Bujor Voinea

Marea teoremă a lui Fermat

Demonstrație
(Ediție complet revizuită)

EDITURA
SemnE

MAREA TEOREMĂ A LUI FERMAT:

Relaţia

$$x^n + y^n = z^n \qquad [\alpha]$$

nu este posibilă în numere întregi pentru nici un exponent $n > 2$*, număr natural.*

DEMONSTRAŢIE

PARTEA I

Voi face demonstraţia pentru n număr prim impar ceea ce este suficient pentru orice $n > 2$.

Considerăm că relaţia $[\alpha]$ este redusă şi că, deci, numerele x, y şi z sunt prime între ele, $(x, y, z) = 1$, cu alte cuvinte, nu au nici un divizor comun.

Pentru claritate arăt aici, pe scurt, calea pe care o va urma demonstraţia în prima etapă:

Printr-o substituţie simplă şi evidentă voi transforma relaţia $[\alpha]$ într-o ecuaţie cu coeficienţi întregi de gradul n, sub forma canonică cea mai obişnuită. Se va căuta cel puţin o rădăcină întreagă şi, de aici, se vor desprinde trei cazuri distincte care vor fi ulterior detaliate. Ordinea numerotării **cazurilor** este absolut convenţională. Se va demonstra imposibilitatea cazurilor I şi III în ipoteza $(x, y, z) = 1$. Cazul II va conduce la două soluţii parametrice diferite după cum x, y şi z nu sunt nici unul divizibile cu n, sau când unul şi numai unul din numerele x, y, z este divizibil cu n.

Pentru a fi consecvent cu mine însumi voi introduce simbolul „$\equiv div$" între două mărimi a şi b atunci când a se divide exact cu b;

$$a \equiv divb$$

având acelaşi înţeles cu b / a, sau $a \equiv 0(\mathrm{mod}\, b)$.

Deci, facem substituţia

$$z = y + k \qquad [1]$$

unde k este un număr întreg pozitiv deoarece $z > y$.

Înlocuim [1] în $[\alpha]$

$$x^n + y^n = (y + k)^n$$

$$x^n + y^n = y^n + C_n^1 y^{n-1}k + \ldots + C_n^{n-1} yk^{n-1} + k^n \;;$$

şi se obţine

$$x^n - k^n = C_n^1 y^{n-1}k + \ldots + C_n^{n-1} yk^{n-1}. \qquad [\beta]$$

Deci

$x^n - k^n \equiv divk$ deoarece $x^n - k^n$ este un număr natural care se poate scrie sub forma părţii din dreapta egalităţii, unde k este divizor întreg.

Pentru ca $x^n - y^n$ să se poată divide cu k se impun următoarele cazuri:

CAZUL I: $x \equiv divk$

CAZUL II: $x^n \equiv divk$, cu $x \not\equiv divk$, $x^{n-i} \not\equiv divk$

CAZUL III: $x^{n-i} \equiv divk$, cu $x \not\equiv divk$, $x^n \equiv divk$

unde $i \le n$ este număr natural ca şi n iar „$\not\equiv div$" exprimă ne-divizibilitatea.

Să analizăm pe rând aceste cazuri.

CAZUL I

Dacă $x \equiv divk$, putem da factor comun pe k şi în partea stângă a egalităţii $[\beta]$

$$x^n\left(\frac{x^n}{k^n}-1\right)=k^n\left(\vartheta^n-1\right),\ \vartheta \text{ număr întreg pozitiv.}$$

Prin urmare scriem

$$k^n\left(\vartheta^n-1\right)=C_n^1y^{n-1}k+...+C_n^{n-1}yk^{n-1}$$

şi, simplificând cu k, obţinem

$$k^{n-1}\left(\vartheta^n-1\right)=C_n^1y^{n-1}+...+C_n^{n-1}yk^{n-2} \qquad [\gamma]$$

Ne convine să interpretăm această relaţie ca pe o ecuaţie de gradul $n-1$ în k:

$$\left(\vartheta^n-1\right)k^{n-1}-C_n^{n-1}yk^{n-2}-C_n^{n-2}y^2k^{n-3}-...-C_n^2y^{n-2}k-C_n^1y^{n-1}=0$$

Termenul liber este deci ny^{n-1}.

Nu intră în discuţie $k=1$ deoarece inversând pe x cu y oricum avem situaţia $k \ne 1$.

- Dacă rădăcina (în cazul în care există ca număr întreg) divide pe y ($y \equiv divk$), din $[1]$ rezultă

$$x \equiv divk\ ,\ z \equiv divk$$

absurd căci contrazice ipoteza $(x,y,z)=1$.

- Dacă n este număr prim vom putea admite $k=n$ or, simplificând odată cu rădăcina întreaga relaţie, noul termen liber este

$$y^{n-1}+\frac{(n-1)n}{2}y^{n-2}$$

dar şi acest termen trebuie să se dividă cu rădăcina $k=n$, de unde $y \equiv divn$ şi din nou $x \equiv divn$, $z \equiv divn$, absurd.

CAZUL I, deci, nu este posibil dacă relaţia $[\alpha]$ este posibilă în numere întregi cu n număr prim impar.

Putem căuta numai soluţiile pozitive căci cele negative sunt simetrice celor negative pentru n prim impar.

CAZUL II

Dacă $x \not\equiv divk$ şi $x^{n-i} \not\equiv divk$, dar $x^n \equiv divk$,
k are cel puţin un divizor ε care are un corespondent în x.

Prin urmare $k \equiv div\varepsilon^n$, care se scrie $k=\varepsilon^n\eta$, sau $k=\varepsilon t$, cu $t=\varepsilon^{n-1}\eta$.

Aici toate mărimile ε, η, t sunt numere întregi pozitive.
Putem deosebi două situaţii diferite:

$$x \equiv div \varepsilon \eta \qquad [A]$$

sau

$$x \equiv div \varepsilon \eta^* \qquad [B]$$

unde $\eta \neq \eta^*$ şi, deci, un factor ce apare sau nu apare şi în x şi în k.

[ATENŢIE: o situaţie de genul $x = 7*11$, $k = 7^2$, aparţine CAZULUI III.]

Să analizăm pe rând cele două situaţii A şi B.

A) Scriem deci $x^n \equiv div \varepsilon^n \eta^n$ sau $x^n = L^n \varepsilon^n \eta^n$, cu L număr întreg şi pozitiv.
Rescriem relaţia [β]

$$x^n - k^n = C_n^1 y^{n-1} k + ... + C_n^{n-1} y k^{n-1}$$

Dacă n este prim, în partea dreaptă a relaţiei se pot da factori comuni n, y, k.
Înlocuim x şi k, respectiv cu $L\varepsilon\eta$ şi εt.

$$\varepsilon^n (L^n \eta^n - t^n) = ny\varepsilon t(y^{n-2} + \frac{1}{n} C_n^2 y^{n-3} \varepsilon t + ... + \frac{1}{n} C_n^{n-1} \varepsilon^{n-2} t^{n-2})$$

şi cu $t = \varepsilon^{n-1}\eta$

$$\varepsilon^n \eta^n (L^n - \varepsilon^{n(n-1)}) = ny\varepsilon^n \eta(y^{n-2} + \frac{1}{n} C_n^2 y^{n-3} \varepsilon^n \eta + ... + \frac{1}{n} C_n^{n-1} \varepsilon^{n(n-2)} \eta^{n-2})$$

putem simplifica cu $\varepsilon^n \eta$

$$\eta^{n-1} (L^n - \varepsilon^{n(n-1)}) = ny(y^{n-2} + \frac{1}{n} C_n^2 y^2 \varepsilon^n \eta + ... + \frac{1}{n} C_n^{n-1} \varepsilon^{n(n-2)} \eta^{n-2})$$

şi chiar dacă $\eta = n$ tot nu este suficient ca să nu avem

$x \equiv div\eta$; $y \equiv div\eta$; $z \equiv div\eta$ ceea ce este absurd.

B) Dacă

$x \equiv div \varepsilon \eta^*$ cu $\eta \neq \eta^*$ relaţie [β] devine

$$L^n \varepsilon^n \eta^{*n} - \varepsilon^{n^2} \eta^n = ny\varepsilon^n \eta(y^{n-2} + \frac{1}{n} C_n^2 y^{n-3} \varepsilon^{n-3} \varepsilon^n \eta + ...)$$

şi, simplificând cu ε^n,

$$L^n \eta^{*n} - \varepsilon^{n(n-1)} \eta^n = ny\eta(y^{n-2} + \frac{1}{n} C_n^2 y^{n-3} \varepsilon^n \eta + ...) \qquad [\beta_1]$$

relaţie care implică acelaşi raţionament ca pentru relaţia [β]. Pentru a fi mai evident notăm formal $L\eta^*$ cu x şi η cu k

$$x^n - \varepsilon^{n(n-1)} k = nyk(y^{n-2} + \frac{1}{n} C_n^2 y^{n-3} \varepsilon^n k + ...)$$

şi scriem din nou $x = L\varepsilon_1 \eta_1^*$, $k = \varepsilon_1^n \eta_1$, pe care le înlocuim

$$L^n \varepsilon_1^n \eta_1^{*n} - \varepsilon^{n(n-1)} \varepsilon_1^{n^2} \eta_1^n = ny\varepsilon_1^n \eta_1(y^{n-2} + \frac{1}{n} C_n^2 y^{n-3} \varepsilon^n \varepsilon_1^n \eta_1 + ...)$$