

DIVIZIBILITATE

ABSTRACT. Articolul prezintă câteva rezultate și exemple privind divizibilitatea.

Lecția se adresează clasei a VI-a.

Autori:

Roxana Diaconescu, profesor Colegiul German Goethe, București

Radu Gologan, președintele Comisiei Naționale a Olimpiadei de Matematică

Rezultatul fundamental în teoria divizibilității numerelor întregi, este teorema împărțirii cu rest. Aceasta caracterizează câtul și restul unei împărțiri, determinându-le în mod unic. Să reamintim enunțul formal al acestei teoreme:

Teoremă. Fiind date numerele întregi m și n , cu $n > 0$, există și sunt unice numerele întregi q și r , astfel încât

$$1. \quad n = mq + r$$

$$2. \quad 0 \leq r < m$$

Numărul q unic determinat mai sus se numește câtul împărțirii iar numărul r unic determinat cu condițiile de mai sus se numește restul împărțirii.

Exemplu: Restul împărțirii numărului -7 la 4 este 1 , căci $-7 = 4 \cdot (-2) + 1$, $0 \leq 1 < 4$ iar restul împărțirii lui 7 la 4 este 3 , căci $7 = 4 \cdot 1 + 3$ și $0 \leq 3 < 4$.

Observație. Dacă considerăm n un număr natural nenul fixat, iar p și q sunt două numere întregi ce dau același rest la împărțirea cu n , vom spune că p și q sunt congruente modulo n și vom scrie $p \equiv q \pmod{n}$.

Astfel dacă r este restul împărțirii lui m la n , avem și $m \equiv r \pmod{n}$.

Aceste notații sunt uneori utile pentru simplificarea scrierii. Nu le vom folosi pe parcursul acestei lecții.

Definiție. Numărul întreg n se divide la numărul natural nenul m , dacă există numărul întreg q altfel încât să avem $n = mq$.

Observația 1. Găsirea lui q din definiția divizibilității se face, de regulă, prin împărțirea lui n la m ; trebuie să obținem restul 0.

Observația 2. Evident numărul 0 se divide la orice număr natural nenul, datorită acestei definiții.

Observația 3. Notăm $m|n$ și citim "m divide n".

Notăm $n:m$ și citim "n se divide cu m".

Se mai spune că m este divizor al lui n

Atenție! Pentru claritatea expunerii și pentru a evita confuziile, considerăm că divizorii sunt întotdeauna numere naturale nenule; deîmpărțitul putând fi și negativ.

Definiție. Un număr natural p , mai mare sau egal cu 2, se numește număr prim dacă singurii săi divizori sunt 1 și el însuși.

Astfel, putem scrie primii termeni ai șirului numerelor prime:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

Încă din antichitate, Euclid a arătat că mulțimea numerelor prime este infinită, iar cea mai mare problemă nerezolvată a matematicii actuale, conjectura lui Riemann, se referă la structura mulțimii numerelor prime. Din păcate explicarea ei depășește mult cadrul unor cunoștințe școlare, dar poate fi înțeleasă după ceva studii speciale de matematică, și poate, cine știe, unul dintre voi va contribui în viitor la rezolvarea ei.

Numerele prime sunt importante pentru că sunt de fapt "cărămizile" aritmeticii, în sensul dat de următoarea

Teoremă. (de descompunere în factori primi) Orice număr natural nenul se scrie în mod unic sub forma

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$$

unde p_1, p_2, \dots, p_k sunt numere prime diferite de 1, iar a_1, a_2, \dots, a_k sunt numere naturale mai mari sau egale cu 1

Scrierea de mai sus cu indici nu trebuie să vă sperie; uitați-vă la câteva exemple:

Avem $360 = 2^3 \cdot 3^2 \cdot 5^1$. Aici $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ și $a_1 = 3$, $a_2 = 2$, $a_3 = 1$.

Deoarece $144 = 2^4 \cdot 3^2$, avem $p_1 = 2$, $p_2 = 3$ și $a_1 = 4$, $a_2 = 2$.

Din această teoremă punem deduce ușor că un număr n se divide la m dacă și numai dacă orice factor prim al lui m este factor prim al lui n și exponentul său în descompunerea lui m este mai mic sau egal cu exponentul său în descompunerea lui n .

Exemplu: $m = 2^3 \cdot 3^2 \cdot 5$ divide $n = 2^3 \cdot 3^5 \cdot 5^2$.

Este foarte important să știți că această teoremă (descompunerea în factori primi) constituie baza unuia din rezultatele moderne din teoria codurilor: coduri imposibil de "spart" se pot construi pe baza descompunerii în factori a unor numere foarte mari (rezultat al matematicienilor Rivest, Shamier și Adelman; pentru o documentare mai adâncă vă recomandăm capitolul I al celebrei cărți; *Vârsta de aur a matematicii* de Keith Devlin, apărută în traducere la Fundația Theta theta@theta.ro.)

O consecință importantă a reprezentării unui număr natural prin descompunerea sa canonică în factori primi, $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, este posibilitatea de a determina numărul divizorilor naturali ai unui număr.

Teoremă. Numărul de divizori naturali ai numărului n având scrierea canonică de mai sus este $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$.

Pentru a demonstra acest rezultat este suficient să observăm că orice divizor are forma $n = p_1^{b_1} \cdot p_2^{b_2} \cdots p_k^{b_k}$ cu $b_1 \leq a_1, b_2 \leq a_2, \dots, b_k \leq a_k$, deci va trebui să numărăm în câte feluri putem găsi sisteme (b_1, b_2, \dots, b_k) cu această proprietate. Cum e foarte simplu de văzut că numerele naturale mai mici decât a_1 sunt $0, 1, 2, \dots, a_1$, în număr de $a_1 + 1$, numere naturale mai mici decât a_2 sunt la fel $a_2 + 1$, și așa mai departe, rezultă că numărul de astfel de sisteme, deci divizori, este $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$.

Exemplu: Numărul $1960 = 2^3 \cdot 5 \cdot 7^2$ are $(3 + 1)(1 + 1)(2 + 1) = 24$ de divizori.

CÂTEVA CONSECINȚE ALE ACESTOR NOȚIUNI ȘI REZULTATE

1. Cel mai mare divizor comun a două numere naturale m și n este, prin definiție, numărul natural cel mai mare ce divide atât m cât și n

(Acest lucru se poate formaliza astfel: d este cel mai mare divizor comun al numerelor m, n dacă $d|n, d|m$ și pentru orice alt număr d' cu $d'|n, d'|m$ avem că $d'|d$).

Se prescurtează uneori prin cmmdc și se notează $(m; n)$.

De exemplu dacă $m = 40 = 2^3 \cdot 5$ și $n = 60 = 2^2 \cdot 3 \cdot 5$, atunci $(m; n) = 2^2 \cdot 5$: deduceți de aici o regulă prin care din scrierea în factori primi a două numere, aflați cel mai mare divizor comun al lor.

Definiție. Două numere m, n se numesc **relativ prime** (sau prime între ele, sau mutual prime) dacă $(m, n) = 1$; altfel spus nu au nici un factor prim comun diferit de 1.

Se demonstrează următorul rezultat important, ce caracterizează algebric faptul că două numere sunt mutual prime.

Teoremă. Două numere naturale m și n sunt relativ prime atunci și numai atunci când există numerele naturale x și y astfel încât $mx - ny = \pm 1$

Aici ± 1 înseamnă una dintre valorile $+1$ sau -1 .

Enunțul de mai sus afirmă de fapt două rezultate: unul direct și altul reciproc. Avem de arătat că dacă numerele sunt relativ prime avem o relație de forma celei de mai sus și reciproc, relația de mai sus implică faptul că numerele sunt prime între ele.

Vom demonstra deocamdată ultima afirmație. Să presupunem pentru acesta că d este un divizor comun pentru m și n (dorim de fapt să arătăm că $d = 1$ este singura posibilitate). Există atunci numerele naturale n_1 și m_1 cu $m = dm_1$ și $n = dn_1$. Introducând acestea în relația $mx - ny = \pm 1$, deducem $dm_1x - dn_1y = \pm 1$ sau $d(m_1x - n_1y) = \pm 1$, ceea ce înseamnă că $d | \pm 1$ adică $d = 1$. Aceasta încheie demonstrația.

2. Observația următoare este extrem de utilă în descrierea unor algoritmi (metode) de calcul ale celui mai mare divizor comun și este în esență ceea ce se numește în algebră **algoritmul lui Euclid**.

Dacă $m > n$ sunt numere naturale, atunci $(m, n) = (n, m) = (m - n, n)$

E un fapt ușor de probat: dacă $d | (m, n)$, deci $m = dm_1$ și $n = dn_1$, atunci $m - n = d(m_1 - n_1)$ deci $d | (m - n)$ și atunci $d | (m - n, n)$. Reciproc, dacă $d' | (m - n, n)$ rezultă la fel că $d' | (m, n)$, prin urmare numerele (m, n) și $(m - n, n)$ au aceeași divizori, deci coincid.

Exemplu: Iată un calcul de cmmdc:

$(451, 287) = (451 - 287, 287) = (287, 164) = (287 - 164, 164) = (123, 164) = (123, 41) = (123 - 41, 41) = (82, 41) = (41, 41) = 41$ deci $(451, 287) = 41$.

Exemplu: Să studiem dacă fracția $\frac{2n+13}{n+7}$ poate fi simplificată pentru vreo valoare număr natural n . Calculăm $(2n + 13, n + 7) = (n + 6, n + 7) = (n + 6, 1) = 1$, deci întotdeauna numărătorul și numitorul sunt prime între ele, fracția este prin urmare ireductibilă.

E importantă de reținut și noțiunea de cel mai mic multiplu comun a două numere naturale ca fiind cel mai mic număr divizibil prin ambele numere date.

Se prescurtează de obicei prin cmmmc și pentru m, n naturale se notează cu $[m, n]$ cmmmc .

Un exercițiu util vouă este următoarea formula de legătură între aceste noțiuni:

$$(m, n) \cdot [m, n] = m \cdot n.$$

3. Noțiunile de mai sus ne permit rezolvarea unor ecuații în numere întregi, numite *ecuații liniare cu 2 necunoscute*. Sunt ecuații de tipul $ax + by = c$ unde $(a, b) = 1$ (de fapt după simplificarea cu factorii comuni ai lui a și b aceasta se poate realiza întotdeauna).

Fie x_0, y_0 o soluție a acestei ecuații (de fapt se demonstrează că poate fi găsită întotdeauna; încercați ca exercițiu să folosiți teorema de la 1 pentru demonstrație).

Așadar avem $ax_0 + by_0 = c$. Dacă x_1, y_1 este o altă soluție în numere întregi, avem evident și $ax_1 + by_1 = c$. Prin scăderea celor două ecuații obținem $a(x_1 - x_0) + b(y_1 - y_0) = 0$ sau $a(x_1 - x_0) = b(y_0 - y_1)$. Cum a și b (prime între ele) nu au factori comuni, ultima egalitate implică $y_0 - y_1$ este multiplu de a iar $x_1 - x_0$ este multiplu de același factor de b , deci există k întreg cu $y_0 - y_1 = ka, x_1 - x_0 = kb$ sau $x_1 = x_0 + kb, y_1 = y_0 - ka$. Așadar toate soluțiile ecuației sunt de forma $x = x_0 + kb, y = y_0 - ka$.

Exemplu: Rezolvați în numere întregi ecuația $3x - 7y = 2$.

Se observă că $x_0 = 3, y_0 = 1$ este o soluție. Prin urmare mulțimea soluțiilor numere întregi ale ecuației este descrisă de $x = 3 + 7k, y = 1 + 3k$ unde k parcurge mulțime numerelor întregi.

Aplicație. *Lema chineză a resturilor* pentru două numere este următorul rezultat:

Fie n_1, n_2 două numere naturale relativ prime iar r_1, r_2 numere naturale cu $r_1 < n_1, r_2 < n_2$. Există atunci numere naturale n care împărțite la n_1 dau restul r_1 și împărțite la n_2 dau restul r_2 .

Pentru a proba afirmația, scriem concluzia cu teorema împărțirii cu rest: $n = n_1q_1 + r_1$ și $n = n_2q_2 + r_2$. Prin scăderea celor două egalități deducem

$$n_1q_1 - n_2q_2 = r_1 - r_2,$$

care este o ecuație liniară cu $(n_1, n_2) = 1$ și necunoscute q_1, q_2 . Scriem soluția generală și apoi $n = n_1q_1 + r_1$ se află din q_1 de exemplu.

Exercițiu. Încercați să formulați lema chineză pentru 3 numere și eventual să o demonstrați singuri.

Aplicație. Să găsim numărul minim de mere necesare astfel încât împărțite în mod egal la 5 copii să rămână 3 și împărțite egal la 7 copii să rămână 4.

Trebuie găsit cel mai mic număr care satisface condițiile lemei chineze: $n = 5n_1 + 3, n = 7n_2 + 4$, prin urmare $5n_1 - 7n_2 = 1$, cu soluția ce se observă

ușor $n_1 = 3, n_2 = 2$, deci soluția generală $n_1 = 3 + 7k, n_2 = 2 + 5k$ unde k este întreg. Evident avem nevoie de n_1 minim și prin urmare $n = 5 \cdot 3 + 3 = 18$ mere.

Unul dintre rezultatele cele mai importante și mai frumoase în teoria numerelor (aritmetică) este așa numita

Mica teoremă a lui Fermat: Pentru orice număr prim $p > 1$ și orice număr natural a , ce nu este multiplu al lui p , numărul

$$a^{p-1} - 1$$

se divide cu p .

Observație. Cu notația “modulo” concluzia teoremei se poate scrie $a^{p-1} \equiv 1 \pmod{p}$.

Iată și demonstrația acestui rezultate (vă sfătuiesc să o citiți mai târziu după ce vă familiarizați cu proprietățile divizibilității).

Să ne uităm la resturile ce apar în șirul de numere $a, 2a, 3a, \dots, (p-1)a$ la împărțirea cu p . Să presupunem că două dintre aceste numere ar da același rest, fie acestea ma și na ; presupunem $p > m > n$, prima inegalitate fiind din definiție. Am avea

$$ma = q_1p + r, \quad na = q_2p + r,$$

de unde prin scădere $(m - n)a = p(q_1 - q_2)$. Dar aceasta ar însemna $p|a$ ceea ce nu se poate prin ipoteză sau $p|m - n$ ceea ce nu se poate căci $m - n < p$. Prin urmare numerele din șirul de mai sus dau resturi diferite la împărțirea cu p , și cum sunt în număr de $p - 1$ le vor da pe toate cele nenule, adică $1, 2, 3, \dots, p - 1$. Prin urmare și produsul numerelor din șir minus produsul resturilor posibile este un număr divizibil la p (aici trebuie să demonstrați ca exercițiu afirmația: dacă numerele a, b dau la împărțirea cu p resturile r_1 respectiv r_2 , atunci numărul $ab - r_1r_2$ se divide cu p). Avem prin urmare $N = a(2a)(3a) \cdots [(p-1)a] - 1 \cdot 2 \cdot 3 \cdots (p-1)$ se divide la p și cum

$$N = 1 \cdot 2 \cdot 3 \cdots (p-1)[a^{p-1} - 1]$$

deducem că $p|a^{p-1} - 1$.

Exemplu: Să aflăm cu teorema lui Fermat, ultima cifră a numărului 2009^{2008} . Să observăm că $2008 = 4 \cdot 502$ și din teorma lui Fermat

$$5|(2009^{502})^4 - 1 = 2009^{2008} - 1.$$

Cum numărul din dreapta este par, ultima lui cifră este 0, deci ultima cifră a numărului dat este 1. Vă sfătuim, în înceiere să folosiți o idee foarte

asemănătoare pentru a proba partea directă a toremei de la 2. O indicație: e suficient să arătați că dacă m, n sunt relativ prime, atunci unul dintre multiplii lui m dă restul 1 la împărțirea cu n . Succes!