Aritmetické funkce

Jako „aritmetické" označujeme funkce $f : \mathbb{N} \to \mathbb{C}$.

Def. (Möbiova funkce): Möbiova funkce μ je dána předpisem:

1.) $\mu(1) = 1$

2.) $n > 1$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde p_i jsou navzájem různá prvočísla $\Rightarrow$

$\mu(n) = (-1)^k$ jestliže $\alpha_1 = \dots = \alpha_k = 1$

$\mu(n) = 0$ jestliže $\exists \alpha_i > 1$

Př.:

n	1	2	3	$4=2^2$	5	$6=2^1\cdot 3^1$	7	$8=2^3$	$10=2^1\cdot 5^1$	$30=2^1\cdot 3^1\cdot 5^1$
$\mu(n)$	1	-1	-1	0	-1	$(-1)^2$	-1	0	$(-1)^2$	$(-1)^3$

Př.: Určete: $\sum\limits_{d|6} \mu(d) = \underset{1}{\mu(1)} + \underset{-1}{\mu(2)} + \underset{-1}{\mu(3)} + \underset{1}{\mu(6)} = \underline{\underline{0}}$

UVAŽUJEME JEN $d>0$

$$\sum_{d|8} \mu(d) = \underset{1}{\mu(1)} + \underset{-1}{\mu(2)} + \underset{0}{\mu(4)} + \underset{0}{\mu(8)} = \underline{\underline{0}}$$

$$\sum_{d|12} \mu(d) = \underset{1}{\mu(1)} + \underset{-1}{\mu(2)} + \underset{-1}{\mu(3)} + \underset{0}{\mu(4)} + \underset{1}{\mu(6)} + \underset{0}{\mu(12)} = \underline{\underline{0}}$$

Věta: Pro každé $n \in \mathbb{N}$ platí $\sum\limits_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 0 & \text{pro } n>1 \\ 1 & \text{pro } n=1 \end{cases}$

Důkaz: Pro $n=1$ věta platí: $\sum\limits_{d|n} \mu(d) = \mu(1) = 1 = \left[\frac{1}{1}\right]$.

Pro $n>1$ předpokládejme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. V sumě $\sum\limits_{d|n} \mu(d)$ jsou nenulové členy $\mu(d)$ jen pro $d=1$, nebo $d = p_{i_1}^1 \cdots p_{i_j}^1$ $\Rightarrow$

$$\sum_{d|n} \mu(d) = \overset{1}{\mu(1)} + \underbrace{\overset{-1}{\mu(p_1)} + \dots + \overset{-1}{\mu(p_k)}}_{\text{vybíráme jedno z } k \text{ prvočísel}} + \underbrace{\overset{(-1)^2}{\mu(p_1 p_2)} + \dots \overset{(-1)^2}{\mu(p_{k-1} p_k)}}_{\text{vybíráme 2 z } k \text{ prvoč.}} + \dots + \underbrace{\overset{(-1)^k}{\mu(p_1 p_2 \cdots p_k)}}_{\text{vybíráme } k \text{ z } k \text{ prvočísel}} =$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \dots + \binom{k}{k}(-1)^k \underset{\text{binomická věta}}{=} (1-1)^k = 0$$

Def (Eulerova funkce): Eulerova funkce je pro každé $n \in \mathbb{N}$ dána předpisem: $\varphi(n) = \sum_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} 1$

Př:

n	1	2	3	4	5	6	7	8	...	p
$\varphi(n)$	1	1	2	2	4	2	6	4	...	$p-1$

Pro p... prvočíslo

Př: Určete

$$\sum_{d|6} \varphi(d) = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1+1+2+2 = \underline{\underline{6}}$$

$$\sum_{d|8} \varphi(d) = \varphi(1)+\varphi(2)+\varphi(4)+\varphi(8) = 1+1+2+4 = \underline{\underline{8}}$$

$$\sum_{d|12} \varphi(d) = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\overset{\overset{4}{\shortparallel}}{\varphi(12)} = 1+1+2+2+2+4 = \underline{\underline{12}}$$

Věta: Pro každé $n \in \mathbb{N}$ platí: $\sum_{d|n} \varphi(d) = n$.

Důkaz: Označme $S = \{1,2,\dots,n\}$. Každé číslo $k \in S$ jistě patří právě do jedné z množin:

$$\left.\begin{array}{l} A(1) = \{k \in S \mid \gcd(k,n)=1\} \\ \vdots \\ A(d) = \{k \in S \mid \gcd(k,n)=d\} \\ \vdots \\ A(n) = \{k \in S \mid \gcd(k,n)=n\} \end{array}\right\} \begin{array}{l} \text{Navzájem disjunktní.} \\ \text{Neprázdné pro } d \mid n \\ (\text{aby } \gcd(k,n)=d) \end{array} \Bigg\} \Rightarrow \bigcup_{d|n} A(d) = S \text{ a navíc}$$

$$\boxed{\sum_{d|n} |A(d)| = |S| = n} \quad (1)$$

Pro $A(d) = \{k \in S \mid \gcd(k,n)=d\}$ označme $B(d) = \{\frac{k}{d} \mid k \in A(d)\}$ a definujme:

$f: A(d) \to B(d)$ předpisem: $f(k) = \frac{k}{d}$ $\Rightarrow$ f je bijekce, neboť:

α) $f(k_1) = f(k_2) \Rightarrow \frac{k_1}{d} = \frac{k_2}{d} \Rightarrow k_1 = k_2 \Rightarrow f$ je injektivní

β) $\forall \frac{k}{d} \in B(d)\ \exists k \in A(d): f(k) = \frac{k}{d}$

Z (1) pak plyne, že $\boxed{\sum_{d|n} |A(d)| = \sum_{d|n} |B(d)| = n}$ (2)

Označme $X(d) = \{q \in \{1,\dots,\frac{n}{d}\} \mid \gcd(q,\frac{n}{d}) = 1\}$. Dokážeme, že $X(d) = B(d)$:

a) $\forall \frac{k}{d} \in B(d)$: $1 \le \frac{k}{d} \le \frac{n}{d}$ (protože $k \in A(d)$, $d|k \wedge k \le n$) navíc $k \in A(d) \Rightarrow \gcd(k,n) = d \Rightarrow$ $= \gcd(\frac{k}{d}, \frac{n}{d}) = 1 \Rightarrow \frac{k}{d} \in X(d)$

b) $\forall q \in X(d)$: $\gcd(q, \frac{n}{d}) = 1 \Rightarrow \gcd(qd, n) = d \Rightarrow q \cdot d = k \in A(d) \Rightarrow q = \frac{k}{d} \in B(d)$

$\Rightarrow$ Z (2) plyne: $n = \sum_{d|n} |B(d)| = \sum_{d|n} |X(d)| = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$

□

Př.: Označme $S = \{1, 2, \dots, 12\}$, $A(d) = \{k \in S \mid \gcd(k, 12) = d\}$; $B(d) = \{\frac{k}{d} \mid k \in A(d)\}$

a) Určete množiny:

$A(1) = \{1, 5, 7, 11\} \Rightarrow B(1) = \{\frac{1}{1}, \frac{5}{1}, \frac{7}{1}, \frac{11}{1}\} = \{1, 5, 7, 11\}$ $\quad \frac{12}{1} = 12$

$A(2) = \{2, 10\} \Rightarrow B(2) = \{\frac{2}{2}, \frac{10}{2}\} = \{1, 5\}$ $\quad \frac{12}{2} = 6$

$A(3) = \{3, 9\} \Rightarrow B(3) = \{1, 3\}$ $\quad \frac{12}{3} = 4$

$A(4) = \{4, 8\} \Rightarrow B(4) = \{1, 2\}$ $\quad \frac{12}{4} = 3$

$A(6) = \{6\} \Rightarrow B(6) = \{1\}$ $\quad \frac{12}{6} = 2$

$A(12) = \{12\} \Rightarrow B(12) = \{1\}$ $\quad \frac{12}{12} = 1$

b) Všimněme si:

1.) $A(5) = A(7) = A(8) = A(9) = A(10) = A(11) = \emptyset$

2.) Počet prvků z $A(d)$ je stejný jako počet prvků z $B(d)$.
Prvku $k \in A(d)$ můžeme přiřadit prvek $\frac{k}{d} \in B(d)$

$\Rightarrow \sum_{d|12} |A(d)| = \sum_{d|12} |B(d)|$

3.) Množiny $A(d)$ jsou disjunktní a $\bigcup A(d) = \{1, 2, \dots, 12\} = S$ $\Rightarrow$

$\Rightarrow \sum_{d|12} |A(d)| = |S| = 12$

4.) Z bodu 2.) a 3.) plyne, že $\sum_{d|12} |B(d)| = 12$.

5.) Prvky z množiny $B(d)$ jsou všechna čísla z intervalu $\langle 1, \frac{12}{d} \rangle$ nesoudělná s $\frac{12}{d}$. $\Rightarrow$ $|B(d)| = \varphi(\frac{12}{d})$.

6.) Z 4.) a 5.) plyne, že $\sum_{d|n} \varphi(\frac{12}{d}) = 12$

7.) $D = \{d \in \mathbb{N} \mid d|12\} = \{1, 2, 3, 4, 6, 12\}$
$D^* = \{\frac{12}{d} \mid d \in D\} = \{\frac{12}{1}, \frac{12}{2}, \frac{12}{3}, \frac{12}{4}, \frac{12}{6}, \frac{12}{12}\} = \{12, 6, 4, 3, 2, 1\}$ $\Big\} \Rightarrow D = D^*$

8.) Z 6.) a 7.) plyne: $12 = \sum_{d|n} \varphi(\underbrace{\frac{12}{d}}_{\text{,,}d\text{"}}) = \sum_{d \in D^*} \varphi(d) = \sum_{d \in D} \varphi(d) = \sum_{d|n} \varphi(d) = 12$

Př.: Určete $\displaystyle\sum_{k=1}^{n}\sum_{\substack{d|k\\ d|n}} \mu(d)$ pro $n = 6$.

$$\sum_{k=1}^{6}\sum_{\substack{d|k\\ d|6}} \mu(d) = \sum_{\substack{d|1\\ d|6}} \mu(d) + \sum_{\substack{d|2\\ d|6}} \mu(d) + \sum_{\substack{d|3\\ d|6}} \mu(d) + \sum_{\substack{d|4\\ d|6}} \mu(d) + \sum_{\substack{d|5\\ d|6}} \mu(d) + \sum_{\substack{d|6\\ d|6}} \mu(d) =$$

$$
\begin{array}{llllll}
= \mu(1) & + & & & & (k=1)\\
+ \mu(1) + \mu(2) & + & & & & (k=2)\\
+ \mu(1) & & + \mu(3) & + & & (k=3)\\
+ \mu(1) + \mu(2) & + & & & & (k=4)\\
+ \mu(1) & & & & & \\
+ \mu(1) + \mu(2) & + \mu(3) & + \mu(6) & & = ? &
\end{array}
$$

$\mu(1)$ se vyskytlo tam, kde $1 \mid k$; $\mu(2)$ se vyskytlo tam, kde $2 \mid k$; …
$\mu(d)$ se vyskytne tam, kde $d \mid k$ $\Rightarrow$ $\mu(d)$ se vyskytne tam, kde k je násobek d $\Rightarrow$ $k = d, 2d, \dots, \left(\frac{n}{d}\right)d = \left(\frac{6}{d}\right)\cdot d$ $\Rightarrow$

$\Rightarrow$ $\mu(d)$ se v součtu objeví celkem $\left(\frac{n}{d}\right) = \frac{6}{d}$ krát.

d musí navíc splňovat $d \mid 6$ $\Rightarrow$

$$\sum_{k=1}^{n}\sum_{\substack{d|k\\ d|n}} \mu(d) = \sum_{k=1}^{6}\sum_{\substack{d|k\\ d|6}} \mu(d) = \sum_{d|6} \frac{6}{d}\cdot \mu(d) = \sum_{d|n} \frac{n}{d}\, \mu(d)$$

Věta: Pro každé $n \in \mathbb{N}$ platí:

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

Důkaz: Uvažme, že $\forall n \in \mathbb{N}$ platí:

$$\left[\frac{1}{\gcd(n,k)}\right] = \begin{cases} 1 & \text{pokud } \gcd(n,k) = 1 \\ 0 & \text{pokud } \gcd(n,k) = d > 1 \end{cases}$$

Proto:

$$\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{\gcd(k,n)}\right] \qquad \Big/ \quad \left[\frac{1}{n}\right] = \sum_{d \mid n} \mu(d) \quad \Rightarrow \quad \left[\frac{1}{(k,n)}\right] = \sum_{d \mid (k,n)} \mu(d)$$

$$\varphi(n) = \sum_{k=1}^{n} \underbrace{\sum_{d \mid (k,n)}}_{} \mu(d)$$

suma přes všechny d dělící $\gcd(k,n)$ → to jsou ale všichni společní dělitelé k a n =>

$$\varphi(n) = \sum_{k=1}^{n} \sum_{\substack{d \mid k \\ d \mid n}} \mu(d)$$

Uvažujme pevné d. Sčítáme přes ta d, která dělí k => (~~nenulové~~) členy součtu dostaneme jen pokud k je násobkem d. Tzn $1 \leq k = q \cdot d \leq n$

$$\Updownarrow$$

$$1 \leq q = \frac{k}{d} \leq \frac{n}{d} \quad \Rightarrow$$

$$\varphi(n) = \sum_{d \mid n} \sum_{q=1}^{\frac{n}{d}} \mu(d) = \sum_{d \mid n} \frac{n}{d} \mu(d)$$

$\square$

Př: 1) $\varphi(6) = \sum_{d \mid 6} \mu(d) \frac{6}{d} = \underset{\overset{\shortparallel}{1}}{\mu(1)} \frac{6}{1} + \underset{\overset{\shortparallel}{-1}}{\mu(2)} \frac{6}{2} + \underset{\overset{\shortparallel}{-1}}{\mu(3)} \frac{6}{3} + \underset{\overset{\shortparallel}{1}}{\mu(6)} \frac{6}{6} =$

$= 6 - 3 - 2 + 1 = \underline{\underline{2}}$ ✓

2.) $\varphi(15) = \sum_{d \mid 15} \mu(d) \frac{15}{d} = \mu(1)\, \cancel{m}(15) + \mu(3) \cdot 5 + \mu(5) \cdot 3 + \mu(15) \cdot 1 =$

$= 1 \cdot 15 + (-1) \cdot 5 + (-1) \cdot 3 + (-1)^2 \cdot 1 =$

$= 15 - 5 - 3 + 1 = \underline{\underline{8}}$

Věta: Pro každé $n \in \mathbb{N}$ platí:

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

Důkaz: Pro $n=1$ je součin prázdný. V takovém případě považujeme jeho hodnotu rovnu 1. $\varphi(1)=1$ je tedy splněno.

Uvažujme $n>1$. Označme $p_1, \dots, p_r$ prvočíselné dělitele čísla n. Potom

$$\prod_{p \mid n}\left(1-\frac{1}{p}\right) = \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = 1 - \sum_{i=1}^{r}\frac{1}{p_i} + \sum \frac{1}{p_i p_j} \overset{\mu(d)}{-} \sum \underbrace{\frac{1}{p_i p_j p_k}}_{d} + \dots + \sum \frac{(-1)^{r-1}}{p_{i_1} \cdots p_{i_{r-1}}} + \frac{(-1)^r}{p_1 \cdots p_r}$$

ve jmenovatelích se vyskytnou všichni dělitelé čísla n, jejichž $\mu(d) \neq 0$

$$= \sum_{d \mid n} \frac{\mu(d)}{d}$$

$$\Rightarrow \quad n \prod_{p \mid n}\left(1-\frac{1}{p}\right) = n \sum_{d \mid n} \frac{\mu(d)}{d} = \sum_{d \mid n} \mu(d) \frac{n}{d} = \varphi(n)$$

podle předchozí věty

$\square$

Př: $n = 3 \cdot 5 \cdot 7 = 105 \Rightarrow$

$$\varphi(105) = 105 \left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 3 \cdot 5 \cdot 7 \left(\frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{5}\right) = \underline{\underline{48}}$$

Pozn: Pokud známe kanonický rozklad čísla n, je snadné najít $\varphi(n)$. V případě, kdy n je „velké" a kanonický rozklad neznáme, je to „velký" problém.

Věta: Eulerova funkce φ splňuje:

1.) $\forall \alpha \in \mathbb{N}\ \forall p \in \mathbb{P}$: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

2.) $\forall\, m, n \in \mathbb{N}$: $\varphi(m \cdot n) = \dfrac{\varphi(m)\,\varphi(n)}{\varphi(d)} \cdot d$, kde $d = \gcd(m,n)$

3.) Jestliže $\gcd(m,n) = 1$, pak $\varphi(m \cdot n) = \varphi(m)\,\varphi(n)$ $\Rightarrow$ φ je multiplikativní funkce

4.) Jestliže $a \mid b$, pak $\varphi(a) \mid \varphi(b)$

5.) $\forall\, n \in \mathbb{N},\ n \geq 3$: $\varphi(n)$ je sudé a jestliže n má r různých prvočíselných lichých dělitelů, pak $2^r \mid \varphi(n)$

<u>Důkaz:</u> 1.) $\varphi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right) = p^\alpha - p^{\alpha-1}$

jinak: $\underbrace{1, 2, \dots, p, \dots, 2p, \dots, 3p, \dots\dots, p^{\alpha-1} \cdot p}_{\text{soudělné s } p^\alpha \text{ jsou jen násobky } k \cdot p} = p^\alpha$ $\Rightarrow k = 1, 2, \dots, p^{\alpha-1}$

$\Rightarrow \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

2.)
$$\frac{\varphi(m \cdot n)}{m \cdot n} = \prod_{p \mid m \cdot n} \left(1 - \frac{1}{p}\right) = \frac{\prod_{p \mid m}\left(1 - \frac{1}{p}\right) \prod_{p \mid n}\left(1 - \frac{1}{p}\right)}{\prod_{\substack{p \mid m \\ \wedge \\ p \mid n}} \left(1 - \frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}}$$

$p \mid d$

3.) Plyne okamžitě z 2.), protože $d = 1$, $\varphi(d) = 1$

4.)
$$\varphi(b) = b \prod_{\substack{p \mid b \\ b = k_1 \cdot a}} \left(1 - \frac{1}{p}\right) = k_1 \cdot a \cdot k_2 \prod_{p \mid a} \left(1 - \frac{1}{p}\right) = k \cdot \underbrace{a \prod_{p \mid a} \left(1 - \frac{1}{p}\right)}_{\varphi(a)}$$

5.) $n \in \mathbb{N},\ n \geq 3 \Rightarrow$ a) n je sudé $\Rightarrow$ $\varphi(n) = n \cdot \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$ je sudé

b) n je liché $\Rightarrow$ má lichého prvoč. dělitele p $\Rightarrow n\left(1 - \frac{1}{p}\right) = k \cdot p \left(1 - \frac{1}{p}\right) = k(\underbrace{p-1}_{\text{sudé}})$

Jestliže $p_1, \dots, p_r$ jsou liší dělitelé (prvočíselní) čísla n $\Rightarrow \varphi(n) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right) = k \cdot \underbrace{(p_1 - 1)}_{= 2k_1} \underbrace{(p_2 - 1)}_{= 2k_2} \cdots \underbrace{(p_r - 1)}_{= 2k_r}$

$\blacksquare$