DIVIZIBILITATE

ABSTRACT. Articolul prezintă câteva rezultate şi exemple privind divizibilitatea.

Lecţia se adresează clasei a VI-a.

Data: 8 noiembrie 2010

Autori:
Roxana Diaconescu, profesor Colegiul German Goethe, Bucureşti
Radu Gologan, preşedintele Comisiei Naţionale a Olimpiadei de Matematică

Rezultatul fundamental în teoria divizibilităţii numerelor întregi, este teorema împărţirii cu rest. Aceasta caracterizează câtul şi restul unei împărţiri, determinându-le în mod unic. Să reamintim enunţul formal al acestei teoreme:

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

1. $n = mq + r$
2. $0 \leq r < m$

Numărul q unic determinat mai sus se numeşte câtul împărţirii iar numărul r unic determinat cu condiţiile de mai sus se numeşte restul împărţirii.

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

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

Astfel dacă r este restul împărţirii lui m la n, avem şi $m \equiv r (\mod n)$.

Aceste notaţii sunt uneori utile pentru simplificarea scrierii. Nu le vom folosi pe parcursul acestei lecţii.

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

Observaţia 1. Găsirea lui q din definiţia divizibilităţii se face, de regulă, prin împărţirea lui n la m; trebuie să obţinem restul 0.

Observaţia 2. Evident numărul 0 se divide la orice număr natural nenul, datorită acestei definiţii.

Observaţia 3. Notăm $m|n$ şi citim "m divide n".

Notăm $n\vdots m$ şi citim "n se divide cu m".
Se mai spune că m este divizor al lui n

Atentie: Pentru claritatea expunerii şi pentru a evita confuziile, considerăm că divizorii sunt întotdeauna numere naturale nenule; deîmpărţitul putând fi şi negativ.

Definiţie. Un număr natural p, mai mare sau egal cu 2, se numeşte număr prim dacă singurii săi divizori sunt 1 şi el însuşi.

Astfel, putem scrie primii termeni ai şirului numerelor prime:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, ...$$

Încă din antichitate, Euclid a arătat că mulţimea numerelor prime este infinită, iar cea mai mare problemă nerezolvată a matematicii actuale, conjectura lui Riemann, se referă la structura mulţimii numerelor prime. Din păcate explicarea ei depăşeşte mult cadrul unor cunoştiinţe şcolare, dar poate fi înţeleasă dupa ceva studii speciale de matematică, şi poate, cine ştie, 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

$$n = p_1^{a_1} \cdot_2^{a_2} \cdots p_k^{a_k}$$

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

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

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

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

Din acestă teoremă punem deduce uşor că un număr n se divide la m dacă şi numai dacă orice factor prim al lui m este factor prim al lui n şi 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 sa ştiţi 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 şi Adelman; pentru o documentare mai adîncă vă recomandăm capitolul I al celebrei cărţi; *Vârsta de aur a matematicii* de Keith Devlin, apărută în traducere la Fundaţia Theta theta@theta.ro.)

O consecinţă importantă a reprezentării unui număr natural prin descompunerea sa canonică în factori primi, $n = p_1^{a_1} \cdot {}_2^{a_2} \cdots p_k^{a_k}$, 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 $n = p_1^{b_1} \cdot {}_2^{b_2} \cdots p_k^{b_k}$ cu $b_1 \leq a_1, b_2 \leq a_2, \ldots, b_k \leq a_k$, deci va trebui să numărăm în câte feluri putem găsi sisteme $(b_1, b_2, \ldots, b_k)$ cu această proprietate. Cum e foarte simplu de văzut că numerele naturale mai mici decât a_1 sunt $0, 1, 2, \ldots, a_1$, în număr de $a_1 + 1$, numere naturale mai mici decăt a_2 sunt la fel $a_2 + 1$, şi aşa 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 CONSECINŢE ALE ACESTOR NOŢIUNI ŞI REZULTATE

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

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

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

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

Definiţie. 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 şi n sunt relativ prime atunci şi numai atunci când există numerele naturale x şi y astfel încât $mx - ny = \pm 1$

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

Enunţul de mai sus afirmă de fapt două rezultate: unul direct şi altul reciproc. Avem de arătat că dacă numerele sunt relativ prime avem o relaţie de forma celei de mai sus şi reciproc, relaţia de mai sus implică faptul că numerele sunt prime între ele.

Vom demonstra deocamdată ultima afirmaţie. Să presupunem pentru acesta că d este un divizor comun pentru m şi n (dorim de fapt să arătăm că $d = 1$ este singura posibilitate). Există atunci numerele naturale n_1 şi m_1 cu $m = dm_1$ şi $n = dn_1$. Introducând acestea în relaţia $mx - ny = \pm 1$, 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 demonstraţia.

2. Observaţia următoare este extrem de utilă în descrierea unor algoritmi (metode) de calcul ale celui mai mare divizor comun şi este în esenţă ceea ce se numeşte în algebră **algoritmul lui Euclid**.

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

E un fapt uşor de probat: dacă $d|(m, n)$, deci $m = dm_1$ şi $n = dn_1$, atunci $m - n = d(m_1 - n_1)$ deci $d|(m - n)$ şi atunci $d|(m - n, n)$. Reciproc, dacă $d'|(m - n, n)$ rezultă la fel că $d'|(m, n)$, prin urmare numerele (m, n) şi $(m - n, n)$ au aceeaşi 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 fracţia $\frac{2n+13}{n+7}$ 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 şi numitorul sunt prime între ele, fracţia este prin urmare ireductibilă.

E importantă de reţinut şi noţiunea 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 şi pentru m, n naturale se notează cu $[m, n]$ cmmmc.

Un exerciţiu util vouă este următoarea formula de legătură între aceste noţiuni:

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

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

Fie x_0, y_0 o soluţie a acestei ecuaţii (de fapt se demonstrează că poate fi găsită întotdeauna; încercaţi ca exerciţiu să folosiţi teorema de la 1 pentru demonstraţie).

Aşadar avem $ax_0 + by_0 = c$. Dacă x_1, y_1 este o altă soluţie în numere întregi, avem evident şi $ax_1 + by_1 = c$. Prin scăderea celor două ecuaţii obţinem $a(x_1 - x_0) + b(y_1 - y_0) = 0$ sau $a(x_1 - x_0) = b(y_0 - y_1)$. Cum a şi b (prime între ele) nu au factori comuni, ultima egalitate implică $y_0 - y_1$ este multilpu de a iar $x_1 - x_0$ este multiplu de acelaşi factor de b, deci există k întreg cu $y_0 - y_1 = ka, x_1 - x_0 = kb$ sau $x_1 = x_0 + kb, y_1 = y_0 - ka$. Aşadar toate soluţiile ecuaţie sunt de forma $x = x_0 + kb, y = y_0 - ka$.

Exemplu: Rezolvaţi în numere întregi ecuaţia $3x - 7y = 2$.

Se observă că $x_0 = 3, y = 1$ este o soluţie. Prin urmare mulţimea soluţiilor numere întregi ale ecuaţiei este descrisă de $x = 3 + 7k, y = 1 + 3k$ unde k parcurge mulţime numerelor întregi.

Aplicaţie. *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 împărţite la n_1 dau restul r_1 şi împărţite la n_2 dau restul r_2.

Pentru a proba afirmaţia, scriem concluzia cu teorema împărţirii cu rest: $n = n_1q_1 + r_1$ şi $n = n_2q_2 + r_2$. Prin scăderea celor două egalităţi deducem

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

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

Exerciţiu. Încearcţi să formulaţi lema chineză pentru 3 numere şi eventual să o demonstraţi singuri.

Aplicaţie. Să găsim numărul minim de mere necesare astfel încât împărţite în mod egal la 5 copii să rămână 3 şi împărţite egal la 7 copii să rămană 4.

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

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

Unul dintre rezultatele cele mai importante şi mai frumoase în teoria numerelor (aritmetică) este aşa numita

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

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

se divide cu p.

Observaţie. Cu notaţia "modulo" concluzia teoremei se poate scrie $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Iată şi demonstraţia acestui rezultate (vă sfătuiesc să o citiţi mai târziu după ce vă familiarizaţi cu proprietăţile divizibilităţii).

Să ne uităm la resturile ce apar în şirul de numere $a, 2a, 3a, \ldots, (p-1)a$ la împărţirea cu p. Să presupunem că două dintre aceste numere ar da acelaşi rest, fie acestea ma şi na; presupunem $p > m > n$, prima inegalitate fiind din definiţie. Am avea

$$ma = q_1 p + r,\ na = q_2 p + r,$$

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 şirul de mai sus dau resturi diferite la împărţirea cu p, şi cum sunt în număr de $p-1$ le vor da pe toate cele nenule, adică $1, 2, 3, \ldots, p-1$. Prin urmare şi produsul numerelor din şir minus produsul resturilor posibile este un număr divizibil la p (aici trebuie să demonstraţi ca exerciţiu afirmaţia: dacă numerele a, b dau la împărţirea cu p resturile r_1 respectiv r_2, atunci numărul $ab - r_1 r_2$ 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 şi 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 $2008 = 4 \cdot 502$ şi 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 folosiţi o idee foarte asemănătoare pentru a proba partea directă a toremei de la 2. O indicaţie: e suficient să arătaţi că dacă m, n sunt relativ prime, atunci unul dintre multiplii lui m dă restul 1 la împărţirea cu n. Succes!