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.
- 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

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 $0 \leq r < m$, nazývají se a, b *kongruentní modulo* m (též *kongruentní podle modulu* m), což zapisujeme takto:

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

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

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

Lemma

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

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

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:

- K libovolné straně můžeme přičíst libovolný násobek modulu:

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

- 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*.

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

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

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

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

- 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

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

- 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

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

Poznámka

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

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

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.

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

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. $\square$

Věta

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

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

(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:

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

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

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

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

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

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

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:

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

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 $39x \equiv 41 \pmod{47}$

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.

Věta (Wilsonova)

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

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

Vcelku přímočarý důkaz je v učebnici.

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

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

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

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$

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

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

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. □

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

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$

přepíšeme na ekvivalentní

$$m_2 \cdot x \equiv m_2 \cdot c_1 \pmod{m_1 m_2}$$
$$m_1 \cdot x \equiv m_1 \cdot c_2 \pmod{m_1 m_2}$$

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

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

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

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

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

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

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

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

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`.

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 $1234 \cdot 5678$.