Eulerova veta

Barbora Novosadová

Na úvod - rekap. kongruencie. Relácia $a \equiv b \,(mod\, n)$ značí, že a, b majú rovnaký zvyšok po delení n. Teda tiež $n|a-b$. Platí nasledovné: nech $a \equiv c \,(mod\, n)$ a $b \equiv d \,(mod\, n)$. Potom

$$\begin{aligned} a+b &\equiv c+d \,(mod\, n);\\ ab &\equiv cd \,(mod\, n);\\ a^n &\equiv c^n \,(mod\, n);\\ \forall x \in \mathbf{N}:\ xa &\equiv xc \,(mod\, n). \end{aligned}$$

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

Poznámka: $\varphi(p) = p - 1$ ak p je prvočíslo.

Lema 1. *Pre* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *je*

$$\begin{aligned} \varphi(n) &= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k}) = \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})\ldots(p_k^{\alpha_k} - p_k^{\alpha_k-1}) = \\ &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k}). \end{aligned}$$

Odvodenie:

- Pre p^α, $\alpha > 0$, p-prvočíslo: $d|p^\alpha \Leftrightarrow p|d$
  Označme $X = \{1, 2, \ldots, p^\alpha\}$ a X_p množinu násobkov p v X. Potom
  $\varphi(p^\alpha) = |X| - |X_p| = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$.
- Pre $p^\alpha q^\beta$, $\alpha, \beta > 0$, p, q-prvočísla: $d|p^\alpha q^\beta \Leftrightarrow p|d \vee q|d$.
  Označme X čísla od 1 do $p^\alpha q^\beta$, X_p čísla z X deliteľné p a X_q čísla z X deliteľné q.
  Potom $\varphi(p^\alpha q^\beta) = |X| - |X_p \cup X_q|$.
  Z princípu zapojenia a vypojenia (inklúzie-exklúzie) dostávame, že
  $|X_p \cup X_q| = |X_p| + |X_q| - |X_p \cap X_q| = \frac{|X|}{p} + \frac{|X|}{q} - \frac{|X|}{pq}|$.
  $\varphi(p^\alpha q^\beta) = |X| - \frac{|X|}{p} - \frac{|X|}{q} + \frac{|X|}{pq} = |X|(1 - \frac{1}{p})(1 - \frac{1}{q})$.
- Pre $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $\alpha_i > 0$, p_i-prvočísla:
  $$d|p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \Leftrightarrow p_1|d \vee p_2|d \vee \ldots \vee p_k|d.$$
  Označme X čísla od 1 po n, X_{p_i} čísla z X deliteľné p_i, $i = 1, 2, \ldots, k$.
  $\varphi(n) = |X| - |X_{p_1} \cup X_{p_2} \cup \ldots \cup X_{p_k}|$.
  $|X| - |X_{p_1} \cup X_{p_2} \cup \ldots \cup X_{p_k}| = |X| - |(X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}) \cup X_{p_k}| = |X| - |X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}| - |X_p| + |(X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}) \cap X_p| = |X| - |X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}| - \frac{|X|}{p_k} - \frac{|X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}|}{p_k} = (1 - \frac{1}{p_k})(|X| - |X_{p_1} \cup X_{p_2} \cup \ldots X_{p_{k-1}}|) = |X|(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$.

Obr. 1: Lemma 1 proof

Veta 2 (Eulerova veta)**.** *Ak* $(a, n) = 1$*, tak* $a^{\varphi(n)} \equiv 1 \,(mod\, n)$*. Poznámka: v skutočnosti je to* $\Leftrightarrow$*, nie len* $\Rightarrow$*.*

Dôkaz. Nech $A = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ je množina čísel menších ako n, ktoré sú s n nesúdeliteľné. Vezmime $a \in A$. Pre všetky a_i, ca_i je tiež nesúdeliteľné s n, keďže a aj a_i sú z A. Takže

$$\exists j: \quad aa_i \equiv a_j \,(mod\, n)$$

a tiež

$$aa_i \equiv aa_j \,(mod\, n) \implies a_i \equiv a_j \,(mod\, n)$$

(v kongruenciách môžeme krátiť nesúdeliteľnými prvkami). Takže množina $\{aa_1, aa_2, \ldots, aa_{\varphi(n)}\}$ je iba permutáciou množiny A.
Z toho

$$\prod_{k=1}^{\varphi(n)} aa_k \equiv \prod_{k=1}^{\varphi(n)} a_k \,(mod\, n),$$
$$a^{\varphi(n)} \prod_{k=1}^{\varphi(n)} a_k \equiv \prod_{k=1}^{\varphi(n)} a_k \,(mod\, n),$$
$$a^{\varphi(n)} \equiv 1 \,(mod\, n).$$

V poslednom sme krátili $\prod_{k=1}^{\varphi(n)} a_k$, keďže je nesúdeliteľné s n. □

Príklad 1. $n = 7$, $a = 5$.
$\varphi(7) = 6$
$5^2 \equiv 4 \,(mod\, 7)$; $5^3 \equiv 4 \cdot 5 \equiv 6 \,(mod\, 7)$; $5^4 \equiv 2 \,(mod\, 7)$; $5^5 \equiv 3 \,(mod\, 7)$; $5^6 \equiv 1 \,(mod\, 7)$

Cvičenie 1. Zisti poslednú cifru: 13^{2020}, 13^{2026}, $3^{815}+2^{270}$, $17^{17^{17}}$

Cvičenie 2. Nájdi zvyšky po delení 7: 2^{10}, 2^{100}, 2^{1000}.

Dôsledok 2.1 (Malá Fermatova veta)**.** *Nech p je prvočíslo. Potom pre $\forall a \in \mathbf{N}$, $a \neq p$:*

$$a^{p-1} \equiv 1 \,(mod\, p)$$
$$a^{p} \equiv p \,(mod\, p)$$

Cvičenie 3. Nájdi najmenšie také $k \in \mathbf{N}$, že

$$65 | 5n^{13} + 13n^5 + 9kn, \quad \forall n \in \mathbf{N}$$

Cvičenie 4. Nech p, q sú prvočísla, $p \neq q$. Dokáž $pq \,|\, p^{q-1} + q^{p-1} - 1$.

Cvičenie 5. Nech p, q sú prvočísla, $p \neq q$. Dokáž

$$p^q + q^p \equiv p + q \,(mod\, pq)$$

Cvičenie 6. Nech $(a, p) = 1$, nech $p - 1 \,|\, k - l$. Potom $a^k \equiv a^l \,(mod\, p)$. Dokáž!

Cvičenie 7. Nech p, q sú prvočísla. Dokáž $5 \,|\, p^5 q - q^5 p$.

Úloha 1. Nech $(a, p) = 1$, nech k je najmenšie také, že $a^k \equiv 1 \,(mod\, p)$. Dokáž $k \,|\, p - 1$.

Riešenie. Sporom. Nech $k \nmid p - 1$. Keďže $k \leq p - 1$, určite existujú $o, r \in \mathbf{Z}$ t.ž. $0 < r < k$ a $ko + r = p - 1$. Potom

$$a^{p-1} \equiv 1 \,(mod\, p),$$
$$1 \equiv a^{ko+r} \equiv \left(a^k\right)^o a^r \equiv a^r \,(mod\, p),$$

čo je spor s minimalitou k.

Cvičenie 8. Existuje také $n \in \mathbf{N}$, že 2026 rôznych prvočísel delí n a zároveň $n \,|\, 2^n - 2$?