LAURENȚIU PANAITOPOL ALEXANDRU GICA

PROBLEME CELEBRE DE TEORIA NUMERELOR

EDITURA UNIVERSITĂȚII DIN BUCUREȘTI
1998

LAURENȚIU PANAITOPOL ALEXANDRU GICA

PROBLEME CELEBRE DE TEORIA NUMERELOR

EDITURA UNIVERSITĂȚII DIN BUCUREȘTI
1998

Referenți științifici: Prof. dr. ION D. ION
Prof. dr. CONSTANTIN POPOVICI

Șos. Panduri, 90-92, București - 76235; Telefon 410.23.84

Tehnoredactare computerizată: Iacob Victoria

ISBN 973-575-196-8

CUPRINS

PREFAȚĂ

Lucrarea de față prezintă opt probleme dificile de teoria numerelor, majoritatea dintre ele fiind publicate pentru prima dată în limba română. Cu o singură excepție demonstrațiile sunt elementare (fără utilizarea analizei complexe).

Fiecare capitol debutează prin indicarea bibliografiei utilizate și cu un mic istoric încheindu-se cu o anexă - deseori foarte consistentă - care permite înțelegerea demonstrațiilor chiar și pentru cititorul mai puțin familiarizat cu descifrarea unor lucrări științifice. Un student care a urmat cursul de „teoria numerelor" (anii II-III) al Facultății de Matematică a Universității București este capabil să urmărească textele prezentate.

Mai trebuie subliniat că lucrarea nu se rezumă la traducerea articolelor indicate; fiecare dintre acestea a fost supus unei operațiuni de prelucrare, de „accesibilizare". Practic s-au păstrat numai ideile fundamentale din lucrările folosite. În câteva dintre articole s-au înlăturat neclaritățile existente sau micile incorectitudini. De asemenea s-a urmărit - atât cât a fost posibil - o uniformizare a modului de prezentare a problemelor.

Această carte, care se vrea o prelungire a tematicii cursului la care ne-am referit mai sus, este de natură să contribuie la orientarea studenților secției didactice în alegerea lucrărilor de diplomă. De asemenea lucrarea este utilă celor care urmează cursul „Metode analitice în teoria numerelor" din cadrul programului de studii aprofundate.

Autorii

Iulie 1995

ECUAȚIA $x^2 - dy^2 = k$. EXISTENȚA SOLUȚIILOR. ALGORITMI DE REZOLVARE

Introducere

În acest capitol se studiază soluțiile întregi ale ecuațiilor de forma

$$x^2 - dy^2 = k,$$

unde $d \in \mathbf{N}$ și $k \in \mathbf{Z}$. Dacă $d = n^2$, $n \in \mathbf{N}$, atunci

$$(x - ny) \cdot (x + ny) = k$$

și modul de rezolvare al unei astfel de ecuații este cunoscut. Deci se impune în plus condiția $\sqrt{d} \notin \mathbf{N}$ și $k \neq 0$ (dacă $k = 0$ și $\sqrt{d} \notin \mathbf{N}$ atunci ecuația $x^2 - dy^2 = 0$ are ca soluții întregi doar perechea $x = y = 0$). În teorema 1 folosindu-se teorema lui Minkovski asupra corpului convex precum și diverse proprietăți ale inelului

$$R = \{m + n\sqrt{d} \mid m, n \in \mathbf{Z}\}$$

se rezolvă problema soluțiilor întregi ale ecuației $x^2 - dy^2 = \pm 1$.

Aceste ecuații sunt în strânsă legătură cu problema structurii unităților inelului R. Mai precis se arată că există o unitate

$$\varepsilon_0 = m + n\sqrt{d},\ m, n \in \mathbf{N},\ (m, n) \neq (1, 0)$$

astfel încât oricare ar fi o altă unitate ε a lui R atunci $\varepsilon = \pm \varepsilon_0^l$ cu $l \in \mathbf{Z}$.

Avem că $m^2 - dn^2 = \pm 1$. Notăm cu ε, fie ε_0 dacă $m^2 - dn^2 = 1$, fie ε_0^2 dacă $m^2 - dn^2 = -1$; $\varepsilon = a + b\sqrt{d}$, $a, b \in \mathbf{N}$, $(a, b) \neq (1, 0)$.

Atunci orice soluție (x_s, y_s) în numere naturale a ecuației Pell $x^2 - dy^2 = 1$ se obține astfel

$$(x_s + \sqrt{d}\, y_s) = \varepsilon^s = (a + b\sqrt{d})^s,\ (\forall)\ s \in \mathbf{N}.$$

Teorema 1 nu este însă folositoare din punctul de vedere al modului efectiv de construcție al unității ε_0, respectiv ε. De aceea se dă mai apoi un algoritm de

construcție pentru ε_0 și ε care utilizează în special chestiuni legate de fracții continue (în paragraful II al anexei se demonstrează tot ce este necesar în legătură cu fracțiile continue pentru a înțelege algoritmul menționat mai sus). După aceea se arată cum pentru un $k \in \mathbf{Z}$, $k \neq 0$ se poate preciza un algoritm pentru găsirea unor elemente

$$\mu_1, \mu_2, \ldots \mu_r \in R, N(\mu_i) = k\ (\forall)\ i = \overline{1,r}$$

(deci dacă $\mu_i = c_i + \sqrt{d}\ d_i$, $c_i, d_i \in \mathbf{Z}$ atunci $c_i^2 - dd_i^2 = k\ (\forall)\ i = \overline{1,r}$), astfel încât $(\forall)\ x, y \in \mathbf{Z}$ astfel ca $x^2 - dy^2 = k$ atunci $x + \sqrt{d}\,y = \pm \mu_i^{*} \varepsilon^l$ (unde $1 \leq i \leq r$, $l \in \mathbf{Z}$, semnul $*$ fie nu înseamnă nimic, fie este semnul de conjugare).

Dacă $x \in \mathbf{R}\backslash Q$, $x > 0$, vom numi reprezentare a lui x sub formă de fracție continuă simplă un șir de numere naturale $a_0, a_1, \ldots a_n, \ldots$ cu proprietatea că

$$a_0 = [x]\ ,\ x = a_0 + \frac{1}{x_1},\ x_1 > 1,$$

$$a_1 = [x_1],\ x_1 = a_1 + \frac{1}{x_2},\ x_2 > 1$$

și în general

$$x = a_0 + \frac{1}{|a_1|} + \frac{1}{|a_2|} + \ldots + \frac{1}{|a_n|} + \frac{1}{|x_{n+1}|},\ x_{n+1} > 1\ (\forall)\ n \in \mathbf{N},$$

$$x_n = a_n + \frac{1}{x_{n+1}},\ a_n = [x_n],\ (\forall)\ n \in \mathbf{N}^*$$

(am folosit notațiile din paragraful II al anexei). Notând

$$\frac{P_n}{Q_n} = a_0 + \frac{1}{|a_1|} + \ldots + \frac{1}{|a_n|}$$

atunci prin inducție se arată că $Q_n \geq n\ (\forall)\ n \in \mathbf{N}^*$. $Q_1 = a_1 \geq 1$ (deoarece $a_1 = [x_1] \geq 1$), $Q_2 = a_1 a_2 + 1 \geq 2$, deci verificarea este făcută. Dacă $Q_{k-1} \geq k - 1$ și $Q_k \geq k$ atunci conform propoziției 1 din paragraful II al anexei

$$Q_{k+1} = Q_k \cdot a_{k+1} + Q_{k-1} \geq k \cdot a_{k+1} + (k-1) \geq k + (k-1) \geq k + 1$$

(dacă $k \geq 2$), deci enunțul $Q_k \geq k\ (\forall)\ k \in \mathbf{N}^*$ este demonstrat prin inducție. Folosind din nou propozițiile 1 și 2 din paragraful II al anexei deducem că:

$$x - \frac{P_n}{Q_n} = \frac{P_n x_{n+1} + P_{n-1}}{Q_n x_{n+1} + Q_{n-1}} - \frac{P_n}{Q_n} = \frac{P_{n-1}Q_n - P_n Q_{n-1}}{Q_n(Q_n x_{n+1} + Q_{n-1})} = \frac{(-1)^n}{Q_n(Q_n x_{n+1} + Q_{n-1})}$$

Deoarece $x_{n+1} > a_{n+1}$ și $Q_n a_{n+1} + Q_{n-1} = Q_{n+1}$, din cele de mai sus deducem că $\left| x - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n\left(Q_n a_{n+1} + Q_{n-1}\right)} = \frac{1}{Q_n Q_{n+1}} \leq \frac{1}{n(n+1)}$ $(\forall)\ n \in \mathbf{N}^*$, ceea ce înseamnă că $\lim_{n\to\infty} \frac{P_n}{Q_n} = x$. Am făcut această observație pentru a vedea că numerele naturale $a_0, a_1, \ldots a_n, \ldots$ determină numărul irațional x.

Ecuația $x^2 - dy^2 = k$

Vom nota în cele ce urmează cu R inelul comutativ: $R = \{m + n\sqrt{d} \mid m, n \in \mathbf{Z}\}$, unde d este un număr natural fixat cu proprietatea că $\sqrt{d} \notin \mathbf{N}$. Vom folosi în continuare următoarele notații: $\alpha \sim \beta$, dacă α și β sunt elemente din R cu proprietatea că există o unitate ε din R astfel încât $\alpha = \varepsilon \cdot \beta$ ($\varepsilon \in R$ se numește unitate dacă $(\exists)\ \varepsilon_1 \in R$ cu proprietatea că $\varepsilon\varepsilon_1 = \varepsilon_1\varepsilon = 1$. Se spune că două elemente α și β din R sunt asociate în divizibilitate dacă $\alpha \sim \beta$). Dacă $\mu \in R$, $\mu = a + b\sqrt{d}$ $(a, b \in \mathbf{Z})$ vom nota cu $\overline{\mu} \in R$ elementul

$$\overline{\mu} = a - b\sqrt{d}, \mu \in R$$

($\overline{\mu}$ se numește conjugatul elementului μ). Vom nota cu $N : R \to \mathbf{Z}$ următoarea funcție (numită și funcția normă)

$$N(\mu) = a^2 - db^2 = \mu \cdot \overline{\mu},$$

dacă $\mu = a + b\sqrt{d}$, unde $a, b \in \mathbf{Z}$. S-a demonstrat în paragraful I al anexei că

$$N(\mu_1 \mu_2) = N(\mu_1) \cdot N(\mu_2)\ (\forall)\ \mu_1, \mu_2 \in R$$

și că ε este unitate în R dacă și numai dacă $N(\varepsilon) = \pm 1$.

Dacă $\mu \in R$, $\mu \neq 0$ vom nota cu $l(\mu)$ următorul vector din R^2: $l(\mu) = (ln|\mu|, ln|\overline{\mu}|)$.

Teorema 1: *Există o unitate ε_0 în inelul R astfel încât oricare ar fi o altă unitate ε a inelului R, există $k \in \mathbf{Z}$ și o alegere a semnului + sau – astfel încât $\varepsilon = \pm \varepsilon_0^k$ (în plus $\varepsilon_0 \neq \pm 1$).*

Demonstrație: Fie q un număr real satisfăcând inegalitatea $q > 2\sqrt{d}$. Pentru $\alpha \in R$, $\alpha \neq 0$ satisfăcând condiția $|N(\alpha)| \leq q$ vom nota cu $Y\alpha$ următoarea mulțime din $\mathbf{R}^2$:

$$Y\alpha = \{(x, y) \in H \mid x \geq ln|\alpha| \text{ și } y \geq ln|\overline{\alpha}|\},$$

unde

$$H = \{x, y) \in \mathbf{R}^2 \mid x + y = ln\, q\}.$$

Arătăm întâi că $(\forall)\ \alpha \in R$, $\alpha \neq 0$, $Y\alpha$ este o mulțime mărginită în $\mathbf{R}^2$.

Într-adevăr dacă $(x, y) \in Y\alpha$ atunci $x \geq ln\ |\alpha|$ și $y \geq ln\ |\overline{\alpha}|$. Însă $(x, y) \in H$, deci $x + y = ln\ q$. Aceasta înseamnă că

$$x = ln\ q - y \leq lnq - ln\ |\overline{\alpha}|$$

și că

$$y = ln\ q - x \leq ln\ q - ln\ |\alpha|.$$

De aici se deduce că $Y\alpha$ este o mulțime mărginită (dacă în plus $|N(\alpha)| \leq q$ atunci $Y\alpha$ este o mulțime nevidă. Într-adevăr din inegalitatea

$$|N(\alpha)| = |\alpha \cdot \overline{\alpha}| \leq q$$

se deduce că

$$ln|\alpha| + ln|\overline{\alpha}| \leq ln\ q$$

de unde și concluzia că $Y\alpha \neq \phi$).

Arătăm acum că

$$Y\alpha\varepsilon = Y\alpha + l(\varepsilon)$$

oricare ar fi ε o unitate în R. Fie $(x, y) \in Y\alpha$; aceasta înseamnă că

$$x + y = ln\ q,\ x \geq ln\ |\alpha| \text{ și } y \geq ln\ |\overline{\alpha}|.$$

Dacă notăm cu

$$(x_1, y_1) = (x, y) + l(\varepsilon) = (x + ln\ |\varepsilon|, y + ln\ |\overline{\varepsilon}|)$$

atunci

$$x_1 + y_1 = x + y + ln\ |\varepsilon| + ln\ |\overline{\varepsilon}| = x + y + ln\ |\varepsilon \cdot \overline{\varepsilon}| = ln\ q$$

(deoarece $x + y = ln\ q$ și $|\varepsilon \cdot \overline{\varepsilon}| = |N(\varepsilon)| = 1$. Conform propoziției 2 din paragraful I al anexei, $\varepsilon \in R$ este unitate dacă și numai dacă $N(\varepsilon) = \pm 1$). De asemenea

$$x_1 = x + ln|\varepsilon| \geq ln\ |\alpha| + ln\ |\varepsilon| = ln\ |\alpha\varepsilon|$$

și

$$y_1 = y + ln\ |\overline{\varepsilon}| \geq ln\ |\overline{\alpha}| + ln\ |\overline{\varepsilon}| = ln\ |\overline{\alpha}\,\overline{\varepsilon}| = ln\ |\overline{\alpha\varepsilon}|$$

(deoarece conform propoziției 4 din paragraful I al anexei avem că $\overline{\mu}_1\overline{\mu}_2 = \overline{\mu_1\mu_2}$ $(\forall)\ \mu_1, \mu_2 \in R$). Aceasta înseamnă că $(x_1, y_1) \in Y\alpha\varepsilon$, deci

$$Y\alpha + l(\varepsilon) \subseteq Y\alpha\varepsilon.$$

Pentru a demonstra incluziunea cealaltă fie $(x_1, y_1) \in Y\alpha\varepsilon$. Aceasta înseamnă că

$$x_1 + y_1 = ln\ q$$

și

$$x_1 \geq ln\ |\alpha\varepsilon|,\ y_1 \geq ln\ |\overline{\alpha}\,\overline{\varepsilon}| = ln\ |\overline{\alpha\varepsilon}|.$$

Notând cu

$$x = x_1 - ln\ |\varepsilon| \text{ și } y = y_1 - ln\ |\overline{\varepsilon}|$$

deducem că

$$x + y = ln\ q,$$
$$x \geq ln\ |\alpha\varepsilon| - ln\ |\varepsilon| = ln\ |\alpha|,$$
$$y \geq ln\ |\overline{\alpha}\,\overline{\varepsilon}| - ln\ |\overline{\varepsilon}| = ln\ |\overline{\alpha}|.$$

Aceasta înseamnă că $(x, y) \in Y\alpha$ și

$$(x_1, y_1) = (x, y) + l(\varepsilon).$$

De aici se deduce că $Y\alpha\varepsilon \subseteq Y\alpha + l(\varepsilon)$ și deci că $Y\alpha\varepsilon = Y\alpha + l(\varepsilon)$, $(\forall)\ \alpha \neq 0$, $\alpha \in R$, $|N(\alpha)| \leq q$ și ε unitate în R.

Al treilea fapt pe care-l vom demonstra este acela că

$$H \subseteq \bigcup_{\substack{|N(\alpha)|\leq q \\ \alpha\in R,\ \alpha\neq 0}} Y\alpha .$$

Pentru a demonstra acest lucru fie $(x, y) \in H$ (aceasta înseamnă că $(x, y) \in \mathbf{R}^2$ și $x + y = ln\ q$). Fie $x_1, y_1 \in \mathbf{R}_+^*$ astfel încât $x = ln\ x_1$ și $y = ln\ y_1$ (deoarece $x + y = ln\ q$ se deduce că $x_1\ y_1 = q$). Vom nota cu X următoarea mulțime din $\mathbf{R}^2$:

$$X = [-x_1, x_1] \times [-y_1, y_1].$$

X este o mulțime mărginită, convexă, simetrică și măsurabilă Lebesque (acestea sunt fapte evidente deoarece X este un dreptunghi). Dacă se notează cu λ măsura Lebesgue din $\mathbf{R}^2$ atunci

$$\lambda(X) = 4x_1 \cdot y_1 = 4 \cdot q > 4 \cdot 2\sqrt{d} = = 4\lambda(T).$$

T este paralelipipedul fundamental asociat rețelei complete

$$\Lambda = \{m(1,1) + n(\sqrt{d}, -\sqrt{d}) \mid m, n \in \mathbf{Z}\};$$

$$T = \{x(1,1) + y(\sqrt{d}, -\sqrt{d}) \mid x, y \in [0,1)\}$$

(Λ este o rețea completă deoarece (1,1) și $(\sqrt{d}, -\sqrt{d})$ sunt vectori liniar independenți peste $\mathbf{R}$ din $\mathbf{R}^2$. Terminologia folosită este cea utilizată în paragraful I al anexei teoremei lui Gauss. Tot acolo se precizează că $\lambda(T)$ se calculează după următoarea formulă:

$$\lambda(T) = \left\| \begin{matrix} 1 & ; & 1 \\ \sqrt{d} & ; & -\sqrt{d} \end{matrix} \right\| = 2\sqrt{d}\Big).$$

Folosind teorema lui Minkovski asupra corpului convex (teorema 1 din locul citat mai sus) deducem existența unor numere întregi m și n astfel încât

$$(m, n) \neq (0, 0) \text{ și } (m(1, 1) + n(\sqrt{d}, -\sqrt{d})) \in X \cap \Lambda.$$

Ținând cont de definiția mulțimii X rezultă că $|m + n\sqrt{d}| \leq x_1$ și că $|m - n\sqrt{d}| \leq y_1$. Notând cu $\alpha = m + n\sqrt{d}$ rezultă că $\alpha \in R$, $\alpha \neq 0$ (deoarece $m, n \in \mathbf{Z}$ și $(m, n) \neq (0,0)$) și că

$$|N(\alpha)| = |\alpha| \cdot |\overline{\alpha}| = |m + n\sqrt{d}| \cdot |m - n\sqrt{d}| \leq x_1\, y_1 = q.$$

Cum

$$x = ln\ x_1 \geq ln\ |m + n\sqrt{d}| = ln\ |\alpha| \text{ și } y = ln\ y_1 \geq ln\ |m - n\sqrt{d}| = ln\ |\overline{\alpha}|$$

rezultă că $(x, y) \in Y\alpha$, ceea ce demonstrează incluziunea $H \subseteq \cup\, Y\alpha$ (reuniunea se face după acele elemente α, $\alpha \in \mathbf{R}$, $\alpha \neq 0$ pentru care $|N(\alpha)| \leq q$). Utilizând propoziția 3 din paragraful I al anexei se deduce existența unui număr finit de

elemente din R $\alpha_1, \alpha_2, ..., \alpha_r$ astfel ca orice $\alpha \in R$ cu $|N(\alpha)| \leq q$ să fie asociat în divizibilitate cu unul dintre elementele $\alpha_1, \alpha_2 ... \alpha_r$.

Deoarece $Y\alpha_i$ este mulțime mărginită $(\forall)\ i = 1, r$ rezultă că mulțimea

$$Y = \bigcup_{i=1}^{r} Y\alpha_i$$

este mulțime mărginită în $\mathbf{R}^2$. Fie $(x, y) \in H$; conform celor demonstrate mai sus există $\alpha \in R$, $\alpha \neq 0$, $|N(\alpha)| \leq q$ astfel ca $(x, y) \in Y\alpha$. Datorită alegerii elementelor $\alpha_1, \alpha_2, ..., \alpha_r$ se deduce existența unui indice i, $1 \leq i \leq r$ cu proprietatea că $\alpha = \varepsilon\alpha_i$ unde ε este unitate în inelul R. Deci

$$(x, y) \in Y\alpha = Y\alpha_i\varepsilon = Y\alpha_i + l(\varepsilon)$$

ceea ce arată că $H \subseteq Y + L$, unde

$$L = \{l(\varepsilon) | \ \varepsilon \text{ unitate în } R\}.$$

Este evident că

$$(0, 0) \in L \ ((0, 0) = l(1))$$

și că $(L, +)$ este subgrup al grupului aditiv $(\mathbf{R}^2, +)$ $(l(\varepsilon_1) + l(\varepsilon_2) = l(\varepsilon_1 \cdot \varepsilon_2)$ și $l(\varepsilon) + l(\varepsilon^{-1}) = 0$ $(\forall)\ \varepsilon, \varepsilon_1$ și ε_2 unități ale inelului $\mathbf{R}$; $(0, 0) \in L)$. Deoarece Y este o mulțime mărginită și H este o mulțime nemărginită rezultă că L este o mulțime infinită, deci în particular $L \neq (0, 0)$. Presupunem că există șirul de elemente $(\varepsilon_n)_{n \in \mathbf{N}}$ de unități în R astfel încât $\lim_{n\to\infty} l(\varepsilon_n) = (0, 0)$ și $\varepsilon_n \neq \pm 1$ $(\forall)\ n \in \mathbf{N}$. Aceasta înseamnă că

$$\lim_{n\to\infty} |\varepsilon_n| = \lim_{n\to\infty} |\overline{\varepsilon}_n| = 1,$$

de unde se deduce că

$$\lim_{n\to\infty} \max \{|\varepsilon_n|, |\overline{\varepsilon}_n|\} = 1.$$

E ușor de văzut că fie $|\varepsilon_n|$, fie $|\overline{\varepsilon}_n|$ se scrie sub forma $m + n\sqrt{d}$ cu $m, n \in \mathbf{N}$.

Dacă $n \geq 1$ atunci max

$$\{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \geq \sqrt{d} \geq \sqrt{2}$$

(deoarece d este un număr natural astfel încât $\sqrt{d} \notin \mathbf{N}$; deci $d \geq 2$}. Dacă $n = 0$ atunci deoarece $\varepsilon_n \neq \pm 1$ $(\forall)\ n \in \mathbf{N}^*$, se deduce că

$$\max \{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \geq m \geq 2.$$

În ambele cazuri

$$\max \{|\varepsilon_n|, |\overline{\varepsilon}_n|\} \geq \sqrt{2},$$

deci nu se poate întâmpla ca $\lim_{n\to\infty} \max \{|\varepsilon_n|, |\varepsilon_n|\} = 1$ și nici ca

$$\lim_{n\to\infty} l(\varepsilon_n) = (0, 0).$$

Toate faptele de mai sus ne conduc la concluzia că există o unitate ε_0 $(\varepsilon_0 \neq \pm 1)$ din R astfel încât

$$\| l(\varepsilon_0) \| = \min \{\| l(\varepsilon) \| \ | \ \varepsilon \text{ unitate în } R, \varepsilon \neq \pm 1\}$$

(s-a folosit notația obișnuită $\| (a, b) \| = \sqrt{a^2 + b^2}$ $(\forall)\, a, b \in \mathbf{R}$). În considerațiile precedente s-a ținut cont, tacit, de observația că $l(\varepsilon) = (0, 0)$ pentru o unitate $\varepsilon \in R$ dacă și numai dacă $\varepsilon = \pm 1$ (demonstrația acestei observații este imediată; în particular rezultă că $\| l(\varepsilon_0) \| > 0$). Înlocuind eventual pe ε_0 cu $\pm \overline{\varepsilon}_0$ sau cu $-\varepsilon_0$ și ținând cont că

$$\| l(\varepsilon_0) \| = \| l(-\varepsilon_0) \| = \| l(\overline{\varepsilon}_0) \| = \| l(-\overline{\varepsilon}_0) \|,$$

se poate presupune că $\varepsilon_0 = m + n\sqrt{d}$ unde $m, n \in \mathbf{N}$ și $(m, n) \neq (1, 0)$; aceasta înseamnă că $\varepsilon_0 > 1$. ε_0 astfel ales poartă numele de unitate fundamentală a inelului R. Deoarece

$$ln\, |\varepsilon| + ln\, |\overline{\varepsilon}| = ln\, 1 = 0$$

pentru $(\forall)\, \varepsilon \in R$, ε unitate, există incluziunea

$$L \subseteq \{(x, y) \in \mathbf{R}^2 \mid x + y = 0\}.$$

Dacă $l(\varepsilon_0) = (\alpha, -\alpha)$ $(\alpha \in \mathbf{R}_+^*$, deoarece $\alpha = ln\, |\varepsilon_0| = ln\, \varepsilon_0 > 0$, pentru că $\varepsilon_0 > 1)$ și $l(\varepsilon) = (\beta, -\beta)$ este un alt element al mulțimii L cu $\beta > 0$ (ε unitate în R), fie $k \in \mathbf{N}^*$ astfel încât $k\alpha \leq \beta < (k+1)\alpha$ (se știe că

$$\| l(\varepsilon) \| = \beta\sqrt{2} \geq \| l(\varepsilon_0) \| = \alpha\sqrt{2},$$

deci $\beta \geq \alpha$ și $k \geq 1$). Fie $\varepsilon_1 \in R$, $\varepsilon_1 = \varepsilon \cdot \varepsilon_0^{-k}$. Atunci

$$l(\varepsilon_1) = l(\varepsilon) - kl(\varepsilon_0) = (\beta - k\alpha, -\beta + k\alpha).$$

Dacă cumva $\beta - k\alpha > 0$ atunci $\varepsilon_1 \neq \pm 1$ și

$$\|l(\varepsilon_1)\| = \sqrt{2}\,(\beta - k\alpha) < \sqrt{2}\,((k+1)\alpha - k\alpha) = \sqrt{2} \cdot \alpha = \| l(\varepsilon_0) \|,$$

ceea ce contrazice alegerea lui ε_0. Deci $\beta = k\alpha$, $l(\varepsilon_1) = 0$, ceea ce implică egalitatea $\varepsilon = \pm \varepsilon_0^k$. Dacă $l(\varepsilon) = (\beta, -\beta)$ este un element al mulțimii L cu $\beta < 0$ atunci aplicând raționamentul de mai sus pentru $\overline{\varepsilon}$ se deduce că există $k \in \mathbf{N}$ cu proprietatea că $\overline{\varepsilon} = \pm \varepsilon_0^k$. Deci $\varepsilon = \pm \varepsilon_0^{-k}$, unde $-k \in \mathbf{Z}$. Ținând cont de toate considerațiile precedente rezultă că orice unitate a inelului R se scrie sub forma $\pm \varepsilon_0^k$, unde $k \in \mathbf{Z}$.

Teorema 1 permite găsirea tuturor soluțiilor naturale (evident și pe cele întregi de asemenea) ale ecuației Pell

$$x^2 - dy^2 = 1.$$

Fie $x, y \in \mathbf{N}$ astfel încât $x^2 - dy^2 = 1$. Dacă notăm $\varepsilon = x + y\sqrt{d}$ atunci $N(\varepsilon) = x^2 - dy^2 = 1$ și deci ε este unitate a inelului R.

Există deci $k \in \mathbf{Z}$ și o alegere a semnului $\pm$ astfel încât $\varepsilon = \pm \varepsilon_0^k$. Dacă în plus se presupune că $(x, y) \neq (1, 0)$ atunci $\varepsilon > 1$. Ținând cont că $\varepsilon_0 > 1$ și că $\varepsilon = \pm \varepsilon_0^k$, $\varepsilon > 1$ deducem că $k \in \mathbf{N}^*$ și că trebuie ales semnul $+$ ($-\varepsilon_0^k < 0$ $(\forall)\, k \in \mathbf{Z}$; $\varepsilon_0^k < 1$, dacă $k \in \mathbf{Z}$ și $k < 0$). Deci $\varepsilon = \varepsilon_0^k$, unde $k \in \mathbf{N}^*$ (dacă $k = 0$ atunci $x = 1$ și $y = 0$). Dacă în plus $N(\varepsilon_0) = -1$ atunci trebuie impusă și condiția:

k este număr natural par (într-adevăr $1 = N(\varepsilon) = N(\varepsilon_0)^k = (-1)^k$ în caz că $N(\varepsilon_0) = -1$). Mai putem scrie soluțiile naturale ale ecuației Pell și sub formă recurentă:

$x_0 = 1 ; y_0 = 0$

$x_1 = m;\ \ y_1 = n,$ dacă $N(\varepsilon_0) = 1$, $\varepsilon_0 = m + n\sqrt{d}$

$x_1 = m^2 + n^2 d;\ \ y_2 = 2mn,$ dacă $N(\varepsilon_0) = -1$.

$x_{a+1} = mx_a + ndy_a;\ \ y_{a+1} = nx_a + my_a,$ dacă $N(\varepsilon_0) = 1$

$x_{a+1} = (m^2 + n^2 d)x_a + 2mndy_a;\ \ y_{a+1} = 2mnx_a + (m^2 + n^2 d)y_a,$ dacă $N(\varepsilon_0) = -1$ pentru $(\forall)\ a \in \mathbf{N}$.

În cele ce urmează ne vom ocupa cu prezentarea unui **algoritm pentru aflarea tuturor soluțiilor întregi ale ecuației**

$$x^2 - dy^2 = k,$$

unde d este număr natural astfel încât $\sqrt{d} \notin \mathbf{N}$ și $k \in \mathbf{Z}^*$.

Notațiile folosite sunt aceleași ca și la începutul acestui capitol.

Acest algoritm a fost prezentat de A. Gica în Bull. Math. de la Soc. Sci. Math. de Roumanie, vol. 38(86), nr. 3-4, 1994-1995, p. 153-156.

Fie $(x, y) \in \mathbf{Z}^2$ astfel încât $x^2 - dy^2 = k$, ceea ce se mai scrie și sub forma $N(\mu) = k$, unde $\mu = x + \sqrt{d}\, y \in R$. Dacă ε_0 este unitatea fundamentală a inelului R găsită în decursul teoremei precedente vom nota atunci cu ε, fie ε_0, dacă $N(\varepsilon_0) = 1$, fie ε_0^2 dacă $N(\varepsilon_0) = -1$. Atunci vectorii $(1, 1)$ și $l(\varepsilon)$ formează o bază în $\mathbf{R}^2$. Dacă există $\alpha, \beta \in \mathbf{R}$ astfel încât

$$\alpha(1, 1) + \beta l(\varepsilon) = 0$$

atunci

$$\alpha + \beta\, ln\, |\varepsilon| = 0$$

și

$$\alpha + \beta\, ln\, |\overline{\varepsilon}| = 0.$$

Cum

$$ln\, |\overline{\varepsilon}| = -\, ln|\varepsilon| \neq 0,$$

din ultimele două egalități se deduce că $\alpha = \beta = 0$. Aceasta demonstrează că vectorii $(1, 1)$ și $l(\varepsilon)$ formează o bază în $\mathbf{R}^2$.

Dacă $\mu = x + y\sqrt{d}$, cu $x, y \in \mathbf{Z}$ și $N(\mu) = k$, atunci $\mu \neq 0$ (deoarece $k \neq 0$) și vectorul $l(\mu)$ din $\mathbf{R}^2$ are sens. Folosind observația anterioară deducem existența numerelor reale α și γ astfel încât:

$$l(\mu) = \alpha(1, 1) + \gamma\, l(\varepsilon).$$

Obținem că

$$ln(\mu) = \alpha + \gamma\, ln\, |\varepsilon|,$$
$$ln(\overline{\mu}) = \alpha + \gamma\, ln|\overline{\varepsilon}|$$

și în particular rezultă și că

$$ln\,|k| = ln\,|N(\mu)| = ln\,|\mu| + ln\,|\overline{\mu}| = 2\alpha + \gamma\, ln\,|N(\varepsilon)| = 2\alpha.$$

Deci $\alpha = \dfrac{ln|k|}{2}$ și

$$l(\mu) = \frac{ln|k|}{2}\,(1,1) + \gamma\, l(\varepsilon).$$

Alegem $a \in \mathbf{Z}$ astfel încât $|a - \gamma| \le \dfrac{1}{2}$ (a este deci cel mai apropiat întreg de γ) și considerăm $\mu_0 = \varepsilon^{-a} \cdot \mu$. Atunci $\mu \sim \mu_0$ și

$$N(\mu_0) = N(\mu) = k.$$

În plus:

$$l(\mu_0) = \frac{ln|k|}{2}\,(1,\,1) + \gamma_1 l(\varepsilon),$$

unde $|\gamma_1| \le \dfrac{1}{2}$, $\gamma_1 = \gamma - a$. Avem deci următoarele egalități:

$$ln\,|\mu_0| = \frac{ln|k|}{2} + \gamma_1\, ln\,\varepsilon$$

și

$$ln\,|\overline{\mu}_0| = \frac{ln|k|}{2} + \gamma_1 ln|\overline{\varepsilon}| = = \frac{ln|k|}{2} - \gamma_1 ln\varepsilon \text{ (deoarece } \varepsilon > 1).$$

De aici se obține că

$$\left| ln|\mu_0| - \frac{ln|k|}{2} \right| \le \frac{1}{2} ln\,\varepsilon$$

și că

$$\left| ln|\overline{\mu}_0| - \frac{ln|k|}{2} \right| \le \frac{1}{2} ln\varepsilon.$$

Inegalitățile de mai sus se scriu și sub forma:

$$ln\sqrt{\frac{|k|}{\varepsilon}} \le ln|\mu_0| \le ln\sqrt{\varepsilon \cdot |k|}$$

$$ln\sqrt{\frac{|k|}{\varepsilon}} \le ln|\overline{\mu}_0| \le ln\sqrt{\varepsilon \cdot |k|}\,.$$

sau (eliminând logaritmii)

$$\sqrt{\frac{|k|}{\varepsilon}} \le |\mu_0| \le \sqrt{\varepsilon \cdot |k|}$$

și

$$\sqrt{\frac{|k|}{\varepsilon}} \le |\overline{\mu}_0| \le \sqrt{|k|\varepsilon}.$$

$|\mu_0|$ sau $|\overline{\mu}_0|$ se poate scrie sub forma $s + t\sqrt{d}$, cu $s, t \in \mathbf{N}$. Avem că

$$t \cdot \sqrt{d} \le \sqrt{\varepsilon \cdot |k|}$$

$(t \cdot \sqrt{d} \le \max\{|\mu_0|, |\overline{\mu}_0|\} \le \sqrt{\varepsilon \cdot |k|})$; deci $t \le \sqrt{\dfrac{\varepsilon \cdot |k|}{d}}$.

De asemenea $s \le \sqrt{\varepsilon \cdot |k|}$. Deci întâi căutăm $\mu_1, \mu_2, ..., \mu_r$ elemente din R de forma $x + y\sqrt{d}$ cu $x, y \in \mathbf{N}, x \le \sqrt{|k|\varepsilon}$, $y \le \sqrt{\dfrac{\varepsilon|k|}{d}}$ și $N(\mu_i) = k\ (\forall)\ i = \overline{1,r}$ (este evident că elementele $\mu_1, ..., \mu_r$ sunt în număr finit; aceasta rezultă de altfel și din propoziția 3, paragraful I al anexei). Concluzia tuturor acestor considerații este aceea că $(\forall)\ \mu \in R$ cu $N(\mu) = k$, atunci $\mu = \pm \dot{\mu}_i \cdot \varepsilon^l$, unde $l \in \mathbf{Z}$, semnul * înseamnă fie semnul de conjugare, fie nimic (i este un număr natural $1 \le i \le r$). Pentru a avea într-adevăr un algoritm ar mai trebui precizat cum, printr-un număr finit de procedee, se poate calcula ε, unitatea fundamentală a ecuației Pell.

Amintim că prin ε am notat fie ε_0 dacă $N(\varepsilon_0) = 1$ (ε_0 este unitatea fundamentală a inelului R), fie ε_0^2 dacă $N(\varepsilon_0) = -1$. Prezentarea acestor procedee urmărește cartea lui Waclaw Sierpinski *Elementary theory of numbers*, Warszawa, 1964, capitolul VIII.

Utilizând notațiile și informațiile din paragraful II al anexei avem că

$$\sqrt{d} = (a_0; \overline{a_1, a_2, ..., a_s}),$$

unde $a_0, a_1, ... a_s \in \mathbf{N}^*$, $a_s = 2a_0$, $a_1 = a_{s-1}$, $a_2 = a_{s-2}$ și așa mai departe. Tot acolo s-a arătat că

$$\sqrt{d} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_{s-1}} + \frac{1|}{|a_s} + \frac{1|}{|x_1} =$$

$$= a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_{s-1}} + \frac{1|}{|a_s - a_0 + \sqrt{d}} =$$

$$= a_0 + \frac{1|}{|a_1} + ... + \frac{1|}{|a_{s-1}} + \frac{1|}{|a_0 + \sqrt{d}}.$$

Folosind propoziția 1 din paragraful II al anexei rezultă că

$$\sqrt{d} = \frac{P_{s-1}\left(a_0 + \sqrt{d}\right) + P_{s-2}}{Q_{s-1}\left(a_0 + \sqrt{d}\right) + Q_{s-2}},$$

unde

$$\frac{P_{s-1}}{Q_{s-1}} = a_0 + \frac{1|}{|a_1} + \ldots + \frac{1|}{|a_{s-1}}$$

și

$$\frac{P_{s-2}}{Q_{s-2}} = a_0 + \frac{1|}{|a_1} + \ldots + \frac{1|}{|a_{s-2}}$$

(P_α, Q_α sunt polinoame în nedeterminatele $a_0, a_1, \ldots, a_\alpha$, $(\forall)\, \alpha \in \mathbf{N}$; propoziția 1 amintită mai sus dă și un algoritm de calculare a acestor polinoame. Formulele din propoziția amintită asigură faptul că $P_{s-1}, Q_{s-1}, P_{s-2}, Q_{s-2}$ sunt numere naturale nenule dacă convenim să facem aceeași notație pentru un polinom și pentru valoarea acelui polinom când se dau anumite valori nedeterminatelor polinomului).

Ținând cont de periodicitatea scrierii lui $\sqrt{d}$ ca fracție continuă deducem că

$$\sqrt{d} = \frac{P_{ks-1}\left(\sqrt{d} + a_0\right) + P_{ks-2}}{Q_{ks-1}\left(\sqrt{d} + a_0\right) + Q_{ks-2}} \quad (\forall)\, k \in \mathbf{N}^*,$$

numerele P_{ks-1}, P_{ks-2}, Q_{ks-1}, Q_{ks-2} fiind naturale nenule (vezi observația de mai sus). Egalitatea de mai sus se scrie și sub forma:

$$\sqrt{d}\ (a_0\, Q_{ks-1} + Q_{ks-2}) + dQ_{ks-1} = \sqrt{d}\ P_{ks-1} + a_0\, P_{ks-1} + P_{ks-2}.$$

Ținând cont că $\sqrt{d} \notin \mathbf{N}$ din cele de mai sus rezultă că:

(1) $\quad a_0\, Q_{ks-1} + Q_{ks-2} = P_{ks-1}\ ;\ d\, Q_{ks-1} = a_0\, P_{ks-1} + P_{ks-2}\ \ (\forall)\, k \in \mathbf{N}^*.$

Înmulțim prima din egalitățile (1) cu $(-P_{ks-1})$, a doua cu $(-Q_{ks-1})$ și apoi adunându-le obținem că:

$$-a_0 Q_{ks-1}.\, P_{ks-1} - P_{ks-1}\, Q_{ks-2}\ - dQ_{ks-1}^2 = -P_{ks-1}^2 - a_0 P_{ks-1} Q_{ks-1} - P_{ks-2} Q_{ks-1}.$$

Această din urmă egalitate se mai poate scrie și sub forma:

$$P_{ks-1}^2 - dQ_{ks-1}^2 = P_{ks-1} Q_{ks-2} - P_{ks-2} Q_{ks-1} = (-1)^{ks}$$

(faptul că $P_{ks-1} \cdot Q_{ks-2} - P_{ks-2}\, Q_{ks-1} = (-1)^{ks}$ este consecință a propoziției 2 din paragraful II al anexei). Dacă s este număr natural impar atunci

$$P_{ks-1}^2 - dQ_{ks-1}^2 = \begin{cases} -1 & \text{dacă } k = 2n+1,\ n \in \mathbf{N} \\ +1 & \text{dacă } k = 2n\ \ ,\ n \in \mathbf{N}^*. \end{cases}$$

Dacă s este număr natural natural par atunci

$$P_{ks-1}^2 - dQ_{ks-1}^2 = 1, (\forall)\, k \in \mathbf{N}^*.$$

Vom arăta că are loc și afirmația reciprocă; anume dacă $t^2 - du^2 = 1$, t, $u \in \mathbf{N}^*$, atunci există $n \in \mathbf{N}^*$ astfel încât $t = P_{ns-1}$ și $u = Q_{ns-1}$. Avem că $t > u$ (într-adevăr

$$t^2 = 1 + du^2 > du^2 \geq u^2,$$

de unde rezultă că $t > u$) și o scriere de forma

$$\frac{t}{u} = b_0 + \frac{1|}{|b_1} + \frac{1|}{|b_2} + \ldots + \frac{1|}{|b_{k-1}}$$

unde, $b_0, b_1, \ldots, b_{k-1} \in \mathbf{N}^*$ (existența unei astfel de scrieri poate fi justificată precum urmează: scriem algoritmul lui Euclid pentru numerele t și u

$$\begin{aligned}
&t = u \cdot q_0 + r_1 && q_i \in \mathbf{N}^* (\forall)\, i = 0,n \\
&u = r_1 \cdot q_1 + r_2 && r_i \in \mathbf{N} (\forall)\, i = 1,n \\
&r_1 = r_2 \cdot q_2 + r_3 && 0 < r_1 < u \\
&\cdot && 0 < r_{i+1} < r_i \qquad i = 1,n-1 \\
&\cdot \\
&\cdot \\
&r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \\
&r_{n-1} = r_n \cdot q_n
\end{aligned}$$

și atunci

$$\frac{t}{u} = q_0 + \frac{1|}{|q_1} + \frac{1|}{|q_2} + \ldots + \frac{1|}{|q_n};$$

$q_0 \geq 1$ deoarece $t > u$). În plus numărul k poate fi ales par. Dacă cumva k este impar avem două posibilități: $b_{k-1} > 1$ și $b_{k-1} = 1$. Dacă $b_{k-1} > 1$ atunci în loc de b_{k-1} vom scrie $b_{k-1} - 1 + \frac{1}{1}$, iar dacă $b_{k-1} = 1$ atunci se omite b_{k-1} și în loc de b_{k-2} se scrie $b_{k-2} + 1$ (se vede imediat că nu se poate întâmpla ca $b_0 = \frac{t}{u} = 1$ deoarece aceasta ar implica $t = u = 1$ și deci $1^2 - d \cdot 1^2 = 1$ ceea ce evident nu se poate). Deci numărul k poate fi ales par. Din egalitatea $t^2 - du^2 = 1$ se deduce că numerele t și u sunt prime între ele. Fie $t', u' \in \mathbf{N}^*$ astfel încât

$$\frac{t'}{u'} = b_0 + \frac{1|}{|b_1} + \ldots + \frac{1|}{|b_{k-2}};$$

conform propoziției 1 din paragraful II al anexei,

$$u = u' \cdot b_{k-1} + u'',$$

unde

$$\frac{t''}{u''} = b_0 + \frac{1|}{|b_1} + \ldots + \frac{1|}{|b_{k-3}}$$

dacă $k \geq 4$ (u'', $t'' \in \mathbf{N}^*$). Dacă $k \geq 4$, atunci $0 < u' < u$, iar dacă $k = 2$ atunci singurul caz în care nu are loc inegalitatea $u' < u$ este acela în care $u' = u = 1$ și $t = b_0 + 1$, $t' = b_0$.

Propoziția 2 din paragraful II al anexei arată că

$$t'u - u't = (-1)^{k-1} = -1$$

deoarece $k - 1$ este număr impar; aceasta înseamnă că

$$tu' - ut' = 1.$$

Scăzând din această ultimă identitate egalitatea

$$t^2 - du^2 = 1$$

se obține că

$$t(u' - t) = u(t' - du).$$

Deoarece u și t sunt prime între ele există $l \in \mathbf{Z}$ astfel încât:

(2) $u' - t = lu$ și $t' - du = lt$.

Deci are loc și identitatea

(3) $u' - (t - b_0u) = (l + b_0)u$.

Din faptul că

$$\frac{t}{u} = b_0 + \frac{1|}{|b_1} + \ldots + \frac{1|}{|b_{k-1}}$$

și k este par rezultă că

$$0 < \frac{t}{u} - b_0 \leq 1 \; (\frac{t}{u} - b_0 > 0$$

deoarece există măcar b_1 ca urmare a faptului că $k \in \mathbf{N}^*$ și k este par) și deci:

(4) $0 < t - b_0u \leq u$.

Cu excepția unui caz indicat mai sus $0 < u' < u$, care împreună cu inegalitatea (4) conduc la concluzia că

$$|u' - (t - b_0u)| < u.$$

Această din urmă egalitate are loc și în cazul $u' = u = 1$ deoarece

$$|u' - (t - b_0u)| = |1 - (t - b_0)| = |1 - 1| = 0 < 1 = u.$$

Aceasta, împreună cu egalitatea (3), conduce la concluzia $l + b_0 = 0$ și deci $l = -b_0$.

Formulele (2) se scriu deci sub forma

$$u' - t = -b_0u$$

și

$$t' - du = -b_0t.$$

Ținând cont de aceste ultime două egalități avem că

$$\frac{t\left(b_0+\sqrt{d}\right)+t'}{u\left(b_0+\sqrt{d}\right)+u'}=\frac{du+t\sqrt{d}}{t+u\sqrt{d}}=\sqrt{d}=b_0+\frac{1|}{|b_1}+\frac{1|}{|b_2}+\ \ldots\ +\frac{1|}{|b_{k-1}}+\frac{1|}{|b_0+\sqrt{d}}$$

(pentru deducerea ultimei egalități s-a folosit din nou propoziția 1 din paragraful II al anexei). Aceasta arată că scrierea lui $\sqrt{d}$ ca fracție continuă simplă este

$$\sqrt{d}=\left(b_0;\overline{b_1,b_2,\ldots,b_{k-1},2b_0}\right).$$

Dacă s este lungimea perioadei lui $\sqrt{d}$ (adică cel mai mic număr natural nenul pentru care

$$\sqrt{d}=\left(a_0;\overline{a_1,\ldots,a_{s-1},a_s}\right)\Big)$$

atunci evident că $s|k$; deci $(\exists)\ n \in \mathbf{N}^*$ astfel încât $k = ns$. În aceste condiții $t = P_{ns-1}$ și $u = Q_{ns-1}$. Dacă s este impar atunci n trebuie să fie par (deoarece k este par). Concluzionând toate considerentele de până acum putem spune că

$$\varepsilon = P_{2s-1} + \sqrt{d}\cdot Q_{2s-1}$$

dacă s este impar și

$$\varepsilon = P_{s-1} + \sqrt{d}\cdot Q_{s-1}$$

dacă s este par. În acest moment avem într-adevăr algoritmul căutat. Deoarece $s < 2\cdot d$ după cel mult $2\cdot d$ operații se află care este expresia lui $\sqrt{d}$ ca fracție continuă:

$$\sqrt{d}=\left(a_0;\overline{a_1,\ldots,a_s}\right)$$

și deci se pot calcula numerele P_{s-1}, Q_{s-1}, P_{2s-1}, Q_{2s-1}, implicit și unitatea fundamentală ε a ecuației Pell.

În continuare vom prezenta încă un algoritm pentru rezolvarea ecuației $x^2 - dy^2 = k$ în numere întregi, algoritm expus în cartea lui Hua Loo Keng *Introduction to Number Theory*, Springer Verlag, Berlin Heidelberg New York, 1982 (capitolele X și XI).

Este suficient să luăm în considerare ecuația $x^2 - dy^2 = k$, unde x și y sunt numere naturale nenule prime între ele. Ecuațiile $x^2 = k$ și $-dy^2 = k$ se rezolvă imediat, iar dacă cumva $(x, y) = e > 1$ atunci e^2/k și putem considera ecuația $x_1^2 - dy_1^2 = \frac{k}{e^2}$.

Dacă $|k| < \sqrt{d}$ atunci aplicăm teorema 3 din paragraful III al anexei. În cazul în care $k \neq (-1)^n c_n$ $(\forall)\ n = \overline{1,s}$ atunci ecuația nu are soluții în numere întregi nenule prime între ele, iar dacă $k = (-1)^n c_n$ pentru un anume n ($n \in \{1, 2,...,s\}$) atunci $x = P_{n-1}$ și $y = Q_{n-1}$ reprezintă o soluție pentru ecuația $x^2 - dy^2 = k$ toate celelalte obținându-se în modul binecunoscut (adică

$$x + \sqrt{d}\,y = (\pm P_{n-1} \pm \sqrt{d}\ Q_{n-1})\cdot \varepsilon^l,$$

unde $l \in \mathbf{Z}$ și ε este unitatea fundamentală a ecuației Pell; aici s-au indicat toate soluțiile întregi). Notațiile folosite aici sunt cele din paragraful II al anexei (numerele c_n se calculează folosind formulele (3) din paragraful citat; s este lungimea perioadei fracției continue care-l reprezintă pe $\sqrt{d}$. Am ținut cont tăcit de faptul că $c_{n+s} = c_n$, $(\forall)\, n \in \mathbf{N}^*$, lucru ce rezultă imediat din demonstrația propoziției 3 din paragraful II al anexei precum și din formulele (3) din același loc).

Dacă $|k| > \sqrt{d}$ (nu poate avea loc egalitatea $|k| = \sqrt{d}$ deoarece $\sqrt{d}$ este număr irațional) atunci scriem $k = \delta \cdot k_0$, unde δ este +1 sau –1, iar $k_0 \in \mathbf{N}^*$ (evident $k_0 > \sqrt{d}$). Deoarece x și y sunt prime între ele există $x_1, y_1 \in \mathbf{Z}$ astfel încât

(5) $xy_1 - yx_1 = \delta.$

Înmulțind ecuația $x^2 - dy^2 = k$ cu $x_1^2 - dy_1^2$ obținem că

$$(x^2 - dy^2)(x_1^2 - dy_1^2) = (xx_1 - dyy_1)^2 - d(xy_1 - x_1y)^2 =$$
$$= (xx_1 - dyy_1)^2 - d = k(x_1^2 - dy_1^2) = \delta k_0(x_1^2 - dy_1^2).$$

Deci are loc egalitatea:

(6) $(xx_1 - dyy_1)^2 - d = \delta k_0(x_1^2 - dy_1^2).$

Dacă x_0, y_0 este o soluție a ecuației (5) atunci soluția generală se scrie sub forma

$$x_1 = x_0 + tx,\ y_1 = y_0 + ty,$$

t fiind un număr întreg arbitrar.

Avem că $xx_1 - dyy_1 = xx_0 - dyy_0 + t(x^2 - dy^2) = xx_0 - dyy_0 + t\delta k_0$. Vom alege numărul întreg t astfel încât să fie îndeplinită inegalitatea

(7) $|xx_1 - dyy_1| \le \dfrac{k_0}{2},$

Notând cu l numărul natural $|xx_1 - dyy_1|$ obținem că

(8) $x_1^2 - dy_1^2 = \dfrac{l^2 - d}{\delta k_0} = \eta h,$

unde $\eta = +1$ sau –1, iar $h \in \mathbf{N}^*$ (pentru deducerea egalității (8) am folosit formula (6)).

Din formula (8) rezultă că

$$h \le \frac{\max\{d, l^2\}}{k_0} < \frac{\max\left\{k_0^2, \dfrac{k_0^2}{4}\right\}}{k_0} = \frac{k_0^2}{k_0} = k_0$$

(am folosit în inegalitățile de mai sus faptul că $\sqrt{d} < k_0$ precum și evaluarea (7) : $l \le \dfrac{k_0}{2}$).

Deci h este un număr natural nenul mai mic strict decât k_0. Dacă $h < \sqrt{d}$ atunci se aplică din nou teorema 3 din paragraful III al anexei și obținem x_1 și y_1 astfel încât $x_1^2 - dy_1^2 = \eta h$.

Din egalitățile $xy_1 - yx_1 = \delta$ și $xx_1 - dyy_1 = \pm l$ obținem formulele:

$$(9) \qquad x = \frac{-\delta d y_1 \pm l x_1}{\eta h}, \quad y = \frac{-\delta x_1 \pm y_1 l}{\eta h}.$$

x și y se obțin deci din egalitatea

$$\eta h\left(x + \sqrt{d}\,y\right) = \left(x_1 + y_1\sqrt{d}\right)\left(-\delta\sqrt{d} \pm l\right).$$

Trecând la norme în această din urmă egalitate obținem că

$$h^2\left(x^2 - dy^2\right) = \left(x_1^2 - dy_1^2\right)\left(l^2 - d\right) = \eta h \cdot \eta h \cdot \delta k_0 = h^2 \delta k_0$$

și deci

$$x^2 - dy^2 = \delta k_0 = k.$$

Deci dacă x și y din formulele (9) sunt numere întregi, ele vor furniza o soluție pentru ecuația $x^2 - dy^2 = k$.

Dacă $h > \sqrt{d}$ atunci aplicăm din nou procedeul de mai sus.

Din considerațiile precedente rezultă următorul algoritm: aflăm întâi toate soluțiile congruenței:

$$l^2 \equiv d \left(\mathrm{mod}\, k_0\right), \text{ unde } l \in \mathrm{N},\ 0 \le l \le \frac{k_0}{2}.$$

Notăm cu $l_1, l_2, \ldots, l_r$ soluțiile congruenței de mai sus care satisfac inegalitățile $0 \le l \le \frac{k_0}{2}$. Notăm de asemenea $\frac{l_i^2 - d}{\delta k_0} = \eta_i h_i$ $(\forall)\, i = \overline{1,r}$, unde η_i este egal cu +1 sau –1, iar $h_i \in \mathbf{N}^*$.

Dacă $k_0 < \sqrt{d}$ atunci se aplică propoziția 3 din paragraful III al anexei. Dacă $k_0 > \sqrt{d}$ atunci se consideră ecuațiile: $x_1^2 - dy_1^2 = \eta_i h_i$ pentru $i = \overline{1,r}$. Folosind observațiile precedente avem că $0 < h_i < k_0$ $(\forall)\, i = \overline{1,r}$.

Pentru un i fixat cuprins între 1 și r avem două posibilități: dacă $h_i < \sqrt{d}$ atunci se aplică propoziția 3 din paragraful III al anexei pentru a stabili forma generală a soluțiilor ecuației $x_i^2 - dy_i^2 = \eta_i h_i$. Atunci

$$x = \frac{-\delta d y_i \pm l_i x_i}{\eta_i h_i},$$

$$y = \frac{-\delta x_i \pm l_i y_i}{\eta_i h_i}$$

și în ipoteza că x și y sunt numere întregi atunci obținem soluții pentru ecuația $x^2 - dy^2 = k$.

Dacă $h_i > \sqrt{d}$ se repetă procedeul anterior (unde δ se înlocuiește cu η_i și k_0 cu h). Întrucât $0 < h_i < k_0$, după un număr finit de operații vom obține toate soluțiile ecuației $x^2 - dy^2 = k$. Sigur că discuția de mai sus se face pentru toate numerele i cuprinse între 1 și r.

Motivul pentru care am expus cei doi algoritmi este acela că niciunul din ei nu e superior celuilalt, ei completându-se reciproc, pentru k sau d mari fiind preferabil primul algoritm, iar pentru k mic (de exemplu $|k| < \sqrt{d}$), al doilea comportă calcule mai puține.

ANEXĂ

I. **Propoziția 1**: $N(\mu_1 \cdot \mu_2) = N(\mu_1)\, N(\mu_2)$, $(\forall)\ \mu_1, \mu_2 \in R$.

Demonstrație: Dacă $\mu_1 = m_1 + n_1\sqrt{d}$, $\mu_2 = m_2 + n_2\sqrt{d}$ (unde m_1, n_1, m_2 și n_2 sunt numere întregi) atunci $\mu_1\mu_2 = m_1m_2 + dn_1n_2 + (m_1n_2 + n_1m_2)\sqrt{d}$ și $N(\mu_1\ \mu_2) = (m_1m_2 + dn_1n_2)^2 - d(m_1n_2 + n_1m_2)^2 = m_1^2m_2^2 + d^2n_1^2n_2^2 - dm_1^2n_2^2 - dn_1^2m_2^2 = m_1^2(m_2^2 - dn_2^2) - dn_1^2(m_2^2 - dn_2^2) = (m_1^2 - dn_1^2)(m_2^2 - dn_2^2) = N(\mu_1)N(\mu_2)$.

Propoziția 2: *Fie* $\varepsilon \in R$. ε *este unitate a inelului* R *dacă și numai dacă* $N(\varepsilon) = \pm 1$.

Soluție: Dacă ε este unitate a inelului R atunci există $\varepsilon_1 \in R$ astfel încât $\varepsilon \cdot \varepsilon_1 = 1$. Ținând cont de propoziția 1 deducem că $N(\varepsilon) \cdot N(\varepsilon_1) = N(1) = 1^2 - d \cdot 0^2 = 1$. Cum $N(\varepsilon)$ și $N(\varepsilon_1)$ sunt numere întregi deducem că $N(\varepsilon) = \pm 1$. Reciproc să presupunem că $N(\varepsilon) = \pm 1$. Cum $N(\mu) = \mu \cdot \overline{\mu}$ $(\forall)\ \mu \in R$ deducem că $\varepsilon \cdot \overline{\varepsilon} = \pm 1$. Dacă $N(\varepsilon) = 1$ rezultă că $\varepsilon \cdot \overline{\varepsilon} = 1$, iar dacă $N(\varepsilon) = -1$ deducem că $\varepsilon \cdot (-\overline{\varepsilon}) = 1$. În ambele situații am obținut că ε este o unitate a inelului R.

Propoziția 3: *Oricare ar fi* $a \in \mathbf{Z}^*$, *cardinalul mulțimii*

$$A = \{\alpha \in R \mid N(\alpha) = a \text{ și } \alpha \not\equiv \beta\ (\forall)\ \alpha, \beta \in A\}_{\alpha \neq \beta}$$

este finit, mai mic sau egal cu a^2.

Soluție: Dacă $a = 0$ cardinalul mulțimii A este egal cu 1. Presupunem în cele ce urmează că $a \in \mathbf{Z}^*$. Fie $\alpha, \beta \in A$ astfel încât $\alpha \neq \beta$ și $\alpha \equiv \beta \pmod{a}$ (aceasta înseamnă că există $\gamma \in R$ astfel încât $\alpha - \beta = a \cdot \gamma$). Avem deci egalitatea

$$\alpha - \beta = a\,\gamma = N(\alpha)\gamma = N(\beta)\,\gamma$$

(deoarece $a = N(\alpha) = N(\beta)$ conform definiției mulțimii A). Gândind inelul R ca fiind inclus în corpul

$$Q(\sqrt{d}) = \{r + s\sqrt{d} \mid r, s \in Q\}$$

și ținând cont că $\alpha, \beta \neq 0$ ($N(\alpha) = N(\beta) = a \neq 0$) putem efectua următoarele calcule $\frac{\alpha}{\beta} = \frac{\beta + a\gamma}{\beta} = 1 + \frac{N(\beta)\cdot\gamma}{\beta} = 1 + \frac{\beta\cdot\overline{\beta}\cdot\gamma}{\beta} = 1 + \overline{\beta}\cdot\gamma$ și

$$\frac{\beta}{\alpha} = \frac{\alpha - a\gamma}{\alpha} = 1 - \frac{N(\alpha)\cdot\gamma}{\alpha} = 1 - \overline{\alpha}\cdot\gamma.$$

Semnificația acestor calcule este aceea că $\frac{\alpha}{\beta}$ și $\frac{\beta}{\alpha}$ sunt elemente ale mulțimii R ceea ce înseamnă că $\alpha \sim \beta$. Acest lucru este imposibil conform definiției mulțimii A. Concluzia este că

$$(\forall)\ \alpha, \beta \in A,\ \alpha \neq \beta$$

atunci

$$\alpha \equiv \beta \pmod{a}.$$

Pe de altă parte se poate constata foarte ușor că $(\forall)\ b \in R$ există

$$m, n \in \mathbf{N} \text{ și } 0 \leq m < |a|,\ 0 \leq n < |a|$$

astfel încât $b \equiv m + n\sqrt{d} \pmod{a}$. Considerațiile anterioare permit concluzia că aplicația

$$\alpha \to \{m, n\}\ [m, n \in \mathbf{N},\ 0 \leq m, n < |a|;\ \alpha \equiv m + n\sqrt{d} \pmod{a}]$$

de la mulțimea A la mulțimea produs

$$\{0, 1, 2, \ldots, |a| - 1\} \times \{0, 1, 2, \ldots, |a| - 1\}$$

este injectivă. Aceasta înseamnă că A este o mulțime finită și, în plus, cardinalul mulțimii A este mai mic sau egal cu a^2.

Propoziția 4: $\overline{\mu_1 \cdot \mu_2} = \overline{\mu}_1 \cdot \overline{\mu}_2$, $(\forall)\ \mu_1, \mu_2 \in R$.

Soluție: Dacă $\mu_1 = m_1 + n_1\sqrt{d}$ și $\mu_2 = m_2 + n_2\sqrt{d}$ $(m_1, m_2, n_1, n_2 \in \mathbf{Z})$ atunci

$$\overline{\mu_1 \cdot \mu_2} = \overline{m_1 m_2 + d n_1 n_2 + \sqrt{d}\left(m_1 n_2 + n_1 m_2\right)} =$$

$$= m_1 m_2 + d n_1 n_2 - \sqrt{d}\ (m_1 n_2 + n_1 m_2)$$

și

$$\overline{\mu}_1 \cdot \overline{\mu}_2 = (m_1 - n_1\sqrt{d})(m_2 - n_2\sqrt{d}) =$$

$$= m_1 m_2 + d n_1 n_2 - \sqrt{d}\ (m_1 n_2 + n_1 m_2) = \overline{\mu_1 \mu_2},$$

ceea ce demonstrează enunțul propoziției 4. Propoziția 4 produce o altă demonstrație pentru propoziția 1

$$N(\mu_1 \mu_2) = (\mu_1 \mu_2) \cdot (\overline{\mu_1 \mu_2}) = (\mu_1 \cdot \overline{\mu}_1) \cdot (\mu_2 \cdot \overline{\mu}_2) = N(\mu_1)\, N(\mu_2).$$

II. Vom folosi în continuare notațiile ce se utilizează în general atunci când e vorba de fracții continue; anume dacă $a_0 \in \mathbf{R}$, $a_1, a_2, ..., a_n \in \mathbf{R}_+^*$ atunci se notează cu $a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_n}$ fracția $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$

Propoziția 1: *Dacă notăm cu R_n fracția $a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + ... + \frac{1|}{|a_n}$ atunci R_n este funcție rațională de a_0, a_1, ... a_n și se poate scrie sub forma $\frac{P_n}{Q_n}$, P_n și Q_n fiind polinoame în variabilele a_0, a_1, ... a_n care satisfac în plus următoarele relații:*

$P_0 = a_0$; $Q_0 = 1$

$P_1 = a_0 a_1 + 1$; $Q_1 = a_1$

$P_k = P_{k-1} \cdot a_k + P_{k-2}$; $Q_k = Q_{k-1} \cdot a_k + Q_{k-2}$, $(\forall)\, k \geq 2$, $k \in \mathbf{N}$.

Demonstrație: Faptul că R_n este funcție rațională de variabilele $a_0, a_1, ... a_n$ este evident. A doua parte a enunțului se demonstrează prin inducție după k. Pentru $k = 0$ și $k = 1$ enunțul este clar. Pentru $k = 2$ avem că

$$R_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} =$$

$$= \frac{(a_0 a_1 + 1) a_2 + a_0}{a_1 \cdot a_2 + 1} = \frac{P_1 \cdot a_2 + P_0}{Q_1 \cdot a_2 + Q_0};$$

deci

$$P_2 = P_1 \cdot a_2 + P_0 \text{ și } Q_2 = Q_1 \cdot a_2 + Q_0.$$

Presupunem acum enunțul adevărat pentru un $k \in \mathbf{N}$, $k \geq 2$ și vom demonstra afirmația din enunț pentru $k + 1$. Deoarece $a_k + \frac{1}{a_{k+1}} > 0$ (deoarece $a_k, a_{k+1} \in \mathbf{R}_+^*$) putem calcula R_{k+1} folosind ipoteza de inducție pentru numerele $a_0, a_1, ... a_{k-1}$ și $a_k + \frac{1}{a_{k+1}}$. Deci

$$R_{k+1}=\frac{P_{k-1}\left(a_k+\frac{1}{a_{k+1}}\right)+P_{k-2}}{Q_{k-1}\left(a_k+\frac{1}{a_{k+1}}\right)+Q_{k-2}}=\frac{P_k+\frac{P_{k-1}}{a_{k+1}}}{Q_k+\frac{Q_{k-1}}{a_{k+1}}}=\frac{P_k\cdot a_{k+1}+P_{k-1}}{Q_k\cdot a_{k+1}+Q_{k-1}}=\frac{P_{k+1}}{Q_{k+1}}$$

(în calculele precedente am ținut cont de ipoteza de inducție care afirmă că $P_k = P_{k-1} \cdot a_k + P_{k-2}$ și $Q_k = Q_{k-1} \cdot a_k + Q_{k-2}$), ceea ce înseamnă că enunțul este adevărat pentru $(\forall)\, k \in \mathbf{N}$.

Propoziția 2: *Folosind notațiile precedente*: $P_{k-1} \cdot Q_k - Q_{k-1}P_k = (-1)^k$ $(\forall)\, k \in \mathbf{N}^*$.

Demonstrație: Procedăm din nou la o inducție după k. Pentru $k = 1$ avem că

$$P_0Q_1 - Q_0P_1 = a_0 \cdot a_1 - 1 \cdot (a_0a_1 + 1) = -1 = (-1)^1,$$

ceea ce este conform enunțului. Presupunem acum enunțul adevărat pentru un $k \in \mathbf{N}^*$. Pentru a calcula $P_k \cdot Q_{k+1} - Q_kP_{k+1}$ ținem cont de propoziția 1, care afirmă că

$$Q_{k+1} = Q_k \cdot a_{k+1} + + Q_{k-1}$$

și

$$P_{k+1} = P_k \cdot a_{k+1} + P_{k-1}$$

precum și de ipoteza de inducție (care ne asigură că $P_{k-1}\, Q_k - Q_{k-1}\, P_k = (-1)^k$). Deci

$$P_k \cdot Q_{k+1} - Q_kP_{k+1} = P_k \cdot (Q_k \cdot a_{k+1} + Q_{k-1}) - Q_k\,(P_k \cdot a_{k+1} + P_{k-1}) =$$
$$= P_k \cdot Q_{k-1} - Q_k \cdot P_{k-1} = -(-1)^k = (-1)^{k+1}$$

ceea ce arată că enunțul propoziției 2 este adevărat pentru $k + 1$ și deci raționamentul prin inducție este terminat.

Propoziția 3: *Dacă d este un număr natural astfel încât $\sqrt{d} \notin \mathbf{N}$ atunci reprezentarea lui $\sqrt{d}$ ca fracție continuă simplă* $\sqrt{d} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \frac{1|}{|a_3} + \ldots$

posedă următoarele calități:

i) *există* $s \in \mathbf{N}^*$, $s < 2d$ *astfel încât* $a_n = a_{n+s}$, $(\forall)\, n \in \mathbf{N}^*$;

ii) $a_s = 2a_0 = 2\left[\sqrt{d}\right]$

iii) *secvența de numere naturale* $a_1, a_2, \ldots, a_{s-1}$ *este simetrică* (*adică* $a_1 = a_{s-1}$, $a_2 = a_{s-2}$ *etc.*).

Demonstrație: Deoarece numerele a_n sunt naturale, nenule atunci:

(1) $a_0 = \left[\sqrt{d}\right]$, $\sqrt{d} = a_0 + \dfrac{1}{x_1}$

Aici $x_1 > 1$ deoarece $0 < \sqrt{d} - a_0 < 1$; avem $0 < \sqrt{d} - a_0$ pentru că $\sqrt{d} \notin \mathbf{N}$. Notând $b_1 = a_0$ și $c_1 = d - a_0^2$ atunci $x_1 = \dfrac{1}{\sqrt{d} - a_0} = \dfrac{\sqrt{d} + a_0}{d - a_0^2} = \dfrac{\sqrt{d} + b_1}{c_1}$

(avem că b_1, $c_1 \in \mathbf{N}^*$; deoarece $a_0 < \sqrt{d}$ rezultă că $a_0^2 - d < 0$, deci $c_1 \in \mathbf{N}^*$). Există deci următoarea relație:

(2) $d - b_1^2 = c_1$.

De asemenea avem că $a_1 = [x_1]$ și $x_1 = a_1 + \dfrac{1}{x_2}$ ($x_2 > 1$; faptul că $x_2 \geq 1$ este evident. Dacă cumva $x_2 = 1$ ar rezulta că $\sqrt{d} \in \mathbf{Q}$, ceea ce evident nu se poate, conform presupunerii că $\sqrt{d} \notin \mathbf{N}$. De asemenea, nu se poate ca $x_1 = a_1$, din același motiv ca mai sus). Notând $b_2 = a_1c_1 - b_1$, $c_2 = 1 - a_1^2c_1 + 2\,a_1b_1$ avem că

$$x_2 = \frac{1}{x_1 - a_1} = \frac{1}{\dfrac{\sqrt{d} + b_1}{c_1} - a_1} = \frac{c_1}{\sqrt{d} + b_1 - a_1c_1} = \frac{c_1\left(\sqrt{d} + a_1c_1 - b_1\right)}{d - \left(a_1c_1 - b_1\right)^2} =$$

$$= \frac{c_1\left(\sqrt{d} + b_2\right)}{d - b_1^2 + 2a_1b_1c_1 - a_1^2c_1^2} = \frac{c_1\left(\sqrt{d} + b_2\right)}{c_1 + 2a_1b_1c_1 - a_1^2c_1^2} = \frac{\sqrt{d} + b_2}{1 + 2a_1b_1 - a_1^2c_1} = \frac{\sqrt{d} + b_2}{c_2}.$$

Definim numerele b_n, $c_n \in \mathbf{Z}$ prin următoarele formule:

(3) $b_{n+1} = a_nc_n - b_n$, $c_{n+1} = c_{n-1} - a_n^2 \cdot c_n + 2\,a_nb_n$, $(\forall)\, n > 1$.

Arătăm prin inducție că are loc relația:

(4) $d - b_n^2 = c_{n-1} \cdot c_n$, $(\forall)\, n \in \mathbf{N}$, $n \geq 2$.

Realizăm întâi verificarea pentru $n = 2$: $d - b_2^2 = d - (a_1c_1 - b_1)^2 =$

$= d - b_1^2 + 2\,a_1b_1c_1 - a_1^2c_1^2 = c_1 + 2a_1b_1c_1 - a_1^2c_1^2 = c_1\,(1 + 2a_1b_1 - a_1^2c_1) = c_1c_2$

[am folosit mai sus relația (2) care spune că $d - b_1^2 = c_1$]. Presupunem că $d - b_n^2 = c_{n-1} \cdot c_n$ pentru un anume $n \in \mathbf{N}$, $n \geq 2$ și vom arăta că are loc formula (4) și pentru $(n + 1)$. Într-adevăr:

$$d - b_{n+1}^2 = d - (a_nc_n - b_n)^2 = d - b_n^2 + + 2a_nc_nb_n - a_n^2c_n^2 =$$

$$= c_{n-1} \cdot c_n + 2\,a_n\,c_nb_n - a_n^2c_n^2 = c_n\,(c_{n-1} + 2\,a_nb_n - a_n^2 \cdot c_n) = c_n\,c_{n+1}$$

(am folosit în egalitățile de mai sus formulele (3) precum și ipoteza de inducție). Valabilitatea formulei (4) este astfel demonstrată.

Pentru orice $n \in \mathbf{N}^*$ avem că $x_n = a_n + \frac{1}{x_{n+1}}$, unde $a_n = [x_n]$ și $x_{n+1} > 1$.

Deci

$$\sqrt{d} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_n + \frac{1}{x_{n+1}}} \Bigg).$$

Arătăm că:

(5) $x_n = \frac{\sqrt{d} + b_n}{c_n}$ $(\forall)\, n \in \mathbf{N}^*$.

Am arătat mai sus că egalitatea (5) are loc pentru $n = 1$ și $n = 2$. Presupunem că ea este adevărată pentru un anume $n \in \mathbf{N}^*$ și vom demonstra că formula (5) are loc și pentru $(n + 1)$.

Într-adevăr

$$x_{n+1} = \frac{1}{x_n - a_n} = \frac{1}{\frac{\sqrt{d} + b_n}{c_n} - a_n} = \frac{c_n}{\sqrt{d} + b_n - a_n c_n} =$$

$$= \frac{c_n\left(\sqrt{d} - b_n + a_n c_n\right)}{d - \left(b_n - a_n c_n\right)^2} = \frac{c_n\left(\sqrt{d} + b_{n+1}\right)}{d - b_{n+1}^2} = \frac{c_n\left(\sqrt{d} + b_{n+1}\right)}{c_n \cdot c_{n+1}} = \frac{\sqrt{d} + b_{n+1}}{c_{n+1}}$$

(am folosit mai sus formulele (3) și (4) precum și ipoteza de inducție. Dacă cumva $c_n = 0$ pentru un anume $n \in \mathbf{N}^*$ atunci egalitatea (4) ne asigură că $d = b_n^2$; deci $\sqrt{d} = |b_n| \in \mathbf{N}$, ceea ce nu se poate. Aceasta înseamnă că $c_n \neq 0$ $(\forall)\, n \in \mathbf{N}^*$. Deci pot fi făcute toate împărțirile anterioare). Egalitatea (5) a fost astfel demonstrată prin inducție. Deoarece $0 < \sqrt{d} - a_0 < 1$ și $c_1 \in \mathbf{N}^*$, $b_1 = a_0$, deducem că

$$0 < \frac{\sqrt{d} - b_1}{c_1} \leq \sqrt{d} - b_1 < 1.$$

De asemenea avem că

$$\frac{\sqrt{d} + b_1}{c_1} = x_1 > 1.$$

Vom demonstra prin inducție că au loc următoarele inegalități:

(6) $0 < \dfrac{\sqrt{d} - b_n}{c_n} < 1 < \dfrac{\sqrt{d} + b_n}{c_n}$ $(\forall)\, n \in \mathbf{N}^*$.

Pentru $n = 1$ inegalitatea (6) a fost probată mai sus. Presupunem că inegalitatea (6) are loc pentru un anume n și o vom demonstra pentru $(n + 1)$. Deoarece

$$x_{n+1} > 1 \text{ și } x_{n+1} = \frac{\sqrt{d} + b_{n+1}}{c_{n+1}}$$

se deduce că

$$\frac{\sqrt{d} + b_{n+1}}{c_{n+1}} > 1.$$

Calculăm expresia

$$\frac{\sqrt{d} - b_{n+1}}{c_{n+1}} = \frac{d - b_{n+1}^2}{c_{n+1}\left(\sqrt{d} + b_{n+1}\right)} = \frac{c_n \cdot c_{n+1}}{c_{n+1}\left(\sqrt{d} + b_{n+1}\right)} = \frac{c_n}{\sqrt{d} + b_{n+1}} =$$

$$= \frac{c_n}{\sqrt{d} + a_n c_n - b_n} = \frac{1}{\dfrac{\sqrt{d} - b_n}{c_n} + a_n}$$

(în acest calcul s-a ținut cont de egalitățile (3) și (4)). Ținând cont că

$$\frac{\sqrt{d} - b_n}{c_n} > 0 \text{ și } a_n > 0$$

se deduce că

$$\frac{\sqrt{d} - b_{n+1}}{c_{n+1}} > 0.$$

Deoarece

$$a_n = [x_n] \geq 1 \text{ și } \frac{\sqrt{d} - b_n}{c_n} > 0$$

se obține că

$$\frac{\sqrt{d} - b_n}{c_n} + a_n > a_n \geq 1$$

și deci, conform calculului anterior,

$$\frac{\sqrt{d} - b_{n+1}}{c_{n+1}} < 1.$$

Inegalitatea (6) a fost demonstrată astfel prin inducție. Dacă cumva $c_n < 0$ pentru un $n \in \mathbf{N}^*$, atunci din (6) rezultă că $\sqrt{d} - b_n < 0$ și $\sqrt{d} + b_n < 0$. Aceste două inegalități conduc la concluzia absurdă că $2\sqrt{d} < 0$. Deci $c_n > 0$, $(\forall)\ n \in \mathbf{N}$ (faptul că $c_n \neq 0$ a fost observat ceva mai înainte). Din (6) și din faptul că $c_n > 0$ $(\forall)\ n \in \mathbf{N}^*$ deducem că

$$\sqrt{d} - b_n < c_n < \sqrt{d} + b_n.$$

Primul și ultimul termen al acestei inegalități furnizează inegalitatea

$$\sqrt{d} - b_n < \sqrt{d} + b_n,$$

adică $b_n > 0$ $(\forall)\ n \in \mathbf{N}^*$. Din faptul că $c_n > 0$ și din inegalitatea (6) mai rezultă și că $b_n < \sqrt{d}$ $(\forall)\ n \in \mathbf{N}^*$ și

$$c_n < \sqrt{d} + b_n < 2\sqrt{d}\ \ (\forall)\ n \in \mathbf{N}^*.$$

Aceasta ne conduce la observația că numărul de perechi (b_n, c_n) distincte este cel mult $\sqrt{d} \cdot 2\sqrt{d} = 2d$ (chiar mai mic strict decât $2d$; într-adevăr numărul de perechi posibile

$$(b_n, c_n) \text{ cu } b_n, c_n \in \mathbf{N},\ 0 < b_n < \sqrt{d},\ 0 < c_n < 2\sqrt{d}$$

este mai mic sau egal cu

$$[\sqrt{d}] \cdot [2\sqrt{d}] < \sqrt{d} \cdot 2\sqrt{d} = 2d.$$

Deoarece $\sqrt{d} \notin \mathbf{N}$ avem că $[\sqrt{d}] < \sqrt{d}$ ceea ce justifică afirmația de mai sus). Există deci $s,\ k \in \mathbf{N}^*,\ s < 2d,\ k < 2d$ astfel încât $b_{k+s} = b_k$ și $c_{k+s} = c_k$. De aici și din formula (5) se deduce că:

(7) $x_k = x_{k+s}$.

Din egalitatea (7) și din faptul că

$$x_{n+1} = \frac{1}{x_n - a_n} = \frac{1}{x_n - [x_n]}\ (\forall)\ n \in \mathbf{N}^*$$

se deduce că $x_{k+1} = x_{k+1+s}$. Continuând raționamentul în același mod se deduce de fapt că $x_n = x_{n+s}$ $(\forall)\ n \in \mathbf{N},\ n \geq k$. Deoarece $a_n = [x_n]$ rezultă și că $a_n = a_{n+s}$ $(\forall)\ n \in \mathbf{N},\ n \geq k$.

Dacă notăm $x'_n = \dfrac{\sqrt{d} - b_n}{c_n}$ atunci $x'_n = -\overline{x_n}$. Trecând la conjugare în relația

$$x_n = a_n + \frac{1}{x_{n+1}}$$

se deduce că

$$-x'_n = \overline{x_n} = \overline{a_n} + \frac{1}{\overline{x_{n+1}}} = a_n - \frac{1}{x'_{n+1}}.$$

Deci

$$\frac{1}{x'_{n+1}} = a_n + x'_n.$$

Aceasta împreună cu inegalitatea (6) (care afirmă că $0 < x'_n < 1$) conduc la egalitatea:

$$(8)\ a_n = \left[\frac{1}{x'_{n+1}}\right] (\forall)\ n \in \mathbf{N}^*.$$

Deoarece $x'_n = -\overline{x_n}$ $(\forall)\ n \in \mathbf{N}^*$, se deduce că $x'_k = x'_{k+s}$; aceasta împreună cu egalitatea (8) duc la concluzia că

$$a_{k-1} = \left[\frac{1}{x'_k}\right] = \left[\frac{1}{x'_{k+s}}\right] = a_{k-1+s},$$

dacă $k > 1$. Cum

$$x_{k-1} = a_{k-1} + \frac{1}{x_k},$$

$$x_{k-1+s} = a_{k-1+s} + \frac{1}{x_{k+s}},$$

$$a_{k-1} = a_{k-1+s},\ x_k = x_{k+s},$$

deducem că $x_{k-1} = x_{k-1+s}$ dacă $k > 1$. Repetând argumentul și ținând cont și de cele demonstrate mai sus rezultă că $x_n = x_{n+s}$, $(\forall)\ n \in \mathbf{N}^*$.

În particular rezultă și că

$$a_n = [x_n] = [x_{n+s}] = a_{n+s}\ (\forall)\ n \in \mathbf{N}^*,$$

$$x'_n = -\overline{x_n} = -\overline{x_{n+s}} = x'_{n+s}\ (\forall)\ n \in \mathbf{N}^*.$$

Deoarece

$$x_n = a_n + \frac{1}{x_{n+1}}\ (\forall)\ n \in \mathbf{N}^*,$$

avem urmă-toarele relații:

$$x_1 = a_1 + \frac{1}{x_2};$$

$$x_2 = a_2 + \frac{1}{x_3};$$

$$\ldots;$$

$$x_s = a_s + \frac{1}{x_{s+1}} = a_s + \frac{1}{x_1},$$

care conduc la următoarea formulă

$$x_1 = a_1 + \frac{1|}{|a_2} + \ldots \frac{1|}{|a_s} + \frac{1|}{|x_1}.$$

De asemenea, formula

$$-x'_n = a_n - \frac{1}{x'_{n+1}} \quad (\forall)\, n \in \mathbf{N}^*$$

implică egalitățile:

$$-x'_1 = a_1 - \frac{1}{x'_2};\ -x'_2 = a_2 - \frac{1}{x'_3};\ \ldots\ ;\ -x'_s = a_s - \frac{1}{x'_{s+1}} = a_s - \frac{1}{x'_1}.$$

Aceste formule se mai pot scrie și în maniera următoare:

$$\frac{1}{x'_2} = a_1 + \frac{1}{\left(\frac{1}{x'_1}\right)};\ \frac{1}{x'_3} = a_2 + \frac{1}{\left(\frac{1}{x'_2}\right)};\ldots;\ \frac{1}{x'_1} = a_s + \frac{1}{\left(\frac{1}{x'_s}\right)}.$$

Concluzionând, cele de mai sus permit scrierea următoarei egalități:

$$\frac{1}{x'_1} = a_s + \frac{1|}{|a_{s-1}} + \frac{1|}{|a_{s-2}} + \ldots + \frac{1|}{|a_1} + \frac{1|}{\left|\left(\frac{1}{x'_1}\right)\right.}.$$

Deoarece $\sqrt{d} = a_0 + \frac{1}{x_1}$ și $-\sqrt{d} = a_0 - \frac{1}{x'_1}$ (această din urmă egalitate se obține prin conjugarea egalității $\sqrt{d} = a_0 + \frac{1}{x_1}$) egalitățile anterioare conduc la următoarele formule pentru $\sqrt{d}$:

$$\sqrt{d} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_s} + \frac{1|}{|x_1}$$

$$\sqrt{d} = a_s - a_0 + \frac{1|}{|a_{s-1}} + \frac{1|}{|a_{s-2}} + \ldots + \frac{1|}{|a_1} + \frac{1|}{\left|\left(\frac{1}{x'_1}\right)\right.}.$$

Din aceste egalități se deduce întâi că

$$a_0 = \left[\sqrt{d}\right] = a_s - a_0,$$

adică

$$a_s = 2\, a_0 = 2\left[\sqrt{d}\right],$$

apoi că

$$a_1 = \left[\frac{1}{\sqrt{d} - a_0}\right] = a_{s-1},\ a_2 = a_{s-2}$$

și așa mai departe (în scrierile de mai sus $x_1 > 1$ și $\frac{1}{x_1'} > 1$). Cu aceasta cerințele propoziției 3 au fost demonstrate în totalitate.

Se utilizează în general notația $\sqrt{d} = \left(a_0; \overline{a_1, a_2, \ldots, a_s}\right)$ pentru a descrie modul în care $\sqrt{d}$ se scrie ca fracție continuă simplă.

III. **Definiție**: Dacă șirul de numere naturale d_0, d_1, d_2, ... ne furnizează reprezentarea numărului $x \in \mathbf{R}_+ \setminus \mathbf{Q}$ ca fracție continuă simplă atunci vom numi *redusă de ordin n a lui x* fracția

$$\frac{P_n}{Q_n} = d_0 + \frac{1|}{|d_1} + \frac{1|}{|d_2} + \ldots + \frac{1|}{|d_n}.$$

O fracție $\frac{a}{b} \in \mathbf{Q}_+$ se va numi *redusă a lui x* dacă există un număr natural *n* astfel încât $\frac{a}{b}$ să fie egal cu $\frac{P_n}{Q_n}$, $a = P_n$, $b = Q_n$.

Teorema 1 (Legendre) *Fie* $\alpha \in \mathbf{R}_+$ *și p, q două numere naturale nenule astfel încât* $\varepsilon\theta = q^2\alpha - pq$, ε *fiind* $+1$ *sau* -1, *iar* θ *un real care verifică inegalitățile* $0 < \theta < 1$ (*din cele de mai sus rezultă că* $q \neq 0$). *Dacă* $n \in \mathbf{N}^*$, $a_0 \in \mathbf{N}$, $a_1, \ldots a_{n-1} \in \mathbf{N}^*$ *satisfac condițiile* $(-1)^{n-1} = \varepsilon$,

$$\frac{p}{q} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_{n-1}}$$

atunci o condiție necesară și suficientă ca $\frac{p}{q}$ *să fie o redusă a lui* α *este aceea că*

$$\theta \leq \frac{Q_{n-1}}{Q_{n-1} + Q_{n-2}},$$

unde

$$a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_{n-2}} = \frac{P_{n-2}}{Q_{n-2}}$$

și

$$a_0 + \frac{1|}{|a_1} + \ldots + \frac{1|}{|a_{n-1}} = \frac{P_{n-1}}{Q_{n-1}} = \frac{p}{q}$$

(P_{n-2}, Q_{n-2}, P_{n-1}, Q_{n-1} *sunt numere naturale,* $Q_{-1} = 0$, $Q_{n-1} \cdot Q_{n-2} \neq 0$).

Demonstrație: Definim β prin egalitatea:

$$(1)\ \alpha = \frac{P_{n-1} \cdot \beta + P_{n-2}}{Q_{n-1} \cdot \beta + Q_{n-2}}.$$

Folosind egalitatea din enunț și faptul că $P_{n-1} = p$, $Q_{n-1} = q$ deducem că:

$$(2)\ \frac{\varepsilon\theta}{Q_{n-1}^2} = \alpha - \frac{P_{n-1}}{Q_{n-1}} = \frac{P_{n-1} \cdot \beta + P_{n-2}}{Q_{n-1} \cdot \beta + Q_{n-2}} - \frac{P_{n-1}}{Q_{n-1}} = \frac{P_{n-2}Q_{n-1} - P_{n-1}Q_{n-2}}{Q_{n-1}\left(Q_{n-1}\beta + Q_{n-2}\right)} =$$

$$= \frac{(-1)^{n-1}}{Q_{n-1}\left(Q_{n-1} \cdot \beta + Q_{n-2}\right)}$$

(pentru ultima egalitate am folosit propoziția 2 din paragraful (II) al anexei). Din cele de mai sus rezultă (ținând cont că $\varepsilon = (-1)^{n-1}$) că

$$\theta = \frac{Q_{n-1}}{Q_{n-1} \cdot \beta + Q_{n-2}}.$$

Din această ultimă egalitate obținem că

$$\beta = \frac{Q_{n-1} - \theta Q_{n-2}}{\theta Q_{n-1}}$$

și deci $\beta > 0$ (aceasta rezultă deoarece $Q_{n-1} \geq Q_{n-2}$, inegalitate care se deduce imediat din propoziția 1 a paragrafului II din această anexă precum și din faptul că $a_i \in \mathbf{N}^*$ $(\forall)$ $i \geq 1$ și $0 < \theta < 1$). Din propoziția 1 din paragraful II al anexei rezultă că

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_{n-1}} + \frac{1|}{|\beta}$$

(s-a ținut cont evident și de formula (1)). De aici deducem că $\frac{p}{q}$ este o redusă a

lui α dacă $\beta \geq 1$. În cazul în care $\beta < 1$ atunci

$$\left[a_{n-1} + \frac{1}{\beta}\right] > [a_{n-1}]$$

de unde deducem imediat că $\frac{p}{q}$ nu este o redusă a lui α. Avem că $\beta \geq 1$ dacă și numai dacă

$$\theta = \frac{Q_{n-1}}{Q_{n-1}\beta + Q_{n-2}} \leq \frac{Q_{n-1}}{Q_{n-1} + Q_{n-2}}.$$

Ținând cont de cele de mai sus rezultă că enunțul teoremei lui Legendre este demonstrat.

Teorema 2: *Fie p și q numere naturale nenule care satisfac inegalitatea $|p^2 - \alpha^2 q^2| < \alpha$ (α fiind un număr irațional pozitiv). Atunci $\frac{p}{q}$ este o redusă a lui α.*

Demonstrație: Ținând cont de inegalitatea din enunț avem că

$$\alpha^2 q^2 - p^2 = \varepsilon \cdot \delta \cdot \alpha,$$

unde ε este $+1$ sau -1 și $0 \leq \delta < 1$. Folosind notațiile din teorema precedentă avem că

$$\theta = \varepsilon\, q\, (\alpha\, q - p) = \frac{\varepsilon q\left(\alpha^2 q^2 - p^2\right)}{\alpha q + p} = \frac{\delta \alpha q}{\alpha q + p}.$$

Fie $d_0, d_1, \ldots d_{n-1}$ câturile succesive obținute prin aplicarea algoritmului lui Euclid pentru numerele p și q. Avem egalitatea

$$\frac{p}{q} = d_0 + \frac{1|}{|d_1} + \frac{1|}{|d_2} + \ldots + \frac{1|}{|d_{n-1}}.$$

Dacă $(-1)^{n-1} = \varepsilon$ atunci luăm $a_i = d_i\ (\forall)\ i = \overline{0, n-1}$. Dacă $(-1)^{n-1} = -\varepsilon$ și $d_{n-1} > 1$ atunci luăm

$$a_i = d_i\ (\forall)\ i = \overline{0, n-2},\ a_{n-1} = d_{n-1} - 1,\ a_n = 1$$

și atunci $(-1)^n = \varepsilon$. Dacă $(-1)^{n-1} = -\varepsilon$ și $d_{n-1} = 1$ atunci luăm

$$a_i = d_i\ (\forall)\ i = \overline{0, n-3},\ a_{n-2} = d_{n-2} + 1 \text{ și } (-1)^{n-2} = \varepsilon$$

(dacă cumva în ultima situație avem că $n = 1$ atunci luăm $a_0 = 0$ și $a_1 = 1$).

Din cele de mai sus rezultă că în orice situație ne-am afla putem găsi niște numere $a_0, a_1, \ldots a_{n-1}$ ($a_0 \in \mathbf{N}$, $a_i \in \mathbf{N}^*$ $(\forall)$ $i = \overline{1, n-1}$) astfel încât $(-1)^{n-1} = \varepsilon$ și

$$\frac{p}{q} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_{n-1}}.$$

Formula pentru θ se rescrie astfel:

$$\theta = \frac{\delta\alpha Q_{n-1}}{\alpha Q_{n-1} + P_{n-1}}.$$

Conform teoremei lui Legendre pentru a ne convinge că enunțul teoremei 2 este adevărat trebuie să arătăm că are loc inegalitatea:

$$\theta = \frac{\delta\alpha Q_{n-1}}{\alpha Q_{n-1} + P_{n-1}} \leq \frac{Q_{n-1}}{Q_{n-1} + Q_{n-2}}$$

sau că

$$\delta\,\alpha\,(Q_{n-1} + Q_{n-2}) \leq \alpha\,Q_{n-1} + P_{n-1}.$$

Deoarece $0 \leq \delta < 1$ este suficient să arătăm că $\alpha\,Q_{n-2} \leq P_{n-1}$ sau că

$$\alpha\,Q_{n-1} - P_{n-1} \leq \alpha\,(Q_{n-1} - Q_{n-2}).$$

Dar

$$\alpha\,Q_{n-1} - P_{n-1} = \frac{\alpha^2 Q_{n-1}^2 - P_{n-1}^2}{\alpha Q_{n-1} + P_{n-1}} = \frac{\varepsilon\delta\alpha}{\alpha Q_{n-1} + P_{n-1}}.$$

Dacă $n = 2$ atunci $\varepsilon = (-1)^{n-1} = -1$ și deci

$$\alpha\,Q_{n-1} - P_{n-1} \leq 0 \leq \alpha\,(Q_{n-1} - Q_{n-2})$$

(în demonstrarea ultimei inegalități ținem cont că

$$Q_{n-1} = Q_1 = a_1 \geq 1 = Q_0 = Q_{n-2}),$$

iar dacă $n > 2$ atunci

$$Q_{n-1} = Q_{n-2} \cdot a_{n-1} + Q_{n-3} \geq Q_{n-2} + 1$$

(egalitatea

$$Q_{n-1} = Q_{n-2} \cdot a_{n-1} + Q_{n-3}$$

rezultă din propoziția 1 a paragrafului II). În această din urmă situație avem că

$$Q_{n-1} - Q_{n-2} \geq 1 > \frac{1}{\alpha Q_{n-1} + P_{n-1}}$$

(deoarece $P_{n-1} = p \geq 1$ și $Q_{n-1} = q \geq 1$, $\alpha > 0$).

Din considerațiile anterioare deducem că

$$\alpha\,Q_{n-1} - P_{n-1} = \frac{\varepsilon\delta\alpha}{\alpha Q_{n-1} + P_{n-1}} \leq \alpha\,(Q_{n-1} - Q_{n-2})$$

în orice situație și deci teorema 2 este demonstrată.

Teorema 3: *Folosind notațiile din paragraful II al anexei avem că ecuația* $x^2 - dy^2 = (-1)^n c_n$ *are întotdeauna soluții în numere naturale, iar dacă k este un număr întreg astfel încât* $|k| < \sqrt{d}$ *și* $k \neq (-1)^n c_n$ $(\forall)$ $n \in \mathbf{N}^*$ *atunci ecuația* $x^2 - dy^2 = k$ *nu are soluții în numere naturale nenule și evident nici în numere întregi nenule.*

Demonstrație: Ținând cont că

$$\sqrt{d} = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \ldots + \frac{1|}{|a_{n-1}} + \frac{1|}{|x_n},$$

$$x_n = \frac{\sqrt{d} + b_n}{c_n}, \ (\forall)\ n \in \mathbf{N}^*$$

(formula (5) din paragraful II al anexei), propoziția 1 din paragraful II al anexei ne asigură că au loc următoarele egalități:

$$\sqrt{d} = \frac{P_{n-1}x_n + P_{n-2}}{Q_{n-1}x_n + Q_{n-2}} = \frac{P_{n-1}\dfrac{\sqrt{d}+b_n}{c_n} + P_{n-2}}{Q_{n-1}\dfrac{\sqrt{d}+b_n}{c_n} + Q_{n-2}} = \frac{P_{n-1}\left(\sqrt{d}+b_n\right) + c_n P_{n-2}}{Q_{n-1}\left(\sqrt{d}+b_n\right) + c_n Q_{n-2}}.$$

Din această ultimă egalitate obținem că

$$P_{n-1}(\sqrt{d} + b_n) + P_{n-2} \cdot c_n = dQ_{n-1} + \sqrt{d}\ (Q_{n-1}b_n + c_n Q_{n-2})$$

și folosind faptul că $\sqrt{d}$ este număr irațional obținem că:

(3) $P_{n-1} = Q_{n-1}\, b_n + c_n\, Q_{n-2}$

(4) $d\, Q_{n-1} = P_{n-1}\, b_n + c_n\, P_{n-2}$.

Dacă din egalitatea (3) înmulțită cu P_{n-1} se scade egalitatea (4) înmulțită cu Q_{n-1}, găsim că

$$P_{n-1}^{\ 2} - dQ_{n-1}^{\ 2} = c_n\,(P_{n-1}\,Q_{n-2} - P_{n-2}\,Q_{n-1}) = (-1)^n\, c_n$$

(pentru ultima egalitate s-a ținut cont de propoziția 2 din paragraful II al anexei).

Dacă $k \in \mathbf{Z}$, $|k| < \sqrt{d}$ și x, y sunt două numere naturale nenule astfel încât $x^2 - dy^2 = k$ atunci aplicăm teorema 2 pentru $p = x$, $q = y$ și $\alpha = \sqrt{d}$ și obținem că $\dfrac{x}{y}$ este o redusă a lui $\sqrt{d}$. Rezultă că există un $n \in \mathbf{N}^*$ astfel încât $x = P_{n-1}$, $y = Q_{n-1}$ și atunci urmând calculul de mai sus deducem că $k = (-1)^n\, c_n$.

În acest moment enunțul teoremei 3 este demonstrat.

TEOREMA ELEMENTULUI PRIM

Introducere

Inainte de anul 1800 Gauss și Legendre au conjecturat următorul enunț:

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1,$$

unde $\pi(x)$ reprezintă numărul de numere prime mai mici sau egale cu x pentru oricare ar fi $x \geq 1$. Acest rezultat este cunoscut sub numele de teorema elementului prim sau legea de repartiție a numerelor prime. Deși nu au putut să demonstreze enunțul, Cebîșev și Riemann au realizat pași importanți spre soluția problemei. Riemann a pus în evidență legătura dintre teorema elementului prim și celebra funcție ζ ce-i poartă numele (funcția ζ a lui Riemann se definește astfel:

$$\zeta(z) = \sum_{n\in\mathbf{N}^*} \frac{1}{n^z},$$

unde $z \in \mathbf{C}$ și partea reală a lui z este strict mai mare decât 1). Ideile lui Riemann au fost exploatate și lărgite de către J. Hadamard și Charles de la Vallée Poussin, care au reușit în anul 1896 (independent unul față de celălalt) să demonstreze teorema elementului prim. In anul 1949 P. Erdos și A. Selberg au dat demonstrații „elementare" pentru teorema elementului prim folosind o formulă a lui Selberg. În acest capitol vom prezenta o variantă simplificată a demonstrației lui Selberg (îmbunătățirile datorându-se lui Levinson și Wright) urmărind articolul lui N. Levinson *A motivated account of an elementary proof of the Prime Number Theorem*, din American Mathematical Monthly, 1969, vol. 76, pag. 225-245. Raționamentul demonstrației se bazează esențial pe identitatea amintită mai sus a lui Selberg (demonstrată în propoziția 2 din paragraful II al anexei). În principal scopul anexei este de a demonstra formula lui Selberg.

Prin ln se înțelege logaritmul natural (în baza e); notația $f = O(g)$, unde $f: [a, +\infty) \to \mathbf{R}$ și $g : [a, \infty) \to \mathbf{R}_+$, este cea clasică, semnificația ei fiind aceea că există $b \geq a$ și o constantă pozitivă M astfel încât

$$|f(x)| \leq M \cdot g(x) \ (\forall)\ x \geq b.$$

Sumele care apar în acest capitol trebuiesc considerate ca fiind indexate după $\mathbf{N}^*$, mai puțin cele în care se precizează în mod explicit altceva. Toate integralele care apar sunt integrale Riemann (eventual improprii); aproape în toate cazurile e foarte ușor de văzut că funcțiile în discuție sunt integrabile Riemann, iar atunci când lucrurile nu sunt clare, se dau justificări detaliate. Exceptând două momente în care se folosește teorema lui Fubini precum și o teoremă de trecere la limită sub integrală, restul poate fi înțeles de către un absolvent de liceu.

Demonstrația teoremei elementului prim

Dacă $x \in \mathbf{R}, x \geq 1$, vom nota cu $\pi(x)$ numărul de numere prime ce sunt mai mici sau egale cu x. Teorema elementului prim se enunță astfel:

Teoremă: $\lim\limits_{x \to +\infty} \dfrac{\pi(x)\ln x}{x} = 1$.

Funcția π este incomodă prin însăși modul ei de definire, de aceea este de preferat (în scopul demonstrării acestei teoreme) de a opera cu funcții legate de funcția π, dar mai „simple" (din punctul de vedere al calculelor și estimărilor ce se pot face). În timpul încercărilor de a demonstra teorema elementului prim s-a desprins ideea că unul dintre cele mai utile instrumente de investigație este funcția ψ a lui Cebîșev.

Definim întâi funcția lui Mangoldt $\Lambda : \mathbf{N}^* \to \mathbf{R}_+$ în modul următor: $\Lambda(n) = \ln p$, dacă $n = p^i$, unde p este un număr prim și i un număr natural nenul și $\Lambda(n) = 0$ în toate celelalte cazuri posibile. Funcția lui Cebîșev ψ este definită pe $[1, \infty)$ și are valori reale pozitive. Formula de definiție este următoarea:

$$\psi(x) = \sum_{j \leq x} \Lambda(j) \quad (\forall) x \geq 1.$$

Fie $x \geq 1$, p un număr prim și $i \in \mathbf{N}$ astfel încât $p^i \leq x < p^{i+1}$; atunci $i = \left[\dfrac{\ln x}{\ln p}\right]$.

Ținând cont de aceasta, funcția ψ se mai poate scrie și sub forma

$$\psi(x) = \sum_{\substack{p \leq x \\ p\text{-prim}}} \left[\frac{\ln x}{\ln p}\right] \cdot \ln p.$$

Vom încerca întâi să demonstrăm următoarea inegalitate:

$$(1) \quad \frac{\psi(x)}{x} \leq \frac{\pi(x)\ln x}{x} < \frac{1}{\ln x} + \frac{\psi(x)\ln x}{x \ln\left(\dfrac{x}{\ln^2 x}\right)} \quad (\forall)\ x > e.$$

Deoarece

$$\lim_{x \to +\infty} \frac{\ln x}{\ln\left(\dfrac{x}{\ln^2 x}\right)} = \lim_{x \to +\infty} \frac{\ln x}{\ln x - 2\ln(\ln x)} = \lim_{y \to +\infty} \frac{y}{y - 2\ln y} = \lim_{y \to +\infty} \frac{1}{1 - 2\dfrac{\ln y}{y}} = 1$$

și $\lim_{x\to+\infty}\frac{1}{\ln x}=0$, este ușor de văzut importanța inegalității (1); dacă putem arăta cumva că $\lim_{x\to+\infty}\frac{\psi(x)}{x}=1$ atunci inegalitatea de mai sus ne asigură că $\lim_{x\to+\infty}\frac{\pi(x)\ln x}{x}=1$, adică tocmai enunțul teoremei elementului prim. Cebîșev a arătat în 1850 că există $x_0\in\mathbf{R}$, $x_0\geq 1$, astfel încât oricare ar fi $x\geq x_0$ are loc inegalitatea $\frac{\psi(x)}{x}<\frac{3}{2}$ (demonstrația acestui fapt este dată în propoziția 2 din paragraful I al anexei).

Deoarece $[y]\leq y\ (\forall)\ y\in\mathbf{R}$, rezultă că

$$\psi(x)=\sum_{\substack{p\leq x\\ p\text{-}prim}}\left[\frac{\ln x}{\ln p}\right]\ln p\leq\sum_{\substack{p\leq x\\ p\text{-}\mathrm{prim}}}\frac{\ln x}{\ln p}\cdot\ln p=\ln x\sum_{\substack{p\leq x\\ p\text{-}\mathrm{prim}}}1=\pi(x)\ln x.$$

Deci prima inegalitate din (1) este astfel demonstrată. Pentru a demonstra cea de a doua inegalitate din (1) să observăm că dacă x, y sunt două numere reale astfel încât $1<y<x$, atunci

$$\pi(x)-\pi(y)=\sum_{\substack{y<p\leq x\\ p\text{-prim}}}1\leq\sum_{\substack{y<p\leq x\\ p\text{-prim}}}\frac{\ln p}{\ln y}\leq\frac{1}{\ln y}\sum_{\substack{p\text{-prim}\\ p\leq x}}\ln p\leq\frac{1}{\ln y}\sum_{j\leq x}\Lambda(j)=\frac{\psi(x)}{\ln y}.$$

Deoarece $\pi(y)<y$, obținem inegalitatea:

$$\pi(x)<y+\frac{\psi(x)}{\ln y},$$

valabilă pentru $(\forall)\ x, y\in\mathbf{R}$ astfel încât $1<y<x$.

Să considerăm funcția f: $[e,+\infty)\to\mathbf{R}$ definită prin formula $f(x)=\frac{x}{\ln^2 x}$.

Deoarece

$$f'(x)=\frac{\ln^2 x-x\cdot 2\ln x\cdot\frac{1}{x}}{\ln^4 x}=\frac{\ln x-2}{\ln^3 x},$$

deducem că f este descrescătoare pe intervalul $[e, e^2]$ și crescătoare pe intervalul $[e^2, +\infty)$. Deci

$$f(x)\geq f(e^2)=\frac{e^2}{\ln^2\left(e^2\right)}=\frac{e^2}{4}>1,\ (\forall)\ x\geq e$$

(deoarece e > 2). Cum

$$\frac{x}{\ln^2 x} < x,\ (\forall)x > \mathrm{e},$$

deducem că în inegalitatea

$$\pi(x) < y + \frac{\psi(x)}{\ln y}$$

putem înlocui pe y cu $\frac{x}{\ln^2 x}$; vom obține deci că

$$\pi(x) < \frac{x}{\ln^2 x} + \frac{\psi(x)}{\ln\left(\frac{x}{\ln^2 x}\right)},\ (\forall)x > \mathrm{e}.$$

Înmulțind ultima inegalitate cu $\frac{\ln x}{x}$ obținem cea de a doua inegalitate din (1).

Dacă n este un număr natural nenul care se scrie sub forma:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

($p_1, p_2, \dots p_r$ sunt numere prime distincte, iar $\alpha_i \in \mathbf{N}^*$ $(\forall)\ i = \overline{1,r}$) atunci

$$\sum_{j|n} \Lambda(j) = \sum_{i=1}^{r} \alpha_i \ln p_i = \sum_{i=1}^{r} \ln p_i^{\alpha_i} = \ln \prod_{i=1}^{r} p_i^{\alpha_i} = \ln n.$$

Aceasta se mai poate scrie și sub forma

$$\ln n = \sum_{i \cdot j = n} \Lambda(j).$$

Dacă notăm cu T funcția $T : [1, \infty) \to \mathbf{R}$, definită prin formula $T(x) = \sum_{n \le x} \ln n$, $(\forall)x \ge 1$, atunci

$$T(x) = x \ln x - x + O(\ln x)$$

(acest lucru este demonstrat pe parcursul soluției propoziției 2 din paragraful I al anexei; este așa numita formă slabă a formulei lui Stirling).

Folosind faptul că

$$\ln n = \sum_{i \cdot j = n} \Lambda(j),$$

deducem următoarea legătură între funcțiile T și ψ:

$$T(x) = \sum_{n \le x} \ln n = \sum_{i \cdot j \le x} \Lambda(j) = \sum_{i \le x} \left(\sum_{j \le \frac{x}{i}} \Lambda(j) \right) = \sum_{i \le x} \psi\left(\frac{x}{i}\right),\ (\forall)x \ge 1.$$

Ca o consecință imediată a propoziției 1 din paragraful II al anexei rezultă următoarea formulă

$$\psi(x) = \sum_{k \le x} \mu(k)\, T\left(\frac{x}{k}\right) (\forall)\, x \ge 1,$$

unde μ este funcția lui Möbius ($\mu : \mathbf{N}^* \to \mathbf{R}$; $\mu(1) = 1$, $\mu(p_1, p_2 \ldots p_r) = (-1)^r$, dacă $p_1, p_2, \ldots, p_r$ sunt numere prime distincte și $\mu(n) = 0$, în orice alt caz). Am amintit aceste lucruri și pentru a argumenta afirmația făcută mai înainte și anume că funcția ψ este mai „simplă" decât funcția π. Din acest moment ne vom preocupa să demonstrăm că $\frac{\psi(x)}{x} \xrightarrow[x \to \infty]{} 1$ (ceea ce va demonstra implicit și teorema elementului prim după cum am văzut mai înainte). Pentru aceasta să definim întâi funcțiile R, $S : [0, \infty) \to \mathrm{R}$ prin următoarele formule:

$$(2)\quad \begin{cases} R(x) = \begin{cases} \psi(x) - x, & \text{dacă } x \ge 2 \\ 0, & \text{dacă } x < 2 \end{cases} \\ S(y) = \begin{cases} \int_2^y \frac{R(x)}{x}\, dx, & \text{dacă } y \ge 2 \\ 0, & \text{dacă } y < 2. \end{cases} \end{cases}$$

Deoarece ψ este o funcție etajată ea este integrabilă pe orice interval de forma $[2, y]$, unde $y \in \mathbf{R}$, $y \ge 2$; deci funcția S este într-adevăr bine definită. Deoarece $\frac{R(x)}{x}$ este integrabilă pe orice interval de forma $[2, y]$, deducem că S este o funcție continuă (continuitatea lui S în punctul 2 se verifică imediat). Mai mult $\frac{R(x)}{x}$ este continuă în orice punct t diferit de p^α, unde p este număr prim și $\alpha \in \mathbf{N}^*$ (aceasta se întâmplă deoarece funcția ψ are această proprietate), ceea ce ne arată (conform unui rezultat bine cunoscut) că funcția S este derivabilă în orice punct t diferit de p^α, unde p este un număr prim și $\alpha \in \mathbf{N}^*$. Calitățile lui S, reliefate mai sus, constituie motivația pentru care această funcție a fost luată în considerare. Scopul următoarelor 8 leme este de a demonstra că

$$\lim_{y \to +\infty} \frac{S(y)}{y} = 0.$$

Înainte de a trece la demonstrarea acestui fapt vom arăta cum presupunerea că

$$\lim_{y \to +\infty} \frac{S(y)}{y} = 0$$

demonstrează că $\lim_{x\to+\infty}\frac{\psi(x)}{x}=1$ și după cum am văzut mai înainte aceasta

soluționează teorema elementului prim. Deoarece

$$\lim_{y\to+\infty}\frac{S(y)}{y}=0,$$

pentru orice ε astfel încât $0<\varepsilon<1$ există $y_\varepsilon\geq 2$ cu proprietatea că $(\forall)\, y\geq y_\varepsilon$ atunci $|S(y)| \leq \frac{\varepsilon^2}{3} y$. Aceasta înseamnă că

$$S(y(1+\varepsilon)) - S(y) \leq \frac{\varepsilon^2}{3}(y(1+\varepsilon)+y) < \varepsilon^2 y,\ (\forall)\, y\geq y_\varepsilon$$

(ultima inegalitate are loc deoarece $\varepsilon<1$). Ținând cont de formulele (2) ultima inegalitate obținută ne arată că

$$\int_y^{y(1+\varepsilon)}\frac{R(u)}{u}\,du\leq\varepsilon^2 y,\ (\forall) y\geq y_\varepsilon.$$

Aceasta se mai scrie și sub forma

$$\int_y^{y(1+\varepsilon)}\frac{\psi(u)}{u}\,du-\int_y^{y(1+\varepsilon)}du\leq\varepsilon^2 y,(\forall) y\geq y_\varepsilon.$$

Cum ψ este evident o funcție crescătoare,

$$\frac{\psi(y)}{y(1+\varepsilon)}\int_y^{y(1+\varepsilon)}du\leq\int_y^{y(1+\varepsilon)}\frac{\psi(u)}{u}\,du\leq$$

$$\leq\varepsilon^2 y+\int_y^{y(1+\varepsilon)}du\leq\varepsilon^2 y+\varepsilon y,\ (\forall) y\geq y_\varepsilon.$$

(am folosit pentru ultima inegalitate concluziile anterioare). Înmulțind inegalitățile de mai sus cu $\frac{1+\varepsilon}{\varepsilon y}$ obținem că

$$\frac{\psi(y)}{y}\leq(1+\varepsilon)^2\ (\forall)\, y\geq y_\varepsilon.$$

Asupra lui y_ε mai facem o presupunere și anume y_ε este ales astfel încât să aibă loc inegalitatea $(1-\varepsilon)\, y_\varepsilon\geq 2$. Evaluând diferența $S(y)-S(y(1-\varepsilon))$ obținem că $S(y)-S(y(1-\varepsilon))\geq-\frac{\varepsilon^2}{3}y-\frac{\varepsilon^2}{3}y(1-\varepsilon)=-\frac{\varepsilon^2}{3}y(2-\varepsilon)\geq-\varepsilon^2 y.$

Folosind din nou formulele (2), ultima inegalitate se transcrie sub forma

$$\int_{y(1-\varepsilon)}^{y} \frac{\psi(u)}{u}du - \int_{y(1-\varepsilon)}^{y} du \geq -\varepsilon^2 y.$$

Deci

$$\int_{y(1-\varepsilon)}^{y} \frac{\psi(u)}{u}du \geq y\varepsilon - y\varepsilon^2 = y\varepsilon(1-\varepsilon).$$

Toate aceste ultime inegalități au loc doar pentru $y \geq y_\varepsilon$. Folosind încă odată faptul că ψ este o funcție crescătoare obținem următoarele inegalități

$$\frac{\psi(y)}{y(1-\varepsilon)} \int_{y(1-\varepsilon)}^{y} du \geq \int_{y(1-\varepsilon)}^{y} \frac{\psi(u)}{u}du \geq y\varepsilon(1-\varepsilon) \quad (\forall) y \geq y_\varepsilon.$$

Aceasta înseamnă că $(\forall)\, y \geq y_\varepsilon$ au loc inegalitățile

$$(1-\varepsilon)^2 \leq \frac{\psi(y)}{y} \leq (1+\varepsilon)^2.$$

De aici deducem că $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$, adică exact ceea ce trebuia demonstrat. În cele opt leme care urmează se va da demonstrația faptului că

$$\lim_{y\to+\infty} \frac{S(y)}{y} = 0.$$

Lema 1 : *Există o constantă pozitivă c astfel încât să aibă loc inegalitățile următoare:*

(3) $|S(y)| \leq cy \quad (\forall)\ y \geq 2$

(4) $|S(y_2) - S(y_1)| \leq c|y_2 - y_1|, \quad (\forall)\ y_1, y_2 \in \mathbf{R}_+.$

Tot în cadrul acestei leme se va arăta că are loc următoarea formulă:

(5) $S(y)\ln y + \sum_{j\leq y} \Lambda(j) S\left(\frac{y}{j}\right) = O(y)$ *pentru* $y \geq 2.$

Demonstrație: Propoziția 2 din paragraful I al anexei furnizează un $x_0 \geq 2$ astfel încât $(\forall)\ x \geq x_0$ să aibă loc inegalitatea $\frac{\psi(x)}{x} < \frac{3}{2}$. Aceasta înseamnă că

$$-x \leq \psi(x) - x \leq \frac{1}{2}x \quad (\forall)\, x \geq x_0.$$

Deci $\overline{\lim_{x\to\infty}} \frac{|R(x)|}{x} \leq 1$. Cum $\frac{|R(x)|}{x} \leq 1$, $(\forall)\ x \geq x_0$ și $\frac{R(x)}{x}$ este o funcție mărginită pe intervalul $[2, x_0]$ (deoarece ψ e mărginită pe $[2, x_0]$ și $a(x) = x$ este

o funcție continuă, mărginită și nenulă pe intervalul $[2, x_0]$) deducem existența unei constante pozitive c astfel încât $|R(x)| \le cx$, $(\forall)\ x \ge 2$. După cum am văzut mai înainte S este funcție derivabilă în orice punct $y \ne p^j$ (unde p e număr prim și $j \in \mathbf{N}^*$) și $S'(y) = \dfrac{R(y)}{y}$. Din cele de mai sus deducem că

(6) $|S'(y)| \le c \quad (\forall)\ y \ne p^j \quad (p$ - prim; $j \in \mathbf{N}^*)$.

Fie $y_1 < y_2$ două numere reale pozitive astfel încât intervalul (y_1, y_2) nu conține nici un punct de forma p^j (p - prim; $j \in \mathbf{N}^*$). Aplicând teorema lui Lagrange deducem existența unui $y_0 \in (y_1, y_2)$ astfel încât

$$S(y_2) - S(y_1) = S'(y_0)\,(y_2 - y_1).$$

Aplicând inegalitatea (6) deducem că

$$|S(y_2) - S(y_1)| \le c\,|y_2 - y_1| \quad (\forall)\ y_1, y_2 \in \mathbf{R}_+$$

astfel încât intervalul (y_1, y_2) nu conține vreun punct de forma p^j. În aplicarea teoremei lui Lagrange s-a ținut cont că S e derivabilă pe intervalul (y_1, y_2) și continuă pe intervalul $[y_1, y_2]$. Fie acum $y_1 < y_2$ două numere reale pozitive arbitrare și fie $y_1 \le a_1 < a_2 < \ldots < a_m \le y_2$ toate numerele de forma p^j (p - prim; $j \in \mathbf{N}^*$) cuprinse în intervalul $[y_1, y_2]$ (există doar un număr finit de astfel de puncte în orice interval finit).

Aplicând cele obținute mai sus deducem că

$$|S(y_2) - S(y_1)| \le |S(y_2) - S(a_m)| + \sum_{i=1}^{m-1} |S(a_{i+1}) - S(a_i)| + |S(a_1) - S(y_1)| \le$$

$$\le c\,(y_2 - a_m) + c \sum_{i=1}^{m-1} (a_{i+1} - a_i) + + c(a_1 - y_1) = c(y_2 - y_1) = c|y_2 - y_1|.$$

Inegalitatea (4) este astfel demonstrată. Dacă punem în (4) $y_1 = 2$, $y_2 = y$, deducem că

$$|S(y)| = |\,S(y) - S(2))\,| \le c(y - 2) \le cy, \ (\forall)\ y \ge 2,$$

ceea ce dovedește inegalitatea (3). Formula lui Selberg demonstrată în propoziția 2, paragraful II din anexă arată că:

$$(7)\ R(x)\ln x + \sum_{n \le x} \Lambda(n) R\left(\frac{x}{n}\right) = O(x), \ (\forall)\ x \ge 1.$$

Fie $y \ge 2$; deoarece $R(z) = 0$, $(\forall)\ z < 2$, deducem că

$$R(x)\ln x + + \sum_{n \le x} \Lambda(n) R\left(\frac{x}{n}\right) = R(x)\ln x + \sum_{n \le [y]} \Lambda(n) R\left(\frac{x}{n}\right), \ (\forall)\ x \in [2, y].$$

Dacă f este o funcție definită pe $[2, \infty]$ cu valori reale astfel încât $f = O(1)$ atunci funcția $g : [2, \infty] \to \mathbf{R}$ definită prin $g(y) = \int_2^y f(x)\,dx$ satisface egalitatea $g(y) = O(y)$ (f este o funcție integrabilă pe orice interval de forma $[2, y]$, $(\forall)\ y \geq 2$). Într-adevăr există $x_0 \geq 2$ astfel încât $|f(x)| \leq a$, $(\forall)\ x \geq x_0$ (a este o constantă reală pozitivă). Atunci, $(\forall)\ y \geq x_0$, avem că

$$|g(y)| \leq \int_2^y |f(x)/dx = \int_2^{x_0} |f(x)|\,dx + \int_{x_0}^y |f(x)|\,dx \leq \int_2^{x_0} |f(x)|\,dx + a\left(y - x_0\right) = O(y).$$

Ținând cont de aceste observații, împărțind relația (7) cu x și integrând apoi pe intervalul [2, y], deducem că

$$\int_2^y \frac{R(x)}{x} \ln x\,dx + \sum_{n \leq [y]} \Lambda(n) \int_2^y R\left(\frac{x}{n}\right) \cdot \frac{1}{x}\,dx = O(y).$$

Pentru a calcula $\int_2^y R\left(\frac{x}{n}\right)\frac{1}{x}dx$ vom uza de schimbarea de variabilă $z = \frac{x}{n}$. Deci

$$\int_2^y R\left(\frac{x}{n}\right)\frac{1}{x}dx = \int_2^y \frac{R\left(\frac{x}{n}\right)}{\frac{x}{n}} \cdot \frac{1}{n}dx = \int_{\frac{2}{n}}^{\frac{y}{n}} R(z) \cdot \frac{1}{z}dz = \int_{\frac{2}{n}}^{2} \frac{R(z)}{z}dz + \int_2^{\frac{y}{n}} \frac{R(z)}{z}dz = S\left(\frac{y}{n}\right),$$

deoarece funcția R este identic nulă pe intervalul $\left[\frac{2}{n}, 2\right]$ (dacă $\frac{y}{n} < 2$ se verifică ușor că identitatea de mai sus are loc). Am arătat deci că:

$$\int_2^y \frac{R(x)}{x} \ln x\,dx + + \sum_{n \leq y} \Lambda(n) S\left(\frac{y}{n}\right) = O(y).$$

Dacă $2 \leq y_1 < y_2$ sunt două numere reale astfel încât intervalul $[y_1, y_2]$ nu conține nici un punct de forma p^j (p - prim; $j \in \mathbf{N}^*$), deducem aplicând formula de integrare prin părți că:

$$\int_{y_1}^{y_2} \frac{R(x)}{x} \ln x\,dx = \int_{y_1}^{y_2} S'(x) \ln x\,dx = S\left(y_2\right)\ln y_2 - S\left(y_1\right)\ln y_1 - \int_{y_1}^{y_2} \frac{S(x)}{x}dx.$$

Din motive de continuitate (S, ln și funcțiile de forma $g(y) = \int_a^y f(x)\,dx$ sau $h(y) = \int_y^q f(x)\,dx$, unde f este o funcție integrabilă pe orice interval finit, sunt continue) formula anterioară are loc chiar dacă y_1 sau y_2 sunt de forma

p^j (p - prim; $j \in \mathbf{N}^*$). Un argument simplu arată acum că

$$\int_{y_1}^{y_2} \frac{R(x)}{x} \ln x \, dx = S(y_2) \ln y_2 - S(y_1) \ln y_1 - \int_{y_1}^{y_2} \frac{S(x)}{x} dx$$

$(\forall)\, y_1, y_2 \in \mathbf{R}$ cu $2 \le y_1 < y_2$. Înlocuind $y_1 = 2$, $y_2 = y$ obținem că

$$\int_2^y \frac{R(x)}{x} \ln x \, dx = \ln y \, S(y) - \int_2^y \frac{S(x)}{x} dx,$$

$(\forall)\, y \ge 2$ (am ținut cont că $S(2) = 0$). Ținând cont că

$$\left| \int_2^y \frac{S(x)}{x} dx \right| \le \int_2^y \left| \frac{S(x)}{x} \right| dx \le c \int_2^y dx = c(y-2) = O(y)$$

și de toate considerațiile anterioare, relația (5) este demonstrată.

Lema 2. *Dacă*

$$\Lambda_2(n) = \Lambda(n) + \sum_{i \cdot j = n} \Lambda(i)\Lambda(j),$$

$(\forall)\, n \in \mathbf{N}^*$, *atunci există o constantă* k_1 *astfel încât:*

$$(8)\ \ln^2 y \cdot |S(y)| \le \sum_{m \le y} \Lambda_2(m) \left| S\left(\frac{y}{m}\right) \right| + k_1 y \ln y, \quad (\forall)\, y \ge 1.$$

Demonstrație. Din relația (5) a lemei precedente deducem imediat existența unei constante a astfel încât

$$\left| S(y) \ln y + \sum_{j \le y} \Lambda(j) S\left(\frac{y}{j}\right) \right| \le a \cdot y,$$

$(\forall)\, y > 0$ (pe intervalul $(0, 2]$ membrul din stânga al inegalității precedente este egal cu 0; același membru din stânga este o funcție continuă pe orice interval de forma $[y_1, y_2]$, unde $y_1 > 0$, iar $f(y) = a \cdot y$ este o funcție continuă și nenulă pe intervalul $[y_1, y_2]$). Să evaluăm în cele ce urmează expresia

$$\left| \sum_{k \le y} \Lambda(k) S\left(\frac{y}{k}\right) \ln \frac{y}{k} + \sum_{k \le y} \sum_{j \le \frac{y}{k}} \Lambda(k)\Lambda(j) S\left(\frac{y}{jk}\right) \right| \le$$

$$\le \sum_{k \le y} \Lambda(k) \left| S\left(\frac{y}{k}\right) \ln \frac{y}{k} + \sum_{j \le \frac{y}{k}} \Lambda(j) S\left(\frac{y}{jk}\right) \right| \le a \cdot \sum_{k \le y} \Lambda(k) \cdot \frac{y}{k}$$

(pentru ultima inegalitate am folosit modul de definire al constantei a). Folosind această evaluare precum și propoziția 3 din paragraful I al anexei concluzionăm că:

$$\sum_{k\le y}\Lambda(k)S\left(\frac{y}{k}\right)\ln\frac{y}{k}+\sum_{j\cdot k\le y}\Lambda(k)\Lambda(j)S\left(\frac{y}{jk}\right)=O(y\ln y)=$$

$$=\ln y\sum_{k\le y}\Lambda(k)S\left(\frac{y}{k}\right)-\sum_{m\le y}S\left(\frac{y}{m}\right)\left(\Lambda(m)\ln m-\sum_{jk=m}\Lambda(j)\Lambda(k)\right)$$

(pentru ultimul semn de egalitate am folosit faptul că $\ln\frac{y}{k}=\ln y-\ln k$ și o schimbare de notație; am scris în loc de k, m). Folosind din nou egalitatea (5) precum și considerațiile anterioare, obținem că

$$\ln y\,(O(y)-S(y)\ln y)-\sum_{m\le y}S\left(\frac{y}{m}\right)\Lambda_2(m)=O(y\ln y)$$

și deci

$$\ln^2 y\,S(y)+\sum_{m\le y}S\left(\frac{y}{m}\right)\Lambda_2(m)=O(y\ln y).$$

În toate considerațiile de mai sus $y>1$. Enunțul lemei 2 este acum imediat.

Lema 3 . *Există o constantă pozitivă k_2 astfel încât:*

$$(9)\ \ln^2 y\cdot\left|S(y)\right|\le 2\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|\ln m+k_2 y\ln y\ \ (\forall)\,y\ge 1.$$

Demonstrație: $\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|\Lambda_2(m)=2\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|\cdot\ln m+J(y),\ \ (\forall)\,y>0,$

unde $J(y)=\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|\left(\Lambda_2(m)-2\ln m\right)=\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|\left(Q(m)-Q(m-1)\right).$

$Q:\mathbf{N}^*\to\mathbf{R}$ este funcția definită la sfârșitul anexei prin formula

$$Q(n)=\sum_{k\le n}(\Lambda_2(k)-2\ln k)$$

$(\forall)\,n\in\mathbf{N}^*$ (convenim ca $Q(0)=0$). În locul citat mai sus (formula (8) de la sfârșitul anexei) se arată că $Q(n)=O(n)$. Deoarece

$$0<\frac{y}{[y]+1}<1,\ S\left(\frac{y}{[y]+1}\right)=0$$

ceea ce ne permite să scriem următoarea formulă pentru J:

$$J(y)=\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|\cdot\left(Q(m)-Q(m-1)\right)=\sum_{m\le y}\left|S\left(\frac{y}{m}\right)\right|Q(m)-$$

$$-\sum_{m\le[y]-1}\left|S\left(\frac{y}{m+1}\right)\right|Q(m)=\sum_{2\le m\le y}Q(m)\left(\left|S\left(\frac{y}{m}\right)\right|-\left|S\left(\frac{y}{m+1}\right)\right|\right).$$

Există o constantă pozitivă b astfel încât, $Q(n)\le bn$, $(\forall)\ n\in\mathbf{N}^*$.

Deoarece $||z|-|t||\le|z-t|$ $(\forall)$ $z, t\in\mathbf{R}$, deducem (ținând cont și de inegalitatea (4) din lema 1) următoarea estimare pentru J:

$$|J(y)|\le\sum_{2\le m\le y}|Q(m)|\left|\left|S\left(\frac{y}{m}\right)\right|-\left|S\left(\frac{y}{m+1}\right)\right|\right|\le$$

$$\le\sum_{2\le m\le y}b\cdot m\left|S\left(\frac{y}{m}\right)-S\left(\frac{y}{m+1}\right)\right|\le\sum_{2\le m\le y}c\cdot b\cdot m\left(\frac{y}{m}-\frac{y}{m+1}\right)=$$

$$=bc\cdot y\sum_{2\le m\le y}\frac{1}{m+1}\le bc\cdot y\sum_{2\le m\le y}\int_{m-1}^{m}\frac{du}{u}=$$

$$=bc\cdot y\int_{1}^{[y]}\frac{du}{u}\le bc\cdot y\int_{1}^{y}\frac{du}{u}=bc\cdot y\cdot\ln y,$$

$(\forall)\ y>1$. Lema 2 încheie demonstrația lemei 3 ($k_2=k_1+bc$).

Lema 4. *Există o constantă pozitivă k_3 astfel încât să aibă loc inegalitatea:*

$$(10)\ \ln^2 y\cdot|S(y)|\le 2\int_{2}^{y}\left|S\left(\frac{y}{u}\right)\right|\ln u\,du+k_3 y\ln y,\ \ (\forall)\ y\ge 2.$$

Demonstrație: Deoarece funcția ln este crescătoare pentru $(\forall)\ m\le y$, avem inegalitatea

$$\ln m\cdot\left|S\left(\frac{y}{m}\right)\right|\le\int_{m}^{m+1}\ln u\cdot\left|S\left(\frac{y}{m}\right)\right|du\le\int_{m}^{m+1}\ln u\left|S\left(\frac{y}{u}\right)\right|du+$$

$$+\int_{m}^{m+1}\ln u\cdot\left|S\left(\frac{y}{m}\right)-S\left(\frac{y}{u}\right)\right|du$$

$\left(m\in\mathbf{N}^*;\ y\in\mathbf{R},\ y\ge 2\right)$. Sumând inegalitățile precedente de la 2 la $[y]$ obținem (ținând cont de inegalitatea (3) din lema 1) că

$$\sum_{m\le y}\ln m\cdot\left|S\left(\frac{y}{m}\right)\right|\le\int_{2}^{[y]}\ln u\cdot\left|S\left(\frac{y}{u}\right)\right|du+\sum_{2\le m\le y}c\int_{m}^{m+1}\ln u\left|\frac{y}{m}-\frac{y}{u}\right|du\le$$

$$\leq \int_2^y \ln u \left| S\left(\frac{y}{u}\right)\right| du + \sum_{2\leq m\leq y} cy \left|\frac{1}{m} - \frac{1}{m+1}\right| \int_m^{m+1} \ln u\, du \leq \int_2^y \ln u \left| S\left(\frac{y}{u}\right)\right| du +$$

$$+ \sum_{2\leq m\leq y} \frac{cy}{m(m+1)} \cdot \ln(m+1) \leq \int_2^y \ln u \left| S\left(\frac{y}{u}\right)\right| du + cy \sum_{2\leq m\leq y} \frac{1}{m+1}$$

(ultima inegalitate are loc deoarece $\ln(x+1) \leq x \quad (\forall)\, x \in \mathbf{R}_+$; termenul corespunzător lui $m = 1$ din suma $\sum_{m\leq y} \ln m \cdot \left| S\left(\frac{y}{m}\right)\right|$ este egal cu zero deoarece ln 1 = 0). Am arătat mai sus că $\sum_{2\leq m\leq y} \frac{1}{m+1} \leq \ln y$ (în cursul demonstrației lemei 3) ceea ce combinat cu inegalitățile precedente ne duce la concluzia că

$$\sum_{m\leq y} \ln m \cdot \left| S\left(\frac{y}{m}\right)\right| \leq \int_2^y \ln u \left| S\left(\frac{y}{u}\right)\right| du + cy \ln y.$$

Aceasta împreună cu concluzia lemei 3 demonstrează enunțul acestei leme (pe post de k_3 vom lua $k_2 + 2c$, k_2 fiind furnizat de lema 3).

Dacă în formula (10) punem $x = \ln y$ și facem schimbarea de variabilă $v = \ln \frac{y}{u}$ deducem că:

$$x^2 \,|\, S(e^x) \,| \leq 2 \int_0^{x-\ln 2} |\, S(e^v) \,| \,(x-v)e^{x-v}\, dv + k_3\, xe^x, \quad (\forall)\, x \geq 0$$

(deoarece (10) are loc evident și pentru $y \in [1,2]$). Dacă $v \in [\, x - \ln 2,\, x]$ atunci $x - v \geq 0$, deci inegalitatea de mai sus se poate scrie și astfel:

$$(11) \quad x^2 \,|\, S(e^x) \,| \leq 2 \int_0^{x-\ln 2} |\, S(e^v) \,| \,(x-v)e^{x-v}\, dv + k_3\, xe^x \leq$$

$$\leq 2\int_0^x |S\,(e^v)|(x-v)\cdot \cdot\, e^{x-v}\, dv + k_3\, xe^x, \quad (\forall)\, x \geq 0.$$

Dacă notăm cu $w : [0, \infty) \to \mathbf{R}$ funcția definită prin formula

(12) $w(x) = e^{-x}\ S(e^x) \quad (\forall)\, x \geq 0$

atunci (11) se mai scrie și

$$(13) \quad |w(x)| \leq \frac{2}{x^2}\int_0^x (x-v)|w(v)|\, dv + \frac{k_3}{x}, \quad (\forall)\, x > 0.$$

Această relație s-a obținut împărțind în inegalitatea (11) cu $x^2 \cdot e^x$.

Lema 5. *Dacă* $\alpha = \overline{\lim_{x\to+\infty}} |w(x)|$, $\gamma = \overline{\lim_{x\to+\infty}} \frac{1}{x}\int_0^x |w(z)|\, dz$ (*unde funcția w este dată de egalitatea* (12)) *atunci* $\alpha \leq 1$ *și* $\alpha \leq \gamma$.

Demonstrație. Am arătat în lema 1 că există $x_0 \geq 2$ astfel încât $\frac{|R(x)|}{x} \leq 1$ $(\forall)\, x \geq x_0$. Luând acum $y \geq x_0$ deducem că

$$\frac{|S(y)|}{y} \leq \frac{\int_2^{x_0} \frac{|R(x)|}{x}\,dx + \int_{x_0}^{y} \frac{|R(x)|}{x}\,dx}{y} \leq \frac{A+(y-x_0)}{y}$$

unde A este o constantă reală pozitivă care nu depinde decât de x_0. Făcând pe y să conveargă la $+\infty$ obținem din cele de mai sus că $\alpha \leq 1$.

În acest moment trebuie să menționăm faptul că lemele 2, 3 și 4 folosesc doar la demonstrarea inegalității $\alpha \leq \gamma$. Uzând de teorema lui Fubini observăm că

$$\int_0^x u\left(\frac{1}{u}\int_0^u |w(v)|\,dv\right)du = \int_0^x\int_0^u |w(v)|\,dv\,du = \int_0^x\left(\int_v^x |w(v)|\,du\right)dv = \int_0^x |w(v)|(x-v)\,dv.$$

Cu această remarcă inegalitatea (13) se mai poate scrie și sub forma:

$$(14)\ |w(x)| \leq \frac{2}{x^2}\int_0^x u\left(\frac{1}{u}\int_0^u |w(v)|\,dv\right)du + \frac{k_3}{x},\ (\forall)\, x > 0.$$

Pentru $\varepsilon > 0$ fie $x_1 \in \mathbf{R}_+^*$ astfel încât, $(\forall)\, u \geq x_1$, să aibă loc inegalitatea:

$$(15)\ \frac{1}{u}\int_0^u |w(v)|\,dv \leq \gamma + \varepsilon.$$

Inegalitatea (3) din lema 1 ne permite următoarea estimare valabilă pentru

$$(\forall)\, u > 0\ ;\ \frac{1}{u}\int_0^u |w(v)|\,dv = \frac{1}{u}\int_0^u e^{-v}\,|\,S(e^v)\,|\,dv \leq \frac{cu}{u} = c.$$

Pentru $x \geq x_1$ folosind inegalitățile (14), (15) precum și considerațiile anterioare deducem evaluarea următoare:

$$|w(x)| \leq \frac{2c}{x^2}\int_0^{x_1} u\,du + \frac{2}{x^2}\int_{x_1}^x u\left(\frac{1}{u}\int_0^u |w(v)|\,dv\right)du + \frac{k_3}{x} \leq$$

$$\leq \frac{cx_1^2}{x^2} + \frac{2(\gamma+\varepsilon)}{x^2}\int_{x_1}^x u\,du + \frac{k_3}{x} \leq \frac{cx_1^2}{x^2} + (\gamma+\varepsilon)\left(1-\frac{x_1^2}{x^2}\right) + \frac{k_3}{x}.$$

În inegalitatea precedentă procedăm la o trecere la limită $x \to +\infty$; concluzia este că $\alpha \leq \gamma + \varepsilon$.

Cum $\varepsilon > 0$ a fost ales arbitrar soluția lemei 5 este în acest moment realizată.

Lema 6. *Există o constantă pozitivă k astfel încât:*

$$(16)\ |\,w(x_2) - w(x_1)\,| \leq k\ |\,x_2 - x_1\,|\quad (\forall)\, x_1, x_2 \in \mathbf{R}_+$$

și

$$(17)\ \|\,w(x_2)\,| - |\,w(x_1)\,\| \leq k\,|\,x_2 - x_1\,|\quad (\forall)\, x_1, x_2 \in \mathbf{R}_+$$

Demonstrație. Folosind observațiile din lema 1 rezultă foarte ușor că w este derivabilă în orice punct x diferit de $j \ln p$ (p - număr prim, $j \in \mathbf{N}^*$) și $w'(x) = -e^{-x} S(e^x) + S'(e^x)$. Din relațiile (3) și (6) (din cuprinsul lemei citate mai sus) obținem că:

$$|w'(x)| \leq 2c = k, \ (\forall)\ x \neq j \ln p \ (p \text{ - prim}; \ j \in \mathbf{N}^*).$$

Uzând de un raționament similar cu cel făcut în lema 1 pentru a arăta că S satisface relația (4), deducem că are loc inegalitatea (16).

Inegalitatea (17) este o consecință directă a inegalității (16) și a faptului că $\| u | - | v \| \leq | u - v |, \ (\forall)\ u, v \in \mathbf{R}$.

Lema 7. *Există o constantă pozitivă M astfel încât oricare ar fi $0 \leq v_1 < v_2$ cu $w(v) \neq 0$, $(\forall)\ v_1 < v < v_2$, să aibă loc inegalitatea:*

$$(18) \int_{v_1}^{v_2} |w(v)| \, dv \leq M.$$

Demonstrație. Aplicând lema 1 din paragraful I al anexei cu

$$c_n = \Lambda(n) \ (\forall)\ n \in \mathbf{N}^* \text{ și } f(t) = \frac{1}{t}$$

deducem că

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \frac{\psi(x)}{x} + \int_1^x \frac{\psi(t)}{t^2} \, dt.$$

Folosind propozițiile 2 și 3 din paragraful I al anexei obținem că

$$\int_1^x \frac{\psi(t)}{t^2} dt = \sum_{n \leq x} \frac{\Lambda(n)}{n} - \frac{\psi(x)}{x} = \ln x + O(1) = \int_2^x \frac{\psi(t)}{t^2} dt \ (x \geq 2).$$

Evaluând $\int_2^x \frac{R(t)}{t^2} \, dt$ se obține formula:

$$(19) \int_2^x \frac{R(t)}{t^2} dt = \int_2^x \frac{\psi(t)}{t^2} dt - \int_2^x \frac{1}{t} dt = O(1).$$

Aplicând teorema lui Fubini se deduce egalitatea:

$$\int_2^x \frac{S(y)}{y^2} dy = \int_2^x \left(\int_2^y \frac{R(t)}{t} \cdot \frac{1}{y^2} dt \right) dy =$$

$$= \int_2^x \left(\int_t^x \frac{R(t)}{t} \cdot \frac{1}{y^2} dy \right) dt = \int_2^x \frac{R(t)}{t^2} dt - \frac{1}{x} \int_2^x \frac{R(t)}{t} dt.$$

Inegalitatea (3) din lema 1, formula (19) împreună cu egalitatea precedentă furnizează estimarea:

$$(20) \int_2^x \frac{S(y)}{y^2} dy = O(1) \ (x \geq 2).$$

Punând $x = e^v$ și uzând de schimbarea de variabilă $y = e^u$ obținem că $\int_{\ln 2}^{v} w(u)\,du = O(1)$ (s-a folosit bineînțeles și formula (20)). De aici și din faptul că funcția $h(z) = \int_{\ln 2}^{z} w(u)\,du$ este continuă pe orice interval finit, rezultă că există o constantă M care să satisfacă inegalitatea

$$\left|\int_{\ln 2}^{v} w(u)\,du\right| \le \frac{M}{2}, \quad (\forall)\, v \in \mathbf{R}_+.$$

De aici se deduce imediat că

$$\left|\int_{v_1}^{v_2} w(u)\,du\right| \le M, \quad (\forall)\, v_1, v_2 \in \mathbf{R}_+;$$

enunțul lemei este în acest moment evident.

Lema 8. *Fie* $g:[0,\infty) \to \mathbf{R}$ *o funcție având următoarele proprietăți:*

i) *g este o funcție continuă și dacă notăm cu* $\alpha = \overline{\lim_{x\to+\infty}} |g(x)|$,

$$\gamma = \overline{\lim_{x\to+\infty}} \frac{1}{x}\int_0^x |g(z)|\,dz$$

atunci $\alpha \le 1$ *și* $\alpha \le \gamma$.

ii) *există o constantă pozitivă k astfel încât* $|g(x_2) - g(x_1)| \le k\,|x_2 - x_1|$ $(\forall)\, x_1, x_2 \in \mathbf{R}_+$.

iii) *există o constantă pozitivă M astfel încât*

$$\int_{v_1}^{v_2} |g(v)|\,dv \le M$$

pentru orice $o \le v_1 < v_2$ *satisfăcând condiția* $g(v) \ne 0$ $(\forall)$ $v_1 < v < v_2$.

În aceste condiții neapărat α *trebuie să fie egal cu zero.*

Demonstrație. Înainte de soluția acestei leme să observăm că funcția W definită anterior satisface ipotezele lemei 8 (aceasta rezultă din lemele 5, 6 și 7).

Presupunând că lema 8 este adevărată deducem că $\lim_{x\to+\infty} |W(x)| = 0 = \lim_{y\to+\infty} \frac{|S(y)|}{y}$.

După cum am observat înainte de a demonstra cele 8 leme, faptul că $\lim_{y\to+\infty} \frac{S(y)}{y} = 0$ implică rezolvarea teoremei elementului prim.

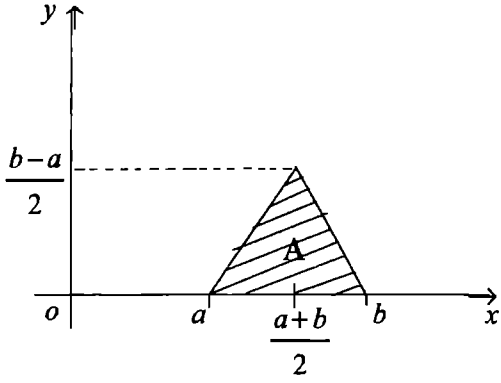
Pentru demonstrația lemei 8 să presupunem că constantele k și M sunt alese astfel încât $M \cdot k > 1$. Fie $\beta \in \mathbf{R}$ astfel încât $\alpha < \beta < \sqrt{Mk}$ $(\alpha \le 1 < M \cdot k)$.

Există atunci $x_\beta \geq 0$ ales astfel ca $|g(x)| \leq \beta$, $(\forall)\ x \geq x_\beta$. Dacă cumva există $x_0 \geq 0$ astfel încât $g(x) \neq 0$ $(\forall)\ x \geq x_0$ atunci ipoteza iii) ne asigură că $\gamma = 0$; cum $0 \leq \alpha \leq \gamma$ aceasta înseamnă că $\alpha = 0$, deci enunțul lemei este demonstrat.

Presupunem acum că funcția g ia valoarea zero în orice vecinătate a lui $+\infty$ (adică $(\forall)\ y_0 \geq 0$ există $y_1 \geq y_0$ astfel încât $g(y_1) = 0$. Fie a și b două zerouri succesive ale funcției ($g(a) = g(b) = 0$ și $g(y) \neq 0$, $(\forall)\ a < y < b$) astfel încât $b > a \geq x_\beta$.

Cazul I: $b - a \geq \dfrac{2M}{\beta}$. Conform acestei presupuneri și ipotezei iii) deducem că (21)

$$\int_a^b |g(x)|\,dx \leq M \leq \frac{\beta(b-a)}{2}.$$



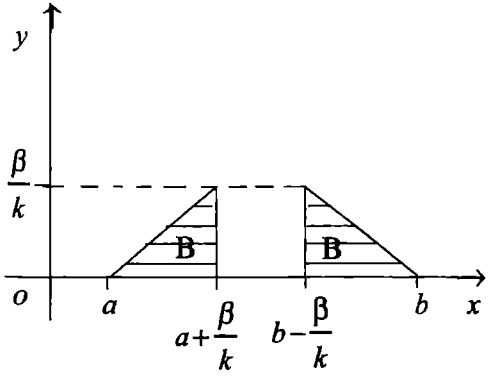
Cazul II: $b - a \leq \dfrac{2\beta}{k}$.

Pentru a evalua $\int_a^b |g(x)|\,dx$ vom folosi ipo-teza ii):

$$\int_a^b |g(x)|\,dx \leq \int_a^{\frac{a+b}{2}} |g(x)-g(a)|\,dx +$$

$$+ \int_{\frac{a+b}{2}}^b |g(b)-g(x)|\,dx \leq k\left(\int_a^{\frac{a+b}{2}} (x-a)\,dx + \int_{\frac{a+b}{2}}^b (b-x)\,dx\right) =$$

$$= k \cdot A = k\left(\frac{b-a}{2}\right)^2 \leq k \cdot \frac{\beta}{k} \cdot \frac{b-a}{2} = \frac{\beta(b-a)}{2}.$$



(A este aria figurii hașurate din desenul de mai sus;

$$\frac{b-a}{2} \leq \frac{\beta}{k},$$

conform presupunerii făcute). Deci și în acest caz are loc inegalitatea (21).

Cazul: III $\dfrac{2\beta}{k} < b - a < \dfrac{2M}{\beta}$.

Deoarece $M \cdot k > \beta^2$ inegalitățile de mai sus au sens. Folosind

faptul că $|g(x)| \le \beta$, $(\forall) x \ge x_\beta$, deducem că $\int_a^b |g(x)|\,dx \le \int_a^{a+\frac{\beta}{k}} |g(x)-g(a)|\,dx +$

$+ \int_{a+\frac{\beta}{k}}^{b-\frac{\beta}{k}} |g(x)|\,dx + \int_{b-\frac{\beta}{k}}^{b} |g(b)-g(x)|\,dx \le k \cdot B + \beta\left(b-a-\frac{2\beta}{k}\right)$ (B este aria figurii

haşurate din desenul de mai sus, $B = \frac{\beta^2}{k^2}$; s-a folosit de asemenea şi ipoteza ii).

Deci, $\int_a^b |g(x)|\,dx \le k \cdot \frac{\beta^2}{k^2} + \beta\left(b-a-\frac{2\beta}{k}\right) = (b-a)\beta\left(1-\frac{\beta}{k(b-a)}\right) \le$

$\le (b-a)\beta\left(1-\frac{\beta^2}{2Mk}\right) \le (b-a)\beta\left(1-\frac{\alpha^2}{2Mk}\right)$ întrucât $b - a < \frac{2M}{\beta}$ şi $\alpha < \beta$.

Deoarece

$$\frac{\beta(b-a)}{2} \le (b-a)\beta\left(1-\frac{\alpha^2}{2Mk}\right),$$

afirmaţie ce rezultă din faptul că $\alpha^2 \le 1 < M \cdot k$ deducem că inegalitatea

$$\int_a^b |g(x)|\,dx \le \beta(b-a)\left(1-\frac{\alpha^2}{2Mk}\right)$$

are loc în toate cele trei cazuri de mai sus. Fie acum $x_\beta \le a < b$ astfel încât $g(a) = g(b) = 0$ dar fără nici o altă presupunere asupra lui a şi b. Fie $D = \{ x \in [a,b] \mid g(x) \ne 0\}$; deoarece g este funcţie continuă atunci D este mulţime deschisă în $[a,b]$ şi chiar în $\mathbf{R}$ (deoarece $a, b \notin D$). Ştim atunci că $D = \bigcup_{i \in I} D_i$, unde $D_i \cap D_j = \varnothing$ $(\forall)$ $i \ne j$, D_i este interval deschis, $(\forall)$ $i \in I$, şi I este

o mulţime cel mult numărabilă. Dacă I este finită atunci $D = \bigcup_{j=1}^{n} D_{i_j}$ şi

$$\int_a^b |g(x)|\,dx = \sum_{j=1}^{n} \int_{D_{i_j}} |g(x)|\,dx \le \sum_{j=1}^{n} \beta \cdot l(D_{i_j}) \left(1-\frac{\alpha^2}{2Mk}\right) \le \beta \cdot (b-a) \cdot \left(1-\frac{\alpha^2}{2Mk}\right)$$

(am notat prin $l(D_{i_j})$ lungimea intervalului D_{i_j}; dacă $D_{i_j} = (a_{i_j}, b_{i_j})$ atunci $l(D_{i_j}) = b_{i_j} - a_{i_j}$. Consideraţiile precedente au permis scrierea inegalităţii

$$\int_{D_{i_j}} |g(x)|\,dx \le \beta \cdot l(D_{i_j}) \cdot \left(1-\frac{\alpha^2}{2Mk}\right)$$

deoarece a_{i_j}, b_{i_j} sunt două zerouri succesive ale funcției g. Faptul că $\sum_{j=1}^{n} l\left(D_{i_j}\right) \le b-a$ rezultă din faptul că $\bigcup_{j=1}^{n} D_{i_j} \subseteq [a,b]$ și că $D_i \cap D_j = \varnothing$, $(\forall)\, i \neq j$).

Dacă I nu este o mulțime finită, cum ea este numărabilă, putem scrie **N*** în loc de I. Să notăm cu $g_n : [a, b] \to \mathbf{R}$ funcția definită prin următoarea formulă:

(22) $g_n(x) = g(x) \cdot \chi_{D_1 \cup D_2 \cup \ldots \cup D_n}(x)$, $(\forall)\, x \in [a,b]$ pentru fiecare $n \in \mathbf{N}^*$.

χ_A însemnează funcția caracteristică a mulțimii $A(\chi_A(x)) = 1$, dacă $x \in A$ și $\chi_A(x) = 0$, dacă $x \notin A$).

Este clar că $|g_n|$ este o funcție integrabilă pe intervalul $[a, b]$ pentru orice $n \in \mathbf{N}^*$, și șirul de funcții $(|g_n|)_{n \in \mathbf{N}^*}$ converge simplu la funcția $|g|$ (pe intervalul $[a, b]$). În plus $\int_a^b |g_n(x)|\,dx \le \int_a^b |g(x)|\,dx$, $(\forall)\, n \in \mathbf{N}^*$. Știm atunci că în aceste condiții șirul de numere reale pozitive $\int_a^b |g_n(x)|\,dx$ converge la numărul $\int_a^b |g(x)|\,dx$.

Folosind un argument de care am uzat ceva mai înainte, deducem că

$$\int_a^b |g_n(x)|\,dx = \sum_{i=1}^{n} \int_{D_i} |g(x)|\,dx \le \sum_{i=1}^{n} \beta \cdot l(D_i) \left(1 - \frac{\alpha^2}{2Mk}\right) \le \beta(b-a)\left(1 - \frac{\alpha^2}{2Mk}\right).$$

Cum

$$\lim_{n \to \infty} \int_a^b |g_n(x)|\,dx = \int_a^b |g(x)|\,dx$$

din cele de mai sus rezultă că

$$\int_a^b |g(x)|\,dx \le \beta(b-a)\left(1 - \frac{\alpha^2}{2Mk}\right).$$

Deci această inegalitate are loc oricare ar fi a și b două zerouri ale funcției g astfel încât $x_\beta \le a < b$. Fie acum x_1 cel mai apropiat zero al funcției g față de x_β, situat la dreapta lui x_β (conform presupunerii făcute la început funcția g ia valoarea zero în orice vecinătate a lui $+\infty$; există deci acel x_1 de mai sus. Dacă $g(x_\beta) = 0$ atunci $x_1 = x_\beta$). Fie $y \ge x_1$ și $\overline{x}$ cel mai apropiat zero al funcției g față de y, situat la stânga lui y (în orice caz $\overline{x} \ge x_1$; dacă $g(y) = 0$ atunci $\overline{x} = y$). Ținând cont de observațiile precedente precum și de ipoteza iii), deducem că

$$\int_0^y |g(x)|\,dx \le \int_0^{x_1} |g(x)|\,dx + \int_{x_1}^{\overline{x}} |g(x)|\,dx + \int_{\overline{x}}^{y} |g(x)|\,dx \le$$

$$\le \int_0^{x_1} |g(x)|\,dx + (\overline{x} - x_1) \cdot \beta \cdot \left(1 - \frac{\alpha^2}{2Mk}\right) + M.$$

Din această inegalitate rezultă că

$$\frac{1}{y}\int_0^y |g(x)|\,dx \le \frac{1}{y}\int_0^{x_1} |g(x)|\,dx + \beta\left(1-\frac{\alpha^2}{2Mk}\right) + \frac{M}{y}\left(\frac{\overline{x}-x_1}{y} \le \frac{\overline{x}}{y} \le 1\right).$$

Trecând la limită spre $+\infty$ cu y, se obține că

$$\gamma \le \beta\left(1-\frac{\alpha^2}{2Mk}\right) \text{ și } \alpha \le \gamma \le \beta\left(1-\frac{\alpha^2}{2Mk}\right).$$

Mai realizăm o trecere la limită și anume $\beta \searrow \alpha$; rezultă că $\alpha \le \alpha - \frac{\alpha^3}{2Mk}$ și că $\alpha^3 \le 0$. De aici deducem că $\alpha \le 0$; cum evident $\alpha \ge 0$ enunțul lemei 8 este în acest moment demonstrat.

ANEXĂ
(Teorema elementului prim)

I. Lema 1 (A b e l). *Fie* $f: [1,\infty) \to \mathbf{R}$ *o funcție derivabilă cu derivata continuă și* $(c_n)_{n\geq 1}$ *niște constante reale. Dacă notăm cu* $c(u) = \sum_{n\leq u} c_n$, *atunci are loc următoarea identitate:*

$$\sum_{n\leq x} c_n f(n) = f(x)c(x) - \int_1^x f'(t)c(t)\mathrm{d}t \quad (\forall)\, x \geq 1.$$

Demonstrație. Funcția c este integrabilă pe intervalul $[1, x]$ deoarece este o funcție etajată. Ținând cont că pe intervalul $[i, i+1)$ c are valoarea $c(i)$ integrala $\int_1^x f'(t)c(t)\mathrm{d}t$ se poate scrie în modul următor:

$$\int_1^x f'(t)\,c(t)\,\mathrm{d}t = \int_1^2 f'(t)c(1)\mathrm{d}t + \int_2^3 f'(t)\,c\,(2)\,\mathrm{d}t + \ldots$$

$$\int_{[x]-1}^{[x]} f'(t)\,c\,([x]-1)\;\mathrm{d}t + \int_{[x]}^{x} f'(t)c([x])\,\mathrm{d}t = c(1)(f(2)-f(1)) + c(2)(f(3)-f(2)) + \ldots$$

$$+ c([x]-1)(f([x]) - f([x]-1)) + c([x])(f\,[(x)] - f([x])) =$$

$$- c(1)f(1) - f(2)(c(2) - c(1)) - f(3)(c(3) - c(2)) \ldots$$

$$- f([x])(c([x]) - c([x] - 1)) + c([x])f(x) =$$

$$- \sum_{n\leq x} c_n f(n) + c(x)f(x)$$

(am ținut cont în cele de mai sus de formula lui Leibniz-Newton, de faptul că $c(i+1) - c(i) = c_{i+1}$ $(\forall)\, i \in \mathbf{N}^*$ și că $c(x) = c([x])$). Deci formula din enunț este demonstrată.

Lema 2. (formula de sumare a lui Euler). *Dacă asupra funcției f se fac aceleași presupuneri ca și în lema precedentă atunci are loc următoarea formulă:*

$$\sum_{n\leq x} f(n) = \int_1^x f(t)\mathrm{d}t + \int_1^x (t-[t])f'(t)\,\mathrm{d}t + f(1) - (x-[x])f(x),\ (\forall)\, x \geq 1.$$

Demonstrație. Folosim lema precedentă cu $c_n = 1$, $(\forall)\, n \in \mathbf{N}^*$. În aceste condiții $c(u) = \sum_{n \le u} 1 = [u]$. Deci

$$\sum_{n \le x} f(n) = f(x)[x] - \int_1^x f'(t)[t]\,dt = f(x)[x] + \int_1^x (t - [t]) f'(t)\,dt - \int_1^x t f'(t)\,dt.$$

Folosind formula de integrare prin părți deducem că

$$\int_1^x t f'(t)\,dt = x f(x) - f(1) - \int_1^x f(t)\,dt.$$

Aceasta împreună cu egalitatea anterioară demonstrează enunțul.

Propoziția 1: $\sum_{n \le x} \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right)$, *pentru* $x \ge 1$ (γ *este constanta lui Euler, adică* $\gamma = \lim_{n \to \infty} a_n$, *unde* $a_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n} - \ln n$).

Demonstrație. Pentru $x \ge 1$ și $f(t) = \frac{1}{t}$ aplicăm lema 2 și obținem formula

$$\sum_{n \le x} \frac{1}{n} = \int_1^x \frac{1}{t}\,dt + \int_1^x \frac{(-t + [t])}{t^2}\,dt + 1 - \frac{x - [x]}{x}$$

(am ținut cont că $f'(t) = -\frac{1}{t^2}$). Ținând cont că $|x - [x]| < 1$ și că $\int_1^x \frac{1}{t}\,dt = \ln x$ deducem că

$$\sum_{n \le x} \frac{1}{n} = \ln x + 1 - \int_1^x \frac{t - [t]}{t^2}\,dt + O\left(\frac{1}{x}\right).$$

Deoarece $0 \le t - [t] < 1$ și $\frac{1}{t^2}$ este integrabilă pe $[1, \infty)$, atunci $\frac{t - [t]}{t^2}$ este integrabilă pe intervalul $[1, \infty)$ și în plus

$$0 \le \int_1^\infty \frac{t - [t]}{t^2}\,dt \le \int_1^\infty \frac{1}{t^2}\,dt = -\frac{1}{t}\Big|_\infty^1 = 1.$$

De asemenea

$$0 \le \int_x^\infty \frac{t - [t]}{t^2}\,dt \le \int_x^\infty \frac{1}{t^2}\,dt = -\frac{1}{t}\Big|_\infty^x = \frac{1}{x},$$

ceea ce înseamnă că $\int_x^\infty \frac{t - [t]}{t^2}\,dt = O\left(\frac{1}{x}\right)$.

Ținând cont de cele de mai sus deducem că

$$\sum_{n\le x}\frac{1}{n}=1+\ln x-\int_1^{\infty}\frac{t-[t]}{t^2}\,dt+O\left(\frac{1}{x}\right).$$

Am observat mai sus că $\frac{t-[t]}{t^2}$ este o funcție integrabilă pe $[1, \infty)$; deci

$$\int_1^{\infty}\frac{t-[t]}{t^2}=\lim_{\substack{n\to\infty\\ n\in\mathbf{N}^*}}\int_1^{n}\frac{t-[t]}{t^2}\,dt.$$

Dar

$$\int_1^{n}\frac{t-[t]}{t^2}\,dt=\sum_{i=1}^{n-1}\int_i^{i+1}\frac{t-i}{t^2}\,dt=\sum_{i=1}^{n-1}\left[\ln(i+1)-\ln i+i\left(\frac{1}{i+1}-\frac{1}{i}\right)\right]=$$

$$=\ln n+\sum_{i=1}^{n-1}\frac{-1}{i+1}=1+\ln n-\sum_{i=1}^{n}\frac{1}{i}\xrightarrow{n\to\infty}1-\gamma.$$

În acest moment enunțul este demonstrat.

Propoziția 2. *Există* $x_0\in\mathbf{R}$, $x_0\ge 1$ *astfel încât oricare ar fi* $x\ge x_0$ *să aibă loc inegalitatea* $\psi(x)<\frac{3x}{2}$ (Cebîșev – 1850).

Demonstrație. Știm că $T(x)=\sum_{n\le x}\psi\left(\frac{x}{n}\right)$ unde $T(x)=\sum_{n\le x}\ln n$. Folosind faptul că ψ este o funcție crescătoare precum și egalitățile anterioare deducem că:

$$T(x)-2T\left(\frac{x}{2}\right)=\psi(x)-\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right)-\psi\left(\frac{x}{4}\right)+\psi\left(\frac{x}{5}\right)-\psi\left(\frac{x}{6}\right)\ldots\ge\psi(x)-\psi\left(\frac{x}{2}\right).$$

Aplicăm lema 2 cu $f(t)=\ln t$ și obținem

$$T(x)=\int_1^{x}\ln t\,dt+\int_1^{x}(t-[t])\cdot\frac{1}{t}\,dt-(x-[x])\ln x.$$

Ținând cont că $0\le y-[y]<1$, $(\forall)\,y\in\mathbf{R}$, deducem că

$$0\le\int_1^{x}\frac{t-[t]}{t}\,dt\le\int_1^{x}\frac{1}{t}\,dt=\ln x$$

și că

$$(x-[x])\ln x=O(\ln x).$$

Deci

$$T(x)=\int_1^{x}(t)'\ln t\,dt+O(\ln x)=x\ln x-\int_1^{x}t\cdot\frac{1}{t}\,dt+O(\ln x)=$$

$$=x\ln x-x+1+O(\ln x)=x\ln x-x+O(\ln x)$$

(am ținut cont mai sus de formula de integrare prin părți. Identitatea obținută mai sus este forma slabă a formulei lui Stirling. Să mai spunem aici că formula lui Stirling este următoarea:

$$\lim_{\substack{n\to\infty \\ n\in\mathbf{N}^*}} \frac{n!e^n}{n^n\cdot\sqrt{2\pi n}}=1\Bigg).$$

Există deci $x_1\in\mathbf{R}$, $x_1\geq 1$ astfel încât

$$|T(x)-x\ln x+x|\leq k\ln x,$$

$(\forall)\ x\geq x_1$ (k este o constantă reală, pozi-tivă). Dacă cumva $2<x_1$, ținând cont că funcția $T(x)-x\ln x+x$ este mărginită pe intervalul $[2, x_1]$ și că funcția ln este continuă și nenulă pe intervalul indicat mai sus deducem că (mărind eventual constanta k)

$$|T(x)-x\ln x+x|\leq k\ln x,$$

$(\forall)\ x\geq 2$. Folosind inegalitatea de mai sus obținem că pentru $x\geq 4$ are loc evaluarea

$$T(x)-2T\left(\frac{x}{2}\right)\leq x\ln x-x+k\ln x-2\cdot\frac{x}{2}\cdot\ln\frac{x}{2}+2\cdot\frac{x}{2}+2k\ln\frac{x}{2}\leq$$

$$\leq x\cdot\ln 2+3\,k\ln x.$$

Ținând cont că T este mărginită și că $x\cdot\ln 2+3k\cdot\ln x$ este continuă și nenulă pe intervalul $[2, 4]$ (evident mai sus trebuie înțeles că T e mărginită pe intervalul $[2, 4\ ]$) deducem (mărindu-l eventual din nou pe k) că

$$T(x)-2T\left(\frac{x}{2}\right)\leq x\cdot\ln 2+3\,k\ln x\ \ (\forall)\ x\geq 2.$$

Ținând cont de inegalitatea

$$\psi(x)-\psi\left(\frac{x}{2}\right)\leq T(x)-2T\left(\frac{x}{2}\right)$$

deducem că

$$\psi(x)-\psi\left(\frac{x}{2}\right)\leq x\ln 2+3\,k\cdot\ln x\ \ (\forall)\ x\geq 2.$$

Pentru orice $j\in\mathbf{N}$ astfel încât $\frac{x}{2^j}\geq 2$, aplicăm inegalitatea de mai sus și obținem

$$\psi\left(\frac{x}{2^j}\right)-\psi\left(\frac{x}{2^{j+1}}\right)\leq\frac{x}{2^j}\ln 2+3\,k\cdot\ln\frac{x}{2^j}\leq\frac{x}{2^j}\ln 2+3\,k\ln x.$$

Cel mai mare număr natural j pentru care $x \geq 2^{j+1}$ este egal cu $\left[\frac{\ln x}{\ln 2}\right]-1$. Sumând inegalitățile anterioare pentru j de la 0 la $\left[\frac{\ln x}{\ln 2}\right]-1$ obținem că

$$\psi(x)-\psi\left(\frac{x}{2^{\left[\frac{\ln x}{\ln 2}\right]}}\right)\leq$$

$$\leq x\cdot\ln 2\left(1+\frac{1}{2}+\ldots+\frac{1}{2^{\left[\frac{\ln x}{\ln 2}\right]-1}}\right)+3k\cdot\left[\frac{\ln x}{\ln 2}\right]\cdot\ln x\leq 2\ln 2\cdot x+\frac{3k}{\ln 2}(\ln x)^2.$$

Ținând cont că $\frac{x}{2^{\left[\frac{\ln x}{\ln 2}\right]}}<2$ deducem că $\psi\left(\frac{x}{2^{\left[\frac{\ln x}{\ln 2}\right]}}\right)=0$ și deci

$$\psi(x)\leq 2\cdot\ln 2\cdot x+\frac{3k}{\ln 2}(\ln x)^2,\ (\forall)\ x\geq 2.$$

Avem că

$$e^{\frac{3}{4}}>1+\frac{3}{4}+\frac{\left(\frac{3}{4}\right)^2}{2}=1+\frac{3}{4}+\frac{9}{32}=1+\frac{33}{32}>2$$

și deci $\frac{3}{4}>\ln 2$, ceea ce se scrie sub forma $\frac{3}{2}>2\ln 2$. Ținând cont de faptul că $\lim_{x\to+\infty}\frac{x}{\ln^2 x}=+\infty$, că $\frac{3}{2}>2\ln 2$ și de ultima inegalitate referitoare la funcția ψ deducem existența unui număr real x_0, $x_0\geq 1$ astfel încât să aibă loc inegalitatea $\psi(x)<\frac{3}{2}x\quad(\forall)\ x\geq x_0$.

Propoziția 3. (Mertens) $\sum_{n\leq x}\frac{\Lambda(n)}{n}=\ln x+O(1)$.

Demonstrație. Calculăm întâi următoarea expresie:

$$\sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\leq x}\Lambda(n)\cdot\sum_{m\leq\frac{x}{n}}1=\sum_{m\leq x}\sum_{n\leq\frac{x}{m}}\Lambda(n)=\sum_{m\leq x}\psi\left(\frac{x}{m}\right)=T(x).$$

În cursul demonstrației propoziției 2 am arătat că $T(x) = x \ln x - x + O(\ln x)$. Deci

$$\sum_{n\le x} \Lambda(n)\cdot\frac{x}{n} - \sum_{n\le x} \Lambda(n)\cdot\left\{\frac{x}{n}\right\} = x\ln x - x + O(\ln x)$$

(am notat prin $\{\alpha\}$-partea fracționară a numărului real α). Împărțind cu x ultima identitate obținem că

$$\sum_{n\le x} \frac{\Lambda(n)}{n} - \sum_{n\le x} \frac{\Lambda(n)}{x}\left\{\frac{x}{n}\right\} = \ln x + O(1).$$

Pe de altă parte

$$\left|\sum_{n\le x} \frac{\Lambda(n)}{x}\left\{\frac{x}{n}\right\}\right| \le \frac{1}{x}\sum_{n\le x}\Lambda(n) = \frac{\psi(x)}{x} = O(1)$$

(faptul că $\frac{\psi(x)}{x} = O(1)$ este o consecință a propoziției 2). Deci

$$\sum_{n\le x} \frac{\Lambda(n)}{n} = \ln x + O(1),$$

adică tocmai ceea ce trebuia demonstrat.

II. Fie $\mu : \mathbf{N}^* \to \mathbf{Z}$ funcția lui Möbius definită precum urmează:

$$\mu(n) = \begin{cases} 1, & \text{dacă } n = 1 \\ (-1)^r, & \text{dacă } n = p_1 p_2 \cdot \ldots p_r, \text{ unde } p_1, \ldots p_r \text{ sunt numere prime distincte} \\ 0, & \text{în celelalte cazuri posibile.} \end{cases}$$

Lemă. *Dacă* $n \in \mathbf{N}$, $n > 1$ *atunci* $\sum_{d|n} \mu(d) = 0$. *Dacă* $n = 1$ *atunci evident* $\sum_{d|1} \mu(d) = 1$.

Demonstrație. Fie $p_1, p_2, \ldots, p_r$ numere prime distincte astfel încât $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots p_r^{e_r}$ ($e_i \in \mathbf{N}^*$ $(\forall)\, i = \overline{1,r}$). Divizorii d ai lui n pentru care $\mu(d) \neq 0$ sunt 1, p_i, pentru $(\forall)\, i = \overline{1,r}$, $p_i \cdot p_j$ pentru $(\forall)\ i \neq j$, $i = \overline{1,r}$, $j = \overline{1,r}$, $p_i \cdot p_j \cdot p_k$ $(\forall)\, i \neq j$, $i \neq k$, $j \neq k$, $i, j, k = \overline{1,r}$ și așa mai departe. Cum divizorii de forma p_i sunt în număr de C_r^1, cei de forma $p_i \cdot p_j$, cu $i \neq j$ sunt în număr de C_r^2 și în general divizorii de forma $p_{i_1} p_{i_2} \ldots p_{i_k}$ $(i_r \neq i_s$ $(\forall)\, r \neq s)$ sunt în număr de C_r^k deducem că $\sum_{d|n} \mu(d) = i + C_r^1(-1)^1 + C_r^2(-1)^2 \ldots + C_r^k(-1)^k + \ldots = (1-1)^r = 0$, ceea ce trebuia demonstrat.

Propoziția 1 : *Fie* $F : [1, \infty) \to \mathbf{R}$ *o funcție definită pe* $[1, \infty)$ *cu valori reale. Definim* $G : [1, \infty) \to \mathbf{R}$ *prin formula* $G(x) = \sum_{n \le x} F\left(\frac{x}{n}\right)$. *Atunci*

$$F(x) = \sum_{k \le x} \mu(k)\, G\left(\frac{x}{k}\right) \quad (\forall)\, x \ge 1.$$

Demonstrație. Să calculăm expresia

$$\sum_{k \le x} \mu(k)\, G\left(\frac{x}{k}\right) = \sum_{k \le x} \mu(k) \sum_{n \le \frac{x}{k}} F\left(\frac{x}{nk}\right) =$$

$$= \sum_{n \cdot k \le x} \mu(k)\, F\left(\frac{x}{nk}\right) = \sum_{m \le x} F\left(\frac{x}{m}\right)\left(\sum_{j/m} \mu(j)\right) = F(x).$$

Pentru ultima egalitate am folosit lema precedentă care afirmă că $\sum_{j|m} \mu(j) = 0 \ \ (\forall)\, m > 1,\ m \in \mathbf{N}$ și că $\sum_{j|1} \mu(j) = 1 = \mu(1)$. Propoziția este astfel demonstrată.

Corolar: $\Lambda(n) = \sum_{k|n} \mu(k) \ln \frac{n}{k} \ \ (\forall)\, n \in \mathbf{N}^*$.

Demonstrație. Ținând cont că $T(x) = \sum_{n \le x} \psi\left(\frac{x}{n}\right)$ și de afirmația propoziției precedente deducem că $\psi(x) = \sum_{k \le x} \mu(k) T\left(\frac{x}{k}\right)$, $(\forall)\ x \ge 1$. Din egalitatea precedentă precum și din definițiile funcțiilor ψ și T deducem că $\sum_{n \le x} \Lambda(n) = \sum_{k \le x} \mu(k) \left(\sum_{j \le \frac{x}{k}} \ln(j) \right) = \sum_{n \le x} \sum_{j \cdot k = n} \mu(k) \ln(j) = \sum_{n \le x} \left(\sum_{k|n} \mu(k) \ln \frac{n}{k} \right)$. În ultima identitate, punând succesiv $x = 1, 2, 3...$, deducem că $\Lambda(n) = \sum_{k|n} \mu(k) \ln \frac{n}{k}$ $(\forall)\, n \in \mathbf{N}^*$.

Propoziția 2 (Atle Selberg). *Pentru* $x \ge 1$ *are loc următoarea identitate:*

$$(1)\ \left(\psi(x) - x\right) \ln x + \sum_{n \le x} \left(\psi\left(\frac{x}{n}\right) - \frac{x}{n} \right) \Lambda(n) = O(x).$$

Demonstrație. Fie $F : [1, \infty) \to \mathbf{R}$ o funcție cu valori reale care va fi precizată mai târziu și $G : [1, \infty) \to \mathbf{R}$ funcția definită prin formula

$$G(x) = \sum_{n \le x} F\left(\frac{x}{n}\right), \ (\forall)\, x \ge 1.$$

Definim funcția J: $[1, \infty) \to \mathbf{R}$.

(2) $J(x)=\sum_{k\le x}\mu(k)\ln\frac{x}{k}G\left(\frac{x}{k}\right)$ pentru $(\forall)\, x\ge 1$.

Explicitând formula de definire a funcției J obținem că

$$J(x)=\sum_{k\le x}\mu(k)\ln\frac{x}{k}\sum_{j\le\frac{x}{k}}F\left(\frac{x}{jk}\right)=\sum_{j\cdot k\le x}\mu(k)\ln\frac{x}{k}F\left(\frac{x}{jk}\right)=$$

$$=\sum_{n\le x}F\left(\frac{x}{n}\right)\left(\sum_{j\cdot k=n}\mu(k)\ln\frac{x}{k}\right)=\sum_{n\le x}F\left(\frac{x}{n}\right)\left(\sum_{k|n}\mu(k)\ln\frac{x}{k}\right)=$$

$$=\sum_{n\le x}F\left(\frac{x}{n}\right)\ln\frac{x}{n}\left(\sum_{k|n}\mu(k)\right)+\sum_{n\le x}F\left(\frac{x}{n}\right)\left(\sum_{k|n}\mu(k)\ln\frac{n}{k}\right)$$

(pentru ultima egalitate am ținut cont de formula $\ln\frac{x}{k}=\ln\frac{x}{n}+\ln\frac{n}{k}$). Ținând cont de lema de la începutul acestui paragraf precum și de corolarul propoziției 1 deducem că

$$J(x)=F(x)\ln x+\sum_{n\le x}F\left(\frac{x}{n}\right)\Lambda(n).$$

Această din urmă identitate împreună cu formula (2) furnizează următoarea egalitate cunoscută sub numele de formula Tatuzawa-Iseki:

(3) $F(x)\ln x+\sum_{n\le x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{k\le x}\mu(k)\ln\frac{x}{k}G\left(\frac{x}{k}\right)$.

În acest moment precizăm cine este funcția $F:[1,\infty)\to\mathbf{R}$. Alegem deci funcția F cu ajutorul următoarei formule: $F(x)=\psi(x)-x+\gamma+1$. În aceste condiții

$$G(x)=\sum_{n\le x}F\left(\frac{x}{n}\right)=T(x)-\sum_{n\le x}\frac{x}{n}+(\gamma+1)\sum_{n\le x}1=T(x)-x\sum_{n\le x}\frac{1}{n}+(\gamma+1)[x]$$

unde γ este constanta lui Euler. Am folosit mai sus și faptul că $\sum_{n\le x}\psi\left(\frac{x}{n}\right)=T(x)$.

Deoarece $[x]=x-\{x\}$, $(\forall)\, x\in\mathbf{R}$, unde $0\le\{x\}<1$, deducem că

$$(\gamma+1)[x]=(\gamma+1)x+O(1).$$

Propoziția 1 din paragraful I al anexei ne arată că

$$x\sum_{n\le x}\frac{1}{n}=x\ln x+\gamma x+O(1).$$

Deci $G(x)=T(x)-x\ln x+x+O(1)$.

Forma slabă a formulei lui Stirling (demonstrată în cursul soluției propoziției 2 din paragraful I al anexei) arată că $T(x) = x \ln x - x + O(\ln x)$, identitate care împreună cu considerațiile anterioare ne conduce la egalitatea $G(x) = O(\ln x)$.

Deoarece $\lim\limits_{x\to+\infty} \dfrac{\sqrt{x}}{\ln^2 x} = \infty$, deducem că $\ln x \cdot G(x) = O(\ln^2 x) = O\left(\sqrt{x}\right)$. Există deci $x_1 \in \mathbf{R}$, $x_1 \geq 1$ și o constantă reală și pozitivă a astfel încât $|\ln x \cdot G(x)| \leq a\sqrt{x}$ $(\forall)\, x \geq x_1$. Ținând cont că $\ln x \cdot G(x)$ este o funcție mărginită pe intervalul $[1, x_1]$ și $\sqrt{x}$ este o funcție continuă și nenulă pe același interval deducem că (mărind eventual constanta a) inegalitatea $|\ln x \cdot G(x)| \leq a\sqrt{x}$ are loc $(\forall)\, x \geq 1$. Putem evalua acum membrul din dreapta al egalității (3):

$$\left|\sum_{k\leq x}\mu(k)\ln\frac{x}{k}G\left(\frac{x}{k}\right)\right| \leq \sum_{k\leq x}\left|\ln\frac{x}{k}G\left(\frac{x}{k}\right)\right| \leq \sum_{k\leq x} a\cdot\sqrt{\frac{x}{k}} = a\sqrt{x}\left(\sum_{k\leq x}\frac{1}{\sqrt{k}}\right) \leq$$

$$\leq a\sqrt{x}\left(1+\sum_{2\leq k\leq x}\int_{k-1}^{k}\frac{1}{\sqrt{u}}\,du\right) = a\sqrt{x}\left(1+\int_{1}^{[x]}\frac{1}{\sqrt{u}}\,du\right) \leq a\sqrt{x}\left(1+\int_{1}^{x}\frac{1}{\sqrt{u}}\,du\right) =$$

$$= a\sqrt{x}\left(1+2\sqrt{x}-2\right) = O(x).$$

(inegalitatea $\dfrac{1}{\sqrt{k}} \leq \displaystyle\int_{k-1}^{k}\frac{1}{\sqrt{u}}\,du$ are loc deoarece $\dfrac{1}{\sqrt{u}} \geq \dfrac{1}{\sqrt{k}}$ $(\forall)\, u \in [k-1, k]$).

Folosind egalitatea (3) deducem că

$$(\psi(x) - x + \gamma + 1)\ln x + \sum_{n\leq x}\left(\psi\left(\frac{x}{n}\right) - \frac{x}{n} + \gamma + 1\right)\Lambda(n) = O(x).$$

Deoarece

$$(\gamma + 1)\ln x = O(x) \text{ și } (\gamma+1)\sum_{n\leq x}\Lambda(n) = = (\gamma + 1)\,\psi(x) = O(x)$$

(conform propoziției 2 din paragraful I) constatăm că are loc identitatea din enunț (formula lui Atle Selberg)

$$(\psi(x) - x)\ln x + \sum_{n\leq x}\left(\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right)\Lambda(n) = O(x).$$

Încheiem acest paragraf cu câteva formule ce vor fi utile în demonstrarea teoremei elementului prim. Propoziția 3 din paragraful I ne asigură că $x\sum\limits_{n\leq x}\dfrac{\Lambda(n)}{n} = x\ln x + O(x)$ care împreună cu formula lui Atle Selberg (egalitatea (1)) furnizează identitatea:

$$(4)\quad \psi(x)\ln x + \sum_{n\leq x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\ln x + O(x).$$

Există o constantă pozitivă b astfel încât $\psi(x) \le bx$, $(\forall)\, x \ge 1$ (aceasta este o consecință imediată a propoziției 2 din paragraful I). De aici rezultă că $\int_1^x \frac{\psi(t)}{t}\,dt = O(x)$. Aplicând lema 1 din paragraful I, punând $c_n = \Lambda(n)$ $(\forall)\, n \in \mathbf{N}^*$ și $f(t) = \ln t$, obținem

$$\sum_{n\le x}\Lambda(n)\ln n = \psi(x)\ln x - \int_1^x \frac{\psi(t)}{t}\,dt = \psi(x)\ln x + O(x)$$

(pentru ultima egalitate am folosit considerațiile anterioare care arătau că $\int_1^x \frac{\psi(t)}{t}\,dt = O(x)$). Avem deci egalitatea:

(5) $\sum_{n\le x}\Lambda(n)\ln n = \psi(x)\ln x + O(x)$.

Un calcul ușor arată că:

(6) $$\sum_{j\le x}\Lambda(j)\psi\left(\frac{x}{j}\right) = \sum_{j\le x}\Lambda(j)\left(\sum_{k\le \frac{x}{j}}\Lambda(k)\right) = \sum_{j\cdot k\le x}\Lambda(j)\Lambda(k).$$

Trebuie menționat că în formulele de mai sus x este un număr real, $x \ge 1$. Definim acum Λ_2: $\mathbf{N}^* \to \mathbf{R}$ prin formula

$$\Lambda_2(n) = \Lambda(n)\ln n + \sum_{j\cdot k=n}\Lambda(j)\Lambda(k),$$

$(\forall)\, n \in \mathbf{N}^*$. Folosind formulele (5) și (6) deducem că

$$\sum_{n\le x}\Lambda_2(n) = \sum_{n\le x}\Lambda(n)\ln n + \sum_{j\cdot k\le x}\Lambda(j)\Lambda(k) =$$

$$= \psi(x)\ln x + \sum_{j\le x}\Lambda(j)\,\psi\left(\frac{x}{j}\right) + O(x) = 2x\ln x + O(x)$$

(pentru ultima egalitate am folosit formula (4)). Deci am obținut o nouă formulă:

(7) $\sum_{n\le x}\Lambda_2(n) = 2x\ln x + O(x)$.

Definim funcția Q: $\mathbf{N}^* \to \mathbf{R}$ prin $Q(n) = \sum_{k\le n}\left(\Lambda_2(k) - 2\ln k\right)$, $(\forall)\, n \in \mathbf{N}^*$ $\left(Q(1) = 0\right)$. Folosind formula (7) și formula lui Stirling în forma ei slabă deducem că $Q(n) = 2n\ln n + O(n) - 2n\ln n + 2n + O(\ln n) = O(n)$. Punem acest rezultat sub forma egalității:

(8) $Q(n) = O(n)$.

TEOREMA LUI DIRICHLET A PROGRESIILOR ARITMETICE

Introducere

Scopul acestui capitol este demonstrarea unui rezultat clasic în teoria numerelor și anume teorema lui Dirichlet privind *existența unui număr infinit de numere prime într-o progresie aritmetică* (*de numere naturale*) *în care primul termen și rația sunt numere naturale prime între ele.* Deci *dacă* $a, b \in \mathbf{N}^*$, $(a, b) = 1$, *atunci există o infinitate de numere naturale* k *pentru care* $a \cdot k + b$ *este număr prim.* Dirichet a demonstrat acest rezultat în anul 1837. Reciproca afirmației de mai sus (dacă $a, b \in \mathbf{N}^*$ sunt astfel încât există o infinitate de numere naturale k pentru care $a \cdot k + b$ este număr prim, atunci $(a, b) = 1$) este evidentă.

Demonstrația prezentată în acest capitol combină argumente din două lucrări: „Teoria numerelor" de Z.I. Borevici și I.R. Șafarevici, Editura Științifică și Enciclopedică, București, 1985, pagina 413 și „Vorlesungen über Zahlentheorie" de E. Landau, Leipzig, 1927, pagina 79 din volumul I („Aus der elementaren und additiven Zahlentheorie").

În paragraful I al anexei se dau câteva rezultate privind caracterele grupurilor abeliene finite, iar în paragraful II se studiază în general seriile de forma $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, unde s este un număr real strict pozitiv, iar a_n sunt numere complexe.

S-a urmărit evitarea utilizării argumentelor de analiză complexă. S-a făcut rabat de la acest deziderat numai la considerarea logaritmului de variabilă complexă. Există o demonstrație - cea dată de Dirichlet - care nu utilizează deloc chestiuni de analiză complexă, cu prețul unei demonstrații laborioase ce folosește teoria formelor pătratice.

Demonstrația teoremei lui Dirichlet

Teoremă (Dirichlet). *Dacă a și b sunt numere naturale strict pozitive, prime între ele, atunci există o infinitate de numere naturale k astfel încât numărul* $a \cdot k + b$ *să fie prim.*

Enunțul este evident adevărat pentru $a = 1$ și $a = 2$ și de aceea în continuare vom presupune că $a \in \mathbf{N}$, $a \geq 3$.

În paragraful I al anexei am definit noțiunile de caracter și caracter numeric modulo a. Dacă notăm cu G grupul unităților inelului claselor de resturi modulo a ($G = U(\mathbf{Z}_a, \cdot)$) un caracter χ al grupului G este un morfism de grupuri între G și $(\mathbf{C}^*, \cdot)$ (grupul multiplicativ al numerelor complexe). Dacă $\chi(g) = 1$ $(\forall)$ $g \in G$ caracterul χ se notează cu χ_0 și se numește caracterul unitate al grupului G. Conform propoziției 1 din paragraful I al anexei există $\varphi(a)$ caractere ale grupului G. Unui caracter χ al grupului G i se asociază o funcție $\chi^* : \mathbf{Z} \to \mathbf{C}$, denumită caracter numeric modulo a, definită prin următoarea formulă: $\chi^*(m) = = \chi(\overline{m})$ dacă m este un număr întreg prim cu a (prin $\overline{m}$ înțelegem clasa modulo a a numărului întreg m) și $\chi^*(m) = 0$, dacă $m \in \mathbf{Z}$ și numerele m și a nu sunt prime între ele. Funcția χ^* are următoarele proprietăți evidente (menționate și în anexă)

i) $\chi^*(m) \neq 0 \Leftrightarrow (a,m) = 1$

ii) $\chi^*(m_1) = \chi^*(m_2)$, dacă $m_1 \equiv m_2 \pmod{a}$ $m_1, m_2 \in \mathbf{Z}$

iii) $\chi^*(m_1 m_2) = \chi^*(m_1)\,\chi^*(m_2)$ $(\forall)$ $m_1, m_2 \in \mathbf{Z}$.

Fără a exista pericol de confuzie, pentru a nu complica scrierea, vom folosi în loc de χ^* tot notația χ (în funcție de context va fi clar dacă este vorba de un caracter al grupului G sau de un caracter numeric modulo a). Pentru caracterul numeric modulo a, provenit din caracterul unitate al grupului G vom păstra denumirea de caracter unitate (și se va nota tot cu χ_0). În propoziția 3 din paragraful II al anexei s-a arătat că suma $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ este convergentă pentru orice caracter numeric modulo a diferit de χ_0 și orice $s > 0$. Dacă se notează cu $L(s, \chi)$ suma seriei precedente, atunci $L(s, \chi)$ este funcție continuă pe intervalul $(0, \infty)$. De asemenea s-a arătat în observația care urmează propoziției 3 din paragraful II al anexei că $\sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s}$ este convergentă pentru orice $s > 1$ și dacă notăm cu $L(s, \chi_0)$ suma seriei precedente, atunci $L(s, \chi_0)$ este funcție continuă pe intervalul $(1, +\infty)$. Rezultatul cheie în demonstrarea teoremei lui Dirichlet este următoarea:

Propoziție: $L(1, \chi) \neq 0$ $(\forall)$ $\chi \neq \chi_0$.

Demonstrație: Vom demonstra întâi enunțul în cazul în care există $m \in \mathbf{Z}$ astfel încât $\chi(m) \in \mathbf{C}\backslash\mathbf{R}$. De aici deducem că $\chi^2(m) \neq 1$ și $\chi^2(m) \neq 0$; deci

$\chi^2 \neq \chi_0$. Conform propoziției 9 din paragraful II al anexei (folosind notația $h = \varphi(a)$, $h \in \mathbf{N}, h \geq 2$) avem că $|L(s, \chi^2)| \leq \frac{h}{2} < h$ pentru $s > 1$.

Pentru $1 < s < 2$ au loc următoarele evaluări:

$$L(s,\chi_0) = \sum_{k=1}^{\infty} \frac{\chi_0(k)}{k^s} = \sum_{\substack{k=1 \\ (k,a)=1}}^{\infty} \frac{1}{k^s} \leq \sum_{k=1}^{\infty} \frac{1}{k^s} = 1 + \sum_{k=2}^{\infty} \frac{1}{k^s} \leq 1 + \sum_{k=2}^{\infty} \int_{k-1}^{k} \frac{1}{x^s} dx =$$

$$= 1 + \int_1^{\infty} \frac{1}{x^s} dx = 1 + \frac{x^{1-s}}{1-s}\Big|_{x=1}^{x=\infty} = 1 + \frac{1}{s-1} = \frac{s}{s-1} < \frac{2}{s-1}.$$

Ținând cont de evaluările precedente

$$(|L(s,\chi^2)| < h, L(s,\chi_0) \in \mathbf{R}_+^*$$

și $L(s, \chi_0) < \frac{2}{s-1}$ pentru $1 < s < 2$) precum și de propoziția 7 din paragraful II al anexei obținem că:

$$(1)\ |L(s,\chi)| \geq \frac{1}{|L(s,\chi_0)|^{\frac{3}{4}}} \cdot \frac{1}{|L(s,\chi^2)|^{\frac{1}{2}}} > \left(\frac{s-1}{2}\right)^{\frac{3}{4}} \cdot \frac{1}{\sqrt{h}} > \frac{(s-1)^{\frac{3}{4}}}{2\sqrt{h}}.$$

În ipoteza că $L(1, \chi) = 0$ atunci:

$$(2)\ |L(s,\chi)| = |L(s,\chi) - L(1,\chi)| = \left|\int_1^s L'(x,\chi)\,dx\right| \leq \int_1^s |L'(x,\chi)|\,dx \leq h(s-1),$$

pentru $1 < s < 2$. Pentru a justifica relația (2) sunt necesare unele explicații. În propoziția 10 din paragraful II al anexei s-a arătat că $L(s,\chi)$ e derivabilă pe $(1, +\infty)$ și că

$$L'(s,\chi) = -\sum_{k=1}^{\infty} \frac{\chi(k)\ln k}{k^s}.$$

Deoarece $\sum_{k=1}^{\infty} \frac{\ln k}{k^{1+\varepsilon}}$ este sumă convergentă pentru $(\forall)\ \varepsilon > 0$ (acest lucru a fost demonstrat în cursul propoziției 10 citate anterior) deducem că $-\sum_{k=1}^{\infty} \frac{\chi(k)\ln k}{k^s}$ converge uniform pe $[1 + \varepsilon, \infty)$ $(\forall)\ \varepsilon > 0$ și deci $L'(s, \chi)$ e continuă pe $(1, +\infty)$. Din cauză că $\chi \neq \chi_0$, $|L'(x, \chi)| < h$ $(\forall)\ x \geq 1$. Funcția $L'(x, \chi)$ este deci integrabilă pe $[1,s]$ $(\forall)\ 1 < s < 2$. Faptul că $|L'(x, \chi)| < h$ $(\forall) x \geq 1$ (demonstrat în aceeași propoziție 10 din paragraful II al anexei) justifică inegalitatea

$\int_1^s |L'(x,\chi)|\,dx \le h(s-1)$. Dacă f este o funcție definită pe un interval I al axei reale cu valori în numere complexe, înțelegem prin faptul că f este derivabilă egalitatea $f = f_1 + i f_2$, unde f_1 și f_2 sunt funcții definite pe I cu valori reale și în plus f_1 și f_2 sunt derivabile. Derivata f' este funcția $f_1' + i f_2'$. Spunem că f este integrabilă dacă f_1 și f_2 sunt integrabile: atunci $\int_I f = \int_I f_1 + i \int_I f_2$ (unde $\int_I f_1$ și $\int_I f_2$ sunt integralele Riemann ale funcțiilor f_1 și f_2 pe intervalul I). Se justifică astfel și egalitatea

$$L(s,\chi) - L(1,\chi) = \int_1^s L'(x,\chi)\,dx$$

(ca o consecință a formulei Leibniz-Newton).

Din inegalitățile (1) și (2) rezultă că

$$h(s-1) \ge |L(s,\chi)| > \frac{(s-1)^{\frac{3}{4}}}{2\sqrt{h}}$$

și deci

(3) $(s-1)^{\frac{1}{4}} > \frac{1}{2h\sqrt{h}}$, $(\forall) 1 < s < 2$.

Alegem $s = 1 + \frac{1}{16h^6}$ (avem că $1 < s < < 2$ deoarece $h \in \mathbf{N}^*$) și deci $(s-1)^{\frac{1}{4}} = \frac{1}{2h\sqrt{h}}$. Inegalitatea (3) este deci imposibilă. Presupunem că $L(1,\chi) = 0$ este deci falsă și enunțul propoziției este demonstrat în acest caz.

În cele ce urmează considerăm celălalt caz posibil și anume situația în care $\chi(n) \in \mathbf{R}$, $(\forall)\, n \in \mathbf{Z}$. Aceasta înseamnă că valorile posibile pentru $\chi(n)$ sunt -1, 0, $+1$, pentru $(\forall)\, n \in \mathbf{Z}$. Folosind propoziția 4 din paragraful II al anexei, precum și ipoteza privind caracterul χ deducem că $L(s,\chi) \ge 0$ $(\forall)\, s > 1$ (într-adevăr

$$L(s,\chi) = \prod_{p\text{-}prim} \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right) (\forall) s > 1,$$

conform propoziției citate anterior. Cum $\chi(p) = -1, 0$ sau 1 pentru orice număr prim p, rezultă că

$$\frac{1}{1 - \frac{\chi(p)}{p^s}} \ge 0$$

și deci $L(s,\chi), \ge 0$ $(\forall)\, s > 1$).

Conform propoziției 3 din paragraful II al anexei $L(s, \chi)$ e funcție continuă pe $(0, \infty)$ (deoarece $\chi \neq \chi_0$) și deci $L(1, \chi) = \lim_{\substack{s \to 1 \\ s>1}} L(s,\chi) \geq 0$, conform celor arătate mai sus. Am obținut deci că $L(1, \chi) \geq 0$. În cele ce urmează vom nota cu f următoarea funcție (definită pe $\mathbf{N}^*$ cu valori în $\mathbf{R}$) :

(4) $f(k) = \sum_{d|k} \chi(d)$ $(\forall)\, k \in \mathbf{N}^*$.

Dacă p este număr prim și l număr natural atunci:

$$f(p^l) = 1 + \chi(p) + \\ +\chi(p^2)+...+\chi(p^l) = \begin{cases} \\ 1, & \text{dacă } \chi(p)=0 \\ l+1, & \text{dacă } \chi(p)=1 \end{cases}$$

$$1+(-1)+1+(-1)... = \begin{cases} 0, & \text{dacă } \chi(p)=-1, 2 \nmid l \\ 1, & \text{dacă } \chi(p)=-1, 2 \mid l. \end{cases}$$

În concluzie:

$$(5) \begin{cases} f(p^l) \geq 0, \ (\forall) l \in \mathbf{N} \\ f(p^l) \geq 1, \ \text{dacă } l \in \mathbf{N},\ l \vdots 2 \end{cases}$$

Fie $a_1, a_2 \in \mathbf{N}^*$ astfel încât $(a_1, a_2) = 1$ și $d/a_1\ a_2$ $(d \in \mathbf{N}^*)$. Există atunci $d_1, d_2 \in \mathbf{N}^*$ astfel încât d_1/a_1, d_2/a_2 și $d = d_1 \cdot d_2$. Ținând cont de această observație deducem că:

$$(6)\ f(a_1a_2) = \sum_{d|a_1a_2} \chi(d) = \sum_{\substack{d_1|a_1 \\ d_2|a_2}} \chi(d_1)\chi(d_2) = \left(\sum_{d_1|a_1} \chi(d_1)\right)\left(\sum_{d_2|a_2} \chi(d_2)\right) = f(a_1) \cdot f(a_2)$$

$(\forall)\ a_1, a_2 \in \mathbf{N}, (a_1, a_2) = 1$.

Din formulele (5) și (6) rezultă că:

$$(7) \begin{cases} f(k) \geq 0, \ (\forall) k \in \mathbf{N}^* \\ f(k) \geq 1, \ \text{dacă } k \text{ este număr natural nenul, pătrat perfect.} \end{cases}$$

În continuare vom folosi următoarele notații:

$m = (4h)^6$, (am notat $h = \varphi(a)$)

$$z = \sum_{n=1}^{m} 2(m-n) f(n) \sum_{\substack{k \cdot l \leq m \\ k>0,\, l>0}} 2(m-kl)\chi(l).$$

Ținând cont că $f(k) \geq 0$ $(\forall)\, k \in \mathbf{N}^*$ și $f(k^2) \geq 1$, $(\forall)\, k \in \mathbf{N}^*$, rezultă că

$$z \geq \sum_{k=1}^{\sqrt{m}} 2(m-k^2) \geq \sum_{k=1}^{\frac{1}{2}\sqrt{m}} 2(m-k^2) \geq \sum_{k=1}^{\frac{1}{2}\sqrt{m}} 2\left(m - \frac{m}{4}\right) =$$

$$= \frac{\sqrt{m}}{2} \cdot 2 \cdot \frac{3m}{4} = \frac{3}{4} m\sqrt{m} = \frac{3}{4} \cdot (4h)^9.$$

Am obținut inegalitatea:

(8) $z \geq \frac{3}{4}(4h)^9$.

Putem scrie pe z sub următoarea formă:

$$(9)\quad \begin{cases} z = z_1 + z_2 \\ z_1 = \sum\limits_{k=1}^{\sqrt[3]{m}} \sum\limits_{\sqrt[3]{m^2} < l \leq \frac{m}{k}} 2(m-kl)\chi(l) \\ z_2 = \sum\limits_{l=1}^{\sqrt[3]{m^2}} \sum\limits_{0<k\leq \frac{m}{l}} 2(m-kl)\chi(l). \end{cases}$$

Aplicând propoziția 8 din paragraful II al anexei pentru

$$\gamma_l = \chi(l)\ ,\ \varepsilon_l = 2(m-kl)\ ,\ \nu \leq \frac{h}{2}$$

(această din urmă inegalitate se justifică folosind propoziția 2 din paragraful II al anexei) deducem că

$$\left| \sum_{\sqrt[3]{m^2} < l \leq \frac{m}{k}} 2(m-kl)\chi(l) \right| \leq \frac{h}{2} \cdot 2m$$

$\left(\text{deoarece } \varepsilon_l \leq 2m, (\forall)\sqrt[3]{m^2} < l \leq \frac{m}{k}\right)$.

Folosind această ultimă inegalitate obținem următoarea evaluare pentru z_1:

$$(10)\quad z_1 \leq \sum_{k=1}^{\sqrt[3]{m}} \left| \sum_{\sqrt[3]{m^2} < l \leq \frac{m}{k}} 2(m-kl)\chi(l) \right| \leq \sum_{k=1}^{\sqrt[3]{m}} hm = m^{\frac{4}{3}}h.$$

Aici, ca și în evaluările din formula (8), am folosit faptul că $\sqrt[3]{m}, \sqrt{m}$ și $\frac{1}{2}\sqrt{m}$ sunt numere naturale. Fie $0 \leq \alpha < 1$, astfel încât $\frac{m}{l} = \left[\frac{m}{l}\right] + \alpha$. Atunci

$$\sum_{0<k\leq \frac{m}{l}} 2(m-kl) = 2m \cdot \left[\frac{m}{l}\right] - 2l \cdot \frac{\left[\frac{m}{l}\right]\left(\left[\frac{m}{l}\right]+1\right)}{2} =$$

$$= 2m\left(\frac{m}{l} - \alpha\right) - l\left[\left(\frac{m}{l} - \alpha\right)^2 + \frac{m}{l} - \alpha\right] =$$

$$= \frac{2m^2}{l} - 2m\alpha - \frac{m^2}{l} + 2m\alpha - l\alpha^2 - m + l\alpha = \frac{m^2}{l} - m + l(\alpha - \alpha^2)$$

(am ținut cont mai sus de faptul că $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$). Deoarece $|\alpha - \alpha^2| \leq 1$ avem că

$$z_2 = \sum_{l=1}^{\sqrt[3]{m^2}} \chi(l) \left(\sum_{0<k\leq \frac{m}{l}} 2(m-kl) \right) =$$

$$= m^2 \sum_{l=1}^{\sqrt[3]{m^2}} \frac{\chi(l)}{l} - m \sum_{l=1}^{\sqrt[3]{m^2}} \chi(l) + \sum_{l=1}^{\sqrt[3]{m^2}} \chi(l)\, l(\alpha - \alpha^2) \leq$$

$$\leq m^2 \left(L(1,\chi) - \sum_{l=\sqrt[3]{m^2}+1}^{\infty} \frac{\chi(l)}{l} \right) + m \cdot \frac{h}{2} + \sqrt[3]{m^2} \cdot \sum_{l=1}^{\sqrt[3]{m^2}} 1 \quad \left(\left| \sum_{l=1}^{\sqrt[3]{m^2}} \chi(l) \right| \leq \frac{h}{2} \right.$$

conform propoziției 2 din paragraful II al anexei și datorită faptului că $\chi \neq \chi_0$). În cursul demonstrației propoziției 9 din paragraful II al anexei s-a arătat că $\left| \sum_{k=u}^{v} \frac{\chi(k)}{k^s} \right| \leq \frac{h}{2} \frac{1}{u^s}$ $(\forall)$ $v \geq u \geq 1$ $(v, u \in \mathbb{N})$, $s > 0$. Punând în această inegalitate $s = 1$, $u = \sqrt[3]{m^2} + 1$ și făcându-l pe v să tindă la infinit deducem că

$$\left| \sum_{l=\sqrt[3]{m^2}+1}^{\infty} \frac{\chi(l)}{l} \right| \leq \frac{h}{2\left(\sqrt[3]{m^2}+1\right)} \leq \frac{h}{2\sqrt[3]{m^2}}.$$

Din toate considerațiile anterioare obținem următoarele evaluări pentru z_2

$$z_2 \leq m^2 L(1,\chi) + m^2 \cdot \frac{h}{2\sqrt[3]{m^2}} + m^{\frac{4}{3}} + m \cdot \frac{h}{2} <$$

$$< m^2 L(1,\chi) + m^{\frac{4}{3}} \cdot h \left(\frac{1}{2} + 1 + \frac{1}{2} \right) = m^2 L(1,\chi) + 2m^{\frac{4}{3}} h$$

$(h = \varphi(a) > 1)$.

Aceasta împreună cu inegalitatea (10) ne conduce la concluzia:

(11) $z = z_1 + z_2 < m^2 \cdot L(1,\chi) + 3m^{\frac{4}{3}} h.$

Amintim că $z \geq \frac{3}{4}(4h)^9$ (conform inegalității (8)); deci $\frac{3}{4}(4h)^9 \leq z <$

$< m^2 L(1,\chi) + 3m^{\frac{4}{3}} h = m^2 L(1,\chi) + 3 \cdot (4h)^8 \cdot h = m^2 L(1,\chi) + \frac{3}{4}(4h)^9$. În acest moment enunțul propoziției este demonstrat.

Demonstrația teoremei lui Dirichlet

Știm că funcția logaritm (considerată ca funcție de variabilă complexă) este multiformă și de aceea trebuie considerată o ramură a sa. Alegerea se face în modul următor:

$$-\ln(1-z)=\sum_{n=1}^{\infty}\frac{z^n}{n},\ (\forall)\, z\in\mathbf{C},\ |z|<1.$$

Astfel pentru orice număr prim p și orice caracter numeric modulo a χ vom avea:

$$-\ln\left(1-\frac{\chi(p)}{p^s}\right)=\sum_{n=1}^{\infty}\frac{\chi(p)^n}{np^{sn}},\ (\forall)\, s\in\mathbf{R},\ s>1.$$

$\left|\frac{\chi(p)}{p^s}\right|\le\frac{1}{p^s}<\frac{1}{p}<1$ și deci are sens scrierea de mai sus.

Deoarece

$$L(s,\chi)=\prod_{p\text{-}prim}\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right)$$

(propoziția 4 din paragraful II al anexei) pentru $s>1$ și $L(s,\chi)\neq 0$ (propoziția 5 din paragraful II al anexei) tot pentru $s>1$ deducem că valoarea lui $\ln L(s,\chi)$ (referitor la ramura considerată) este egală cu:

$$(12)\ \ln L(s,\chi)=\sum_{p\text{-}prim}\sum_{n=1}^{\infty}\frac{\chi(p)^n}{np^{sn}}.$$

Dacă notez cu $R(s,\chi)=\sum_{p\text{-}prim}\sum_{n=2}^{\infty}\frac{\chi(p)^n}{np^{sn}}$, pentru $s>1$, atunci

$$|R(s,\chi)|\le\sum_{p\text{-}prim}\sum_{n=2}^{\infty}\frac{1}{np^{sn}}\le\sum_{p\text{-}prim}\sum_{n=2}^{\infty}\frac{1}{p^n}=$$

$$=\sum_{p\text{-}prim}\frac{1}{p^2}\cdot\frac{1}{1-\frac{1}{p}}=\sum_{p\text{-}prim}\frac{1}{p(p-1)}\le\sum_{n=1}^{\infty}\frac{1}{n(n+1)}=\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right)=1$$

(aceasta arată și faptul că seria care definește pe $R(s,\chi)$ este într-adevăr convergentă). Cum $\sum_{p\text{-}prim}\frac{\chi(p)}{p^s}$ este serie convergentă pentru orice $s>1$ atunci din formula (12) deducem că:

(13) $\ln L(s,\chi) = \sum_{p\text{-}prim} \frac{\chi(p)}{p^s} + R(s,\chi) \quad (\forall) s > 1.$

Deoarece seria $\sum_{p\text{-}prim} \frac{\chi(p)}{p^s}$ este absolut convergentă pentru $s > 1$ deducem că

$$\sum_{p\text{-}prim} \frac{\chi(p)}{p^s} = \sum_{\overline{c}\in G} \chi(\overline{c}) \cdot \left(\sum_{\substack{p\text{-}prim \\ \overline{p}=\overline{c}}} \frac{1}{p^s} \right),$$

(în stânga egalității precedente χ este caracter numeric modulo a, iar în dreapta egalității apare caracterul lui G corespunzător caracterului numeric modulo a).

Notând cu

$$f(s,\overline{c}) = \sum_{\substack{p\text{-}prim \\ \overline{p}=\overline{c}}} \frac{1}{p^s}$$

pentru $s > 1$, egalitatea (13) devine:

(14) $\ln L(s,\chi) = \sum_{\overline{c}\in G} \chi(\overline{c}) f(s,\overline{c}) + R(s,\chi).$

Înmulțind egalitatea (14) cu $\chi(\overline{b}^{-1})$ și apoi sumând egalitățile obținute după toate caracterele χ ale grupului G (care sunt în număr de $\varphi(a)$) rezultă că:

(15) $\sum_{\chi\in X} \chi(\overline{b}^{-1}) \ln L(s,\chi) = \sum_{\chi\in X} \sum_{\overline{c}\in G} \chi(\overline{b}^{-1}\overline{c}) f(s,\overline{c}) + \sum_{\chi\in X} \chi(\overline{b}^{-1}) R(s,\chi) =$

$= \sum_{\overline{c}\in G} \sum_{\chi\in X} \chi(\overline{b}^{-1}\overline{c}) f(s,\overline{c}) + R_{\overline{b}}(s)$, unde

$$R_{\overline{b}}(s) = \sum_{\chi\in X} \chi(\overline{b}^{-1}) R(s,\chi)$$

și X este grupul caracterelor grupului G (vezi paragraful I al anexei). Conform pro-poziției 5 din paragraful I al anexei $\sum_{\chi\in X} \chi(\overline{b}^{-1}\overline{c}) = 0$, dacă $\overline{b} \neq \overline{c}$ și $\sum_{\chi\in X} \chi(\overline{b}^{-1}\overline{c}) = \varphi(a) = |G|$, dacă $\overline{b} = \overline{c}$. În concluzie:

(16) $\ln L(s,\chi_0) + \sum_{\substack{\chi\neq\chi_0 \\ \chi\in X}} \chi(\overline{b}^{-1}) \ln L(s,\chi) = \varphi(a) f(s,\overline{b}) + R_{\overline{b}}(s).$

Să presupunem că există doar un număr finit de numere prime p de forma $ak + b$, cu $k \in \mathbf{N}$ (aceasta înseamnă că $\overline{p} = \overline{b}$). În această ipoteză

$$\lim_{\substack{s\to 1 \\ s>1}} f(s,\overline{b}) = \sum_{\substack{p-prim \\ \overline{p}=\overline{b}}} \frac{1}{p} < \infty.$$

Pe de altă parte

$$\left| R_{\overline{b}}(s) \right| \leq \sum_{\chi \in X} \left| R(s,\chi) \right| \leq \varphi(a)$$

(deoarece $|R(s,\chi)| \leq 1$) pentru orice $s > 1$. De aceea când trecem la limită cu $s \to 1$, $s > 1$ termenul $|R_{\overline{b}}(s)|$ rămâne mărginit. Conform propoziției 3 din paragraful II al anexei deducem că

$$\lim_{\substack{s \to 1 \\ s>1}} \sum_{\substack{\chi \neq \chi_0 \\ \chi \in X}} \chi(\overline{b}^{-1}) \ln L(s,\chi) = \sum_{\substack{\chi \neq \chi_0 \\ \chi \in X}} \chi(\overline{b}^{-1}) \ln L(1,\chi)$$

(aici s-a folosit în mod esențial propoziția demonstrată ceva mai înainte și care afirmă că $L(1,\chi) \neq 0$ dacă $\chi \neq \chi_0$). Din toate considerațiile precedente precum și din egalitatea (16) deducem că $\ln L(s, \chi_0)$ rămâne mărginită atunci când s tinde la 1 prin valori strict mai mari decât 1. De aici rezultă că $L(s, \chi_0)$ rămâne mărginită când $s \to 1$, $s > 1$. Însă (conform propoziției 4 din paragraful II al anexei)

$$L(s,\chi_0) = \prod_{p\text{-}prim} \left(\frac{1}{1 - \frac{\chi_0(p)}{p^s}} \right) = \prod_{\substack{p\text{-}prim \\ p \nmid a}} \left(\frac{1}{1 - \frac{1}{p^s}} \right) =$$

$$= \prod_{p\text{-}prim} \left(\frac{1}{1 - \frac{1}{p^s}} \right) \cdot \prod_{\substack{p\text{-}prim \\ p \mid a}} \left(1 - \frac{1}{p^s} \right) = \left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) \cdot \prod_{\substack{p\text{-}prim \\ p \mid a}} \left(1 - \frac{1}{p^s} \right)$$

(egalitatea $\prod_{p\text{-}prim} \left(\frac{1}{1 - \frac{1}{p^s}} \right) = \left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right)$ pentru $s > 1$ a fost demonstrată în observația ce urmează propoziția 4 citată mai sus). Cum

$$\lim_{\substack{s \to 1 \\ s>1}} \prod_{\substack{p\text{-}prim \\ p \mid a}} \left(1 - \frac{1}{p^s} \right) = \prod_{\substack{p\text{-}prim \\ p \mid a}} \left(1 - \frac{1}{p} \right)$$

și $\lim_{\substack{s \to 1 \\ s>1}} \left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) = \infty$ (deoarece seria armonică $\sum_{n=1}^{\infty} \frac{1}{n}$ este divergentă) deducem că $L(s, \chi_0)$ nu rămâne mărginită când $s \to 1$, $s > 1$.

Contradicția obținută ne arată că presupunerea făcută, aceea că există doar un număr finit de numere prime de forma $ak + b$, este falsă și deci enunțul teoremei lui Dirichlet a fost demonstrat.

ANEXĂ
(Teorema lui Dirichlet a progresiilor aritmetice)

I. **Definiție**: Se numește *caracter al grupului abelian finit* G un morfism al grupului G în grupul multiplicativ al corpului numerelor complexe. Dacă $\chi : (G, \bullet) \to (C^*, \bullet)$ este caracter al grupului abelian finit G atunci:

i) $\chi(xy) = \chi(x) \cdot \chi(y)$, $(\forall)\ x,y \in G$

ii) $\chi(e) = 1$, unde e este elementul neutru al grupului G. Se observă imediat că dat fiind un caracter χ al grupului G de cardinal n, atunci $\chi(x)$ este rădăcină de ordinul n a unității în $\mathbf{C}^*$ deoarece $(\chi(x))^n = \chi(x^n) = \chi(e) = 1$, $(\forall)\ x \in G$. Notând cu $X = \{\chi \mid \chi$ caracter al grupului $G\}$ atunci mulțimea X poate fi înzestrată cu o structură de grup în modul următor: pentru $\chi_1, \chi_2 \in X$ definim $\chi_1 \cdot \chi_2$ prin formula $(\chi_1 \cdot \chi_2)(x) = \chi_1(x) \cdot \chi_2(x)$, $(\forall)\ x \in G$. Este evident că $\chi_1 \cdot \chi_2$ aparține lui X, că operația definită mai sus este comutativă și asociativă, că elementul neutru pentru această operație este caracterul χ_0 (numit și caracterul unitate) definit prin formula $\chi_0(x) = 1$, $(\forall)\ x \in G$, și că inversul unui caracter χ (relativ la operația definită mai sus) este dat prin formula $\chi^{-1}(x) = \overline{\chi(x)}$, $(\forall)\ x \in G$ (conform unei observații anterioare $\chi(x)$ este rădăcină de ordinul n a unității în $\mathbf{C}$, $(\forall)\ \chi \in X$ și $x \in G$; deci în particular rezultă și faptul că $|\chi(x)| = 1$, $(\forall)\ \chi \in X$ și $x \in G$).

Propoziția 1: *Dacă G este grup abelian finit atunci grupul caracterelor lui G (adică X) este izomorf cu grupul G.*

Demonstrație: Dintr-o consecință a teoremei factorilor invarianți se știe că $G \simeq G_1 \times G_2 \times \ldots \times G_m$, unde $G_1, G_2, \ldots G_m$ sunt grupuri ciclice finite. Este deci suficient să demonstrăm enunțul în cazul în care $G = G_1 \times G_2 \times \ldots \times G_m$, $G_1, G_2, \ldots, G_m$ fiind grupuri ciclice finite. Dacă $\chi_1, \chi_2, \ldots, \chi_m$ sunt caractere ale grupurilor $G_1, G_2 \ldots G_m$ atunci funcția $\chi : G \to \mathbf{C}^*$ definită prin formula

$$\chi(x_1, x_2, \ldots x_m) = \prod_{i=1}^{m} \chi_i(x_i),\ (\forall)\ x_i \in G_i,$$

$i = \overline{1,m}$, este un caracter al grupului G. Reciproc dacă χ este un caracter al grupului G atunci notând prin χ_i funcția definită pe G_i cu valori complexe dată de formula $\chi_i(x_i) = \chi(e_1, e_2, \ldots e_{i-1}, x_i, e_{i+1}, \ldots e_m)$, unde e_j este elementul neutru al

grupului G_j, $(\forall) j = \overline{1,m}$, avem că χ_i este caracter al grupului G_i, $(\forall) i = \overline{1,m}$ și că $\chi(x_1, x_2, \ldots x_m) = \prod_{i=1}^{m} \chi_i(x_i)$. De aici rezultă că $X \simeq X_1 \times X_2 \times \ldots \times X_m$, unde X_i este grupul caracterelor grupului G_i, $(\forall) i = \overline{1,m}$. Pentru a demonstra enunțul este suficient deci să considerăm cazul când G este grup ciclic finit. Dacă $|G| = n$, α este un generator al grupului G și $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ atunci există un unic caracter $\chi \in X$ astfel încât $\chi(\alpha) = \varepsilon$ (într-adevăr, $(\forall) x \in G$ există $j \in \mathbf{N}$, $0 \leq j < n$ astfel încât $x = \alpha^j$ și deci

$$\chi(x) = \chi(\alpha)^j = \varepsilon^j = \cos \frac{2\pi j}{n} + i \sin \frac{2\pi j}{n}).$$

Notăm prin χ_0, χ, χ^2, χ^3,... χ^{n-1} caracterele lui X determinate unic prin condiția $\chi^j(\alpha) = \varepsilon^j$. Cum am observat la începutul acestui paragraf, pentru orice caracter $f \in X$ avem că $f(\alpha)$ este rădăcină de ordinul n a unității, deci există $j \in \mathbf{N}$, $0 \leq j \leq n-1$ astfel încât $f(\alpha) = \varepsilon^j$. Aceasta înseamnă ca $f = \chi^j$. Deci grupul X este ciclic de ordin n, generat de caracterul χ. Enunțul propoziției 1 este astfel demonstrat. În particular rezultă și că $|G| = |X| = n$.

Propoziția 2: *Fie G un grup abelian finit și H un subgrup al lui G. Atunci orice caracter al grupului H poate fi prelungit (în $|G : H|$ moduri) la un caracter al grupului G.*

Demonstrație: Dacă X este grupul caracterelor lui G și Y este grupul caracterelor lui H atunci definim aplicația $\varphi : X \to Y$ prin formula $\varphi(\chi) = \chi_{/H}$. Este evident că φ este morfism de grupuri și vom nota cu $A = \ker \varphi$. Avem că $\chi \in A$, dacă și numai dacă $\chi(h) = 1$, $(\forall) h \in H$ (dacă $\chi \in X$). Pentru fiecare caracter $\chi \in A$ putem construi un caracter $\overline{\chi}$ al grupului factor $\frac{G}{H}$ în modul următor: $\overline{\chi}(\overline{x}) = \chi(x)$, $(\forall) x \in G$ (am notat prin $\overline{x}$ clasa lui x modulo H). $\overline{\chi}$ este bine definit deoarece dat fiind $y \in G$ astfel încât $\overline{x} = \overline{y}$ atunci $x = yh$, cu $h \in H$ și deci $\chi(x) = \chi(yh) = \chi(h)\chi(y) = \chi(y)$, deoarece $\chi(h) = 1$, $(\forall) h \in H$ ($\chi \in A$). Este evident faptul că $\overline{\chi}$ este un caracter al grupului $\frac{G}{H}$. Reciproc, dacă ψ este un caracter al grupului factor $\frac{G}{H}$, atunci putem defini un caracter al grupului G, aparținând mulțimii A, prin formula $\chi(x) = \psi(\overline{x})$, $(\forall) x \in G$ ($\chi(h) = \psi(\overline{h}) = \psi(\overline{e}) = 1$, $(\forall) h \in H$, deci $\chi \in A$). Din considerațiile precedente deducem că A

este izomorf cu grupul caracterelor grupului factor $\frac{G}{H}$ și deci în particular (ținând cont de propoziția 1) $|A| = \left|\frac{G}{H}\right| = |G:H|$. Aplicând teorema fundamentală de izomorfism lui φ rezultă că $\frac{G}{A} \simeq Im\ \varphi$ și trecând la cardinale în relația precedentă obținem ca

$$|Im\ \varphi| = \left|\frac{G}{A}\right| = \frac{|G|}{|A|} = \frac{\cdot|G|}{|G:H|} = |H|$$

(s-a folosit în egalitățile precedente și teorema lui Lagrange). Cum $|Y| = |H|$ (conform propoziției 1) din cele de mai sus rezultă că φ este surjectivă. Afirmațiile din enunț sunt acum imediate.

Propoziția 3: *Dacă G este grup abelian finit și x este un element al lui G diferit de elementul neutru e, există* $\chi \in X$ *astfel încât* $\chi(x) \neq 1$.

Demonstrație: Fie H subgrupul ciclic generat de x în G. Avem că $|H| = m > 1$ (deoarece $x \neq e$). Fie χ_1 caracterul lui H unic determinat de condiția $\chi_1(x) = \cos\frac{2\pi}{m} + i \sin\frac{2\pi}{m}$; evident $\chi_1(x) \neq 1$. Aplicând propoziția 2 există un caracter χ al grupului G astfel încât $\chi_{H} = \chi_1$. Deci $\chi(x) = \chi_1(x) \neq 1$, ceea ce trebuia demonstrat.

Propoziția 4: *Fie un grup abelian finit G și* $\chi \in X$. *Notăm cu* $S = \sum_{x \in G} \chi(x)$. *Atunci* $S = |G|$ *dacă* $\chi = \chi_0$ *și* $S = 0$ *dacă* $\chi \neq \chi_0$.

Demonstrație: Dacă $\chi = \chi_0$ enunțul este evident. Dacă $\chi \neq \chi_0$, există $y \in G$ astfel încât $\chi(y) \neq 1$. Când x parcurge G atunci $x \cdot y$ parcurge mulțimea G, deci $S = \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x) \cdot \chi(y) = \chi(y) \cdot S$. Cum $\chi(y) \neq 1$ rezultă că $S = 0$.

Propoziția 5: *Dacă x este un element fixat al grupului abelian finit G și* $T = \sum_{\chi \in X} \chi(x)$ *atunci* $T = |G|$ *dacă* $x = e$ *și* $T = 0$ *dacă* $x \neq e$.

Demonstrație: Dacă $x = e$ enunțul este evident. Dacă $x \neq e$ atunci conform propoziției 3 există $\chi' \in X$ astfel încât $\chi'(x) \neq 1$. Când χ parcurge mulțimea X atunci $\chi\chi'$ parcurge mulțimea X, deci

$$T = \sum_{\chi \in X} \chi(x) = \sum_{\chi \in X} (\chi\chi')(x) = \sum_{\chi \in X} \chi(x) \cdot \chi'(x) = \chi'(x) \cdot T.$$

Cum $\chi'(x) \neq 1$, rezultă imediat că $T = 0$.

În cursul acestui capitol $G = \cup(\mathbf{Z}_a, \bullet)$ (grupul unităților inelului claselor de resturi modulo a), unde $a \in \mathbf{N}$, $a \geq 3$. Dacă χ este un caracter al grupului G vom nota cu $\chi^* : \mathbf{Z} \to \mathbf{C}$ funcția definită prin următoarele formule $\chi^*(m) =$

$= \chi(\overline{m})$, dacă $m \in \mathbf{Z}$, $(m, a) = 1$ (prin $\overline{m}$ înțelegem clasa modulo a numărului m) și $\chi^*(m) = 0$, dacă $m \in \mathbf{Z}$, $(m, a) \neq 1$. χ^* se numește caracter numeric modulo a și are următoarele proprietăți evidente:

i) $\chi^*(m) \neq 0 \Leftrightarrow (a, m) = 1$;

ii) $\chi^*(m_1) = \chi^*(m_2)$ dacă $m_1, m_2 \in \mathbf{Z}$, $m_1 \equiv m_2 \pmod{a}$;

iii) $\chi^*(m_1 m_2) = \chi^*(m_1) \cdot \chi^*(m_2)$, $(\forall)\, m_1, m_2 \in \mathbf{Z}$.

Pentru a nu complica scrierea în loc de χ^* vom folosi tot notația χ, în funcție de context fiind clar dacă e vorba de un caracter al grupului G sau de caracterul numeric corespunzător.

II. Propoziția 1: *Fie* $(a_n)_{n \in \mathbf{N}}$ *un șir de numere complexe cu proprietatea că există* $c \in \mathbf{R}_+$, *astfel încât* $|A_n| \leq c$, $(\forall)\, n \in \mathbf{N}^*$, *unde* $A_n = \sum_{k=1}^{n} a_k$ $(\forall)\, n \in \mathbf{N}^*$.

Pentru fiecare $s > 0$ *seria* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *este convergentă și dacă notăm cu* $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *atunci* f *este o funcție continuă pe intervalul* $(0, \infty)$.

Demonstrație: Fie σ un număr real strict pozitiv; $(\forall)\, \varepsilon > 0$ există $n_0 \in \mathbf{N}^*$ astfel încât dacă $n \in \mathbf{N}$, $n \geq n_0$ atunci $\frac{1}{n^\sigma} < \varepsilon$. Dacă $s \geq \sigma$ și $n \in \mathbf{N}$, $n \geq n_0$ atunci $\frac{1}{n^s} \leq \frac{1}{n^\sigma} < \varepsilon$. Fie M și N numere naturale astfel încât $M > N > n_0$. Avem că $\sum_{k=N}^{M} \frac{a_k}{k^s} = \sum_{k=N}^{M} \frac{A_k - A_{k-1}}{k^s} = \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N-1}^{M-1} \frac{A_k}{(k+1)^s} = \sum_{k=N}^{M-1} A_k \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{A_M}{M^s} - \frac{A_{N-1}}{N^s}$, pentru $(\forall)\, s \in \mathbf{R}_+^*$. Dacă s e număr real satisfăcând inegalitatea $s \geq \sigma$ din ipoteză precum și din considerațiile anterioare deducem că are loc următoarea evaluare

$$\left| \sum_{k=N}^{M} \frac{a_k}{k^s} \right| \leq \sum_{k=N}^{M-1} c \left(\frac{1}{k^s} - \frac{1}{(k+1)^s} \right) + \frac{c}{M^s} + \frac{c}{N^s} = \frac{2c}{N^s} < \frac{2c}{n_o^\sigma} < 2c\varepsilon .$$

De aici rezultă imediat că seria $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ este convergentă pentru orice $s > 0$. De asemenea mai rezultă și faptul că convergența este uniformă pe intervalul $[\sigma, +\infty)$ $(\forall)\, \sigma > 0$. Deoarece funcțiile $\sum_{k=1}^{n} \frac{a_k}{k^s}$ sunt continue pe $(0, \infty)$ $(\forall)\, n \in \mathbf{N}^*$, din cele de mai sus rezultă că f este funcție continuă pe $(0, \infty)$.

Propoziția 2: *Dacă* χ *e caracter numeric modulo* a $(a \in \mathbf{N}, a \geq 3)$, *iar* u *și* v *sunt numere naturale astfel încât* $v \geq u \geq 1$ *atunci* $\left| \sum_{k=u}^{v} \chi(k) \right| \leq \frac{\varphi(a)}{2}$ *în cazul în care* $\chi \neq \chi_0$.

Demonstrație: Deoarece $a \in \mathbf{N}$, $a \geq 3$ rezultă că $2 \mid \varphi(a)$ și deci $\frac{\varphi(a)}{2}$ este număr natural. Folosind propoziția 4 din paragraful precedent deducem că $\sum_{k=\alpha-a+1}^{\alpha} \chi(k) = 0$ pentru orice număr natural $\alpha \geq a$ (se mai ține cont și de faptul că $\chi(\beta) = 0$ pentru orice număr întreg β care nu e prim cu a).

Această observație arată că este suficient să demonstrăm enunțul propoziției în cazul în care $v - u + 1 \leq a$. În această ipoteză cel mult $\varphi(a)$ termeni din șirul $\chi(u), \chi(u+1), ..., \chi(v)$ sunt nenuli.

Dacă $\varphi(k) \neq 0$ pentru un $k \in \mathbf{Z}$ atunci știm că $|\chi(k)| = 1$. Ținând cont de aceste considerații rezultă, în cazul în care cel mult $\frac{\varphi(a)}{2}$ termeni sunt nenuli (dintre numerele $\chi(u), \chi(u+1),... \chi(v)$), că $\left|\sum_{k=u}^{v} \chi(k)\right| \leq \frac{\varphi(a)}{2}$. Dacă numărul de termeni nenuli din șirul $\chi(u), \chi(u+1),.... \chi(v)$ este mai mare strict decât $\frac{\varphi(a)}{2}$ atunci numărul de termeni nenuli din șirul

$$\chi(v+1), \chi(v+2),.... \chi(u+a-1)$$

este mai mic strict decât $\frac{\varphi(a)}{2}$. În acest caz avem că

$$\left|\sum_{k=u}^{v} \chi(k)\right| = \left|\sum_{k=u}^{u+a-1} \chi(k) - \sum_{k=v+1}^{u+a-1} \chi(k)\right| = \left|\sum_{k=v+1}^{u+a-1} \chi(k)\right| < \frac{\varphi(a)}{2}$$

(am ținut cont încă o dată de faptul că $\sum_{k=u}^{u+a-1} \chi(k) = 0$). Enunțul propoziției 2 este astfel demonstrat.

Propoziția 3: *Dacă χ este un caracter numeric modulo a diferit de χ_0 (caracterul unitate) atunci $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ este o serie convergentă pentru orice număr real s strict pozitiv. Notând cu $L(s, \chi)$ suma seriei precedente pentru orice $s > 0$, atunci $L(s, \chi)$ este funcție continuă pe intervalul $(0, \infty)$.*

Demonstrație: Aplicăm propoziția 1 din acest paragraf pentru $a_n = \chi(n)$, $(\forall)\, n \in \mathbf{N}^*$, $c = \frac{\varphi(a)}{2}$ și enunțul propoziției 3 este astfel demonstrat (conform propoziției 2 $|A_n| \leq \frac{\varphi(a)}{2}$, $(\forall)\, n \in \mathbf{N}^*$, unde $A_n = \sum_{k=1}^{n} a_k$; aici ca și mai sus $a \in \mathbf{N}$, $a \geq 3$).

Observație: $\sum_{n=1}^{\infty}\frac{\chi_0(n)}{n^s}$ *este serie convergentă pentru orice* $s > 1$. *Dacă se notează cu* $L(s, \chi_0)$ *suma seriei precedente pentru* $s > 1$ *atunci* $L(s, \chi_0)$ *este funcție continuă pe intervalul* $(1, \infty)$. *Dacă* s_0 *este un număr real fixat,* $s_0 > 1$ *atunci*

$$\sum_{n=1}^{\infty}\left|\frac{\chi_0(n)}{n^s}\right| \le \sum_{n=1}^{\infty}\frac{1}{n^s} \le \sum_{n=1}^{\infty}\frac{1}{n^{s_0}}$$

$(\forall)\ s \in \mathbf{R}$, $s \ge s_0$. Cum seria $\sum_{n=1}^{\infty}\frac{1}{n^{s_0}}$ este convergentă deducem că $\sum_{n=1}^{\infty}\frac{\chi_0(n)}{n^s}$ converge uniform pe intervalul $[s_0, +\infty)$ și cum $\sum_{n=1}^{k}\frac{\chi_0(n)}{n^s}$ este funcție continuă de s pe $[s_0, \infty)$, $(\forall)\ k \in \mathbf{N}^*$ rezultă în final că $L(s, \chi_0)$ este funcție continuă pe $[s_0, +\infty)$, $(\forall)\ s_0 > 1$. Afirmația enunțată în observație este astfel demonstrată.

Propoziția 4: *Cu notațiile precedente* $L(s, \chi) = \prod_{p\text{-}prim}\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right)$ *pentru orice număr real* $s > 1$ *și* χ *caracter numeric modulo* a.

Demonstrație: Notăm cu p_i al i - lea număr prim. Fie $\varepsilon > 0$ și $s > 1$. Există atunci $r_0 \in \mathbf{N}^*$ astfel încât $\sum_{n=p_{r_0}+1}^{\infty}\frac{1}{n^s} < \varepsilon$. Deoarece $\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$, $(\forall)\ z \in \mathbf{C}$, $|z| < 1$ (convergența fiind absolută) și

$$\left|\frac{\chi(p)}{p^s}\right| \le \frac{1}{p^s} < \frac{1}{p} < 1$$

pentru orice număr prim, rezultă că

$$\prod_{i=1}^{r}\left(\frac{1}{1-\frac{\chi(p_i)}{p_i^s}}\right) = \prod_{i=1}^{r}\left(\sum_{m_i=0}^{\infty}\frac{\chi(p_i^{m_i})}{p_i^{m_i s}}\right) = \sum_{\substack{m_i \in \mathbf{N} \\ i=\overline{1,r}}}\frac{\chi(p_1^{m_1}p_2^{m_2}\dots p_r^{m_r})}{(p_1^{m_1}p_2^{m_2}\dots p_r^{m_r})^s}$$

pentru $(\forall)\ r \in \mathbf{N}^*$.

Pentru $r \in \mathbf{N}^*$, $r \ge r_0$ deducem, din cele de mai sus, că:

$$\left|L(s,\chi) - \prod_{i=1}^{r}\left(\frac{1}{1-\frac{\chi(p_i)}{p_i^s}}\right)\right| \le \sum_{n=p_{r_0+1}}^{\infty}\frac{1}{n^s} < \varepsilon$$

(am ținut cont de faptul că orice divizor prim al unui număr natural $n \leq p_{r_0}$ trebuie să fie de forma p_j cu $j \leq r_0$). Enunțul propoziției 4 este astfel demonstrat.

Observație: *Folosind același raționament ca și în propoziția 4 se arată că*

$$\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p-prim}\left(\frac{1}{1-\frac{1}{p^s}}\right)$$

pentru orice s > 1.

Propoziția 5: $L(s,\chi) \neq 0$ *pentru orice caracter numeric modulo a și* $s > 1$.

Demonstrație: Deoarece $|\mu(n)\chi(n)| \leq 1$ $(\forall)$ $n \in \mathbf{N}^*$ (unde μ este funcția lui Möbius) atunci seria $\sum_{n=1}^{\infty}\frac{\mu(n)\chi(n)}{n^s}$ converge absolut pentru orice $s > 1$. Deoarece $\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ converge absolut pentru s > 1 obținem că

$$L(s,\chi)\cdot\left(\sum_{n=1}^{\infty}\frac{\mu(n)\chi(n)}{n^s}\right)=\sum_{m,n\in\mathbf{N}^*}\frac{\mu(n)\chi(mn)}{(mn)^s}=\sum_{k=1}^{\infty}\frac{\chi(k)}{k^s}\left(\sum_{d|k}\mu(d)\right)=1$$

(conform lemei din paragraful II al anexei teoremei elementului prim $\sum_{d|k}\mu(d)$ este egală cu 1, dacă $k = 1$ și este egală cu 0, dacă $k \in \mathbf{N}$, $k > 1$). De aici rezultă imediat enunțul propoziției 5.

Propoziția 6: $(1-\eta)^3 \cdot |1-\eta e^{i\nu}|^4 \cdot |1-\eta e^{2i\nu}|^2 < 1$ $(\forall)$ $\nu \in \mathbf{R}$ *și* $0 < \eta < 1$ ($e^{i\nu} = \cos\nu + i\sin\nu$, $(\forall)$ $\nu \in \mathbf{R}$; $i \in \mathbf{C}$, $i^2 = -1$).

Demonstrație: Deoarece $\alpha^2 \geq 0$, $(\forall)$ $\alpha \in \mathbf{R}$, deducem că

$$2\cos\nu + \cos 2\nu = 2\cos\nu + 2\cos^2\nu - 1 = 2\left(\cos\nu + \frac{1}{2}\right)^2 - \frac{3}{2} \geq -\frac{3}{2},$$

$(\forall)$ $\nu \in \mathbf{R}$. Deoarece $|1-\eta e^{i\nu}| = \sqrt{(1-\eta\cos\nu)^2+\eta^2\sin^2\nu} = \sqrt{1-2\eta\cos\nu+\eta^2}$, $(\forall)$ $\nu \in \mathbf{R}$, deducem că

$$|1-\eta e^{i\nu}|^4 \cdot |1-\eta e^{2i\nu}|^2 =$$

$$= (1-2\eta\cos\nu+\eta^2)\cdot(1-2\eta\cos\nu+\eta^2)\cdot(1-2\eta\cos 2\nu+\eta^2) \leq$$

$$\leq\left(\frac{1-2\eta\cos\nu+\eta^2+1-2\eta\cos\nu+\eta^2+1-2\eta\cos 2\nu+\eta^2}{3}\right)^3 =$$

$$=\left[1-\frac{2}{3}\eta(2\cos\nu+\cos 2\nu)+\eta^2\right]^3$$

(s-a ținut cont mai sus de inegalitatea mediilor: $\sqrt[3]{abc} \le \frac{a+b+c}{3}$, $(\forall)\ a, b, c \in \mathbf{R}_+$, care se mai scrie și sub forma

$$abc \le \left(\frac{a+b+c}{3}\right)^3.$$

La începutul demonstrației s-a arătat că

$$-\frac{2}{3}(2\cos v + \cos 2v) \le 1 \text{ și deci } |1-\eta e^{iv}|^4 \cdot |1-\eta e^{2iv}|^2 \le$$

$$\le (1+\eta+\eta^2)^3 < \left(\frac{1}{1-\eta}\right)^3$$

conform ipotezei $0 < \eta < 1$. Enunțul propoziției 6 este astfel demonstrat.

Propoziția 7: *$L(s, \chi_0)^3 \cdot |L(s, \chi)|^4\ |L(s, \chi^2)|^2 \ge 1$ pentru $s > 1$ și χ caracter numeric modulo a.*

Demonstrație: Dacă p este un număr prim care nu-l divide pe a, atunci $\chi(p) \ne 0$ și deci $\chi(p) = e^{vi}$, cu $v \in \mathbf{R}$. Dacă notăm cu $\eta = \frac{1}{p^s}$, atunci $0 < \eta < 1$ și aplicând propoziția precedentă deducem că:

$$\left(1-\frac{\chi_0(p)}{p^s}\right)^3 \cdot \left|1-\frac{\chi(p)}{p^s}\right|^4 \cdot \left|1-\frac{\chi^2(p)}{p^s}\right|^2 \le 1 \quad \left(\chi_0(p)=1\right).$$

Dacă p este un număr prim care divide pe a atunci inegalitatea de mai sus are loc deoarece $\chi_0(p) = \chi(p) = 0$. Înmulțind inegalitățile precedente pentru toate numerele prime p, obținem enunțul ținând cont de propoziția 4 din acest paragraf.

Propoziția 8: *Fie $u \le v$ două numere naturale și γ_k niște numere complexe, unde k este număr natural satisfăcând inegalitățile $u \le k \le v$. Fie de asemenea numerele reale $\varepsilon_u, \varepsilon_{u+1}, \ldots \varepsilon_v$ care satisfac inegalitățile $\varepsilon_u \ge \varepsilon_{u+1} \ge \ldots \ge \varepsilon_v \ge 0$. Notăm cu $R(k) = \sum_{k'=u}^{k} \gamma_{k'}$ pentru orice $k \in \mathbf{N}$, $u \le k \le v$ și cu $v = \max_{u \le k \le v} |R(k)|$. Atunci* $\left|\sum_{k=u}^{v} \varepsilon_k \gamma_k\right| \le \varepsilon_u \cdot v$.

Demonstrație: Notăm $R(u-1) = 0$. Atunci

$$\sum_{k=u}^{v} \varepsilon_k \gamma_k = \sum_{k=u}^{v} \varepsilon_k \big(R(k) - R(k-1)\big) =$$

$$= \sum_{k=u}^{v} \varepsilon_k R(k) - \sum_{k=u-1}^{v-1} \varepsilon_{k+1} R(k) =$$

$$= \sum_{k=u}^{v-1} R(k)\ (\varepsilon_k - \varepsilon_{k+1}) + \varepsilon_v R(v) - \varepsilon_u R(u-1) =$$

$$= \sum_{k=u}^{v-1} R(k)(\varepsilon_k - \varepsilon_{k+1}) + \varepsilon_v R(v).$$

Ținând cont de enunț deducem că

$$\left|\sum_{k=u}^{v}\varepsilon_k\gamma_k\right| \le \sum_{k=u}^{v-1}\nu(\varepsilon_k-\varepsilon_{k+1})+\nu\varepsilon_v=\nu\varepsilon_u;$$

ceea ce trebuia demonstrat.

Propoziția 9: $|L(s,\chi)| \le \frac{\varphi(a)}{2}$ *pentru orice* $s > 1$ *și* χ *caracter numeric modulo a diferit de* χ_0 ($a \in \mathbf{N}$, $a \ge 3$).

Demonstrație: Aplicăm propoziția precedentă pentru $\gamma_k = \chi(k)$, $(\forall)\, k \in \mathbf{N}$, $u \le k \le v$, $u \ge 1$, $\varepsilon_k = \frac{1}{k^s}$, $(\forall)\, k \in \mathbf{N}$, $u \le k \le v$, ținând cont și de propoziția 2 din acest paragraf care afirmă că $\left|\sum_{k=u_1}^{v_1}\chi(k)\right| \le \frac{\varphi(a)}{2}$, $(\forall)\, u_1 \le v_1$, $u_1, v_1 \in \mathbf{N}^*$ (consecință a acestui fapt: $\nu \le \frac{\varphi(a)}{2}$). Rezultă că

$$\left|\sum_{k=u}^{v}\frac{\chi(k)}{k^s}\right| \le \frac{\varphi(a)}{2}\cdot\frac{1}{u^s},$$

$(\forall)\, v \ge u \ge 1$ ($v, u \in \mathbf{N}$). Dacă în această ultimă inegalitate punem $u = 1$ și facem pe v să tindă la $+\infty$, obținem enunțul. De fapt enunțul are loc pentru orice $s > 0$.

Propoziția 10: $L(s, \chi)$ *este funcție derivabilă pe intervalul* $(1, \infty)$ *pentru orice* χ *caracter numeric modulo a. Are loc următoarea formulă*

$$L'(s,\chi) = -\sum_{k=1}^{\infty}\frac{\chi(k)\ln k}{k^s}$$

(*dacă* $\chi \ne \chi_0$ *atunci* $L(s, \chi)$ *e funcție derivabilă pe* $(0, \infty)$ *și are loc formula de mai sus*). *În plus dacă* $\chi \ne \chi_0$ *și* $s \ge 1$ *atunci* $|L'(s, \chi)| < \varphi(a)$.

Demonstrație: Fie $\varepsilon > 0$ și $s \ge 1 + \varepsilon$ deci

$$\left|\frac{\chi(k)\ln k}{k^s}\right| \le \frac{\ln k}{k^{1+\varepsilon}},$$

$(\forall)\, k \in \mathbf{N}^*$. Deoarece $\lim_{k\to\infty}\frac{\ln k}{k^{\frac{\varepsilon}{2}}} = 0$, pentru un $\alpha > 0$ fixat există $k_0 \in \mathbf{N}^*$ astfel încât $\left|\frac{\ln k}{k^{\frac{\varepsilon}{2}}}\right| \le \alpha$, pentru $(\forall)\, k \in \mathbf{N}$, $k \ge k_0$. Avem că

$$\sum_{k=1}^{\infty}\left|\frac{\chi(k)\ln k}{k^s}\right| \le \sum_{k=1}^{k_0}\frac{\ln k}{k^{1+\varepsilon}} + \alpha\sum_{k=k_0+1}^{\infty}\frac{1}{k^{1+\frac{\varepsilon}{2}}}.$$

Cum $\sum_{k=k_0+1}^{\infty} \frac{1}{k^{1+\frac{\varepsilon}{2}}}$ este convergentă deducem că șirul de funcții g_n converge uniform pe $[1+\varepsilon, \infty)$, $(\forall)\ \varepsilon > 0$, unde

$$g_n(s) = -\sum_{k=1}^{n} \frac{\chi(k)\ln k}{k^s}.$$

Deoarece $g_n(s) = f_n'(s)$, unde $f_n(s) = \sum_{k=1}^{n} \frac{\chi(k)}{k^s}$, și $\lim_{n\to\infty} f_n(s) = L(s,\chi)$, $(\forall)\ s > 1$, rezultă că $L(s, \chi)$ e derivabilă pe intervalul $(1, \infty)$ și

$$L'(s,\chi) = -\sum_{k=1}^{\infty} \frac{\chi(k)\ln k}{k^s}.$$

Pentru a justifica această afirmație vezi Gh. Siretchi *Calcul diferențial și integral*, volumul I, Editura Științifică și Enciclopedică, București, 1985, pagina 416, teorema 12.1.14. Acest rezultat clasic de analiză afirmă că fiind dat un șir de funcții derivabile f_n definite pe un interval I astfel încât $(f_n(y))_{n\in\mathbf{N}}$ este șir convergent măcar pentru un punct $y \in I$ și astfel încât șirul derivatelor f_n' converge uniform pe I la o funcție g atunci există o funcție f definită pe I astfel încât $f' = g$ și f_n converge uniform la f pe I. Deși în locul citat funcțiile au valori numere reale, enunțul este adevărat pentru funcții cu valori complexe (definite însă pe submulțimi ale lui **R**); pentru aceasta în raționamentele făcute este suficient de a considera modulul de numere complexe și de a utiliza inegalitatea lui Lagrange în loc de teorema clasică a lui Lagrange.

Fie $h : [3, +\infty) \to \mathbf{R}$ funcția definită prin formula: $h(x) = \frac{\ln x}{x^s}$ ($s \in \mathbf{R}$, $s \geq 1$). Evident h este funcție derivabilă pe $[3, +\infty)$ și

$$h'(x) = \frac{x^{s-1} - sx^{s-1}\cdot \ln x}{x^{2s}} = \frac{1 - s\ln x}{x^{s+1}},$$

$(\forall)\ x \geq 3$. Pentru $x \geq 3$ avem că $1 - s\ln x \leq 1 - s\ln 3 \leq 1 - s \leq 0$; deci h este funcție descrescătoare pe $[3, +\infty)$. Rezultă că

$$\frac{\ln u}{u^s} \geq \frac{\ln v}{v^s},$$

$(\forall)\ v \geq u \geq 3$. Dacă $\chi \neq \chi_0$ aplicăm propoziția 8 pentru $v \geq u \geq 3$ ($v, u \in \mathbf{N}$), $\gamma_k = \chi(k)$ (conform propoziției 2 din acest paragraf $\nu \leq \frac{\varphi(a)}{2}$) și $\varepsilon_k = \frac{\ln k}{k^s}$, $(\forall)\ u \leq k \leq v$, $k \in \mathbf{N}$. Obținem că

$$\left|\sum_{k=u}^{v} \frac{\chi(k)\ln k}{k^s}\right| \leq \frac{\varphi(a)}{2}\cdot\frac{\ln u}{u^s} \leq \frac{\varphi(a)}{2}\cdot\frac{\ln u}{u}.$$

Atunci

$$\left|\sum_{k=u}^{\infty}\frac{\chi(k)\ln k}{k^s}\right| \le \frac{\ln 2}{2^s}+\frac{\varphi(a)}{2}\cdot\frac{\ln 3}{3}<\frac{1}{2}+\frac{\varphi(a)}{2}\cdot\frac{\ln e^2}{3}<\frac{1}{2}+\frac{\varphi(a)}{2}\le\varphi(a)$$

(s-a procedat la o trecere la limită cu $v\to+\infty$ în inegalitatea

$$\left|\sum_{k=u}^{v}\frac{\chi(k)\ln k}{k^s}\right| \le \frac{\varphi(a)}{2}\,\frac{\ln u}{u}$$

și la înlocuirea $u = 3$). Pentru $s \ge s_0 > 0$ avem că

$$\left|\sum_{k=u}^{v}\frac{\chi(k)\ln k}{k^s}\right| \le \frac{\varphi(a)}{2}\,\frac{\ln u}{u^{s_0}}$$

dacă $u \ge e^{\frac{1}{s_0}}$; aceasta semnifică convergența seriei $\left(-\sum_{k=1}^{\infty}\frac{\chi(k)\ln k}{k^s}\right)$, convergență uniformă pe $[s_o, +\infty)$. Folosind același argument pe care l-am menționat mai sus deducem că $L(s, \chi)$ este funcție derivabilă pe $(0, \infty)$ (dacă $\chi \ne \chi_0$) și are loc formula

$$L'(s,\chi)=-\sum_{k=1}^{\infty}\frac{\chi(k)\ln k}{k^s}.$$

Enunțul propoziției 10 este astfel demonstrat.

Observație: *Argumentul care se dă, de obicei, pentru a arăta că $L(s, \chi)$ e derivabilă pe* $(1,\infty)$ (*respectiv pe* $(0,\infty)$ *dacă* $\chi \ne \chi_0$) *și că*

$$L'(s,\chi)=-\sum_{k=1}^{\infty}\frac{\chi(k)\ln k}{k^s}$$

este teorema lui Weierstrass asupra șirurilor uniform convergente de funcții analitice definite pe un anume domeniu din **C** (*domeniu înseamnă mulțime deschisă și conexă*). Pentru aceasta trebuie arătat în prealabil că $\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ converge pentru orice $s \in C$, Re $s > 1$ (partea reală a lui s este strict mai mare decât 1). Dacă $\chi \ne \chi_0$ seria precedentă converge pentru orice $s \in \mathbf{C}$, Re $s > 0$. Mai trebuie arătat că convergența este uniformă pe mulțime $\{s \in \mathbf{C} \mid \text{Re } s > \sigma\}$ $(\forall)\ \sigma \in \mathbf{R}$, $\sigma > 1$. Dacă $\chi \ne \chi_0$ atunci convergența este uniformă pe mulțimea $\{s \in \mathbf{C} \mid \text{Re } s > \sigma\}$ $(\forall)\ \sigma \in \mathbf{R}$, $\sigma > 0$.

Inegalitatea

$$\left|\sum_{k=u}^{v}\frac{\chi(k)\ln k}{k^s}\right| \le \frac{\varphi(a)}{2}\,\frac{\ln u}{u^s} \le \frac{\varphi(a)}{2}\,\frac{\ln u}{u^{s_0}}$$

pentru $s \ge s_0 > 0$, $\chi \ne \chi_0$ și $u \ge e^{\frac{1}{s_0}}$, menționată mai sus, se justifică folosind din nou propoziția 8 din acest paragraf și faptul că funcția $h(x) = \frac{\ln x}{x^s}$ este descrescătoare pe intervalul $\left[e^{\frac{1}{s_0}}; +\infty\right]$.

TEOREMA LUI BRUN

Introducere

Scopul acestui capitol este demonstrarea unui rezultat aparținând lui Brun care afirmă că

$$\sum_{p \in G} \frac{1}{p} < \infty,$$

unde G este mulțimea numerelor prime p pentru care și $p + 2$ e număr prim (o pereche de numere prime p și $p + 2$ se numește pereche de numere prime gemene).

Deci sau G este o mulțime finită, sau $\sum_{p \in G} \frac{1}{p}$ *este o serie convergentă în cazul în care G este mulțime infinită.* Acest rezultat a fost demonstrat de V. Brun în articolul *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\ldots$ *où les dénominateurs sont* „nombres premiers jumeaux" *est convergente ou finie* din Bull. Sc. Math, volum 43 din 1919, paginile 100-104 și 124-128. Demonstrația din acest capitol urmărește soluția dată de Landau în *Vorlesungen über Zahlentheorie*, volumul I (*Aus der elementaren und additiven Zahlentheorie*), paginile 71-78 (*Der Brunsche Satz über Prim-zahlzwillinge*).

Nu se știe până acum dacă mulțimea G este finită sau infinită.

În finalul capitolului se dă și o demonstrație pentru faptul că $\sum_{p\text{-}prim} \frac{1}{p}$ este o serie divergentă.

Demonstrația teoremei lui Brun

Teorema 1. (B r u n). *Dacă notăm cu*

$$G = \{p \in \mathbf{N} \mid p \text{ număr prim și } p + 2 \text{ e număr prim}\}$$

atunci seria $\sum_{p \in G} \frac{1}{p}$ *este convergentă.*

Pentru a demonstra teorema 1 avem nevoie de următorul rezultat:

Teorema 2: *Dacă notăm cu $P(x)$ numărul de numere prime $p \le x$ pentru care și $p + 2$ este număr prim atunci există o constantă strict pozitivă c_1 astfel încât:*

$$P(x) < c_1 \frac{x}{\ln^2 x} (\ln \ln x)^2 \quad (\forall) x \ge 3.$$

Demonstrația teoremei 2: Fie $x > 5$ și y un număr real satisfăcând inegalitatea $5 \le y < x$ unde y va fi precizat ulterior ca funcție de x. Este evidentă următoarea inegalitate:

(1) $P(x) \le y + Q(x)$,

unde prin $Q(x)$ s-a notat numărul de numere naturale n pentru care $y < n \le x$, n și $n + 2$ fiind numere prime. Dacă notăm prin $r = \pi(y)$ (adică numărul de numere prime mai mici sau egale cu y) atunci $r \ge 3$ deoarece $y \ge 5$. Vom nota deasemenea cu $p_2, p_3, ..., p_r$ numerele prime impare mai mici sau egale cu $y (p_1 = 2)$ și cu $A(x)$ numărul de numere naturale n pentru care $0 < n \le x$, $n \not\equiv 0 \pmod{p_h}$ și $n \not\equiv -2 \pmod{p_h}$ $(\forall)$ $h = \overline{2,r}$. Are loc inegalitatea:

(2) $Q(x) \le A(x)$.

Într-adevăr dacă $n \in \mathbf{N}$ este un număr natural numărat de $Q(x)$ atunci $y < n \le x$, n și $n+2$ fiind numere prime. De aici rezultă imediat că $n \not\equiv 0 \pmod{p_h}$ și $n \not\equiv -2 \pmod{p_h}$ $(\forall)$ $h = \overline{2,r}$ (deoarece n și $n + 2$ sunt numere prime mai mari strict decât orice p_h, $h = \overline{2,r}$). Inegalitatea 2 este astfel demonstrată. Inegalitățile (1) și (2) furnizează evaluarea:

(3) $P(x) \le y + A(x)$.

Pentru orice $n \in \mathbf{N}^*$ notăm cu $\Omega(n) = \sum_{i=1}^{s} \alpha_i$, unde $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots q_s^{\alpha_s}$; $q_1, q_2, ..., q_s$ fiind numere prime distincte (Ω este într-un anume fel „lungimea" lui n). Avem că $\Omega(n \cdot m) = \Omega(n) + \Omega(m)$, $(\forall)$ $n, m \in \mathbf{N}^*$. De asemenea vom nota cu $B(d, x)$, pentru fiecare $d \in \mathbf{N}^*$, impar și liber de pătrate, numărul de numere naturale strict pozitive n pentru care $n \le x$ și în plus pentru fiecare număr prim $p|d$ este satisfăcută una din următoarele condiții: $n \equiv 0 \pmod{p}$ sau $n \equiv -2 \pmod{p}$. Este clar că $B(1, x) = [x]$. Pentru fiecare $d \in \mathbf{N}^*$, impar și liber de pătrate, deducem, folosind lema chineză a resturilor demonstrată în paragraful II al anexei teoremei lui Gauss, că sistemul

(4) $n \equiv \alpha_p \pmod{p}$ $(\forall)$ p - prim, $p \mid d$

are soluții oricare ar fi $\alpha_p \in \mathbf{Z}$ (sistemul a fost considerat în necunoscuta n). În particular acest lucru este adevărat pentru $\alpha_p = 0$ sau $\alpha_p = -2$. Avem $2^{\Omega(d)}$ sisteme

de forma (4) în care $\alpha_p = 0$ sau $\alpha_p = -2$ oricare ar fi p un număr prim care divide pe d. Ținând cont de modul de definiție al numărului $B(d, x)$, de observațiile anterioare precum și de propoziția 3 din paragraful II al anexei rezultă că:

$$(5) \quad |B(d, x) - 2^{\Omega(d)} \frac{x}{d}| < 2^{\Omega(d)}.$$

Notând cu

$$A = \{n \in \mathbf{N}^* \mid n \le [x],\ n \not\equiv 0 \pmod{p_h} \text{ și } n \not\equiv -2 \pmod{p_h}\ (\forall)\ h = \overline{2,r}\},$$

$$B_{p_h} = \{n \in \mathbf{N}^* \mid n \le [x],\ n \equiv 0 \pmod{p_h} \text{ sau } n \equiv -2 \pmod{p_h}\},$$

atunci

$$A = \{1, 2, \ldots, [x]\} \setminus \left(\bigcup_{h=2}^{r} B_{p_h} \right)$$

și ținând cont că $A(x) = |A|$, $B(p_h, x) = |B_{p_h}|$ $(\forall)\ h = \overline{2,r}$,

$$\left| B_{p_{i_1}} \cap B_{p_{i_2}} \cap \ldots \cap B_{p_{i_s}} \right| = B\left(p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_s}, x \right)$$

propoziția 1 din paragraful II al anexei ne arată că:

$$(6) \quad A(x) \le \sum_{\substack{d \mid k \\ \Omega(d) \le m-1}} \mu(d) B(d, x)$$

unde $k = p_2 \cdot p_3 \cdot \ldots \cdot p_r$, iar m este un număr natural impar ce va fi precizat ulterior ca fiind funcție de x (în inegalitatea (6) μ este funcția lui Möbius definită în paragraful II al anexei teoremei elementului prim prin formula $\mu(q_1 \cdot q_2 \cdot \ldots \cdot q_r) = (-1)^r$, dacă $q_1, q_2, \ldots, q_r$ sunt numere prime distincte, $\mu(1) = 1$ și $\mu(n) = 0$, dacă există p număr prim astfel încât p^2 / n; numerele $B(d,x)$ pot fi definite pentru orice $d \in \mathbf{N}^*$, nu neapărat pentru numere impare și libere de pătrate). Pentru a deduce inegalitatea (6) s-a ținut cont și de faptul că $B(1, x) = [x]$. Din inegalitatea (5) rezultă că:

$$2^{\Omega(d)} \cdot \frac{x}{d} - 2^{\Omega(d)} < B(d,x) < 2^{\Omega(d)} + 2^{\Omega(d)} \frac{x}{d}$$

și că

$$\mu(d) B(d,x) < 2^{\Omega(d)} + 2^{\Omega(d)} \cdot \frac{x}{d} \cdot \mu(d).$$

Folosind această din urmă inegalitate precum și evaluarea (6) deducem că:

$$(7) \quad A(x) < x \sum_{\substack{d \mid k \\ \Omega(d) \le m-1}} \frac{2^{\Omega(d)} \mu(d)}{d} + \sum_{\substack{d \mid k \\ \Omega(d) \le m-1}} 2^{\Omega(d)}.$$

Convenind să notăm $C_{r-1}^h = 0$ dacă $h > r-1$ și C_{r-1}^h pentru $h \le r-1$, combinări de $r-1$ luate câte h, atunci:

$$(8)\quad \sum_{\substack{d|k \\ \Omega(d)\le m-1}} 2^{\Omega(d)} = \sum_{h=0}^{m-1} 2^h \cdot C_{r-1}^h \le 2^m \sum_{h=0}^{m-1} C_{r-1}^h \le$$

$$\le 2^m \sum_{h=0}^{m-1} r^h = 2^m \cdot \frac{r^m - 1}{r-1} < 2^m \cdot r^m \le (2y)^m.$$

În evaluările de mai sus am folosit că

$$C_{r-1}^h = \frac{(r-1)(r-2)...(r-h)}{h!} \le (r-1)(r-2)...(r-h) \le r^h,$$

dacă $h \le r-1$, $C_{r-1}^h = 0 < r^h$, dacă $h > r-1$, $\frac{1}{r-1} < 1$ deoarece $r \ge 3$, $r \le y$ deoarece $r = \pi(y) \le y$.

Pe de altă parte

$$\sum_{\substack{d|k \\ \Omega(d)\le m-1}} \frac{2^{\Omega(d)}\mu(d)}{d} = \sum_{d|k} \frac{\mu(d)\cdot 2^{\Omega(d)}}{d} - \sum_{n=m}^{r-1} \sum_{\substack{d|k \\ \Omega(d)=n}} \frac{\mu(d)\cdot 2^{\Omega(d)}}{d} =$$

$$= \prod_{\substack{2<p\le p, \\ p\text{-}prim}} \left(1 - \frac{2}{p}\right) - \sum_{n=m}^{r-1} (-1)^n \cdot 2^n \cdot \sum_{\substack{d|k \\ \Omega(d)=n}} \frac{1}{d} = \prod_{\substack{2<p\le y \\ p\text{-}prim}} \left(1 - \frac{2}{p}\right) - \sum_{n=m}^{r-1} (-1)^n \cdot 2^n \cdot S_n.$$

Pentru egalitatea

$$\sum_{d|k} \frac{\mu(d)\cdot 2^{\Omega(d)}}{d} = \prod_{\substack{2<p\le p, \\ p\text{-}prim}} \left(1 - \frac{2}{p}\right)$$

am folosit faptul că funcția $f: \mathbf{N}^* \to \mathbf{R}$ definită prin formula $f(n) = \frac{2^{\Omega(n)}}{n}$, este total multiplicativă $\left(f(n\cdot m) = \frac{2^{\Omega(n\cdot m)}}{nm} = \frac{2^{\Omega(n)+\Omega(m)}}{n\cdot m} = \frac{2^{\Omega(n)}}{n} \cdot \frac{2^{\Omega(m)}}{m} = f(n)f(m),\right.$ $\left.(\forall)\, n,\ m \in \mathbf{N}^*\right)$ și deci se poate aplica propoziția 2 din paragraful II al anexei.

Dacă $m \ge r$ suma $\sum_{n=m}^{r-1} \sum_{\substack{d|k \\ \Omega(d)=n}} \frac{\mu(d)2^{\Omega(d)}}{d}$ se consideră egală cu zero. Am notat cu S_n expresia $\sum_{2\le i_1<i_2<...<i_n\le r} \frac{1}{p_{i_1}} \cdot \frac{1}{p_{i_2}} \cdot ... \cdot \frac{1}{p_{i_n}}$, dacă $m \le r-1$ și $S_n = 0$, dacă $m \ge r$. Folosind

propoziția 4 din paragraful II al anexei rezultă că

$$S_n \le \frac{S_1}{n!} \le \frac{(e\,S_1)^n}{n^n} \le \left(\frac{3c_2 \ln\ln y}{n}\right)^n$$

(am folosit în evaluările precedente că $S_1 = \sum_{i=2}^{r} \frac{1}{p_i}$, $e^n = \sum_{h=0}^{\infty} \frac{n^h}{h!} > \frac{n^n}{n!}$, $e < 3$ și $S_1 < c_2 \ln\ln y$ pentru o anume constantă $c_2 \in \mathbf{R}_+^*$ furnizată de propoziția 3 din paragraful I al anexei; $r = \pi(y)$ și $y \ge 5$). Din considerațiile precedente precum și din propoziția 4 din paragraful I al anexei deducem că:

$$(9)\quad \left|\sum_{\substack{d|k \\ \Omega(d)\le m-1}} \frac{\mu(d)\cdot 2^{\Omega(d)}}{d}\right| \le \prod_{\substack{2<p\le y \\ p\text{-prim}}} \left(1-\frac{2}{p}\right) + \sum_{n=m}^{r-1} 2^n \cdot S_n \le \frac{c_3}{(\ln y)^2} + \sum_{n=m}^{r-1} \left(\frac{6c_2 \ln\ln y}{n}\right)^n \le$$

$$\le \frac{c_3}{(\ln y)^2} + \sum_{n=m}^{r-1} \left(\frac{c_4 \ln\ln y}{m}\right)^n \le \frac{c_3}{(\ln y)^2} + \sum_{n=m}^{r-1} \frac{1}{2^n} \le \frac{c_3}{(\ln y)^2} + \sum_{n=m}^{\infty} \frac{1}{2^n} = \frac{c_3}{(\ln y)^2} + \frac{2}{2^m},$$

unde $c_4 \in \mathbf{R}_+^*$ este > 2 și $> 6c_2$, $c_3 \in \mathbf{R}_+^*$ este furnizat de propoziția 4 din paragraful I al anexei și am presupus că îl pot alege pe m astfel încât să fie îndeplinită inegalitatea

(10) $m > 2\,c_4 \ln\ln y$.

Din inegalitățile (7), (8), (9) și (3) rezultă că:

(11) $P(x) < y + \frac{c_3 x}{(\ln y)^2} + \frac{2x}{2^m} + (2y)^m$ în ipoteza că $5 \le y < x$, m număr natural impar care satiface inegalitatea (10).

În acest moment vom preciza cine sunt numerele y și m:

(12) $y = x^{\frac{1}{3c_4 \ln\ln x}}$; $m = 2[c_4 \ln\ln x] - 1$.

Arătăm că există $c_5 \in \mathbf{R}_+^*$, $c_5 > 5$ astfel încât, $(\forall)\ x \ge c_5$, să fie îndeplinite condițiile impuse numerelor y și m. Deoarece $\lim_{x\to\infty} \ln y = \lim_{x\to\infty} \frac{\ln x}{3c_4 \ln\ln x} = \infty$ rezultă că $\lim_{x\to\infty} y = \infty$ și deci $y \ge 5$ pentru x mai mare sau egal cu o anumită constantă.

De asemenea deoarece $3c_4 \ln\ln x > 1$, pentru x mai mare sau egal cu o anumită constantă, deducem că $y < x$ (pentru x mai mare decât constanta amintită mai sus). Deoarece $2c_4 \ln(3\,c_4 \ln\ln x) > 3$ pentru x mai mare decât o anumită

constantă deducem că: $2c_4 \ln \ln y = 2c_4 \ln \frac{\ln x}{3c_4 \ln \ln x} = 2c_4 \ln \ln x -$ $- 2c_4 \ln (3 c_4 \cdot \ln \ln x) < 2c_4 \ln \ln x - 3 < 2 ([c_4 \ln \ln x] + 1) - 3 = m$ pentru x mai mare decât constanta amintită mai sus. Există deci $c_5 \in \mathbf{R}_+^*$, $c_5 > 5$ astfel încât $(\forall) x \geq c_5$ avem că $5 \leq y < x$, m număr natural impar care satisface inegalitatea (10), unde y și m sunt numerele definite prin formulele (12). Deci are loc inegalitatea (11):

$$P(x) < y + \frac{c_3 x}{(\ln y)^2} + \frac{2x}{2^m} + (2y)^m.$$

În cele ce urmează arătăm că fiecare din cei patru termeni din membrul drept al inegalității precedente sunt mai mici sau egali cu $\frac{x}{\ln^2 x}(\ln \ln x)^2$ înmulțit cu o constantă, pentru x suficient de mare.

Avem că

$$y = x^{\frac{1}{3c_4 \ln \ln x}} \leq x^{\frac{1}{2}} \leq \frac{x}{\ln^2 x}(\ln \ln x)^2$$

pentru x suficient de mare deoarece $\lim\limits_{x \to \infty} \ln \ln x = \infty$ și $\lim\limits_{x \to \infty} \frac{x^{\frac{1}{2}}}{\ln^2 x} = \infty$. Al doilea, din cei patru termeni menționați anterior, este egal cu

$$\frac{c_3 x}{(\ln y)^2} = \frac{c_3 x \cdot (3c_4 \ln \ln x)^2}{\ln^2 x} = c_3 \cdot (3c_4)^2 \frac{x (\ln \ln x)^2}{\ln^2 x}.$$

De asemenea

$$\frac{2x}{2^m} < \frac{2x}{2^{2c_4 \ln \ln x - 3}} = \frac{16x}{2^{2c_4 \ln \ln x}} = \frac{16x}{(\ln x)^{2c_4 \ln 2}} < \frac{16x}{(\ln x)^2} < \frac{16x (\ln \ln x)^2}{(\ln x)^2}$$

(egalitatea $2^{2c_4 \ln \ln x} = (\ln x)^{2c_4 \ln 2}$ este adevărată deoarece logaritmind-o obținem că $2\ c_4(\ln \ln x) \cdot \ln 2 = 2\ c_4\ \ln 2 \ln \ln x$, ceea ce este evident adevărat; în evaluările de mai sus am folosit și că $2 \ln 2 > 1$, $c_4 > 2$).

$$(2y)^m \leq (2y)^{2c_4 \ln \ln x} = e^{2c_4 \ln \ln x} \cdot \left(\frac{\ln x}{3c_4 \ln \ln x} + \ln 2 \right) =$$

$$= e^{\frac{2}{3} \ln x + 2c_4 \ln 2 \ln \ln x} < e^{\frac{3}{4} \ln x} = x^{\frac{3}{4}}$$

pentru x suficient de mare $\left(\text{deoarece } \lim_{x\to\infty}\frac{\ln x}{\ln\ln x}=\infty\right)$. Cum $x^{\frac{3}{4}}<\frac{x(\ln\ln x)^2}{(\ln x)^2}$, pentru x suficient de mare, din observațiile anterioare deducem că există c_6, $c_7\in\mathbf{R}_+^*$, $c_7>5$ astfel încât:

$$P(x)<c_6\cdot\frac{x(\ln\ln x)^2}{(\ln x)^2},\quad(\forall)\,x\geq c_7\,(c_7\geq c_5).$$

Cum funcția $g(x)=\frac{x(\ln\ln x)^2}{(\ln x)^2}$ este continuă și strict pozitivă pe intervalul $[3, c_7]$, enunțul teoremei 2 este demonstrat.

Demonstrația teoremei 1. dacă notăm cu p_r' al r-lea număr al mulțimii G atunci $p_r'>r+1$.

Cum

$$P(p_r')=r<\frac{c_1p_r'}{(\ln p_r')^2}(\ln\ln p_r')^2<\frac{c_8p_r'}{(\ln p_r')^{\frac{3}{2}}}$$

pentru o anumită constantă $c_8\in\mathbf{R}_+^*$ și $p_r'>r+1$, $(\forall)\,r\in\mathbf{N}$, deducem că $r<\frac{c_8p_r'}{\ln^{\frac{3}{2}}(r+1)}$ și că

$$\sum_{p\in G}\frac{1}{p}<\sum_{r=1}^{\infty}\frac{c_8}{r\ln^{\frac{3}{2}}(r+1)}.$$

În scrierea inegalităților precedente am folosit teorema 1 precum și faptul că

$$\frac{x(\ln\ln x)^2}{(\ln x)^2}<\frac{x}{(\ln x)^{\frac{3}{2}}},$$

$\left(\text{pentru } x \text{ suficient de mare (aici se ține cont de faptul că } \lim_{x\to\infty}\frac{(\ln x)^{\frac{1}{2}}}{(\ln\ln x)^2}=\infty\right)$.

Avem că

$$\sum_{r=1}^{\infty}\frac{1}{r[\ln(r+1)]^{\frac{3}{2}}}=\frac{1}{(\ln 2)^{\frac{3}{2}}}+\frac{1}{2(\ln 3)^{\frac{3}{2}}}+\sum_{r=3}^{\infty}\frac{1}{r[\ln(r+1)]^{\frac{3}{2}}}<$$

$$<\frac{1}{(\ln 2)^{\frac{3}{2}}}+\frac{1}{2(\ln 3)^{\frac{3}{2}}}+\sum_{r=3}^{\infty}\frac{1}{r(\ln r)^{\frac{3}{2}}}<\frac{1}{(\ln 2)^{\frac{3}{2}}}+\frac{1}{2(\ln 3)^{\frac{3}{2}}}+\sum_{r=3}^{\infty}\int_{r-1}^{r}\frac{1}{t(\ln t)^{\frac{3}{2}}}\,dt=$$

$$= \frac{1}{(\ln 2)^{\frac{3}{2}}} + \frac{1}{2(\ln 3)^{\frac{3}{2}}} + \int_2^{\infty} \frac{1}{t(\ln t)^{\frac{3}{2}}}\,dt.$$

Cum

$$\int_2^{\infty} \frac{1}{t(\ln t)^{\frac{3}{2}}}\,dt = (-2)\cdot \int_2^{\infty} \left[(\ln t)^{-\frac{1}{2}}\right]' dt =$$

$$= (-2)\left(\left((\ln t)^{-\frac{1}{2}}\right)\Big|_{t=2}^{t=\infty}\right) = -2\left(-(\ln 2)^{-\frac{1}{2}}\right) = \frac{2}{(\ln 2)^{\frac{1}{2}}} = \frac{2}{\sqrt{\ln 2}}$$

$\left(\text{am ținut cont că } \lim_{t\to\infty} \frac{1}{\sqrt{\ln t}} = 0\right)$ din considerațiile precedente rezultă că

$\sum_{r=1}^{\infty} \frac{1}{r\left(\ln(r+1)\right)^{\frac{3}{2}}}$ este convergentă și deci $\sum_{p\in G} \frac{1}{p}$ este convergentă.

Să arătăm acum că $\sum_{p\text{-}prim} \frac{1}{p}$ este o serie divergentă. Pentru aceasta vom folosi propoziția 2 din paragraful I al anexei care afirmă că $p_r < a_{10} r \ln r$ pentru o anumită constantă $a_{10} \in \mathbf{R}_+^*$ și $(\forall)\, r > 1$. Pentru a arăta că suma $\sum_{p\text{-}prim} \frac{1}{p}$ este divergentă, este suficient să arătăm că $\sum_{r=2}^{\infty} \frac{1}{r \ln r}$ este divergentă. Aceasta se întâmplă deoarece pentru orice număr natural n, $n \geq 2$ avem că

$$\sum_{r=2}^{\infty} \frac{1}{r\ln r} > \sum_{r=2}^{n} \frac{1}{r\ln r} > \sum_{r=2}^{n} \int_r^{r+1} \frac{1}{x\ln x}\,dx = \int_2^{n+1} \frac{1}{x\ln x}\,dx = \ln\ln(n+1) - \ln\ln 2.$$

Deci $\sum_{p-prim} \frac{1}{p}$ este divergentă și în particular rezultă că mulțimea numerelor prime este infinită. Enunțul teoremei lui Brun nu permite nici o concluzie asupra problemei dacă mulțimea G este finită sau infinită.

ANEXĂ
(Teorema lui Brun)

I. **Lema 1**. *Dacă n este un număr natural și p este număr prim atunci exponentul lui p în descompunerea în factori primi a lui n! este egal cu* $\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$.

Soluție. Evident că în suma de mai sus doar un număr finit de termeni sunt nenuli (într-adevăr există $i_0 \in \mathbf{N}^*$ cu proprietatea că $p^{i_0} > n$. Avem că $\left[\frac{n}{p^i}\right] = 0$, $(\forall)\ i \geq i_0,\ i \in \mathbf{N}$).

Numărul numerelor naturale nenule, divizibile cu p și mai mici sau egale cu n este egal cu $\left[\frac{n}{p}\right]$. La fel pentru orice $i \in \mathbf{N}^*$ numărul numerelor naturale nenule, divizibile cu p^i și mai mici sau egale cu n este egal cu $\left[\frac{n}{p^i}\right]$. Ținând cont de aceste observații lema este demonstrată. Enunțul lemei 1 este cunoscut sub numele de teorema lui Legendre.

Propoziția 1. *Există două constante pozitive strict, pe care le notăm cu* a_1 *și* a_2 *astfel încât*

$$a_1 \frac{x}{\ln x} < \pi(x) < a_2 \frac{x}{\ln x}$$

oricare ar fi $x \geq 2$ ($\pi(x)$ *reprezintă numărul numerelor prime mai mici sau egale cu* x).

Demonstrație. Enunțul este imediat dacă ținem cont de teorema elementului prim care afirmă că $\lim_{x\to\infty} \frac{\pi(x)\cdot \ln x}{x} = 1$. Vom da însă în continuare și o demon-

straţie directă a propoziţiei 1 fără a utiliza teorema elementului prim. Fie $n \in \mathbf{N}^*$, $n \geq 2$. Pentru fiecare p, număr prim mai mic sau egal cu $2n$, notăm cu r cel mai mare număr natural pentru care $p^r \leq 2n$ (evident r depinde de p; mai precis $r = \left[\frac{\ln 2n}{\ln p} \right]$. Dependenţa lui r de p nu a fost pusă în evidenţă prin intermediul notaţiei pentru a nu se îngreuna scrierea). Vom arăta că are loc inegalitatea:

$$(1) \qquad \prod_{n<p\leq 2n} p \leq \frac{(2n)!}{n! \cdot n!} \leq \prod_{p\leq 2n} p^r .$$

Se subînţelege că în inegalitatea (1) numerele p care apar sunt numere prime.

Deoarece $\frac{(2n)!}{n! \cdot n!} = C_{2n}^n$ este număr natural şi orice număr prim p astfel încât $n < p \leq 2n$ divide $(2n!)$, dar nu divide $(n!)^2$, prima parte a inegalităţii (1) este demonstrată. Pentru partea a doua a inegalităţii (1) trebuie să observăm că dacă p este un număr prim astfel încât $p \mid \frac{(2n)!}{n! \cdot n!}$, atunci $p \leq 2n$ şi exponentul lui p în descompunerea în factori primi a lui $\frac{(2n)!}{n! \cdot n!}$ este egal, conform lemei 1 cu

$$\sum_{i=1}^{\infty} \left(\left[\frac{2n}{p^i} \right] - 2 \left[\frac{n}{p^i} \right] \right) = \sum_{i=1}^{r} \left(\left[\frac{2n}{p^i} \right] - 2 \left[\frac{n}{p^i} \right] \right),$$

(ultima egalitate se întâmplă deoarece $p^i > 2n$, pentru $i \geq r + 1$). Pentru orice număr real y avem că

$$[y] - 2\left[\frac{y}{2} \right] < y - 2\left(\frac{y}{2} - 1 \right) = 2$$

şi cum $[y] - 2\left[\frac{y}{2} \right]$ este număr întreg deducem că $[y] - 2\left[\frac{y}{2} \right] \leq 1$, $(\forall)\, y \in \mathbf{R}$. Ţinând cont de această observaţie şi de consideraţiile anterioare deducem că exponentul lui p în descompunerea în factori primi a lui $\frac{(2n)!}{n! \cdot n!}$ este mai mic sau egal cu $\sum_{i=1}^{r} 1 = r$.

Aceasta demonstrează și a doua parte a inegalității (1). Din inegalitățile (1) rezultă că:

$$(2)\quad n^{\pi(2n)-\pi(n)} < \prod_{n<p\le 2n} p \le C_{2n}^{n} \le \prod_{p\le 2n} p^{r} \le (2n)^{\pi(2n)}$$

Am ținut cont în inegalitățile (2) de faptul că numărul de numere prime p care satisfac condiția $n < p \le 2n$ este egal cu $\pi(2n) - \pi(n)$, numărul de numere prime $p \le 2n$ este egal cu $\pi(2n)$ și $p^r \le 2n$. Logaritmând inegalitatea (2) obținem că:

$$(3)\quad \big(\pi(2n)-\pi(n)\big)\ln n \le \ln C_{2n}^{n} \le \pi(2n)\cdot \ln 2n \quad (\forall) n \in \mathbf{N},\ n \ge 2.$$

Deoarece

$$C_{2n}^{n} \le \sum_{j=0}^{2n} C_{2n}^{j} = (1+1)^{2n} = 2^{2n},$$

inegalitatea (3) ne permite să concluzionăm că

$$\big(\pi(2n)-\pi(n)\big)\ln n \le \ln C_{2n}^{n} \le \ln 2^{2n} = 2n\cdot \ln 2;$$

există deci $a_3 \in \mathbf{R}_+^*$ astfel încât:

$$(4)\quad \pi(2n)-\pi(n) < a_3 \frac{n}{\ln n},\quad (\forall) n \in \mathbf{N},\ n \ge 2.$$

Deoarece

$$C_{2n}^{n} = \frac{(2n)!}{n!\cdot n!} = \frac{(n+1)(n+2)\ldots 2n}{1\cdot 2\cdot \ldots \cdot n} = \prod_{a=1}^{n} \frac{n+a}{a} \ge \prod_{a=1}^{n} 2 = 2^{n},$$

a doua parte a inegalității (3) ne asigură că

$$\pi(2n)\cdot \ln 2n \ge \ln C_{2n}^{n} \ge \ln 2^{n} = n \ln 2.$$

Există deci $a_4 \in \mathbf{R}_+^*$ astfel încât:

$$(5)\quad \pi(2n) > a_4 \frac{n}{\ln n}$$

Aceasta rezultă din inegalitatea precedentă precum și din faptul că $\lim\limits_{n\to\infty} \dfrac{\ln n}{\ln 2n} = 1$.

(5) are loc pentru $n \in \mathbf{N},\ n \ge 2$). Dacă $x \in \mathbf{R}, x \ge 4$ atunci folosind (5) precum și faptul că $2\left[\dfrac{x}{2}\right] \le 2\cdot \dfrac{x}{2} = x$, deducem existența unei constante $a_5 \in \mathbf{R}_+^*$ astfel încât să aibă loc inegalitățile:

$$\pi(x) \ge \pi\left(2\cdot\left[\frac{x}{2}\right]\right) > a_4 \frac{\left[\frac{x}{2}\right]}{\ln\left[\frac{x}{2}\right]} > a_5 \frac{x}{\ln x}$$

(pentru scrierea ultimei inegalități, și deci și pentru justificarea existenței constantei a_5, s-a folosit faptul că $\lim_{x\to\infty}\frac{\left[\frac{x}{2}\right]}{x}=\frac{1}{2}$ și $\lim_{x\to\infty}\frac{\ln x}{\ln\left[\frac{x}{2}\right]}=1$). Deci

$\pi(x)>a_5\frac{x}{\ln x}$, $(\forall)\, x\geq 4$. Deoarece $\frac{x}{\ln x}$ este funcție continuă pe intervalul [2,4] și $\pi(x)\geq 1$, $(\forall)\, x\in[2,4]$ deducem existența lui $a_1\in\mathbf{R}_+^*$ astfel încât:

$$\pi(x)>a_1\frac{x}{\ln x},\quad (\forall)\, x\geq 2.$$

Deoarece

$$y=2+2\left(\frac{y}{2}-1\right)<2+2\left[\frac{y}{2}\right],$$

$(\forall)\, y\in\mathbf{R}$, și $\pi(\alpha+2)\leq\pi(\alpha)+2$, $(\forall)\,\alpha\in\mathbf{N}$, ținând cont de inegalitatea (4), deducem existența lui $a_6\in\mathbf{R}_+^*$ astfel încât pentru orice $y\geq 4$ să aibă loc următoarele evaluări:

$$\pi(y)-\pi\left(\frac{y}{2}\right)\leq\pi\left(2+2\left[\frac{y}{2}\right]\right)-\pi\left(\frac{y}{2}\right)\leq 2+\pi\left(2\left[\frac{y}{2}\right]\right)-\pi\left(\left[\frac{y}{2}\right]\right)<$$

$$<2+a_3\cdot\frac{\left[\frac{y}{2}\right]}{\ln\left[\frac{y}{2}\right]}<a_6\frac{y}{\ln y}$$

(am ținut seama mai sus de faptul că

$$\pi\left(\frac{y}{2}\right)=\pi\left(\left[\frac{y}{2}\right]\right),\ \lim_{y\to\infty}\frac{\left[\frac{y}{2}\right]}{y}=\frac{1}{2},\ \lim_{y\to\infty}\frac{\ln y}{\ln\left[\frac{y}{2}\right]}=1,\ \lim_{y\to\infty}\frac{y}{\ln y}=\infty).$$

Se deduce imediat existența lui $a_7\in\mathbf{R}_+^*$ astfel încât $\pi(y)-\pi\left(\frac{y}{2}\right)<a_7\frac{y}{\ln y}$, $(\forall)\, y\geq 2$. Folosind această din urmă inegalitate precum și faptul că $\pi(\alpha)\leq\alpha$, $(\forall)\,\alpha\in\mathbf{R}_+$, rezultă că

$$(\ln y)\cdot\pi(y)-\left(\ln\frac{y}{2}\right)\cdot\pi\left(\frac{y}{2}\right)=\left(\pi(y)-\pi\left(\frac{y}{2}\right)\right)\ln y+(\ln 2)\cdot\pi\left(\frac{y}{2}\right)<$$

$$<a_7\cdot\frac{y}{\ln y}\cdot\ln y+\frac{y}{2}=y\left(a_7+\frac{1}{2}\right)=a_8 y,$$

evaluare ce are loc $(\forall)\ y \geq 2(\ln 2 < \ln e = 1)$. $a_8 \in \mathbf{R}_+^*$ deoarece $a_8 = a_7 + \frac{1}{2}$.

Dacă $x \in \mathbf{R}$, $x \geq 2$ și $m \in \mathbf{N}$ astfel încât $\frac{x}{2^m} \geq 2$ atunci

$$\pi\left(\frac{x}{2^m}\right)\ln\frac{x}{2^m} - \pi\left(\frac{x}{2^{m+1}}\right)\ln\frac{x}{2^{m+1}} < a_8 \cdot \frac{x}{2^m}$$

conform celor demonstrate mai sus. Dacă v este cel mai mare număr natural astfel încât $\frac{x}{2^v} \geq 2\left(\text{deci}\ \frac{x}{2^{v+1}} < 2\right)$ atunci considerațiile anterioare precum și faptul că $\ln\frac{x}{2^{v+1}} \cdot \pi\left(\frac{x}{2^{v+1}}\right) = 0$ ne conduc la următoarele inegalități

$$\pi(x)\ln x = \sum_{m=0}^{v}\left(\pi\left(\frac{x}{2^m}\right)\ln\frac{x}{2^m} - \pi\left(\frac{x}{2^{m+1}}\right)\ln\frac{x}{2^{m+1}}\right) <$$

$$< \sum_{m=0}^{v} a_8 \cdot \frac{x}{2^m} < a_8 \cdot x \cdot \sum_{m=0}^{\infty}\frac{1}{2^m} = 2a_8 x = a_2 x.$$

În acest moment propoziția 1 este demonstrată.

Propoziția 2. *Dacă notăm cu p_r al r-lea număr prim, pentru orice $r \in \mathbf{N}$, $r > 1$, avem inegalitățile:*

$$a_9\, r \ln r < p_r < a_{10}\, r \cdot \ln r, \text{ unde } a_9, a_{10} \in \mathbf{R}_+^*.$$

Demonstrație. E ușor de văzut că $p_r > r$, $(\forall) r \in \mathbf{N}^*$. Într-adevăr $p_1 = 2 > 1$, $p_2 = 3 > 2$ și dacă presupunem că $p_r > r$, pentru un $r \in \mathbf{N}$, $r \geq 2$ atunci $p_{r+1} \geq p_r + 2 > r + 2 > r + 1$. Afirmația $p_r > r$, $(\forall) r \in \mathbf{N}^*$, este demonstrată astfel prin inducție. Dacă $r \in \mathbf{N}$, $r > 1$ atunci $p_r \geq p_2 = 3$ și aplicând atunci propoziția 1 pentru $x = p_r$ deducem că $r = \pi(p_r) < a_2 \cdot \frac{p_r}{\ln p_r}$. Ținând cont că $p_r > r$, $(\forall) r \in \mathbf{N}^*$, această din urmă inegalitate se mai scrie și sub forma

$$p_r > \frac{r \ln p_r}{a_2} > \frac{r \ln r}{a_2} = a_9 \cdot r \ln r$$

(unde $a_9 = \frac{1}{a_2}$; $a_9 \in \mathbf{R}_+^*$ deoarece $a_2 \in \mathbf{R}_+^*$). Tot din propoziția 1 rezultă că

$\frac{a_1 p_r}{\ln p_r} < r$, $(\forall)\, r \in \mathbf{N}$, $r > 1$. Această din urmă inegalitate se mai scrie și sub forma $a_1 < \frac{r \ln p_r}{p_r}$. Deoarece $\lim_{x\to\infty} \frac{\ln x}{\sqrt{x}} = 0$, deducem existența unei constante pozitive a astfel încât $\frac{\ln p_r}{\sqrt{p_r}} < a_1$, $(\forall)\, r \in \mathbf{N}^*$, $r \geq a$. Deci $\frac{\ln p_r}{\sqrt{p_r}} < a_1 < \frac{r \ln p_r}{p_r}$, $(\forall)\, r \in \mathbf{N}^*$, $r \geq a$. Primul și ultimul termen al precedentei inegalități furnizează evaluările $\sqrt{p_r} < r$ și $p_r < r^2$ valabile pentru $r \in \mathbf{N}^*$, $r \geq a$. Logaritmând obținem că $\ln p_r < 2 \ln r$, pentru $r \in \mathbf{N}^*$, $r \geq a$. Aceasta împreună cu faptul că $a_1 \cdot p_r < r \ln p_r$, $(\forall)\, r \in \mathbf{N}$, $r \geq 2$ conduc la inegalitatea: $p_r < \frac{2}{a_1} r \ln r$, valabilă pentru $r \in \mathbf{N}^*$, $r \geq a$. Enunțul propoziției 2 este acum imediat.

Propoziția 3: *Există* $a_{11} \in \mathbf{R}_+^*$ *astfel încât* $\sum_{2<p\leq x} \frac{1}{p} < a_{11} \ln \ln x$, $(\forall)\, x \geq 3$ (*suma de mai sus se face după acele numere prime p pentru care* $2 < p \leq x$).

Demonstrație: Deoarece

$$\frac{1}{r \ln r} \leq \int_{r-1}^{r} \frac{1}{y \ln y}\, dy$$

$(\forall)\, r \geq 3$, $p_r > a_9 \cdot r \ln r$, $(\forall)\, r \geq 2$, $r \in \mathbf{N}$ (conform propoziției 2) și $\pi(x) \leq [x]$, $(\forall)\, x \geq 0$, deducem că

$$\sum_{2<p\leq x} \frac{1}{p} = \sum_{r=2}^{\pi(x)} \frac{1}{p_r} < \frac{1}{a_9} \sum_{r=2}^{\pi(x)} \frac{1}{r \ln r} \leq \frac{1}{a_9} \sum_{r=2}^{[x]} \frac{1}{r \ln r} =$$

$$= \frac{1}{a_9}\left(2 \ln 2 + \sum_{r=3}^{[x]} \frac{1}{r \ln r}\right) \leq \frac{1}{a_9}\left(2 \ln 2 + \sum_{r=3}^{[x]} \int_{r-1}^{r} \frac{1}{y \ln y}\, dy\right) = \frac{1}{a_9}\left(2 \ln 2 + \int_{2}^{[x]} \frac{(\ln y)'}{\ln y}\, dy\right) =$$

$$= \frac{1}{a_9}\left(2 \ln 2 + \ln \ln [x] - \ln \ln 2\right) < \frac{1}{a_9}\left(2 \ln 2 - \ln \ln 2 + \ln \ln x\right) < a_{11} \ln \ln x, (\forall)\, x \geq 3$$

(pentru valabilitatea ultimei inegalități s-a folosit faptul că $\lim_{x\to\infty} \ln \ln x = \infty$).

Propoziția 4: $\prod_{2<p\leq x}\left(1 - \frac{2}{p}\right) < \frac{a_{12}}{(\ln x)^2}$, $(\forall)\, x \geq 3$, *pentru o anumită constantă strict pozitivă* a_{12} (*ca și mai sus produsul se face după numerele prime p pentru care* $2 < p \leq x$).

Demonstrație. Să observăm întâi că, $(\forall)\ m \in \mathbf{N}$, $m \geq 2$,

$$\prod_{\substack{p \leq m \\ p\text{-}prim}} \left(\frac{1}{1-\frac{1}{p}} \right) = \prod_{\substack{p \leq m \\ p\text{-}prim}} \left(\sum_{n=0}^{\infty} \left(\frac{1}{p} \right)^n \right) = \sum \frac{1}{a},$$

unde ultima sumă se face după acele numere naturale nenule a care au toți divizorii primi mai mici sau egali cu m. De aici deducem că

$$\sum_{\alpha=1}^{[x]} \frac{1}{\alpha} \leq \prod_{p \leq x} \left(\frac{1}{1-\frac{1}{p}} \right),$$

$(\forall)\ x \geq 3$. Deoarece $\int_r^{r+1} \frac{dx}{x} < \frac{1}{r}$, $(\forall)\ r \geq \mathbf{N}^*$, $\int_1^x \frac{dy}{y} < \int_1^{[x]+1} \frac{dy}{y}$ $(\forall)\ x \geq 1$, deducem că

$$\frac{1}{4} \prod_{2<p\leq x} \left(1-\frac{2}{p} \right) < \frac{1}{4} \prod_{2<p\leq x} \left(1-\frac{2}{p}+\frac{1}{p^2} \right) = \prod_{p\leq x} \left(1-\frac{1}{p} \right)^2 =$$

$$= \left[\prod_{p\leq x} \left(1-\frac{1}{p} \right) \right]^2 \leq \left(\sum_{a=1}^{[x]} \frac{1}{a} \right)^{-2} \leq \left(\int_1^{[x]+1} \frac{dy}{y} \right)^{-2} < \left(\int_1^x \frac{dy}{y} \right)^{-2} = \frac{1}{(\ln x)^2},$$

$(\forall)\ x \geq 3$.

Enunțul propoziției 4 este astfel demonstrat.

II. Dacă $\mu : \mathbf{N}^* \to \mathbf{Z}$ este funcția lui Möbius definită în paragraful II al anexei teoremei elementului prim, atunci $\sum_{d|n} \mu(d) = 0$, dacă $n > 1$, $n \in \mathbf{N}$, și $\sum_{d|n} \mu(d) = 1$, dacă $n = 1$ (aceste fapte au fost demonstrate în lema din locul citat mai sus).

Propoziția 1. *Dacă $n, m \in \mathbf{N}$, $n \geq 1$, m număr par,*

$$B = \{1, 2, ..., n\} \setminus \left(\bigcup_{i=1}^{s} A_i \right),$$

unde $A_1, A_2, ..., A_s$ sunt submulțimi ale mulțimii $\{1, 2, ..., n\}$ $(s \in \mathbf{N}^*)$, atunci

$$|B| \leq n - \sum_{i=1}^{s} |A_i| + \sum_{i<j} |A_i \cap A_j| - ... + (-1)^m \sum_{i_1<i_2<...<i_m} |A_{i_1} \cap ... \cap A_{i_m}|$$

(pentru $m = 0$ trebuie demonstrat că $|B| \leq n$, ceea ce este evident; prin $|X|$ înțelegem cardinalul mulțimii X).

Demonstrație: Arătăm întâi că $\sum_{l=0}^{a} (-1)^l C_b^l \geq 0$ oricare ar fi a și b numere naturale, $a \leq b$ și a este număr par. Pentru aceasta demonstrăm că

$\sum_{l=0}^{a}(-1)^l C_b^l = (-1)^a C_{b-1}^a$, oricare ar fi a și b numere naturale supuse condiției $a<b$.

Vom realiza o recurență după a. Verificarea pentru $a = 0$ este imediată. Presupunem că egalitatea de mai sus este adevărată pentru $a \in \mathbf{N}$, $a < b$ și $a + 1 < b$. Atunci folosind ipoteza de recurență precum și faptul că $C_b^{a+1} = C_{b-1}^{a+1} + C_{b-1}^a$ deducem că

$$\sum_{l=0}^{a+1}(-1)^l C_b^l = \sum_{l=0}^{a}(-1)^l C_b^l + (-1)^{a+1} C_b^{a+1} =$$

$$= (-1)^a C_{b-1}^a + (-1)^{a+1} C_b^{a+1} = (-1)^{a+1}\left(C_b^{a+1} - C_{b-1}^a\right) = (-1)^{a+1} \cdot C_{b-1}^{a+1}.$$

Deci raționa-mentul prin recurență este încheiat. Pentru a arăta acum că $\sum_{l=0}^{a}(-1)^l C_b^l \geq 0$ $(\forall)$ $a, b \in \mathbf{N}$, $a \leq b$, a număr par, deosebim două cazuri: dacă $a < b$ atunci $\sum_{l=0}^{a}(-1)^l C_b^l = (-1)^a C_{b-1}^a = C_{b-1}^a \geq 0$ conform celor demonstrate anterior, iar dacă $a = b$ atunci $\sum_{l=0}^{b}(-1)^l C_b^l = (1-1)^b = 0$. Să trecem acum la demonstrația propoziției 1. Fie $\alpha \in \{1, 2, ..., n\}$; presupunem că elementul α aparține mulțimilor $A_{i_1}, A_{i_2}, \ldots, A_{i_t}$ $(t \in \mathbf{N}^*)$ și nu aparține nici unei alte mulțimi A_i cu excepția celor indicate mai sus. Atunci contribuția lui α în suma

$$n - \sum_{i=1}^{m}\left|A_i\right| + \sum_{i<j}\left|A_i \cap A_j\right| + \ldots + (-1)^m \sum_{j_1<j_2<\ldots<j_m}\left|A_{j_1} \cap A_{j_2} \cap A_{j_m}\right|$$

este egală cu $\sum_{l=0}^{t}(-1)^l C_t^l = 0$, dacă $t < m$ și este egală cu $\sum_{l=0}^{m}(-1)^l C_t^l$, dacă $t \geq m$. În orice caz ne-am situa contribuția lui α în suma indicată mai sus este un număr pozitiv (conform celor arătate la începutul demonstrației avem că $\sum_{l=0}^{m}(-1)^l C_t^l \geq 0$). Dacă α nu aparține nici unei mulțimi A_i atunci contribuția sa în suma indicată mai sus este egală cu 1. Conform tuturor considerațiilor precedente enunțul propoziției 1 este imediat.

Propoziția 2. *Dacă f este o funcție multiplicativă (adică $f: \mathbf{N}^* \to \mathbf{R}$, $f(1) = 1$ și $f(m \cdot n) = f(m)f(n)$, $(\forall)$ $m, n \in \mathbf{N}^*$, $(m, n) = 1$) atunci*

$$\sum_{d|a}\mu(d)f(d) = \prod_{i=1}^{k}(1 - f(p_i))$$

pentru orice număr natural $a \neq 1$ care se scrie sub forma $a = \prod_{i=1}^{k} p_i^{\alpha_i}$, unde $\alpha_i \in \mathbf{N}^*$, $(\forall)$ $i = \overline{1,k}$ și, $p_1, p_2, \ldots, p_k$ sunt numere prime distincte.

Demonstrație: Din formulele lui Viète știm că

$$(x-\beta_1)(x-\beta_2)...(x-\beta_k) = x^k - s_1x^{k-1} + s_2x^{k-2} - s_3x^{k-3} ... + (-1)^k s_k$$

unde

$$s_l = \sum_{1\le i_1<i_2..<i_l\le k} \beta_{i_1}\cdot\beta_{i_2}\cdot...\cdot\beta_{i_l},$$

$(\forall)\ l = = \overline{1,k}$. Punând în această identitate $x = 1$, $\beta_i = p_i$, $(\forall)\ i = \overline{1,k}$, se obține imediat egalitatea din enunț folosind faptul că f este multiplicativă și $\mu(d) = 0$ pentru orice $d \in \mathbf{N}$ pentru care există un număr prim p astfel încât p^2 / d.

Propoziția 3. *Fie* $x \in \mathbf{R}_+^*$, $d \in \mathbf{N}^*$ *și* $n_0 \in \mathbf{Z}$. *Dacă notăm cu A mulțimea următoare*: $\{n \in \mathbf{N}^* \mid n \le x, n \equiv n_0 \pmod d\}$ *atunci* $\left| |A| - \frac{x}{d} \right| < 1$ (|*A*| *înseamnă cardinalul mulțimii A*).

Demonstrație. Fie $k \in \mathbf{N}$, astfel încât $kd \le x < (k+1)d$. Este evident că $A \cap (id, (i+1)\text{d}]$ e formată dintr-un element $(\forall)\ i = \overline{0,k-1}$ și $A \cap (kd, (k+1)d]$ e fie mulțimea vidă, fie o mulțime formată dintr-un singur element. Deci $|A|$ este egal fie cu k, fie cu $k+1$. Cum $k = \left[\frac{x}{d}\right]$ enunțul propoziției 3 se obține imediat.

Propoziția 4: *Fie* $x_1, x_2,..., x_s \in \mathbf{R}_+$ *și* $n \in \mathbf{N}^*$, $n \le s$. *Atunci* $s_n \le \frac{s_1^n}{n!}$, *unde*

$$s_1 = \sum_{i=1}^{s} x_i \text{ și } s_n = \sum_{1\le i_1<i_2<..<i_n\le s} x_{i_1}x_{i_2}...x_{i_n}.$$

Demonstrație. Pentru $1 \le i_1 < i_2 < ... < i_n \le s$ este clar că coeficientul lui $x_{i_1}\cdot x_{i_2}\cdot...\cdot x_{i_n}$ din $s_1^n = (x_1 + ... + x_s)^n$ este egal cu $n!$ și cu această observație enunțul propoziției 4 este acum evident.

TEOREMA LUI SCHNIRELMAN

Introducere

Scopul acestui capitol este demonstrarea unui rezultat aparținând lui L.Schnirelman și anume : *există un număr natural s astfel încât orice număr natural mai mare sau egal cu 2 se scrie ca suma a cel mult s numere prime (nu neapărat distincte)*. Demonstrația prezentată aici urmărește soluția dată de Schnirelman în articolul său: *Uber additive Eigenschaften von Zahlen*, Math., Ann. 107 (1933), paginile 649-690. Demonstrația se bazează în special pe noțiunea de densitate a unui șir strict crescător de numere naturale nenule (faptele legate de această noțiune sunt demonstrate în paragraful II al anexei; cheia demonstrației teoremei lui Schnirelman este de fapt teorema 2 din paragraful II al anexei) și pe așa numita „metodă a ciurului" (folosită pentru a demonstra teorema 2 a lui Brun).

Ținând cont de teorema lui Vinogradov care afirmă că *orice număr natural impar suficient de mare se scrie ca suma a cel mult trei numere prime*, deducem existența unui $n_0 \in \mathbf{N}$, $n_0 \geq 2$, astfel încât *orice număr natural mai mare sau egal cu* n_0 *se scrie ca suma a cel mult patru numere prime*.

Demonstrația dificilei teoreme a lui Vinogradov poate fi găsită în articolul *Representation of an odd number as a sum of three primes*, Comptes Rendus (Doklady) de l'Académie des Sciences de l'URSS, 1937, 15, paginile 191-294. Shapiro și Warga au demonstrat elementar că *orice număr natural suficient de mare se scrie ca suma a cel mult 20 de numere prime* (*On representation of large integers as sums of primes*, Comm. pure Appl. Math, 3, 1950, pagina 153). Rafinând procedeele lui Schnirelman, Yin Wen-Lin a demonstrat că *orice număr natural suficient de mare se scrie ca suma a cel mult 18 numere prime*, demonstrația fiind de asemeni elementară (*Note on the representation of large integers as sums of primes*, Bull. Acad. Polon. Sci. Cl. III, 4 (1956), paginile 793-795).

Să mai spunem că dacă conjunctura lui Goldbach ar fi adevărată adică *orice număr par mai mare sau egal cu 4 se scrie ca sumă a două numere prime atunci orice număr natural mai mare sau egal cu 2 se scrie ca suma a cel mult trei numere prime.*

Teorema lui Schnirelman

Scopul principal al acestui capitol este demonstrarea următorului rezultat:

Teorema 1 (Schnirelman). *Există un număr natural s astfel încât orice număr natural mai mare sau egal cu 2 se scrie ca suma a cel mult s numere prime (nu neapărat distincte).*

Demonstrația acestei teoreme se bazează pe următoarele două rezultate:

Teorema 2. *Dacă notăm* $a_1 = 1$, $a_{i+1} = p_i$ $(\forall)\ i \in \mathbf{N}^*$ (p_i *semnifică ca de obicei al i-lea număr prim*), $A(u, x)$ *numărul de soluții al ecuației* $a_i - a_j = u$, *unde* a_i, $a_j \le x$, *pentru orice u și x numere naturale satisfăcând inegalitatea* $0 < u \le x$, *atunci există o constantă* c_1 *și un* $x_1 \in \mathbf{N}^*$ *astfel încât*

$$A(u,x) \le c_1 \frac{x}{\ln^2 x} S(u),$$

$(\forall)\ x \ge x_1$ $(x \in \mathbf{N})$, unde

$$S(u) = \prod_{\substack{p \ge 17 \\ p|u,\ p\text{-prim}}} \left(\frac{p}{p-2} \right)$$

(*în caz că nu există p prim astfel încât* $p \ge 17$, $p|u$ *atunci* $S(u) = 1$). Acest rezultat este legat de numele lui Viggo Brun.

Teorema 3. *Există o constantă* c_2 *astfel încât* $\sum_{u=1}^{x} S^2(u) \le c_2 x$, $(\forall)\ x \in \mathbf{N}^*$ ($S(u)$ *are aceeași semnificație ca mai sus*).

Să observăm acum (înainte de a demonstra teoremele 2 și 3) cum se demonstrează teorema 1 pe baza celor două rezultate precedente; se va folosi în mod esențial teorema 2 din paragraful II al anexei.

Folosind notațiile precedente precum și enunțurile teoremelor 2 și 3 deducem că pentru $x \ge x_1$, $x \in \mathbf{N}$ au loc următoarele inegalități:

$$\sum_{u=1}^{x} A^2(u,x) \le c_1^2 \frac{x^2}{\ln^4 x} \sum_{u=1}^{x} S^2(u) \le c_1^2 c_2 \frac{x^3}{\ln^4 x},$$

c_1 și c_2 fiind niște constante reale strict pozitive. Notăm $\varphi : [1, \infty) \to \mathbf{R}_+$ funcția $\varphi(x) = \ln x$. Evident că $\varphi(i) = O\left(\sqrt{i}\right)$ și conform propoziției 2 din paragraful I al anexei teoremei lui Brun $a_i = O(i \ln i) = O(i\, \varphi(i))$. Ipotezele teoremei 2 din paragraful II al anexei sunt îndeplinite și există deci un număr $n \in \mathbf{N}^*$ astfel încât orice număr natural nenul se scrie ca suma a cel mult n elemente ale șirului

$(a_i)_{i \in \mathbf{N}^*}$. Evident că $n \geq 2$. Arătăm că acum putem alege $s = n + 1$. Într-adevăr fie $m \geq 7$. Conform celor demonstrate anterior $m - 2 = a_{i_1} + a_{i_2} + \ldots + a_{i_t}$, cu $t \in \mathbf{N}^*$, $t \leq n$ ($a_{i_1}, a_{i_2}, \ldots, a_{i_t}$ sunt termeni ai șirului $(a_j)_{j \in \mathbf{N}^*}$ de mai sus). Putem considera că în această scriere apare cel mult odată numărul 1. Dacă apar cel puțin doi de unu atunci înlocuim $1 + 1$ cu 2 și repetând acest procedeu de câte ori este nevoie obținem o scriere a lui $m - 2$ ca mai sus în care 1 apare cel mult odată. Dacă 1 apare exact odată în scrierea lui $m - 2$ (presupunem că $a_{i_1} = 1$) $m = 3 + a_{i_2} + \ldots + a_{i_t}$, $a_{i_2}, a_{i_3}, \ldots a_{i_t}$ fiind numere prime. Dacă 1 nu apare deloc în scrierea lui $m - 2$ de mai sus atunci $m = 2 + a_{i_1} + a_{i_2} + \ldots + a_{i_t}$, $a_{i_1}, a_{i_2}, \ldots a_{i_t}$ fiind numere prime. Din cele de mai sus rezultă că orice număr natural mai mare sau egal cu 2 se scrie ca suma a cel mult $s = n + 1$ numere prime (evident că 2, 3, 4, 5, 6 se scriu ca suma a cel mult 2 numere prime și $2 \leq n \leq n + 1 = s$). Teorema lui Schnirelman este deci demonstrată în ipoteza că enunțurile teoremelor 2 și 3 sunt adevărate.

Demonstrația teoremei 3

Avem că

$$S(u) = \prod_{\substack{p \geq 17 \\ p/u,\ p\text{-prim}}} \left(\frac{p}{p-2}\right) = \prod_{\substack{p \geq 17 \\ p/u,\ p\text{-prim}}} \left(1 + \frac{2}{p-2}\right)$$

precum și urmă-toarea evaluare:

$$S^2(u) = \prod_{\substack{p \geq 17 \\ p/u,\ p\text{-prim}}} \left(1 + \frac{4}{p-2} + \frac{4}{(p-2)^2}\right) \leq \prod_{\substack{p \geq 17 \\ p/u,\ p\text{-prim}}} \left(1 + \frac{5}{p-2}\right) = 1 +$$

$$+ \sum_{\substack{p \geq 17 \\ p/u,\ p\text{-prim}}} \frac{5}{p-2} + \sum_{\substack{p,q \geq 17 \\ p,q/u,\ p,q\text{-prime} \\ p \neq q}} \frac{5}{p-2} \cdot \frac{5}{q-2} + \ldots,$$

valabilă $(\forall)\, u \in \mathbf{N}^*$ $\left(\frac{4}{(p-2)^2} \leq \frac{1}{p-2}\right.$ deoarece $p \geq 6$; în caz că nu există p prim astfel încât $p \geq 17$, $p|u$ atunci $S(u) = 1$ și evaluările de mai sus au sens considerând sumele care apar mai sus ca fiind egale cu zero).

Pentru un $x \in \mathbf{N}^*$ și p număr prim, $p \geq 17$, $p \leq x$, termenul $\frac{5}{p-2}$ apare în suma $\sum_{u=1}^{x} S^2(u)$ de $\left[\frac{x}{p}\right]$ ori (deoarece $p, 2p, 3p, \ldots, \left[\frac{x}{p}\right]p$ sunt toți multiplii de p,

mai mici sau egali cu x). De asemenea dacă p, q sunt numere prime astfel încât $p \neq q$, $17 \leq p, q \leq x$ atunci $\frac{5}{p-2} \cdot \frac{5}{q-2}$ apare în $\sum_{u=1}^{x} S^2(u)$ de $\left[\frac{x}{pq}\right]$ ori și așa mai departe. Ținând cont de inegalitatea $[y] \leq y$ $(\forall)$ $y \in \mathbf{R}$, deducem din cele de mai sus că

$$\sum_{u=1}^{x} S^2(u) \leq x + \sum_{\substack{p\text{-prim} \\ 17 \leq p \leq x}} \frac{x}{p} \cdot \frac{5}{p-2} + \sum_{\substack{p,q\text{-prime} \\ 17 \leq p,q \leq x \\ p \neq q}} \frac{x}{pq} \cdot \frac{5}{p-2} \cdot \frac{5}{q-2} + \ldots =$$

$$= x\left(1 + \sum_{\substack{p\text{-prim} \\ 17 \leq p \leq x}} \frac{5}{p(p-2)} + \sum_{\substack{p,q\text{-prime} \\ 17 \leq p,q \leq x \\ p \neq q}} \frac{5}{p(p-2)} \cdot \frac{5}{q(q-2)} + \ldots\right) =$$

$$= x \prod_{\substack{p\text{-prim} \\ 17 \leq p \leq x}} \left(1 + \frac{5}{p(p-2)}\right) \leq x \prod_{k=17}^{x} \left(1 + \frac{5}{k(k-2)}\right) \leq$$

$$\leq x\, e^{\sum_{k=17}^{x} \frac{5}{k(k-2)}} \leq x\, e^{\sum_{k=17}^{\infty} \frac{5}{k(k-2)}} \leq x\, e^{\sum_{k=17}^{\infty} \frac{5}{(k-1)(k-2)}} = x\, e^{5 \cdot \frac{1}{15}} = x\, e^{\frac{1}{3}} \leq 2x$$

(am ținut cont în cele de mai sus de inegalitatea $1 + x \leq e^x$ $(\forall)$ $x \in \mathbf{R}$, de faptul că

$$\frac{5}{k(k-2)} < \frac{5}{(k-1)(k-2)}$$

precum și de egalitatea

$$\sum_{k=17}^{\infty} \frac{1}{(k-1)(k-2)} = \sum_{k=17}^{\infty} \left(\frac{1}{(k-2)} - \frac{1}{(k-1)}\right) = \frac{1}{15}.$$

Deci teorema 3 este demonstrată cu $c_2 = 2$.

Demonstrația teoremei 2: Deocamdată $x_1 \in \mathbf{N}^*$, $x_1 \geq 17^9$. Pe parcursul demonstrației vom puncta momentele în care x_1 mai trebuie mărit pentru a fi îndeplinite anumite inegalități (care nu-l implică însă în nici un fel pe u). Notăm cu $q_1, q_2, q_3, \ldots q_r$ numerele prime cuprinse în intervalul $[17, x^{\frac{1}{9}}]$ care nu-l divid pe u; $x \geq x_1$, $x \in \mathbf{N}$, $17 \leq q_1 < q_2 < q_3 < \ldots < q_r$ (se poate întâmpla să nu existe p număr prim astfel încât $p \nmid u$, $17 \leq p \leq x^{\frac{1}{9}}$; aceasta nu constituie nici un impediment pentru considerațiile ce urmează). $A(u, x)$ înseamnă numărul de soluții al ecuației $a_i - a_j = u$, unde $a_i \leq x$, $((\forall)\ 0 < u \leq x;\ u \in \mathbf{N})$. Soluțiile ecuației prim

precedente în care $a_i \le x^{\frac{1}{9}}$ sau $a_j \le x^{\frac{1}{9}}$ sunt în număr de cel mult $2x^{\frac{1}{9}}$. Soluțiile ecuației $a_i - a_j = u$, unde $x^{\frac{1}{9}} < a_i \le x$, $a_j > x^{\frac{1}{9}}$ (condițiile acestea asigură faptul că $q_k \nmid a_i$, $q_k \nmid a_j$ $(\forall)\ k = \overline{1,r}$) se află printre soluțiile ecuației $a - b = u$, $a,b \in \mathbf{N}$, $q_k \nmid a \cdot b$, $(\forall)\ k = \overline{1,r}$ $a \le x$. Pentru a afla soluțiile ultimei ecuații e suficient să indicăm toate numerele $a \in \mathbf{N}$, $a \ge u$, pentru care $q_k \nmid a(a-u)$, $(\forall)\ k = \overline{1,r}$. Din considerațiile anterioare deducem că

(1) $A(u, x) \le 2x^{\frac{1}{9}} + P(x; q_1, q_2, \ldots q_r)$,

unde am notat prin $P(x; q_1, q_2, \ldots q_r)$ numărul de numere naturale nenule n pentru care $n \not\equiv 0 \pmod{q_k}$ și $n \not\equiv u \pmod{q_k}$, $(\forall)\ k = \overline{1,r}$ și $n \le x$. În general vom nota cu $P(A, D, x; d_1, e_1, t_1; d_2, e_2, t_2; \ldots; d_r, e_r, t_r)$ numărul de numere naturale nenule n pentru care $n \le x$, $n \not\equiv A \pmod{D}$, $(n - d_i)(n - e_i) \not\equiv 0 \pmod{t_i}$, $(\forall)\ i = 1, r$, unde $D \in \mathbf{N}^*$, $A \in \mathbf{N}$, $t_1, t_2, \ldots, t_r$ sunt numere prime distincte pentru care $t_i \nmid D$, $(\forall)\ i = \overline{1,r}$, iar $d_1, e_1, d_2, e_2, \ldots, d_r, e_r$ sunt numere întregi pentru care $e_i \not\equiv d_i \pmod{t_i}$, $(\forall)\ i = \overline{1,r}$. Pentru a ușura scrierea vom omite anumite simboluri ele fiind sau subînțelese sau fără relevanță pentru scopurile urmărite (în general obținerea unor inegalități care nu depind de simbolurile omise). În cazul nostru, $d_i = 0$ și $e_i = u$ $(\forall)\ i = \overline{1,r}$, $t_i = q_i$, $(\forall)\ i = 1,r$ ($d_i \equiv e_i \pmod{t_i}$ deoarece $q_i \nmid u$, $(\forall)\ i = \overline{1,r}$), $D = 1$, A un număr natural oarecare (de exemplu $A = 0$). Definim

$$(2)\quad \begin{cases} h_0 = 1{,}29 \\ h = \dfrac{89}{69} \end{cases} \qquad 1 < h < ho\ (h \simeq 1{,}289855).$$

Au loc următoarele inegalități

$$(3)\quad \begin{cases} 1 - \dfrac{2}{q_1} \ge 1 - \dfrac{2}{17} \ge 1 - 0{,}12 = 0{,}88 > 0{,}61 > \dfrac{1}{h_0^2} \\ \dfrac{1}{\ln h_0} \sim \dfrac{1}{0{,}2546} < 4 \le 17 \le q_1 \ \text{ deci } \ \dfrac{1}{\ln h_0} < q_1, \end{cases}$$

eroarea în scrierea logaritmului natural este de cel mult 10^{-4}.

Folosind corolarul teoremei 2 din paragraful I al anexei deducem existența unei constante c_5 pentru care $\lim\limits_{z \to \infty} \left(\sum\limits_{\substack{p\text{-prim} \\ p \le z}} \dfrac{1}{p} - \ln\ln z - c_5 \right) = 0$. Calculăm mare număr

$$\lim_{z\to\infty}\left(\sum_{\substack{p\text{-prim}\\ z<p\le z^h}}\frac{1}{p}\right)=\lim_{z\to\infty}\left(\sum_{\substack{p\text{-prim}\\ p\le z^h}}\frac{1}{p}-\ln\ln z^h-c_5-\sum_{\substack{p\text{-prim}\\ p\le z}}\frac{1}{p}+\ln\ln z+c_5+\ln\ln z^h-\ln\ln z\right)$$

$=\lim_{z\to\infty}\left(\ln(h\ln z)-\ln\ln z\right)=\ln h<\ln h_0$ (în plus limita precedentă este mai mare strict decât 0 deoarece $h > 1$). Conform teoremei 3 din paragraful I al anexei știm că există o constantă reală strict pozitivă c_6 pentru care

$$\lim_{z\to\infty}\ln^2 z\cdot\prod_{\substack{p\text{-prim}\\ 3\le p\le z}}\left(1-\frac{2}{p}\right)=c_6.$$

Putem calcula atunci următoarea limită $\lim_{z\to\infty}\prod_{\substack{z\le p\le z^h\\ p\text{-prim}}}\left(1-\frac{2}{p}\right)=$

$$=\lim_{z\to\infty}\left(\ln^2 z^h\cdot\prod_{\substack{3\le p\le z^h\\ p\text{-prim}}}\left(1-\frac{2}{p}\right)\cdot\frac{1}{\ln^2 z\prod_{\substack{3\le p\le z\\ p\text{-prim}}}\left(1-\frac{2}{p}\right)}\cdot\frac{\ln^2 z}{\ln^2 z^h}\right)=\frac{c_6}{c_6}\lim_{z\to\infty}\frac{\ln^2 z}{h^2\ln^2 z}=$$

$=\frac{1}{h^2}>\frac{1}{h_0^2}$. Din cele demonstrate mai sus deducem existența unui $z_0\in\mathbf{R}_+$ pentru care să se întâmple următoarele inegalități

$$(4)\quad\begin{cases}0<\sum_{\substack{p\text{-prim}\\ z<p\le z^h}}\frac{1}{p}<\ln h_0\\ \prod_{\substack{p\text{-prim}\\ z<p\le z^h}}\left(1-\frac{2}{p}\right)>\frac{1}{h_0^2}\end{cases}\qquad(\forall)\,z\in\mathbf{R},\,z>z_0.$$

Rezultatele din anexa teoremei lui Brun (propozițiile 3 și 4 din paragraful I al anexei teoremei lui Brun) nu erau suficiente pentru justificarea inegalităților (4), de aceea a fost realmente necesar demonstrarea teoremelor 2 și 3 din paragraful I al anexei, care constituie întăriri ale rezultatelor citate mai sus. În cele ce urmează vom defini o secvență de numere naturale

$$r_{n+1}=0<r_n<r_{n-1}<\ldots<r_1<<r=r_0.$$

Dacă $q_r>z_0$ alegem $r_1<r$ astfel încât q_{r_1} este cel mai mare număr prim mai mic sau egal cu $q_r^{\frac{1}{h}}$, în ipoteza că $q_{r_1}>z_0$. Apoi alegem r_2 astfel încât q_{r_2} este cel mai

mare număr prim mai mic sau egal cu $q_r^{\frac{1}{h^2}}$ în ipoteza că $q_{r_2} > z_0$ (în această situație conform formulelor (4) deduc că $\sum_{\substack{q_r^{\frac{1}{h^2}} < p \le q_r^{\frac{1}{h}} \\ p\text{-prim}}} \frac{1}{p} > 0$ și deci $r_2 < r_1$; la fel $\sum_{\substack{q_r^{\frac{1}{h}} < p \le q_r \\ p\text{-prim}}} \frac{1}{p} > 0$, în situația în care $q_{r_1} > z_0$ și deci $r_1 < r_0$).

Continuăm această alegere a numerelor r_m atâta vreme cât $q_{r_m} > z_0$. Fie q_{r_k} cel mai mic număr prim care a fost ales ca mai sus. Conform formulelor (4) au loc următoarele inegalități:

$$(5)\quad \begin{cases} 0 < \sigma_1 = \sum_{v=r_1+1}^{r} \frac{1}{q_v} < \ln h_0,\ \Pi_1 = \prod_{v=r_1+1}^{r} \left(1 - \frac{2}{q_v}\right) > \frac{1}{h_0^2} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 < \sigma_k = \sum_{v=r_k+1}^{r_{k-1}} \frac{1}{q_v} < \ln h_0,\ \Pi_k = \prod_{v=r_k+1}^{r_{k-1}} \left(1 - \frac{2}{q_v}\right) > \frac{1}{h_0^2} \end{cases}$$

(într-adevăr, $(\forall)\ i = \overline{1,k}$, $0 < \sigma_i < \sum_{\substack{q_r^{\frac{1}{h^i}} < p \le q_r^{\frac{1}{h^{i-1}}} \\ p\text{-prim}}} \frac{1}{p} < \ln h_0$ deoarece $q_r^{\frac{1}{h^i}} \ge q_{r_i} > z_0$ și se poate aplica într-adevăr formula (4). La fel

$$\Pi_i \ge \prod_{\substack{q_r^{\frac{1}{h^i}} < p \le q_r^{\frac{1}{h^{i-1}}} \\ p\text{-prim}}} \left(1 - \frac{2}{p}\right) > \frac{1}{h_0^2},$$

$(\forall)\ i = \overline{1,k}$, deoarece $q_r^{\frac{1}{h^i}} \ge q_{r_i} > z_0$ și se poate aplica într-adevăr formula (4)).

Inegalitățile $r = r_0 > r_1 > r_2 > \ldots\ldots > r_k$ se justifică în aceeași manieră în care s-a arătat mai sus că $r_2 < r_1 < r = r_0$. Vom alege succesiv numerele naturale r_m $(m = \overline{k+1,\ n+1})$ ca fiind cele mai mici numere naturale μ pentru care au loc simultan inegalitățile:

$$(6)\quad \begin{cases} 0 < \sum_{v=\mu+1}^{r_{m-1}} \frac{1}{q_v} < \ln h_0 \\ \prod_{v=\mu+1}^{r_{m-1}} \left(1 - \frac{2}{q_v}\right) > \frac{1}{h_0^2}. \end{cases}$$

Acest μ există într-adevăr deoarece $\frac{1}{q_{r_{m-1}}} \leq \frac{1}{q_1} < \ln h_0$ și $1 - \frac{2}{q_{r_{m-1}}} \geq 1 - \frac{2}{q_1} > \frac{1}{h_0^2}$

conform formulelor (3).

Și pentru $m = \overline{k+1,\ n+1}$ folosim notațiile:

$$\sigma_m = \sum_{v=r_m+1}^{r_{m+1}} \frac{1}{q_v}, \quad \Pi_m = \prod_{v=r_m+1}^{r_{m+1}} \left(1 - \frac{2}{q_v}\right)$$

Conform celor arătate anterior au loc inegalitățile

(7) $0 < \sigma_i < \ln h_0,\ \Pi_i > \frac{1}{h_0^2},\ (\forall)\ i = \overline{1,n+1}.$

Dacă $q_r \leq z_0$ (sau cel mai mare număr prim q_i care este mai mic sau egal cu $q_r^{\frac{1}{h}}$, este mai mic sau egal cu z_0) atunci r_m (pentru $m = \overline{1,n+1}$) se definește ca fiind cel mai mic număr natural μ pentru care au loc inegalitățile (6) (definirea se face evident succesiv. Definim întâi r_1; cu ajutorul lui r_1, definim r_2 și așa mai departe). Și în acest caz folosim notațiile anterioare σ_i, Π_i (au loc inegalitățile (7), $(\forall)\ i = \overline{1,n+1}$). Este evident că procedeul anterior este finit. Toate aceste preparative se fac pentru a putea majora pe $P(x, q_1, q_2, \ldots q_r)$ și implicit (conform inegalității (1)) pe $A(u, x)$, ceea ce este chiar scopul teoremei 2.

Să arătăm că are loc o egalitate de tipul:

(9) $$P(A, D, x; t_1, t_2, \ldots, t_r) = P(A, D, x; t_1, t_2, \ldots, t_{r-1}) -$$
$$- P(A_1, Dt_r, x; t_1, t_2, \ldots, t_{r-1}) - P(A_2, Dt_r, x; t_1, t_2, \ldots, t_{r-1}).$$

Pentru a demonstra egalitatea (9) să observăm că numerele numărate de $P(A, D, x; t_1, t_2, \ldots, t_r)$ sunt acelea numărate de $P(A, D, x; t_1, t_2, \ldots, t_{r-1})$ din care se scot acele numere naturale nenule z pentru care $z \equiv A \pmod D$, $z \leq x$ și în plus $z \equiv d_r \pmod{t_r}$ sau $z \equiv e_r \pmod{t_r}$. Fie $A_1 \in \mathbf{N}$ astfel încât $A_1 \equiv A \pmod D$ și $A_1 \equiv d_r \pmod{t_r}$, $A_2 \in \mathbf{N}$ astfel încât $A_2 \equiv A \pmod D$ și $A_2 \equiv e_r \pmod{t_r}$ (există A_1 și A_2 conform lemei chineze a resturilor; $t_i \nmid D$, $(\forall)\ i = \overline{1,r}$). De asemenea $A_1 \not\equiv A_2 \pmod{Dt_r}$ deoarece $d_r \not\equiv e_r \pmod{t_r}$. Formula (9) este astfel demonstrată. Ea va fi scrisă simbolic (pentru a ușura scrierea):

(10) $P(D,x; t_1 \ldots t_m) = P(D,x; t_1, \ldots, t_{m-1}) - 2P(Dt_m, x; t_1, t_2, \ldots, t_{m-1})$.

Aplicând formula (10) de mai multe ori în cazul nostru particular obținem că:

(11) $$P(x; q_1, q_2, \ldots q_r) = P(1, x) - 2P(q_1, x) - 2P(q_2, x; q_1) -$$
$$- 2P(q_3, x; q_1, q_2) - \ldots - 2P(q_r, x; q_1, q_2, \ldots q_{r-1}).$$

Aplicând din nou formula (10) în egalitatea (11) de mai multe ori

$$(P(q_2, x; q_1) = P(q_2; x) - 2P(q_1 q_2, x);$$

$$P(q_3, x; q_1, q_2) = P(q_3, x; q_1) - 2P(q_3 q_2, x; q_1)$$

și așa mai departe) obținem:

$$(12)\ P(x; q_1, q_2, \ldots q_r) = P(1, x) - 2\sum_{\alpha=1}^{r} P(q_\alpha, x) + 4\sum_{\alpha=1}^{r}\sum_{\beta=1}^{\alpha-1} P(q_\alpha q_\beta, x; q_1, q_2, \ldots q_{\beta-1}).$$

(Pentru a ușura scrierea am pus în suma dublă de mai sus pe α să parcurgă numerele naturale de la 1 la r însă e clar că, pentru $\alpha = 1$, $\nexists\, \beta \in \mathbf{N}^*$, $\beta < \alpha$ și deci termenul corespunzător lui $\alpha = 1$ trebuie considerat 0. În cele ce urmează vom mai folosi această convenție). Deoarece

$$P(D, x; t_1, \ldots, t_m) \le P(D, x; t_1, t_2, \ldots, t_j),$$

$(\forall)\, j \le m$, din formula (12) deducem:

$$(13)\qquad P(x; q_1, q_2, \ldots, q_r) \le P(1,x) - 2\sum_{\alpha=1}^{r} P(q_\alpha, x) + 4\sum_{\alpha=1}^{r}\sum_{\beta<\alpha} P(q_\alpha q_\beta, x; q_1, q_2, \ldots, q_{\min(\beta-1, r_1)}).$$

Continuând procedeul care a condus la (13) obținem:

$$(14)\qquad P(x; q_1, q_2, \ldots, q_r) \le P(1,x) - 2\sum_{\alpha=1}^{r} P(q_\alpha, x) + 4\sum_{\alpha=1}^{r}\sum_{\beta<\alpha} P(q_\alpha q_\beta, x) -$$

$$-8\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\sum_{\gamma=1}^{\min(\beta-1, r_1)} P(q_\alpha q_\beta q_\gamma, x) \ldots - 2^{2n-1}\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\sum_{\gamma=1}^{\min(\beta-1, r_1)}\sum_{\delta<\gamma} \ldots \sum_{\lambda=1}^{\min(\theta-1, r_{n-1})} P(q_\alpha q_\beta q_\gamma q_\delta \ldots q_\lambda, x) +$$

$$+ 2^{2n}\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\sum_{\gamma=1}^{\min(\beta-1, r_1)}\sum_{\delta<\gamma} \ldots \sum_{\lambda=1}^{\min(\theta-1, r_{n-1})}\sum_{\mu<\lambda} P\left(q_\alpha q_\beta \ldots q_\lambda q_\mu, x; q_1 q_2 \ldots q_{\min(\mu-1, r_n)}\right).$$

Deoarece

$$P(D,x; t_1, \ldots, t_m) \le P(D,x)$$

și

$$\left[\frac{x}{D}\right] \le P(D,x) \le \left[\frac{x}{D}\right] + 1$$

(conform propoziției 3 din paragraful 2 al anexei teoremei lui Brun), deducem (folosind (14)) inegalitatea:

$$(15)\ P(x; q_1, q_2, \ldots, q_r) \le x\left[1 - 2\sum_{\alpha=1}^{r}\frac{1}{q_\alpha} + 4\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\frac{1}{q_\alpha q_\beta} - \right.$$

$$\left. - 8\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\sum_{\gamma=1}^{\min(\beta-1, r_1)}\frac{1}{q_\alpha q_\beta q_\gamma} + \ldots + 2^{2n}\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\ldots\sum_{\lambda=1}^{\min(\theta-1, r_{n-1})}\sum_{\mu<\lambda}\frac{1}{q_\alpha q_\beta \ldots q_\lambda q_\mu}\right] + R, \text{ unde}$$

R este suma unor termeni reali de modul cel mult 1 ($P(D,x) = \dfrac{x}{D} + \varepsilon$, unde $|\varepsilon| \le 1$)). Pentru a putea să-l evaluăm pe R trebuie să putem majora numărul de termeni ai sumei de mai sus. Numărul de termeni ai sumei de

mai sus este mai mic sau egal cu numărul de termeni din $\left(1-\sum_{\alpha=1}^{r}\frac{2}{q_\alpha}\right)\left(1-\sum_{\beta=1}^{r_1-1}\frac{2}{q_\beta}\right)\left(1-\sum_{\gamma=1}^{r_2}\frac{2}{q_\gamma}\right)\left(1-\sum_{\delta=1}^{r_3-1}\frac{2}{q_\delta}\right)$ (după ce se fac înmulțirile). Deci

$$R \le r\,(r+1)\,r_1(r_1+1)\ldots r_{n-1}(r_{n-1}+1) \le (2r+1)^2\,(2r_1+1)^2\ldots(2r_{n-1}+1)^2$$

(deoarece $r, r_1, \ldots, r_{n-1} \in \mathbf{N}$). Avem că $q_l \ge 2l+1$, $(\forall)\ l = \overline{1,r}$ (se demonstrează prin recurență după l. $q_1 \ge 17 \ge 2\cdot 1+1 = 3$. Dacă $q_l \ge 2l+1$ atunci

$$q_{l+1} \ge q_l + 2 \ge 2l+3 = 2(l+1)+1.$$

Acest raționament a mai fost făcut). Conform observațiilor precedente, precum și datorită alegerii lui $r_1, r_2, \ldots, r_n$, rezultă că:

(16) $$R \le q_r^2 q_{r_1}^2 q_{r_2}^2 \ldots q_{r_{n-1}}^2 \le q_r^2 q_r^{\frac{2}{h}} q_r^{\frac{2}{h^2}} \ldots q_r^{\frac{2}{h^k}} q_{r_{k+1}}^2 \ldots q_{r_{n-1}}^2.$$

Să arătăm acum că $q_{r_{k+1}} \le z_0$. Avem două cazuri de analizat: 1) $q_r^{\frac{1}{h^{k+1}}} > z_0$ și 2) $q_r^{\frac{1}{h^{k+1}}} \le z_0$.

Să analizăm prima situație. În ipoteza că $q_{r_{k+1}} > z_0$ atunci conform definiției lui k trebuie neapărat să aibă loc inegalitățile: $q_r^{\frac{1}{h^k}} \ge q_{r_k} > q_{r_{k+1}} > q_r^{\frac{1}{h^{k+1}}} > z_0$.

Aplicând formulele (4) (pentru $z = q_r^{\frac{1}{h^{k+1}}}$) deducem atunci că

$$0 < \sum_{\nu=r_{k+1}}^{r_k}\frac{1}{q_\nu} < \ln h_0$$

și

$$\prod_{\nu=r_{k+1}}^{r_k}\left(1-\frac{2}{q_\nu}\right) > \frac{1}{h_0^2}.$$

ceea ce contrazice alegerea lui r_{k+1} (vezi formulele (6); r_{k+1} era cel mai mic număr natural pentru care au loc inegalitățile (6) cu $m = k+1$. Din cele de mai sus s-a văzut că și $\mu = r_{k+1} - 1$ satisface inegalitățile (6), ceea ce este evident absurd). Deci în primul caz neapărat $q_{r_{k+1}} \le z_0$. Să analizăm acum cel de-al doilea caz și să presupunem din nou că $q_{r_{k+1}} > z_0$. Alegem $z \in \mathbf{R}$ astfel încât $z_0 < z < q_{r_{k+1}}$. Deducem, ținând cont de inegalitatea $q_r^{\frac{1}{h^{k+1}}} \le z_0$, că $z_0 < z < q_{r_{k+1}} < q_{r_k} \le q_r^{\frac{1}{h^k}} = \left(q_r^{\frac{1}{h^{k+1}}}\right)^h \le z_0^h < z^h$. Aplicând din

nou formulele (4), pentru acest z se obține că

$$0 < \sum_{\nu=r_{k+1}}^{r_k} \frac{1}{q_\nu} < \ln h_0$$

și

$$\prod_{\nu=r_{k+1}}^{r_k} \left(1 - \frac{2}{q_\nu}\right) > \frac{1}{h_0^2}$$

ceea ce constituie o contradicție cu alegerea lui r_{k+1} după cum s-a văzut ceva mai sus. Deci și în acest caz $q_{r_{k+1}} \leq z_0$. Din considerațiile precedente precum și din inegalitatea (16) deducem existența unei constante reale pozitive c_7 astfel încât să aibă loc inegalitățile:

$$(17) \quad R \leq c_7 q_r^{\frac{2h}{h-1}} = c_7 q_r^{\frac{89}{10}} \leq c_7 x^{\frac{89}{90}} \leq c_7 \frac{x}{\ln^2 x}.$$

Trebuie precizat în acest moment că x_1, trebuie ales suficient de mare astfel încât oricare ar fi $x \geq x_1$ să aibă loc inegalitatea $\ln^2 x \leq x^{\frac{1}{90}}$ (există un astfel de x_1 deoarece $\lim_{x\to\infty} \frac{x^{\frac{1}{90}}}{\ln^2 x} = \infty$). În stabilirea inegalității (17) s-a ținut cont că $h = \frac{89}{69}$, $q_r \leq x^{\frac{1}{9}}$ și

$$1 + \frac{1}{h} + \ldots + \frac{1}{h^k} \leq \sum_{i=0}^{\infty} \frac{1}{h^i} = \frac{1}{1 - \frac{1}{h}} = \frac{h}{h-1}.$$

Folosind notațiile:

$$E^{(1)} = \sum_{\alpha=1}^{r} \frac{2}{q_\alpha},$$

$$E^{(2)} = \sum_{\alpha=1}^{r} \sum_{\beta<\alpha} \frac{2}{q_\alpha} \cdot \frac{2}{q_\beta},$$

$$E^{(3)} = \sum_{\alpha=1}^{r} \sum_{\beta<\alpha} \sum_{\gamma=1}^{\min(\beta-1, r_1)} \frac{2}{q_\alpha} \cdot \frac{2}{q_\beta} \cdot \frac{2}{q_\gamma}, \ldots,$$

$$E^{(2n)} = \sum_{\alpha=1}^{r} \sum_{\beta<\alpha} \sum_{\gamma=1}^{\min(\beta-1, r_1)} \ldots \sum_{\lambda=1}^{\min(\theta-1, r_{n-1})} \sum_{\mu<\lambda} \frac{2}{q_\alpha} \cdot \frac{2}{q_\beta} \cdot \frac{2}{q_\gamma} \ldots \frac{2}{q_\lambda} \cdot \frac{2}{q_\mu},$$

$$E = 1 - E^{(1)} + E^{(2)} - E^{(3)} + \ldots + E^{(2n)},$$

deducem din inegalitățile (17), (15) și (1) că:

(18) $A(u, x) \leq 2\, x^{\frac{1}{9}} + c_7 \frac{x}{\ln^2 x} + xE$, $(\forall)\, x \geq x_1$.

Pentru a putea demonstra teorema lui Brun trebuie să reușim să-l evaluăm pe E în mod convenabil. Vom nota cu $E_m^{(i)}$ o sumă de același tip cu $E^{(i)}$ în care se impune în plus condiția ca toți indicii care apar (α, β, γ ...) să fie mai mari strict decât r_m; m poate fi orice număr natural de la 1 la $n+1$, iar $i \in \mathbf{N}^*$. Pentru $m \leq n$ avem că $E_m^{(i)} = 0$, dacă $i > 2m$. Într-adevăr, dacă $i > 2m$, atunci al $(2m+1)$-lea indice (α e primul indice, β al doilea și așa mai departe) trebuie să fie mai mic sau egal cu r_m pe de o parte și mai mare strict decât r_m pe de altă parte (vezi definiția lui $E_m^{(i)}$), deci suma care-l definește pe $E_m^{(i)}$ nu va conține nici un termen; ceea ce înseamnă că $E_m^{(i)} = 0$. Este evident că $E_{n+1}^{(i)} = 0$ pentru $i > 2n$, $E_{n+1}^{(i)} = E^{(i)}$, $(\forall)\, i = \overline{1,2n}$. Vom nota cu $E_m = 1 - E_m^{(1)} + E_m^{(2)} - E_m^{(3)} + \ldots$ (ultimul termen al sumei este $E_m^{(2m)}$, dacă $m \leq n$ și $E_{n+1}^{(2n)}$, dacă $m = n+1$). Este evident că $E_{n+1} = E$. Vom nota cu $S_m^{(1)}$, $S_m^{(2)}$,... funcțiile simetrice elementare calculate pentru valorile: $\frac{2}{q_{r_m+1}}, \frac{2}{q_{r_m+2}} \ldots \frac{2}{q_{r_{m-1}}}$. În continuare vom stabili o formulă de recurență pentru $E_m^{(i)}$.

Suma tuturor termenilor care apar în $E_m^{(i)}$ și pentru care toți indicii sunt mai mici sau egali cu r_{m-1}, este egală cu $S_m^{(i)}$.

Suma tuturor termenilor care apar în $E_m^{(i)}$ și pentru care doar primul indice (adică α) este mai mare strict decât r_{m-1}, este egală cu $E_{m-1}^{(1)} S_m^{(i-1)}$. Suma tuturor termenilor care apar în $E_m^{(i)}$ și pentru care doar primii doi indici (α și β) sunt mai mari strict decât r_{m-1}, este egală cu $E_{m-1}^{(2)} S_m^{(i-2)}$. În general, suma tuturor termenilor care apar în $E_m^{(i)}$ și pentru care doar primii l indici sunt mai mari strict decât r_{m-1}, este egală cu $E_{m-1}^{(l)} S_m^{(i-l)}$. Suma tuturor termenilor care apar în $E_m^{(i)}$ și pentru care toți indicii sunt mai mari strict decât r_{m-1}, este egală cu $E_{m-1}^{(i)}$. Am obținut deci formula:

(19) $E_m^{(i)} = S_m^{(i)} + E_{m-1}^{(1)} S_m^{(i-1)} + E_{m-1}^{(2)} S_m^{(i-2)} + \ldots + E_{m-1}^{(i)}$

valabilă pentru orice $m = \overline{2,n+1}$. Cu ajutorul ei deducem că:

(20) $E_m = 1 - (S_m^{(1)} + E_{m-1}^{(1)}) + (S_m^{(2)} + E_{m-1}^{(1)} S_m^{(1)} + E_{m-1}^{(2)}) - \ldots + (S_m^{(2m-2)} + E_{m-1}^{(1)} S_m^{(2m-3)} + \ldots + E_{m-1}^{(2m-2)}) - (S_m^{(2m-1)} + E_{m-1}^{(1)} S_m^{(2m-2)} + \ldots + E_{m-1}^{(2m-2)} S_m^{(1)}) + (S_m^{(2m)} + E_{m-1}^{(1)} S_m^{(2m-1)} + \ldots + E_{m-1}^{(2m-2)} S_m^{(2)})$ (am folosit mai sus și faptul că $E_{m-1}^{(j)} = 0$, $(\forall) j > 2m-2$, $(\forall)\, m = \overline{2,n+1}$).

Expresia lui E_m din formula (20) o vom compara cu:

(21) $E_{m-1}\Pi_m = E_{m-1}\prod_{v=r_m+1}^{r_{m-1}}\left(1-\frac{2}{q_v}\right) = (1-E_{m-1}^{(1)}+E_{m-1}^{(2)}\ldots.)(1-S_m^{(1)}+S_m^{(2)}-\ldots) =$

$= 1-(S_m^{(1)}+E_{m-1}^{(1)})+(S_m^{(2)}+E_{m-1}^{(1)}S_m^{(1)}+E_{m-1}^{(2)})-\ldots+(S_m^{(2m-2)}+E_{m-1}^{(1)}S_m^{(2m-3)}+\ldots$

$+E_{m-1}^{(2m-2)})-(S_m^{(2m-1)}+E_{m-1}^{(1)}S_m^{(2m-2)}+\ldots+E_{m-1}^{(2m-2)}S_m^{(1)})+(S_m^{(2m)}+E_{m-1}^{(1)}S_m^{(2m-1)}+\ldots$

$+E_{m-1}^{(2m-2)}S_m^{(2)})-(S_m^{(2m+1)}+E_{m-1}^{(1)}S_m^{(2m)}+\ldots+E_{m-1}^{(2m-2)}S_m^{(3)})+\ldots$

Conform inegalității lui Schlomilch (teorema 4 din paragraful I al anexei) avem că:

(22) $\frac{S_m^{(1)}}{t}>\frac{2S_m^{(2)}}{(t-1)S_m^{(1)}}>\frac{3S_m^{(3)}}{(t-2)S_m^{(2)}}>\ldots>\frac{tS_m^{(t)}}{S_m^{(t-1)}}$, unde $t = r_{m-1} - r_m$. De aici deducem că $\frac{S_m^{(j+1)}}{S_m^{(j)}}<\frac{j(t-j)S_m^{(j)}}{(j+1)(t-j+1)S_m^{(j-1)}}<\frac{S_m^{(j)}}{S_m^{(j-1)}}$, $(\forall)\, j=\overline{1,t-1}\,(S_m^{(0)}=1)$. Din aceste inegalități rezultă că $\frac{S_m^{(t)}}{S_m^{(t-1)}}<\frac{S_m^{(t-1)}}{S_m^{(t-2)}}<\ldots<\frac{S_m^{(2)}}{S_m^{(1)}}<S_m^{(1)}=2\sigma_m<2\ln h_0 =$

$= 2\ln 1{,}29 < 2\cdot 0{,}255 = 0{,}51 < 1$ și ca o consecință:

(23) $S_m^{(t)} < S_m^{(t-1)} < \ldots < S_m^{(3)} < S_m^{(2)} < S_m^{(1)} < 0{,}51 < 1.$

Comparând expresiile (20), (21) și ținând cont de inegalitățile (23) deducem următoarea evaluare importantă:

(24) $E_m \le E_{m-1}\,\Pi_m + (S_m^{(2m+1)} + E_{m-1}^{(1)}S_m^{(2m)} + \ldots + E_{m-1}^{(2m-2)}S_m^{(3)})$ (convenim că $S_m^{(j)} = 0\,(\forall) j \in \mathbf{N}, j > t$). Să observăm că din formulele (22) printr-un raționament de recurență concluzionăm că:

(25) $S_m^{(i)} \le \frac{(S_m^{(1)})^i}{i!}$, $(\forall)\, i \in \mathbf{N}^*$ (dacă $i > t$ inegalitatea este absolut evidentă).

Într-adevăr, pentru $i = 1$ inegalitatea este clară (de fapt e chiar egalitate în acest caz). Presupunem că formula (25) e adevărată pentru un i și vrem să o demonstrăm pentru $i + 1$ (în caz că $i + 1 \le t$; altminteri este evident). Din (22) deducem că $\frac{S_m^{(i+1)}}{S_m^{(i)}}<\frac{(t-i)}{t(i+1)}S_m^{(1)}<\frac{S_m^{(1)}}{(i+1)}$. Deci $S_m^{(i+1)} < S_m^{(i)}\cdot\frac{S_m^{(1)}}{(i+1)} \le \frac{(S_m^{(1)})^i}{i!}\cdot\frac{S_m^{(1)}}{i+1} = \frac{(S_m^{(1)})^{i+1}}{(i+1)!}$ (am folosit ipoteza de recurență). Formula (25) este astfel demonstrată.

Notând cu $\Phi_m = S_m^{(2m+1)} + E_{m-1}^{(1)}S_m^{(2m)} + \ldots + E_{m-1}^{(2m-2)}S_m^{(3)}$ obținem succesiv următoarele inegalități

$$E_2 \le E_1\Pi_2 + \Phi_2 \le \Pi_2(E_1 + h_0^2\Phi_2)$$

$E_3 \le E_2\Pi_3 + \Phi_3 \le \Pi_3 (E_2 + h_0^2\Phi_3) \le \Pi_3 (\Pi_2 (E_1 + h_0^2\Phi_2) + h_0^2\Phi_3) \le$
$\le \Pi_3 \cdot \Pi_2(E_1 + h_0^2\Phi_2 + h_0^4\Phi_3)$

și așa mai departe până când deducem că

(26) $E = E_{n+1} \le \Pi_2 \cdot \Pi_3 \ldots \cdot \Pi_{n+1}(E_1 + h_0^2\Phi_2 + h_0^4\Phi_3 + \ldots + h_0^{2n}\Phi_{n+1})$.

Pentru a obține rezultatele de mai sus s-au folosit inegalitățile (24) și (7) $\left(\Pi_i > \frac{1}{h_0^2},\ (\forall)\ i = \overline{1,n+1}\right)$. Notând cu $\tau = 2 \ln h_0$ din (7) rezultă că $S_m^{(1)} = 2\sigma_m <$
$< 2 \ln h_0 = \tau < 1$ și deci (conform inegalității (25)) $S_m^{(i)} \le \frac{\tau^i}{i!}$, $(\forall)\ i \in \mathbf{N}^*$. Această din urmă inegalitate, împreună cu fomula (19), conduce la următoarele evaluări:

(27) $E_m^{(i)} \le \frac{\tau^i}{i!} + E_{m-1}^{(1)} \frac{\tau^{i-1}}{(i-1)!} + \ldots + E_{m-1}^{(i)}$

(28) $\Phi_m \le \frac{\tau^{2m+1}}{(2m+1)!} + E_{m-1}^{(1)} \frac{\tau^{2m}}{(2m)!} + \ldots + E_{m-1}^{(2m-2)} \frac{\tau^3}{3!}$.

Avem că $E_1^{(2)} = S_1^{(2)} < S_1^{(1)} = E_1^{(1)} < \tau$ (vezi (23)); de aici rezultă că $E_1^{(i)} < 9\left(\frac{\tau}{2}\right)^i$, $(\forall)\ i \in \mathbf{N}^*$. Verificarea trebuie făcută doar pentru $i = 1$ și $i = 2$ deoarece $E_1^{(i)} = 0$ pentru $i > 2$.

Cum $E_1^{(1)} < \tau < \frac{9\tau}{2}$ și $E_1^{(2)} < \tau < \frac{9\tau^2}{4}$ ($\tau = 2 \ln h_0 = 2 \ln 1{,}29 \simeq 2 \cdot 0{,}2546 >$
$> 2 \cdot 0{,}25 = 0{,}5 > 0{,}(4) = \frac{4}{9}$) rezultă că inegalitatea

(29) $E_1^{(i)} < 9\left(\frac{\tau}{2}\right)^i$, $(\forall)\ i \in \mathbf{N}^*$, este adevărată.

Punând $m = 2$ în inegalitatea (27) și ținând cont de (29) obținem că

(30) $$E_2^{(i)} \le \frac{\tau^i}{i!} + 9\frac{\tau}{2} \cdot \frac{\tau^{i-1}}{(i-1)!} + 9\left(\frac{\tau}{2}\right)^2 \cdot \frac{\tau^{i-2}}{(i-2)!} + \ldots + 9\left(\frac{\tau}{2}\right)^i \le$$
$$\le 9\left(\frac{\tau}{2}\right)^i \cdot \left[\frac{2^i}{i!} + \frac{2^{i-1}}{(i-1)!} + \frac{2^{i-2}}{(i-2)!} + \ldots + 1\right] \le 9\left(\frac{\tau}{2}\right)^i e^2,$$

$(\forall)\ i \in \mathbf{N}^*$. Raționând în același mod obținem că $E_3^{(i)} \le 9\left(\frac{\tau}{2}\right)^i e^4$, $(\forall)\ i \in \mathbf{N}^*$, și în general:

(31) $E_m^{(i)} \le 9e^{2(m-1)}\left(\frac{\tau}{2}\right)^i$, $(\forall)\ m, i \in \mathbf{N}^*$, $m \le n + 1$.

Folosind această din urmă inegalitate împreună cu evaluarea (28) obținem că:

$$(32)\quad \Phi_m \le \frac{\tau^{2m+1}}{(2m+1)!} + 9e^{2(m-2)}\frac{\tau}{2}\cdot\frac{\tau^{2m}}{(2m)!} + 9e^{2(m-2)}\left(\frac{\tau}{2}\right)^2\cdot\frac{\tau^{2m-1}}{(2m-1)!} + \dots$$

$$+9e^{2(m-2)}\left(\frac{\tau}{2}\right)^{(2m-2)}\cdot\frac{\tau^3}{3!} \le 9e^{2(m-2)}\left(\frac{\tau}{2}\right)^{2m+1}\left[\frac{2^{2m+1}}{(2m+1)!} + \frac{2^{2m}}{(2m)!} + \frac{2^{2m-1}}{(2m-1)!} + \dots \frac{2^3}{3!}\right] \le$$

$$\le 9e^{2(m-2)}\left(\frac{\tau}{2}\right)^{2m+1}\left[e^2 - \frac{2^2}{2!} - \frac{2}{1!} - 1\right] = 9e^{2(m-2)}\left(\frac{\tau}{2}\right)^{2m+1}\left(e^2 - 5\right)$$

$(\forall)\ m = \overline{2,n+1}$. Să observăm acum că $e^2 h_0^2\left(\frac{\tau}{2}\right)^2 \simeq 7{,}3891\cdot(1{,}29)^2\cdot(0{,}2546)^2 \simeq$

$\simeq 0{,}7970539 < 1$ $\left(e^2 h_0^2\left(\frac{\tau}{2}\right)^2 < 7{,}3892\cdot(1{,}29)^2\cdot(0{,}255)^2 \simeq 0{,}7995712 < 1\right)$.

Folosind inegalitățile (26) și (32) rezultă că

$$E < \Pi_2\Pi_3 \dots \Pi_{n+1}\left(E_1 + h_0^2\Phi_2 + h_0^4\Phi_3 + \dots + h_0^{2n}\Phi_{n+1}\right) <$$

$$< \Pi_2\Pi_3 \dots \Pi_{n+1}\left(E_1 + 9\left(\frac{\tau}{2}\right)^5(e^2-5)h_0^2 + 9(e^2-5)\left(\frac{\tau}{2}\right)^7 h_0^4 e^2 + \dots + 9(e^2-5)\left(\frac{\tau}{2}\right)^{2n+3} e^{2(n-1)}\right) <$$

$$< \Pi_2\Pi_3\dots\Pi_{n+1}\left(E_1 + 9(e^2-5)\left(\frac{\tau}{2}\right)^5 h_0^2\cdot\sum_{i=0}^{\infty}\left(e^2\left(\frac{\tau}{2}\right)^2 h_0^2\right)^i\right) =$$

$$= \Pi_2\Pi_3\dots\Pi_{n+1}\left(E_1 + \frac{9(e^2-5)\left(\frac{\tau}{2}\right)^5 h_0^2}{1-\left(e\cdot\frac{\tau}{2}h_0\right)^2}\right)$$

(deoarece $e^2\cdot h_0^2\left(\frac{\tau}{2}\right)^2 < 1$). Am demonstrat deci următoarea inegalitate:

$$(33)\quad E < h_0^2\Pi_1\Pi_2\dots\Pi_{n+1}\left(E_1 + \frac{9(e^2-5)\left(\frac{\tau}{2}\right)^5 h_0^2}{1-\left(e\cdot\frac{\tau}{2}h_0\right)^2}\right).$$

Am demonstrat ceva mai sus că $E_1^{(2)} < E_1^{(1)}$ ceea ne arată că

$$E_1 = 1 - E_1^{(1)} + + E_1^{(2)} < 1$$

(în stabilitatea inegalității (33) am ținut cont de inegalitățile (7) care ne asigură că $\Pi_1 > \frac{1}{h_0^2}$ și deci $\Pi_1 h_0^2 > 1$) Evaluând $h_0^2\left(1+\frac{9(e^2-5)h_0^2(\ln h_0)^5}{1-(eh_0\ln h_0)^2}\right)$ obținem că:

$$(34)\quad E \le \Pi_1\Pi_2 \dots \Pi_{n+1}\cdot 2{,}1 = 2{,}1\prod_{v=1}^{r}\left(1-\frac{2}{q_v}\right)$$

Pentru a obține evaluarea precedentă se ține cont că $h_0 = 1{,}29$, $\ln h_0 \simeq 0{,}2546$ și $e^2 \simeq 7{,}3891$). Ca o consecință imediată a teoremei 3 din paragraful I al anexei (aici se poate invoca și propoziția 4 din paragraful I al anexei teoremei lui Brun) există o constantă c_8, reală și strict pozitivă, astfel încât

$$\prod_{\substack{17\le p\le x^{\frac{1}{9}}\\ p\text{-}prim}}\left(1-\frac{2}{p}\right)\le\frac{c_8}{\ln^2 x^{\frac{1}{9}}}=\frac{81c_8}{\ln^2 x}.$$

Deci

$$E \le 2{,}1\prod_{v=1}^{r}\left(1-\frac{2}{q_v}\right)=$$

$$=2{,}1\prod_{\substack{17\le p\le x^{\frac{1}{9}}\\ p\text{-}prim}}\left(1-\frac{2}{p}\right)\cdot\prod_{\substack{p\text{-}prim\\ p/u\\ x^{\frac{1}{9}}\ge p\ge 17}}\left(\frac{p}{p-2}\right)\le 2{,}1\cdot\frac{81c_8}{\ln^2 x}\cdot\prod_{\substack{p\text{-}prim\\ p\ge 17,\ p/u}}\left(\frac{p}{p-2}\right)=$$

$$=2{,}1\cdot\frac{81c_8}{\ln^2 x}\,S(u)=\frac{c_9\,S(u)}{\ln^2 x}.$$

Inegalitatea (18) împreună cu evaluarea precedentă permit următoarea estimare:

$$A(u,x)\le 2x^{\frac{1}{9}}+c_7\frac{x}{\ln^2 x}+c_9\frac{x}{\ln^2 x}S(u).$$

Pentru un x_1 suficient de mare și o constantă reală strict pozitivă c_{10} are loc inegalitatea

$$A(u,x)\le c_{10}\frac{x}{\ln^2(x)}\big(2+S(u)\big)\le$$

$$\le c_{10}\frac{x}{\ln^2(x)}\big(2S(u)+S(u)\big)=3c_{10}\frac{x}{\ln^2(x)}S(u),$$

$(\forall)\, x \geq x_1$ deoarece

$$S(u) = \prod_{\substack{p\text{-prim} \\ p \geq 17,\ p/u}} \left(\frac{p}{p-2} \right) \geq 1.$$

În acest moment teorema lui Brun este demonstrată și deci rezultatul lui Schnirelmann este argumentat complet.

Observație. *În general procedeul de evaluare al termenului* $P(A, d, x; d_1, e_1, t_1; d_2, e_2, t_2; \ldots; d_r, e_r, t_r)$ *urmărește aceeași schemă ca evaluarea termenului* $P(x; q_1, q_2, \ldots, q_r)$ *din teorema 2. Acest procedeu poartă numele de „metoda ciurului lui Eratostene" și este legat de numele lui Brun (vezi articolul „Le crible d'Eratosthène et le théorème de Goldbach", Vid. Selsk. Skr. I Math. Nat. Kl. Kristiania 1920, No3).*

ANEXĂ
(Teorema lui Schnirelman)

I. **Teorema 1**. (*A b e l*). Fie $0 < \lambda_1 < \lambda_2 < \lambda_3 < \ldots$ *un şir de numere reale cu proprietatea că* $\lambda_n \xrightarrow[n\to\infty]{} \infty$. *Dacă* φ *este o funcţie cu valori complexe definită pentru* $x \geq 0$ *să se arate că* :

$$\sum_{n=1}^{k} a_n \varphi(\lambda_n) = A(\lambda_k)\varphi(\lambda_k) - \sum_{n=1}^{k-1} A(\lambda_n)\Big(\varphi(\lambda_{n+1}) - \varphi(\lambda_n)\Big),$$

unde $A(x) = \sum_{\lambda_n \leq x} a_n$, *pentru* $x \geq \lambda_1$ ($a_n \in \mathbf{C}$, $(\forall)\, n \in \mathbf{N}^*$), $k \in \mathbf{N}^*$. *Dacă* φ *este o funcţie cu derivata continuă în intervalul* $(0, \infty)$, *atunci*

$$\sum_{\lambda_n \leq x} a_n \varphi(\lambda_n) = A(x)\,\varphi(x) - \int_{\lambda_1}^{x} A(t)\,\varphi'(t)\mathrm{d}t,$$

pentru $x \geq \lambda_1$.

În ipoteza că $\lim_{x\to\infty} A(x)\varphi(x) = 0$, *are loc egalitatea*

$$\sum_{n=1}^{\infty} a_n \varphi(\lambda_n) = -\int_{\lambda_1}^{\infty} A(t)\,\varphi'(t)\mathrm{d}t,$$

în situaţia în care cel puţin unul din cei doi termeni ai egalităţii precedente are sens.

Demonstraţie. Dacă notăm cu $A(\lambda_0) = 0$, atunci

$$\sum_{n=1}^{k} a_n \varphi(\lambda_n) = \sum_{n=1}^{k} \Big(A(\lambda_n) - A(\lambda_{n-1})\Big)\varphi(\lambda_n) =$$

$$= A(\lambda_k)\,\varphi(\lambda_k) + \sum_{n=1}^{k-1} A(\lambda_n)\,\varphi(\lambda_n) - \sum_{n=2}^{k} A(\lambda_{n-1})\,\varphi(\lambda_n) =$$

$$= A(\lambda_k)\,\varphi(\lambda_k) + \sum_{n=1}^{k-1} A(\lambda_n)\,\varphi(\lambda_n) - \sum_{n=1}^{k-1} A(\lambda_n)\,\varphi(\lambda_{n+1}) =$$

$$= A(\lambda_k)\,\varphi(\lambda_k) - \sum_{n=1}^{k-1} A(\lambda_n)\Big(\varphi(\lambda_{n+1}) - \varphi(\lambda_n)\Big)$$

și primul punct al teoremei este demonstrat. Pentru a doua parte a enunțului fie k cel mai mare număr natural nenul pentru care $\lambda_k \le x$. Atunci

$$\sum_{\lambda_n \le x} a_n \varphi(\lambda_n) = \sum_{n=1}^{k} a_n \varphi(\lambda_n) = A(\lambda_k)\,\varphi(\lambda_k) - \sum_{n=1}^{k-1} A(\lambda_n)\left(\varphi(\lambda_{n+1}) - \varphi(\lambda_n)\right)$$

conform punctului demonstrat mai sus. Pe de altă parte, deoarece funcția $A(x)$ este constantă pe orice interval de forma $[\lambda_n, \lambda_{n+1})$ (și egală cu $A(\lambda_n)$), avem că

$$A(x)\,\varphi(x) - \int_{\lambda_1}^{x} A(t)\,\varphi'(t)\,dt = A(x)\,\varphi(x) - \int_{\lambda_1}^{\lambda_k} A(t)\,\varphi'(t)\,dt - \int_{\lambda_k}^{x} A(t)\,\varphi'(t)\,dt =$$

$$= A(x)\,\varphi(x) - \sum_{n=1}^{k-1} A(\lambda_n) \int_{\lambda_n}^{\lambda_{n+1}} \varphi'(t)\,dt - A(\lambda_k) \int_{\lambda_k}^{x} \varphi'(t)\,dt =$$

$$= A(x)\,\varphi(x) - \sum_{n=1}^{k-1} A(\lambda_n) \cdot \left(\varphi(\lambda_{n+1}) - \varphi(\lambda_n)\right) - A(\lambda_k)\left(\varphi(x) - \varphi(\lambda_k)\right) =$$

$$= A(\lambda_k)\,\varphi(\lambda_k) - \sum_{n=1}^{k-1} A(\lambda_n)\left(\varphi(\lambda_{n+1}) - \varphi(\lambda_n)\right) \quad \left(A(x) = A(\lambda_k)\right).$$

Am folosit mai sus formula de integrare prin părți precum și faptul că două funcții integrabile care sunt egale aproape peste tot au aceeași integrală (evident în cursul acestei demonstrații și a acestei teoreme este vorba despre integrala Riemann). Ultima parte a enunțului este evidentă.

Teorema 2. $\sum_{\substack{p \le x \\ p-prim}} \frac{1}{p} = \ln\ln x + c_1 + O\left(\frac{1}{\ln x}\right)$ *pentru* $x \ge 2$, *unde* c_1 *este o constantă reală.*

Demonstrație. Avem nevoie de unele preparative. Întâi $\ln n! = n \ln n + O(n)$. Aceasta se poate demonstra aplicând criteriul lui Cesaro - Stolz șirului

$$d_n = \frac{\ln n! - n\ln n}{n}.$$

Se obține că

$$\lim_{n\to\infty} d_n = \lim_{n\to\infty} \frac{\ln(n+1)! - (n+1)\ln(n+1) - \ln n! + n\ln n}{(n+1) - n} =$$

$$= \lim_{n\to\infty} \left(-n\ln(n+1) + n\ln n\right) = \lim_{n\to\infty} n \ln \frac{n}{n+1} =$$

$$= \lim_{n\to\infty} \frac{n}{-(n+1)} \ln\left(1 - \frac{1}{n+1}\right)^{-(n+1)} = -\ln e = -1$$

iar aceasta justifică formula: $\ln n! = n \ln n + O(n)$. Se poate observa de asemenea că această formulă este consecința imediată a formulei lui Stirling

$$\lim_{n\to\infty} \frac{n!}{n^n e^{-n}\sqrt{2\pi n}} = 1$$

(de altfel formula $\ln n! = n \ln n + O(n)$ mai poartă numele de forma slabă a formulei lui Stirling).

În al doilea rând avem nevoie de formula de evaluare asimptotică a lui Mertens

$$\sum_{\substack{p\le x \\ p\text{-}prim}} \frac{\ln p}{p} = \ln x + O(1) \quad \forall\, x \ge 2.$$

Conform teoremei lui Legendre (demonstrată în lema 1 din paragraful I al anexei teoremei lui Brun) avem că

$$n! = \prod_{\substack{p\le n \\ p\text{-}prim}} p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots},$$

sau

$$\ln n! = \sum_{\substack{p^r\le n \\ p\text{-}prim}} \left[\frac{n}{p^r}\right] \cdot \ln p.$$

Deci

$$\ln n! \ge \sum_{\substack{p\le n \\ p\text{-}prim}} \left[\frac{n}{p}\right] \cdot \ln p \ge \sum_{\substack{p\le n \\ p\text{-}prim}} \left(\frac{n}{p} - 1\right) \ln p =$$

$$= n \sum_{\substack{p\le n \\ p\text{-}prim}} \frac{\ln p}{p} - \ln \prod_{\substack{p\text{-}prim \\ p\le n}} p \ge n \sum_{\substack{p\le n \\ p\text{-}prim}} \frac{\ln p}{p} - \ln 4^n = n \sum_{\substack{p\le n \\ p\text{-}prim}} \frac{\ln p}{p} - n \ln 4$$

(am folosit mai sus inegali-tatea $[y] > y - 1$ precum și inegalitatea $\prod_{\substack{p\le n \\ p\ prim}} p \le 4^n$ demonstrată în lema 2 a anexei teoremei lui Scherk). În cele de mai sus n este un număr natural nenul. Conform formei slabe a formulei lui Stirling există o constantă pozitivă c_2 astfel încât

$$-c_2 n \le \ln n! - n \ln n \le c_2 n$$

și deci

$$n \ln n \geq \ln n! - c_2 n \geq n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} - n \ln 4 - - c_2 n,$$

pentru orice $n \in \mathbf{N}^*$. În concluzie,

$$\ln n \geq \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} - \ln 4 - c_2$$

pentru $(\forall)\ n \in \mathbf{N}^*$. Pe de altă parte

$$\ln n! = \sum_{\substack{p^r \leq n \\ p\text{-prim}}} \left[\frac{n}{p^r}\right] \ln p \leq \sum_{\substack{p^r \leq n \\ p\text{-prim}}} \frac{n}{p^r} \ln p \leq$$

$$\leq n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} + n \sum_{\substack{p \leq n \\ p\text{-prim}}} \ln p \left(\frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \ldots\right) =$$

$$= n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} + n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p^2} \cdot \frac{1}{1 - \frac{1}{p}} = n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} + n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p(p-1)} \leq n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} + n c_3,$$

unde c_3 este o constantă pozitivă și anume

$$c_3 = \sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)}$$

(suma precedentă este cu siguranță convergentă deoarece $(\exists)\ a > 0$ astfel încât, $\frac{\ln k}{k-1} < \frac{a}{\sqrt{k}}$, $(\forall)\ k \in \mathbf{N},\ k \geq 2$ și suma $\sum_{k=2}^{\infty} \frac{1}{k\sqrt{k}}$ este convergentă). Am obținut deci că

$$n \ln n \leq \ln n! + c_2 n \leq n \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} + n c_3 + n c_2,$$

care se mai scrie sub forma

$$\ln n \leq \sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} + c_2 + c_3,$$

$(\forall)\ n \in \mathbf{N}^*$. Din considerațiile anterioare deducem că

$$\sum_{\substack{p \leq n \\ p\text{-prim}}} \frac{\ln p}{p} = \ln n + O(1).$$

Dacă $x \geq 2$ atunci $\sum_{\substack{p \leq x \\ p-prim}} \frac{\ln p}{p} = \ln[x] + O(1) = \ln x + \ln \frac{[x]}{x} + O(1) = \ln x + O(1)$

deoarece

$$1 \geq \frac{[x]}{x} > \frac{x-1}{x} = 1 - \frac{1}{x} \geq 1 - \frac{1}{2}$$

și

$$0 \geq \ln \frac{[x]}{x} \geq \ln\left(1 - \frac{1}{2}\right).$$

Formula lui Mertens este astfel demonstrată. Pentru a demonstra teorema 2 vom folosi teorema 1 precum și formula lui Mertens. Dacă $p_1, p_2, \ldots, p_i, \ldots$ este secvența numerelor prime ordonate crescător notăm cu $a_n = \frac{\ln p_n}{p_n}$, $A(x) = \sum_{p_n \leq x} a_n$ (pentru $x \geq 3$), $\lambda_n = p_n$, $\varphi(x) = \frac{1}{\ln x}$, $B(x) = \sum_{p_n \leq x} \frac{1}{p_n} = \sum_{p_n \leq x} \frac{a_n}{\ln p_n} = \sum_{\lambda_n \leq x} a_n \varphi(\lambda_n) =$

$= \frac{A(x)}{\ln x} - \int_2^x A(t)(\varphi'(t))\,dt = \frac{A(x)}{\ln x} + \int_2^x \frac{A(t)}{t \ln^2 t}\,dt$ conform teoremei 1 (se observă că φ are calitățile cerute pe orice interval $[1 + \varepsilon, \infty)$, $(\forall)\ \varepsilon > 0$. În enunțul teoremei 1 este esențial că φ are calitățile indicate pe orice interval de forma $[\lambda_1 - \varepsilon, \infty)$, cu $\varepsilon > 0$). Conform formulei lui Mertens $A(x) = \ln x + f(x)$, unde f este o funcție care satisface inegalitatea $|f(x)| \leq c_4$, $(\forall)\ x \geq 2$, c_4 fiind o constantă pozitivă. Înlocuind pe A în egalitatea de mai sus obținem că

$$B(x) = 1 + \frac{f(x)}{\ln x} + \int_2^x \left(\frac{1}{t \ln t} + \frac{f(t)}{t \ln^2 t}\right) dt =$$

$$= \ln \ln x - \ln \ln 2 + 1 + \frac{f(x)}{\ln x} + \int_2^x \frac{f(t)}{t \ln^2 t}\,dt =$$

$$= \ln \ln x + c_1 + \frac{f(x)}{\ln x} - \int_x^\infty \frac{f(t)}{t \ln^2 t}\,dt,$$

unde am notat

$$c_1 = 1 - \ln \ln 2 + \int_2^\infty \frac{f(t)}{t \ln^2 t}\,dt.$$

Funcția $\frac{f(t)}{t \ln^2 t}$ este integrabilă pe orice interval de forma $[k, \infty)$ (cu $k \geq 2$) și

$$\left| \int_k^\infty \frac{f(t)}{t \ln^2 t}\,dt \right| \leq \int_k^\infty \frac{|f(t)|}{t \ln^2 t}\,dt \leq c_4 \int_k^\infty \frac{1}{t \ln^2 t}\,dt = c_4 \left(-\frac{1}{\ln t}\right)\Bigg|_{t=k}^{t=\infty} = \frac{c_4}{\ln k}.$$

Rezultă deci că

$$\left|\frac{f(x)}{\ln x}-\int_x^{\infty}\frac{f(t)}{t\ln^2 t}\,dt\right|\le\frac{|f(x)|}{\ln x}+\left|\int_x^{\infty}\frac{f(t)}{t\ln^2 t}\,dt\right|\le\frac{c_4}{\ln x}+\frac{c_4}{\ln x}=\frac{2c_4}{\ln x}$$

$(\forall)\ x\ge 2$. Din această inegalitate precum și din faptul că

$$B(x)=\ln\ln x+c_1+\frac{f(x)}{\ln x}-\int_x^{\infty}\frac{f(t)}{t\ln^2 t}\,dt$$

deducem că

$$\sum_{\substack{p\le x\\ p\text{-}prim}}\frac{1}{p}=\ln\ln x+c_1+O\left(\frac{1}{\ln x}\right),\quad(\forall)\ x\ge 2.$$

Corolar. *Există o constantă* c_1 *astfel încât*

$$\lim_{x\to\infty}\left(\sum_{\substack{p\le x\\ p\text{-}prim}}\frac{1}{p}-\ln\ln x-c_1\right)=0.$$

Demonstrație. Afirmația este evidentă ținând cont de teorema 2.

Teorema 3. *Există o constantă* c_5 *astfel încât*

$$\lim_{x\to\infty}\ln^2 x\cdot\prod_{\substack{p\text{-}prim\\ 3\le p\le x}}\left(1-\frac{2}{p}\right)=c_5.\left(c_5>0\right).$$

Demonstrație. Fie

$$g(x)=\ln^2 x\prod_{\substack{3\le p\le x\\ p\text{-}prim}}\left(1-\frac{2}{p}\right),$$

$(\forall)\ x\ge 3$. Ținând cont că

$$\sum_{n=1}^{\infty}\frac{z^n}{n}=-\ln(1-z),$$

$(\forall)\ z\in\mathbf{R}$, $|z|<1$, deducem că

$$\ln g(x)=2\ln\ln x+\sum_{\substack{3\le p\le x\\ p-prim}}\ln\left(1-\frac{2}{p}\right)=$$

$$2\ln\ln x-\sum_{\substack{3\le p\le x\\ p-prim}}\sum_{n=1}^{\infty}\left(\left(\frac{2}{p}\right)^n\cdot\frac{1}{n}\right)=$$

$$2\ln\ln x-2\sum_{\substack{3\le p\le x\\ p-prim}}\frac{1}{p}-\sum_{\substack{3\le p\le x\\ p\text{-}prim}}\sum_{n=2}^{\infty}\frac{1}{n}\cdot\left(\frac{2}{p}\right)^n.$$

Deoarece

$$\left|\sum_{\substack{3\le p\le x\\ p\text{-}prim}}\sum_{n=2}^{\infty}\frac{1}{n}\cdot\left(\frac{2}{p}\right)^n\right| \le \sum_{\substack{3\le p\le x\\ p\text{-}prim}}\left(\frac{2}{p}\right)^2\cdot\frac{1}{\left(1-\frac{2}{p}\right)} =$$

$$=4\sum_{\substack{3\le p\le x\\ p\text{-}prim}}\frac{1}{p(p-2)}\le 4\sum_{\substack{3\le p\le x\\ p\text{-}prim}}\frac{1}{(p-2)^2}\le 4\sum_{n=1}^{\infty}\frac{1}{n^2}=4\cdot\frac{\pi^2}{6}<\infty,$$

rezultă că

$$\lim_{x\to\infty}\ln g(x)=\lim_{x\to\infty}\left[2\left(\ln\ln x-\sum_{\substack{2\le p\le x\\ p\text{-}prim}}\frac{1}{p}\right)+1-c_6\right]=-2c_1+1-c_6,$$

unde c_1 este constanta din teo-rema 2, iar

$$c_6=\lim_{x\to\infty}\sum_{\substack{3\le p\le x\\ p\text{-}prim}}\sum_{n=2}^{\infty}\frac{1}{n}\cdot\left(\frac{2}{p}\right)^n$$

(s-a observat mai sus că această limită există într-adevăr). De aici deducem imediat că $\lim_{x\to\infty} g(x)=e^{-2c_1+1-c_6}=c_5$ (În cele de mai sus s-a folosit dezvoltarea

$$\ln\left(1-\frac{2}{p}\right)=-\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{2}{p}\right)^n$$

pentru p număr prim, $p\ge 3$, care are loc deoarece $\left|\frac{2}{p}\right|\le\frac{2}{3}<1$). Faptul că $c_5>0$ este evident.

Teorema 4. (*Schlömilch*) *Dacă* $x_1, x_2, ..., x_n$ *sunt* n *numere reale pozitive diferite* ($n\in\mathbf{N}$, $n\ge 2$) *și dacă* $s_1, s_2, ..., s_n$ *sunt polinoamele simetrice fundamentale în* $x_1, x_2, ..., x_n$ (*adică* $s_1=x_1+x_2+...+x_n$, $s_2=x_1x_2+...+x_{n-1}x_n$, ..., $s_n=x_1x_2...x_n$) *atunci au loc inegalitățile*:

(1) $$\frac{s_1}{n}>\frac{2s_2}{(n-1)s_1}>\frac{3s_3}{(n-2)s_2}>...>\frac{ns_n}{s_{n-1}}.$$

Demonstrație: Să demonstrăm întâi prima din inegalitățile precedente: $s_1^2\cdot(n-1)>2ns_2$ sau echivalent

$$(n-1)\left(x_1^2+x_2^2+...+x_n^2\right)+2(n-1)s_2>2ns_2,$$

$$(n-1)\left(x_1^2+x_2^2+...+x_n^2\right)-2s_2>0.$$

Însă ultima inegalitate se mai scrie sub forma

$$(x_1 - x_2)^2 + (x_1 - x_3)^2 + \ldots + (x_1 - x_n)^2 + \ldots + (x_{n-1} - x_n)^2 > 0.$$

Cum valabilitatea acestei inegalități este evidentă (numerele $x_1, \ldots x_n$ sunt diferite) rezultă că $\frac{s_1}{n} > \frac{2s_2}{(n-1)s_1}$. Celelalte inegalități vor fi probate prin inducție după n. Pentru $n = 2$ enunțul este demonstrat (pentru $n = 2$ nu există decât prima din inegalitățile (1)). Presupunem enunțul adevărat pentru $n - 1 \geq 2$ și vrem să-l demonstrăm pentru n. Înlocuind elementele $x_1, x_2, \ldots, x_n$ cu $tx_1, tx_2, \ldots, tx_n$, unde $t \in \mathbf{R}_+^*$, numerele $s_1, \ldots, s_n$ vor fi înlocuite cu $ts_1, t^2s_2, t^3s_3, \ldots, t^ns_n$. De aici deducem că este suficient să demonstrăm inegalitățile (1) pentru numerele $tx_1, tx_2, \ldots, tx_n$. Alegându-l pe t convenabil putem presupune deci că unul din numerele $x_1, \ldots, x_n$ (de exemplu x_1) este egal cu 1.

Dorim să demonstrăm inegalitatea:

(2) $$\frac{is_i}{(n-i+1)s_{i-1}} > \frac{(i+1)s_{i+1}}{(n-i)s_i}, \quad i = \overline{2, n-1}$$ (pentru $i = 1$ s-a demonstrat mai sus). Dacă notăm $s_1', s_2', \ldots s_{n-1}'$ polinoamele simetrice fundamentale în $x_2, x_3, \ldots, x_n$ obținem (ținând cont că $x_1 = 1$) că $s_i = s_{i-1}' + s_i'$, $s_{i-1} = s_{i-2}' + s_{i-1}'$, $s_{i+1} = s_i' + s_{i+1}'$. Facem convenția $s_0' = s_0 = 1$, $s_n' = 0$. Inegalitatea (2) se scrie deci

(3) $$i(n-i)(s_{i-1}' + s_i')^2 > (i+1)(n-i+1)(s_{i-2}' + s_{i-1}')(s_i' + s_{i+1}').$$

Trecând termenul $(i+1)(n-i+1)\, s_{i-1}' \cdot s_i'$ în partea stângă se obține

(4) $$i(n-i)(s_{i-1}')^2 + i(n-i)(s_i')^2 + (in - i^2 - n - 1)s_{i-1}' s_i' > (i+1)(n-i+1)\,[s_{i-2}'\, s_i' + s_{i-2}' s_{i+1}' + s_{i-1}' s_{i+1}'].$$

Conform ipotezei de inducție au loc următoarele inegalități:

(5) $$\frac{(i-1)s_{i-1}'}{(n-i+1)s_{i-2}'} > \frac{i\, s_i'}{(n-i)s_{i-1}'} > \frac{(i+1)s_{i+1}'}{(n-i-1)s_i'}.$$

Ținând cont de inegalitățile (5) putem evalua membrul din dreapta al inegalității (4)

$$(i+1)(n-i+1)\,[s_{i-2}'s_i' + s_{i-2}'s_{i+1}' + s_{i-1}'s_{i+1}'] <$$

$$< (i+1)(n-i+1) \cdot \frac{(i-1)(n-i)}{i(n-i+1)}\left(s_{i-1}'\right)^2 +$$

$$+ (i+1)(n-i+1) \cdot \frac{(i-1)(n-i-1)}{(n-i+1)(i+1)} s_{i-1}'s_i' + (i+1)(n-i+1) \cdot \frac{i(n-i-1)}{(i+1)(n-i)}\left(s_i'\right)^2 =$$

$$= \frac{(i^2-1)(n-i)}{i}\left(s_{i-1}'\right)^2 + (i-1)(n-i-1)s_{i-1}'s_i' + \frac{i[(n-i)^2-1]}{(n-i)}\left(s_i'\right)^2$$

(trebuie observat că această inegalitate are loc și pentru $i = n - 1$). Pentru a ne convinge de valabilitatea inegalității (4) ar fi suficient să arătăm că are loc următoarea inegalitate

$$(6) \qquad \frac{(i^2-1)(n-i)}{i}\left(s'_{i-1}\right)^2+(i-1)(n-i-1)s'_{i-1}s'_i+\frac{i[(n-i)^2-1]}{n-i}\left(s'_i\right)^2 \le$$

$$\le i(n-i)\left(s'_{i-1}\right)^2+i(n-i)\left(s'_i\right)^2+(in-i^2-n-1)s'_{i-1}s'_i.$$

Inegalitatea (6) se mai scrie sub forma:

$$(7) \quad \frac{n-i}{i}\left(s'_{i-1}\right)^2+\frac{i}{n-i}\left(s'_i\right)^2-2s'_{i-1}s'_i \ge 0$$

Această din urmă inegalitate este însă evidentă deoarece poate fi pusă sub forma:

$$\frac{i}{(n-i)}\left[\frac{(n-i)}{i}s'_{i-1}-s'_i\right]^2 \ge 0.$$

Teorema 4 este în acest moment demonstrată.

II. Dacă F este un șir strict crescător de numere naturale nenule având primul termen 1, vom spune că F are densitate egală cu α dacă

$$\alpha=\inf\left\{\beta\middle|\beta\ge 0,\ \frac{N(x)}{x}\ge\beta,\ (\forall)\,x\in\mathbf{N}^*\right\},$$

unde $N(x)$ este numărul de termeni ai șirului F care sunt mai mici sau egali cu x ($0 \le \alpha \le 1$; se observă imediat că $\alpha = 1$ dacă și numai dacă F coincide cu $\mathbf{N}^*$. Vom scrie $D(F) = \alpha$.

Lemă: *Dacă $F_1, F_2, ..., F_k$ sunt șiruri de densitate $\alpha_1, \alpha_2, ..., \alpha_k$; $D(F_1) = \alpha_1$, $D(F_2) = \alpha_2, ..., D(F_k) = \alpha_k$; atunci $F_1 + F_2 + ... + F_k$ este un șir de densitate mai mare sau egală cu un α. Aici și peste tot în acest capitol $F_1, F_2, ..., F_k$ sunt șiruri strict crescătoare de numere naturale nenule ($k \in \mathbf{N}^*$) având primul termen 1. Prin $F_1 + F_2 + ... + F_k$ se înțeleg elementele de formă $b_1 + b_2 + ... + b_k$, b_i fiind element al șirului F_i sau $b_i = 0$ (însă nu se poate întâmpla ca $b_1 = b_2 = ... = b_k = 0$) $(\forall)\ i = \overline{1,k}$, aceste elemente fiind ordonate crescător (două elemente egale se scriu o singură dată). În plus $1 - D(F_1 + F_2 + ... + F_k) \le (1 - \alpha_1)(1 - \alpha_2) ... (1 - \alpha_k)$.*

Demonstrație: Pentru $k = 1$ enunțul este clar. În continuare vom demonstra enunțul pentru $k = 2$. Fie $x \in \mathbf{N}^*, f_{1,1}, f_{1,2}, ..., f_{1,n}$ termenii șirului F_1 care sunt mai mici sau egali cu x. Deci $n \ge \alpha_1 x$ (deoarece $\frac{N_1(x)}{x} \ge \alpha_1$). Numărul de termeni de forma $f_{1i} + f$ cuprinși strict în intervalul $(f_{1i}, f_{1,i+1})$ (unde f este termen al șirului F_2) este egal cu $N_2(f_{1,i+1} - f_{1,i} - 1)$ ($N_f(x)$ înseamnă numărul de termeni ai șirului

F_j care sunt mai mici sau egali cu x); deci este mai mare sau egal cu $\alpha_2(f_{1,i+1} - f_{1,i} - 1)$. Evaluarea de mai sus este valabilă pentru orice $i = \overline{1, n-1}$. Numărul de termeni de forma $f_{1,n} + f$ (unde $f \in F_2$) cuprinși în intervalul $(f_{1,n}, x]$ este egal cu $N_2(x - f_{1,n})$ și este deci mai mare sau egal cu $\alpha_2(x - f_{1,n})$ (deoarece $D(F_2) = \alpha_2$).

Trebuie menționat că termenii $f_{1,1}, f_{1,2}, ..., f_{1,n}$ sunt aranjați în ordine strict crescătoare. Deci numărul de termeni ai șirului $F_1 + F_2$ care sunt mai mici sau egali cu x este cel puțin

$$n + \sum_{i=1}^{n-1} \alpha_2 (f_{1,i+1} - f_{1,i} - 1) + \alpha_2(x - f_{1,n}) =$$

$$= n - \alpha_2 f_{1,1} - \alpha_2(n-1) + \alpha_2 x = n + \alpha_2(x - n),$$

$f_{1,1} = 1$. Deoarece $n \geq \alpha_1 x$ deducem că

$$n + \alpha_2 (x - n) = n(1 - \alpha_2) + \alpha_2 x \geq \alpha_1(1 - \alpha_2) x + \alpha_2 x =$$

$$= x(\alpha_1 + \alpha_2 - \alpha_1\alpha_2)(1 - \alpha_2) \geq 0,$$

deoarece

$$\alpha_2 \leq \frac{N_2(x)}{x} \leq 1.$$

Din cele de mai sus rezultă că

$$D(F_1 + F_2) \geq \alpha_1 + \alpha_2 - \alpha_1\alpha_2 (\alpha_1 + \alpha_2) - \alpha_1\alpha_2 = \alpha_1(1 - \alpha_2) + \alpha_2 > 0)$$

și deci,

$$1 - D(F_1 + F_2) \leq 1 - \alpha_1 - \alpha_2 + \alpha_1\alpha_2 = (1 - \alpha_1)(1 - \alpha_2).$$

În cazul general enunțul se demonstrează prin inducție. Presupunem afirmația adevărată pentru un număr $k \in \mathbf{N}$, $k \geq 2$. Notând $F = F_2 + + F_3 + ... + F_{k+1}$ atunci conform ipotezei de inducție $1 - D(F) \leq (1 - \alpha_2)(1 - \alpha_3), ... (1 - \alpha_{k+1})$. Folosind ceea ce am demonstrat mai înainte, rezultă că

$$1 - D(F_1 + F_2 + ... + F_{k+1}) = 1 - D(F_1 + F) \leq$$

$$\leq (1 - \alpha_1)\,[1 - 1 + (1 - \alpha_2)(1 - \alpha_3) ... (1 - \alpha_{k+1})] =$$

$$= (1 - \alpha_1)(1 - \alpha_2)(1 - \alpha_3) ... (1 - \alpha_{k+1}).$$

Raționamentul prin inducție este astfel încheiat.

Teorema 1: *Fie F este un șir strict crescător de numere naturale nenule de densitate egală cu $\alpha > 0$ atunci* $4\left[\frac{1}{\alpha}\right] F = \mathbf{N}^*$. *Prin nF se înțelege $F + F + + F + ... + F$, F apărând de n ori.*

Demonstrație. Să demonstrăm întâi următoarea observație: dacă F_1 și F_2 sunt șiruri strict crescătoare de numere naturale pentru care

$$D(F_1) = \alpha_1,$$

$$D(F_2) = \alpha_2$$

și

$$\alpha_1 + \alpha_2 > 1,$$

atunci

$$F_1 + F_2 = \mathbf{N}^*.$$

Fie $x \in \mathbf{N}^*$ și

$$a_1 = 1 < a_2 < a_3 < < ... < a_n \leq x$$

toți termenii șirului F_1 care sunt mai mici sau egali cu x. Dacă $a_n = x$ este clar că $x \in F_1 + F_2$. Presupunem în continuare că $a_n < x$. Fie $b_1 = 1 < b_2 < < b_3 < ... < b_m \leq x$ toți termenii șirului F_2 care sunt mai mici decât x. Dacă $x - a_i \neq b_j$, $(\forall)$ $i = \overline{1,n}$, $j = \overline{1,m}$, deducem că în intervalul $[1, x]$ există cel puțin $m + n$ numere naturale, deci $m + n \leq x$. Pe de altă parte, deoarece $D(F_1) = \alpha_1$ și $D(F_2) = \alpha_2$, deducem că

$$m + n \geq \alpha_1 x + \alpha_2 x = (\alpha_1 + \alpha_2)\, x > x$$

pentru că $\alpha_1 + \alpha_2 > 1$. S-a ajuns la o contradicție. Există deci i $(1 \leq i \leq n)$ și j $(1 \leq j \leq m)$ astfel încât $x - a_i = b_j$; aceasta înseamnă că x aparține șirului $F_1 + F_2$ $(x = a_i + b_j)$. S-a demonstrat astfel că $F_1 + F_2 = \mathbf{N}^*$. Să trecem acum la demonstrarea enunțului teoremei 1. Notăm $h = 4\left[\frac{1}{\alpha}\right]$. Dacă $\alpha > \frac{1}{2}$ atunci $1 \leq \frac{1}{\alpha} < 2$ (este clar că $\alpha \leq 1$ deoarece $\alpha \leq \frac{N(x)}{x} \leq 1$; $N(x)$ înseamnă numă-rul de termeni ai șirului F care sunt mai mici sau egali cu x) și deci $\left[\frac{1}{\alpha}\right] = 1$, $h = 4$. $D(F) + D(F) \geq 2\alpha > 1$, ceea ce înseamnă, conform observației cu care am început demonstrația, că $2F = \mathbf{N}^*$. Cu atât mai mult $hF = 4F = \mathbf{N}^*$. Trebuie analizat acum cazul $\alpha \leq \frac{1}{2}$. Conform aceleiași observații cu care am început demonstrația acestei teoreme este suficient să demonstrăm că $D\left(\frac{h}{2}F\right) > \frac{1}{2}$. Atunci $D\left(\frac{h}{2}F\right) + + D\left(\frac{h}{2}F\right) > 1$ și deci $hF = \frac{h}{2}F + \frac{h}{2}F = \mathbf{N}^*$; h este număr par. Conform lemei

$$\left(1 - D\left(\frac{h}{2}F\right)\right) \leq (1-\alpha)^{\frac{h}{2}}.$$

Logaritmând obținem succesiv următoarele inegalități

$$\ln\left(1-D\left(\frac{h}{2}F\right)\right)\le\frac{h}{2}\ln(1-\alpha)=\frac{h}{2}\left(-\alpha-\frac{\alpha^2}{2}-\frac{\alpha^3}{3}-\ldots\right)\le-\alpha\cdot\frac{h}{2}=$$

$$=-2\alpha\cdot\left[\frac{1}{\alpha}\right]\le-2\alpha\left(\frac{1}{\alpha}-1\right)=-2(1-\alpha)\le-2\left(1-\frac{1}{2}\right)=-1=\ln\frac{1}{e}<\ln\frac{1}{2}.$$

Am ținut cont mai sus că $0<\alpha\le\frac{1}{2}$, $\left[\frac{1}{\alpha}\right]>\frac{1}{\alpha}-1$. Din cele de mai sus obținem că

$1-D\left(\frac{h}{2}F\right)<\frac{1}{2}$ și $D\left(\frac{h}{2}F\right)>\frac{1}{2}$. Cum s-a observat mai sus aceasta demonstrează că $hF=\mathbf{N}^*$. Enunțul teoremei 1 este în acest moment demonstrat.

Teorema 2: *Fie* $\varphi:[1,\infty)\to\mathrm{R}_+$ *o funcție crescătoare pentru care* $\varphi(i)=O\left(\sqrt{i}\right)$. *Fie F un șir strict crescător de numere naturale nenule notat cu* $n_1=1, n_2, n_3,\ldots$, *pentru care* $n_i=O(i\varphi(i))$. *Pentru* $0\le y\le x$ ($y\in\mathbf{N}$) *notăm cu* $A(y,x)$ *numărul de soluții al ecuației* $n_i-n_j=y$ cu $n_i, n_j\in F$, $n_i\le x$ (*deci și* $n_j\le x$). *Presupunem că*:

(1) $\sum_{y=1}^{x}A^2(y,x)=O\left(\frac{x^3}{\varphi^4(x)}\right)$. *Să se arate că există un număr natural* $n\in\mathbf{N}^*$ *astfel încât* $nF=\mathbf{N}^*$.

Demonstrație. Alegem $x_0\ge 2$, c_1, c_2, c_3 constante reale strict pozitive astfel încât $\varphi(x)\le c_2\sqrt{x}$, $\sum_{y=1}^{x}A^2(y,x)\le c_3\frac{x^3}{\varphi^4(x)}$, $(\forall)\,x\ge x_0$ și $n_i\le c_1\,i\,\varphi(i)$, $(\forall)\,i\ge N\left(\frac{x_o}{2}\right)+1$, unde ca de obicei $N(z)$ înseamnă numărul de termeni ai șirului F care sunt mai mici sai egali cu z. Fie $x\ge x_o$ ($x\in\mathbf{N}$). Atunci au loc inegalitățile

(2) $$\frac{x}{2}<n_{N\left(\frac{x}{2}\right)+1}<c_1\left(N\left(\frac{x}{2}\right)+1\right)\varphi\left(N\left(\frac{x}{2}\right)+1\right)\le 2c_1N\left(\frac{x}{2}\right)\varphi(x).$$

Am folosit mai sus faptul că $N\left(\frac{x}{2}\right)\ge N(1)=1$, $N\left(\frac{x}{2}\right)+1\le\frac{x}{2}+1\le x$, $x\ge 2$ și φ este funcție crescătoare. Pentru orice $m\in\mathbf{N}^*$ notăm cu $B(m)$ numărul

de soluții al ecuației $m = n_i + n_j$, unde $n_i, n_j \in F$, iar cu $M(x)$ numărul acelor $m \in \mathbf{N}^*$, $m \le x$ pentru care $B(m) \neq 0$. Numărul $\sum_{m=1}^{x} B(m)$ reprezintă numărul de soluții pentru inecuația $n_i + n_j \le x$, unde $n_i, n_j \in F$. Dacă $n_i, n_j \in F$ astfel încât $n_i \le \frac{x}{2}$ și $n_j \le \frac{x}{2}$ atunci evident $n_i + n_j \le x$; aceasta înseamnă că $\sum_{m=1}^{x} B(m) \ge N^2\left(\frac{x}{2}\right)$.

Ținând cont de această ultimă observație precum și de inegalitățile (2) obținem

$$(3) \quad \frac{x^4}{2^8 c_1^4 \varphi^4(x)} \le N^4\left(\frac{x}{2}\right) \le \left(\sum_{m=1}^{x} B(m)\right)^2 \le M(x) \sum_{m=1}^{x} B^2(m).$$

Ultima inegalitate se justifică cu inegalitatea Cauchy-Buniakovski). $\sum_{m=1}^{x} B^2(m)$ este egal cu numărul de cvadruplete (n_i, n_j, n_u, n_v) de elemente ale lui F pentru care

$$n_i + n_j = n_u + n_v = m,$$

unde m este orice număr natural cuprins în intervalul $[1, x]$. Dacă $n_i = n_u$ atunci $n_j = n_v$ și numărul de astfel de cvadruplete este

$$\sum_{m=1}^{x} B(m) \le \sum_{m=1}^{x} \left(\frac{B^2(m)+1}{2}\right) = \frac{x}{2} + \frac{1}{2} \sum_{m=1}^{x} B^2(m).$$

Dacă $n_i > n_u$ atunci $1 \le n_i - n_u = n_v - n_j \le x$ și numărul de astfel de cvadruplete este cel mult egal cu $\sum_{y=1}^{x} A^2(y,x)$. Dacă $n_i < n_u$ atunci $1 \le n_u - n_i = n_j - n_v \le x$ și numărul de astfel de cvadruplete este cel mult egal cu $\sum_{y=1}^{x} A^2(y,x)$. Din cele de mai sus obținem că

$$\sum_{m=1}^{x} B^2(m) \le \frac{x}{2} + + \frac{1}{2} \sum_{m=1}^{x} B^2(m) + 2 \sum_{y=1}^{x} A^2(y,x),$$

sau

$$\sum_{m=1}^{x} B^2(m) \le x + 4 \sum_{y=1}^{x} A^2(y,x) \le x + 4c_3 \frac{x^3}{\varphi^4(x)} \le \le \left(c_2^4 + 4c_3\right) \frac{x^3}{\varphi^4(x)}$$

(am ținut cont că $\varphi(x) \le c_2 \sqrt{x}$, $(\forall) x \ge x_0$). Inegalitatea precedentă împreună cu inegalitatea (3) ne conduc la următoarea evaluare:

(4) $$\frac{x^4}{2^8 c_1^4 \varphi^4(x)} \leq M(x)\left(c_2^4 + 4c_3\right) \cdot \frac{x^3}{\varphi^4(x)}.$$

Există deci o constantă c_4 strict pozitivă încât $M(x) \geq c_4 x$, $(\forall)$ $x \geq x_0$. Numărul de termeni ai șirului $F + F = 2F$ care sunt mai mici sau egali cu x este mai mare sau egal decât $M(x)$ și de aici deducem imediat că $2F$ are densitate pozitivă mai mare sau egală decât minimul dintre numerele $\frac{1}{x_0}$ și c_4 (este important aici că $1 \in F$ și deci $1 \in 2F$). Aplicând teorema 1 lui $2F$ rezultă imediat enunțul teoremei 2.

Observație: *Din condițiile enunțului* $(n_i = O(i\,\varphi(i)))$ *rezultă imediat că* φ *este o funcție strict pozitivă de la un rang încolo, ceea ce permite operația de împărțire cu* φ, *care a fost făcută mai sus.*

TEOREMA LUI SCHERK

Introducere

Scopul acestui capitol este demonstrarea unui rezultat aparținând lui H. F. Scherk și anume: *există o alegere a semnelor „+" și „–" astfel încât să aibă loc următoarele egalități:*

$p_{2n} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-2} + p_{2n-1}$

$p_{2n+1} = 1 \pm p_1 \pm p_2 \pm ... \pm p_{2n-1} + 2p_n$, *pentru* $n \in \mathbf{N}^*$ *unde* p_n *semnifică al n-lea număr prim.* Acest rezultat a fost conjuncturat de Scherk în 1830 și a fost demonstrat în 1928 de S. S. Pillai.

Demonstrația pe care o dăm aici urmează prezentarea lui Waclaw Sierpinski din *Elementary theory of numbers*, Warszawa, 1964, capitolul 3, paragraful 11, pagina 140. Se demonstrează de asemenea un rezultat al lui Sierpinski și anume: pentru $n \in \mathbf{N}^*$ există o alegere a semnelor + și – astfel încât să aibă loc egalitatea $p_{2n+1} = p_{2n} \pm p_{2n-1} \pm p_{2n-2} \pm ... \pm p_2 \pm p_1$. În propozițiile 1 și 3 se arată că putem preciza exact unele semne + și – din cele trei egalități precedente, alternând prima jumătate a semnelor sau pe cea de a doua. Rezultatele expuse în propozițiile 1 și 3 au fost demonstrate de L. Panaitopol în *Bull. Math. de la Soc. Sci. Math. de la R.S. de Roumanie*, volumul 31 (79), nr. 3, 1987, paginile 249–253. Pentru demonstrația propozițiilor 1 și 3 (mai exact pentru demonstrația teoremei 4 din anexă) s-au folosit inegalitățile lui Rosser și Schoenfeld (se arată locul în care poate fi găsită demonstrația acestor inegalități).

Pentru soluția teoremei lui Scherk este nevoie de unele rezultate ce sunt în legătură cu teorema lui Cebîșev (sau postulatul lui Bertrand, cum i se mai spune). Aceste rezultate sunt demonstrate în anexă (inclusiv teorema lui Cebîșev care afirmă că $(\forall)\ n \in \mathbf{N}$, $n > 3$ există p număr prim astfel încât încât $n < p < 2n - 2$. Acest rezultat a fost conjencturat de P. Bertrand în 1845 și a fost demonstrat de P. Cebîșev în 1850).

Teoremă (S c h e r k): *Oricare ar fi n un număr natural nenul există o alegere a semnelor + și – astfel încât să aibă loc egalitățile următoare:*

(1) $p_{2n} = 1 \pm p_1 \pm p_2 \ldots \pm p_{2n-2} + p_{2n-1}$,

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

Avem nevoie de următoarea lemă:

Lemă 1 : *Fie* $(q_n)_{n \in \mathbf{N}^*}$ *un șir strict crescător de numere naturale având următoarele calități:*

i) $q_1 = 2,\ q_2 = 3, q_3 = 5, q_4 = 7, q_5 = 11, q_6 = 13, q_7 = 17$;

ii) q_n *este impar*, $(\forall)\ n \in \mathbf{N}, n \geq 2$;

iii) $q_{n+1} < 2\, q_n$, $(\forall)\ n \in \mathbf{N}^*$.

Pentru orice $n \in \mathbf{N}, n \geq 3$ *și orice număr natural impar mai mic sau egal cu* q_{2n+1} *există o alegere a semnelor + și – astfel încât numărul impar* $(\leq q_{2n+1})$ *să se scrie sub forma*:

$\pm q_1 \pm q_2 \pm \ldots \pm q_{2n+1} + q_{2n}$.

Demonstrație : Se va face demonstrația prin inducție după n. Pentru $n = 3$ trebuie verificat că orice număr natural impar mai mic sau egal cu $17 = q_7$ se poate scrie sub forma: $\pm 2 \pm 3 \pm 5 \pm 7 \pm 11 + 13$.

Într-adevăr au loc următoarele egalități:

$1 = -2 + 3 + 5 - 7 - 11 + 13 = -q_1 + q_2 + q_3 - q_4 - q_5 + q_6$

$3 = 2 - 3 - 5 + 7 - 11 + 13 = q_1 - q_2 - q_3 + q_4 - q_5 + q_6$

$5 = 2 + 3 + 5 - 7 - 11 + 13 = q_1 + q_2 + q_3 - q_4 - q_5 + q_6$

$7 = -2 - 3 - 5 - 7 + 11 + 13 = -q_1 - q_2 - q_3 - q_4 + q_5 + q_6$

$9 = 2 + 3 - 5 + 7 - 11 + 13 = q_1 + q_2 - q_3 + q_4 - q_5 + q_6$

$11 = 2 - 3 - 5 - 7 + 11 + 13 = q_1 - q_2 - q_3 - q_4 + q_5 + q_6$

$13 = 2 - 3 + 5 + 7 - 11 + 13 = q_1 - q_2 + q_3 + q_4 - q_5 + q_6$

$15 = -2 + 3 + 5 + 7 - 11 + 13 = -q_1 + q_2 + q_3 + q_4 - q_5 + q_6$

$17 = 2 + 3 - 5 - 7 + 11 + 13 = q_1 + q_2 - q_3 - q_4 + q_5 + q_6$.

Presupunem acum că enunțul lemei este adevărat pentru un număr natural $n \geq 3$. Fie $2k - 1$ un număr natural impar mai mic sau egal cu q_{2n+3}. Are loc inegalitatea

(3) $-q_{2n+2} < 2k - 1 - q_{2n+2} < q_{2n+2}$.

Prima parte a inegalității (3) are o justificare evidentă iar a doua este o consecință a condiției iii) din ipoteză

$$2k - 1 \leq q_{2n+3} < < 2\, q_{2n+2}\ .$$

Există deci o alegere a semnului + sau – astfel încât

(4) $0 \leq \pm (2k - 1 - q_{2n+2}) < q_{2n+2}$.

Folosind din nou condiția iii) din ipoteză, deducem că:

(5) $-q_{2n+1} \leq \pm (2k - 1 - q_{2n+2}) - q_{2n+1} < q_{2n+1}$.

Aceasta deoarece $\pm (2k-1-q_{2n+2}) < q_{2n+2} < 2q_{2n+1}$. Există deci o alegere a semnului + sau – astfel încât să aibă loc inegalitățile:

(6) $0 \le \pm [\pm (2k-1-q_{2n+2}) - q_{2n+1}] \le q_{2n+1}$.

Deoarece q_{2n+2} și q_{2n+1} sunt numere impare rezultă că termenul din mijlocul inegalităților de mai sus este număr natural impar și deci conform ipotezei de inducție există o alegere semnelor + și – astfel încât să aibă loc egalitatea

$\pm [\pm (2k-1-q_{2n+2}) - q_{2n+1}] = \pm q_1 \pm q_2 \ldots \pm q_{2n-1} + q_{2n}$. De aici deducem imediat că are loc o egalitate de tipul:

$2k-1 = \pm q_1 \pm q_2 \ldots \pm q_{2n+1} + q_{2n+2}$. Raționamentul prin inducție este încheiat și lema este demonstrată.

Să trecem acum la demonstrarea egalității (2) din teorema lui Scherk. Pentru aceasta (ca și pentru demonstrarea egalității (1) să observăm că șirul numerelor prime (p_n) îndeplinește cele trei condiții din ipoteza lemei precedente (primele două condiții sunt evidente iar cea de a treia este demonstrată în anexă – teorema 1) deci enunțul acestei leme poate fi aplicat în acest caz particular.

Dacă n este un număr natural, mai mare sau egal cu 3, atunci $p_{2n+1} - p_{2n} - 1$ este un număr natural impar $\le p_{2n+1}$. Aplicând lema precedentă rezultă că există o alegere a semnelor + și – astfel încât $p_{2n+1} - p_{2n} - 1 = \pm p_1 \pm p_2 \ldots \pm p_{2n-1} + p_{2n}$. Egalitatea (2) este astfel demonstrată pentru $n \in \mathbf{N}^*$, $n \ge 3$. Deoarece

$$p_3 = 5 = 1 - 2 + 2 \cdot 3 = 1 - p_1 + 2p_2$$

și

$$p_5 = 11 = 1 - 2 + 3 - 5 + 2 \cdot 7 = 1 - p_1 + p_2 - p_3 + 2p_4,$$

deducem că egalitatea (2) este valabilă $(\forall)\, n \in \mathbf{N}^*$.

Pentru $n \ge 3$, $p_{2n+2} - p_{2n+1} - 1$ este un număr natural impar mai mic sau egal cu p_{2n+1} (deoarece $p_{2n+2} < 2p_{2n+1}$ conform teoremei 1 din anexă). Aplicând din nou lema precedentă obținem (pentru o alegere a semnelor + și –) o egalitate de tipul $p_{2n+2} - p_{2n+1} - 1 = \pm p_1 \pm p_2 \ldots \pm p_{2n-1} + p_{2n}$. Deci egalitatea (1) este demonstrată pentru $n \in \mathbf{N}$, $n \ge 4$. Deoarece $p_2 = 3 = 1 + 2 = 1 + p_1$, $p_4 = 7 = 1 - 2 + 3 + 5 = 1 - p_1 + p_2 + p_3$, $p_6 = 13 = 1 + 2 - 3 - 5 + 7 + 11 = 1 + p_1 - p_2 - p_3 + p_4 + p_5$, egalitatea (1) este valabilă, $(\forall)\, n \in \mathbf{N}^*$; teorema lui Scherk este deci demonstrată.

Propoziția 1: *Există o alegere a semnelor + și – astfel încât*

(7) $p_{2n} = p_{2n-1} - p_{2n-2} + p_{2n-3} - p_{2n-4} \ldots + (-1)^{n+1} p_n + p_{n-1} \pm p_{n-2} \ldots \pm p_2 \pm p_1 + 1$, $(\forall)\, n \in \mathbf{N}$, $n \ge 7$ și

(8) $p_{2n+1} = 2p_{2n} - p_{2n-1} + p_{2n-2} - \ldots + (-1)^n p_n \pm p_{n-1} \ldots \pm p_2 \pm p_1 + 1$ $(\forall)\, n \ge 8$, $n \in \mathbf{N}$.

Demonstrație : Pentru a demonstra egalitatea (7) în cazul când n este număr par considerăm $x_n = p_{2n} - p_{2n-1} + p_{2n-2} \ldots + p_n - p_{n-1}$. Este evident că x_n este număr par strict pozitiv. De asemenea

$$x_n = p_{2n} - (p_{2n-1} - p_{2n-2}) - (p_{2n-3} - p_{2n-4}) \ldots - (p_{n+1} - p_n) - p_{n-1} < p_{2n} - p_{n-1} < p_{2n+1} - p_{n-2} < 2p_{n-2},$$

pentru $n \in \mathbf{N}$, $n \ge 18$.

Ultima inegalitate din evaluările precedente ($p_{2n+1} < 3p_{n-2}$, pentru $n \in \mathbf{N}$, $n \geq 18$) este valabilă în virtutea punctului i) al teoremei 4 din anexă. Deci $x_n - 1$ este un număr impar satisfăcând inegalitățile $0 < x_n - 1 < 2p_{n-2} - 1$ $(\forall)\, n \in \mathbf{N}$, $n \geq 18$, n număr par. Printr-un calcul ușor se arată că ultima inegalitate are loc chiar pentru $(\forall)\ n \in \mathbf{N}$, $n \geq 10$, n număr par.

Secvența $p_1, p_2, \ldots, p_{n-2}, 2p_{n-2} - 1$ satisface condițiile lemei 1 pentru orice $n \in \mathbf{N}$, $n \geq 10$, n număr par (vezi din nou teorema 1 din anexă) și cum $x_n - 1$ este un număr natural impar $< 2p_{n-2} - 1$ lema 1 asigură posibilitatea alegerii semnelor + și – astfel încât să aibă loc egalitatea

$$x_n - 1 = p_{n-2} \pm p_{n-3} \pm \ldots \pm p_2 \pm p_1.$$

Aceasta înseamnă că egalitatea (7) are loc pentru orice număr natural par $n \geq 10$ (Se observă imediat că concluziile lemei 1 se mențin dacă în locul șirului q_n se pune o secvență de numere naturale care îndeplinește aceleași condiții).

Dacă n este număr natural impar, $n \geq 9$ atunci considerăm

$$y_n = p_{2n} - p_{2n-1} + p_{2n-2} - \ldots + p_{n+1} - p_n \cdot y_n$$

număr natural par strict pozitiv care satisface inegalitatea $y_n < p_{2n} - p_n \leq 2p_{n-1}$ (inegalitatea $y_n < p_{2n} - p_n$ se arată grupând termenii în modul următor $y_n = p_{2n} - (p_{2n-1} - p_{2n-2}) - \ldots - (p_{n+2} - p_{n+1}) - p_n$; inegalitatea $p_{2n} \leq 2p_{n-1} + p_n$ pentru $n \geq 9$, n impar este consecința punctului iii) al teoremei 4 din anexă). Secvența $p_1, p_2, \ldots, p_{n-1}, 2p_{n-1} - 1$ satisface condițiile lemei 1 și cum $y_n - 1$ este un număr natural impar mai mic decât $2p_{n-1} - 1$ atunci (conform lemei 1) există o alegere a semnelor + și – astfel încât să aibă loc egalitatea

$$y_n - 1 = p_{n-1} \pm p_{n-2} \ldots \pm p_2 \pm p_1.$$

Egalitatea (7) este deci demonstrată pentru $(\forall)\ n \in \mathbf{N}$, $n \geq 9$. Ținând cont de egalitățile:

$$43 = p_{14} = 41 - 37 + 31 - 29 + 23 - 19 + 17 + 13 - 11 + 7 + 5 + 3 - 2 + 1 =$$
$$= p_{13} - p_{12} + p_{11} - p_{10} + p_9 - p_8 + p_7 + p_6 - p_5 + p_4 + p_3 + p_2 - p_1 + 1.$$
$$53 = p_{16} = p_{15} - p_{14} + p_{13} - p_{12} + p_{11} - p_{10} + p_9 - p_8 + p_7 + p_6 + p_5 + p_4 -$$
$$- p_3 - p_2 - p_1 + 1 = 47 - 43 + 41 - 37 + 31 - 29 + 23 - 19 + 17 + 13 +$$
$$+ 11 + 7 - 5 - 3 - 2 + 1,$$

formula (7) este adevărată pentru orice $n \in \mathbf{N}$, $n \geq 7$.

Pentru a demonstra egalitatea (8) în cazul în care n este număr par considerăm pe $x_n = p_{2n+1} - 2p_{2n} + p_{2n-1} - p_{2n-2} \ldots + p_{n+1} - p_n + p_{n-1}$. x_n număr întreg par. $x_n - 1 = (p_{2n+1} - p_{2n}) + (p_{2n-1} - p_{2n-2}) + \ldots + (p_{n+1} - p_n) - p_{2n} + p_{n-1} - 1 \geq 2 - p_{2n} + p_{n-1} - 1 > 1 - p_{2n+1} + p_{n-2} > 1 - 2p_{n-2}$, pentru $n \geq 18$ (ultima inegalitate din șirul de evaluări de mai sus are loc conform punctului i) din teorema 4 prezentată în anexă). Punctul ii) al teoremei amintite ne asigură că $p_{2n+1} < p_{2n} + p_n$, pentru $n \in \mathbf{N}$, $n \geq 3$.

Deci

$$x_n - 1 = (p_{2n+1} - p_{2n}) - (p_{2n} - p_{2n-1}) - (p_{2n-2} - p_{2n-3}) \ldots$$
$$- (p_n - p_{n-1}) - 1 < p_n - 1 < 2p_{n-2} - 1,$$

pentru $n \in \mathbf{N}$, $n \geq 18$ (ultima inegalitate are loc datorită teoremei 3 a anexei). Din cele de mai sus rezultă că $|x_n - 1|$ este un număr natural impar care satisface inegalitățile $0 < |x_n - 1| < 2p_{n-2} - 1$. Aplicând lema 1 secvenței $p_1, p_2, \ldots, p_{n-2}, 2p_{n-2} - 1$ deducem că există (pentru $n \in \mathbf{N}$, $n \geq 18$) o alegere a semnelor + și – astfel încât $|x_n - 1| = p_{n-2} \pm p_{n-3} \ldots \pm p_2 \pm p_1$. De aici rezultă imediat egalitatea (8) pentru n par, $n \geq 18$. Pentru $n = 10, 12, 14, 16$ se arată prin calcul direct că $|x_n - 1| < 2p_{n-2} - 1$ și raționamentul se face ca mai sus. Pentru $n = 8$ avem următoarea egalitate $p_{17} = 59 = 2p_{16} - p_{15} + p_{14} - p_{13} + p_{12} - p_{11} + p_{10} - p_9 + p_8 - p_7 - p_6 - p_5 + p_4 + p_3 - p_2 - p_1 + 1$.

În cazul în care n este număr natural impar atunci considerăm

$$y_n = p_{2n+1} - - 2p_{2n} + p_{2n-1} - p_{2n-2} \ldots - p_{n+1} + p_n. \; y_n - 1$$

este număr întreg impar care satisface următoarele inegalități

$$y_n - 1 = (p_{2n+1} - p_{2n}) + (p_{2n-1} - p_{2n-2}) + \ldots + (p_{n+2} - p_{n+1}) - p_{2n} + p_n - 1 > 2 - p_{2n} + p_n - 1 \geq 1 - 2p_{n-1}$$

(ultima inegalitate are loc pentru $n \in \mathbf{N}$, n impar, $n \geq 9$, conform punctului iii) din teorema 4 a anexei). De asemenea

$$y_n - 1 = p_{2n+1} - p_{2n} - (p_{2n} - p_{2n-1}) - \ldots - (p_{n+1} - p_n) - 1 < p_n - 1 < 2p_{n-1} - 1$$

(avem că $p_{2n+1} - p_{2n} < p_n$ pentru $n \in \mathbf{N}$, $n \geq 3$ conform punctului ii) din teorema 4 a anexei și $p_n < 2p_{n-1}$ $(\forall)\, n \in \mathbf{N}$, $n \geq 2$ conform teoremei 1 a anexei). Din cele de mai sus rezultă că $|y_n - 1|$ este un număr natural impar care satisface inegalitățile $0 < |y_n - 1| < 2p_{n-1} - 1$, pentru $n \in \mathbf{N}$, $n \geq 9$, n impar. Aplicând lema 1 secvenței $p_1, p_2, \ldots, p_{n-1}, 2p_{n-1} - 1$ rezultă că există o alegere a semnelor + și – astfel încât să aibă loc o egalitate de tipul:

$$|y_n - 1| = p_{n-1} \pm p_{n-2} \pm \ldots \pm p_2 \pm p_1 .$$

De aici și din cele de mai sus deducem imediat valabilitatea egalității (8) pentru orice număr natural mai mare sau egal cu 8.

Propoziția 2 : *Pentru orice $n \in \mathbf{N}$, $n \geq 1$ există o alegere a semnelor + și – astfel încât să aibă loc o egalitate de tipul*:

$$p_{2n+1} = p_{2n} \pm p_{2n-1} \ldots \pm p_2 \pm p_1.$$

Demonstrație : Pentru $n \geq 3$ enunțul rezultă imediat din lema 1 (cum am mai spus șirul numerelor prime satisface condițiile lemei 1 conform teoremei 1 din anexă). $p_5 = 11 = 7 + 5 - 3 + 2 = p_4 + p_3 - p_2 + p_1$, $p_3 = 5 = 3 + 2 = p_2 + p_1$; aceasta arată că propoziția 2 este adevărată pentru orice $n \in \mathbf{N}^*$.

Lema 2: *Dacă $(q_n)_{n \in \mathbf{N}^*}$ este un șir strict crescător de numere naturale satisfăcând condițiile din lema 1 atunci pentru orice $n \geq 4$ și orice număr natural par $2k$ mai mic strict decât q_{2n} există o alegere a semnelor + și – astfel încât să aibă loc egalitatea:*

$$2k = q_{2n-1} \pm q_{2n-2} \pm \ldots \pm q_2 \pm q_1.$$

Demonstrație : Au loc inegalitățile $-q_{2n-1} \leq 2k - q_{2n-1} < q_{2n} - q_{2n-1} < q_{2n-1}$ (ultima inegalitate are loc conform teoremei 1 din anexă) ceea ce înseamnă că $|2k - q_{2n-1}|$ este un număr natural impar mai mic sau egal cu q_{2n-1}. Cum

$n-1 \geq 3$ lema 1 ne asigură posibilitatea alegerii semnelor + și – astfel încât să aibă loc o egalitate de tipul $|2k - q_{2n-1}| = q_{2n-2} \pm q_{2n-3} \pm ... \pm q_2 \pm q_1$.

Enunțul lemei 2 este în acest moment evident.

Propoziția 3 : *Pentru* $n \in \mathbf{N}$, $n \geq 6$ *există o alegere a semnelor* + *și* – *astfel încât să aibă loc egalitatea*:

(9) $p_{2n+1} = p_{2n} - p_{2n-1} + p_{2n-2} - ... + (-1)^n p_n + p_{n-1} \pm p_{n-2} \pm ... \pm p_2 \pm p_1$.

Demonstrație : În cazul în care n este par considerăm numărul

$$x_n = p_{2n+1} - - p_{2n} + p_{2n-1} - ... + p_{n+1} - p_n \cdot x_n$$

este un număr natural par care satisface inegalitățile

$$0 < x_n < p_{2n+1} - p_n < 2p_{n-1} - 1,$$

pentru $n \in \mathbf{N}$, $n \geq 10$, n par (ultima inegalitate are loc conform punctului iv) din teorema 4 a anexei). Aplicăm lema 2 secvenței $p_1, p_2, ..., p_{n-1}, 2p_{n-1} - 1$ și numărului natural par $x_n < 2p_{n-1} - 1$. Există deci o alegere a semnelor + și – astfel încât să aibă loc egalitatea $x_n = p_{n-1} \pm p_{n-2} \pm ... \pm p_2 \pm p_1$. Aceasta înseamnă că egalitatea (9) are loc pentru orice număr natural par ≥ 10.

Dacă n este număr natural impar, ≥ 9 considerăm

$$y_n = p_{2n+1} - p_{2n} + p_{2n-1} - ... + p_n - p_{n-1} \cdot y_n$$

număr natural par care satisface inegalitățile

$$0 < y_n < p_{2n+1} - p_{n-1} < 3 \cdot p_{n-2} - p_{n-2} - 1 = 2p_{n-2} - 1,$$

pentru $n \in \mathbf{N}$, n impar, $n \geq 19$ (inegalitatea $p_{2n+1} < 3p_{n-2}$ este consecință a punctului i) din teorema 4 a anexei, iar inegalitatea $-p_{n-1} < -p_{n-2} - 1$ este evidentă). Printr-un calcul direct se poate verifica că $0 < y_n < 2p_{n-2} - 1$ și pentru $n = 9, 11, 13, 15, 17$.

Aplicând (pentru $n \in \mathbf{N}$, n impar, $n \geq 9$) lema 2 secvenței $p_1, p_2, ..., p_{n-2}, 2p_{n-2} - 1$ și numărului natural par y_n ($0 < y_n < 2p_{n-2} - 1$) deducem că există o alegere a semnelor + și – astfel încât să aibă loc egalitatea $y_n = p_{n-2} \pm p_{n-3} \pm ... \pm p_2 \pm p_1$. Deci egalitatea (9) este adevărată pentru orice $n \in \mathbf{N}$, $n \geq 9$. Pentru a încheia demonstrația să observăm că au loc următoarele egalități

$p_{13} = 41 = p_{12} - p_{11} + p_{10} - p_9 + p_8 - p_7 + p_6 + p_5 - p_4 + p_3 + p_2 + p_1 =$
$= 37 - 31 + 29 - 23 + 19 - 17 + 13 + 11 - 7 + 5 + 3 + 2.$

$p_{15} = 47 = p_{14} - p_{13} + p_{12} - p_{11} + p_{10} - p_9 + p_8 - p_7 + p_6 + p_5 + p_4 + p_3 -$
$- p_2 - p_1 = 43 - 41 + 37 - 31 + 29 - 23 + 19 - 17 + 13 + 11 + 7 +$
$+ 5 - 3 - 2.$

$p_{17} = 59 = p_{16} - p_{15} + p_{14} - p_{13} + p_{12} - p_{11} + p_{10} - p_9 + p_8 + p_7 + p_6 -$
$- p_5 + p_4 - p_3 - p_2 + p_1 = 53 - 47 + 43 - 41 + 37 - 31 + 29 - 23 +$
$+ 19 + 17 + 13 - 11 + 7 - 5 - 3 + 2.$

Deci egalitatea (9) are loc pentru orice $n \in \mathbf{N}$, $n \geq 6$.

ANEXA
(Teorema lui Scherk)

Lema 1: $C_{2n}^{n} > \frac{4^n}{2\sqrt{n}}$, $(\forall) n \in \mathbf{N}, n > 1$.

Demonstrație: Inegalitatea de mai sus se demonstrează prin inducție după n. $C_4^2 = 6 > \frac{4^2}{2\sqrt{2}}$; enunțul este deci adevărat pentru $n = 2$. Dacă $C_{2n}^{n} > \frac{4^n}{2\sqrt{n}}$ pentru $n \in \mathbf{N}$, $n > 1$ atunci

$$C_{2(n+1)}^{n+1} = \frac{(2n+2)!}{[(n+1)!]^2} = \frac{(2n+2)(2n+1)}{(n+1)^2} \cdot C_{2n}^{n} =$$

$$= \frac{2(2n+1)}{n+1} \cdot C_{2n}^{n} > \frac{2(2n+1)}{n+1} \cdot \frac{4^n}{2\sqrt{n}} = \frac{2(2n+1) \cdot 4^n}{\sqrt{n+1} \cdot \sqrt{4n^2+4n}} > \frac{2 \cdot 4^n}{\sqrt{n+1}} = \frac{4^{n+1}}{2\sqrt{n+1}}$$

și demonstrația este încheiată $(2n+1 > \sqrt{4n^2+4n}$, deoarece $(2n + 1)^2 = 4n^2 + 4n + 1)$.

Lema 2: *Dacă notăm cu P_n produsul numerelor prime mai mici sau egale cu n atunci $P_n < 4^n$ $(\forall) n \in \mathbf{N}^*$ $(P_1 = 1)$.*

Demonstrație: Avem $P_1 = 1 < 4^1$, $P_2 = 2 < 4^2$. Fie $n \in \mathbf{N}$, $n > 2$ astfel încât enunțul lemei 2 este adevărat pentru orice număr natural mai mic strict decât n. Dacă n este par atunci $P_n = P_{n-1} < 4^{n-1} < 4^n$.

Dacă $n = 2k + 1$ $(k \in \mathbf{N}^*)$, atunci fiecare număr prim p, pentru care

$$k + 2 \leq \leq p \leq 2k + 1,$$

divide numărul

$$C_{2k+1}^{k} = \frac{(2k+1) \cdot 2k \ldots (k+2)}{k!}.$$

Deoarece

$$(1+1)^{2k+1} > C_{2k+1}^{k} + C_{2k+1}^{k+1} = 2C_{2k+1}^{k}$$

deducem că $C_{2k+1}^{k} < 4^k$. $P_{k+1} < 4^{k+1}$ conform ipotezei de inducție. Din considerațiile precedente rezultă că

$$P_n \le P_{k+1} \cdot C_{2k+1}^{k} < 4^{k+1} \cdot 4^k = 4^{2k+1} = 4^n.$$

Enunțul lemei 2 este astfel demonstrat.

Lema 3: *Dacă p este un număr prim astfel încât* $p \mid C_{2n}^{n}$ *și* $p \ge \sqrt{2n}$ *atunci exponentul lui p în descompunerea în factori primi a lui* C_{2n}^{n} *este egal cu* 1.

Demonstrație: Conform lemei 1 (teorema Legendre) din paragraful I al anexei teoremei lui Brun, exponentul lui p în C_{2n}^{n} este egal cu $\sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right)$.

Avem că $p=\sqrt{2n}$ doar în cazul $n = 2$. Deci $p = 2$ și exponentul lui 2 în $C_4^2 = 6$ este egal cu 1. Putem presupune deci că $p>\sqrt{2n}$. Această presupunere asigură faptul că $\left[\frac{2n}{p^k}\right] = 0$, pentru orice $k \in \mathbf{N}$, $k \ge 2$. Deci

$$\sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right)=\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]<\frac{2n}{p}-2\left(\frac{n}{p}-1\right)=2.$$

În acest moment enunțul este demonstrat $\left(\sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right)\ge 1 \text{ deoarece } p \mid C_{2n}^{n}\right)$.

Lema 4: *Dacă n este un număr natural mai mare strict decât* 2, *atunci nici un număr prim p pentru care* $\frac{2}{3}n < p \le n$ *nu poate să dividă numărul* C_{2n}^{n}.

Demonstrație. Dacă p este un număr prim astfel încât $\frac{2}{3}n < p \le n$ atunci $1 \le \frac{n}{p} < \frac{3}{2}$ și $2 \le 2\frac{n}{p} < 3$. Deci $\left[\frac{n}{p}\right]=1, \left[\frac{2n}{p}\right]=2$ și $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 = 0$. Dacă $k \in \mathbf{N}$, $k \ge 2$ atunci $p^k \ge p^2 > \frac{4n^2}{9}$ și $\frac{2n}{p^k} \le \frac{2n}{p^2} < \frac{9}{2n} \le \frac{9}{10} < 1$ pentru $n \ge 5$. De aici deducem că $\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]=0$ pentru orice $k \in \mathbf{N}$, $k \ge 2$.

Folosind din nou teorema lui Legendre (lema 1 din paragraful I al anexei teoremei lui Brun) enunțul lemei 4 este demonstrat pentru $n \geq 5$. Dacă $n = 3$ sau $n = 4$ rezultă că $p = 3$. Cum $3 \nmid C_6^3 = 20$ și $3 \nmid C_8^4 = 70$ enunțul lemei 4 este demonstrat și în cazurile $n = 3$ și $n = 4$.

Lema 5. *Exponentul numărului prim p în descompunerea în factori primi a lui* C_{2n}^n *este egal cu* 1 *dacă* $n < p < 2n$.

Demonstrație. Dacă p este un număr prim astfel încât $n < p < 2n$ atunci $1 < \frac{2n}{p} < 2$ și $\frac{n}{p} < 1$. Aceasta înseamnă că $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 1 - 2 \cdot 0 = 1$. Dacă $k \in \mathbf{N}, k \geq 2$ atunci $\frac{2n}{p^k} \leq \frac{2n}{p^2} < \frac{2}{n}$. Dacă $n \geq 2$ din inegalitățile precedente deducem că $\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] = 0$ pentru $k \geq 2$. Folosind din nou teorema lui Legendre (invocată și mai sus) enunțul lemei 5 este demonstrat. Dacă $n = 1$ nu există p prim care să satisfacă inegalitățile $n < p < 2n$.

Lema 6: $\pi(n) \leq \frac{n}{2} - 1$ *pentru* $n \in \mathbf{N}, n \geq 14$.

Demonstrație: $\pi(14) = 6 = \frac{14}{2} - 1$. Enunțul este deci adevărat pentru $n = 14$.

Dacă $n \in \mathbf{N}, n \geq 15$ atunci numerele $1, 9, 15, 4, 6, 8, 10 \ldots\ldots, 2\left[\frac{n}{2}\right]$ nu sunt prime și sunt mai mici sau egale cu n. Deci $\pi(n) \leq n - \left(3 + \left[\frac{n}{2}\right] - 1\right) =$

$= n - 2 - \left[\frac{n}{2}\right] < n - 2 - \left(\frac{n}{2} - 1\right) = \frac{n}{2} - 1.$

Lema 7: *Dacă notăm cu* R_n *produsul numerelor prime p care satisfac inegalitățile* $n < p \leq 2n$ *atunci* $R_n > \frac{4^{\frac{n}{3}}}{2\sqrt{n}(2n)^{\sqrt{\frac{n}{2}}}}$ $(\forall) n \geq 98$ (*dacă nu există p prim astfel încât* $n < p \leq 2n$ *atunci convenim că* $R_n = 1$).

Demonstrație: Din modul de definire al numărului R_n se deduce că $R_n \mid C_{2n}^n$ și deci $C_{2n}^n = R_n \cdot Q_n$ unde $Q_n \in \mathbf{N}^*$. Folosind lema 5 deducem că orice

divizor prim p al lui Q_n trebuie să fie mai mic sau egal cu n. Din lema 4 rezultă mai mult, anume că orice divizor prim p al lui Q_n trebuie să fie $\leq \frac{2n}{3}$. Să observăm că dacă $q^r \mid C_{2n}^n$, q fiind număr prim, atunci $q^r \leq 2n$. Să presupunem că $q^r > 2n$. Aceasta înseamnă că $\left[\frac{2n}{q^k}\right] = 0, (\forall) k \geq r$ și deci exponentul lui q în C_{2n}^n este egal cu

$$\sum_{k=1}^{r-1}\left(\left[\frac{2n}{q^k}\right] - 2\left[\frac{n}{q^k}\right]\right) \leq r - 1$$

($[2y] - 2[y] < 2y - 2(y-1) = 2$ și deci $[2y] - 2[y] \leq 1$, $(\forall)\, y \in \mathbf{R}$). Aceasta însă contrazice ipoteza $q^r \mid C_{2n}^n$. Deci $q^r \leq 2n$.

Dacă exponentul unui număr prim p în descompunerea lui Q_n este mai mare strict decât 1 atunci $p < \sqrt{2n}$. Q_n se poate scrie sub forma $Q_n = A_n \cdot B_n$, unde $A_n, B_n \in \mathbf{N}^*$, $(A_n, B_n) = 1$, A_n este produs de numere prime diferite, iar B_n are calitatea că orice număr prim q care divide pe B_n trebuie să satisfacă și relația $q^2 \mid B_n$. Deoarece orice divizor prim al lui Q_n este $\leq \frac{2n}{3}$, rezultă că $A_n \leq P_{\left[\frac{2n}{3}\right]} < 4^{\left[\frac{2n}{3}\right]} \leq 4^{\frac{2n}{3}}$. Ținând cont de observațiile precedente (dacă $q^r \mid C_{2n}^n$ și q e prim atunci $q^r \leq 2n$ și dacă exponentul unui număr prim p în descompunerea lui Q_n este mai mare strict decât 1, atunci $p < \sqrt{2n}$ conform lemei 3), deducem că $B_n \leq (2n)^{\pi\left(\left[\sqrt{2n}\right]\right)}$. Deoarece $n \geq 98$, atunci $[\sqrt{2n}] \geq 14$ și

$$\pi\left(\left[\sqrt{2n}\right]\right) \leq \frac{\left[\sqrt{2n}\right]}{2} - 1 < \frac{\sqrt{2n}}{2} = \sqrt{\frac{n}{2}}.$$

Folosind inegalitățile obținute pentru A_n și B_n rezultă că $Q_n = A_n \cdot B_n < 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{\frac{n}{2}}}$, pentru $n \geq 98$. Ținând cont și de lema 1 obținem inegalitățile: $\frac{4^n}{2\sqrt{n}} < C_{2n}^n = R_n \cdot Q_n < R_n \cdot 4^{\frac{2n}{3}} \cdot (2n)^{\sqrt{\frac{n}{2}}}$. Lema 7 este astfel demonstrată.

Lema 8: $2^k > 18(k+1)$, $(\forall)\, k \in N$, $k \geq 8$ și $2^x > 18x$, $(\forall)\, x \in \mathbf{R}$, $x \geq 8$.

Demonstrație: Prima parte e enunțului se demonstrează prin inducție după k. Pentru $k = 8$ enunțul este adevărat deoarece $2^8 = 256 > 18 \cdot 9 = 162$. Presupunând că $2^k > 18\ (k+1)$ (pentru un $k \in N$, $k \geq 8$) deducem că $2^{k+1} = 2^k \cdot 2 > 36\ (k+1) > 18\ (k+2)$. Raționamentul prin inducție este încheiat. Dacă $x \in \mathbf{R}$, $x \geq 8$ atunci $2^x \geq 2^{[x]} > 18([x]+1) > 18x$ (am folosit prima parte a enunțului precum și inegalitatea $[x] + 1 > x$).

Lema 9: $2^k > 6(k+1)$, $(\forall)\, k \in \mathbf{N}$, $k \geq 6$ și $2^x > 6x$, $(\forall)\, x \in \mathbf{R}$, $x \geq 6$.

Demonstrație: Se face exact la fel ca demonstrația lemei 8.

Lema 10: *$R_n > 2n$ pentru orice $n \in \mathbf{N}$, $n \geq 648$.*

Demonstrație: Conform lemei 7 este suficient să demonstrăm că $4^{\frac{n}{3}} > 4n\sqrt{n} \cdot (2n)^{\sqrt{\frac{n}{2}}}$, $(\forall)\ n \in \mathbf{N}$, $n \geq 648$. Deoarece $n \geq 648$ rezultă că $\frac{\sqrt{2n}}{6} \geq \frac{2 \cdot 18}{6} = 6$ și deci $2^{\frac{\sqrt{2n}}{6}} > \sqrt{2n}$ (conform lemei 9). Ridicând ultima inegalitate la puterea $\sqrt{2n}$ obținem că: $2^{\frac{n}{3}} > \left(\sqrt{2n}\right)^{\sqrt{2n}} = (2n)^{\sqrt{\frac{n}{2}}}$. Folosind lema 8 (și ținând cont că $\frac{2n}{9} > 8$ pentru $n \geq 648$) deducem că $2^{\frac{2n}{9}} > 18 \cdot \frac{2n}{9} = 4n$. De aici rezultă imediat că $2^{\frac{n}{3}} > 4n \cdot \sqrt{4n} > 4n\sqrt{n}$. Această ultimă inegalitate, împreună cu evaluarea $2^{\frac{n}{3}} > (2n)^{\sqrt{\frac{n}{2}}}$, conduce la inegalitatea $4^{\frac{n}{3}} > 4n\sqrt{n}(2n)^{\sqrt{\frac{n}{2}}}$. Enunțul este deci demonstrat.

Lema 11: *Dacă $n \in \mathbf{N}$, $n \geq 648$ atunci există cel puțin două numere prime mai mari strict decât n și mai mici decât $2n$.*

Demonstrație. Dacă ar exista cel mult un număr prim având calitățile indicate mai sus atunci R_n ar trebui să satisfacă inegalitatea $R_n \leq 2n$; ceea ce nu este posibil pentru $n \in \mathbf{N}$, $n \geq 648$ conform lemei 10. Enunțul lemei 11 este astfel demonstrat prin reducere la absurd.

Lema 12. *Dacă $n \in \mathbf{N}$, $n > 5$ atunci există cel puțin două numere prime p astfel încât $n < p \leq 2n$ (de fapt $p < 2n$ deoarece pentru $n \in \mathbf{N}$, $n > 5$, $2n$ este număr compus).*

Demonstrație: Conform lemei 11 trebuie să demonstrăm enunțul pentru $n \in \mathbf{N}$, $6 \leq n \leq 647$. Pentru $n = 6$ enunțul este adevărat deoarece $6 < 7 < 11 < 12 = 2 \cdot 6$. Fie acum următoarea secvență de numere naturale: $q_1 = 7$, $q_2 = 11$, $q_3 = 13$, $q_4 = 19$, $q_5 = 23$, $q_6 = 37$, $q_7 = 43$, $q_8 = 73$, $q_9 = 83$, $q_{10} = 139$, $q_{11} = 163$, $q_{12} = 277$, $q_{13} = 317$, $q_{14} = 547$, $q_{15} = 631$, $q_{16} = 653$, $q_{17} = 1259$. Numerele din această secvență sunt toate numere naturale prime și în plus este verificată

inegalitatea $q_{k+2} < 2 \cdot q_k$, $(\forall)\ k = \overline{1,15}$. Fie acum $n \in \mathbf{N}$, $6 < n \leq 647$. Există un unic $k \in \mathbf{N}^*$, $k \leq 15$ astfel încât $q_k \leq n < q_{k+1}$. Deoarece $q_{k+2} < 2 \cdot q_k \leq 2n$ deducem că între n și $2n$ se află cel puțin două numere prime și anume q_{k+1} și q_{k+2}.

Teorema 1. $p_{k+1} < 2 \cdot p_k$, $(\forall)\ k \in \mathbf{N}^*$.

Demonstrație. Dacă $k \in \mathbf{N}$, $k \geq 4$ atunci $p_k \geq 7 > 5$ și conform lemei 12 deducem că $p_{k+1} < 2\,p_k$ (se întâmplă chiar mai mult și anume $p_{k+2} < 2 \cdot p_k$). Deoarece $p_2 = 3 < 2 \cdot 2 = 2p_1$, $p_3 = 5 < 2 \cdot 3 = 2 \cdot p_2$, $p_4 = 7 < 2 \cdot 5 = 2p_3$, enunțul teoremei 1 este în acest moment demonstrat.

Deși pentru demonstrația teoremei lui Scherk vom folosi doar rezultatul enunțat în teorema 1, vom demonstra în continuare un rezultat celebru de teoria numerelor enunțat în 1845 de Bertrand și demonstrat de Cebîșev în 1850.

Teorema 2. *Dacă* $n \in \mathbf{N}$, $n > 3$ *atunci există un număr prim* p *astfel încât* $n < p < 2n - 2$.

Demonstrație: Folosind lema 12 pentru $n \in N$, $n \geq 6$ deducem că există două numere prime p și q încât $n < p < q < 2n$. De aici rezultă imediat că $p \leq 2n - 2$ și enunțul teoremei 2 este demonstrat pentru că $2n - 2$ este număr compus pentru $n \in \mathbf{N}$, $n \geq 6$. Dacă $n = 5$, atunci $5 < 7 < 2 \cdot 4 = 8$ și dacă $n = 4$, atunci $4 < 5 < 6 = 2n - 2$. Enunțul teoremei 2 este în acest moment demonstrat.

Corolar. *Dacă* $n \in \mathbf{N}$, $n > 1$ *atunci există* p *un număr prim astfel încât* $n < p < 2n$.

Demonstrație: Dacă $n \in \mathbf{N}$, $n \geq 4$, atunci totul rezultă din teorema 2. Dacă $n = 3$, atunci $3 < 5 < 2 \cdot 3 = 6$ și dacă $n = 2$, atunci $2 < 3 < 2 \cdot 2 = 4$. Enunțul corolarului este demonstrat.

În cursul demonstrației teoremei 1 s-a probat și următorul rezultat:

Teorema 3: $p_{k+2} \underset{\neq}{\leq} 2p_k$, $(\forall)\ k \in \mathbf{N}$, $k \geq 4$.

Teorema 4: *Au loc următoarele inegalități*:

i) $p_{2n+1} < 3\,p_{n-2}$, *pentru* $n \in \mathbf{N}$, $n \geq 18$;

ii) $p_{2n+1} < p_{2n} + p_n$, *pentru* $n \in \mathbf{N}$, $n \geq 3$;

iii) $p_{2n} \leq p_n + 2p_{n-1}$, *pentru* $n \in \mathbf{N}$, $n \geq 9$, *n impar*;

iv) $p_{2n+1} < p_n + 2p_{n-1} - 1$, *pentru* $n \in \mathbf{N}$, $n \geq 10$, *n par*.

Demonstrație. Pentru demonstrarea teoremei 4 avem nevoie de următoarele rezultate:

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

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

Demonstrația rezultatelor anterioare poate fi găsită în articolul *Aproximate formulas for some functions of prime numbers* de Rosser J. B. și Schoenfeld L. din Illinois J. Math. volumul 6, 1962, paginile 64–89.

În cele ce urmează vom demonstra doar inegalitatea i), modul de demonstrare pentru celelalte inegalități fiind absolut același. Vom arăta în continuare că funcția

$$f(x)=\frac{4}{3}\big(\ln(x-2)+\ln\ln(x-2)\big)-\ln(2x+1)-\ln\ln(2x+1)-\frac{3}{2}$$

este pozitivă pe intervalul $[230, +\infty)$. Să observăm că funcția f este crescătoare. Într-adevăr

$$f'(x)=\frac{4}{3}\cdot\frac{1}{x-2}+\frac{4}{3}\cdot\frac{1}{\ln(x-2)}\cdot\frac{1}{x-2}-\frac{2}{2x+1}-\frac{1}{\ln(2x+1)}\cdot\frac{2}{2x+1}>0,$$

deoarece

$$\frac{4}{3(x-2)}>\frac{2}{2x+1} \text{ și } \frac{1}{\ln(x-2)}>\frac{1}{\ln(2x+1)},$$

pentru $(\forall)\ x\in[230, +\infty)$; aceasta înseamnă că funcția f este crescătoare pe intervalul amintit. Folosind tabela cu logaritmi naturali vom calcula

$$f(230)=\frac{4}{3}\big(\ln 2{,}28+\ln 100\big)+\frac{4}{3}\ln(\ln 2,28+\ln 100)-$$

$$-\ln 4{,}61-\ln 100-\ln(\ln 4{,}61+\ln 100)-\frac{3}{2}\approx$$

$$\approx\frac{4}{3}(0,8242+4{,}6051)+\frac{4}{3}\ln(0,8242+4,6051)-$$

$$-(1{,}5282+4,6051)-\ln(1,5282+4,6051)-1{,}5\geq$$

$$\geq\frac{4}{3}\cdot 5{,}4293+\frac{4}{3}\ln 5,42-6,1333-\ln 6,14-1,5\approx$$

$$\approx 7,2390+\frac{4}{3}\cdot 1{,}6901-6,1333-1,8148-1,5\approx$$

$$\approx 1,1057+2,2534-1,8148-1,5=1{,}1057++0,4386-1,5=0,0443.$$

Cum eroarea în scrierea logaritmilor este de cel mult 0,0001, din cele de mai sus deducem că $f(230)>0$ și cum f este funcție crescătoare rezultă că f este funcție pozitivă pe intervalul $[230, +\infty)$. De aici obținem imediat următoarea inegalitate:

$$(3)\qquad \frac{4}{3}\left(\ln(n-2)+\ln\ln(n-2)-\frac{3}{2}\right)>\ln(2n+1)+\ln\ln(2n+1)-\frac{1}{2},$$

$(\forall)\ n\in\mathbf{N},\ n\geq 230.$

Folosind inegalitățile (1) și (2) precum și faptul că

$$3(n-2)>\frac{4}{3}(2n+1)$$

pentru $n \geq 230$, deducem că

$$3p_{n-2} > 3(n-2)\left(\ln(n-2) + \ln\ln(n-2) - \frac{3}{2}\right) >$$

$$> \frac{4}{3}(2n+1)\left(\ln(n-2) + \ln\ln(n-2) - \frac{3}{2}\right) >$$

$$> \left(\ln(2n+1) + \ln\ln(2n+1) - \frac{1}{2}\right) \cdot (2n+1) > p_{2n+1}$$

pentru $n \geq 230$ (am ținut cont în șirul de inegalități de mai sus de inegalitatea (3)). Pentru a demonstra inegalitatea din enunț pentru $18 \leq n \leq 230$ vom proceda într-o manieră asemănătoare procedeului din soluția lemei 12. Fie secvența: $p_{37} = 157$, $p_{39} = 167$, $p_{41} = 179$, $p_{45} = 197$, $p_{47} = 211$, $p_{51} = 233$, $p_{55} = 257$, $p_{61} = 283$, $p_{65} = 313$, $p_{75} = 379$, $p_{87} = 449$, $p_{99} = 523$, $p_{121} = 661$, $p_{145} = 829$, $p_{177} = 1051$, $p_{217} = 1327$, $p_{273} = 1753$, $p_{339} = 2281$, $p_{429} = 2971$, $p_{461} = 3259$, de numere naturale prime cu proprietatea că dacă $p_{2\alpha+1}, p_{2\beta+1}$ sunt doi termeni consecutivi ai secvenței precedente, atunci $p_{2\beta+1} < 3p_{\alpha-1}$; în plus $p_{37} = p_{2\cdot 18+1} = 157 < 3 \cdot 53 = 3 \cdot p_{16} = 3 \cdot p_{18-2}$ (să menționăm că: $p_{16} = 53$, $p_{17} = 59, p_{18} = 61, p_{19} = 67, p_{21} = 73$, $p_{22} = 79, p_{24} = 89, p_{26} = 101, p_{29} = 109$, $p_{31} = 127, p_{36} = 151, p_{42} = 181$, $p_{48} = 223, p_{59} = 277, p_{71} = 353, p_{87} = 449$, $p_{107} = 587, p_{135} = 761, p_{168} = 997, p_{213} = 1303$). Fie acum p_{2i+1}, unde $2i + 1 \in \mathbf{N}$ și $37 \leq 2i + 1 \leq 461$, un număr prim care este situat în intervalul $(p_{2\alpha+1}, p_{2\beta+1}]$, unde $p_{2\alpha+1}$ și $p_{2\beta+1}$ sunt doi termeni consecutivi ai secvenței indicate mai sus. Atunci $2i + 1 \geq 2\alpha + 3$, $i \geq \alpha + 1$, $i - 2 \geq \alpha - 1$. Folosind aceste inegalități precum și calitățile secvenței de mai sus ($p_{2\beta+1} < 3p_{\alpha-1}$) deducem că $p_{2i+1} \leq p_{2\beta+1} < 3 \cdot p_{\alpha-1} \leq 3\, p_{i-2}$ ceea ce reprezintă chiar inegalitatea i) pentru orice $i = \overline{19,230}$. Pentru $i = 18$ avem că $p_{37} = 157 < 3 \cdot p_{16} = 3 \cdot 53 = 159$. Deci inegalitatea i) este valabilă pentru orice $n \in \mathbf{N}$, $n \geq 18$.

TEOREMA LUI WARING

Introducere

În anul 1640 Fermat propunea următorul enunț: *orice număr natural se poate scrie ca suma a patru pătrate de numere naturale.* Folosind o identitate a lui Euler, Lagrange reușește să demonstreze acest enunț în anul 1770 (enunțul de mai sus este astăzi cunoscut sub numele de teorema lui Lagrange. Demonstrația acestei teoreme este dată în paragraful I al anexei).

Edward Waring în *Meditationes Algebraice* (ediția din 1770 și ediția din 1782), prin examinarea unor cazuri particulare, afirmă că orice număr natural se scrie ca suma a nouă cuburi de numere naturale, 19 puteri a 4-a de numere naturale, ș.a.m.d. Prin teorema lui Waring astăzi se înțelege faptul că *pentru orice k, număr natural nenul, există un număr natural nenul g(k), ce nu depinde decât de k, astfel încât,* $(\forall)\, n \in \mathbf{N}$, există $n_i \in \mathbf{N}\left(i=\overline{1,g(k)}\right)$ *așa încât*

$$n=\sum_{i=1}^{g(k)} n_i^k.$$

După demonstrarea unor cazuri particulare de către diverși matematicieni (pentru $k=2, 3, 4, 5, 6, 7, 8$ și 10) în anul 1909 Hilbert reușește să demonstreze teorema lui Waring [D. Hilbert *Beweis fur die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsche Problem)*, Göttinger Nachrichten, 1909 pagina 17–36 și *Math. Annalen*, volum LXVII(67), 1909, pagina 281–300]. În acest capitol se dă demonstrația teoremei lui Waring urmând articolul lui W. J. Ellison intitulat *Waring's Problem* și publicat în *American Mathematical Monthly*, volumul 78 din 1971, paginile 10–36. Demonstrația din acest articol urmează ideile lui Hilbert, precum și îmbunătățirile aduse demonstrației lui Hibert, îmbunătățiri datorate lui Hausdorff, Stridsberg și Ellison. Raționamentul principal al demonstrației se bazează pe o inducție după k precum și pe o consecință a unei leme a lui Hilbert care afirmă că *dacă teorema lui Waring este adevărată pentru un număr natural nenul k atunci ea este adevărată și pentru* $2k$. În anexă există șase paragrafe structurate după cum urmează; în

paragraful I se dau două demonstrații diferite ale teoremei lui Lagrange (una din ele folosește teorema lui Minkovski asupra corpului convex), în paragraful II se demonstrează că mulțimea polinoamelor omogene de grad n în k variabile cu coeficienți reali formează un spațiu vectorial peste $\mathbf{R}$ de dimensiune C_{n+k-1}^{k-1} ($k, n \in \mathbf{N}$; $k \geq 1$), (paragrafele III, IV, V și VI se ocupă cu demonstrarea unor fapte „clasice" despre mulțimile convexe în $\mathbf{R}^n$, scopul lor fiind demonstrarea unei afirmații „cheie" ce apare în soluția lemei lui Hilbert (anume $g \in$ co S).

Un absolvent al anului I al Facultății de Matematică poate parcurge fără dificultate acest text.

Demonstrația teoremei lui Waring

Pentru a da demonstrația teoremei lui Waring (pusă sub forma teoremei 1) vom arăta echivalența acestei cu teorema 2 și apoi vom trece la demonstrația acestei a doua teoreme.

Teorema 1 (W a r i n g) *Pentru orice k număr natural nenul există $g(k)$, un număr natural nenul care nu depinde decât de k, astfel încât orice număr natural n se poate scrie sub forma*

$$n = \sum_{i=1}^{g(k)} n_i^k, \text{ unde } n_i \in \mathbf{N}, \ (\forall)\ i = \overline{1, g(k)}.$$

Teorema 2. *Dacă k este ca în teorema* 1 *există atunci A și M numere naturale nenule* și $\lambda_1, \lambda_2, ..., \lambda_M$, *numere raționale pozitive, care depind doar de k astfel încât orice număr natural N astfel încât $N \geq A$ se poate scrie sub forma* $N = \sum_{i=1}^{M} \lambda_i n_i^k$, *unde* $n_i \in \mathbf{N}$, $(\forall)\ i = \overline{1, M}$.

Luând $A = 1$, $M = g(k)$ și $\lambda_1 = \lambda_2 = ... = \lambda_M = 1$ este evident că teorema 1 implică teorema 2. Pentru a demonstra implicația cealaltă considerăm $\sigma \in \mathbf{N}$, cel mai mic multiplu comun pentru numitorii numerelor λ_i. În aceste condiții numerele $\sigma_i = \lambda_i \cdot \sigma$ sunt numere naturale. Fie $x \in \mathbf{N}$, $x \geq \sigma \cdot A$. Există atunci numerele naturale N și θ astfel încât $x = N \cdot \sigma + \theta$, unde $N \geq A$ și $0 \leq \theta < \sigma$ (conform teoremei împărțirii cu rest). Uzând de teorema 2 deducem următoarea scriere pentru N : $N = \sum_{i=1}^{M} \lambda_i n_i^k$ (n_i fiind numere naturale, $(\forall)\ i = \overline{1, M}$). Din considerațiile anterioare rezultă că x se poate scrie sub forma

$$x = \mathrm{N}\sigma + \theta = = \sum_{i=1}^{M} \sigma_i \cdot n_i^k + \theta;$$

deci orice număr natural x, $x \geq \sigma \cdot$ A se poate scrie ca suma a cel mult $\left\{ \sigma - 1 + \sum_{i=1}^{M} \sigma_i \right\}$ k-puteri. Aceasta înseamnă că orice număr natural se poate

ca suma a cel mult $\left\{A\sigma+\sigma-1+\sum_{i=1}^{M}\sigma_i\right\}$ k-puteri. Am demonstrat deci și faptul că teorema 2 implică teorema 1, deci cele două enunțuri sunt echivalente.

Cheia demonstrației teoremei 2 este următoarea lemă ce aparține lui Hilbert.

Lema 1. *Pentru orice k, număr natural există* λ_0, λ_1, ..., λ_N, *numere raționale pozitive* (*unde* $N=\dfrac{(2k+1)(2k+2)(2k+3)(2k+4)}{24}$) *și numerele întregi* $\alpha_{0,1}$, $\alpha_{0,2}$, ..., $\alpha_{0,5}$, $\alpha_{1,1}$, $\alpha_{1,2}$, ..., $\alpha_{1,5}$, ..., $\alpha_{N,1}$, ..., $\alpha_{N,5}$ *astfel încât să aibă loc egalitatea*

$$\left(x_1^2+x_2^2+...+x_5^2\right)^k=\sum_{i=0}^{N}\lambda_i\left(\alpha_{i1}x_1+...+\alpha_{i5}x_5\right)^{2k},$$

oricare ar fi x_1, x_2, ..., x_5 *numere reale.*

Demonstrație: Conform propoziției din paragraful II al anexei, mulțimea formelor (polinoamelor) omogene de grad $2k$ în 5 variabile cu coeficienți reali formează un spațiu vectorial V peste $\mathbf{R}$ de dimensiune $C_{2k+4}^4=N=\dfrac{(2k+1)(2k+2)(2k+3)(2k+4)}{24}$.

Considerăm S mulțimea vectorilor din V dați de fomele $L = L(\alpha) = (\alpha_1x_1 + ... + \alpha_5x_5)^{2k}$, unde α_1, α_2 ,..., α_5 sunt orice numere raționale.

Notăm prin co S intersecția tuturor submulțimilor convexe ale lui V care conțin pe S (co S se numește *acoperirea convexă a lui S*).

Conform teoremei lui Carathéodory, demonstrată în paragraful III al anexei, orice element a aparținând lui co S poate fi scris sub forma $a=\sum_{i=0}^{N}\lambda_i s_i$ unde $s_i \in S$, $(\forall)\ i=\overline{0,N}$, $\lambda_i \in \mathbf{R}_+$, $(\forall)\ i=\overline{0,N}$ și în plus $\sum_{i=0}^{N}\lambda_i=1$. În același loc citat mai sus s-a demonstrat faptul că dacă a e vector rațional (adică toate coordonatele sale sunt numere raționale) și toți vectorii din S sunt raționali (ceea ce în cazul nostru este evident adevărat) atunci numerele λ_i de mai sus pot fi alese chiar raționale. Conform considerațiilor precedente pentru a demonstra lema e suficient a arăta că un multiplu rațional al formei $\left(X_1^2+X_2^2+...+X_5^2\right)^k$ aparține lui co S.

Fie $g \in V$ vectorul dat de formula

$$g=\frac{\int_{R_0}\left(\alpha_1X_1+...+\alpha_5X_5\right)^{2k}d\alpha_1...d\alpha_5}{\int_{R_0}d\alpha_1...d\alpha_5},$$

unde

$$R_0 = \left\{ (\alpha_1, \alpha_2 \ldots \alpha_5) \in \mathbf{R}^5 \middle| \alpha_1^2 + \alpha_2^2 + \ldots + \alpha_5^2 \leq 1 \right\}$$

și $d\alpha_1\, d\alpha_2 \ldots d\alpha_5$ este măsura Lebesgue din $\mathbf{R}^5$.

Să menționăm aici faptul că în anexă am folosit în locul notației tradiționale pentru măsura Lebesgue din $\mathbf{R}^m$ notația „ν" pentru a ușura scrierea. Să mai spunem că semnificația formulei pentru explicitarea lui g este următoarea: coordonata lui g corespunzând monomului $X_1^{\beta_1} \ldots X_5^{\beta_5}$, unde $\beta_1, \ldots,$ β_5 sunt numere naturale astfel încât $\sum_{i=1}^{5} \beta_i = 2k$, este dată de formula

$$\frac{\int\limits_{R_0} n \cdot \alpha_1^{\beta_1} \ldots \alpha_5^{\beta_5}\, d\alpha_1 \ldots d\alpha_5}{\int\limits_{R_0} d\alpha_1 \ldots d\alpha_5},$$

unde n este un număr natural care depinde doar de $\beta_1, \ldots, \beta_5$ (mai exact $n \cdot \alpha_1^{\beta_1} \ldots \alpha_5^{\beta_5}$ este coeficientul lui $X_1^{\beta_1} \ldots X_5^{\beta_5}$ în descompunerea polinomului $(\alpha_1 X_1 + \ldots + \alpha_5 X_5)^{2k}$ în sumă de monoame).

Afirmăm că $g \in$ co S. Această afirmație esențială pentru demonstrația lemei, va fi demonstrată la sfârșitul paragrafului VI din anexă.

g este un polinom omogen de grad $2k$ în variabilele $x_1, \ldots, x_5$. Fie acum x_1, $x_2, \ldots, x_5$ numere reale fixate astfel încât $x_1^2 + x_2^2 + \ldots + x_5^2 > 0$.

Pentru a calcula valoarea lui g în punctul $(x_1, x_2, \ldots, x_5)$ vom face următoarea schimbare de variabilă:

$$(*) \begin{cases} t_1 = \beta_{11}\alpha_1 + \ldots + \beta_{15}\alpha_5 \\ \vdots \\ t_5 = \beta_{51}\alpha_1 + \ldots + \beta_{55}\alpha_5, \end{cases}$$

unde $\beta_{1i} = \dfrac{x_i}{\sqrt{x_1^2 + x_2^2 + \ldots + x_5^2}}$, $(\forall)\ i = \overline{1,5}$, iar ceilalți $\beta_{ij} \left(i \geq 2,\ i = \overline{2,5}\ \ j = \overline{1,5} \right)$ sunt aleși astfel încât matricea $\left(\beta_{ij} \right)_{i,j=\overline{1,5}}$ să fie o matrice ortogonală (dacă notăm $e_1 = (\beta_{11}, \beta_{12}, \ldots, \beta_{15})$ acesta este un vector unitar din $\mathbf{R}^5$; știm atunci că există e_2, e_3, e_4, e_5, astfel încât $e_1, e_2, \ldots, e_5$ să formeze o bază ortonormată a lui $\mathbf{R}^5$. Dacă notăm coordonatele lui e_j cu $\beta_{j,1}, \ldots, \beta_{j,5}$ atunci matricea $\left(\beta_{ij} \right)_{i,j=\overline{1,5}}$ este o matrice ortogonală). Ținând cont de formula lui g, de schimbarea de variabilă considerată mai sus precum și de faptul că o transformare ortogonală

transformă pe R_0 în R_0 deduc că $g = c_1\left(x_1^2+...+x_5^2\right)^k \int\limits_{R_0} t_1^{2k}\mathrm{d}t_1...\mathrm{d}t_5$ (am ținut cont de formula schimbării de variabilă și de faptul că modulul determinantului unei matrici ortogonale este 1). g se poate scrie sub forma $g = c\left(x_1^2+x_2^2+...+x_5^2\right)^k$ unde

$$c_1^{-1} = \int\limits_{R_0} \mathrm{d}\alpha_1...\mathrm{d}\alpha_5, \quad c = c_1 \int\limits_{R_0} t_1^{2k}\mathrm{d}\,t_1...\mathrm{d}\,t_5.$$

Constanta c este strict pozitivă (funcția t_1^{2k} este continuă, mai mare sau egală cu 0 pe R_0 și măsura Lebesgue a mulțimii punctelor din R_0 în care această funcție se anulează este 0). Cum egalitatea $g = c\left(x_1^2 + x_2^2+...+x_5^2\right)^k$ are loc oricare ar fi $x_1, x_2, ..., x_5$ numere reale care satisfac condiția $x_1^2 + x_2^2+...+x_5^2 > 0$ (c nu depinde de $x_1, ..., x_5$) și g este și el un polinom în $x_1, ..., x_5$ atunci egalitatea de mai sus are loc și pentru punctul $(x_1, ..., x_5) = (0,0, ..., 0)$.

Cum am menționat mai sus $g \in$ co S. Deoarece $0 \in$ co S și co S este evident o mulțime convexă atunci $\lambda \cdot g \in$ co S, $(\forall)\ \lambda \in [0, 1]$.

În particular alegem $\lambda = \dfrac{r}{c}$, unde $r \in Q_+^*$ și $0 < r < c$. Din cele de mai sus rezultă că $r\cdot\left(X_1^2+...+X_5^2\right)^k$ este un vector rațional ce aparține lui co S. Conform considerațiilor de la începutul demonstrației lemei (legate de teorema lui Carathéodory) lema este în acest moment demonstrată.

Să mai menționăm aici că dacă T este mulțimea vectorilor din V dați de formele $L = (\alpha_1X_1 +...+ \alpha_5X_5)^{2k}$, unde $\alpha_i \in \mathbf{R}$, $(\forall)\ i = \overline{1,5}$, satisfac condiția $\alpha_1^2 + \alpha_2^2+...+\alpha_5^2 \le 1$ atunci într-un limbaj intuitiv (dar imprecis) g este „centrul de greutate" asociat corpului T (în orice punct T are masa 1).

Lema lui Hilbert este importantă mai ales pentru următoarele trei corolare:

Corolar 1. *Pentru orice k și y, numere naturale nenule, există întregii α_0, α_1, ..., α_N, β_0, ..., β_N și numerele raționale pozitive λ_0, λ_1, ..., λ_N (unde N, λ_i, α_i depind doar de k) astfel încât să aibă loc egalitatea*:

$$\left(x_1^2 + y\right)^k = \sum_{i=0}^{N}\lambda_i\left(\alpha_i x_1 + \beta_i\right)^{2k} \ (\forall)\ x_1 \in \mathbf{R}$$

(*să notăm faptul că β_0, β_1, ..., β_N depind de y*).

Demonstrație: folosind lema 1 și faptul că orice număr natural se scrie ca suma a patru pătrate de numere naturale (acest fapt este demonstrat în paragraful I al anexei) enunțul corolarului este evident.

Corolar 2: *Dacă teorema 2 e adevărată pentru $k = m$ atunci ea este adevărată și pentru $k = 2m$.*

Demonstrație. Dacă punem în corolarul 1 $x_1 = 0$ și $k = m$ deducem existența unor numere raționale pozitive $\lambda_0, \lambda_1, ..., \lambda_N$ care nu depind decât de m (N este un număr natural care nu depinde și el decât de m) astfel încât pentru orice $y \in \mathbf{N}$ există $\beta_0, \beta_1, ..., \beta_N$ numere naturale așa încât $y^m = \sum_{i=0}^{N} \lambda_i \cdot \beta_i^{2m}$ (în enunțul corolarului 1 numerele $\beta_0, \beta_1, ..., \beta_N$ erau întregi însă, deoarece ele apar la puteri pare, pot fi considerate chiar numere naturale). Cum teorema 2 este adevărată pentru $k = m$ există atunci A și M, numere naturale nenule ce nu depind decât de m, astfel încât orice număr natural $P \geq A$ se poate scrie sub forma

$$P = \sum_{i=0}^{M} \mu_i \cdot y_i^m$$

($\mu_0, \mu_1, ..., \mu_M$ sunt numere raționale pozitive care nu depind decât de m; $y_i \in \mathbf{N}$, $(\forall)\ i = \overline{0, M}$). Aplicând considerațiile de mai sus pentru orice $j = \overline{0, M}$ există numerele naturale $\beta_{j,i}$ ($i = \overline{0, N}$) astfel încât $y_j^m = \sum_{i=0}^{N} \lambda_i \beta_{j,i}^{2m}$. Deci

$$P = \sum_{j=0}^{M} \mu_j y_j^m = \sum_{j=0}^{M} \sum_{i=0}^{N} \mu_j \cdot \lambda_i \cdot \beta_{j,i}^{2m} = \sum_{i=0}^{M \cdot N} \nu_i \cdot m_i^{2m},$$

unde $\nu_i (i = \overline{0, M \cdot N})$ sunt numere raționale pozitive care nu depind decât de m (sau de $2m$) Deci teorema 2 este adevărată și pentru $k = 2m$. În continuare facem următoarea:

Convenție de notație: Dacă n este un număr natural care se scrie sub forma $n = \sum_{i=1}^{M} \lambda_i n_i^k$ unde $M \in \mathbf{N}$ și $\lambda_1, \lambda_2, ..., \lambda_M \in Q_+$ sunt numere ce nu depind decât de k ($n_i \in \mathbf{N}$ $(\forall)\ i = \overline{1, M}$) vom scrie atunci $n = \Sigma(k)$.

Această convenție a fost făcută pentru a ușura scrierea în cele ce urmează.

Exemple: a) *Dacă* $a = \Sigma(k)$ și $b = \Sigma(k)$ *atunci* $a + b = \Sigma(k)$

b) *Dacă* $a = \Sigma(2k)$ *atunci* $a = \Sigma(k)$

c) *Dacă* $a = \Sigma(k)$ *atunci conform corolarului 2 avem și relația* $a = \Sigma(2k)$.

Exemplele de mai sus sunt aproape imediate însă sunt importante în tot ceea ce urmează.

Corolar 3: Fie r, m, x și T numere naturale astfel încât $r < m$ și $x^2 < T$. Are loc atunci următoarea egalitate:

$$\sum_{v=0}^{r-1} B_{vr} x^{2v} T^{m-v} + x^{2r} T^{m-r} = \Sigma(m),$$

unde coeficienții B_{vr} sunt numere naturale și sunt funcții explicite doar de m și r (conform convenției de mai sus numerele $\lambda_1, ..., \lambda_M$ nu depind de x și T ci doar de m).

Demonstrație: Să observăm întâi că dacă în egalitatea de la corolarul 1 punem $k = m + r$ și derivăm în raport cu x_1 de $2r$ ori obținem o egalitate de forma:

$$(*) \quad \sum_{v=0}^{r} \alpha_{v,r} x_1^{2v} \left(x_1^2 + y\right)^{m-v} = \Sigma(m),$$

unde $\alpha_{v,r}$ sunt numere naturale nenule care depind doar de r și m (egalitatea

$$\frac{\partial}{\partial x_1^{2r}} \left(x_1^2 + y\right)^{m+r} = \sum_{v=0}^{r} \alpha_{v,r} x_1^{2v} \left(x_1^2 + y\right)^{m-v}$$

se obține ușor prin recurență de la $r = 0$ până la $r = m - 1$ uzând în plus și de formula de derivare a produsului aparținând lui Leibniz anume

$$(f \cdot g)^{(n)} = \sum_{k=0}^{n} C_n^k f^{(k)} \cdot g^{(n-k)},$$

unde f și g sunt funcții definite pe $\mathbf{R}$ cu valori în $\mathbf{R}$). Aparent în partea dreaptă a identității (*) scrierea $\Sigma(m)$ nu ar fi justificată fiindcă există o dependență a coeficienților $\lambda_1, \ldots, \lambda_M$ de r. Însă cum r depinde de m (anume $r < m$, $r \in N$) lucrurile sunt clare și scrierea este justificată.

Pentru a demonstra enunțul corolarului vom face o recurență de la $r = 0$ până la $r = m - 1$. Pentru $r = 0$ enunțul este clar. Dacă în identitatea (*) punem $x_1 = x$ și $y = T - x^2$ ($y \in \mathbf{N}$ deoarece $T > x^2$) obținem identitatea:

$$(**) \quad \sum_{v=0}^{r} \alpha_{v,r} x^{2v} T^{m-v} = \Sigma(m),$$

Punem în egalitatea de mai sus $r = 1$ și obținem egalitatea $a_{0,1} T^m + \alpha_{1,1} x^2 T^{m-1} = \Sigma(m)$, unde $\alpha_{0,1}$ și $\alpha_{1,1}$ sunt numere naturale care depind de m. Fie β un număr natural astfel încât $\alpha_{0,1} + \beta$ să fie multiplu de $\alpha_{1,1}$. Există deci $B_{0,1}$ un număr natural nenul astfel încât $\alpha_{0,1} + \beta = \alpha_{1,1} \cdot B_{0,1}$. Considerațiile precedente ne arată că $B_{0,1}$ nu depinde decât de m (la fel și numărul natural β).

În consecință

$$\alpha_{1,1} \cdot B_{0,1} \cdot T^m + \alpha_{1,1} x^2 T^{m-1} = (\alpha_{0,1} + \beta) T^m + \alpha_{1,1} x^2 T^{m-1} =$$
$$= \beta T^m + (\alpha_{0,1} T^m + x^2 T^{m-1} \cdot \alpha_{1,1}) = \beta T^m + \Sigma(m) = \Sigma(m)$$

(deoarece β nu depinde decât de m). Împărțind egalitatea de mai sus cu $\alpha_{1,1}$ obținem că $B_{0,1} T^m + x^2 T^{m-1} = \Sigma(m)$, ceea ce demonstrează corolarul pentru $r = 1$.

Presupunem acum că enunțul corolarului este adevărat pentru orice $i = \overline{0,r}$, că $r + 1 < m$ și vom arăta că enunțul este adevărat pentru $r + 1$. Conform (**)

$$(1) \quad \alpha_{0,r+1} T^m + \alpha_{1,r+1} x^2 T^{m-1} + \ldots + \alpha_{r,r+1} x^{2r} T^{m-r} + \alpha_{r+1,r+1} x^{2r+2} T^{m-r-1} = \Sigma(m),$$

unde $\alpha_{i,r+1}$ sunt numere naturale care nu depind decât de $r+1$ și $m\left(i = \overline{0,r+1}\right)$.

Conform ipotezei de recurență avem egalitatea:

$$(2) \quad B_{0,r} T^m + B_{1,r} x^2 T^{m-1} + \ldots + B_{r-1,r} x^{2r-2} T^{m-r+1} + x^{2r} T^{m-r} \cdot = \Sigma(m),$$

unde $B_{i,r}$ sunt numere naturale ce nu depind decât de r și m. Fie α un număr

natural astfel încât $\alpha + \alpha_{r,r+1}$ să fie multiplu de $\alpha_{r+1,r+1}$; există deci $B_{r,r+1}$ număr natural care nu depinde decât de m și $r+1$ (la fel ca și α) așa încât

$$\alpha + \alpha_{r,r+1} = \alpha_{r+1,r+1} \cdot B_{r,r+1}.$$

Înmulțim egalitatea (2) cu α și adunăm apoi relația obținută cu egalitatea (1). Vom obține următoarea egalitate:

$$(3)\quad \begin{cases} \beta_{0,r+1}T^m + \ldots + \beta_{r-1,r+1}x^{2r-2}T^{m-r+1} + \alpha_{r+1,r+1} \cdot B_{r,r+1}x^{2r}T^{m-r} + \\ + \alpha_{r+1,r+1}x^{2r+2}T^{m-(r+1)} = \Sigma(m), \end{cases}$$

unde $\beta_{i,r+1}$ sunt numere naturale care nu depind decât de $r+1$ și m (pentru $(\forall)\, i = \overline{0, r-1}$). Continuând procedeul de mai sus, folosind și ipoteza de recurență pentru $r-1$ apoi pentru $r-2$ etc., vom obține o relație de forma

$$(4)\quad \sum_{v=0}^{r} \alpha_{r+1,r+1} \cdot B_{v,r+1}x^{2v}T^{m-v} + \alpha_{r+1,r+1}x^{2r+2}T^{m-(r+1)} = \Sigma(m).$$

Împărțind apoi la $\alpha_{r+1,r+1}$ vom obține enunțul ($B_{v,r+1}$ sunt numere naturale ce nu depind decât de $r+1$ și m).

Lema 2: *Fie A și k numere naturale nenule. Atunci pentru T număr real pozitiv suficient de mare, orice număr natural n cuprins în intervalul $[AT^k,\ A(T+1)^k]$ se poate scrie sub forma:*

$$n = AT^k + b_1 T^{k-1} + \ldots + b_{k-1} T + b_k,$$ *unde $b_1, b_2, \ldots b_k$ sunt numere naturale satisfăcând inegalitățile $0 \le b_i < T \quad (\forall)\, i = \overline{1,k}$.*

Demonstrație. E suficient de arătat că pentru T suficient de mare are loc inegalitatea $A \cdot T^k + (T-1)(T^{k-1} + \ldots T + 1) > A(T+1)k$. Aceasta este însă evident deoarece pentru un anume T_0 număr real, oricare ar fi $T \ge T_0$ are loc inegalitatea $T^k - 1 > A \cdot C_k^1 T^{k-1} + AC_k^2 T^{k-2} + \ldots + A$ (dacă f este un polinom neconstant cu coeficientul dominant strict pozitiv atunci $\lim_{x \to +\infty} f(x) = +\infty$).

Demonstrația teoremei 2: Se face o inducție după k. Pentru $k = 1$ enunțul este evident iar pentru $k = 2$ enunțul este adevărat conform teoremei lui Lagrange demonstrată în paragraful (I) al anexei).

Pentru un număr natural $m \ge 3$ presupunem că teorema 2 este adevărată pentru orice $k \in \mathbf{N}^*$, $k \le m-1$ și vom arăta că teorema 2 este adevărată și pentru $k = m$. Ideea fundamentală este de a arăta că putem găsi numerele naturale A și N_0 depinzând doar de m astfel încât dacă $T \ge N_0$ este un întreg oarecare, orice $n \in N$ inclus în intervalul $[AT^m; A(T+1)^m]$ poate fi scris sub forma $n = \Sigma(m)$.

Întrucât orice număr natural $l \ge A \cdot N_0^m$ este inclus într-un interval de forma $[AT^m; A(T+1)^m]$ teorema 2 ar fi demonstrată.

Vom arăta întâi că dacă T e un număr întreg suficient de mare (și pozitiv) atunci orice număr natural n de forma $n = A \cdot T^m + b_{m-1}T^{m-1} + \ldots + \quad + b_1 \cdot T$ (unde b_i sunt numere naturale satisfăcând inegalitățile $0 \le b_i \le T-1$ $(\forall)$

$i = \overline{1,m-1}$) se poate scrie sub forma $n = \Sigma(m)$. Fie T și $N_{m-\nu}$ ($\nu = \overline{1,m-1}$) numere naturale care vor fi alese mai târziu; ele vor satisface în plus și condiția $N_{m-\nu} < T$ $(\forall)\, \nu = \overline{1,m-1}$. Conform ipotezei de inducție, teorema 2 este adevărată pentru orice $k \le m-1$, $k \in \mathbf{N}^*$; ținând cont atunci de corolarul 2 deducem că teorema 2 este adevărată pentru toate numerele naturale pare mai mici sau egale cu $2m-2$. Există deci $r \in \mathbf{N}$ (care depinde doar de m) și numerele naturale $x_{i,j}$ ($i = \overline{1,r}$; $j = \overline{1,m-1}$) astfel încât să aibă loc egalitatea:

$$(5)\quad \sum_{i=1}^{r} x_{i,j}^{2j} = N_{m-j},\ (\forall)\ j = \overline{1,m-1}.$$

Punem în egalitatea enunțată în corolarul 3, $x = x_{ij}$ și adunăm egalitățile astfel obținute pentru $i = \overline{1,r}$ (se aplică corolarul 3 deoarece $x_{i,j}^2 \le x_{i,j}^{2j} \le \sum_{i=1}^{r} x_{i,j}^{2j} = N_{m-j} < T$). Ținând cont și de formula (5) obținem următoarea egalitate:

$$(6)\quad \sum_{\nu=0}^{j-1} B_{\nu,j} T^{m-\nu} \cdot \sum_{i=1}^{r} x_{ij}^{2\nu} + N_{m-j} T^{m-j} = \Sigma(m).$$

Trebuie menționat că aici (ca și în cursul demonstrației corolarului 3) am folosit repetat faptul amintit în exemplul a), apropo de convenția de notație (anume dacă $a = \Sigma(m)$ și $b = \Sigma(m)$ atunci $a + b = \Sigma(m)$).

Egalitatea (6) are loc pentru orice $j = \overline{1,m-1}$. Dacă notăm $c_{\nu,j} = B_{\nu,j} \sum_{i=1}^{r} x_{ij}^{2\nu}$ și sumăm în (6) după j de la 1 la $m-1$ obținem:

$$(7)\quad \sum_{j=1}^{m-1} \left(\sum_{\nu=0}^{j-1} c_{\nu,j} \cdot T^{m-\nu} + N_{m-j} T^{m-j} \right) = \Sigma(m).$$

Numerele $B_{\nu,j}$ sunt naturale și depind doar de m și j. Scriem formula (7) din nou punând în evidență polinomul în T obținut:

$$(8)\quad a^m T^m + a_{m-1} T^{m-1} + \ldots + a_1 T = \Sigma(m).$$

Ținând cont de (7), a_i ($i = \overline{1,m}$) sunt numere naturale date de formulele:

$$(9)\quad \begin{cases} a_1 = N_1 \\ a_i = N_i + \sum_{j=1}^{i-1} c_{m-i,m-j} \quad (\forall)\ i = \overline{2,m-1} \\ a_m = r\left(B_{0,1} + B_{0,2} + \ldots + B_{0,m-1}\right) = A_1 - 1. \end{cases}$$

Este clar din cele de mai sus că A_1 nu depinde decât de m. Am arătat mai sus că $x_{i,j}^{2j} < T$, deci $x_{i,j} < T^{\frac{1}{2j}}$, $(\forall)\ i = \overline{1,r}$ și $j = \overline{1,m-1}$.

Pentru $v = \overline{1,j-1}$ avem că $x_{i,j}^{2v} \le T^{\frac{j-1}{j}} = T^{1-\frac{1}{j}} \le T^{1-\frac{1}{m-1}} = T^{\frac{m-2}{m-1}}$ (deoarece $j \le m-1$; $x_{i,j}$ și T sunt numere naturale). Considerațiile anterioare permit evaluarea $c_{v,j} \le B \cdot r \cdot T^{\frac{m-2}{m-1}}$, $(\forall)\ v = \overline{1,j-1}$, unde $B = \max\{B_{v,j} \mid v = \overline{0,j-1},\ j = \overline{1,m-1}\}$.

Deci

$$a_i - N_i \le (m-1) \cdot B \cdot r\, T^{\frac{m-2}{m-1}}$$

pentru $i = \overline{1,m-1}$. În acest moment putem preciza modul în care trebuie ales T. Anume T este un număr natural care trebuie să satisfacă inegalitatea $T > Br(m-1)T^{\frac{m-2}{m-1}}$. Aceasta se întâmplă dacă T e ales astfel încât $T > [Br(m-1)]^{m-1}$, $T \in \mathbf{N}$.

Deci $T > a_i - N_i \ge 0$ $(\forall)$ $i = \overline{1,m-1}$. Putem trece acum la demonstrarea primului pas; pe postul lui A se va afla deocamdată numărul A_1 amintit mai sus (vezi formula 9). Fie deci b_i $(i = \overline{1,m-1})$ numere naturale arbitrare care satisfac inegalitățile $b_i < T$, $(\forall)$ $i = \overline{1,m-1}$.

Vom preciza acum cine sunt numerele naturale $N_1, N_2, \ldots, N_{m-1}$. Întâi de toate $N_1 = b_1$. Deoarece N_1 este bine determinat în acest moment, același lucru se poate spune și despre $c_{m-2,m-1}$ (într-adevăr din egalitatea $N_1 = \sum_{i=1}^{r} x_{i,m-1}^{2(m-1)}$ se determină numerele $x_{i,m-1}$ deci și $c_{m-2,m-1} = B_{m-2,m-1} \sum_{i=1}^{r} x_{i,m-1}^{2(m-2)}$; cuvântul „determinat" folosit mai sus se referă la existența numerelor în cauză și nu neapărat și la unicitatea lor). Putem alege acum N_2 astfel încât $a_2 \equiv b_2 \pmod{T}$. Cum $a_i < 2T$, $(\forall)$ $i = \overline{1,m-1}$ (vezi alegerea lui T de mai sus care asigură inegalitatea $T > a_i - N_i$, $(\forall)$ $i = \overline{1,m-1}$ și faptul că toate numerele N_i sunt strict mai mici decât T prin alegerea lor) atunci $a_2 < 2T$. Dacă $a_2 \ge T$ aleg pe $N_3 \in \mathbf{N}$, $0 \le N_3 < T$ astfel încât $1 + a_3 \equiv b_3 \pmod{T}$. Dacă $a_2 < T$, atunci pe N_3 îl alegem astfel încât $a_3 \equiv b_3 \pmod{T}$ (evident ca și mai sus $N_3 \in \mathbf{N}$; $0 \le N_3 < T$). Să mai observăm că, deoarece N_1 și N_2 sunt determinate, același lucru se poate spune și despre $c_{m-3,m-1}$ și $c_{m-3,m-2}$; această observație împreună cu formula (9) ne arată că într-adevăr alegerea lui N_3 ca mai sus este realmente posibilă. Evident $0 \le a_3 < 2T$.

Dacă $a_3 \ge T$ alegem $N_4 \in \mathbf{N}$, $0 \le N_4 < T$ astfel încât $1 + a_4 \equiv b_4 \pmod{T}$. Dacă însă $a_3 < T$ alegem $N_4 \in \mathbf{N}$, $0 \le N_4 < T$ astfel încât $a_4 \equiv b_4 \pmod{T}$. La fel ca și mai sus aceste alegeri sunt posibile deoarece sunt determinate numerele

naturale $c_{m-4,m-1}$, $c_{m-4,m-2}$ și $c_{m-4,m-3}$ (aceasta deoarece sunt bine determinate numerele N_1, N_2 și N_3). Continuăm în același mod procedeul de construcție pentru a obține numerele N_1, N_2, ..., N_{m-1}. Din modul de construcție al acestor numere deducem că $A_1 \cdot T^m + b_{m-1} T^{m-1} + ... + b_1 T$ este fie $(A_1-1)T^m + a_{m-1}T^{m-1} + ... + a_1 T$, fie $A_1 \cdot T^m + a_{m-1}T^{m-1} + ... + a_1 T$. În orice situație ne-am afla, folosind și formula (8) deducem că $A_1 T^m + b_{m-1}T^{m-1} + ... + b_1 T = \Sigma(m)$. După cum am văzut în considerațiile anterioare A_1 este un număr natural ce nu depinde decât de m; primul pas al demonstrației este astfel făcut.

Putem preciza în acest moment cine sunt numerele A și N_0 anunțate la începutul demonstrației. Dacă $T_1 = 1 + \max \{ A_1 \cdot C_m^i \ / \ i = \overline{0,m} \}$ atunci $N_0 = \max \{T_1, [B \cdot r \cdot (m-1)]^{m-1}\}$, iar A va fi egal cu $2A_1 + 1$. Fie acum C_0, C_1,... C_{m-1} numere naturale satisfăcând inegalitățile $0 \le C_i < T$, $(\forall)\ i = \overline{0,m-1}$ ($T \in \mathbf{N}$; $T \ge N_0$). Vom arăta că

$$A \cdot T^m + C_{m-1}T^{m-1} + ... + C_1 T + C_0 = \Sigma(m);$$

acest fapt combinat cu lema 2 și cu considerațiile de la începutul demonstrației realizează soluția teoremei 2 și implicit a teoremei 1.

Alegem α, $\alpha \in N$ și $0 \le \alpha < T$, astfel încât $A_1 + \alpha \equiv C_0 \pmod T$. Conform primului pas din demonstrație avem următoarea formulă:

(10) $A_1 (T+1)^m + \alpha (T+1) = \Sigma(m)$.

Alegem b_1, $b_1 \in \mathbf{N}$ și $0 \le b_1 < T$, astfel încât $\varepsilon_1 + A_1 C_m^1 + \alpha + b_1 \equiv C_1 \pmod T$ unde $\varepsilon_1 = 0$, dacă $A_1 + \alpha < T$ și $\varepsilon_1 = 1$, dacă $A_1 + \alpha \ge T$ (în orice caz $A_1 + \alpha < 2T$ conform alegerii lui α și T).

b_2 este ales astfel încât $b_2 \in \mathbf{N}$, $0 \le b_2 < T$ și $\varepsilon_2 + A_1 C_m^2 + b_2 \equiv C_2 \pmod T$, unde $\varepsilon_2 = 0$, dacă $\varepsilon_1 + A_1 C_m^1 + \alpha + b_1 < T$, $\varepsilon_2 = 1$ dacă $T \le \varepsilon_1 + A_1 C_m^1 + \alpha + b_1 < 2T$ și $\varepsilon_2 = 2$, dacă $2T \le \varepsilon_1 + A_1 C_m^1 + \alpha + b_1 < 3T$ (altă alternativă nu există fiindcă alegerea lui T și α ne asigură inegalitatea $\varepsilon_1 + A_1 \cdot C_m^1 + \alpha + b_1 < 3T$).

b_3 este ales astfel încât $b_3 \in \mathbf{N}$, $0 \le b_3 < T$ și $\varepsilon_3 + A_1 C_m^3 + b_3 \equiv C_3 \pmod T$, unde $\varepsilon_3 = 0$, dacă $\varepsilon_2 + A_1 C_m^2 + b_2 < T$ și $\varepsilon_3 = 1$, dacă $T \le \varepsilon_2 + A_1 C_m^2 + b_2 < 2T$ (altă posibilitate nu există). În același mod construim b_4, b_5, ..., b_{m-1}. Conform primului pas al demonstrației are loc formula

(11) $A_1 T^m + b_{m-1} T^{m-1} + ... + b_1 \cdot T = \Sigma(m)$.

Adunând formulele (10) și (11) rezultă, ținând cont de modul în care au fost definite numerele α, b_1, b_2, ..., b_{m-1}, că

$$(2A_1 + 1) T^m + C_{m-1} T^{m-1} + ... + C_1 T + + C_0 = \Sigma(m),$$

ceea ce termină demonstrația teoremei.

Să mai menționăm în final că în afara inexactității menționate la sfârșitul paragrafului (VI) al anexei (singura mai serioasă de altfel) mai există două „scăpări" în textul lui Ellison. Anume în demonstrația corolarului 3 se lasă impresia că identitatea (**) este suficientă pentru demonstrația enunțului. Însă un calcul foarte ușor arată că afirmația „$\alpha_{r,r} \mid \alpha_{v,r}$, $(\forall)\ v = \overline{0,r-1}$" este cu siguranță falsă. De aceea recurența făcută în demonstrația corolarului 3 este indispensabilă.

În cursul demonstrației teoremei 2 se afirmă că $x_{i,j} \leq T^{\frac{1}{2m-2}}$, lucru care nu e deloc clar (de fapt $x_{i,j} \leq T^{\frac{1}{2j}}$ și aceasta e suficient pentru trebuințele demonstrației).

ANEXĂ
(Teorema lui Waring)

I. *Orice număr natural poate fi scris ca suma a patru pătrate de numere naturale* (*teorema lui Waring în cazul particular* $k = 2$). *Acest rezultat poartă numele de* **teorema lui Lagrange**.

Soluție: Conform identității lui Euler

$$(X_1^2 + X_2^2 + X_3^2 + X_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (X_1y_1 + X_2y_2 + X_3y_3 + X_4y_4)^2 +$$
$$+ (X_1y_2 - X_2y_1 + X_3y_4 - X_4y_3)^2 + (X_1y_3 - X_3y_1 + X_4y_2 - X_2y_4)^2 +$$
$$+ (X_1y_4 - X_4y_1 + X_2y_3 - X_3y_2)^2,$$

este suficient să demonstrăm enunțul pentru numere prime impare (pentru 2 enunțul este clar; $2 = 1^2 + 1^2$). Deci trebuie arătat că orice număr prim impar se scrie ca suma a patru pătrate de numere naturale.

Arătăm acum că dacă p este un număr prim impar atunci există numerele naturale x și y astfel încât $0 \le x < p$, $0 \le y < p$ și

$1 + x^2 + y^2 \equiv 0 \pmod{p}$.

Pentru aceasta fie

$$A = \left\{ x^2 \,\middle|\, 0 \le x \le \frac{p-1}{2}; x \in \mathbf{N} \right\}$$

și

$$B = \left\{ -1 - y^2 \,\middle|\, 0 \le y \le \frac{p-1}{2},\ y \in \mathbf{N} \right\}.$$

Cele $\frac{p+1}{2}$ elemente din A sunt necongruente modulo p și la fel cele $\frac{p+1}{2}$ elemente ale lui B sunt necongruente modulo p. Cum $|A| + |B| = p + 1$ deducem, ținând cont de afirmația anterioară, existența unor $x_0, y_0 \in \mathbf{N}$, $0 \le x_0 < p$, $0 \le y_0 < p$ astfel încât $1 + x_0^2 + y_0^2 \equiv 0 \pmod{p}$, (de fapt $x_0 \le \frac{p-1}{2}$ și $y_0 \le \frac{p-1}{2}$).

În aceleași condiții ca mai sus (adică p număr prim impar) fie m cel mai mic număr natural nenul cu proprietatea că $m \cdot p$ se scrie ca suma a patru pătrate de numere naturale (există cel puțin un astfel de m căci am văzut mai sus că există x_0, y_0 numere naturale astfel încât $0^2 + 1^2 + x_0^2 + y_0^2 = m_0 \cdot p$ unde $m_0 \in \mathbf{N}^*$). Pentru a demonstra teorema ar fi suficient să arătăm că $m = 1$. Întâi de toate putem afirma că acest m este strict mai mic decât p deoarece $m \cdot p \leq m_0 p = 1 + x_0^2 + y_0^2$, unde x_0 și y_0 sunt numere naturale astfel încât $0 \leq x_0 \leq \frac{p-1}{2}$ și $0 \leq y_0 \leq \frac{p-1}{2}$.

Deci, $m \cdot p \leq 1 + x_0^2 + y_0^2 \leq 1 + \frac{(p-1)^2}{4} \cdot 2 = \frac{p^2 - 2p + 3}{2} < \frac{p^2}{2} < p^2$ de unde rezultă că $m < p$.

Din definiția lui m rezultă că există x_1, x_2, x_3, x_4 numere naturale astfel încât $m \cdot p = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Arătăm acum că m nu poate fi par. Într-adevăr dacă m ar fi par atunci $x_1^2 + x_2^2 + x_3^2 + x_4^2$ ar fi un număr par, deci numerele x_1, x_2, x_3, și x_4 sunt fie toate pare, fie toate impare, fie două pare și două impare. Dacă cumva suntem în ultimul caz putem presupune că x_1 și x_2 sunt pare, iar x_3, x_4 sunt impare.

Avem următoarea identitate:

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 =$$

$$= \frac{1}{2}\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right) = \frac{m}{2} \cdot p.$$

Dacă m este par atunci $\frac{x_1 + x_2}{2}, \frac{x_1 - x_2}{2}, \frac{x_3 + x_4}{2}, \frac{x_3 - x_4}{2}$ sunt numere întregi (vezi presupunerea făcută mai sus în cazul când două dintre numerele x_1, x_2, x_3, x_4 sunt pare și două sunt impare; am presupus în acest caz că x_1 și x_2 sunt pare, iar x_3, x_4 sunt impare). Cum $\frac{m}{2}$ este un număr natural nenul care are proprietatea că există z_1, z_2, z_3, z_4 numere naturale astfel încât $\frac{m}{2} \cdot p = z_1^2 + z_2^2 + z_3^2 + z_4^2$ și cum inegalitatea $\frac{m}{2} < m$ este evidentă obținem o contrazicere a definiției lui m. Deci m este impar; în plus știm că $1 \leq m < p$. Pentru a demonstra că $m = 1$ presupunem

că $m > 1$ și vom ajunge din nou la o contrazicere a definiției lui m ca fiind cel mai mic număr natural nenul pentru care $m \cdot p$ se scrie ca sumă a patru pătrate de numere naturale. Deoarece $m > 1$ și m impar rezultă că $m \geq 3$. Fie r_k resturile împărțirii lui x_k la m pentru fiecare $k = \overline{1,4}$.

Dacă $0 \leq r_k \leq \frac{m-1}{2}$ vom scrie $y_k = r_k$, iar în cazul când $\frac{m+1}{2} \leq r_k \leq m-1$ vom nota $y_k = r_k - m$ (acest lucru se face pentru $k = \overline{1,4}$). În ambele cazuri vom avea

$$x_k = q_k \cdot m + y_k$$

și

$$-\frac{m-1}{2} \leq y_k \leq \frac{m-1}{2},$$

$q_k \in \mathbf{N}$ pentru $k = \overline{1,4}$.

Evaluăm acum suma:

$$(*) \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2m(x_1q_1 + x_2q_2 + x_3q_3 + x_4q_4) +$$

$$+ m^2\left(q_1^2 + q_2^2 + q_3^2 + q_4^2\right) = m \cdot p - 2m(x_1q_1 + x_2q_2 + x_3q_3 + x_4q_4) +$$

$$+ m^2\left(q_1^2 + q_2^2 + q_3^2 + q_4^2\right) = m \cdot n,$$

unde n este un număr natural.

Avem că $n > 0$. Intr-adevăr ipoteza $n = 0$ ar implica faptul că $y_1 = y_2 = y_3 = y_4 = 0$ ceea ce înseamnă că $m \mid x_k$, pentru orice $k = \overline{1,4}$. De aici deducem că $m^2 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = m \cdot p$ de unde rezultă că $m \mid p$ ceea ce nu se poate fiindcă $1 < m < p$ și p este număr prim.

Avem că

$$m \cdot n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4 \cdot \left|\frac{m-1}{2}\right|^2 < m^2$$

de unde rezultă că $n < m$. Avem de asemenea următoarea identitate:

$$(**) \quad m^2 \cdot n \cdot p = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) =$$

$$(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 +$$

$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

obținută folosind identitatea lui Euler. Primul număr al cărui pătrat apare în partea dreaptă a egalității de mai sus este

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 =$$

$$= x_1(x_1 - q_1m) + x_2(x_2 - q_2m) + x_3(x_3 - q_3m) + x_4(x_4 - q_4m) =$$

$$= x_1^2 + x_2^2 + x_3^2 + x_4^2 - m(x_1q_1 + x_2q_2 + x_3q_3 + x_4q_4) =$$

$$= mp - m(x_1q_1 + x_2q_2 + x_3q_3 + x_4q_4) = mz_1,$$

unde z_1 este număr întreg. Următorul număr al cărui pătrat apare în partea dreaptă a egalității (**) este

$$x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 =$$
$$= x_1(x_2 - q_2m) - x_2(x_1 - q_1m) + x_3(x_4 - q_4m) - x_4(x_3 - q_3m) =$$
$$= m(-x_1q_2 + x_2q_1 - x_3q_4 + x_4q_3) = m \cdot z_2,$$

unde $z_2 \in \mathbf{Z}$. Analog deducem că

$$x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 = mz_3$$

și

$$x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 = mz_4,$$

unde z_3 și z_4 sunt numere întregi.

Înlocuind în (**) $x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$ cu mz_1, $x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$ cu mz_2, $x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4$ cu mz_3 și $x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2$ cu mz_4 obținem

$$m^2np = m^2\left(z_1^2 + z_2^2 + z_3^2 + z_4^2\right)$$

și simplificând cu m^2 se obține

$$np = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

Deci $n \cdot p$ se poate scrie ca suma a patru pătrate de numere naturale, n fiind un număr natural satisfăcând inegalitățile $0 < n < m$. Aceasta contrazice definiția lui m. Contradicția a provenit din presupunerea că $m > 1$. Deci $m = 1$, ceea ce înseamnă că orice număr prim se scrie ca suma a patru pătrate de numere naturale. Conform primelor observații ale acestei soluții, aceasta înseamnă că orice număr natural se poate scrie ca suma a patru pătrate de numere naturale. Această demonstrație urmează ideile lui Lagrange din soluția pe care acesta a dat-o în anul 1770. Vom mai da în continuare o demonstrație a acestui rezultat, demonstrație ce se bazează pe teorema lui Minkovski asupra corpului convex. Avem nevoie de următoarele rezultate:

Lema 1: *Fie* $(G, +)$ *un subgrup al grupului* $(\mathbf{Z}^n, +)$, *de rang n peste* $\mathbf{Z}$ (G *este considerat aici ca* $\mathbf{Z}$ *– submodul al* $\mathbf{Z}$ *– modulului liber* $\mathbf{Z}^n$; *este cunoscut că* G *este atunci* $\mathbf{Z}$ *– modul liber de rang mai mic sau egal cu n*). *Fie* $x_1, x_2, ..., x_n$ *și* $e_1, e_2, ..., e_n$ $\mathbf{Z}$ *– baze pentru* G, *respectiv* $\mathbf{Z}^n$. *Se poate considera* $e_i = (0, 0, ..., 1, 0, ..., 0)$ *vectorul ce are* 1 *pe poziția i și* 0 *în rest. Fie* $a_{ij} \in \mathbf{Z}$ *astfel încât* $x_i = \sum_{j=1}^{n} a_{ij}e_j$ $(\forall)$ $i = \overline{1,n}$. *Să se arate că indicele lui* G *în* $\mathbf{Z}^n$ *este egal cu modulul determinantului matricii ce are drept componente numerele* a_{ij}, $i = \overline{1,n}$ *și* $j = \overline{1,n}$.

Soluție: Se știe că există $y_1, y_2, ..., y_n$ respectiv $f_1, f_2, ..., f_n$ $\mathbf{Z}$-baze pentru G și $\mathbf{Z}^n$ precum și numerele naturale $d_1, d_2, ..., d_n$ astfel încât $y_i = d_if_i$ și $d_1|d_2| \ ... \ | \ d_n$ (vezi teorema 2.1. pag. 223 din *Algebra*; autori Ion. D. Ion și

N. Radu; Editura Didactică și Pedagogică, București, 1991). Să arătăm acum că $[\mathbf{Z}^n : G] = d_1\ d_2 \ldots d_n$. Într-adevăr oricare ar fi α din $\mathbf{Z}^n$ el se scrie în mod unic sub forma $\alpha = \sum_{i=1}^{n} \alpha_i f_i \left(\alpha_i \in \mathbf{Z}, (\forall)\, i = \overline{1,n}\right)$. Scriind teorema împărțirii cu rest pentru α_i și d_i deduc că $\alpha_i = q_i d_i + \beta_i$, unde q_i și β_i sunt numere întregi, β_i satisfăcând inegalitatea $0 \le \beta_i < d_i$.

Deci

$$\alpha = \sum_{i=1}^{n} q_i d_i f_i + \sum_{i=1}^{n} \beta_i f_i = \sum_{i=1}^{n} q_i y_i + \sum_{i=1}^{n} \beta_i f_i\ .$$

Evident elementul $\sum_{i=1}^{n} q_i y_i$ aparține lui G. Deci pot defini o funcție $f: \mathbf{Z}^n \to \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \ldots \times \mathbf{Z}_{d_n}$ prin $f(\alpha) = \left(\overline{\beta_1}, \overline{\beta_2}, \ldots, \overline{\beta_n}\right)$ (am folosit același semn pentru clasele de resturi modulo d_1, modulo d_2, ..., modulo d_n). E ușor de arătat că această aplicație este un morfism surjectiv de grupuri și în plus $\operatorname{Ker} f = G$. Aplicând teorema fundamentală de izomorfism pentru grupuri obținem că $\mathbf{Z}^n/G \simeq \mathbf{Z}_{d_1} \times \mathbf{Z}_{d_2} \times \ldots \times \mathbf{Z}_{d_n}$ și în particular că $[\mathbf{Z}^n : G] = d_1.\ d_2.\ d_3\ \ldots.\ d_n$. Fie $B = \left(b_{ij}\right)_{i,j=\overline{1,n}}$ o matrice cu elemente din $\mathbf{Z}$ astfel încât $y_i = \sum_{j=1}^{n} b_{ij} x_j$, $(\forall)\ i = \overline{1,n}$. Deoarece $x_1, x_2, \ldots, x_n$ și $y_1, y_2, \ldots, y_n$ sunt $\mathbf{Z}$-baze pentru G atunci $\det B = \pm 1$.

Elementele $b_{ij} \in \mathbf{Z}$ există deoarece $x_1, x_2, \ldots, x_n$ este o $\mathbf{Z}$-bază a lui G. Folosind aceleași considerente există o matrice $C = \left(c_{ij}\right)_{i,j=\overline{1,n}}$ cu elemente întregi astfel încât $e_i = \sum_{j=1}^{n} c_{ij} f_j$ $(\forall)\ i = \overline{1,n}$; în plus $\det C = \pm 1$.

Avem următoarele egalități

$$y_i = \sum_{j=1}^{n} b_{ij} x_j = \sum_{j=1}^{n} \sum_{k=1}^{n} b_{ij} \cdot a_{jk} \cdot e_k = \sum_{j=1}^{n} \sum_{k=1}^{n} \sum_{e=1}^{n} b_{ij} a_{jk} c_{ke} f_e = d_i f_i\ .$$

Dacă notăm cu D matricea ce are pe poziția (i,i) elementul d_i, $(\forall)\ i = \overline{1,n}$, și în rest 0, din faptul că $f_1, f_2, \ldots, f_n$ este o $\mathbf{Z}$-bază a lui $\mathbf{Z}^n$ deducem că $D = BAC$. Trecând în această egalitate la determinanți obținem că $\det D = \pm \det A = d_1 \cdot d_2 \cdot \ldots \cdot d_n$. Deci $[\mathbf{Z}^n : G] = d_1\ d_2 \cdot \ldots \cdot d_n = \det D = |\det A|$, ceea ce trebuia demonstrat.

Lema 2. *Fie* $n, m, k_1, k_2, \ldots, k_m$ *numere naturale* și a_{ij} $(i = \overline{1,m},\ j = \overline{1,n})$ *numere întregi. Fie* $G = \left\{ u = \left(u_1, u_2, \ldots u_n\right) \in \mathbf{Z}^n \,\middle|\, \sum_{j=1}^{n} a_{ij} u_j \equiv 0 \left(\bmod k_i\right), (\forall)\ i = \overline{1,m} \right\}$.

Atunci G este un $\mathbf{Z}$ – submodul al lui $\mathbf{Z}^n$ de rang n pentru care $v(G)$ (volumul paralelipipedului fundamental asociat lui G) este mai mic sau egal decât $k_1 \cdot k_2 \ldots k_m$.

Demonstrație. Faptul că G este un $\mathbf{Z}$-submodul al lui $\mathbf{Z}^n$ este imediat. Dacă notez cu $k = k_1 \cdot k_2 \cdot \ldots \cdot k_n$ atunci $v_i = (0, 0, \ldots, 0, k, 0, \ldots, 0)$, unde pe poziția i se află k și în rest 0, este un element al lui G pentru orice $i = \overline{1,n}$. Cum v_1, $v_2, \ldots, v_n$ sunt elemente liniar independente peste $\mathbf{Z}$ ale lui G deducem că rangul lui G este n. Folosind notațiile lemei precedente, dacă $x_1, x_2, \ldots, x_n$ și $e_1, e_2, \ldots, e_n$ sunt $\mathbf{Z}$-baze pentru G, respectiv $\mathbf{Z}^n$ ($e_1, e_2, \ldots, e_n$ fiind chiar baza canonică a lui $\mathbf{Z}^n$) și a_{ij} sunt numere întregi astfel încât $x_i = \sum_{j=1}^{n} a_{ij} e_j, (\forall)\ i = \overline{1,n}$, atunci $v(G) = |\det A| = [\mathbf{Z}^n : G]$. Definim acum o funcție $f : \mathbf{Z}^n \to \mathbf{Z}_{k_1} \times \mathbf{Z}_{k_2} \times \ldots \times \mathbf{Z}_{k_m}$ prin condiția:

$$f(u_1, u_2, \ldots, u_n) = \left(\sum_{j=1}^{n} \overline{a_{1j} u_j}\ ;\ \sum_{j=1}^{n} \overline{a_{2j} u_j}\ ;\ldots;\ \sum_{j=1}^{n} \overline{a_{mj} u_j} \right).$$

Despre f se poate afirma că este un morfism de grupuri (evident că $\mathbf{Z}^n$ și G sunt privite ca grupuri cu operația de adunare) și că $\operatorname{Ker} f = G$.

Din teorema fundamentală de izomorfism deducem că $\dfrac{\mathbf{Z}^n}{G} \simeq Im\, f$, de unde rezultă că $[\mathbf{Z}^n : G] = |Im f| \le \left| \mathbf{Z}_{k_1} \times \mathbf{Z}_{k_2} \times \ldots \times \mathbf{Z}_{k_m} \right| = k_1 \cdot k_2 \cdot \ldots \cdot k_m$, ceea ce demonstrează inegalitatea $v(G) \le k_1 \cdot k_2 \cdot \ldots \cdot k_m$.

Putem trece acum la demonstrarea teoremei lui Lagrange și anume că orice număr natural n se poate scrie ca suma a patru pătrate de numere naturale. Se presupune evident că n e liber de pătrate, adică $n = p_1 \cdot p_2 \cdot, \ldots, \cdot p_g$, unde p_1, $p_2, \ldots, p_g$ sunt numere prime distincte. Pentru fiecare p prim care divide pe n consider a_p și b_p numere întregi astfel încât $a_p^2 + b_p^2 + 1 \equiv 0 \pmod p$ (existența numerelor a_p și b_p a fost demonstrată în decursul primei soluții). Fie acum $G = \{(u_1, u_2, u_3, u_4) \in \mathbf{Z}^4 / u_1 \equiv a_p u_3 + b_p u_4 \pmod p$ și $u_2 \equiv b_p u_3 - a_p u_4 \pmod p$, $(\forall)\ p$-prim, $p \mid n\}$. Conform lemei 2, G este un $\mathbf{Z}$ – submodul de rang 4 al lui $\mathbf{Z}^4$ și $v(G) \le p_1^2 \cdot p_2^2 \cdot \ldots \cdot p_g^2 = n^2$.

Deci $2^4\, v(G) \le 2^4 \cdot n^2 < \dfrac{1}{2}\pi^2 (2n)^2 = v\left(B_4^{2\cdot n}\right)$, unde

$$B_4^{2\cdot n} = \{(x, y, z, t) \in \mathbf{R}^4 \mid x^2 + y^2 + z^2 + t^2 < 2n\}.$$

Folosind teorema lui Minkovski asupra corpului convex (demonstrată în capitolul privitor la teorema lui Gauss) deducem că există $u = (u_1, u_2, u_3, u_4) \in G$, un punct diferit de originea lui $\mathbf{R}^4$, astfel încât $u \in B_4^{2n}$. Deci $0 < u_1^2 + u_2^2 + u_3^2 + u_4^2 < 2n$. Pe de altă parte datorită alegerii numerelor a_p

și b_p deducem că $p \mid u_1^2+u_2^2+u_3^2+u_4^2$ pentru oricare divizor prim p al lui n. Deci $n \mid u_1^2+u_2^2+u_3^2+u_4^2$ și cum $0 < u_1^2+u_2^2+u_3^2+u_4^2 < 2n$ rezultă că avem egalitatea $n = u_1^2+u_2^2+u_3^2+u_4^2$, ceea ce demonstrează teorema. Pentru a arăta mai sus că $v(B_4^{2n}) = \frac{1}{2}\pi^2 \cdot (2n)^2$ este suficient să arătăm că $v(B_4) = \frac{1}{2}\pi^2$, unde $B_4 = \{(x, y, z, t) \in \mathbf{R}^4 \mid x^2+y^2+z^2+t^2 < 1\}$. Folosind teorema lui Fubini deducem că

$$v(B_4) = \int\limits_{x^2+y^2<1} \left(\int\limits_{t^2+z^2<1-x^2-y^2} 1 \mathrm{d}t\, \mathrm{d}z \right) \mathrm{d}x\, \mathrm{d}y = \int\limits_{x^2+y^2<1} \pi\left(1-x^2-y^2\right) \mathrm{d}x\, \mathrm{d}y.$$

Folosind schimbarea de coordonate polare uzuală rezultă că

$$v(B_4) = 2\pi^2 \int_0^1 \left(1-r^2\right) \cdot r\, \mathrm{d}r = 2\pi^2 \left[\frac{r^2}{2}\Big|_0^1 - \frac{r^4}{4}\Big|_0^1 \right] = 2\pi^2 \left(\frac{1}{2} - \frac{1}{4} \right) = 2\pi^2 \cdot \frac{1}{4} = \frac{\pi^2}{2},$$

ceea ce justifică egalitatea

$$v\left(B_4^{2n}\right) = \frac{\pi^2}{2} \cdot (2n)^2.$$

Această a doua demonstrație este inspirată din cartea *An introduction to the Geometry of number* de J. W. S. Cassels (Berlin. Springer, 1971) pagina 99.

II. **Propoziție**: *Fie n și k două numere naturale nenule. Mulțimea formelor (polinoamelor) omogene de grad n în k variabile, cu coeficienți reali, formează un spațiu vectorial V peste* **R** *de dimensiune* C_{n+k-1}^{k-1}.

Soluție: Faptul că V este un spațiu vectorial peste **R** este evident, o bază a sa fiind formată de monoamele $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$, unde $\alpha_1, \alpha_2, \ldots, \alpha_k$ sunt numere naturale îndeplinind condiția $\sum_{i=1}^{k} \alpha_i = n$. Pentru a demonstra că dimensiunea lui V peste **R** este C_{n+k-1}^{k-1} vom proceda la o inducție după k, numărul de variabile. Dacă $k = 1$ atunci evident că dimensiunea lui V este $1 = C_n^0$. Dacă $k = 2$ se poate observa ușor că dimensiunea lui V peste **R** este $n + 1 = C_{n+1}^1$. Presupunem enunțul adevărat pentru k și îl vom demonstra pentru $k+1$. Trebuie calculat câte cupluri $(\alpha_1, \alpha_2, \ldots, \alpha_{k+1})$ de numere naturale există cu proprietatea că $\sum_{i=1}^{k+1} \alpha_i = n$.

Dacă $(\alpha_1, \alpha_2, \ldots, \alpha_{k+1})$ este un astfel de cuplu atunci $\alpha_{k+1} \le \sum_{i=1}^{k+1} \alpha_i = n$, deci α_{k+1} este un număr natural satisfăcând inegalitățile $0 \le \alpha_{k+1} \le n$. Pentru un α_{k+1} număr

natural fixat cuprins între 0 și n, conform ipotezei de inducție, există $C_{n-\alpha_{k+1}+k-1}^{k-1}$ posibilități de alegere a numerelor naturale α_1, α_2, ..., α_k astfel încât $\sum_{i=1}^{k}\alpha_i = n-\alpha_{k+1}$. Aceste considerații ne arată că dimensiunea lui V peste $\mathbf{R}$ este egală cu $\sum_{\alpha=0}^{n} C_{n-\alpha+k-1}^{k-1} = \sum_{\alpha=0}^{n} C_{\alpha+k-1}^{k-1}$. Pentru a calcula această sumă se folosește formula $C_m^{k-1} + C_m^k = C_{m+1}^k$ oricare ar fi $m \in \mathbf{N}$, $m \geq k$. Deci

$$\sum_{\alpha=0}^{n} C_{\alpha+k-1}^{k-1} = \underbrace{C_k^k + C_k^{k-1}} + C_{k+1}^{k-1} + \ldots + C_{n+k-1}^{k-1} = \underbrace{C_{k+1}^k + C_{k+1}^{k-1}} + \ldots + C_{n+k-1}^{k-1} =$$

$$= C_{k+2}^k + C_{k+2}^{k-1} + \ldots + C_{n+k-1}^{k-1} = \ldots = C_{n+k-1}^k + C_{n+k-1}^{k-1} = C_{n+k}^k.$$

Aceasta demonstrează că enunțul este adevărat pentru orice k, număr natural nenul.

III. **Teorema lui Carathéodory**. *Fie X o submulțime a lui $\mathbf{R}^n$. Atunci*

$$\operatorname{co} X = \left\{ y \in \mathbf{R}^n \,\middle|\, y = \sum_{i=1}^{s} \lambda_i x_i \,;\, \sum_{i=1}^{s} \lambda_i = 1; \lambda_i \geq 0 \ (\forall)\ i = \overline{1,s}\ ,\ s \leq n+1 \right\}$$

este cea mai mică submulțime convexă a lui $\mathbf{R}^n$ care conține pe X; deci $\operatorname{co} X = \bigcap_{\substack{Y \text{ convexă};\ Y \subseteq \mathbf{R}^n \\ X \subseteq Y}} Y$. *Dacă în plus vectorii lui X sunt raționali (adică coordonatele oricărui $x \in X$ sunt raționale) și $y \in \operatorname{co} X$ este un vector rațional, atunci acei λ_i de mai sus pot fi toți aleși numere raționale.*

Demonstrație. Fie

$$B = \left\{ y \in R^n \,\middle|\, y = \sum_{i=1}^{m} \lambda_i x_i \,;\, \sum_{i=1}^{m} \lambda_i = 1;\ \lambda_i \geq 0,\ (\forall)\ i = \overline{1,m},\ m \in \mathbf{N} \right\}.$$

Este ușor de arătat că $X \subseteq B$, B este o mulțime convexă și în plus orice submulțime a lui $\mathbf{R}^n$, convexă, și care conține pe X trebuie să conțină mulțimea B. Deci $B = \operatorname{co} X$. Trebuie arătat că dacă $y = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_k x_k$ este un element al lui $\operatorname{co} X \left(\lambda_i \geq 0, (\forall) i = \overline{1,k};\ \sum_{i=1}^{k} \lambda_i = 1 \right)$, atunci acel k de mai sus poate fi ales mai mic sau egal cu $n+1$. Dacă cumva $k > n+1$, din teoria sistemelor de ecuații liniare deducem existența numerelor α_1, α_2, ..., α_k, nu toate nule astfel încât:

$$(*) \quad \begin{cases} \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_k x_k = 0 \\ \alpha_1 + \alpha_2 + \ldots + \alpha_k = 0 \end{cases}$$ (sistemul alăturat are $n+1$ ecuații, k necunoscute, este compatibil fiind omogen și în plus $k > n+1$). Fie

$$A = \left\{ r \in \mathbf{R} / r\alpha_i \geq -\lambda_i, (\forall)\ i = \overline{1,k} \right\};$$

atunci A este o mulțime închisă ($A = \overline{A}$). A este nevidă ($A \neq \phi$) deoarece $0 \in A$ și A este diferită de $\mathbf{R}$, întrucât cel puțin un α_i este nenul. Din cele de mai sus deduc că ∂A, frontiera mulțimii A, este nevidă, deci există $r_0 \in \partial A$. Pentru acest $r_0 \in \partial A$ există cel puțin un $i_0 \in \mathbf{N}$, $1 \leq i_0 \leq k$ astfel încât $\lambda_{i_0} + r_0\alpha_{i_0} = 0$ (în caz contrar dacă $\lambda_i + r_0\alpha_i > 0$ $(\forall)$ $i = \overline{1,k}$ atunci $r_0 \in$ Å, ceea ce nu se poate). Ținând cont de relațiile(*) deducem că

$$\begin{cases} y = (\lambda_1 + r_0\alpha_1)x_1 + (\lambda_2 + r_0\alpha_2)x_2 + \ldots (\lambda_k + r_0\alpha_k)x_k \\ \lambda_i + r_0\alpha_i \geq 0, \ (\forall) i = \overline{1,k}; \ \sum_{i=1}^{k}(\lambda_i + r_0\alpha_i) = 1 \\ \lambda_{i_0} + r_0\alpha_{i_0} = 0. \end{cases}$$

Repetând acest argument de câte ori este nevoie deducem că orice element y aparținând lui co X poate fi scris sub forma $y = \sum_{i=1}^{s}\lambda_i x_i$, unde $\lambda_i \geq 0$ oricare ar fi i de la 1 la s, $\sum_{i=1}^{s}\lambda_i =$ și în plus s este un număr natural mai mic sau egal cu $n+1$. Dacă cumva y și x_i sunt vectori raționali pentru orice $i = \overline{1,s}$ atunci folosind teoria sistemelor de ecuații liniare deducem că numerele λ_i pot fi alese chiar raționale, ceea ce termină demonstrația teoremei.

IV. **Propoziția 1**: *Dacă X este o submulțime convexă a lui $\mathbf{R}^n$, atunci $\overline{X}$ este de asemenea o mulțime convexă.*

Demonstrație: Arătăm întâi că $B(X, \delta) = \{y \in \mathbf{R}^n \mid \exists\, x \in X$ astfel încât distanța de la x la y, pe care o vom nota cu $|x - y|$, să fie mai mică strict decât $\delta\}$ este o mulțime convexă oricare ar fi $\delta \in \mathbf{R}_+^*$. Pentru aceasta fie $y_1, y_2 \in B(X, \delta)$ și λ_1, λ_2 numere reale pozitive satisfăcând egalitatea $\lambda_1 + \lambda_2 = 1$. Știm că există $x_1, x_2 \in X$ astfel încât $|x_1 - y_1| < \delta$ și $|x_2 - y_2| < \delta$. Atunci

$$|\lambda_1 y_1 + \lambda_2 y_2 - \lambda_1 x_1 - \lambda_2 x_2| \leq$$

$$\leq \lambda_1 |x_1 - y_1| + \lambda_2 |x_2 - y_2) < \delta(\lambda_1 + \lambda_2) = \delta$$

și cum $\lambda_1 x_1 + \lambda_2 x_2 \in X$ (deoarece X este convexă) atunci

$$\lambda_1 y_1 + \lambda_2 y_2 \in \in B(X, \delta).$$

Această arată că $B(X, \delta)$ este o mulțime convexă. Cum $\overline{X} = \bigcap_{\delta > 0} B(X, \delta)$ și intersecția unor mulțimi convexe este în continuare o mulțime convexă, cele de mai sus ne arată că $\overline{X}$ este convexă dacă X este o submulțime convexă a lui $\mathbf{R}^n$.

Lemă. *Fie X o mulțime convexă pentru care $\overset{\circ}{X} \neq \emptyset$; fie $x_1 \in \overline{X}$ și $x_2 \in \overset{\circ}{X}$; atunci $(x_1, x_2] \subseteq \overset{\circ}{X}$ (prin $(x_1, x_2]$ înțelegem segmentul de capete x_1 și x_2,*

deschis în x_1 și închis în x_2). Aici ca și mai înainte X este considerată ca o submulțime a lui $\mathbf{R}^n$.

Demonstrație: Facem întâi demonstrația în cazul $x_1 \in X$. Știm că există $\delta > 0$ astfel încât $B(x_2, \delta) \subseteq X$. Fie $y \in (x_1, x_2]$; aceasta înseamnă că există două numere reale λ și μ astfel încât $y = \lambda x_1 + \mu x_2$, unde $\lambda \geq 0$ și $\mu > 0$, $\lambda + \mu = 1$. Fie $z \in B(y, \mu\delta)$. Aceasta înseamnă că

$$|z - (\lambda x_1 + \mu x_2)| < \mu\delta$$

sau împărțind la μ,

$$\left| \frac{z - \lambda x_1}{\mu} - x_2 \right| < \delta.$$

De aici deducem că

$$\frac{z - \lambda x_1}{\mu} \in B(x_2, \delta) \subseteq X,$$

deci

$$\frac{z - \lambda x_1}{\mu} \in X.$$

Cum

$$z = \mu \cdot \frac{z - \lambda x_1}{\mu} + \lambda \cdot x_1,$$

deducem că $z \in X$ (deoarece $\mu \geq 0$, $\lambda \geq 0$, $\mu + \lambda = 1$, $x_1 \in X$, $\frac{z - \lambda x_1}{\mu} \in X$ și X e convexă).

Aceasta înseamnă că $B(y, \mu\delta) \subseteq X$, deci $(x_1, x_2] \subseteq \overset{\circ}{X}$. Trecem la demonstrația cazului general și anume când $x_1 \in \overline{X}$. Ca și mai înainte fie $\delta > 0$ astfel încât $B(x_2, \delta) \subseteq \overset{\circ}{X}$ și $y \in (x_1, x_2)$ (dacă $y = x_2$, enunțul este evident adevărat). Deoarece $x_1 \in \overline{X}$, există $z_1 \in X$ astfel încât

$$|z_1 - x_1| < \frac{\delta |x_1 - y|}{|x_2 - y|} \quad (|x_2 - y| \neq 0,$$

deoarece $y \neq x_2$). Definim pe z_2 prin egalitatea

$$z_2 - x_2 = -\frac{|x_2 - y|}{|x_1 - y|}(z_1 - x_1).$$

Dacă $y = \lambda x_2 + \mu x_1$, unde $\mu, \lambda \in \mathbf{R}_+^*$ și $\mu + \lambda = 1$ atunci se poate arăta ușor că

$$\lambda = \frac{|x_1 - y|}{|x_1 - x_2|} = \frac{|x_1 - y|}{|x_1 - y| + |x_2 - y|}$$

și

$$\mu = \frac{|x_2 - y|}{|x_1 - y| + |x_2 - y|}.$$

Deci $y = \frac{|x_1 - y|}{|x_1 - y| + |x_2 - y|} x_2 + \frac{|x_2 - y|}{|x_1 - y| + |x_2 - y|} x_1 = \frac{|x_1 - y| z_2 + |x_2 - y| z_1}{|x_1 - y| + |x_2 - y|}$,

ultima egalitate rezultând din modul de definire al lui z_2. Aceasta înseamnă că $y \in [z_1, z_2]$. Cum

$$|z_2 - x_2| = \frac{|x_2 - y|}{|x_1 - y|} |z_1 - x_1| < \delta,$$

rezultă că $z_2 \in \overset{\circ}{X}$. Dacă $z_1 \neq y$ conform primei părți a demonstrației (să nu uităm că $z_1 \in X$) rezultă că $y \in \overset{\circ}{X}$. Dacă $z_1 = y$ atunci

$$|y - x_1| = |z_1 - x_1| < \frac{\delta |x_1 - y|}{|x_2 - y|}.$$

Împărțind cu $|x_1 - y|$ ultima inegalitate ($|x_1 - y| \neq 0$) obținem că $|x_2 - y| < \delta$, adică $y \in B(x_2, \delta) \subseteq \overset{\circ}{X}$, ceea ce este conform cu cerința enunțului.

Propoziția 2: *Fie $X \subseteq \mathbf{R}^n$ o mulțime convexă astfel încât $\overset{\circ}{X} \neq \emptyset$. În aceste condiții $\overline{\overset{\circ}{X}} = \overset{\circ}{X}$.*

Demonstrație: Deoarece $X \subseteq \overline{X}$ incluziunea $\overset{\circ}{X} \subseteq \overline{\overset{\circ}{X}}$ este evidentă. Fie $x \notin \overset{\circ}{X}$ și $x_1 \in \overset{\circ}{X}$ (există un astfel de x_1 deoarece $\overset{\circ}{X} \neq \emptyset$). Pe dreapta care trece prin punctele x_1 și x, orice punct y astfel încât $x \in (x_1, y)$, nu aparține lui $\overline{X}$ (aceasta datorită lemei precedente; dacă $y \in \overline{X}$, conform lemei amintite ar rezulta că $x \in \overset{\circ}{X}$, ceea ce nu e adevărat). Aceasta înseamnă că $x \notin \overline{\overset{\circ}{X}}$ (dacă cumva $x \in \overline{\overset{\circ}{X}}$, atunci ar exista un $y \in \overline{X}$ pe dreapta ce conține pe x și x_1 astfel încât $x \in (x_1, y)$, ceea ce nu se poate). Deci $\overset{\circ}{X} = \overline{\overset{\circ}{X}}$, ceea ce trebuia demonstrat.

Propoziția 3: *Dacă $X \subseteq \mathbf{R}^n$ este o mulțime convexă astfel încât $\overset{\circ}{X} \neq \emptyset$, atunci $\overline{X} = \overline{\overset{\circ}{X}}$.*

Demonstrație: Deoarece $\overset{\circ}{X} \subseteq X$, atunci incluziunea $\overline{\overset{\circ}{X}} \subseteq \overline{X}$ este evidentă. Fie $x \in \overline{X}$ și $x_1 \in \overset{\circ}{X}$. Conform lemei demonstrate în acest paragraf $(x, x_1] \subseteq \overset{\circ}{X}$, de unde se deduce imediat că $x \in \overline{\overset{\circ}{X}}$. Deci are loc incluziunea $\overline{X} \subseteq \overline{\overset{\circ}{X}}$, ceea ce înseamnă că $\overline{\overset{\circ}{X}} = \overline{X}$.

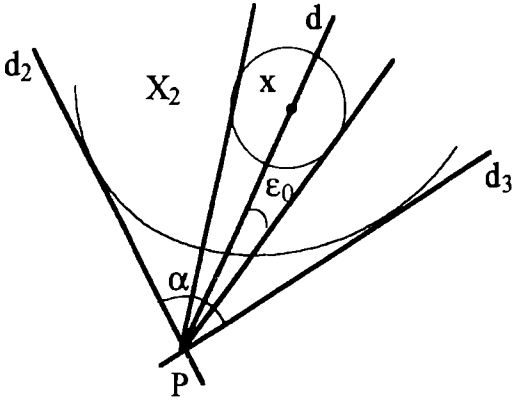
V. În cele ce urmează vom numi $\mathcal{L} \subseteq \mathbf{R}^n$ varietatea liniară de dimensiune r $(0 \le r \le n)$ o submulțime de forma $\mathcal{L} = V + a$, unde V este un subspațiu vectorial de dimensiune r al lui $\mathbf{R}^n$ și a este un vector oarecare din $\mathbf{R}^n$. Dacă dimensiunea lui $\mathcal{L}$ este $n-1$, $\mathcal{L}$ se va numi hiperplan. În cazul în care $\mathcal{L}$ este un hiperplan, există o exprimare foarte comodă pentru $\mathcal{L}$. Dacă $y = (y_1, y_2, ..., y_n)$ și $z = (z_1, z_2, ..., z_n)$ sunt doi vectori din $\mathbf{R}^n$ notăm prin $y \cdot z$ produsul scalar uzual din $\mathbf{R}^n$, deci $y \cdot z = \sum_{i=1}^{n} y_i \cdot z_i$. Dacă $\mathcal{L} = V + a$ și $e_1, e_2, ..., e_{n-1}$ este o bază ortonormată a lui V (adică $e_i \cdot e_j = 0$ dacă $i \neq j$ și $e_i \cdot e_i = 1$; existența unei astfel de baze este un lucru cunoscut), fie e_n un vector din $\mathbf{R}^n$ astfel încât $e_1, e_2, ..., e_n$ să fie o bază ortonormată a lui $\mathbf{R}^n$. Dacă $x = \alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_{n-1} e_{n-1} + a$ este un vector din $\mathcal{L}$ $(\alpha_i \in \mathbf{R}\ (\forall)\ i = \overline{1, n-1})$ atunci $xe_n = a \cdot e_n = \lambda$, unde λ este o constantă reală. Pe de altă parte $b \in \mathbf{R}^n$ este un vector nenul, mulțimea punctelor din $\mathbf{R}^n$ pentru care $x \cdot b = \lambda$ (unde λ este o constantă reală) este un hiperplan după cum ușor se poate verifica.

Putem enunța în acest moment principalul rezultat al acestui paragraf:

Propoziția 1: *Fie* $X = \overset{\circ}{X}$ *o submulțime convexă a lui* $\mathbf{R}^n$ *și* $\mathcal{L}$ *o varietate liniară de dimensiune r a lui* $\mathbf{R}^n$ *astfel încât* $\mathcal{L} \cap X = \emptyset$ *și* $0 \le r < n$. *Există atunci un hiperplan* β *astfel încât* $\mathcal{L} \subseteq \beta$ *și* $\beta \cap X = \emptyset$.

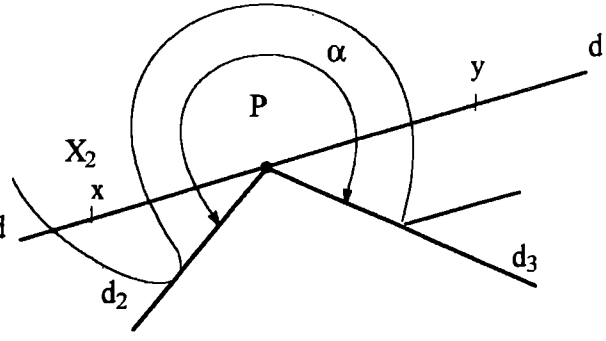
Demonstrație: Fie β varietatea liniară de dimensiune maximă astfel încât $\mathcal{L} \subseteq \beta$ și $\beta \cap X = \emptyset$. Fie s dimeniunea lui β; trebuie arătat că $s = n - 1$ (faptul că $s \le n - 1$ este evident). Fie D varietatea liniară ortogonală lui β. Dacă $\beta = V + a$, unde V este un subspațiu vectorial de dimensiune s al lui $\mathbf{R}^n$, atunci $D = W + a$, unde $\mathbf{R}^n = V \oplus W$ (dacă $e_1, e_2, ..., e_s$ este o bază ortonormată a lui V și $e_{s+1}, e_{s+2}, ..., e_n$ sunt niște vectori astfel încât $e_1, e_2, ..., e_n$ să fie o bază ortonormată a lui $\mathbf{R}^n$, atunci W este subspanțiul vectorial al lui $\mathbf{R}^n$ generat de vectorii $e_{s+1}, e_{s+2}, ..., e_n$). Deci dimensiunea lui D este egală cu $n - s$. Proiecția lui β pe D este un punct P care are coordonatele vectorului a, iar proiecția lui X pe D este o mulțime X_1 convexă și deschisă. Făcând o translație de vector $-a$ aceasta revine la un exercițiu foarte simplu și anume, dacă $f\ \mathbf{R}^n \to \mathbf{R}^r$ este definită astfel $f(x_1, x_2, ..., x_n) = (x_1, x_2, ..., x_r)$, unde $0 \le r \le n$, atunci $f(A)$ este mulțime deschisă în $\mathbf{R}^r$, dacă A este deschisă în $\mathbf{R}^n$ și $f(B)$ este convexă în $\mathbf{R}^r$, dacă B este convexă în $\mathbf{R}^n$.

Dacă $r = 0$ atunci $f(x_1, x_2, ..., x_n) = 0$, $(\forall)\ x_1, x_2, ..., x_n \in \mathbf{R}$. Este evident că $P \notin X_1$. Datorită alegerii lui β ca fiind varietatea liniară de dimensiune maximă astfel încât $\mathcal{L} \subseteq \beta$ și $\beta \cap X = \phi$ deducem că orice dreaptă din D care trece prin punctul P taie (intersectează) pe X_1. Dacă dimensiunea lui D este 1 atunci $s = n - 1$ și enunțul este demonstrat. Dacă dimensiunea lui D este mai mare sau egală cu 2 atunci există un plan $\pi \subseteq D$ care trece prin punctul P. $\pi \cap X_1 = X_2$; X_2 este o mulțime nevidă (orice dreaptă din π care trece prin P conține cel puțin un punct al mulțimii X_2), convexă și deschisă în π. De asemenea $P \notin X_2$. Putem realiza următorul desen:



Dacă d este o semidreaptă din π cu originea în P și care trece printr-un punct $x \in X_2$, există atunci un $\delta > 0$ astfel încât orice $y \in \pi$, astfel încât $|y - x| \leq \delta$, trebuie să aparțină lui X_2; aceasta înseamnă că există un ε_0 astfel încât oricare ar fi $0 < \varepsilon \leq \varepsilon_0$ și oricare ar fi o semidreaptă d_1 care pornește din P și face un unghi ε față de semidreapta d, atunci d_1 conține un punct din X_2. Această constatare împreună cu faptul că X_2 este conexă (fiind convexă), implică faptul că semidreptele cu un capăt în P și care taie pe X_2 formează un sector unghiular de unghi α (semidreptele „frontieră" ale acestui sector unghiular nu aparțin mulțimii indicate mai sus datorită observațiilor făcute; pe figură acestea au fost notate cu d_2 și d_3). Dacă cumva $\alpha \leq \pi$ atunci prelungind pe d_2 obținem o dreaptă care trece prin P dar nu conține nici un punct din X_2; aceasta este o contradicție fiindcă știm că orice dreaptă a lui π care trece prin P taie pe X_2.

Dacă cumva $\alpha > \pi$ atunci există d și d_1 două semidrepte ce se află una în prelungirea celeilalte, fiecare conținând câte un punct din X_2 (x, respectiv y). Deoarece X_2 este convexă, deducem că $[x, y] \subseteq X_2$, ceea ce înseamnă că $P \in X_2$, aceasta fiind o contradicție. Deci



singura posibilitate este că dimensiunea lui D este 1 ceea ce implică că dimensiunea lui β este $n-1$. Enunțul este demonstrat în acest moment.

Propoziția 2: *Fie X_1 și X_2 două submulțimi convexe ale lui $\mathbf{R}^n$ astfel încât $X_1 \cap X_2 = \emptyset$ și $X_1 = \overset{\circ}{X}_1$. Există atunci un hiperplan β care separă X_1 de X_2.*

Demonstrație. Fie $A = X_1 - X_2 = \{y \in \mathbf{R}^n \mid y = x_1 - x_2, x_1 \in X_1 \text{ și } x_2 \in X_2\}$. Deoarece

$$A = \bigcup_{x_2 \in X_2} (X_1 - x_2)$$

și reuniunea unor mulțimi deschise este în continuare mulțime deschisă, deducem că $A = \overset{\circ}{A}$. $X_1 - x_2$ este deschisă deoarece este translatata mulțimii deschise X_1 cu vectorul $-x_2$. Dacă λ și μ sunt două numere reale, pozitive, astfel încât $\lambda + \mu = 1$ și $y = x_1 - x_2$, $z = z_1 - z_2$ sunt două elemente din A ($x_1, z_1 \in X_1$ și $x_2, z_2 \in X_2$) atunci

$$\lambda y + \mu z = (\lambda x_1 + \mu z_1) - (\lambda x_2 + \mu z_2) \in A$$

deoarece X_1 și X_2 sunt mulțimi convexe. Deci A este deschisă, convexă și în plus $0 \notin A$ (deoarece $X_1 \cap X_2 = \emptyset$). Folosind propoziția 1 există un hiperplan β astfel încât $0 \in \beta$ și $\beta \cap A = \emptyset$. Presupunem că β e dat de ecuația $a \cdot x = 0$ (unde a e un vector nenul al lui $\mathbf{R}^n$). Deoarece $\beta \cap A = \emptyset$ atunci $a \cdot x > 0$ pentru orice $x \in A$ (sau varianta cealaltă $a \cdot x < 0$, $(\forall)\ x \in A$, care se tratează în mod analog). Inegalitatea de mai sus se poate scrie și sub forma $ax_1 > ax_2$ pentru oricare $x_1 \in X_1$ și $x_2 \in X_2$. De aici deducem că există

$$\inf\{a \cdot x \mid x \in X_1\} = \lambda > -\infty$$

și X_1 și X_2 sunt separate de hiperplanul $a \cdot x = \lambda$.

Avem nevoie în continuare de câteva definiții.

Definiție: i) Fie $X \subseteq \mathbf{R}^n$; se spune că *hiperplanul β taie pe X* dacă există puncte ale lui X, în fiecare din cele două regiuni deschise determinate de β.

ii) În aceeași situație ca mai sus dacă hiperplanul β intersectează pe $\overline{X}$ și nu taie pe X atunci β se numește *hiperplan de sprijin*.

Definiție. Fie $X \subseteq \mathbf{R}^n$ o submulțime convexă. Se numește *dimensiunea liniară a lui X* (se notează cu dim X) cel mai mare număr natural r astfel încât X conține $r+1$ puncte $x_1, x_2, \ldots, x_{r+1}$ pentru care vectorii $x_2 - x_1$, $x_3 - x_1, \ldots, x_{r+1} - x_1$ sunt liniar independenți.

Observație. *Se arată ușor că dacă dim $X = n$, unde X este o submulțime convexă a lui $\mathbf{R}^n$, atunci $\overset{\circ}{X} \neq \emptyset$.* Într-adevăr dacă $x_1, x_2, \ldots, x_{n+1} \in X$ sunt ca în definiția de mai sus atunci punctul

$$y = \frac{x_1 + x_2 + \ldots + x_{n+1}}{n+1} \in \overset{\circ}{X}$$

argumentul decisiv aici este că deoarece $x_2 - x_1, ..., x_{n+1} - x_1$ sunt vectori liniar independenți, atunci pentru orice $z \in \mathbf{R}^n$ există $\alpha_1, ..., \alpha_n$ numere reale astfel încât

$$z - x_1 = \alpha_1(x_2 - x_1) + ... + \alpha_n(x_{n+1} - x_1);$$

de aici deducem că orice $z \in \mathbf{R}^n$ se poate scrie sub forma $z = \sum_{i=1}^{n+1} \lambda_i x_i$, unde $\lambda_i \in \mathbf{R}$, $(\forall)\ i = \overline{1, n+1}$ și $\sum_{i=1}^{n+1} \lambda_i =$. Există deci o funcție bijectivă și bicontinuă f de la $A = \{(\lambda_1, ..., \lambda_{n+1}) \in \mathbf{R}^{n+1} \mid \sum_{i=1}^{n+1} \lambda_i =$ $\}$ la $\mathbf{R}^n$ definită prin $f(\lambda_1, ..., \lambda_{n+1}) =$ $= \sum_{i=1}^{n+1} \lambda_i x_i$. Există deci $\delta > 0$ astfel încât pentru orice $z \in B(y, \delta)$ să existe $\lambda_1, ..., \lambda_{n+1}$ numere reale suficient de apropiate de $\frac{1}{n+1}$ - deci pozitive - astfel încât $z = \sum_{i=1}^{n+1} \lambda_i x_i$ și $\sum_{i=1}^{n+1} \lambda_i =$. De aici rezultă că $z \in X$, deci $B(y, \delta) \subseteq X$, adică $y \in \overset{\circ}{X}$.

Propoziția 3: *Prin orice punct al frontierei unei mulțimi convexe $X \subseteq \mathbf{R}^n$, trece cel puțin un hiperplan de sprijin.*

Demonstrație: Dacă $\dim X < n$ enunțul e clar (X poate fi „scufundată" în acest caz într-un hiperplan). Dacă $\dim X = n$ fie $P \in \partial X$. Considerăm $X_1 = \overset{\circ}{X}$ și $X_2 = P$ ($X_1 \neq \varnothing$ conform observației precedente și X_1 este convexă conform lemei din paragraful (IV). Aplicând propoziția 2 deducem existența unui hiperplan β care separă $\overset{\circ}{X}$ de P. Aceasta înseamnă că β nu taie $\overset{\circ}{X}$ și deci β nu taie X (deoarece $X \subseteq \overline{X} = \overline{\overset{\circ}{X}}$ conform propoziției 3 din paragraful (IV). Deoarece $P \in \partial X \subseteq \overline{X} = \overline{\overset{\circ}{X}}$ (conform aceluiași rezultat citat mai sus), atunci β trebuie să-l conțină neapărat pe P. Propoziția este demonstrată în acest moment.

VI. În acest paragraf, dacă $X \subseteq \mathbf{R}^n$ este o submulțime convexă astfel încât $\dim X = m$ ($0 \leq m \leq n$; $m \in \mathbf{N}$), atunci pe X o vom considera „scufundată" în $\mathcal{L}(X)$, cea mai mică varietate liniară care conține pe X. Este evident faptul că $\mathcal{L}(X)$ are dimensiunea m. Vom numi interior *relativ al lui X*, interiorul lui X, relativ la $\mathcal{L}(X)$. Conform observației făcută în paragraful precedent (ținând cont că $\dim X = \dim \mathcal{L}(X) = m$) interiorul relativ al lui X este nevid.

Teoremă. *Fie*

$$B = \{x = (x_1, x_2, ..., x_n) \in \mathbf{R}^n \mid \sum_{i=1}^{n} x_i^2 \leq 1\},$$

fie $f_1, f_2, ..., f_m$ *funcții continue definite pe* B *cu valori reale și* A *următoarea submulțime a lui* $\mathbf{R}^m$, $A = \{y = (y_1, y_2, ..., y_m) \in \mathbf{R}^m \mid (\exists)\, x = (x_1, x_2, ..., x_n) \in B$ *astfel încât* $y_i = f_i(x)$, $(\forall)\, i = \overline{1,m}\}$. *Notez cu* $C = (z_1, z_2, ..., z_m)$ *punctul din* $\mathbf{R}^m$ *ale cărui coordonate sunt date de formulele* $z_i = \frac{\int_B f_i \, dv}{v(B)}$, $(\forall)\, i = \overline{1,m}$ (v *este măsura Lebesgue din* $\mathbf{R}^n$). *Să se arate că* C *aparține interiorului relativ al mulțimii co* A.

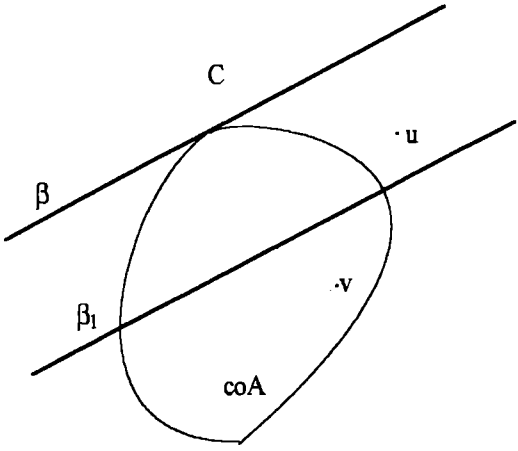
Observație. *Într-un limbaj imprecis, dar intuitiv, semnificația teoremei precedente este că „centrul de greutate" al mulțimii* A *aparține interiorului relativ al mulțimii co* A.

Demonstrație: Conform observațiilor făcute la începutul acestui paragraf putem considera că dim (co A) = m (dacă nu se întâmplă așa atunci înlocuim pe $\mathbf{R}^m$ cu $\mathcal{L}(\text{co } A)$) și deci trebuie demonstrat că $C \in \overset{\cdot}{\text{co}}\, A$. Întâi să demonstrăm un lucru ușor și anume că $C \in \overline{\text{co } A}$. Pentru fiecare $l \in \mathbf{N}^*$ să considerăm $B_1^l, B_2^l, ..., B_{r_l}^l$ o partiție a lui B adică B_j^l este mulțime măsurabilă Lebesgue, $(\forall)\, j = \overline{1,r_l}$, $B_j^l \cap B_i^l = \emptyset$, $(\forall)\, i \neq j$, $i = \overline{1,r_l}$, $j = \overline{1,r_l}$ și în plus $\bigcup_{i=1}^{r_l} B_i^l = B$) astfel încât $v(B_i^l) < \frac{1}{l}$, $(\forall)\, i = \overline{1,r_l}$. Pentru fiecare $i = \overline{1,r_l}$ alegem un punct $\xi_{i,l}$, aparținând lui B_i^l. Fie

$$z_l = \sum_{i=1}^{r_l} \frac{v(B_i^l)}{v(B)} (f_1(\xi_{i,l}), f_2(\xi_{i,l}), ..., f_m(\xi_{i,l})).$$

Este evident că $z_l \in$ co A, $(\forall)\, l \in \mathbf{N}^*$ (deoarece $\frac{v(B_i^l)}{v(B)} \geq 0$, $(\forall)\, i = \overline{1,r_l}$, $\sum_{i=1}^{r_l} \frac{v(B_i^l)}{v(B)} = 1$ și $(f_1(\xi_{i,l}), f_2(\xi_{i,l}), ..., f_m(\xi_{i,l})) \in A$, $(\forall)\, i = \overline{1,r_l}$) și că $z_l \xrightarrow{l \to \infty} C$ (datorită definiției integralei Lebesgue). Toate acestea ne asigură faptul că $C \in \overline{\text{co } A}$. Dacă enunțul nu ar fi adevărat atunci C ar aparține lui $\overline{\text{co } A} \setminus \overset{\cdot}{\text{co}}\, A = \partial(\text{co } A)$. Conform propoziției 3 din paragraful (V) există un hiperplan de

sprijin β pentru co A astfel încât $C \in \beta$. Dacă hiperplanul β este dat de ecuația $a \cdot y = \lambda$ (a e un vector nenul din $\mathbf{R}^n$ și $\lambda \in \mathbf{R}$) să presupunem că co A aparține regiunii determinate de inecuația $a \cdot y \leq \lambda$.



$\beta = \{y \in \mathbf{R}^m \mid ay = \lambda\}$
$\beta_1 = \{y \in \mathbf{R}^m \mid ay = \lambda_1\}$

Există atunci un $\lambda_1 \in \mathbf{R}$, $\lambda_1 < \lambda$ astfel încât

$$A_1 = \{y \in \mathbf{R}^m \mid y \in \text{co } A \text{ și } \lambda_1 \leq a \cdot y \leq \lambda\}$$

și

$$A_2 = \{y \in \mathbf{R}^m \mid y \in \text{co } A \text{ și } a \cdot y < \lambda_1\}$$

să fie mulțimi nevide (asta se întâmplă deoarece dim (co A) = m). Fie $f: B \to \mathbf{R}^m$ definită prin $f(x) = (f_1(x), f_2(x), \ldots f_m(x))$; este evident că f este o funcție continuă. Fie $B_1 = f^{-1}(A_1)$ și $B_2 = f^{-1}(A_2)$. B_1 și B_2 sunt mulțimi măsurabile Lebesgue (B_1 este închisă în B și B_2 este deschisă în B deoarece

$$B_1 = f^{-1}(\{y \in \mathbf{R}^m \mid \lambda_1 \leq ay \leq \lambda\}),$$
$$B_2 = f^{-1}(\{y \in \mathbf{R}^m \mid ay < \lambda_1\}),$$

f este continuă și mulțimile $\{y \in \mathbf{R}^m \mid \lambda_1 \leq ay \leq \lambda\}$, respectiv $\{y \in \mathbf{R}^m \mid ay < \lambda_1\}$ sunt închise, respectiv deschise în $\mathbf{R}^m$. B_1 și B_2 sunt mulțimi boreliene, deci și măsurabile Lebesgue (vezi Miron Nicolescu *Funcții reale și elemente de topologie*, Editura Didactică și pedagogică, București, 1968, pagina 220, consecința teoremei din 8.4.1); în plus măsura lor Lebesgue este strict pozitivă (deoarece B_1 și B_2 conțin fiecare câte o mulțime nevidă și deschisă în B. Pentru B_2 acest lucru e clar, ea însăși fiind nevidă și deschisă în B iar pentru B_1 acest lucru rezultă din faptul că B_1 conține mulțimea $f^{-1}(\{y \in \mathbf{R}^m \mid \lambda_1 < a \cdot y < \lambda\})$ care este deschisă în B și este și nevidă. Dacă cumva mulțimea precedentă ar fi vidă, cum $C \in \overline{\text{co } A}$, atunci există $a_1 \in A \cap \beta$. Deoarece $A_2 \neq \emptyset$ atunci există $a_2 \in A_2 \cap A$. Presupunerea că mulțimea $\{y \in \mathbf{R}^m \mid \lambda_1 < ay < \lambda\}$ nu conține nici un punct din A și existența punctelor a_1 și a_2 de mai sus ne-ar duce la concluzia că A este neconexă. Însă A fiind imaginea prin funcția continuă f a mulțimii

conexe B este și ea conexă). Fie $u = (u_1, u_2, ..., u_m)$ și $v = (v_1, v_2, ..., v_m)$ puncte din $\mathbf{R}^m$ ale căror coordonate sunt date de formulele:

$$u_i = \frac{\int_{B_1} f_i \, dv}{v(B_1)}$$

$$(\forall)\, i = \overline{1,m}.$$

$$v_i = \frac{\int_{B_2} f_i \, dv}{v(B_2)}$$

Aceste formule au sens deoarece $v(B_1) > 0$ și $v(B_2) > 0$. Repetând argumentul din prima parte a demonstrației deducem că u aparține regiunii determinate de inegalitățile $\lambda_1 \leq ay \leq \lambda$ și v aparține regiunii determinată de inegalitatea $ay \leq \lambda_1$ (se aplică deci același argument prin care am arătat că $C \in \overline{\text{co}}\, A$). Este evidentă formula

$$C = \frac{v(B_1)}{v(B)} u + \frac{v(B_2)}{v(B)} \cdot v.$$

Calculăm

$$ac = \frac{v(B_1)}{v(B)} a \cdot u + \frac{v(B_2)}{v(B)} a \cdot v.$$

Ținând cont că $\lambda_1 \leq au \leq \lambda$ și $av \leq \lambda_1$ deducem că

$$a \cdot C \leq \frac{v(B_1)}{v(B)} \lambda + \frac{v(B_2)}{v(B)} \lambda_1 < \frac{v(B_1)}{v(B)} \lambda + \frac{v(B_2)}{v(B)} \lambda = \lambda.$$

Însă aceasta contrazice faptul că $C \in \beta$ (elementele lui β satisfaceau ecuația $ay = \lambda$ pe când noi am obținut mai sus că $aC < \lambda$). Contradicția a provenit din faptul că am presupus că $C \notin \overset{\cdot}{\overset{\frown}{\text{co}}}\, A$. În acest moment teorema este demonstrată.

Să demonstrăm acum o afirmație din lema 1 (Hilbert) apărută în cursul demonstrației teoremei lui Waring. Folosind notațiile de acolo trebuie arătat că $g \in \text{co}\, S$.

Dacă T este mulțimea vectorilor din V dați de formele $L = (\alpha_1 X_1 + ... + \alpha_5 X_5)^{2k}$, unde α_i sunt numere reale astfel încât $\sum_{i=1}^{5} \alpha_i^2 \leq 1$ atunci teorema demonstrată în acest paragraf ne arată că g aparține interiorului relativ al mulțimii co T. Este evident că $T \subseteq \overline{S} \subseteq \overline{\text{co}\, S}$. Cum $\overline{\text{co}\, S}$ este mulțime convexă (se folosește faptul că co S este convexă și propoziția 1 din paragraful (IV)) rezultă că $T \subseteq \text{co}\, T \subseteq \overline{\text{co}\, S}$. Fie $\mathfrak{L}$ varietatea liniară de dimensiune minimă care conține pe co S (deoarece $\mathfrak{L}$ e submulțime închisă a lui V, rezultă că $\overline{\text{co}\, S} \subseteq \mathfrak{L}$).

Vom folosi notația $\overset{\frown}{\text{co}}\, S$ pentru a desemna interiorul relativ al lui co S. Folosind observația din paragraful (V) și propoziția 2 din paragraful (IV) ($\overline{\overset{\circ}{\text{co}}\, S} = \overset{\frown}{\text{co}}\, S =$ $= \overset{\circ}{\text{co}}\, S$) deducem că dim $\overline{\text{co}\, S}$ = dim co S. Deoarece co $T \subseteq \overline{\text{co}\, S}$ deducem că dim co $T \leq$ dim $\overline{\text{co}\, S}$ = dim co S. Dacă r = dim co S, fie $y_1, y_2, ..., y_{r+1}$ vectori din S astfel încât $y_2 - y_1, y_3 - y_1, ..., y_{r+1} - y_1$ să fie liniar independenți. Pot alege un număr real λ, strict pozitiv, suficient de mare astfel încât $\frac{y_i}{\lambda} \in T$, ($\forall$) $i = 1, r+1$. Cum evident $\frac{y_2}{\lambda} - \frac{y_1}{\lambda}, ..., \frac{y_{r+1}}{\lambda} - \frac{y_1}{\lambda}$ sunt liniar independenți deducem că dim co $T \geq r$ = dim co S, de unde rezultă că dim co T = dim co S = $=$ dim $\overline{\text{co}\, S}$. Conform celor spuse mai sus $g \in \overset{\frown}{\text{co}}\, T \subseteq \overline{\overset{\circ}{\text{co}}\, S} = \overset{\frown}{\text{co}}\, S \subseteq$ co S (faptul că $\overline{\overset{\circ}{\text{co}}\, S} = \overset{\frown}{\text{co}}\, S$ rezultă din propoziția 2 paragraful IV, iar incluziunea $\overset{\frown}{\text{co}}\, S \subseteq$ co S este evidentă), ceea ce demonstrează afirmația. După cum se vede demonstrația acestei afirmații nu este deloc simplă și a necesitat un travaliu destul de însemnat (deși din punct de vedere intuitiv lucrurile păreau destul de simple). Să mai menționăm aici că demonstrațiile din paragrafele (III), (IV) și (V) ale acestei anexe sunt luate din cartea *Convexity* a lui H. G. Eggleston, Cambridge, University Press, 1969.

TEOREMA LUI GAUSS A CELOR TREI PĂTRATE

Introducere

Scopul acestui capitol este demonstrarea unei teoreme aparținând lui Gauss, care afirmă că *un număr natural m* se *poate scrie că suma a trei pătrate de numere naturale dacă și numai dacă* $m \neq 4^a(8n + 7)$, *pentru orice* $a, n \in \mathbf{N}$.

Demonstrația dată urmează articolul lui Ankeny N. C. *Sums of three squares* din Proc. Amer. Math. Soc., volumul 8 din 1957, paginile 316–319. Această soluție folosește esențial o teoremă a lui Dirichlet care afirmă că dacă $a, b \in \mathbf{N}^*$, $(a, b) = 1$, atunci există o infinitate de numere prime de forma $ak + b$, $k \in \mathbf{N}$. Demonstrația acestei teoreme a lui Dirichlet se poate găsi în *Teoria numerelor* de Z. I. Borevici și I. R. Șafarevici, Editura Științifică și Enciclopedică, București, 1985, pagina 413, sau în această carte. În demonstrația teoremei lui Gauss se mai folosește de asemenea și teorema lui Minkovski asupra corpului convex demonstrată în paragraful (I) al anexei (teorema 1). Să menționăm aici faptul că în enunțul teoremei lui Minkovski se poate considera că ν este măsura Jordan pe $\mathbf{R}^n$. Aceasta deoarece orice mulțime convexă și mărginită din $\mathbf{R}^n$ este măsurabilă Jordan și o mulțime mărginită Y nu poate intersecta decât un număr finit de mulțimi de forma $T + z$, unde z parcurge punctele unei rețele complete $\mathcal{R}$, iar T este paralelipipedul fundamental asociat lui $\mathcal{R}$ (a se urmări demonstrația din paragraful (I) al anexei). Cu ajutorul teoremei lui Minkovski se demonstrează că un număr natural $n \neq 0$ se poate scrie ca suma a două pătrate de numere naturale dacă și numai dacă orice număr prim de forma $4k + 3$ care divide pe n trebuie să apară în descompunerea în factori primi a lui n la o putere pară (propoziția 2 din paragraful (I) al anexei). O demonstrație elementară a acestui rezultat poate fi găsită în *Elementary theory of numbers* de Waclaw Sierpinski, Warszawa, 1964, pagina 351.

Se presupun cunoascute de asemenea câteva fapte legate de simbolul Legendre și Jacobi. Dacă $a \in \mathbf{Z}$ și p este un număr prim astfel încât $p \nmid a$ atunci $\left(\frac{a}{p}\right)$ se consideră egal cu 1, dacă a este rest pătratic modulo p (adică $(\exists)\ b \in \mathbf{Z}$ cu proprietatea că $b^2 \equiv a \pmod{p}$) și egal cu -1, dacă a nu e rest pătratic modulo p. Au loc următoarele proprietăți:

1) dacă $a, b \in \mathbf{Z}$ și $p \nmid a \cdot b$, $a \equiv b \pmod{p}$, atunci $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2) dacă $a, b \in \mathbf{Z}$ și $p \nmid a \cdot b$, atunci $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

3) dacă p este număr prim impar, atunci $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

4) dacă p este număr prim impar, atunci $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

5) dacă p și q sunt numere prime impare distincte, atunci: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Dacă m și n sunt două numere naturale (chiar întregi pot fi considerate), prime între ele și $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ (unde $\alpha_i \in \mathbf{N}^*$, $(\forall)\ i = \overline{1,r}$ și $p_1, p_2, \ldots, p_r$ sunt numere prime distincte) atunci se definește simbolul Jacobi după formula

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)^{\alpha_i},$$

unde $\left(\frac{m}{p_i}\right)$ este simbolul Legendre definit mai sus pentru $(\forall)\ i = \overline{1,r}$. Deși notația folosită pentru cele două simboluri este aceeași nu se pot ivi confuzii legate de acest fapt. Simbolul Jacobi are următoarele proprietăți:

1) dacă n este un număr întreg impar, atunci $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;

2) dacă n este un număr întreg impar, atunci $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Teoremă (*G a u s s*): *Un număr natural m se poate scrie ca suma a trei pătrate de numere naturale dacă și numai dacă* $m \neq 4^a(8n+7)$, *pentru orice a și n, numere naturale.*

Demonstrație : Una din implicații este ușoară. Anume vom arăta că dacă $m = 4^a(8n+7)$, unde a și n sunt numere naturale atunci m nu se poate scrie sub forma $m = x^2 + y^2 + z^2$ cu $x, y, z \in \mathbf{N}$. Să analizăm întâi cazul $a = 0$. Presupunem că există x, y și z numere naturale astfel încât $8n + 7 = x^2 + y^2 + z^2$. Din motive de paritate, deducem că ori toate numerele x, y, z sunt impare ori două dintre ele sunt pare și unul impar. Deoarece $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$ pentru $(\forall)\ k \in \mathbf{Z}$, deducem că orice număr impar ridicat la pătrat este congruent cu 1 modulo 8. Dacă cumva x, y și z sunt toate numere naturale impare, atunci conform observației anterioare $x^2 + y^2 + z^2 \equiv 1 + 1 + 1 \equiv 3 \pmod 8$. Deci în această situație nu putem avea că $x^2 + y^2 + z^2 = 8n + 7$. Se poate observa foarte ușor că un număr natural par ridicat la pătrat este congruent modulo 8, fie cu 0, fie cu 4. Aceasta înseamnă că în cazul în care două dintre numerele x, y, z sunt pare și unul impar, avem că $x^2 + y^2 + z^2$ este congruent modulo 8, fie cu $0 + 0 + 1 = 1$, fie cu $0 + 4 + 1 = 5$, fie cu $4 + 4 + 1 \equiv 1 \pmod 8$. Deci nici în acest caz nu poate avea loc egalitatea $x^2 + y^2 + z^2 = 8n + 7$. Am arătat astfel că orice număr natural de forma $8n + 7$ ($n \in \mathbf{N}$) nu se poate scrie ca suma a trei pătrate de numere naturale.

Presupunem acum că există $a \in \mathbf{N}^*$ și $n \in \mathbf{N}$ astfel încât $4^a(8n+7) = m$ se poate scrie ca suma a trei pătrate de numere naturale. În aceste condiții vom nota cu a_0 cel mai mic număr natural nenul pentru care există $n_0 \in \mathbf{N}$ astfel încât $4^{a_0}(8n_0+7)$ se poate scrie ca suma a trei pătrate de numere naturale:

$$4^{a_0}(8n_0+7) = x^2 + y^2 + z^2$$

cu $x,y,z \in \mathbf{N}$. Deoarece $4^{a_0}(8n_0+7)$ este număr par (deoarece $a_0 \in \mathbf{N}$, $a_0 \geq 1$), deducem că fie toate numerele x, y și z sunt pare, fie unul dintre ele este par iar celelalte două sunt impare. În ipoteza că toate numerele x, y, z sunt pare, există atunci numerele naturale x_1, y_1, z_1, astfel încât $x = 2x_1$, $y = 2y_1$ și $z = 2z_1$. Din egalitatea

$$4^{a_0}(8n_0+7) = x^2 + y^2 + z^2$$

deducem că

$$4^{a_0-1}(8n_0+7) = x_1^2 + y_1^2 + z_1^2.$$

Ținând cont de definiția numărului a_0 rezultă că $a_0 - 1 = 0$. Aceasta ar însemna că $8n_0 + 7 = x_1^2 + y_1^2 + z_1^2$, ceea ce este imposibil conform primei părți a acestei demonstrații. Mai rămâne de analizat cazul în care unul din umerele x, y, z este par iar celelalte două sunt impare. În acest caz

$$x^2 + y^2 + z^2 \equiv 2 \pmod 4$$

și cum $4^{a_0}\ 8n_0 + 7 \equiv 0 \pmod 4$, egalitatea

$$4^{a_0}(8n_0 + 7) = x^2 + y^2 + z^2$$

este imposibilă. Toate acestea termină demonstrația faptului că orice număr natural de forma $4^a(8n + 7)$ (unde a și n aparțin lui $\mathbf{N}$) nu se poate scrie ca suma a trei pătrate de numere naturale.

Vom demonstra că orice număr natural m, care nu este de forma $4^a(8n + 7)$ (unde $a, n \in \mathbf{N}$), se poate scrie ca suma a trei pătrate de numere naturale. Dacă prima implicație a teoremei lui Gauss nu necesită decât argumente privind congruențele, cea de a doua aduce în joc raționamente mai subtile; în special teorema lui Minkovski asupra corpului convex și teorema lui Dirichlet privind numerele prime dintr-o progresie aritmetică.

Este suficient să arătăm că oricare ar fi m, număr natural nenul, liber de pătrate, $m \neq 8n + 7$, $(\forall)\ n \in \mathbf{N}$, atunci m se poate scrie ca suma a trei pătrate de numere naturale [într-adevăr, dacă $b \in \mathbf{N}^*$, $b \neq 4^a\ (8n + 7)$, $(\forall)\ a,n \in \mathbf{N}$, atunci putem scrie pe b sub forma $b = m \cdot d^2$, unde m este un număr natural liber de pătrate și $d \in \mathbf{N}^*$. Dacă cumva $m = 8l + 7$ ($l \in \mathbf{N}$), atunci scriindu-l pe d sub forma $d = 2^a \cdot \beta$, unde $a, \beta \in \mathbf{N}$, β impar, atunci $b = (8l + 7) \cdot 4^a \cdot \beta^2 \cdot \beta$ fiind un număr natural impar, β^2 va fi congruent modulo 8 cu 1. Aceasta ar însemna că b se poate scrie sub forma $4^a\ (8n + 7)$, ceea ce nu se poate conform presupunerii făcute asupra lui b. Aceasta înseamnă că $m \neq 8l + 7$, $(\forall)\ l \in \mathbf{N}$, și în acest moment s-a justificat afirmația de mai sus și anume că este suficient să demonstrăm că orice număr natural, liber de pătrate, diferit de $8n + 7$, $(\forall)\ n \in \mathbf{N}$, se poate scrie ca suma a trei pătrate de numere naturale). În cele ce urmează vom deosebi două cazuri: primul va fi acela în care m este un număr natural, liber de pătrate, $m \equiv 3 \pmod 8$, iar al doilea va fi acela în care m este un număr natural, liber de pătrate, $m \equiv 1 \pmod 8$, sau $m \equiv 2 \pmod 8$, sau $m \equiv 5 \pmod 8$, sau $m \equiv 6 \pmod 8$. Aceste două cazuri epuizează toate posibilitățile în situația dată. Într-adevăr dacă $m \in \mathbf{N}$, m liber de pătrate, $m \neq 8n + 7$, $(\forall)\ n \in \mathbf{N}$, atunci m nu poate fi congruent modulo 8 decât cu 1, 2, 3, 5 sau 6 modulo 8. Dacă $m = 0$ atunci enunțul teopremei lui Gauss este evident adevărat: $m = 0^2 + 0^2 + 0^2$.

Cazul I : $m \in \mathbf{N}^*$, m liber de pătrate, $m \equiv 3 \pmod 8$.

În acest caz scriem $m = p_1 \cdot p_2 \cdot \ldots \cdot p_r$, unde $p_1, p_2 \ldots p_r$ sunt numere prime distincte, impare. Există un număr prim q care satisface următoarele condiții:

(1) $\left(\dfrac{-2q}{p_j}\right) = 1$, $(\forall)\ j = \overline{1,r}$;

(2) $q \equiv 1 \pmod 4$.

Pentru a justifica această afirmație să observăm că, deoarece $(p_i, p_j) = 1$, $(\forall)\ i,j = \overline{1,r}$, $i \neq j$ și $(p_j, 4) = 1$, $(\forall)\ j = \overline{1,r}$, atunci conform lemei chineze a resturilor (demonstrată în paragraful (II) al anexei) există un număr natural m_0 astfel încât $m_0 \equiv -2 \pmod{p_j}$, $(\forall)\ j = \overline{1,r}$ și $m_0 \equiv 1 \pmod 4$. Din

modul de alegere al numărului m_0 se vede imediat că $(m_0, 4m) = 1$. Pentru progresia aritmetică $\{m_0 + 4mk \mid k \in \mathbf{N}\}$ aplicăm teorema lui Dirichlet privitoare la numerele prime dintr-o progresie aritmetică (pentru care termenul inițial al progresiei și rația ei sunt două numere naturale prime între ele) și deducem că există un număr prim q de forma $q = m_0 + 4mk, k \in \mathbf{N}$. Ținând cont de proprietățile lui m_0, rezultă că $q \equiv 1 \pmod 4$ și $q \equiv -2 \pmod{p_j}$, $(\forall)\, j = \overline{1, r}$. În particular rezultă și faptul că $(q, 4m) = 1$.

Ținând cont de condițiile precedente putem calcula simbolul Legendre

$$\left(\frac{-2q}{p_j}\right) = \left(\frac{-2}{p_j}\right)\left(\frac{q}{p_j}\right) = \left(\frac{-2}{p_j}\right)\left(\frac{-2}{p_j}\right) = 1$$

$(\forall)\ j = \overline{1,r}$. În acest moment s-a justificat existența numărului prim q care satisface condițiile (1) și (2). Vom arăta următoarea egalitate:

$$(3) \qquad \left(\frac{-m}{q}\right) = 1.$$

Într-adevăr înmulțind egalitățile (1) pentru j de la 1 la r, obținem că

$$1 = \prod_{j=1}^{r}\left(\frac{-2q}{p_j}\right) = \prod_{j=1}^{r}\left(\frac{-1}{p_j}\right)\cdot\prod_{j=1}^{r}\left(\frac{2}{p_j}\right)\cdot\prod_{j=1}^{r}\left(\frac{q}{p_j}\right) =$$

$$= \left(\frac{-1}{m}\right)\cdot\left(\frac{2}{m}\right)\cdot\prod_{j=1}^{r}\left[\left(\frac{p_j}{q}\right)(-1)^{\frac{p_j-1}{2}\cdot\frac{q-1}{2}}\right] =$$

$$= \left(\frac{-1}{m}\right)\cdot\left(\frac{2}{m}\right)\prod_{j=1}^{r}\left(\frac{p_j}{q}\right) = \left(\frac{-1}{m}\right)\cdot\left(\frac{2}{m}\right)\cdot\left(\frac{m}{q}\right) =$$

$$= (-1)^{\frac{m-1}{2}}\cdot(-1)^{\frac{m^2-1}{8}}\left(\frac{m}{q}\right) = (-1)\cdot(-1)\cdot\left(\frac{m}{q}\right) = \left(\frac{m}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{m}{q}\right) = \left(\frac{-m}{q}\right).$$

În egalitățile precedente am ținut cont de proprietățile simbolurilor lui Legendre și Iacobi, de legea reciprocității pătratelor a lui Gauss-Legendre [dacă a și b sunt două numere prime impare, distincte, atunci $\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$], de faptul că $m \equiv 3 \pmod 8$ [ceea ce înseamnă că numerele naturale $\frac{m-1}{2}$ și $\frac{m^2-1}{8}$ sunt

impare] și în afârșit de faptul că $q \equiv 1 \pmod 4$ [ceea ce ne asigură că $\left(\frac{-1}{q}\right) = 1$].

Relația 3) este astfel demonstrată. Semnificația acestei relații este aceea că există un număr întreg b astfel încât $b^2 \equiv -m \pmod q$. În plus b poate fi ales impar [dacă cumva b este par atunci considerăm numărul $q - b$ care este evident impar și $(q-b)^2 \equiv b^2 \equiv -m \pmod q$]. Există (conform alegerii lui b) un număr întreg h_1 cu proprietatea că:

(4) $b^2 - qh_1 = -m.$

Dacă în egalitatea (4) trecem la congruența modulo 4 obținem, ținând cont că b e impar (deci $b^2 \equiv 1 \pmod 4$), $q \equiv 1 \pmod 4$ și $m \equiv 3 \pmod 8$, următoarea relație: $1 - h_1 \equiv 1 \pmod 4$ și $4 \mid h_1$. Ținând cont de aceasta precum și de identitatea (4) rezultă că există $h \in \mathbf{Z}$ astfel încât:

(5) $b^2 - 4qh = -m.$

Fie a, b, x, y, u numere întregi astfel încât $(a, b) = 1$, $x^2 \equiv u \pmod a$ și $y^2 \equiv u \pmod b$. Deoarece $(a,b) = 1$ există $k, l \in \mathbf{Z}$ astfel încât $al - bk = y - x$ [știm că există $l_1, k_1 \in \mathbf{Z}$ cu proprietatea că $al_1 - bk_1 = 1$; luăm $l = l_1(y-x)$ și $k = k_1(y-x)$]. Fie $z = x + al = y + bk$; evident $z \in \mathbf{Z}$, $z^2 \equiv x^2 \equiv u \pmod a$ și $z^2 \equiv y^2 \equiv u \pmod b$. Deoarece $(a,b) = 1$, din cele de mai sus rezultă că $z^2 \equiv u \pmod{a \cdot b}$. Acest argument împreună cu relațiile (1) și cu un raționament prin recurență permit găsirea unui număr întreg c astfel încât $c^2 \equiv -2q \pmod m$. Ținând cont că $(2q, m) = 1$, rezultă că $(c, m) = 1$. Există deci un număr întreg t cu proprietatea că $t \cdot c \equiv 1 \pmod m$. Ținând cont de congruențele $c^2 \equiv (-2q) \pmod m$ și $t \cdot c \equiv 1 \pmod m$ se deduce că numărul întreg t satisface congruența:

(6) $t^2 \cdot (-2q) \equiv 1 \pmod m.$

Fie $f: \mathbf{R}^3 \to \mathbf{R}^3$ următoarea aplicație liniară:

$$(7)\quad \begin{cases} f(x,y,z) = (R,S,T) \\ R = 2tqx + tby + m \cdot z \\ S = \sqrt{2q}\, x + \dfrac{b}{\sqrt{2q}}\, y \\ T = \sqrt{\dfrac{m}{2q}}\, y. \end{cases}$$

Definim mulțimile X și X_1 din $\mathbf{R}^3$ prin condițiile:

$$(8)\quad \begin{cases} X = \left\{(R,S,T) \in \mathbf{R}^3 \,\middle|\, R^2 + S^2 + T^2 < 2m\right\} \\ X_1 = \left\{(x,y,z) \in \mathbf{R}^3 \,\middle|\, f(x,y,z) \in X\right\} = f^{-1}(X). \end{cases}$$

Este evident că X este o mulțime simetrică (dacă $\alpha \in X$ atunci $-\alpha \in X$), convexă, măsurabilă Lebesgue și $v(X)=\frac{4}{3}\pi(2m)^{\frac{3}{2}}$ (v este măsura Lebesgue din $\mathbf{R}^3$). Mărginirea lui X este la fel de evidentă (X este o bilă în $\mathbf{R}^3$ cu centrul în origine și raza $\sqrt{2m}$). Determinantul transformării liniare f este egal cu:

$$\begin{vmatrix} 2tq; & tb; & m \\ \sqrt{2q}; & \frac{b}{\sqrt{2q}}; & 0 \\ 0; & \sqrt{\frac{m}{2q}}; & 0 \end{vmatrix} = -\sqrt{\frac{m}{2q}} \begin{vmatrix} 2tq; & m \\ \sqrt{2q}; & 0 \end{vmatrix} = \sqrt{\frac{m}{2q}} \cdot m\sqrt{2q} = m^{\frac{3}{2}} \neq 0$$

(aceasta înseamnă că f este o transformare bijectivă; are deci sens f^{-1} care este și ea o aplicație liniară bijectivă). Deoarece o mulțime convexă, simetrică și mărginită este dusă printr-o aplicație liniară într-o mulțime având aceleași calități, din faptul că $X_1 = f^{-1}(X)$ deducem că X_1 este mărginită, simetrică și convexă. Folosind formula schimbării de variabilă deducem că X_1 este măsurabilă Lebesgue și $v(X) = v(X_1) \cdot m^{\frac{3}{2}}$. Ținând cont că

$$v(X)=\frac{4}{3}\pi(2m)^{\frac{3}{2}}$$

rezultă că

$$v(X_1)=\frac{2^{\frac{7}{2}}\cdot\pi}{3}.$$

Vom considera rețeaua completă din $\mathbf{R}^3$ (vezi definiția din anexă precum și semnificația termenilor folosiți) $\mathcal{R}=\mathbf{Z}^3$. Paralelipipedul fundamental asociat lui $\mathcal{R}$ este $[0, 1) \times [0, 1) \times [0, 1)$ și are evident măsura Lebesgue egală cu $\Delta = 1$.

Deoarece

$$v(X_1)=\frac{\pi\cdot 2^{\frac{7}{2}}}{3} > 2^{\frac{7}{2}} > 2^3 = 2^3 \cdot \Delta,$$

folosind teorema lui Minkovski asupra corpului convex aplicată lui X_1 și $\mathcal{R}$, rezultă că există $(x_1, y_1, z_1) \in \mathbf{Z}^3$, $(x_1, y_1, z_1) \neq (0, 0, 0)$, astfel încât $(x_1, y_1, z_1) \in X_1$ (aceasta înseamnă că $R_1^2 + S_1^2 + T_1^2 < 2m$, unde R_1, S_1, T_1 se obțin din formula (7) înlocuind x, y și z, cu x_1, y_1 și z_1).

Calculând expresia $R_1^2 + S_1^2 + T_1^2$ obținem că

$$R_1^2 + S_1^2 + T_1^2 = R_1^2 + \left(\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1\right)^2 + \left(\sqrt{\frac{m}{2q}}y_1\right)^2 =$$

$$= R_1^2 + \frac{1}{2q}\left(2qx_1 + by_1\right)^2 + \frac{m}{2q}y_1^2 =$$

$$= R_1^2 + 2qx_1^2 + 2bx_1y_1 + \frac{\left(b^2+m\right)y_1^2}{2q} =$$

$$= R_1^2 + 2qx_1^2 + 2bx_1y_1 + 2hy_1^2 = R_1^2 + 2v,$$

unde R_1 este un număr întreg ($R_1 = 2tqx_1 + tby_1 + mz_1$) iar v este dat de formula:

(9) $\quad v = q\,x_1^2 + b\,x_1y_1 + h\,y_1^2$.

În egalitățile de mai sus am ținut cont de relația (5) care spune că $b^2 + m = 4qh$. Din formula (9) rezultă că $v \in \mathbf{Z}$; cum însă $2v = S_1^2 + T_1^2 \geq 0$, deducem că $v \in \mathbf{N}$.

(10) $\quad R_1^2 + S_1^2 + T_1^2 = R_1^2 + 2v;\ R_1^2 + S_1^2 + T_1^2 \in \mathbf{N}$.

Explicitându-l pe R_1 și trecând la o congruență modulo m în egalitatea (10) obținem că

$$R_1^2 + 2v = (2tq\,x_1 + tb\,y_1 + m\,z_1)^2 + \frac{1}{2q}\,(2q\,x_1 + by_1)^2 + \frac{my_1^2}{2q} =$$

$$= a \cdot m + t^2(2qx_1 + by_1) + \frac{\left(2qx_1 + by_1\right)^2}{2q} + \frac{my_1^2}{2q} =$$

$$= \frac{2q \cdot a \cdot m + \left(2qx_1 + by_1\right)^2\left(2qt^2 + 1\right) + my^2}{2q} \equiv 0 \pmod{m}.$$

Aceasta se întâmplă deoarece ultima fracție este un număr întreg al cărei numărător se divide cu m, iar $(m, 2q) = 1$. Din formula (6) se obține că $m \mid (2q\,t^2 + 1)$, deci într-adevăr numărătorul fracției precedente se divide cu m. Să mai spunem că aici s-a notat $a = m\,z_1^2 + 2z_1(2tq\,x_1 + tb\,y_1)$ pentru a ușura scrierea. Calculul precedent ne-a arătat că:

(11) $\quad R_1^2 + 2v \equiv 0 \pmod{m}$.

Deoarece $(x_1, y_1, z_1) \neq (0, 0, 0)$, $(R_1, S_1, T_1) = f(x_1, y_1, z_1)$ și f este o aplicație liniară bijectivă, deducem că $(R_1, S_1, T_1) \neq (0, 0, 0)$; aceasta înseamnă că $0 < R_1^2 + S_1^2 + T_1^2$. Deoarece $(x_1, y_1, z_1) \in X_1$, are loc și inegalitatea

$R_1^2 + S_1^2 + T_1^2 < 2m$. Aceste două din urmă inegalități împreună cu relațiile (10) și (11) ne conduc la următoarea egalitate:

(12) $R_1^2 + 2v = m; \quad v \in \mathbf{N}$ și $R_1 \in \mathbf{Z}$.

Vom arăta în cele ce urmează că orice număr prim impar p pentru care $p^{2n+1} \mid v$ și $p^{2n+2} \nmid v$ ($n \in \mathbf{N}$) trebuie să fie de forma $4k+1$ ($k \in \mathbf{N}$). Aceasta împreună cu propoziția 2 din paragraful (I) al anexei ne arată că $2 \cdot v$ se poate scrie ca suma a doua pătrate de numere naturale. Folosind relația (12) deducem că m se poate scrie ca suma a trei pătrate de numere naturale [dacă cumva $R_1 < 0$ înlocuim pe R_1 cu $(-R_1)$ ținând cont că $R_1 = (-R_1)^2$]. Deci teorema lui Gauss ar fi demonstrată în cazul în care $m \equiv 3 \pmod 8$.

Dacă p este ca mai sus (p prim impar, $p^{2n+1} \mid v$, $p^{2n+2} \nmid v$, $n \in \mathbf{N}$) vom deosebi două subcazuri; primul este acela în care $p \nmid m$, iar al doilea este acela în care $p \mid m$. Să presupunem întâi că $p \nmid m$. Din relația (12) deducem atunci că:

(13) $\left(\frac{m}{p}\right) = 1.$

Dacă cumva $p = q$, atunci din identitatea (5) deducem că $\left(\frac{-m}{p}\right) = 1$, ceea ce împreună cu relația (13) ne conduce la concluzia că $\left(\frac{-1}{p}\right) = 1$. Cum

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1,$$

deducem că numărul prim p trebuie să fie de forma $4k+1$ ($k \in \mathbf{N}$), ceea ce trebuia arătat. În continuare vom analiza situația în care $p \neq q$. Din calculul care precede formula (9) rezultă că are loc următoarea egalitate:

(14) $4qv = (2q\,x_1 + b\,y_1)^2 + m\,y_1^2$.

Deoarece $p \neq q$ și $p \neq 2$, din identitatea (14) deducem că există $e, f \in \mathbf{Z}$ cu proprietatea că $p^{2n+1} \mid e^2 + mf^2$ și $p^{2n+2} \nmid e^2 + mf^2$. Aici $e = 2q\,x_1 + b\,y_1$ și $f = y_1$. Fie $a \in \mathbf{N}$ cu proprietatea că $p^a \mid (e, f)$ și $p^{a+1} \nmid (e,f)$; există atunci $e_1, f_1 \in \mathbf{Z}$ astfel încât $e = e_1 \cdot p^a$, $f = f_1 \cdot p^a$ și $p \nmid (e_1, f_1)$.

Din faptul că $p^{2a} \mid (e^2 + mf^2)$, $p^{2n+1} \mid (e^2 + mf^2)$ și $p^{2n+2} \nmid (e^2 + mf^2)$ rezultă că $2a \leq 2n + 1$, apoi $2a < 2n + 1$ și $p \mid (e_1^2 + mf_1^2)$. Cum $p \nmid (e_1, f_1)$ și $p \nmid m$ obținem că $p \nmid e_1$ și $p \nmid f_1$. Deoarece $p \nmid f_1$ există $f_2 \in \mathbf{Z}$ astfel încât $f_1 \cdot f_2 \equiv 1 \pmod p$. Faptul că $p \mid e^2 + mf_1^2$ implică congruența $e_1^2 \equiv -mf_1^2$

(mod p) și înmulțind această din urmă congruență cu f_2^2 obținem că $(e_1 \cdot f_2)^2 \equiv -m \pmod{p}$. Deoarece $p \nmid m$ aceasta înseamnă că:

(15) $\left(\frac{-m}{p}\right)=1.$

Combinând relațiile (13) și (15) rezultă că $\left(\frac{-1}{p}\right)=1$; cum s-a văzut ceva mai înainte aceasta înseamnă că numărul prim p este de forma $4k+1$ ($k \in \mathbf{N}$), ceea ce trebuia arătat.

Vom analiza în continuare cel de al doilea subcaz și anume acela în care $p \mid m$.

Calculul care precede formula (9) împreună cu egalitatea (12) permit scrierea următoarei identități:

(16) $R_1^2+\frac{1}{2q}\left[\left(2qx_1+by_1\right)^2+my_1^2\right]=m.$

Deoarece $p \mid v$ și $p \mid m$, din egalitatea $R_1^2 + 2v = m$ deducem că $p \mid R_1^2$ și deci $p \mid R_1$ (p este număr prim). Înmulțim relația (16) cu $2q$ și obținem:

(17) $2q \cdot R_1^2 + (2qx_1 + by_1)^2 + my_1^2 = 2q \cdot m.$

Cum $p \mid R_1$, $p \mid m$, din formula (17) deducem că $p \mid (2qx_1 + by_1)^2$ și că $p \mid (2qx_1 + by_1)$. Împărțim relația (17) cu p și trecem la o congruență modulo p; ținând cont că $\frac{R_1^2}{p}$ și $\frac{(2qx_1+by_1)^2}{p}$ sunt numere naturale congruente cu 0 modulo p obținem că

$$\frac{m}{p}y_1^2 \equiv 2q \cdot \frac{m}{p} \pmod{p}.$$

Cum m este un număr natural liber de pătrate și $p \mid m$ deducem că $\left(p,\frac{m}{p}\right)=1$; ținând cont de această observație, din ultima congruență rezultă că $y_1^2 \equiv 2q \pmod{p}$. Aceasta înseamnă că are loc egalitatea $\left(\frac{2q}{p}\right)=$. Deoarece $p \mid m$, din relațiile (1) se deduce că $\left(\frac{-2q}{p}\right)=1$. Combinând aceste ultime două egalități se

obține că $\left(\frac{-1}{p}\right)=1$; după cum am mai observat aceasta implică faptul că p este de forma $4k+1$ ($k \in \mathbf{N}$). În acest moment cazul I este demonstrat.

Cazul II: $m \in \mathbf{N}^*$, m liber de pătrate, $m \equiv 1, 2, 5$ sau $6 \pmod 8$.

Se alege q, un număr prim care să satisfacă următoarele condiții: $\left(\frac{-q}{p_j}\right)=1$ $(\forall)$ p_j un divizor prim impar al lui m, $q \equiv 1 \pmod 4$ și în plus dacă m este par $\left(\frac{-2}{q}\right)=(-1)^{\frac{m_1-1}{2}}$, unde $m = 2m_1$.

[În acest caz m_1 este un număr natural impar, deoarece $4 \nmid m$. Condiția $\left(\frac{-2}{q}\right)=(-1)^{\frac{m_1-1}{2}}$, se mai scrie în modul următor: $q \equiv 1 \pmod 8$, dacă $m_1 = 4k+1$ și $q \equiv 5 \pmod 8$, dacă $m_1 = 4k+3$ ($k \in \mathbf{N}$). Am ținut cont în transcrierea condiției precedente de faptul că se impusese anterior ca q că fie congruent cu 1 modulo 4]. Existența numărului prim q satisfăcând condițiile precedente se probează în același fel ca și în cazul I (se utilizează lema chineză a resturilor precum și teorema lui Dirichlet privitoare la numerele prime dintr-o progresie aritmetică în care rația și termenul inițial al progresiei sunt două numere naturale prime între ele). Dacă m este impar și $m = \prod_{j=1}^{r} p_j$ (unde $p_1, p_2, \ldots, p_r$ sunt numere prime impare, distincte) atunci ținând cond de condițiile precedente se deduce că

$$1 = \prod_{j=1}^{r}\left(\frac{-q}{p_j}\right) = \prod_{j=1}^{r}\left(\frac{-1}{p_j}\right)\cdot\prod_{j=1}^{r}\left(\frac{q}{p_j}\right)=\left(\frac{-1}{m}\right)\prod_{j=1}^{r}\left[\left(\frac{p_j}{q}\right)(-1)^{\frac{p_j-1}{2}\cdot\frac{q-1}{2}}\right]=$$

$$=(-1)^{\frac{m-1}{2}}\cdot\prod_{j=1}^{r}\left(\frac{p_j}{q}\right)=\left(\frac{m}{q}\right)=\left(\frac{-m}{q}\right)$$

S-a ținut cont mai sus că $q \equiv 1 \pmod 4$ și că $\frac{m-1}{2}$ este un număr natural par în cazul în care $m \equiv 1$ sau $5 \pmod 8$. Vezi și demonstrația relației (3). Dacă m este par, atunci $m = 2m_1 = 2\prod_{j=1}^{r} p_j$ (unde $p_1, p_2, \ldots, p_r$ sunt numere prime impare, distincte). Ținând cont de modul de definire al lui q rezultă că

$1=\prod_{j=1}^{r}\left(\frac{-q}{p_j}\right)=\left(\frac{-1}{m_1}\right)\prod_{j=1}^{r}\left(\frac{p_j}{q}\right)=(-1)^{\frac{m_1-1}{2}}\left(\frac{m_1}{q}\right)=(-1)^{\frac{m_1-1}{2}}\left(\frac{2m_1}{q}\right)\left(\frac{2}{q}\right)=(-1)^{\frac{m_1-1}{2}}\left(\frac{m}{q}\right)(-1)^{\frac{m_1-1}{2}}=$

$=\left(\frac{m}{q}\right)=\left(\frac{-m}{q}\right)$. Deci în amândouă cazurile are loc egalitatea (3) și anume

$\left(\frac{-m}{q}\right)=1$. Există deci $b, h \in \mathbf{Z}$ astfel încât $b^2 - qh = -m$. În același mod în care s-a demonstrat relația (6) se arată că există $t \in \mathbf{Z}$ astfel încât $t^2 \cdot (-q) \equiv 1 \pmod{p_j}$, $(\forall)\, p_j$ un număr prim impar care-l divide pe m. Dacă m este par atunci pe t îl alegem în plus să fie un număr impar (dacă cumva acel t găsit mai sus este par îl înlocuim cu $m_1 - t$, unde $m_1 = \prod_{j=1}^{r} p_j$, $m = 2m_1, p_1, p_2, \ldots, p_r$ sunt numere prime impare, distincte). În locul aplicației liniare f se va considera $f_1: \mathbf{R}^3 \to \mathbf{R}^3$ o aplicație liniară, într-un mod asemănător cu formula (7) de definire a funcției f. Și anume $f_1(x, y, z) = (R, S, T)$ unde R, S și T sunt definite astfel:

$$(7')\quad \begin{cases} R = tqx + tby + mz \\ S = \sqrt{q}x + \dfrac{b}{\sqrt{q}}y \\ T = \sqrt{\dfrac{m}{q}}y, \end{cases}$$

Mulțimile X și X_1 sunt definite analog cu formula (8) și anume:

$$(8')\quad \begin{cases} X = \{(R,S,T) \in \mathbf{R}^3 \mid R^2 + S^2 + T^2 < 2m\} \\ X_1 = \{(x,y,z) \in \mathbf{R}^3 \mid f_1(x,y,z) \in X\}. \end{cases}$$

Raționamentul curge în continuare exact ca și în cazul I, cu următoarele mici modificări. Determinantul transformării liniare f_1, este egal tot cu $m^{\frac{3}{2}}$,

$$v(X) = \frac{4}{3}\pi(2m)^{\frac{3}{2}}$$

și

$$v(X_1) = \frac{2^{\frac{7}{2}} \cdot \pi}{3} > 2^3.$$

Aplicând teorema lui Minkovski se deduce existența lui $(x_1, y_1, z_1) \neq (0, 0, 0)$ astfel încât $(x_1, y_1, z_1) \in \mathbf{Z}^3 \cap X_1$; fie

$$(R_1, S_1, T_1) = f_1(x_1, y_1, z_1) \neq (0, 0, 0).$$

$$R_1^2 + S_1^2 + T_1^2 = R_1^2 + + \frac{1}{q}\left[(qx_1 + by_1)^2 + my_1^2\right] = R_1^2 + v,$$

unde $R_1 \in \mathbf{Z}$, $v \in \mathbf{N}$,

$$v = qx_1^2 + 2bx_1y_1 + hy_1^2.$$

$$R_1^2 + v = a \cdot m + t^2(qx_1 + by_1)^2 + \frac{1}{q}(qx_1 + by_1)^2 + \frac{my_1^2}{q} =$$

$$= \frac{amq + (t^2q+1)(qx_1 + by_1)^2 + my_1^2}{q} \equiv 0 \pmod{m},$$

(deoarece ultima fracție este un număr natural al cărei numărător se divide cu m, iar $(m, q) = 1$ conform alegerii lui q. Din modul în care a fost ales t se deduce că $p_j \mid (t^2q + 1)$, $(\forall)\, p_j$ un divizor prim impar al lui m. Dacă în plus m este par atunci $2 \mid t^2 \cdot q + 1$ fiindcă t a fos ales impar iar q este evident impar. Cum m e liber de pătrate, din cele de mai sus rezultă că $m \mid (t^2q + 1)$, deci într-adevăr numărătorul fracției precedente se divide cu m). Cum $0 < R_1^2 + v < 2m$; $R_1^2 + v \in \mathbf{N}$ și $R_1^2 + v \equiv 0 \pmod{m}$, se deduce că $R_1^2 + v = m$. Demonstrația faptului că orice număr prim impar pentru care $p^{2n+1} \mid v$ și $p^{2n+2} \nmid v$ ($n \in \mathbf{N}$), trebuie să fie de forma $4k + 1$ ($k \in \mathbf{N}$) este identică cu cea din cazul I. De aici se deduce (folosind din nou propoziția 2 din paragraful I al anexei) că v se scrie ca suma a două pătrate de numere naturale și deci m se scrie ca suma a trei pătrate de numere naturale, ceea ce trebuia demonstrat.

Se văd acum și motivele pentru care apărea 2 în diversele condiții din cazul I. El a fost introdus pentru a se asigura valabilitatea relației (3) : $\left(\frac{-m}{q}\right) = 1$.

Într-adevăr dacă în loc de (1) s-ar fi cerut doar că $\left(\frac{-q}{p_j}\right) = 1$, atunci

$$\left(\frac{-m}{q}\right) = \left(\frac{-1}{m}\right) = = (-1)^{\frac{m-1}{2}} = -1 \ (m \equiv 3 (\text{mod } 8)).$$

Prin introducerea acelui $2\left[\left(\frac{-2q}{p_j}\right) = 1\right]$ s-a obținut că $\left(\frac{-m}{q}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right) =$

$= (-1)^{\frac{m-1}{2}} \cdot (-1)^{\frac{m^2-1}{2}} = (-1)(-1) = 1$ (deoarece $m \equiv 3 \pmod 8$, m liber de pătrate).

ANEXĂ
(Teorema lui Gauss)

I. Fie $e_1, e_2, ..., e_n$ vectori liniar independenți din $\mathbf{R}^n$;

$$\mathcal{R} = \{y \in \mathbf{R}^n \mid y = \sum_{i=1}^{n} \alpha_i e_i, \alpha_i \in \mathbf{Z}, (\forall) i = \overline{1,n}\},$$

$$T = \{y \in \mathbf{R}^n \mid y = \sum_{i=1}^{n} \alpha_i e_i,\ \alpha_i \in [0,1),\ (\forall) i = \overline{1,n}\}.$$

$\mathcal{R}$ se numește *rețea completă*, iar T se numește *paralelipipedul fundamental asociat rețelei* $\mathcal{R}$.

Propoziția 1: *Cu notațiile precedente avem că*

$$\mathbf{R}^n = \bigcup_{z \in \mathcal{R}} (T + z) \text{ și că } (T + z_1) \cap (T + z_2) = \varnothing$$

$(\forall)\ z_1 \neq z_2$, z_1 și z_2 *aparținând lui* $\mathcal{R}$.

Demonstrație: Incluziunea $\bigcup_{z \in \mathcal{R}} (T + z) \subseteq \mathbf{R}^n$ este evidentă. Pentru a demonstra cealaltă incluziune fie $x \in \mathbf{R}^n$. Cum $e_1, e_2, ..., e_n$ formează o bază a spațiului vectorial $\mathbf{R}^n$, deducem că există $\gamma_1, ..., \gamma_n$ numere reale astfel încât $x = \sum_{i=1}^{n} \gamma_i e_i$. Dacă scriem $\gamma_i = m_i + \alpha_i$, unde $m_i \in \mathbf{Z}$ și $\alpha_i \in [0, 1)$, $(\forall)\ i = \overline{1,n}$ ($m_i = [\gamma_i]$ și $\alpha_i = \{\gamma_i\}$) atunci $x = \sum_{i=1}^{n} m_i e_i + \sum_{i=1}^{n} \alpha_i e_i$. Cum $\sum_{i=1}^{n} m_i e_i \in \mathcal{R}$ și $\sum_{i=1}^{n} \alpha_i e_i \in T$, prima parte a enunțului este demonstrată. Pentru cea de a doua parte a propoziției să presupunem că există $z_1, z_2 \in \mathcal{R}$, $z_1 \neq z_2$ astfel încât $(T + z_1) \cap (T + z_2) \neq \varnothing$. Există deci $\alpha_i, \beta_i \in [0, 1)$ cu proprietatea că

$$z_1 + \sum_{i=1}^{n} \alpha_i e_i = z_2 + \sum_{i=1}^{n} \beta_i e_i.$$

Aceasta înseamnă că există niște numere întregi m_i ($i = \overline{1,n}$) astfel încât

$$\sum_{i=1}^{n} m_i e_i = \sum_{i=1}^{n} (\beta_i - \alpha_i)\, e_i,$$

unde $z_1 - z_2 = \sum_{i=1}^{n} m_i e_i$; $z_1 - z_2 \in \mathcal{R}$, deoarece z_1 și z_2 aparțin lui $\mathcal{R}$. Din această egalitate deducem că $\beta_i - \alpha_i = m_i$, $(\forall)\ i = 1,n$. Cum $(\beta_i - \alpha_i) \in (-1,1)$ și $m_i \in \mathbf{Z}$, $(\forall)\ i = \overline{1,n}$, din cele de mai sus rezultă că $m_i = 0$, $(\forall)\ i = 1,n$ și deci că $z_1 = z_2$. S-a ajuns la o contradicție; aceasta înseamnă că presupunerea făcută a fost falsă și deci enunțul propoziției 1 este adevărat.

Să notăm în cele ce urmează cu $\Delta = v(T)$, unde v este măsura Lebesgue din $\mathbf{R}^n$. Dacă notăm cu f următoarea aplicație liniară pe $\mathbf{R}^n$

$$f(x_1, x_2, ..., x_n) = \left(\sum a_{ij} x_j\right)_{i=\overline{1,n}},$$

$(\forall)\ x_l \in \mathbf{R}$, $l = \overline{1,n}$, unde $e_i = (a_{1i}, a_{2i}, ..., a_{n,i})$, $(\forall)\ i = \overline{1,n}$ atunci motivația faptului că T este o mulțime măsurabilă Lebesgue este aceea că $T = f(A)$, A fiind următoarea submulțime a lui $\mathbf{R}^n$:

$$A = \{(x_1, x_2, ..., x_n) \in \mathbf{R}^n \mid x_i \in [0, 1),\ (\forall)\ i = \overline{1,n}\}.$$

Cum $v(A) = 1$, din cele de mai sus se deduce folosind formula schimbării de variabilă că

$$v(T) = \int_T dv = \int_{f(A)} dv = \int_A |\det(a_{ij})_{i,j=\overline{1,n}}|\, dv = |\det(a_{ij})_{i,j=\overline{1,n}}|.$$

Să mai observăm și faptul că numărul $D = v(T)$ nu depinde decât de $\mathcal{R}$ și nu depinde de baza $e_1, e_2, ..., e_n$ a $\mathbf{Z}$-modulului $\mathcal{R}$. Într-adevăr dacă $f_1, f_2, ..., f_n$ este o altă bază a $\mathbf{Z}$-modulului liber $\mathcal{R}$, atunci există numerele întregi $b_{ij} (i,j = \overline{1,n})$ astfel încât $f_i = \sum_{j=1}^{n} b_{ij} e_j$. În plus, deoarece $e_1, e_2, ..., e_n$ și $f_1, f_2, ..., f_n$ sunt $\mathbf{Z}$-baze ale lui $\mathcal{R}$, modulul determinantului matricii $(b_{ij})_{i,j=\overline{1,n}}$ este egal cu 1.

Dacă

$$T' = \{x \in \mathbf{R}^n \mid x = \sum_{i=1}^{n} \alpha_i f_i,\ \alpha_i \in [0, 1)\ (\forall)\ i = \overline{1,n}\},$$

atunci folosind din nou formula schimbării de variabilă rezultă că $v(T') = |\det(b_{ij})_{i,j=\overline{1,n}}| \cdot v(T) = v(T)$. Aceasta justifică observația făcută mai înainte și anume că Δ nu depinde decât de $\mathcal{R}$.

Teorema 1 (teorema lui Minkovski asupra corpului convex). *Dacă $\mathcal{R}$, T și Δ au semnificațiile precizate mai sus, iar $X \subseteq \mathbf{R}^n$ este o mulțime mărginită, convexă și simetrică (aceasta înseamnă că dacă $x \in X$*

atunci și $(-x) \in X$), *astfel încât* $v(X) > 2^n \cdot \Delta$ *atunci mulțimea* X *conține un punct al lui* $\mathcal{R}$, *diferit de origine.*

Demonstrație: Se știe că orice mulțime convexă și mărginită este măsurabilă Jordan și Lebesgue; de aceea în enunțul de mai sus nu s-a impus ca X să fie o mulțime măsurabilă Lebesgue (acest lucru fiind inutil după cum s-a observat mai înainte).

Să demonstrăm întâi următoarea afirmație: dacă Y este o mulțime mărginită, măsurabilă Lebesgue, astfel încât $(Y + z_1) \cap (Y + z_2) = \emptyset$, $(\forall)\ z_1 \neq z_2$, z_1, $z_2 \in \mathcal{R}$, atunci $v(Y) \leq \Delta$.

Din propoziția 1 știm că

$$\mathbf{R}^n = \bigcup_{z \in \mathcal{R}} (T + z) = \bigcup_{z \in \mathcal{R}} (T - z)$$

și că

$$(T - z_1) \cap (T - z_2) = \emptyset,$$

$(\forall)\ z_1, z_2 \in \mathcal{R}$, $z_1 \neq z_2$. Folosind aceste observații precum și proprietățile măsurii Lebesgue deducem că

$$v(Y) = v(Y \cap \mathbf{R}^n) = v\left(Y \cap \left(\bigcup_{z \in \mathcal{R}} (T - z)\right)\right) =$$

$$= v\left(\bigcup_{z \in \mathcal{R}} \left(Y \cap (T - z)\right)\right) = \sum_{z \in \mathcal{R}} v\left(Y \cap (T - z)\right)$$

($\mathcal{R}$ este o mulțime numărabilă). Cum translatata mulțimii $Y \cap (T - z)$ cu vectorul z este mulțimea $(Y + z) \cap T$ și cum $v(B + b) = v(B)$ oricare ar fi $b \in \mathbf{R}^n$ și $B \subseteq \mathbf{R}^n$ o mulțime măsurabilă Lebesgue, deducem că

$$v(Y) = \sum_{z \in \mathcal{R}} v\left(Y \cap (T - z)\right) = \sum_{z \in \mathcal{R}} v\left((Y + z) \cap T\right) =$$

$$v\left(\bigcup_{z \in \mathcal{R}} \left((Y + z) \cap T\right)\right) = v\left(\left(\bigcup_{z \in \mathcal{R}} (Y + z)\right) \cap T\right) \leq v(T) = \Delta.$$

Pentru egalitatea

$$\sum_{z \in \mathcal{R}} v\left((Y + z) \cap T\right) = = v\left(\bigcup_{z \in \mathcal{R}} \left((Y + z) \cap T\right)\right),$$

am folosit faptul că

$$((Y + z_1) \cap T) \cap ((Y + z_2) \cap T) \subseteq (Y + z_1) \cap (Y + z_2) = \emptyset,$$

$(\forall)\ z_1, z_2 \in \mathcal{R}$, cu $z_1 \neq z_2$, deci

$$((Y + z_1) \cap T) \cap ((Y + z_2) \cap T) = \emptyset,$$

$(\forall)\, z_1, z_2 \in \mathcal{R}\ z_1 \neq z_2$. Cum $\nu(\beta \cdot B) = \beta^n \cdot \nu(B)\ (\forall)\ \beta \in \mathbf{R}_+$ și $(\forall)\ B \subseteq \mathbf{R}^n$, B fiind o mulțime măsurabilă Lebesgue, rezultă că ν

$$\nu\left(\frac{1}{2}X\right) = \frac{1}{2^n}\nu(X) > \Delta$$

(ultima inegalitate se datorează ipotezei teoremei). Dacă cumva

$$\left(\frac{1}{2}X + z_1\right) \cap \left(\frac{1}{2}X + z_2\right) = \varnothing,$$

$(\forall)\, z_1, z_2 \in \mathcal{R}$, $z_1 \neq z_2$ atunci prima parte a demonstrației arată că $\nu\left(\frac{1}{2}X\right) \leq \Delta$, ceea ce contrazice inegalitatea $\nu\left(\frac{1}{2}X\right) > \Delta$ obținută mai sus. Există deci $z_1 \neq z_2$, $z_1, z_2 \in \mathcal{R}$ astfel încât

$$\left(\frac{1}{2}X + z_1\right) \cap \left(\frac{1}{2}X + z_2\right) \neq \varnothing.$$

Aceasta înseamnă că există x_1 și x_2, două puncte din X cu proprietatea că

$$\frac{1}{2}x_1 + z_1 = \frac{1}{2}x_2 + z_2.$$

Faptul că X este o mulțime simetrică față de origine ne asigură că punctul $(-x_2)$ aparține lui X. Folosind și convexitatea mulțimii X rezultă că punctul $\frac{1}{2}x_1 + \frac{1}{2}(-x_2)$ aparține și el mulțimii $X\left(\frac{1}{2} + \frac{1}{2} = 1\right)$. Deci

$$\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X \cap \mathcal{R}$$

și în plus

$$\frac{1}{2}x_1 + \frac{1}{2}(-x_2) = z_2 - z_1 \neq 0,$$

ceea ce demonstrează enunțul teoremei lui Minkovski. În cele ce urmează vom demonstra un cunoscut rezultat din teoria numerelor folosind teorema lui Minkovski.

Propoziția 2. *Un număr natural n se scrie ca suma a două pătrate de numere naturale dacă și numai dacă orice număr prim de forma* $4k + 3$ *care divide pe n trebuie să apară în descompunerea în factori primi a lui n la o putere pară* ($n \neq 0$).

Demonstrație. Presupunem că există numerele naturale a, b și k precum și un număr prim p de forma $4l + 3$ ($l \in \mathbf{N}$) astfel încât $n = a^2 + b^2$, $p^{2k+1} \mid n$ și $p^{2k+2} \nmid n$. Se deduce imediat că a și b sunt numere naturale nenule. Fie $\alpha \in \mathbf{N}$ astfel încât $p^\alpha \mid (a, b)$ și $p^{\alpha+1} \nmid (a, b)$. Din cele de mai sus rezultă că

$$n = p^{2\alpha}(a_1^2 + b_1^2),$$

unde $a_1, b_1 \in \mathbf{N}^*$ și $p \nmid (a_1, b_1)$. Presupunerea făcută ceva mai sus ne asigură că $2\alpha < 2k + 1$; există deci o scriere de forma $n_1 = a_1^2 + b_1^2$, unde $p \mid n_1$ și $p \nmid (a_1, b_1)$. Trecând la congruența modulo p în ultima egalitate, obținem că $0 \equiv a_1^2 + b_1^2 \pmod{p}$. Cum $p \nmid (a_1, b_1)$ din cele de mai sus rezultă că $p \nmid a_1$ și $p \nmid b_1$. Ridicăm congruența $a_1^2 \equiv -b_1^2 \pmod{p}$ la puterea $2l + 1$; ținând cont de mica teoremă a lui Fermat precum și de faptul că $p \nmid a_1$ și $p \nmid b_1$, deducem că $1 \equiv -1 \pmod{p}$, ceea ce este evident absurd.

Una din implicații este în acest moment demonstrată.

Să presupunem acum că orice număr prim de forma $4k + 3$ ($k \in \mathbf{N}$) care-l divide pe n trebuie să apară în descompunerea în factori primi a lui n la o putere pară. Vom arăta că atunci n se scrie ca suma a două pătrate de numere naturale.

În ipoteza făcută mai sus avem că $n = d^2 \cdot m$, unde m este un număr natural liber de pătrate și în plus orice număr prim p care-l divide pe m nu poate fi de forma $4k+3$. Deci $m = \prod_{i=1}^{r} p_i$, unde $p_1, p_2, \ldots, p_r$ sunt numere prime distincte de forma $4k+1$, unul din ele putând fi 2 (dacă cumva $m = 1$ atunci $n = d^2$ și enunțul este evident adevărat).

Vom arăta întâi că orice număr prim p de forma $4k + 1$ se poate scrie ca sumă două pătrate de numere naturale. Pentru p prim, $p = 4k + 1$ ($k \in \mathbf{N}^*$), arătăm că există un număr natural i astfel încât $p \mid (i^2 + 1)$. Pentru aceasta vom folosi teorema lui Wilson care afirmă ca $(p - 1)! \equiv -1 \pmod{p}$.

Au loc, în mod evident, următoarele congruențe modulo p:

$$1 \equiv -(p-1) \pmod{p}$$
$$2 \equiv -(p-2) \pmod{p}$$

$$\frac{p-1}{2} \equiv -\left(p - \frac{p-1}{2}\right) = -\left(\frac{p+1}{2}\right) \pmod{p}$$
$$\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod{p}$$

$$2 \equiv 2 \pmod{p}$$
$$1 \equiv 1 \pmod{p}$$

Înmulțind congruențele de mai sus și notând cu i numărul natural $\left(\frac{p-1}{2}\right)!$ obținem că

$$i^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod{p}.$$

Deoarece $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$ și

$$(p-1)! \equiv -1 \pmod{p}$$

conform teoremei lui Wilson, deducem că $p \mid i^2 + 1$. Fie acum

$$\Lambda = \{(u_1, u_2) \in \mathbf{Z}^2 \mid u_1 - i\,u_2 \equiv 0 \pmod{p}\},$$

unde i este numărul natural indicat mai sus. Lema 2 din paragraful I al anexei teoremei lui Waring ne arată că $\wedge$ este o rețea în $\mathbf{R}^2$ (rețea completă) și că Δ (adică volumul paralelipipedului fundamental asociat lui Λ) este mai mic sau egal cu p. Fie $X \subseteq \mathbf{R}^2$ următoarea mulțime: $X = \{(x, y) \in \mathbf{R}^2 \mid x^2 + y^2 < 2p\}$. Este evident că X este o mulțime mărginită, simetrică, convexă și măsurabilă Lebesgue, măsura ei fiind egală cu $v(X) = \pi \cdot 2p$. Din cele de mai sus rezultă că $2^2 \cdot \Delta \leq$ $\leq 4 \cdot p < 2 \cdot \pi \cdot p = v(X)$ și deci putem aplica teorema lui Minkovski. Aceasta ne asigură existența unei perechi $(u_1, u_2) \in \Lambda \cap X$ și în plus $(u_1, u_2) \neq (0, 0)$. Dacă explicităm concluziile anterioare obținem că $u_1, u_2 \in \mathbf{Z}$, $u_1 \equiv iu_2 \pmod{p}$, $(u_1, u_2) \neq (0, 0)$ și în plus $u_1^2 + u_2^2 < 2p$. Alegerea lui i asigură următoarele congruențe modulo p :

$$u_1^2 + u_2^2 \equiv i^2 u_2^2 + u_2^2 \equiv u_2^2 (i^2 + 1) \equiv 0 \pmod{p}.$$

Deci

$$0 < u_1^2 + u_2^2 < 2p,\ p \mid u_1^2 + u_2^2 \text{ și } u_1^2 + u_2^2 \in \mathbf{N};$$

singura posibilitate este ca $u_1^2 + u_2^2$ să fie egal chiar cu p. În acest moment am arătat că orice număr prim de forma $4k + 1$ se scrie ca suma a două pătrate de numere naturale.

Identitatea

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

ne arată că dacă două numere naturale au proprietatea că se pot scrie ca suma a două pătrate de numere naturale, atunci și produsul celor două numere are aceeași proprietate. Folosind faptul că $m = \prod_{i=1}^{r} p_i$, unde p_i sunt numere prime distincte de forma $4k+1$ și eventual unul dintre ele poate fi 2, că orice număr prim de forma $4k+1$ se scrie ca suma a două pătrate de numere naturale, că $2 = 1^2 + 1^2$ precum și observația precedentă, printr-o recurență rezultă imediat că m se poate scrie

sub forma $m = a^2 + b^2$, unde a și b sunt numere naturale. Deci

$$n = d^2(a^2 + b^2) = (ad)^2 + (bd)^2$$

și enunțul este demonstrat în acest moment.

II. **Teoremă**. *Fie* $m_1, m_2, ..., m_n$ *numere naturale nenule astfel încât* $(m_i, m_j) = 1$, $(\forall)\ i, j = \overline{1,n}$, $i \neq j$ $(n \in \mathbf{N}^*)$. *Dacă* $a_i \in \mathbf{Z}$, *oricare ar fi* $i = \overline{1,n}$, *atunci există* $m \in \mathbf{Z}$ *cu proprietatea că* $m \equiv a_i \pmod{m_i}$, $(\forall)\ i = \overline{1,n}$ (*acest rezultat este cunoscut sub numele de lema chineză a resturilor*).

Demonstrație. Deoarece $(m_1, m_i) = 1$, $(\forall)\ i = \overline{2,n}$, există $b_i, c_i \in \mathbf{Z}\ (i = \overline{2,n})$ astfel ca $b_i m_1 + c_i m_i = 1$, $(\forall)\ i = \overline{2,n}$. Considerăm numărul $x_1 = a_1 \cdot \prod_{i=2}^{n}(1 - b_i m_1)$. Este clar că $x_1 \equiv a_1 \pmod{m_1}$ și $x_1 \equiv 0 \pmod{m_i}$, $(\forall)\ i = \overline{2,n}$. În același mod găsim numerele întregi $x_2, x_3, ..., x_n$ cu proprietatea că $x_j \equiv a_j \pmod{m_j}$ și $x_j \equiv 0 \pmod{m_i}$, $(\forall)\ i = \overline{1,n}$, $i \neq j$. Dacă luăm acum $m = \sum_{i=1}^{n} x_i$, atunci evident m are proprietățile cerute în enunț. Să mai observăm aici că orice număr de forma $m + a$, unde $a \in \mathbf{Z}$ este un multiplu de $m_1 \cdot m_2 \cdot ... \cdot m_n$, are aceeași proprietate ca și m. De aici deducem în particular că în plus față de calitățile impuse în enunț, m poate fi ales chiar număr natural.

Tiparul s-a executat sub c-da nr. 234/1996 la
Tipografia Editurii Universității din București

ISBN 973-575-196-8

Lei 13