CURS 3

Teorema fundamentală a aritmeticii

Reamintim din cursul anterior:

• Spunem că $n \in \mathbb{Z}^*$ este un **număr compus** dacă el are şi alţi divizori în afară de ± 1 şi $\pm n$.

• Spunem că $p \in \mathbb{Z}^*$ este **ireductibil** (sau **indecompozabil**) dacă $p \neq \pm 1$ şi el nu este compus.

• Spunem că $p \in \mathbb{Z}^*$ este un **prim** dacă sunt îndeplinite condiţiile $\begin{cases} p \notin \{-1, 1\}, \\ p \mid ab \Rightarrow p \mid a \text{ sau } p \mid b. \end{cases}$

• În $\mathbb{Z}$ nu facem distincţie între ,,număr ireductibil" şi ,,număr prim" deoarece

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

Demonstraţie. Dacă p este un număr prim şi $a, b \in \mathbb{Z}^*$ astfel încât $p = ab$ atunci $p \mid ab$ şi deducem $p \mid a$ sau $p \mid b$. Dacă $p \mid a$, din $p = ab$ rezultă şi $a \mid p$. Prin urmare,

$$a = \pm p \text{ şi } b = \pm 1,$$

deci p este ireductibil. Analog se tratează cazul $p \mid b$.

Reciproc, fie p un număr ireductibil şi $a, b \in \mathbb{Z}$ astfel încât $p \mid ab$. Să considerăm că $p \nmid a$. Aşa cum am văzut în cursul anterior, algoritmul lui Euclid ne asigură că c.m.m.d.c. există pentru orice două numere întregi. Aşadar, există $d = (a, p) \in \mathbb{N}$. Cum p este ireductibil şi $d \mid p$ avem $d \in \{1, |p|\}$. Din $p \nmid a$ rezultă $d \neq |p|$, prin urmare $d = 1$. Dar

$$p \mid ab \text{ şi } (p, a) = 1 \;\Rightarrow\; p \mid b,$$

deci p este un număr prim.

Observaţiile 1. a) Spre deosebire de demonstraţia dată la cursul anterior, cea de mai sus nu foloseşte reprezentarea Bézout a c.m.m.d.c., fapt care va fi util în abordarea divizibilităţii în domenii de integritate. Vom vedea (fără schimbări consistente în demonstraţie) că *în orice domeniu de integritate în care orice două elemente au un c.m.m.d.c. un element este prim dacă şi numai dacă este ireductibil.*

b) Din definiţia numerelor prime rezultă imediat că un număr p este prim dacă şi numai dacă $-p$ este prim. Aşadar, *numerele întregi prime sunt numerele naturale prime şi opusele lor.* Având în vedere acest fapt, dar şi din considerente care vin din structura programei şcolare, în continuare vom folosi termenul **număr prim** cu sensul de număr natural prim.

c) Proprietatea secundă din definiţia numerelor (întregi) prime poate fi extinsă la produse cu un număr arbitrar de factori. Astfel,

$$p \text{ prim şi } p \mid a_1 \cdot \ldots \cdot a_n \;\Rightarrow\; \exists i \in \{1, \ldots, n\} \text{ astfel încât } p \mid a_i.$$

Aşa cum vom vedea în următoarele teoreme, numerele prime au un rol fundamental în studiul divizibilităţii în $\mathbb{N}$ şi $\mathbb{Z}$.

Teorema 2. (Teorema fundamentală a aritmeticii (în $\mathbb{N}$))
Orice număr natural $n \geq 2$ se scrie ca un produs de numere prime. Această scriere este unică, abstracţie făcând de ordinea factorilor. Mai precis, pentru orice $n \in \mathbb{N}$, $n \geq 2$ există $p_1, \ldots, p_k$ numere prime (nu neapărat diferite) astfel încât

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

şi din $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$, cu $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ numere prime, rezultă $k = l$ şi existenţa unei funcţii bijective $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ astfel încât

$$p_i = q_{\sigma(i)}, \ \forall i \in \{1, \ldots, k\}.$$

Demonstraţie. Pentru existenţa descompunerii în factori primi vom folosi metoda inducţiei complete în raport cu $n \in \mathbb{N}$, $n \geq 2$.

Etapa de verificare: Pentru că 2 este număr prim, e clar că proprietatea e valabilă pentru $n = 2$ ($k = 1$, $p_1 = 2$).

Etapa de demonstraţie: Presupunem că orice $m \in \mathbb{N}$, $2 \leq m < n$ se descompune într-un produs cu toţi factorii numere prime şi arătăm că şi n are aceeaşi proprietate. Avem două cazuri:
i) Dacă n este prim, proprietatea este evidentă ($k = 1$, $p_1 = n$).
ii) Dacă n nu este prim, atunci există $a, b \in \mathbb{N}$ cu $n = ab$, $a \notin \{1, n\}$. Deci $1 < a, b < n$ şi aplicând ipoteza inducţiei, obţinem:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_j \text{ şi } b = p_{j+1} \cdot p_{j+2} \cdot \ldots \cdot p_k,$$

unde $p_i \in \mathbb{N}$, sunt numere prime pentru orice $i = 1, \ldots, k$. Atunci

$$n = a \cdot b = p_1 \cdot p_2 \cdot \ldots \cdot p_j \cdot p_{j+1} \cdot p_{j+2} \cdot \ldots \cdot p_k,$$

adică n admite o descompunere în factori primi.

Ca să demonstrăm unicitatea descompunerii în factori primi, considerăm două descompuneri ale lui n în produse de factori primi

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

unde $k, l \in \mathbb{N}^*$. Pentru că înmulţirea este (asociativă şi) comutativă, putem presupune

$$p_1 \leq p_2 \leq \ldots \leq p_k \text{ şi } q_1 \leq q_2 \leq \ldots \leq q_l.$$

Din $p_k \mid n = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ rezultă că există $i \in \{1, \ldots, l\}$ astfel încât $p_k \mid q_i$, deci $p_k \leq q_l$. Analog se demonstrează şi inegalitatea $q_l \leq p_k$, deci $p_k = q_l$ şi

$$p_1 \cdot p_2 \cdot \ldots \cdot p_{k-1} = q_1 \cdot q_2 \cdot \ldots \cdot q_{l-1}.$$

Continuăm procedeul de mai sus şi obţinem $p_{k-1} = q_{l-1}$ şi mai departe $p_{k-i} = q_{l-i}$ pentru orice $0 \leq i \leq \min\{k, l\}$. Dacă am avea $k \neq l$, atunci s-ar obţine că 1 este un produs de numere prime, ceea ce e imposibil. Aşadar $k = l$ şi $p_i = q_i$ pentru orice $i \in \{1, \ldots, k\}$.

Întrucât înmulţirea numerelor naturale este comutativă şi asociativă, putem aduce împreună toţi factorii primi egali din descompunerea lui n din teorema anterioară. Astfel obţinem:

Corolarul 3. Pentru orice $n \in \mathbb{N}$, $n \geq 2$, există $k \in \mathbb{N}^*$, numerele prime distincte $p_1, \ldots, p_k$ şi $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$ astfel încât

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Această descompunere este unică dacă facem abstracţie de ordinea factorilor.

Descompunerea din Corolarul 3 se numeşte **descompunerea canonică** a lui n (în produs de puteri de numere prime).

Exemplul 4. De exemplu, pentru 360 descompunerea canonică este $360 = 2^3 \cdot 3^2 \cdot 5$.

Fie $(\alpha_k)_{k>0}$ un şir de numere naturale. Spunem că numerele α_k ($k \in \mathbb{N}^*$) sunt **aproape toate nule** dacă există $k_0 \in \mathbb{N}^*$ astfel încât $\alpha_k = 0$ pentru orice $k > k_0$. Folosind această terminologie putem reformula Corolarul 3 astfel:

Corolarul 5. Considerăm şirul crescător al numerelor prime

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots\ .$$

Pentru orice $n \in \mathbb{N}^*$ există un singur şir $(\alpha_k)_{k>0}$ de numere naturale aproape toate nule astfel încât

$$n = \prod_{k \geq 1} p_k^{\alpha_k}.$$

Observaţia 6. Pentru $n = 1$, avem $n = \prod_{k\geq 1} p_k^0$, i.e. şirul $(\alpha_k)_{k>0}$ este şirul constant nul şi toţi factorii produsului sunt 1. Pentru orice $n \geq 2$, în produsul $\prod_{k\geq 1} p_k^{\alpha_k}$ din corolarul de mai sus doar un număr finit de factori sunt diferiţi de 1, ceea ce dă sens scrierii oricărui număr natural nenul sub forma indicată în corolarul anterior.

Exemplul 7. Pentru $n = 5$, şirul $(\alpha_k)_{k>0}$ are pe 1 pe poziţia a treia ($\alpha_3 = 1$) şi pe 0 pe celelalte poziţii. Pentru $n = 360$ avem $(\alpha_k)_{k>0} = (3, 2, 1, 0, 0, \ldots, 0, \ldots)$.

Această formă a teoremei fundamentale a aritmeticii ne permite să scriem:

Propoziţia 8. Fie $m = \prod_{k\geq 1} p_k^{\alpha_k}$ şi $n = \prod_{k\geq 1} p_k^{\beta_k}$ descompunerile numerelor naturale $m, n > 0$ date de Corolarul 5. Atunci:
a) $m \mid n \Leftrightarrow \alpha_k \leq \beta_k,\ \forall k > 0$;
b) $(m, n) = \prod_{k\geq 1} p_k^{\min\{\alpha_k, \beta_k\}}$;
c) $[m, n] = \prod_{k\geq 1} p_k^{\max\{\alpha_k, \beta_k\}}$.

Observaţiile 9. i) Echivalenţa a) din propoziţia anterioară este o reformulare a faptului $m \mid n$ dacă şi numai dacă toţi factorii din descompunerea lui m apar şi în descompunerea lui n.
ii) Egalităţile b) şi c) sunt întâlnite şi în gimnaziu. Forma în care le folosesc elevii porneşte de la descompunerile canonice ale celor două numere m şi n şi astfel ei ştiu că *c.m.m.d.c. al numerelor m şi n este un produs de puteri ale factorilor primi comuni celor descompuneri, fiecare factor prim fiind luat la puterea cu exponentul nenul cel mai mic*, iar *c.m.m.m.c. al numerelor m şi n este un produs de puteri ale factorilor primi comuni şi necomuni din cele două descompuneri, fiecare factor prim fiind luat la puterea cu exponentul cel mai mare.*

Teorema fundamentală a aritmeticii poate fi formulată şi în $\mathbb{Z}$ astfel:

Teorema 10. Pentru orice număr întreg $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ există $u \in \{-1, 1\}$ şi numerele întregi prime (nu neapărat diferite) $p_1, \ldots, p_k$ astfel încât

$$n = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

şi dacă $n = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_l$, cu $u, v \in \{-1, 1\}$ şi $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ numere întregi prime, atunci $k = l$ şi există o funcţie bijectivă $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ astfel încât

$$p_i \in \{-q_{\sigma(i)}, q_{\sigma(i)}\}, \ \forall i \in \{1, \ldots, k\}.$$

Observaţiile 11. 1) Observăm că descompunerea lui n de mai sus este unică, abstracţie făcând de ordinea factorilor şi de semnul lor. Reformulând teorema înlocuind ,,numere întregi prime" cu ,,numere prime" (a se vedea observaţia 1 b)) semnul lui n este preluat de u, ceea ce face ca ceilalţi factori din descompunere să fie unic determinaţi până la o bijecţie.
2) Şi pentru numere întregi $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ putem da descompunerii în factori primi o formă similară descompunerii canonice a unui număr natural.

Exerciţiul 1. Să se arate că numărul $\sqrt{6}$ este iraţional.

Soluţie: Prin reducere la absurd, presupunem că $\sqrt{6} \in \mathbb{Q}$. Atunci există $m, n \in \mathbb{N}^*$ astfel încât $\frac{m}{n} = \sqrt{6}$. Dacă $d = (m, n)$ şi $m = du$, $n = dv$, atunci $\sqrt{6} = \frac{u}{v}$ şi $(u, v) = 1$. Rezultă că $6v^2 = u^2$. Cum $6 = 2 \cdot 3$, avem $2 \mid u^2$. Cum 2 este număr prim, rezultă că $2 \mid u$. Aşadar $u = 2k$, prin urmare $6v^2 = 4k^2$, de unde găsim $2 \mid v^2$. Folosim din nou faptul că 2 este prim şi obţinem $2 \mid v$, deci $2 \mid (u, v)$, contradicţie. Aşadar $\sqrt{6} \notin \mathbb{Q}$.

Definiţia 12. Un număr întreg d este **liber de pătrate** dacă nu se divide prin pătratul nici unui număr prim.

Observaţiile 13. a) Un număr $d \in \mathbb{Z} \setminus \{-1, 0, 1\}$ este liber de pătrate dacă şi numai dacă toţi factorii primi care apar în descompunerea sa au exponentul 1.
b) Un raţionament cu totul analog cu cel din exerciţiul anterior se poate desfăşura pentru a arăta că $\sqrt{p} \in \mathbb{C} \setminus \mathbb{Q}$ *pentru orice număr întreg prim* p.

Exerciţiul 2. Să se arate că există o infinitate de numere prime.

Soluţie: Pentru a arăta că există o infinitate de numere prime este suficient să demonstrăm că oricare ar fi $S = \{p_1, \ldots, p_m\}$ o mulţime de numere prime există un număr prim $p \notin S$.

Fie $S = \{p_1, \ldots, p_m\}$ o mulţime nevidă de numere prime. Numărul $n = p_1 \cdot \ldots \cdot p_m + 1$ este mai mare sau egal decât 2, prin urmare există un divizor prim p al lui n.

Dacă am avea $p \in S$, din $p \mid p_1 \cdot \ldots \cdot p_m + 1$ şi $p \mid p_1 \cdot \ldots \cdot p_m$ rezultă că $p \mid 1$, contradicţie. Deci $p \notin S$, ceea ce trebuia demonstrat.