Möbiova inverzní formule

Konečná tělesa

29. května 2020

Obsah přednášky

Sekce 5: Definujeme Möbiovu funkci a dokážeme Möbiovu formuli. Ukážeme si některé aplikace, například se naučíme pomocí Möbiovy inverzní fromule počítat cyklotomické polynomy.

Möbiova funkce

Definice

Möbiova funkce je zobrazení $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) := \begin{cases} 1 & \text{pokud } n = 1, \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel}, \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p. \end{cases}$$

Möbiova funkce

Definice

Möbiova funkce je zobrazení $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) := \begin{cases} 1 & \text{pokud } n = 1, \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel}, \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p. \end{cases}$$

Lemma (5.1)

Pro libovolné $1 < n \in \mathbb{N}$ *platí rovnost*

$$\sum_{d \mid n} \mu(d) = 0.$$

Möbiova funkce

Definice

Möbiova funkce je zobrazení $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) := \begin{cases} 1 & \text{pokud } n = 1, \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel}, \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p. \end{cases}$$

Lemma (5.1)

Pro libovolné $1 < n \in \mathbb{N}$ *platí rovnost*

$$\sum_{d \mid n} \mu(d) = 0.$$

Důkaz.

□

Möbiova funkce

Definice

Möbiova funkce je zobrazení $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) := \begin{cases} 1 & \text{pokud } n = 1, \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel}, \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p. \end{cases}$$

Lemma (5.1)

Pro libovolné $1 < n \in \mathbb{N}$ *platí rovnost*

$$\sum_{d \mid n} \mu(d) = 0.$$

Důkaz.

- Buď $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ rozklad na prvočinitele.

Möbiova funkce

Definice

Möbiova funkce je zobrazení $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) := \begin{cases} 1 & \text{pokud } n = 1, \\ (-1)^k & \text{pokud } n \text{ je součin } k \text{ různých prvočísel}, \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p. \end{cases}$$

Lemma (5.1)

Pro libovolné $1 < n \in \mathbb{N}$ *platí rovnost*

$$\sum_{d \mid n} \mu(d) = 0.$$

Důkaz.

- Buď $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ rozklad na prvočinitele.
- Potom

$$\sum_{d \mid n} \mu(d) = \mu(1) + \sum_i \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \dots$$

$$= 1 - \binom{n}{1} + \binom{n}{2} - \dots + (-1)^n \binom{n}{n} = (1-1)^n = 0.$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení.*

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \cdot \sum_{c \mid \frac{n}{d}} h(c) \right)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \cdot \sum_{c \mid \frac{n}{d}} h(c) \right) = \sum_{d \mid n} \sum_{c \mid \frac{n}{d}} \mu(d) \cdot h(c)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \cdot \sum_{c \mid \frac{n}{d}} h(c) \right) = \sum_{d \mid n} \sum_{c \mid \frac{n}{d}} \mu(d) \cdot h(c) = \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} \mu(d) \cdot h(c)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \cdot \sum_{c \mid \frac{n}{d}} h(c) \right) = \sum_{d \mid n} \sum_{c \mid \frac{n}{d}} \mu(d) \cdot h(c) = \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} \mu(d) \cdot h(c)$$

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

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \cdot \sum_{c \mid \frac{n}{d}} h(c) \right) = \sum_{d \mid n} \sum_{c \mid \frac{n}{d}} \mu(d) \cdot h(c) = \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} \mu(d) \cdot h(c)$$

$$= \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} h(c) \cdot \mu(d) = \sum_{c \mid n} h(c) \cdot \left(\sum_{d \mid \frac{n}{c}} \mu(d) \right)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\boldsymbol{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \textit{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \textit{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Rightarrow)$

$$\sum_{d \mid n} \mu(d) \cdot H\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \cdot \sum_{c \mid \frac{n}{d}} h(c) \right) = \sum_{d \mid n} \sum_{c \mid \frac{n}{d}} \mu(d) \cdot h(c) = \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} \mu(d) \cdot h(c)$$

$$= \sum_{c \mid n} \sum_{d \mid \frac{n}{c}} h(c) \cdot \mu(d) = \sum_{c \mid n} h(c) \cdot \left(\sum_{d \mid \frac{n}{c}} \mu(d) \right) = h(n).$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Leftarrow)$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Důkaz.

($\Leftarrow$)

$$\sum_{d \mid n} h(d)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d \mid n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d \mid n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Důkaz.

$(\Leftarrow)$

$$\sum_{d \mid n} h(d) = \sum_{d \mid n} \sum_{c \mid d} \mu(c) H\left(\frac{d}{c}\right)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d|n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Důkaz.

($\Leftarrow$)

$$\sum_{d|n} h(d) = \sum_{d|n} \sum_{c|d} \mu(c) H\left(\frac{d}{c}\right) = \sum_{e|n} \sum_{c|\frac{n}{e}} \mu(c) H(e)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d|n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Důkaz.

($\Leftarrow$)

$$\sum_{d|n} h(d) = \sum_{d|n} \sum_{c|d} \mu(c) H\left(\frac{d}{c}\right) = \sum_{e|n} \sum_{c|\frac{n}{e}} \mu(c) H(e) = \sum_{e|n} H(e) \sum_{c|\frac{n}{e}} \mu(c)$$

□

Möbiova inverzní formule

Věta (5.2 - Möbiova inverzní formule)

Nechť $\mathbf{G} = (G, +)$ *je Abelova grupa a* $H, h\colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \sum_{d|n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d), \qquad \text{pro všechna } n \in \mathbb{N}.$$

Důkaz.

($\Leftarrow$)

$$\sum_{d|n} h(d) = \sum_{d|n} \sum_{c|d} \mu(c) H\left(\frac{d}{c}\right) = \sum_{e|n} \sum_{c|\frac{n}{e}} \mu(c) H(e) = \sum_{e|n} H(e) \sum_{c|\frac{n}{e}} \mu(c) = H(n)$$

□

Věta (5.2 - Möbiova inverzní formule (multiplikativní značení))

Nechť $\boldsymbol{G} = (G, \cdot)$ *je Abelova grupa a* $H, h \colon \mathbb{N} \to G$ *dvojice zobrazení. Potom*

$$H(n) = \prod_{d|n} h(d), \qquad \text{pro všechna } n \in \mathbb{N}$$

právě když

$$h(n) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)}, \qquad \text{pro všechna } n \in \mathbb{N}.$$

Aplikace 1 - součin monických ireducibilních polynomů

Značení

Označme $I_{q,n}(x)$ součin všech monických ireducibilních poynomů stupně n nad tělesem $\mathbb{F}_q$.

Aplikace 1 - součin monických ireducibilních polynomů

Značení

Označme $I_{q,n}(x)$ součin všech monických ireducibilních poynomů stupně n nad tělesem $\mathbb{F}_q$.

Platí, že

$$x^{q^n} - x = \prod_{d|n} I_{q,d}(x).$$

Aplikace 1 - součin monických ireducibilních polynomů

Značení

Označme $I_{q,n}(x)$ součin všech monických ireducibilních poynomů stupně n nad tělesem $\mathbb{F}_q$.

Platí, že

$$x^{q^n} - x = \prod_{d|n} I_{q,d}(x).$$

Použitím Möbiovy inverzní formule dostaneme, že

$$I_{q,n}(x) = \prod_{d|n} (x^{q^d} - x)^{\mu\left(\frac{n}{d}\right)}.$$

Aplikace 2 - počet monických ireducibilních polynomů

Značení

Označme $i_{q,n}$ počet monických ireducibilních poynomů stupně n nad tělesem $\mathbb{F}_q$.

Aplikace 2 - počet monických ireducibilních polynomů

Značení

Označme $i_{q,n}$ počet monických ireducibilních poynomů stupně n nad tělesem $\mathbb{F}_q$.

Platí, že

$$q^n = \sum_{d|n} d \cdot i_{q,d}$$

Aplikace 2 - počet monických ireducibilních polynomů

Značení

Označme $i_{q,n}$ počet monických ireducibilních poynomů stupně n nad tělesem $\mathbb{F}_q$.

Platí, že

$$q^n = \sum_{d|n} d \cdot i_{q,d}$$

Použitím Möbiovy inverzní formule na zobrazení $H(n) = q^n$ a $h(n) = n \cdot i_{q,n}$ a vydělením n dostaneme, že

$$i_{q,n} = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d,$$

Příklad

Součin všech monických ireducibilních polynomů stupně 6 nad tělesem $\mathbb{F}_3$ je

$$I_{3,6}(x) = (x^{3^6} - x)^{\mu(1)}(x^{3^2} - x)^{\mu(3)}(x^{3^3} - x)^{\mu(2)}(x^3 - x)^{\mu(6)}$$
$$= \frac{(x^{3^6} - x)(x^3 - x)}{(x^{3^2} - x)(x^{3^3} - x)} = \frac{(x^{728} - 1)(x^2 - 1)}{(x^8 - 1)(x^{26} - 1)} = x^{629} + \cdots$$

Příklad

Součin všech monických ireducibilních polynomů stupně 6 nad tělesem $\mathbb{F}_3$ je

$$\begin{aligned} I_{3,6}(x) &= (x^{3^6} - x)^{\mu(1)}(x^{3^2} - x)^{\mu(3)}(x^{3^3} - x)^{\mu(2)}(x^3 - x)^{\mu(6)} \\ &= \frac{(x^{3^6} - x)(x^3 - x)}{(x^{3^2} - x)(x^{3^3} - x)} = \frac{(x^{728} - 1)(x^2 - 1)}{(x^8 - 1)(x^{26} - 1)} = x^{629} + \cdots \end{aligned}$$

Příklad

Počet všech monických ireducibilních polynomů stupně 6 nad tělesem $\mathbb{F}_3$ je

$$\begin{aligned} i_{3,6} &= \frac{1}{6}\left(\mu(1) \cdot 3^6 + \mu(2) \cdot 3^3 + \mu(3) \cdot 3^2 + \mu(6) \cdot 3\right) \\ &= \frac{1}{6}\left(3^6 - 3^3 - 3^2 + 3\right) = 116. \end{aligned}$$

Aplikace 3 - výpočet cyklotomických polynomů

Uvažujeme polynomy nad konečným tělesem $\mathbb{F}_q$. Pro přirozené číslo n nesoudělné s q budeme počítat n-tý cyklotomický polynom Q_n. Vyjdeme ze vztahu

$$x^n - 1 = \prod_{d|n} Q_d(x).$$

Aplikace 3 - výpočet cyklotomických polynomů

Uvažujeme polynomy nad konečným tělesem $\mathbb{F}_q$. Pro přirozené číslo n nesoudělné s q budeme počítat n-tý cyklotomický polynom Q_n. Vyjdeme ze vztahu

$$x^n - 1 = \prod_{d|n} Q_d(x).$$

Položíme $H(n) = x^n - 1$, $h(n) = Q_n(x)$ a aplikujeme Möbiovu inverzní formuli. Dostaneme

$$Q_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Příklad

$$Q_{12}(x) = \prod_{d|12} (x^{\frac{12}{d}} - 1)^{\mu(d)} = (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)}$$

Příklad

$$Q_{12}(x) = \prod_{d|12} (x^{\frac{12}{d}} - 1)^{\mu(d)} = (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)}$$

$$(x^4 - 1)^{\mu(3)} (x^3 - 1)^{\mu(4)} (x^2 - 1)^{\mu(6)} (x^1 - 1)^{\mu(12)}$$

Příklad

$$Q_{12}(x) = \prod_{d|12} (x^{\frac{12}{d}} - 1)^{\mu(d)} = (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)}$$

$$(x^4 - 1)^{\mu(3)} (x^3 - 1)^{\mu(4)} (x^2 - 1)^{\mu(6)} (x^1 - 1)^{\mu(12)}$$

$$= (x^{12} - 1)^1 (x^6 - 1)^{-1} (x^4 - 1)^{-1} (x^3 - 1)^0 (x^2 - 1)^1 (x^1 - 1)^0$$

Příklad

$$Q_{12}(x) = \prod_{d|12} (x^{\frac{12}{d}} - 1)^{\mu(d)} = (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)}$$

$$(x^4 - 1)^{\mu(3)} (x^3 - 1)^{\mu(4)} (x^2 - 1)^{\mu(6)} (x^1 - 1)^{\mu(12)}$$

$$= (x^{12} - 1)^1 (x^6 - 1)^{-1} (x^4 - 1)^{-1} (x^3 - 1)^0 (x^2 - 1)^1 (x^1 - 1)^0$$

$$= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1.$$