- $a \equiv b \pmod m$
- $c \equiv d \pmod m$

$\overset{def.}{\Leftrightarrow}\ m \mid (a-b)$

$\Rightarrow\ a \square c \equiv b \square d \pmod m$

$+, -, \cdot$

$m \mid a,\ m \mid b \Rightarrow m \mid (a+b),\ m \mid (a-b),\ m \mid (a \cdot b)$

$m \mid (a-b),\ m \mid (c-d) \Rightarrow m \mid (a-b)+(c-d) = (a+c)-(b+d)$

$\Downarrow$

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

---

1) a)

$a \equiv b \pmod m \Leftrightarrow ca \equiv cb \pmod{cm}$

„$\Rightarrow$": $m \mid (a-b) \Rightarrow \exists k \in \mathbb{Z}.\ m \cdot k = a-b$

$c \cdot m \cdot k = c(a-b)$

$cm \mid c(a-b) = ca-cb$

$ca \equiv cb \pmod m$

„$\Leftarrow$": to samo z prawa dolewa

1b) $NSD(c, m)$

„$\Rightarrow$": $a \equiv b \pmod m \Rightarrow ac \equiv bc \pmod m$

$m \mid (a-b) \Rightarrow m \mid c(a-b) = ca-cb$

„$\Leftarrow$" $ac \equiv bc \pmod m \Rightarrow m \mid (ac-bc) = c(a-b)$

$m \mid c \cdot (a-b) \Rightarrow m \mid a-b$

$NSD(c, m) = 1$

---

2)a $x \equiv 2 \pmod 8$ $\quad 8 \mid (x-2)$

$x = 2$

$x = 8k+2$

$k \in \mathbb{Z}$

$8k+l,\ l \in \{0, 1, \dots, 7\}$

$\Rightarrow \cancel{8k} + l \equiv 2 \pmod 8$

$l \equiv 2 \pmod 8$

$\Rightarrow l = 2$

c) $6x \equiv 2 \pmod 8 \quad /:2$

$3x \equiv 1 \pmod 4 \quad /\cdot 3$

$x \equiv 3 \pmod 4$

$x = 4k+3$

b) $3x \equiv 2 \pmod 5 \quad /\cdot 2$ $\quad 3 \cdot 2 \equiv 1 \pmod 5$

$x \equiv 4 \pmod 5$

$x = 5k+4$

d) $x^2 \equiv 36 \pmod{45}$

$45 \mid x^2 - 36 = (x-6)(x+6)$

$45 = 5 \cdot 3 \cdot 3$

$3 \mid (x-6)$

$3 \mid (x+6)$

i) $5 \mid (x-6) \Rightarrow 15 \mid x-6$

ii) $5 \mid (x+6) \Rightarrow 15 \mid x+6$

$x \equiv -6 \equiv 9 \pmod{15}$

$x = 15k+9$

$x \equiv 6 \pmod{15}$

$x = 15k+6$

3) $n^2 \equiv 1 \pmod 8$, n liché

$n = 8k + \ell$, $\boxed{\ell \in \{1,3,5,7\}}$

$(8k+\ell)^2 = \underbrace{64k^2}_{0} + \underbrace{16k\ell}_{0} + \ell^2 \equiv 1 \pmod 8$

$\ell^2 \equiv 1 \pmod 8$

$1 \checkmark \quad 3 \cdot 3 = 9 \equiv 1 \checkmark$

$5 \cdot 5 = 25 \equiv 1 \checkmark \quad 7 \cdot 7 = 49 \equiv 1 \checkmark$

4) $x^2 \equiv 1 \pmod p$, p prvočíslo

$p \mid (x^2 - 1) = (x-1)(x+1)$

(i) $p \mid (x-1) \Rightarrow x \equiv 1 \pmod p \Rightarrow x = pk + 1$

(ii) $p \mid (x+1) \Rightarrow x \equiv -1 = p-1 \pmod p$

$\Rightarrow x = pk - 1$

$k \in \mathbb{Z}$

5) $x^2 + 10x + 6 \equiv 0 \pmod{17}$ * $\boxed{0 \equiv -17 \pmod{17}}$

$x^2 + 10x + 6 - 17 \equiv 0 \pmod{17}$

$x^2 + 10x - 11 \equiv 0 \pmod{17}$

$(x+11)(x-1) \equiv 0 \pmod{17}$

$17 \mid (x+11)(x-1)$

$\boxed{\begin{array}{l} x = 17k - 11 \\ x = 17k + 1 \end{array}}$

alternativní pokus:

$(x+5)^2 \equiv 19 \pmod{17}$

$17 \mid (x+5)^2 - 19$

$a^2 - b^2 = (a-b)(a+b)$

6)a) $1000a + 100b + 10c + d = \underbrace{999a + 99b + 9c}_{9} + \underbrace{a+b+c+d}_{9}$

$9 \mid (a+b+c+d)$

b) $1000a + 100b + 10c + d = 990a + 99b + \underbrace{10a + b + 10c + d}_{-a+b-c+d} =$

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

7) $\boxed{a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \dots + a + 1)}$