CURS 1

Teorema împărţirii cu rest în $\mathbb{Z}$

Teorema împărţirii cu rest reprezintă un instrument de bază în studiul numerelor întregi.

Teorema 1. (Teorema împărţirii cu rest în $\mathbb{N}$) Oricare ar fi numerele naturale a şi b, cu $b \neq 0$, există o singură pereche de numerele naturale $(q, r) \in \mathbb{N} \times \mathbb{N}$, astfel încât:

$$a = b \cdot q + r \text{ şi } r < b. \tag{1}$$

Demonstraţie. Fie a, $b \in \mathbb{N}$, cu $b \neq 0$.

Demonstrăm existenţa numerelor q, $r \in \mathbb{N}$, astfel încât $a = b \cdot q + r$ şi $r < b$. Fie

$$\mathcal{S} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : a = by + x\} \subseteq \mathbb{N}$$

şi observăm că $\mathcal{S} \neq \emptyset$ pentru că $a \in \mathcal{S}$ $(a = b \cdot 0 + a)$. Rezultă că există $r \in \mathcal{S}$ cel mai mic element din $\mathcal{S}$. Cum $r \in \mathcal{S}$, deducem că există $q \in \mathbb{N}$ cu proprietatea $a = bq + r$.

Presupunem că $r \geq b$. Atunci $r - b \in \mathbb{N}$ şi $a = b(q + 1) + r - b$, deci $r - b \in \mathcal{S}$. Din ipoteza $b \neq 0$ deducem $r - b < r$, ceea ce contrazice alegerea lui r. Aşadar $r < b$ şi perechea (r, b) satisface condiţia (1).

Pentru demonstraţia unicităţii, să presupunem că ar exista două perechi (q_1, r_1), (q_2, r_2) care satisfac (1) pentru aceleaşi numere $a, b \in \mathbb{N}$, $b \neq 0$. Deci

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \text{ şi } r_1 < b,\ r_2 < b.$$

Presupunem că $q_1 < q_2$. Rezultă că există $x \in \mathbb{N}^*$, astfel încât $q_2 = q_1 + x$. Obţinem

$$bq_1 + r_1 = b(q_1 + x) + r_2 \Rightarrow bq_1 + r_1 = bq_1 + bx + r_2,$$

de unde, prin simplificare, $r_1 = b \cdot x + r_2$, ceea ce implică $b \cdot x \leq r_1$.

Dar din $x \in \mathbb{N}^*$ deducem că $1 \leq x$, deci $b \leq bx \leq r_1$, contradicţie.

Analog se arată că nu putem avea $q_2 < q_1$. Rezultă că $q_1 = q_2$ şi mai departe

$$b \cdot q_1 + r_1 = b \cdot q_1 + r_2,$$

de unde, prin simplificare, $r_1 = r_2$ şi demonstraţia este încheiată.

Corolarul 2. (Teorema împărţirii cu rest în $\mathbb{Z}$) Oricare ar fi numerele întregi a şi b, cu $b \neq 0$, există şi sunt unice numerele întregi q şi r, astfel încât

$$a = b \cdot q + r \text{ şi } 0 \leq r < |b|. \tag{2}$$

Demonstraţie. Fie $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci $|a|$, $|b| \in \mathbb{N}$, cu $|b| \neq 0$ şi aplicăm teorema împărţirii cu rest în $\mathbb{N}$. Deducem că există numerele h, $k \in \mathbb{N}$, astfel încât

$$|a| = |b| \cdot h + k, \text{ unde } 0 \leq k < |b|.$$

Considerăm cazurile:

I. $a \geq 0$ şi $b > 0$. Atunci $a = b \cdot h + k$. Luăm $q = h$ şi $r = k$.

II. $a \geq 0$ şi $b < 0$. Atunci $a = b \cdot (-h) + k$. Luăm $q = -h$ şi $r = k$.
III. $a < 0$ şi $b > 0$. Considerăm aici subcazurile:
a) $k = 0$. Atunci $-a = b \cdot h$, adică $a = b \cdot (-h)$. Luăm $q = -h$ şi $r = 0$.
b) $k \neq 0$. Atunci

$$a = b \cdot (-h) + (-k) = -b - b \cdot h + b - k = -b \cdot (1 + h) + (b - k).$$

Luăm $q = -(1 + h)$ şi $r = b - k < b$, deci $0 \leq r < |b|$.
IV. $a < 0$ şi $b < 0$. Considerăm două subcazuri, ca în cazul anterior:
a) $k = 0$. Atunci $-a = -b \cdot h$, de unde $a = b \cdot h$. Luăm $q = h$ şi $r = 0$.
b) $k \neq 0$. Atunci $-a = -b \cdot h + k$, de unde

$$a = b \cdot h - k = b \cdot h + b - b - k = b \cdot (h + 1) + (-b - k).$$

Luăm $q = h + 1$ şi $r = -b - k < -b$, deci $0 \leq r < |b|$.

Pentru demonstrarea unicităţii, să presupunem că ar exista două perechi (q_1, r_1), (q_2, r_2) care satisfac condiţiile (2) pentru aceleaşi numere $a, b \in \mathbb{Z}$, $b \neq 0$. Deci

$$a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2 \text{ şi } 0 \leq r_1 < |b|,\ 0 \leq r_2 < |b|.$$

Rezultă că $|r_2 - r_1| < |b|$ şi $b(q_1 - q_2) = r_2 - r_1$.

Cum $|q_1 - q_2| \in \mathbb{N}$, $|q_1 - q_2| \geq 1$ ar implica

$$|b| \leq |b||q_1 - q_2| = |r_2 - r_1| < |b|,$$

contradicţie. Deducem că $|q_1 - q_2| = 0$, deci $q_1 = q_2$. Atunci

$$b \cdot q_1 + r_1 = b \cdot q_1 + r_2,$$

de unde, prin simplificare, $r_1 = r_2$ şi demonstraţia este încheiată.

Dacă a, b, q şi r sunt ca în Corolarul 2, vom spune că numărul q este **câtul împărţirii** lui a la b, iar r este **restul împărţirii** lui a la b. În acest context se mai foloseşte terminologia **deîmpărţit** pentru a, respectiv **împărţitor** pentru b.

Exemplul 3. Prezentăm câteva exemple concrete:
i) $a = 7$, $b = 3 \Rightarrow q = 2$ şi $r = 1$;
ii) $a = -7$, $b = 3 \Rightarrow q = -3$ şi $r = 2$;
iii) $a = 7$, $b = -3 \Rightarrow q = -2$ şi $r = 1$;
iv) $a = -7$, $b = -3 \Rightarrow q = 3$ şi $r = 2$;
v) $a = -6$, $b = 3 \Rightarrow q = -2$ şi $r = 0$.

Observaţia 4. În practică identitatea dată de teorema împărţirii cu rest este uneori înlocuită cu

$$a = bk + s,\ -|b|/2 < s \leq |b|/2.$$

De exemplu, dacă împărţim la 3, putem scrie $a = 3q + r$, $r \in \{0, 1, 2\}$ sau $a = 3k + s$ cu $s \in \{0, \pm 1\}$. A doua variantă este utilă dacă trebuie să-l ridicăm pe a la o putere pară, pentru că deducem imediat $a^{2m} = \mathcal{M}_3 + t$, $t \in \{0, 1\}$, i.e. orice pătrat perfect dă prin împărţire la 3 restul 0 sau 1 ($\mathcal{M}_3$ notează faptul că numărul pe care l-am înlocuit cu acest simbol dă restul 0 prin împărţire la 3, adică este un multiplu al lui 3).

Divizibilitatea în $\mathbb{Z}$

Definiţia 5. Fie $a, b \in \mathbb{Z}$. Spunem că a **divide pe** b şi notăm $a \mid b$ sau $b \vdots a$ dacă există un număr întreg q, astfel încât $b = a \cdot q$. Aceasta defineşte o relaţia binară omogenă pe $\mathbb{Z}$ care se numeşte **relaţia de divizibilitate** pe $\mathbb{Z}$. Dacă $a \mid b$, mai spunem că a **este divizor pentru** b sau a **este factor al lui** b sau b **este multiplu pentru** a sau b **factorizează prin** a.

Observaţia 6. Dacă $a \neq 0$, următoarele afirmaţii sunt echivalente:

a) $a \mid b$;

b) b este multiplu pentru a, fapt notat prin $b = \mathcal{M}_a$;

c) restul împărţirii lui b la a este 0.

Următoarea teoremă prezintă câteva proprietăţi elementare ale relaţiei de divizibilitate.

Teorema 7. (Proprietăţi ale relaţiei de divizibilitate)
Fie $a, b, c \in \mathbb{Z}$. Sunt adevărate afirmaţiile:
(i) $\pm 1 \mid a$, $\pm a \mid a$, $a \mid 0$;
(ii) dacă $0 \mid a$, atunci $a = 0$;
(iii) dacă $a \mid b$ şi $b \mid c$, atunci $a \mid c$;
(iv) dacă $a \mid b$ şi $b \mid a$, atunci $a = \pm b$;
(v) dacă $a \mid b$ şi $a \mid c$, atunci $a \mid (b + c)$;
(vi) dacă $a \mid b$, atunci $a \mid bc$;
(vii) dacă $a \mid b + c$ şi $a \mid b$, atunci $a \mid c$;
(viii) dacă $a \mid b$ şi $b \neq 0$, atunci $|a| \leq |b|$.

Demonstraţie. (i) Fie $a \in \mathbb{Z}$. Atunci

$$a = 1 \cdot a, \text{ respectiv } a = (-1) \cdot (-a),\ a = a \cdot 1 \text{ şi } a = (-a) \cdot (-1),$$

unde a, $-a$, 1, $-1 \in \mathbb{Z}$, iar $a \mid 0$ deoarece $0 = a \cdot 0$, unde $0 \in \mathbb{Z}$.
(ii) Din ipoteze obţinem

$$\begin{aligned} a \mid b &\Rightarrow \exists q_1 \in \mathbb{Z},\ b = a \cdot q_1; \\ b \mid c &\Rightarrow \exists q_2 \in \mathbb{Z},\ c = b \cdot q_2. \end{aligned}$$

Atunci,

$$c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2),\ \text{cu } q_1 \cdot q_2 \in \mathbb{Z}.$$

Deci, $a \mid c$.
(iii) Din ipoteze obţinem

$$\begin{aligned} a \mid b &\Rightarrow \exists q_1 \in \mathbb{Z},\ b = a \cdot q_1; \\ b \mid a &\Rightarrow \exists q_2 \in \mathbb{Z},\ a = b \cdot q_2. \end{aligned}$$

Atunci,

$$a = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2) \Rightarrow q_1 \cdot q_2 = 1.$$

Prin urmare, $q_1, q_2 \in \mathbb{Z}$ sunt inversabile, aşadar $q_1 \in \{-1, 1\}$ şi $a = \pm b$.

Lăsăm cititorului demonstrarea celorlalte proprietăţi ca exerciţiu.

Fie $a \in \mathbb{Z}$. Numim **divizori banali** (**divizori improprii**) ai lui a numerele ± 1 şi $\pm a$. Un divizor al lui a diferit de ± 1 şi de $\pm a$ se numeşte **divizor propriu** al lui a.

Observaţiile 8. a) Relaţia de divizibilitate pe $\mathbb{Z}$ este o relaţie de preordine pe $\mathbb{Z}$.
b) Relaţia de divizibilitate pe $\mathbb{Z}$ nu este o relaţie de ordine, deoarece ea nu este antisimetrică, după cum arată următorul exemplu:

$$2, -2 \in \mathbb{Z},\ 2|(-2) \text{ şi } (-2)|2, \text{ dar } 2 \neq -2.$$

c) Restricţia la $\mathbb{N}$ a relaţiei de divizibilitate din $\mathbb{Z}$ este o relaţie de ordine deoarece reflexivitatea şi tranzitivitatea se păstrează, iar dacă $a, b \in \mathbb{N}$ cu $a \mid b$ şi $b \mid a$, atunci $a = b$.

Un număr $d \in \mathbb{Z}$ este un **divizor comun** al numerelor întregi a şi b dacă $d \mid a$ şi $d \mid b$.

Fie $a, b \in \mathbb{Z}^*$. Dacă d este divizor comun pentru numerele $a, b \in \mathbb{Z}^*$, atunci $|d| \leq \min\{|a|, |b|\}$. Rezultă că există un cel mai mare element în mulţimea divizorilor comuni ai numerelor a şi b. Acest număr se numeşte **cel mai mare divizor comun al numerelor a şi b** şi se notează cu $d = (a, b)$ sau $d = \text{c.m.m.d.c.}(a, b)$.

Observaţiile 9. 1) Cum 1 este întotdeauna divizor comun, deducem că $(a, b) \in \mathbb{N}^*$ pentru orice $a, b \in \mathbb{Z}$.
2) Dacă exact unul din numerele a şi b este 0, atunci definiţia celui mai mare divizor comun poate fi extinsă pentru această situaţie.
3) Dacă $a, b \in \mathbb{Z}^*$, atunci

$$(a, b) = d \Leftrightarrow \begin{cases} d \in \mathbb{N}^*, \\ d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{N},\ c \mid a \text{ şi } c \mid b \Rightarrow c \leq d \end{cases}$$

Următorul rezultat este foarte util în practică şi ne spune că cel mai mare divizor comun a două numere întregi poate fi obţinut ca o combinaţie liniară a acestora.

Teorema 10. (reprezentarea Bézout a c.m.m.d.c.)
Dacă $a, b \in \mathbb{Z}^*$ şi $d = (a, b)$, atunci există $u, v \in \mathbb{Z}$ astfel încât

$$d = au + bv.$$

Demonstraţie. Fie $S = \{ax + by \mid ax + by > 0,\ x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$. Constatăm că $S \neq \emptyset$ pentru că $a = a \cdot 1 + b \cdot 0$ şi $-a = a \cdot (-1) + b \cdot 0$, prin urmare sau $a \in S$ sau $-a \in S$. Deci există d cel mai mic element din S. Fie $u, v \in \mathbb{Z}$ astfel încât $d = au + bv$.

Vom demonstra că $d \mid a$. Pentru aceasta aplicăm teorema împărţirii cu rest şi scriem $a = dq + r$, $0 \leq r < d$. Rezultă că

$$r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq).$$

Din $r < d$ rezultă $r \notin S$. Dar $1 - uq, -vq \in \mathbb{Z}$, deci $r \leq 0$ şi rezultă $r = 0$. Aşadar $d \mid a$. Analog se arată că $d|b$.

Fie $c \in \mathbb{N}$ cu $c \mid a$ şi $c \mid b$. Rezultă că $c \mid au + bv = d$, şi de aici găsim $c \leq |d| = d$. Aşadar $d = (a, b)$.

Dacă scriem $(a, b) = au + bv$, $u, v \in \mathbb{Z}$, atunci spunem că am ales o **reprezentare Bézout** pentru (a, b). Atragem atenţia că această reprezentare nu este unică.

Exemplul 11. De exemplu, $(2,3) = 1 = 2 \cdot 2 + 3 \cdot (-1) = 2 \cdot (-4) + 3 \cdot 3$.

Corolarul 12. Fie $a, b \in \mathbb{Z}^*$, $d = (a,b)$ şi $T = \{ax + by \mid x, y \in \mathbb{Z}\}$. Atunci

$$T = d\mathbb{Z}.$$

Demonstraţie. Reamintim că $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$ şi demonstrăm egalitatea prin dublă incluziune.

Fie $z \in T$. Atunci există $x, y \in \mathbb{Z}$ astfel încât $z = ax + by$. Din $d \mid a$ şi $d \mid b$ deducem $d \mid ax + by = z$, deci $z \in d\mathbb{Z}$. Aşadar $T \subseteq d\mathbb{Z}$ (elementul z a fost ales arbitrar).

Reciproc, dacă $z \in d\mathbb{Z}$, atunci există $k \in \mathbb{Z}$ cu $z = dk$. Fie $u, v \in \mathbb{Z}$ cu $d = au + bv$. Atunci $z = auk + bvk \in T$. Aşadar $d\mathbb{Z} \subseteq T$ şi soluţia este încheiată.

Urmărind finalul demonstraţiei Teoremei 10, deducem imediat:

Corolarul 13. Fie $a, b \in \mathbb{Z}^*$ şi $d \in \mathbb{N}^*$. Atunci

$$(a,b) = d \Leftrightarrow \begin{cases} d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{Z},\ c \mid a \text{ şi } c \mid b \Rightarrow c \mid d \end{cases}$$

Observaţiile 14. i) Definiţia c.m.m.d.c. aşa cum a fost dată anterior este mai uşor de asimilat de elevii de gimnaziu, ea putând fi corelată cu relaţie de ordine ,,naturală" din $\mathbb{Z}$. Totuşi, caracterizarea de mai sus este mai potrivită ca definiţie pentru c.m.m.d.c. Ea poate fi folosită ca definiţie pentru c.m.m.d.c. şiîn diverse tipuri de inele unde nu avem definită o relaţie ca $\leq$ din $\mathbb{Z}$ (de exemplu în $\mathbb{C}[X]$). În $\mathbb{Z}$ ea permite definirea c.m.m.d.c. pentru orice două numere întregi, chiar şi atunci când sunt ambele 0: *pentru* $a, b \in \mathbb{Z}$, *c.m.m.d.c.* $d = (a,b)$ *este numărul natural* $d \in \mathbb{N}$ *pentru care avem* $\begin{cases} d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{Z},\ c \mid a \text{ şi } c \mid b \Rightarrow c \mid d\,. \end{cases}$

Evident din această definiţie rezultă că $(0,0) = 0$.

ii) Atragem atenţia asupra faptului că dacă nu impunem mai sus ca numărul întreg d să fie chiar natural atunci atât d cât şi $-d$ satisfac condiţiile din definiţia de mai sus. În acest context, un c.m.m.d.c. este de fapt un reprezentant al unei o clase de echivalenţă. Pentru cazul inelului $\mathbb{Z}$, această clasă este mulţimea $\{-d, d\}$ din care s-a ales reprezentantul natural.