Teória čísel – kongruencie

Mirka Sotáková

Základné vlastnosti

Majme tri celé čísla $a,\ b$ a m. Hovoríme, že a je *kongruentné* s b *modulo* m a píšeme $a \equiv b \pmod{m}$, ak rozdiel $a-b$ je deliteľný m. Číslo m nazývame *modul* kongruencie. Z definície ľahko plynú nasledujúce vlastnosti:

- $a \equiv a \pmod{m}$ (reflexivita).
- $a \equiv b \pmod{m}$ práve vtedy keď $b \equiv a \pmod{m}$ (symetria).
- ak $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$, potom $a \equiv c \pmod{m}$ (tranzitivita).
- Pre pevné m je na základe týchto troch vlastností kongruencia modulo m ekvivalenciou na $\mathbb{Z}$.
- Pre pevné m, každá *trieda ekvivalencie* vzhľadom na kongruenciu modulo m obsahuje práve jeden prvok množiny $\{0, 1, 2, \ldots, m-1\}$. Tieto triedy nazývame aj *zvyškovými* triedami. Množina obsahujúca po jednom prvku z každej triedy sa nazýva *úplný systém zvyškov*.
- Ak $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, potom $a \pm c \equiv b \pm d \pmod{m}$ a $ac \equiv bd \pmod{m}$.
- Ak $a \equiv b \pmod{m}$, potom $a \equiv b \pmod{d}$ pre ľubovoľného deliteľa $d|m$.
- Ak $a \equiv b \pmod{m},\ a \equiv b \pmod{n}$ a m a n sú navzájom nesúdeliteľné, potom $a \equiv b \pmod{mn}$.

Veta. *Majme úplný systém zvyškov modulo m. Prvok tejto množiny v nej má multiplikatívny inverz (inverzný prvok vzhľadom na násobenie) práve vtedy, keď je nesúdeliteľný s m. Inak povedané, platí: Pre $a \in \mathbb{Z}$ existuje $b \in \mathbb{Z}$ také, že $ab \equiv 1 \pmod{m}$, práve vtedy, keď $(a, m) = 1$ ((x, y) je najvetší spoločný deliteľ čísel x a y).*

Dôsledok. *Riešme lineárnu kongruenciu $ax \equiv b \pmod{m}$, kde bez ujmy na všeobecnosti predpokladajme, že $0 \leq a, b < m$. Potom ak $(a, m) = 1$, existuje riešenie a všetky riešenia majú tvar $x = x_0 + mn$ pre $n \in \mathbb{N}$ a x_0, ktoré rieši danú kongruenciu. Ak $(a, m) = d$, potom riešenie existuje práve vtedy, ak $d|b$ a v tomto prípade je kongruencia ekvivalentná (má rovnaké riešenaia) s kongruenciou $a'x \equiv b' \pmod{m'}$, kde $a' = a/d,\ b' = b/d,\ m' = m/d$.*

Dôsledok. *Ak $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$ a $(c, m) = 1$ (aj $(d, m) = 1$), potom $ac^{-1} \equiv bd^{-1} \pmod{m}$ (kde c^{-n} oznacuje n-tú mocninu akéhokoľvek inverzného prvku k c modulo m).*

Veta. (Malá Fermatova) *Buď p prvočíslo. Potom pre každé $a \in \mathbb{Z}$, ktoré nie je*

deliteľné p, platí $a^{p-1} \equiv 1 \pmod{p}$.

Veta. (Čínska zvyšková) *Riešme sústavu kongruencií*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

Nech pre každú dvojicu $i \neq j$ platí $(m_i, m_j) = 1$. Potom existuje riešenie tejto sústavy a každé dve riešenia sú si navzájom kongruentné modulo $M = m_1 m_2 \dots m_r$.

Dôsledok. *Eulerova funkcia φ (označujúca počet kladných celých čísel nesúdeliteľných s daným kladným celým číslom n, menších nebo rovných n) je multiplikatívna, teda $\varphi(mn) = \varphi(m)\varphi(n)$, vždy keď $(m, n) = 1$.*

Veta. *Ak $(a, m) = 1$, potom* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Veta.

$$\sum_{d|n,\ d>0} \varphi(d) = n.$$

A ešte niekoľko užitočných slov o rozkladoch (polynómov na koreňové činitele).

Veta. *Pre všetky dvojice $b \in \mathbb{Z},\ n \in \mathbb{N}$ platí $b^n - 1 = (b-1)(b^{n-1} + b^{n-2} + \dots + b^2 + b^1 + 1)$.*

Veta. *Nech $(b, m) = 1$ a $a, c \in \mathbb{N}$. Ak $b^a \equiv 1 \pmod{m}$ a $b^c \equiv 1 \pmod{m}$ a $(a, c) = d$, potom $b^d \equiv 1 \pmod{m}$.*

Veta. *Nech p je prvočíslo a $p|(b^n - 1)$, potom platí: alebo $p|(b^d - 1)$ pre nejaké $d|n,\ d \neq n$ alebo $p \equiv 1 \pmod{n}$. Ak $p > 2$ a n je nepárne, potom v druhom prípade $p \equiv 1 \pmod{2n}$.*