Aritmetične funkcije

Marko Petkovšek

Fakulteta za matematiko in fiziko
Oddelek za matematiko

24. februar 2017

Oznaka

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Oznaka

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Definicija

Aritmetična funkcija je preslikava oblike

$$f : \mathbb{N} \to A, \quad A \subseteq \mathbb{C}.$$

Oznaka

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Definicija

Aritmetična funkcija je preslikava oblike

$$f : \mathbb{N} \to A, \quad A \subseteq \mathbb{C}.$$

Aritmetična funkcija f je multiplikativna, če za poljubni tuji števili $a, b \in \mathbb{N}$ velja:

$$f(ab) = f(a)f(b).$$

Zgledi aritmetičnih funkcij

1. $\tau(n) =$ *število pozitivnih deliteljev števila n*

Zgledi aritmetičnih funkcij

1. $\tau(n) =$ *število pozitivnih deliteljev števila n*
2. $\sigma(n) =$ *vsota pozitivnih deliteljev števila n*

Zgledi aritmetičnih funkcij

1. $\tau(n) =$ *število pozitivnih deliteljev števila* n
2. $\sigma(n) =$ *vsota pozitivnih deliteljev števila* n

Zgled

n	pozitivni delitelji n	$\tau(n)$	$\sigma(n)$
1	1	1	1
2	1, 2	2	3
3	1, 3	2	4
4	1, 2, 4	3	7
5	1, 5	2	6
6	1, 2, 3, 6	4	12

Zgledi aritmetičnih funkcij

1. $\tau(n) =$ *število pozitivnih deliteljev števila n*
2. $\sigma(n) =$ *vsota pozitivnih deliteljev števila n*

Zgled

n	pozitivni delitelji n	$\tau(n)$	$\sigma(n)$
1	1	1	1
2	$1, 2$	2	3
3	$1, 3$	2	4
4	$1, 2, 4$	3	7
5	$1, 5$	2	6
6	$1, 2, 3, 6$	4	12

Trditev

Funkciji τ in σ sta multiplikativni.

Eulerjeva funkcija

Eulerjeva funkcija

Definicija

Za vse $n \in \mathbb{N}$ s $\varphi(n)$ označimo število celih števil iz množice $\{1, 2, \ldots, n\}$, ki so tuja številu n. Preslikavo $\varphi : \mathbb{N} \to \mathbb{N}$ imenujemo Eulerjeva funkcija.

Eulerjeva funkcija

Definicija

Za vse $n \in \mathbb{N}$ s $\varphi(n)$ označimo število celih števil iz množice $\{1, 2, \ldots, n\}$, ki so tuja številu n. Preslikavo $\varphi : \mathbb{N} \to \mathbb{N}$ imenujemo Eulerjeva funkcija.

Zgled

n	$\{1, 2, \ldots, n\}$	$\varphi(n)$
1	$\{\mathbf{1}\}$	1
2	$\{\mathbf{1}, 2\}$	1
3	$\{\mathbf{1}, \mathbf{2}, 3\}$	2
4	$\{\mathbf{1}, 2, \mathbf{3}, 4\}$	2
5	$\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, 5\}$	4
6	$\{\mathbf{1}, 2, 3, 4, \mathbf{5}, 6\}$	2

Vprašanje: $\varphi(10^{10}) = \varphi(10000000000) = ?$

Vprašanje: $\varphi(10^{10}) = \varphi(10000000000) = \,?$

Trditev

Naj bo p praštevilo. Potem je $\varphi(p) =$

Vprašanje: $\varphi(10^{10}) = \varphi(10000000000) = \ ?$

Trditev

Naj bo p praštevilo. Potem je $\varphi(p) = p - 1$.

Vprašanje: $\varphi(10^{10}) = \varphi(10000000000) = ?$

Trditev

Naj bo p praštevilo. Potem je $\varphi(p) = p - 1$.

Trditev

Naj bo p praštevilo in $k \in \mathbb{N}$. *Potem je* $\varphi(p^k) =$

Vprašanje: $\varphi(10^{10}) = \varphi(10000000000) = ?$

Trditev

Naj bo p praštevilo. Potem je $\varphi(p) = p - 1$.

Trditev

Naj bo p praštevilo in $k \in \mathbb{N}$. *Potem je* $\varphi(p^k) = p^k - p^{k-1}$.

Vprašanje: $\varphi(10^{10}) = \varphi(10000000000) = \,?$

Trditev

Naj bo p praštevilo. Potem je $\varphi(p) = p - 1$.

Trditev

Naj bo p praštevilo in $k \in \mathbb{N}$. *Potem je* $\varphi(p^k) = p^k - p^{k-1}$.

Izrek

Če sta a in b tuji naravni števili, je $\varphi(ab) = \varphi(a)\varphi(b)$.

Posledica

$$\varphi(n) \;=\; n \times \prod_{p \,|\, n} \left(1 - \frac{1}{p}\right)$$

Posledica

$$\varphi(n) \; = \; n \times \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Izrek

$$\sum_{d \mid n} \varphi(d) \; =$$

Posledica

$$\varphi(n) \;=\; n \times \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Izrek

$$\sum_{d \mid n} \varphi(d) \;=\; n$$

Izrek (Eulerjev izrek)

Naj bosta $n \in \mathbb{N}$ in $a \in \mathbb{Z}$ tuji števili. Potem je

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Izrek (Eulerjev izrek)

Naj bosta $n \in \mathbb{N}$ *in* $a \in \mathbb{Z}$ *tuji števili. Potem je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Posledica (mali Fermatov izrek)

Naj bo p *praštevilo in* $a \in \mathbb{Z}$ *celo število, ki ni deljivo s* p*. Potem je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Möbiusova funkcija

Möbiusova funkcija

Definicija

Preslikavo $\mu : \mathbb{N} \to \mathbb{Z}$, *definirano s predpisom*

$$\mu(n) = \begin{cases} 0, & \textit{če } n \textit{ deljiv s kvadratom praštevila,} \\ (-1)^r, & \textit{sicer,} \end{cases}$$

kjer je r število različnih prafaktorjev števila n, imenujemo Möbiusova funkcija.

Definicija

Preslikavo $\mu : \mathbb{N} \to \mathbb{Z}$, *definirano s predpisom*

$$\mu(n) = \begin{cases} 0, & \textit{če } n \textit{ deljiv s kvadratom praštevila}, \\ (-1)^r, & \textit{sicer}, \end{cases}$$

kjer je r število različnih prafaktorjev števila n, imenujemo Möbiusova funkcija.

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Izrek

Če sta a in b tuji naravni števili, je $\mu(ab) = \mu(a)\mu(b)$.

Izrek

Če sta a in b tuji naravni števili, je $\mu(ab) = \mu(a)\mu(b)$.

Trditev

Za vse $n \in \mathbb{N}$ velja enačba

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases}$$

kjer d preteče vse pozitivne delitelje števila n.

Izrek

Če sta a in b tuji naravni števili, je $\mu(ab) = \mu(a)\mu(b)$.

Trditev

Za vse $n \in \mathbb{N}$ velja enačba

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases}$$

kjer d preteče vse pozitivne delitelje števila n.

Posledica

$$\mu(n) = \begin{cases} 1, & n = 1, \\ -\displaystyle\sum_{d \mid n,\, d<n} \mu(d), & n > 1. \end{cases}$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji* $f, g : \mathbb{N} \to \mathbb{C}$ *velja:*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji $f, g : \mathbb{N} \to \mathbb{C}$ velja:*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

Zgledi uporabe

$$\sum_{d \mid n} \varphi(d) = n \implies$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji* $f, g : \mathbb{N} \to \mathbb{C}$ *velja:*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

Zgledi uporabe

$$\sum_{d \mid n} \varphi(d) = n \implies \varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji* $f, g : \mathbb{N} \to \mathbb{C}$ *velja:*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

Zgledi uporabe

$$\sum_{d \mid n} \varphi(d) = n \implies \varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$$

$$\tau(n) = \sum_{d \mid n} 1 \implies$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji* $f, g : \mathbb{N} \to \mathbb{C}$ *velja:*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

Zgledi uporabe

$$\sum_{d \mid n} \varphi(d) = n \implies \varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$$

$$\tau(n) = \sum_{d \mid n} 1 \implies \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) = 1$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji* $f, g : \mathbb{N} \to \mathbb{C}$ *velja:*

$$g(n) = \sum_{d\,|\,n} f(d) \iff f(n) = \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) g(d)$$

Zgledi uporabe

$$\sum_{d\,|\,n} \varphi(d) = n \implies \varphi(n) = \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) d$$

$$\tau(n) = \sum_{d\,|\,n} 1 \implies \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) \tau(d) = 1$$

$$\sigma(n) = \sum_{d\,|\,n} d \implies$$

Izrek

(Möbiusov obrat) *Za aritmetični funkciji* $f, g : \mathbb{N} \to \mathbb{C}$ *velja:*

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$$

Zgledi uporabe

$$\sum_{d \mid n} \varphi(d) = n \implies \varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$$

$$\tau(n) = \sum_{d \mid n} 1 \implies \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) = 1$$

$$\sigma(n) = \sum_{d \mid n} d \implies \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma(d) = n$$