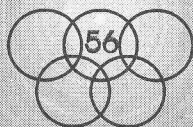


**Camelia Magdaș
Dorin Moldovan**

Introducere în Teoria Numerelor

**Biblioteca Olimpiadelor
de
Matematică**



**Editura GIL
Zalău**

1	Divizibilitate	1
1.1	Teorie	1
1.2	Exerciții	5
1.3	Probleme	8
1.4	Rezolvări exerciții	9
1.5	Rezolvări probleme	14
2	Algoritmul lui Euclid	19
2.1	Teorie	19
2.2	Exerciții	23
2.3	Probleme	24
2.4	Rezolvări exerciții	25
2.5	Rezolvări probleme	30
3	Congruențe	32
3.1	Teorie	32
3.2	Exerciții	37
3.3	Probleme	38
3.4	Rezolvări exerciții	39
3.5	Rezolvări probleme	48
4	Teorema chineză a resturilor	53
4.1	Teorie	53
4.2	Exerciții	58
4.3	Probleme	60
4.4	Rezolvări exerciții	61
4.5	Rezolvări probleme	79
5	Teorema lui Wilson	83
5.1	Teorie	83
5.2	Exerciții	85
5.3	Probleme	86
5.4	Rezolvări exerciții	87
5.5	Rezolvări probleme	96
6	Teorema lui Fermat	103
6.1	Teorie	103
6.2	Exerciții	104
6.3	Probleme	105
6.4	Rezolvări exerciții	105
6.5	Rezolvări probleme	111

7 Teorema lui Euler	115
7.1 Teorie	115
7.2 Exerciții	117
7.3 Probleme	119
7.4 Rezolvări exerciții	119
7.5 Rezolvări probleme	124
8 Ecuații diofantiene cuadratice	127
8.1 Teorie	127
8.2 Exerciții	132
8.3 Probleme	133
8.4 Rezolvări exerciții	134
8.5 Rezolvări probleme	139
9 Simbolul lui Legendre	143
9.1 Teorie	143
9.2 Exerciții	152
9.3 Probleme	153
9.4 Rezolvări exerciții	153
9.5 Rezolvări probleme	158
10 Secvențe Farey	162
10.1 Teorie	162
10.2 Exerciții	164
10.3 Probleme	166
10.4 Rezolvări exerciții	166
10.5 Rezolvări probleme	169
Bibliografie	174

1.1 Teorie

Teorema 1.1: Definirea câtului și restului

Fie m și n două numere întregi astfel încât $m > 0$ și $n > 0$. Există și sunt unice două numere întregi q și r astfel încât:

$$a) \quad n = m \cdot q + r$$

$$b) \quad 0 \leq r < m$$

Demonstrație. Considerăm mulțimea care conține numerele:

$$\{n - m + 1, n - m + 2, \dots, n - 0\}$$

Această mulțime conține m numere consecutive. Printre aceste m numere consecutive exact unul este divizibil cu m și astfel există un unic număr $r \in \{0, 1, \dots, m - 1\}$ astfel încât $n - r$ este divizibil cu m și $0 \leq r < m$. Câtul împărțirii lui $n - r$ la m este determinat în mod unic. Notăm acest cât cu q . De aici rezultă că $n - r = mq$ ceea ce este echivalent cu $n = mq + r$. $\square$

Definiția 1.1

Numărul întreg n este divizibil cu numărul întreg pozitiv m dacă există un număr întreg q astfel încât $n = mq$.

Exemplu Numărul întreg 24 este divizibil cu 8 deoarece $24 = 8 \cdot 3$ și 3 este un întreg pozitiv.

Definiția 1.2

Scriem $m \mid n$ și citim: „ m divide pe n “.

Exemplu Considerăm numerele întregi 3 și 18. Este adevărat că $3 \mid 18$ și citim acest lucru astfel: „3 divide pe 18“.

Definiția 1.3

Scriem $n : m$ și citim: „ n este divizibil cu m “.

Exemplu Considerăm întregii 64 și 8. Este adevărat că $64 : 8$ și citim: „64 este divizibil cu 8”.

Teorema 1.2: Descompunerea în factori primi

Orice număr întreg pozitiv n mai mare decât 1 poate fi scris 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 distincte, iar $a_1, a_2, \dots, a_k$ sunt numere întregi pozitive mai mari sau egale cu 1.

Demonstrație. Această teoremă poate fi demonstrată utilizând inducția matematică. Cazul de bază este evident deoarece singura reprezentare posibilă a numărului 2 ca produs de numere prime este $2 = 2^1$. În continuare vom demonstra că dacă orice număr mai mic sau egal decât n poate fi reprezentat în mod unic ca produs de numere prime atunci această afirmație este adevărată și pentru $n+1$. Fie p un număr prim și k un număr natural nenul astfel încât $p^k \mid n+1$ și $p^{k+1} \nmid n+1$. Numărul $N = \frac{n+1}{p^k}$ este mai mic decât $n+1$ și mai mare sau egal decât 1. Dacă $N = 1$ atunci singura reprezentare posibilă a lui $n+1$ ca produs de numere prime este $n+1 = p^k$, iar dacă $N \geq 2$ atunci din $N \leq n$ rezultă că N poate fi reprezentat în mod unic ca produs de numere prime. Cum $p \nmid N$ rezultă că înmulțind acest produs cu p^k obținem tot o reprezentare unică, ceea ce încheie demonstrația. $\square$

Exemple

- a) $128 = 2^7$
- b) $18 = 2^1 \cdot 3^2$
- c) $900 = 2^2 \cdot 3^2 \cdot 5^2$
- d) $210 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1$
- e) $2310 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1$

Teorema 1.3: Numărul divizorilor

Numărul divizorilor pozitivi ai numărului n scris conform Teoremei 1.2 este egal cu:

$$D(n) = (a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_k + 1)$$

Demonstrație. Dacă $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ atunci toți divizorii săi au forma:

$$p_1^{i_1} \cdot p_2^{i_2} \cdot \dots \cdot p_k^{i_k}$$

cu $0 \leq i_j \leq a_j$ pentru orice $j \in \{1, 2, \dots, k\}$. Există $(a_1 + 1)$ valori posibile pentru i_1 . Aceste valori sunt $\{0, 1, 2, \dots, a_1\}$. Din aceasta rezultă că există $(a_1 + 1)$ valori posibile pentru $p_1^{i_1}$. De asemenea, există $(a_2 + 1)$ valori posibile pentru i_2 și așa mai departe. În final rezultă că există $(a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_k + 1)$ valori posibile pentru $p_1^{i_1} \cdot p_2^{i_2} \cdot \dots \cdot p_k^{i_k}$. Astfel, numărul divizorilor lui n este egal cu:

$$D(n) = (a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_k + 1)$$

□

Example

- a) $D(128) = D(2^7) = 7 + 1 = 8$. Mulțimea divizorilor pozitivi ai numărului 128 este:

$$S(128) = \{1, 2, 4, 8, 16, 32, 64, 128\}$$

- b) $D(18) = D(2^1 \cdot 3^2) = (1 + 1) \cdot (2 + 1) = 2 \cdot 3 = 6$. Mulțimea divizorilor pozitivi ai numărului 18 este:

$$S(18) = \{1, 2, 3, 6, 9, 18\}$$

- c) $D(900) = D(2^2 \cdot 3^2 \cdot 5^2) = (2 + 1) \cdot (2 + 1) \cdot (2 + 1) = 27$. Mulțimea divizorilor pozitivi ai numărului 900 este:

$$S(900) = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 25, 30, 36, 45, 50, 60, 75, 90, 100, 150, 180, 225, 300, 450, 900\}$$

- d) $D(210) = D(2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1) = (1+1) \cdot (1+1) \cdot (1+1) \cdot (1+1) = 2 \cdot 2 \cdot 2 \cdot 2 = 16$. Mulțimea divizorilor pozitivi ai numărului 210 este:

$$S(210) = \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}$$

- e) $D(2310) = D(2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1) = (1+1) \cdot (1+1) \cdot (1+1) \cdot (1+1) \cdot (1+1) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$. Mulțimea divizorilor pozitivi ai numărului 2310 este:

$$S(2310) = \{1, 2, 3, 5, 6, 7, 10, 11, 14, 15, 21, 22, 30, 33, 35, 42, 55, 66, 70, 77, 105, 110, 154, 165, 210, 231, 330, 385, 462, 770, 1155, 2310\}$$

Definiția 1.4

Dacă $a, b \in \mathbb{N}^*$ atunci cel mai mare divizor comun $c.m.m.d.c.(a, b)$ al acestor două numere este cel mai mare întreg pozitiv care divide atât pe a cât și pe b .

Exemplu Cel mai mare divizor comun al numerelor 20 și 36 este egal cu $c.m.m.d.c.(20, 36) = 4$.

Definiția 1.5

Numerele întregi pozitive a și b sunt prime între ele dacă $c.m.m.d.c.(a, b) = 1$.

Exemplu Numerele 14 și 15 sunt prime între ele pentru că $c.m.m.d.c.(14, 15) = 1$, dar numerele 14 și 35 nu sunt prime între ele pentru că $c.m.m.d.c.(14, 35) = 7$ și $7 \neq 1$.

Definiția 1.6

Dacă $a, b \in \mathbb{N}^*$ atunci cel mai mic multiplu comun $c.m.m.m.c.[a, b]$ al numerelor a și b este cel mai mic număr întreg pozitiv care este divizibil atât cu a cât și cu b .

Exemplu Cel mai mic multiplu comun al numerelor 14 și 5 este egal cu $c.m.m.m.c.[14, 5] = 70$.

Teorema 1.4

Dacă $a, b \in \mathbb{N}^*$ atunci:

$$a, b = ab$$

Demonstrație. Notăm cu $d = c.m.m.d.c.(a, b)$ cel mai mare divizor comun al numerelor a și b . Rezultă că există numerele a_1 și b_1 astfel încât $(a_1, b_1) = 1$, $a = da_1$ și $b = db_1$. Cel mai mic multiplu comun al numerelor a și b este egal cu $c.m.m.m.c.[a, b] = da_1b_1$. Următoarele două relații sunt adevărate:

$$a, b = (da_1b_1) \cdot d \quad (1.1.1)$$

și

$$ab = (da_1) \cdot (db_1) \quad (1.1.2)$$

Din 1.1.1 și 1.1.2 rezultă că:

$$a, b = ab$$

□

Definiția 1.7

Dacă $a_1, a_2, \dots, a_n \in \mathbb{N}^*$ atunci cel mai mare divizor comun al acestor n numere este $c.m.m.d.c.(a_1, a_2, \dots, a_n)$ și este cel mai mare întreg pozitiv care divide pe $a_1, a_2, \dots, a_n$.

Exemplu Cel mai mare divizor comun al numerelor 36, 27 și 45 este egal cu $c.m.m.d.c.(36, 27, 45) = 9$.

Definiția 1.8

Dacă $a_1, a_2, \dots, a_n \in \mathbb{N}^*$ atunci cel mai mic multiplu comun al acestor n numere este $c.m.m.m.c.[a_1, a_2, \dots, a_n]$ și este cel mai mic întreg pozitiv care este divizibil cu $a_1, a_2, \dots, a_n$.

Exemplu Cel mai mic multiplu comun al numerelor 2, 4 și 5 este egal cu $c.m.m.m.c.[2, 4, 5] = 20$.

1.2 Exerciții

Exercițiul 1 Se consideră două numere naturale $n = 2015$ și $m = 337$. Să se determine două numere întregi q și r astfel încât $n = mq + r$ și $0 \leq r < m$. Să se arate că aceste două numere q și r sunt unice.

Exercițiul 2 Să se specifice care dintre următoarele afirmații sunt adevărate și care sunt false. Justificați răspunsurile:

- a) 35 este divizibil cu 5
- b) 2310 este divizibil cu 4
- c) 231 este divizibil cu 3
- d) 1001 este divizibil cu 9
- e) 110 este divizibil cu 25

Exercițiul 3 Determinați care dintre următoarele afirmații sunt adevărate și care sunt false:

- a) $5 \mid 1025$
- b) $11 \mid 121$
- c) $3 \mid 101210$
- d) $4 \mid 114$
- e) $7 \mid 343$

Exercițiul 4 Determinați care dintre următoarele afirmații sunt adevărate și care sunt false:

- a) $2025 : 15$
- b) $1021 : 3$
- c) $101201 : 3$
- d) $2048 : 8$
- e) $1025 : 15$

Exercițiul 5 Să se scrie ca și produs de numere prime, conform Teoremei 1.2, următoarele numere:

- a) 4025
- b) 2021
- c) 2332
- d) 2048
- e) 1025

Exercițiul 6 Calculați numărul divizorilor pozitivi pentru următoarele numere:

- a) 1024
- b) 2340
- c) 102
- d) 1003
- e) 4024

Exercițiul 7 Determinați valorile următoarelor expresii:

- a) $c.m.m.d.c.(14, 102)$
- b) $c.m.m.d.c.(64, 24)$
- c) $c.m.m.d.c.(7, 9)$
- d) $c.m.m.d.c.(1024, 96)$
- e) $c.m.m.d.c.(405, 35)$

Exercițiul 8 Determinați valorile următoarelor expresii, unde $n \in \mathbb{N}^*$:

- a) $c.m.m.d.c.(2^n, 3^n)$
- b) $c.m.m.d.c.(4^n, 6^n)$
- c) $c.m.m.d.c.(2^n + 1, 2^n + 3)$
- d) $c.m.m.d.c.(2^n + 1, 4^n + 1)$
- e) $c.m.m.d.c.(2^n, 5^n)$

Exercițiul 9 Să se determine care dintre următoarele perechi de numere sunt prime între ele:

- a) 12 și 13
- b) 102 și 130
- c) 237 și 224
- d) 1002 și 337
- e) 232 și 553

Exercițiul 10 Determinați care dintre următoarele perechi de numere sunt prime între ele, unde $n \in \mathbb{N}^*$:

- a) 2^n și 7^n
- b) $2^{n+1} + 2$ și $2^{n+1} + 4$
- c) $3^{n+1} + 1$ și 4^{n+1}
- d) $5^{n+1} + 5$ și 10^{n+1}
- e) $4^{n+1} + 1$ și $4^{n+1} - 1$

Exercițiul 11 Determinați valorile următoarelor expresii utilizând Teorema 1.4 și rezultatele obținute la Exercițiul 7:

- a) $c.m.m.m.c.[14, 102]$
- b) $c.m.m.m.c.[64, 24]$
- c) $c.m.m.m.c.[7, 9]$
- d) $c.m.m.m.c.[1024, 96]$
- e) $c.m.m.m.c.[405, 35]$

Exercițiul 12 Determinați valorile următoarelor expresii, unde $n \in \mathbb{N}^*$, utilizând Teorema 1.4 și rezultatele obținute la Exercițiul 8:

- a) $c.m.m.c.[2^n, 3^n]$
- b) $c.m.m.c.[4^n, 6^n]$
- c) $c.m.m.c.[2^n + 1, 2^n + 3]$
- d) $c.m.m.c.[2^n + 1, 4^n + 1]$
- e) $c.m.m.c.[2^n, 5^n]$

Exercițiul 13 Fără a utiliza Teorema 1.4 demonstrați că următoarele expresii sunt adevărate:

- a) $12, 13 = 12 \cdot 13$
- b) $12, 8 = 12 \cdot 8$
- c) $101, 102 = 101 \cdot 102$
- d) $24, 25 = 24 \cdot 25$
- e) $1001, 101 = 1001 \cdot 101$

Exercițiul 14 Evaluați următoarele expresii:

- a) $c.m.m.d.c.(2, 4, 8)$
- b) $c.m.m.d.c.(4, 8, 14, 2)$
- c) $c.m.m.d.c.(18, 30, 42, 12, 54)$
- d) $c.m.m.d.c.(14, 35, 49, 56, 76)$
- e) $c.m.m.d.c.(25, 35, 45, 5000, 15)$

Exercițiul 15 Evaluați următoarele expresii:

- a) $c.m.m.m.c.[2, 4, 8]$
- b) $c.m.m.m.c.[18, 6, 24]$
- c) $c.m.m.m.c.[5, 25, 15]$
- d) $c.m.m.m.c.[11, 33, 55]$
- e) $c.m.m.m.c.[9, 18, 27]$

1.3 Probleme

Problema 1 Câte perechi de numere întregi pozitive (a, b) există astfel încât $c.m.m.d.c.(a, b) = 6$ și $c.m.m.m.c.[a, b] = 1 \cdot 2 \cdot 3 \cdot \dots \cdot 30$?

Problema 2 Să se determine toate perechile de numere întregi pozitive (a, b) care satisfac ecuația:

$$\frac{1}{a} + \frac{1}{b} + \frac{201}{c.m.m.m.c. [a, b]} = \frac{1}{c.m.m.d.c. (a, b)}$$

Problema 3 Să se determine toate perechile de numere întregi pozitive (a, b) care satisfac ecuația:

$$\frac{1}{a^2} + \frac{1}{b^2} + \frac{23}{(c.m.m.m.c. [a, b])^2} = \frac{1}{(c.m.m.d.c. (a, b))^2}$$

Problema 4 Să se arate că pentru orice numere întregi pozitive a și b următoarea expresie este adevărată:

$$c.m.m.d.c. (a + b, c.m.m.m.c. [a, b]) = c.m.m.d.c. (a, b)$$

Problema 5 Să se arate că fracția $\frac{12n+1}{30n+2}$ este ireductibilă pentru orice $n \in \mathbb{N}^*$.

1.4 Rezolvări exerciții

Exercițiul 1 Două numere q și r care satisfac relația $n = mq + r$ sunt $q = 5$ și $r = 330$. Următorul pas este să arătăm că aceste numere sunt unice. Prin reducere la absurd presupunem că există două numere q' și r' diferite de q și r astfel încât $n = mq' + r'$ și $0 \leq r' < m$. Rezultă că:

$$mq + r = mq' + r'$$

Acum, din această relație vom deduce că:

$$m(q - q') = r' - r$$

Dacă $q = q'$ atunci $m \cdot 0 = r - r'$ și în consecință $r = r'$, în contradicție cu presupunerea făcută că q' și r' sunt diferite de q și r . Similar, dacă $r = r'$ atunci $m(q - q') = 0$, și astfel $q = q'$ deoarece valoarea lui m este 337 și $337 > 0$. Astfel, putem să presupunem că $q \neq q'$ și $r \neq r'$.

Din faptul că $m(q - q') = r' - r$, rezultă că:

$$|m(q - q')| = |r' - r|$$

Din $q \neq q'$ rezultă că $|q - q'| \geq 1$. De aici deducem că:

$$|m(q - q')| \geq m \tag{1.4.1}$$

În continuare vrem să demonstrăm că $|r' - r| < m$. Numărul r' satisface relația $0 \leq r' < m$ și numărul r satisface relația $0 \leq r < m$. Dacă înmulțim a doua

relație cu -1 obținem $-m < -r \leq 0$. Din relațiile $0 \leq r' < m$ și $-m < -r \leq 0$ obținem că:

$$0 - m < r' - r < m + 0$$

Această relație este echivalentă cu:

$$-m < r' - r < m$$

În final, această relație se poate rescrie sub forma:

$$|r' - r| < m \quad (1.4.2)$$

Din 1.4.1 și 1.4.2 rezultă că:

$$|m(q - q')| > |r' - r|$$

Această relație este în contradicție cu:

$$|m(q - q')| = |r' - r|$$

În concluzie rezultă că presupunerea inițială că există două numere q' și r' diferite de q și r astfel încât $n = mq' + r'$ și $0 \leq r' < m$ este greșită. Deducem așadar că q și r sunt unice.

Exercițiul 2

- adevărat, pentru că ultima cifră a numărului 35 este 5. 35 poate fi scris sub forma $35 = 5 \cdot 7$.
- fals, pentru că numărul format din ultimele două cifre ale lui 2310 este 10, iar 10 nu este divizibil cu 4.
- adevărat, deoarece suma cifrelor numărului 231 este egală cu $2 + 3 + 1 = 6$, iar 6 este divizibil cu 3. 231 poate fi scris sub forma $231 = 3 \cdot 77$.
- fals, deoarece suma cifrelor numărului 1001 este egală cu $1 + 0 + 0 + 1 = 2$, iar 2 nu este divizibil cu 9.
- fals, deoarece numărul format din ultimele două cifre ale numărului 110 este 10 și 10 nu este divizibil cu 25.

Exercițiul 3

- adevărat, deoarece ultima cifră a numărului 1025 este 5. 1025 poate fi scris sub forma $1025 = 5 \cdot 205$.
- adevărat, 121 poate fi scris sub forma $121 = 11 \cdot 11$.
- fals, deoarece suma cifrelor numărului 101210 este egală cu $1 + 0 + 1 + 2 + 1 + 0 = 5$, iar 5 nu este divizibil cu 3.
- fals, deoarece numărul format din ultimele două cifre ale numărului 114 este 14, iar 14 nu este divizibil cu 4.
- adevărat, numărul 343 poate fi scris sub forma $343 = 7 \cdot 7 \cdot 7$.