CURS 2

Algoritmul lui Euclid

Reamintim că pentru $a, b \in \mathbb{Z}$, c.m.m.d.c. $d = (a, b)$ este numărul natural $d \in \mathbb{N}$ pentru care avem

$$\begin{cases} d \mid a \text{ şi } d \mid b, \\ c \in \mathbb{Z},\ c \mid a \text{ şi } c \mid b \Rightarrow c \mid d\,. \end{cases}$$

Un caz special în studiul divizibilităţii îl ocupă perechile de numere care nu au divizori comuni proprii. Spunem că $a, b \in \mathbb{Z}$ sunt **relativ prime** (sau **prime între ele**) dacă $(a, b) = 1$. Aceste perechi pot fi caracterizate cu ajutorul reprezentărilor Bézout.

Propoziţia 1. Numerele întregi a şi b sunt relativ prime dacă şi numai dacă există $u, v \in \mathbb{Z}$ astfel încât $au + bv = 1$.

Demonstraţie. ($\Rightarrow$) Evident, există o reprezentare Bézout a c.m.m.d.c. (a, b) care este 1.
($\Leftarrow$) Fie $d = (a, b)$. Din $d \mid a$ şi $d \mid b$ rezultă că $d \mid au + bv = 1$, deci $d = 1$.

Corolarul 2. Dacă $a, b \in \mathbb{Z}^*$ şi $d = (a, b)$, atunci $d \neq 0$ şi $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstraţie. Din $d = (a, b)$ rezultă că există $u, v \in \mathbb{Z}$ astfel încât $d = au + bv$. Atunci $1 = \frac{a}{d}\,u + \frac{b}{d}\,v$, deci $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Folosim consideraţiile făcute până acum ca să demonstrăm proprietăţi importante ale relaţiei de divizibilitate.

Teorema 3. Fie $a, b, c \in \mathbb{Z}$. Sunt adevărate afirmaţiile:
(i) dacă $a \mid b$, $b \mid c$ şi $(a, b) = 1$, atunci $ab \mid c$;
(ii) **(Lema lui Euclid)** dacă $a \mid bc$ şi $(a, b) = 1$, atunci $a \mid c$.

Demonstraţie. (i) Fie $r, s \in \mathbb{Z}$ astfel încât $c = ar = bs$ şi $u, v \in \mathbb{Z}$ cu $au + bv = 1$. Atunci

$$c = c \cdot 1 = c(au + bv) = bsau + arbv = ab(su + rv).$$

Cum $su + rv \in \mathbb{Z}$, deducem că $ab \mid c$.
(ii) Fie $u, v, k \in \mathbb{Z}$ astfel încât $au + bv = 1$ şi $bc = ka$. Calculăm

$$c = c \cdot 1 = c(au + bv) = acu + bcv = acu + kav = a(cu + bv),$$

deci $a \mid c$.

În continuare, vom demonstra o teoremă care furnizează un procedeu de aflare a celui mai mare divizor comun, numit **algoritmul lui Euclid**, şi o metodă de a determina o reprezentare Bézout. Observăm că $(a, b) = (-a, b) = (a, -b) = (-a, -b)$. De asemenea, am văzut că

$$(a, 0) = a,\ \forall a \in \mathbb{Z},$$

deci este suficient să considerăm doar cazul $a, b \in \mathbb{N}^*$.

Teorema 4. (Algoritmul lui Euclid)
Fie a, $b \in \mathbb{N}^*$, cu $b \neq 0$ şi $b \leq a$. Considerăm identităţile următoarelor împărţiri:

$$\begin{aligned}
a &= b \cdot q_0 + r_0, && \text{unde } r_0 < b; \text{ fie } r_0 \neq 0; && (E_0)\\
b &= r_0 \cdot q_1 + r_1, && \text{unde } r_1 < r_0; \text{ fie } r_1 \neq 0; && (E_1)\\
r_0 &= r_1 \cdot q_2 + r_2, && \text{unde } r_2 < r_1; \text{ fie } r_2 \neq 0; && (E_2)\\
&\dots && \dots &&\\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1}, && \text{unde } r_{n-1} < r_{n-2}; \text{ fie } r_{n-1} \neq 0; && (E_{n-1})\\
r_{n-2} &= r_{n-1} \cdot q_n + r_n, && \text{unde } r_n < r_{n+1}; \text{ fie } r_n \neq 0; && (E_n)\\
r_{n-1} &= r_n \cdot q_{n+1} + r_{n+1}, && \text{unde } r_{n+1} = 0. && (E_{n+1})
\end{aligned}$$

Atunci cel mai mare divizor comun al numerelor a şi b este ultimul rest diferit de zero al acestor împărţiri, adică:

$$(a, b) = r_n.$$

Demonstraţie. Observăm că şirul resturilor diferite de zero este un şir strict descrescător

$$r_0 > r_1 > r_2 > ...$$

de numere naturale, deci acest şir este finit, adică, după un număr finit de împărţiri obţinem restul zero.

Demonstrăm că $r_n \mid a$ şi $r_n \mid b$ folosind inducţia completă pentru propoziţia

$$P(i) : r_n \mid r_{n-i}, \text{ unde } 0 \leq i \leq n.$$

Propoziţia $P(0)$ este, evident, adevărată. Din pasul (E_{n+1}) deducem că $r_n \mid r_{n-1}$. Presupunem că $r_n \mid r_{n-j}$ pentru orice $1 \leq j \leq i$ şi demonstrăm că $r_n \mid r_{n-(i+1)}$.

Pentru aceasta folosim relaţia $r_{n-(i+1)} = r_{n-i} \cdot q_{n-(i-1)} + r_{n-(i-1)}$, de unde concluzia este evidentă.

Deci r_n divide pe r_0 şi pe r_1, iar din egalitatea găsită în pasul (E_1) deducem $r_n \mid b$. Apoi folosim (E_0) ca să deducem şi $r_n \mid a$.

Fie $c \in \mathbb{N}$, astfel încât $c \mid a$ şi $c \mid b$. Vom arăta că $c \mid r_n$. Folosind din nou identităţile din enunţ, avem:

$$c \mid a = b \cdot q_0 + r_0 \text{ şi } c \mid (b \cdot q_0) \Rightarrow c \mid r_0.$$

Apoi obţinem:

$$c \mid b = r_0 \cdot q_1 + r_1 \text{ şi } c \mid (r_0 \cdot q_1) \Rightarrow c | r_1,$$

şi continuăm raţionamentul, parcurgând identităţile împărţirilor de la prima spre ultima. În final găsim

$$c \mid r_{n-2} = r_{n-1} \cdot q_n + r_n \text{ şi } c \mid (r_{n-1} \cdot q_n),$$

deci $c \mid r_n$.

În concluzie, $r_n = (a, b)$.

Observaţia 5. Plecând de la identităţile (E_0)–(E_n) putem găsi o reprezentare Bézout astfel: înlocuim succesiv resturile, plecând de la (E_n) către (E_0)

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \cdots,$$

iar în final obţinem pe r_n sub forma $r_n = au + bv$.

Observaţia 6. Algoritmul lui Euclid ne asigură că pentru orice două numere întregi există c.m.m.d.c.

Spunem că $m \in \mathbb{Z}$ este un **multiplu comun** al numerelor întregi a şi b dacă $a \mid m$ şi $b \mid m$.

Fie $a, b \in \mathbb{Z}^*$. Dacă m este multiplu comun pentru numerele a şi b, atunci $|m| \geq \max\{|a|, |b|\}$. Rezultă că există un cel mai mic element în mulţimea multiplilor comuni strict pozitivi ai numerelor a şi b. Acest număr se numeşte **cel mai mic multiplu comun al numerelor a şi b** şi se notează cu $m = [a, b] = \text{c.m.m.m.c.}(a, b)$. Aşadar,

$$[a, b] = m \Leftrightarrow \begin{cases} m \in \mathbb{N}^*, \\ a \mid m \text{ şi } b \mid m, \\ c \in \mathbb{N}^*, a \mid c \text{ şi } b \mid c \Rightarrow m \leq c. \end{cases}$$

Teorema 7. Oricare ar fi $a, b \in \mathbb{N}^*$, are loc egalitatea:

$$ab = (a, b)[a, b].$$

Demonstraţie. Fie $d = (a, b)$. Atunci există $r, s \in \mathbb{N}^*$ astfel încât $a = dr$, $b = ds$ şi $(r, s) = 1$. Notăm $m = drs = as = br$, deci m este multiplu comun al numerelor a şi b.

Dacă $c \in \mathbb{N}^*$ este un multiplu comun pentru a şi b, atunci există $x, y \in \mathbb{N}^*$ cu $c = ax = by$. Alegem o reprezentare Bézout $1 = ru + sv$ a lui 1 ($u, v \in \mathbb{Z}$). Calculăm

$$c = c \cdot 1 = c(ru + sv) = byru + axsv = m(yu + xv),$$

deci $m \mid c$. Din $m, c \in \mathbb{N}^*$ rezultă că $m \leq c$.

Din demonstraţia de mai sus se deduce imediat:

Corolarul 8. Fie $a, b \in \mathbb{Z}^*$ şi $m \in \mathbb{N}^*$. Atunci

$$m = [a, b] \Leftrightarrow \begin{cases} a \mid m \text{ şi } b \mid m, \\ c \in \mathbb{Z}, a \mid c \text{ şi } b \mid c \Rightarrow m \mid c. \end{cases}$$

Observaţia 9. Putem rescrie definiţia c.m.m.m.c. astfel: *pentru $a, b \in \mathbb{Z}$, c.m.m.m.c. $m = [a, b]$ este numărul natural $m \in \mathbb{N}$ pentru care avem* $\begin{cases} a \mid m \text{ şi } b \mid m, \\ c \in \mathbb{Z}, a \mid c \text{ şi } b \mid c \Rightarrow m \mid c. \end{cases}$

Observaţia 10. Din teorema anterioară rezultă că Algoritmul lui Euclid nu este un instrument util doar pentru calculul c.m.m.d.c. ci şi pentru calculului c.m.m.m.c.

Dacă $n \in \mathbb{Z}$, atunci spunem că divizorii ± 1 şi $\pm n$ ai lui n sunt **divizori improprii** (sau **banali**). Spunem că $n \neq 0$ este un **număr compus** dacă el are şi alţi divizori în afară de cei banali. Un număr p este **ireductibil** (sau **indecompozabil**) dacă $p \neq \pm 1$ şi el nu este compus.

Definiţia 11. Spunem că $p \in \mathbb{Z}$ este un **număr prim** dacă sunt îndeplinite condiţiile:

$$\begin{cases} p \neq \pm 1, \\ p \mid ab \Rightarrow p \mid a \text{ sau } p \mid b. \end{cases}$$

Observaţia 12. Să observăm că în limbajul obişnuit legat de studiul numerelor naturale în loc de ,,număr ireductibil" de foloseşte ,,număr prim". Aceasta se bazează pe faptul că cele două noţiuni sunt echivalente în $\mathbb{Z}$, conform Teoremei 13. Totuşi, vom vedea că există inele unde cele două noţiuni nu sunt identice.

Teorema 13. Un număr întreg este prim dacă şi numai dacă el este ireductibil.

Demonstraţie. Presupunem că există un număr prim p care nu este ireductibil. Rezultă că există $a, b \in \mathbb{Z} \setminus \{\pm 1, \pm p\}$ astfel încât $p = ab$.

Din faptul că p este prim şi $p \mid ab$ deducem $p \mid a$ sau $p \mid b$. Dacă $p \mid a$, din $p = ab$ rezultă şi $a \mid p$, deci $a = \pm p$, contradicţie. Analog se obţine o contradicţie dacă $p \mid b$. Aşadar presupunerea iniţială este falsă, deci *orice număr prim este ireductibil.*

Reciproc, fie p un număr ireductibil şi $a, b \in \mathbb{Z}$ astfel încât $p \mid ab$. Atunci există $k \in \mathbb{Z}$ astfel încât $ab = pk$. Să presupunem că $p \nmid a$ şi $p \nmid b$. Atunci $(p, b) \neq |p|$ implică $(p, b) = 1$. Prin urmare, există $u, v \in \mathbb{Z}$ astfel încât $1 = pu + bv$. Rezultă că $a = apu + abv = pau + pkv$ se divide cu p, contradicţie. Aşadar presupunerea iniţială este falsă, deci *orice număr ireductibil este prim.*