Diskrétní matematika – 2. týden
Elementární teorie čísel – kongruence

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

podzim 2020

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant
Matematika drsně a svižně, *e*-text na
`www.math.muni.cz/Matematika_drsne_svizne`.

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant
Matematika drsně a svižně, *e*-text na
`www.math.muni.cz/Matematika_drsne_svizne`.
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2012/M6520/um/main-print.pdf`
- Jiří Herman, Radan Kučera, Jaromír Šimša, **Metody řešení matematických úloh**. MU Brno, 2001.
- William Stein, **Elementary Number Theory: Primes, Congruences, and Secrets**, Springer, 2008. Dostupné na
`http://wstein.org/ent/ent.pdf`
- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**,
`http://www.math.muni.cz/~kucera/texty/ATC10.pdf`

Plán přednášky

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Definice

Jestliže dvě celá čísla a, b mají při dělení přirozeným číslem m týž zbytek r, kde $0 \le r < m$, nazývají se a, b *kongruentní modulo* m (též *kongruentní podle modulu* m), což zapisujeme takto:

$$\underline{a \equiv b} \pmod{m}.$$

← stejný zb. po dělení m

V opačném případě řekneme, že a, b nejsou kongruentní modulo m, a píšeme

$$a \not\equiv b \pmod{m}.$$

mod 5

$0 \pmod 5 = 5 \pmod 5$

⋮	0	5	10
⋮	1	6	11
−3	2	7	⋮
−2	3	8	⋮
−1	4	9	

navzájem kongr.

zbytková třída

Lemma

Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ *jsou následující podmínky ekvivalentní:*

1. $a \equiv b \pmod{m}$,
2. $a = b + mt$ pro vhodné $t \in \mathbb{Z}$,
3. $m \mid a - b$.

liší se o násobek m

Základní vlastnosti kongruencí

Přímo z definice plyne:

- $a \equiv a \pmod{m}$, tj. kongruence podle modulu m je *reflexivní*,
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$, tj. kongruence podle modulu m je *symetrická*,
- $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$, tj. kongruence podle modulu m je *tranzitivní*.

Jedná se tedy o *ekvivalenci*, jejíž třídy budeme nazývat *zbytkové třídy* modulo m.

$a \pmod{m} = \{ b \in \mathbb{Z} \mid a \equiv b \pmod{m} \}$
$= \{ \dots, a-m, a, a+m, \dots \}$

Základní vlastnosti kongruencí

Přímo z definice plyne:

- $a \equiv a \pmod{m}$, tj. kongruence podle modulu m je *reflexivní*,
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$, tj. kongruence podle modulu m je *symetrická*,
- $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$, tj. kongruence podle modulu m je *tranzitivní*.

Jedná se tedy o *ekvivalenci*, jejíž třídy budeme nazývat *zbytkové třídy* modulo m.

Dokážeme nyní další vlastnosti:

Př. $m=2$ ... sudá vs lichá čísla

- K libovolné straně můžeme přičíst libovolný násobek modulu:

$$\underline{a \equiv b} \pmod{m} \quad \Rightarrow \quad a \equiv b + k \cdot m \pmod{m}.$$

$-3 \equiv 2 \pmod{5}$

- Kongruence podle téhož modulu můžeme *sčítat*, tedy i *vynásobit týmž číslem*:

$m \mid b_1 - a_1$, $m \mid b_2 - a_2$

$m \mid (b_1 + b_2) - (a_1 + a_2)$

$$\begin{array}{ll} a_1 \equiv b_1 \pmod{m}, & \\ a_2 \equiv b_2 \pmod{m} & \Rightarrow \quad a_1 + a_2 \equiv b_1 + b_2 \pmod{m}. \\ a \equiv b \pmod{m} & \Rightarrow \quad k \cdot a \equiv k \cdot b \pmod{m}. \end{array}$$

součet kongruence   k kopií $a \equiv b$

- Kongruence podle téhož modulu můžeme *sčítat*, tedy i *vynásobit týmž číslem*:

$$\begin{aligned} a_1 &\equiv b_1 \pmod{m}, \\ a_2 &\equiv b_2 \pmod{m} \end{aligned} \quad \Rightarrow \quad a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$

$$a \equiv b \pmod{m} \quad \Rightarrow \quad k \cdot a \equiv k \cdot b \pmod{m}.$$

- Kongruence podle téhož modulu můžeme *násobit*, tedy i *umocnit na totéž číslo*.

$m \mid b_1 - a_1$, $m \mid b_2 - a_2$ $\Rightarrow$ $m \mid b_1(b_2 - a_2) + (b_1 - a_1)a_2$

tj. $m \mid b_1 b_2 - a_1 a_2$

$$\begin{aligned} a_1 &\equiv b_1 \pmod{m}, \\ a_2 &\equiv b_2 \pmod{m} \end{aligned} \quad \Rightarrow \quad a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

$$a \equiv b \pmod{m} \quad \Rightarrow \quad a^k \equiv b^k \pmod{m}.$$

vynásobíme k kopií

- Kongruence podle téhož modulu můžeme *sčítat*, tedy i *vynásobit týmž číslem*:

$$\begin{aligned} a_1 &\equiv b_1 \pmod{m}, \\ a_2 &\equiv b_2 \pmod{m} \end{aligned} \quad \Rightarrow \quad a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$

$$a \equiv b \pmod{m} \quad \Rightarrow \quad k \cdot a \equiv k \cdot b \pmod{m}.$$

obecně pouze implikace

- Kongruence podle téhož modulu můžeme *násobit*, tedy i *umocnit na totéž číslo*.

$$\begin{aligned} a_1 &\equiv b_1 \pmod{m}, \\ a_2 &\equiv b_2 \pmod{m} \end{aligned} \quad \Rightarrow \quad a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

$$a \equiv b \pmod{m} \quad \Rightarrow \quad a^k \equiv b^k \pmod{m}.$$

- Obě strany kongruence můžeme vydělit číslem k, jestliže je nesoudělné s modulem.

$$k \cdot a \equiv k \cdot b \pmod{m}, \quad \boxed{(k, m) = 1} \quad \Rightarrow \quad a \equiv b \pmod{m}.$$

$\underbrace{2 \cdot 0}_{0} \equiv \underbrace{2 \cdot 2}_{4} \pmod 4 \quad \not\Rightarrow \quad 0 \equiv 2 \pmod 4$

$k \cdot a \equiv k \cdot b \pmod m$

$m \mid kb - k \cdot a = k \cdot (b-a)$

protože $(m,k) = 1 \Rightarrow m \mid b-a$

tj. $a \equiv b \pmod m$

- Jestliže $n \mid m$, pak

$n \mid m \mid b - a$

$$a \equiv b \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{n}.$$

Naopak pokud $a \equiv b \pmod{n}$, dostáváme $m/n = k$ možných řešení

$$a \equiv b,\ a \equiv b + n,\ \ldots,\ \text{nebo } a \equiv b + (k-1)n \pmod{m}.$$

$a \equiv 1 \pmod{10} \Rightarrow a \equiv 01, 11, \ldots, 91 \pmod{100}$

↳ a má posl. cifru 1

$a = 10 \cdot k + 1$ $a = 100\ell + 01$

$\underbrace{- - -}_{\text{cif. zápis } k} 1$ $\underbrace{- - -}_{\text{cif zápis } \ell} 01$

kx se zopakují všechny zb. mod n

$$\underbrace{\underbrace{0\ 1\ \dots\ n-1}_{\text{zbytky mod } n}\quad \underbrace{n\ (n+1)\ 1-7\ 2n-1}_{\text{ty samé zbytky mod } n}\quad \dots\quad \underbrace{(k-1)n\ \dots\ kn-1}_{\%}}_{\text{zbytky modulo } m}$$

- Jestliže $n \mid m$, pak

$$a \equiv b \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{n}.$$

Naopak pokud $a \equiv b \pmod{n}$, dostáváme $m/n = k$ možných řešení

$$a \equiv b,\ a \equiv b+n,\ \dots,\ \text{nebo}\ a \equiv b+(k-1)n \pmod{m}.$$

$100 = [4, 25]$

- Jestliže $m = [m_1, m_2]$ je nejmenší společný násobek, pak

$$a \equiv b \pmod{\overset{4}{m_1}},\ a \equiv b \pmod{\overset{25}{m_2}} \Leftrightarrow a \equiv b \pmod{\overset{100}{m}}.$$

$m_1 \mid b-a \;,\; m_2 \mid b-a \Rightarrow [m_1, m_2] \mid b-a$

- Jestliže $n \mid m$, pak

$$a \equiv b \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{n}.$$

Naopak pokud $a \equiv b \pmod{n}$, dostáváme $m/n = k$ možných řešení

$$a \equiv b,\ a \equiv b + n,\ \dots,\ \text{nebo } a \equiv b + (k-1)n \pmod{m}.$$

- Jestliže $m = [m_1, m_2]$ je nejmenší společný násobek, pak

$$a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2} \ \Leftrightarrow \ a \equiv b \pmod{m}.$$

- *Obě strany* kongruence *a modul* lze vynásobit nebo vydělit libovolným číslem

$m \mid b-a \iff k \cdot m \mid k \cdot (b-a)$

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad k \cdot a \equiv k \cdot b \pmod{\underline{k} \cdot m}.$$

Poznámka

Některé vlastnosti kongruencí jsme již používali, aniž bychom si toho povšimli – například příklad z minulého týdne lze přeformulovat do tvaru a,b dávají zb. 1

$$a \equiv 1 \pmod{m},\ b \equiv 1 \pmod{m} \quad \Rightarrow \quad ab \equiv 1 \pmod{m},$$

což je speciální případ zpředhozího tvrzení.

vždy

$a \equiv 2$, $b \equiv 2$ $\Longrightarrow$ $a \cdot b \equiv 4$

a dává zb. 2 , b taky $\Longrightarrow$ $a \cdot b$ dává zb. 4

skoro vždy

$m = 3$ neplatí $a \cdot b \equiv 4 \equiv \underline{\underline{1}}$

Poznámka

Některé vlastnosti kongruencí jsme již používali, aniž bychom si toho povšimli – například příklad z minulého týdne lze přeformulovat do tvaru

$$a \equiv 1 \pmod m,\ b \equiv 1 \pmod m \quad \Rightarrow \quad ab \equiv 1 \pmod m,$$

což je speciální případ zpředhozího tvrzení.
Nejde o náhodu. Libovolné tvrzení používající kongruence můžeme snadno přepsat pomocí dělitelnosti. Užitečnost kongruencí tedy netkví v tom, že bychom pomocí nich mohli řešit úlohy, které bez nich řešit nejsme schopni, ale v tom, že jde o velmi vhodný způsob zápisu. Osvojíme-li si ho, výrazně tím zjednodušíme jak vyjadřování, tak i některé úvahy. Je to typický jev: v matematice hraje vhodná symbolika velmi závažnou úlohu.

$m \mid a \iff a \equiv 0 \pmod m$

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

$5^{20} \equiv\ ? \pmod{26}$

Vlastnosti mocnin

$\to 5^2 \equiv 25 \equiv -1$

$\to 5^4 \equiv (5^2)^2 \equiv (-1)^2 \equiv 1$

$5^{20} \equiv (5^4)^5 \equiv 1^5 \equiv 1$

$\leadsto$ 5^{20} dává zb. 1 po dělení 26

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Příklad

Dokažte, že pro libovolné prvočíslo p a libovolná $a, b \in \mathbb{Z}$ platí

$$a^p + b^p \equiv (a+b)^p \pmod{p}.$$

Př. $p=2$ $(a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \pmod 2$

$p=3$ $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \equiv a^3 + b^3 \pmod 3$

$3a^2b \equiv 0$, $3ab^2 \equiv 0$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1

$$(a+b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1} b + \dots + \binom{p}{k} a^{p-k} b^k + \dots}_{} + b^p \equiv a^p + b^p \pmod p$$

chceme pro $k = 1, \dots, p-1$: $\underbrace{\binom{p}{k} \equiv 0 \pmod p}_{\text{tj. } p \mid \binom{p}{k}}$

$$\binom{p}{k} = \frac{\overbrace{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}^{k \text{ činitelů}}}{\underbrace{k \cdot (k-1) \cdot \ldots \cdot 1}_{k \text{ činitelů}}}$$

$\frac{(p-1) \cdot \ldots \cdot (p-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1} \in \mathbb{Z}$

nejsou děl. p protože $< p$

$= p \cdot (\text{celé číslo})$

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Příklad

Dokažte, že pro libovolné prvočíslo p a libovolná $a, b \in \mathbb{Z}$ platí

$$a^p + b^p \equiv (a+b)^p \pmod{p}.$$

Příklad

Najděte "inverzi" k číslu 39 modulo 47, tj. najděte x takové, že $39 \cdot x \equiv 1 \pmod{47}$.

$39 \cdot x \equiv 1 \pmod{47}$

nesoudělnost

využijeme $(47, 39) = 1$

47	39	
1	0	47
0	1	39
1	-1	8
-4	5	7
~~5~~	-6	1

zbytečné

$\underline{5} \cdot 47 - 6 \cdot 39 = 1$

$\downarrow \pmod{47}$

$-6 \cdot 39 \equiv 1 \pmod{47}$

$\Rightarrow$ $x = -6$ je řešení

Inverze modulo m

Věta

Je-li a nesoudělné s modulem m, tj. $(a, m) = 1$, pak existuje řešení

$$a \cdot x \equiv 1 \pmod{m}.$$

Toto řešení značíme $x \equiv a^{-1}$ a nazýváme inverzí k a modulo m. Jakožto zbytková třída je toto řešení jediné.

motivace: chceme řešit $a \cdot x \equiv b \pmod{m}$

→ vydělení a

= vynásobení $\frac{1}{a} \notin \mathbb{Z}$

$a \cdot \frac{1}{a} = 1$

Inverze modulo m

Věta

Je-li a nesoudělné s modulem m, tj. $(a, m) = 1$, *pak existuje řešení*

$$a \cdot x \equiv 1 \pmod{m}.$$

Toto řešení značíme $x \equiv a^{-1}$ *a nazýváme inverzí k a modulo m. Jakožto zbytková třída je toto řešení jediné.*

Důkaz.

Zobrazení $x \pmod{m} \mapsto a \cdot x \pmod{m}$ na zbytkových třídách je injektivní (vlastnost dělení); protože je zbytkových tříd na obsou stranách stejně, totiž m, jedná se o bijekci a jednička $1 \pmod{m}$ má jediný vzor. $\square$

$a \cdot x \equiv a \cdot y \Rightarrow x \equiv y$

$(a, m) = 1$

$x \longmapsto a \cdot x$

$\not\equiv \qquad \not\equiv$

$y \longmapsto a \cdot y$

$\underline{k=2}$ $\rightarrow$ $2^{-1} \equiv 3 \quad (5)$

$$\begin{array}{lcl} 0 \pmod 5 & \xmapsto{2x} & 0 \\ 1 \pmod 5 & \mapsto & 2 \\ 2 \quad (5) & \mapsto & 4 \\ \underline{3 \quad (5)} & \mapsto & 1 \\ 4 \quad (5) & \mapsto & 3 \end{array}$$

! násobení 2 je bijekce na zb. třídách

$\Rightarrow$ 1 leží v obraze

Věta

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. *Označme* $d = (a, m)$. *Pak kongruence*

$$a \cdot x \equiv b \pmod{m}$$

nejjedn. $d=1$

(o jedné neznámé x*) má řešení právě tehdy, když* $d \mid b$.
Pokud platí $d \mid b$, *má tato kongruence právě* d *řešení (modulo* m*).*

Věta

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. *Označme* $d = (a, m)$. *Pak kongruence*

$$a \cdot x \equiv b \pmod{m}$$

$a \equiv a' \leftarrow a' = a + t \cdot m$

$(a, m) = (a', m)$

(o jedné neznámé x) má řešení právě tehdy, když $d \mid b$.
Pokud platí $d \mid b$, *má tato kongruence právě d řešení (modulo m).*

Důkaz.

Dokážeme nejprve, že uvedená podmínka je nutná:

$$d \mid \underline{(a \cdot x, m)} = \underline{(b, m)} \mid \underline{b}.$$

Dokončení důkazu.

Prvně předpokládejme $d = 1$. Pak inverze $a^{-1} \pmod{m}$ existuje a vynásobením rovnice

$$a \cdot x \equiv b \pmod{m}$$

touto inverzí dostaneme hledané řešení

$a^{-1} x$

$$x \equiv a^{-1} \cdot b \pmod{m}.$$

Dokončení důkazu.

Prvně předpokládejme $d = 1$. Pak inverze $a^{-1} \pmod{m}$ existuje a vynásobením rovnice

$$a \cdot x \equiv b \pmod{m}$$

touto inverzí dostaneme hledané řešení

$$x \equiv a^{-1} \cdot b \pmod{m}.$$

$d \neq 1$ — d dělí m, a, b

Obecně prvně obě strany i modul vydělíme největším společným dělitelem d, dostaneme při označení $a' = a/d$, $b' = b/d$, $m' = m/d$ ekvivalentní rovnici

$$a' \cdot x \equiv b' \pmod{m'} \to x \equiv (a')^{-1} \cdot b' \pmod{m'}$$

kde již $(a', m') = 1$ a postupujeme podle první části. $\square$

Algoritmus

Začneme s ekvivalentní soustavou dvou kongruencí

$$\underline{m \cdot x \equiv 0 \pmod{m}}$$ – platí pro jakékoliv x
$$\underline{a \cdot x \equiv b \pmod{m}}$$

a vždy první rovnici systému nahradíme rovnicí vzniklou odečtením vhodného násobku druhé rovnice (tak abychom koeficient m nahradili jeho zbytkem po dělení číslem a),

Algoritmus

Začneme s ekvivalentní soustavou dvou kongruencí

$$m \cdot x \equiv 0 \pmod{m}$$
$$a \cdot x \equiv b \pmod{m}$$

a vždy první rovnici systému nahradíme rovnicí vzniklou odečtením vhodného násobku druhé rovnice (tak abychom koeficient m nahradili jeho zbytkem po dělení číslem a), dokud nedostaneme koeficienty d a 0:

$$d \cdot x \equiv b' \pmod{m}$$
$$0 \cdot x \equiv c \pmod{m}$$

Algoritmus

Začneme s ekvivalentní soustavou dvou kongruencí

$$\begin{aligned} m \cdot x &\equiv 0 \pmod{m} \\ a \cdot x &\equiv b \pmod{m} \end{aligned}$$

a vždy první rovnici systému nahradíme rovnicí vzniklou odečtením vhodného násobku druhé rovnice (tak abychom koeficient m nahradili jeho zbytkem po dělení číslem a), dokud nedostaneme koeficienty d a 0:

$$\begin{aligned} \underline{d \cdot x} &\equiv b' \pmod{m} \\ \underline{0 \cdot x} &\equiv c \pmod{m} \end{aligned}$$

Máme dvě možnosti:

- $c \equiv 0$ a soustava, a tedy i původní rovnice, má řešení vzniklé z první rovnice vydělením d, totiž: $x \equiv b'/d \pmod{m/d}$;
- $c \not\equiv 0$ a soustava, a tedy i původní rovnice, nemá řešení.

Příklad

Řešte $39x \equiv 41 \pmod{47}$ $\quad 39^{-1} \equiv -6 \longrightarrow$

$$47x \equiv 0$$
$$39x \equiv 41 \quad \big\downarrow -1\cdot x$$
$$8x \equiv -41 \equiv 6 \quad \big\downarrow -4x$$
$$7x \equiv 17 \quad \big\downarrow -1x$$
$$1\cdot x \equiv -58 \equiv -11 \quad \big\downarrow -7x$$

$\longleftarrow$ vydělit 2 ?

$$0x \equiv 94 \equiv 0 \quad \checkmark$$

má řešení!

vydělíme koef. u x

$$x \equiv -11 \pmod{47}$$

$4x \equiv 1 \pmod{8}$

$8x \equiv 0$

$4x \equiv 1$

$0x \equiv -2 \Rightarrow$ nemá řešení

$4x \equiv 1 \pmod{10}$

$10x \equiv 0$

$4x \equiv 1$

$2x \equiv -2 \pmod{10} \not\Rightarrow x \equiv -1 \pmod{5}$

$0x \equiv 5 \Rightarrow$ nemá řešení

Příklad

Řešte $39x \equiv 41 \pmod{47}$

Poznámka

Teoretický, i když ne příliš praktický postup, pro jednoduchost v případě $(a, m) = 1$: z Bezoutovy věty dostaneme $ka + lm = 1$, použijeme

$$a \cdot x \equiv b = (ka + lm)b \equiv kab \pmod{m}$$

a vydělíme a, takže $x \equiv kb \pmod{m}$. (Zbytečně počítáme koeficient l.)

Wilsonova věta

Pomocí věty o řešitelnosti lineárních kongruencí lze dokázat mj. významnou Wilsonovu větu udávající nutnou (i postačující) podmínku prvočíselnosti. Takové podmínky jsou velmi významné ve výpočetní teorii čísel, kdy je třeba efektivně poznat, je-li dané velké číslo prvočíslem. Bohužel dosud není známo, jak rychle vypočítat modulární faktoriál velkého čísla, proto není v praxi Wilsonova věta k tomuto účelu používána.

Wilsonova věta

Pomocí věty o řešitelnosti lineárních kongruencí lze dokázat mj. významnou Wilsonovu větu udávající nutnou (i postačující) podmínku prvočíselnosti. Takové podmínky jsou velmi významné ve výpočetní teorii čísel, kdy je třeba efektivně poznat, je-li dané velké číslo prvočíslem. Bohužel dosud není známo, jak rychle vypočítat modulární faktoriál velkého čísla, proto není v praxi Wilsonova věta k tomuto účelu používána.

Věta (Wilsonova)

Přirozené číslo $n > 1$ je prvočíslo, právě když

počítá se těžko i modulo n

$$(n-1)! \equiv -1 \pmod{n}$$

Vcelku přímočarý důkaz je v učebnici.

n prvočíslo

$\Updownarrow$

$(n-1)! \equiv -1 \pmod{n}$

n není prvočíslo $\quad a \mid n \Rightarrow a \mid (n-1)!$

n je prvočíslo

$((n-1)!, n) \neq 1$

$(-1, n) = 1$

napr. $n = 7$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ $\quad 2^{-1} \equiv 4 \ (7)$

$\equiv$

$\equiv 1 \cdot 2 \cdot 3 \cdot 2^{-1} \cdot 3^{-1} \cdot (-1)$ $\quad 3^{-1} \equiv 5 \ (7)$

$\equiv \qquad \equiv$

$x \cdot x \equiv 1 \iff x^2 - 1 \equiv 0 \iff (x-1)(x+1) \equiv 0$

Plán přednášky

Soustavy lineárních kongruencí

$ax \equiv b \rightarrow x \equiv c$

Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle předchozí věty rozhodnout o řešitelnosti každé z nich.
V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$.

Soustavy lineárních kongruencí

Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle předchozí věty rozhodnout o řešitelnosti každé z nich. V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$. Dostaneme tak soustavu kongruencí

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

Soustavy lineárních kongruencí

Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle předchozí věty rozhodnout o řešitelnosti každé z nich.
V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$. Dostaneme tak soustavu kongruencí

$$
\begin{aligned}
x &\equiv c_1 \pmod{m_1}\\
&\ \vdots\\
x &\equiv c_k \pmod{m_k}
\end{aligned}
$$

$$\left.\begin{aligned} x &\equiv c_1 \ (m_1)\\ x &\equiv c_2 \ (m_2)\end{aligned}\right\} x \equiv c_{12} \ (m_{12})$$

$$x \equiv c_3 \ (m_3)$$

Zřejmě stačí vyřešit případ $k = 2$, řešení soustavy více kongruencí snadno obdržíme opakovaným řešením soustav dvou kongruencí.

Věta

Nechť c_1, c_2 *jsou celá čísla,* m_1, m_2 *přirozená. Označme* $d = (m_1, m_2)$ *a* $m = [m_1, m_2]$*. Soustava dvou kongruencí*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

v případě $c_1 \not\equiv c_2 \pmod{d}$ *nemá řešení. Jestliže naopak* $c_1 \equiv c_2 \pmod{d}$*, pak existuje celé číslo* c *tak, že* $x \in \mathbb{Z}$ *vyhovuje soustavě, právě když vyhovuje kongruenci*

$$x \equiv c \pmod{m}.$$

Věta

Nechť c_1, c_2 jsou celá čísla, m_1, m_2 přirozená. Označme $d = (m_1, m_2)$ a $m = [m_1, m_2]$. Soustava dvou kongruencí

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

v případě $c_1 \not\equiv c_2 \pmod{d}$ nemá řešení. Jestliže naopak $c_1 \equiv c_2 \pmod{d}$, pak existuje celé číslo c tak, že $x \in \mathbb{Z}$ vyhovuje soustavě, právě když vyhovuje kongruenci

$$x \equiv c \pmod{m}.$$

Důkaz.

Má-li soustava nějaké řešení $x \in \mathbb{Z}$, platí nutně $x \equiv c_1 \pmod{d}$, $x \equiv c_2 \pmod{d}$, a tedy i $c_1 \equiv c_2 \pmod{d}$. Odtud plyne, že v případě $c_1 \not\equiv c_2 \pmod{d}$ soustava nemůže mít řešení.

Dokončení důkazu.

Uvažujme zobrazení

$\{$zb. tř. mod $m\} \to \{$zb. tř. mod $m_1\} \times \{$zb. tř. mod $m_2\}$

$$c \pmod{m} \mapsto (c \pmod{m_1}, c \pmod{m_2}),$$

které zbytkové třídě modulo m přiřadí dvojici odpovídajících zbytkových tříd modulo m_1, m_2. Toto zobrazení je injektivní (viz vlastnosti kongruencí).

$$c \equiv c' \pmod{m} \Leftarrow c \equiv c' \pmod{m_1} \quad c \equiv c' \pmod{m_2}$$

Dokončení důkazu.

Uvažujme zobrazení $m = [m_1, m_2] = m_1 \cdot m_2$ prvků

m prvků

$$c \pmod m \mapsto (c \pmod{m_1}, c \pmod{m_2}),$$

které zbytkové třídě modulo m přiřadí dvojici odpovídajících zbytkových tříd modulo m_1, m_2. Toto zobrazení je injektivní (viz vlastnosti kongruencí).

Předpokládejme prvně $(m_1, m_2) = 1$, pak $m = m_1 m_2$ a na obou stranách máme stejný počet prvků, jedná se tedy o bijekci a dvojice (c_1, c_2) má jediný vzor – tím je zbytková třída $c \pmod m$ taková, že $c \equiv c_1 \pmod{m_1}$, $c \equiv c_2 \pmod{m_2}$, tedy řešení soustavy. $\square$

Dokončení důkazu.

Uvažujme zobrazení

$$c \pmod{m} \mapsto (c \pmod{m_1}, c \pmod{m_2}),$$

které zbytkové třídě modulo m přiřadí dvojici odpovídajících zbytkových tříd modulo m_1, m_2. Toto zobrazení je injektivní (viz vlastnosti kongruencí).

Dokončení důkazu.

Uvažujme zobrazení

$$c \pmod{m} \mapsto (c \pmod{m_1}, c \pmod{m_2}),$$

které zbytkové třídě modulo m přiřadí dvojici odpovídajících zbytkových tříd modulo m_1, m_2. Toto zobrazení je injektivní (viz vlastnosti kongruencí).

Nechť nyní d je libovolné. Počítejme dvojice tříd ze zadání, tj. takových, že $c_1 \equiv c_2 \pmod{d}$. Libovolné $c_1 \pmod{m_1}$ určuje $c_2 \pmod{d}$ a to odpovídá právě m_2/d třídám $c_2 \pmod{m_2}$. Dohromady tak je těchto dvojic $m_1 \cdot (m_2/d) = [m_1, m_2] = m$ a zobrazení je opět bijekce (jen jsme potřebovali zmenšit množinu napravo ze všech dvojic na ty "kompatibilní"). $\square$

Čínská zbytková věta (CRT)

Ve čtvrtém století se čínský matematik Sun Ze (Sun Tsu) ptal na číslo, které při dělení třemi dává zbytek 2, při dělení pěti zbytek 3 a při dělení sedmi je zbytek opět 2.

Důsledek (Čínská zbytková věta)

Nechť $m_1, , \dots, m_k \in \mathbb{N}$ jsou po dvou nesoudělná, $a_1, \dots, a_k \in \mathbb{Z}$. Pak platí: soustava

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

má jediné řešení modulo $m_1 \cdot m_2 \cdots m_k$.

Uvědomme si, že jde o docela silné tvrzení (které ve skutečnosti platí v podstatně obecnějších algebraických strukturách), umožňující nám při předepsání libovolných zbytků podle zvolených (po dvou nesoudělných) modulů garantovat, že existuje číslo s těmito předpsanými zbytky.

Algoritmus

Prvně obměna na algoritmus pro jednu rovnici: soustavu

$$
\begin{aligned}
x &\equiv c_1 \pmod{m_1} & / \cdot m_2 \\
x &\equiv c_2 \pmod{m_2} & / \cdot m_1
\end{aligned}
$$

přepíšeme na ekvivalentní

$$
\begin{aligned}
m_2 \cdot x &\equiv m_2 \cdot c_1 \pmod{m_1 m_2} \\
m_1 \cdot x &\equiv m_1 \cdot c_2 \pmod{m_1 m_2}
\end{aligned}
$$

a vyřešíme podobně jako předtím.

Algoritmus

Prvně obměna na algoritmus pro jednu rovnici: soustavu

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

$\Leftrightarrow x = m_1 \cdot t + c$

přepíšeme na ekvivalentní

$$\begin{aligned} m_2 \cdot x &\equiv m_2 \cdot c_1 \pmod{m_1 m_2} \\ m_1 \cdot x &\equiv m_1 \cdot c_2 \pmod{m_1 m_2} \end{aligned}$$

a vyřešíme podobně jako předtím.
O něco lepší bývá převedení první rovnice na "parametrický" tvar $x = m_1 \cdot t + c_1$, dosazení do druhé rovnice

$$m_1 \cdot t + c_1 \equiv c_2 \pmod{m_2},$$

dosadíme řešení

vyřešení vzhledem k t, dosazení do $x = m_1 \cdot t + c_1$ a převedení na "implicitní" tvar.

$$x = 90s + 41 = 90(5r+2) + 41 = 450r + 221 \iff \boxed{x \equiv 221 \pmod{450}}$$

Příklad

Řešte systém kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25}. \end{aligned}$$

$\to$ $x = 10t + 1$

$x = 10(9s+4) + 1$

$x = 90s + 41$

$10t + 1 \equiv 5 \quad (18)$

$10t \equiv 4 \quad (18)$

$18t \equiv 0$

$10t \equiv 4$

$8t \equiv -4$

$2t \equiv 8 \quad (18) \longrightarrow t \equiv 4 \quad (9) \longrightarrow t = 9s + 4$

$0t \equiv -36 \equiv 0$ ok

$90s + 41 \equiv -4 \quad (25)$

$25s \equiv 0$

$15s \equiv 5 \quad (25)$

$10s \equiv -5$

$5s \equiv 10 \quad (25) \to s \equiv 2 \ (5)$

$0s \equiv -25 \equiv 0$ ok

$s = 5r + 2$

Příklad

Řešte systém kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25}. \end{aligned}$$

Řešení

Výsledkem je $x \equiv 221 \pmod{450}$.

Čínskou zbytkovou větu můžeme použít také „v opačném směru“.

Příklad

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

$3564 = 4 \cdot 81 \cdot 11$

vyřešíme mod 4, 81, 11 zvlášť $\to$ CRT

$$\boxed{x \equiv 3 \ (4)}$$

$$\Longleftrightarrow \quad 46x \equiv 24 \ (81)$$

$$5x \equiv 2 \ (11)$$

$$\boxed{x \equiv -4 \ (11)}$$

$81x \equiv 0$

$46x \equiv 24$

$35x \equiv -24$

$11x \equiv 48$

$2x \equiv -168 \equiv -6$

$$\boxed{x \equiv 78 \equiv -3 \ (81)}$$

$0x \equiv 0$ ✓

Čínskou zbytkovou větu můžeme použít také „v opačném směru“.

Příklad

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Řešení

Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a má tedy kongruence řešení. Protože $\varphi(3564) = 2 \cdot (3^3 \cdot 2) \cdot 10 = 1080$, je řešení tvaru $x \equiv 915 \cdot 23\,941^{1079} \pmod{3564}$. Úprava čísla stojícího na pravé straně by však vyžádala značné úsilí. Proto budeme kongruenci řešit poněkud jinak.

Řešení

Víme, že $x \in \mathbb{Z}$ řešením dané kongruence, právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11}. \end{aligned}$$

Řešení

Víme, že $x \in \mathbb{Z}$ řešením dané kongruence, právě když je řešením soustavy

$$
\begin{aligned}
23941x &\equiv 915 \pmod{2^2}\\
23941x &\equiv 915 \pmod{3^4}\\
23941x &\equiv 915 \pmod{11}.
\end{aligned}
$$

Vyřešíme-li postupně každou z kongruencí soustavy, dostaneme ekvivalentní soustavu

$$
\begin{aligned}
x &\equiv 3 \pmod{4}\\
x &\equiv -3 \pmod{81}\\
x &\equiv -4 \pmod{11},
\end{aligned}
$$

Řešení

Víme, že $x \in \mathbb{Z}$ řešením dané kongruence, právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11}. \end{aligned}$$

Vyřešíme-li postupně každou z kongruencí soustavy, dostaneme ekvivalentní soustavu

$x = 4t + 3$

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv -3 \pmod{81} \\ x &\equiv -4 \pmod{11}, \end{aligned}$$

$4t + 3 \equiv -3$

$4t \equiv -6$

$t \equiv 120 \equiv 39 \; (81)$

$t = 81s + 39$

odkud snadno postupem pro řešení soustav kongruencí dostaneme $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence.

Modulární reprezentace čísel

Při počítání s velkými čísly je někdy výhodnější než s dekadickým či binárním zápisem čísel pracovat s tzv. *modulární reprezentací* (též *residue number system*), která umožňuje snadnou paralelizaci výpočtů s velkými čísly. Takový systém je určen k-ticí modulů (obvykle po dvou nesoudělných) a každé číslo menší než jejich součin je pak jednoznačně reprezentováno k-ticí zbytků (jejichž hodnoty nepřevyšují příslušné moduly) – viz např. `http://goo.gl/oM25m`.

$3\cdot 5\cdot 7\cdot 11\cdot 13$

Příklad

Pětice modulů $3, 5, 7, 11, 13$ nám umožní jednoznačně reprezentovat čísla menší než $\boxed{15015}$ a efektivně provádět (v případě potřeby distribuované) běžné aritmetické operace. Vypočtěme např. součin čísel 1234 a 5678, v této modulární soustavě reprezentovaných péticemi $[1, 4, 2, 2, 12]$ a $[2, 3, 1, 2, 10]$.

Příklad

Pětice modulů $3, 5, 7, 11, 13$ nám umožní jednoznačně reprezentovat čísla menší než 15015 a efektivně provádět (v případě potřeby distribuovaně) běžné aritmetické operace. Vypočtěme např. součin čísel 1234 a 5678, v této modulární soustavě reprezentovaných pěticemi $[1, 4, 2, 2, 12]$ a $[2, 3, 1, 2, 10]$. Součin provedeme po složkách a dostaneme $[2, 2, 2, 4, 3]$, což na závěr pomocí CRT převedeme zpět na 9662, což je modulo 15015 totéž jako $1234 \cdot 5678$.