Kongruencie

27. októbra 2023

Definícia kongruencie

Definícia

Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Hovoríme, že a a b sú *kongruentné modulo* n, ak $n \mid a - b$. Označenie: $a \equiv b \pmod{n}$.

- $a \equiv b \pmod{n}$ znamená rovnaký zvyšok po delení n.
- Napríklad $13 \equiv 1 \pmod{4}$, $13 \equiv 8 \pmod{5}$.

Kongruencia je relácia ekvivalencie

Lema

Nech $n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$.

(i) $a \equiv a \pmod{n}$

(ii) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

(iii) $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

Definícia

Triedy ekvivalencie zodpovedajúce relácii $a \equiv b \pmod{n}$ nazývame *zvyškové triedy modulo n*. Zvyškovú triedu čísla k označujeme $\overline{k}$.

Sčitovanie a násobenie kongruencií

Veta

Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. *Nech* $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$. *Potom*

$$a + c \equiv b + d \pmod{n},$$
$$ac \equiv bd \pmod{n}.$$

Dôsledok

Ak $a_i \equiv b_i \pmod{n}$ *pre všetky* $i = 1, \ldots k$, *tak*

$$a_1 + \cdots + a_k \equiv b_1 + \cdots + b_k \pmod{n},$$
$$a_1 \ldots a_k \equiv b_1 \ldots b_k \pmod{n}.$$

Sčitovanie a násobenie kongruencií

Dôsledok

Ak $a \equiv b \pmod{n}$ *pre nejaké* $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, *tak platí pre všetky* $k \in \mathbb{N}$ *aj kongruencia*

$$a^k \equiv b^k \pmod{n}.$$

Ak f *je polynóm s celočíselnými koeficientmi, tak*

$$f(a) \equiv f(b) \pmod{n}.$$

Fermatove číslo F_5

$$641 \mid F_5 = 2^{32} + 1$$

$$2^{32} + 1 \equiv 0 \pmod{641}$$
$$2^{32} \equiv -1 \pmod{641}$$

Fermatove číslo F_5

$$641 = 625 + 16 = 5^4 + 2^4$$
$$641 = 640 \cdot 10 + 1 = 5 \cdot 2^7 + 1$$

Prvú rovnosť vynásobíme číslom 2^{28}. Pri druhej rovnosti využijeme $n + 1 \mid n^4 - 1$.

$$641 \mid 5^4 \cdot 2^{28} + 2^{32}$$
$$641 \mid 5^4 \cdot 2^{28} - 1$$

Potom 641 delí aj rozdiel týchto dvoch čísel, t.j.

$$641 \mid 2^{32} + 1 = F_5.$$

Mersennove číslo M_{11}

$$23 \mid M_{11} = 2^{11} - 1$$

$$2^{11} \equiv 1 \pmod{23}$$

Krátenie v kongruenciách

Veta

Ak $(m, n) = 1$, *tak existuje* $u \in \mathbb{Z}$ *také, že* $um \equiv 1 \pmod{n}$.
Ak $(m, n) = 1$, *tak pre ľubovoľné celé čísla* k, l *platí implikácia* $km \equiv lm \pmod{n} \Rightarrow k \equiv l \pmod{n}$.

Redukované zvyškové triedy

Definícia

Zvyškovú triedu modulo n nazveme *redukovanou*, ak každý jej prvok je nesúdeliteľný s číslom n.

Veta

Množina všetkých redukovaných zvyškových tried modulo n tvorí grupu vzhľadom na násobenie.

Krátenie v kongruenciách

Veta

Ak $ac \equiv bc \pmod{n}$ *a* $d = (n, c)$, *tak* $a \equiv b \pmod{\frac{n}{d}}$.

Ďalšie vlastnosti

Tvrdenie

Ak $a \equiv b \pmod{n}$ *a* $m \mid n$, *tak platí* $a \equiv b \pmod{m}$.
Ak $a \equiv b \pmod{n}$ *a* $a \equiv b \pmod{m}$, *kde* m *a* n *sú nesúdeliteľné, teda* $(m, n) = 1$, *tak* $a \equiv b \pmod{mn}$.

Dôsledok

Ak platí $a \equiv b \pmod{m_i}$, *pričom* m_i, $i = 1, 2, \ldots, n$, *sú po dvoch nesúdeliteľné, tak platí aj* $a \equiv b \pmod{m}$, *kde* $m = m_1 \ldots m_n$.

Rád prvku v grupe

Propozícia

Nech G je konečná komutatívna grupa, $|G| = n$. Neutrálny prvok tejto grupy označme e a jej prvky označme ako $a_1, \ldots, a_n$ (t.j. $G = \{a_1, \ldots, a_n\}$). Ukážte, že pre ľubovoľné $a \in G$ platí:

- $G = \{aa_1, \ldots, aa_n\}$;
- $a^n = e$.

Rád prvku v grupe

$$a^n = e$$

- Stručne: Rád prvku delí počet prvkov grupy.
- Argument použitý vyššie na zdôvodnenie $a^n = e$ využíva komutatívnosť.
- Platí aj pre nekomutatívne grupy – dôsledok Lagrangeovej vety.

Mersennove čísla

Tvrdenie

Nech p, q sú prvočísla a $q \mid M_p = 2^p - 1$. Potom $p \mid q - 1$.

Fermatove čísla

Veta (Euler)

Ak p je prvočíslo a $p \mid F_m$, tak p je tvaru $p = k2^{m+1} + 1$ pre nejaké $k \in \mathbb{N}$.

Kongruencie v grupách

Relácia ekvivalencie $\equiv$ na grupe $(G, *)$ je (grupová) kongruencia ak

$$a \equiv a', b \equiv b' \Rightarrow a * b \equiv a' * b'.$$

Rôzne pohľady na faktorové grupy:

- Kongruencie
- Normálne podgrupy
- Jadrá homomorfizmov

Kongruencie v okruhoch

Relácia ekvivalencie $\equiv$ na okruhu $(R, +, \cdot)$ je (okruhová) kongruencia ak z $a \equiv a'$ a $b \equiv b'$ vyplýva

$$a + b \equiv a' + b'$$
$$a \cdot b \equiv a' \cdot b'$$

Rôzne pohľady na faktorové okruhy:

- Kongruencie
- Ideály
- Jadrá homomorfizmov

Lineárne kongruencie

Veta

Kongruencia

$$ax \equiv b \pmod{n} \tag{1}$$

má riešenie práve vtedy keď $d \mid b$, *kde* $d = (a, n)$.
Navyše, ak kongruencia (1) má riešenie, tak počet (navzájom nekongruentných) riešení je d. *Ak* x_0 *je ľubovoľné riešenie* (1), *tak všetky riešenia tejto kongruencie sú tvaru* $x_0 + \frac{kn}{d}$.

Lineárne kongruencie

$$34x \equiv 60 \pmod{98}$$

Riešenia:

$$x \equiv -4 \pmod{98}$$
$$x \equiv 45 \pmod{98}$$

Čínska veta o zvyškoch

Veta (Čínska veta o zvyškoch)

Nech $m_1, \ldots, m_n$ sú po dvoch nesúdeliteľné čísla. Nech $b_1, \ldots, b_n \in \mathbb{Z}$. Potom systém kongruencií

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

má práve jedno riešenie modulo $m_1 \ldots m_n$ (čiže existuje práve jedno $x \in \{0, 1, \ldots, m_1 \ldots m_n - 1\}$ spĺňajúce všetky uvedené kongruencie).

Čínska veta o zvyškoch

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 6 \pmod 7$$

Čínska veta o zvyškoch

Veta

Nech $m_1, \ldots, m_n$ *sú po dvoch nesúdeliteľné čísla. Nech* $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ *a pre každé* $k = 1, 2, \ldots, n$ *platí* $(a_k, m_k) = 1$. *Potom systém kongruencií*

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}$$

má práve jedno riešenie modulo $m_1 \ldots m_n$.

Čínska veta o zvyškoch

Veta

Nech $f(x)$ je polynóm s celočíselnými koeficientmi. Nech $m_1, \ldots, m_r \in \mathbb{N}$ sú po dvoch nesúdeliteľné a nech $M = m_1 \ldots m_r$. Potom kongruencia

$$f(x) \equiv 0 \pmod{M} \tag{2}$$

má riešenie práve vtedy, keď každá z kongruencií

$$f(x) \equiv 0 \pmod{m_k}, \qquad k = 1, \ldots, r \tag{3}$$

má riešenie. Ak $v(m_k)$ označuje počet riešení kongruencie (3), tak

$$v(M) = v(m_1)v(m_2)\ldots v(m_k)$$

je počet riešení kongruencie (2).