Diskrétní matematika

Petr Kovář
petr.kovar@vsb.cz

Vysoká škola báňská – Technická univerzita Ostrava

zimní semestr 2022/2023
DiM 470-2301/01, 470-2301/03*, 470-2301/05

O tomto souboru

Tento soubor je zamýšlen především jako pomůcka pro přednášejícího. Řadu důležitých informací v souboru nenajdete, protože přednášející je říká, ukazuje, případně maluje na tabuli. Přednášky jsou na webu k dispozici, aby studenti mohli snadno dohledat probíraná témata z přednášek, které zameškali.

Pro samostatné studium doporučuji skripta:

- M. Kubesa: Základy diskrétní matematiky, výukový text
- P. Kovář: Úvod do teorie grafů, výukový text

Pro přípravu ke zkoušce a písemkám doporučuji cvičebnici:

- P. Kovář: Cvičení z diskrétní matematiky, sbírka příkladů

Vše na http://homel.vsb.cz/~kov16/predmety_dm.php

Přehled přednášky

Kapitola 6. Kongruence a modulární aritmetika

- motivace
- dělení a dělitelnost
- relace kongruence
- modulární aritmetika
- lineární kongruence o jedné neznámé
- metody řešení
- příklady využití

6. Kongruence a modulární aritmetika

Moderní elektronická komunikace se neobejde bez kódování a kryptografie.

- kódování – uložení či přenos zpráv, kdy může dojít k nežádoucímu porušení dat a my přesto potřebujeme minimalizovat ztráty
- kryptografie – uložení či přenos zpráv, které nemají být přístupně třetím stranám

Stojí na výsledcích teorie čísel a teorie grup.

Příklady aplikací

- záznam CD, mp3
- telefonní hovory
- čárové kódy, ISBN
- RSA šifrování

Uvedeme mírný úvod do teorie čísel. Budeme počítat s celými čísly, zpravidla z omezené množiny čísel (8, 16, 32 bitů . . .).

Motivační příklady

Nejprve ukážeme, jak počítat „modulo n“ a budeme umět zodpovědět následující otázky:

Příklad

Zařízení přečetlo UPC čárový kód. Je 041331021641 platný UPC kód?

Příklad

Zapsali jsme si ISBN knihy 0-03-001559-5. Je to platný ISBN kód?

Později ukážeme, jak *některé* chyby nejen poznat, ale i opravit.

Příklad

Víme-li, že nejspíš čtvrtá cifra UPC kódu 041331021641 je chybná, jaká je správná cifra?

Příklad

Víme, že ISBN knihy 0-03-001559-5 je chybné. Víme, že při psaní často omylem prohazujeme sousední znaky. Podaří se zjistit správný ISBN kód?

Dělitelnost

Mějme dvě celá čísla a, b. Řekneme, že a dělí b, jestliže existuje takové celé číslo k, že $a \cdot k = b$, zapisujeme $a \mid b$.
V opačném případě říkáme, že a nedělí b, zapisujeme $a \nmid b$.
Číslu a říkáme dělitel čísla b a číslu b říkáme násobek čísla a.

Příklad

Platí $3 \mid 6, \quad 3 \mid 15$.
Dále platí $2 \mid -6, \quad 5 \mid -5 \quad$ a $\quad 7 \mid 0$.
Naproti tomu $6 \nmid 3, \quad 2 \nmid 5, \quad 4 \nmid -6, \quad 0 \nmid 1$.
Platí však $0 \mid 0$, neboť $0 = k0$, dokonce pro libovolné $k \in \mathbb{Z}$.
Nulou sice nemůžeme dělit, avšak nula může být dělitelem, byť je dělitelem pouze nuly.

Operace vs. relace

Dělení je operace $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$.
Výsledkem dělení jednoho libovolného čísla druhým nenulovým číslem je třetí číslo.

Příklad

Platí $18 : 3 = 6, \quad 0 : 7 = 0, \quad 18 : 4 = \frac{9}{2}$.

Dělitelnost je relace $| \subset \mathbb{Z} \times \mathbb{Z}$.
Dvě čísla (v daném pořadí) buď jsou v relaci – jedno je dělitelem druhého, nebo nejsou.

Příklad

3 dělí číslo 18.
7 dělí číslo 0.
4 nedělí číslo 18.

Vlastnosti dělitelnosti

Věta

Mějme celá čísla b, c a nenulové celé číslo a. Platí

- Jestliže $a \mid b$ a současně $a \mid c$, pak $a \mid (b + c)$.
- Jestliže $a \mid b$ pak $a \mid bc$ pro všechna celá čísla c.
- Jestliže $a \mid b$ a současně $b \mid c$, pak $a \mid c$.

Příklady

Protože $3 \mid 12$, tak $3 \mid 12c$ pro libovolné celé číslo c.
(ale nejen $12c$, také $12c + 3$, $12c + 6$ a $12c + 9$)

Důsledek

Mějme celá čísla b, c a nenulové celé číslo a. Jestliže $a \mid b$ a současně $a \mid c$, pak $a \mid rb + sc$ pro libovolná celá čísla r, s.

Věta o jednoznačnosti podílu a zbytku

Věta o jednoznačnosti podílu a zbytku

Pro každé celé číslo a a každé přirozené číslo b existují taková jednoznačně určená celá čísla q a r, kde $0 \leq r < b$, že $a = qb + r$.

Číslu q říkáme podíl a číslu r zbytek po dělení čísla a číslem b.

Příklad

Pro $a = 111$ a $b = 9$ platí:

$$\begin{aligned} 111 &= 11 \cdot 9 + 12 \\ 111 &= 12 \cdot 9 + 3 \quad \text{musí platit } 0 \leq r < 9 \\ 111 &= 13 \cdot 9 - 6 \end{aligned}$$

Příklad

Platí $7 \mid 21$, proto $21 = 3 \cdot 7 + 0$, zbytek $r = 0$.
Platí $8 \nmid 21$, proto $21 = 2 \cdot 8 + 5$, zbytek $r = 5 \neq 0$.

Dvě operace dělení se zbytkem

Podle Věty o dělení celých čísel se zbytkem můžeme každé dvojici jednoznačně přidělit celočíselný podíl a zbytek po celočíselném dělení.

Operace dělení se zbytkem

Mějme dvě celá čísla a, b.
V rovnosti $a = q \cdot b + r$ dané ve Větě o dělení celých čísel je číslo a dělencem, číslo b je dělitelem, číslo q je celočíselným podílem a číslo r je zbytkem po dělení čísla a číslem b.
Následující zápis vyjadřuje operace podílu a zbytku celočíselného dělení.

$$q = a \operatorname{div} b, \quad r = a \bmod b$$

Příklad

Pro $a = 111$ a $b = 9$ z předchozího příkladu platí:

$$111 \operatorname{div} 9 = 12, \qquad 111 \bmod 9 = 3$$

Pozor, „mod“ zapsané v závorce má jiný význam.

Kongruence

Mějme celá čísla a, b a přirozené číslo m. Řekneme, že čísla a, b jsou kongruentní modulo m, jestliže dávají stejný zbytek po dělení číslem m. Zapisujeme

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

V opačném případě píšeme

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

Formálně můžeme pomocí operace „mod“ zapsat

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a \bmod m = b \bmod m.$$

Příklad

Platí $7 \equiv 1 \pmod{2}$, protože číslo 7 je liché.
Platí $12 \equiv 0 \pmod{2}$, protože číslo 12 je sudé.
Platí $61\,725 \equiv 0 \pmod{3}$, protože 61 725 je násobek čísla 3.

Ekvivalentní formulace kongruence dvou čísel

Lemma

Mějme celá čísla a, b a přirozené číslo m. Potom $a \equiv b \pmod{m}$ právě tehdy, když $m \mid (b - a)$.

Příklad

Platí $8\,298 \equiv 8\,228 \pmod{7}$, protože rozdíl čísel $8\,298 - 8\,228 = 70$ je násobek 7.

Lemma

Mějme celá čísla a, b a přirozené číslo m. Potom $a \equiv b \pmod{m}$ právě tehdy, když existuje celé číslo k takové, že $b = a + km$.

Příklad

Určete $748\,549 \bmod 7$ (zbytek po dělení čísla 748 549 číslem 7).

Platí $748\,549 = 700\,000 + 48\,549 \equiv 48\,549 = 49\,000 - 451 \equiv -451 = -490 + 39 \equiv 39 = 35 + 4 \equiv 4 \pmod{7}$.

Vlastnosti kongruencí

Kongruence se stejným modulem můžeme sčítat i násobit.

Věta

Mějme celá čísla a, b, c, d a přirozené číslo m.
Jestliže platí $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, potom platí také
$a + c \equiv b + d \pmod{m}$, $ac \equiv bd \pmod{m}$.

Příklad

Protože $7 \equiv 12 \pmod{5}$ a $-7 \equiv 3 \pmod{5}$, tak také
$7 - 7 \equiv 12 + 3 \pmod{5}$ a $7 \cdot (-7) \equiv 12 \cdot 3 \pmod{5}$.

Pozor, opačná implikace obecně neplatí!

Příklad

Například $3 + 6 \equiv 7 + 5 \pmod{3}$, ale $3 \not\equiv 7 \pmod{3}$ a $6 \not\equiv 5 \pmod{3}$.
Podobně $10 \cdot 6 \equiv 4 \cdot 15 \pmod{5}$, ale $10 \not\equiv 4 \pmod{5}$ a $6 \not\equiv 15 \pmod{5}$.

Modulární aritmetika

Zbytky po dělení stejným dělitelem (modulem) můžeme sčítat a násobit. Výsledek vyjádříme opět jako zbytek po dělení modulem m.

Definice

Mějme celá čísla a, b. Zavedeme operace „$+_m$“ a „$\cdot_m$“ pomocí klasického součtu a operace „mod“.

$$a +_m b = (a + b) \bmod m, \qquad a \cdot_m b = (a \cdot b) \bmod m.$$

Říkáme také, že počítáme se zbytkovými třídami modulo m.

Příklad

Počítání na hodinách: $9 +_{12} 5 = 2, \quad (9 + 5) \bmod 12 = 2.$

Příklad

Součet dvou sudých čísel nebo součet dvou lichých čísel je sudé číslo.

$$a +_m b = (a + b) \bmod 2.$$

Modulární aritmetika - pokračování

Takto definované operace mají „pěkné“ vlastnosti. Jsou

- uzavřené na množině $\{0, 1 \ldots, m-1\}$ (zbytků modulo m),
- komutativní, $a +_m b = b +_m a, \qquad a \cdot_m b = b \cdot_m a,$
- jsou asociativní,

$$a +_m (b +_m c) = (a +_m b) +_m c, \qquad a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c,$$

- i distributivní vzhledem ke sčítání,

$$a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c,$$

- existují opačná čísla $-a = m - a$.
- Pozor inverzní čísla existovat nemusí!

Největší společný dělitel a nejmenší společný násobek

Víme, že prvočíslo je takové přirozené číslo, které má *právě dva* přirozené dělitele: jedničku a sebe sama.

Definice

Mějme dvě nenulová celá čísla a, b. Největší společný dělitel čísel a, b je takový kladný společný dělitel m čísel a, b, který je dělitelný jejich libovolným společným dělitelem. Značíme je $\mathrm{NSD}(a, b)$ nebo jen (a, b). Jestliže navíc $\mathrm{NSD}(a, b) = 1$, říkáme, že a, b jsou nesoudělná.

Příklady

Čísla 91 a 77 jsou soudělná, platí $\mathrm{NSD}(91, 77) = 7$.
Čísla 92 a 77 jsou nesoudělná, platí $\mathrm{NSD}(92, 77) = 1$.

Můžeme mít množinu po dvou nesoudělných čísel.

Nalezení prvočíselného rozkladu, resp. ověření, zda číslo je prvočíslo, je náročná úloha.

Euklidův algoritmus

Slouží k nalezení největšího společného dělitele dvou přirozených čísel a, b.

- je snadná implementace,
- není potřeba prvočíselný rozklad.

Euklidův algoritmus

Mějme dvě přirozená čísla a, b. Vydělíme číslo a číslem b se zbytkem (s využitím Věty o jednoznačnosti podílu a zbytku) a opakovaně dělíme dělitele zbytkem, dokud nebude zbytek nulový.

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n + 0 \end{aligned}$$

Poslední nenulový zbytek r_n je hledaným největším společným dělitelem.

Příklad

Najděte největšího společného dělitele čísel 414 a 662.

Označíme $a = 414$, $b = 662$. (Šikovnější je označit $a = 662$, $b = 414$.)

Postupujeme dle Euklidova algoritmu:

$$\begin{aligned} 414 &= 662 \cdot 0 + 414 \\ 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Největší společný dělitel $(414, 662) = 2$.

Euklidův algoritmus – implementace

Na vstupu máme dvě přirozená čísla a, b. Opakovaně dělíme se zbytkem.

Euklidův algoritmus

```
int a,b;              // přirozená čísla
x = a;                // dělenec
y = b;                // dělitel
while (y<>0) {
   r = x mod y;       // určíme zbytek r
   x = y;             // budeme dělit dělitele
   y = r;             // dělíme zbytkem z předchozí iterace
}
return x;             // (a,b) je poslední nenulový zbytek
```

Proměnná `x` obsahuje poslední *nenulový* zbytek, což je hledaný největší společný dělitel čísel a, b.

Další využití Euklidova algoritmu

Euklidův algoritmus funguje nejen pro celá čísla, ale na každé množině se dvěma (pěknými) operacemi.

- pro dělení polynomů
- pro tzv. Gaussova celá čísla

Následující věta říká, že největší společný dělitel čísel a,b je možno vyjádřit jako lineární kombinaci čísel a, b.

Bézoutova věta

Mějme přirozená čísla a, b. Existují celá čísla r, s taková, že $\mathrm{NSD}(a, b) = ra + sb$.

Bézoutova věta dává šikovný nástroj pro praktické řešení některých úloh s kongruencemi.

Euklidův algoritmus je snadné rozšířit a koeficienty r, s z Bézoutovy rovnosti určit.

Příklad

Ukázali jsme, že největší společný dělitel čísel 414 a 662 je 2. Najděte Bézoutovy koeficienty r, s, aby $2 = r \cdot 414 + s \cdot 662$.

Postupem dle Euklidova algoritmu jsme určili:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Nyní z předposlední rovnosti vyjádříme $\mathrm{NSD}(414, 662)$ a dosadíme z předchozích rovností.

$$\begin{aligned} 2 &= 166 - 2 \cdot 82 \\ 2 &= 166 - 2 \cdot (248 - 166 \cdot 1) = (-2) \cdot 248 + 3 \cdot 166 \\ 2 &= (-2) \cdot 248 + 3 \cdot (414 - 248 \cdot 1) = 3 \cdot 414 + (-5) \cdot 248 \\ 2 &= 3 \cdot 414 + (-5) \cdot (662 - 414 \cdot 1) = 8 \cdot 414 + (-5) \cdot 662 \end{aligned}$$

Hledané koeficienty jsou $r = 8$, $s = -5$.

Pomocí Bézoutovy věty lze snadno ukázat

Věta

Mějme přirozená čísla a, b, c. Jestliže $a \mid bc$ a přitom $(a, b) = 1$, tak $a \mid c$.

V kongruencích můžeme krátit číslem nesoudělným s modulem m.

Věta

Mějme celá čísla a, b, c a přirozené číslo m. Jestliže $ac \equiv bc \pmod{m}$ a přitom $(m, c) = 1$, tak $a \equiv b \pmod{m}$.

V kongruencích můžeme krátit společným dělitelem obou stran a modulu m.

Věta

Mějme celá čísla a, b, c a přirozené číslo m. Jestliže $ac \equiv bc \pmod{cm}$, tak $a \equiv b \pmod{m}$.

Tato pozorování využijeme v poslední části přednášky.

Lineární kongruence

Definice

Mějme celá čísla a, b, přirozené číslo m a proměnnou x. Kongruenci

$$ax \equiv b \pmod{m}$$

nazýváme lineární kongruence o jedné neznámé.

Vyřešit kongruenci znamená najít *všechny* hodnoty proměnné x, pro které je kongruence splněna.

Příklad

Řešením kongruence $x \equiv 1 \pmod{2}$ jsou právě všechna lichá čísla.
Řešením kongruence $x \equiv 4 \pmod{7}$ jsou všechna čísla $x = 7k + 4$, $k \in \mathbb{Z}$.
Řešením kongruence $3x \equiv 0 \pmod{7}$ jsou všechna čísla $x = 7k$, $k \in \mathbb{Z}$.
Řešením kongruence $3x \equiv 4 \pmod{7}$ jsou všechna čísla $x = 7k + 6$, $k \in \mathbb{Z}$.
Kongruence $3x \equiv 1 \pmod{6}$ nemá žádné řešení.

Nyní ukážeme, jak řešení najít, pokud nějaké řešení existuje.

Řešení lineárních kongruencí

Pro řešení kongruencí jsou (stejně jako pro řešení rovnic) vhodné tzv. inverze modulo m.

Definice

Mějme celé číslo a a přirozené číslo m, kde $m > 1$. Celé číslo $\overline{a}$ nazveme inverzí k číslu a modulo m, jestliže platí $\overline{a} \cdot a \equiv 1 \pmod{m}$.

Příklad

Číslo 5 je inverzí čísla 3 modulo 7, protože $5 \cdot 3 = 15 \equiv 1 \pmod{7}$.
Číslo 3 je inverzní samo k sobě modulo 8, protože $3 \cdot 3 \equiv 1 \pmod{8}$.
Číslo 7 je inverzí čísla 3 modulo 10, protože $7 \cdot 3 \equiv 1 \pmod{10}$.
Číslo 8 nemá inverzi modulo 10, protože $8 \cdot x$ je sudé a $8 \cdot x \not\equiv 1 \pmod{10}$.

Následující věta ukazuje, kdy inverze modulo m existuje.

Věta

Mějme celé číslo a a přirozené číslo m, kde $m > 1$. Jestliže jsou čísla a, m nesoudělná, tak existuje inverze $\overline{a}$ čísla a modulo m a je jediná modulo m.

Důkaz existence je konstruktivní, dává návod jak k a inverzi $\overline{a}$ najít.

Věta

Mějme celé číslo a a přirozené číslo m, kde $m > 1$. Jestliže jsou čísla a, m nesoudělná, tak existuje inverze $\overline{a}$ čísla a modulo m a je jediná modulo m.

Důkaz: Protože čísla a, m jsou nesoudělná, tak podle Bézoutovy věty existují taková celá čísla r, s, že

$$r \cdot a + s \cdot m = 1.$$

To znamená, že

$$\begin{aligned} r \cdot a + s \cdot m &\equiv 1 \pmod{m} \\ r \cdot a &\equiv 1 \pmod{m} \end{aligned}$$

Číslo r je hledanou inverzí $\overline{a}$ modulo m, platí $\overline{a} = r$.
Jednoznačnost nebudeme dokazovat. □

Platí i opačné tvrzení: pokud $\mathrm{NSD}(a, m) > 1$, tak inverze čísla a modulo m neexistuje.

Příklad

Protože $(3, 7) = 1$, tak můžeme napsat $1 = 5 \cdot 3 - 2 \cdot 7 \equiv 3 \cdot 5 \pmod 7$.
Číslo 5 je inverzí k číslu 3 modulo 7, platí $\overline{3} = 5$.

Pozor, pokud číslo a není nesoudělné s modulem m, tak inverze nemůže existovat!

Příklad

Mějme čísla 14, 6. Platí $(14, 6) = 2$, a podle Bézoutovy věty můžeme napsat $2 = 1 \cdot 14 - 2 \cdot 6$ a menší číslo s touto vlastností neexistuje.
Avšak pro žádné číslo $\overline{a}$ nemůže platit $14\overline{a} \equiv 1 \pmod 6$.

Řešitelnost lineárních kongruencí můžeme shrnout:

Věta

Mějme celá čísla a, b a přirozené číslo m.
Lineární kongruence $ax \equiv b \pmod m$ má řešení právě tehdy, když $NSD(a, m)$ dělí b.

Řešení lineárních kongruencí

Nyní můžeme řešit lineární kongruence o jedné neznámé analogicky jako se řeší lineární rovnice.

Příklad

Najděte všechna řešení lineární kongruence $3x \equiv 4 \pmod 7$.

Nejprve najdeme k číslu 3 inverzi modulo 7. Podle předchozího příkladu $\overline{3} = 5$.
Nyní obě strany kongruence vynásobíme inverzí 5. Dostaneme

$$\begin{aligned} 5 \cdot 3x &\equiv 5 \cdot 4 \pmod 7 \\ x &\equiv 20 \pmod 7 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Řešením jsou všechna čísla, která po dělení 7 dávají zbytek 6.
Řešení jsou čísla $x = 7k + 6$, kde $k \in \mathbb{Z}$.

Nejpracnější část řešení je nalezení inverze modulo m.

Využijeme věty pro úpravy a zjednodušení kongruencí

Mějme celá čísla a, b, c, d a přirozené číslo m.
Mějme kongruence $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$.

- Kongruence se stejným modulem můžeme sčítat.

$$a + c \equiv b + d \pmod{m}$$

- Kongruence se stejným modulem můžeme násobit.

$$ac \equiv bd \pmod{m}$$

- Kongruence můžeme roznásobit libovolným číslem c.

$$ac \equiv bc \pmod{m}$$

- V kongruencích můžeme krátit číslem c nesoudělným s modulem, tj. pro $(c, m) = 1$ platí

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

- V kongruencích můžeme krátit číslem $c = \mathrm{NSD}(a, b, m)$.

$$ac \equiv bc \pmod{mc} \quad \Rightarrow \quad a \equiv b \pmod{m}$$

Tyto úpravy nám umožní zjednodušovat a řešit lineární kongruence.

Příklad

Najděte a ověřte řešení kongruence $5x \equiv 2 \pmod{13}$.

Využitím $\overline{5} = 8$ dostaneme $x \equiv 16 \pmod{13}$, tedy $x = 13t + 3$, $t \in \mathbb{Z}$.

Jiné řešení: přičtením modulu 13 k pravé straně $5x \equiv 2 + 13 \pmod{13}$.
Krácením 5 dostaneme $x \equiv 3 \pmod{13}$, tedy $x = 13t + 3$, $t \in \mathbb{Z}$.

Zkouška? Stačí dosadit $5(13t + 3) \equiv 5 \cdot 13t + 15 \equiv 0t + 2 \pmod{13}$.

Příklad

Najděte řešení kongruence $3x \equiv 2 \pmod{15}$.

Tato kongruence nemá řešení, protože $(3, 15) = 3$ a číslem 3 nelze krátit.

Příklad

Najděte řešení kongruence $3x \equiv 6 \pmod{15}$.

Vykrátíme číslem 3 obě strany modul. Dostaneme $x \equiv 2 \pmod{5}$.
Tato kongruence má řešení $x = 5t + 2$, $t \in \mathbb{Z}$, přestože $(3, 15) = 3$.
Vykrátili jsme celou kongruenci i modul číslem 3.

Oprava ISBN kódu

Kamarád měl výbornou učebnici jazyka C. Její ISBN-10 kód je 80-05-001?4-1. Osmou cifru nemůžeme přečíst. Jaká to má být cifra?

Víme, že ISBN-10 kód musí splňovat

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} \equiv 0 \pmod{11}.$$

Sestavíme lineární kongruenci.

$$\begin{aligned} 8 + 0 + 0 + 20 + 0 + 0 + 7 + 8x_8 + 36 + 10 &\equiv 0 \pmod{11} \\ 8x_8 + 81 &\equiv 0 \pmod{11} \\ 8x_8 &\equiv -81 \pmod{11} \\ 8x_8 &\equiv 7 \pmod{11} \\ 7 \cdot 8x_8 &\equiv 7 \cdot 7 \pmod{11} \\ x_8 &\equiv 49 \equiv 5 \pmod{11} \end{aligned}$$

Chybějící cifra ISBN-10 kódu je 5. (Využili jsme, že $\overline{8} = 7$ modulo 11.)
Hledaný ISBN-10 kód učebnice je 80-05-00154-1.

Čínská zbytková věta

Následující věta říká, že existuje jednoznačné řešení soustav lineárních kongruencí s navzájem nesoudělnými moduly.

Čínská zbytková věta

Mějme po dvou nesoudělná přirozená čísla $m_1, m_2, \ldots, m_n$ větší než jedna. Mějme celá čísla $a_1, a_2, \ldots, a_n$. Soustava kongruencí

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

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

Řešení lze vyčíslit. Nyní ukážeme obecnou metodu.

Historicky dle problémů řešených ve starých rukopisech se větě říká „Čínská zbytková věta“.

Důkaz předchozí věty je konstruktivní, často však lze řešení najít jednodušeji (případnou) úpravou a zpětným dosazením kongruencí.

Příklad

Najděte řešení soustavy kongruencí

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Na základě předchozích tvrzení vidíme, že řešení první kongruence

$$x \equiv 1 \pmod 5$$

je $x = 1 + 5t$, kde $t \in \mathbb{Z}$.
Toto řešení dosadíme do druhé kongruence

$$\begin{aligned} 1 + 5t &\equiv 2 \pmod 6 \\ 5t &\equiv 1 \pmod 6 \\ -t &\equiv 1 \pmod 6 \\ t &\equiv -1 = 5 \pmod 6 \end{aligned}$$

Řešení kongruence

$$t \equiv 5 \pmod 6$$

je $t = 6u + 5$, kde $u \in \mathbb{Z}$.
Dosazením do $x = 1 + 5t$ dostáváme řešení prvních dvou kongruencí

$$x = 1 + 5(6u + 5) = 30u + 26, u \in \mathbb{Z},$$

což dosadíme do třetí kongruence. Dostáváme

$$\begin{aligned} 30u + 26 &\equiv 3 \pmod 7 \\ 2u - 2 &\equiv 3 \pmod 7 \\ 4 \cdot 2u &\equiv 4 \cdot 5 \pmod 7 \\ u &\equiv 6 \pmod 7. \end{aligned}$$

Řešením je $u = 7v + 6$, kde $v \in \mathbb{Z}$, což dosadíme do řešení soustavy prvních dvou kongruencí.

$$x = 30u + 26 = 30(7v + 6) + 26 = 210v + 206, v \in \mathbb{Z}.$$

Dostáváme řešení soustavy všech tří kongruencí.

Využití kongruencí – hashovací funkce

Při ukládání velkého objemu dat můžeme nové záznamy x přidávat na konec databáze. To je nevýhodné při vyhledávání záznamů – musíme prohledat celou databázi.
Je-li m záznamů, tak potřebujeme $O(m)$ kroků.

Myšlenka hashovací funkce: Odhadneme očekávanou velikost databáze m a alokujeme odpovídající paměť. Nový záznam s klíčem k vložíme do databáze na pozici $h(k)$, kde

$$h(k) = k \bmod m,$$

případně na další volné místo za $h(k)$.
Místo prohledávání databáze záznam pak hledáme na pozici $h(k)$.

Příklad

Databáze na škole s 15 000 studenty, rodné číslo.

Hashovací funkce by mohla být $h(k) = \mathit{rodne\_cislo} \bmod 15\ 000$.
Lépe však $h(k) = \mathit{rodne\_cislo} \bmod 30\ 000$.

Využití kongruencí – Pseudonáhodná čísla

Opravdu náhodné číslo je výpočetně „drahé“.
Pseudonáhodné vypočítáme snadno a rychle

$$x_{n+1} = (ax_n + b) \bmod m,$$

kde a, b, m jsou vhodně zvolená čísla. Inicializační hodnota x_0 je „seed“.

Příklad

Například pro $a = 7$, $b = 4$, $m = 9$ a $x_0 = 1$ dostáváme

$$\begin{aligned} x_1 &= (7x_0 + 4) \bmod 9 = 11 \bmod 9 = 2 \\ x_2 &= (7x_1 + 4) \bmod 9 = 18 \bmod 9 = 0 \\ x_3 &= (7x_0 + 4) \bmod 9 = 4 \bmod 9 = 4 \\ x_4 &= (7x_0 + 4) \bmod 9 = 32 \bmod 9 = 5 \\ &\vdots \end{aligned}$$

Dostaneme posloupnost $1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, \ldots$

Často využívaný náhodný generátor: $a = 7^5$, $b = 0$, $m = 2^{31} - 1$.

Využití kongruencí – kontrolní součty

Paritní součty

Mějme zprávu s n bity $x_1, x_2, \ldots, x_n$.
Vysílající přidá další bit, kontrolní součet

$$x_{n+1} = (x_1 + x_2 + \cdots + x_n) \bmod 2.$$

Pokud nastane *jedna* (případně lichý) počet chyb, příjemce zjistí, že

$$x_1 + x_2 + \cdots + x_n + x_{n+1} \not\equiv 0 \pmod 2$$

a může vyžádat znovuzaslání/znovupřečetní zprávy.

Pokud je kontrolních bitů více, můžeme chybná data OPRAVIT.
(příklad uvedeme později)

Využití kongruencí – UPC kódy

UPC kódy (Universal Product Code)

Existuje řada variant UPC kódů, zpravidla obsahují nějaký kontrolní součet. UPC-A kód má 12 číslic. Musí platit

$$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0 \pmod{10}$$

Příklad

Je 041331021641 platný UPC kód?

Platí $0+4+3+3+9+1+0+2+3+6+12+1 = 44 \equiv 4 \pmod{10}$, proto kód není platný.

Aplikace řešení lineárních kongruencí

Rekonstrukce UPC kódu čísla

Víme, že UPC kód 041331021641 není platný. Podrobnějším zkoumáním vidíme, že čtvrtý znak kódu je znehodnocen. Jaký je správný UPC kód?

Víme, že cifry UPC kódu 041?31021641 musí splňovat

$$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0 \pmod{10}$$

Sestavíme lineární kongruenci

$$\begin{aligned} 0+4+3+x_4+9+1+0+2+3+6+12+1 &\equiv 0 \pmod{10} \\ x_4+41 &\equiv 0 \pmod{10} \\ x_4 &\equiv -1 \pmod{10} \\ x_4 &\equiv 9 \pmod{10} \end{aligned}$$

Hledaná cifra UPC kódu je 9. UPC kód je 041931021641.

Snadno ověříme, že

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} =$$
$$= 0+4+3+9+9+1+0+2+3+6+12+1 = 50 \equiv 0 \pmod{10}$$

Další využití kongruencí

- ISBN/ISSN
- rodná čísla
- čísla bankovek
- čísla bankovních účtů
- jednoduché šifry

Aplikace řešení lineárních kongruencí

Rekonstrukce rodného čísla

Babička zapomněla své rodné číslo. Pamatuje si samozřejmě data narození a část posledního čtyřčíslí. Podařilo se zrekonstruovat následující část rodného čísla: 346509?248. Jaká je chybějící cifra?

Víme, že pro cifry rodného čísla musí platit

$$x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8 + x_9x_{10} \equiv 0 \pmod{11}.$$

Sestavíme lineární kongruenci

$$\begin{aligned} 34 + 65 + 9 + (10x + 2) + 48 &\equiv 0 \pmod{11} \\ 1 - 1 - 2 + 10x + 2 + 4 &\equiv 0 \pmod{11} \\ 10x &\equiv -4 \pmod{11} \\ -x &\equiv -4 \pmod{11} \\ x &\equiv 4 \pmod{11} \end{aligned}$$

Hledaná cifra je 4.

Příště

Algoritmizace diskrétních struktur

- programové interpretace struktur
- implementace množin
- generování výběrů
- generátory náhodných čísel
- kombinatorická exploze