4.1 (i) $5x \equiv 12 \mod 23$ $\quad |\cdot 5$

$$25x \equiv 60 \mod 23$$

$$2x \equiv -9 \mod 23 \quad |\cdot 12$$

$$24x \equiv -108 \mod 23$$

$$x \equiv -108+115 \equiv 7 \mod 23$$

$$\boxed{x \equiv 7 \mod 23}$$

Jinak: $5x \equiv 12 \mod 23$ $\quad |\cdot 5^{21}$

$$23x \equiv \cancel{0} \mod 23$$

$(5, 23) = 1$ $\qquad 5^{\varphi(23)} \equiv 1 \mod 23$

$$5^{22} \equiv 1 \mod 23$$

$$5 \cdot 5^{21} \equiv 1 \mod 23$$

$$\underbrace{5^{21} 5}_{1} x \equiv 5^{21} \cdot 12 \mod 23$$

$$x \equiv 5^{21} 12 = 5 \cdot 12 (5^2)^{10} \equiv$$

$$\equiv 5 \cdot 12 \cdot 2^{10} = 5 \cdot 12 \cdot (2^5)^2 \equiv$$

$$\equiv 5\cdot 12(+9)^2 \equiv 60\cdot 81$$
$$\equiv -9\cdot 12 \equiv -3\cdot 36 \equiv$$
$$\equiv -3\cdot 13 \equiv -39 \equiv 7 \mod 23$$

Ještě jinak: $5x = 12 \mod 23 \quad /\cdot 14$

$(5,23) = 1 \rightsquigarrow 5\cdot a + 23\cdot b = 1$

$5\cdot a \equiv 1 \mod 23$

uhádnutí a, b $\rightsquigarrow 5\cdot 14 + \underbrace{23\cdot(-3)}_{-69} = 1$

$$5\cdot 14\, x \equiv 14\cdot 12 \mod 23$$
$$x \equiv 7\cdot 24 \mod 23$$
$$x \equiv 7 \mod 23$$

Teorie: $ax \equiv b \mod m$

má řešení $\iff d \mid b$

$d = (a,m)$

- $f(x) \equiv 0 \mod m$ — tříd mod m

f polynom $\rightsquigarrow$ řešením je sjednocení

4.1.(ii) $33x = 7 \mod 143$

$$d = (33, 143) = 11$$

$$143 = 11 \cdot 13$$

$11 \nmid 7$ nemá řešení

4.1.(iii) $210x \equiv 40 \mod 212$ $\quad /:5$

$$42x \equiv 8 \mod 212$$

$$212 = 4 \cdot 53$$

$$d = (42, 212) = 2 \mid 8$$

lépe $\quad -2x \equiv 40 \mod 212 \quad /:2$

$$-x \equiv 20 \mod 106$$

$$x \equiv -20 \mod 106$$

$\Rightarrow \quad x = 212a - 20$

nebo $\quad x = 212a - 20 + 106$

Výsledek: $\quad x \equiv -20 \mod 212$

nebo $\quad x \equiv 86 \mod 212$

Pr 4.2: (i) $2x \equiv 3 \mod 7 \;/\cdot 4$
$x \equiv 8 \mod 15$

$8x \equiv 12 \mod 7$
$x \equiv 8 \mod 15$

$$\boxed{\begin{aligned} x &\equiv 5 \mod 7 \\ x &\equiv 8 \mod 15 \end{aligned}}$$

$x = 7y + 5$

$7y + 5 \equiv 8 \mod 15 \;/\cdot 2$

$14y \equiv 2 \cdot 3 \mod 15$

$-y \equiv 6 \mod 15$

$y \equiv -6 \mod 15$

↳ dosadimo do $x = 7y+5$

$x = 7(15r - 6) + 5$

$= 105r - 42 + 5 = 105r - 37$

Výsledek: $x \equiv -37 \mod 105$

Teorie: Čínská zbytková věta

$x \equiv a_1 \mod m_1$

$\vdots$

$x \equiv a_k \mod m_k$

Jsou-li $a_1, \dots, a_k$ po dvou nesoudělná, pak má soustava právě jedno řešení mod $m_1 \cdot \ldots \cdot m_k$

Věta: $x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$d = (m_1, m_2)$

má řešení $\Longleftrightarrow a_1 \equiv a_2 \mod d$

Řešení najdem mod NSN(m_1, m_2)

Př 4.2 (ii)

$$x \equiv 3 \mod 10 = 2 \cdot 5$$
$$x \equiv 8 \mod 15 = 3 \cdot 5$$
$$x \equiv 5 \mod 84 = 4 \cdot 3 \cdot 7$$

$$\Leftrightarrow \quad \begin{aligned} x &\equiv 3 \mod 2 \\ x &\equiv 3 \mod 5 \end{aligned}$$

$$\Leftrightarrow \quad \begin{aligned} x &\equiv 8 \mod 3 \\ x &\equiv 8 \mod 5 \end{aligned}$$

$$\Leftrightarrow \quad \begin{aligned} x &\equiv 5 \mod 4 \\ x &\equiv 5 \mod 3 \\ x &\equiv 5 \mod 7 \end{aligned}$$

$$\left.\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 1 \mod 4 \\ x &\equiv 5 \mod 7 \end{aligned}\right\} \text{ jediné řešení } \mod 3 \cdot 5 \cdot 4 \cdot 7 = 420$$

↳ $x = 3y - 1$ dosadíme do zbývajících 3 kongruencí

$$3y - 1 \equiv 3 \mod 5 \quad /\cdot 2$$
$$3y - 1 \equiv 1 \mod 4$$
$$3y - 1 \equiv 5 \mod 7 \quad /\cdot 2$$

$$y \equiv 8 \equiv 3 \mod 5$$
$$-y \equiv 2 \mod 4$$
$$3y \equiv 6 \mod 7$$

$$\boxed{\begin{aligned} y &\equiv 3 \mod 5 \\ y &\equiv -2 \mod 4 \\ y &\equiv 2 \mod 7 \end{aligned}}$$

atd.

. . . . výsledek . .

$$x \equiv 173 \mod 420$$

Př 4.3. (i) $\quad 7x^{17} \equiv 11 \mod 41$

$\cdot 6$

$42x^{17} \equiv 66 \mod 41$

$$\boxed{x^{17} \equiv 25 \mod 41}$$

41 má primitivní kořen 6

$\Rightarrow \quad x = 6^y$

$(6^y)^{17} = 6^{17y} \equiv 25 \mod 41$

$\qquad\qquad\qquad\qquad\qquad\quad \rotatebox{90}{$\equiv$}$

$\qquad\qquad\qquad\qquad\qquad\quad 6^{\text{něco}}$

$6^2 = 36 \equiv -5 \mod 41$

$6^4 \equiv 25 \mod 41$

$6^{17y} \equiv 6^4 \mod 41$

prim.

$17y \equiv 4 \mod \varphi(41) = 40$

$\cdot 2$

$34y \equiv 8 \mod 40$

$$-6y \equiv 8 \mod 40 \quad /:2$$

$$-3y \equiv 4 \mod 20 \quad /\cdot 7$$

$$-21y \equiv 28 \mod 20$$

$$-y \equiv 8 \mod 20$$

$$y \equiv 12 \mod 20$$

$y = 40a + 12$ nebo

$y = 40a + 12 + 20$

$\Rightarrow \quad y \equiv 12$ nebo $y \equiv 32$ mod 40

??

$$17y \equiv 4 \mod 40 = 5 \cdot 8$$

$$\Leftrightarrow \quad 17y \equiv 4 \mod 5$$

$$17y \equiv 4 \mod 8$$

$$2y \equiv 4 \mod 5$$

$$y \equiv 4 \mod 8$$

$$y = 5r + 2 \rightarrow \left|\begin{array}{l} y \equiv 2 \mod 5 \\ y \equiv 4 \mod 8 \end{array}\right.$$

$$5r + 2 \equiv 4 \mod 8$$

$$-3r \equiv 2 \mod 8 \quad / \cdot 3$$

$$-9r \equiv 6 \mod 8$$

$$-r \equiv -2 \mod 8$$

$$r \equiv 2 \mod 8$$

$$r = 8w + 2$$

$$\hookrightarrow y = 5r + 2 = 40w + 10 + 2$$

$$\boxed{y \equiv 12 \mod 40}$$

$$6^{40} \equiv 1 \mod 41$$

$$x = 6^{y} \mod 41$$

$$6^{12} \equiv (36)^{6} \equiv (-5)^{6} \equiv ((-5)^{3})^{2} \equiv$$

$\equiv (-125)^2 \equiv (-2)^2 \equiv 4 \mod 41$

$\boxed{x \equiv 4 \mod 41}$ ← výsledok

<u>Teorie</u>: koreň: $x^n \equiv a \mod m$

Nechť $(a,m)=1$, m má primitívní korene. Pak

$x^n \equiv a \mod m$ $\quad d=(n,\varphi(m))$

má řešení $\Leftarrow$ $a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m$

- pak ex. d řešení $\mod m$

Náš příklad: $d=(17,40)=1$

$25^{40} \equiv 1 \mod 41$

platí E. věta

4.3(ii) $x^3 \equiv 3 \mod 18$

$(3, 18) = 3 > 1 \Rightarrow$ nejde použít předchozí věta

$x = 3y$

$27y^3 \equiv 3 \mod 18$

$(27, 18) = 9 \nmid 3$

nemá řešení

(iii) $x^2 \equiv 18 \mod 63$

$(18, 63) = 9 \mid x^2 \Rightarrow x = 3y$

$\boxed{9y^2 \equiv 18 \mod 63}$ $:9$

$(9, 63) = 9 \mid 18 \Rightarrow$

$y^2 \equiv 2 \mod 7$

$\leadsto$ předchozí věta: $(2, 7) = 1$

$a^{\frac{\varphi(m)}{d}} = 2^{\frac{\varphi(7)}{2}} = 2^3 = 1$ $\qquad d = (n, \varphi(m))$

mod 7

$d = (2,6) = 2$

$\Rightarrow$ existují řešení dvě pro y
(právě 2)

$y^2 \equiv 2 \mod 7$ má řešení
$y \equiv \pm 3 \mod 7$

$y \in \{\pm 3, \pm 10, \pm 17, \pm 24, \dots\} \mod 63$

$\begin{matrix} \\ \shortparallel \\ 7 \cdot 9 \end{matrix}$

$3y \in \{\pm 9, \pm 30, \underset{\underset{\pm 12}{\equiv}}{\pm 51}\}$

Závěr!
nebo

$$\left.\begin{aligned} x &\equiv \pm 9 \\ x &\equiv \pm 12 \\ x &\equiv \pm 30 \end{aligned}\right\} \mod 63$$