redusă este o cea mai bună aproximare, cu excepţia eventuală a redusei* $\pi_0 = \frac{p_0}{q_0}$.

Observaţie. Dacă $\alpha = [a_0; 2]$, atunci $\pi_0 = \frac{a_0}{1}$ nu este o cea mai bună aproximare, căci $|1 \cdot \alpha - a_0| = \frac{1}{2} = |1 \cdot \alpha - a_0 - 1|$. In schimb, $\pi_1 = \alpha$ este, evident, o cea mai bună aproximare.

Vom examina numai cazul $\alpha \neq [a_0; 2]$. Fie $\frac{p_m}{q_m}$ o redusă a lui α, cu $m \geq 1$. Considerăm numerele $|y\alpha - x|$, unde $y \in \mathbf{N}^*, y \leq q_m$, 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 raţional.

Fie $\alpha = [a_0; a_1, ..., a_n]$, cu $a_n \geq 2$, fracţia 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 $2x_0 + 1 = p_n = a_np_{n-1} + p_{n-2}$, de unde $q_{n-1} < y_0$, dar $|q_{n-1}\alpha - p_{n-1}| = \frac{1}{q_n} = \frac{1}{2y_0} \leq \frac{1}{2} = |y_0\alpha - p_0|$, 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 $q_1, q_2, ...$ este strict crescător, avem $k \leq m$ (căci $q_k \leq q_m$). Dacă $k = m$, am terminat, dacă, însă, $k < m$, atunci, folosind (11), avem

$$|q_k\alpha - p_k| > \frac{1}{q_k + q_{k+1}} \geq \frac{1}{q_{m-1} + q_m} \geq \frac{1}{q_{m-1} + a_{m+1}q_m} = \frac{1}{q_{m+1}} \geq |q_m\alpha - p_m|$$

ceea ce ar contrazice definiţia lui y_0.

In prima parte a demonstraţiei am arătat că, exceptând numerele $\alpha = [a_0; 2]$, luând un $q \in \mathbf{N}^*$ (în locul lui q_m), există o cea mai bună aproximare $\frac{x_0}{y_0}$(deci o redusă a lui α) cu $y_0 \leq q$. In 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 $q_1 = 1$, deci $\alpha = [a_0; 1, ...]$.
■

5.3 Fracţii periodice şi pur periodice

In continuăre ne vom ocupa de dezvoltarea în fracţii continue periodice a numerelor iraţionale pătratice.

Definiţia 5.3.1. Fracţia continuă infinită $[a_0; a_1, ...]$ se zice *periodică* dacă există $h \in \mathbf{N}^*$ şi $k \in \mathbf{N}^*$ cu $a_n = a_{n+h+1}$ pentru fiecare $n \geq k$. Convenim să notăm o asemenea

fracţie continuă cu $[a_0; a_1, ..., a_{k-1}, \overline{a_k, a_{k+1}, ..., a_{k+h}}]$.

Pentru asemenea fracţii continue putem calcula valoarea mai simplu decât ca limită a şirului de reduse.

Exemplu. Fie $\alpha = [1; 2, 2, 2, 2, ...]$.Avem $\alpha = [1; \alpha_1]$, unde $\alpha_1 = [2; 2, 2, 2, 2, ...] = [\widehat{2}]$. De asemenea, $\alpha_1 = [2; \alpha_2]$, unde $\alpha_2 = \alpha_1$, deci $\alpha_1 = 2 + \frac{1}{\alpha_1}$, adică $\alpha_1^2 - 2\alpha_1 - 1 = 0$, de unde $\alpha_1 = 1 + \sqrt{2}$. Revenind la α, obţinem $\alpha = 1 + \frac{1}{\alpha_1} = \sqrt{2}$.

In general, dacă $\alpha = [a_0; a_1, ..., a_{k-1}, \overline{a_k, a_{k+1}, ..., a_{k+h}}]$, atunci

$\alpha_k = [\overline{a_k; a_{k+1}, ..., a_{k+h}}] = a_{k+h+1}$ şi, conform lui (6)

$$\alpha = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}} = \frac{\alpha_k p_{k+h} + p_{k+h-1}}{\alpha_k q_{k+h} + q_{k+h-1}}.$$

Din a doua egalitate urmează că α_k este rădăcina unei ecuaţii de gradul doi cu coeficienţi întregi

$$A\alpha_k^2 + B\alpha_k + C = 0$$

iar prima egalitate ne dă

$$\alpha = \frac{-q_{k-2}\alpha + p_{k-2}}{q_{k-1}\alpha - p_{k-1}}$$

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 rădăcină a unei ecuaţii de gradul doi cu coeficienţi întregi.

Definitia 5.3.2. Numerele iraţionale, rădăcini ale unei ecuaţii de gradul doi cu coeficienţi întregi (nu toţi nuli), se numesc *iraţionale pătratice*.

In anul 1770, Joseph Louis de Lagrange (1736-1813) a demonstrat următorul rezultat

Propoziţia 5.3.3.(*Lagrange) Un număr iraţional este pătratic dacă şi numai dacă fracţia sa continuă este periodică.*

Demonstraţie. Am arătat deja că orice fracţie continuă periodică este un iraţional pătratic.

Să presupunem acum că α este rădăcină a ecuaţiei cu coeficienţi întregi $Ax^2 + Bx + C = 0$, unde $A \neq 0$ şi $0 < B^2 - 4AC$ nu este pătrat perfect.

Fie $\alpha = [a_0; a_1, ..., a_{n-1}, \alpha_n]$. Cu relaţia (6), avem

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

şi, deci,

$$A(p_{n-1}a_n + p_{n-2})^2 + B(q_{n-1}a_n + q_{n-2})(p_{n-1}a_n + p_{n-1}) + C(q_{n-1}a_n + q_{n-2})^2 = 0$$

adica α_n este rădăcina ecuaţiei $A_n x^2 + B_n x + C_n = 0$, unde

$$\begin{aligned} A_n &= Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2 \quad (12) \\ B_n &= Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + q_{n-1}p_{n-2}) + Cq_{n-1}q_{n-2} \quad (13) \\ C_n &= Ap_{n-2}^2 + Bp_{n-2}q_{n-2} + Cq_{n-2}^2. \quad (14) \end{aligned}$$

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 aceeaşi paritate. Prin calcul direct se verifică şi că

$$B_n^2 - 4A_nC_n = (B^2 - 4AC)(p_{n-1}q_{n-2} + q_{n-1}p_{n-2})^2 = B^2 - 4AC. \quad (15)$$

Folosind însă faptul că $A\alpha^2 + B\alpha + C = 0$, relaţia (12) se scrie:

$$\begin{aligned} A_n &= Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2 - q_{n-1}^2(A\alpha^2 + B\alpha + C) \\ &= A(p_{n-1}^2 - q_{n-1}^2\alpha^2) + B(p_{n-1} - \alpha q_{n-1})q_{n-1} \\ &= (p_{n-1} - \alpha q_{n-1})(A(p_{n-1} + \alpha q_{n-1}) + Bq_{n-1}). \end{aligned}$$

Cu ajutorul lui (11), vom avea

$$\begin{aligned} |A_n| &\leq \frac{1}{q_n}|A(p_{n-1} + \alpha q_{n-1}) + Bp_{n-1}| \leq \frac{1}{q_{n-1}}|A(p_{n-1} + \alpha q_{n-1}) + Bp_{n-1}| \\ &\leq |A||\frac{p_{n-1}}{q_{n-1}} + \alpha| + |B| \leq |A|(|\frac{p_{n-1}}{q_{n-1}} - \alpha| + 2|\alpha|) + |B| \leq |A|(1 + 2|\alpha|) + |B|. \end{aligned}$$

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 anumiţi 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 inducţie, $a_n = a_{n+h+1}$ pentru $n \geq k$, deci fracţia continuă a lui α este periodică. ■

Cele mai simple fracţii 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 fracţie continuă pur periodică. Avem $a_0 = a_{n+1} \geq 1$ şi $\alpha = [a_0; a_1, ..., a_n, \alpha]$, deci, folosind (6), $\alpha = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}$, 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, $\alpha > a_0 \geq 0$, deducem că cealaltă rădăcină a trinomului este cuprinsă între -1 şi 0. Evident α este de forma $\frac{P + \sqrt{D}}{Q}$, iar cealaltă rădăcină este $\frac{P - \sqrt{D}}{Q}$. Pentru un iraţional pătratic $\alpha = \frac{P + \sqrt{D}}{Q}$, vom nota $\widetilde{\alpha} = \frac{P - \sqrt{D}}{Q}$ şi îl vom numi pe $\widetilde{\alpha}$ conjugatul lui α.

Definitia 5.3.4. Numărul iraţional 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 5.3.5. *(E. Galois) Fracţia continuă a lui α este pur periodică dacă şi numai dacă este un iraţional pătratic redus.*

Demonstraţie. Am văzut mai sus că orice fracţie continuă pur periodică este un iraţional pătratic redus (vom prescurta în continuare prin 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 inducţie, rezultă că α_n este i.p.r. pentru fiecare n. Ştim că fracţia 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 $a_{k+h} = [a_{k+h}; \alpha_{k+h+1}] = [a_{k+h}; \alpha_k]$. Avem deci $\widetilde{\alpha}_{k-1} = (a_{k-1} + \frac{1}{\alpha_k})^{\sim} = a_{k-1} + \frac{1}{\widetilde{\alpha}_k} \in (-1, 0), \widetilde{\alpha}_{k+h} = \alpha_{k+h} + \frac{1}{\widetilde{\alpha}_k} \in (-1, 0)$.

Deducem de aici că $a_{k-1} \in (-1 - \frac{1}{\widetilde{\alpha}_k}, -\frac{1}{\widetilde{\alpha}_k})$ şi $a_{k+h} \in (-1 - \frac{1}{\widetilde{\alpha}_k}, -\frac{1}{\widetilde{\alpha}_k})$, deci $a_{k-1} = a_{k+h} = [-\frac{1}{\widetilde{\alpha}_k}]$.

Am ajuns la o contradicţie, deci $\alpha = [\overline{a_0; a_1, ..., a_h}]$. ■

Ce se întâmplă dacă ,,răsturnăm" perioada unui i.p.r.?

Propoziţia 5.3.6. *Fie* $\alpha = [\overline{a_0; a_1, ..., a_n}]$ *şi* $\beta = [\overline{a_{0n}; a_{n-1}, ..., a_0}]$. *Atunci* $\alpha = -\frac{1}{\widetilde{\beta}}$.

Demonstraţie. Intrucât $\alpha = [a_0; a_1, ..., a_n, \alpha]$, folosind (6), avem, după cum am mai văzut,

$$q_n \alpha^2 + (q_{n-1} - p_n)\alpha - p_{n-1} = 0. \quad (16)$$

Cum $\beta = [a_n; a_{n-1}, ..., a_0, \beta]$, cu ajutorul Propoziţiei 5.1.6 se deduce, analog,

$$p_{n-1}\beta^2 + (q_{n-1} - p_n)\beta - q_n = 0,$$

de unde $p_{n-1}\widetilde{\beta}^2 + (q_{n-1} - p_n)\widetilde{\beta} - q_n = 0$,

$$-\widetilde{\beta}^2(q_n(-\frac{1}{\widetilde{\beta}})^2 + (q_{n-1} - p_n)(-\frac{1}{\widetilde{\beta}}) - p_{n-1}) = 0$$

şi, deoarece ecuaţia (16) are o singură rădăcină pozitivă, $\alpha = -\frac{1}{\widetilde{\beta}}$. ■

Cele mai simple iraţionale pătratice sunt cele de forma $\sqrt{D}$, unde $D \in \mathbf{Q}_+$ şi $\sqrt{D} \notin \mathbf{Q}$. Fracţiile lor continue, în cazul $D > 1$, au proprietăţi remarcabile:

Propoziţia 5.3.7. *Fie* $D \in \boldsymbol{Q}, D > 1, \sqrt{D} \notin \boldsymbol{Q}$. *Atunci*

$$\sqrt{D} = [a_0; \overline{a_1, ..., a_n, 2a_0}].$$

In plus, partea $a_1, a_2, ..., a_n$ *a perioadei este simetrică, adică* $a_k = a_{n+1-k}$, *pentru* $1 \leq k \leq n$.

Demonstraţie. Avem $a_0 = [\sqrt{D}]$, deci $\alpha = a_0 + \sqrt{D} > 1$ şi $\widetilde{\alpha} = a_0 - \sqrt{D} \in (-1, 0)$, deci α este i.p.r. şi $[\alpha] = 2a_0$, deci $\alpha = [\overline{2a_0; a_{01}, ..., a_n}]$. Deducem de aici că: $\sqrt{D} = [a_0; \overline{a_1, ..., a_n, 2a_0}]$ şi, încă, $-a_0 + \sqrt{D} = [0; \overline{a_1, ..., a_n, 2a_0}]$, de unde $\beta \overset{not}{=} \frac{1}{-a_0 + \sqrt{D}} = [a_1; \overline{a_2, ..., a_n, 2a_0}]$.

Folosind Propoziţia 5.3.3, 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 şi reciproca:

Dacă $\alpha = [a_0; \overline{a_1, ..., a_n, 2a_0}], (a_0 \geq 1)$, unde $a_k = a_{n+1-k}$, atunci $\alpha + a_0 = \overline{[2a_0; a_1, ..., a_n]}$ şi $\frac{1}{\alpha - a_0} = \overline{[a_1; a_2, ..., a_n, 2a_0]} = \overline{[a_n; a_{n-1}, ..., a_1, 2a_0]}$ şi, din Propoziţia 5.3.3, vom avea $\alpha + a_0 = (-\alpha + a_0)^{\sim}$, deci $\alpha = -\widetilde{\alpha}$, adică în scrierea $\alpha = \frac{P + \sqrt{D}}{Q}$, avem $\frac{P + \sqrt{D}}{Q} = \frac{-P + \sqrt{D}}{Q}$, de unde $P = 0$, deci $\alpha = \sqrt{\frac{\sqrt{D}}{Q^2}}$. ■

Pe noi ne interesează informaţia pe care ne-o dă Propoziţia 5.3.7 despre fracţia continuă a lui $\sqrt{D}$ în cazul $D \in \mathbf{N}$, cu $\sqrt{D} \notin \mathbf{Q}$.

Exemple 1. Să dezvoltăm în fracţie continuă numărul $\alpha = \sqrt{5}$.

Avem $a_0 = 2, \alpha_1 = \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2$,

$a_1 = 4, \alpha_2 = \frac{1}{\alpha_1} - a_1 = \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 = \alpha_1$, deci $\sqrt{5} = [2; \overline{4}]$.

2. Să găsim fracţia continuă a lui $\sqrt{7}$.

$a_0 = 2, \alpha_1 = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3}$

$a_1 = 4, \alpha_2 = \frac{3}{\sqrt{7} - 1} = \frac{3(\sqrt{7} + 1)}{6} = \frac{\sqrt{7} + 1}{2}$

$a_2 = 1, \alpha_3 = \frac{2}{\sqrt{7} - 1} = \frac{2(\sqrt{7} + 1)}{6} \frac{\sqrt{7} + 1}{3}$

$a_3 = 1, \alpha_4 = \frac{3}{\sqrt{7} - 2} = \frac{3(\sqrt{7} + 2)}{3} = \sqrt{7} + 2$

$a_4 = 4, \alpha_5 = \frac{1}{\sqrt{7} - 1} = \alpha_1$, deci $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$.

Acest şir poate fi destul de lung:

$\sqrt{991} = [31; \overline{2, 12, 10, 2, 2, 2, 1, 1, 2, 6, 1, 1, 1, 1, 3, 1, 8, 4, 1, 2, 1, 2, 3, 1, 4, 1, 20, 6, 4, 31, 4, 6, 20, 1, 4, 1, 3, 2, 1, 4, 8, 1, 3, 1, 1, 1, 1, 2, 1, 1, 2, 2, 2, 10, 12, 2, 62}]$.

In continuăre vom pune în evidenţă un algoritm de dezvoltare a lui $\alpha = \sqrt{D}$ în fracţie continuă (cu $D \in \mathbf{N}^*$ astfel încât $\alpha \notin Q$).

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 obţinem: $a_1 = [\alpha_1]$ şi $\alpha_1 = a_1 + \frac{1}{\alpha_1}$, deci

$$\begin{aligned} \alpha_2 &= \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{\sqrt{D} + b_1}{c_1} - a_1} = \frac{c_1}{\sqrt{D} + b_1 - a_1 c_1} = \frac{c_1(\sqrt{D} + a_1 c_1 - b_1)}{D - (a_1 c_1 - b_1)^2} \\ &= \frac{c_1(\sqrt{D} + a_1 c_1 - b_1)}{D - b_1^2 - a_1^2 c_1^2 + 2a_1 b_1 c_1} = \frac{\sqrt{D} + a_1 c_1 - b_1}{1 - a_1^2 c_1 + 2a_1 b_1} = \frac{\sqrt{D} + b_2}{c_2} \end{aligned}$$

unde $b_2 = a_1 c_1 - b_1$ şi $c_2 = 1 - a_1^2 c_1 + 2a_1 b_1$.

Pentru $n \in \mathbf{N}, n \geq 2$, fie $b_{n+1} = a_n c_n - b_1$ şi $c_{n+1} = c_{n-1} - a_1^2 c_n + 2a_n b_n$ şi să arătăm că pentru $n \geq 2$:

$$(1) \qquad D - b_n^2 = c_{n-1} c_n.$$

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:

$D-b_{n+1}^2 = D-(a_nc_n-b_n)^22 = D-b_n^2-a_n^2c_n^2+2a_nb_nc_n = c_{n-1}c_n-a_n^2c_n^2+2a_nb_nc_n = c_n(c_{n-1} - a_n^2c_n + +2a_nb_n) = c_nc_{n+1}$ şi astfel (1) este adevărată pentru orice $n \geq 2$.

Să arătăm acum că pentru orice $n \geq 1$

$$(2) \qquad \alpha_n = \frac{\sqrt{D} + b_n}{c_n}$$

După calculele de la început avem că (2) se verifică pentru $n = 1, 2$.

Dacă presupunem că (2) este verificată pentru n, atunci:

$$\begin{aligned} \alpha_{n+1} &= \frac{1}{\alpha_n - a_n} = \frac{1}{\frac{\sqrt{D} + b_n}{c_n} - a_n} = \frac{c_n}{\sqrt{D} + b_n - a_nc_n} = \frac{c_n(\sqrt{D} + a_nc_n - b_n)}{D - (a_nc_n - b_n)^2} \\ &= \frac{c_n(\sqrt{D} + b_{n+1})}{c_nc_{n+1}} = \frac{\sqrt{D} + b_{n+1}}{c_{n+1}} \end{aligned}$$

(am ţinut cont şi de (1)), astfel că (2) este adevărată pentru orice $n \in \mathbf{N}$.

In mod evident $c_1 \in \mathbf{N}$. Atunci $b_1 = a_0 = [\sqrt{D}] < \sqrt{D}$ şi astfel $0 < \sqrt{D} - b_1 < 1$, deci $0 < \frac{\sqrt{D} - b_1}{c_1} < 1$. Cum $\alpha_1 > 1$ deducem că $\frac{\sqrt{D} + b_1}{c_1} > 1$. Astfel $0 < \frac{\sqrt{D} - b_1}{c_1} < 1 < \frac{\sqrt{D} + b_1}{c_1}$.

Să arătăm acum că pentru orice $n \in \mathbf{N}^*$

$$(3) \qquad 0 < \frac{\sqrt{D} - b_n}{c_n} < 1 < \frac{\sqrt{D} + b_n}{c_n}$$

(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

$$\frac{\sqrt{D} - b_{n+1}}{c_{n+1}} = \frac{\sqrt{D} - b_{n+1}^2}{c_{n+1}(\sqrt{D} + b_{n+1})} = \frac{c_n}{\sqrt{D} + b_{n+1}} = \frac{c_n}{\sqrt{D} + a_nc_n - b_n} = \frac{1}{\frac{\sqrt{D} - b_n}{c_n} + a_n}$$

de unde deducem că $0 < \frac{\sqrt{D} - b_{n+1}}{c_{n+1}} < 1$ (ţinând cont şi de ipoteza de inducţie).

Astfel (3) este adevărată pentru orice $n \in \mathbf{N}$.

Dacă $c_n < 0$ pentru un anumit $n \in \mathbf{N}$, 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 $n \in \mathbf{N}^*$.

In consecinţă $\sqrt{D} - b_n < c_n < \sqrt{D} + b_n$, deci $\sqrt{D} - b_n < \sqrt{D} + b_n$ şi astfel $b_n > 0$ pentru orice $n \in \mathbf{N}^*$.

Din (3) deducem că $b_n < \sqrt{D}$ şi astfel $c_n < \sqrt{D} + b_n < 2\sqrt{D}$. Din observaţia 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 diferiţi, fiecare dintre aceştia fiind mai mici decât $2D$. Astfel, cel puţin doi termeni ai şirului $(\alpha_n)_{n\geq 1}$ sunt egali.

Deci există $k, s \in \mathbf{N}$ astfel încât $k, s < 2D$ şi (4) $\alpha_k = \alpha_{k+s}$. Deoarece $\alpha_{n+1} = \frac{1}{\alpha_n - [\alpha_n]}$ pentru $n \geq 1$, din (4) deducem că $\alpha_{k+1} = \alpha_{k+s+1}$ şi mai general, $\alpha_n = \alpha_{n+s}$ pentru $n \geq k$.

Astfel, şirurile $(\alpha_n)_{n\geq 1}$ şi $(a_n)_{n\geq 1}$ sunt periodice (căci $a_n = [\alpha_n]$ pentru $n \geq 1$).

Fie (5) $\alpha'_n = \frac{\sqrt{D}-b_n}{c_n}$ pentru $n \geq 1$; ţinând cont de (1) deducem imediat că $a_n = [\frac{1}{x'_{n+1}}]$ pentru orice $n \geq 1$.

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 $n \in \mathbf{N}^*$.

Deducem imediat formulele:

$$\alpha_1 = a_1 + \frac{1|}{|a_2} + ... + \frac{1|}{|a_s} + \frac{1|}{|\alpha_1} \text{ şi } \frac{1}{\alpha'_1} = a_s + \frac{1|}{|a_{s-1}} + ... + \frac{1|}{|a_1} + \frac{1|}{|\frac{1}{x'_1}}.$$

Deoarece $\alpha_1 > 1$ şi $\frac{1}{\alpha'_1} > 1$ aceste ultime relaţii 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 $x \in \mathbf{R}$ şi $k \in \mathbf{N}^*$, atunci $[\frac{x}{k}] = [\frac{[x]}{k}]$ 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 $D \in \mathbf{N}^*$ astfel încât $\sqrt{D} \notin \mathbf{Q}$) în fracţie continuă.

Alegem $a_0 = [\sqrt{D}], b_0 = 0, c_0 = 1$ şi apoi construim şirurile $(a_n)_{n\geq 0}, (b_n)_{n\geq 0}$ şi $(c_n)_{n\geq 0}$ cu ajutorul recurenţelor :

$$(6) \qquad \begin{cases} a_n = [\frac{a_0+b_n}{c_n}] \\ b_n = a_{n-1}c_{n-1} - b_{n-1}, \text{ pentru } n \geq 1. \\ c_n = \frac{D-b_n^2}{c_{n-1}} \end{cases}$$

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 $\sqrt{D} = [a_0; \overline{a_1, ..., a_s}]$.

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 $D \in \mathbf{N}^*$ astfel încât $\sqrt{D} \notin \mathbf{Q}$) 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: (6) $b_n = a_{n-1}c_{n-1} - b_{n-1}, c_n = \frac{D - b_n^2}{c_{n-1}}, a_n = [c_n = \frac{a_0 + b_n}{c_n}]$, 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 $\sqrt{D} = [a_0; \overline{a_1, ..., a_{n-1}, a_n, a_{n-1}, ..., a_1, 2a_0}]$ (adică lungimea perioadei minime este pară).

Dacă $c_{n+1} = c_n$, atunci $\sqrt{D} = [a_0; \overline{a_1, ..., a_n, a_n, ..., a_1, 2a_0}]$ (adică lungimea perioadei minime este impară).

Numerele $b_n, c_n \in \mathbf{N}$ 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) avem:

$b_1 = a_0c_0 - b_0 = a_0 = 31, c_1 = \frac{1009 - b_1^2}{c_0} = \frac{1009 - 31^2}{1} = 48, a_1 = [\frac{a_0 + b_1}{c_1}] = [\frac{31 + 31}{48}] = 1$.

Apoi: $b_2 = a_1c_1 - b_1 = 17, c_2 = \frac{1009 - b_2^2}{c_1} = 15, a_2 = [\frac{a_0 + b_2}{c_2}] = [\frac{31 + 17}{17}] = 3$.

Aplicând din nou recurenţele (6) 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 $a \in \mathbf{N}, a \geq 3, D = a^2 - 2$ 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, $b_1 = a_0 = a - 1, c_1 = D - a_0^2 = a^2 - 2 - (a-1)^2 = 2a - 3, a_1 = [\frac{a_0 + b_1}{c_1}] = [\frac{2a - 2}{2a - 3}] = [1 + \frac{1}{2a - 3}] = 1$.

Continuăm, $b_2 = a_1c_1 - b_1 = 2a - 3 - (a-1) = a - 2, c_2 = \frac{D - b_2^2}{c_1} = \frac{a^2 - 2 - (a-2)^2}{2a - 3} = \frac{4a - 6}{2a - 3} = 2, a_2 = [\frac{a_0 + b_2}{c_2}] = [\frac{a - 1 + a - 2}{2}] = [a - \frac{3}{2}] = a - 2$.

Apoi $b_3 = a_2c_2 - b_2 = (a-2)^2 - (a-2) = a - 2, c_3 = \frac{D - b_3^2}{c_2} = \frac{a^2 - 2 - (a-2)^2}{2} = \frac{4a - 6}{2} = 2a - 3, a_3 = [\frac{a_0 + b_3}{c_3}] = [\frac{a - 1 + a - 2}{2a - 3}] = 1$;

$b_4 = a_3c_3 - b_3 = 2a - 3 - (a-2) = a - 1, c_4 = \frac{D - b_4^2}{c_3} = \frac{a^2 - 2 - (a-1)^2}{2a - 3} = 1, a_4 = [\frac{a_0 + b_4}{c_4}] = [\frac{a - 1 + a - 1}{1}] = 2a - 2$.

In sfârşit, $b_5 = a_4c_4 - b_4 = 2a - 2 - (a-1) = a - 1 = b_4, c_5 = \frac{D - b_5^2}{c_4} = \frac{a^2 - 2 - (a-1)^2}{1} = 2a - 3 = c_1$.

Din cele expuse mai înainte avem $s = 4$, astfel că $\sqrt{a^2 - 2} = [a-1; \overline{1, a-2, 1, 2a-2}]$.

Analog se obţine $\sqrt{a^2 + 1} = [a; \overline{2a}]$ şi $\sqrt{a^2 + 2} =]a; \overline{a, 2a}]$ pentru orice $a \in \mathbf{N}$.

Observaţie. Acest paragraf a fost redactat în cea mai mare parte după lucrarea [16].

Capitolul 6

Teoreme de reprezentare pentru numere întregi

6.1 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 $d \equiv a(\text{mod}4)$. 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 ($k \in \mathbf{N}$).

Conform teoremei fundamentale a aritmeticii pe n îl putem scrie sub forma $n = 2^k \cdot n_1 \cdot n_2$ cu $k \in \mathbf{N}$, $n_1 = \prod_{\substack{p \text{ prim} \\ p \equiv 1(\text{mod } 4)}} p^r$ iar $n_2 = \prod_{\substack{q \text{ prim} \\ q \equiv 3(\text{mod } 4)}} q^s$.

In cadrul acestui paragraf vom da răspuns la următoarele chestiuni:

P_1. Pentru care numere naturale n există $x, y \in \mathbf{Z}$ astfel încât $n = x^2 + y^2$ $(*)$.

P_2. In caz că pentru n fixat ecuaţia $(*)$ are cel puţin o soluţie atunci să se determine numărul tuturor soluţiilor sale.

Observaţie. Dacă ecuaţia $(*)$ are o soluţie (x, y) în $\mathbf{N} \times \mathbf{N}$, atunci în $\mathbf{Z} \times \mathbf{Z}$ ecuaţia $(*)$ va avea soluţiile $(\pm x, \pm y)$.

Astfel

i) Dacă $x = y = 0$ atunci cu necesitate $n = 0$ şi ecuaţia $(*)$ are o unică soluţie: $(0, 0)$;

ii) Dacă $x \neq 0$ şi $y = 0$ atunci soluţia $(x, 0)$ din $\mathbf{N} \times \mathbf{N}$ generează patru soluţii în $\mathbf{Z} \times \mathbf{Z}$ şi anume: $(x, 0), (0, x), (-x, 0)$ şi $(0, -x)$;

iii) Dacă $x = 0$ şi $y \neq 0$ atunci soluţia $(0, y)$ din $\mathbf{N} \times \mathbf{N}$ generează de asemenea patru soluţii în $\mathbf{Z} \times \mathbf{Z}$ 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 $\mathbf{N} \times \mathbf{N}$ generează opt soluţii în $\mathbf{Z} \times \mathbf{Z}$ 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 $\mathbf{N} \times \mathbf{N}$ generează patru soluţii în $\mathbf{Z} \times \mathbf{Z}$ 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 $(*)$, trebuie să specificăm neapărat urmatoarele:

a) Dacă este vorba de numărul de soluţii din $\mathbf{N} \times \mathbf{N}$ sau din $\mathbf{Z} \times \mathbf{Z}$;

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 $\mathbf{N} \times \mathbf{N}$: $(1, 0)$ şi $(0, 1)$ pe când în $\mathbf{Z} \times \mathbf{Z}$ 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 $\mathbf{N} \times \mathbf{N}$ (pe $(1, 0)$) pe când în $\mathbf{Z} \times \mathbf{Z}$ are două soluţii (pe $(1, 0)$ şi $(-1, 0)$).

2. Ecuaţia $x^2 + y^2 = 2$ are în $\mathbf{N} \times \mathbf{N}$ o soluţie unică şi anume pe $(1, 1)$, pe când în $\mathbf{Z} \times \mathbf{Z}$ 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 $\mathbf{Z} \times \mathbf{Z}$ trei soluţii şi anume: $(1, 1), (-1, 1)$ şi $(-1, -1)$.

3. Ecuaţia $x^2 + y^2 = 5$ are în $\mathbf{N} \times \mathbf{N}$ două soluţii: $(1, 2)$ şi $(2, 1)$ pe când în $\mathbf{Z} \times \mathbf{Z}$ 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 $\mathbf{N} \times \mathbf{N}$ (pe $(1, 2)$) pe când în $\mathbf{Z} \times \mathbf{Z}$ are patru soluţii: $(1, 2), (-1, 2), (1, -2)$ şi $(-1, -2)$.

Lema 6.1.1. *Dacă p este un număr prim de forma 4k+1, atunci*

$$[(\frac{p-1}{2})!]^2 + 1 \equiv 0 (\text{mod } p).$$

Demonstraţie. Scriind că

$$(p-1)! = (1 \cdot 2 \cdot ... \cdot \frac{p-1}{2})[\frac{p+1}{2} \cdot ... \cdot (p-1)] = (\frac{p-1}{2})![\frac{p+1}{2} \cdot ... \cdot (p-1)]$$

deducem imediat egalităţile modulo p:

$$(p-1)! = (\frac{p-1}{2})!(-1)^{\frac{p-1}{2}}(\frac{p-1}{2})! = [(\frac{p-1}{2})!]^2.$$

Conform teoremei lui Wilson $(p-1)! + 1 \equiv 0 (\text{mod } p)$, astfel că $[(\frac{p-1}{2})!]^2 + 1 \equiv 0 (\text{mod } p)$. ■

Lema 6.1.2. *(Thue) Dacă $p \in \mathbf{N}$ este un număr prim iar $a \in \mathbf{Z}$ astfel încât $p \nmid a$, atunci există numerele naturale nenule $x, y < \sqrt{p}$ astfel încât la o alegere convenabilă a semnelor + sau - să avem $ax \pm y \equiv 0 (mod\ p)$.*

Demonstraţie. Dacă $m = [\sqrt{p}]$, atunci $(m+1)^2 > p$ şi considerăm mulţimea $X = \{ax - y : 0 \leq x, y \leq m\}$. Cum $|X| = (m+1)^2 > p$, rezultă că există două perechi diferite $(x_1, y_1), (x_2, y_2) \in X$ cu $x_1 \geq x_2$ şi $p \mid (ax_1 - y_1) - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$.

Egalitatea $x_1 = x_2$ este imposibilă, căci în caz contrar ar rezulta că $p \mid y_1 - y_2$ (lucru imposibil căci $0 \leq y_1, y_2 \leq m \leq \sqrt{p} < p$). De asemenea, egalitatea $y_1 = y_2$ este imposibilă, căci în caz contrar ar rezulta $p \mid a(x_1 - x_2)$, deci $p \mid x_1 - x_2$ - imposibil (căci $0 \leq x_1, x_2 \leq m \leq \sqrt{p} < p$).

Deci $x = x_1 - x_2 \in \mathbf{N}^*$ (dacă $x < 0$, atunci notăm $x = x_2 - x_1$) şi cum $y_1 - y_2 \in \mathbf{Z}^*$, există o alegere convenabilă a semnelor + sau - astfel încât $y = \pm(y_1 - y_2) \in \mathbf{N}^*$.

Cum $x = x_1 - x_2 \leq x_1 \leq m < \sqrt{p}$, 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. ■

Teorema 6.1.3. *(Fermat) Orice număr prim p de forma 4k+1 se poate scrie ca suma pătratelor a două numere naturale.*

Demonstraţie. Considerăm $a = (\frac{p-1}{2})!$. Evident, $a \in \mathbf{N}^*$ şi $(a, p) = 1$.

Conform Lemei 6.1.2, există o alegere convenabilă a semnelor + şi - astfel încât $ax \pm y \equiv 0 (\text{mod } p)$. Atunci $a^2x^2 - y^2 = (ax + y)(ax - y) \equiv 0 (\text{mod } p)$ şi conform Lemei 6.1.1 $a^2 + 1 \equiv 0 (\text{mod } p)$, de unde deducem că $a^2x^2 + x^2 \equiv 0 (\text{mod } p)$ iar de aici că $(a^2x^2 + x^2) - (a^2x^2 - y^2) = x^2 + y^2 \equiv 0 (\text{mod } p)$, adică putem scrie $x^2 + y^2 = kp$ cu $k \in \mathbf{N}^*$.

Cum $x, y < \sqrt{p}$ deducem că $x^2 + y^2 < 2p$, adică $kp < 2p$, deci $k < 2$, adică $k = 1$ (căci $x, y \in \mathbf{N}^*$). Deducem că $p = x^2 + y^2$ şi astfel Teorema lui Fermat este complet demonstrată. ■

Corolar 6.1.4. *Dacă $n \in \boldsymbol{N}^*$ conţine 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 $x, y \in \boldsymbol{N}$.*

Demonstraţie. Totul rezultă din Teorema 6.1.3 şi din aceea că un produs finit de expresii de forma $x^2 + y^2$ este de aceeaşi formă (conform identităţii $(x^2 + y^2)(z^2 + t^2) = (xz + yt)^2 + (xt - yz)^2$). ■

Vom demonstra acum că scrierea unui număr natural ca sumă de două pătrate de numere naturale este unică, dacă nu ţinem cont de ordinea termenilor.

In fapt, vom demonstra o propoziţie mai generală :

Propozitia 6.1.5. *Fie $a, b \in \boldsymbol{N}$. Dacă un număr natural prim p se scrie sub forma $p = ax^2 + by^2$ cu $x, y \in \boldsymbol{N}$, atunci aceasta scriere este unică (cu conventia că în cazul în care $a = b = 1$ să nu ţinem cont de ordinea termenilor).*

Demonstraţie. Să presupunem că p are două descompuneri: $p = ax^2 + by^2 = ax_1^2 + by_1^2$ cu $x, y, x_1, y_1 \in \mathbf{N}$.

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 $(axx_1 + byy_1)(xy_1 + yx_1) = (ax^2 + by^2)x_1y_1 + (ax_1^2 + by_1^2)xy = p(x_1y_1 + xy)$ 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). ■

Observaţii.

1. Din propoziţia de mai înainte deducem că dacă numărul natural n poate fi reprezentat în cel puţin două moduri diferite ca sumă de două pătrate de numere naturale (cu condiţia să nu considerăm diferite descompunerile ce se deosebesc numai prin ordinea termenilor), atunci cu necesitate n nu este prim.

De exemplu, din egalităţile $2501 = 1^2 + 50^2 = 10^2 + 49^2$ 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 uşurinţă că numerele 10, 18 şi 45 au descompuneri unice sub forma $10 = 12 + 3^2, 18 = 3^2 + 3^2, 45 = 3^2 + 6^2$ şi totuşi ele nu sunt numere prime (se subântelege că nu am ţinut cont de ordinea termenilor).

Putem acum răspunde la chestiunea P_1 formulată la începutul paragrafului:

Teorema 6.1.6. *(Fermat-Euler) 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 $x, y \in \boldsymbol{N}$ dacă şi numai dacă toţi exponenţii s din scrierea lui n_2 sunt numere pare.*

Demonstraţie. Revenim la scrierea lui n sub forma $n = 2kn_1n_2$ cu $k \in \mathbf{N}$, $n_1 = \prod_{\substack{p \text{ prim} \\ p \equiv 1 (\mathrm{mod}\ 4)}} p^r$ şi $n_2 = \prod_{\substack{q \text{ prim} \\ q \equiv 3 (\mathrm{mod}\ 4)}} q^s$.

Cum $2 = 1^2 + 1^2$ iar conform Teoremei 6.1.3 fiecare factor prim $p \equiv 1 (\mathrm{mod}\ 4)$ din scrierea lui n_1 se scrie sub forma $x^2 + y^2$ cu $x, y \in \mathbf{N}$ deducem imediat că n_1 se poate scrie sub aceeaşi formă şi aceeaşi proprietate o va avea şi $2^k n_1$ (adică $2^k n_1 = z^2 + t^2$ cu $z, t \in \mathbf{N}$).

Dacă presupunem că fiecare exponent s din scrierea lui n_2 este par, atunci în mod evident $n_2 = m^2$ cu $m \in \mathbf{N}$ şi atunci $n = 2^k n_1 n_2 = (z^2 + t^2)m^2 = (zm)^2 + (tm)^2$.

Reciproc, fie $n \in \mathbf{N}$ ce se poate scrie sub forma $n = x^2 + y^2$ cu $x, y \in \mathbf{N}$ şi să demonstrăm că dacă q^s este cea mai mare putere a unui număr prim $q \equiv 3 (\mathrm{mod}\ 4)$ 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 $d^2 \mid n$ şi dacă notăm $x_1 = \frac{x}{d}$ şi $y_1 = \frac{y}{d}, n_1 = \frac{n}{d^2}$, obţinem 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 împărţit egalitatea $n = x^2 + y^2$) conţine eventual o putere pară a lui q, deducem că $q \mid n_1$ 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 $\mathbf{Z}_q$ deducem că $0 = x_1^2 + y_1^2$ şi cum am presupus că $q \nmid y_1$ deducem că $0 = x_1^2(y_1^{-1})^2 + 1 \Leftrightarrow (x_1 y_1^{-1})^2 = -1$ de unde $(\frac{-1}{q}) = (\frac{(x_1 y_1^{-1})^2}{q}) = 1$.

Insă în cadrul Capitolului 4 am stabilit că $(\frac{-1}{q}) = (-1)^{\frac{q-1}{2}}$ şi cum $q \equiv 3(\text{mod } 4)$ deducem că $\frac{q-1}{2}$ este impar, astfel că $(\frac{-1}{q}) = -1$, absurd.

Deci s este par. Raţionând inductiv deducem că toţi exponenţii 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, $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$. Se cunoaşte faptul că $(\mathbf{Z}[i], +, \cdot)$ este un inel comutativ în care $U(\mathbf{Z}[i], +, \cdot) = \{\pm 1, \pm i\}$, precum şi faptul că elementele prime din $\mathbf{Z}[i]$ sunt (până la o multiplicare cu ± 1 sau $\pm i$) urmatoarele:

(i) $1 \pm i$;

(ii) Numerele prime p din $\mathbf{N}$ cu $p \equiv 3(\text{mod } 4)$;

(iii) Numerele de forma $a + bi$ cu $a, b \in \mathbf{N}^*$ şi $a^2 + b^2 = p$, unde p este un număr natural prim şi $p \equiv 1(\text{mod } 4)$.

Reamintim că descompunerea numerelor din $\mathbf{Z}[i]$ în factori primi este unică (în ipoteza că nu se ţine seama de multiplicările cu $\pm 1, \pm i$, şi de ordinea factorilor).

Pentru $z = a + bi \in \mathbf{Z}[i]$ definim *norma* lui z prin $N(z) = a^2 + b^2$. Evident, dacă $N(z) = p$ cu p prim, $p \equiv 1(\text{mod } 4)$, atunci $a \neq b$ (căci în caz contrar $p = 2a^2 \equiv 0(\text{mod } 2)$).

Fie acum $n \in \mathbf{N}$ scris sub forma $n = 2^k n_1 n_2$ cu $k \in \mathbf{N}, n_1 = \prod_{\substack{p \text{ prim} \\ p \equiv 1(\text{mod } 4)}} p^r$ iar $n_2 = \prod_{\substack{q \text{ prim} \\ q \equiv 3(\text{mod } 4)}} q^s$.

Atunci descompunerea lui n în factori primi în $\mathbf{Z}[i]$ va fi:

$$n = [(1+i)(1-i)]^k n_1 \cdot \prod_{\substack{a^2+b^2=p \\ p \text{ prim} \\ p \equiv 1(\text{mod } 4)}} [(a+bi)(a-bi)]^r \cdot \prod_{\substack{q \text{ prim} \\ q \equiv 3(\text{mod } 4)}} q^s \text{ (unde}$$

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 $u, v \in \mathbf{Z}$) îi corespund pentru $u + iv$ şi $u - iv$ descompuneri de forma:

$$(*) \qquad u + iv = i^t \cdot (1+i)^{k_1}(1-i)^{k_2} \cdot \prod [(a+bi)^{r_1}(a-bi)^{r_2}] \cdot q^{s_1}$$

$$(**) \qquad u + iv = i^{-t} \cdot (1+i)^{k_2}(1-i)^{k_1} \cdot \prod [(a+bi)^{r_2}(a-bi)^{r_1}] \cdot q^{s_2}$$

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 $u, v \in \mathbf{Z}$ dată de relaţiile $(*)$ şi $(**)$ 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 6.1.6).

Pentru alegerea lui t avem 4 posibilităţi (căci $t \in \{0,1,2,3\}$). Pentru k_1 avem $k+1$ posibilităţi de alegere (căci $k_1 \in \{0,1,...,k\}$) 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 $\mathbf{Z}[i]$) (unde produsul $\prod(r+1)$ se face după toţi primii $p \equiv 1(\text{mod } 4)$ astfel încât $p^r \mid n$).

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 $\prod_{\substack{p \text{ prim} \\ p^r \mid n}} (1+r) = d(n_1)$ (căci $n_1 = \prod_{\substack{p \text{ prim} \\ p \equiv 1(\text{mod } 4)}} p^r$).

Din cele de mai înainte deducem că numărul total de soluţii întregi ale ecuaţiei $x^2+y^2 = n$ este $4d(n_1)$.

Să aratăm 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

$$(***) \qquad \sum_{\substack{0 \le m_i \le r_i \\ 0 \le k_j \le s_j}} p_1^{m_1}\cdot ... \cdot p_n^{m_n} \cdot q_1^{k_1} \cdot ... \cdot q_t^{k_t} = \prod_{\substack{p^r \mid n \\ p \equiv 1(\text{mod } 4)}} (1+p+...+p^r) \cdot \prod_{\substack{q^s \mid n \\ q \equiv 3(\text{mod } 4)}} (1+q+...+q^s).$$

Dacă $d|n$, atunci este clar că avem $d \equiv 1(\text{mod } 4)$ dacă şi numai dacă în $(***)$ $\sum_{j=1}^{t} k_j$ este par, în caz contrar având $d \equiv 3(\text{mod } 4)$.

Dacă înlocuim pe q cu -1 atunci produsul $\prod_{\substack{q^s \mid n \\ q \equiv 3(\text{mod } 4)}} (1+q+...+q^s)$ este

zero chiar dacă un singur exponent s este impar; dacă toţi aceşti exponenţi s sunt pari atunci $\prod_{\substack{q^s \mid n \\ q \equiv 3(\text{mod } 4)}} (1+q+...+q^s) = 1$ şi astfel membrul drept din $(***)$ devine $\prod_{\substack{p^r \mid n \\ p \equiv 1(\text{mod } 4)}} (1+p+...+p^r)$ astfel că termenii dezvoltării acestui produs sunt exact toţi divizorii lui n_1. Pentru a obţine $d(n_1)$ fiecare termen trebuie să fie numărat ca 1. Acest lucru este uşor de realizat dacă în $(***)$ înlocuim în partea dreaptă şi pe p cu 1, obţinând $\prod_{\substack{p^r \mid n \\ p \equiv 1(\text{mod } 4)}} (1+r)$. Dacă privim acum membrul stâng al egalităţii $(***)$ după ce în partea dreaptă am înlocuit fiecare p cu 1 şi fiecare q cu -1 este clar că fiecare $d \mid n, d \equiv 1(\text{mod } 4)$ este numărat ca +1 şi fiecare $d \mid n, d \equiv 3(\text{mod } 4)$ este numărat ca -1.

Astfel, membrul stâng din $(***)$ 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 6.1.6 (Fermat-Euler) :

Teorema 6.1.7. *Fie $n \in \boldsymbol{N}^*$ iar $n = 2^k n_1 n_2$ (cu $k \in \boldsymbol{N}, n_1 = \prod_{\substack{p \text{ prim}, p \mid n \\ p \equiv 1(mod\ 4)}} p^r$ iar $n_2 = \prod_{\substack{q \text{ prim}, q \mid n \\ q \equiv 3(mod\ 4)}} q^s$) descompunerea lui n în factori primi.*

Atunci ecuaţia $x^2 + y^2 = n$ are soluţie în $\boldsymbol{Z}$ dacă şi numai dacă toţi exponenţii s din descompunerea lui n_2 sunt pari.

Numărul soluţiilor din $\boldsymbol{Z} \times \boldsymbol{Z}$ 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 $d \equiv a(mod\ 4), a = 1, 3$.

Exemple.

1. Dacă $n = 1$, atunci $d_1(1) = 1$ şi $d_3(1) = 0$, astfel că în $\mathbf{Z} \times \mathbf{Z}$ ecuaţia $x^2 + y^2 = 1$ va avea 4(1-0)=4 soluţii.

2. Dacă $n = 2$, atunci $d_1(2) = 1$ şi $d_3(2) = 0$, astfel că în $\mathbf{Z} \times \mathbf{Z}$ ecuaţia $x^2 + y^2 = 2$ va avea 4(1-0)=4 soluţii.

3. Dacă $n = 5$, atunci $d_1(5) = 2$ şi $d_3(5) = 0$, astfel că în $\mathbf{Z} \times \mathbf{Z}$ 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 6.1.3) că dacă p este un număr prim de forma $4k + 1$, atunci există $x, y \in \mathbf{N}^*$ astfel încât $p = x^2 + y^2$(cum $d_1(p) = 2$ iar $d_3(p) = 0$, conform Teoremei 6.1.7 ecuaţia $x^2 + y^2 = p$ va avea în $\mathbf{Z} \times \mathbf{Z}$ 4(2-0)=8 soluţii. Se reconfirmă concluzia de la observaţia de la începutul paragrafului 1, cazul iv)).

In continuare vom prezenta o metodă de găsire a numerelor x, y atunci când se dă p

(metoda dată de Lagrange în anul 1808, dupa ce, tot el demonstrase în 1785 că lungimea perioadei pentru fracţia continuă a lui $\sqrt{p}$ este impară pentru numerele prime p de forma $4k+1$).

Pentru aceasta să ne reamintim că la capitolul de fracţii continue a fost prezentat următorul algoritm de dezvoltare în fracţie continuă a unui iraţional pătratic $\alpha = \sqrt{D}$:

Punem $a_0 = [\sqrt{D}], b_0 = 0, c_0 = 1$ şi apoi construim prin recurenţă

$$a_{n+1} = [\frac{a_0 + b_{n+1}}{c_{n+1}}], b_{n+1} = a_n c_n - b_n, c_{n+1} = \frac{D - b_{n+1}^2}{c_n}.$$

Calculul se continuă până când $b_{n+1} = b_n$ sau $c_{n+1} = c_n$.

i) Dacă $b_{n+1} = b_n$, atunci $\sqrt{D} = [a_0; \overline{a_1, ..., a_{n-1}, a_n, a_{n-1}, ..., a_1, 2a_0}]$(adică lungimea perioadei minime este pară);

ii) Dacă $c_{n+1} = c_n$, atunci $\sqrt{D} = [a_0; \overline{a_1, ..., a_n, a_n, ..., a_1, 2a_0}]$(adică lungimea perioadei minime este impară).

Numerele b_n şi c_n de mai sus sunt cele din scrierea lui $\alpha_n = \frac{b_n + \sqrt{D}}{c_n}$.

Să trecem acum la rezolvarea ecuaţiei $x^2 + y^2 = p$, cu p un număr prim de forma $4k+1$ (de exemplu în $\mathbf{N} \times \mathbf{N}$).

După cum am amintit mai sus, lungimea perioadei minime pentru fracţia continuă a lui $\sqrt{p}$ este impară. Deci $\sqrt{p} = [a_0; \overline{a_1, ..., a_n, a_n, ..., a_1, 2a_0}]$.

Numărul $\alpha_{n+1} = [\overline{a_n; a_{n-1}, ..., a_1, 2a_0, a_1, ..., a_n}]$ are perioada simetrică, deci - ţinând cont de Propozitia 5.3.14 - deducem că $\alpha_{n+1} \cdot \widetilde{\alpha}_{n+1} = -1$ (notaţiile sunt cele de la Capitolul 5).

Pe de altă parte, $\alpha_{n+1} = \frac{b_{n+1} + \sqrt{p}}{c_{n+1}}$, $\widetilde{\alpha}_{n+1} = \frac{b_{n+1} - \sqrt{p}}{c_n}$ astfel că obţinem

$$\frac{b_{n+1} + \sqrt{p}}{c_{n+1}} \cdot \frac{b_{n+1} - \sqrt{p}}{c_n} = -1 \Leftrightarrow b_{n+1}^2 + c_{n+1}^2 = p$$

şi astfel (b_{n+1}, c_{n+1}) este singura soluţie din $\mathbf{N} \times \mathbf{N}$ a ecuaţiei $x^2 + y^2 = p$ (evident dacă nu ţinem cont de ordinea termenilor).

Exemplu. Să se rezolve ecuaţia $x^2 + y^2 = 1009$ în $\mathbf{N} \times \mathbf{N}$.

Evident, numărul $p = 1009$ este prim de forma $4k+1$. Avem $a_0 = 31, b_0 = 0, c_0 = 1$ şi apoi

$b_1 = a_0 c_0 - b_0 = 31, c_1 = \frac{1009 - b_1^2}{c_0} = 48, a_1 = [\frac{31 + 31}{48}] = 1,$

$b_2 = a_1 c_1 - b_1 = 17, c_2 = \frac{1009 - b_2^2}{c_1} = 15, a_2 = [\frac{31 + 17}{15}] = 3,$

$b_3 = a_2 c_2 - b_{02} = 28, c_3 = \frac{1009 - b_3^2}{c_2} = 15 = c_2$. Prin urmare suntem în cazul ii) astfel că $\sqrt{1009} = [31; \overline{1, 3, 3, 1, 62}]$ 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 $\mathbf{N} \times \mathbf{N}$ este (15, 28) (dacă nu ţinem cont de ordinea termenilor).

6.2 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 identitatea lui Euler, potrivit căreia dacă $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbf{Z}$, atunci

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2 - \\ -x_2y_1+x_3y_4-x_4y_3)^2 + (x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 + (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$$

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 6.2.1. *(Lagrange) Fie p este un număr prim; atunci:*

(1) *Există m şi $x_1, x_2, x_3, x_4 \in \boldsymbol{N}$ astfel încât $mp = x_1^2+x_2^2+x_3^2+x_4^2$ $(1 \le m < p)$;*

(2) *Dacă m este cel mai mic număr natural ce verifică (1), atunci $m = 1$.*

Demonstraţie. Pentru a proba (1), să considerăm mulţimile:

$$X = \{x^2 : x = 0, 1, 2, ..., \frac{p-1}{2}\} \text{ şi } Y = \{-x^2-1 : x = 0, 1, 2, ..., \frac{p-1}{2}\}.$$

Să observăm că elementele lui X şi Y nu sunt congruente două câte două modulo p (separat).

Intr-adevăr, dacă există $x_1, x_2 \in \{0, 1, 2, ..., \frac{p-1}{2}\}$ astfel încât $x_1^2 \equiv x_2^2 (\text{mod } p)$ cu $x_1 > x_2$ atunci $p \mid (x_1-x_2)(x_1+x_2)$ 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 $x, y \in \{0, 1, 2, ..., \frac{p-1}{2}\}$ astfel încât $x^2 \equiv -y^2-1 (\text{mod } p)$, altfel zis există $m \in \mathbf{N}$ astfel încât $mp = x^2+y^2+1$.

Clar

$$1 \le m = \frac{1}{p}(x^2+y^2+1) \le \frac{1}{p}[2(\frac{p-1}{2})^2+1] = \frac{p-1}{2}\cdot\frac{p-1}{2} + \frac{1}{p} < \frac{p-1}{2} + \frac{1}{p} < p.$$

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:

$$(\frac{x_1+x_2}{2})^2 + (\frac{x_1-x_2}{2})^2 + (\frac{x_3+x_4}{2})^2 + (\frac{x_3-x_4}{2})^2 = \frac{m}{2}\cdot p$$

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 $3 \leq m < p$.

Alegem y_1, y_2, y_3, y_4 astfel încât $x_i \equiv y_i (\text{mod } m), -\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2}, i = 1,2,3,4$ şi în mod evident $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 (\text{mod } m)$, deci $mn = y_1^2 + y_2^2 + y_3^2 + y_4^2$ pentru un anumit n. Mai mult, $0 \leq n \leq \frac{4}{m} \cdot (\frac{m-1}{2})^2 < m$.

Evident, $n \neq 0$ (căci în caz contrar ar rezulta $y_j = 0$ pentru orice $j = 1,2,3,4$, ceea ce ar implica $x_j \equiv 0 (\text{mod } m), j = 1,2,3,4$, şi deci $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 (\text{mod } m^2)$, de unde $p \equiv 0 (\text{mod } m)$, ceea ce este imposibil deoarece $3 \leq m < p$).

Deci $n \geq 1$ şi deducem imediat că $m^2np = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$, 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 $x_i \equiv y_i (\text{mod } m) (-\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2}), i = 1,2,3,4$ atunci $m \mid z_j, j = 2,3,4$ şi din egalitatea de mai sus rezultă că $m \mid z_1$.

Avem deci că $np = (\frac{z_1}{m})^2 + (\frac{z_2}{m})^2 + (\frac{z_3}{m})^2 + (\frac{z_4}{m})^2$, ceea ce din nou contrazice minimalitatea lui m(căci $n < m$).

In concluzie $m = 1$ şi totul este acum clar. ■

Corolar 6.2.2. *(Iacobi) Pentru orice număr natural n există x, y, z, t întregi astfel încât $n = x^2 + 2y^2 + 3z^2 + 6t^2$.*

Demonstraţie. Conform Teoremei 6.2.1 există $a, b, c, d \in \mathbf{Z}$ astfel încât $n = a^2 + b^2 + c^2 + d^2$. Să arătăm că modulo nişte renumerotări sau schimbări de semn, putem presupune că $3 \mid a + b + c$. Acest lucru este evident dacă cel puţin trei dintre numerele a, b, c, d sunt multiplii de 3. Presupunem că numai două dintre ele (să zicem c şi d) sunt multiplii de 3. Atunci $a \equiv \pm 1 (\text{mod } 3)$ şi $b \equiv \pm 1 (\text{mod } 3)$, deci la o alegere convenabilă a semnelor + şi - avem $3 \mid a \pm b$, deci $3 \mid a \pm b + c$. In sfârşit, dacă cel puţin 3 dintre numerele a, b, c, d(să zicem a, b, c) nu sunt divizibile cu 3, atunci la o alegere convenabilă a semnelor + şi - avem $3 \mid a \pm b \pm c$. Putem astfel presupune că $a + b + c = 3z$ cu $z \in \mathbf{Z}$. Cum pentru 3 numerre întregi cel puţin două sunt congruente modulo 2, putem presupune că $a \equiv b (\text{mod } 2)$, adică $a + b = 2k$ cu $k \in \mathbf{Z}$, deci $a - b = 2(k - b) = 2y$ cu $y \in \mathbf{Z}$. Cum avem identitatea

$$3(a^2 + b^2 + c^2) = (a + b + c)^2 + 2(\frac{a+b}{2} - c)^2 + 6(\frac{a+b}{2})^2$$

deducem că $3(a^2 + b^2 + c^2) = (a + b + c)^2 + 2(k - c)^2 + 6y^2$, de unde rezultă că $3 \mid k - c$, deci $k - c = 3t$ cu $t \in \mathbf{Z}$.

Atunci $a^2 + b^2 + c^2 = 3z^2 + 6t^2 + 2y^2$, deci $n = a^2 + b^2 + c^2 + d^2 = d^2 + 2y^2 + 3z^2 + 6t^2$. ■

6.3 Scrierea numerelor naturale sub forma $x^2 + 2y^2$

Lema 6.3.1. *Un număr prim p se scrie sub forma $p = x^2 + 2y^2$ dacă şi numai dacă $p = 2$ sau $p \equiv 1 (mod\ 8)$ sau $p \equiv 3 (mod\ 8)$.*

Demonstraţie. Pentru $p = 2$ avem $2 = 0^2 + 2 \cdot 1^2$, aşa că fie $p \geq 3$ (deci $(p, 2) = 1$)). Dacă $p = x^2+2y^2$ rezultă $(x, 2p) = 1$ şi $(y, p) = 1$, iar $x^2 \equiv -2y^2 (\text{mod } p)$. Fie $z \in \mathbf{Z}$ astfel încât $yz \equiv 1(\text{mod } p)$. Atunci $(xz)^2 \equiv -2(\text{mod } p)$ şi deci $(\frac{-2}{p}) = 1$, adică $(\frac{-1}{p})(\frac{2}{p}) = 1 \Leftrightarrow (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = 1 \Leftrightarrow \frac{p-1}{2} + \frac{p^2-1}{8} = 2k$ cu $k \in \mathbf{Z} \Leftrightarrow \frac{(p-1)(p+5)}{8} = 2k \Leftrightarrow p \equiv 1(\text{mod } 8)$ sau $p \equiv 3(\text{mod } 8)$.

Reciproc, dacă $p \equiv 1(\text{mod } 8)$ sau $p \equiv 3(\text{mod } 8)$ atunci $(\frac{-2}{p}) = 1$ şi deci există $a \in \mathbf{Z}$ astfel încât $a^2 \equiv -2(\text{mod } p)$. Din Lema lui Thue(Lema 6.1.2) deducem că există numerele întregi x şi y cu $0 < x, y < \sqrt{p}$ şi $p \mid (ax^2 - y^2)$. Atunci $p \mid (a^2+2))x^2-(2x^2+y^2)]$ şi cum $p \mid (a^2 + 2) \Rightarrow 2x^2 + y^2 = pk, 0 < 2x^2 + y^2 < 3p$ deci $k = 1$ sau $k = 2$.

Pentru $k = 1$ rezultă că $p = 2x^2 + y^2$.

Pentru $k = 2$ rezultă că $2p = 2x^2 + y^2 \Rightarrow 2 \mid y, y = 2 \Rightarrow p = x^2 + 2z^2$. ■

Lema 6.3.2. *Dacă numărul prim p este de forma $p = 8k + 5$ sau $p = 8k + 7$ iar $p \mid x^2 + 2y^2$ cu $x, y \in \boldsymbol{Z}$, atunci $p \mid x$ şi $p \mid y$.*

Demonstraţie. Dacă $p \nmid x \Rightarrow p \nmid y$, deci există $z \in \mathbf{Z}$ astfel încât $yz \equiv 1(\text{mod } p)$. Cum $x^2 \equiv -2y^2(\text{mod } p) \Rightarrow (xz)^2 \equiv -2(\text{mod } p)$. Cum $(xz, p) = 1 \Rightarrow (\frac{-2}{p}) = 1 \Rightarrow p \equiv 1(\text{mod } p)$ sau $p \equiv 3(\text{mod } p)$- absurd! Deci $p \mid x$ şi implicit $p \mid y$. ■

Teorema 6.3.3. *Fiind dat $n \in \boldsymbol{N}$, există $x, y \in \boldsymbol{Z}$ astfel încât $n = x^2 + 2y^2$ dacă şi numai dacă factorii primi ai lui n de forma $8k + 5$ şi $8k + 7$ au exponentul par.*

Demonstraţie. Fie $n = a^2b$ cu b liber de pătrate; numărul n se scrie sub forma $x^2 + 2y^2$ dacă şi numai dacă b se scrie sub aceeaşi formă. Dacă $p \equiv 5$ sau $7(\text{mod } 8)$, $p \mid b$ şi $b = x^2+2y^2$ din Lema 6.3.2 rezultă că $p \mid x$ şi $p \mid y$, adică $p^2 \mid b$ - absurd. Deci $b = \prod_{i=1}^{k} p_i$ unde $p_i = 2$ sau $p_i = 1$ sau $3(\text{mod } 8)$. Atunci, conform Lemei 6.3.1, $b = x^2+2y^2$. Rezultă în final că $n = (ax)^2 + 2(ay)^2$. ■

6.4 Alte teoreme de reprezentare a numerelor întregi

Teorema 6.4.1. *(Erdös-Suranyi) Orice număr $k \in \boldsymbol{Z}$ se poate scrie într-o infinitate de moduri sub forma $k = \pm 1^2 \pm 2^2 \pm ... \pm m^2$ cu $m \in \boldsymbol{N}$.*

Demonstraţie. Facem inducţie matematică observând că este suficient să presupunem $k \in \mathbf{N}$.

Observam că

$$\begin{aligned} 0 &= 1^2 + 2^2 - 3^2 + 4^2 - 5^2 - 6^2 + 7^2 \\ 1 &= 1^2 \\ 2 &= -1^2 - 2^2 - 3^2 + 4^2 \\ 3 &= -1^2 + 2^2 \\ 4 &= -1^2 - 2^2 + 3^2. \end{aligned}$$

Să presupunem acum că pentru un $k \in \mathbf{N}$ avem $k = \pm 1^2 \pm 2^2 \pm ... \pm m^2$.

Cum $(m+1)^2-(m+2)^2-(m+3)^2+(m+4)^2=4$, avem $k+4=\pm 1^2\pm 2^2\pm ...$ $\pm m^2+(m+1)^2-(m+2)^2-(m+3)^2+(m+4)^2$ 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. ■

In legătură cu alte tipuri de reprezentări ale numerelor întregi recomandam cititorului lucrarea lui **Emil Grosswald: Representations of Integers as Sums of Squares, Springer-Verlag, 1985.**

Printre alte rezultate, în cartea respectivă se prezintă şi urmatoarele:

Teorema 6.4.2. *Un număr natural n se poate scrie sub forma $n=x^2+y^2+z^2$, cu $x,y,z\in \boldsymbol{Z}$ dacă şi numai dacă n nu este de forma $4^k(8m+7)$ cu $k,m\in \boldsymbol{N}$.*

Demonstraţie. Pentru a păstra caracterul elementar al acestei cărţi, vom prezenta doar demonstraţia unei implicaţii: *dacă $n=4^k(8m+7)$ cu $k,m\in \boldsymbol{N}$ atunci n nu se poate scrie sub forma $n=x^2+y^2+z^2$ cu $x,y,z\in \boldsymbol{Z}$.*

Să analizăm la început cazul $k=0$ şi să presupunem prin absurd că există $x,y,z\in \mathbf{Z}$ astfel încât $8m+7=x^2+y^2+z^2$. Cum $8m+7$ este impar deducem că ori toate numerele x,y,z sunt impare, ori unul este impar şi celelalate două sunt pare. Este simplu de văzut că dacă $x\in \mathbf{Z}$ este impar atunci $x^2\equiv 1(\text{mod } 8)$, astfel că dacă x,y,z sunt impare, atunci $x^2+y^2+z^2\equiv 3(\text{mod } 8)$, deci egalitatea $8m+7=x^2+y^2+z^2$ este imposibilă.

Dacă de exemplu x este impar iar y,z sunt pare, atunci deducem imediat că că $x^2+y^2+z^2\equiv 1$ sau $5(\text{mod } 8)$, deci din nou egalitatea $8m+7=x^2+y^2+z^2$ este imposibilă.

Presupunem acum că există $k\in \mathbf{N}^*$ şi $m\in \mathbf{N}$ astfel încât $n=4^k(8m+1)$ se poate scrie sub forma $x^2+y^2+z^2$ cu $x,y,z\in \mathbf{Z}$ şi fie k_0 cel mai mic număr natural nenul cu proprietatea că există $m_0\in \mathbf{N}$ şi astfel încât $4^{k_0}(8m_0+7)=x^2+y^2+z^2$. Cum $4^{k_0}(8m_0+7)$ este par, deducem că numerele x,y,z sunt fie toate pare, fie unul par iar celelalte două impare.

Dacă $x=2x_1, y=2y_1, z=2z_1$ cu $x_1,y_1,z_1\in \mathbf{Z}$ atunci din egalitate $4^{k_0}(8m_0+7)=x^2+y^2+z^2\Rightarrow 4^{k_0-1}(8m_0+7)=x_1^2+y_1^2+z_1^2$. Ţinând cont de alegerea lui k_0 rezultă că $k_0-1=0$, adică $k_0=1$ şi atunci obţinem egalitatea $8m_0+7=x_1^2+y_1^2+z_1^2$ ceea ce este imposibil datorită primei părţi a demonstraţiei.

Dacă de exemplu x este par iar y,z sunt impare, din nou egalitate $4^{k_0}(8m_0+7)=x^2+y^2+z^2$ este imposibilă deoarece $4^{k_0}(8m_0+7)\equiv 0(\text{mod } 4)$, pe când $x^2+y^2+z^2\equiv 2(\text{mod } 4)$.

Pentru cealălaltă implicaţie (care implică printre altele rezultate superioare precum teorema lui Minkowski asupra corpului convex şi teorema lui Dirichlet privind numerele prime într-o progresie aritmetică), recomandăm cititorului lucrarea [36].■

Teorema 6.4.3. *Numărul soluţiilor întregi (x, y, z) ale ecuaţiei $x^2+y^2+z^2=n$*

este dat de $\frac{16}{\pi} \cdot \sqrt{n} \cdot L(1,\chi) \cdot q(n) \cdot P(n)$, *unde* $n = 4^a n_1, (4 \nmid n_1)$,

$$q(n) = \begin{cases} 0, \text{ dacă } n_1 \equiv 7(\text{mod } 8); \\ 2^{-a}, \text{ dacă } n_1 \equiv 3(\text{mod } 8); \\ 3 \cdot 2^{-a-1}, \text{ dacă } n_1 \equiv 1,2,5 \text{ sau } 6(\text{mod } 8). \end{cases}$$

$$P(n) = \prod_{\substack{p \text{ prim} \\ p \geq 3 \\ p^{2b} \mid n}} [1 + \sum_{j=1}^{b-1} p^{-j} + p^{-b}(1 - \frac{\overline{\frac{-n}{p^{2b}}}}{p} \cdot \frac{1}{p})^{-1}]$$

($P(n) = 1$ *dacă* n *nu conţine pătrate), iar* $L(s,\chi) = \sum_{m=1}^{\infty} \chi(m) m^{-s}$, *cu* $\chi(m) = (\frac{-4n}{m})$ *(simbolul lui Jacobi !).*

Cum şi demonstraţia acestei teoreme este destul de laborioasă, am renunţat la prezentarea ei în detaliu (cititorul interesat poate găsi această demonstraţie în cartea citată mai sus).

Teorema 6.4.4. *(H.E.Richert) Orice număr natural* $n > 6$ *se poate scrie ca sumă de diferite numere prime.*

Demonstraţie. Pentru a demonstra teorema lui Richert avem nevoie de două rezultate preliminare:

Lema 1. *Fie* $m_1, m_2, ...$ *un şir infinit crescător de numere naturale astfel încât pentru un* $k \in \boldsymbol{N}$, *(1)* $m_{i+1} \leq 2m_i$ *pentru orice* $i > k$.

Presupunem că există $a \in \boldsymbol{N}$ *şi* $r, s_{r-1} \in \boldsymbol{N}$ *astfel încât* $s_{r-1} \geq m_{k+r}$ *astfel încât fiecare dintre numerele*:

(2) $a+1, a+2, ..., a+s_{r-1}$ *este suma diferitelor numere din şirul* $m_1, m_2, ..., m_{k+r-1}$.

Atunci fiecare dintre numerele:

(3) $a+1, a+2, ..., a+s_r$ *este suma diferitelor numere din şirul* $m_1, m_2, ..., m_{k+r}$ şi mai mult, $s_r \geq m_{k+r+1}$.

Intr-adevăr, fie n un număr din şirul (3). Dacă $n \leq a + s_{r-1}$ nu mai avem ce demonstra deoarece conform ipotezei n este sumă de diferiţi termeni ai şirului $m_1, m_2, ..., m_{k+r-1}$.

Să presupunem că $n > a + s_{r-1}$. Cum $s_{r-1} \geq m_{k+r}$, avem $n \geq a + 1 + m_{k+r}$, deci $n - m_{k+r} \geq a + 1$, adică numărul $n - m_{k+r}$ este un termen al şirului (2) şi în consecinţă se va scrie ca sumă de termeni din şirul $m_1, m_2, ..., m_{k+r-1}$. Rezultă că şi n este atunci sumă de diferiţi termeni din şirul $m_1, m_2, ..., m_{k+r}$. Mai mult, ţinând cont de (1) deducem că $m_{r+k+1} \leq 2m_{k+r}$ şi astfel $s_r = s_{r-1} + m_{k+r} \geq 2m_{k+1} \geq m_{k+r+1}$. Astfel Lema 1 este probată.

Lema 2. *Fie* $m_1, m_2, ...$ *un şir infinit de numere naturale astfel încât (1) are loc pentru un număr natural* k, *şi există* $s_0, a \in \boldsymbol{N}$ *astfel încât* $s_0 \geq m_{k+1}$ *astfel încât fiecare dintre numerele (4)* $a+1, a+2, ..., a+s_0$ *este sumă de diferiţi termeni din şirul* $m_1, m_2, ..., m_k$.

Atunci orice număr natural $> a$ *se scrie ca sumă de termeni ai şirului* $m_1, m_2, ...$

Intr-adevăr, conform Lemei 1 (cu $r = 1, 2, ..., t, t \in \mathbf{N}$) fiecare dintre numerele (5) $a + 1, a + 2, ..., a + s_t$ se scrie ca sumă de termeni din şirul $m_1, m_2, ..., m_{k+t}$. Cum însă $s_r > s_{r-1}, r = 1, 2, ..., t$, observăm că pentru orice număr natural n există un număr natural t astfel încât $n \leq a + s_t$.

In consecinţă, orice număr natural $n > a$ este unul dintre termenii şirului (5) cu t convenabil ales şi astfel va fi sumă de diferiti termeni din şirul $m_1, m_2, ...$ Cu aceasta Lema 2 este şi ea probată.

Să revenim acum la demonstraţia teoremei. Fie $m_i = p_i$ cu $i = 1, 2, ...$(p_i-fiind al i-ulea număr prim). Conform Corolarului 2.3.21 de la Capitolul 2, numerele m_i verifică condiţiile 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 consecinţă imediată a Lemei 2. ■

Corolar 6.4.5. *Orice număr natural* $n \geq 10$ *se poate scrie ca sumă de diferite numere prime impare.*

Demonstraţie. Intr-adevăr, dacă alegem $m_i = p_{i+1}$ atunci condiţiile Lemei 2 de la demonstraţia Teoremei 6.3.4 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. ■

Observaţie. In lucrarea **A. Makowski, Partitions into unequal primes din Bull. Acad. Sci. Sér. Sci. Math. Astr. Phys., 8(1960), pp. 125-126** se demonstrează urmatoarele rezultate :

Teorema 6.4.6. *Orice număr natural* $n > 55$ *se poate scrie ca sumă de diferite numere prime de forma 4k-1.*

Teorema 6.4.7. *Orice număr natural* $n > 121$ *se poate scrie ca sumă de numere prime de forma 4k+1.*

Teorema 6.4.8. *Orice număr natural* $n > 161$ *se poate scrie ca sumă de numere prime de forma 6k-1.*

Teorema 6.4.9. *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 6.4.10. *(Schnirelman) Există un număr natural s astfel încât orice număr natural mai mare sau egal cu 2 se scrie ca sumă a cel mult s numere prime (nu neapărat distincte).*

Cititorul poate găsi demonstraţia acestei teoreme în lucrarea [20], p.107 (preluată

dupa articolul original al lui **Schnirelman: Uber additive Eigeenschaften von Zahlen din Math. Ann. 107, 1933, pp. 649-690**).

In 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):

Teorema 6.4.11. *(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:

Corolar 6.4.12. *Există $n_0 \in \boldsymbol{N}, n_0 \geq 2$, astfel încât orice număr natural n, $n \geq n_0$, se scrie ca sumă a cel mult patru numere prime.*

Observaţii.

1. **Shapiro** şi **Warga** în lucrarea: O**n representation of large integers as sums of primes din Comm. Pure Appl. Math, 3, 1950, p. 153** demonstrează elementar un rezultăt mai slab: *Orice număr natural suficient de mare se scrie ca sumă a cel mult 20 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. Acăd. Polon. Sci. cl III, 4, 1956, pp. 793-795** demonstrează elementar că *orice număr natural suficient de mare se scrie ca sumă a cel mult 18 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 sumă a două numere prime.*

Dacă această conjectură ar fi adevarată (lucru neprobat până acum) atunci ar rezulta că *orice număr natural mai mare sau egal cu 2 se scrie ca sumă a cel mult 3 numere prime.*

Cel mai bun rezultat demonstrat până acum este datorat lui Chen: e*xistă $n_0 \in \boldsymbol{N}$ asfel încât orice număr natural $n \geq n_0$ se poate scrie sub forma $n = p + m$, unde p este prim iar m este prim sau produs de două numere prime.*

4. In 1770, Waring a conjecturat (iar în 1909 Hilbert a demonstrat) că pentru orice număr natural $k \geq 2$ există $s \in \mathbf{N}^*$(ce depinde de forma lui k) astfel încât orice număr natural n se scrie sub forma $n = \sum_{i=1}^{s} n_i^k$ cu $n_i \in \mathbf{N}, 1 \leq i \leq s$.

Capitolul 7

Ecuaţii diofantice

In cele ce urmează prin *ecuaţie diofantică* înţelegem o ecuaţie de forma

$$f(x_1, ..., x_n) = 0, \text{ cu } f \in \mathbf{Z}[X_1, ..., X_n].$$

A rezolva o astfel de ecuaţie diofantică revine la a găsi toate n-uplurile $(a_1, ..., a_n) \in \mathbf{Z}^n$ pentru care $f(a_1, ..., a_n) = 0$.

Observaţie.

Denumirea de ecuaţii diofantice provine de la numele matematicianului grec Diofant (aprox. secolul III era noastră).

7.1 Ecuaţia $ax + by + c = 0, a, b, c \in \mathbf{Z}$ (1)

Lema 7.1.1. *Ecuaţia (1) are soluţie în $\mathbf{Z}$ dacă şi numai dacă $d = (a, b) \mid c$.*

Demonstraţie. In mod evident, dacă $x, y \in \mathbf{Z}$ astfel încât $ax + by + c = 0$, atunci cum $c = -ax - by$ deducem că $d \mid c \Leftrightarrow c = dt$ cu $t \in \mathbf{Z}$.

Reciproc, să presupunem că $d|c$. Atunci din algoritmul lui Euclid deducem că există $x_1, y_1 \in \mathbf{Z}$ astfel încât $d = ax_1 + by_1$. Atunci $c = dt = (ax_1 + by_1)t = a(x_1t) + b(y_1t) \Leftrightarrow a(x_1t) + b(y_1t) - c = 0 \Leftrightarrow a(-x_1t) + b(-y_1t) + c = 0$, adică $(-x_1t, -y_1t)$ este soluţie a ecuaţiei $ax + by + c = 0$. ■

Lema 7.1.2. *Dacă $(a, b) = 1$ iar (x_0, y_0) este soluţie particulară a ecuaţiei (1), atunci soluţia generală din $\mathbf{Z}$ a acestei ecuaţii este dată de $x = x_0 - kb$ şi $y = y_0 + ka$, cu $k \in \mathbf{Z}$.*

Demonstraţie. Dacă $x = x_0 - kb$ şi $y = y_0 + ka$ (cu $(x_0, y_0) \in \mathbf{Z}^2$ soluţie particulară a lui (1) şi $k \in \mathbf{Z}$), atunci $ax + by + c = a(x_0 - kb) + b(y_0 + ka) + c = ax_0 + by_0 + c - abk + abk = 0$.

Fie acum $(x, y)\mathbf{Z}^2$ astfel încât $ax + by + c = 0$. 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 $k \in \mathbf{Z}$) $\Leftrightarrow y = y_0 + ka$. Deducem imediat că $a(x_0 - x) = bka$, de unde $x = x_0 - kb$. ■

Corolar 7.1.3. *Fie $a, b, c \in \boldsymbol{Z}$ astfel încât $d = (a, b) | c, a = da', b = db', c = dc'$. Dacă $(x_0, y_0) \in \boldsymbol{Z}^2$ 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 $k \in \boldsymbol{Z}$.*

Observaţie.

Ţinând cont de Lema 7.1.2 şi Corolarul 7.1.3 deducem că atunci când suntem puşi în situaţia de a rezolva o ecuaţie diofantică de forma (1) (în cazul în care $d = (a, b) \neq c$) 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 data de Lema 7.1.2.

Să prezentăm acum un procedeu de a gasi o soluţie particulară (x_0, y_0) a ecuaţiei (1) (cu $a, b, c \in \mathbf{Z}, (a, b) = 1$). Pentru aceasta vom dezvolta numărul raţional $\alpha = \frac{a}{b}$ în fracţie continuă. Păstrând notaţiile de la Capitolul 5 observăm că ultima redusă $\frac{p_n}{q_n}$ a lui α este chiar $\frac{p_n}{q_n} = \frac{a}{b} = \alpha$.

Ţinând cont de Propoziţia 5.1.3 de la Capitolul 5 putem scrie:

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \Leftrightarrow \frac{a}{b} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \Leftrightarrow aq_{n-1} - bp_{n-1} + (-1)^n = 0$$

de unde (prin înmulţire a ambilor membrii ai ultimei egalităţi cu $(-1)^n c$) obţinem că $a[(-1)^n c q_{n-1}] + b[(-1)^{n+1} c p_{n-1}] + c = 0$.

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 7.1.2 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 $k \in \mathbf{Z}$.

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 $\mathbf{Z}^2$ (conform Lemei 7.1.2).

Pentru a găsi soluţia generală a ecuaţiei $(*)$ să găsim o soluţie particulară $(x_0, y_0) \in \mathbf{Z}^2$ a ecuaţiei $(*)$.

Prin calcul direct găsim urmatoarea dezvoltare în fracţie continuă a lui $\alpha = \frac{317}{182}$: $\frac{317}{182} = [1; 1, 2, 1, 6, 1, 5]$.

Redusele lui $\alpha = \frac{317}{182}$ se obţin completând de la stânga la dreapta tabelul:

a		1	1	2	1	6	1	5
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 soluţie particulară va fi $x_0 = (-1)^n c q_{n-1} = (-1)^6 \cdot 94 \cdot q_5 = 94 \cdot 31 = 2914, y_0 = (-1)^{n+1} c p_{n-1} = (-1)^7 \cdot 94 \cdot p_5 = -94 \cdot 54 = -5076$.

Astfel, soluţia generală a ecuaţiei $(*)$ va fi $x = 2914 - 182k, y = -5076 + 317k$, cu $k \in \mathbf{Z}$.

7.2 Ecuaţia $x^2 + y^2 = z^2$ (2)

In primul rând trebuie observat că dacă tripletul (x, y, z) de numere întregi verifică ecuaţia (2), atunci aceeaşi ecuaţie va fi satisfacută de orice triplet de forma $(\lambda x, \lambda y, \lambda z)$, cu $\lambda \in \mathbf{Z}$ şi reciproc.

De aceea, pentru a găsi toate soluţiile ecuaţiei (2) (constând din numere diferite de zero) este suficient să găsim (soluţiile (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 soluţie (x, y, z) a ecuaţiei (2) două dintre numerele x, y, z au un divizor comun $\lambda \neq \pm 1$, atunci şi al treilea număr se divide cu λ.

De aceea ne putem restrânge la soluţiile ce constau din numere relativ prime două câte două, pe care le vom numi *soluţii primitive*.

Dacă (x, y, z) este o soluţie a lui (2), atunci în mod evident şi (y, x, z) este soluţie.

Pe de alta parte, dacă (x, y, z) este soluţie, 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 $4k + 1$).

In plus, dacă (x, y, z) este soluţie, atunci şi $(\pm x, \pm y, \pm z)$ vor fi soluţii.

Lema 7.2.1. *Orice soluţie particulară (x, y, z) de numere naturale (cu n par) a ecuaţiei (2) este de forma* $x = 2mn, y = m^2 - n^2, z = m^2 + n^2$ *cu* $m, n \in \boldsymbol{N}$ *şi* $n < m, (n, m) = 1$ *iar m, n au parităti diferite.*

Demonstraţie. Identitatea $(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$ arată că numerele de forma din enunţ sunt soluţii ale ecuaţiei (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 $(m, n) = 1$). Insă atunci m^2 şi n^2 sunt simultan pare sau impare, ceea ce este imposibil căci prin ipoteză m şi n au parităţi diferite. Deci soluţia din enunţ este primitivă.

Reciproc, fie (x, y, z) o soluţie primitivă a lui (2) cu $x, y, z \in \mathbf{N}$ 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 $\lambda = \pm 1$, 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 $c = n^2 (m, n \in \mathbf{N})$ iar de aici $a^2 = m^2 n^2 \Leftrightarrow a = mn$, 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 7.2.2. *Soluţia generală a ecuaţiei (2) este* $x = 2rmn, y = r(m^2 - n^2), z = r(m^2 + n^2)$ *cu* $r, m, n \in \boldsymbol{Z}$.

7.3 Ecuaţia $x^4 + y^4 = z^4$ (3)

In cadrul acestui paragraf vom demonstra un rezultat ceva mai general şi anume:

Lema 7.3.1. *Ecuaţia* $x^4 + y^4 = z^2$ (**4**) *nu are soluţii în* $\boldsymbol{Z}^*$.

Demonstraţie. Să presupunem că ar există o soluţie în $\mathbf{Z}^*$ a ecuaţiei (4). Putem presupune în mod evident că această soluţie constă din numere din $\mathbf{N}^*$.

Cum orice mulţime nevidă de numere naturale are un cel mai mic element, atunci printre soluţiile ecuaţiei (4) există una (x, y, z) cu z minim.

Analog ca în cazul ecuaţiei (2) se arată că x sau y trebuie sa 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 parităţi diferite astfel încât $x^2 = 2mn, y^2 = m^2 - n^2$ şi $z = m^2 + n^2$. Dacă $m = 2k$ şi $n = 2t + 1$ atunci $y^2 = 4(k^2 - t^2 - t - 1) + 3$, 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 $mq = (\frac{x}{2})^2$. Cum $(m, n) = 1$ deducem că $m = z_1^2, q = t^2$ cu z_1, t naturale şi $(z_1, t) = 1$.

In 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 $a, b \in \mathbf{N}^*, a > b, (a, b) = 1$ şi de parităţi diferite astfel încât $2t^2 = 2ab \Leftrightarrow t^2 = ab, y = a^2 - b^2, z_1^2 = a^2 + b^2$.

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 că $z_1 \geq z \Leftrightarrow z_1^2 \geq z \Leftrightarrow m \geq m^2 + n^2$, ceea ce este absurd. ■

Corolar 7.3.2. *Ecuaţia (3) nu poate avea soluţii (x, y, z) cu* $x, y, z \in \boldsymbol{Z}^*$.

Observaţie. Ecuaţia (3) este legată de ceea ce în teoria numerelor a fost cunoscută începând cu anul 1637 sub numele de *Marea teorema a lui Fermat* (deşi corect ar fi fost să fie numită *Marea Conjectură a lui Fermat*!):

Dacă $n \geq 3, x, y, z \in Z$ **astfel încât** $x^n + y^n = z^n$**, atunci** $xyz = 0$(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 $\mathbf{Z}^*$ (Corolarul 7.3.2).

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!).

In ce priveşte cazul general, $n > 4$, Fermat a notat (pe marginea unei pagini din ,,Aritmetica" lui Diofant) că a găsit ,,o demonstraţie cu adevărat minunată" a acestui fapt, dar ,,aceasta 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. 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 afirmaţie sau alta, ulterior s-a reuşit a se demonstra această afirmaţie.

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 Shimura-Taniyama-Weil) din care conjectura lui Fermat rezultă ca un corolar.

Din păcate demonstraţia lui Wiles este destul de dificilă, ea neavând un caracter elementar, limitând astfel accesul la înţelegerea ei pentru un foarte mare număr de matematicieni.

Celor care poseda cunoştiinţe solide de aritmetica geometriei algebrice le recomandăm lucrarea lui A.Wiles din care rezultă conjectura lui Fermat:

A.Wiles: Modular Elliptic Curves and Fermat's Last Theorem, Annals of Math., vol. 141, pp. 443-551, 1995.

7.4 Ecuaţii de tip Pell: $x^2 - Dy^2 = \pm 1 (D \in \mathbf{N})$ (5)

Ca şi în paragrafele precedente, pentru a rezolva ecuaţia (5) în $\mathbf{Z}$ este suficient să găsim soluţiile sale $x, y \in \mathbf{N}^*$. Dacă $D = n^2$ cu $n \in \mathbf{N}^*$, atunci $(x - ny)(x + ny) = 1$ şi se arată imediat că această ecuaţie nu are soluţii (x, y) cu $x, y \in \mathbf{N}^*$.

Rămâne deci să ne ocupăm doar de cazul $D \in \mathbf{N}^*$ şi $\sqrt{D} \in \mathbf{I}$.

In Capitolul 5 (Propozitia 5.3.7) am văzut că fracţia continuă a lui $\sqrt{D}$ este de forma: $\sqrt{D} = [a_0; \overline{a_1 ..., a_n, 2a_0}]$, adică $\sqrt{D} = [a_0; a_1 ..., a_n, a_0 + \sqrt{D}]$, de unde $\sqrt{D} = \frac{p_n(a_0 + \sqrt{D}) + p_{n-1}}{q_n(a_0 + \sqrt{D}) + q_{n-1}}$ 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 7.4.1. *Toate soluţiile ecuaţiei (5) sunt date de reduse ale lui* $\sqrt{D}$.

Demonstraţie. Egalitatea $p_n^2 - Dq_n^2 = (-1)^{n+1}$ rămâne adevărată şi dacă în locul lui n punem $k(n+1) - 1$ (deoarece nu este nevoie să considerăm cea mai scurtă perioadă). Astfel

$$(*) \qquad p_{k(n+1)-1}^2 - Dq_{k(n+1)-1}^2 = (-1)^{k(n+1)},$$

ceea ce ne arată că o infinitate de reduse ale lui $\sqrt{D}$ ne dau soluţii pentru ecuaţia $x^2 - Dy^2 = \pm 1$.

Fie acum $p, q \in \mathbf{N}^*$ astfel încât $|p^2 - Dq^2| = 1$. Vrem să demonstrăm că $\frac{p}{q}$ este o redusă a lui $\sqrt{D}$. Să presupunem prin absurd că $\frac{p}{q}$ nu este o redusă a lui $\sqrt{D}$. Atunci conform observaţiei de după Propoziţia 5.2.1 de la Capitolul 5, există o redusă $\frac{p_k}{q_k}$ a lui $\sqrt{D}$ cu : $|q_k - p_k| < |q - p|$ şi $q_k < q$.

Avem $|q_k + p_k| \leq 2q_k\sqrt{D} + |p_k - Dq_k| \leq 2(q-1)\sqrt{D} + |q\sqrt{D} - p| = 2q\sqrt{D} - (2\sqrt{D} - |q\sqrt{D} - p|) < 2q\sqrt{D} - |q\sqrt{D} - p| \leq |q\sqrt{D} + p|$, de unde rezultă că: $0 < |p_k^2 - Dq_k^2| = |q_k\sqrt{D} - p_k| \cdot |q_k\sqrt{D} + p_k| < |q^2 D - p^2| = 1$, ceea ce este absurd.

Rezultă deci că toate soluţiile ecuaţiei $x^2 - Dy^2 = \pm 1$ sunt date de reduse ale lui $\sqrt{D}$.

Fie acum $p_k^2 - Dq_k^2 = \pm 1$ o astfel de soluţie.

Avem $\sqrt{D} = [a_0; a_1, ..., a_k, \alpha_{k+1}]$. Ştim că α_{k+1} este un iraţional pătratic redus care satisface ecuaţia:

$$A_{k+1}x^2 + B_{k+1}x + C_{k+1} = 0, \text{ unde } A_{k+1} = p_k^2 - Dq_k^2 = \pm 1$$

.

In plus, $B_{k+1}^2 - 4A_{k+1}C_{k+1} = 4D$ şi B_{k+1} este par.

Rezultă $\alpha_{k+1} = \frac{B_{k+1}}{2} + \sqrt{D}$ şi cum α_{k+1} este iraţional pătratic redus avem $a_{k+1} = a_0 + \sqrt{D}$ şi deci $\overline{[2a_0; a_1, ..., a_k]}$ este o perioadă a lui $\sqrt{D}$, deci toate soluţiile ecuaţiei (5) sunt de forma $(\star)$. ■

Observaţie. Este de reţinut algoritmul de găsire a soluţiei $x_0^2 - Dy_0^2 = 1$, cu cele mai mici x_0 şi y_0 naturale nenule:

$$\frac{x_0}{y_0} = \begin{cases} [a_0; a_1, ..., a_n], & \text{dacă perioada minimă are lungimea pară;} \\ [a_0; a_1 ..., a_n, 2a_0, a_1, ..., a_n], & \text{dacă } n \text{ este par (adică perioada este impară).} \end{cases}$$

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: $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$, $\frac{p_3}{q_3} = [2; 1, 1, 1] = \frac{8}{3}$, deci $x_0 = 8$ şi $y_0 = 3$.

b) Ecuaţia $x^2 - 13y^2 = -1$.

Avem: $\sqrt{13} = [3; \overline{1, 1, 1, 6}]$, $\frac{p_4}{q_4} = \frac{18}{5}$, deci $x_0 = 18$ şi $y_0 = 5$.

Să mai notăm faptul că ecuaţiile de forma $x^2 - Dy^2 = m$ cu $D, m \in \mathbf{Z}$ sunt cunoscute sub numele de *ecuaţii de tip Pell* (deşi Pell nu s-a ocupat de studiul unor astfel de ecuaţii, această greşeală de numire datorându-se lui Euler).

7.5 Ecuaţii de tipul $ax^2 + by^2 + cz^2 = 0$, cu $a, b, c \in \mathbf{Z}$ (6)

In cadrul acestui paragraf ne vom ocupa de rezolvarea ecuaţiei diofantice (6), unde $a, b, c \in \mathbf{Z}$ sunt libere de pătrate (adică nu conţin în descompunerea lor factori de forma d^2 cu d prim), iar $(a, b) = (b, c) = (c, a) = 1$.

In mod evident, dacă $a, b, c \geq 0$ sau $a, b, c \leq 0$ 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 $m, n \in \mathbf{Z}$, vom scrie m **R** n dacă există $x \in \mathbf{Z}$ astfel încât $x^2 \equiv m (\text{mod } n)$, (adică m este rest pătratic modulo n).

Teorema 7.5.1. *(Legendre) Fie $a, b, c \in \boldsymbol{Z}$, libere de patrate, oricare două relativ prime, neavând toate acelaşi semn. In aceste condiţii ecuaţia $ax^2 + by^2 = z^2$ (7) are o soluţie netriviala 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 urmatoarea formă echivalentă:

Teorema 7.5.2. *Fie a, b numere naturale libere de patrate. 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* $d = (a, b)$.

Intr-adevăr, să presupunem că Teorema 7.5.2 este adevarată şi să considerăm ecuaţia $ax^2 + by^2 + cz^2 = 0$ cu a, b, c ca în enunţul Teoremei 7.5.1 (să presupunem că $a, b > 0$, iar $c < 0$). Atunci $-acx^2 - bcy^2 - z^2 = 0$ satisface condiţiile din Teorema 7.5.2 Dacă (x, y, z) este o soluţie netrivială, atunci, deoarece c este liber de pătrate, $c \mid z$. Punând $z = cz'$ şi simplificând ajungem la o soluţie netrivială pentru (6). Lăsăm ca exerciţiu probarea faptului că Teorema 7.5.1 implică Teorema 7.5.2.

Să trecem acum la demonstrarea Teoremei 7.5.2.

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 $r, s \in \mathbf{Z}$ astfel încât $b = r^2 + s^2$; 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 $Ax^2 + by^2 = z^2$ satisfacând aceleaşi condiţii că în enunţul Teoremei 7.5.2, $0 < A < a$ şi astfel încât dacă forma astfel construită are o soluţie netrivială, atunci acea soluţie verifică şi forma din enunţul Teoremei 7.5.2.. Astfel, după un număr de paşi, schimbând de fiecăre 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 $T, c \in \mathbf{Z}$ astfel încât (8) $c^2 - b = aT = aAm^2$, cu $A, m \in \mathbf{Z}, A$ liber de pătrate, iar $|c| \leq a$. Să arătăm că $0 < A < a$.

Intr-adevăr, din (8) deducem că $0 \leq c^2 = aAm^2 + b < a(Am^2 + 1)$, adică $A \geq 0$. Cum b este liber de pătrate deducem că $A > 0$. Mai mult, din (8) deducem că $aAm^2 < c^2 \leq \frac{a^2}{4}$ astfel că $A = Am^2 < \frac{a}{4} < a$. Să arătăm acum că A **R** b.

Fie $b = b_1 d, a = a_1 d$, 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) $c^2 - b_1 d = a_1 dAm^2$ şi cum d este liber de pătrate deducem că $d \mid c$. Punând $c = c_1 d$ şi simplificând obţinem (10) $dc_1^2 - b_1 = a_1 Am^2$. Atunci $Aa_1 m^2 \equiv -b_1 (\mathrm{mod}\ d)$ sau $Aa_1^2 m^2 \equiv -a_1 b_1 (\mathrm{mod}\ d)$.

Insă $(m, d) = 1$ 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, $c^2 \equiv aAm^2 (\text{mod } b_1)$ 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 $b = b_1 d$ 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 $-A_1 b_2$ **R** r.

Din (8) deducem că: $c_2 - rb_2 = arA_1 m^2$ (11). Cum r este liber de pătrate deducem că $r \mid c$. Dacă $c = rc_1$ atunci $aA_1 m^2 \equiv -b_2 (\text{mod } r)$. Cum a **R** b rezultă că a **R** r. Scriind acum că $-aA_1 b_2 m^2 \equiv b_2^2 (\text{mod } r)$ şi observând că $(a, r) = (m, r) = 1$, concluzionăm că $-A_1 b_2$ **R** r.

Să presupunem acum că $AX^2 + bY^2 = Z^2$ are o soluţie netrivială. Atunci $AX^2 = Z^2 - bY^2$ (12). Din (12) şi (6) prin multiplicare obţinem : $A(Axm)^2 = (Z^2 - bY^2)(c^2 - b) = (Zc + bY)^2 - b(cY + Z)^2$.

Atunci (6) are soluţia : $x = AXm, y = cY + Z, z = Zc + bY$ ceea ce completează demonstraţia (căci $X \neq 0$ şi $m \neq 0$ deoarece b este liber de pătrate). ■

Corolar 7.5.3. *Fie $a, b, c \in \boldsymbol{Z}$ libere de pătrate, cu (a,b)=(a, c)=(b, c)=1 şi nu au toate acelaşi semn. Dacă pentru un număr prim $p \geq 2$ congruenţa $ax^2 + by^2 + cz^2 \equiv 0 (mod\ p^m)$ are soluţie $(x, y, z) \in \boldsymbol{Z}^3$, pentru orice $m \in \boldsymbol{N}^*$ astfel încât nici o componentă a sa nu se divide prin p, atunci $ax^2 + by^2 + cz^2 = 0$ are soluţie netrivială întreagă (x, y, z).*

Demonstraţie. Fie $m = 2$ şi să presupunem că $p \mid a$. Atunci dacă (x, y, z) este o soluţie ca în corolar, să arătăm că $p \nmid yz$.

Dacă $p \mid y$, atunci $p \mid cz^2$ care implică $p \mid z$ (deoarece $(a, c) = 1$). Atunci $p^2 | ax^2$ şi cum $p \nmid x$ obţinem contradicţia $p^2 \mid a$. Similar $p \nmid z$. Atunci $by^2 + cz^2 \equiv 0 (\text{mod } p)$, 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 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 $m \in \mathbf{N}$ şi o soluţie reală, însă nu are soluţie netrivială întreagă [vezi **H. Reichardt: Einige im Kleinen überall lösbare, im Grossen unlösbare diophan-**

tische Gleichungen, J. Reine Angew und Math., 184(1942) pp. 12-18].

7.6 Ecuaţii de tip Bachet

Prin *ecuaţie diofantică de tip Bachet* înţelegem ecuaţiile de forma

$$y^2 = x^3 + k \text{ cu } k \in \mathbf{Z}. \ (\mathbf{7})$$

Aceste tipuri de ecuaţii au generat la vremea lor interes deosebit, iar în 1621 Bachet a afirmat că pentru $k = -2$ ecuaţia (7) are soluţie unică $x = 3, y = 5$.

Teorema 7.6.1. *(Lebesque) Ecuaţia $y^2 = x^3 + 7$ nu are soluţie în $\boldsymbol{Z}^2$.*

Demonstraţie. Dacă x este par atunci $y^2 \equiv 3(\text{mod } 4)$ ceea ce este absurd. De asemenea, dacă $x \equiv 3(\text{mod } 4)$ atunci $y^2 \equiv 2(\text{mod } 4)$ din nou absurd. Deci $x \equiv 1(\text{mod } 4)$. Scriind $y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$, cum $x^2 - 2x + 4 \equiv 3(\text{mod } 4)$, deducem că $y^2 \equiv -1(\text{mod } 4) \Leftrightarrow y^2 \equiv 3(\text{mod } 4)$ din nou absurd. ■

Teorema 7.6.2. *Ecuaţia $y^2 = x^3 - 16$ nu are soluţie în $\boldsymbol{Z}^2$.*

Demonstraţie. Dacă x este par, $x = 2a$, atunci y este de asemenea par, deci $y = 2b$ cu $a, b \in \mathbf{Z}$. Atunci $b^2 + 4 = 2a^3$, deci $b = 2c$ şi $a = 2d(c, d \in \mathbf{Z})$. Atunci $c^2 + 1 = 4d^3$- absurd. Deci x şi y sunt impare. Deducem că $x^3 \equiv 1(\text{mod } 8)$, deci $x \equiv 1(\text{mod } 8)$. Atunci $x - 2 \equiv -1(\text{mod } 8)$ şi $(x - 2) \mid (x^3 - 8) = y^2 + 8$. Deducem că $x - 2$ nu poate avea factori primi p de forma $p \equiv 1, 3(\text{mod } 8)$, deci există un prim p ce divide $y^2 + 8$ iar $p \equiv 5(\text{mod } 8)$ sau $p \equiv 7(\text{mod } 8)$.

Atunci $1 = (\frac{y^2}{p}) = (\frac{-8}{p}) = (\frac{-2}{p})$, contradicţie (vezi Ex. 8 de la Capitolul 4). ■

7.7 Rezolvarea în numere întregi a sistemelor de ecuaţii liniare

In cadrul acestui paragraf vom prezenta condiţii necesare şi suficiente ca un sistem de m ecuaţii liniare cu n necunoscute cu coeficienţi din $\mathbf{Z}$ să aibă soluţie întreagă precum şi modul de aflare a soluţiei generale în caz de compatibilitate.

Definiţia 7.7.1. O matrice $U \in M_n(\mathbf{Z})(n \geq 2)$ se zice *unimodulară* dacă $det(U) = \pm 1$.

In mod evident U este unimodulară dacă şi numai dacă U este inversabilă în $M_n(\mathbf{Z})$. Grupul unităţilor monoidului $(M_n(\mathbf{Z}), \cdot)$ se notează prin $GL_n(\mathbf{Z})$ şi poartă numele de *grupul general liniar de ordin n al lui $\boldsymbol{Z}$.*

Pentru $n \geq 1, i, j \in \mathbf{N}, i \neq j, 1 \leq i, j \leq n$ şi $\lambda \in Z$ vom nota prin $T_{ij}(\lambda)$ maticea din $M_n(\mathbf{Z})$ ce are 1 pe diagonala principală, λ pe poziţia (i, j) şi 0 în rest.

Reamintim că pentru $m, n \in \mathbf{N}, m, n \geq 2$, matricea unitate I_n este matricea din $M_n(\mathbf{Z})$ ce are 1 pe diagonala principală şi 0 în rest, iar matricea nulă $O_{m,n}$ este matricea din $M_{m,n}(\mathbf{Z})$ 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.

In mod evident $det(T_{ij}(\lambda)) = 1$ şi $det(D_i) = -1$, de unde deducem că $T_{i,j}, D_i \in GL_n(\mathbf{Z})$.

Definiţia 7.7.2. Matricele de forma $T_{ij}(\lambda)$ şi D_i cu $\lambda \in \mathbf{Z}, 1 \leq i,j \leq n$ definite anterior se numesc *elementare*. Inmulţirea la stânga sau la dreapta a unei matrice A cu o matrice elementară poartă numele de *transformare elementară*.

Din felul în care se înmulţesc două matrice, următorul rezultat este imediat:

Teorema 7.7.3. *Fie $m, n \in \boldsymbol{N}, m, n \geq 2$ şi $A \in M_{m,n}(\boldsymbol{Z})$.*

1) *Dacă $T_{ij}(\lambda)$ este o matrice elementară din $M_m(\boldsymbol{Z})$, 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_iA 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 $T_{23}(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbf{Z})$, 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 $T_{12}(\lambda) = \begin{pmatrix} 1 & \lambda & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in M_4(\mathbf{Z})$, 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 $D_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbf{Z})$, 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 $D_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \in M_4(\mathbf{Z})$, atunci

$$AD_4 = \begin{pmatrix} a_{11} & a_{12} & a_{13} & -a_{14} \\ a_{21} & a_{22} & a_{23} & -a_{24} \\ a_{31} & a_{32} & a_{33} & -a_{34} \end{pmatrix}.$$

Definiţia 7.7.4. Fie $n \in \mathbf{N}, n \geq 2$ şi $1 \leq i, j \leq n$. Matricea $P_{ij} \in M_n(\mathbf{Z})$ ce se obţine din I_n punând pe poziţiile (i,i) şi (j,j) în loc de 1 pe 0 şi care în plus pe poziţiile (i,j) şi (j,i) are 1 poartă numele de *matrice de transpoziţie.*

Exemplu. Dacă $n = 4$, atunci $P_{23} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Corolar 7.7.5. *Ţinând cont de Teorema 7.7.3 deducem că*
Pentru orice $n \in \boldsymbol{N}, n \geq 2$ şi $1 \leq i, j \leq n$ avem egalitatea

$$P_{ij} = D_i T_{ij}(1) T_{ij}(-1) T_{ji}(1).$$

In particular, $det(P_{ij}) = -1$, deci $P_{ij} \in GL_n(\boldsymbol{Z})$.

De asemenea avem următorul rezultat:

Lema 7.7.6. *Fie $m, n \in N, m, n \geq 2$ şi $A \in M_{m,n}(\boldsymbol{Z})$.*

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 7.7.7. Fie $m, n \in N, m, n \geq 2$ şi $A, B \in M_{m,n}(\mathbf{Z})$. Vom spune că A este *aritmetic echivalentă* cu B, şi vom scrie $A \sim B$, dacă există $U \in GL_m(\mathbf{Z})$ şi $V \in GL_n(\mathbf{Z})$ astfel încât $UAV = B$.

Se verifică imediat că relaţia $\sim$ este o echivalenţă pe $M_{m,n}(\mathbf{Z})$.

Lema 7.7.8. *Oricare ar fi $A \in M_{m,n}(\boldsymbol{Z})$ există $0 \leq r \leq min\{m, n\}$ şi $d_1, ..., d_r \in \boldsymbol{N}^*$ astfel încât*

$$A \sim \begin{pmatrix} d_1 & & & & & & 0 \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix} \in M_{m,n}(\mathbf{Z}).$$

Demonstraţie. Pentru fiecăre matrice $A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \in M_{m,n}(\mathbf{Z})$ definim:

$$m(A) = \begin{cases} 0, \text{ dacă } det(A) = 0; \\ min\{|a_{ij}|, a_{ij} \neq 0\}, \text{ dacă } det(A) \neq 0. \end{cases}$$

Vom face inducţie 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 $B \in M_{m,n}(\mathbf{Z})$ cu $m(B) < m(A)$ ca şi pentru matricele din $M_{m-1,n-1}(\mathbf{Z})$.

Există atunci $1 \le i_0 \le m$ şi $1 \le j_0 \le n$ astfel încât $m(A) = |a_{i_0 j_0}|$. Prin diferite permutări de linii şi coloane ale lui A putem presupune că $i_0 = j_0 = 1$ (adică $A \sim P_{1i_0} A P_{1j_0}$). 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 $D_1 A$).

Cazul 1. Presupunem că $a_{11} \mid a_{1j}$ pentru $2 \le j \le n$ şi $a_{11} \mid a_{i1}$ pentru $2 \le i \le m$, adică există $q_{1j}, q_{i1} \in \mathbf{Z}$ astfel încât $a_{1j} = a_{11} \cdot q_{1j}$ cu $2 \le j \le n$ şi $a_{i1} = a_{11} \cdot q_{i1}$ cu $2 \le i \le m$.

Adunând la coloanele $2, 3, ..., n$ coloana 1 a lui A înmulţită respectiv cu $-q_{12}, -q_{13}$, $..., -q_{1n}$ şi procedând analog pentru linii, obţinem: $A \sim \begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix}$, cu $A' \in M_{m-1,n-1}(\mathbf{Z})$.

Aplicând ipoteza de inducţie lui A' deducem că există $U' \in GL_{m-1}(\mathbf{Z})$ şi $V' GL_{n-1}(\mathbf{Z})$ astfel încât

$$U'A'V' = \begin{pmatrix} d_2 & & & & & 0 \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix} \in M_{m-1,n-1}(\mathbf{Z}), \text{ unde } d_i \in \mathbf{N}^* \text{ pentru}$$

$2 \le i \le r$.

Alegând $U = \begin{pmatrix} 1 & 0 \\ 0 & U' \end{pmatrix}$, $V = \begin{pmatrix} 1 & 0 \\ 0 & V' \end{pmatrix}, d_1 = a_{11}$ avem $U \in GL_m(\mathbf{Z}), V \in$ $GL_n(\mathbf{Z})$ 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 $A \in M_{m,n}(\mathbf{Z})$.

Cazul 2. Să presupunem că există în prima linie (sau prima coloana) a lui A un element (să zicem a_{1j_0}, cu $2 \le j_0 \le n$) ce nu divide pe a_{11}. Impărţind 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 $B \sim A$ care are în poziţia $(1, j_0)$ elementul r_{1j_0}.

Cum $m(B) \leq r_{1j_0} < a_{11} = m(A)$, conform ipotezei de inducţie, B este echivalentă cu o matrice de forma celei din enunţ şi atunci şi A va avea aceeaşi proprietate. ■

Observaţie. Analizând demonstraţia Lemei 7.7.8 se observă că matricea diagonală cu căre A este echivalentă se obţine aplicând asupra lui A un număr finit de transformări elementare.

Lema 7.7.9. *Orice matrice unimodulară $U \in GL_n(\boldsymbol{Z})$, este egală cu produsul unui numar finit de matrici elementare.*

Demonstraţie. Conform observaţiei anterioare, există matricele elementare $R_1, ..., R_s, Q_1, ..., Q_t$ astfel încât

$$R_1...R_sUQ_1...Q_t = D = \begin{pmatrix} d_1 & & & & & & 0 \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix} \in M_m(\mathbf{Z}).$$

Cum $1 = |det(U)| = det(D)$, rezultă că $det(D) \neq 0$, deci $r = n$. Din $d_i \in \mathbf{N}^*, 1 \leq i \leq n$ şi $d_1...d_n = 1$ deducem că $d_1 = d_2 = ... = d_n = 1$, adică $D = I_n$ şi atunci $U = R_1^{-1}...R_s^{-1}Q_t^{-1}...Q_1^{-1}$. 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. ■

Lema 7.7.10. *Pentru orice $a, b \in \boldsymbol{Z}$ avem* $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} (a,b) & 0 \\ 0 & [a,b] \end{pmatrix}$.

Demonstraţie. Fie $d = (a, b)$ şi $a_1, b_1 \in \mathbf{Z}$ pentru care $a = da_1$ şi $b = db_1$. Conform Corolarului 1.2.7 de la Capitolul 1, există $h, k \in \mathbf{Z}$ astfel încât $d = ha + kb$, 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 $U, V \in GL_2(\mathbf{Z})$ şi cum $ab = (a, b)[a, b]$ obţinem că :

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim U \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} V = \begin{pmatrix} (a,b) & 0 \\ 0 & [a,b] \end{pmatrix}. ■$$

In cele ce urmează vom prezenta un rezultat important (cunoscut sub numele de *Teorema factorilor invarianţi*).

Teorema 7.7.11. *Fie $m, n \in \boldsymbol{N}, m, n \geq 2$ şi $A \in M_{m,n}(\boldsymbol{Z})$. Atunci există*

$f_1, ..., f_r \in \boldsymbol{N}^*$ *cu* $r = min\{m, n\}$ *unic determinaţi astfel încât* $f_1 \mid f_2 \mid ... \mid f_r$ *şi*

$$A \sim \begin{pmatrix} f_1 & & & & & 0 \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix} \in M_{m,n}(\mathbf{Z}).$$

Demonstraţie . Conform Lemei 7.7.9 avem

$$A \sim \begin{pmatrix} d_1 & & & & & 0 \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix} = D$$

cu $d_i \in \mathbf{N}^*, 1 \leq i \leq r = min\{m, n\}$ iar $D \in M_{m,n}(\mathbf{Z})$.

Făcând la nevoie permutări de linii sau coloane putem presupune că $d_1 \leq d_2 \leq ... \leq d_r$.

Dacă pentru $i < j, d_i \nmid d_j$, atunci conform Lemei 7.7.10 există matricile unimodulare $U = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, V = \begin{pmatrix} p & q \\ s & t \end{pmatrix}$ astfel încât

$$U \begin{pmatrix} d_i & 0 \\ 0 & d_j \end{pmatrix} V = \begin{pmatrix} (d_i, d_j) & 0 \\ 0 & [d_i, d_j] \end{pmatrix}.$$

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.

In mod evident, $U' \in GL_m(\mathbf{Z}), V' \in GL_n(\mathbf{Z})$ 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 $d_1 \mid d_j, 2 \leq j \leq r$ atunci se defineşte $f_1 = d_1$. Dacă există $j \geq 2$ astfel încât $d_1 \nmid d_j$ 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 $d_i' \mid d_j'$ cu $2 \leq j \leq r$ şi se ia $f_1 = d_1'$. Dacă $d_2' \mid d_j', 3 \leq j \leq r$ atunci vom lua $f_2 = d_2'$. In caz contrar, se aplică procedeul de mai înainte ş.a.m.d.. Astfel, după un numar finit de paşi se obţine o matrice de forma celei din enunt echivalentă cu A.

Să arătăm acum unicitatea numerelor $r, f_1, f_2, ..., f_r$.

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 $f_1 \mid f_2 \mid ... \mid f_r$, avem $\Delta_1(D) = f_1, \Delta_2(D) = f_1 f_2, ..., \Delta_r(D) = f_1 f_2 ... f_r$ iar $\Delta_i(D) = 0$, pentru $r \leq i \leq min\{m, n\}$.

Cu aceasta teorema este complet demonstrată. ■

Definiţia 7.7.12. Dacă $A \in M_{m,n}(\mathbf{Z})$, atunci matricea unic determinată $B = \begin{pmatrix} f_1 & & & & & 0 \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix} \in M_{m,n}(\mathbf{Z})$, cu $f_1 \mid f_2 \mid ... \mid f_r$ astfel încât $A \sim B$ se numeşte *forma diagonal canonică* a lui A. Numerele $f_1, ..., f_r > 1$ se zic *factorii invarianţi* ai lui A.

Exemplu ([22]). Să găsim forma diagonal cănonică a matricei

$$A = \begin{pmatrix} 6 & 2 & -12 & 8 \\ -6 & 0 & 12 & -6 \\ 12 & 2 & -24 & 14 \end{pmatrix}.$$

Inmulţind 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 $B = T_{31}(-1)AP_{12}T_{12}(-3)T_{13}(6)T_{14}(-4) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -6 & 12 & -6 \\ 0 & 6 & -12 & 6 \end{pmatrix}$.

Inmulţind 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 $D = T_{32}(-1)D_2BT_{23}(2)T_{24}(-1) = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ ce reprezintă forma diagonal cănonică a matricei A, 2 şi 6 fiind factorii invarianţi ai acesteia.

Fie $U = T_{32}(-1)D2T_{31}(-1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$ 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 $U \in GL_3(\mathbf{Z}), V \in GL_4(\mathbf{Z})$ 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 ecuaţii cu n necunoscute:

$$(S)\begin{cases} a_{11}X_1 + ... + a_{1n}X_n = b_1 \\ a_{21}X_1 + ... + a_{2n}X_n = b_2 \\ ..... \\ a_{m1}X_1 + ... + a_{mn}X_n = b_m \end{cases}$$

cu coeficienţii $a_{ij}, b_j \in \mathbf{Z}, 1 \leq i \leq m, 1 \leq j \leq n$.

Prin *soluţie întreagă a lui (S)* înţelegem un n-uplu $(\lambda_1, ..., \lambda_n) \in \mathbf{Z}^n$ astfel încât

$$\sum_{j=1}^{n} a_{ij}\lambda_j = b_i \text{ pentru orice } 1 \leq i \leq m.$$

Dacă notăm $A = \begin{pmatrix} a_{11} & ... & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & ... & a_{mn} \end{pmatrix}, b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ şi $X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ atunci sistemul (S) se scrie matricial sub forma $AX = b$.

Definiţia 7.7.13. Dacă $U \in GL_n(\mathbf{Z}), U = (u_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ atunci transformarea $X_i = \sum_{j=1}^{n} u_{ij}Y_j, 1 \leq i \leq n$ (sau matriceal $X = UY$) se numeşte *substituţie întreagă*

unimodulară, unde $Y = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}$.

Propoziţia 7.7.14. *Fie* $U \in GL_n(\boldsymbol{Z}), U = (u_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ *şi numerele reale* α_i, β_i *cu* $1 \le i \le n$ *astfel încât* $\beta_i = \sum_{j=1}^{n} u_{ij}\alpha_j, 1 \le i \le n$.

Atunci $\beta_i \in \boldsymbol{Z}$ *pentru* $1 \le i \le n$ *dacă şi numai dacă* $a_j \in \boldsymbol{Z}$ *pentru* $1 \le j \le n$. *Mai mult,* $(\beta_1, ..., \beta_n)$ *este soluţie întreagă a sistemului (S) dacă şi numai dacă* $(\alpha_1, ..., \alpha_n)$ *este soluţie întreagă a sistemului* $(AU)Y = b$.

Demonstraţie. O implicaţie este evidentă.

Să presupunem acum că $\beta_i \in \mathbf{Z}$ pentru $1 \le i \le n$ şi fie $V \in GL_n(\mathbf{Z})$ astfel încât $VU = UV = I_n$. 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 $\alpha_i \in \mathbf{Z}$ pentru $1 \le i \le n$. Ultima afirmaţie este evidentă. ■

Lema 7.7.15. *Dacă* $a_1, ..., a_n \in \boldsymbol{Z}$, *atunci există* $U \in GL_n(\boldsymbol{Z})$ *astfel încât* $(a_1, ..., a_n)U = (d, 0, ..., 0)$, *unde* $d = (a_1, a_2, ..., a_n)$.

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 $a_1', a_2' \in \mathbf{Z}$ iar $(a_1', a_2') = 1$, de unde deducem că există $h, k \in \mathbf{Z}$ astfel încât $ha_1' + ka_2' = 1$ şi fie $U = \begin{pmatrix} h & -a_2' \\ k & a_1' \end{pmatrix}$ (cum $det(U) = ha_1' + ka_2' = 1$ deducem că $U \in GL_2(\mathbf{Z})$).

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 $V_1 \in GL_{n-1}(\mathbf{Z})$ astfel încât $(a_2, ..., a_n)V_1 = (d_1, 0, ..., 0)$, unde $d_1 = (a_2, a_3, ..., a_n)$ astfel că dacă notăm $V = \begin{pmatrix} 1 & 0 \\ 0 & V_1 \end{pmatrix} \in GL_n(\mathbf{Z})$ avem $(a_1, ..., a_n)V = (a_1, d_1, 0, ..., 0)$.

Conform cazului $n = 2$ există $W_1 \in GL_2(\mathbf{Z})$ astfel încât $(a_1, d_1)W_1 = (d_1, 0)$, unde $d = (a_1, d_1)$.

Dacă alegem $W = \begin{pmatrix} W_1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in GL_n(\mathbf{Z})$ atunci $W \in GL_n(\mathbf{Z})$ şi $(a_1, ..., a_n)U = (d, 0, ..., 0)$, unde $U = VW$ (se observă că $d = (a_1, ..., a_n)$).■

Să considerăm acum ecuaţia:

$(*)$ $\quad a_1X_1 + ... + a_nX_n = b$, cu $a_1, ..., a_n, b \in \mathbf{Z}$.

Pentru $n = 2$ am arătat în §1 în ce condiţii această ecuaţie are soluţii întregi şi felul în care acestea se găsesc. In cele ce urmează vom face acelaşi lucru cu ecuaţia $(*)$ pentru $n \leq 2$ (prezentând deci o generalizare a Lemelor 7.1.1 şi 7.1.2).

Teorema 7.7.16. *Ecuaţia $(*)$ cu coeficienţi întregi admite soluţii întregi dacă şi numai dacă $d \mid (a_1, ..., a_n)$. Dacă $U \in GL_n(\boldsymbol{Z}), U = (u_{ij})_{1 \leq i,j \leq n}$ este astfel încât $(a_1, ..., a_n)U = (d, 0, ..., 0)$, (conform Lemei 7.6.15) atunci $(x_1^0, ..., x_n^0)$ cu $x_i^0 = u_{i1} \cdot \frac{b}{d}, 1 \leq i \leq n$ este soluţie întreagă particulară a ecuaţiei $(*)$. Soluţia generală din $\boldsymbol{Z}$ a ecuaţiei $(*)$ va fi de forma $(x_1, ..., x_n)$ cu , $x_i = x_i^0 + \sum_{j=2}^{n} u_{ij}t_j, t_j \in \boldsymbol{Z}, 1 \leq i \leq n$.*

Demonstraţie. Dacă $U \in GL_n(\mathbf{Z})$ ca în enunţ, atunci făcând substituţia întreagă unimodulară $X = UY$ obţinem $(d, 0, ..., 0)Y = b$. Atunci deducem că aceasta ultimă ecuaţie are soluţie întreagă dacă şi numai dacă $d \mid b$ iar o soluţie întreagă particulară a acesteia este $(\frac{b}{d}, 0, ..., 0)$, soluţia generală fiind de forma $(\frac{b}{d}, t_2, ..., t_n)$ cu $t_j \in \mathbf{Z}, 2 \leq j \leq n$ arbitrare. Conform Propoziţiei 7.7.14 obţinem că

$$\begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix} = U \begin{pmatrix} \frac{b}{d} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} u_{11}\frac{b}{d} \\ \vdots \\ u_{n1}\frac{b}{d} \end{pmatrix}$$

este soluţia întreagă particulară a ecuaţiei $(*)$ iar dacă $(x_1, ..., x_n)$ este soluţia întreagă oarecare a lui $(*)$, atunci

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = U \begin{pmatrix} \frac{b}{d} \\ t_2 \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} u_{11}\frac{b}{d} + \sum_{j=2}^{n} u_{1j}t_j, t_j \\ \vdots \\ u_{n1}\frac{b}{d} + \sum_{j=2}^{n} u_{nj}t_j, t_j \end{pmatrix}$$

adică $x_i = x_i^0 + \sum_{j=2}^{n} u_{ij}t_j, t_j \in \mathbf{Z}, 1 \leq i \leq n$. ■

Observaţii.

1. Când $d \mid b$, descrierea soluţiilor întregi ale ecuaţiei $(*)$ din enunţul teoremei precedente se face cu ajutorul matricei unimodulare U. Calculul lui U se face folosind de $n - 1$ ori algoritmul lui Euclid extins.

Intr-adevăr, într-o primă etapă, cu ajutorul acestui algoritm determinăm succesiv:

$$\begin{aligned} d_1 &= (a_{n-1}, a_n), h_1a_{n-1} + k_1a_n = d_1 \\ d_2 &= (a_{n-2}, d_1), h_2a_{n-2} + k_2d_1 = d_2 \\ ... &\quad ... \quad ..... \\ d &= d_{n-1} = (a_2, d_{n-2}), h_{n-1}a_{n-1} + k_1d_{n-2} = d_{n-1} = d \end{aligned}$$

şi atunci avem

$$U=\begin{pmatrix} 1 & & & & 0\\ & \ddots & & & \\ & & 1 & & \\ & & & h_1 & -a_n\\ 0 & & & k_1 & a'_{n-1}\end{pmatrix}\begin{pmatrix} 1 & & & & & 0\\ & \ddots & & & & \\ & & 1 & & & \\ & & & h_2 & -d'_1 & \\ & & & k_2 & a'_{n-1} & \\ 0 & & & & & 1\end{pmatrix}\ldots$$

$$\begin{pmatrix} h_{n-1} & -d'_{n-1} & & & 0\\ k_{n-1} & a'_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1\end{pmatrix}, \text{ unde } a_n=d_1a'_n, a_{n-1}=d_1a'_{n-1}, d_1=d_2d'_1, a_{n-2}=$$

$d_2a'_{n-2}$, etc.

2. Când $n=2$ obţinem rezultatele de la §1.

Lema 7.7.17. *Fie $n\geq 2$ şi $A=(a_{ij})_{1\leq i,j\leq n}\in M_n(\boldsymbol{Z})$ astfel încât $\Delta=det(A)>0$. Atunci există $U\in GL_n(\boldsymbol{Z})$ astfel încât*

$$AU=\begin{pmatrix} c_{11} & 0 & \ldots & 0\\ c_{21} & c_{22} & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots\\ c_{n1} & c_{n2} & \ldots & c_{nn}\end{pmatrix} \text{ unde } c_{ii}>0, 1\leq i\leq n \text{ şi } \ 0\leq c_{i1}, c_{i2}, ..., c_{ii-1}<$$

$c_{ii}, 1\leq i\leq n$.

Demonstraţie. Fie $c_{11}=(a_{11}, a_{12}, ..., a_{1n})$. Conform Lemei 7.7.15 există $U_1\in GL_n(\mathbf{Z})$ astfel încât $(a_{11}, a_{12}, ..., a_{1n})U_1=(c_{11}, 0, ..., 0)$ şi deci

$$AU_1=\begin{pmatrix} c_{11} & 0 & \ldots & 0\\ a'_{21} & a'_{22} & \ldots & a'_{2n}\\ \ldots & \ldots & \ldots & \ldots\\ a'_{n1} & a'_{n2} & \ldots & a'_{nn}\end{pmatrix} \text{unde } a'_{ij}\in\mathbf{Z}.$$

Aplicând din nou aceeaşi lemă găsim $V\in GL_{n-1}(\mathbf{Z})$ astfel încât $(a'_{22}, a'_{23}, ..., a'_{2n})V=(c_{22}, 0, ..., 0)$ unde $c_{22}=(a'_{22}, a'_{23}, ..., a'_{2n})$. Punând $U_2=\begin{pmatrix} 1 & 0\\ 0 & V\end{pmatrix}$ avem $U_2\in GL_n(\mathbf{Z})$ şi se obţine

$$AU_1U_2=\begin{pmatrix} c_{11} & 0 & 0 & \ldots & 0\\ a''_{21} & c_{22} & 0 & ... & 0\\ a''_{31} & a''_{32} & a''_{33} & \ldots & a''_{3n}\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ a''_{n1} & a''_{n2} & a''_{n3} & ... & a''_{nn}\end{pmatrix}.$$

Dacă $0\leq a''_{21}<c_{22}$ luăm $c_{21}=a''_{21}$, în caz contrar scriem $a''_{21}=c_{22}q_{21}+r_{21}$ cu

$0 \leq r_{21} < c_{22}$. Atunci $AU_1U_2T_{21}(-q_{21}) = \begin{pmatrix} c_{11} & 0 & \dots & 0 \\ r_{21} & c_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \end{pmatrix}$ şi alegem $c_{21} = r_{21}$.

Continuând se găseşte matricea $U = U_1U_2... \in GL_n(\mathbf{Z})$ astfel încât matricea AU este de forma celei din enunţ. ■

Teorema 7.7.18. *Fie* (S_1) $\sum_{j=1}^{n} a_{ij}X_j = b_i, 1 \leq i \leq n$ *un sistem de* n *ecuaţii liniare cu* n *necnoscute astfel încât* $a_{ij}, b_i \in \boldsymbol{Z}$ *şi* $det(A) > 0$ *(*A *fiind matricea* $A = (a_{ij})_{1 \leq i,j \leq n}$*).*

Atunci sistemul (S_1) *admite soluţie întreagă dacă şi numai dacă congruenţele* (C) $\sum_{j=j}^{n} a_{ij}X_j \equiv b_i (mod\ m), 1 \leq i \leq n$ *au soluţie întreagă pentru orice* $m \in \boldsymbol{Z}$ *astfel încât* $0 < m \leq \Delta$.

Demonstraţie. Implicaţia de la stânga la dreapta este evidentă.

Să presupunem acum că (C) are soluţie pentru orice $0 < m \leq \Delta$. Scriem pe (C) sub forma matricială astfel $AX \equiv b (\text{mod } m), 0 < m \leq \Delta$.

Dacă $X = UY$ este o substituţie întreagă unimodulară, atunci $(AU)Y \equiv b (\text{mod } m)$, $0 < m \leq \Delta$. Alegând $U \in GL_n(\mathbf{Z})$ dată de Lema 7.7.15 sistemul (S_1) devine

$$\begin{cases} c_{11}Y_1 = b_1 \\ c_{21}Y_1 + c_{22}Y_2 = b_2 \\ ..... \\ c_{n1}Y_1 + c_{n2}Y_2 + ... + c_{nn}Y_n = b_n \end{cases}$$

Evident $\Delta = c_{11}c_{22}...c_{nn}$, deci $0 < c_{11}c_{22}...c_{ii} \leq \Delta, 1 \leq i \leq n$.

Cum $0 < c_{11} \leq \Delta$, congruenţa $c_{11}Y_1 = b_1 (\text{mod } c_{11})$ are soluţie, deci există $h, k \in \mathbf{Z}$ astfel încât $c_{11}h = b_1 + kc_{11}$, de unde $c_{11}\alpha_1 = b_1$ cu $\alpha_1 = h - k$.

Adunând ecuaţia $c_{11}Y_1 = b_1$ (înmulţită cu $-c_{21}$) cu ecuaţia $c_{12}Y_1 + c_{22}Y^2 = b_2$ (înmulţită cu c_{11}) se obţine $c_{11}c_{22}Y_2 = -c_{21}b_1 + c_{11}b_2$.

Conform ipotezei, congruenţa $c_{11}c_{22}Y_2 = c_{21}b_1 + c_{11}b_2 (\text{mod } c_{11}c_{22})$ are soluţie, deci există $h', k' \in \mathbf{Z}$ astfel încât $c_{11}c_{22}h' = -c_{21}c_{11}\alpha_1 + c_{11}b_2 + k'c_{11}c_{22}$. Simplificând cu $c_{11} \neq 0$, obţinem $c_{21}\alpha_1 + c_{22}\alpha_2 = b_2$, unde $\alpha_2 = h' - k' \in \mathbf{Z}$.

Analog, din primele trei ecuaţii în Y_1, Y^2, Y_3 obţinem $c_{11}c_{22}c_{33}Y_3 = c_{11}c_{22}b_3 - c_{31}c_{22}b_1 - c_{11}c_{22}b_1 - c_{11}c_{32}b_2 + c_{21}c_{32}b_1$.

Inlocuind $b_1 = c_{11}\alpha_1, b_2 = c_{21}\alpha_1 + c_{22}\alpha_2$ şi pornind de la condiţia că aceasta ultimă ecuaţie să fie solubilă modulo $c_{11}c_{22}c_{33}$, găsim $\alpha_3 \in \mathbf{Z}$ astfel încât $c_{31}\alpha_1 + c_{32}\alpha_2 + c_{33}\alpha_3 = b_3$.

Continuând în acelaşi mod găsim o soluţie întreagă $(\alpha_1, \alpha_2, ..., \alpha_n)$ a sistemului $AUY = b$ şi atunci $(\beta_1, \beta_2, ..., \beta_n)$, unde $\beta_i = \sum_{j=1}^{n} u_{ij}\alpha_j, 1 \leq i \leq n$ este o soluţie întreagă a sistemului (S_1) $AX = b$. ■

Observaţie. Cum $\mathbf{Z}_m$-urile sunt finite, rezultă din teorema de mai sus că putem stabili printr-un numar finit de încercări dacă sistemul (S_1) are sau nu soluţii întregi.

Teorema următoare soluţionează cazul sistemelor omogene.

Teorema 7.7.19. *Sistemul de ecuaţii liniare* (S_2) $\sum_{j=1}^{n} a_{ij}X_j = 0, 1 \leq i \leq m$ *cu* $a_{ij} \in \boldsymbol{Z}, (m < n)$ *admite o soluţie întreagă netrivială* $(x_1, ..., x_n)$ *ce satisface condiţia* $|x_j| \leq (a_1 a_2 ... a_m)^{\frac{1}{n-m}}, 1 \leq j \leq n$, *unde* $a_i = \sum_{j=1}^{n} |a_{ij}|, 1 \leq i \leq m$.

Demonstraţie. Fie $L_i(X_1, ..., X_n) = \sum_{j=1}^{n} a_{ij}X_j, 1 \leq i \leq m, b_i = \sum_{a_{ij}>0} a_{ij}, -c_i = \sum_{a_{ij}<0} a_{ij}X_j, 1 \leq i \leq m$.

Atunci $a_i = b_i + c_i$ cu $1 \leq i \leq m$ şi fie $a \in \mathbf{N}$. Dacă $0 \leq \alpha j \leq a$ cu $1 \leq j \leq n$, atunci $-c_i a \leq L_i(\alpha_1, ..., \alpha_n) \leq b_i a, 1 \leq i \leq m$, deci $L_i(\alpha_1, ..., \alpha_n)$ ia cel mult $a_i a + 1$ valori întregi.

Alegând $\alpha = [(a_1 a_2 ... a_m)^{\frac{1}{n-m}}]$ (partea întreagă!) atunci $a > (a_1 a_2 ... a_m)^{\frac{1}{n-m}} - 1$, de unde $(a+1)^n > (a+1)^m a_1 ... a_n > (a_1 a + 1)...(a_m a + 1)$.

Deducem că există $(\alpha'_1, ..., \alpha'_n) \neq (\alpha''_1, ..., \alpha''_n)$ cu $0 \leq \alpha'_i, \alpha''_i \leq a$ astfel încât $L_i(\alpha'_1, ..., \alpha'_n) = L_i(\alpha'_1, ..., \alpha'_n), 1 \leq i \leq n$.

Alegând $x_i = \alpha'_i - \alpha''_i, 1 \leq i \leq n$, avem că $L_i(x_1, ..., x_n) = 0, 1 \leq i \leq m$ şi $|x_j| \leq (a_1 a_2 ... a_m)^{\frac{1}{n-m}}, 1 \leq j \leq n$. Mai mult, $(x_1, ..., x_n) \neq (0, ..., 0)$ şi astfel teorema este demonstrată. ■

Cu ajutorul formei diagonal canonice a matricelor din $M_{m,n}(\mathbf{Z})$ putem acum soluţiona problema existenţei şi descrierii soluţiilor întregi ale unui sistem de m ecuaţii liniare cu n necunoscute cu coeficienţi întregi.

Teorema 7.7.20. *Fie sistemul de m ecuaţii liniare în n necunoscute cu coeficienţi întregi*

(S) $\sum_{j=1}^{n} a_{ij}X_j = b_i, 1 \leq i \leq m, 1 \leq i \leq n.$

Dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M_{m,n}(\boldsymbol{Z})$ *şi* $U \in GL_m(\boldsymbol{Z}), V \in GL_n(\boldsymbol{Z}), U = (u_{ij}), V = (v_{ij})$ *sunt astfel încât* $UAV = \begin{pmatrix} f_1 & & & & & 0 \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$ *(vezi Teorema 7.7.11), atunci condiţia necesară şi suficientă ca (S) să aibă soluţii întregi este ca* $f_k \mid \sum_{j=1}^{m} u_{kj}b_j, 1 \leq k \leq r$ *şi* $\sum_{j=1}^{m} u_{ij}b_j = 0, r < j \leq min\{m, n\}$.

In aceste condiţii $(x_1^0, ..., x_n^0)$, *unde* $x_i^0 = \sum_{k,j=1}^{r,m} \frac{v_{ik}u_{kj}b_j}{f_k}, 1 \leq i \leq n$, *este o soluţie întreagă a sistemului (S). Mai mult, un sistem* $(x_1, ..., x_n)$ *de numere întregi este soluţie*

a lui (S) dacă şi numai dacă $x_i = x_i^0 + \sum_{k=r+1}^{n} v_{ik}t_k, t_k \in \mathbf{Z}, 1 \leq i \leq n.$

Demonstraţie. Scriem sistemul (S) sub forma matriciala $AX = b$. Cum $UAVV^{-1}X = Ub$, notând $Y = V^{-1}X$ avem (S') $DY = UL$ unde

$$D = \begin{pmatrix} f_1 & & & & & 0 \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$$

.

Deducem că $f_kY_k = \sum_{j=1}^{m} u_{jk}b_j, 1 \leq k \leq r$ şi $0 = \sum_{j=1}^{m} u_{kj}b_j, r < k \leq min\{m, n\}$. Este clar că $DY = Ub$ admite soluţie întreagă dacă şi numai dacă $f_k \mid \sum_{j=1}^{m} u_{kj}b_j$, $1 \leq k \leq r$ şi o soluţie particulară a sistemului (S') este:

$$(\sum_{j=1}^{m} \frac{u_{1j}b_j}{f_1}, ..., \sum_{j=1}^{m} \frac{u_{rj}b_j}{f_r}, 0, ..., 0)$$

iar soluţia generală a sistemului (S') este:

$$(\sum_{j=1}^{m} \frac{u_{1j}b_j}{f_1}, ..., \sum_{j=1}^{m} \frac{u_{rj}b_j}{f_r}, t_{r+1}, ..., t_n)$$

cu $t_{r+1}, ..., t_n$ arbitrari din $\mathbf{Z}$. Cum $X = VY$ deducem că soluţiile sistemului (S) sunt cele din enunţ. ■

Exemplu. Să considerăm sistemul:

$$(*) \begin{cases} 6X_1 + 2X_2 - 12X_3 + 8X_4 = 10 \\ -6X_1 + 12X_3 - 6X_4 = 18 \\ 12X_1 + 2X_2 - 24X_3 + 14X_4 = -8 \end{cases}$$

Avem $A = \begin{pmatrix} 6 & 2 & -12 & 8 \\ -6 & 0 & 12 & -6 \\ 12 & 2 & -24 & 14 \end{pmatrix}$.

După exemplul de la Teorema 7.7.11 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

$$\begin{aligned}
\sum_{j=1}^{4} u_{1j}b_j &= 10 \text{ şi } 2 \mid 10, \text{unde } 2 = f_1 \\
\sum_{j=1}^{3} u_{2j}b_j &= -18 \text{ şi } 6 \mid -18, \text{unde } 6 = f_2 \\
\sum_{j=1}^{3} u_{3j}b_j &= 0
\end{aligned}$$

rezulta că sistemul $(*)$ are soluţie în numere întregi (conform Teoremei 7.7.20).

Urmând algoritmul dat de Teorema 7.7.20, deducem că o soluţie particulară a lui $(*)$ este $(x_1^0, x_2^0, x_3^0, x_4^0) = (-3, 14, 0, 0)$ iar soluţia generală este:

$$\begin{aligned}
x_1 &= -3 + 2t_3 - t_4 \\
x_2 &= 14 - t_4 \\
x_3 &= t_3 \\
x_4 &= t_4
\end{aligned}$$

cu $t_3, t_4 \in \mathbf{Z}$ arbitrare.

Observaţie. Acest paragraf a fost redactat în cea mai mare parte după lucrarea [22].

Capitolul 8

Puncte laticeale în plan şi spaţiu

8.1 Puncte laticeale în plan

Să considerăm planul euclidian $\mathcal{E}$ raportat la un sistem ortogonal de axe de coordonate.

Definiţia 8.1.1. Un punct M de coordonate (a, b) din planul euclidian $\mathcal{E}$ se zice *punct laticeal* dacă $a, b \in \mathbf{Z}$.

Teorema 8.1.2.(*Steinhaus-Sierpinski*) *Pentru fiecare număr $n \in \boldsymbol{N}^*$ există în planul euclidian $\mathcal{E}$ un cerc ce conţine în interiorul său exact n puncte laticeale.*

Demonstraţie. Să considerăm în $\mathcal{E}$ punctul C de coordonate $(\sqrt{2}, \frac{1}{3})$ şi să demonstrăm că dacă $M(a, b)$ si $N(c, d)$ sunt două puncte laticeale din $\mathcal{E}$ ce au aceeaşi distanţă la punctul C, atunci $M \equiv N$. Intr-adevăr, dacă $CM = CN$, atunci:

$$\begin{aligned}(a-\sqrt{2})^2+(b-\frac{1}{3})^2 &= (c-\sqrt{2})^2+(d-\frac{1}{3})^2 \Leftrightarrow \\ 2(c-a)\sqrt{2} &= c^2+d^2-a^2-b^2+\frac{2}{3}(b-d),\end{aligned}$$

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 $b, d \in \mathbf{Z}$, $d + b - \frac{1}{3} = 0$, ceea ce implică $b = d$, adică $M \equiv N$.

Ţinând cont de observaţia de mai înainte, punctele laticeale din $\mathcal{E}$ pot fi ordonate în funcţie de distanţele lor la $C(\sqrt{2}, \frac{1}{3})$. Fie deci M_1 punctul laticeal 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 laticeale cu proprietatea că dacă notăm prin d_i distanţa de la M_i la $C, i = 1, 2, ...$, atunci $d_1 < d_2 < d_3 < ....$ Atunci cercul cu centru în punctul C şi de rază d_{n+1} conţine în interiorul său doar punctele laticeale $M_1, M_2, ..., M_n$ 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 $n \in \mathbf{N}$ există un cerc de arie n ce conţine în interiorul său exact n puncte laticeale.

Teorema 8.1.3. *(A. Schinzel) Pentru orice număr natural $n \in \boldsymbol{N}$ există în $\mathcal{E}$ un cerc ce conţine pe circumferinţa sa exact n puncte laticeale.*

Demonstraţie. Dacă n este par, adică $n = 2k$ cu $k \in \mathbf{N}$, vom demonstra că cercul de centru $(\frac{1}{2}, 0)$ şi rază $\frac{1}{2} \cdot 5^{\frac{k-1}{2}}$ conţine pe circumferinţa sa exact n puncte laticeale, pe când atunci când n este impar, adică $n = 2k+1$ cu $k \in \mathbf{N}$, cercul de centru $(\frac{1}{3}, 0)$ şi raza $\frac{1}{3} \cdot 5^k$ conţine pe circumferinţa sa exact n puncte laticeale. Pentru aceasta vom apela la Teorema 6.1.7 potrivit căreia numărul total de perechi (x, y) din $\mathbf{Z} \times \mathbf{Z}$ pentru care $x^2 + y^2 = n$ este egal cu $4(d_1(n) - d_3(n))$, unde $d_1(n)$ este numărul divizorilor lui n de forma $4t + 1$ iar $d_3(n)$ este numărul divizorilor primi de forma $4t + 3$(atunci când numărăm perechile (x, y) facem distincţie între (x, y) şi (y, x) pentru $x \neq y$).

Cazul 1: $n = 2k, k \in \mathbf{N}$. Să considerăm ecuaţia (1) $x^2 + y^2 = 5k - 1$. Toţi divizorii lui 5^{k-1} sunt puteri ale lui 5, deci toţi aceşti divizori sunt de forma $4t+1$. Cum numărul acestor divizori este k deducem că $d_1(5^{k-1}) = k$ iar cum $d_3(5^{k-1}) = 0$ atunci numărul perechilor $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ pentru care $x^2 + y^2 = 5k - 1$ este $4(k - 0) = 4k$. Cum 5^{k-1} este impar trebuie ca x sau y să fie impar.

Cercul de centru $C_1(\frac{1}{2}, 0)$ şi rază $\frac{1}{2} \cdot 5^{\frac{k-1}{2}}$ are ecuaţia:

$$(\alpha - \frac{1}{2})^2 + \beta^2 = \frac{1}{4} \cdot 5^{k-1} \Leftrightarrow (2\alpha - 1)^2 + 4\beta^2 = 5^{k-1} \Leftrightarrow (2\alpha - 1)^2 + (2\beta)^2 = 5^{k-1}(2).$$

Deci un punct $M(\alpha, \beta)$ se află pe circumferinţa 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_1 nu rezultă că şi $M(\beta, \alpha)$ se află pe C_1. Astfel, numărul punctelor $M(\alpha, \beta)$ de pe cercul C_1 cu $(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z}$ este egal cu numărul perechilor ordonate $(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z}$ ce verifică ecuaţia (2). Se observă că ecuaţia (2) este de tipul (1), astfel că numărul soluţiilor $(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z}$ ale lui (2) este egal cu numărul soluţiilor ordonate $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ ce verifică (1), adică cu $\frac{4k}{2} = 2k = n$.

Cazul 2: $n = 2k+1, k \in \mathbf{N}$. Ca în cazul 1, dacă vom considera ecuaţia $x^2+y^2 = 5^{2k}$ (3); numărul perechilor $(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z}$ ce verifică (3) este egal cu

$$4[d_1(5^{2k}) - d_3(5^{2k})] = 4[(2k + 1) - 0] = 8k + 4.$$

Să observăm acum că punctul $M(\alpha, \beta)$ se află pe circumferinţa cercului $C_2(\frac{1}{3}, 0)$ şi rază $5^k \Leftrightarrow (\alpha - \frac{1}{3})^2 + \beta^2 = \frac{1}{9} \cdot 5^{2k} \Leftrightarrow (4)(3\alpha - 1)^2 + (3\beta)^2 = 5^{2k}$. Astfel, numărul de puncte laticeale $M(\alpha, \beta)$ de pe C_2 este egal cu numărul soluţiilor ordonate $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ ale ecuaţiei (3) cu $x = 3\alpha - 1$ şi $y = 3\beta$. Pentru a determina numărul acesta, să împărţim cele $8k + 4$ soluţii din $\mathbf{Z}$ ale lui (3) în 8 familii:

$(x, y), (x, -y), (-x, y), (-x, -y), (y, x), (y, -x)(-y, x), (-y, -x)$.

Dacă $x = 0$ atunci familia se reduce la 4 soluţii: $(0, y), (0, -y), (y, 0), (-y, 0)$.

De asemenea, dacă $x = y$ există numai 4 soluţii în familia de mai sus: $(x, x), (-x, x), (x, -x), (-x, -x)$. Cum 5^{2k} este impar această posibilitate este exclusă.

Soluţiile lui (3) cu o componentă nulă sunt: $(0, 5^k), (0, -5^k), (5^k, 0)$ şi $(-5^k, 0)$.

In consecinţă, familia celor $8k + 4$ soluţii se împarte în k familii de 8 soluţii şi o familie de 4 soluţii.

Observăm de asemenea că ecuaţia (4) este de tipul (3), cu $x \equiv -1(mod\ 3)$ şi $y \equiv 0(mod\ 3)$) şi că $5^{2k} = 25^k \equiv 1^k \equiv 1(mod\ 3)$. Deoarece pătratul unui număr întreg este congruent cu 0 sau 1 *modulo* 3, dacă $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ şi $x^2 + y^2 = 5^{2k}$ atunci trebuie ca unul dintre x^2 sau y^2 să fie congruent cu 1 iar celălalt cu 0 *modulo* 3.

Fie x şi $-x$ termeni din familia celor 8 soluţii ce sunt divizibili prin 3. In acest caz y sau $-y$ este congruent cu -1 *modulo* 3. Să presupunem că $y \equiv -1(mod\ 3)$. Atunci numai cele 2 soluţii (y, x) şi $(y, -x)$ au primul termen congruent cu -1 modulo 3 şi pe al doilea congruent cu 0 *modulo* 3 (observăm că în familia celor 4 soluţii, $(-5^k, 0)$ sau $(5^k, 0)$ este de tipul de mai înainte).

In concluzie, fiecare din cele k familii de 8 soluţii (x, y) ale lui (3) conţin exact 2 soluţii ale lui (4) şi o singură familie din cele 4 soluţii ale lui (3) conţine o singura soluţie a lui (4). Obţinem în total $2k + 1 = n$ soluţii pentru (4), astfel că pe cercul C_2 se află exact $2k + 1 = n$ puncte laticeale. ■

Teorema 8.1.4. *(G. Browkin) Pentru orice număr natural $n \in \boldsymbol{N}$, există în $\mathcal{E}$ un pătrat ce conţine în interiorul său exact n puncte laticeale.*

Demonstraţie. Vom încerca să ,,ordonam" punctele laticeale din $\mathcal{E}$ într-un şir $P_1, P_2, ...$ Pentru aceasta vom utiliza funcţia $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{R}_+$, $f(x, y) = |x + y\sqrt{3} - \frac{1}{3}| + |x\sqrt{3} - y - \frac{1}{\sqrt{3}}|$, pentru orice $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

Să arătăm la început că dacă $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}$ şi $f(a, b) = f(c, d)$, atunci $(a, b) = (c, d)$, adică $a = c$ şi $b = d$.

Intr-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 $p, q, r, s \in \{\pm 1\}$.

Ţinând cont că $\sqrt{3}$ este număr iraţional şi că o egalitate de forma $x+y\sqrt{3} = x^{'}+y^{'}\sqrt{3}$ cu $(x, y), (x^{'}, y^{'}) \in \mathbf{Z} \times \mathbf{Z}$ implică $x = x^{'}$ şi $y = y^{'}$, din (1) deducem că:

$$(2) \begin{cases} pa - qb - rc + sd + \frac{r-p}{3} = 0 \text{ şi} \\ rd + sc - pb - qa + \frac{q-s}{3} = 0. \end{cases}$$

Din (2) deducem cu necesitate că $\frac{r-p}{3} = \frac{q-s}{3}$, lucru posibil doar pentru $r = p$ şi $q = s$, astfel că (2) capătă forma echivalentă:

$$(3) \begin{cases} p(a - c) + q(d - b) = 0 \text{ şi} \\ p(d - b) + q(c - a) = 0. \end{cases}$$

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 considerăam în $\mathcal{E}$ dreptele d şi d' de ecuaţii:

$$\begin{aligned}(d) &: x + y\sqrt{3} - \frac{1}{3} = 0\\ (d') &: x\sqrt{3} - y - \frac{1}{\sqrt{3}} = 0.\end{aligned}$$

Evident, $d \perp d'$ şi $(d) \cap (d') = \{(\frac{1}{3}, 0)\}$.

Ţinând cont de formula ce dă distanţa unui punct $P(x, y)$ la (d) şi 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 laticeal $P_1(x_1, y_1)$ în apropierea lui R pentru care $f(x_1, y_1)$ este cea mai mică valoare a lui $f(x, y)$ (când $x, y \in \mathbf{Z}$). Conform celor stabilite la început punctul P_1 este unic.

In felul acesta putem ordona punctele laticeale într-un şir $P_1, P_2, ...$ (scriind că $P_i(x_i, y_i) < P_{i+1}(x_{i+1}, y_{i+1}) \Leftrightarrow f(x_i, y_i) < f(x_{i+1}, y_{i+1})$).

Dacă $P_n(x_n, y_n)$ este al n-lea punct laticeal în această ordonare, să notăm $a_n = f(x_n, y_n)$, iar

$$\begin{aligned}h(x, y) &= x(1 + \sqrt{3}) + y(\sqrt{3} - 1) - \frac{1}{3} - \frac{1}{\sqrt{3}}\\ g(x, y) &= x(1 - \sqrt{3}) + y(\sqrt{3} + 1) - \frac{1}{3} + \frac{1}{\sqrt{3}}.\end{aligned}$$

Să considerăm acum cele 4 drepte: $h(x, y) = \pm a_{n+1}$ şi $g(x, y) = \pm a_{n+1}$; se verifică imediat că cele 4 drepte formează un pătrat.

Dacă avem un punct laticeal $P(x, y)$ atunci $-a_{n+1} < h(x, y) < a_{n+1} \Leftrightarrow |h(x, y)| < a_{n+1}$, adică P se găseşte între dreptele de ecuaţie $h(x, y) = a_{n+1}$ şi $h(x, y) = -a_{n+1}$ şi reciproc.

Similar, se deduce că punctul $P(x, y)$ se află între dreptele de ecuaţii $g(x, y) = a_{n+1}$ şi $g(x, y) = -a_{n+1} \Leftrightarrow |g(x, y)| < a_{n+1}$.

Astfel, punctul $P(x, y)$ se afla în interiorul pătratului din figura 4 $\Leftrightarrow |h(x, y)| < a_{n+1}$ şi $|g(x, y)| < a_{n+1}$.

Insă se verifică imediat că pentru numerele reale $a, b, c (c > 0)$: $|a| < c$ şi $|b| < c$ $\Leftrightarrow |\frac{a+b}{2}| + |\frac{a-b}{2}| < c$ şi astfel:

$$\begin{cases} |h(x, y)| < a_{n+1}, \\ |\dfrac{h(x, y) + g(x, y)}{2}| + |\dfrac{h(x, y) - g(x, y)}{2}| < a_{n+1} \Leftrightarrow f(x, y) < a_{n+1}, \\ |g(x, y)| < a_{n+1} \end{cases}$$ adică punctul laticeal $P(x, y)$ se află în interiorul pătratului din Fig. 4 dacă şi numai dacă $f(x, y) < a_{n+1}$.

Atunci în interiorul pătratului din figură sunt exact punctele laticeale $P_1, P_2, ..., P_n$, ce sunt în număr de n. ■

Teorema 8.1.5. *(Pick) Fie P un poligon convex în plan care conţine m puncte laticeale în interiorul său, k puncte laticeale pe laturi sau vârfuri şi vârfurile sale sunt puncte laticeale. Atunci Aria(P)*$= m + \frac{k}{2} - 1$.

Demonstraţie. Să demonstrăm formula la început pentru cazul $m = 0, k = 3$ (aceasta exprimă faptul că P este un triunghi cu vârfurile în nodurile reţelei şi care nu mai conţine alte noduri pe laturi sau în interior). Atunci $S = \frac{1}{2}$ (vezi figura 5).

Să trecem acum la cazul general. Descompunem poligonul P în triunghiuri cu vârfurile în puncte laticeale şi care nu mai conţin puncte laticeale 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 o parte, suma unghiurilor lor este $180^\circ \cdot n$ iar pe de alta 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 $180^\circ = 180^\circ \cdot (k-2) + 360^\circ \cdot m$, de unde $n = 2m + k - 2$ şi cum $S = \frac{n}{2}$ deducem că $S = m + \frac{k}{2} - 1$. ■

Observaţii.

1. Teorema lui Pick este valabilă şi pentru poligoane oarecare (nu neapărat convexe), însă demonstraţia ei este diferită de cazul convex.

Pentru aceasta vom considera două poligoane Q_1 şi Q_2 care au toate vârfurile în puncte laticeale şi care sunt adiacente prin una din laturile comune AB (vezi figura 6).

Să presupunem cunoscut şi formula $S = m + \frac{k}{2} - 1$ este adevarată pentru amândouă aceste poligoane; vom demonstra că în acest caz, formula va fi adevarată şi pentru poligonul mai mare Q, obţinut prin reuniunea lui Q_1 şi Q_2.

Intr-adevăr, fie S_1, m_1 şi k_1 - aria, numărul punctelor laticeale din interiorul poligonului şi numărul punctelor laticeale de pe frontiera lui Q_1, iar S_2, m_2 şi k_2-numerele corespunzatoare 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 laticeale din interiorul sau şi numărul k de puncte laticeale 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 laticeale interioare se vor adăuga toate punctele laticeale situate pe AB cu excepţia lui A şi B) şi $k = (k_1 - k') + (k_2 - k') + 2$ (în ultimul termen +2 figureaza nodurile A şi B). Deci:

$$\begin{aligned} S &= S_1 + S_2 = m_1 + \frac{k_1}{2} - 1 + m_2 + \frac{k_2}{2} - 1 \\ &= (m_1 + m_2 + k' - 2) + \frac{k_1 + k_2 - 2k' + 2}{2} - 1 \\ &= m + \frac{k}{2} - 1. \end{aligned}$$

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 laticeale:

Dacă un poligon convex simetric fata de centrul sau (care este un punct laticeal) nu mai conţine în interiorul său alte puncte laticeale, atunci aria sa este < 4 (ca unitate de arie se considera aria unui pătrat al reţelei).

Nu vom prezenta aici demonstraţia teoremei lui Minkowski deoarece ea este destul de laborioasă, dar în esenţă este asemanatoare cu cea a teoremei lui Pick (indicăm cititorului lucrarea [20]).

Pentru un număr natural n fie $t(n)$=numărul de reprezentări ale lui n ca suma de doua pătrate de numere naturale (două reprezentări fiind considerate diferite dacă diferă ordinea termenilor) - vezi Teorema 6.1.7 de la Capitolul 6.

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 $4k + 1$ are o unică reprezentare ca sumă de două pătrate de numere naturale (dacă nu ţinem cont de ordinea termenilor; vezi Propozitia 6.1.5. de la Capitolul 6). De aici deducem că dacă p este prim de forma $4k + 1$, atunci $\tau(p) = 8$ (căci dacă (a, b) este o soluţie, atunci sunt soluţii şi (b, a) ca şi $(\pm a, \pm b), (\pm b, \pm a)$).

Observăm că dacă $n = x^2+y^2$, atunci $|x|, |y| \leq \sqrt{n}$; deducem imediat că $\tau(n) \leq \sqrt{4}$. Pentru $n \in \mathbf{N}^*$, fie $T(n) = \tau(1) + \tau(2) + ... + \tau(n)$. Atunci $T(n)$ este numărul de soluţii din $\mathbf{Z}$ ale inegalităţilor: $0 < x^2 + y^2 \leq n$.

Lema 8.1.6. *Pentru orice* $n \in \boldsymbol{N}^*, T(n) = 4 \sum\limits_{k=0}^{[\sqrt{n}]} [\sqrt{n - k^2}]$.

Demonstraţie. Dacă $x = 0$, atunci $y^2 \leq n \Leftrightarrow |y| \leq \sqrt{n}$, deci numărul numerelor y pentru care $0 < x^2 + y^2 \leq n$ este $2[\sqrt{n}]$.

Dacă $x = k \neq 0$, atunci $k^2 \leq n$, deci $|k| \leq \sqrt{n}$ iar $y^2 \leq n - k^2$, adică $|y| \leq \sqrt{n - k^2}$ (deci numărul y-cilor este $1 + 2[\sqrt{n - k^2}]$; am adunat şi pe 1 deoarece $y = 0$ trebuie considerat).

Deoarece $k \in \{\pm 1, \pm 2, ..., \pm[\sqrt{n}]\}$ iar semnele $\pm$ nu influenţează valoarea lui k^2, obţinem că:

$$T(n) = 2[\sqrt{n}] + 2 \sum_{k=0}^{[\sqrt{n}]} [1 + 2\sqrt{n - k^2}] = 4[\sqrt{n}] + 4 \sum_{k=0}^{[\sqrt{n}]} [\sqrt{n - k^2}] = 4 \sum_{k=0}^{[\sqrt{n}]} [\sqrt{n - k^2}].$$

Astfel, de exemplu, pentru $n = 100$ avem

$T(100) = 4([\sqrt{100}] + [\sqrt{99}] + [\sqrt{96}] + [\sqrt{91}] + [\sqrt{84}] + [\sqrt{75}] + [\sqrt{64}] + [\sqrt{51}] + [\sqrt{36}] + [\sqrt{19}]) = 4(10 + 9 + 9 + 9 + 8 + 8 + 7 + 6 + 4) = 316$.

Interpretare geometrică pentru $T(n)$

Pentru $n \in \mathbf{N}, 1+T(n)$ reprezintă numărul de perechi din $\mathbf{Z}^2$ ce satisface inegalitatea $x^2 + y^2 \leq n$.

Astfel, $1+T(n)$ reprezintă numărul punctelor laticeale din interiorul cercului C_n de centru $(0,0)$ şi rază $\sqrt{n}$ (eventual de pe circumferinţă).

In continuare, la fiecare punct laticeal vom asocia un pătrat ce are centrul în punctul respectiv, laturile paralele cu axele de coordonate şi aria 1 (vezi Fig.7).

Dacă notăm cu P aria acoperită de pătratele asociate punctelor laticeale care nu sunt în afara cercului C_n, aceasta este egală cu numărul acestora, adică $P = 1 + T(n)$. Cercul C_{1n} de centru $(0,0)$ şi rază $\sqrt{n}+\frac{1}{\sqrt{2}}$ contine în interior sau pe circumferinţă toate punctele acoperite de pătratele asociate punctelor laticeale din C_n (aceasta deoarece în mod evident $\frac{1}{\sqrt{2}}$ este cea mai mare distanţă posibilă a unui punct din interiorul pătratului de arie 1 la centrul pătratului).

Atunci $P \leq aria(C_{1n}) \Leftrightarrow P \leq \pi(\sqrt{n}+\frac{1}{\sqrt{2}})^2$.

Pe de altă parte, dacă notăm cu C_{2n} cercul de centru $(0,0)$ şi raza $\sqrt{n}-\frac{1}{\sqrt{2}}$, atunci din $aria(C_{2n}) \leq P$ deducem că $\pi(\sqrt{n}-\frac{1}{\sqrt{2}})^2 \leq P$.

Inlocuind $P = 1+T(n)$ 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 $0 < \frac{1}{2}\pi - 1 < 1 \leq \sqrt{n}$ deducem că:

$$\begin{aligned}\pi(\sqrt{n}+\frac{1}{\sqrt{2}})^2 - 1 &= \pi n + \pi\sqrt{2}\sqrt{n} + \frac{1}{2}\pi - 1 < \pi n + 6\sqrt{n} \text{ şi}\\ \pi(\sqrt{n}-\frac{1}{\sqrt{2}})^2 - 1 &= \pi n - \pi\sqrt{2}\sqrt{n} + \frac{1}{2}\pi - 1 < \pi n - 6\sqrt{n}\end{aligned}$$

de unde $\pi n - 6\sqrt{n} < T(n) < \pi n + 6\sqrt{n} \Leftrightarrow |\frac{T(n)}{n} - \pi| < \frac{6}{\sqrt{n}}$ iar de aici deducem:

Propoziţia 8.1.7. $\lim\limits_{n\to\infty} \frac{T(n)}{n} = \pi$

După cum am văzut $T(100) = 316$, deci $\frac{T(100)}{100} = 3,16$. Analog $T(400) = 1256$, deci $\frac{T(400)}{400} = 3,14$ iar $\frac{T(1000)}{1000} = 3,148$.

Avem astfel posibilitatea de a aproxima pe π considerând valori din ce în ce mai mari pentru n.

8.2 Puncte laticeale în spaţiu

Considerăm spaţiul $\mathbf{R}^3$ raportat la un sistem ortogonal de axe $0xyz$.

Definiţia 8.2.1 Un punct $M(x,y,z) \in \mathbf{R}^3$ se zice *punct laticeal*, dacă $(x,y,z) \in \mathbf{Z}^3$.

Multe rezultate legate de puncte laticeale din plan au extinderi aproape imediate la puncte laticeale din spaţiu.

Lema 8.2.2. *Dacă* $p,q,r \in \boldsymbol{Q}$ *şi* $p\sqrt{2}+q\sqrt{3}+r\sqrt{5} \in \boldsymbol{Q}$, *atunci* $p = q = r = 0$.

Demonstraţie. Fie $p\sqrt{2}+q\sqrt{3}+r\sqrt{5} = k \in \mathbf{Q}$. 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 $2pq\sqrt{6}+2kr\sqrt{5} = k^2+5r^2-2p^2-3q^2 \in \mathbf{Q}$, de unde $2pq = 2kr = k^2+5r^2-2p^2-3q^2 = 0$ iar de aici $p = q = r = 0$. ■

Teorema 8.2.3. *Pentru orice număr natural $n \in \boldsymbol{N}^*$ există în spaţiu o sferă ce conţine în interiorul său exact n puncte laticeale.*

Demonstraţie. Să arătăm la început că sfera de centru $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ are cel mult un punct laticeal pe suprafaţa ei.

Intr-adevăr, să presupunem că pe suprafaţa sferei cu centrul în punctul de coordonate $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ există două puncte laticeale de coordonate (a, b, c) respectiv (d, e, f).

Scriind că

$$(a-\sqrt{2})^2 + (b-\sqrt{3})^2 + (c-\sqrt{5})^2 = (d-\sqrt{2})^2 + (e-\sqrt{3})^2 + (f-\sqrt{5})^2$$

obţinem $2\sqrt{2}(d-a) + 2\sqrt{3}(e-b) + 2\sqrt{5}(f-c) = d^2+e^2+f^2-a^2-b^2-c^2 \in \mathbf{Q}$ şi atunci conform Lemei 8.2.2, $d-a = e-b = f-c = 0 \Leftrightarrow a = d, b = e, c = f$.

Ca în cazul plan (Teorema 8.1.2) putem ordona punctele laticeale din spaţiu într-un şir crescător $M_1, M_2, ...$ în funcţie de distanţele $d_1, d_2, ...$ ale acestora la punctul de coordonate $(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Astfel, sfera cu centrul în punctul de coordonate $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ şi raza d_{n+1} conţine în interiorul său exact n puncte laticeale din spaţiu şi anume pe $M_1, M_2, ..., M_n$. ■

Teorema 8.2.4. *(T. Kulikowski) Pentru orice număr natural $n \in \boldsymbol{N}^*$ există în spaţiu o sferă ce conţine pe suprafaţa sa exact n puncte laticeale.*

Demonstraţie. Conform Teoremei 8.1.3 există un cerc în planul $0xy$ de ecuaţie $(x-a)^2 + (y-b)^2 = c$ (cu $a, b, c \in \mathbf{Q}, c > 0$) ce trece prin exact n puncte laticeale de coordonate (x, y). Identificând punctele laticeale de coordonate (x, y) din planul $0xy$ cu punctele de coordonate $(x, y, 0)$ din spaţiul $0xyz$ putem trage concluzia că cercul $(x-a)^2 + (y-b)^2 = c$ conţine exact n puncte laticeale $(x, y, 0)$ din spaţiu.

Să considerăm acum sfera cu centrul în punctul de coordonate $(a, b, \sqrt{2})$ şi de rază $\sqrt{c+2}$ a cărei ecuaţie în sistemul de axe $0xyz$ este:

$$(1) \quad (x-a)^2 + (y-b)^2 + (z-\sqrt{2})^2 = c+2 \Leftrightarrow$$
$$(2) \quad (x-a)^2 + (y-b)^2 + z^2 - 2z\sqrt{2} = c.$$

Conform Teoremei lui Schinzel, $a, b, c \in \mathbf{Q}$ (putem avea de exemplu $a = \frac{1}{2}$ sau $\frac{1}{3}$ şi $b = 0$ iar c pătratul unui număr întreg).

Astfel, dacă $(x, y, z) \in \mathbf{Z}^3$ verifică ecuaţia (2), atunci cu necesitate $z = 0$ şi atunci obţinem $(x-a)^2 + (y-b)^2 = c$ ce are numai n soluţii.

Cele n puncte laticeale de pe sfera de ecuaţie (1) sunt cele ce se obţin intersectând suprafaţa sferică cu planul de ecuaţie $z = 0$ (obţinând astfel cercul de ecuaţie (2) ce trece prin exact n puncte laticeale).

In concluzie, sfera de centru $(a, b, \sqrt{2})$ şi rază $\sqrt{c+2}$ trece prin exact n puncte laticeale din spaţiu, de forma $(x, y, 0)$. ■

Capitolul 9

Clase speciale de numere întregi

9.1 Numere de tip Fermat

Se numesc *numere de tip Fermat* numerele naturale de forma $F_n = 2^{2^n} + 1$ cu $n \in \mathbf{N}$; avem deci $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 65537, F_4 = 2294967297$ ş.a.m.d.

Fermat a ajuns la studiul numerelor de forma F_n din mai multe considerente.

El a observat că dacă numărul $2^m + 1 (m \geq 1)$ este prim, atunci cu necesitate m este de forma $m = 2^n$ cu $n \in \mathbf{N}$. Intr-adevăr, dacă există un divizor impar k al lui m, atunci $m = kt$ cu $t \in \mathbf{N}$ şi atunci $2^m + 1 = (2^t)^k = (2^t + 1)[(2^t)^{k-1} - (2^t)^{k-2} + ... - 2^t + 1]$ contrazicând faptul că $2^m + 1$ este prim.

Pe de altă parte, tot Fermat a observat că numerele F_0, F_1, F_2, F_3 şi F_4 sunt prime iar de aici el a tras concluzia pripită că F_n este număr prim pentru orice $n \in \mathbf{N}$. Numai că Euler l-a contraziz, arătând că F_5 este compus avându-l ca divizor pe 641(vom vedea mai târziu cum arată divizorii primi ai unui număr F_n). Iată însă rapid o soluţie a faptului că F_5 se divide prin 641. Avem $F_5 = 2^{2^5} + 1 = 2^{28}(5^4 + 2^4) - (5 \cdot 2^7)^4 = 2^{28} \cdot 641 - (640^4 - 1) = 2^{28} \cdot 641 - (640 - 1)(640 + 1)(640^2 + 1) = 641[2^{28} - 639 \cdot (640^2 + 1)] = 641 \cdot 6700417$.

Importanţa numerelor lui Fermat a început să crească datorită unui celebru rezultat al lui Gauss potrivit căruia un poligon regulat cu n laturi($n \geq 3$) poate fi construit cu rigla şi compasul dacă şi numai dacă n este de forma $n = 2^k p_1 p_2 ... p_r$ unde $k, r \in \mathbf{N}$ iar fiecare dintre numerele $3 \leq p_1 < p_2 < ... < p_r$ sunt numere Fermat prime.

Legat de mulţimea numerelor Fermat $(F_n)_{n \in \mathbf{N}}$ se pun mai multe probleme(nerezolvate încă!):

P_1: In şirul $(F_n)_{n \in \mathbf{N}}$ există o infinitate de numere prime?

P_2: In şirul $(F_n)_{n \in \mathbf{N}}$ există o infinitate de numere compuse?

Legat de $\mathbf{P}_1$ să amintim că în afară de numerele F_0, F_1, F_2, F_3, F_4 şi F_5 nu se mai

cunoaşte un alt număr Fermat prim!

Legat de $\mathbf{P}_2$ să amintim că se cunosc peste 100 de numere Fermat compuse (cel mai mare fiind F_{23471} care are un număr de 10^{7000} cifre şi care se divide prin $5 \cdot 2^{23473} + 1$). Nu se ştie în schimb dacă F_{22} este prim sau compus.

Propoziţia 9.1.1. *(i) Numerele Fermat sunt de forma* $12k + 5$ *cu* $k \in \boldsymbol{N}^*$;

(ii) Pentru orice număr natural n, $F_n = (F_n - 1)^2 + 2$ *iar* $F_{n+1} = F_n F_{n-1} ... F_1 F_0 + 2$*; dacă* $m, n \in \boldsymbol{N}, m \neq n$, *atunci* $(F_m, F_n) = 1$;

(iii) Dacă n *este par atunci* $F_n \equiv 3 (mod\ 7)$ *iar dacă* n *este impar, atunci* $F_n \equiv 5 (mod\ 7)$;

(iv) Pentru nicio valoare a lui n, *numărul* F_n *nu este pătrat sau cub perfect*;

(v) Pentru $n \geq 2$ *divizorii primi* p *ai lui* F_n *sunt de forma* $p = 2^{n+2} \cdot k + 1 (k \in \boldsymbol{N}^*)$.

Demonstraţie. (i). Scriem $2^n = 2 \cdot m$ şi cum $4^m \equiv 4 (\text{mod } 12)$, deducem că $F_n = 4^m + 1 \equiv 5 (\text{mod } 12)$.

(ii). Prima egalitate se face prin calcul direct iar pentru a doua utilizăm inducţia matematică după n, obţinând că $F_1 = 5 = F_0 + 2$ iar $F_{n+1} = (F_n - 2)F_n + 2$ şi aplicăm ipoteza de inducţie pentru F_n. Fie de exemplu $m < n$ şi $d = (F_m, F_n)$. Din a doua egalitate deducem că $d \mid 2$ şi cum F_m şi F_n sunt impare, atunci $d = 1$.

(iii). Evident, $F_0 = 3 \equiv 3 (\text{mod } 7)$. Cum pentru orice $n \geq 1, F_{n+1} = (F_n - 1)^2 + 2$, atunci $F_{n+2} = (F_{n+1} - 1)^2 + 2 = [(F_n - 1)^2 + 2 - 1]^2 + 2 = [(F_n - 1)^2 + 1]^2 + 2 = (F_n - 1)^4 + 2(F_n - 1) + 3$ iar dacă presupunem că $F_n = 7k + 3$, atunci $F_{n+2} = 7k_1 + 2^4 + 2(7k_2 + 2) + 3 = 7k_3 + 16 + 4 + 3 = 7k_3 + 3$ şi totul rezultă prin inducţie.

Pentru cazul impar procedăm analog.

(iv). Dacă prin absurd pentru un anumit $n \in \mathbf{N}$ există $k \in \mathbf{N}$ astfel încât $F_n = k^2 \Rightarrow 2^{2^n} = (k - 1)(k + 1) \Rightarrow k - 1 = 2^a, k + 1 = 2^b$ cu $a < b \Rightarrow 2^{b-1} - 2^{a-1} = 1 \Rightarrow a = 1 \Rightarrow k = 3 \Rightarrow 2^{2^n} = 8$ - absurd!

Să presupunem de asemenea prin absurd că pentru un anumit $n \in \mathbf{N}$ există $k \in \mathbf{N}$ astfel încât $F_n = k^3$. Conform celor stabilite mai înainte, pentru orice $n \in \mathbf{N}, F_n \equiv 3 (\text{mod } 7)$ sau $F_n \equiv 5 (\text{mod } 7)$ pe când $k^3 \equiv -1, 0, 1 (\text{mod } 7)$, deci şi egalitatea $F_n = k^3$ este imposibilă.

(v). Dacă p este un divizor prim al lui F_n, atunci $2^{2^n} \equiv -1 (\text{mod } p) \Rightarrow 2^{2^{n+1}} \equiv 1 (\text{mod } p)$. Fie $i \in \mathbf{N}$ cel mai mic număr natural cu proprietatea că $2^i \equiv 1 (\text{mod } p)$ (vezi § 8 de la Capitolul 1). Atunci $i \mid 2^{n+1}$, deci $i = 2^k$ cu $k \leq n + 1$. Dacă $k \leq n$, din $2^{2^k} \equiv 1 (\text{mod } p)$ deducem că $2^{2^n} \equiv 1 (\text{mod } p)$- absurd!. Deci $k = n + 1$. Conform micii teoreme a lui Fermat, $2^{p-1} \equiv 1 (\text{mod } p)$ şi atunci $2^{n+1} \mid p - 1$, adică $p - 1 = 2^{n+1} h$ cu $h \geq 1$ iar $n \geq 2$. Astfel $p = 8t + 1$ şi $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = 1$, adică 2 este rest pătratic modulo p. Atunci $2^{\frac{p-1}{2}} \equiv 1 (\text{mod } p) \Rightarrow \frac{p-1}{2} \mid 2^{n+1} \cdot k$ ş în final $p = 2^{n+2} \cdot k + 1$. ■

Observaţie. Punctul (v) al propoziţiei de mai sus permite identificarea cu uşurinţă a acelor numere prime care ar putea fi divizori ai unui număr Fermat. De exemplu, pentru F_5, eventualii divizori primi ai săi trebuie să fie de forma $p = 2^7 \cdot k + 1 = 128k + 1$, adică 257,641, ş.a.m.d., aşa că a fost relativ uşor pentru Euler să identifice factorul 641 al lui

F_5. De asemenea, în [48] la p. 349 se demonstrează că $5 \cdot 2^{1947} + 1 \mid F_{1945}$.

Teorema 9.1.2. *(Lucas-1891) Pentru $n \in \boldsymbol{N}, F_n$ este număr prim dacă şi numai dacă $F_n \mid 3^{\frac{F_n-1}{2}} + 1$.*

Demonstraţie. „⇒". Conform celor stabilite în cadrul Propoziţiei 9.1.1, (i), F_n este de forma $12k + 5$. Pe de altă parte, dacă un număr prim p este de forma $p = 12k + 5$, atunci $(\frac{p}{3}) = (\frac{-1}{3}) = -1$, deci $3^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$. Astfel, dacă $p = F_n$ este prim, atunci $F_n = p \mid 3^{\frac{p-1}{2}} + 1 = 3^{\frac{F_n-1}{2}} + 1$.

„⇐". Să presupunem că $F_n \mid 3^{\frac{F_n-1}{2}} + 1$; atunci $3 \nmid F_n$ şi fie $p \mid F_n$ un divizor prim, $p \neq 3$ iar i cel mai mic număr natural pentru care $3^i \equiv 1(\text{mod } p)$(vezi § 8 de la Capitolul 1). Conform micii teoreme a lui Fermat, $p \mid 3^{F_n-1} - 1 \Rightarrow 3^{F_n-1} \equiv -1(\text{mod } p) \Rightarrow 3^{2^{2^n}} \equiv 1(\text{mod } p) \Rightarrow i \mid 2^{2^n}$. Dacă $i = 2^k$ cu $k < 2^n$, atunci $2^k \mid 2^{2^n} - 1 = \frac{F_n-1}{2} \Rightarrow i \mid \frac{F_n-1}{2}$. Cum $p \mid 3^i - 1, p \mid 3^{\frac{F_n-1}{2}} - 1$ şi astfel din $p \mid F_n \Rightarrow p \mid 3^{\frac{F_n-1}{2}} + 1$, de unde $p \mid 2$, adică $p = 2$ ceea ce este imposibil deoarece F_n este impar. Prin urmare $i = 2^{2^n}$ şi cum $i \mid p - 1 \Rightarrow p = 2^{2^n}k + 1$. Cum $p \geq 2^{2^n} + 1 = F_n$ şi $p \mid F_n \Rightarrow F_n = p$, deci F_n este prim. ■

9.2 Numere de tip Mersenne

Se numesc *numere de tip Mersenne*, numerele naturale de forma $M_n = 2^n - 1$. Astfel, $M_0 = 0, M_1 = 1, M_2 = 3, M_3 = 7, M_4 = 15$, etc. In mod evident, dacă n este compus, atunci şi M_n este compus, astfel că pentru ca M_n să fie prim cu necesitate şi n trebuie să fie prim. Cum $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$, tragem concluzia că pentru ca M_n să fie prim nu este suficient doar ca n să fie prim.

Marin Mersenne a trăit în secolul 17 (1588-1648), însă numerele ce-i poartă azi numele erau cunoscute încă din antichitate de Euclid.

Din păcate nu se ştie până azi dacă există o infinitate de numere prime p astfel încât M_p să fie prim, după cum nici dacă există o infinitate de numere prime p pentru care M_p este compus. Unul din lucrurile importante care a impus studiul numerelor Mersenne este acela că cele mai mari numere prime cunoscute până acum sunt de tip Mersenne(se cunosc 42 de astfel de numere).

Iată un criteriu care ne permite să stabilim dacă un număr Mersenne este compus sau nu:

Propoziţia 9.2.1. *Fie p un număr prim, $p \geq 3$ astfel încât $q = 2p + 1$ este prim şi $p \equiv 3(mod\ 4)$. Atunci $q \mid M_p$, deci M_p este compus.*

Demonstraţie. Din $p = 4k + 3$ deducem că $q = 8k + 7$, deci $(\frac{2}{p}) = 1$, adică $2^{\frac{q-1}{2}} \equiv 1(\text{mod } q) \Rightarrow 2^{q-1} \equiv 1(\text{mod } q) \Rightarrow q \mid 2^{q-1} - 1$. ■

Observaţie. Din propoziţia de mai înainte deducem că $23 \mid M_{11}, 47 \mid M_{23}, 167 \mid M_{83}, 263 \mid M_{131}, 2039 \mid M_{1019}$, etc.

Propoziţia 9.2.2. *Fie $p \geq 3$ un număr prim, $1 \leq h < p, n = hp + 1$ sau $n = hp^2 + 1, n \nmid 2^h - 1$, dar $2^{n-1} \equiv 1(mod\ n)$. Atunci n este număr prim.*

Demonstraţie. Fie $n = hp^b + 1$, unde $b \in \{1, 2\}$ şi $d = ord2(\text{mod } n)$(deci d este cel mai mic număr natural nenul cu proporietatea că $2^d \equiv 1(\text{mod } n)$). Atunci $d \mid n-1, d \nmid h$ şi cum $n-1 = hp^b \Rightarrow p \mid d$. Insă $d \mid \varphi(n)$, deci $p \mid \varphi(n) = p_1^{\alpha_1 - 1}...p_k^{\alpha_k - 1}(p_1 - 1)...(p_k - 1)$, unde n are descompunerea $n = p_1^{\alpha_1}...p_k^{\alpha_k}$. Cum $p \nmid n \Rightarrow p \mid (p_1 - 1)...(p_k - 1) \Rightarrow p$ are un factor prim $q \equiv 1(\text{mod } p)$, adică $p = mq + 1$.

Cum $n \equiv 1 \equiv q(\text{mod } p) \Rightarrow m \equiv 1(\text{mod } p)$. Dacă $m > 1$, atunci $n = (up + 1)(vp + 1), 1 \leq u \leq v$ şi $hp^{p-1} = uvp + v + u$.

Dacă $b = 1$ se obţine $hp = uvp + v + u$, de unde $p \leq uvp < h < p$ -absurd.

Dacă $b = 2$ avem $hp = uvp+v+u, p \mid u+v, u+v \geq p$, de unde $2v \geq u+v \geq p, v > \frac{1}{2}p$ şi $uv < h < p, uv \leq p-2, u \leq \frac{p-2}{v} < \frac{2(p-2)}{p} < 2$. Deci $u = 1$, dacă $v \geq p-1, u \geq p-1$- din nou absurd!

Rezultă $m = 1$ şi $n = q$ este prim. Să presupunem acum că $2p + 1 \mid M_p$ şi să considerăm $h = 2$ şi $n = 2p + 1$ în enunţul propoziţiei anterioare. Avem $h < p$ şi $\nmid 2^h - 1$ dar $2^{n-1} = 2^{2p} \equiv 1(\text{mod } n)$. Deci $2p + 1$ este prim. ■

In [37] se demonstrează:

Teorema 9.2.3. *(Lucas-Lehmer) Pentru $p \in \boldsymbol{N}^*$ număr prim impar, $M_p = 2^p - 1$ este prim dacă şi numai dacă $M_p \mid a_{p-1}$, unde $(a_i)_{i \geq 1}$ este dat de $a_1 = 4$ şi $a_{n+1} = a_n^2 - 2$ pentru $n \geq 1$.*

Observaţii.

1. Nu se ştie încă dacă există o infinitate de numere Mersenne M_p cu p prim; cel mai mare număr Mersenne prim cunoscut este $M_{6972593}$ şi are 2098960 cifre(a fost determinat în 1999 de Nayan Hajratwala).

2. Cel mai mare număr Mersenne compus cunoscut este M_p cu $p = 39051 \cdot 2^{6001} - 1$(care este prim); acest număr a fost pus în evidenţă în 1987 de A. Keller.

9.3 Numere de tip Fibonacci

Numim *şir Fibonacci* şirul $(F_n)_{n \geq 1}$ definit prin $F_1 = F_2 = 1$ şi $F_{n+1} = F_n + F_{n-1}$ pentru $n \geq 2$.

Acest şir de numere a fost introdus în anul 1228 de către matematicianul italian Leonardo Fibonacci pornind de la studiul înmulţirii iepurilor de casă.

Ţinând cont că ecuaţia caracteristică ataşată şirului lui Fibonacci este $x^2 - x - 1 = 0$ cu rădăcinile $x_1 = \frac{1 - \sqrt{5}}{2}$ şi $x_2 = \frac{1 + \sqrt{5}}{2}$, deducem imediat că pentru orice $n \geq 1$,

$$F_n = \frac{1}{\sqrt{5}}(x_2^n - x_1^n) = \frac{1}{2^n\sqrt{5}}[(1 + \sqrt{5})^n - (1 - \sqrt{5})^n].$$

Următorul rezultat conţine o serie de proprietăţi interesante ale şirului $(F_n)_{n \geq 1}$.

Propoziţia 9.3.1. *(i) Pentru orice $m, n \geq 2$ are loc egalitatea $F_{m+n} = F_{m-1}F_n + F_mF_{n-1}$;*

(ii) Pentru orice $n \geq 1$ avem $(F_n, F_{n+1}) = 1$;

(iii) Dacă $m \mid n$*, atunci* $F_m \mid F_n$;

(iv) Dacă $n \geq 5$ *şi* F_n *este prim, atunci şi* n *este prim.*

Demonstraţie. (i). Se face inducţie matematică după m(sau n).

(ii). Presupunem prin absurd că există $m \geq 1$ astfel încât $(F_m, F_{m+1}) = d > 1$ şi îl alegem pe m minim cu această proprietate. Cum $F_{m+1} = F_m + F_{m-1}$ deducem că $d \mid F_{m-1}$ şi atunci $(F_{m-1}, F_m) \geq d > 1$, contrazicând minimalitatea lui m.

(iii). Să presupunem că $m \mid n$, adică $n = mk$ cu $k \geq 1$. Cum $F_n = \frac{1}{\sqrt{5}}(x_2^n - x_1^n)$ şi $F_m = \frac{1}{\sqrt{5}}(x_2^m - x_1^m)$ avem $\frac{F_n}{F_m} = \frac{x_2^n - x_1^n}{x_2^m - x_1^m} = \frac{(x_2^m)^k - (x_1^m)^k}{x_2^m - x_1^m} = x_1^{m(k-1)} + x_1^{m(k-2)}x_2^m + ... + x_2^{m(k-1)} = [x_1^{m(k-1)} + x_2^{m(k-1)}] + [x_1^{m(k-2)}x_2^m + x_1^m x_2^{m(k-2)}] + ... \in \mathbf{Z}$(deoarece din $x_1 + x_2 = 1$ şi $x_1 x_2 = -1$ deducem că $x_1^t + x_2^t \in \mathbf{Z}$ pentru orice $t \geq 1$), de unde concluzia.

(iv). Să presupunem prin absurd că n nu este prim; atunci $n = kt$ cu $k \geq 3$ şi din (i) deducem că $F_k \mid F_n$ (cu $F_k \geq 2$) contrazicând faptul că F_n este prim. ■

Corolar 9.3.2. *(i) Pentru orice* $n, k \geq 1$ *avem* $(F_{nk-1}, F_n) = 1$*;*

(ii) Pentru orice $m, n \geq 1$ *avem* $(F_m, F_n) = F_{(m,n)}$*;*

(iii) Dacă $m, n \geq 1$ *şi* $(m, n) = 1$*, atunci* $F_m F_n \mid F_{mn}$.

Demonstraţie. (i). Fie $(F_{nk-1}, F_n) = d > 1$. Cum $F_{nk+1} = F_{nk} + F_{nk-1}, d \mid F_n$ şi $F_n \mid F_{nk}$ deducem că $d \mid F_{nk}$ şi deci $(F_{nk-1}, F_{nk}) \geq d > 1$ ceea ce este absurd (conform cu (ii) din Propoziţia 9.3.1).

(ii). Fie $d = (m, n)$. Dacă $n > m$ atunci scriind algoritmul lui Euclid $n = mq_1 + r_1, m = r_1 q_2 + r_2, r_1 = r_2 q_3 + r_3, ..., r_{i-1} = r_i q_{i+1}$, atunci $d = r_i$. Ţinând cont de Propoziţia 9.3.1 avem:

$$(F_m, F_n) = (F_m, F_{mq_1+r_1}) = (F_m, F_{mq_1-1}F_{r_1} + F_{mq_1}F_{r_1+1}) = (F_m, F_{mq_1-1}F_{r_1}) = (F_m, F_{r_1}).$$

Insă $(F_m, F_{r_1}) = (F_{r_1}, F_{r_2})$, deci

$$(F_m, F_n) = (F_m, F_{r_1}) = (F_{r_1}, F_{r_2}) = ... = (F_{r_i-1}, F_{r_i}) = F_{r_i} = F_d.$$

(iii). Din $(m, n) = 1$ şi (ii) deducem că $(F_m, F_n) = F_1 = 1$. Din Propoziţia 9.3.1 deducem că $F_m \mid F_{mn}$ şi $F_n \mid F_{mn}$ iar cum $(F_m, F_n) = 1$ deducem că $F_m F_n \mid F_{mn}$. ■

Teorema 9.3.3. *Fie* $p \geq 2$ *un număr prim.*

(i) Dacă $p = 5k \pm 1$*, atunci* $p \mid F_{p-1}$;

(i) Dacă $p = 5k \pm 2$*, atunci* $p \mid F_{p+1}$.

Demonstraţie. (i). Cum pentru $p = 2, F_3 = 2$, putem presupune $p \neq 2$ şi $p \neq 5$. Cum $F_n = \frac{1}{2^n\sqrt{5}}[(1+\sqrt{5})^n - (1-\sqrt{5})^n]$ deducem că $2^{n-1}F_n = C_n^1 + C_n^3 5 + C_n^5 5^2 + ...$

Pentru $n = p$, cum $p \mid C_p^k$ pentru $1 \leq k \leq p-1$ şi $2^{p-1} \equiv 1 (\text{mod } p)$, deducem că $F_p \equiv 5^{\frac{p-1}{2}} (\text{mod } p)$. Atunci $5^{\frac{p-1}{2}} \equiv (\frac{5}{p}) (\text{mod } p)$ şi deci $F_p \equiv \pm 1 (\text{mod } p)$.

Din cele de mai sus deducem imediat că $2^p F_{p+1} \equiv C_{p+1}^1 + C_{p+1}^p 5^{\frac{p-1}{2}} \equiv 1 + 5^{\frac{p-1}{2}} (\text{mod } p)$, deci $2F_{p+1} \equiv 1 + 5^{\frac{p-1}{2}} (\text{mod } p)$.

Din legea reciprocităţii pătratice a lui Gauss(vezi Teorema 4.2.2) avem $(\frac{5}{p})(\frac{p}{5}) = (-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = 1$, deci $(\frac{5}{p}) = (\frac{p}{5})$, adică $(\frac{p}{5}) \equiv p^{\frac{5-1}{2}} (\text{mod } p)$, de unde deducem că $(\frac{5}{p}) = (\frac{p}{5}) = 1$ dacă $p = 5k \pm 1$ şi $(\frac{5}{p}) = (\frac{p}{5}) = -1$ dacă $p = 5k \pm 2$.

In primul caz deducem că $F_p \equiv 5^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$,$2F_{p+1} \equiv 1 + 5^{\frac{p-1}{2}} \equiv 2(\text{mod } p)$, $F_{p+1} \equiv 1(\text{mod } p), F_{p-1} = F_{p+1} - F_p \equiv 1 - 1 \equiv 0(\text{mod } p)$, iar în cazul al doilea $2F_{p+1} \equiv 1 + 5^{\frac{p-1}{2}} \equiv 0(\text{mod } p)$ şi atunci $F_{p+1} \equiv 0(\text{mod } p)$. ■

Teorema 9.3.4. *(Zeckendorf) Orice număr natural $n \geq 1$ se reprezintă în mod unic ca sumă de termeni distincţi şi neconsecutivi ai şirului lui Fibonacci:*

$$n = \sum_{j=1}^{m} F_{i_j}, i_j - i_{j-1} \geq 2.$$

Demonstraţie. Se verifică imediat că proprietatea din enunţ este adevărată pentru $n \leq F_4 = 3$.

Să presupunem că ea este adevărată pentru toate numerele naturale până la $F_k, k \geq 4$ şi să o demonstrăm pentru numărul n astfel încât $F_k < n \leq F_{k+1}$. Dacă $n = F_{k+1}$ totul este clar. In caz contrar, $n = F_k + (n - F_k)$ şi $n - F_k < F_{k+1} - F_k = F_{k-1}$, deci conform ipotezei de inducţie

$$n - F_k = F_{i_1} + ... + F_{i_r}, i_{j+1} \leq i_j - 2, i_1 \leq k - 2.$$

Deducem că $n = F_k + F_{i_1} + ... + F_{i_r}$. Unicitatea reprezentării din enunţ rezultă tot prin inducţie, observând că dacă $F_k \leq n < F_{k+1}$ atunci F_k apare obligatoriu în reprezentarea lui n. Intr-adevăr, o sumă de numere Fibonacci F_{k_i} cu $k_{i+1} \leq k_i - 2, i = 1, ..., r-1$ şi $k_r \geq 2$ este cel mult $F_{k_1} + F_{k_1-2} + ... = (F_{k_1+1} - F_{k_1-1}) + (F_{k_1-1} - F_{k_1-3}) + ... = F_{k_1+1} - 1$.

Deducem că dacă $n = F_k$ atunci aceasta este reprezentarea unică a lui n, iar dacă $F_k < n < F_{k+1}$ atunci reprezentarea lui n îl conţine obligatoriu pe F_k şi $n - F_k < F_{k-1}$. In continuare folosim reprezentarea unică a lui $n - F_k$. ■

9.4 Alte cazuri speciale de numere

a. Numere perfecte

Un număr natural n se zice *perfect* dacă $\sigma(n) = 2n$ (adică suma $\sigma(n) - n$ a divizorilor săi naturali strict mai mici decât n este egală cu n).

Numerele perfecte au fost studiate încă din antichitate, fiind cunoscute numerele perfecte mai mici decât 10000 şi anume: 6, 28, 496 şi 8128.

Caracterizarea numerelor perfecte este dată de:

Teorema 9.4.1. *Un număr natural n este perfect dacă şi numai dacă $n = 2^t(2^{t+1} - 1)$, cu $t \in \boldsymbol{N}$ iar $2^{t+1} - 1$ este număr prim.*

Demonstraţie. Necesitatea(Euler). Să presupunem că $n = 2^t m$ (cu $t \in \mathbf{N}$ şi m impar) este perfect, adică $\sigma(2^t m) = 2^{t+1}m$. Cum $(2^t, m) = 1$ iar σ este multiplicativă, $\sigma(2^t m) = \sigma(2^t) \cdot \sigma(m)$, astfel că $\sigma(n) = \sigma(2^t m) = \sigma(2^t) \cdot \sigma(m) = (1 + 2 + 2^2 + ... + 2^t)\sigma(m) == (2^{t+1} - 1)\sigma(m) = 2^{t+1}m$.

Din ultima egalitate deducem că $2^{t+1} \mid (2^{t+1}-1)\sigma(m)$ şi deoarece $(2^{t+1}, 2^{t+1}-1) = 1$ (fiindcă $2^{t+1} - 1$ este impar) rezultă că $2^{t+1} \mid \sigma(m)$, adică $\sigma(m) = 2^{t+1}d$ cu $d \in \mathbf{N}$. Rezultă că $m = (2^{t+1} - 1)d$.

Dacă $d \neq 1$, numerele $1, d$ şi $(2^{t+1} - 1)d$ sunt divizori distincţi ai lui m şi vom avea $\sigma(m) \geq 1 + d + (2^{t+1} - 1)d = 2^{t+1}d + 1 > 2^{t+1}d$. Dar $\sigma(m) > 2^{t+1}d$ este în contradicţie cu $\sigma(m) = 2^{t+1}d$, deci $d = 1$, adică $m = 2^{t+1} - 1$. Dacă m nu este prim atunci $\sigma(m) > (2^{t+1} - 1) + 1 = 2^{t+1}$ (fiindcă ar avea şi alţi divizori în afară de 1 şi $2^{t+1} - 1$) şi contrazice $\sigma(m) = 2^{t+1}$.

Deci dacă n este perfect atunci cu necesitate $n = 2^t(2^{t+1} - 1)$ cu $t \in \mathbf{N}$ şi $2^{t+1} - 1$ prim.

Suficienţa(Euclid). Dacă $n = 2^t(2^{t+1} - 1)$ cu $t \in \mathbf{N}$ şi $2^{t+1} - 1$ prim, atunci $\sigma(n) = \sigma(2^t(2^{t+1} - 1)) = \sigma(2^t) \cdot \sigma(2^{t+1} - 1) = (1 + 2 + 2^2 + ... + 2^t)(1 + (2^{t+1} - 1)) = (2^{t+1} - 1)2^{t+1} = 2^n$, adică n este perfect.

Astfel, numerele pare perfecte sunt strâns legate de numerele prime Mersenne; cum nu se ştie încă dacă există sau nu o infinitate de numere prime Mersenne, nu se ştie nici dacă există sau nu o infinitate de numere pare perfecte.

Legat de numerele impare perfecte, din păcate nu se ştie până acum nici dacă există astfel de numere!

In [43] şi [37] sunt date anumite rezultate ale lui Euler, Pomerance, Chein, Muskat, Grün, Touchard şi Perisastri legate de condiţii necesare ca un număr perfect să fie perfect.

b. Numere pseudo-prime, absolut pseudo-prime şi Carmichael

Un număr natural compus n se zice:

i) *pseudo-prim* dacă $2^n \equiv 2(\text{mod } n)$;

ii) *absolut pseudo-prim* dacă pentru orice întreg a avem $a^n \equiv a(\text{mod } n)$;

iii) *număr Carmichael* dacă $a^{n-1} \equiv 1(\text{mod } n)$ pentru orice întreg a pentru care $(a, n) = 1$.

Legat de aceste numere, o concluzie este clară: aceste categorii de numere au apărut în strânsă legătură cu mica teoremă a lui Fermat(vezi §6 de la Capitolul 1): dacă p este prim, atunci pentru orice număr întreg $a, a^p \equiv a(\text{mod } p)$.

In particular, $2^p \equiv 2(\text{mod } p)$ pentru orice număr prim p.

Astfel, o întrebare se pune în mod natural: dacă $n \in \mathbf{N}$ şi $2^p \equiv 2(\text{mod } p)$ (adică n este pseudo-prim) rezultă că n este prim?

Pentru $n \leq 300$ se ştie (încă de acum 4500 de ani de matematicienii chinezi!) că răspunsul la întrebarea de mai sus este afirmativ.

Numai că pentru $n = 341$ conform Exc. 65 de la Capitolul 1 avem că $2^{341} \equiv 2(\text{mod } 341)$ pe când 341 nu este prim ci compus: $341 = 11 \cdot 31$.

Observaţii ([37]).

1. Numerele pseudo-prime mai mici ca 10000 sunt 341, 361 şi 1103.

2. H. Beezer a demonstrat că există o infinitate de numere pare ce sunt pseudo-perfecte, cel mai mic fiind $161038 = 2 \cdot 73 \cdot 1103$.

3. Există numere pseudo-prime ce sunt pătrate perfecte precum 1093^2 şi 3511^2; nu se ştie încă dacă există o infinitate de astfel de numere.

Legat de numerele pseudo-prime impare avem următorul rezultat:

Teorema 9.4.2. *Dacă n este impar pseudo-prim, atunci şi $N = 2^n - 1$ este pseudo-prim.*

Demonstraţie. Avem $2^{n-1} \equiv 1(\text{mod } n)$ şi deci $\frac{2^{n-1}-1}{n} = k \in \mathbf{N}$, astfel că $2^{N-1} - 1 = 2^{2^n-2} - 1 = (2^n)^{2k} - 1 = (2^n - 1)(2^{n(2k-1)} + 2^{n(2k-2)} + ... + 1) \equiv 0(\text{mod } N)$, deci $2^N \equiv 2(\text{mod } N)$. ■

Corolar 9.4.3. *Există o infinitate de numere pseudo-prime impare.*

Ca exemple de numere absolut pseudo-prime avem pe $561 = 3 \cdot 11 \cdot 17$ sau $278545 = 5 \cdot 17 \cdot 29 \cdot 113$(vezi [37]).

In schimb, numărul 341 nu este absolut pseudo-prim, deşi este pseudo-prim (vezi Exc. 65 de la Capitolul 1).

Cel mai mic număr Carmichael este 561; alte exemple sunt: 1105, 1729, 2465, 2821, 6601 sau 8911; cel mai mare număr Carmichael cunoscut are 1057 cifre.

Nu se ştie însă dacă exită sau nu o infinitate de numere Carmichael.

In [37] este dată următoarea teoremă de caracterizare a numerelor Carmichael:

Teorema 9.4.3. *Un număr compus $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ este număr Carmichael dacă şi numai dacă sunt îndeplinite următoarele condiţii:*

(i) n este impar;

(ii) $k \geq 3$;

(iii) $\alpha_i = 1$ şi $p_i - 1 \mid n - 1$ pentru orice $1 \leq i \leq k$.

Demonstraţie. ,,$\Rightarrow$". Presupunem că există $1 \leq i \leq k$ astfel încât $\alpha_i \geq 2$. Fie $a = p_1 p_2 ... p_k + 1$ şi deci $(a, n) = 1$. Dacă $a^{n-1} \equiv 1(\text{mod } n)$, atunci avem succesiv:

$$\begin{aligned} a^{n-1} \equiv 1(\text{mod } p_i^2) \quad &\Leftrightarrow \quad (p_1 p_2 ... p_k + 1)^{n-1} \equiv 1(\text{mod } p_i^2) \Leftrightarrow C_{n-1}^0 (p_1 p_2 ... p_k)^{n-1} + ... \\ &+ \quad C_{n-1}^{n-3} (p_1 p_2 ... p_k)^2 + C_{n-1}^{n-2} (p_1 p_2 ... p_k)^{n-2} \equiv 0(\text{mod } p_i^2) \\ &\Leftrightarrow \quad (n-1) p_1 p_2 ... p_k \equiv 0(\text{mod } p_i^2). \end{aligned}$$

Cum $(p_i^2, n) = 1$, rezultă contradicţia $p_i^2 \mid p_1 p_2 ... p_k$ şi deci $\alpha_i = 1$ pentru orice $1 \leq i \leq k$, adică $n = p_1 p_2 ... p_k$.

Fie b o rădăcină primitivă (mod p_i) şi $m = n/p_i$. Considerăm ecuaţia $b + \lambda p_i = \mu m + 1$. Deoarece $(p_i, m) = 1$, această ecuaţie are soluţia (λ_0, μ_0). Numărul $a = b + \lambda_0 p_i$ este rădăcină primitivă (mod p_i) şi în plus $(a, n) = 1$.

Avem deci $a^{n-1} \equiv 1(\text{mod } p_i)$ şi $n-1 = (p_i-1)c_i + r_i, 0 \leq r_i < p_i - 1$. Aşadar $a^{r_i} \equiv 1(\text{mod } p_i)$ şi cum a este rădăcină primitivă, rezultă $r_i = 0$, adică $p_i - 1 \mid n-1$ pentru orice $1 \leq i \leq k$.

Cel puţin unul dintre factorii p_i este impar şi deci $p_i - 1$ este par şi, cum $p_i - 1 \mid n-1$, rezultă că n este impar.

Pentru $k = 2$ avem $n = p_1p_2, p_1 < p_2$. Fie a o rădăcină primitivă pentru p_2 şi în plus $(a, n) = 1$. Din $a^{p_1p_2-1} \equiv 1(\text{mod } p_2)$ rezultă $a^{p_1(p_2-1)+p_1-1} \equiv 1(\text{mod } p_2)$ şi deci $a^{p_1-1} \equiv 1(\text{mod } p_2)$. Aceasta constituie o contradicţie deoarece $p_1 - 1 < p_2 - 1$ şi a este rădăcină primitivă.

,, $\Leftarrow$ ". Fie $(a, n) = 1$. Rezultă $a^{p_i-1} \equiv 1(\text{mod } p_i)$ pentru orice $1 \leq i \leq k$ şi deci, notând $M = [p_1 - 1, p_2 - 1, ..., p_k - 1]$, rezultă $a^M \equiv 1(\text{mod } p_i)$, $1 \leq i \leq k$. Cum $n = p_1p_2...p_k$, rezultă $a^M \equiv 1(\text{mod } n)$. Deoarece $p_i - 1 \mid n - 1$ pentru orice $1 \leq i \leq k$ rezultă $M \mid n - 1$ şi $a^{n-1} \equiv 1(\text{mod } n)$. ■

c. Numere triunghiulare

Pentru $n \in \mathbf{N}$, al n-ulea număr triunghiular se defineşte ca fiind $t_n = \frac{n(n+1)}{2} = 1 + 2 + ... + n$.

Iată câteva proprietăţi importante ale numerelor triunghiulare:

Teorema([37], [47])

(1) Există o infinitate de numere triunghiulare care sunt pătrate perfecte;

(2) *Nu există numere triunghiulare care să fie puterea a patra a unui număr natural*;

(3) *Dacă* $r \in \boldsymbol{Q}_+$ *şi* $\sqrt{r} \notin \boldsymbol{Q}_+$, *atunci există* m, n *naturale astfel încât* $r = \frac{t_m}{t_n}$;

(4) *Dintre numerele* $r \in \boldsymbol{Q}_+$ *cu* $\sqrt{r} \in \boldsymbol{Q}_+$ *există o infinitate care se scriu sub forma* $r = \frac{t_m}{t_n}$ *şi o infinitate care nu se scriu sub această formă.*

Capitolul 10

Exerciţii propuse (enunţuri)

10.1 Elemente de aritmetică

1. Să se arate că numărul natural n este divizibil cu 2 (cu 5) dacă şi numai dacă cifra unităţilor sale este divizibilă prin 2 respectiv prin 5).

2. Să se arate că numărul natural n este divizibil cu 4 (cu 25) dacă şi numai dacă numărul format din ultimele sale două cifre este divizibil cu 4 (respectiv cu 25).

Mai general, numărul natural n este divizibil cu 2^k (cu 5^k) dacă şi numai dacă numărul format de ultimele k cifre din scrierea sa în baza zecimală este divizibil cu 2^k (respectiv cu 5^k).

3. Să se arate că numărul natural n este divizibil cu 3 (cu 9) dacă şi numai dacă suma cifrelor sale este divizibilă cu 3 (respectiv cu 9).

4. Să se arate că numărul natural n este divizibil cu 11 dacă şi numai dacă suma alternantă a cifrelor sale este divizibilă cu 11.

5. Să se arate că numărul natural n este divizibil cu 17 (cu 49) dacă şi numai dacă diferenţa, respectiv suma, dintre dublul numărului obţinut din numărul dat suprimându-i ultimele două cifre şi numărul format de cifrele suprimate în ordinea în care se află în numărul dat sunt divizibile cu 17 (respectiv cu 49).

6. Să se arate că numărul natural n este divizibil cu 17 (cu 59) dacă şi numai dacă diferenţa dintre triplul numărului obţinut din numărul dat suprimându-i ultimele trei cifre şi numărul format din cifrele suprimate în ordinea în care se află numărul dat este multiplu de 17 (respectiv 59).

7. Să se arate că numărul natural n este divizibil cu 97 (cu 103) dacă şi numai dacă suma, respectiv diferenţa, dintre triplul numărului obţinut din numărul dat suprimându-i ultimele două cifre şi numărul format din cifrele suprimate în ordinea în care se află în numărul dat este multiplu de 97 (respectiv 103).

8. Să se arate că numărul natural n este divizibil cu 101 dacă şi numai dacă despărţindu-l în grupe de câte două cifre începând de la dreapta, diferenţa dintre suma

numerelor formate de grupele de rang impar şi suma numerelor formate de grupele de rang par este divizibilă cu 101.

9. Să se arate că numărul natural n este divizibil prin $10k \pm 1$ dacă şi numai dacă suprimându-i ultima cifră şi scăzând, respectiv adunând, de k ori cifra suprimată se obţine un număr divizibil cu $10k \pm 1$.

Ca aplicaţie să se enunţe criterii de divizibilitate cu 19, 29, 49, 21, 31 şi 41.

10. In ce sistem de numeraţie este valabilă înmulţirea $25 \times 314 = 10274$?

11. In ce bază 297 este divizor al lui 792 ?

12. In orice sistem de numeraţie, numărul 10101 este divizibil cu 111.

13. In orice bază mai mare ca 7 numărul 1367631 este cub perfect.

14. Un număr natural este divizibil cu 2, în sistemele de numeraţie cu bază pară, dacă şi numai dacă ultima sa cifră este pară, şi în sistemele de numeraţie cu bază impară, dacă şi numai dacă numărul cifrelor impare este par.

15. Un număr natural este divizibil cu 3, în sistemele de numeraţie cu baza $b = 3m$, dacă ultima sa cifră este multiplu de 3, în sistemele de numeraţie cu baza $b = 3m+1$, dacă suma cifrelor sale este multiplu de 3, în sistemele de numeraţie cu baza $b = 3m - 1$, dacă diferenţa între suma cifrelor de ordin par şi suma cifrelor de ordin impar este multiplu de 3.

16. Să se arate că diferenţa dintre un număr natural şi inversul său, scrise în baza b, se divide cu $b - 1$. Dacă numărul cifrelor numărului dat este impar această diferenţă se divide şi prin $b + 1$.

17. Un număr natural scris în baza b se divide prin $bk + 1$ sau $bk - 1$ (unde k este tot natural) dacă şi numai dacă suprimându-i ultima cifră şi scăzând respectiv adunând de k ori cifra suprimată se obţine un număr divizibil prin $bk + 1$ sau $bk - 1$.

18. Se aşază cifrele 1, 2, 3, 4, 5, 6, 7, 8 într-o ordine oarecare şi se obţine numărul n în sistemul de numeraşie cu baza 12, apoi într-o altă ordine oarecare şi se obţine numărul m (în aceeaşi bază). Să se arate că $n \nmid m$.

19. Să se arate că oricare ar fi numărul n scris în sistemul de numeraţie cu baza 10, există un alt număr de n cifre, scris doar cu cifrele 1 şi 2 divizibil prin 2^n. Să se studieze problema şi în sistemele de numeraţie cu baza 4 şi 6.

20. Să se demonstreze că în sistemul de numeraţie cu baza 6, nici un număr format din mai multe cifre, toate egale, nu este pătrat perfect.

21. Să se arate că în sistemul de numeraţie cu baza 12, nici un număr format din mai multe cifre, toate egale nu poate fi pătrat perfect.

22. Să se demonstreze că în sistemul de numeraţie cu baza 6, nici un număr cu toate cifrele egale nu este cub perfect.

23. Să se demonstreze că pentru orice număr natural n avem $\frac{S(8N)}{S(N)} \geq \frac{1}{8}$, unde S(A) este suma cifrelor numărului A (în scrierea zecimală).

24. Să se arate că pentru $n \geq 4$ numărul $1! + 2! + ... + n!$ nu este pătrat perfect.

25. Fie $n \in \mathbf{N}$.

(i) Să se arate că $16 \mid 24n^2 + 8n$;

(ii) Să se deducă de aici că restul împărţirii lui $(2n+1)^4$ prin 16 este 1;

(iii) Dacă există $x_1, ..., x_k \in \mathbf{N}$ astfel încât $16n + 15 = x_1^4 + x_2^4 + ... + x_k^4$, atunci $k \geq 15$.

26. Să se arate că dacă $\frac{p}{q}$ şi $\frac{r}{s}$ sunt fracţii ireductibile astfel încât $\frac{p}{q} + \frac{r}{s} = 1$, atunci $q = s$.

27. Să se arate că dacă $a, b \in \mathbf{N}^*$, atunci $(a, b)[a, b] = a \cdot b$.

28. Fie $x_1, x_2, ..., x_n \in \{\pm 1\}$ astfel încât $x_1x_2 + x_2x_3 + ... + x_{n-1}x_n + x_nx_1 = 0$. Să se demonstreze că $4 \mid n$.

29. Să se demonstreze că pentru orice număr prim p, numărul: $\underbrace{11...1}_{p \text{ ori}}\underbrace{22...2}_{p \text{ ori}}\underbrace{33...3}_{p \text{ ori}}...\underbrace{99...9}_{p \text{ ori}} - 123456789$ se divide prin p.

30. Dacă $n \in \mathbf{N}^*$, atunci cea mai mare putere naturală a lui 2 ce divide pe $[(1+\sqrt{3})^{2n+1}]$ este $n+1$.

31. Dacă $p \geq 3$ este un număr prim, atunci:

$$[(\sqrt{5}+2)^p] - 2^{p+1} \equiv 0 (\text{mod } p)$$

32. Să se arate că pentru orice număr natural $n \in \mathbf{N}^*$ exponentul maxim al lui 2 în $(n+1)(n+2)...(2n)$ este n.

33. Să se arate că orice număr natural $n \in \mathbf{N}^*$ admite multiplii ce se scriu în sistemul zecimal doar cu 0 şi 1. Să se deducă de aici că orice număr natural $n \in \mathbf{N}$ astfel încât $(n, 10) = 1$ admite multiplii în care toate cifrele sunt 1.

34. Să se arate că dacă $a, m, n \in \mathbf{N}^*, a \geq 2$ iar n este impar, atunci $(a^n - 1, a^m + 1)$ este 1 sau 2.

35. Dacă $a, m, n \in \mathbf{N}^*$ şi $m \neq n$, atunci:

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, \text{dacă } a \text{ este par} \\ 2, \text{dacă } a \text{ este impar.} \end{cases}$$

36. Fie $n \in \mathbf{N}^*$ şi $x = [(2+\sqrt{3})^n]$. Atunci $\frac{(x-1)(x+3)}{12}$ este pătratul unui număr natural.

37. Dacă $n \in \mathbf{N}, n \geq 2$, atunci $n \nmid 2^n - 1$.

38. Dacă p este un număr prim, atunci $C_{2p}^p \equiv 2 (\text{mod } p)$.

39. Fie p un număr prim iar $a, b \in \mathbf{N}$ astfel încât $a \geq b$. Atunci $C_{pa}^{pb} \equiv C_a^b (\text{mod } p)$.

40. Dacă $a, b, c \in \mathbf{N}^*$, atunci $([a, b], c) = [(a, c), (b, c)]$.

41. Dacă $a, b, c \in \mathbf{N}^*$, atunci $[a, b, c] = \frac{abc(a, b, c)}{(a, b)(a, c)(b, c)}$.

42. Dacă $a, b, c \in \mathbf{N}^*$, atunci $\frac{[a, b, c]^2}{[a, b][a, c][b, c]} = \frac{(a, b, c)^2}{(a, b)(a, c)(b, c)}$.

43. Fie $a_1, a_2, a_3, a_4, a_5 \in \mathbf{Z}$. Dacă:

(*i*) $9 \mid \sum_{k=1}^{3} a_k^3$, atunci $3 \mid \prod_{k=1}^{3} a_k$;

(*ii*) $9 \mid \sum_{k=1}^{5} a_k^3$, atunci $3 \mid \prod_{k=1}^{5} a_k$.

44. Să se arate că $2^{2\cdot 73\cdot 1103} - 2 \equiv 0 (\mod 2 \cdot 73 \cdot 1103)$.

45. Să se arate că $2^{2^5} + 1 \equiv 0 (\mod 641)$.

46. Să se rezolve sistemul:

$$\begin{cases} x \equiv 1 (\mod 7) \\ x \equiv 4 (\mod 9) \\ x \equiv 3 (\mod 5). \end{cases}$$

47. Fie $f \in \mathbf{Z}[X]$ şi $n = p_1^{\alpha_1} ... p_t^{\alpha_t}$ descompunerea lui n în factori primi. Să se arate că $f(x) \equiv 0 (\mod n)$ are soluţie dacă şi numai dacă $f(x) \equiv 0 (\mod p_i^{\alpha_i})$ are soluţie pentru $i = 1, 2, ..., t$.

48. Să se arate că $x^2 \equiv 1 (\mod 2^b)$ are o soluţie dacă $b = 1$, două soluţii dacă $b = 2$ şi 4 soluţii dacă $b \geq 3$.

49. Factorialul căror numere naturale n se termină în 1000 zerouri?

50. Dacă $m, n \in \mathbf{N}$, atunci $\frac{(2m)!(2n)!}{m!n!(m+n)!} \in \mathbf{N}$.

51. Dacă $d_1, d_2, ..., d_k$ sunt toţi divizorii naturali ai unui număr natural $n \geq 1$ atunci $(d_1 d_2 ... d_k)^2 = n^k$.

52. Fie $A = \frac{1}{1 \cdot 2} + \frac{1}{3 \cdot 4} + ... + \frac{1}{1997 \cdot 1998}$ şi $B = \frac{1}{1000 \cdot 1998} + \frac{1}{1001 \cdot 1997} + ... + \frac{1}{1998 \cdot 1000}$. Arătaţi că $\frac{A}{B} \in \mathbf{N}^*$.

53. Demonstraţi că un produs de opt numere naturale consecutive nu poate fi pătratul unui număr natural.

54. Fie $a, b, c \in \mathbf{Z}$ astfel încât $a+b+c | a^2+b^2+c^2$. Demonstraţi că există o infinitate de valori naturale distincte ale lui n pentru care $a + b + c | a^n + b^n + c^n$.

55. Dacă $n \in \mathbf{N}$ şi $a_n = 1^n + 2^n + 3^n + 4^n$, atunci ultima cifră a lui a_n este 4 dacă $n \equiv 0 (\mod 4)$ şi 0 în rest.

56. Demonstraţi că $1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \notin \mathbf{N}$ pentru orice $n \in \mathbf{N}^*, n \geq 2$.

57. Să se demonstreze că pentru orice număr natural $n \geq 1$, numărul

$$S_n = 1 + \frac{1}{3} + \frac{1}{5} + ... + \frac{1}{2n-1} + \frac{1}{2n+1}$$

nu este întreg.

58. Să se demonstreze că pentru orice număr impar a se găseşte un număr natural b astfel încât $2^b - 1$ se divide la a.

59. Fie m, n naturale cu $m > 1$ şi $2^{2m+1} - n^2 \geq 0$. Să se arate că $2^{2m+1} - n^2 \geq 7$.

60. Fie p un număr prim iar $1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-2} + \frac{1}{p-1} = \frac{m}{n}$ cu $m, n \in \mathbf{N}^*, (m, n) = 1$. Să se demonstreze că $p \mid m$.

61. Fie $m, n \in \mathbf{N}^*$. Să se arate că pentru orice alegere a numerelor $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{m+1} \in \{\pm 1\}$, numărul $N = \varepsilon_1 \cdot \frac{1}{n} + \varepsilon_2 \cdot \frac{1}{n+1} + \varepsilon_3 \cdot \frac{1}{n+2} + ... + \varepsilon_{m+1} \cdot \frac{1}{n+m} \notin \mathbf{Z}$.

62. Fie a, m, n numere naturale nenule. Să se arate că $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

63. Dacă $a, b, c \in \mathbf{Z}$ şi $6 \mid a+b+c$ atunci $6 \mid a^3+b^3+c^3$.

64. Să se arate că primele 100 de cifre de după virgulă ale numărului $(\sqrt{26}+5)^{101}$ sunt toate zero.

65. Să se arate că $2^{341} \equiv 2 (\text{mod } 341)$.

10.2 Mulţimea numerelor prime

1. Fie $a, b, c, d \in \mathbf{N}^*$ astfel încât $ad = bc$. Să se arate că $a+b+c+d$ nu poate fi număr prim.

2. Determinaţi toate numerele naturale $n \in \mathbf{N}$ pentru care numerele $n+1, n+3, n+7, n+9, n+13$ şi $n+15$ sunt simultan prime.

3. Determinaţi toate numerele naturale $n \in \mathbf{N}$ pentru care numerele $n, n+2, n+6, n+8, n+12$ şi $n+14$ sunt simultan prime.

4. Să se determine numerele prime p pentru care $p|2^p+1$.

5. Fie $n \in \mathbf{N}$ astfel încât 2^n+1 este număr prim. Atunci $n = 0$ sau $n = 2^m$, cu $m \in \mathbf{N}$.

6. Dacă $n \geq 10$, atunci $p_n^2 < 2^n$(p_n fiind al n-ulea termen din şirul numerelor prime).

7. Fie p un număr prim şi $b_1, b_2, ..., b_r$ numere întregi cu $0 < b_i < p$ pentru orice $1 \leq i \leq r$. Să se arate că utilizând numerele $b_1, b_2, ..., b_r$ se pot forma $r+1$ sume ce dau resturi diferite la împărţirea prin p.

8. Dacă p este un număr prim arbitrar, atunci din orice $2p-1$ numere întregi se pot alege p astfel încât suma lor să se dividă prin p.

9. Dacă $n \geq 2$ este un număr natural oarecare, atunci dintre oricare $2n-1$ numere întregi se pot alege n astfel încât suma lor să se dividă prin n.

10. Demonstraţi că orice număr natural $n \geq 7$ se poate scrie sub forma $n = a+b$ cu $a, b \in \mathbf{N}, a, b \geq 2$ şi $(a, b) = 1$.

11. Demonstraţi că pentru orice $k \geq 3, p_{k+1} + p_{k+2} \leq p_1 p_2 ... p_k$.

12. Pentru fiecare $n \in \mathbf{N}^*$ notăm prin q_n cel mai mic număr prim astfel încât $q_n \nmid n$. Să se arate că $\lim\limits_{n\to\infty} \frac{q_n}{n} = 0$.

13. Să se arate că pentru $n \geq 12$, $\frac{n}{p_n} < \frac{1}{3}$.

14. Să se arate că pentru orice $n \geq 230, p_{2n+1} < 3p_{n-2}$.

10.3 Funcţii aritmetice

1. Să se determine toate numerele $n \in \mathbf{N}^*$ pentru care $\varphi(n!) = 2^n$.

2. Dacă $m, n \in \mathbf{N}^*$, atunci $\varphi(mn) \leq \sqrt{\varphi(m^2)\varphi(n^2)}$.

3. Să se demonstreze că pentru orice $n \in \mathbf{N}^*$

$$\tau(1) + \tau(2) + ... + \tau(n) = [\frac{n}{1}] + [\frac{n}{2}] + ... + [\frac{n}{n}]$$

(unde reamintim că $\tau(n)$ =numărul divizorilor naturali ai lui n).

4. Să se demonstreze că pentru orice $n \in \mathbf{N}^*$

$$\sigma(1) + \sigma(2) + ... + \sigma(n) = [\frac{n}{1}] + 2 \cdot [\frac{n}{2}] + ... + n \cdot [\frac{n}{n}]$$

(unde reamintim că $\sigma(n)$=suma divizorilor naturali ai lui n).

5. Să se demonstreze că pentru orice $n \in \mathbf{N}^*$

$$\tau(n) = \sum_{m \geq 1} ([\frac{n}{m}] - [\frac{n-1}{m}]).$$

6. Dacă $x \in \mathbf{R}$ şi $n \in \mathbf{N}^*$, atunci

$$[x] + [x + \frac{1}{n}] + [x + \frac{2}{n}] + ... + [x + \frac{n-1}{n}] = [nx].$$

(Hermite)

7. Să se demonstreze că pentru un număr natural $n \geq 2$, $\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n}$ dacă şi numai dacă n este prim ($\pi(n)$=numărul numerelor prime mai mici decât n).

8. Să se demonstreze că $\lim\limits_{n \to \infty} \frac{\sigma(n!)}{n!} = \infty$.

9. Fie $f :\in \mathbf{N}^* \to \mathbf{N}^*$ astfel încât $f(mn) = f(m)f(n)$ pentru orice $m, n \in \mathbf{N}^*$ iar $(p_k)_{k \geq 0}$ şirul numerelor prime. Dacă $f(p_k) = k + 1$ pentru orice $k \in \mathbf{N}$, atunci $\sum\limits_{n \geq 1} \frac{1}{f^2(n)} = 2$.

10. Funcţia μ este multiplicativă.

11. Dacă m, n sunt numere naturale, $m, n \geq 1$, atunci

$$[mx] + [mx + \frac{m}{n}] + ... + [mx + \frac{(n-1)m}{n}] = [nx] + [nx + \frac{n}{m}] + ... + [nx + \frac{(m-1)n}{m}].$$

10.4 Resturi pătratice

1. Să se calculeze $(\frac{15}{71}), (\frac{6}{35})$ şi $(\frac{335}{2999})$.

2. Să se arate că există o infinitate de numere prime de forma $4n + 1$, cu $n \in \mathbf{N}$.

3. Dacă $p \geq 5$ este un număr prim, atunci:

$$(\frac{-3}{p}) = \begin{cases} 1, \text{ dacă } p \equiv 1 (\text{mod } 6) \\ -1, \text{ dacă } p \equiv -1 (\text{mod } 6) \end{cases}$$

4. Să se arate că există o infinitate de numere prime de forma $6n + 1$, cu $n \in \mathbf{N}$.

5. Să se stabilească dacă congruenţa $x^2 \equiv 10 (\text{mod } 13)$ are sau nu soluţii.

6. Aceeaşi chestiune pentru congruenţa $x^2 \equiv 21 (\text{mod } 23)$.

7. Dacă p este un număr prim de forma $6k + 1$, atunci există $x, y \in \mathbf{N}$ astfel încât $p = 3x^2 + y^2$.

8. Să se arate că $(\frac{-2}{p}) = \begin{cases} 1, \text{ dacă } p \equiv 1, 3 (\text{mod } 8) \\ -1, \text{ dacă } p \equiv -1, -3 (\text{mod } 8). \end{cases}$

10.5 Fracţii continue

1. Să se arate că:

$\sqrt{a^2-1}=(a-1;\overline{1,2a-2}),\sqrt{a^2-a}=(a-1;\overline{2,2a-2}),$ pentru $a\in\mathbf{N},a\geq 2.$

2. Dacă a este un număr impar atunci

$$\sqrt{a^2+4}=(a;\overline{\frac{a-1}{2},1,1,\frac{a-1}{2},2a})\text{ dacă }a\geq 2\text{ şi}$$

$$\sqrt{a^2+4}=(a-1;\overline{1,\frac{a-3}{2},2,\frac{a-3}{2},1,2a-2})\text{ dacă }a\geq 4.$$

3. Dacă $a\in\mathbf{N}^*$, atunci $\sqrt{4a^2+4}=(2a;\overline{a,4a})$.

4. Dacă $a,n\in\mathbf{N}^*$, atunci

$$\begin{aligned}\sqrt{(na)^2+a}&=(na;\overline{2n,2na}),\\ \sqrt{(na)^2+2a}&=(na;\overline{n,2na}),\\ \sqrt{(na)^2+-a}&=(na-1;\overline{1,2n-2,1,2(na-1)})(n\geq 2).\end{aligned}$$

5. Să se determine numerele naturale de 3 cifre $\overline{xyx}$ astfel încât $317\mid\overline{xyz398246}$.

6. Fie $\alpha=[a_0;a_1,...,a_n,a_{n+1},...,a_{2n+1}]$ unde $a_{n+i}=a_{n-i+1},1\leq i\leq n$. Dacă notăm redusele lui α prin $\pi_n=\frac{p_n}{q_n}$, atunci $p_{2n+1}=p_n^2+p_{n-1}^2$ şi $q_{2n}=q_n^2+q_{n-1}^2$, pentru orice $n\in\mathbf{N}$.

7. Fie $\alpha=[1;a_1,...,a_n,a_n,...,a_2,a_1]$ iar $\pi_n=\frac{p_n}{q_n}$ a n-a redusă a lui $\alpha(n\in\mathbf{N}^*)$. Să se arate că $q_{2n}=\frac{p_{2n}p_{2n+1}-1}{p_{2n}+p_{2n+1}}$.

8. Dacă $\pi_n=\frac{p_n}{q_n}$ este a n-a redusă a fracţiei continue ataşată lui $\sqrt{2}$ atunci

$$\lim_{n\to\infty}\{(\sum_{k=0}^{n}q_k)\sqrt{2}\}-q_{n+1}=-\frac{\sqrt{2}}{2}.$$

9. Dacă $\pi_n=\frac{p_n}{q_n}$ este a n-a redusă a lui $\sqrt{2}$, atunci

(i) $p_{n+1}=p_n+2q_n$, (ii) $q_{n+1}=p_n+q_n$,

(iii) $p_{n+1}=q_{n+1}+q_n$, (iv) $6p_{n+1}=p_{n+3}+p_{n-1}(n\geq 3)$,

(v) $6q_{n+1}=q_{n+2}+q_{n-1}(n\geq 3)$, (vi) $p_{n+1}=6(p_n-p_{n-2})+p_{n-3}(n\geq 3)$,

(vii) $q_{n+1}=6(q_n-q_{n-1})+q_{n-3}(n\geq 3)$, $(viii)$ $p_n^2-2q_n^2=(-1)^{n+1}$,

(ix) $p_{n-1}^2-p_np_{n-2}=2(-1)^{n-1}(n\geq 2)$.

10. Să se demonstreze că pentru orice $a\in\mathbf{N}^*$ numitorii reduselor de rang par ai fracţiei continue a lui $\sqrt{a^2+1}$ sunt numere naturale impare, iar cei de rang impar sunt numere naturale pare.

11. Să se dezvolte în fracţie continuă $\sqrt{D}$ cu $D=[(4m^2+1)n+m]^2+4mn+1,m,n\in\mathbf{N}^*$.

10.6 Teoreme de reprezentare pentru numere întregi

1. Fie $q \in \mathbf{Q}, 0 < q < 1$. Să se arate că există $n \in \mathbf{N}^*$ astfel încât $\frac{1}{n+1} \leq q < \frac{1}{n}$.

Să se deducă de aici că orice $q \in \mathbf{Q}$ cu $0 < q < 1$ se poate reprezenta sub forma $q = \sum_{i=0}^{k} \frac{1}{n_i + 1}$ cu $n_i \in \mathbf{N}$ toate distincte şi $k \in \mathbf{N}^*$. Să se efectueze această descompunere în cazurile particulare $q = \frac{7}{22}$ şi $q = \frac{47}{60}$.

2. Să se arate că orice număr natural n se poate reprezenta în mod unic sub forma

$$n = e_0 + 3e_1 + ... + 3^k e_k$$

unde pentru orice $i, 0 \leq i \leq k, e_i \in \{-1, 0, 1\}$.

3. Să se arate că orice fracţie subunitară ireductibilă $\frac{a}{b}$ se poate scrie sub forma

$$\frac{a}{b} = \frac{1}{q_1} + \frac{1}{q_1 q_2} + ... + \frac{1}{q_1 q_2 ... q_n}$$

unde $q_1, ..., q_n \in \mathbf{N}^*, q_1 \leq q_2 \leq ... \leq q_n$.

4. Demonstraţi că orice număr întreg n admite o infinitate de reprezentări sub forma $n = x^2 + y^2 - z^2$ cu x, y, z numere naturale mai mari ca 1.

5. Demonstraţi că numărul 3^{2k} (cu $k \in \mathbf{N}^*$) se poate scrie ca sumă a 3^k numere naturale consecutive.

6. Demonstraţi că pentru orice $z \in \mathbf{Z}$, un număr raţional $x > 1$ se poate scrie sub forma

$$x = (1 + \frac{1}{k})(1 + \frac{1}{k+1})...(1 + \frac{1}{k+s}), \text{ cu } s \in \mathbf{N} \text{ şi } k \in \mathbf{Z}, k > z.$$

7. Să se arate că orice număr prim $p \geq 3$ se poate scrie în mod unic ca diferenţa a două pătrate de numere naturale.

8. Care numere naturale pot fi scrise ca diferenţă de două pătrate de numere întregi?

9. Să se arate că numerele întregi de forma $4m+3$ nu se pot scrie sub forma $x^2 - 3y^2$ cu $x, y \in \mathbf{N}$.

10. Să se arate că dacă n se poate scrie sub forma $x^2 - 3y^2$ cu $x, y \in \mathbf{N}$, atunci n se poate scrie sub această formă într-o infinitate de moduri.

11. Dacă p este prim, $p > 3$ atunci $4p^2 + 1$ se poate scrie ca sumă de 3 pătrate de numere naturale.

12. Să se arate că orice fracţie ireductibilă $\frac{m}{n}$ cu $0 < \frac{m}{n} < 1$ poate fi scrisă sub forma

$$\frac{m}{n} = \frac{1}{q_1} + \frac{1}{q_2} + ... + \frac{1}{q_r}$$

unde $q_i \in \mathbf{N}^*$ pentru $1 \leq i \leq r$ astfel încât $q_1 < q_2 < ... < q_r$ şi $q_k \mid q_{k-1}$ pentru orice $2 \leq k \leq r$.

13. Demonstraţi că dacă $n \in \mathbf{N}^*$, atunci orice număr $k \in \{1, 2, ..., \frac{n(n+1)}{2}\}$ se poate scrie sub forma $k = \frac{1}{a_1} + \frac{2}{a_2} + ... + \frac{n}{a_n}$ cu $a_1, a_2, ..., a_n \in \mathbf{N}^*$.

14. Să se arate că numărul descompunerilor unui număr natural nenul n ca sumă de numere naturale nenule consecutive este egal cu numărul divizorilor impari ai lui n.

15. Să se demonstreze că orice număr natural n poate fi scris sub forma

$$\frac{(x+y)^2+3x+y}{2},$$

unde x şi y sunt numere naturale şi că această reprezentare este unică.

10.7 Ecuaţii diofantice

1. Să se arate că în $\mathbf{Z}^3$ ecuaţia $x^2+y^2+z^2=2xyz$ are numai soluţia banală (0, 0, 0).

2. Să se arate că în $\mathbf{Z}^3$ ecuaţia $x^2+y^2+z^2+t^2=2xyzt$ are numai soluţia banală (0, 0, 0, 0).

3. Să se arate că în $\mathbf{N}^2$ ecuaţia $3^x-2^y=1$ admite numai soluţiile (1,1) şi (2,3).

4. Să se rezolve ecuaţia $x^2+y^2+2xy-mx-my-m-1=0$ în $\mathbf{N}^2$ şiind că $m\in\mathbf{N}$.

5. Să se arate că ecuaţia $x^2-y^3=7$ nu admite soluţii $(x,y)\in\mathbf{N}^2$.

6. Să se arate că ecuaţia $x^2-2y^2+8z=3$ nu admite soluţii $(x,y,z)\in\mathbf{Z}^3$.

7. Dacă $x,y,z\in\mathbf{N}$ iar $x^2+y^2+1=xyz$, atunci $z=3$.

8. Să se rezolve în $\mathbf{N}^{*3}$ ecuaţia $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1$.

9. Să se rezolve în $\mathbf{N}^{*2}$ ecuaţia $\frac{1}{x}+\frac{1}{y}=\frac{1}{a}$, unde $a\in\mathbf{Z}^*$.

10. Să se rezolve în $\mathbf{Q}_+^*$ ecuaţia $x^y=y^x$.

11. Să se rezolve în $\mathbf{N}^{*4}$ ecuaţia $\frac{1}{x^2}+\frac{1}{y^2}+\frac{1}{z^2}+\frac{1}{t^2}=1$.

12. Să se demonstreze că există o infinitate de perechi $(x,y)\in\mathbf{N}^2$ pentru care $3x^2-7y^2+1=0$.

13. Să se rezolve în $\mathbf{N}^4$ ecuaţia $x^2+y^2+z^2=t^2$.

14. Să se determine $x,y,z,t\in\mathbf{N}$ pentru care $xy=zt$.

15. Dacă $x,y,z\in\mathbf{N}$ astfel încât $x^2+y^2+z^2=1993$, atunci $x+y+z$ nu este pătrat perfect.

16. Dacă $n,p\in\mathbf{N}^*$, atunci ecuaţia $x_1^p+...+x_n^p=(x_1+...+x_n)^p+1$ nu are soluţii în numere întregi.

17. Să se arate că ecuaţia $y^2=x^5-4$ nu are soluţii întregi.

18. Să se arate că ecuaţia $y^2=x^3+7$ nu are soluţii întregi.

19. Să se arate că ecuaţia $y^2=x^3+47$ nu are soluţii întregi.

20. Să se arate că ecuaţia $x^3+2y^3+4z^3-6xyz=0$ nu are în $\mathbf{Z}^3$ decât soluţia (0,0,0).

21. Să se arate că ecuaţia $x^2+y^2=4^z$ nu are soluţii în $\mathbf{N}^{*3}$.

10.8 Puncte laticeale în plan şi spaţiu

1. Să se demonstreze că dacă un cerc având raza de lungime un număr natural trece prin două puncte laticeale situate la distanţa 1 unul de celălalt, atunci pe circumferinţa sa nu se mai află nici un alt punct laticeal.

2. Să se demonstreze că dacă pentru orice număr natural n există în plan un cerc de centru având coordonatele (a, b) ce conţine în interiorul său exact n puncte laticeale, atunci a şi b nu pot fi simultan raţionale.

3. Fie $\mathcal{C}$ cercul circumscris pătratului determinat de punctele laticeale de coordonate (0, 0), (1978, 0), (1978, 1978) şi (0, 1978).

Să se demonstreze că $\mathcal{C}$ nu mai conţine pe circumferinţa sa nici un alt punct laticeal diferit de cele patru vârfuri ale pătratului.

4. Să se demonstreze că oricare ar fi 9 puncte laticeale în spaţiu, există cel puţin un punct laticeal situat în interiorul unui segment determinat de punctele date.

10.9 Clase speciale de numere întregi

1. Demonstraţi că nici unul dintre numerele lui Fermat $F_n = 2^{2^n} + 1$ cu $n > 1$ nu se poate scrie sub foma $p + q$, cu p şi q numere prime.

2. Arătaţi că F_4 este cel mai mic divizor prim al numărului $12^{2^{15}} + 1$.

3. Să se arate că orice număr impar n este divizor pentru o infinitate de numere Mersenne.

4. Să se arate că pentru $m, n \geq 2$ nu putem găsi $k \in \mathbf{N}$ astfel încât $M_k = k^m$.

5. Câte cifre are numărul $M_{101} = 2^{101} - 1$?

6. Să se demonstreze că pentru orice număr compus impar n care divide pe M_{n-1}, există un număr compus impar m cu $m > n$ care de asemenea divide pe M_{m-1}.

7. Să se arate că numărul $n = 2 \cdot 73 \cdot 1103 \cdot 2089$ este pseudo-prim.

8. Să se arate că $t_{132}^2 + t_{143}^2 = t_{164}^2$.

9. Să se arate că şirul $(F_n)_{n\geq}$ de numere Fibonacci verifică relaţiile:

(i) $\sum_{k=1}^{n} F_{2k} = F_{2n+1} - 1$;

(ii) $F_{2n} + F_n^2 = 2F_nF_{n+1}$;

(iii) $F_{2n} = F_{n+1}^2 - F_{n-1}^2$;

(iv) $\sum_{k=1}^{2n-1} F_kF_{k+1} = F_{2n}^2$;

(v) $F_{n+3}^2 - 2F_{n+2}^2 - 2F_{n+1}^2 + F_n^2 = 0$.

Capitolul 11

Soluţii

11.1 Elemente de aritmetică

1. Vom scrie n în sistemul zecimal sub forma $n = a_m 10^m + a_{m-1}10^{m-1} + ... + a_2 10^2 + a_1 10 + a_0$, unde $a_0, a_1, ..., a_m$ sunt numere naturale cuprinse între 0 şi 9, $a_m \neq 0$. Prin urmare a_0 reprezintă cifra unităţilor, a_1 cifra zecilor, a_2 cifra sutelor, ş.a.m.d.

Intr-adevăr, $n = 10(a_m 10^{m-1} + a_{m-1}10^{m-2} + ... + a_2 10 + a_1) + a_0$, deci $n = 10k + a_0$. Prin urmare, $2 \mid n$ implică $2 \mid (n - 10k)$, adică $2 \mid a_0$. Reciproc, $2 \mid a_0$ implică $2 \mid 10k + a_0$, adică $2 \mid n$.

Demonstraţia divizibilităţii cu 5 se face analog.

2. Soluţia este asemănatoare cu cea de la exc. 1.

3. Avem $n = a_m 10^m + a_{m-1}10^{m-1} + ... + a_2 10^2 + a_1 10 + a_0 = a_m(10^m - 1) + a_{m-1}(10^{m-1} - 1) + ... + a_2(10^2 - 1) + a_1(10 - 1) + (a_m + a_{m-1} + ... + a_1 + a_0)$.

Din formula $10^k - 1 = (10 - 1)(10^{k-1} + 10^{k-2} + ... + 1) = 9k'$, rezultă că $10^k - 1$ este multiplu de 9, oricare ar fi $k \in \mathbf{N}^*$. Prin urmare, $n = 9k + (a_m + a_{m-1} + ... + a_1 + a_0)$, adică n este divizibil cu 3, respectiv cu 9, dacă şi numai dacă suma cifrelor sale este divizibila cu 3, respectiv cu 9.

4. Vom scrie n în sistemul zecimal sub forma $n = a_m 10^m + a_{m-1}10^{m-1} + ... + a_2 10^2 + a_1 10 + a_0$, unde $a_0, a_1, ..., a_m$ sunt numere naturale cuprinse între 0 şi 9, $a_m \neq 0$. Trebuie demonstrat că $11 \mid \sum_{k=0}^{m} (-1)k_{al}$.

Pentru a demonstra această afirmaţie, vom scrie cu ajutorul formulei binomului lui Newton:

$$10^k = (11 - 1)^k = 11^k - C_k^1 \cdot 11^{k-1} + ... + (-1)^k = 11k' + (-1)^k, k' \in \mathbf{Z}.$$

Prin urmare, $n = 11p + \sum_{k=0}^{m} (-1)k_{al}$ şi deci n este divizibil cu 11 dacă şi numai dacă $\sum_{k=0}^{m} (-1)k_{al}$ este divizibilă cu 11.

5. Fie $N = \overline{a_n a_{n-1}...a_1 a_0}$ numărul dat iar $N' = \overline{a_n a_{n-1}...a_2}$ numărul obţinut din N suprimându-i ultimele două cifre. In mod evident, $N = 10^2 N' + \overline{a_1 a_0}$. Atunci $10^2(2N' - \overline{a_1 a_0}) = 2(10^2 N') - 100 \cdot \overline{a_1 a_0} = 2(N - \overline{a_1 a_0}) - 100 \cdot \overline{a_1 a_0} = 2N - 102 \cdot \overline{a_1 a_0} = 2N - 17 \cdot 6 \cdot \overline{a_1 a_0}$, de unde deducem că $17 \mid N \Leftrightarrow 17 \mid (2N' - \overline{a_1 a_0})$.

Cum $10^2(2N' + \overline{a_1 a_0}) = 2(10^2 N') + 100 \cdot \overline{a_1 a_0} = 2(N - \overline{a_1 a_0}) + 100 \cdot \overline{a_1 a_0} = 2N + 98 \cdot \overline{a_1 a_0} = 2N + 2 \cdot 49 \cdot \overline{a_1 a_0}$, deducem că $49 \mid N \Leftrightarrow 49 \mid (2N + \overline{a_1 a_0})$.

6, 7. Soluţia este asemănătoare cu cea de la exc. 4.

8. Fie $N = \overline{a_n a_{n-1}...a_1 a_0}$ un număr cu $n+1$ cifre. Să presupunem că n este impar. Atunci numerele formate din câte două cifre de rang impar sunt $\overline{a_1 a_0}, \overline{a_5 a_4}, ...,$ $\overline{a_{n-6} a_{n-7}}, \overline{a_{n-2} a_{n-3}}$ iar cele de rang par vor fi $\overline{a_3 a_2}, \overline{a_7 a_6}, ..., \overline{a_{n-4} a_{n-5}}, \overline{a_n a_{n-1}}$ astfel că dacă notăm $N_1 = \overline{a_1 a_0} + \overline{a_5 a_4} + ... + \overline{a_{n-6} a_{n-7}} + \overline{a_{n-2} a_{n-3}}$ şi $N_2 = \overline{a_3 a_2} + \overline{a_7 a_6} + ... + \overline{a_{n-4} a_{n-5}} + \overline{a_n a_{n-1}}$ atunci

$$\begin{aligned} N_1 &= a_0 + a_4 + ... + a_{n-7} + a_{n-3} + 10(a_1 + a_5 + ... + a_{n-6} + a_{n-2}), \\ N_2 &= a_2 + a_6 + ... + a_{n-5} + a_{n-1} + 10(a_3 + a_7 + ... + a_{n-4} + a_n), \text{ iar} \\ N_1 - N_2 &= (a_0 + 10a_1 - a_2 - 10a_3) + (a_4 + 10a_5 - a_6 - 10a_7) + ... + (a_{n-3} + \\ &\quad 10a_{n-2} - a_{n-1} - 10a_n). \end{aligned}$$

Scriind că $N = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_2 10^2 + a_1 10 + a_0$ avem:

$$\begin{aligned} &N - (N_1 - N_2) = (10^2 + 1)a_2 + (10^3 + 10)a_3 + (10^4 - 1)a_4 + (10^5 - 10)a_5 + \\ &(10^6 + 1)a_6 + (10^7 + 10)a_7 + ... + (10^{n-3} - 1)a_{n-3} + (10^{n-2} - 10)a_{n-2} + \\ &(10^{n-1} + 1)a_{n-1} + (10^n + 10)a_n = (10^2 + 1)a_2 + 10(10^2 + 1)a_3 + (10^4 - 1)a_4 + \\ &10(10^4 - 1)a_5 + (10^6 + 1)a_6 + 10(10^6 + 1)a_7 + ... + (10^{n-3} - 1)a_{n-3} + \\ &10(10^{n-3} - 1)a_{n-2} + (10^{n-1} + 1)a_{n-1} + 10(10^{n-1} + 1)a_n. \end{aligned}$$

Se arată uşor acum că toţi coeficienţii lui $a_2, a_3, ..., a_n$ se divid prin 101, de unde concluzia (cazul n par tratându-se analog).

9. Fie $N = \overline{a_n a_{n-1}...a_1 a_0}$ numărul dat iar $N' = \overline{a_n a_{n-1}...a_1}$, adică $N = 10N' + a_0$. Atunci $10(N' - ka_0) = 10N' - 10ka_0 = N - a_0 - 10ka_0 = N - (10k+1)a_0$, de unde concluzia că $(10k+1) \mid N \Leftrightarrow (10k+1) \mid (N' - ka_0)$.

Analog pentru cazul $10k - 1$.

Observăm că $19 = 2 \cdot 10 - 1, 29 = 3 \cdot 10 - 1, 49 = 5 \cdot 10 - 1, 21 = 2 \cdot 10 + 1, 31 = 3 \cdot 10 + 1,$ şi $41 = 4 \cdot 10 + 1$ iar acum criteriile de divizibilitate prin $19, ..., 41$ se enunţă ţinând cont de formularea generală.

10. Notând cu x baza sistemului de numeraţie avem: $(2x+5)(3x^2 + x + 4) = x^4 + 2x^2 + 7x + 4$ de unde rezultă că $x^4 - 6x^3 - 15x^2 - 6x - 16 = 0$ sau $(x+2)(x-8)(x^2+1) = 0$. Deci $x = 8$.

11. In baza 19.

12. Rezultă din identitatea : $b^4+b^2+1=(b^2+b+1)(b^2-b+1)$.

13. $b^6+3b^5+6b^4+7b^3+6b^2+3b+1=(b^2+b+1)^3$.

14. Fie $N=\overline{a_na_{n-1}...a_1a_0}_{(u)}$ cu $u=2k$. Deducem imediat că $2\mid N\Leftrightarrow 2\mid a_0$.

Dacă $u=2k+1$ atunci $N=a_0+a_1(2k+1)+...+a_n(2k+1)^n$ şi se observă că $2\mid N\Leftrightarrow 2\mid(a_0+a_1+...+a_n)$ iar $2\mid(a_0+a_1+...+a_n)\Leftrightarrow$ numărul numerelor impare din mulţimea $\{a_0,a_1,...,a_n\}$ este par.

15. Fie $N=\overline{a_na_{n-1}...a_1a_0}_{(b)}=a_0+a_1b+...+a_nb^n$ cu $0\leq a_i\leq b, 1\leq i\leq n$.

Dacă $b=3m$, atunci $N-a_0$ este multiplu de b, deci de 3, astfel că $3\mid N\Leftrightarrow 3\mid a_0$.

Dacă $b=3m+1$, atunci $N=a_0+a_1(3m+1)+...+a_n(3m+1)^n=a_0+a_1+...+a_n+3t$, cu $t\in\mathbf{N}$, de unde deducem că $3\mid N\Leftrightarrow 3\mid(a_0+a_1+...+a_n)$.

Dacă $b=3m-1$, atunci $N=a_0+a_1(3m-1)+...+a_n(3m-1)^n=a_0-a_1+a_2-a_3+...+a_n(-1)^n+3t$, cu $t\in\mathbf{N}$, de unde deducem că $3\mid N\Leftrightarrow 3\mid(a_0-a_1+a_2-a_3+...+a_n(-1)^n)=[a_0+a_2+...-(a_1+a_3+...)]$.

16. Fie $N=\overline{a_na_{n-1}...a_1a_0}_{(b)}$ şi $\overline{N}=\overline{a_0a_1...a_{n-1}a_n}_{(b)}$ inversatul sau. Atunci $N=a_0+a_1b+...+a_nb^n$ iar $\overline{N}=a_n+a_{n-1}b+...+a_0b^n$, deci $N-\overline{N}=a_0(1-b^n)+a_1(b-b^{n-1})+...+a_n(b^n-1)$, de unde concluzia că $b-1\mid N-\overline{N}$.

Numărul cifrelor lui N este $n+1$. Dacă $n+1$ este impar atunci n este par, $n=2k$ cu $k\in\mathbf{N}$. Cum în acest caz $1-b^n, b-b^{n-1}=b(1-b^{n-2}),...,b^n-1$ se divid prin $b^2-1==(b-1)(b+1)$, deducem că $b+1\mid N$.

17. Fie $N=\overline{a_na_{n-1}...a_1a_0}_{(b)}=a_0+a_1b+...+a_nb^n$ iar $N'=\overline{a_na_{n-1}...a_1}_{(b)}$ numărul obţinut din N suprimându-i ultima cifră a_0, evident $N=a_0+bN'$.

Avem $N'-ka_0=a_1+...+a_nb^{n-1}-ka_0$, deci $b(N'-ka_0)=a_1b+...+a_nb^n-kba_0=(a_0+...+a_nb^n)-a_0(kb+1)=N-a_0(kb+1)$, de unde deducem că $bk+1\mid N'-ka_0$.

Analog pentru $bk-1$.

18. Suma cifrelor, scrisă în baza 10, este 36, deci $n=M_{11}+3$ şi $m=M_{11}+3$. Nu putem avea $m=nq, M_{11}+3=(M_{11}+3)q$ cu $1<q<8$.

19. Prin inducţie după n. Pentru $n=1$ sau $n=2$, se verifică pentru că avem $2\mid 2$ şi $2^2\mid 12$. Presupunem că pentru n proprietatea este adevărată, adică există un număr N de n cifre astfel încât $2^n\mid N$. Să o demonstrăm pentru $n+1$.

Fie $N=2^nq$. Dacă q este par, atunci numărul $2\cdot 10^n+N$, care are $n+1$ cifre, se divide cu 2^{n+1}. Dacă q este impar, atunci numărul $10^n+N=2^n(5^n+q)$, care are $n+1$ cifre, se divide cu 2^{n+1}.

20. Se ţine cont de faptul că în baza 6 un număr este divizibil cu 4 dacă şi numai dacă numărul format din ultimele sale două cifre este divizibil cu 4.

21. Pătratul unui număr par este M_4, iar pătratul unui număr impar este M_8+1. Ultima cifră a unui pătrat perfect scris în baza 12 poate fi 0, 1, 4, 9. Rămân deci posibile numai numerele formate cu cifra 1, 4 sau 9. Dar $11...1=M_8+5, 44...4=M_4, 99...9=$

$M_8 + 5$. Dar din faptul că numerele de forma 11...1 nu pot fi pătrate perfecte, rezultă că nici numerele de forma $44...4 = 4 \cdot 11...1$ nu pot fi pătrate perfecte, şi nici cele de forma 99...9.

22. Pentru ca un număr să fie cub perfect, el trebuie să fie de forma $9m$ sau $9m \pm 1$. Ţinând cont că în sistemul de numeraţie cu baza 6, un număr este divizibil cu 9 dacă şi numai dacă numărul format din ultimele sale două cifre este divizibil cu 9, şi cum numerele de forma $aa...a$ sunt $11...1 = M_9 + 7, 22...2 = M_9 + 5, 33...3 = M_9 + 3, 44...4 = M_9 + 1, 55...5 = M_9 - 1$, rezultă că numerele formate numai cu cifra 1 , 2 sau 3 nu pot fi cuburi perfecte. Dar nici numerele formate numai cu cifra 4 nu pot fi cuburi perfecte pentru că am avea $44...4 = A^3$. Cum membrul stâng este par, rezultă că şi membrul drept este par, deci $2 \mid A^3 \Rightarrow 2 \mid A \Rightarrow 8 \mid A^3$, dar $44...4 = 4 \cdot 11...1 = 4(2k + 1)$ şi deci $8 \nmid 44...4$.

Ramân doar numerele formate cu cifra 5. Dar $55...5 = 5 \cdot 11...1 = 5(1 + 6 + 6^2 + ... + 6^{n-1}) = 5 \cdot \frac{6^n - 1}{5} = 6^n - 1$.

Dacă am avea $6^n - 1 = A^3$ sau $A^3 + 1 = 6^n$ ar trebui ca A să fie impar, deci $A + 1$ par. Dar $A^3 + 1 = (A + 1)(A^2 - A + 1) = 6^n$. Deoarece numerele $A + 1, A^2 - A + 1$ sunt prime între ele sau au pe 3 ca divizor comun şi $A + 1$ este par, rezultă că $A + 1 = 2^n \cdot 3^k$ şi $A^2 - A + 1 = 3^{n-k}, k = 0$ sau $k = 1$. Iar din aceste două relaţii deducem că $2^{2n} \cdot 3^{2k} - 2^n \cdot 3^{k+1} + 3 = 3^{n-k}$.

Pentru $k = 0$, această relaţie nu poate fi satisfacută fiindcă $3 \nmid 2^{2n}$.

Pentru $k = 1$, de asemenea nu poate fi satisfacută fiindcă ar rezulta $n = 2$ şi totodată, $2^4 \cdot 3^2 - 2^2 \cdot 3^2 + 3 = 3$, care este falsă.

23. Se observă că $S(8 \cdot 125) = S(1000) = 1$.

Ne sunt necesare urmatoarele proprietati ale functiei S(N):

1) $S(A + B) = S(A) + S(B)$,

2) $S(A_1 + ... + A_n) = S(A_1) + ... + S(A_n)$,

3) $S(nA) \leq nS(A)$,

4) $S(AB) \leq S(A)S(B)$.

Pentru a ne convinge de 1) este suficient să ne închipuim că numerele A şi B se adună scrise unul sub celălalt. Proprietatea 2) rezultă din 1) printr-o inducţie simplă, 3) este un caz particular al lui 2). Dacă ne închipuim că numerele A şi B se înmulţesc scrise unul sub celalalt şi la ficare cifră a numărului B aplicăm 3) rezultă 4). Acum este uşor să demonstrăm inegalitatea cerută: $S(N) = S(1000N) = S(125 \cdot 8N) \leq S(125) \cdot S(8N) = 8 \cdot S(8N)$ adică $\frac{S(8N)}{S(N)} \geq \frac{1}{8}$.

24. Putem scrie $m_n = 1! + 2! + ... + n! = 33 + \sum_{k=5}^{5} k!$ şi astfel ultima cifră a lui m_n este 3, deci m_n nu poate fi pătrat perfect. Cum $m_4 = 33$, nici m_4 nu este pătrat perfect.

25. i) Putem scrie $24n^2+8n = 8n(3n+1)$ şi se consideră acum cazurile când n este par sau impar.

ii) Se dezvoltă $(2n+1)^4$ şi se ţine cont de i).

iii) Fie $a \in \mathbf{N}$. După punctul precedent, dacă a este impar, atunci restul împărţirii lui a^4 prin 16 este 1 pe când atunci când a este par, evident $16 \mid a^4$. Putem presupune, fără a restrânge generalitatea că $x_1, ..., x_p$ sunt impare iar $x_{p+1}, ..., x_k$ sunt pare ($1 \leq p \leq k$). Atunci $x_1^4 + ... + x_p^4 - 15 = 16n - (x_{p+1}^4 + ... + x_k^4)$.

Insă membrul drept se divide prin 16 şi cum resturile împărţirii prin 16 a lui $x_1, ..., x_p$ sunt toate egale cu 1 deducem că membrul stâng este de forma $16t + p - 15$, de unde cu necesitate $p \geq 15$, cu atât mai mult $k \geq 15$.

26. Putem presupune că $q, s \in \mathbf{N}^*$. Condiţia din enunţ se scrie atunci $sp = q(s-r)$ de unde deducem că $s \mid q(s-r)$. Pe de alta parte, deoarece $\frac{r}{s}$ este ireductibilă, avem $(s, s-r) = 1$, de unde cu necesitate $s \mid q$. Analog $q \mid s$, de unde $q = s$.

27. Fie $a = p_1^{\alpha_1}...p_n^{\alpha_n}$ şi $b = p_1^{\beta_1}...p_n^{\beta_n}$ descompunerile în factori primi ale lui a şi b (cu $\alpha_i, \beta_i \in \mathbf{N}, 1 \leq i \leq n$). Atunci $(a,b) = p_1^{\gamma_1}...p_n^{\gamma_n}$ iar $[a,b] = p_1^{\delta_1}...p_n^{\delta_n}$ unde $\gamma_i = min(a_i, b_i)$ iar $\delta_i = max(a_i, b_i)$, $1 \leq i \leq n$, astfel că: $(a,b)[a,b] = p_1^{\gamma_1+\delta_1}...p_n^{\gamma_n+\delta_n} = p_1^{\alpha_1+\beta_1}...p_n^{\alpha_n+\beta_n} = (p_1^{\alpha_1}...p_n^{\alpha_n})(p_1^{\beta_1}...p_n^{\beta_n}) = ab$ (am ţinut cont de faptul că $\gamma_i + \delta_i = min(\alpha_i, \beta_i) + max(a_i, b_i) = a_i + b_i$, pentru orice $1 \leq i \leq n$).

28. Cum suma $x_1x_2 + ... + x_nx_1$ are exact n termeni (fiecare fiind -1 sau 1) deducem cu necesitate că n este par (căci numărul termenilor egali cu -1 trebuie să fie egal cu numărul termenilor egali cu +1; dacă k este numărul acestora, atunci $n = 2k$).

Deoarece $(x_1x_2)(x_2x_3)...(x_nx_1) = (x_1x_2...x_n)^2 = 1$ deducem că -1 apare de un număr par de ori, adică $k = 2k'$ şi deci $n = 4k'$ cu $k' \in \mathbf{N}^*$.

29. Fie $12...9 = A, \underbrace{11...1}_{p \text{ ori}}...\underbrace{99...9}_{p \text{ ori}} = B, 1\underbrace{00...0}_{p \text{ ori}}2\underbrace{00...0}_{p \text{ ori}}...8\underbrace{00...0}_{p \text{ ori}} = C, \underbrace{11...1}_{p \text{ ori}} = D$.

Atunci $C = 10^{8p} + 2 \cdot 10^{7p} + 3 \cdot 10^{6p} + ... + 8 \cdot 10^p + 9$ iar $B = D \cdot C, C - A = 3(10^{8p} - 10^8) + 2(10^{7p} - 10^7) + 3(10^{6p} - 10^6) + ... + 8(10^p - 10)$, $10^p - 10 = (9D+1) - 10 = 9(D-1)$.

Conform Micii Teoreme a lui Fermat (Corolarul 1.5.3. de la Capitolul 1) $10^p - 10, 10^{2p} - 10^2, ..., 10^{8p} - 10^8$ se divid prin p ca şi $9(D-1)$. Astfel, $B - A = DC - AD + AD - A = D(C-A) + A(D-1)$, adică $p \mid B - A$.

30. Avem:

$$(1+\sqrt{3})^{2n+1} = 1 + C_{2n+1}^1\sqrt{3} + C_{2n+1}^2 3 + C_{2n+1}^3 3\sqrt{3} + ... + C_{2n+1}^{2n}3^n + C_{2n+1}^{2n+1}3^n\sqrt{3}$$

iar

$$(1-\sqrt{3})^{2n+1} = 1 - C_{2n+1}^1\sqrt{3} + C_{2n+1}^2 3 - C_{2n+1}^3 3\sqrt{3} + ... + C_{2n+1}^{2n}3^n - C_{2n+1}^{2n+1}3^n\sqrt{3},$$

de unde

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

sau

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

Cum $0 < \sqrt{3} - 1 < 1$ şi $(1+\sqrt{3})^{2n+1} + (1-\sqrt{3})^{2n+1} \in \mathbf{N}$, deducem că

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

Insă prin calcul direct deducem că:

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

Dacă $(2+\sqrt{3})^n = a_n + b_n\sqrt{3}$ (cu $a_n, b_n \in \mathbf{N}$), atunci $(2-\sqrt{3})^n = a_n - b_n$ şi astfel:

$$[(2+\sqrt{})^{2n+1}] = 2^n(2a_n + 6b_n) = 2^{n+1}(a_n + 3b_n).$$

Insă $a_n + 3b_n$ este impar (deoarece $(a_n + 3b_n)(a_n - 3b_n) = a_n^2 - 9b_n^2 = (a_n^2 - 3b_n^2) - 6b_n^2 = (a_n - b_n\sqrt{3})(a_n + b_n\sqrt{3}) - 6b_n^2 = (2-\sqrt{3})^n(2+\sqrt{3})^n - 6b_n^2 = 1 - 6b_n^2$, de unde concluzia că $n+1$ este exponentul maxim al lui 2 în $[(1+\sqrt{3})^{2n+1}]$.

31. Analog ca în cazul exerciţiului 30, deducem că $(\sqrt{5}+2)^p - (\sqrt{5}-2)^p \in \mathbf{Z}$ şi cum $0 < \sqrt{5} - 2 < 1$, atunci $[(\sqrt{5}+1)^p] = (\sqrt{5}+2)^p - (\sqrt{5}-2)^p = 2[C_p^1 5^{\frac{p-1}{2}} \cdot 2 + C_p^3 5^{\frac{p-3}{2}} \cdot 2^3 + ... + C_p^{p-2} 5 \cdot 2^{p-2}] + 2^{p+1}$, astfel că $[(\sqrt{5}+2)^p] - 2^{p+1} = 2[C_p^1 5^{\frac{p-1}{2}} \cdot 2 + ... + C_p^{p-2} 5 \cdot 2^{p-2}]$ de unde concluzia din enunţ (deoarece se arată imediat că $C_p^k \equiv 0 (\text{mod } p)$ pentru $k = 1, 2, ..., p-2$).

32. Fie $E_n = (n+1)(n+2)...(2n)$. Cum $E_{n+1} = (n+2)(n+3)...(2n)(2n+1)(2n+2) = 2E_n(2n+1)$, prin inducţie matematică se probează că $2^n \mid E_n$, însă $2^{n+1} \nmid E_n$.

33. Pentru fiecare $k \in \mathbf{N}^*$, fie $a_k = \underbrace{\overline{11...1}}_{k \text{ ori}}$. Considerând şirul $a_1, a_2, ..., a_n, a_{n+1}, ...$, conform principiului lui Dirichlet există $p, q \in \mathbf{N}^*, p < q$ astfel încât $n \mid a_q - a_p$.

Insă $a_q - a_p = m \cdot 10^p$, unde $m = \underbrace{\overline{11...1}}_{q-p \text{ ori}}$. Dacă $(n, 10) = 1$ atunci m este multiplu de n.

34. Fie $d = (a^n - 1, a^m + 1)$. Atunci putem scrie $a^n = kd + 1, a^m = rd - 1$ cu $k, r \in \mathbf{N}^*$, astfel că $a^{mn} = (a^n)^m = (kd+1)^m = td + 1$ (cu $t \in \mathbf{N}^*$) şi analog $a^{mn} = (a^m)^n == (rd-1)^n = ud - 1$ (cu $u \in \mathbf{N}^*$, caci n este presupus impar).

Deducem că $td + 1 = ud - 1 \Leftrightarrow (u-t)d = 2$, de unde $d \mid 2$.

35. Fie $d = (a^{2^m} + 1, a^{2^n} + 1)$ şi să presupunem că $m < n$.

Cum $a^{2^n} - 1 = (a-1)(a+1)(a^2+1)(a^{2^2}+1)...(a^{2^{n-1}}+1)$, iar $a^{2^m} + 1$ este unul din factorii din dreapta, deducem că $d \mid a^{2^n} - 1$.

Deoarece $d \mid a^{2^n} + 1$ deducem că $d \mid (a^{2^n}+1) - (a^{2^n}-1) = 2$, adică $d = 1$ sau $d = 2$.

Dacă a este impar, cum $a^{2^n} + 1$ şi $a^{2^m} + 1$ vor fi pare, deducem că în acest caz $(a^{2^m} + 1, a^{2^n} + 1) = 2$, pe când dacă a este par, cum $2 \nmid a^{2^m} + 1$ şi $2 \nmid a^{2^n} + 1$, deducem că în acest caz $(a^{2^m} + 1, a^{2^n} + 1) = 1$.

36. Prin inducţie matematică dupa n se arată că $(2+\sqrt{3})^n = p_n + q_n$ cu $p_n, q_n \in \mathbf{N}$ şi $3q_n^2 = p_n^2 - 1$ (ţinând cont că $p_{n+1} = 2p_n + 3q_n$ şi $q_{n+1} = p_n + 2q_n$).

Atunci $(2+\sqrt{3})^n = p_n + \sqrt{3q_n^2} = p_n + \sqrt{p_n^2 - 1}$ şi $\frac{p_n^2 - 1}{3} = q_n^2$ este pătrat perfect. Cum însă $p_n - 1 \leq \sqrt{p_n^2 - 1} < p_n$ deducem că $2p_n - 1 \leq p_n + \sqrt{p_n^2 - 1} < 2p_n$ sau $2p_n - 1 \leq (2+\sqrt{3})^n < 2p_n$ şi astfel $x = [(2+\sqrt{3})^n] = 2p_n - 1$.

Deducem că

$$\frac{(x-1)(x+3)}{12} = \frac{(2p_n - 2)(2p_n + 2)}{12} = \frac{p_n^2 - 1}{3} = q_n^2.$$

37. Presupunem prin absurd că există $n \in \mathbf{N}, n \geq 2$ astfel încât $n \mid 2^n - 1$. Cum $2^n - 1$ este impar, cu necesitate şi n este impar. Fie $p \geq 3$ cel mai mic număr prim cu proprietatea că $p \mid n$. Conform teoremei lui Euler, $2^{\varphi(p)} \equiv 1 (\text{mod } p)$. Dacă m este cel mai mic număr natural pentru care $2^m \equiv 1 (\text{mod } p)$, atunci cu necesitate $m \mid \varphi(p) = p-1$ astfel că m are un divizor prim mai mic decât p.

Insă $2^n \equiv 1 (\text{mod } n)$ şi cum $p \mid n$ deducem că $2^n \equiv 1 (\text{mod } p)$ şi astfel $m \mid n$. Ar rezulta că n are un divizor prim mai mic decât p-absurd!.

38. Avem

$$\begin{aligned} 4^p &= (1+1)^{2p} = C_{2p}^0 + C_{2p}^1 + ... + C_{2p}^{p-1} + C_{2p}^p + C_{2p}^{p+1} + ... + C_{2p}^{2p-1} + C_{2p}^{2p} \\ &= 2 + 2(C_{2p}^0 + C_{2p}^1 + ... + C_{2p}^{p-1}) + C_{2p}^p. \end{aligned}$$

Insă pentru $1 \leq k \leq p-1$,

$$C_{2p}^k = \frac{(2p)(2p-1)...(2p-k+1)}{1 \cdot 2 \cdot ... \cdot k} = p \cdot \frac{(2p)(2p-1)...(2p-k+1)}{1 \cdot 2 \cdot ... \cdot k}$$

şi cum $C_{2p}^k \in N$ iar pentru $1 \leq k \leq p-1, k \nmid p$, atunci nici $1 \cdot 2 \cdot ... \cdot k \nmid p$, deci $C_{2p}^k \equiv 0 (\text{mod } p)$.

Deducem că $4^p \equiv (2 + C_{2p}^p) (\text{mod } p)$ sau $(4^p - 4) \equiv (C_{2p}^p - 2) (\text{mod } p)$.

Dacă $p = 2$ atunci $C_4^2 = 6$ iar $C_4^2 - 2 = 6 - 2 = 4 \equiv 0 (\text{mod } 2)$.

Dacă $p \geq 3$, atunci $(4, p) = 1$ şi conform Teoremei lui Euler, $4^p - 4 \equiv 0 (\text{mod } p)$, de unde şi $C_{2p}^p - 2 \equiv 0 (\text{mod } p) \Leftrightarrow C_{2p}^p \equiv 2 (\text{mod } p)$.

39. Am văzut că pentru orice $1 \leq k \leq p-1, p \mid C_p^k$, deci în $\mathbf{Z}_p[X]$ avem $(1+X)^p = 1 + X^p$.

Astfel $\sum_{k=0}^{pa} C_{pa}^k X^k = (1+X)^{pa} = [(1+X)^p]^a = (1+X^p)^a = \sum_{j=0}^{a} C_a^j X^{jp}$. Deoarece coeficienţii aceloraşi puteri trebuie să fie congruenţi modulo p, deducem că $C_{pa}^{pb} \equiv C_a^b (\text{mod } p)$ (deoarece C_{pa}^{pb} este coeficientul lui X^{pb} din stânga iar C_a^b este coeficientul tot al lui X^{pb} însă din dreapta) pentru $0 \leq b \leq a$.

40. Se alege $a = p_1^{\alpha_1} ... p_n^{\alpha_n}, b = p_1^{\beta_1} ... p_n^{\beta_n}$ şi $c = p_1^{\gamma_1} ... p_n^{\gamma_n}$, cu $p_1, p_2, ..., p_n$ numere prime iar $\alpha_i, \beta_i, \gamma_i \in \mathbf{N}$ pentru $1 \leq i \leq n$.

Atunci

$$\begin{aligned}
[a,b] &= p_1^{\max(\alpha_1,\beta_1)}...p_n^{\max(\alpha_n,\beta_n)} \text{ pe când} \\
([a,b],c) &= p_1^{\min(\max(\alpha_1,\beta_1),\gamma_1)}...p_n^{\min(\max(\alpha_n,\beta_n),\gamma_n)} \text{ iar} \\
[(a,c),(b,c)] &= [p_1^{\min(\alpha_1,\gamma_1)}...p_n^{\min(\alpha_n,\gamma_n)}, p_1^{\min(\beta_1,\gamma_1)}...p_n^{\min(\beta_n,\gamma_n)}] \\
&= p_1^{\max(\min(\alpha_1,\gamma_1),\min(\beta_1,\gamma_1))}...p_n^{\max(\min(\alpha_n,\gamma_n),\min(\beta_n,\gamma_n))},
\end{aligned}$$

de unde egalitatea cerută deoarece pentru oricare trei numere reale α, β, γ:

$$min[max(\alpha,\beta),\gamma] = max[min(\alpha,\gamma),(\beta,\gamma)]$$

(se ţine cont de diferitele ordonări pentru α, β, γ, de ex. $\alpha \leq \beta \leq \gamma$).

41. Ţinând cont de exerciţiile 27 şi 40 avem:

$$\begin{aligned}
[a,b,c] &= [[a,b],c] = \frac{[a,b]\cdot c}{([a,b],c)} = \frac{\frac{abc}{(a,b)}}{[(a,c),(b,c)]} = \frac{abc}{(a,b)[(a,c),(b,c)]} \\
&= \frac{abc}{(a,b)\cdot\frac{(a,c)\cdot(b,c)}{((a,c),(b,c))}} = \frac{abc(a,b,c)}{(a,b)(a,c)(b,c)}.
\end{aligned}$$

42. Se procedează analog ca la exerciţiul precedent.

43. i) Se ţine cont de faptul că dacă a nu este multiplu de 3, adică $a = 3k \pm 1$, atunci a^3 este de aceeaşi formă (adică $a^3 \equiv \pm 1 (\text{mod } 3)$).

Cum $9 \nmid \pm 1 \pm 1 \pm 1$ deducem că cel puţin unul dintre numerele a_1, a_2, a_3 trebuie să se dividă prin 3.

ii) Analog ca la i) ţinându-se cont de faptul că $9 \nmid \pm 1 \pm 1 \pm 1 \pm 1 \pm 1$.

44. Avem $2 \cdot 73 \cdot 1103 = 161038$ şi $161037 = 3^2 \cdot 29 \cdot 617$. Deci $2^{161037} - 1$ se divide prin $2^9 - 1$ şi $2^{29} - 1$, dar cum $2^9 \equiv 1 (\text{mod } 73)$ şi $2^{29} \equiv 1 (\text{mod } 1103)$ deducem că el se divide şi prin $73 \cdot 1103$ (numerele fiind prime între ele).

45. Cum $641 = 640 + 1 = 5 \cdot 2^7 + 1$ şi $641 = 625 + 16 = 5^4 + 2^4$ rezultă că $5 \cdot 2^7 \equiv -1 (\text{mod } 641)$ şi $2^4 \equiv -5^4 (\text{mod } 641)$.

Din prima congruenţă rezultă $54 \cdot 2^{28} \equiv 1 (\text{mod } 641)$, care înmulţită cu a doua dă $5^4 \cdot 2^{32} \equiv -5^4 (\text{mod } 641)$, de unde $2^{32} \equiv -1 (\text{mod } 641)$ (vezi şi §1 de la Capitolul 9).

46. In cazul nostru particular avem: $b_1 = 1, b_2 = 4, b_3 = 3, m_1 = 7, m_2 = 9, m_3 = 5$ (ţinând cont de notaţiile de la Teorema 1.6.1.) iar $m = 315$.

Cu notaţiile de la demonstraţia Teoremei 1.6.1., avem $n_1 = 315/7 = 45, n_2 = 315/9 = 35$ iar $n_3 = 315/5 = 63$.

Alegem $r_i, s_i \in \mathbf{Z}, 1 \leq i \leq 3$ astfel încât

$$\begin{aligned}
r_1 \cdot 7 + s_1 \cdot 45 &= 1 \text{ (cu ajutorul algoritmului lui Euclid)} \\
r_2 \cdot 9 + s_2 \cdot 35 &= 1 \\
r_3 \cdot 5 + s_3 \cdot 63 &= 1.
\end{aligned}$$

Alegem $e_i = s_i \cdot n_i, 1 \leq i \leq 3$ (adică $e_1 = 45s_1, e_2 = 35s_2$ şi $e_3 = 63s_3$) iar soluţia va fi $x_0 = 1 \cdot e_1 + 4 \cdot e_2 + 3 \cdot e_3$.

47. Dacă $f(x) \equiv 0(\text{mod } n)$ are o soluţie, atunci acea soluţie verifică şi $f(n) \equiv 0(\text{mod } p_i^{\alpha_i})$ pentru orice $1 \leq i \leq t$.

Reciproc, dacă x_i este o soluţie a congruenţei $f(x) \equiv 0(\text{mod } p_i^{\alpha_i})$ pentru $1 \leq i \leq t$, atunci conform Teoremei 1.6.1., sistemul $x \equiv x_i(\text{mod } p_i^{\alpha_i})$ cu $1 \leq i \leq t$ va avea o soluţie şi astfel $f(x) \equiv 0(\text{mod } p_1^{\alpha_1} \cdot ... \cdot p_t^{\alpha_t} = n)$.

48. Totul rezultă din Teorema 1.8.14.

49. Fie $n \in \mathbf{N}$ astfel încât $n!$ se termină în 1000 de zerouri. Cum la formarea unui zerou participă produsul $2 \cdot 5$, numărul zerourilor în care se termină $n!$ va fi egal cu exponentul lui 5 în $n!$ (acesta fiind mai mic decât exponentul lui 2 în $n!$).

Avem deci $[\frac{n}{5}] + [\frac{n}{5^2}] + ... = 1000$ (conform Teoremei 1.3.9.).

Cum $[\frac{n}{5}] + [\frac{n}{5^2}] + ... \leq \frac{n}{5} + \frac{n}{5^2} + ... < \frac{n}{5} \cdot \frac{1}{1 - \frac{1}{5}} = \frac{n}{4}$, cu necesitate $1000 < \frac{n}{4} \Leftrightarrow n > 4000$.

De aici şi din faptul că $[a] > a - 1$ deducem că $1000 > \frac{n}{5} + \frac{n}{5^2} + \frac{n}{5^3} + \frac{n}{5^4} + \frac{n}{5^5} - 5 > \frac{n}{5}(1 + \frac{1}{5} + \frac{1}{25}) + 6 + 1 - 5 = \frac{31}{125}n + 2$, de unde $n < \frac{(1000 - 2) \cdot 125}{31} = 4025, 2$.

Numărul $n = 4005$ verifică, dar $n = 4010$ nu mai verifică .

Deci $n \in \{4005, 4006, 4007, 4008, 4009\}$.

50. Se demonstrează uşor că dacă $a, b \in \mathbf{R}_+$, atunci:

$$[2a] + [2b] \geq [a] + [b] + [a + b]. \quad (*)$$

Exponentul unui număr prim p în $(2m)!(2n)!$ este $e_1 = \sum_{k \in \mathbf{N}^*} ([\frac{2n}{p^k}] + [\frac{2m}{p^k}]$ iar în $m!n!(m + n)!$ este $e_2 = \sum_{k \in \mathbf{N}^*} ([\frac{n}{p^k}] + [\frac{m}{p^k}] + [\frac{n + m}{p^k}]$(conform Teoremei 1.3.9.).

Conform inegalităţii $(*)$ $e_1 \geq e_2$ de unde concluzia că $\frac{(2m)!(2n)!}{m!n!(m + n)!} \in \mathbf{N}$.

51. Dacă $d_1 = 1, d_2, ..., d_{k-1}, d_k = n$ sunt divizorii naturali ai lui n, atunci $\frac{n}{d_1}, \frac{n}{d_2}, ..., \frac{n}{d_k}$ sunt aceiaşi divizori, rearanjaţi însă, de unde deducem că $d_1 \cdot d_2 \cdot ... \cdot d_k = \frac{n}{d_1} \cdot \frac{n}{d_2} \cdot ... \cdot \frac{n}{d_k} \Leftrightarrow (d_1 \cdot d_2 \cdot ... \cdot d_k)^2 = n^k$

52. Cum $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ pentru orice $k \in \mathbf{N}^*$, avem

$$\begin{aligned} A &= 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + ... + \frac{1}{1997} - \frac{1}{1998} = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{1998} \\ &- 2(\frac{1}{2} + \frac{1}{4} + ... + \frac{1}{1998}) = 1 + \frac{1}{2} + ... + \frac{1}{1998} - 1 - \frac{1}{2} - ... - \frac{1}{999} \\ &= \frac{1}{1000} + \frac{1}{1001} + ... + \frac{1}{1998}. \end{aligned}$$

Astfel,

$$\begin{aligned} 2A &= \frac{1}{1000}+\frac{1}{1998}+\frac{1}{1001}+\frac{1}{1997}+...+\frac{1}{1998}+\frac{1}{1000} \\ &= \frac{2998}{1000\cdot 1998}+...+\frac{2998}{1998\cdot 1000}=2998\cdot B, \end{aligned}$$

de unde $\frac{A}{B}=1499\in\mathbf{N}^*$.

53. Fie $p=(n-3)(n-2)(n-1)n(n+1)(n+2)(n+3)(n+4)$ cu $n\in\mathbf{N}, n\geq 4$.

Dacă $n\in\{4,5,6\}$ prin calcul direct se arată că p nu este pătrat perfect.

Pentru $n\geq 7$ avem:

$$p=(n^2-3n)(n^2-3n+2)(n^2+5n+4)(n^2+5n+6)=[(n^2-3n+1)2-1]\cdot[(n^2+5n+5)^2-1]$$

şi atunci (utilizând faptul că $(a^2-1)(b^2-1)=(ab-1)^2-(a-b)^2$) se arată că

$$[(n^2-3n+1)(n^2+5n+5)-2]^2<p<[(n^2-3n+1)(n^2+5n+5)-1]^2.$$

Cum p este cuprins între două pătrate consecutive atunci el nu mai poate fi pătrat perfect.

54. Dacă $a+b+c\mid a^2+b^2+c^2$, atunci $a+b+c\mid 2(ab+ac+bc)$.

Din identitatea $(ab+ac+bc)^2=a^2b^2+a^2c^2+b^2c^2+2abc(a+b+c)$ deducem că $a+b+c\mid 2(a^2b^2+a^2c^2+b^2c^2)$.

Utilizând identităţile:

$$(a^{2^k}b^{2^k}+a^{2^k}c^{2^k}+b^{2^k}c^{2^k})^2=a^{2^{k+1}}b^{2^{k+1}}+a^{2^{k+1}}c^{2^{k+1}}+b^{2^{k+1}}c^{2^{k+1}}+2a^kb^kc^k(a^{2^k}+b^{2^k}+c^{2^k})$$

şi

$$(a^{2^k}++b^{2^k}+c^{2^k})^2=a^{2^{k+1}}+b^{2^{k+1}}+c^{2^{k+1}}+2(a^{2^k}b^{2^k}+b^{2^k}c^{2^k}+a^{2^k}c^{2^k}),$$

prin inducţie matematică (după k) se arată că $a+b+c\mid a^{2^k}+b^{2^k}+c^{2^k}$ şi $a+b+c\mid 2(a^{2^k}b^{2^k}+b^{2^k}c^{2^k}+a^{2^k}c^{2^k})$, pentru orice $k\in\mathbf{N}$.

55. Avem $1^{n+4}\equiv 1^n(\text{mod } 10)$ şi $2^{n+4}\equiv 2^n(\text{mod } 10), 3^{n+4}\equiv 3^n(\text{mod } 10)$ şi $4^{n+4}\equiv 4^n(\text{mod } 10)$, de unde deducem că $a_{n+4}\equiv a_n(\text{mod } 10)$.

Astfel, dacă:

i) $n\equiv 0(\text{mod } 4)$, ultima cifră a lui a_n coincide cu ultima cifră a lui $a_n=1+8+16+256$, adică 4 ;

ii) $n\equiv 1(\text{mod } 4)$, ultima cifră a lui a_n coincide cu ultima cifră a lui $a_1=1+2+3+4$, care este zero;

iii) $n\equiv 2(\text{mod } 4)$, ultima cifră a lui a_n coincide cu ultima cifră a lui $a_2=1+4+9+16$, care este zero;

iv) $n\equiv 3(\text{mod } 4)$, ultima cifră a lui a_n coincide cu ultima cifră a lui $a_3=1+8+27+64$, care este zero.

56. Fie s cel mai mare număr natural cu proprietatea că $2^s = n$ şi considerăm $\sum_{k=0}^{n} \frac{2^{s-1}}{k}$ care se poate scrie sub forma $\frac{a}{b} + \frac{1}{2}$ cu b impar.

Dacă $\frac{a}{b} + \frac{1}{2} \in \mathbf{N}^*$, atunci $b = 2$ (conform exc. 26), absurd.

57. Fie $m = max\{k \in \mathbf{N} : 3^k \leq 2n + 1 < 3^{k+1}\} \geq 1$. Fiecare termen al sumei S_n are ca numitor un număr impar; printre aceşti numitori există unul singur egal cu 3^m iar ceilalţi vor avea forma $3^k \cdot t$ cu t impar, $0 \leq k \leq m$ şi 3 nu îl divide pe t. Atunci cel mai mic multiplu comun al numitorilor va avea forma $3^k \cdot r$ cu r nedivizibil prin 3. Astfel $S_n = \frac{3l+r}{3^m \cdot r} \notin \mathbf{N}$.

58. Considerăm numerele $2^0 - 1, 2^1 - 1, 2^2 - 1, ..., 2^a - 1$. Acestea sunt $a+1$ numere. Două dintre ele cel puţin dau aceleaşi resturi la împărţirea prin a conform Principiului lui Dirichlet. Să presupunem că $2^k - 1$ şi $2^m - 1$ dau resturi egale la împărţirea prin a şi $k < m$. Atunci numărul $(2^m - 1) - (2^k - 1) = 2^k(2^{m-k} - 1)$ se divide prin a şi întrucât a este impar, rezultă că $2^{m-k} - 1$ se divide la a.

La fel se demonstrează şi urmatoarea afirmaţie mai generală: dacă numerele naturale a şi c sunt prime între ele atunci se găseşte un număr natural b astfel încât $c^b - 1$ se divide prin a. Afirmaţia rezultă din urmatoarea Teoremă a lui Euler : Pentru orice numere naturale a şi c, numărul $a^{\varphi(a)+1} - c$ se divide cu a, unde $\varphi(a)$ este numărul numerelor naturale mai mici decât a şi prime cu el, având formula de calcul $\varphi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) ... (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$.

59. Vom demonstra că ecuaţiile $(*)$ $2^{2m+1} - n^2 = k, k = 0, 1, ..., 6$ nu au soluţii. Să observăm că 8 divide 2^{2m+1}.

i). Pentru $k = 0$ ecuaţia $(*)$ nu are soluţie deoarece 2^{2m+1} nu este pătrat perfect;

ii). Pentru $k = 1, 3$ sau 5, dacă $(*)$ ar avea soluţie ar rezulta că n este impar; atunci ar rezulta că n^2 este de forma $8t+1$ şi deci k ($k = 1, 3, 5$) ar trebui să fie de forma $8r-1$, absurd!

iii). Dacă $k = 2$ sau 4 atunci n ar trebui să fie par şi $4 \mid 2^{2m+1} - n^2$ adică $4 \mid k$ (pentru $k = 2, 4$), absurd! Deci $2^{2m+1} - n^2 \geq 7$.

60. Cum $p - 1$ este par, suma din stânga are un număr par de termeni, aşa că îi putem grupa astfel:

$1 + \frac{1}{2} + ... + \frac{1}{p-2} + \frac{1}{p-1} = (1 + \frac{1}{p-1}) + (\frac{1}{2} + \frac{1}{p-2}) + ... = \frac{p}{p-1} + \frac{p}{2(p-2)} + ...$, deci în final obţinem o egalitate de forma $\frac{p \cdot q}{(p-1)!} = \frac{m}{n} \Leftrightarrow pqn = (p-1)!m$ şi cum $p \nmid (p-1)!$ deducem că $p \mid m$.

61. Pentru fiecare $1 \leq k \leq m$ scriem $n + k = 2^{\alpha_k} \cdot u_k$ cu u_k impar şi fie $\alpha_t = max\{\alpha_k : 1 \leq k \leq m\}$.

Pentru $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{m+1} \in \{\pm 1\}$ avem $N = \varepsilon_1 \cdot \frac{1}{n} + \varepsilon_2 \cdot \frac{1}{n+1} + ... + \varepsilon_{m+1} \cdot \frac{1}{n+m} = \sum_{k=1}^{m} \frac{\varepsilon_k}{2^{\alpha_k} u_k} = \frac{\text{sumă de numere pare } + \text{un număr impar}}{2^t \cdot u}$ cu u impar. Deci $N = \frac{p}{q}$ cu p impar iar q par, de unde concluzia că $N \notin \mathbf{Z}$.

62. Să presupunem că $m \geq n$ şi fie $d = (a^m - 1, a^n - 1)$. Impărţind pe m la n putem scrie $m = nq_1 + r_1$ cu $0 \leq r_1 < n$. Cum $d \mid a^m - 1$ şi $d \mid a^n - 1$ deducem că $d \mid a^m - a^n = a^n(a^{m-n} - 1) \Rightarrow d \mid a^{m-n} - 1$. Continuând recursiv deducem că $d \mid a^{m-2n} - 1, ..., d \mid a^{m-nq_1} - 1 = a^{r_1} - 1$. Scriind că $n = r_1q_2 + r_2$ cu $0 \leq r_2 < r_1$, ca mai sus deducem $d \mid a^{r_2} - 1$. Ţinând cont de algoritmul lui Euclid de găsire a lui (m, n) deducem că $d \mid a^{(m,n)} - 1$. Cum în mod evident $a^{(m,n)} - 1 \mid a^m - 1, a^n - 1 \Rightarrow a^{(m,n)} - 1 \mid d$, de unde $d = a^{(m,n)} - 1$.

63. Avem că $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$. Din $6 \mid a + b + c$ deducem că cel puţin unul din numerele a, b, c este par şi atunci $6 \mid 3abc$, de unde concluzia că $6 \mid a^3 + b^3 + c^3$.

64. Scriem $(\sqrt{26}+5)^{101} = [(\sqrt{26}+5)^{101} - (\sqrt{26}-5)^{101}] + (\sqrt{26}-5)^{101}$ şi observăm că $a = (\sqrt{26}+5)^{101} - (\sqrt{26}+-5)^{101} \in \mathbf{Z}$ iar $(\sqrt{26}-5)^{101} = \frac{1}{(\sqrt{26}+5)^{101}} < \frac{1}{(2 \cdot 5)^{101}} = \frac{1}{10^{101}}$, deci $(\sqrt{26}+5)^{101} = a, \underbrace{0...0}_{100 \text{ ori}} 1$.

65. Avem că $2^{10} \equiv 1 (\text{mod } 31)$ şi cum $2^{10} \equiv 1 (\text{mod } 11) \Rightarrow 2^{10} \equiv 1 (\text{mod } 11 \cdot 31)$, astfel că $2^{340} \equiv 1 (\text{mod } 341)$, deci $2^{341} \equiv 2 (\text{mod } 341)$.

11.2 Mulţimea numerelor prime

1. Din condiţia $ad = bc$ deducem existenţa numerelor naturale x, y, z, t astfel încât $a = xy, b = xz, c = yt$ şi $d = zt$. Atunci $a + b + c + d = (x + t)(y + z)$ care este altfel număr compus.

2. Pentru $n = 0, n + 15 = 15$ este compus. Pentru $n = 1, n + 3 = 4$ este compus, pentru $n = 2, n + 7 = 9$ este compus, pentru $n = 3, n + 3 = 6$ este compus, pe când pentru $n = 4$ obţinem şirul: $5, 7, 11, 13, 17, 19$ format din numere prime.

Să arătăm că $n = 4$ este singura valoare pentru care problema este adevarată. Fie deci $n = 5$. Dacă $n = 5k$, atunci $5 \mid n + 15$. Dacă $n = 5k + 1$, atunci $5 \mid n + 9$, dacă $n = 5k + 2$, atunci $5 \mid n + 3$, dacă $n = 5k + 3$, atunci $5 \mid n + 7$, pe când dacă $n = 5k + 4$, atunci $5 \mid n + 1$.

Observaţie. A. Schinzel a emis conjectura că există o infinitate de numere n pentru care numerele $n + 1, n + 3, n + 7, n + 9$ şi $n + 13$ sunt prime (de exemplu pentru $n = 4$, 10 sau 100 conjectura lui Schinzel se verifică).

3. Ca la exerciţiul 2 se arată că numai $n = 5$ satisface condiţiile enunţului.

4. Conform Micii Teoreme a lui Fermat $p \mid 2^p - 2$. Cum trebuie şi ca $p \mid 2^p + 1$ deducem cu necesitate că $p \mid 3$ adică $p = 3$. Atunci $3 \mid 2^3 + 1 = 9$.

5. Dacă $n = 0$ atunci $2^0 + 1 = 2$ este prim.

Dacă $n = 1$ atunci alegem $m = 0$ şi $2^{2^0} + 1 = 3$ este prim.

Să presupunem acum că $n \geq 2$. Dacă prin absurd n nu este de forma 2^m cu $m = 1$, atunci n se scrie sub forma $n = 2^k(2t+1)$, cu $t, k \in \mathbf{N}$ şi atunci $2^n + 1 = 2^{2^k(2t+1)} + 1 = (2^{2^k})^{2t+1} + 1 = M \cdot (2^{2^k} + 1)$ şi deci $2^n + 1$ nu mai este prim, absurd. Deci $n = 0$ sau $n = 2^m$, cu $m \in \mathbf{N}$.

6. Facem inducţie matematică după n. Pentru $n = 10, p_{10} = 29$ şi $29^2 < 2^{10}$. Conform Lemei 2. 3.15., dacă $n \geq 6$, atunci între n şi 2n găsim cel puţin două numere prime, deducem că $p_{n-1} < p_n < p_{n+1} < 2p_{n-1}$, deci dacă admitem inegalitatea din enunţ pentru orice k cu $10 < k \leq n$, atunci $p_n^2 < 4p_{n-1}^2 < 4 \cdot 2^{n-1} = 2^{n+1}$.

7. Facem inducţie după r; pentru $r = 1$ totul este clar deoarece sumele dau ca resturi 0 şi b_1.

Să presupunem afirmaţia adevărată pentru $r = k < p - 1$ şi neadevărată pentru $r = k + 1$ şi vom ajunge la o contradicţie.

Presupunem că sumele formate din k termeni $b_1, b_2, ..., b_k$ dau $k + 1$ resturi diferite $0, s_1, s_2, ..., s_k$. Atunci, întrucât după adaugarea lui $b = b_{k+1}$ numărul sumelor diferite nu trebuie să se mărească, toate sumele $0 + b, s_1 + b, ..., s_k + b$ (modulo p) vor fi cuprinse în mulţimea $\{0, s_1, s_2, ..., s_k\}$ (cu alte cuvinte, dacă la orice element al acestei mulţimi se adaugă b, atunci se obţine din nou un element din aceeaşi mulţime). Astfel, aceasta mulţime conţine elementele $0, b, 2b, 3b, ..., (p-1)b$.

Deoarece $ib - jb = (i - j)b$ iar $0 < i - j < p$ şi $0 < b < p$, atunci în $\mathbf{Z}_p, ij \neq jb$. Contradicţia provine din aceea că mulţimea $\{0, s_1, s_2, ..., s_k\}$ conţine p elemente diferite deşi am presupus că $k + 1 < p$.

8. Fie $a_1 = a_2 = ... = a_p = a_{p+1} = ... = a_{2p-1}$ resturile împărţirii celor $2p - 1$ numere la p. Să conşiderăm acum numerele:

$$(*) \qquad a_{p+1} - a_2, a_{p+2} - a_3, ..., a_{2p-1} - a_p.$$

Dacă unul dintre aceste numere este 0, de exemplu $a_{p+j} - a_{j+1} = 0$, atunci $a_{j+1} = a_{j+2} = ... = a_{j+p}$ iar suma celor p numere $a_{j+1}, a_{j+2}, ..., a_{j+p}$ se divide la p.

Să examinăm cazul în care toate numerele din (*) sunt nenule. Fie x restul împărţirii sumei $a_1 + a_2 + ... + a_p$ la p. Dacă $x = 0$ totul este clar. Dacă $x \neq 0$, ţinând cont de exerciţiul 8, putem forma din diferentele (*) o sumă care să dea restul $p - x$ la împărţirea cu p.

Adăugând respectivele diferenţe la $a_1 + a_2 + ... + a_p$ şi efectuând reducerile evidente obţinem o sumă formată din p termeni care se divide prin p.

9. Să demonstrăm că dacă afirmaţia problemei este adevărată pentru $n = a$ şi $n = b$ atunci ea este adevărată şi pentru $n = ab$.

Astfel este suficient să demonstrăm afirmaţia pentru n prim (aplicând exerciţiul 9).

Fie date deci $2ab - 1$ numere întregi. Intrucât afirmaţia este presupusă adevărată pentru $n = b$ şi $2ab - 1 > 2b - 1$, din cele $2ab - 1$ numere se pot alege b astfel încât suma acestora se divide prin b.

Apoi din cele rămase (dacă nu sunt mai puţine de $2b-1$) alegem încă b numere care se bucură de această proprietate, ş.a.m.d.

Deoarece $2ab-1=(2a-1)b+(b-1)$ atunci această operaţie se poate repeta de $2a-1$ ori şi să se obţină $2a-1$ alegeri de câte b numere astfel încât media aritmetică a celor b numere este număr întreg. Cum afirmaţia este presupusă adevărată pentru $n=a$, din aceste $2a-1$ medii aritmetice se pot alege a astfel încât suma acestora să se dividă prin a.

Este clar atunci că cele ab numere formate din cele a alegeri de câte b numere au proprietatea cerută, căci $ab=a+a+a+...+a$ (de b ori).

10. Dacă n este impar, $n\geq 7$ atunci $n=2+(n-2)$ şi cum $n-2$ este impar, $(2,n-2)=1$ iar $2>1$ şi $n-2>1$.

Să presupunem acum că n este par şi $n\geq 8$.

Dacă $n=4k$ (cu $k\geq 2$), atunci $n=(2k+1)+(2k-1)$ şi cum $2k+1>2k-1>1$ iar $(2k+1,2k-1)=1$ din nou avem descompunerea dorită.

Dacă $n=4k+2(k\geq 1)$, atunci $n=(2k+3)+(2k-1)$ iar $2k+3>2k-1>1$. Să arătăm că $(2k+3,2k-1)=1$. Fie $d\in\mathbf{N}^*$ astfel încât $d\mid 2k+3$ şi $d\mid 2k-1$. Deducem că $d\mid(2k+3)-(2k-1)=4$, adică $d\mid 4$. Cum d trebuie să fie impar deducem că $d=1$.

11. Cum $k=3, p_1p_2...p_k\leq p_1p_2p_3=2\cdot 3\cdot 5>6$, deci conform exerciţiului 11 putem scrie $p_1p_2...p_k=a+b$ cu $a,b\in\mathbf{N}^*,(a,b)=1$. Avem deci $(a,p_i)=(b,p_j)=1$ pentru orice $i,j\in\{1,2,...,k\}$. Fie $p\mid a$ şi $q\mid b$ cu p şi q prime şi să presupunem că $p<q$. Cum $(p,p_1p_2...p_k)=1$ rezultă că $p\geq p_{k+1}$, deci $q=p_{k+2}$. Cum $a+b=p+q$ deducem relaţia cerută.

12. Fie $m\in\mathbf{N}, m\geq 4$, şi $n\in\mathbf{N}$ astfel încât $n>p_1p_2...p_m$. Există atunci $k\geq m\geq 4$ astfel încât $p_1p_2...p_k\leq n<p_1p_2...p_kp_{k+1}$. Avem că $q_n<p_{k+1}+1<p_k+p_{k+1}$ (căci dacă $q_n\geq p_{k+1}+1>p_{k+1}$ după alegerea lui q_n, atunci fiecare dintre numerele $p_1,p_2,...,p_k,p_{k+1}$ vor fi divizori ai lui n şi am avea $n=p_1p_2...p_kp_{k+1}$, absurd).

Cum $k\geq 4$, conform exerciţiului 12 avem $q_n<p_1p_2...p_{k-1}$ şi deci $\frac{q_n}{n}<\frac{1}{p_k}<\frac{1}{k}\leq\frac{1}{m}$ şi cum m este oarecare deducem că $\frac{q_n}{n}\to 0$ când $n\to\infty$.

13. Avem $\frac{12}{p_{12}}=\frac{12}{37}<\frac{1}{3}$. Presupunem prin absurd că există $n>12$ astfel încât $\frac{n}{p_n}>\frac{1}{3}$. Alegem cel mai mic n cu această proprietate. Atunci $\frac{n-1}{p_{n-1}}<\frac{1}{3}$, de unde deducem că $p_{n-1}<p_n<3n<p_{n-1}+3$, adică $p_n=p_{n-1}+1$, absurd.

14. Considerăm $f:[230,+\infty)\to\mathbf{R}, f(x)=\frac{4}{3}(\ln(x-2)+\ln(\ln(x-2)))-\ln(2x+1)-\ln(\ln(2x+1))-\frac{3}{2}$.

Deoarece pentru $x\geq 230$, $\frac{4}{3(x-2)}>\frac{2}{2x+1}$ şi $\frac{1}{\ln(x-2)}>\frac{1}{\ln(2x+1)}$ deducem imediat că

$$f'(x)=\frac{4}{3}\cdot\frac{1}{x-2}+\frac{4}{3}\cdot\frac{1}{\ln(x-2)}\cdot\frac{1}{x-2}-\frac{2}{2x+1}-\frac{1}{\ln(2x+1)}\cdot\frac{2}{2x+1}>0,$$

adică f este crescătoare pe intervalul $[230,+\infty)$.

Folosind tabelele de logaritmi se arată imediat că $f(230) \approx 0,0443$ şi cum eroarea în scrierea logaritmilor este de cel mult 0,0001, din cele de mai sus deducem că $f(230) > 0$, adică $f(x) > 0$, pentru orice $x \geq 230$.

Deducem astfel că pentru orice $n \in \mathbf{N}, n \geq 230$, avem inegalitatea:

$$\frac{4}{3}(\ln(n-2) + \ln(\ln(n-2)) - \frac{4}{3}) > \ln(2n+1) - \ln(\ln(2n+1)) - \frac{1}{2}.$$

Ţinând cont de această ultimă inegalitate, de inegalităţile din observaţia dinaintea Teoremei 2.4.7. de la Capitolul 2, ca şi de faptul că pentru $n \geq 230$ avem $3(n-2) > \frac{4}{3}(2n+1)$ deducem că pentru $n \geq 230$ avem:

$$\begin{aligned} 3p_{n-2} &> 3(n-2)[\ln(n-2) + \ln(\ln(n-2)) - \frac{3}{2}] > \frac{4}{3}[\ln(n-2) + \ln(\ln(n-2)) - \frac{3}{2}] \\ &> [\ln(2n+1) + \ln(\ln(2n+1)) - \frac{1}{2}] \cdot (2n+1) > p_{n+1} \end{aligned}$$

Observaţie. In [36] p.149 se demonstrează că inegalitatea din enunţ este valabilă şi pentru orice $18 \leq n < 230$.

De asemenea se demonstrează şi urmatoarele inegalităţi:

1) $p_{2n+1} < p_{2n} + p_n$ pentru orice $n \in \mathbf{N}, n \geq 3$;

2) $p_{2n} < p_n + 2p_{n-1}$ pentru orice $n \in \mathbf{N}, n \geq 9, n$ impar;

3) $p_{2n+1} < p_{2n} + 2p_{n-1} - 1$ pentru orice $n \in \mathbf{N}, n \geq 10, n$ par.

11.3 Funcţii aritmetice

1. Din $\varphi(n!) = 2^n$ deducem că $\varphi(1 \cdot 2 \cdot 3 \cdot ... \cdot n) = 2^n$. Cum φ este multiplicativă iar pentru $n \geq 6, n = 3^\alpha \cdot m$ cu $\alpha \geq 2$ şi $(3, m) = 1$ deducem că $\varphi(n!) = \varphi(3^\alpha \cdot m) = \varphi(3^\alpha) \cdot \varphi(m) = (3^\alpha - 3^{\alpha-1}) \cdot \varphi(m) = 3^{\alpha-1} \cdot 2 \cdot \varphi(m)$, astfel că ar trebui ca $3^{\alpha-1} \mid 2^n$ - absurd. Deci $n \leq 5$. Prin calcul direct se arată că numai $n = 5$ convine.

2. Fie p_i factorii primi comuni ai lui m şi n, q_j factorii primi ai lui m ce nu apar în descompunerea lui n şi r_k factorii primi ai lui n ce nu apar în descompunerea lui m. Atunci:

$$\begin{aligned} \varphi(mn) &= mn\prod_i(1 - \frac{1}{p_i})\prod_j(1 - \frac{1}{q_j})\prod_k(1 - \frac{1}{r_k}) \\ \varphi(m^2) &= m^2\prod_i(1 - \frac{1}{p_i})\prod_j(1 - \frac{1}{q_j}) \\ \varphi(n^2) &= n^2\prod_i(1 - \frac{1}{p_i})\prod_k(1 - \frac{1}{r_k}) \end{aligned}$$

(produsele se înlocuiesc cu 1 dacă nu există factori primi p_i, q_j, r_k).

Ridicând la pătrat ambii membrii ai inegalităţii din enunţ şi ţinând cont de egalităţile precedente, aceasta se reduce la inegalitatea evidentă

$$\prod_j(1 - \frac{1}{q_{ij}})\prod_k(1 - \frac{1}{r_k}) \leq 1.$$

Avem egalitate atunci când m şi n au aceiaşi factori primi.

3. Avem

(*) $[\frac{n+1}{k}] = \begin{cases} [\frac{n}{k}[+ 1, \text{ dacă } k \mid n+1 \\ [\frac{n}{k}[, \text{ dacă } k \nmid n+1. \end{cases}$

Vom face inducţie după n (pentru $n = 1$ totul va fi clar).

Să presupunem egalitatea din enunţ adevărată pentru n şi să o demonstrăm pentru $n+1$, adică

$$\tau(1) + \tau(2) + ... + \tau(n+1) = [\frac{n+1}{1}] + [\frac{n+1}{2}] + ... + [\frac{n+1}{n}] + [\frac{n+1}{n+1}].$$

Conform cu (*) în membrul al doilea rămân neschimbaţi termenii al căror numitor nu divide pe $n+1$ şi cresc cu 1 acei termeni al căror numitor $k \mid n+1$ cu $k \leq n$. Deci membrul drept creşte exact cu numărul divizorilor lui $n+1$ (adică cu $\tau(n+1)$) şi astfel proprietatea este probată pentru $n+1$.

4. Ca şi în cazul exerciţiului 4 se face inducţie matematică după n.

5. Dacă $m \mid n$, atunci $n = mq$ şi $[\frac{n}{m}] = q, n-1 = mq-1 = m(q-1)+m-1$, deci $[\frac{n-1}{m}] = q-1$. Astfel $[\frac{n}{m}] - [\frac{n-1}{m}] = q-(q-1) = 1$, deci $\sum\limits_{m|n} ([\frac{n}{m}] - [\frac{n-1}{m}]) = \tau(n)$.

Dacă $m \nmid n$, atunci $n = mq + r$ cu $0 < r < m$ şi $[\frac{n}{m}] = q$. Dar $n-1 = mq+r-1$, $0 \leq r-1 < m$ şi deci $[\frac{n-1}{m}] = q$, adică $[\frac{n}{m}] - [\frac{n}{m}] = 0$ pentru $m \nmid n$.

Avem deci $\sum\limits_{m \geq 1} ([\frac{n}{m}] - [\frac{n-1}{m}]) = \tau(n)$.

6. Dacă $f(x) = [x] + [x + \frac{1}{n}] + ... + [x + \frac{n-1}{n}] - [nx]$, atunci $f(x+1) = f(x)$, deci este suficient să demonstrăm egalitatea din enunţ pentru $0 \leq x \leq 1$.

Scriind că $\frac{k}{n} \leq x < \frac{k+1}{n}$ cu $k \leq n$, atunci $[nx] = k$ iar $f(x) = \underbrace{0 + ... + 0}_{(n-k) \text{ ori}} + \underbrace{1 + ... + 1}_{k \text{ ori}} - k = 0$.

7. Dacă n este prim, atunci $\pi(n) = \pi(n-1) + 1$, deci $\frac{\pi(n)}{n} - \frac{\pi(n-1)}{n-1} = \frac{1}{n} \cdot (1 - \frac{\pi(n-1)}{n-1})$. Cum $\pi(k) < k$ pentru $k \geq 1$ deducem imediat că $\frac{\pi(n)}{n} > \frac{\pi(n-1)}{n-1}$.

Să presupunem acum că $\frac{\pi(n)}{n} > \frac{\pi(n-1)}{n-1}$. Dacă n nu este prim, atunci el este compus şi $\pi(n) = \pi(n-1)$ astfel că am obţine că $\frac{1}{n-1} < \frac{1}{n}$, absurd!.

8. Se arată usor că $\frac{\sigma(m)}{m} = \frac{1}{d_1} + ... + \frac{1}{d_t}$ unde $d_1, ..., d_t$ sunt divizorii naturali ai lui m (evident $t = \tau(m)$).

Deoarece printre divizorii lui $n!$ găsim cel puţin numerele naturale $\leq n$, deducem că $\frac{\sigma(n!)}{n!} \geq \frac{1}{1} + \frac{1}{2} + ... + \frac{1}{n} \underset{n \to \infty}{\longrightarrow} \infty$.

9. Conform unei observaţii anterioare, $p_n < \ln(\ln n + \ln \ln n)$ pentru orice $n \geq 6$; de unde deducem că $p_n < (n+1)^{\frac{5}{3}}$ pentru orice $n \geq 6$.

De asemenea deducem că $f(1) = f(1) \cdot f(1)$, de unde $f(1) = 1, f(2) = f(p_1) = 2, f(3) = f(p_2) = 3, f(5) = 4, f(7) = 5, f(11) = 6$, respectiv, $f(6) = f(2) \cdot f(3) = 6, f(4) = f(2) \cdot f(2) = 4, f(8) = f^3(2) = 8, f(9) = f^2(3) = 9, f(10) = f(2) \cdot f(5) = 2 \cdot 4 = 8$, ş.a.m.d.

Cum $p_1 = 2 < 2^{\frac{5}{3}}, p_2 = 3 < 3^{\frac{5}{3}}, p_3 = 5 < 4^{\frac{5}{3}}, p_4 = 7 < 5^{\frac{5}{3}}, p_5 = 11 < 6^{\frac{5}{3}}$, deducem că (1) $p_n < (n+1)^{\frac{5}{3}}$ pentru orice $n \geq 1$.

Să demonstrăm prin inducţie că şi $f(n) > n^{\frac{5}{3}}$ pentru orice $n \geq 2$.

Dacă n este prim, atunci există $k \geq 1$ astfel încât $n = p_k$ şi $f(n) = f(p_k) = k+1 > p_k^{\frac{5}{3}} = n^{\frac{5}{3}}$

Dacă n este compus atunci $n = p_1^{\alpha_1}...p_s^{\alpha_s}$ şi $f(n) = \prod_{i=1}^{s} f(p_i^{\alpha_i}) > \prod_{i=1}^{s} (p_i^{\frac{5}{3}})^{\alpha_i} = n^{\frac{5}{3}}$

Cum seria $\sum_{n \geq 1} \frac{1}{f^2(n)}$ este absolut convergentă, conform unei Teoreme a lui Euler

$$\begin{aligned} S &= \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{f^2(p)}} = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{f^2(p_k)}} = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{(k+1)^2}} \\ &= \prod_{k=1}^{\infty} \frac{(k+1)^2}{k(k+2)} = \lim_{n \to \infty} \frac{2(n+1)}{(n+2)} = 2 \end{aligned}$$

de unde $S = 2$.

10. Fie $m, n \in \mathbf{N}^*$ cu $(m, n) = 1$. Dacă m are factori pătratici atunci şi mn are factori pătratici şi astfel $\mu(mn) = \mu(m) \cdot \mu(n) = 0$.

Fie $m = p_1...p_k, n = q_1...q_t$ cu p_i şi q_j numere prime distincte. Atunci $mn = p_1...p_k q_1...q_t$ şi cum $(m, n) = 1$, atunci $p_i \neq q_j$, deci $\mu(mn) = (-1)^{k+t} = (-1)^k(-1)^t = \mu(m) \cdot \mu(n)$.

11. Avem $\sum_{k=0}^{m-1} [x + \frac{k}{m} + \frac{j}{n}] = [mx + \frac{mj}{n}]$ şi $\sum_{j=0}^{n-1} [x + \frac{k}{m} + \frac{j}{n}] = [nx + \frac{nk}{m}]$ şi astfel ambele sume din enunţ sunt egale cu $\sum_{k=0}^{m-1} \sum_{j=0}^{n-1} [x + \frac{k}{m} + \frac{j}{n}]$.

11.4 Resturi pătratice

1. Avem $(\frac{15}{71}) = (\frac{3}{71})(\frac{5}{71}) = -(\frac{71}{3})(\frac{71}{5}) = -(\frac{2}{3})(\frac{1}{5}) = 1$,
$(\frac{6}{35}) = (\frac{6}{5})(\frac{6}{7}) = (\frac{1}{5})(\frac{-1}{7}) = -1$,
$(\frac{335}{2999}) = -(\frac{2999}{335}) = -(\frac{-16}{335}) = -(\frac{-1}{335}) = 1$.

2. Presupunem prin reducere la absurd că există doar un număr finit de numere prime de forma $4n+1$ cu $n \in \mathbf{N}^*$; fie acestea $p_1, p_2, .., p_k$. Considerăm numărul $N = 1 + (2p_1p_2...p_k)^2 > 1$. In mod evident, divizorii primi naturali ai lui N sunt numere impare (căci N este impar). Fie $p \mid N$ un divizor prim impar al lui N. Deducem că $p \mid 1 + (2p_1p_2...p_k)^2 \Leftrightarrow (2p_1p_2...p_k)^2 \equiv -1 (\text{mod } p)$ deci $(\frac{-1}{p}) = 1$ adică p este de forma

$4t+1$ (căci am văzut că $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$). Deci, cu necesitate $p \in \{p_1, p_2, ..., p_k\}$ şi am obţinut astfel o contradicţie evidentă: $p \mid 1 + (2p_1p_2...p_k)^2$.

3. Avem $(\frac{-3}{p}) = (\frac{-1 \cdot 3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{3})(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = (\frac{p}{3}) = (\frac{r}{3})$ cu $p \equiv r(\text{mod } 3), r = 0, 1, 2$. Evident nu putem avea $r = 0$.

Dacă $r = 1$, atunci $(\frac{1}{3}) = 1$. Dacă $r = 2$, atunci $(\frac{2}{3}) = (-1)^{\frac{9-1}{8}} = -1$.

Dar $p \equiv 2(\text{mod } 3) \Leftrightarrow p \equiv -1(\text{mod } 3)$. De asemenea $3 \mid p \pm 1 \Leftrightarrow 6 \mid p \pm 1$ deoarece p este impar.

4. Presupunem ca şi în cazul precedent că ar exista numai un număr finit $p_1, p_2, ..., p_k$ de numere prime de forma $6n+1$. Vom considera $N = 3 + (2p_1p_2...p_k)^2 > 3$. Cum N este impar, fie p un divizor prim impar al lui N.

Obţinem că $(2p_1p_2...p_k)^2 \equiv -3(\text{mod } p) = 1$, adică $(\frac{-3}{p})$. Ţinând cont de exerciţiul 3 de mai înainte deducem că p este de forma $6t+1$, adică $p \in \{p_1, p_2, ..., p_k\}$ - absurd (căci din $p \mid N \Rightarrow p = 3$ care nu este de forma $6t+1$).

5. Ţinând cont de exerciţiul 2 avem:

$$\begin{aligned}(\frac{10}{13}) &= (\frac{2 \cdot 5}{13}) = (\frac{2}{13})(\frac{5}{13}) = (-1)^{\frac{13^2-1}{8}}(-1)^{\frac{5-1}{2}\cdot\frac{13-1}{2}}(\frac{13}{5}) = -(\frac{13}{5}) = -(\frac{3}{5}) \\ &= -(-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}}(\frac{5}{3}) = -(\frac{5}{3}) = -(\frac{2}{3}) = -(-1)^{-\frac{-3-1}{4}} = 1,\end{aligned}$$

deci 10 este rest patratic modulo 13 şi în consecinţă ecuaţia $x^2 \equiv 10(\text{mod } 13)$ are soluţii.

6. Avem $(\frac{21}{23}) = (-1)^{\frac{21-1}{2}\cdot\frac{23-1}{2}}(\frac{23}{21}) = (-1)^{\frac{20}{2}\cdot\frac{22}{2}}(\frac{2}{21}) = (-1)^{\frac{21^2-1}{2}} = -1$, deci congruenţa $x^2 \equiv 1(\text{mod } 23)$ nu are soluţii.

7. Să presupunem că p este un număr prim de forma $6k+1$. Atunci $(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{3})$ şi cum $(\frac{p}{3}) = (\frac{1}{3}) = 1$ deducem că:

$$(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{3}{p}) = (\frac{p}{3}) = 1$$

adică -3 este rest pătratic modulo p, deci există $a \in \mathbf{Z}$ astfel încât $a^2 + 3 \equiv 0(\text{mod } p)$.

Conform lemei lui Thue (vezi Lema 6.1.2. de la Capitolul 6) există $x, y \in \mathbf{N}$ astfel încât $x, y \leq \sqrt{p}$ care au proprietatea că la o alegere convenabilă a semnelor + sau -, $p \mid ax \pm y$. Deducem că $p \mid a^2x^2 - y^2$ şi $p \mid a^2 + 3 \Rightarrow p \mid 3x^2 + y^2 \Leftrightarrow 3x^2 + y^2 = pt$ cu $t \in \mathbf{N}$ (cum $x, y \leq \sqrt{p} \Rightarrow 3x^2 + y^2 < 4p$, adică $t < 4$). Rămâne valabil numai cazul $t = 1$ (dacă $t = 2$ va rezulta că p nu este prim iar dacă $t = 3$ deducem că $3 \mid y, y = 3z$ şi $p = x^2 + 3$).

8. Avem ą $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$. Dacă $p \equiv 1, 3(\text{mod } 8)$ atunci $(\frac{-1}{p}) = (\frac{2}{p}) = \pm 1$, deci $(\frac{-2}{p}) = (\pm 1)^2 = 1$. Dacă $p \equiv -1, -3(\text{mod } 8)$ atunci $(\frac{-1}{p}) = -(\frac{2}{p})$, deci $(\frac{-2}{p}) = (-1) \cdot 1 = -1$.

11.5 Fracţii continue

1.- 4. Se aplică algoritmul de după Propoziţia 5.3.15.

5. Dacă notăm cu $a = \overline{xyz}$, cum $1000000 = 3154 \cdot 317 + 182$ şi $398 \cdot 246 = 1256 \cdot 317 + 94$ obţinem că $182a + 94 = 317b$ sau $-182a + 317b = 94$. O soluţie particulară este $a_0 = -5076, b_0 = -2914$ iar soluţia generală este:

$$\begin{aligned} a &= -5076 + 317t \\ b &= -2914 + 182t, \text{ cu } t \in \mathbf{Z}. \end{aligned}$$

Pentru ca a să fie un număr de 3 cifre trebuie să luam $t = 17, 18$ şi 19 obţinând corespunzator numerele $a = 316, 630$ şi 947.

6. Pentru $0 \leq s \leq n$ avem:

$$\begin{aligned} & p_{n-s} \cdot p_{n+s} + p_{n+s-1} \cdot p_{n-s-1} = (p_{n-s-1} \cdot a_{n-s} + p_{n-s-2}) p_{n+s} + p_{n+s-1} \cdot p_{n-s-1} = \\ = \; & p_{n-s-1}(p_{n+s} \cdot a_{n+s} + p_{n+s-1}) + p_{n+s} \cdot p_{n-s-2} = p_{n-s-1}(p_{n+s} \cdot a_{n+s+1} + p_{n+s-1}) + \\ + \; & p_{n+s} \cdot p_{n-s-2} = p_{n-s-1} \cdot p_{n+s+1} + p_{n+s} \cdot p_{n-s-2} = p_{n-(s+1)} \cdot p_{n+(s+1)} + \\ + \; & p_{n+(s+1)-1} \cdot p_{n-(s+1)-1} \end{aligned}$$

Pentru $s = 0$ obţinem

$$p_n \cdot p_n + p_{n-1} \cdot p_{n-1} = p_{n-1} \cdot p_{n+1} + p_n \cdot p_{n-2} = ... = p_{-1} \cdot p_{2n+1} + p_{2n} \cdot p_{-2} = p_{2n+1}$$

sau $p_{2n+1} = p_n^2 + p_{n-1}^2$.

Analog se arată că

$$q_{n-s} \cdot q_{n+s} + q_{n+s-1} \cdot q_{n-s-1} = q_{n-(s+1)} \cdot q_{n+(s+1)} + q_{n+(s+1)-1} \cdot q_{n-(s+1)-1} \text{ pentru } 1 \leq s \leq n,$$

de unde pentru $s = 0$ obţinem

$$q_n^2 + q_{n-1}^2 = q_{n-1} \cdot q_{n+1} + q_n \cdot q_{n-2} = ... = q_{-1} \cdot q_{2n+1} + q_{2n} \cdot q_2 = q_{2n}.$$

7. Se deduc imediat relaţiile: $q_{2n} = p_{2n+1} - q_{2n+1}$ şi $p_{2n+1} \cdot q_{2n} - p_{2n} \cdot q_{2n+1} = -1$, de unde $q_{2n} = \dfrac{p_{2n} p_{2n+1} - 1}{p_{2n} + p_{2n+1}}$.

8. Avem $q_0 = 1, q_1 = 2$ şi $q_n = 2q_{n-1} + q_{n-2}$ pentru $n \geq 2$, de unde deducem că pentru orice $k \in \mathbf{N}, q_k = \dfrac{(1+\sqrt{2})^{k+1} - (1-\sqrt{2})^{k+1}}{2\sqrt{2}}$.

Astfel $(\sum_{k=0}^{n} q_k)\sqrt{2} = q_{n+1} - \dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}(1-\sqrt{2})^{n+2}$, de unde concluzia.

9. Se face inducţie matematică după n ţinându-se cont de relaţiile de recurenţă pentru $(p_n)_{n \geq 0}$ şi $(q_n)_{n \geq 0}$ (date de Propozitia 5.3.1.).

10. Se ştie că $\sqrt{a^2+1}=[a;\overline{2a}]$. Prin inducţie matematică se arată că

$$q_{2n}=2a\sum_{k=0}^{n-1}q_{2k+1}+1 \text{ şi } q_{2n+1}=2a\sum_{k=0}^{n}q_{2k}.$$

11. Cum $[(4m^2+1)n+m]^2\geq D\leq[(4m^2+1)n+m+1]^2$ deducem că: $a_0=[\sqrt{D}]=(4m^2+1)n+m$.

Avem $D-a_0^2=4mn+1$ iar dacă $\sqrt{D}=a_0+\frac{1}{\alpha_1}$ deducem că $\alpha_1=\frac{1}{\sqrt{D}-a_0}=\frac{\sqrt{D}+a_0}{D-a_0^2}$ şi cum $a_0<\sqrt{D}<a_0+1, 2a_0<\sqrt{D}<2a_0+1$ şi cum $a_0=(4mn+1)m+n$ avem $2m+\frac{2n}{4mn+1}<\frac{\sqrt{D}+a_0}{D-a_0^2}<2m+\frac{2n+1}{4mn+1}$.

Ţinând cont că $\frac{2n+1}{4mn+1}<1$ avem că $a_1=[\alpha_1]=2m$.

Scriind că $\alpha_1=a_1+\frac{1}{\alpha_2}$ deducem că $\alpha_2=\frac{1}{\alpha_1-a_1}=\frac{\sqrt{D}+(4mn+1)m-n}{4mn+1}$.

Cum $a_0<\sqrt{D}<a_0+1$ şi $(4mn+1)m+n<\sqrt{D}<(4mn+1)m+n+1$, avem $2m<\alpha_2<2m+\frac{1}{4mn+1}$ de unde $a_2=[\alpha_2]=2m$.

Scriind acum $\alpha_2=a_2+\frac{1}{\alpha_3}$ deducem imediat că

$$\alpha_3=\frac{(4mn+1)[\sqrt{D}+(4mn+1)m+n]}{D-[(4mn+1)m+n]^2}=\sqrt{D}+(4mn+1)m+n=\sqrt{D}+a_0,$$

de unde $a_3=[\alpha_3]=2a_0$, de unde $\sqrt{D}=[(4mn+1)m+n;\overline{2m,2m,2(4mn+1)m+2n}]$.

11.6 Teoreme de reprezentare pentru numere întregi

1. Pentru prima parte putem alege $n=[\frac{1}{q}]$ dacă $\frac{1}{q}\notin\mathbf{N}$ şi $n=[\frac{1}{q}]-1$ dacă $\frac{1}{q}\in\mathbf{N}$.

Fie acum $q\in\mathbf{Q}\cap(0,1)$. Conform celor de mai înainte, există $n_0\in\mathbf{N}$ astfel încât $\frac{1}{n_0+1}\leq q<\frac{1}{n_0}$. Dacă $q=\frac{1}{n_0+1}$ atunci proprietatea este stabilită. In caz contrar avem: $0<q-\frac{1}{n_0+1}=q_1<\frac{1}{n_0(n_0+1)}<1$, deci $q_1\in\mathbf{Q}\cap(0,1)$.

Din nou există $n_1\in\mathbf{N}$ astfel încât $\frac{1}{n_1+1}\leq q_1<\frac{1}{n_1}$. Deoarece $\frac{1}{n_1+1}\leq q_1=q_0-\frac{1}{n_0+1}<\frac{1}{n_0}-\frac{1}{n_0+1}=\frac{1}{n_0(n_0+1)}$ deducem imediat că $n_1+1>n_0(n_0+1)\geq n_0+1$ iar de aici faptul că $n_1>n_0$.

Procedând recursiv, după k paşi vom găsi $q_k\in\mathbf{Q}\cap(0,1)$ şi $n_k\in\mathbf{N}$ astfel încât $\frac{1}{n_k+1}\leq q_k<\frac{1}{n_k}$ şi $n_k>n_{k-1}>...>n_0$.

Să arătăm că procedeul descris mai sus nu poate continua indefinit iar pentru aceasta să presupunem că $q_k=\frac{a_k}{b_k}$. Vom avea $q_{k+1}=\frac{a_{k+1}}{b_{k+1}}=\frac{a_k}{b_k}-\frac{1}{n_k+1}=\frac{a_k(n_k+1)-b_k}{b_k(n_k+1)}$, de unde $a_{k+1}=a_k(n_k+1)-b_k$. Din $a_kn_k-b_k<0$ rezultă imediat $a_{k+1}<a_k$ şi din aproape în aproape $a_{k+1}<a_k<...<a_0$.

Cum între 1 şi a_0 există numai un număr finit de numere naturale, va exista $k_0 \in \mathbf{N}$ pentru care $q_{k_0} - \frac{1}{n_{k_0}+1} = 0$, de unde $q = \sum_{i=0}^{k_0} \frac{1}{n_i+1}$ (faptul că termenii sumei sunt distincţi este o consecinţă a inegalităţilor $n_{k_0} > n_{k_0-1} > ... > n_0$).

In cazurile particulare din enunţ reprezentările sunt date de:

$$\frac{7}{22} = \frac{1}{3+1} + \frac{1}{14+1} + \frac{1}{559+1} \text{ şi } \frac{47}{60} = \frac{1}{1+1} + \frac{1}{3+1} + \frac{1}{29+1}.$$

2. Facem inducţie matematică după n. Pentru $n = 1$, avem $e_0 = 1$ iar $e_i = 0$ pentru $i \geq 1$.

Să presupunem afirmaţia adevarată pentru n şi fie i_0 primul dintre indicii $0, 1, ..., k$ pentru care e_{i_0} este -1 sau 0. Atunci:

$$n+1 = e_0' + 3e_1' + ... + 3^k e_k', \text{ unde } e_i' \begin{cases} -1, \text{ pentru } i < i_0 \\ e_{i_0} + 1, \text{ pentru } i = i_0 \\ e_i, \text{ pentru } i > i_0. \end{cases}$$

Dacă un astfel de indice nu există, urmează $e_0' = e_1' = ... = e_k' = 1$ şi atunci $n + 1 = -1 - 3 + ... + 3^k + 3^{k+1}$. Unicitatea se stabileşte prin reducere la absurd.

3. Fie $q_1 \in \mathbf{N}^*$ cu proprietatea $\frac{1}{q_1} \leq \frac{a}{b} < \frac{1}{q_1 - 1}$. Atunci $\frac{a}{b} - \frac{1}{q_1} = \frac{aq_1 - b}{bq_1}$ şi are numărătorul mai mic strict decât a (căci din $\frac{a}{b} < \frac{1}{q_1 - 1} \Rightarrow aq_1 - b < a$).

Fie $q_2 \in \mathbf{N}^*$ astfel încât $\frac{1}{q_2} \leq \frac{aq_1 - b}{b} < \frac{1}{q_2 - 1}$. Deoarece $aq_1 - b < a$ rezultă $\frac{aq_1 - b}{b} < \frac{a}{b}$, deci $q_2 \geq q_1$.

Rezultă $\frac{1}{q_1 q_2} \leq \frac{aq_1 - b}{b} < \frac{1}{q_1(q_2 - 1)}$.

Avem $\frac{a}{b} - \frac{1}{q_1} - \frac{1}{q_1 q_2} = \frac{aq_1 q_2 - bq_2 - b}{bq_1 q_2}$ (fracţie cu numărator mai mic decât $aq_1 - b$).

Continuând procedeul, numărătorul fracţiei scade continuu cu cel puţin 1 la fiecare pas.

După un număr finit de paşi el va fi zero, deci $\frac{a}{b} = \frac{1}{q_1} + \frac{1}{q_1 q_2} + ... + \frac{1}{q_1 q_2 ... q_n}$.

4. Fie $n = 2k - 1$ cu $k \in \mathbf{N}$. Atunci pentru $e > k$ avem identitatea:

$$n = 2k - 1 = (2e^2 - k)^2 + (2e)^2 - (2e^2 - k + 1)^2$$

(deci putem alege $x = 2e^2 - k, y = 2e, z = 2e^2 - k + 1$).

Dacă n este par, adică $n = 2k$, de asemenea pentru $e > k$ avem identitatea:

$$n = 2k = (2e^2 + 2e - k)^2 + (2e + 1)^2 - (2e^2 + 2e - k + 1)^2$$

(deci în acest caz putem alege $x = 2e^2 + 2e - k, y = 2e + 1, z = 2e^2 + 2e - k + 1$).

Evident, în ambele cazuri, putem alege $e > k$ astfel încât $x, y, z > 1$.

5. Scriind că $3^{2k} = (n+1) + (n+2) + ... + (n+3^k)$ deducem că $n = \frac{3^k - 1}{2} \in \mathbf{N}$.

6. Pentru orice $k, s \in \mathbf{N}^*$ avem $(1+\frac{1}{k})(1+\frac{1}{k+1})...(1+\frac{1}{k+s}) = 1+\frac{s+1}{k}$.

Dacă $x > 1, x \in \mathbf{Q}$ atunci putem scrie $x-1 = \frac{m}{n}$ cu $m, n \in \mathbf{N}^*$ şi $n > z$ (cu z arbitrar, căci nu trebuie neapărat ca $(m,n) = 1$!). Este suficient acum să alegem $k = n$ şi $s = m-1$.

7. Fie $p = x^2 - y^2$ cu $x > y$ şi deci $p = (x-y)(x+y)$ şi cum p este prim $x - y = 1$ şi $x + y = p$ (în mod unic!), de unde $x = \frac{p+1}{2}$ şi $y = \frac{p-1}{2}$.

Deci $p = (\frac{p+1}{2})^2 - (\frac{p-1}{2})^2$.

8. Dacă numărul natural n se poate scrie ca diferenţă de două pătrate ale numerelor întregi a şi b, atunci n este impar sau multiplu de 4 şi reciproc.

Intr-adevăr, fie $n = a^2 - b^2$. Pentru a şi b de aceeaşi paritate rezultă că n este multiplu de 4. Pentru a şi b de parităţi diferite rezultă n impar.

Reciproc, dacă $n = 4m$, atunci $n = (m+1)^2 - (m-1)^2$ iar dacă $n = 2m+1$, atunci $n = (m+1)^2 - m^2$.

9. Se ţine cont de faptul că pătratul oricărui număr întreg impar este de forma $8m+1$.

10. Se ţine cont de identitatea $(2x+3y)^2 - 3(x+2y)^2 = x^2 - 3y^2$.

11. Din p prim şi $p > 3$ rezultă $p = 6k \pm 1$ şi atunci:

$$4p^2 + 1 = 4(6k \pm 1)^2 + 1 = (8k \pm 2)^2 + (8k \pm 1)^2 + (4k)^2.$$

12. Facem inducţie matematică după m (pentru $m = 1$ atunci afirmaţia este evidentă). Să presupunem afirmaţia adevarată pentru toate fracţiile cu numărătorii mai mici ca m şi să o demonstrăm pentru fracţiile cu numărătorii m.

Să presupunem deci că $1 < m < n$. Impărţind pe n la m avem:

$$(1) \qquad n = m(d_0 - 1) + m - k = md_0 - k \text{ cu } d_0 > 1 \text{ şi } 0 < k < m,$$

de unde $md_0 = n + k \Leftrightarrow$

$$(2) \qquad \frac{m}{n} = \frac{1}{d_0}(1 + \frac{k}{n}).$$

Cum $k < m$, aplicănd ipoteza de inducţie lui $\frac{k}{n}$ avem:

$$(3) \qquad \frac{k}{n} = \frac{1}{d_1} + \frac{1}{d_1 d_2} + ... + \frac{1}{d_1 d_2 ... d_r}, \text{ cu } d_i \in \mathbf{N}, d_i > 1 \text{ pentru } 1 \leq i \leq r.$$

Din (2) şi (3) deducem că:

$$\frac{m}{n} = \frac{1}{d_0} + \frac{1}{d_0 d_1} + ... + \frac{1}{d_0 d_1 ... d_r}$$

şi cu aceasta afirmaţia este probată.

De exemplu: $\frac{5}{7} = \frac{1}{2} + \frac{1}{2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \frac{1}{2\cdot 3\cdot 4\cdot 7} = \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{168}$.

13. Clar, dacă $k = \frac{1}{a_1} + \frac{2}{a_2} + ... + \frac{n}{a_n}$ cu $a_1, ..., a_n \in \mathbf{N}^*$, atunci $k \leq 1+2+...+n = \frac{n(n+1)}{2}$.

Să probam acum reciproca. Dacă $k = 1$ atunci putem alege $a_1 = a_2 = ... = a_n = \frac{n(n+1)}{2}$. Dacă $k = n$ alegem $a_1 = 1, a_2 = 2, ..., a_n = n$.

Pentru $1 < k < n$ alegem $a_{k-1} = 1$ şi $a_i = \frac{n(n+1)}{2} - k + 1$(căci $\sum_{i=1}^{n} \frac{i}{a_i} = k - 1 + \frac{\frac{n(n+1)}{2} - k + 1}{\frac{n(n+1)}{2} - k + 1} = k$).

Dacă $n < k < \frac{n(n+1)}{2}$ atunci scriind pe k sub forma $k = n + p_1 + p_2 + ... + p_i$ cu $n - 1 \geq p_1 > p_2 > ... > p_i \geq 1$, atunci putem alege şi $a_j = j$ în rest.

14. Fie $n \in \mathbf{N}^*$. Dacă $n = a + (a+1) + ... + (a+k-1), (k > 1)$ atunci $n = \frac{k(2a+k-1)}{2}$ şi pentru k impar, k este divizor impar al lui n, iar pentru k par, $2a+k-1$ este divizor impar al lui n. Deci oricărei descompuneri îi corespunde un divizor impar al lui n.

Reciproc, dacă q este un divizor impar al lui n, considerăm $2n = pq$ (cu p par) şi fie $a = \frac{1}{2}|p-q| + \frac{1}{2}$ şi $b = \frac{1}{2}(p+q) + \frac{1}{2}$.

Se observă că $a, b \in \mathbf{N}^*$ şi $a \leq b$. In plus,

$$a + b = \frac{p+q+|p-q|}{2} \text{ iar } b - a + 1 = \frac{p+q-|p-q|}{2}.$$

Deci $(a+b)(b-a+1) = pq = 2n$. Am obţinut că $a + (a+1) + ... + b = \frac{(a+b)(b-a+1)}{2} = n$. (Se observă că dacă $q_1 \neq q_2$ sunt divizori impari ai lui n atunci cele două soluţii construite sunt distincte).

15. Vom nota suma $x + y$ prin s şi vom transcrie formula dată astfel:

$$n = \frac{(x+y)^2 + 3x + y}{2} = \frac{s^2 + s}{2} + x. \qquad (1)$$

Condiţia că x şi y sunt numere naturale este echivalentă cu $x \geq 0$ şi $s \geq x$, x şi s numere naturale. Pentru s dat, x poate lua valorile $0, 1, ..., s$. In mod corespunzator, n determinat de formula (1) ia valorile $\frac{s^2+s}{2}, \frac{s^2+s}{2} + 1, ..., \frac{s^2+s}{2} + s$. Astfel, fiecărui $s = 0, 1, 2...$ îi corespunde o mulţime formată din $s+1$ numere naturale n. Să observăm că ultimul număr al mulţimii corespunzatoare lui s este cu 1 mai mic decât primul număr al mulţimii corespunzatoare lui $s+1$: $\frac{s^2+s}{2} + 1 + s = \frac{(s+1)^2 + (s+1)}{2}$. De aceea, aceste mulţimi vor conţine toate numerele naturale n şi fiecare n va intra numai într-o astfel de mulţime, adică lui îi va corespunde o singură pereche de valori s şi x.

11.7 Ecuaţii diofantice

1. $x = y = z = 0$ verifică ecuaţia. Dacă unul dintre numerele x, y, z este zero atunci şi celelalte sunt zero. Fie $x > 0, y > 0, z > 0$. Cum membrul drept este par trebuie ca şi

membrul stâng să fie par astfel că sunt posibile situaţiile (x, y impare, z par) sau (x, y, z pare).

In primul caz membrul drept este multiplu de 4 iar membrul stâng este de forma $4k + 2$, deci acest caz nu este posibil.

Fie deci $x = 2^\alpha x_1, y = 2^\beta y_1, z = 2^\gamma z_1$ cu $x_1, y_1, z_1 \in \mathbf{Z}$ impare iar $\alpha, \beta, \gamma \in \mathbf{N}^*$.

Inlocuind în ecuaţie obţinem

$$2^{2\alpha}x_1^2 + 2^{2\beta}y_1^2 + 2^{2\gamma}z_1^2 = 2^{\alpha+\beta+\gamma}x_1y_1z_1,$$

astfel că dacă, de exemplu, $\alpha = min(\alpha, \beta, \gamma)$,

$$(1) \qquad 2^{2\alpha}(x_1^2 + 2^{2(\beta-\alpha)}y_1^2 + 2^{2(\gamma-\alpha)}z_1^2) = 2^{\alpha+\beta+\gamma+1}x_1y_1z_1.$$

Dacă $\beta > \alpha$ şi $\gamma > \alpha \Rightarrow \alpha + \beta + \gamma > 2\alpha$ şi egalitatea (1) nu este posibilă (membrul stâng este impar iar cel drept este par). Din aceleaşi considerente nu putem avea $\alpha = \beta = \gamma$.

Dacă $\beta = \alpha$ şi $\gamma > \alpha$ din nou $\alpha + \beta + \gamma + 1 > 2\alpha + 1$ (din paranteză se mai scoate 2^1) şi din nou (1) nu este posibilă.

Rămâne doar căzul $x = y = z = 0$.

2. In esenţă soluţia este asemănătoare cu cea a exerciţiului 1. Sunt posibile cazurile :

i) x, y pare, z, t impare - imposibil (căci membrul drept este de forma $4k$ iar cel stâng de forma $4k + 2$);

ii) x, y, z, t impare, din nou imposibil (din aceleaşi considerente);

iii) x, y, z, t pare : $x = 2^\alpha x_1, y = 2^\beta y_1, z = 2^\gamma z_1$ şi $t = 2^\delta t_1$ cu x_1, y_1, z_1, t_1 impare iar $\alpha, \beta, \gamma, \delta \in \mathbf{N}^*$.

Fie $\alpha = min(\alpha, \beta, \gamma, \delta)$; înlocuind în ecuaţie se obţine:

$$(2) \qquad 2^{2\alpha}(x_1^2 + 2^{2(\beta-\alpha)}y_1^2 + 2^{2(\gamma-\alpha)}z_1^2 + 2^{2(\delta-\alpha)}t_1^2) = 2^{\alpha+\beta+\gamma+\delta+1}x_1y_1z_1t_1.$$

Dacă $\beta, \gamma, \delta > \alpha$ egalitatea (1) nu este posibilă deoarece paranteza din (1) este impară şi $\alpha + \beta + \gamma + \delta + 1 > 2\alpha$.

Dacă $\beta = \alpha, \gamma, \delta > \alpha$, din paranteza de la (1) mai iese 2 factor comun şi din nou $\alpha + \beta + \gamma + \delta + 1 > 2\alpha + 1$.

Contradicţii rezultă imediat şi în celelalte situaţii.

Rămâne deci doar posibilitatea $x = y = z = t = 0$.

3. Se verifică imediat că $(1, 1)$ şi $(2, 3)$ sunt soluţii ale ecuaţiei. Să aratăm că sunt singurele.

Fie $(x, y) \in \mathbf{N}^2, 2x \geq 3, y > 1$ astfel încât $3^x - 2^y = 1$; atunci $3^x - 1 = 2^y$ sau

$$(1) \qquad 3^{x-1} + 3^{x-2} + ... + 3 + 1 = 2^{y-1}.$$

Dacă $y > 1$, membrul drept din (1) este par, de unde concluzia că x trebuie să fie par. Fie $x = 2n$ cu $n \in \mathbf{N}$. Deoarece $x \neq 2$ deducem că $x \geq 4$, deci $y > 3$. Ecuaţia iniţială se scrie atunci $9^n - 1 = 2^y$, sau $9^{n-1} + 9^{n-2} + ... + 9 + 1 = 2^{y-3}$.

Deducem din nou că n este par, adică $n = 2m$ cu $m \in \mathbf{N}$. Ecuaţia iniţială devine $3^{4m} - 1 = 2^y$ său $81^m - 1 = 2^y$, imposibil (căci membrul stâng este multiplu de 5).

4. Ecuaţia se mai scrie sub forma $(x + y + 1)(x + y - m - 1) = 0$ şi cum $x, y \in \mathbf{N}$, atunci $x + y + 1 \neq 0$, deci $x + y = m + 1$ ce admite soluţiile $(k, m + 1 - k)$ şi $(m + 1 - k, k)$ cu $k = 0, 1, ..., m + 1$.

5. Dacă $y \equiv 0 (\mathrm{mod}\ 2)$ atunci $x^2 \equiv 7 (\mathrm{mod}\ 8)$ ceea ce este imposibil căci 7 nu este rest pătratic modulo 8. Dacă $y \equiv 1 (\mathrm{mod}\ 2), y = 2k + 1$ atunci $x^2 + 1 = y^3 + 2^3 = (y + 2)[(y - 1)^2 + 3]$, de unde trebuie ca $(2k)^2 + 3 \mid x^2 + 1$. Acest lucru este imposibil deoarece $(2k)^2 + 3$ admite un divizor prim de forma $4k + 3$ pe când $x^2 + 1$ nu admite un astfel de divizor.

6. Dacă y este par, $x^2 = y^2 - 8z + 3 \equiv 0 (\mathrm{mod}\ 8)$, ceea ce este imposibil. Dacă y este impar, $y = 2k + 1$, $x^2 = 3 - 8z + 8k^2 + 8k + 2 \equiv 5 (\mathrm{mod}\ 8)$, ceea ce este de asemenea imposibil (căci x este impar şi modulo 8 pătratul unui număr impar este egal cu 1).

7. Presupunem că $z \neq 3$ şi îl fixăm. Fie $(x, y) \in \mathbf{N}^2$ o soluţie a ecuaţiei (cu z fixat). Dacă $x = y$, atunci $x = y = 1$ şi deci $z = 3$, absurd!.

Putem presupune $x < y$ iar dintre toate soluţiile va există una (x_0, y_0) cu y_0 minim. Fie $x_1 = x_0 z - y_0$ şi $y_1 = x_0$.

Avem: $y_0(x_0 z - y_0) = x_0^2 + 1 > 1$, deci $x_1 \in \mathbf{N}$. Cum

$$\begin{aligned} x_1^2 + y_1^2 + 1 &= (x_0 z - y_0)^2 + x_0^2 + 1 = x_0^2 + y_0^2 + 1 + x_0^2 z^2 - 2x_0 y_0 z \\ &= x_0 y_0 z + x_0^2 z^2 - 2x_0 y_0 z = x_0^2 z^2 - x_0 y_0 z = x_0 z(x_0 z - y_0) \\ &= x_0 z x_1 = x_1 y_1 z. \end{aligned}$$

adică şi (x_1, y_1) este soluţie a ecuaţiei. Cum $x_1 < y_1$ iar $y_1 < y_0$ se contrazice minimalitatea lui y_0, absurd, deci $z = 3$.

8. Ecuaţia fiind simetrică în x, y şi z să găsim soluţia pentru care $x \leq y \leq z$.

Atunci $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leq \frac{3}{x} \Leftrightarrow 1 \leq \frac{3}{x} \Leftrightarrow x \leq 3$.

Cazul $x = 1$ este imposibil. Dacă $x = 2$ atunci ecuaţia devine $\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$ şi deducem imediat că $y = z = 4$ sau $\{y, z\} = \{3, 6\}$.

Dacă $x = 3$ atunci ecuaţia devine $\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$, de unde $y = z = 3$.

Prin urmare $x = y = z = 3$ sau $\{x, y, z\} = \{2, 4\}$ (două egale cu 4) sau $\{x, y, z\} = \{2, 3, 6\}$.

9. Ecuaţia se pune sub forma echivalentă $(x - a)(y - a) = a^2$. Dacă notăm prin n numărul divizorilor naturali ai lui a^2, atunci ecuaţia va avea $2n - 1$ soluţii, ele obţinându-se din sistemul:

$\begin{cases} x-a=\pm d \\ y-a=\pm\frac{a^2}{d}(\text{ cu } d \mid a^2, d\in\mathbf{N}^*). \end{cases}$

Nu avem soluţie în cazul $x-a=-a$ şi $y-a=-a$.

10. O soluţie evidentă este $y=x$ cu $x\in\mathbf{Q}_+^*$.

Să presupunem că $y\neq x, y>x$. Atunci $w=\frac{x}{y-x}\in\mathbf{Q}_+^*$ şi $y=(1+\frac{1}{w})x$. Astfel $x^w=x^{(1+\frac{1}{w})x}$ şi cum $x^y=y^x$ atunci $x^{(1+\frac{1}{w})x}=y^x$ ceea ce dă $x^{1+\frac{1}{w}}=y=(1+\frac{1}{w})x$, de unde $x^{\frac{1}{w}}=1+\frac{1}{w}$, deci $x=(1+\frac{1}{w})^w, y=(1+\frac{1}{w})^{w+1}$ (1).

Fie $w=\frac{n}{m}$ şi $x=\frac{r}{s}$ din $\mathbf{Q}$ ireductibile. Din (1) deducem că $(\frac{m+n}{n})^{\frac{n}{m}}=\frac{r}{s}$, de unde $\frac{(m+n)^n}{n^n}=\frac{r^m}{s^m}$. Cum ultima egalitate este între fracţii ireductibile deducem că $(m+n)^n=r^m$ şi $n^n=s^m$. Deci vor există numerele naturale k,l astfel încât $m+n=k^m, r=k^n$ şi $n=l^m, s=l^n$. Astfel $m+l^m=k^m$, de unde $k\leq l+1$.

Dacă $m>1$, am avea $k^m\leq(l+1)^m\leq l^m+ml^{m-1}+1>l^m+m$, prin urmare $k^m>l^m+m$, imposibil.

Astfel $m=1$, de unde $w=\frac{n}{m}=n$ şi astfel avem soluţia $x=(1+\frac{1}{n})^n, y==(1+\frac{1}{n})^{n+1}$ cu $n\in\mathbf{N}^*$ arbitrar.

De aici deducem că singura soluţie în $\mathbf{N}$ este pentru $n=1$ cu $\{x,y\}=\{2,4\}$.

11. Evident nici unul dintre x,y,z,t nu poate fi egal cu 1. De asemenea nici unul nu poate fi superior lui 3, căci dacă de exemplu $x\geq 3$, cum $y,z,t\geq 2$ atunci: $\frac{1}{x^2}+\frac{1}{y^2}+\frac{1}{z}+\frac{1}{t}\leq\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{9}=\frac{31}{36}<1$, imposibil!. Deci $x=2$ şi analog $y=z=t=2$.

12. Se observă imediat că perechea $(3,2)$ verifică ecuaţia din enunţ. Dacă $(a,b)\in\mathbf{N}^2$ este o soluţie a ecuaţiei atunci ţinând cont de identitatea :

$$3(55a+84b)^2-7(36a+55b)^2=3a^2-7b^2$$

deducem că şi $(55a+84b, 36a+55b)$ este o altă soluţie (evident diferită de (a,b)).

13. Să observăm la început că cel puţin două dintre numerele x,y,z trebuie să fie pare, căci dacă toate trei sunt impare atunci $x^2+y^2+z^2$ va fi de forma $8k+3$, deci nu putem găsi $t\in\mathbf{N}$ astfel încât $t^2\equiv 3(\text{mod } 8)$ (pătratul oricărui număr natural este congruent cu 0 sau 1 modulo 4).

Să presupunem de exemplu că y şi z sunt pare, adică $y=2l$ şi $z=2m$ cu $l,m\in\mathbf{N}$. Deducem imediat că $t>x$ şi fie $t-x=u$. Ecuaţia devine $x^2+4l^2+4m^2=(x+u)^2\Leftrightarrow u^2=4l^2+4m^2-2xu$. Cu necesitate u este par, adică $u=2n$ cu $n\in\mathbf{N}$. Obţinem $n^2=l^2+m^2-nx$, de unde $x=\frac{l^2+m^2-n^2}{n}$ iar $t=x+u=x+2n=\frac{l^2+m^2+n^2}{n}$. Cum $x\in\mathbf{N}$, deducem că $n^2<l^2+m^2\Leftrightarrow n<\sqrt{l^2+m^2}$.

In concluzie

$$(1)\qquad x=\frac{l^2+m^2-n^2}{n}, y=2l, z=2m, t=\frac{l^2+m^2+n^2}{n}$$

cu $m,n,l\in\mathbf{N}, n\mid l^2+m^2$ şi $n<\sqrt{l^2+m^2}$.

Reciproc orice x, y, z, t daţi de (1) formează o soluţie pentru ecuaţia $x^2+y^2+z^2 = t^2$. Intr-adevăr, cum

$$(\frac{l^2+m^2-n^2}{n})^2 + (2l)^2 + (2m)^2 = (\frac{l^2+m^2+n^2}{n})^2$$

pentru orice l, m, n, ţinând cont de (1) deducem că $x^2 + y^2 + z^2 = t^2$.

14. Alegem x şi z arbitrare şi atunci cum $(\frac{x}{(x,z)}, \frac{z}{(x,z)}) = 1$, din $\frac{x}{(x,z)} \cdot y = \frac{z}{(x,z)} \cdot t$ deducem că $\frac{z}{(x,z)} \mid y$, adică $y = \frac{uz}{(x,z)}$, deci $t = \frac{ux}{(x,z)}$.

Pe de altă parte, luând pentru x, z, u valori arbitrare şi punând $y = \frac{uz}{(x,z)}$ şi $t = \frac{ux}{(x,z)}$ obţinem că soluţia generală în $\mathbf{N}^4$ a ecuaţiei $xy = zt$ este $x = ac, y = bd, z = ad$ şi $t = bc$ cu $a, b, c, d \in \mathbf{N}$ arbitrari.

15. Presupunem prin absurd că $x^2 + y^2 + z^2 = 1993$ şi $x + y + z = a^2$, cu $a \in \mathbf{N}$. Cum $a^2 = x+y+z < \sqrt{3(x^2+y^2+z^2)} = \sqrt{5979} < 78$, deducem că $a^2 \in \{1, 4, 9, ..., 64\}$. Cum $(x + y + z)^2 = x^2 + y^2 + z^2 + 2(xy + yz + xz)$ deducem că $x + y + z$ trebuie să fie impar, adică $a^2 \in \{1, 9, 25, 49\}$. De asemenea, din $(x + y + z)^2 > x^2 + y^2 + z^2$ şi $25^2 < 1993$ deducem că $a^2 = 49$, de unde sistemul

$$\begin{cases} x^2 + y^2 + z^2 = 1993 \\ x + y + z = 49 \end{cases}$$

Inlocuind $y + z = 49 - x$ obţinem $(49 - x)^2 = (y + z)^2 > y^2 + z^2 = 1993 - x^2$, adică $x^2 - 49x + 204 > 0$, deci $x < \frac{49-\sqrt{1585}}{2}$ sau $x > \frac{49+\sqrt{1585}}{2}$. In primul căz $x \geq 45$ deci $x^2 = 2025 > 1993$, absurd. In al doilea căz $x \leq 4$. Problema fiind simetrică în x, y, z deducem analog că şi $y, z \leq 4$, deci $49 = x + y + z = 4 + 4 + 4 = 12$, absurd.

Observaţie. De fapt ecuaţia $x^2 + y^2 + z^2 = 1993$ are în $\mathbf{N}^3$ doar soluţiile: $(2, 30, 33)$, $(2, 15, 42), (11, 24, 36), (15, 18, 38), (16, 21, 36)$ şi $(24, 24, 29)$.

16. Ecuaţia nu are soluţii în numere întregi pentru că membrii săi sunt de parităţi diferite.

Intr-adevăr, $x_1^p + ... + x_n^p \equiv x_1 + ... + x_n (\text{mod } 2)$ şi $(x_1 + ... + x_n)^2 \equiv x_1 + ... + x_n (\text{mod } 2)$ sau $(x_1 + ... + x_n)^2 + 1 \equiv x_1 + ... + x_n + 1 (\text{mod } 2)$, de unde deducem că $x_1^p + ... + x_n^p - (x_1 + ... + x_n)^2 - 1$ este impar, deci nu poate fi zero.

17. Reducând modulo 11 se obţine că $x^5 \equiv \pm 1 (\text{mod } 11)$ (aplicând Mică Teorema a lui Fermat) iar $x^5 \equiv 0 (\text{mod } 11)$ dacă $x \equiv 0 (\text{mod } 11)$.

Pe de altă parte, $y^2 + 4 \equiv 4, 5, 8, 2, 9, 7 (\text{mod } 11)$ deci egalitatea $y^2 = x^5 - 4$, cu $x, y \in \mathbf{Z}$ este imposibilă.

18. Avem $y^2 = x^3+7 \Leftrightarrow y^2+1 = x^3+8 = (x+2)(x^2-2x+4)$. Dacă x este par, atunci $y^2 \equiv 7 (\text{mod } 8)$; cum pătratul oricărui număr întreg este congruent cu 1 modulo 8, acest caz este imposibil, deci x este impar. Atunci $x^2-2x+4 = (x-1)^2+3$ este de forma $4k+3$, deci va avea un divizor prim de q de aceeaşi formă. Atunci $q \mid y^2+1 \Rightarrow y^2 \equiv -1 (\text{mod } q)$.

Din teorema lui Fermat deducem că $y^{q-1} \equiv 1(\text{mod } q)$. Cum $y^4 \equiv 1(\text{mod } q) \Rightarrow 4 \mid q-1$, adică q este de forma $4k+1$, absurd!

19. Dacă $y^2 = x^3+47$, atunci $y^2+13^2 = y^2+169 = x^3+216 = (x+6)(x^2-6x+36)$. Dacă $x \equiv 0,2,3(\text{mod } 4)$ atunci $y^2 \equiv 2,3(\text{mod } 4)$, absurd. Dacă $x \equiv 1(\text{mod } 4)$ atunci există un prim $p \equiv 3(\text{mod } 4)$ ce divide $x^2-6x+36$, deci $y^2 \equiv -13(\text{mod } p)$. Astfel, $1 = (\frac{y^2}{p}) = (\frac{-13^2}{p}) = (\frac{-1}{p})$, absurd!

20. Evident, (0,0,0) este soluţie a ecuaţiei. Se duduce imediat că dacă (x,y,z) este o soluţie a ecuaţiei din enunţ, atunci $x = 2x_1, y = 2y_1, y = 2y_1$ cu $x_1, y_1, z_1 \in \mathbf{Z}$. Deducem imediat că $x_1^3 + 2y_1^3 + 4z_1^3 - 6x_1y_1z_1 = 0$. Continuând procedeul deducem că la rândul lor numerele x_1, y_1, z_1 sunt pare, ş.a.m.d., adică $2^n \mid x, 2^n \mid y, 2^n \mid z$ pentru orice $n \in \mathbf{N}$, de unde cu necesitate $x = y = z = 0$.

21. Se duduce imediat că dacă $(x,y,z) \in \mathbf{N}^{*3}$ este o soluţie a ecuaţiei din enunţ, atunci $x = 2x_1, y = 2y_1, y = 2y_1$ cu $x_1, y_1, z_1 \in \mathbf{N}^*$. Atunci $x_1^2 + y_1^2 = 4^{z-1}$, astfel că dacă alegem soluţia (x,y,z) cu z minim tot soluţie este şi $(x/2, y/2, z-1)$ iar $z-1 < z$, contradicţie.

11.8 Puncte laticeale în plan şi spatiu

1. Fie A şi B puncte laticeale situate la distanţa 1 între ele prin care trece cercul C din enunţ (de rază $r \in \mathbf{N}^*$). Vom considera un sistem ortogonal de axe cu originea în A având pe AB drept axa $x'x$ şi perpendiculara în A pe AB drept axa $y'y$ (vezi Fig. 9)

Dacă C este centrul acestui cerc, atunci coordonatele lui C sunt $(\frac{1}{2}, \sqrt{r^2-\frac{1}{4}})$.

Dacă $M(x,y)$ mai este un alt punct laticeal prin care trece C, atunci $x, y \in \mathbf{Z}$ şi

$$(x-\frac{1}{2})^2 + (y-\sqrt{r^2-\frac{1}{4}})^2 = r^2 \Leftrightarrow x^2 - x + \frac{1}{4} + y^2 + r^2 - 2y\sqrt{r^2-\frac{1}{4}} - \frac{1}{4} = r^2$$

$$\Leftrightarrow x^2 + y^2 - x = 2y\sqrt{r^2-\frac{1}{4}} = y\sqrt{4r^2-1}.$$

Ultima egalitate implică $4r^2 - 1 = k^2$ cu $k \in \mathbf{Z} \Leftrightarrow (2r-k)(2r+k) = 1 \Leftrightarrow$

$$\begin{cases} 2r-k=1 \\ 2r+k=1 \end{cases} \text{ sau } \begin{cases} 2r-k=-1 \\ 2r+k=-1 \end{cases} \Leftrightarrow \begin{cases} r=\frac{1}{2} \\ k=0 \end{cases} \text{ sau } \begin{cases} r=-\frac{1}{2} \\ k=0 \end{cases} \text{ - absurd !.}$$

2. Fie $x = \frac{p}{q}$ şi $y = \frac{r}{q}$ cu $p, q, r \in \mathbf{Z}, q \neq 0$.

Atunci punctele laticeale de coordonate $(r,-p)$ şi $(-r,p)$ au aceeaşi distanţă până la punctul de coordonate (x,y) deoarece:

$$(r-\frac{p}{q})^2 + (-p-\frac{r}{q})^2 = (-r-\frac{p}{q})^2 + (p-\frac{r}{q})^2.$$

Prin urmare, pentru orice punct de coordonate raţionale există doua puncte laticeale distincte egal depărtate de acel punct.

Dacă presupunem prin absurd că $a \in \mathbf{Q}$ şi $b \in \mathbf{Q}$, atunci conform cu observaţia de mai înainte, există doua puncte laticeale distincte ce sunt egal depărtate de punctul de

coordonate (a, b). Astfel dacă cercul cu centrul în punctul de coordonate (a, b) contine în interiorul său n puncte laticeale, atunci un cerc concentric cu acesta însă de rază mai mare va conţine în interiorul său cel puţin $n + 2$ puncte laticeale, neexistând astfel de cercuri cu centrul în punctul de coordonate (a, b) care să conţină în interiorul său exact $n + 1$ puncte laticeale -absurd !. Deci $a \in \mathbf{Q}$ sau $b \in \mathbf{Q}$.

3.

Se observă (vezi Fig. 10) că centrul cercului va avea coordonatele (989, 989) şi raza $r = 989\sqrt{2}$, astfel că un punct $M(x, y) \in \mathbf{C} \Leftrightarrow$

$$(1) \quad (x - 989)^2 + (y - 989)^2 = 2 \cdot 989^2.$$

Cum membrul drept din (1) este par deducem că dacă $(x, y) \in \mathbf{Z}^2$, atunci $x - 989$ şi $y - 989$ au aceeaşi paritate.

Astfel $A = \frac{1}{2}(x + y) - 989$ şi $B = \frac{1}{2}(x - y) - 989$ sunt numere întregi.

Deducem imediat că $x-989 = A+B$ şi $y-989 = A-B$ şi cum $(A+B)^2+(A-B)^2 = 2A^2 + 2B^2$, (1) devine:

$$(2) \quad A^2 + B^2 = 989^2.$$

Observăm că $n = 989^2 = 232 \cdot 432$. Conform Teoremei 6.1.7. de la Capitolul 6 ecuaţia (2) va avea soluţii întregi.

Prin calcul direct se constată că numărul $d_1(n)$ al divizorilor lui n de forma $4k + 1$ este $d_1(n) = 5$ iar numărul $d_3(n)$ al divizorilor lui n de forma $4k+3$ este $d_3(n) = 4$ astfel că în conformitate cu Teorema 6.1.7. de la Capitolul 6, numărul de soluţii naturale ale ecuaţiei (2) este $4(d_1(n) - d_3(n)) = 4(5 - 4) = 4$.

Cum (0, 0), (0, 989), (989, 0) şi (989, 989) verifică (2) deducem că acestea sunt toate, de unde şi concluzia problemei.

4. Fie date punctele laticeale $P_i(x_i, y_i, z_i), x_i, y_i, z_i \in \mathbf{Z}, 1 \leq i \leq 9$.

Definim $f : \{P_1, ..., P_9\} \to \{0, 1\} \times \{0, 1\} \times \{0, 1\}$ prin

$$f(P_i) = (x_i - 2[\frac{x_i}{2}], y_i - 2[\frac{y_i}{2}], z_i - 2[\frac{z_i}{2}]), 1 \leq i \leq 9.$$

Cum domeniul are 9 elemente iar codomeniul are 8, f nu poate să fie injectivă. Deci există $i, j \in \{1, 2, ..., 9\}, i \neq j$ pentru care $f(P_i) = f(P_j)$, adică $x_i-x_j, y_i-y_j, z_i-z_j \in 2\mathbf{Z}$.

In acest caz $\frac{x_i + x_j}{2}, \frac{y_i + y_j}{2}, \frac{z_i + z_j}{2} \in \mathbf{Z}$. Am găsit astfel punctul laticeal $P(\frac{x_i + x_j}{2}, \frac{y_i + y_j}{2}, \frac{z_i + z_j}{2})$ care este mijlocul segmentului P_iP_j.

Observaţie. Problema se poate extinde imediat la cazul a $m \geq 2^k+1$ puncte laticeale din $\mathbf{R}^k$.

11.9 Clase speciale de numere întregi

1. Cum pentru $n > 1$ F_n este impar, dacă există p, q prime astfel încât $F_n = p + q$ atunci cu necesitate $p = 2$ şi $q > 2$ şi astfel $q = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1)$-absurd.

2. Analog ca în cazul Propoziţiei 9.1.1 care stabileşte forma divizorilor primi ai unui număr Fermat, se demonstrează mai general că dacă a este un număr natural par, $n \in \mathbf{N}$ şi p este prim astfel încât $p \mid a^{2^n} + 1$, atunci p este de forma $p = 2^{n+1} \cdot k + 1$ cu $k \in \mathbf{N}$. Deci dacă p este prim şi $p \mid 12^{2^{15}} + 1$ atunci $p = 2^{16} \cdot k + 1 \geq 2^{16} + 1 = F_4$. Cum F_4 este prim, conform Propoziţiei 9.1.1 $F_4 \mid 3^{2^{15}} + 1$, adică $3^{2^{15}} \equiv -1 (\text{mod } F_4)$. Insă $2^{2^{16}} = 2^{F_4 - 1} \equiv 1 (\text{mod } F_4)$, deci $4^{2^{15}} \equiv 1 (\text{mod } F_4)$ şi atunci $12^{2^{15}} = 3^{2^{15}} \cdot 4^{2^{15}} \equiv -1 (\text{mod } F_4)$, adică $F_4 \mid 12^{2^{15}} + 1$, deci F_4 este cel mai mic divizor prim al lui $12^{2^{15}} + 1$.

3. Fie $m = k\varphi(n)$ cu $k \in \mathbf{N}^*$. Atunci $2^m - 1 = 2^{k\varphi(n)} - 1 = (2^{\varphi(n)})^k - 1$, de unde concluzia că $2^{\varphi(n)} - 1 \mid M_n$. Cum $(2, n) = 1$, conform teoremei lui Euler deducem că $n \mid 2^{\varphi(n)} - 1 \Rightarrow n \mid M_m$.

4. Presupunem prin absurd că pentru $m, n \geq 2$ există $k \in \mathbf{N}^*$ astfel încât $2^n - 1 = k^m \Leftrightarrow 2^n = k^m + 1$ (cu necesitate k este impar şi $k \geq 3$). Pentru m par rezultă contradicţia $2^n \equiv 2 (\text{mod } 8)$ iar pentru m impar avem $2^n = (k+1)(k^{m-1} - k^{m-2} + ... + 1)$, egalitate contradictorie deoarece $k^{m-1} - k^{m-2} + ... + 1$ este impar şi ≥ 3.

5. Se ştie că dacă $a \in \mathbf{N}^*, 10^{n-1} \leq a < 10^n \Leftrightarrow n - 1 \leq \lg a < n$, atunci a are n cifre.

Avem $M_{101} + 1 = 2^{101} \Rightarrow \lg(M_{101} + 1) = 101 \cdot \lg 2 \approx 101 \cdot 0,30103 = 30,40403$, deci M_{101} are 31 cifre.

6. Fie $n = n_1 n_2$ cu n_1, n_2 impare şi $n_1, n_2 \geq 3$ astfel încât $n \mid 2^{n-1} - 1$. Notând $m = 2^n - 1$, în mod evident $m > n$. Cum $m = 2^n - 1 = (2^{n_1})^{n_2} - 1 \Rightarrow 2^{n_1} - 1 \mid m$ şi cum $1 < 2^{n_1} - 1 < m$ deducem că m este compus. Avem $2^{n-1} - 1 = kn$ şi $m - 1 = 2kn$, astfel că $2^{m-1} - 1 = 2^{2kn} - 1 = (2^n)^{2k} - 1 \Rightarrow m = 2^n - 1 \mid 2^{m-1} - 1$.

7. ([38]) Trebuie să demonstrăm că $2^n \equiv 2 (\text{mod } n)$. Să observăm că numerele 73, 1103 şi 2089 sunt prime. De asemenea putem scrie $73 = 72 + 1, 2 \cdot 1103 = 72k + 46$ iar $2089 = 72h + 1$, deci $n - 1 = 72l + 45$, de unde deducem că $2^{n-1} - 1 = 2^{72l} \cdot 2^{45} - 1$. Din mica teoremă a lui Fermat deducem că $2^{72} \equiv 1 (\text{mod } 73)$ şi deci $2^{n-1} - 1 \equiv 2^{45} - 1 (\text{mod } 73)$. Cum $2^9 - 1 \equiv 0 (\text{mod } 73)$ deducem că (1) $2^{n-1} - 1 \equiv 1 (\text{mod } 73)$.

Avem $2089 \equiv -115 (\text{mod } 1102); 2 \cdot 73 \equiv 146 (\text{mod } 1102)$ şi astfel $n - 1 \equiv 841 (\text{mod } 1102)$. Cum $(*)$ $1103 \cdot 2089 \cdot 233 = 2^{29} - 1$ deducem că $2^{29} \equiv 1 (\text{mod } 1103)$; cum $841 = 29^2$ deducem că $2^{n-1} \equiv (2^{29})^{29} \equiv 1 (\text{mod } 1103)$(2). De asemenea $n - 1 \equiv 261 (\text{mod } 2089)$ şi deci $2^{n-1} \equiv 2^{261} \equiv (2^{29})^9 (\text{mod } 2089)$. Ţinând cont de $(*)$ deducem că $2^{29} \equiv 1 (\text{mod } 2089)$ şi astfel $2^{n-1} \equiv 1 (\text{mod } 2089)$ (3). Din (1), (2) şi (3) deducem că $2^n \equiv 2 (\text{mod } n)$, adică n este pseudo-prim.

8. Prin calcul direct.

Observaţie. Nu se ştie încă dacă există o imfinitate de numere triunghiulare pitagoreice.

9. Pentru (ii), (iii) şi (vi) facem calcule directe iar pentru (i), (iv) şi (v) facem inducţie matematică după n ţinând cont că $F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$, unde $\alpha = \frac{1 + \sqrt{5}}{2}$ şi $\beta = \frac{1 - \sqrt{5}}{2}$.

ANEXA 1: Numerele prime de la 1 la 10000(numerele scrise bold reprezintă perechi de numere prime gemene)

2	167	389	631	**883**	**1153**	1447	1709	2011	**2309**	2617	2887
3	173	397	**641**	887	1163	**1451**	**1721**	2017	**2311**	2621	2897
5	**179**	401	**643**	907	1171	**1453**	**1723**	**2027**	2333	2633	2903
7	**181**	409	647	911	1181	1459	1733	**2029**	**2339**	2647	2909
11	**191**	**419**	653	919	1187	1471	1741	2039	**2341**	**2657**	2917
13	**193**	**421**	**659**	929	1193	**1481**	1747	2053	2347	**2659**	2927
17	**197**	**431**	**661**	937	1201	**1483**	1753	2063	2351	2663	2939
19	**199**	**433**	673	941	1213	**1487**	1759	2069	2357	2671	2953
23	211	439	677	947	1217	**1489**	1777	**2081**	2371	2677	2957
29	223	443	683	953	1223	1493	1783	**2083**	2377	2683	2963
31	**227**	449	691	967	**1229**	1499	**1787**	**2087**	**2381**	**2687**	**2969**
37	**229**	457	701	971	**1231**	1511	**1789**	**2089**	**2383**	**2689**	**2971**
41	233	**461**	709	977	1237	1523	1801	2099	2389	2693	**2999**
43	**239**	**463**	719	983	1249	1531	1811	**2111**	2393	2699	**3001**
47	**241**	467	727	991	1259	1543	1823	**2113**	2399	2707	3011
53	251	479	733	997	**1277**	1549	1831	**2129**	2411	**2711**	3019
59	257	487	739	1009	**1279**	1553	1847	**2131**	2417	**2713**	3023
61	263	491	743	1013	1283	1559	1861	2137	2423	2719	3037
67	**269**	499	751	**1019**	**1289**	1567	1867	**2141**	2437	**2729**	3041
71	**271**	503	757	**1021**	**1291**	1571	**1871**	**2143**	2441	**2731**	3049
73	277	509	761	**1031**	1297	1579	**1873**	2153	2447	2741	3061
79	**281**	**521**	769	**1033**	**1301**	1583	**1877**	2161	2459	2749	3067
83	**283**	**523**	773	1039	**1303**	1597	**1879**	2179	2467	2753	3079
89	293	541	787	**1049**	1307	1601	1889	2203	2473	2767	3083
97	307	547	797	**1051**	**1319**	1607	1901	2207	2477	2777	3089
101	**311**	557	**809**	**1061**	**1321**	1609	1907	2213	2503	**2789**	3109
103	**313**	563	**811**	**1063**	1327	1613	1913	2221	2521	**2791**	**3119**
107	317	**569**	**821**	1069	1361	**1619**	**1931**	**2237**	2531	2797	**3121**
109	331	**571**	**823**	1087	1367	**1621**	**1933**	**2239**	2539	**2801**	3137
113	337	577	**827**	**1091**	1373	1627	**1949**	2243	2543	**2803**	3163
127	**347**	587	**829**	**1093**	1381	1637	**1951**	2251	**2549**	2819	**3167**
131	**349**	593	839	1097	1399	1657	1973	**2267**	**2551**	2833	**3169**
137	353	**599**	853	1103	1409	1663	1979	**2269**	2557	2837	3181
139	359	**601**	**857**	1109	1423	**1667**	1987	2273	2579	2843	3187
149	367	607	**859**	1117	**1427**	**1669**	1993	2281	**2591**	2851	3191
151	373	613	863	1123	**1429**	1693	**1997**	2287	**2593**	2857	3203
157	379	**617**	877	1129	1433	**1697**	**1999**	2293	2609	2861	3209
163	383	**619**	**881**	**1151**	1439	**1699**	2003	2297	2617	2879	3217

3221	3547	3881	**4231**	4591	4951	5303	**5653**	6011	6343	6719	7069
3229	**3557**	3889	**4241**	4597	4957	5309	**5657**	6029	6353	6733	7079
3251	**3559**	3907	**4243**	4603	**4967**	5323	**5659**	6037	6359	6737	7103
3253	3571	**3917**	4253	4621	**4969**	5333	5669	6043	6361	**6761**	7109
3257	**3581**	**3919**	**4259**	**4637**	4973	5347	5683	6047	6367	**6763**	7121
3259	**3583**	3923	**4261**	**4639**	4987	5351	5689	6053	6373	**6779**	**7127**
3271	3593	**3929**	**4271**	4643	4993	5381	5693	6067	6379	**6781**	**7129**
3299	3607	**3931**	**4273**	**4649**	4999	5387	5701	6073	6389	**6791**	7151
3301	3613	3943	4283	**4651**	5003	5393	5711	6079	6397	**6793**	7159
3307	3617	3947	4289	4657	**5009**	5399	5717	**6089**	6421	6803	7177
3313	3623	3967	4297	4663	**5011**	5407	5737	**6091**	6427	6823	7187
3319	3631	3989	4327	4673	**5021**	5413	**5741**	6101	6449	**6827**	7193
3323	3637	**4001**	**4337**	4679	**5023**	**5417**	**5743**	6113	6451	**6829**	7207
3329	3643	**4003**	**4339**	4691	5039	**5419**	5749	6121	6469	6833	**7211**
3331	3659	4007	4349	4703	5051	5431	5779	**6131**	6473	6841	**7213**
3343	**3671**	4013	4357	**4721**	5059	5437	5783	**6133**	6481	6857	7219
3347	**3673**	**4019**	4363	**4723**	5077	**5441**	5791	6143	6491	6863	7229
3359	3677	**4021**	4373	4729	5081	**5443**	5801	6151	6521	**6869**	7237
3361	3691	4027	4391	4733	5087	5449	5807	6163	6529	**6871**	7243
3371	3697	**4049**	4397	4751	**5099**	5471	5813	6173	6547	6883	7247
3373	3701	**4051**	4409	4759	**5101**	**5477**	5821	**6197**	6551	6899	7253
3389	3709	4057	**4421**	4783	5107	**5479**	5827	**6199**	6553	6907	7283
3391	3719	4073	**4423**	**4787**	5113	5483	5839	6203	6563	6911	7297
3407	3727	4079	4441	**4789**	5119	**5501**	5843	6211	6569	6917	**7307**
3413	3733	**4091**	4447	4793	5147	**5503**	**5849**	6217	6571	**6947**	**7309**
3433	3739	**4093**	4451	4799	5153	5507	**5851**	6221	6577	**6949**	7321
3449	3761	4099	4457	4801	5167	**5519**	5857	6229	6581	**6959**	**7331**
3457	**3767**	4111	4463	4813	5171	**5521**	5861	6247	6599	**6961**	**7333**
3461	**3769**	**4127**	**4481**	4817	5179	5527	**5867**	6257	6607	6967	**7349**
3463	3779	**4129**	**4483**	4831	5189	5531	**5869**	6263	6619	6971	**7351**
3467	3793	4133	4493	4861	5197	5557	**5879**	**6269**	6637	6977	7369
3469	3797	4139	4507	4871	5209	5563	**5881**	**6271**	6653	6983	7393
3491	3803	4153	4513	4877	5227	5569	5897	6277	6659	6991	7411
3499	**3821**	**4157**	**4517**	4889	**5231**	5573	5903	6287	6661	6997	7417
3511	**3823**	**4159**	**4519**	4903	**5233**	5581	5923	**6299**	6673	7001	7433
3517	3833	4177	4523	4909	5237	5591	5927	**6301**	6679	7013	7451
3527	3847	4201	**4547**	4919	5261	5623	5939	6311	**6689**	7019	**7457**
3529	**3851**	4211	**4549**	**4931**	5273	5639	5953	6317	**6691**	7027	**7459**
3533	**3853**	**4217**	4561	**4933**	**5279**	5641	5981	6323	**6701**	7039	7477
3539	3863	**4219**	4567	4937	**5281**	5647	5987	6329	**6703**	7043	7481
3541	3877	**4229**	4583	4943	5297	**5651**	6007	6337	6709	7057	**7487**

7489	7673	7883	8117	8329	8581	8761	**8999**	9203	**9419**	**9629**	9839
7499	7681	7901	8123	8353	**8597**	8779	**9001**	9209	**9421**	**9631**	9851
7507	7687	7907	8147	8363	**8599**	8783	9007	9221	**9431**	9643	**9857**
7517	7691	7919	8161	8369	8609	8803	**9011**	9227	**9433**	9661	**9859**
7523	7699	7927	8167	8377	8623	8807	**9013**	**9239**	**9437**	9677	9871
7529	7703	7933	8171	**8387**	**8627**	**8819**	9029	**9241**	**9439**	9679	9883
7537	7717	7937	8179	**8389**	**8629**	**8821**	**9041**	9257	**9461**	9689	9887
7541	7723	**7949**	8191	8419	8641	8831	**9043**	9277	**9463**	9697	9901
7547	7727	**7951**	8209	8423	8647	**8837**	9049	**9281**	9467	**9719**	9907
7549	7741	7963	**8219**	**8429**	8663	**8839**	9059	**9283**	9473	**9721**	9923
7559	7753	7993	**8221**	**8431**	8669	8849	9067	9293	9479	9733	**9929**
7561	**7757**	**8009**	**8231**	8443	8677	**8861**	9091	9311	9491	9739	**9931**
7573	**7759**	**8011**	**8233**	8447	8681	**8863**	9103	9319	9497	9743	9941
7577	7789	8017	8237	8461	8689	8867	9109	9323	9511	9749	9949
7583	7793	8039	8243	8467	8693	8887	9127	9337	9521	**9767**	9967
7589	7817	8053	8263	8501	8699	8893	9133	**9341**	9533	**9769**	9973
7591	7823	8059	8269	8513	8707	8923	9137	**9343**	9539	9781	
7603	7829	8069	8273	8521	8713	8929	9151	9349	9547	9787	
7607	7841	8081	8287	8527	8719	8933	9157	9371	9551	9791	
7621	7853	**8087**	**8291**	**8537**	8731	8941	9161	9377	9587	9803	
7639	7867	**8089**	**8293**	**8539**	8737	8951	9173	9391	9601	9811	
7643	7873	8093	8297	8543	8741	8963	9181	9397	9613	9817	
7649	**7877**	8101	8311	8563	8747	**8969**	9187	9403	9619	9829	
7669	**7879**	8111	8317	8573	8753	**8971**	9199	9413	9623	9833	

ANEXA 2: Funcţia $\pi(x)$ şi estimările sale

Reamintim că pentru $x \in \mathbf{R}$, prin $\pi(x)$ am notat numărul numerelor prime $p \leq x$(vezi §3 de la Capitolul 2) iar pentru $x \geq 2, L_i(x) = \int_2^x \frac{1}{\ln t} dt$.

Avem următorul tabel care ne dă estimări pentru $\pi(x)$, $\frac{x}{\lg x}$, $L_i(x)$, $\frac{\pi(x)}{x/\lg x}$, $\frac{\pi(x)}{L_i(x)}$ şi din care deducem felul în care au fost sugerate anumite conjecturi(în special cele aLe lui Gauss):

x	$\pi(x)$	$\frac{x}{\lg x}$	$L_i(x)$	$\frac{\pi(x)}{x/\lg x}$	$\frac{\pi(x)}{L_i(x)}$
1000	168	145	178	1,158	0,9438
10000	1229	1086	1246	1,132	0,9864
100000	9592	8686	9630	1,104	0,9961
1000000	78498	72382	78628	1,084	0,9983
10000000	664579	620420	664918	1,071	0,9994
100000000	5761455	5428681	5762209	1,061	0,99986
1000000000	50847478	48254630	50849253	1,054	0,99996

Astfel, Gauss a conjecturat că pentru orice $x \in \mathbf{R}_+, \pi(x) < L_i(x)$(se observă că această inegalitate este adevărată pentru valorile lui x din tabel). Cu toate acestea, conjectura lui Gauss este falsă. Astfel **J.E. Littewood** în articolul **Sur la distribution des nombres premiers** din **C.R. Acad. Sci. Paris, vol 158, 1914, pp. 1869-1872**, numai că a infirmat conjectura lui Gauss dar a şi probat existenţa unui şir $(x_n)_{n\geq 0}$ de numere reale astfel încât $\lim_{n\to\infty} x_n = \infty$ şi $(-1)^{n+1}[\pi(x) - L_i(x)] > 0$ pentru orice $n \in \mathbf{N}$(rezultând astfel că $\pi(x) - L_i(x)$ îşi schimbă semnul de o infinitate de ori).

ANEXA 3: Numerele lui Fermat, numerele lui Mersene şi numere perfecte

In tabelul următor am selectat anumite informaţii despre numerele $F_1, F_2, ..., F_{22}$:

n	Factori primi	Descoperit de	Data descoperirii
1	5	Fermat	
2	17	Fermat	
3	257	Fermat	
4	65537	Fermat	
5	641	Euler	1732
5	6700417	Euler	1732
6	274177	Landry	1880
6	67280421310721	Landry, LeLasseur, Gerardin	1880
7	59649589127497217	Morrison, Brillhart	1970
7	5704689200685129054721	Morrison, Brillhart	1970
8	1238926361552897	Morehead, Western	1909
9	2424833	Western	1903
9	compus	Brillhart	1967
10	45592577	Selfridge	1953
10	6487031809	Brillhart	1962
10	455925777	Brillhart	1967
11	319489	Cunningham	1899
11	974849	Cunningham	1899
12	114689	Lucas, Pervouchine	1877
12	26017793	Western	1903
12	63766529	Western	1903
12	190274191361	Hallyburton, Brillhart	1974
13	2710954639361	Hallyburton, Brillhart	1974
14	compus(factor necunoscut)	Selfridge, Hurwitz	1961
15	1214251009	Kraitchik	1925
16	825753601	Selfridge	1953
17	compus		
18	13631489	Western	1903
19	70525124609	Riesel	1962
20	compus	Young, Bell	1988
21	448529642913	Wrathall	1963
22	natură necunoscută		

Din analiza acestui tabel se desprind următoarele:

1) Numerele F_1, F_2, F_3, F_4 sunt prime;

2) Primul număr Fermat care nu este prim este F_5(infirmându-se astfel o conjectură a lui Fermat potrivit căreiatote numerele $F_n, n \geq 1$ sunt prime);

3) Până la acest moment doar pentru $n = 5, 6, 7, 8, 9$ şi 11 se cunoaşte că sunt numere compuse(cunoscându-se complet descompunerea lor în factori primi);

4) F_{14} este cel mai mic număr Fermat despre care se ştie că este compus, fără însă a i se cunoaşte factorii primi;

5) F_{22} este cel mai mic număr Fermat despre care nu se cunoaşte dacă este prim sau nu.

Iată tabelul primelor 12 numere Mersenne:

p	$M_p = 2^p - 1$
2	3
3	7
5	31
7	127
13	8191
17	131071
19	524287
31	2147483647
61	2305843009213693951
89	618970019642690137449562111
107	162259276829213363391578010288127
127	170141183460469231731687303715884105727

Conform Teoremei 9.4.1 de la Capitolul 9, numărul n este perfect daă şi numai dacă n este de forma $n = 2^{p-1}(2^p - 1)$ cu $p \in \mathbf{N}^*$ iar $M_p = 2^p - 1$ este prim(acest rezultat datorâdu-se lui Euclid şi Euler).

Iată tabelul primelor 30 de numere perfecte $n = 2^{p-1}(2^p - 1)$:

n	Numărul de cifre	Data descoperirii	Descoperit de
$6 = 2(2^2 - 1)$	1	?	Cunoscut de Euclid
$28 = 2^2(2^3 - 1)$	2	?	Cunoscut de Euclid
$496 = 2^4(2^5 - 1)$	3	?	Cunoscut de Euclid
$8128 = 2^6(2^7 - 1)$	4	?	Cunoscut de Euclid
$33550336 = 2^{12}(2^{13} - 1)$	8	1456	Necunoscut
$8589869056 = 2^{16}(2^{17} - 1)$	10	1588	Cataldi
$137438691328 = 2^{18}(2^{19} - 1)$	12	1588	Cataldi
$2^{30}(2^{31} - 1)$	19	1772	L.Euler
$2^{60}(2^{61} - 1)$	37	1883	I.M. Pervouchine
$2^{88}(2^{89} - 1)$	54	1911	R.E. Powers

n	Numărul de cifre	Data descoperirii	Descoperit de
$2^{106}(2^{107}-1)$	65	1914	R.E. Powers
$2^{126}(2^{127}-1)$	77	1876	E. Lucas
$2^{520}(2^{521}-1)$	314	1952	R. Robinson
$2^{606}(2^{607}-1)$	366	1952	R. Robinson
$2^{1278}(2^{1279}-1)$	770	1952	R. Robinson
$2^{2202}(2^{2203}-1)$	1327	1952	R. Robinson
$2^{2280}(2^{2281}-1)$	1373	1952	R. Robinson
$2^{3216}(2^{3217}-1)$	1937	1957	H. Riesel
$2^{4252}(2^{4253}-1)$	2561	1961	A. Hurwitz
$^{4422}(2^{4}423-1)$	2663	1961	A. Hurwitz
$2^{9688}(2^{9689}-1)$	5834	1963	D. Gillies
$2^{9940}(2^{9941}-1)$	5985	1963	D. Gillies
$2^{11212}(2^{11213}-1)$	6571	1936	D. Gillies
$2^{19936}(2^{19937}-1)$	12003	1971	B. Tuckerman
$2^{21700}(2^{21701}-1)$	13066	1978	L. Nickel, C. Noll
$2^{23208}(2^{23209}-1)$	13973	1979	C. Noll
$2^{44496}(2^{44497}-1)$	26790	1979	H. Nelson, D. Slowinski
$2^{86242}(2^{86243}-1)$	51924	1982	D. Slowinski
$2^{110502}(2^{110503}-1)$	66530	1988	W.N. Colquitt, L. Welsh
$2^{132048}(2^{132049}-1)$	79502	1991	W.N. Colquitt, L. Welsh

Observaţie. Laura Nickel şi Curt Noll avea numai 18 ani când au pus în evidenţă al 25-lea număr perfect. Nu se cunoaşte dacă există sau nu numere perfecte între cele corespunzătoare lui $p = 132049$ şi $p = 216091$.

Bibliography

[1] Albu,T., Ionescu,I., *Principiul includerii şi excluderii*, Gazeta matematică, Seria B, nr.6 (1969).

[2] Alexandru, V., Goşoiu, M. N., *Elemente de teoria numerelor*, Ed. Universităţii Bucureşti, 1999.

[3] Andreescu, T., Andrica, D., *O introducere în studiul ecuaţiilor diofantiniene*, Ed. Gil, Zalău, 2002.

[4] Banea, H., *Probleme de matematică traduse din revista sovietică Kvant*, Ed. Didactică şi Pedagogică, Bucureşti, 1983.

[5] Buşneag, D, Maftei, I.V., *Teme pentru cercurile si concursurile de matematica ale elevilor*, Ed. Scrisul Românesc, Craiova, 1983.

[6] Buşneag, D., Boboc, Fl., Piciu, D., *Aritmetică şi teoria numerelor*, Ed. Universitaria, Craiova, 1999.

[7] Buşneag, D., Piciu, D., *Lecţii de algebră*, Ed. Universitaria, Craiova, 2002.

[8] Buşneag, D., Dincă, A., Ebâncă, D., Niculescu, C.P., Popescu, M., Vladimirescu, I., Vraciu, G., *Concursul de matematică "Gheorghe Ţiţeica*" 1979-1998, Ed. Gil, Zalău ,1999.

[9] Buşneag, D., Chirteş, Fl., Piciu, D., *Probleme de logică şi teoria mulţimilor*, Ed. Universitaria, Craiova, 2003.

[10] Buşneag, D., Chirteş, Fl., Piciu, D., *Complemente de algebră*, Ed. Gil, Zalău, 2006.

[11] Carthy, Mc., *Introduction to Arithmetical Functions*, Springer-Verlag, 1986.

[12] Chahal, J.S., *Topics in Number Theory*, Plenum Press ,1988.

[13] Cuculescu, I., *Olimpiadele internaţionale de matematică ale elevilor*, Ed. Tehnică, Bucureşti, 1984.

[14] Cucurezeanu, I., *Probleme de aritmetică şi teoria numerelor*, Ed. Tehnică, Bucureşti, 1976.

[15] Descombes, E., *Éleménts de théorie des nombres*, Press Universitaires de France, 1986.

[16] Eckstein, G., *Fracţii continue*, Revista Matematică de Timişoara, nr. 1 (1986), 17-36.

[17] Herman, J., Kučera, R., Šimša, J., *Equations and Inequalities, Elementary Problems and Theorems in Algebra and Number Theory*, Springer(CMS), 2000.

[18] Hincin, A.I., *Fracţii continue*, Ed. Tehnică, Bucureşti, 1960.

[19] Honsberger, R., *Mathematical gems*, The Mathematical Association of America, vol.1,1973.

[20] Iaglom, A.M., Iaglom, I.M., *Probleme neelementare tratate elementar*, Ed.Tehnică, Bucureşti,1983.

[21] Iliescu, I., Ionescu, B., Radu, D., *Probleme de matematică pentru admiterea în învăţământul superior*, Ed. Didactică şi Pedagogică , Bucureşti, 1976.

[22] Ion,D.I., Niţă, C., *Elemente de aritmetică cu aplicaţii în tehnici de calcul*, Ed. Tehnică, Bucureşti, 1978.

[23] Ion, I.D., Radu, N., *Algebra*, Ed. Didactică şi Pedagogică, Bucureşti, 1991.

[24] Ion, I.D., Nastasescu, C., Niţă, C., *Complemente de Algebră*, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1994.

[25] Irleand, K., Rosen, M.A., *Classical Introduction to Modern Number Theory*, Second edition, Springer, 1990.

[26] Konisk, J.M., Mercier, A., *Introduction à la théorie des nombers*, Modulo Editeur, 1994.

[27] Mollin, A.R., *Fundamental number theory with applications*, CRC Press LLC, New York, 1998.

[28] Morozova, A.E., Petakov, I.S., Skortov, V.A., *Olimpiadele internaţionale de matematică*, Ed. Tehnică, Bucureşti, 1978.

[29] Năstăsescu, C., *Introducere în teoria mulţimilor*, Ed. Didactică şi Pedagogică, Bucureşti, 1974.

[30] Năstăsescu, C., *Asupra grupurilor finite*, Gazeta matematică (Perfecţionare metodică şi metodologică), nr.4 (1981).

[31] Năstăsescu, C., Niţă, C., Vraciu, C., *Bazele algebrei*, Vol. I, Ed. Academiei, Bucureşti, 1986.

[32] Năstăsescu, C., Ţena, M., Andrei, G., Odărăşanu, I., *Probleme de structuri algebrice*, Ed.Tehnică, Bucureşti, 1988.

[33] Năstăsescu, C., Niţă, C., Brandiburu, M., Joiţa, D., *Exerciţii de algebră*, Ed. Didactică şi Pedagogică , Bucureşti, 1992.

[34] Năstăsescu, C., Niţă, C., Vraciu, C., *Aritmetică şi algebră*, Ed. Didactică şi Pedagogică S.A., Bucureşti, 1993.

[35] Niven, I., Zuckerman, H.S., Montgomery, H.L., *An introduction to the Theory of Numbers*, Fifth edition, John and Sons, Inc., 1991.

[36] Panaitopol, L., Gica, L., *Probleme celebre de teoria numerelor*, Ed. Universităţii din Bucureşti, 1998.

[37] Panaitopol, L., Gica, L., *O introducere în aritmetică şi teoria numerelor*, Ed. Universităţii din Bucureşti, 2001.

[38] Panaitopol, L., Gica, L., *Probleme de aritmetică şi teoria numerelor. Idei şi metode de rezolvare*, Ed. Gil, Zalău, 2006.

[39] Popescu, D., Oboroceanu, G., *Exerciţii şi probleme de algebră, combinatorică şi teoria mulţimilor*, Ed. Didactică şi Pedagogică, Bucureşti, 1983.

[40] Popovici, C.P., *Teoria Numerelor*, Ed. Didactică şi Pedagogică, Bucureşti, 1973.

[41] Posnikov, M.M., *Despre teorema lui Fermat (Introducere în teoria algebrică a numerelor)*, Ed. Didactică şi Pedagogică, Bucureşti, 1983.

[42] Radovici Mărculescu, P., *Probleme de teoria elementară a numerelor*, Ed. Tehnică, Bucureşti, 1983.

[43] Ribenboim, P., *Nombres premiers; mysteres et records*, Press Universitaire de France, 1994.

[44] Rosen, K.H., *Elementary Number Theory and its Applications*, Addison-Wesley Publishing Company, 1988.

[45] Rusu, E., *Bazele teoriei numerelor*, Ed. Tehnică, Bucureşti, 1953.

[46] Serre, J.P., *A Course in Arithmetics*, Springer-Verlag, 1973.

[47] Shidlovsky, A.B., *Transcedental numbers*, Walter de Gayter, 1989.

[48] Sierpinsky, W., *Elementary Theory of Numbers*, Polski Academic Nauk, Warsaw, 1964.

[49] Sierpinsky, W., *Ce ştim şi ce nu ştim despre numerele prime*, Ed. Ştiinţifică, Bucureşti, 1966.

[50] Sierpinsky, W., *250 Problemes des Théorie Elementaire des Nombres*, Collection Hachette Universite, 1972.

[51] Tomescu, I.(coordonator) şi alţii, *Probleme date la olimpiadele de matematică pentru licee (1950 - 1990)*, Ed. Ştiinţifică, Bucureşti, 1992.

[52] *Colecţia Gazeta matematică*, 1964-2007.