NUMERE PRIME. NUMERE COMPUSE

Rezumat. Articolul prezintă câteva rezultate legate de numerele prime (infinitatea numerelor prime, descompunerea în factori primi, numărul divizorilor naturali, forma numerelor prime, numerele prime și pătratele sau cuburile perfecte), precum și exemple de probleme reprezentative cu numere prime.

Lecția se adresează clasei a VI-a.

Autor: Ion Cicu, profesor, Școala Gimnazială nr. 96, București

Numerele prime reprezintă o clasă specială în mulțimea numerelor naturale.

Definiție. Numim *număr prim* orice număr natural $p \geq 2$ care are exact doi divizori naturali, pe 1 și pe el însuși. Orice număr natural diferit de 0 și de 1 care nu este număr prim se numește *număr compus*.

Observație. 2 este singurul număr prim care este și număr par. Toate celelalte numere prime sunt impare.

Justificare. Orice număr par mai mare decât 2 se divide cu 2, deci are și alți divizori în afară de 1 și de el însuși; prin urmare, nu este număr prim.

O modalitate de a găsi numerele prime mai mici sau egale cu un număr dat n o reprezintă *ciurul lui Eratostene*. Pentru aceasta, scriem în ordine crescătoare numerele naturale de la 2 până la n și apoi eliminăm pe rând multiplii lui 2 (în afară de 2), multiplii lui 3 (în afară de 3), multiplii următorului număr pe care nu l-am eliminat încă (în afară de el) și așa mai departe. Ne oprim în momentul în care următorul număr neeliminat, să-l notăm p, verifică relația $p^2 > n$. Numerele rămase în șir sunt numere prime.

De exemplu, pentru $n = 25$ eliminăm multiplii lui 2 și ai lui 3, apoi multiplii lui 5; abia după aceea ne oprim, pentru că următorul număr neeliminat este 7 și $7^2 > 25$. Dacă ne-am fi oprit la 5 (pentru care $5^2 = 25$), numărul compus 25 ar fi rămas în șir.

Câte numere prime există?

Problema numărului de numere prime a fost rezolvată încă din Antichitate de Euclid.

Teoremă. Există o infinitate de numere prime.

Demonstrație. Presupunem, prin reducere la absurd, că există doar un număr finit de numere prime și notăm cu $P = \{p_1, p_2, \ldots, p_n\}$ mulțimea tuturor numerelor prime. Construim numărul

$$r = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Numărul r este mai mare decât 1, deci are cel puțin un divizor prim; să-l notăm cu q. Cum P conține toate numerele prime, q este unul dintre numerele $p_1, p_2, \ldots, p_n$, deci q divide produsul $p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Atunci q divide și diferența $r - p_1 \cdot p_2 \cdot \ldots \cdot p_n = 1$, ceea ce este imposibil. Am ajuns la o contradicție, deci mulțimea numerelor prime nu este finită. □

Atenție! Demonstrația nu spune că numărul $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ este întotdeauna prim. De exemplu, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$. Ea spune doar că divizorii primi ai acestui număr sunt diferiți de $p_1, p_2, \ldots, p_n$.

Descompunerea în factori primi

Cel mai important rezultat referitor la numerele prime îl reprezintă teorema fundamentală a aritmeticii.

Teoremă. Orice număr compus se scrie ca produs de numere prime, nu neapărat diferite. Scrierea este unică dacă nu ținem seama de ordinea factorilor.

Demonstrație (existența scrierii). Fie N un număr compus. Fiind număr compus, N are un divizor număr prim; să-l notăm cu p_1. Atunci putem scrie

$$N = p_1 \cdot N_1, \quad \text{cu } N_1 < N.$$

Acum, pentru N_1 putem avea două situații: este număr prim sau este număr compus. Dacă N_1 este număr prim, am terminat: numărul N s-a scris ca produs de două numere prime. Dacă N_1 este număr compus, atunci el are un divizor număr prim; să-l notăm cu p_2. Vom putea scrie

$$N_1 = p_2 \cdot N_2, \quad \text{cu } N_2 < N_1,$$

și atunci N se va scrie

$$N = p_1 \cdot p_2 \cdot N_2, \quad \text{cu } N_2 < N_1 < N.$$

Considerațiile făcute despre N_1 le putem face acum despre N_2. Procedând astfel, vom ajunge ca în scrierea lui N ca produs să apară numai factori primi. Procesul se termină la un moment dat, deoarece numerele $N_1, N_2, \ldots$ devin din ce în ce mai mici. □

Unicitatea scrierii o admitem aici fără demonstrație.

Deoarece o parte dintre factori pot fi egali, pentru orice număr compus N putem scrie

$$N = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}, \tag{1}$$

unde $p_1, p_2, \ldots, p_k$ sunt factorii primi (diferiți) ai produsului, iar $n_1, n_2, \ldots, n_k$ ne arată de câte ori se repetă fiecare factor. Scrierea (1) se numește *descompunerea numărului N în produs de puteri de numere prime*. Uneori spunem mai simplu *descompunerea în factori primi a numărului N*.

Exemplu. Să luăm numărul 24. Avem $24 = 2 \cdot 12$. Deoarece $12 = 2 \cdot 6$, putem scrie $24 = 2 \cdot 2 \cdot 6$. Acum, pentru că $6 = 2 \cdot 3$, vom scrie

$$24 = 2 \cdot 2 \cdot 2 \cdot 3, \quad \text{adică} \quad 24 = 2^3 \cdot 3.$$

Calculele de mai sus pot fi așezate astfel: în stânga liniei verticale scriem numărul dat și, sub el, câturile obținute pe rând; în dreapta scriem factorul prim la care împărțim numărul de pe același rând.

24	2
12	2
6	2
3	3
1	

Atunci $24 = 2^3 \cdot 3$.

Numărul divizorilor unui număr natural

Faptul că un număr natural se scrie ca produs de puteri de numere prime ne permite să aflăm numărul divizorilor naturali ai acelui număr.

Să presupunem că $N = p_1^{n_1}$. Atunci divizorii lui N sunt $1, p_1, p_1^2, \ldots, p_1^{n_1}$. Observăm că numărul divizorilor este $n_1 + 1$.

Dacă $N = p_1^{n_1} \cdot p_2^{n_2}$, pentru a scrie toți divizorii vom folosi tabelul de mai jos. În acest tabel, pe prima linie sunt scrise puterile lui p_2 (începând cu $p_2^0 = 1$), iar pe prima coloană puterile lui p_1. Toți ceilalți divizori se obțin prin înmulțirea unui element din prima coloană cu un element de pe prima linie.

1	p_2	p_2^2	$\cdots$	$p_2^{n_2}$
p_1	$p_1 \cdot p_2$	$p_1 \cdot p_2^2$	$\cdots$	$p_1 \cdot p_2^{n_2}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$p_1^{n_1}$	$p_1^{n_1} \cdot p_2$	$p_1^{n_1} \cdot p_2^2$	$\cdots$	$p_1^{n_1} \cdot p_2^{n_2}$

Numărul divizorilor este egal cu numărul căsuțelor din tabel, iar acesta se obține înmulțind numărul căsuțelor de pe prima coloană cu numărul căsuțelor de pe prima linie. Cum pe prima coloană avem $n_1 + 1$ căsuțe, iar pe prima linie $n_2 + 1$ căsuțe, tragem concluzia că numărul divizorilor lui $N = p_1^{n_1} \cdot p_2^{n_2}$ este $(n_1 + 1)(n_2 + 1)$. În general, putem formula următoarea

Teoremă. Numărul divizorilor naturali ai numărului $N = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ este egal cu

$$(n_1 + 1)(n_2 + 1) \ldots (n_k + 1).$$

Alte teoreme despre numere prime

Teoremă. Orice număr prim $p \geq 5$ are forma $6k + 1$ sau $6k + 5$.

Demonstrație. Orice număr natural are una dintre formele $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$ sau $6k + 5$. Numerele de forma $6k$, $6k + 2$ și $6k + 4$ se divid cu 2, iar cele de forma $6k + 3$ se divid cu 3; cum sunt mai mari decât 3, ele nu sunt numere prime. Rămân doar formele $6k + 1$ și $6k + 5$. □

Atenție! Din teorema anterioară nu putem trage concluzia că un număr de forma $6k + 1$ sau $6k + 5$ este număr prim (de exemplu, $25 = 6 \cdot 4 + 1$ nu este prim). Ceea ce putem afirma este că un număr despre care știm deja că este prim și mai mare decât 3 are una dintre aceste forme.

Teoremă. Dacă un număr prim p divide un pătrat perfect N, atunci p^2 îl divide pe N.

Demonstrație. Dacă N este pătrat perfect, atunci $N = A^2$. Fie $A = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ descompunerea în factori primi a lui A. Atunci $N = p_1^2 \cdot p_2^2 \cdot \ldots \cdot p_k^2$. Din ipoteză, p divide N, deci, din unicitatea descompunerii în factori primi, p este unul dintre factorii $p_1, p_2, \ldots, p_k$. Cum fiecare p_i apare la puterea a doua, rezultă că p^2 divide pe N. □

La fel putem arăta următoarea

Teoremă. Dacă un număr prim p divide un cub perfect N, atunci p^3 îl divide pe N.

Probleme cu numere prime

Problema 1. Găsiți numerele prime a, b, c știind că $a + 4b + 8c = 66$.

Soluție. Rezolvarea unei astfel de probleme se bazează pe paritatea numerelor și pe faptul că suma a două numere de aceeași paritate este un număr par, iar suma a două numere de parități diferite este un număr impar. În cazul nostru, $4b$ și $8c$ sunt numere pare. De asemenea, 66 este un număr par. Rezultă că a trebuie să fie număr par. Cum a este număr prim, obținem $a = 2$. Atunci ecuația devine $2 + 4b + 8c = 66$, adică $4b + 8c = 64$. Împărțind prin 4, rezultă $b + 2c = 16$. Acum, $2c$ este număr par și 16 este număr par, deci b este număr par. Cum b este număr prim, avem $b = 2$. Înlocuind în ultima relație, obținem $c = 7$, care este număr prim. Așadar $a = 2$, $b = 2$, $c = 7$.

Problema 2. Determinați numerele naturale n pentru care toate numerele n, $n + 4$, $n + 6$, $n + 10$, $n + 12$, $n + 16$, $n + 22$ sunt numere prime.

Soluție. Ideea de rezolvare este următoarea: găsim, prin încercări, o soluție și apoi arătăm că este unică. În cazul nostru, observăm că pentru $n = 7$ obținem numerele 7, 11, 13, 17, 19, 23 și 29, toate numere prime.

Să arătăm acum că $n = 7$ este singura soluție. Orice număr natural, în raport cu 7, are una dintre formele $7k$, $7k+1$, $7k+2$, $7k+3$, $7k+4$, $7k+5$, $7k+6$. Cu excepția lui 7, niciun număr de forma $7k$ nu este număr prim, deci, dacă $n \neq 7$, atunci n nu are forma $7k$. Mai departe:

- pentru $n = 7k + 1$, avem $n + 6 = 7k + 7 = 7(k + 1)$;
- pentru $n = 7k + 2$, avem $n + 12 = 7k + 14 = 7(k + 2)$;
- pentru $n = 7k + 3$, avem $n + 4 = 7k + 7 = 7(k + 1)$;
- pentru $n = 7k + 4$, avem $n + 10 = 7k + 14 = 7(k + 2)$;
- pentru $n = 7k + 5$, avem $n + 16 = 7k + 21 = 7(k + 3)$;
- pentru $n = 7k + 6$, avem $n + 22 = 7k + 28 = 7(k + 4)$.

În fiecare caz am obținut un multiplu al lui 7 mai mare decât 7, deci un număr care nu este prim, cu două excepții, care apar pentru $k = 0$: $n = 1$, pentru care $n + 6 = 7$, dar $n = 1$ nu este prim, și $n = 3$, pentru care $n + 4 = 7$, dar $n + 6 = 9$ nu este prim. În concluzie, singura soluție este $n = 7$.

Problema 3. Arătați că, dacă n este un număr natural nenul care are un număr par de divizori, atunci n nu poate fi pătrat perfect.

Soluție. Numărul 1 are un singur divizor, deci $n \geq 2$. Dacă n este număr prim, atunci n nu este pătrat perfect: n se divide cu n, dar nu se divide cu n^2 (vezi teorema despre numerele prime care divid un pătrat perfect).

Fie acum n un număr compus și descompunerea sa în factori primi

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k},$$

unde $p_1, p_2, \ldots, p_k$ sunt factorii primi (diferiți) ai descompunerii, $n_1, n_2, \ldots, n_k$ sunt numere naturale nenule, iar $k \geq 1$ este un număr natural.

Un număr natural a este pătrat perfect dacă există un număr natural b astfel încât $a = b^2$. Dacă $n = b^2$, atunci descompunerea în factori primi a lui n se obține ridicând la pătrat descompunerea lui b, deci toți exponenții sunt numere pare (descompunerea fiind unică). Așadar, numărul $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ poate fi pătrat perfect numai dacă toți exponenții care apar sunt numere pare.

Numărul divizorilor lui n este $(n_1+1)(n_2+1)\ldots(n_k+1)$ și, cum acesta este un număr par, deducem că cel puțin un factor al produsului este număr par. Numerotând convenabil factorii primi, putem presupune că acesta este primul, n_1+1. Deci $n_1+1=2m$, cu m număr natural nenul, de unde $n_1=2m-1$, adică un număr impar.

Deoarece unul dintre exponenți este număr impar, tragem concluzia că n nu poate fi pătrat perfect.