Diskrétní matematika – cvičení 4. týden

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

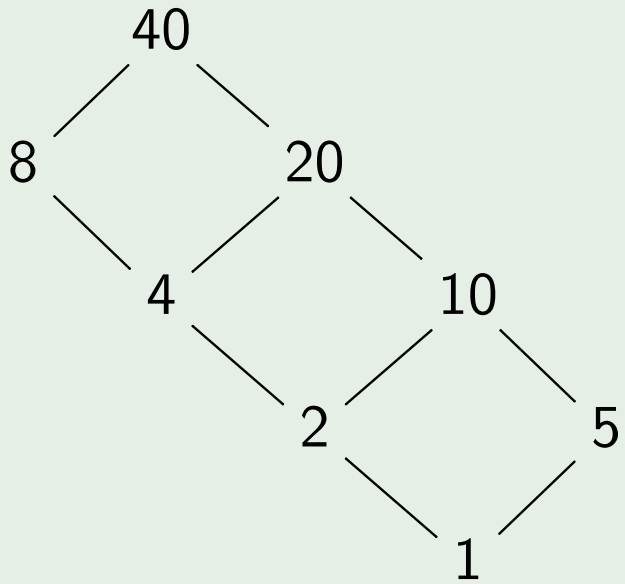
jaro 2020

Příklad

Určete primitivní kořen modulo 41.

Řešení

Protože je 41 prvočíslo, máme $\varphi(41) = 41 - 1 = 40$ a řád každého čísla dělí 40:

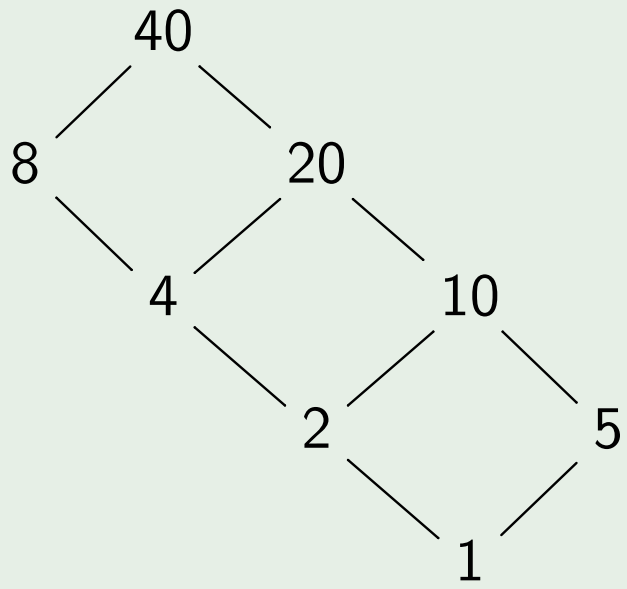


Hledáme číslo a řádu 40. Podle Eulerovy věty $a^{40} \equiv 1$, budeme kontrolovat, zda $a^{20} \not\equiv 1$, $a^{8} \not\equiv 1$.

Příklad

Určete primitivní kořen modulo 41.

Řešení



Platí totiž: jestliže řád a není 40, pak $a^{20} \equiv 1$ nebo $a^8 \equiv 1$.
Obecně je potřeba testovat mocniny s exponentem $\varphi(m)/p$, kde p je prvočíslo dělící $\varphi(m)$, v našem případě $\varphi(41) = 40 = 2^3 \cdot 5$, proto se testují exponenty $40/2$, $40/5$.

Příklad

Určete primitivní kořen modulo 41.

Řešení

Protože $a \equiv 1$ má řád 1, začneme s $a \equiv 2$: počítáme

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^4 \equiv 16, \quad 2^8 \equiv 256 \equiv 10$$

a konečně $2^{16} \equiv 100 \equiv 18$, takže

$$2^{20} \equiv 2^{16} \cdot 2^4 \equiv 18 \cdot 16 \equiv 1, \qquad 2^8 \equiv 10.$$

Vidíme, že řád čísla 2 je 20, případně ještě menší a nejedná se o primitivní kořen modulo 41.

Příklad

Určete primitivní kořen modulo 41.

Řešení

Pokračujeme s $a \equiv 3$: počítáme

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^4 \equiv 81 \equiv -1, \quad 3^8 \equiv 1, \quad 3^{16} \equiv 1,$$

takže

$$3^{20} \equiv 3^{16} \cdot 3^4 \equiv -1, \qquad 3^8 \equiv 1.$$

Vidíme, že řád čísla 3 je 8 (menší být opravdu nemůže, dokažte to z diagramu dělitelů) a nejedná se o primitivní kořen modulo 41.

Příklad

Určete primitivní kořen modulo 41.

Řešení

Číslo $a \equiv 4$ zkoušet nemusíme, neboť $4^{10} \equiv 2^{20} \equiv 1$ a má tedy řád maximálně 10. Obecně mocnina čísla, které není primitivním kořenem, nemůže být primitivním kořenem.
Pokračujeme s $a \equiv 5$: počítáme

$$5^1 \equiv 5, \quad 5^2 \equiv 25, \quad 5^4 \equiv 10, \quad 5^8 \equiv 18, \quad 5^{16} \equiv 37,$$

takže

$$5^{20} \equiv 5^{16} \cdot 5^4 \equiv 37 \cdot 41 \equiv 1, \qquad 5^8 \equiv 18.$$

Vidíme, že řád čísla 5 je 20, případně ještě menší a nejedná se o primitivní kořen modulo 41.

Příklad

Určete primitivní kořen modulo 41.

Řešení

Pokračujeme s $a \equiv 6 = 2 \cdot 3$, proto

$$6^{20} \equiv 2^{20} \cdot 3^{20} \equiv 1 \cdot (-1) \equiv -1, \qquad 6^8 \equiv 2^8 \cdot 3^8 \equiv 10 \cdot 1 \equiv 10.$$

Konečně jsme našli primitivní kořen 6 modulo 41.

Příklad

Určete *všechny* primitivní kořeny modulo 41.

Řešení

Protože je 6 primitivní kořen, jsou všechny zbytky

$$6^0, 6^1, 6^2, \ldots, 6^{39}$$

různé (a $6^0 \equiv 6^{40}$), zároveň jsou nesoudělné s 41 a je jich $\varphi(41) = 40$, takže tvoří redukovanou soustavu zbytků, tj. jedná se právě o všechny zbytky $1, \ldots, 40$. Můžeme proto primitivní kořeny hledat mezi těmito čísly.
$6^0 \equiv 1$ má řád 1, 6^1 má řád 40, přesuňme se tedy k 6^2.

Příklad

Určete *všechny* primitivní kořeny modulo 41.

Řešení

Zjevně

$$(6^2)^{20} \equiv 6^{40} \equiv 1,$$

takže 6^2 určitě nebude primitivním kořenem (ve skutečnosti má řád přesně 20), podobně například

$$(6^{15})^8 \equiv (6^{3\cdot 5})^8 \equiv 6^{3\cdot 40} \equiv 1.$$

Mělo by být víceméně jasné, že kdykoliv a^r bude mít exponent r *soudělný* s 40, bude jeho řád menší než 40: buď bude exponent r dělitelný 2 a pak $(a^r)^{20} \equiv a^{\frac{r}{2}\cdot 40} \equiv 1$ nebo bude exponent r dělitelný 5 a pak $(a^r)^8 \equiv a^{\frac{r}{5}\cdot 40} \equiv 1$.

Příklad

Určete *všechny* primitivní kořeny modulo 41.

Řešení

Naopak a^r bude primitivní kořen, pokud $(r, 40) = 1$, demonstrujme to na $r = 3$, tedy zkoumejme mocniny čísla a^3, které dávají zbytek 1:

$$(a^3)^s \equiv a^{3s} \equiv a^0 \equiv 1 \Leftrightarrow 40 \mid 3s \Leftrightarrow 40 \mid s.$$

V poslední ekvivalenci se využívá nesoudělnost 40 a 3, pomocí kongruencí je to nám dobře známé

$$3s \equiv 0 \Rightarrow s \equiv 0 \pmod{40}.$$

Příklad

Určete *všechny* primitivní kořeny modulo 41.

Řešení

Každopádně vidíme, že řád a^3 je vskutku 40 a jedná se o primitivní kořen, podobně všechna čísla a^r, kde r je nesoudělné s 40; jsou to tedy právě:

$$a^1, a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}, a^{21}, a^{23}, a^{27}, a^{29}, a^{31}, a^{33}, a^{37}, a^{39}.$$

Samozřejmě víme, že jich je
$\varphi(40) = \varphi(2^3 \cdot 5) = (2^3 - 2^2) \cdot (5 - 1) = 16.$

Příklad

Spočtěte nějaké jednoduché lineárních kongruence, např.
$130x \equiv 150 \pmod{232}$.

Řešení

Uvedená kongruence je ekvivalentní soustavě

$$\begin{aligned} 232x &\equiv 0 \pmod{232} \\ 130x &\equiv 150 \pmod{232} \end{aligned}$$

kterou budeme dále upravovat ekvivalentními úpravami – přičítáním násobku jednoho řádku k druhému:

$$\begin{aligned} &\xrightarrow{-1\cdot \mathrm{II}} 102x \equiv -150 \equiv 82 && 102x \equiv 82 \\ 130x \equiv 150 \quad &\xrightarrow{-1\cdot \mathrm{I}} && 28x \equiv 68 \end{aligned}$$

Příklad

Spočtěte nějaké jednoduché lineárních kongruence, např.
$130x \equiv 150 \pmod{232}$.

Řešení

$$\begin{aligned} 102x &\equiv 82 \xrightarrow{-3\cdot\mathrm{II}} 18x \equiv -122 \equiv 110 \\ 28x &\equiv 68 \qquad\qquad 28x \equiv 68 \xrightarrow{-1\cdot\mathrm{I}} \end{aligned}$$

$$\begin{aligned} 18x &\equiv 110 \xrightarrow{-1\cdot\mathrm{II}} 8x \equiv 152 \equiv -80 \\ 10x &\equiv -42 \qquad\qquad 10x \equiv -42 \xrightarrow{-1\cdot\mathrm{I}} \end{aligned}$$

$$\begin{aligned} 8x &\equiv -80 \xrightarrow{-4\cdot\mathrm{II}} 0x \equiv -232 \equiv 0 \\ 2x &\equiv 38 \qquad\qquad 2x \equiv 38 \end{aligned}$$

Příklad

Spočtěte nějaké jednoduché lineárních kongruence, např.
$130x \equiv 150 \pmod{232}$.

Řešení

Původní rovnice a tedy i původní soustava je ekvivalentní soustavě

$$2x \equiv 38 \pmod{232}$$
$$0x \equiv 0 \pmod{232}$$

Druhá rovnice je zbytečná, první rovnici lze vydělit koeficientem u x – celou včetně modulu! (Ani jedno nemusí být pravda v případě, kdy původní rovnice nemá řešení, viz dále!) Dostáváme tak ekvivalentně

$$x \equiv 19 \pmod{116}$$

Řešení

Přehledněji lze psát takto, kde všechny po sobě jdoucí *dvojice* rovnic jsou ekvivalentní:

$$
\begin{aligned}
232x &\equiv 0 \\
130x &\equiv 150 \\
102x &\equiv 82 \\
28x &\equiv 68 \\
18x &\equiv 110 \\
10x &\equiv -42 \\
8x &\equiv -80 \\
2x &\equiv 38 \pmod{232} \qquad \Leftrightarrow \qquad x \equiv 19 \pmod{116} \\
0x &\equiv 0
\end{aligned}
$$

Poznámka

Že je potřeba počítat až do konce si demonstrujeme na dvou jednoduchých příkladech, prvně $4x \equiv 1 \pmod{10}$:

$$\begin{aligned} 10x &\equiv 0 \\ 4x &\equiv 1 \\ 2x &\equiv 8 \pmod{10} \qquad \Leftrightarrow \quad x \equiv 4 \pmod{5} \\ 0x &\equiv 5 \end{aligned}$$

Bez posledního řádku bychom se mohli mylně domnívat, že $x \equiv 4 \pmod{5}$ je řešením.

Poznámka

V jiném případě $4x \equiv 1 \pmod{14}$ dostaneme podobně:

$$\begin{aligned} 14x &\equiv 0 \\ 4x &\equiv 1 \\ 2x &\equiv 11 \pmod{14} \\ 0x &\equiv 7 \end{aligned}$$

V tomto případě dokonce předposlední rovnici vydělit dvěma nelze. Poznamenejme, že pokud je poslední rovnost splněna, lze předposlední rovnici vždy vydělit (to plyne z teorie, nebudeme to dále rozebírat).

Příklad

Spočtěte nějaké jednoduché lineárních kongruence, např.
$130x \equiv 150 \pmod{232}$.

Řešení

Řešením je tedy jediná zbytková třída modulo 116, zabývejme se ještě krátce počtem řešení jakožto zbytkových tříd modulo 232, stejně jak je formulováno zadání. Ve zbytkových třídách modulo 232 se zbytkové třídy modulo 116 vyskytnou každá dvakrát:

$$\underbrace{\underbrace{0\ 1\ \ldots\ 115}_{116}\ \underbrace{116\ 117\ \ldots\ 231}_{116}}_{232} \equiv \underbrace{\underbrace{0\ 1\ \ldots\ 115}_{116}\ \underbrace{0\ 1\ \ldots\ 115}_{116}}_{232}$$

Zbytková třída $19 \pmod{116}$ tedy odpovídá dvěma zbytkovým třídám $19 \pmod{232}$ a $19 + 116 \pmod{232}$. To jsou dvě řešení původní úlohy.

Příklad

Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 7 && \pmod{27} \\ x &\equiv -3 && \pmod{11} \end{aligned}$$

Řešení

Podobně jako na konci posledního příkladu dá $7 \pmod{27}$ jedenáct zbytkových tříd modulo $[27, 11] = 27 \cdot 11 = 297$, konkrétně

$$7, 7 + 27, 7 + 2 \cdot 27, \ldots, 7 + 10 \cdot 27.$$

Obdobně zbytková třída $-3 \equiv 8 \pmod{11}$ dá dvacet sedm zbytkových tříd

$$8, 8 + 11, 8 + 2 \cdot 11, \ldots, 8 + 26 \cdot 11.$$

Příklad

Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 7 && \pmod{27} \\ x &\equiv -3 && \pmod{11} \end{aligned}$$

Řešení

Na těchto seznamech je právě jedno číslo společné a to je řešením úlohy. Tento postup je však *velmi* nepraktický (exponenciální časová složitost). O něco lepší je počítat podobně jako v případě jedné rovnice – prvně převedeme obě kongruence na společný modul $[27, 11] = 27 \cdot 11 = 297$:

$$\begin{aligned} 11x &\equiv 77 && \pmod{297} \\ 27x &\equiv -81 && \pmod{297} \end{aligned}$$

a nyní postupným upravováním vyřešíme.

Příklad

Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 7 && \pmod{27} \\ x &\equiv -3 && \pmod{11} \end{aligned}$$

Řešení

$$\begin{aligned} 27x &\equiv -81 && \pmod{297} \\ 11x &\equiv 77 && \pmod{297} \\ 5x &\equiv -235 \equiv 62 && \pmod{297} \\ x &\equiv -47 \equiv 250 && \pmod{297} \end{aligned}$$

Nevýhodou je počítání s relativně velkými čísly (řádově 297); vhodnou modifikací lze počítat s čísly menšími (řádově 27 a 11) tím, že pravou stranu zapisujeme jako kombinaci 27 a 11:

Příklad

Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 7 && \pmod{27} \\ x &\equiv -3 && \pmod{11} \end{aligned}$$

Řešení

$$\begin{aligned} 27x &\equiv -3 \cdot 27 && \pmod{297} \\ 11x &\equiv 7 \cdot 11 && \pmod{297} \\ 5x &\equiv -3 \cdot 27 - 14 \cdot 11 && \pmod{297} \\ x &\equiv 6 \cdot 27 + 35 \cdot 11 \equiv 6 \cdot 27 + 8 \cdot 11 \equiv 250 && \pmod{297} \end{aligned}$$

(protože je $27 \cdot 11 \equiv 0$, lze koeficienty u 27 redukovat modulo 11, resp. koeficienty u 11 redukovat modulo 27). O něco přímočařejší a podobně efektivní je substituční metoda.

Příklad

Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 7 && \pmod{27} \\ x &\equiv -3 && \pmod{11} \end{aligned}$$

Řešení

První kongruence $x \equiv 7 \pmod{27}$ má řešení právě $x = 27t + 7$, to dosadíme do druhé kongruence a vyřešíme vzhledem k t:

$$\begin{aligned} 27t + 7 &\equiv -3 && \pmod{11} \\ 5t &\equiv 1 && \pmod{11} \\ t &\equiv 9 && \pmod{11} \end{aligned}$$

Příklad

Vyřešte soustavu kongruencí

$$\begin{aligned} x &\equiv 7 && \pmod{27} \\ x &\equiv -3 && \pmod{11} \end{aligned}$$

Řešení

Opět můžeme psát $t = 11s + 9$ a toto dosadíme do prvního vyjádření:

$$x = 27t + 7 = 27 \cdot (11s + 9) + 7 = 297s + 250$$

To je již řešením soustavy (v "parametrickém tvaru"), lze jej samozřejmě zpětně zapsat jako kongruenci $x \equiv 250 \pmod{297}$.

Příklad

Vyřešte soustavu kongruencí

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

Řešení

Vyřešíme posledním způsobem: z první rovnice máme $x = 10t + 1$, dosadíme do druhé, dostaneme $10t + 1 \equiv 5 \pmod{18}$, tj. $10t \equiv 4 \pmod{18}$ a vyřešíme vzhledem k t:

Příklad

Vyřešte soustavu kongruencí

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

Řešení

$$\begin{aligned} 18t &\equiv 0 \\ 10t &\equiv 4 \\ 8t &\equiv -4 \\ 2t &\equiv 8 \pmod{18} \qquad \Leftrightarrow \quad t \equiv 4 \pmod{9} \\ 0t &\equiv 0 \end{aligned}$$

Tedy $t = 9s + 4 \Rightarrow x = 10t + 1 = 10 \cdot (9s + 4) + 1 = 90s + 41.$

Příklad

Vyřešte soustavu kongruencí

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

Řešení

Řešením soustavy prvních dvou kongruencí je $x = 90s + 41$, to dosadíme do třetí kongruence: $90s + 41 \equiv -4 \pmod{25}$, tj. $15s \equiv 5 \pmod{25}$ a opět vyřešíme vzhledem k s.

$$\begin{aligned} 25s &\equiv 0 \\ 15s &\equiv 5 \\ 10s &\equiv 20 \\ 5s &\equiv 10 \pmod{25} \quad \Leftrightarrow \quad s \equiv 2 \pmod{5} \\ 0s &\equiv 0 \end{aligned}$$

Příklad

Vyřešte soustavu kongruencí

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

Řešení

Máme $s \equiv 2 \pmod{5}$, tj. $s = 5r + 2$ a dosazením získáme

$$x = 90s + 41 = 90 \cdot (5r + 2) + 41 = 450r + 221$$

nebo ekvivalentně $x \equiv 221 \pmod{450}$.

Příklad

Řešte kongruenci $23941x \equiv 915 \pmod{3564}$.

Řešení

Lze řešit standardně, ale čísla budou vycházet velká. Alternativně rozložme $3564 = 4 \cdot 81 \cdot 11$ na součin prvočíselných mocnin a počítejme příklad prvně modulo 4, 81, 11 a na závěr dejme výsledky dohromady pomocí CRT.

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ 46x &\equiv 24 \pmod{81} \\ 5x &\equiv 2 \pmod{11} \end{aligned} \quad \Leftrightarrow \quad \begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv -3 \pmod{81} \\ x &\equiv 7 \pmod{11} \end{aligned}$$

Začneme řešit od nejmenšího modulu: $x = 4t + 3$ dosadíme do poslední kongruence: $4t + 3 \equiv 7 \pmod{11}$, tj. $4t \equiv 4 \pmod{11}$ má zjevně řešení $t \equiv 1 \pmod{11}$, takže $t = 11s + 1$, tj. $x = 44s + 7$ a dosadíme do druhé kongruence: $44s + 7 \equiv -3 \pmod{81}$, tj. $44s \equiv -10 \pmod{81}$ a vyřešíme vzhledem k s.

Příklad

Řešte kongruenci $23941x \equiv 915 \pmod{3564}$.

Řešení

$$
\begin{aligned}
81s &\equiv 0 \\
44s &\equiv -10 \\
37s &\equiv 10 \\
7s &\equiv -20 \\
2s &\equiv 29 \\
1s &\equiv 55 \pmod{81} \\
0s &\equiv 0
\end{aligned}
$$

Dosazením $x = 44s + 7 = 44 \cdot (81r + 55) + 7 = 3564r + 2427$, tj. $x \equiv 2427 \pmod{3564}$.