DÚ

① $3x-1+a \equiv 0 \ (6)$
$2x-7 \equiv 0 \ (9)$

$2x \equiv 7 \ (9)$
$x \equiv -1 \ (9)$
$x = -1+9s, s \in \mathbb{Z}$ a dosadíme:

$3(-1+9s)-1+a \equiv 0 \ (6)$
$27s \equiv 4-a \pmod 6$
$3s \equiv 4-a \ (6)$

Podmínka řešitelnosti: $(3,6)=3 \mid 4-a$
Tj. $a \equiv 1 \pmod 3$

Píšeme $a = 1+3k$, $k \in \mathbb{Z}$
$3s \equiv 3-3k \ (6) \ /:3$
$s \equiv 1-k \pmod 2$

$x = 8-9k+18t \Leftarrow s = 1-k+2t, k \in \mathbb{Z} \Leftarrow$
$= 8-9\left(\frac{a-1}{3}\right)+18t = 11-3a+18t, t \in \mathbb{Z}$
$x \equiv 11-3a \pmod{18}$
za podmínky, že $a \equiv 1 \ (3)$.

② Řešte kongruenci $x^5+2 \equiv 0 \pmod{35}$

Řeš: soustava

$x^5+2 \equiv 0 \ (5)$ | $x^5+2 \equiv 0 \ (7)$

MFV: $x^5 \equiv x \ (5)$ | 1. výjimečné 7 možností
$x+2 \equiv 0 \ (5)$ | 2. vyzkoušíme
$\forall x \in \mathbb{Z}$ | $x \equiv 3 \ (5)$ | ad 2. $x \equiv 0 \ (7)$ není řešení | 3. přes primitivní kořen

nemůžeme vyloučit řešení a dosadit do 2. kongruence

$x \not\equiv 0 \ (7) \Rightarrow$ vyjádřit x:
$x^6+2x \equiv 0 \ (7)$
$1+2x \equiv 0 \ (7)$
$2x \equiv 6 \ (7)$
$x \equiv 3 \ (7)$

$x^6 \equiv 1 \ (7)$ pro $x \not\equiv 0 \ (7)$

Řešením je $x \equiv 3 \ (35)$.

Alternativně postupem 3.: zjistíme primitivní kořen modulo 7

n	1	2	3	4	5	6
(mod 7) 2^n	2	4	1			
3^n	3	2	6	4	5	1

$x^5 \equiv -2 \ (7)$
$(3^y)^5 \equiv 3^5 \ (7)$
$3^{5y} \equiv 3^5 \ (7) \Leftrightarrow 5y \equiv 5 \pmod 6$
$x \equiv 3^1 \equiv 3 \ (7) \Leftarrow y \equiv 1 \ (6)$

substituce $x \equiv 3^y$
$-2 \equiv 3^5$

(3) $x^6 - 1 \equiv 0 \pmod{35}$

Řeš:

$x^6 \equiv 1 \ (5)$ $\quad x^6 \equiv 1 \ (7)$

$x^5 \equiv x \ (5)$ $\quad x^2 \equiv 1 \ (5)$ $\quad$ MFV: $x \not\equiv 0 \ (7)$

$5 \mid x^2 - 1 = (x+1)(x-1)$ $\quad x \equiv \pm 1, \pm 2, \pm 3 \ (7)$

$\Rightarrow 5 \mid x+1 \vee 5 \mid x-1$

$x \equiv \pm 1 \ (5) \Leftrightarrow x \equiv 1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 26, 29, 31, 34 \pmod{35}$

kongruence mod 12 řešil: $\nearrow$ $x \equiv \pm 1, \pm 4, \pm 6, \pm 9, \pm 11, \pm 16 \pmod{35}$

(4) Určete počet řešení kongruence

$x^7 \equiv 12 \pmod{29^2}$

Řeš.: binomická kongruence + Henselovo lemma

$x^7 \equiv 12 \pmod{29}$

Řešíme s využitím prim. báze mod 29

n	1	2	3	4	5	6	7	...	14	...	28
$(\mathrm{mod}\ 29)$ 2^n	2	4	8	16	3	6	12		-1		1

subst. $x \equiv 2^y \ (29)$, $12 \equiv 2^7 \ (29)$ $\quad (2^y)^7 \equiv 2^7 \ (29)$

$7y \equiv 7 \ (28) \ | :7 \quad (7, 28) \mid 7 \Rightarrow 7$ řešení

$y \equiv 1 \ (4) \Rightarrow x \equiv 2^1, 2^5, 2^9, 2^{13}, 2^{17}, 2^{21}, 2^{25} \ (29)$

$x \equiv 2, 3, 19, 17, -8, -12, -18 \ (29)$

Henselovo lemma: pro řešení $a \in \mathbb{Z}$ kongruence mod p platí, že pokud $f'(a) \not\equiv 0 \ (p)$, kongruence mod p^n má jediné řešení $x \equiv a \pmod{p}$.

$f(x) = x^7 - 12$

$f'(x) = 7 \cdot x^6 \quad 7 \cdot x^6 \equiv 0 \pmod{29} \Leftrightarrow$

$\Leftrightarrow x^6 \equiv 0 \ (29) \Leftrightarrow 29 \mid x \Leftrightarrow x \equiv 0 \ (29)$.

Hensel $\Rightarrow$ máme 7 řešení kongruence $x^7 \equiv 12 \pmod{29^2}$

(5) Určete počet řešení $x^7 \equiv 0 \ (29^2)$

Řeš: mod 29: $x^7 \equiv 0 \ (29) \Leftrightarrow 29 \mid x^7 \Leftrightarrow 29 \mid x \Leftrightarrow x \equiv 0 \ (29)$

$f'(0) \equiv 0 \pmod{29} \Rightarrow$ nelze přímo Hensel $\quad x = 29k, k \in \mathbb{Z}$

$29^7 k^7 \equiv 0 \pmod{29^2}$

$0 k^7 \equiv 0 \pmod{29^2}$

(6) Řešte kongruenci $6x^2+5x+1 \equiv 0 \ (13)$

Řeš: i) $(3x+1)(2x+1) \equiv 0 \ (13) \Leftrightarrow 13 \mid (3x+1)(2x+1)$

$\Leftrightarrow 13 \mid 3x+1 \ \vee \ 13 \mid 2x+1$

$\Leftrightarrow 3x+1 \equiv 0 \ (13) \ \vee \ 2x+1 \equiv 0 \ (13)$

$x \equiv 4 \ (13) \ \vee \ x \equiv 6 \ (13)$

ii) standardní způsob:

(1) normovat $\rightsquigarrow$ $x^2+Bx+C \equiv 0 \ (p)$

(2) doplnit na čtverec $(x+\frac{B}{2})^2 - \frac{B^2}{4}+C$

(3) vyřešit binomickou kongruenci $y^2 \equiv A \ (p)$

ad (1) $6x^2+5x+1 \equiv 0 \ (13) \ | \cdot(-2)$

$-12x^2-10x-2 \equiv 0 \ (13)$

$x^2+3x-2 \equiv 0 \ (13)$

ad (2) $x^2+16x-2 \equiv 0 \ (13)$

$(x+8)^2-64-2 \equiv 0 \ (13)$

y

$y^2 \equiv 66 \ (13)$

$y^2 \equiv 1 \ (13)$

$y \equiv \pm 1 \ (13) \Rightarrow x \equiv -7 \ (13) \ \vee \ x \equiv -9 \ (13)$

$x \equiv 6 \ (13) \ \vee \ x \equiv 4 \ (13)$

Pozn: $2x=1$ sudá = lichá

kongruence $6x^2+5x+1 \equiv 0 \ (\mathrm{mod}\ m)$ je řešitelná $\forall m \in \mathbb{N}$

(a přitom rovnice $6x^2+5x+1=0$ nemá řešení v $\mathbb{Z}$)

$\parallel$

$(3x+1)(2x+1)=0$ řešení: $x=-\frac{1}{3}, -\frac{1}{2} \notin \mathbb{Z}$

$(3x+1)(2x+1) \equiv 0 \ (\mathrm{mod}\ 2^k \cdot \ell)$ $\quad m = 2^k \cdot \ell, \ 2 \nmid \ell$

$(2^k, \ell) = 1$

$(3x+1)(2x+1) \equiv 0 \ (\mod 2^k)$

mod řešení, tj. $2^k \mid (3x+1)(2x+1)$

$3x+1 \equiv 0 \ (\mod 2^k)$

mod řešení, tj. $2^k \mid 3x+1$

$3x \equiv -1 \ (\mod 2^k)$

je řeš. $\Leftrightarrow (3, 2^k) \mid -1$ ✓

$\parallel$

1

$(3x+1)(2x+1) \equiv 0 \ (\mod \ell)$

mod řešení

$2x+1 \equiv 0 \ (\mod \ell)$

mod řešení

$2x \equiv -1 \ (\mod \ell)$

je řešitelná $\Leftrightarrow (2, \ell) \mid -1$ ✓

$\parallel$

1