Numere prime din progresii aritmetice

Petru Minuţ[1]

Un număr natural p, $p > 1$, se numeşte *număr prim* dacă nu are alţi divizori înafară de 1 şi p.

Lemă. *Un număr natural n, $n > 1$, are un divizor prim.*

Demonstraţie. Fie M mulţimea tuturor numerelor naturale care sunt divizori ai lui n diferiţi de 1. $M \neq \emptyset$, deoarece $n \in M$. În M există un număr care este cel mai mic, p. Arătăm, prin reducere la absurd, că p este prim. Presupunem că p este compus: $p = ab$, $1 < a < p$. Din $a \mid p$ şi $p \mid n$ rezultă că $a \mid n$. Am găsit un divizor al lui n mai mic ca p ceea ce contrazice alegerea lui p.

Teorema 1. *În mulţimea numerelor naturale există o infinitate de numere prime.*

Demonstraţie. Există numere prime. De exemplu 2, care nu poate avea alţi divizori în afară de 1 şi 2. Folosim metoda reducerii la absurd. Presupunem că există o mulţime finită de numere prime în $\mathbb{N}$, $P = \{p_1, p_2, \ldots, p_k\}$. Considerăm numărul ajutător $N = p_1 p_2 \ldots p_k + 1$. Deoarece $N > 1$, există un număr prim p, $p \mid N$. Din $p \in P$ rezultă că $p \mid p_1 p_2 \ldots p_k$. Dacă două numere sunt multipli de p, atunci diferenţa lor este multiplu de p. Rezultă că $p \mid 1$, ceea ce implică $p = 1$ şi contrazicem definiţia numărului prim.

Observaţie. Teorema 1 o găsim enunţată şi demonstrată pentru prima oară în opera lui **Euclid** *"Elemente"* (sec. III î. Ch.) şi este cunoscută sub denumirea de *teorema lui Euclid*. Se cunosc numeroase demonstraţii ale acestei teoreme.

Singurul număr prim par este 2. Aranjăm numerele impare în două şiruri:

$$\underline{3}, \underline{7}, \underline{11}, 15, \ldots, 4k-1, \ldots \tag{1}$$

$$1, \underline{5}, 9, \underline{13}, \ldots, 4k+1, \ldots \tag{2}$$

Constatăm că în aceste şiruri (progresii aritmetice), mergând până la termeni de rang tot mai mare, găsim noi termeni care sunt numere prime. Dacă luăm şi alte progresii aritmetice, de exemplu:

$$\underline{3}, \underline{13}, \underline{23}, 33, \underline{43}, \underline{53}, 63, \underline{73}, 83, \ldots \tag{3}$$

$$\underline{2}, \underline{7}, 12, \underline{17}, 22, 27, 32, \underline{37}, 42, \underline{47}, \ldots \tag{4}$$

constatăm acelaşi lucru. Este uşor de demonstrat că în progresia (1) există o infinitate de numere prime.

Teorema 2. *Există o infinitate de numere prime de forma $p = 4k-1$, $k \in \mathbb{N}$.*

Demonstraţie. Procedăm prin reducere la absurd. Am pus deja în evidenţă câteva numere prime de această formă (şirul (1)). Presupunem că există un număr finit de numere prime de acest fel: $p_1, p_2, \ldots, p_n$. Construim numărul ajutător $N = 4p_1 p_2 \ldots p_n - 1$. Deoarece $N > 1$, există p prim, $p \mid N$. Orice număr prim p diferit de 2 este de forma $p = 4k-1$ sau $p = 4k+1$. Dacă toţi divizorii primi ai lui N sunt de forma $p = 4k+1$, numărul N este de forma $N = 4h+1$, deci $4 \mid N-1$ şi $4 \mid N+1$, ceea ce implică $4 \mid 2$. Contradicţie! Există divizori primi ai lui N de forma $4k-1$. Fie

[1] Prof. dr., Univ. "D. Cantemir", Tg. Mureş

p un asemenea divizor. Rezultă că $p \in \{p_1, p_2, \ldots, p_n\}$, deci $p \mid 4p_1p_2 \ldots p_n$ şi cum $p \mid N$ rezultă $p = 1$. Contradicţie! Presupunerea că există un număr finit de numere prime de forma $p = 4k - 1$ nu poate fi adevărată.

Teorema 2 se generalizează după cum urmează:

Teorema 3. *Pentru orice număr natural n, $n \neq 0$, există o infinitate de numere prime p de forma $p = nk - 1$, $k \in \mathbb{N}$.*

Demonstraţie. Pentru $n = 1$, $\{nk - 1 \mid k \in \mathbb{N}\} = \mathbb{N} \cup \{-1\}$ şi afirmaţia teoremei este adevărată (teorema lui Euclid). Pentru $n = 2$, $\{nk - 1 \mid k \in \mathbb{N}\} = \{-1, 1, 3, 5, 7, \ldots\}$ şi afirmaţia teoremei este adevărată (există o infinitate de numere prime impare).

Pentru demonstraţia teoremei în cazul $n > 2$ vom folosi lema următoare:

Lemă. *Pentru orice număr natural n, $n > 1$, avem:*

$$\prod_{\substack{1 \leq r < n \\ (r,n)=1}} r \equiv \pm 1 \pmod{n}. \tag{5}$$

Demonstraţie. Pentru $n = 2$ congruenţa este evidentă. Pentru $n > 2$ şi r fixat, $1 \leq r < n$, $(r, n) = 1$, ştim că există soluţie unică pentru congruenţa $rx \equiv 1 \pmod{n}$. Deci, există un singur r', $1 \leq r' < n$, $(r', n) = 1$ astfel încât $rr' \equiv 1 \pmod{n}$. În membrul întâi al congruenţei (5) înlocuim produsele rr' cu 1 pentru toţi r pentru care $r' \neq r$. Rezultă că $\prod_{(r,n)=1} r \equiv \prod_{\substack{(r,n)=1 \\ r^2 \equiv 1 \pmod{n}}} r$. Observăm că pentru r cu proprietatea că $r^2 \equiv 1 \pmod{n}$ avem $r(n - r) \equiv -1 \pmod{n}$. Rezultă că membrul întâi al congruenţei (5) este congruent cu $(-1)^k$, unde $2k$ este numărul acelor r cu proprietatea $r^2 \equiv 1 \pmod{n}$ (r şi $n - r$ au ambii această proprietate). Lema este demonstrată.

Revenim la demonstraţia teoremei în cazul $n > 2$. Vom arăta prin reducere la absurd, că există o infiniate de numere prime p de forma $p = nak - 1$, $k \in \mathbb{N}$, unde a este produsul numerelor naturale mai mici ca n şi prime cu n luat cu semnul $+$ sau $-$ după cum produsul acestor numere este congruent cu $+1$ sau -1 modulo n. Presupunem că există un număr finit de numere p de forma $p = nak - 1$: $p_1, p_2, \ldots, p_s$. Considerăm numărul ajutător $N = nap_1p_2 \ldots p_s - 1$. $N > 1$ deoarece chiar în cazul $s = 0$, $N = na - 1 > n - 1 \geq 1$. Există p prim, $p \mid N$; p este de forma $p = nau + r$, $(r, Na) = 1$. Din $p = Nau + r \equiv nu + r \pmod{n}$ rezultă că p şi $nu + r$ dau acelaşi rest la împărţirea cu n. Rezultă că $r < n$ şi nu putem avea $1 < r < n - 1$ deoarece ar rezulta că $r \mid n$ sau $r \mid a$, deci $r \mid p$ şi contrazicem faptul că p este prim. Prin urmare, p este de forma $p = nau \pm 1$. Dacă toţi divizorii lui N ar fi de forma $p = nu + 1$, N ar fi şi el de această formă. Prin urmare, există un divizor prim p al lui N de forma $p = nau - 1$. Rezultă că $p \in \{p_1, p_2, \ldots, p_s\}$, $p \mid nap_1p_2 \ldots p_s$ şi cum $p \mid N$ am avea $p \mid 1$, deci $p = 1$ şi contrazicem definiţia numărului prim.

Teorema 2 se obţine din Teoremei 3 luând $n = 4$. Din Teorema 3 rezultă că există o infinitate de numere prime p de forma $p = 6k - 1$, $k \in \mathbb{N}$ sau $p = 8k - 1$, $k \in \mathbb{N}$ ş.a.m.d.

Pentru a arăta că progresia (2) conţine o infinitate de numere prime vom folosi următoarea

Lemă. *Oricare ar fi numărul natural n, $n > 1$, numărul $(n!)^2 + 1$ are divizori primi şi aceştia sunt de forma $p = 4k + 1$.*

Demonstraţie. Pentru $n > 1$, numărul $(n!)^2 + 1$ este impar, mai mare ca 1. Există $p \mid (n!)^2 + 1$, $p \neq 2$. Deci p este de forma $p = 4k + 1$ sau $p = 4k + 3$. Dacă p este de forma $p = 4k+3$, din $p \mid (n!)^2+1$ rezultă $p \mid (n!)^{2(2k+1)}+1$, adică $p \mid (n!)^{p-1}+1$ şi apoi $p \mid (n!)^p + n!$. Conform cu *mica teoremă a lui Fermat* $p \mid (n!)^p - n!$. Rezultă $p \mid 2n!$, deci $p \leq n$, $p \mid n!$ ceea ce implică $p \mid 1$, contradicţie!

Teorema 4. *Există o infinitate de numere prime p de forma $p = 4k + 1$, $k \in \mathbb{N}$.*

Demonstraţie. Folosim din nou metoda lui Euclid. Presupunem că există un număr finit de numere prime de forma $4k + 1$: $p_1 = 5 < p_2 < \cdots < p_s$ şi considerăm numărul ajutător $N = [(p_1 p_2 \ldots p_s)!]^2 + 1$. Acesta admite, conform lemei, un divizor prim p de forma $p = 4k + 1$ şi ajungem din nou la contradicţia $p \mid 1$.

Pentru generalizarea Teoremei 4 avem nevoie de câteva chestiuni pregătitoare. Fie k un număr natural, $k \geq 1$. Ecuaţia $x^k - 1 = 0$ are rădăcinile $x_h = e^{\frac{2\pi h}{k} i} = \cos \dfrac{2h\pi}{k} + i \sin \dfrac{2h\pi}{k}$, $h = 0, 1, \ldots k - 1$. Considerăm polinomul $F_n(x) = \prod_{(h,n)=1} \left(x - e^{\frac{2h\pi}{k} i}\right)$, unde produsul se face după numerele $h \in \{0, 1, \ldots, n-1\}$ care sunt prime cu n. Gradul lui $F_n(x)$ este $\varphi(n)$ ($\varphi(n)$ = numărul numerelor naturale mai mici ca n şi prime cu n, este cunoscută sub numele de *funcţia indicatoare a lui Euler*). Observăm că $x^k - 1 = \prod_{n \mid k} F_n(x)$ (produsul se face după divizorii pozitivi ai lui k). Fie $x^k - 1 = F_k(x) G_k(x)$, unde $G_k(x)$ este cel mai mic multiplu comun al polinoamelor $x^n - 1$, $n \mid k$, $n < k$, având coeficientul termenului de grad cel mai înalt egal cu 1. Deoarece $G_k(x)$ este un polinom cu coeficienţi întregi, atunci şi $F_k(x)$ este un polinom cu coeficienţi întregi. Observăm că pentru orice număr întreg x, $x \neq \pm 1$, avem $F_k(x) G_k(x) \neq 0$.

Lema 1. *Fie n un divizor propriu al lui k ($n \neq 1$, $n \neq k$). Pentru orice număr întreg x, $x \neq \pm 1$, avem: $\left(x^n - 1, \dfrac{x^k - 1}{x^n - 1}\right) \mid k$.*

Demonstraţie. Notăm $k = nd$, $x^n - 1 = y$. Vom avea:

$$\frac{x^k - 1}{x^n - 1} = \frac{(y+1)^d - 1}{y} = y^{d-1} + C_d^1 y^{d-2} + \cdots + d \equiv d \pmod{y}.$$

Dacă $\delta = \left(x^n - 1, \dfrac{x^k - 1}{x^n - 1}\right)$, din $\delta \mid y$ rezultă $\delta \mid d$ şi, cum $d \mid k$, rezultă $\delta \mid k$.

Lema 2. *Fie $x \in \mathbb{Z}$, $x \neq \pm 1$. Orice divizor prim, comun lui $F_k(x)$ şi $G_k(x)$ este un divizor al lui k.*

Demonstraţie. Fie p prim, $p \mid F_k(x)$, $p \mid G_k(x)$. Din $p \mid G_k(x)$ rezultă că există $n \in \mathbb{N}^*$, $n \mid k$, $n < k$, astfel încât $p \mid F_n(x)$ (deoarece $G_k(x) = \prod_{n \mid k,\, k<x} F_n(x)$ şi dacă un număr prim divide un produs atunci el divide cel puţin unul dintre factori). Din $p \mid x^n - 1$ şi $p \mid F_k(x)$ rezultă $p \mid \dfrac{x^k - 1}{x^n - 1}$ şi $p \mid \left(x^{n-1}, \dfrac{x^k - 1}{x^n - 1}\right)$. Conform Lemei 1, $p \mid k$.

Teorema 5. *Pentru orice număr natural k, $k \geq 1$, există o infinitate de numere prime de forma $p = nk + 1$, $n \in \mathbb{N}$.*

Demonstraţie. Pentru $k = 1$ enunţul teoremei este adevărat (*teorema lui Euclid*). Pentru $k > 1$, arătăm mai întâi că există numere prime de forma $p = nk + 1$.

Pentru $x = ky$, $y \in \mathbb{Z}$ vom avea: $F_k(x) G_k(x) = x^k - 1 \equiv -1 \pmod{k}$. Deoarece ecuaţiile $F_k(x) = \pm 1$ au un număr finit de rădăcini, putem alege y astfel încât $F_k(x) \neq \pm 1$. Există numere prime p care sunt divizori ai lui $F_k(x)$. Deoarece $p \nmid k$ $(p \mid k \Rightarrow p \mid x \Rightarrow p \mid 1)$, rezultă (conform Lemei 2) că $p \nmid G_k(x)$ şi deci $p \nmid x^n - 1$, oricare ar fi numărul natural n, $n \mid k$, $n < k$. Deci $x^n \not\equiv 1 \pmod{n}$, $n \mid k$, $n < k$ şi $x^k \equiv 1 \pmod{n}$. Fie $n = (k, p-1)$. Există două numere întregi s şi t astfel încât $n = sk + t(p-1)$. Rezultă că $x^n = \left(x^k\right)^s \left(x^{p-1}\right)^t \equiv 1 \pmod{p}$. Nu putem avea $n < k$, deci $n = k$. Conform cu *mica teoremă a lui Fermat* $x^{p-1} \equiv 1 \pmod{p}$. Rezultă că $p-1$ este multiplu de k. Într-adevăr, dacă δ este cea mai mică putere întreagă, strict pozitivă a lui x astfel încât $x^\delta \equiv 1 \pmod{p}$, atunci $x^a \equiv 1 \pmod{p} \Leftrightarrow \delta \mid a$. Dacă $a = \delta b$, atunci $x^a = \left(x^\delta\right)^b \equiv 1 \pmod{p}$. Dacă $x^a \equiv 1 \pmod{p}$, $a = b\delta + r$, $0 \leq r < \delta$, nu putem avea $\delta > 0$ deoarece $x^a \equiv x^r \equiv 1 \pmod{p}$ şi contrazicem alegerea lui δ. Deci, $p - 1 = nk$, adică $p = nk + 1$.

Fie p_1 un număr prim de forma $p_1 = n_1 k + 1$. Luăm $k_1 = p_1 k$. Conform primei părţi a demonstraţiei există un număr prim p_2 de forma $p_2 = np_1 k + 1$, adică pentru orice număr prim p_1 de forma $p_1 = nk + 1$ există un număr prim p_2 de aceeaşi formă, $p_2 > p_1$. Rezultă că există o infinitate de numere prime p de forma $p = nk + 1$, $n \in \mathbb{N}$.

Enunţul cel mai general, care cuprinde drept cazuri particulare toate teoremele prezentate, îl constitue teorema următoare, cunoscută în literatura matematică sub denumirea de *teorema lui Dirichlet*.

Teorema 6. *Oricare ar fi numerele $l \in \mathbb{Z}$ şi $k \in \mathbb{N}^*$, $(l, k) = 1$, progresia aritmetică*

$$l, l + k, l + 2k, \ldots l + nk, \ldots$$

conţine o infinitate de numere prime.

Condiţia $(l, k) = 1$ este necesară . Dacă $(l, k) = d > 1$, toţi termenii progresiei sunt multipli de d. Demonstraţia Teoremei 6, în cazul general, nu poate fi făcută prin metode ale matematicii elementare.

Problema numărului de numere prime dintr-o progresie aritmetică a fost pusă pentru prima oară în 1775 de *Leonard Euler* în cazul particular $l = 1$. În cartea sa *"Théorie des nombres" A. M. Legendre* a dat o demonstraţie Teoremei 6 bazată pe o ipoteză, care ulterior s-a dovedit a fi falsă. Prima demonstraţie a teoremei a fost dată în 1837 de *Lejeune P. G. Dirichlet* care a creat un aparat analitic special (*seriile Dirichlet*). Demonstraţia lui *Dirichlet* este considerată actul de naştere al teoriei analitice a numerelor.

Bibliografie

1. **I. Creangă, C. Cazacu, P. Minuţ, Gh. Opaiţ, C. Reischer** - *Introducere în teoria numerelor*, Editura didactică şi pedagogică, Bucureşti, 1965.
2. **Hua Loo Keng** - *Introduction to Number Theory*, Springer Verlag, Berlin, Heidelberg, 1982.
3. **P. Minuţ** - *Teoria numerelor. Capitole introductive*, Editura "Crenguţa Gâldău", Iaşi, 1997.
4. **C. P. Popovici** - *Teoria numerelor*, Ed. didactică şi pedagogică, Bucureşti, 1973.
5. **W. Sierpinski** - *Ce ştim şi ce nu ştim despre numerele prime*, Editura ştiinţifică, Bucureşti, 1966.