Eulerova funkcia

25. novembra 2022

Eulerova funkcia

Definícia

Nech $m \in \mathbb{N}$. Ako $\varphi(m)$ označíme počet čísel z množiny $\{1, 2, \ldots, m\}$ nesúdeliteľných s m. Funkciu φ nazývame *Eulerova funkcia.*

- $\varphi(1) = 1$
- $\varphi(12) = |\{1, 5, 7, 11\}| = 4$
- $\varphi(p) = p - 1$
- $\varphi(p^k) = p^k - p^{k-1}$

Eulerova funkcia

Veta

Eulerova funkcia φ je multiplikatívna.

Veta

Nech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla n. Potom

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

Eulerova funkcia

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$$

pre $d = (m, n)$

Malá Fermatova veta

Lema

Nech p je prvočíslo a nech $1 \leq i \leq p-1$. Potom $p \mid \binom{p}{i}$, čiže

$$\binom{p}{i} \equiv 0 \pmod{p}.$$

Lema

Nech p je prvočíslo. Potom

$$a^p \equiv a \pmod{p} \tag{2}$$

pre každé celé číslo a.

Malá Fermatova veta

Veta (Malá Fermatova veta)

Nech p je prvočíslo a nech a je celé číslo také, že $p \nmid a$. Potom

$$a^{p-1} \equiv 1 \pmod{p} \tag{3}$$

Kombinatorický dôkaz

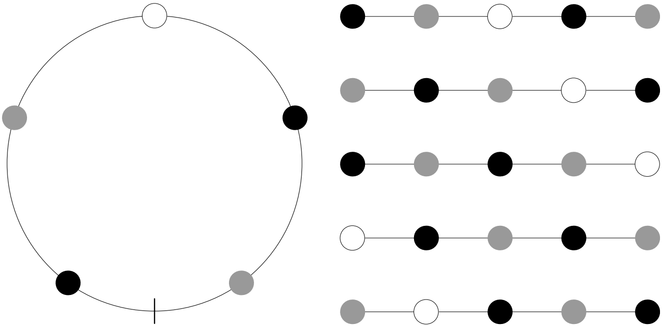

Figure: Ofarbenie zopnutého náhrdelníka a 5 ofarbení rozopnutého náhrdelníka, ktoré mu zodpovedajú

Eulerova veta

Lema

Nech $n \in \mathbb{N}$ *a* p *je prvočíslo. Ak* $n \equiv 1 \pmod{p^\alpha}$*, tak* $n^p \equiv 1 \pmod{p^{\alpha+1}}$.

Veta (Eulerova veta)

Nech $a, n \in \mathbb{N}$ *sú také, že* $(a, n) = 1$*. Potom*

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

Súčet cez všetkých deliteľov

Veta

Pre ľubovoľné prirodzené číslo n platí

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

Asymptotické správanie Eulerovej funkcie

Tvrdenie

Nech $(a_n)_{n=1}^{\infty}$ je postupnosť čísel takých, že $0 < a_k < 1$ a

$$\sum_{k=1}^{\infty} a_k = +\infty.$$

Potom

$$\prod_{k=1}^{\infty} (1 - a_k) = 0.$$

Asymptotické správanie Eulerovej funkcie

Veta

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1$$

$$\liminf_{n\to\infty} \frac{\varphi(n)}{n} = 0$$

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$$