Řešení lineárních kongruencí

+ aplikace
- rodné číslo
- číslo bank. účtu

Řešení soustavy kongruencí

+ Začátek - Úvod do grafů

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

$x = ?$

Př: Najděte řešení kongruence

$x \equiv 21 \pmod{9}$

Můžeme zjednodušit.

$x \equiv 2\cdot 9 + 3 \pmod{9}$

$x \equiv 3 \pmod{9}$

$x = \ldots, -24, -15, -6, 3, 12, 21, 30, 39, \ldots$

stručnější zápis $x = 9\cdot k + 3, \; k \in \mathbb{Z}$

Př: Vyřešte kongruenci
$x \equiv -93 \pmod{11}$

$x \equiv -99 + 6 \pmod{11}$

$x \equiv 6 \pmod{11}$

Řešení:

$x = \ldots -16, -5, 6, 17, 28, 39$

$x = 11 \cdot k + 6, \quad k \in \mathbb{Z}$

Př: Řešte kongruenci

a) $2x \equiv 34 \pmod 8$

$a \cdot \cancel{c} \equiv b \cdot \cancel{c} \pmod{m \cdot \cancel{c}}$

$a \cdot \cancel{c} \equiv b \cdot \cancel{c} \pmod m$

pro $NSD(c, m) = 1$

lze dělit 2 (včetně modulu)

$x \equiv 17 \pmod 4$

$x \equiv 16 + 1 \pmod 4$

$x \equiv 4 \cdot 4 + 1 \pmod 4$

$x \equiv 1 \pmod 4 \quad \Rightarrow \quad x = 4k + 1, \quad k \in \mathbb{Z}$

b) $2x \equiv 33 \pmod 8$

Krátit nelze, zjednodušíme:

$2x \equiv 32 + 1 \pmod 8$

$2x \equiv 4 \cdot 8 + 1 \pmod 8$

$2x \equiv 1 \pmod 8$ → řešením by bylo x takové, že $2 \cdot x \equiv 1$ tj $x = \bar{2}$ ← inverze

Ale $\bar{2} \pmod 8$ neexistuje, protože $NSD(8, 2) = 2 \neq 1$

Kongruence nemá řešení!

c) $2x \equiv 5 \pmod 9$

Potřebujeme najít $\bar{2} \pmod 9$ abychom osamost. x.

tj $\underbrace{\bar{2} \cdot 2}_{1} x \equiv \bar{2} \cdot 5 \pmod 9$

Inverze existuje protože $NSD(2,9) = 1$

Najdeme inverzi (Eukl. alg + Bezout. věta)

$9 = 4 \cdot 2 + 1 \rightarrow NSD(9,2) = 1$

$2 = 2 \cdot 1 + 0$

inverze

$1 = 9 - 4 \cdot 2 = 1 \cdot 9 + (-4) \cdot 2$

inverze $\bar{2} \pmod 9 = \underline{\underline{-4}}$

můžeme vzít i $-4 + 9 = \underline{\underline{5}}$

Dořešíme kongruenci - vynásobíme ji inverzí

$5 \cdot 2x \equiv 5 \cdot 5 \pmod 9$

$x \equiv 25 \pmod 9$

$x \equiv 2 \cdot 9 + 7 \pmod 9$

$x \equiv 7 \pmod 9 \Rightarrow \underline{x = 9 \cdot k + 7, \ k \in \mathbb{Z}}$

Jiný (rychlejší) postup řešení (není obecný).

$2x \equiv 5 \pmod 9$

$2x \equiv 5 + 9 \pmod 9$

$2x \equiv 14 \pmod 9$ vykrátíme 2

$x \equiv 7 \pmod 9 \Rightarrow \underline{x = 9k + 7, \ k \in \mathbb{Z}}$

Aplikace řešení kongruencí.

Ověřte zda je dané číslo platným rodným číslem.

$\underbrace{01}\,\underbrace{11}\,\underbrace{\cancel{2}1}\,\underbrace{03}\,\underbrace{82}$

Rodné č. musí splňovat

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

$$01 + 11 + 21 + 03 + 82 \equiv 0 \pmod{11}$$

$$36 + 82 \equiv 0 \pmod{11}$$

$$3 + 5 \equiv 0 \pmod{11}$$

$$8 \not\equiv 0 \pmod{11} \Rightarrow$$

Dané číslo není platné r. číslo.

Předpokládejme, že 5-tá cifra je špatně.

$$01 + 11 + (10x+1) + 03 + 82 \equiv 0 \pmod{11}$$

$$10x + 5 + 5 \equiv 0 \pmod{11}$$

$$10x + 10 + 1 \equiv 1 \pmod{11}$$

$$10x \equiv 1 \pmod{11}$$

odtud x je $\overline{10} \pmod{11}$

Eukl. alg.

$$11 = 1 \cdot 10 + 1 \quad \rightarrow \quad NSD(11, 10) = 1$$

$$10 = 10 \cdot 1 + 0$$

$$1 = 11 - 1 \cdot 10 = 1 \cdot 11 + (-1) \cdot 10$$

← inverze

$$\bar{x} = -1 \equiv -1 + 11 \equiv 10 \pmod{11}$$

Dořešíme kongruenci

$$\underbrace{10\cdot 10}_{100\equiv 1\ (\mathrm{mod}\ 11)}\cdot x \equiv 10\cdot 1 \pmod{11}$$

$$x \equiv 10 \pmod{11} \Rightarrow \underline{x = 11k + 10,\ k\in\mathbb{Z}}$$

Pátá cifra by musela být 10 - to nelze.

Dané číslo není platným r. č.

6.7.14. Kontrolní schéma čísla bankovních institucí na šeku je $7x_1 + 3x_2 + 9x_3 + 7x_4 + 3x_5 + 9x_6 + 7x_7 + 3x_8 + 9x_9 \equiv 0 \pmod{10}$. První cifra kódu je znehodnocena ?06480665. Určete její hodnotu.

Dosadíme cifry kódu do uvedeného schema

$$7\cdot x + 3\cdot 0 + 9\cdot 6 + 7\cdot 4 + 3\cdot 8 + 9\cdot 0 + 7\cdot 6 + 3\cdot 6 + 9\cdot 5 \equiv 0 \pmod{10}$$

$$7x + 54 + 28 + 24 + 42 + 18 + 45 \equiv 0 \pmod{10}$$

$$7x + 4 + 8 + 4 + 2 + 8 + 5 \equiv 0 \pmod{10}$$

$$7x + 31 \equiv 0 \pmod{10}$$

$$7x \equiv 9 \pmod{10}$$

Potřebujeme inverzi $\bar{7} \pmod{10}$

$\bar{7} \pmod{10} = 3$ protože $3\cdot 7 = 21 \equiv 1 \pmod{10}$

$$3\cdot 7x \equiv 3\cdot 9 \pmod{10}$$

$$x \equiv 7 \pmod{10}$$

Řešení kongruence $x = 10k + 7,\ k\in\mathbb{Z}$

Řešení pro daný kód $\underline{\underline{x = 7}}$

Soustavy kongruencí

Vyřešte soustavu kongruencí

$$x \equiv 3 \pmod{7} \qquad (1)$$
$$x \equiv 7 \pmod{12} \qquad (2)$$
$$x \equiv 4 \pmod{17} \qquad (3)$$

z kongr. (1) plyne

$$x = 7k_1 + 3 \qquad (4)$$

dosadíme do (2)

$$7k_1 + 3 \equiv 7 \pmod{12}$$
$$7k_1 \equiv 4 \pmod{12}$$
$$7 \cdot 7 k_1 \equiv 7 \cdot 4 \pmod{12}$$
$$k_1 \equiv 28 \pmod{12}$$
$$k_1 \equiv 4 \pmod{12}$$

Uhodnuto

$\bar{7} \pmod{12} = 7$

Lze určit Eukl. Al. + nalezením Bezout. k.

odtud určíme k_1 jako náso- jiného k_2

$$k_1 = 12 \cdot k_2 + 4$$

dosadíme za k_1 do (4)

$$x = 7 \cdot (12 \cdot k_2 + 4) + 3 = \underline{\overbrace{84k_2 + 31}^{x}} \qquad (5)$$

dosadíme do třetí kongruence za x

$$\overbrace{84k_2 + 31}^{x} \equiv 4 \pmod{17}$$
$$16k_2 + (-3) \equiv 4 \pmod{17}$$
$$16k_2 \equiv 7 \pmod{17}$$

$\overline{16} \pmod{17} = 16$

$$\underbrace{16\cdot 16}_{1}\cdot k_2 \equiv 16\cdot 7 \pmod{17}$$

$$k_2 \equiv 112 \pmod{17}$$

$$k_2 \equiv 10 \pmod{17}$$

dosadíme zpátky do (5) $\quad k_2 = 17\cdot k_3 + 10$

$$x = 84(17\cdot k_3 + 10) + 31$$

$$x = 1428k_3 + 871, \quad k_3 \in \mathbb{Z}$$

$$x \equiv 871 \pmod{1428}$$

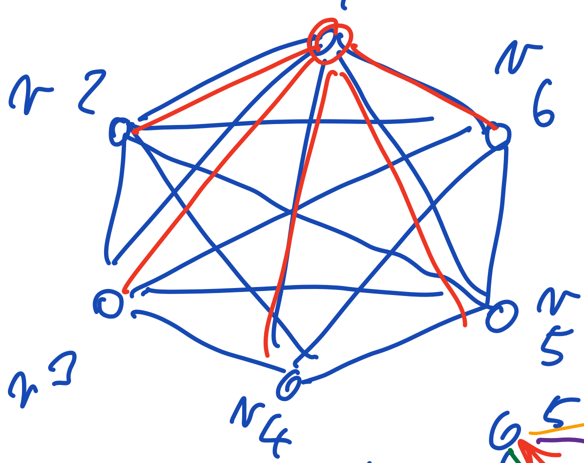
Grafy

Úvod do grafů

- Základní třídy grafů
- Princip sudosti
- Věta Havlova – Hakimiho

Př: Jestliže pořádáme turnaj 6-týmů kdy se mají odehrát všechny zápasy a každý tým může hrát jen 1 zápas denně. V kolika nejméně dnech lze turnaj odehrát?

$G(V,E)$



K_6

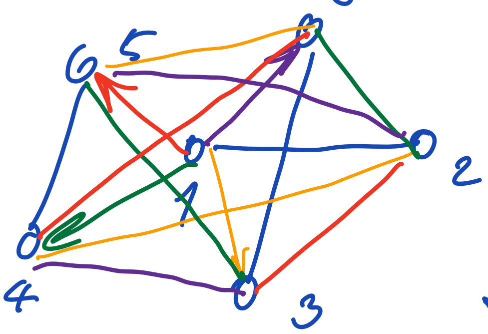
K_n

$|V(K_n)| = n$

$|E(K_6)| = \frac{6\cdot 5}{2} = 15$

$|E(K_n)| = \frac{n\cdot(n-1)}{2} = \binom{n}{2}$

1. den



Turnaj lze odehrát v 5 dnech. každý den 3 zápasy. Rozpis dle

- Určete počty vrcholů a hran pro graf

$P_n, C_n, K_n, K_{m,n}$

$\deg(v_2) = 2$

- P_n P_5 - cesta

$\Delta(P_5) = 2$

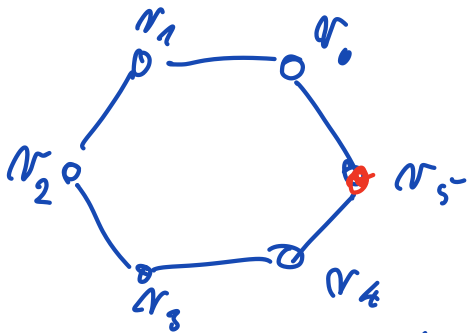
$\delta(P_5) = 1$

$G(V,E)$ $\quad |V(P_5)| = 5$ $\quad |V(P_n)| = n$

$|V(G)|$ $\quad |E(P_5)| = 4$ $\quad |E(P_n)| = n-1$

$|E(G)|$

- C_6 $\quad C_6$ – cyklus $\quad |V(C_n)| = n$, $\quad |E(C_n)| = n$

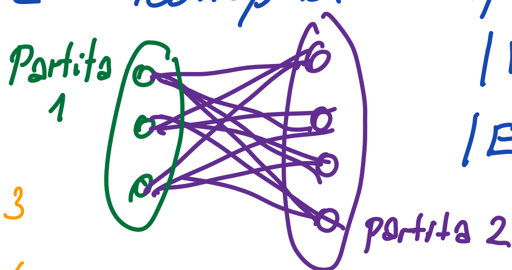


$deg(v_5) = 2$

$\delta(C_6) = \Delta(C_6) = 2$

- $K_{m,n}$ ← kompletní bipartitní graf

$K_{3,4}$



$|V(K_{3,4})| = 3+4 = 7$ $\quad |V(K_{m,n})| = m+n$

$|E(K_{3,4})| = 3 \cdot 4 = 12$ $\quad |E(K_{m,n})| = m \cdot n$

$\delta(K_{3,4}) = 3$

$\Delta(K_{3,4}) = 4$

Pro $m \geq n$ $\delta(K_{m,n}) = n$ a $\Delta(K_{m,n}) = m$

- Srovnejte který graf má více hran, vrcholů?

$K_{6,7}$, K_{10}

$|V(K_{6,7})| = 13 > 10 = |V(K_{10})|$

$|E(K_{6,7})| = 6 \cdot 7 = 42 < 45 = \binom{10}{2} = |E(K_{10})|$

Stupňová posloupnost

Zapište st. posloupnosti grafů P_5, C_4, K_4, $K_{3,2}$. Jaký je $\delta(G)$ a $\Delta(G)$?

P_5 $(2,2,2,1,1)$

K_4 $(3,3,3,3)$

C_4 $(2,2,2,2)$

$K_{3,2}$ $(3,3,2,2,2)$

Princip sudosti + pokračování příště.