

MB141 – 11. cvičení

Kongruence

Martin Čadek

Jarní semestr 2020

(A)

Příklad 1. Najděte zbytek po dělení čísla $2^{97^{99}}$ číslem 26.

$26 = 2 \cdot 13$. Číslo $2^{97^{99}}$ je jako mocnina 2 dělitelná dvěma. Tedy $2^{97^{99}} \equiv 0 \pmod{2}$.

Máme zbytek po dělení číslem 13. 13 je prvočíslo, podle malé Fermatovy věty je

$$2^{12} \equiv 1 \pmod{13}$$

Zjistíme, jaký zbytek po dělení 12 dává exponent

$$97^{99} = \underbrace{97 \cdot 97 \cdot \dots \cdot 97 \cdot 97}_{99 \times} \equiv (96+1) \cdot (96+1) \cdot \dots \cdot (96+1)$$

$$\equiv 1 \cdot 1 \cdot \dots \cdot 1 \cdot 1 \equiv 1 \pmod{12}$$

Tedy

$$2^{97^{99}} = 2^{12k+1} = (2^{12})^k \cdot 2 \equiv 1^k \cdot 2 \equiv 2 \pmod{13}$$

Číslo $\pmod{26}$ dává zbytek po dělení 13 zbytek 2

(B)

Příklad 1. Najděte zbytek po dělení čísla 2^{9799} číslem 26.

pon 2 a $13+2=15$. Sudé a lich je páse 2.
Tedy zbytek po dělení čísla 2^{9799} číslem 26
je 2.

(A)

Příklad 2. Najděte všechna řešení kongruence $14x \equiv 19 \pmod{23}$.

Kongruence $ax \equiv b \pmod{n}$ má řešení, právě když největší společný dělitel $d = (a, n)$ dělí číslo b . V našem případě $(14, 23) = 1$ a tedy kongruence musí mít řešení.

1. metoda řešení - pomocí Bezoutovy věty.

Najdeme čísla c, d tak, že
 $14c + 23d = 1 = (14, 23)$.

Metodou z minulého cvičení

14	23	$14c + 23d$
0	1	23
1	0	14
-1	1	9
2	-1	5

14	23	$14c + 23d$
5	-3	1

Tedy $14 \cdot 5 + 23(-3) = 1$
 $14 \cdot 5 \equiv 1 \pmod{23}$

(B)

Příklad 2. Najděte všechna řešení kongruence $14x \equiv 19 \pmod{23}$.

Kongruenci $14 \cdot 5 \equiv 1 \pmod{23}$

vynásobíme 19 (to je přesná strana naší rovnice).

Dostaneme $14 \cdot 5 \cdot 19 \equiv 19 \pmod{23}$

Tedy řešení je $x \equiv 5 \cdot 19 \equiv 5 \cdot (-4) \equiv -20 \equiv 3 \pmod{23}$.

2. metoda řešení - pomocí Eulerovy věty (malé Fermatovy věty). Eulerova funkce $\varphi(23) = 23 - 1 = 22$, neboť

23 je prvočíslo. Platí, že $14^{\varphi(23)} \equiv 1 \pmod{23}$

Tedy rovnici $14x \equiv 19 \pmod{23}$

vynásobíme číslem 14^{22-1} . Dostaneme

©

Příklad 2. Najděte všechna řešení kongruence $14x \equiv 19 \pmod{23}$.

$$14^{22} x \equiv 14^{21} \cdot 19 \pmod{23}$$

$$x \equiv 14^{21} \cdot 19$$

Spočítáme tedy zbytek po dělení čísla $14^{21} \cdot 19$ číslem 23:

$$14^{21} \cdot 19 \equiv 2^6 \cdot 2^6 \cdot 2^6 \cdot 2^3 \cdot (7^2)^{10} \cdot 7 \cdot (-4) \equiv$$

$$\equiv (-5)(-5)(-5) \cdot 8 \cdot 3^{10} \cdot 7 \cdot (-4) \equiv$$

$$\equiv 2(-5) \cdot 8 \cdot 3^3 \cdot 3^3 \cdot 3^3 \cdot 3 \cdot 7 \cdot (-4) \equiv$$

$$\equiv 2(-5) \cdot 8 \cdot 4 \cdot 4 \cdot 4 \cdot 3 \cdot 7 \cdot (-4) \equiv$$

$$\equiv 16 \cdot 16 \cdot 16 \cdot 5 \cdot 3 \cdot 7 \equiv (-7)(-7)(-7) \cdot 7 \cdot 5 \cdot 3$$

$$\equiv 3 \cdot (-3) \cdot 3 \cdot 5 \equiv (-4) \cdot 5 \equiv -20 \equiv 3$$

Tedy $x \equiv 3 \pmod{23}$

(D)

Příklad 2. Najděte všechna řešení kongruence $14x \equiv 19$
(mod 23).

3. metoda je upravením levé i pravé strany pomocí modulu (v tomto případě 23) a dělení. Mnohdy je to nejrychlejší způsob, ale není algoritmický a v případě n'ce skusivost:

$$14x \equiv 19 \pmod{23}$$

$$14x \equiv -4 \pmod{23}$$

$$7x \equiv -2 \pmod{23}$$

$$7x \equiv 21 \pmod{23}$$

$$x \equiv 3 \pmod{23}$$

2 je nesoudělné s 23
můžeme dělit

$(7, 23) = 1$, můžeme dělit

4. metoda - upravením dvou kongruencí $23x \equiv 0$ a

$$14x \equiv 19 \pmod{23}$$

(E)

Příklad 2. Najděte všechna řešení kongruence $14x \equiv 19$
(mod 23).

$$23x \equiv 0 \pmod{23}$$

$$14x \equiv 19 \pmod{23}$$

$$9x \equiv -19 \equiv 4 \pmod{23}$$

$$5x \equiv 15 \pmod{23}$$

$$x \equiv 2 \cdot 15 - 4 \pmod{23}$$

$$x \equiv 26 \pmod{23}$$

$$x \equiv 3 \pmod{23}$$

odečtením

od 2. odečteme 3.

Zde bychom mohli dělit 5,
ale od 2 + 4. kongruence
odečtem 3.

Tento způsob je analogický hledání koeficientů c, d takových, že $14c + 23d = 1$, jinou místo rovnosti považiva kongruenci mod 23.

(A)

Příklad 3. Najděte všechna řešení kongruence $325x \equiv 694 \pmod{471}$.

Počítat $325^{g(471)-1}$ se nám jistě nechce.

Pomocí Bezoutovy věty by se jistě šlo zkusit sami. Zde si předvedeme kombinaci 4. a 3.

metody:

$$(1) \quad 471x \equiv 0 \pmod{471}$$

$$(2) \quad 325x \equiv 694 \pmod{471}$$

$$(3) \quad 146x \equiv -694 \pmod{471}$$

sanktita odcitena
(1) - (2)

$$(4) \quad 73x \equiv -347 \pmod{471}$$

delime 2

$$73x \equiv 124$$

$$(5) \quad 33x \equiv -6 \cdot 124 \pmod{471}$$
$$\equiv 198 \pmod{471}$$

(1) - 6 * (4)

$$(6) \quad 5x \equiv 10 \cdot 198 - 694 \pmod{471}$$
$$\equiv 344 \pmod{471}$$

10 * (5) - (2)

3

Příklad 3. Najděte všechna řešení kongruence $325x \equiv 694 \pmod{471}$.

Od (3) odečteme 29 krát (6)

$$\begin{aligned}x &\equiv -694 - 29 \cdot 344 \\ &\equiv -694 + 29 \cdot 127 \\ &\equiv 2989 \equiv 163\end{aligned}$$

Řešením naší kongruence je $x \equiv 163 \pmod{471}$.

Příklad 4. Najděte všechna celá čísla, která vyhovují soustavě kongruencí

(A)

$$\begin{aligned}21x &\equiv 27 \pmod{24}, \\26x &\equiv 10 \pmod{25}, \\27x &\equiv 30 \pmod{17}.\end{aligned}$$

Nejprve zjednodušíme

$$\begin{aligned}21x &\equiv 3 \pmod{24} \\x &\equiv 10 \pmod{25} \\10x &\equiv 13 \pmod{17}\end{aligned}$$

V 1. kongruenci pro modul 8 obě strany dělitelně 3 změni.

Přeloží soustavu ekvivalentně

$$\begin{aligned}7x &\equiv 1 \pmod{8} \\x &\equiv 10 \pmod{25} \\10x &\equiv 13 \pmod{17}.\end{aligned}$$

Najdeme řešení poslední kongruenci. 2 rovnice

$$\begin{aligned}17x &\equiv 0 \pmod{17} \\10x &\equiv 13 \pmod{17}\end{aligned}$$

Příklad 4. Najděte všechna celá čísla, která vyhovují soustavě kongruencí

(B)

$$21x \equiv 27 \pmod{24},$$

$$26x \equiv 10 \pmod{25},$$

$$27x \equiv 30 \pmod{17}.$$

Dokážeme

$$7x \equiv -13 \equiv 4 \pmod{17}$$

$$3x \equiv 9 \pmod{17}$$

$$x \equiv 3 \pmod{17}$$

Tedy $x = 17y + 3$. *Dosadíme do 2. kongruence*

$$x = 17y + 3 \equiv 10 \pmod{25}$$

$$-8y \equiv 7 \pmod{25}$$

$$-24y \equiv 21 \pmod{25}$$

$$y \equiv 21 \pmod{25}$$

Proto $y = 25z + 21$,

$$x = 17(25z + 21) + 3 = 17 \cdot 25z + 17 \cdot 21 + 3$$

Dosadíme do 1. kongruence

Příklad 4. Najděte všechna celá čísla, která vyhovují soustavě kongruencí

②

$$21x \equiv 27 \pmod{24},$$

$$26x \equiv 10 \pmod{25},$$

$$27x \equiv 30 \pmod{17}.$$

$$7x = 7 \cdot (17 \cdot 25z + 17 \cdot 21 + 3) \equiv 1 \pmod{8}$$

$$(-1)(1 \cdot 1 \cdot z + 1 \cdot 5 + 3) \equiv 1 \pmod{8}$$

$$-z - 8 \equiv 1 \pmod{8}$$

$$z \equiv 7 \pmod{8}$$

$$z = 8a + 7$$

Dosazením

$$x = 17 \cdot 25(8a + 7) + 17 \cdot 21 + 3 = 3400a + 17 \cdot 25 \cdot 7$$

$$+ 17 \cdot 21 + 3 \equiv 3400a + 3335$$

Všechna celá čísla, která vyhovují sadě daných kongruencí jsou tvaru $3400a + 3335$, kde $a \in \mathbb{Z}$.

(A)

Příklad 5. Najděte inverzní prvek k číslu 157 modulo 2475.

Podle Eulerovy věty

$$157^{\varphi(2475)} \equiv 1 \pmod{2475}$$

(157 a 2475 jsou nesoudělná), je inverse k číslu

$$157 \pmod{2475} \text{ rovná } 157^{\varphi(2475)-1} \pmod{2475}.$$

Platí $2475 = 25 \cdot 11 \cdot 9$, tedy $\varphi(2475) = 5 \cdot 4 \cdot 10 \cdot 3 \cdot 2$
 $= 1200$ ($\varphi(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}) = p_1^{\alpha_1-1} (p_1-1) p_2^{\alpha_2-1} (p_2-1) p_3^{\alpha_3-1} (p_3-1)$)

Číslo $157^{1199} \pmod{2475}$ se nám nechce počítat (nemáme na výpočet existující efektivní algoritmy - viz. příloha 12. přednáška). Budeme tedy řešit kongruenci

$$157x \equiv 1 \pmod{2475}$$

Příklad 5. Najděte inverzní prvek k číslu 157 modulo 2475.

Uděláme to tentokrát tak, se ji rozdělíme na tři kongruence

$$(1) \quad 157x \equiv 1 \pmod{25}$$

$$(2) \quad 157x \equiv 1 \pmod{11}$$

$$(3) \quad 157x \equiv 1 \pmod{9}$$

Řešíme 1. kongruenci:

$$157x \equiv 1 \pmod{25}$$

$$7x \equiv 1 \pmod{25}$$

$$49x \equiv 7 \pmod{25}$$

$$-x \equiv 7 \pmod{25}$$

$$x \equiv 18 \pmod{25}$$

Přelo $x = 25y + 18$. Dosadíme do 2. kongruence

$$157(25y + 18) \equiv 1 \pmod{11}$$

$$3(3y - 4) \equiv 1 \pmod{11}$$

(c)

Příklad 5. Najděte inverzní prvek k číslu 157 modulo 2475.

$$9y - 12 \equiv 1 \pmod{11}$$

$$-2y \equiv 2 \pmod{11}$$

$$y \equiv -1 \equiv 10 \pmod{11}$$

Přelo $y = 11z + 10$, $x = 25(11z + 10) + 18$. Dosadíme
do 3. kongruence:

$$157(25(11z + 10) + 18) \equiv 1 \pmod{9}$$

$$4 \{ (-2)(2z + 1) \} \equiv 1 \pmod{9}$$

$$(-8)(2z + 1) \equiv 1 \pmod{9}$$

$$2z - \equiv 0 \pmod{9}$$

$$z \equiv 0 \pmod{9}$$

$$\begin{aligned} \text{Přelo } z = 9a, \quad x &= 25(11 \cdot 9a + 10) + 18 = \\ &= 2475a + 268 = 2475a + 268 \end{aligned}$$

Inverzní prvek je $268 \pmod{2475}$.

Příklad 6. Najděte všechny primitivní kořeny

(A)

(a) modulo 20,

(b) modulo 26.

(a) $20 = 2^2 \cdot 5$. Eulerova funkce je $\varphi(20) = 2 \cdot (2-1) \cdot (5-1) = 8$

Vezmeme nesoudělné slytky mod 20 (nesoudělné s 20). Jejich řád je nejmenší kladné celé číslo n takové, že $a^n \equiv 1 \pmod{20}$.

Pro všechna tato čísla platí podle Eulerovy věty $a^{\varphi(20)} = a^8 \equiv 1 \pmod{20}$.

Prvky, jejichž řád je $8 = \varphi(20)$, nazýváme primitivními kořeny.

Nesoudělné slytky s 20 jsou

$$1, 3, 7, 9, 11 \equiv -9 \pmod{20}, 13 \equiv -7, 17 \equiv -3, 19 \equiv -1$$

Řád těchto prvků musí dělit číslo $\varphi(20) = 8$.

Příklad 6. Najděte všechny primitivní kořeny

(B)

(a) modulo 20,

(b) modulo 26.

Je tedy 1, 2, 4 nebo 8.

Zřejmě $1^1 \equiv 1$, $3^2 \equiv 9$, $3^4 \equiv 81 \equiv 1$, $7^2 = 49 \equiv 9$, $7^4 \equiv 9^2 \equiv 1$,
 $9^2 \equiv 1$, $11^2 = (-9)^2 \equiv 1$, $13^2 = (-7)^2 \equiv 9$, $13^4 = (-7)^4 \equiv 1$, $17^4 \equiv$
 $(-3)^4 \equiv 1$, $19^2 \equiv (-1)^2 \equiv 1$.

Tedy řád je 2 u prvků 9, 11, 19 a 4 u prvků 3, 7, 13 a 17. Řádný prvek není primitivní kořen.

(b) $26 = 2 \cdot 13$, $\varphi(26) = 1 \cdot 12 = 12$

Tedy řád prvků může být 1, 2, 3, 4, 6, 12.

$3^3 \equiv 1$, $5^2 \equiv -1$, $5^4 \equiv 1$, $7^2 \equiv 49 \equiv -3$, $7^6 \equiv 9$, $7^6 \equiv -27 \equiv -1$, $7^3 \equiv 5$

$7^{12} \equiv 1$ Tedy 7 je primitivní kořen. Tole's plati

pro 19 $\equiv -7$, $9^2 \equiv 3$, $9^3 \equiv 3 \cdot 9 \equiv 1$, $17^6 \equiv (-9)^6 \equiv ((-9)^3)^2 \equiv (-1)^2 \equiv 1$,

Příklad 6. Najděte všechny primitivní kořeny

©

(a) modulo 20,

(b) modulo 26.

$$11^2 \equiv 121 \equiv 17, \quad 11^3 \equiv 17 \cdot 11 \equiv 181 \equiv 5, \quad 11^4 \equiv 17^2 \equiv (9)^2 \equiv 3,$$

$$11^6 \equiv 5^2 \equiv -1, \quad 11^{12} \equiv 1$$

11 je roven primitivní moc a také bude platit

$$\text{a } 26 - 11 = 15,$$

Primitivní prvky jsou 7, 11, 15 a 19.