§6 Teorema de bază a aritmeticii. Forma canonică a numărului compus

Teorema (Teorema de bază a aritmeticii)

Orice nr. natural mai mare ca 1 este prim sau se descompune în mod unic ~~de fa~~ în produs de factori primi.

(Unicitatea descompunerii este cu exactitate de ordine a factorilor)

1. Demonstr. existența descompunerii (vom folosi metoda inducției matematice)

1) Pentru $a=2$, avem că a este prim. are loc afirmația din teorema

2) Presupunem că afirmația este adevărată pentru: $\forall a,\quad 2 \le a < n$

3) $a=n$, dacă n - prim, teorema este demonstrată, iar dacă n - este compus, atunci există:

$n_1, n_2 \in N$

$2 \le n_1 < n$

$2 \le n_2 < n$

$a = n_1 \cdot n_2$

În baza presupunerii $\Rightarrow$ n_1 și n_2 sau sunt nr. prime sau se descompun în produs de factori primi.

$n_1 = p_1 p_2 \dots p_s$

$n_2 = q_1 q_2 \dots q_t$

p_i și q_j – prime
$i = \overline{1,s}$
$j = \overline{1,t}$

$a = p_1 p_2 \dots p_s\, q_1 q_2 \dots q_t$

Concluzie: din 1) 2) 3) $\xRightarrow{\text{princ. ind. mat}}$ că afirmația este adevărată pentru orice $a > 1$, adică $\forall a > 1$ sau sunt prime sau se descompun în prod. de factori primi.

2 Unicitatea descompunerii

Presupunem că a posedă două descompuneri în produs de factori primi

$a = p_1 p_2 \dots p_k$ (1)

$a = q_1 q_2 \dots q_r$ (2)

$p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_r$

Dacă presupunem că $k < r$. din prop. nr. prime, obținem:

$1 = q'_{k+1} \cdot q'_{k+2} \dots q_r$, q'_i - nr. prime

contradicție.

Presupunem $k > r$.

$1 = p'_{r+1} \cdot p'_{r+2} \dots p'_k$ - contradicție

p'_i - nr. prime, astfel am demonstrat că $k = r$.

Revenind la $\underbrace{p_1 p_2 \dots p_k}_{\vdots p_1} = \underbrace{q_1 q_2 \dots q_k}_{\vdots p_1} \Rightarrow$

$\Rightarrow \exists q_1' = p_1$

$\exists q_2' = p_2$

$\dots$

$\exists q_k' = p_k$

$\{q_1', \dots q_k'\} = \{q_1, q_2 \dots q_k\}$

$\{p_1 p_2 \dots p_k\} = \{q_1, q_2 \dots q_k\}$

Reprezentările (1) și (2) coincid

03.05.13.

§7. Reprezentarea canonică a nr. natural

Fie $a \in N$, $a > 1$. Conform teorem. de bază a aritmeticii nr. a se descompune în produs de factori primi.

Admitem că în descompunerea nr. a nr. p_1 se repetă de α_1 ori, nr. p_2 – α_2 ori, p_s – α_s ori, atunci nr. a poate fi scris:

$p_1, p_2, \dots, p_s$ – nr. prime diferite

$\boxed{a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_s^{\alpha_s}}$ – reprezentare canonică a lui a

Exemplu:

$a = 360.$ $\quad p_1 = 2^3$ $\quad a = 2^3 \cdot 3^2 \cdot 5^1$

360	2
180	2
90	2
45	3
15	3
5	5
1	

$p_2 = 3^2$

$p_3 = 5^1$

Teoremă 1

Nr d este divizor natural al nr a, dacă şi numai dacă $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, $0 \leq \beta_i \leq \alpha_i$, $i = \overline{0,s}$

Necesitatea

Admitem că $a \vdots d$, vom demonstr. că d se reprezintă sub forma.

$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$

$\exists\, q \in N$, încît $a = d \cdot q$.

Observăm că orice divizor al nr. d, este şi divizor al nr a

Dacă p_1 - este un divizor prim al numărului $d \rightarrow d \vdots p_1 \Rightarrow a \vdots p_1$

Analog observăm că:

$d \vdots p_1^{\gamma_1} \Rightarrow a \vdots p_1^{\gamma_1}$

Observăm că dacă $d \vdots p_i$, $i = \overline{1,s}$,

putem afirma că $d \vdots p_1 p_2 \dots p_s \Rightarrow$
$d \vdots p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s}$, deoarece
d este divizor a lui a, obținem
că $0 \le \gamma_i \le \alpha_i$,
Dacă considerăm că $\beta_i = \gamma_i$, obținem
$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, $0 \le \beta_i \le \alpha_i$

Suficiența
Fie $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, iar
$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, $0 \le \beta_i \le \alpha_i$,
vom demonstra că $a \vdots d$
Deoarece $\alpha_i - \beta_i \ge 0$, considerăm
nr $q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_s^{\alpha_s - \beta_s}$,
observă că $d \cdot q = a \Rightarrow a \vdots d$ ■

Teorema 2
Dacă $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}$ $\alpha_i \ge 0$,
$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_s^{\beta_s}$ $\beta_i \ge 0$,
atunci cel mai mare diviz
comun al nr a și b = d
$(a, b) = d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s}$,
$\gamma_i = \min(\alpha_i, \beta_i)$
■ Într-adevăr conf. T.1
din faptul că d este
divizor comun a numerelor

(a, b) ; $p_i^{\alpha_i}$; $p_i^{\gamma_i}$

$p_i^{\beta_i}$; $p_i^{\gamma_i}$ $\xRightarrow{d(a,b)}$ $\gamma_i = \min(\alpha_i; \beta_i)$

Ехтимол:

$a = 360$, $a = 2^3 \cdot 3^2 \cdot 5$ 7^0

$b = 252$, $b = 2^2 \cdot 3^2 \cdot 7 \cdot 5^0$

$$\begin{array}{r|l} 252 & 2 \\ 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

$d = 2^2 \cdot 3^2 = 4 \cdot 9 = 36$.