Osnovni pojmovi teorije brojeva

Marko Đikić

Univerzitet u Nišu
Prirodno Matematički Fakultet

februar 2010

Istraživačka stanica Petnica

Definicija

Neka su a i b prirodni brojevi. Kažemo da broj a deli broj b ako postoji prirodan broj c tako da je $ac = b$. Zapisujemo

$$a|b.$$

- $a|b \wedge a|c \Rightarrow a|b \pm c$
- $a|b \Rightarrow xa|xb$, za svako $x \in \mathbb{N}$
- $ab|ac \Rightarrow b|c$.

Teorema (o deljenju sa ostatkom)

Neka su a i b prirodni brojevi. Tada postoje jedinstveni brojevi q i r, sa svojstvom da je $0 \leq r < b$ i da je

$$a = q \cdot b + r.$$

Definicija

Neka su a i b prirodni brojevi. Kažemo da broj a deli broj b ako postoji prirodan broj c tako da je $ac = b$. Zapisujemo

$$a|b.$$

- $a|b \wedge a|c \Rightarrow a|b \pm c$
- $a|b \Rightarrow xa|xb$, za svako $x \in \mathbb{N}$
- $ab|ac \Rightarrow b|c$.

Teorema (o deljenju sa ostatkom)

Neka su a i b prirodni brojevi. Tada postoje jedinstveni brojevi q i r, sa svojstvom da je $0 \leq r < b$ i da je

$$a = q \cdot b + r.$$

Definicija

Neka su a i b prirodni brojevi. Kažemo da broj a deli broj b ako postoji prirodan broj c tako da je $ac = b$. Zapisujemo

$$a|b.$$

- $a|b \wedge a|c \Rightarrow a|b \pm c$
- $a|b \Rightarrow xa|xb$, za svako $x \in \mathbb{N}$
- $ab|ac \Rightarrow b|c$.

Teorema (o deljenju sa ostatkom)

Neka su a i b prirodni brojevi. Tada postoje jedinstveni brojevi q i r, sa svojstvom da je $0 \leq r < b$ i da je

$$a = q \cdot b + r.$$

Definicija

Neka su a i b prirodni brojevi. Kažemo da broj a deli broj b ako postoji prirodan broj c tako da je $ac = b$. Zapisujemo

$$a|b.$$

- $a|b \wedge a|c \Rightarrow a|b \pm c$
- $a|b \Rightarrow xa|xb$, za svako $x \in \mathbb{N}$
- $ab|ac \Rightarrow b|c$.

Teorema (o deljenju sa ostatkom)

Neka su a i b prirodni brojevi. Tada postoje jedinstveni brojevi q i r, sa svojstvom da je $0 \leq r < b$ i da je

$$a = q \cdot b + r.$$

Definicija

Neka su a i b prirodni brojevi. Kažemo da broj a deli broj b ako postoji prirodan broj c tako da je $ac = b$. Zapisujemo

$$a|b.$$

- $a|b \wedge a|c \Rightarrow a|b \pm c$
- $a|b \Rightarrow xa|xb$, za svako $x \in \mathbb{N}$
- $ab|ac \Rightarrow b|c$.

Teorema (o deljenju sa ostatkom)

Neka su a i b prirodni brojevi. Tada postoje jedinstveni brojevi q i r, sa svojstvom da je $0 \leq r < b$ i da je

$$a = q \cdot b + r.$$

Definicija

Broj $n \in \mathbb{N}$ je prost ako je veći od 1 *i deljiv jedino brojevima* 1 *i* n.

Lema

Svaki broj je deljiv nekim prostim brojem.

- Beskonačno mnogo prostih brojeva.

Teorema (Osnovna teorema aritmetike)

Za svaki prirodan broj n veći od 1 *postoje jedinstveni $k \in \mathbb{N}$, prosti brojevi $p_1 < p_2 < \ldots < p_k$ i $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ takvi da je*

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

- Eratostenovo sito.

Definicija

Broj $n \in \mathbb{N}$ je prost ako je veći od 1 *i deljiv jedino brojevima* 1 *i* n.

Lema

Svaki broj je deljiv nekim prostim brojem.

- Beskonačno mnogo prostih brojeva.

Teorema (Osnovna teorema aritmetike)

Za svaki prirodan broj n veći od 1 *postoje jedinstveni $k \in \mathbb{N}$, prosti brojevi $p_1 < p_2 < \ldots < p_k$ i $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ takvi da je*

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

- Eratostenovo sito.

Definicija

Broj $n \in \mathbb{N}$ je prost ako je veći od 1 i deljiv jedino brojevima 1 i n.

Lema

Svaki broj je deljiv nekim prostim brojem.

- Beskonačno mnogo prostih brojeva.

Teorema (Osnovna teorema aritmetike)

Za svaki prirodan broj n veći od 1 postoje jedinstveni $k \in \mathbb{N}$, prosti brojevi $p_1 < p_2 < \ldots < p_k$ i $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ takvi da je

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

- Eratostenovo sito.

Definicija

Broj $n \in \mathbb{N}$ je prost ako je veći od 1 *i deljiv jedino brojevima* 1 *i* n.

Lema

Svaki broj je deljiv nekim prostim brojem.

- Beskonačno mnogo prostih brojeva.

Teorema (Osnovna teorema aritmetike)

Za svaki prirodan broj n veći od 1 *postoje jedinstveni $k \in \mathbb{N}$, prosti brojevi $p_1 < p_2 < \ldots < p_k$ i $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ takvi da je*

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

- Eratostenovo sito.

Definicija

Broj $n \in \mathbb{N}$ je prost ako je veći od 1 *i deljiv jedino brojevima* 1 *i* n.

Lema

Svaki broj je deljiv nekim prostim brojem.

- Beskonačno mnogo prostih brojeva.

Teorema (Osnovna teorema aritmetike)

Za svaki prirodan broj n veći od 1 *postoje jedinstveni $k \in \mathbb{N}$, prosti brojevi $p_1 < p_2 < \ldots < p_k$ i $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ takvi da je*

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

- Eratostenovo sito.

- Ako je p prost, tada važi $p|ab \Rightarrow p|a \vee p|b$.
- Ako je p prost, tada iz $p|a^2$ sledi $p^2|a^2$.

Definicija

Neka su a i b prirodni brojevi. Najveći zajednički delilac brojeva a i b je broj d, takav da $d|a$ i $d|b$, a nijedan broj veći od d nema tu osobinu. Pišemo $d = (a, b)$.

Najmanji zajednički sadržalac, s, brojeva a i b je takav broj da $a|s$ i $b|s$, a nijedan broj manji od s nema tu osobinu. Pišemo $s = [a, b]$.

- Ako je $d = (a, b)$ tada $1 = (\frac{a}{d}, \frac{b}{d})$.
- $(a, b)[a, b] = ab$.

- Ako je p prost, tada važi $p|ab \Rightarrow p|a \vee p|b$.
- Ako je p prost, tada iz $p|a^2$ sledi $p^2|a^2$.

Definicija

Neka su a i b prirodni brojevi. Najveći zajednički delilac brojeva a i b je broj d, takav da $d|a$ i $d|b$, a nijedan broj veći od d nema tu osobinu. Pišemo $d = (a, b)$.

Najmanji zajednički sadržalac, s, brojeva a i b je takav broj da $a|s$ i $b|s$, a nijedan broj manji od s nema tu osobinu. Pišemo $s = [a, b]$.

- Ako je $d = (a, b)$ tada $1 = (\frac{a}{d}, \frac{b}{d})$.
- $(a, b)[a, b] = ab$.

- Ako je p prost, tada važi $p|ab \Rightarrow p|a \vee p|b$.
- Ako je p prost, tada iz $p|a^2$ sledi $p^2|a^2$.

Definicija

Neka su a i b prirodni brojevi. Najveći zajednički delilac brojeva a i b je broj d, takav da $d|a$ i $d|b$, a nijedan broj veći od d nema tu osobinu. Pišemo $d = (a, b)$.
Najmanji zajednički sadržalac, s, brojeva a i b je takav broj da $a|s$ i $b|s$, a nijedan broj manji od s nema tu osobinu. Pišemo $s = [a, b]$.

- Ako je $d = (a, b)$ tada $1 = (\frac{a}{d}, \frac{b}{d})$.
- $(a, b)[a, b] = ab$.

- Ako je p prost, tada važi $p|ab \Rightarrow p|a \vee p|b$.
- Ako je p prost, tada iz $p|a^2$ sledi $p^2|a^2$.

Definicija

Neka su a i b prirodni brojevi. Najveći zajednički delilac brojeva a i b je broj d, takav da $d|a$ i $d|b$, a nijedan broj veći od d nema tu osobinu. Pišemo $d = (a, b)$.
Najmanji zajednički sadržalac, s, brojeva a i b je takav broj da $a|s$ i $b|s$, a nijedan broj manji od s nema tu osobinu. Pišemo $s = [a, b]$.

- Ako je $d = (a, b)$ tada $1 = (\frac{a}{d}, \frac{b}{d})$.
- $(a, b)[a, b] = ab$.

- Ako je p prost, tada važi $p|ab \Rightarrow p|a \vee p|b$.
- Ako je p prost, tada iz $p|a^2$ sledi $p^2|a^2$.

Definicija

Neka su a i b prirodni brojevi. Najveći zajednički delilac brojeva a i b je broj d, takav da $d|a$ i $d|b$, a nijedan broj veći od d nema tu osobinu. Pišemo $d = (a, b)$.
Najmanji zajednički sadržalac, s, brojeva a i b je takav broj da $a|s$ i $b|s$, a nijedan broj manji od s nema tu osobinu. Pišemo $s = [a, b]$.

- Ako je $d = (a, b)$ tada $1 = (\frac{a}{d}, \frac{b}{d})$.
- $(a, b)[a, b] = ab$.

Definicija

Kažemo da su prirodni brojevi a i b kongruentni po modulu m ako $m|a-b$. Zapisujemo $a \equiv_m b$.

- Neka je $a \equiv_m b$ i $c \equiv_m d$. Tada je i: $a \pm b \equiv_m c \pm d$, $ac \equiv_m bd$, $a^n \equiv_m b^n$.
- Ako je $a \equiv_{m_1} b$ i $a \equiv_{m_2} b$, tada je $a \equiv_{[m_1,m_2]} b$.
- Kada iz $ac \equiv_m bc$ smemo da zaključimo $a \equiv_m b$?
- Koliki ostatak daje broj 5^{2010} pri deljenju sa 13?
- Kriterijumi deljivosti.

Definicija

Kažemo da su prirodni brojevi a i b kongruentni po modulu m ako $m|a-b$. Zapisujemo $a \equiv_m b$.

- Neka je $a \equiv_m b$ i $c \equiv_m d$. Tada je i: $a \pm b \equiv_m c \pm d$, $ac \equiv_m bd$, $a^n \equiv_m b^n$.
- Ako je $a \equiv_{m_1} b$ i $a \equiv_{m_2} b$, tada je $a \equiv_{[m_1,m_2]} b$.
- Kada iz $ac \equiv_m bc$ smemo da zaključimo $a \equiv_m b$?
- Koliki ostatak daje broj 5^{2010} pri deljenju sa 13?
- Kriterijumi deljivosti.

Definicija

Kažemo da su prirodni brojevi a i b kongruentni po modulu m ako $m|a-b$. Zapisujemo $a \equiv_m b$.

- Neka je $a \equiv_m b$ i $c \equiv_m d$. Tada je i: $a \pm b \equiv_m c \pm d$, $ac \equiv_m bd$, $a^n \equiv_m b^n$.
- Ako je $a \equiv_{m_1} b$ i $a \equiv_{m_2} b$, tada je $a \equiv_{[m_1,m_2]} b$.
- Kada iz $ac \equiv_m bc$ smemo da zaključimo $a \equiv_m b$?
- Koliki ostatak daje broj 5^{2010} pri deljenju sa 13?
- Kriterijumi deljivosti.

Definicija

Kažemo da su prirodni brojevi a i b kongruentni po modulu m ako $m|a-b$. Zapisujemo $a \equiv_m b$.

- Neka je $a \equiv_m b$ i $c \equiv_m d$. Tada je i: $a \pm b \equiv_m c \pm d$, $ac \equiv_m bd$, $a^n \equiv_m b^n$.
- Ako je $a \equiv_{m_1} b$ i $a \equiv_{m_2} b$, tada je $a \equiv_{[m_1,m_2]} b$.
- Kada iz $ac \equiv_m bc$ smemo da zaključimo $a \equiv_m b$?
- Koliki ostatak daje broj 5^{2010} pri deljenju sa 13?
- Kriterijumi deljivosti.

Definicija

Kažemo da su prirodni brojevi a i b kongruentni po modulu m ako $m|a-b$. Zapisujemo $a \equiv_m b$.

- Neka je $a \equiv_m b$ i $c \equiv_m d$. Tada je i: $a \pm b \equiv_m c \pm d$, $ac \equiv_m bd$, $a^n \equiv_m b^n$.
- Ako je $a \equiv_{m_1} b$ i $a \equiv_{m_2} b$, tada je $a \equiv_{[m_1,m_2]} b$.
- Kada iz $ac \equiv_m bc$ smemo da zaključimo $a \equiv_m b$?
- Koliki ostatak daje broj 5^{2010} pri deljenju sa 13?
- Kriterijumi deljivosti.

Definicija

Kažemo da su prirodni brojevi a i b kongruentni po modulu m ako $m|a-b$. Zapisujemo $a \equiv_m b$.

- Neka je $a \equiv_m b$ i $c \equiv_m d$. Tada je i: $a \pm b \equiv_m c \pm d$, $ac \equiv_m bd$, $a^n \equiv_m b^n$.
- Ako je $a \equiv_{m_1} b$ i $a \equiv_{m_2} b$, tada je $a \equiv_{[m_1,m_2]} b$.
- Kada iz $ac \equiv_m bc$ smemo da zaključimo $a \equiv_m b$?
- Koliki ostatak daje broj 5^{2010} pri deljenju sa 13?
- Kriterijumi deljivosti.

Definicija

Neka je n prirodan broj veći od 1*. Ako skup A ispunjava sledeća dva svojstva:*
1^o *Svaka dva različita elementa iz A imaju različit ostatak pri deljenju sa m;*
2^o *Za svaki prirodan broj postoji element skupa A koji daje isti istatak pri deljenju sa m kao i taj broj,*
tada A nazivamo potpun sistem ostataka po modulu m.

Definicija

Ako iz potpunog sistema ostataka po modulu m izbacimo sve brojeve koji nisu uzajamno prosti sa m, dobijamo redukovan sistem ostataka po modulu m.

Definicija

Funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ *koja svakom broju n pridruži broj brojeva manjih od n koji su uzajamno prosti sa n, naziva se Ojlerova funkcija.*

Definicija

Neka je n prirodan broj veći od 1*. Ako skup A ispunjava sledeća dva svojstva:*
1^o *Svaka dva različita elementa iz A imaju različit ostatak pri deljenju sa m;*
2^o *Za svaki prirodan broj postoji element skupa A koji daje isti istatak pri deljenju sa m kao i taj broj,*
tada A nazivamo potpun sistem ostataka po modulu m.

Definicija

Ako iz potpunog sistema ostataka po modulu m izbacimo sve brojeve koji nisu uzajamno prosti sa m, dobijamo redukovan sistem ostataka po modulu m.

Definicija

Funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ *koja svakom broju n pridruži broj brojeva manjih od n koji su uzajamno prosti sa n, naziva se Ojlerova funkcija.*

Definicija

Neka je n prirodan broj veći od 1*. Ako skup A ispunjava sledeća dva svojstva:*
1^o *Svaka dva različita elementa iz A imaju različit ostatak pri deljenju sa m;*
2^o *Za svaki prirodan broj postoji element skupa A koji daje isti istatak pri deljenju sa m kao i taj broj,*
tada A nazivamo potpun sistem ostataka po modulu m.

Definicija

Ako iz potpunog sistema ostataka po modulu m izbacimo sve brojeve koji nisu uzajamno prosti sa m, dobijamo redukovan sistem ostataka po modulu m.

Definicija

Funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ *koja svakom broju n pridruži broj brojeva manjih od n koji su uzajamno prosti sa n, naziva se Ojlerova funkcija.*

Teorema

Neka su a i m prirodni brojevi za koje je $(a, m) = 1$. Tada je

$$a^{\varphi(m)} \equiv_m 1.$$

Dokazati da za svaka tri prirodna broja a, b i c važi:

$$abc = [a, b, c](ab, bc, ca).$$

Dokazati ili opovrgnuti tvrđenje: Za svaki prirodan broj n postoji neki broj koji je deljiv sa n i čiji je zbir cifara n.

Naći sve parove prirodnih brojeva (a, n) *tako da*

$$n|(a+1)^n - a^n.$$

Neka je n prirodan broj. Ako je broj $1 + 2^n + 4^n$ *prost, tada je n stepen trojke. Dokazati.*

Neka je a prirodan broj i neka je niz (x_n) definisan na sledeći način: $x_1 = a$ i

$$x_{n+1} = \begin{cases} \frac{x_n}{2}, & \text{ako je } x_n \text{ paran broj;} \\ \frac{3x_n+1}{2}, & \text{ako je } x_n \text{ neparan broj} \end{cases}$$

za svaki prirodan broj n. Dokazati da je bar jedan član tog niza paran broj.