SESIUNEA DE COMUNICĂRI MATEMATICE

Șirul numerelor naturale prime este infinit

Turturică Luminița Ștefania

Universitatea Ovidius din Constanța
Facultatea de matematică și informatică

Decembrie 2023

Despre Euclid

Numit și *Euclid din Alexandria*, Euclid a fost un matematician grec care a trăit și a predat în Alexandria în Egipt, în timpul domniei lui Ptolemeu I (323-283 î.Hr.). Este cunoscut prin opera sa principală, *Elementele*, care sistematizează cunoașterea matematică dezvoltată în cursul secolelor anterioare.

http://aleph0.clarku.edu/ djoyce/ elements/bookI/bookI.html

Demonstrația lui Euclid

Fie mulțimea de numere prime

$$\{p_1, p_2, \cdots, p_r\}.$$

Considerăm numărul

$$n = p_1 p_2 \cdots p_r + 1.$$

Acesta are un divizor prim p care nu poate fi unul dintre p_i pentru că

$$p_i | n$$

și

$$p_i | p_1 \cdots p_r$$

ceea ce implică

$$p_i | 1,$$

imposibil. Astfel o mulțime finită

$$\{p_1, p_2, \cdots, p_r\}$$

nu poate fi colecție a tuturor numerelor prime.

Demonstrația cu numere Fermat

Să ne reamintim mai întâi numerele Fermat

$$F_n = 2^{2^n} + 1,$$

pentru orice $n = 1, 2, \cdots$. Vom demonstra că oricare două numere Fermat sunt relativ prime. Cum fiecare are cel puțin un divizor prim, trebuie să avem un număr infinit de numere prime. Se verifică ușor relația de recurență

$$\prod_{k=0}^{n-1} F_k = F_n - 2, n \geq 1,$$

prin inducție după n. Dacă m este un divizor pentru F_k și F_n, $k < n$, atunci m divide

$$\prod_{k=0}^{n-1} F_k - F_n = -2,$$

deci m divide 2 de unde rezultă că $m = 1$ sau $m = 2$. Dar numerele Fermat sunt impare deci $m = 2$ este imposibil.

Demonstrația cu numere Mersenne

Vom demonstra că oricum alegem un număr prim p găsim unul strict mai mare decât el. Vom considera numărul Mersenne

$$2^p - 1.$$

Vom arăta că orice factor prim q al lui $2^p - 1$ este mai mare decât p, de unde rezultă concluzia dorită. Fie q un număr prim care divide $2^p - 1$, deci

$$q | 2^p - 1,$$

adică

$$2^p \equiv 1 (\mod q).$$

Cum p este prim, înseamnă că elementul 2 are ordinul p în grupul multiplicativ $(\mathbf{Z}_q^*, \cdot)$ al corpului $\mathbf{Z}_q$.
Acest grup are $q - 1$ elemente. Conform teoremei lui Lagrange, avem

$$p | q - 1$$

de unde obținem $p < q$.

A patra demonstrație

Fie $\pi(x) = \#\{p \in \mathbf{P} | p \leq x\}$. Numerele din $\mathbf{P} = \{p_1, p_2, \cdots\}$ sunt în ordine crescătoare. Considerăm

$$\ln(x) = \int_1^x \frac{1}{t}\, dt = \int_1^2 \frac{1}{t}\, dt + \int_2^3 \frac{1}{t}\, dt + \cdots + \int_n^x \frac{1}{t}\, dt$$

Dacă $n \leq x < n+1 \implies \ln(x) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \sum \frac{1}{m}$, unde $\sum \frac{1}{m}$ se extinde la toate numerele naturale m care au numai divizori primi $p \leq x$.

$$\sum \frac{1}{m} = \sum \prod_{p \leq x} \frac{1}{p^{k_p}} = \prod_{p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

$$\implies \ln(x) \leq \prod_{p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \tag{1}$$

Evident, $p_k \geq k+1, \forall k$. Din (1) $\implies \ln(x) \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$. Cum $\lim_{x\to\infty} \ln(x) = \infty \implies \lim_{x\to\infty} \pi(x) = \infty$.

A cincea demonstrație

Topologie pe $\mathbf{Z}$: Pentru $a, b \in \mathbf{Z}, b > 0, N_{a,b} = \{a + nb | n \in \mathbf{Z}\}$. $\mathcal{O} \subset \mathbf{Z}$ este deschisă dacă $\mathcal{O} = \varnothing$ sau $\forall a \in \mathcal{O}, \exists b > 0$ astfel încât $N_{a,b} \subset \mathcal{O}$.

Observație

$\mathcal{O}$ deschisă și $\mathcal{O} \neq \varnothing \implies \mathcal{O}$ este infinită.

Observație

$$N_{a,b} = \mathbf{Z} - \bigcup_{i=1}^{b-1} N_{a+i,b},$$

deci $N_{a,b}$ este închisă. Pentru $n \neq \pm 1, \exists p$ prim astfel încât $p | x \implies x \in N_{0,p}$, deci

$$\mathbf{Z} - \{\pm 1\} = \bigcup_{p \in \mathbf{P}} N_{0,p}.$$

$\mathbf{P} =$ *finită* $\implies \bigcup_{p \in \mathbf{P}} N_{0,p}$ *închisă* $\implies \{\pm 1\}$ *este deschisă, contradicție.*

Infinitatea numerelor prime prin formula lui Euler pentru π

Euler a publicat mai multe formule pentru numărul π. Una dintre acestea este

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1}.$$

John Arioni a sugerat o modalitate de a deduce această formulă care aduce aminte de tratarea lui Euler asupra seriei armonice:

$$\begin{aligned}
\frac{\pi}{4} &= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots \\
&= \left(1 - \frac{1}{3} + \frac{1}{3^2} - \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots\right)\left(1 - \frac{1}{7} + \frac{1}{7^2} - \cdots\right)\cdots \\
&= \prod_{p \equiv 3 mod 4} \sum_{k=0}^{\infty} \frac{(-1)^k}{p^k} \prod_{p \equiv 1 mod 4} \sum_{k=0}^{\infty} \frac{1}{p^k} = \prod_{p \equiv 3 mod 4} \frac{p}{1+p} \prod_{p \equiv 1 mod 4} \frac{p}{1-p}.
\end{aligned}$$

Infinitatea numerelor prime. Demonstrație pe un singur rând

Dacă mulțimea numerelor prime este finită atunci are loc următoarea inegalitate:

$$0 < \prod_p \sin\left(\frac{\pi}{p}\right) = \prod_p \sin\left(\frac{\pi(1 + 2\prod_{p'} p')}{p}\right) = 0.$$

S. Northshield, A One-Line Proof of the Infinitude of Primes, *Am Math Monthly* Volume 122, Number 5, May 2015, pp. 466-466(1)

$$\sin\frac{\pi}{p} = \sin\left(\frac{\pi}{p} + \frac{\pi \cdot 2\prod_{p'} p'}{p}\right) \text{ pentru că } \frac{\pi \cdot 2\prod_{p'} p'}{p} = 2k\pi, k \in \mathbf{Z}.$$

Fie $1 + 2\prod_{p'} p' = q$. Atunci q are un divizor prim p, deci $q = pq'$, și

$$\sin\left(\frac{\pi \cdot pq'}{p}\right) = \sin q'\pi = 0.$$

Infinitatea numerelor prime folosind puteri ale lui 2

Pentru orice număr întreg pozitiv n, expresia

$$f(n) = 2^{2^{n+1}} + 2^{2^n} + 1$$

are cel puțin $n + 1$ factori primi diferiți.

Demonstrație

Demonstrăm afirmația prin inducție și folosind relația:

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1). \tag{2}$$

Să presupunem că

$$2^{2^{k+1}} + 2^{2^k} + 1$$

are cel puțin $k + 1$ factori diferiți. Atunci

$$2^{2^{k+2}} + 2^{2^{k+1}} + 1 = (2^{2^{k+1}} + 2^{2^k} + 1)(2^{2^{k+1}} - 2^k + 1).$$

Dar

$$2^{2^{k+1}} + 2^{2^k} + 1 \text{ și } 2^{2^{k+1}} - 2^{2^k} + 1$$

sunt relativ prime. Atunci

$$2^{2^{k+2}} + 2^{2^k} + 1$$

va avea cel puțin

$$(k + 1) + 1 = k + 2$$

factori distincți.

$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+2} + F_n, \forall n \geq 0$. Presupunem că există un număr finit de numere prime:

$$2, p_1, p_2, \cdots, p_k, \text{ unde } p_1, \cdots, p_k$$

sunt impare. Astfel, elementele din lista numerelor lui Fibonacci $F_{p_1}, F_{p_2}, \cdots, F_{p_k}$, trebuie să fie divizibile prin numere prime diferite deoarece $cmmdc(F_{p_i}, F_{p_j}) = 1, i \neq j$. Deci fiecare $F_{p_i}, i = 1, \cdots, k$ este divizibil cu un singur număr prim din lista $p_1, \cdots, p_k$.. Prin urmare, F_{p_i} trebuie să fie de forma

$$2^a p^b,$$

unde p este număr prim impar. Dar, $F_{19} = 37 \cdot 113$ nu este un asemenea număr. Deci presupunerea că avem un număr finit de numere prime este falsă.

$\sum_{p\in\mathbf{P}} \frac{1}{p}$ este divergentă

Arătăm mai mult decât că există o infinitate de numere prime și anume arătăm că seria

$$\sum_{p\in\mathbf{P}} \frac{1}{p}$$

este divergentă. Demonstrația dată se datorează lui Erdös. Presupunem că

$$\sum_{p\in\mathbf{P}} \frac{1}{p}$$

converge. Atunci există $k \in \mathbf{N}$ astfel încât

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Numim $p_1, p_2, \cdots, p_k$ numere prime "mici" și $p_{k+1}, p_{k+2}, \cdots$ numere prime "mari". Pentru un număr arbitrar N avem:

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Fie N_s numărul întregilor strict pozitivi $n \leq N$ care sunt divizibili cu cel puțin un număr prim "mic" și N_b numărul întregilor strict pozitivi $n \leq N$ care sunt divizibili cu cel puțin un număr prim "mare". Vom demonstra că

$$N_b + N_s < N$$

și așa obținem contradicție, pentru că, de fapt, $N = N_b + N_s$.

$$N_b \leq \sum_{i \geq k+1} \left[\frac{N}{p_i}\right] \leq \sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Acum ne uităm la N_s. Scriem

$$n = a_n b_n^2, \tag{3}$$

unde $a_n =$ parte liberă de pătrate, deci fiecare a_n este un produs de numere prime "mici" diferite. Cum $\{p_1, \cdots, p_k\}$ are 2^k submulțimi, există cel mult 2^k părți libere de pătrate. Avem

$$b_n^2 \leq a_n b_n^2 \implies b_n \leq \sqrt{n} \leq \sqrt{N}.$$

Obținem

$$N_s \leq 2^k \sqrt{N}$$

Putem alege N astfel încât

$$2^k\sqrt{N} \leq \frac{N}{2} \iff N \geq 2^{2k+2}.$$

Fie acum

$$N = 2^{2k+2} \implies N_b + N_s < \frac{N}{2} + \frac{N}{2} \implies N_b + N_s < N,$$

contradicție, pentru ca $N = N_b + N_s$.

Bibliografie

1. Aigner M., Ziegler G.M., *Proofs from THE BOOK*, Springer, 2013.

2. https://www.cut-the-knot.org/proofs/OneLineProofOfInfinitudeOfPrimes.shtml

VĂ MULȚUMESC PENTRU ATENȚIE!