§5 Nr. prime
Proprietăți.

Fie N - mulț. nr. naturale, care este o submulțime din Z

Definiție

Numărul $a \in N$, $a > 1$, se numește **prim** dacă unicii divizori ai lui sunt 1 și a.

2, 3, 5, 7, 11, 13, 17, 19,

Definiție

Numarul $a \in N$, $a > 1$, care nu-i prim se numeste **număr compus**.

4, 6, 8, 9, 10, 12, ...

În asa mod, mulț. nr. naturale N se divizează în 3 clase.

Teorema 1

Cel mai mic divizor natural diferit de 1, al numarului compus a este un nr. prim, care nu întrece $\sqrt{a}$

a - compus

p - cel m. mic div. natural

$p \neq 1$. $a \vdots p$.

1) p - nr. prim ?

2) $p \leq \sqrt{a}$ - ?

1) $a \vdots p \Rightarrow a = pq$

admitem că p - compus.

$p = p_1 \cdot p_2$

$1 < p_1 < p$
$1 < p_2 < p.$

$a = p_1 p_2 q \Rightarrow a \vdots p_1$

$p_1 < p$ - contradicție cu ipoteza

p - prim.

2) $p \leq \sqrt{a}$ - ?

avem: $a = p \cdot q$
$p \leq q$, deoarece p c.m. mic d. comun.

$p^2 \leq pq$
$p^2 \leq a \Rightarrow p \leq \sqrt{a}$. c.t.d.d.

Exemple:

(253, 257).

$\sqrt{253} \approx 15$
$\underline{2}, \underline{3}, \underline{5}, \underline{7}, 11, 13.$

$\sqrt{257} \approx 16$
$\underline{2}, \underline{3}, \underline{5}, \underline{7}, \underline{11}, \underline{13}$

Teorema 2
Mulțimea nr. prime este infinită.

Notăm prin P - mult. nr. prime.

Admitem contrariul: P - mulț. finită.
Atunci notăm mulț. nr. prime
$P = \{p_1, p_2, p_3, \ldots, p_n\}$.
Alcătuim numarul
$$a = \underbrace{p_1 \cdot p_2 \cdots p_n}_{2k} + 1$$

1) Admitem că a - este nr. prim $\Rightarrow a \in P$,

$a = p_i$

$\underbrace{p_i}_{\vdots p_i} = \underbrace{p_1 \cdot p_2 \cdots p_n}_{\vdots p_i} + 1 \Rightarrow 1 \vdots p_i$ - contradicție

În așa mod concluzionăm ca **a** nu poate fi nici compus nici prim.

2. a - compus $\overset{T_1}{\Rightarrow}$ că $\exists P$ - nr. prim care este un divizor al lui a $(a \vdots P)$

$a = P \cdot q$

$\underbrace{Pq}_{\vdots P} = \underbrace{p_1 \cdot p_2 \cdots p_n}_{\vdots P} + 1 \Rightarrow 1 \vdots P$.

În așa mod concluzionăm că mulțimea P nu poate fi finită, dar doar infinită.

Unele proprietăți ale nr. prime

1°. a - nr. compus, iar p - nr. prim
atunci $\Rightarrow a \vdots p$ sau $(a,p)=1$ (reciproc prime)

$\blacksquare$ 1) Admitem că $a \not\vdots\, p$
$(a,p)=1$? (vom demonstra că a și p - reciproc prime)

Presupunem că $(a,p)=d \Rightarrow p \vdots d$, $a \vdots d$

Deoarece: $d=1$ și $d=p$ sau $a \not\vdots\, p \Rightarrow d=1$
$(a,p)=1$.

2) Admitem că $(a,p) \neq 1 \Rightarrow a,p = d \Rightarrow$
$p \vdots d \Rightarrow d=p$. $(d \neq 1)$

$(a,p)=p \Rightarrow a \vdots p$. $\blacksquare$

2° Dacă p_1 și p_2 sunt două numere prime, încît $p_1 \vdots p_2 \Rightarrow p_1 = p_2$

3° Dacă $a,b \vdots p$; p - prim $\Rightarrow a \vdots p \lor b \vdots p$.

$\blacksquare$ Admitem că $ab \vdots p$ și $a \not\vdots\, p$. $b \vdots p$ - ?
conform proprietății 1 din faptul că
$a \not\vdots\, p \Rightarrow (a,p)=1 \xRightarrow{\text{repr. lin.}} \exists\, x,y \in \mathbb{Z}$,

încît $ax+py=1 \,/ \times b$

~~(a,p)~~ $\underbrace{bax}_{\vdots p} + \underbrace{bpy}_{\vdots p} = b \Rightarrow b \vdots p$.

$\blacksquare$