Marea teoremă a lui Fermat pentru polinoame

Temistocle BÎRSAN[1]

1. Odată cu căderea Constantinopolului (1453), mulţi învăţaţi bizantini s-au îndreptat spre Europa de Vest aducând cu ei manuscrise preţioase - manuscrisele care supravieţuiseră devastării Bibliotecii din Alexandria se adunaseră de-a lungul timpului în această capitală a lumii.

Prin hazardul împrejurărilor, şase din cele 13 volume ale *Aritmeticii* lui **Diofant** au ajuns în Franţa. Învăţatul şi amatorul de matematică francez **Claude Gaspar Bachet de Méziriac** îşi dă seama de importanţa cărţii lui Diofant şi publică în 1621 o versiune în limba latină a *Aritmeticii*, care cuprinde peste o sută de probleme şi rezolvările detaliate ale lui Diofant.

Pentru **Pierre Fermat** (1601-1665) *Aritmetica* lui *Diofant* a fost cartea care l-a pus în contact cu bogatele cunoştinţe ale popoarelor antice în direcţia teoriei numerelor şi sursa de inspiraţie pentru noi şi subtile probleme pe care singur şi le formula. Fermat obişnuia să noteze pe marginile cărţii lui Diofant comentarii, calcule şi schiţe de demonstraţii. Nu s-a preocupat să-şi publice rezultatele şi demonstraţiile, dar se amuza comunicându-şi rezultatele altor matematicieni ai timpului şi provocându-i la rezolvarea acestora.

În Cartea a II-a a *Aritmeticii*, Fermat găseşte informaţii bogate relativ la tripletele pitagoreice, adică trei numere naturale ce verifică ecuaţia lui Pitagora

$$x^2 + y^2 = z^2. \tag{1}$$

Ştia că Euclid demonstrase că există o infinitate de astfel de triplete. Ce se întâmplă, însă, dacă în loc de (1) se consideră ecuaţia

$$x^n + y^n = z^n, \tag{2}$$

unde $n \geq 3$? Răspunsul lui Fermat, notat ca observaţie pe marginea cărţii lui Diofant, este cu totul surprinzător: *nu există nici o soluţie a ecuaţiei* (2) *cu numere x, y, z nenule, dacă $n = 3, 4, \ldots$* . Urmează notat următorul comentariu:

Cuius rei demonstrationem mirabilem sane detex hanc marginis exiguitas non caperet [**4**]. (Mă aflu în posesia unei demonstraţii minunate a acestei afirmaţii, dar marginea paginii este prea strâmtă pentru a o cuprinde.)

Această extraordinară descoperire, care astăzi poartă numele de **Marea teoremă a lui Fermat**, cât şi alte rezultate, ar fi putut să rămână necunoscute lumii matematicienilor şi să se piardă, dacă, după moartea lui Fermat, fiul său cel mai mare n-ar fi examinat însemnările scrise de tatăl său pe margini şi n-ar fi publicat *Aritmetica lui Diofant conţinând şi observaţiile lui Pierre de Fermat* (Toulouse, 1670).

Pe parcursul câtorva secole, cele mai sclipitoare minţi de matematicieni au încercat şi şi-au adus contribuţia la rezolvarea acestei enigme (şi, totodată, provocări) lăsată de Fermat: **Euler**, **Sophie Germain**, **Dirichlet**, **Legendre**, **Lamé**, **Cauchy**, **Kummer** ş. a. Drumul ce duce la demonstrarea *Marii teoreme a lui Fermat* este

[1] Prof. dr., Catedra de matematică, Univ. Tehnică "Gh. Asachí", Iaşi

presărat cu reuşite parţiale, ambiţii, înfrângeri, decepţii, orgolii, intrigi, tentative de sinucidere etc. [**4**].

În anul 1995, după opt ani de muncă neîntreruptă, în completă izolare faţă de colegii săi şi păstrând o discreţie totală asupra cercetărilor sale, englezul **Andrew Wiles** pune capăt enigmei de peste 350 de ani: *Marea teoremă a lui Fermat este demonstrată!* Demonstraţia dată de Wiles este, însă, accesibilă unui număr restrâns de specialişti; în fapt, Wiles pentru a atinge scopul a dovedit justeţea *Conjecturii Taniyama - Shimura* utilizând o aparatură matematică modernă şi sofisticată: curbe eliptice, forme modulare, reprezentări Galois ş. a. [**5**].

2. Este cunoscut faptul că inelul $\mathbb{Z}$ al numerelor întregi şi inelul $\mathbb{C}[X]$ al polinoamelor cu coeficienţi numere complexe au proprietăţi asemănătoare. De aceea apare ca firească problema rezolvării ecuaţiilor (1) şi (2) în $\mathbb{C}[X]$.

În privinţa ecuaţiei (1) constatăm uşor, ca şi în cazul numeric, că are o infinitate de soluţii: $\forall p, q \in \mathbb{C}[X]$, luăm

$$x(X) = [p(X)]^2 - [q(X)]^2, \quad y(X) = 2p(X)\,q(X), \quad z(X) = [p(X)]^2 + [q(X)]^2$$

şi verificăm direct că tripleta $(x(X), y(X), z(X))$ este o soluţie a ecuaţiei (1) în $\mathbb{C}[X]$.

Similar cu Marea teoremă a lui Fermat se formulează

Teorema lui Fermat pentru polinoame ([3], [5]). *Dacă n este un întreg, $n \geq 3$, atunci ecuaţia* (2) *nu are soluţii în* $\mathbb{C}[X]$ *cu polinoame neconstante şi relativ prime.*

Surprinzător, spre deosebire de Marea teoremă a lui Fermat, pentru acest rezultat se cunoaşte o demonstraţie elementară şi simplă, accesibilă unui elev de liceu. Rezultatul este cunoscut din sec. al XIX-lea şi a fost demonstrat utilizând cunoştinţe de geometrie algebrică. Demonstraţia elementară la care ne-am referit se sprijină pe o teoremă de dată recentă datorată matematicienilor **W. Stothers** (1981) şi, independent, **R. C. Mason** (1983), teoremă foarte importantă şi în sine. Sunt necesare câteva (puţine!) pregătiri.

Fie $p \in \mathbb{C}[X]$ un polinom neconstant având rădăcinile $a_1, a_2, \ldots, a_k$ cu ordinele de multiplicitate respective $m_1, m_2, \ldots, m_k$; deci p se scrie sub forma

$$p(X) = \alpha \prod_{i=1}^{k} (X - a_i)^{m_i}, \quad \alpha \in \mathbb{C}^*. \tag{3}$$

Notăm gradul polinomului p şi numărul rădăcinilor sale distincte cu $\deg p$ şi respectiv $n_0(p)$, adică

$$\deg p = m_1 + m_2 + \cdots + m_k, \quad n_0(p) = k.$$

Menţionăm că, dacă $p, q \in \mathbb{C}$ sunt neconstante, avem

$$\deg(pq) = \deg p + \deg q, \quad n_0(pq) \leq n_0(p) + n_0(q),$$

cu egalitate dacă şi numai dacă p şi q sunt relativ prime.

Derivata formală a polinomului p dat de (3) este

$$p'(X) = \alpha[m_1 (X - a_1)^{m_1 - 1} (X - a_2)^{m_2} \cdots (X - a_k)^{m_k} + \cdots +$$
$$+ m_k (X - a_1)^{m_1} \cdots (X - a_{k-1})^{m_{k-1}} (X - a_k)^{m_k - 1}]$$

şi, ca urmare, cel mai mare divizor comun al polinoamelor p şi p' are forma

$$(p, p') = \beta (X - a_1)^{m_1 - 1} (X - a_2)^{m_2 - 1} \cdots (X - a_k)^{m_k - 1}.$$

Atunci

$$\deg (p, p') = (m_1 - 1) + (m_2 - 1) + \cdots + (m_k - 1) = \deg p - n_0 (p),$$

de unde obţinem relaţia

$$\deg p = \deg (p, p') + n_0 (p). \tag{4}$$

Teorema Mason - Stothers. *Fie $p, q, r \in \mathbb{C}[X]$ neconstante şi relativ prime. Dacă are loc egalitatea $p + q = r$, atunci*

$$\max \{\deg p, \deg q, \deg r\} \leq n_0 (pqr) - 1. \tag{5}$$

Demonstraţie (dată de **Noah Snyder** [**3**], p.30). Vom începe cu două observaţii utile. Mai întâi, în prezenţa condiţiei $p+q = r$, polinoamele p, q, r sunt relativ prime dacă şi numai dacă sunt prime două câte două. Apoi, întrucât enunţul teoremei este simetric în p, q, r (căci putem scrie egalitatea şi sub forma $p + q + r = 0$), nu restrângem generalitatea dacă vom presupune că polinomul r are gradul cel mai ridicat. Ca urmare, inegalitatea de demonstrat se scrie

$$\deg r \leq n_0 (pqr) - 1. \tag{5'}$$

Avem

$$p'q - pq' = p' (p + q) - p (p' + q') = p'r - pr'.$$

Constatăm că (p, p') şi (q, q') divid membrul stâng, iar (r, r') divide membrul drept, deci şi pe cel stâng. Cum p, q, r sunt prime două câte două, urmează că produsul $(p, p') \cdot (q, q') \cdot (r, r')$ divide $p'q - pq'$. În consecinţă,

$$\deg (p, p') + \deg (q, q') + \deg (r, r') \leq \deg (p'q - pq') \leq \deg p + \deg q - 1$$

sau, datorită relaţiei (4) şi analoagelor ei,

$$\deg p - n_0 (p) + \deg q - n_0 (q) + \deg r - n_0 (r) \leq \deg p + \deg q - 1,$$

deci

$$\deg r \leq n_0 (p) + n_0 (q) + n_0 (r) - 1.$$

Cum p, q, r sunt prime două câte două, obţinem în final

$$\deg r \leq n_0 (pqr) - 1,$$

care este tocmai relaţia (5′) de demonstrat.

Demonstraţia Teoremei lui Fermat pentru polinoame. Presupunem că ecuaţia (2) pentru $n \geq 3$ ar avea o soluţie $(x (X), y (X), z (X))$ cu polinoame neconstante relativ prime. Aplicăm teorema Mason - Stothers polinoamelor $p(X) = [x(X)]^n$, $q (X) = [y (X)]^n$ şi $r (X) = [z (X)]^n$. Obţinem

$$\deg [x (X)]^n \leq n_0 ([x (X)]^n \cdot [y (X)]^n \cdot [z (X)]^n) - 1$$

sau

$$n \deg x (X) \leq n_0 (x (X) \cdot y (X) \cdot z (X)) - 1.$$

Ţinând seama că $x(X)$, $y(X)$ şi $z(X)$ sunt prime două câte două şi de faptul că $n_0(p) \leq \deg p$, $\forall p \in \mathbb{C}[X]$, vom avea

$$\begin{aligned} n \deg x(X) &\leq n_0(x(X)) + n_0(y(X)) + n_0(z(X)) - 1 \leq \\ &\leq \deg x(X) + \deg y(X) + \deg z(X) - 1. \end{aligned}$$

Obţinem astfel inegalitatea

$$n \deg x(X) \leq \deg x(X) + \deg y(X) + \deg z(X) - 1,$$

precum şi inegalităţile analoage scrise pentru $y(X)$ şi $z(X)$, care adunate dau

$$n(\deg x(X) + \deg y(X) + \deg z(X)) \leq 3(\deg x(X) + \deg y(X) + \deg z(X)) - 3,$$

adică

$$(n-3)(\deg x(X) + \deg y(X) + \deg z(X)) \leq -3.$$

Evident, dacă $n \geq 3$, această relaţie ne conduce la o absurditate, ceea ce încheie demonstraţia.

3. Analogia care există între inelele $\mathbb{Z}$ şi $\mathbb{C}[X]$ pune în mod firesc problema "translării" teoremei Mason - Stothers de la polinoame la numerele întregi astfel încât Marea teoremă a lui Fermat să poată fi demonstrată elementar.

D. Masser şi **J. Oesterle** (1986) au ajuns la aşa - numita *conjectură abc* ca urmare a unor consideraţii de geometrie algebrică şi teoria funcţiilor modulare (şi nu în legătură cu teorema Mason - Stothers).

Dacă $m \in \mathbb{N}^*$ are descompunerea în factori primi $m = \prod_{i=1}^{k} p_i^{m_i}$, atunci vom numi *radicalul lui* m numărul $N_0(m) = \prod_{i=1}^{k} p_i$.

Conjectura abc ([2], [3]). *Dat $\varepsilon > 0$, există o constantă $C(\varepsilon)$ astfel încât pentru orice întregi a, b, c nenuli şi relativ primi cu $a + b = c$ avem inegalitatea*

$$\max\{|a|, |b|, |c|\} \leq C(\varepsilon)(N_0(abc))^{1+\varepsilon}.$$

Această conjectură spune că, dacă în descompunerea numerelor a, b, c există factori primi cu exponenţi mari, aceşti factori sunt compensaţi prin factori primi mai mulţi, dar cu exponentul 1.

Să enunţăm acum aşa - numita

Teorema lui Fermat asimptotică. *Există un întreg pozitiv n_1 cu proprietatea că, dacă $n \geq n_1$, atunci ecuaţia (2) nu are soluţii cu x, y, z întregi şi $xyz \neq 0$.*

Cu aceleaşi argumente ca în cazul polinoamelor se poate dovedi următoarea

Teoremă ([2], [3]). *Conjectura abc implică Teorema lui Fermat asimptotică.*

Demonstraţie. Fie date x, y, z pozitive şi relativ prime astfel încât tripleta (x, y, z) să fie soluţie a ecuaţiei (2), adică $x^n + y^n = z^n$.

Notăm $a = x^n$, $b = y^n$ şi $c = z^n$ şi observăm că

$$N_0(abc) = N_0(x^n y^n z^n) = N_0(xyz) \leq xyz.$$

Utilizând conjectura abc obţinem

$$x^n \leq C(\varepsilon)(xyz)^{1+\varepsilon}, \quad y^n \leq C(\varepsilon)(xyz)^{1+\varepsilon}, \quad z^n \leq C(\varepsilon)(xyz)^{1+\varepsilon}.$$

Prin înmulţire, rezultă că

$$(xyz)^n \leq [C(\varepsilon)]^3 (xyz)^{3+3\varepsilon},$$

de unde

$$(n-3-3\varepsilon)\log(xyz) \leq 3\log C(\varepsilon)$$

şi cum $xyz > 2$, obţinem

$$n < \frac{3\log C(\varepsilon)}{\log 2} + 3 + 3\varepsilon.$$

Notăm

$$n_1 = \left[\frac{3\log C(\varepsilon)}{\log 2} + 3 + 3\varepsilon\right]. \tag{6}$$

Urmează că ecuaţia (2) nu are soluţii ce verifică condiţiile specificate dacă $n \geq n_1$, ceea ce trebuia demonstrat.

Observaţie. Această cale nu oferă o demonstraţie a Marii teoreme a lui Fermat. Într-adevăr, numărul n_1 definit de (6) depinde de $C(\varepsilon)$ (putem considera $\varepsilon = 1$ şi $C(1)$ pentru a fixa ideile). Determinarea efectivă a constantei $C(\varepsilon)$ nu este cunoscută. Dacă, de exemplu, $C(1)$ s-ar putea efectiv determina, atunci demonstraţia Marii Teoreme a lui Fermat s-ar reduce la un număr finit de cazuri, care ar putea fi abordate prin calcul direct.

4. Interesul pentru Marea teoremă a lui Fermat nu s-a stins nici după demonstrarea ei. Au rămas întrebări fără răspuns, sunt formulate altele noi. Dacă Fermat nu a dat decât o demonstraţie eronată, care ar putea fi natura greşelii făcute? Dacă această demonstraţie ar fi corectă, care este acel argument ingenios produs de geniul lui Fermat ce a scăpat atâtor matematicieni iluştri? Este posibilă o demonstraţie elementară, accesibilă şi unor persoane cu cunoştinţe obişnuite de matematică?

În 1966, **Andrew Beal** instituie un premiu pentru demonstrarea sau infirmarea aşa - numitei *Conjecturi Beal*, care este o generalizare a problemei lui Fermat:

Ecuaţia $x^p + y^q = z^r$, p, q, r *numere întregi mai mari ca* 2, *nu are nici o soluţie cu* x, y, z *întregi pozitivi şi relativ primi* ([**6**], [**1**]).

Bibliografie

1. **A. Corduneanu** - *Despre Marea teoremă a lui Fermat*, Recreaţii Matematice, 1 (1999), nr.1, 37-39.
2. **S. Lang** - *Old and new conjectured diophantine inequalities*, Bull. AMS, 23 (1990), 37-75.
3. **S. Lang** - *Math Talks for Undergraduates*, Springer, 1999.
4. **S. Singh** - *Marea teoremă a lui Fermat*, Humanitas, Bucureşti, 1998.
5. **A. Wiles** - *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math., 142 (1995), 443-551.
6. *** - *Beal's Conjecture*, The New Zealand Math. Mag., 35 (1998), no.2, 38.