

# Möbiova inverzní formule

Petr Vodstrčil

`petr.vodstrcil@vsb.cz`

Katedra aplikované matematiky, Fakulta elektrotechniky a informatiky,  
Vysoká škola báňská–Technická univerzita Ostrava



20.6.–22.6. 2018

(Výjezdní zasedání KAM, Bořetice)

# Formulace problému

Uvažujme posloupnost  $\{a(n)\}_{n=1}^{\infty}$  a definujme posloupnost  $\{b(n)\}_{n=1}^{\infty}$  jejich „částečných součtů“ předpisem

$$b(n) \stackrel{\text{def}}{=} \sum_{d|n} a(d).$$

# Formulace problému

Uvažujme posloupnost  $\{a(n)\}_{n=1}^{\infty}$  a definujme posloupnost  $\{b(n)\}_{n=1}^{\infty}$  jejich „částečných součtů“ předpisem

$$b(n) \stackrel{\text{def}}{=} \sum_{d|n} a(d).$$

Ve výše uvedené sumě sčítáme přes všechny kladné dělitele čísla  $n$ .

# Formulace problému

Uvažujme posloupnost  $\{a(n)\}_{n=1}^{\infty}$  a definujme posloupnost  $\{b(n)\}_{n=1}^{\infty}$  jejich „částečných součtů“ předpisem

$$b(n) \stackrel{\text{def}}{=} \sum_{d|n} a(d).$$

Ve výše uvedené sumě sčítáme přes všechny kladné dělitele čísla  $n$ .

Například

$$b(20) = a(1) + a(2) + a(4) + a(5) + a(10) + a(20).$$

# Formulace problému

Uvažujme posloupnost  $\{a(n)\}_{n=1}^{\infty}$  a definujme posloupnost  $\{b(n)\}_{n=1}^{\infty}$  jejich „částečných součtů“ předpisem

$$b(n) \stackrel{\text{def}}{=} \sum_{d|n} a(d).$$

Ve výše uvedené sumě sčítáme přes všechny kladné dělitele čísla  $n$ .

Například

$$b(20) = a(1) + a(2) + a(4) + a(5) + a(10) + a(20).$$

## Problém.

Pro každé  $n \in \mathbb{N}$  bychom chtěli zpětně vyjádřit  $a(n)$  pomocí čísel  $b(1), b(2), \dots$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$



$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$a(5) = b(5) - b(1),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

⇒

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$a(5) = b(5) - b(1),$$

$$a(6) = b(6) - b(3) - b(2) + b(1),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$a(5) = b(5) - b(1),$$

$$a(6) = b(6) - b(3) - b(2) + b(1),$$

$$a(7) = b(7) - b(1),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$a(5) = b(5) - b(1),$$

$$a(6) = b(6) - b(3) - b(2) + b(1),$$

$$a(7) = b(7) - b(1),$$

$$a(8) = b(8) - b(4),$$

$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

⋮

$\implies$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$a(5) = b(5) - b(1),$$

$$a(6) = b(6) - b(3) - b(2) + b(1),$$

$$a(7) = b(7) - b(1),$$

$$a(8) = b(8) - b(4),$$

$$a(9) = b(9) - b(3),$$

$$\begin{aligned}
b(1) &= a(1), \\
b(2) &= a(1) + a(2), \\
b(3) &= a(1) + a(3), \\
b(4) &= a(1) + a(2) + a(4), \\
b(5) &= a(1) + a(5), \\
b(6) &= a(1) + a(2) + a(3) + a(6), \\
b(7) &= a(1) + a(7), \\
b(8) &= a(1) + a(2) + a(4) + a(8), \\
b(9) &= a(1) + a(3) + a(9), \\
b(10) &= a(1) + a(2) + a(5) + a(10), \\
&\vdots
\end{aligned}$$

 $\implies$ 

$$\begin{aligned}
a(1) &= b(1), \\
a(2) &= b(2) - b(1), \\
a(3) &= b(3) - b(1), \\
a(4) &= b(4) - b(2), \\
a(5) &= b(5) - b(1), \\
a(6) &= b(6) - b(3) - b(2) + b(1), \\
a(7) &= b(7) - b(1), \\
a(8) &= b(8) - b(4), \\
a(9) &= b(9) - b(3), \\
a(10) &= b(10) - b(5) - b(2) + b(1), \\
&\vdots
\end{aligned}$$



$$b(1) = a(1),$$

$$b(2) = a(1) + a(2),$$

$$b(3) = a(1) + a(3),$$

$$b(4) = a(1) + a(2) + a(4),$$

$$b(5) = a(1) + a(5),$$

$$b(6) = a(1) + a(2) + a(3) + a(6),$$

$$b(7) = a(1) + a(7),$$

$$b(8) = a(1) + a(2) + a(4) + a(8),$$

$$b(9) = a(1) + a(3) + a(9),$$

$$b(10) = a(1) + a(2) + a(5) + a(10),$$

$$\vdots$$
$$\implies$$

$$a(1) = b(1),$$

$$a(2) = b(2) - b(1),$$

$$a(3) = b(3) - b(1),$$

$$a(4) = b(4) - b(2),$$

$$a(5) = b(5) - b(1),$$

$$a(6) = b(6) - b(3) - b(2) + b(1),$$

$$a(7) = b(7) - b(1),$$

$$a(8) = b(8) - b(4),$$

$$a(9) = b(9) - b(3),$$

$$a(10) = b(10) - b(5) - b(2) + b(1),$$

$$\vdots$$

$$a(1500) =$$

$$\begin{aligned}
b(1) &= a(1), \\
b(2) &= a(1) + a(2), \\
b(3) &= a(1) + a(3), \\
b(4) &= a(1) + a(2) + a(4), \\
b(5) &= a(1) + a(5), \\
b(6) &= a(1) + a(2) + a(3) + a(6), \\
b(7) &= a(1) + a(7), \\
b(8) &= a(1) + a(2) + a(4) + a(8), \\
b(9) &= a(1) + a(3) + a(9), \\
b(10) &= a(1) + a(2) + a(5) + a(10), \\
&\vdots
\end{aligned}$$

 $\implies$ 

$$\begin{aligned}
a(1) &= b(1), \\
a(2) &= b(2) - b(1), \\
a(3) &= b(3) - b(1), \\
a(4) &= b(4) - b(2), \\
a(5) &= b(5) - b(1), \\
a(6) &= b(6) - b(3) - b(2) + b(1), \\
a(7) &= b(7) - b(1), \\
a(8) &= b(8) - b(4), \\
a(9) &= b(9) - b(3), \\
a(10) &= b(10) - b(5) - b(2) + b(1), \\
&\vdots
\end{aligned}$$

$$a(1500) = b(1500) - b(750) - b(500) - b(300) + b(250) + b(150) + b(100) - b(50).$$

## Definice.

Pro dvě posloupnosti  $u = \{u(n)\}_{n=1}^{\infty}$  a  $v = \{v(n)\}_{n=1}^{\infty}$  bude symbol  $u \star v$  (Dirichletův součin) představovat posloupnost

$$(u \star v)(n) \stackrel{\text{def}}{=} \sum_{d|n} u\left(\frac{n}{d}\right)v(d)$$

## Definice.

Pro dvě posloupnosti  $u = \{u(n)\}_{n=1}^{\infty}$  a  $v = \{v(n)\}_{n=1}^{\infty}$  bude symbol  $u \star v$  (Dirichletův součin) představovat posloupnost

$$(u \star v)(n) \stackrel{\text{def}}{=} \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right)$$

## Definice.

Pro dvě posloupnosti  $u = \{u(n)\}_{n=1}^{\infty}$  a  $v = \{v(n)\}_{n=1}^{\infty}$  bude symbol  $u \star v$  (Dirichletův součin) představovat posloupnost

$$(u \star v)(n) \stackrel{\text{def}}{=} \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2).$$

## Definice.

Pro dvě posloupnosti  $u = \{u(n)\}_{n=1}^{\infty}$  a  $v = \{v(n)\}_{n=1}^{\infty}$  bude symbol  $u \star v$  (Dirichletův součin) představovat posloupnost

$$(u \star v)(n) \stackrel{\text{def}}{=} \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2).$$

## Poznámka.

Operace  $\star$  je zřejmě komutativní (rovnost  $\sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right)$ ) a není obtížné ukázat i její asociativitu

## Definice.

Pro dvě posloupnosti  $u = \{u(n)\}_{n=1}^{\infty}$  a  $v = \{v(n)\}_{n=1}^{\infty}$  bude symbol  $u \star v$  (Dirichletův součin) představovat posloupnost

$$(u \star v)(n) \stackrel{\text{def}}{=} \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2).$$

## Poznámka.

Operace  $\star$  je zřejmě komutativní (rovnost  $\sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right)$ ) a není obtížné ukázat i její asociativitu, neboť

$$\begin{aligned} [(u \star v) \star w](n) &= \sum_{d_0 d_3 = n} (u \star v)(d_0)w(d_3) = \sum_{d_0 d_3 = n} \left[ \left( \sum_{d_1 d_2 = d_0} u(d_1)v(d_2) \right) w(d_3) \right] = \\ &= \sum_{d_0 d_3 = n} \left[ \sum_{d_1 d_2 = d_0} u(d_1)v(d_2)w(d_3) \right] = \sum_{d_1 d_2 d_3 = n} u(d_1)v(d_2)w(d_3) \end{aligned}$$

## Definice.

Pro dvě posloupnosti  $u = \{u(n)\}_{n=1}^{\infty}$  a  $v = \{v(n)\}_{n=1}^{\infty}$  bude symbol  $u \star v$  (Dirichletův součin) představovat posloupnost

$$(u \star v)(n) \stackrel{\text{def}}{=} \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2).$$

## Poznámka.

Operace  $\star$  je zřejmě komutativní (rovnost  $\sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right)$ ) a není obtížné ukázat i její asociativitu, neboť

$$\begin{aligned} [(u \star v) \star w](n) &= \sum_{d_0 d_3 = n} (u \star v)(d_0)w(d_3) = \sum_{d_0 d_3 = n} \left[ \left( \sum_{d_1 d_2 = d_0} u(d_1)v(d_2) \right) w(d_3) \right] = \\ &= \sum_{d_0 d_3 = n} \left[ \sum_{d_1 d_2 = d_0} u(d_1)v(d_2)w(d_3) \right] = \sum_{d_1 d_2 d_3 = n} u(d_1)v(d_2)w(d_3) = \dots = [u \star (v \star w)](n). \end{aligned}$$



$$(u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2)$$

## Příklad.

Nechť  $\mathbf{1}$  představuje posloupnost samých jedniček, tj  $\mathbf{1}(n) = 1$  pro každé  $n \in \mathbb{N}$ .  
Pak  $(\mathbf{1} \star \mathbf{1})(n)$  je

$$(u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2)$$

## Příklad.

Nechť  $\mathbf{1}$  představuje posloupnost samých jedniček, tj  $\mathbf{1}(n) = 1$  pro každé  $n \in \mathbb{N}$ . Pak  $(\mathbf{1} \star \mathbf{1})(n)$  je počet všech kladných dělitelů čísla  $n$ .

$$(u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2)$$

## Příklad.

Nechť  $\mathbf{1}$  představuje posloupnost samých jedniček, tj  $\mathbf{1}(n) = 1$  pro každé  $n \in \mathbb{N}$ . Pak  $(\mathbf{1} \star \mathbf{1})(n)$  je počet všech kladných dělitelů čísla  $n$ .

## Poznámka.

Neutrálním prvkem operace  $\star$  je posloupnost  $e = (1, 0, 0, 0, 0, 0, \dots)$ , neboť pro každou posloupnost  $u$  platí  $u \star e = u$ .

$$(u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) = \sum_{d|n} u(d)v\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} u(d_1)v(d_2)$$

## Příklad.

Nechť  $\mathbf{1}$  představuje posloupnost samých jedniček, tj  $\mathbf{1}(n) = 1$  pro každé  $n \in \mathbb{N}$ . Pak  $(\mathbf{1} \star \mathbf{1})(n)$  je počet všech kladných dělitelů čísla  $n$ .

## Poznámka.

Neutrálním prvkem operace  $\star$  je posloupnost  $e = (1, 0, 0, 0, 0, 0, \dots)$ , neboť pro každou posloupnost  $u$  platí  $u \star e = u$ .

## Poznámka.

Uvědomme si, že vztah mezi posloupností  $a = \{a(n)\}_{n=1}^{\infty}$  a posloupností jejich „částečných součtů“  $b = \{b(n)\}_{n=1}^{\infty} = \left\{ \sum_{d|n} a(d) \right\}_{n=1}^{\infty}$  lze zapsat pomocí operace  $\star$  jako

$$b = a \star \mathbf{1}.$$

## Definice.

Möbiovou funkcí  $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$  rozumíme funkci definovanou následovně:

- $\mu(1) \stackrel{\text{def}}{=} 1,$

## Definice.

Möbiovou funkcí  $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$  rozumíme funkci definovanou následovně:

- $\mu(1) \stackrel{\text{def}}{=} 1$ ,
- pro  $n \in \mathbb{N}$ ,  $n \geq 2$ , uvažujme rozklad čísla  $n$  na prvočinitele, tzn.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , kde  $p_1, p_2, \dots, p_k$  jsou vzájemně různá prvočísla a  $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$ , a definujme

$$\mu(n) \stackrel{\text{def}}{=} \begin{cases} (-1)^k, & \text{je-li } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1, \\ 0, & \text{existuje-li } i \in \{1, 2, \dots, k\} \text{ takové, že } \alpha_i > 1. \end{cases}$$

## Definice.

Möbiovou funkcí  $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$  rozumíme funkci definovanou následovně:

- $\mu(1) \stackrel{\text{def}}{=} 1$ ,
- pro  $n \in \mathbb{N}$ ,  $n \geq 2$ , uvažujme rozklad čísla  $n$  na prvočinitele, tzn.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , kde  $p_1, p_2, \dots, p_k$  jsou vzájemně různá prvočísla a  $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$ , a definujme

$$\mu(n) \stackrel{\text{def}}{=} \begin{cases} (-1)^k, & \text{je-li } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1, \\ 0, & \text{existuje-li } i \in \{1, 2, \dots, k\} \text{ takové, že } \alpha_i > 1. \end{cases}$$

## Příklad.

$$\mu(10) = \mu(2 \cdot 5) = (-1)^2 = 1,$$

## Definice.

Möbiovou funkcí  $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$  rozumíme funkci definovanou následovně:

- $\mu(1) \stackrel{\text{def}}{=} 1$ ,
- pro  $n \in \mathbb{N}$ ,  $n \geq 2$ , uvažujme rozklad čísla  $n$  na prvočinitele, tzn.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , kde  $p_1, p_2, \dots, p_k$  jsou vzájemně různá prvočísla a  $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$ , a definujme

$$\mu(n) \stackrel{\text{def}}{=} \begin{cases} (-1)^k, & \text{je-li } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1, \\ 0, & \text{existuje-li } i \in \{1, 2, \dots, k\} \text{ takové, že } \alpha_i > 1. \end{cases}$$

## Příklad.

$$\mu(10) = \mu(2 \cdot 5) = (-1)^2 = 1, \quad \mu(20) = \mu(2^2 \cdot 5) = 0,$$



## Definice.

Möbiovou funkcí  $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$  rozumíme funkci definovanou následovně:

- $\mu(1) \stackrel{\text{def}}{=} 1$ ,
- pro  $n \in \mathbb{N}$ ,  $n \geq 2$ , uvažujme rozklad čísla  $n$  na prvočinitele, tzn.  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , kde  $p_1, p_2, \dots, p_k$  jsou vzájemně různá prvočísla a  $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$ , a definujme

$$\mu(n) \stackrel{\text{def}}{=} \begin{cases} (-1)^k, & \text{je-li } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1, \\ 0, & \text{existuje-li } i \in \{1, 2, \dots, k\} \text{ takové, že } \alpha_i > 1. \end{cases}$$

## Příklad.

$$\mu(10) = \mu(2 \cdot 5) = (-1)^2 = 1, \quad \mu(20) = \mu(2^2 \cdot 5) = 0,$$

$$\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1.$$

Nyní dokážeme jednu důležitou vlastnost Möbiovy funkce  $\mu$ .

**Lemma.**

*Platí  $\mathbf{1} \star \mu = \mathbf{e}$ ,*

Nyní dokážeme jednu důležitou vlastnost Möbiovy funkce  $\mu$ .

## Lemma.

Platí  $\mathbf{1} \star \mu = \mathbf{e}$ , tzn.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{pro } n = 1, \\ 0, & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

Nyní dokážeme jednu důležitou vlastnost Möbiovy funkce  $\mu$ .

## Lemma.

Platí  $\mathbf{1} \star \mu = \mathbf{e}$ , tzn.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{pro } n = 1, \\ 0, & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

## Důkaz.

Případ  $n = 1$  je triviální, neboť  $\mu(1) = 1$ .

Nyní dokážeme jednu důležitou vlastnost Möbiovy funkce  $\mu$ .

## Lemma.

Platí  $\mathbf{1} \star \mu = \mathbf{e}$ , tzn.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{pro } n = 1, \\ 0, & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

## Důkaz.

Případ  $n = 1$  je triviální, neboť  $\mu(1) = 1$ .

Předpokládejme, že  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  (rozklad na prvočinitele).  
Z definice Möbiovy funkce

$$\sum_{d|n} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} - \dots + (-1)^k \binom{k}{k}$$

Nyní dokážeme jednu důležitou vlastnost Möbiovy funkce  $\mu$ .

## Lemma.

Platí  $\mathbf{1} \star \mu = e$ , tzn.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{pro } n = 1, \\ 0, & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

## Důkaz.

Případ  $n = 1$  je triviální, neboť  $\mu(1) = 1$ .

Předpokládejme, že  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  (rozklad na prvočinitele). Z definice Möbiovy funkce a z binomické věty pak dostaneme

$$\sum_{d|n} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} - \dots + (-1)^k \binom{k}{k} = (1 - 1)^k = 0,$$

což jsme chtěli dokázat. □

Věta.

*Nechť  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  jsou dvě posloupnosti splňující vztah*

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d).$$

Věta.

*Nechť  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  jsou dvě posloupnosti splňující vztah*

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d).$$

*Pak platí*

$$(\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d).$$



## Věta.

Nechť  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  jsou dvě posloupnosti splňující vztah

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d).$$

Pak platí

$$(\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right)\mu(d).$$

## Poznámka.

Například platí, že

$$a(12) = b(12)\mu(1) + b(6)\mu(2) + b(4)\mu(3) + b(3)\mu(4) + b(2)\mu(6) + b(1)\mu(12)$$

## Věta.

Nechť  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  jsou dvě posloupnosti splňující vztah

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d).$$

Pak platí

$$(\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d).$$

## Poznámka.

Například platí, že

$$\begin{aligned} a(12) &= b(12)\mu(1) + b(6)\mu(2) + b(4)\mu(3) + b(3)\mu(4) + b(2)\mu(6) + b(1)\mu(12) = \\ &= b(12) \cdot 1 + b(6) \cdot (-1) + b(4) \cdot (-1) + b(3) \cdot 0 + b(2) \cdot 1 + b(1) \cdot 0 \end{aligned}$$

## Věta.

Nechť  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  jsou dvě posloupnosti splňující vztah

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d).$$

Pak platí

$$(\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d).$$

## Poznámka.

Například platí, že

$$\begin{aligned} a(12) &= b(12)\mu(1) + b(6)\mu(2) + b(4)\mu(3) + b(3)\mu(4) + b(2)\mu(6) + b(1)\mu(12) = \\ &= b(12) \cdot 1 + b(6) \cdot (-1) + b(4) \cdot (-1) + b(3) \cdot 0 + b(2) \cdot 1 + b(1) \cdot 0 = \\ &= b(12) - b(6) - b(4) + b(2). \end{aligned}$$

$$\left[ (\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d) \right] \implies \left[ (\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) \right].$$

$$\left[ (\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d) \right] \implies \left[ (\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) \right].$$

## Důkaz.

Předpoklad

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d)$$

znamená, že  $b = a \star \mathbf{1}$ .

$$\left[ (\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d) \right] \implies \left[ (\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) \right].$$

## Důkaz.

Předpoklad

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d)$$

znamená, že  $b = a \star \mathbf{1}$ . Pak je ale jasné, že

$$b \star \mu = (a \star \mathbf{1}) \star \mu = a \star (\mathbf{1} \star \mu) = a \star e = a.$$



$$\left[ (\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d) \right] \implies \left[ (\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) \right].$$

## Důkaz.

Předpoklad

$$(\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d)$$

znamená, že  $b = a \star \mathbf{1}$ . Pak je ale jasné, že

$$b \star \mu = (a \star \mathbf{1}) \star \mu = a \star (\mathbf{1} \star \mu) = a \star e = a.$$



## Poznámka.

Ve skutečnosti platí i opačná implikace, neboť

$$a = b \star \mu \implies a \star \mathbf{1} = (b \star \mu) \star \mathbf{1} = b \star (\mu \star \mathbf{1}) = b \star e = b.$$

## Definice.

Eulerovu funkci  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definujeme předpisem

$$\varphi(n) \stackrel{\text{def}}{=} |\{k \in \mathbb{N} : k \leq n \wedge \text{nsd}(k, n) = 1\}|.$$



## Definice.

Eulerovu funkci  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definujeme předpisem

$$\varphi(n) \stackrel{\text{def}}{=} |\{k \in \mathbb{N} : k \leq n \wedge \text{nsd}(k, n) = 1\}|.$$

Pro  $n \in \mathbb{N}$  tedy  $\varphi(n)$  představuje počet čísel z množiny  $\{1, \dots, n\}$ , která jsou s číslem  $n$  nesoudělná.

## Definice.

Eulerovu funkci  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definujeme předpisem

$$\varphi(n) \stackrel{\text{def}}{=} |\{k \in \mathbb{N} : k \leq n \wedge \text{nsd}(k, n) = 1\}|.$$

Pro  $n \in \mathbb{N}$  tedy  $\varphi(n)$  představuje počet čísel z množiny  $\{1, \dots, n\}$ , která jsou s číslem  $n$  nesoudělná.

## Příklad.

$$\varphi(4) = |\{1, 3\}| = 2,$$

## Definice.

Eulerovu funkci  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definujeme předpisem

$$\varphi(n) \stackrel{\text{def}}{=} |\{k \in \mathbb{N} : k \leq n \wedge \text{nsd}(k, n) = 1\}|.$$

Pro  $n \in \mathbb{N}$  tedy  $\varphi(n)$  představuje počet čísel z množiny  $\{1, \dots, n\}$ , která jsou s číslem  $n$  nesoudělná.

## Příklad.

$$\varphi(4) = |\{1, 3\}| = 2, \quad \varphi(12) = |\{1, 5, 7, 11\}| = 4,$$

## Definice.

Eulerovu funkci  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definujeme předpisem

$$\varphi(n) \stackrel{\text{def}}{=} |\{k \in \mathbb{N} : k \leq n \wedge \text{nsd}(k, n) = 1\}|.$$

Pro  $n \in \mathbb{N}$  tedy  $\varphi(n)$  představuje počet čísel z množiny  $\{1, \dots, n\}$ , která jsou s číslem  $n$  nesoudělná.

## Příklad.

$$\varphi(4) = |\{1, 3\}| = 2, \quad \varphi(12) = |\{1, 5, 7, 11\}| = 4,$$

$$\varphi(1\,000\,000) = ?$$

## Definice.

Eulerovu funkci  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  definujeme předpisem

$$\varphi(n) \stackrel{\text{def}}{=} |\{k \in \mathbb{N} : k \leq n \wedge \text{nsd}(k, n) = 1\}|.$$

Pro  $n \in \mathbb{N}$  tedy  $\varphi(n)$  představuje počet čísel z množiny  $\{1, \dots, n\}$ , která jsou s číslem  $n$  nesoudělná.

## Příklad.

$$\varphi(4) = |\{1, 3\}| = 2, \quad \varphi(12) = |\{1, 5, 7, 11\}| = 4,$$

$$\varphi(1\,000\,000) = ?$$

## Poznámka.

Eulerova funkce hraje naprosto zásadní úlohu v kryptografii.

Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$\frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}, \frac{12}{12}$



## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$$\frac{1}{12}, \quad \frac{2}{12}, \quad \frac{3}{12}, \quad \frac{4}{12}, \quad \frac{5}{12}, \quad \frac{6}{12}, \quad \frac{7}{12}, \quad \frac{8}{12}, \quad \frac{9}{12}, \quad \frac{10}{12}, \quad \frac{11}{12}, \quad \frac{12}{12}$$

$\frac{1}{1}$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$$\frac{1}{12}, \quad \frac{2}{12}, \quad \frac{3}{12}, \quad \frac{4}{12}, \quad \frac{5}{12}, \quad \frac{6}{12}, \quad \frac{7}{12}, \quad \frac{8}{12}, \quad \frac{9}{12}, \quad \frac{10}{12}, \quad \frac{11}{12}, \quad \frac{12}{12}$$
  
$$\frac{1}{2}, \quad \frac{1}{1}$$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$\frac{1}{12}$ ,	$\frac{2}{12}$ ,	$\frac{3}{12}$ ,	$\frac{4}{12}$ ,	$\frac{5}{12}$ ,	$\frac{6}{12}$ ,	$\frac{7}{12}$ ,	$\frac{8}{12}$ ,	$\frac{9}{12}$ ,	$\frac{10}{12}$ ,	$\frac{11}{12}$ ,	$\frac{12}{12}$
		$\frac{1}{3}$ ,			$\frac{1}{2}$ ,		$\frac{2}{3}$ ,				$\frac{1}{1}$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$\frac{1}{12}$ ,	$\frac{2}{12}$ ,	$\frac{3}{12}$ ,	$\frac{4}{12}$ ,	$\frac{5}{12}$ ,	$\frac{6}{12}$ ,	$\frac{7}{12}$ ,	$\frac{8}{12}$ ,	$\frac{9}{12}$ ,	$\frac{10}{12}$ ,	$\frac{11}{12}$ ,	$\frac{12}{12}$
		$\frac{1}{4}$ ,	$\frac{1}{3}$ ,		$\frac{1}{2}$ ,		$\frac{2}{3}$ ,	$\frac{3}{4}$ ,			$\frac{1}{1}$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$\frac{1}{12}$ ,	$\frac{2}{12}$ ,	$\frac{3}{12}$ ,	$\frac{4}{12}$ ,	$\frac{5}{12}$ ,	$\frac{6}{12}$ ,	$\frac{7}{12}$ ,	$\frac{8}{12}$ ,	$\frac{9}{12}$ ,	$\frac{10}{12}$ ,	$\frac{11}{12}$ ,	$\frac{12}{12}$
	$\frac{1}{6}$ ,	$\frac{1}{4}$ ,	$\frac{1}{3}$ ,		$\frac{1}{2}$ ,		$\frac{2}{3}$ ,	$\frac{3}{4}$ ,	$\frac{5}{6}$ ,		$\frac{1}{1}$

## Věta.

Pro všechna  $n \in \mathbb{N}$  platí

$$\sum_{d|n} \varphi(d) = n.$$

## Důkaz.

Uvažujme  $n$  zlomků  $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ , které převedeme do základního tvaru a roztřídíme podle jmenovatelů. Jmenovatelé po vykrácení jsou pak právě dělitelé čísla  $n$ . Zároveň je jasné, že různých zlomků se jmenovatelem  $d$  je přesně  $\varphi(d)$ .  $\square$

## Konkrétní situace pro $n = 12$ .

$\frac{1}{12}$ ,	$\frac{2}{12}$ ,	$\frac{3}{12}$ ,	$\frac{4}{12}$ ,	$\frac{5}{12}$ ,	$\frac{6}{12}$ ,	$\frac{7}{12}$ ,	$\frac{8}{12}$ ,	$\frac{9}{12}$ ,	$\frac{10}{12}$ ,	$\frac{11}{12}$ ,	$\frac{12}{12}$
$\frac{1}{12}$ ,	$\frac{1}{6}$ ,	$\frac{1}{4}$ ,	$\frac{1}{3}$ ,	$\frac{5}{12}$ ,	$\frac{1}{2}$ ,	$\frac{7}{12}$ ,	$\frac{2}{3}$ ,	$\frac{3}{4}$ ,	$\frac{5}{6}$ ,	$\frac{11}{12}$ ,	$\frac{1}{1}$

## Věta.

Je-li  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , pak

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

## Věta.

Je-li  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , pak

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

## Důkaz.

Z Möbiovy inverzní formule ( $a(n) = \varphi(n)$ ,  $b(n) = n$ ) a vztahu  $\sum_{d|n} \varphi(d) = n$  plyne

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



## Věta.

Je-li  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , pak

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

## Důkaz.

Z Möbiovy inverzní formule ( $a(n) = \varphi(n)$ ,  $b(n) = n$ ) a vztahu  $\sum_{d|n} \varphi(d) = n$  plyne

$$\begin{aligned} \varphi(n) = a(n) &= \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) = \sum_{d|n} \frac{n}{d} \mu(d) = n \sum_{d|n} \frac{\mu(d)}{d} = \\ &= n \left(1 + \sum_{1 \leq i \leq k} \frac{(-1)}{p_i} + \sum_{1 \leq i < j \leq k} \frac{1}{p_i p_j} + \dots + \frac{(-1)^k}{p_1 \dots p_k}\right) \end{aligned}$$

## Věta.

Je-li  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , pak

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

## Důkaz.

Z Möbiovy inverzní formule ( $a(n) = \varphi(n)$ ,  $b(n) = n$ ) a vztahu  $\sum_{d|n} \varphi(d) = n$  plyne

$$\begin{aligned} \varphi(n) = a(n) &= \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) = \sum_{d|n} \frac{n}{d} \mu(d) = n \sum_{d|n} \frac{\mu(d)}{d} = \\ &= n \left(1 + \sum_{1 \leq i \leq k} \frac{(-1)}{p_i} + \sum_{1 \leq i < j \leq k} \frac{1}{p_i p_j} + \dots + \frac{(-1)^k}{p_1 \dots p_k}\right) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right). \quad \square \end{aligned}$$

$$\left( \varphi(n) = n \prod_{i=1}^k \left( 1 - \frac{1}{p_i} \right) \right)$$

## Příklad.

$$\varphi(2018) = \varphi(2 \cdot 1009) = 2018 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{1009} \right) = 1008,$$

$$\left( \varphi(n) = n \prod_{i=1}^k \left( 1 - \frac{1}{p_i} \right) \right)$$

## Příklad.

$$\varphi(2018) = \varphi(2 \cdot 1009) = 2018 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{1009} \right) = 1008,$$

$$\varphi(1\,000\,000) = \varphi(2^6 \cdot 5^6) = 1\,000\,000 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{5} \right) = 400\,000,$$

$$\vdots$$

$$\left( \varphi(n) = n \prod_{i=1}^k \left( 1 - \frac{1}{p_i} \right) \right)$$

## Příklad.

$$\varphi(2018) = \varphi(2 \cdot 1009) = 2018 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{1009} \right) = 1008,$$

$$\varphi(1\,000\,000) = \varphi(2^6 \cdot 5^6) = 1\,000\,000 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{5} \right) = 400\,000,$$

$$\vdots$$

## Cvičení.

Najděte všechna přirozená čísla  $n$ , pro která platí

$$\varphi(n) = \frac{n}{3}.$$

$$\left( (u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) \right)$$

## Cvičení.

Nechť  $\tau(n)$  představuje počet dělitelů čísla  $n$  a  $\sigma(n)$  jejich součet. Dokažte, že

$$(\forall n \in \mathbb{N}) : \sigma(n) = \sum_{d|n} \tau\left(\frac{n}{d}\right)\varphi(d).$$

$$\left( (u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) \right)$$

## Cvičení.

Nechť  $\tau(n)$  představuje počet dělitelů čísla  $n$  a  $\sigma(n)$  jejich součet. Dokažte, že

$$(\forall n \in \mathbb{N}) : \sigma(n) = \sum_{d|n} \tau\left(\frac{n}{d}\right)\varphi(d).$$

## Řešení.

Víme, že

$$\mathbf{1} \star \mathbf{1} = \tau, \quad \mathbf{1} \star \varphi = \text{id} \quad \text{a} \quad \mathbf{1} \star \text{id} = \sigma.$$

$$\left( (u \star v)(n) = \sum_{d|n} u\left(\frac{n}{d}\right)v(d) \right)$$

## Cvičení.

Nechť  $\tau(n)$  představuje počet dělitelů čísla  $n$  a  $\sigma(n)$  jejich součet. Dokažte, že

$$(\forall n \in \mathbb{N}) : \sigma(n) = \sum_{d|n} \tau\left(\frac{n}{d}\right)\varphi(d).$$

## Řešení.

Víme, že

$$\mathbf{1} \star \mathbf{1} = \tau, \quad \mathbf{1} \star \varphi = \text{id} \quad \text{a} \quad \mathbf{1} \star \text{id} = \sigma.$$

Proto platí

$$\sigma = \mathbf{1} \star \text{id} = \mathbf{1} \star (\mathbf{1} \star \varphi) = (\mathbf{1} \star \mathbf{1}) \star \varphi = \tau \star \varphi.$$



## Cvičení.

Je známo, že  $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ . Pokuste se stanovit součty řad

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}, \quad \sum_{n=1}^{\infty} \frac{\tau(n)}{n^2}, \quad \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^2} \quad a \quad \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^2}.$$

## Cvičení.

Je známo, že  $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ . Pokuste se stanovit součty řad

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}, \quad \sum_{n=1}^{\infty} \frac{\tau(n)}{n^2}, \quad \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^2} \quad a \quad \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^2}.$$

## Zobecnění pro Riemannovu funkci.

Víme, že  $\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$ . Vyjádřete součty řad

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^x}, \quad \sum_{n=1}^{\infty} \frac{\tau(n)}{n^x}, \quad \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^x} \quad a \quad \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^x}$$

pomocí Riemannovy funkce  $\zeta$ .

## Věta.

Nechť  $a = \{a_n\}_{n=1}^{\infty}$  a  $b = \{b_n\}_{n=1}^{\infty}$  jsou dvě posloupnosti a  $x \in \mathbb{R}$ .

Předpokládejme, že řady  $\sum_{n=1}^{\infty} \frac{a_n}{n^x}$  a  $\sum_{n=1}^{\infty} \frac{b_n}{n^x}$  konvergují absolutně. Pak pro posloupnost  $c = \{c_n\}_{n=1}^{\infty}$  definovanou předpisem  $c = a \star b$  (Dirichletův součin) platí

$$\sum_{n=1}^{\infty} \frac{c_n}{n^x} = \sum_{n=1}^{\infty} \frac{a_n}{n^x} \cdot \sum_{n=1}^{\infty} \frac{b_n}{n^x}.$$

## Věta.

Nechť  $a = \{a_n\}_{n=1}^{\infty}$  a  $b = \{b_n\}_{n=1}^{\infty}$  jsou dvě posloupnosti a  $x \in \mathbb{R}$ .

Předpokládejme, že řady  $\sum_{n=1}^{\infty} \frac{a_n}{n^x}$  a  $\sum_{n=1}^{\infty} \frac{b_n}{n^x}$  konvergují absolutně. Pak pro posloupnost  $c = \{c_n\}_{n=1}^{\infty}$  definovanou předpisem  $c = a \star b$  (Dirichletův součin) platí

$$\sum_{n=1}^{\infty} \frac{c_n}{n^x} = \sum_{n=1}^{\infty} \frac{a_n}{n^x} \cdot \sum_{n=1}^{\infty} \frac{b_n}{n^x}.$$

## Důkaz.

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{a_k}{k^x} \cdot \sum_{l=1}^{\infty} \frac{b_l}{l^x} &= \sum_{k,l=1}^{\infty} \frac{a_k b_l}{(kl)^x} = \sum_{n=1}^{\infty} \left( \sum_{kl=n} \frac{a_k b_l}{n^x} \right) = \\ &= \sum_{n=1}^{\infty} \frac{1}{n^x} \left( \sum_{kl=n} a_k b_l \right) = \sum_{n=1}^{\infty} \frac{c_n}{n^x}. \end{aligned}$$



## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[ Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ . ]

## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[ Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ . ]

$$\frac{a_1 z}{1 - z} = a_1 z + a_1 z^2 + a_1 z^3 + a_1 z^4 + a_1 z^5 + a_1 z^6 + \dots$$

## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ .]

$$\frac{a_1 z}{1 - z} = a_1 z + a_1 z^2 + a_1 z^3 + a_1 z^4 + a_1 z^5 + a_1 z^6 + \dots$$

$$\frac{a_2 z^2}{1 - z^2} = + a_2 z^2 + a_2 z^4 + a_2 z^6 + \dots$$



## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[ Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ . ]

$$\frac{a_1 z}{1 - z} = a_1 z + a_1 z^2 + a_1 z^3 + a_1 z^4 + a_1 z^5 + a_1 z^6 + \dots$$

$$\frac{a_2 z^2}{1 - z^2} = + a_2 z^2 + a_2 z^4 + a_2 z^6 + \dots$$

$$\frac{a_3 z^3}{1 - z^3} = + a_3 z^3 + a_3 z^6 + \dots$$

## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[ Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ . ]

$$\frac{a_1 z}{1 - z} = a_1 z + a_1 z^2 + a_1 z^3 + a_1 z^4 + a_1 z^5 + a_1 z^6 + \dots$$

$$\frac{a_2 z^2}{1 - z^2} = + a_2 z^2 + a_2 z^4 + a_2 z^6 + \dots$$

$$\frac{a_3 z^3}{1 - z^3} = + a_3 z^3 + a_3 z^6 + \dots$$

$$\frac{a_4 z^4}{1 - z^4} = + a_4 z^4 + \dots$$

⋮

## Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[ Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ . ]

$$\frac{a_1 z}{1 - z} = a_1 z + a_1 z^2 + a_1 z^3 + a_1 z^4 + a_1 z^5 + a_1 z^6 + \dots$$

$$\frac{a_2 z^2}{1 - z^2} = + a_2 z^2 + a_2 z^4 + a_2 z^6 + \dots$$

$$\frac{a_3 z^3}{1 - z^3} = + a_3 z^3 + a_3 z^6 + \dots$$

$$\frac{a_4 z^4}{1 - z^4} = + a_4 z^4 + \dots$$

⋮

---

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n} = b_1 z + b_2 z^2 + b_3 z^3 + b_4 z^4 + b_5 z^5 + b_6 z^6 + \dots$$

# Lambertova řada.

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n}$$

[Tuto řadu budeme chtít vyjádřit ve tvaru  $\sum_{n=1}^{\infty} b_n z^n$ .]

$$\frac{a_1 z}{1 - z} = a_1 z + a_1 z^2 + a_1 z^3 + a_1 z^4 + a_1 z^5 + a_1 z^6 + \dots$$

$$\frac{a_2 z^2}{1 - z^2} = + a_2 z^2 + a_2 z^4 + a_2 z^6 + \dots$$

$$\frac{a_3 z^3}{1 - z^3} = + a_3 z^3 + a_3 z^6 + \dots$$

$$\frac{a_4 z^4}{1 - z^4} = + a_4 z^4 + \dots$$

⋮

$$b_n = \sum_{d|n} a_d$$

$$\sum_{n=1}^{\infty} \frac{a_n z^n}{1 - z^n} = b_1 z + b_2 z^2 + b_3 z^3 + b_4 z^4 + b_5 z^5 + b_6 z^6 + \dots$$

## Příklad.

Víme, že

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

## Příklad.

Víme, že

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

Proto platí

$$\sum_{n=1}^{\infty} \frac{\mu(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} e(n)z^n = z.$$

## Příklad.

Víme, že

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

Proto platí

$$\sum_{n=1}^{\infty} \frac{\mu(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} e(n)z^n = z.$$

## Příklad.

Protože platí  $\sum_{d|n} \varphi(d) = n$ ,

## Příklad.

Víme, že

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

Proto platí

$$\sum_{n=1}^{\infty} \frac{\mu(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} e(n)z^n = z.$$

## Příklad.

Protože platí  $\sum_{d|n} \varphi(d) = n$ , dostaneme

$$\sum_{n=1}^{\infty} \frac{\varphi(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} nz^n$$



## Příklad.

Víme, že

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

Proto platí

$$\sum_{n=1}^{\infty} \frac{\mu(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} e(n)z^n = z.$$

## Příklad.

Protože platí  $\sum_{d|n} \varphi(d) = n$ , dostaneme

$$\sum_{n=1}^{\infty} \frac{\varphi(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} nz^n = z \left( \sum_{n=1}^{\infty} z^n \right)' = z \left( \frac{z}{1-z} \right)' = \frac{z}{(1-z)^2}.$$

## Příklad.

Víme, že

$$\sum_{d|n} \mu(d) = e(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pro } n \in \mathbb{N} \setminus \{1\}. \end{cases}$$

Proto platí

$$\sum_{n=1}^{\infty} \frac{\mu(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} e(n)z^n = z.$$

## Příklad.

Protože platí  $\sum_{d|n} \varphi(d) = n$ , dostaneme

$$\sum_{n=1}^{\infty} \frac{\varphi(n)z^n}{1-z^n} = \sum_{n=1}^{\infty} nz^n = z \left( \sum_{n=1}^{\infty} z^n \right)' = z \left( \frac{z}{1-z} \right)' = \frac{z}{(1-z)^2}.$$

## Příklad.

$$\sum_{n=1}^{\infty} \frac{z^n}{1-z^n} = \sum_{n=1}^{\infty} \tau(n)z^n.$$

## Věta.

Nechť  $f$  a  $g$  jsou dvě funkce definované na intervalu  $\langle 1, +\infty \rangle$ . Pak platí

$$\left[ (\forall x \in \langle 1, +\infty \rangle) : g(x) = \sum_{k=1}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right) \right] \iff$$
$$\iff \left[ (\forall x \in \langle 1, +\infty \rangle) : f(x) = \sum_{k=1}^{\lfloor x \rfloor} g\left(\frac{x}{k}\right) \mu(k) \right].$$

## Věta.

Nechť  $f$  a  $g$  jsou dvě funkce definované na intervalu  $\langle 1, +\infty \rangle$ . Pak platí

$$\left[ (\forall x \in \langle 1, +\infty \rangle) : g(x) = \sum_{k=1}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right) \right] \iff$$
$$\iff \left[ (\forall x \in \langle 1, +\infty \rangle) : f(x) = \sum_{k=1}^{\lfloor x \rfloor} g\left(\frac{x}{k}\right) \mu(k) \right].$$

Symbol  $\lfloor x \rfloor$  představuje dolní celou část čísla  $x$ , tj.  $\lfloor x \rfloor$  je celé číslo splňující

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

$$g(x) = \sum_{k=1}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right) \iff f(x) = \sum_{k=1}^{\lfloor x \rfloor} g\left(\frac{x}{k}\right) \mu(k)$$

## Poznámka.

Jsou-li  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  dvě posloupnosti, klasickou verzi Möbiovy inverzní formule dostaneme z výše uvedené věty tak, že definujeme

$$f(x) \stackrel{\text{def}}{=} \begin{cases} a(x) & \text{pro } x \in \mathbb{N}, \\ 0 & \text{pro } x \in \mathbb{R} \setminus \mathbb{N} \end{cases} \quad \text{a} \quad g(x) \stackrel{\text{def}}{=} \begin{cases} b(x) & \text{pro } x \in \mathbb{N}, \\ 0 & \text{pro } x \in \mathbb{R} \setminus \mathbb{N}. \end{cases}$$

$$g(x) = \sum_{k=1}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right) \iff f(x) = \sum_{k=1}^{\lfloor x \rfloor} g\left(\frac{x}{k}\right) \mu(k)$$

## Poznámka.

Jsou-li  $\{a(n)\}_{n=1}^{\infty}$  a  $\{b(n)\}_{n=1}^{\infty}$  dvě posloupnosti, klasickou verzí Möbiovy inverzní formule dostaneme z výše uvedené věty tak, že definujeme

$$f(x) \stackrel{\text{def}}{=} \begin{cases} a(x) & \text{pro } x \in \mathbb{N}, \\ 0 & \text{pro } x \in \mathbb{R} \setminus \mathbb{N} \end{cases} \quad \text{a} \quad g(x) \stackrel{\text{def}}{=} \begin{cases} b(x) & \text{pro } x \in \mathbb{N}, \\ 0 & \text{pro } x \in \mathbb{R} \setminus \mathbb{N}. \end{cases}$$

Uvědomme si totiž, že pak platí

$$\left[ (\forall n \in \mathbb{N}) : b(n) = \sum_{d|n} a(d) \right] \iff \left[ (\forall x \in \langle 1, +\infty \rangle) : g(x) = \sum_{k=1}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right) \right]$$

a

$$\left[ (\forall n \in \mathbb{N}) : a(n) = \sum_{d|n} b\left(\frac{n}{d}\right) \mu(d) \right] \iff \left[ (\forall x \in \langle 1, +\infty \rangle) : f(x) = \sum_{k=1}^{\lfloor x \rfloor} g\left(\frac{x}{k}\right) \mu(k) \right]$$

## Věta.

Nechť  $f$  a  $g$  jsou funkce definované na intervalu  $\langle 1, +\infty \rangle$ . Dále buď  $s \in \mathbb{R}$  takové, že pro každé  $x \in \langle 1, +\infty \rangle$  řady

$$\sum_{k,l=1}^{\infty} \frac{f(klx)}{(kl)^s} \quad \text{a} \quad \sum_{k,l=1}^{\infty} \frac{g(klx)}{(kl)^s}$$

absolutně konvergují. Pak platí

$$\left[ (\forall x \in \langle 1, +\infty \rangle) : g(x) = \sum_{k=1}^{\infty} \frac{f(kx)}{k^s} \right] \iff$$
$$\iff \left[ (\forall x \in \langle 1, +\infty \rangle) : f(x) = \sum_{k=1}^{\infty} \frac{g(kx)\mu(k)}{k^s} \right].$$

# A ještě jedna úloha na závěr

## Cvičení.

Pro  $x \in \mathbb{R}^+$  najděte součet řady

$$\sum_{k=1}^{\infty} \left[ \frac{x}{k} \right] \mu(k).$$





Michal Bulant, Algebra 2 – Teorie čísel,

<https://www.math.muni.cz/~bulik/vyuka/Algebra-2/alg2-screen.pdf>.



[https://en.wikipedia.org/wiki/Möbius\\_inversion\\_formula](https://en.wikipedia.org/wiki/Möbius_inversion_formula).

**Děkuji za pozornost.**