Příklad 1

a) $(113, 50)$

$113 : 50 = 2$ zb. 13 $\Rightarrow 13 = 113 - 2 \cdot 50$

$50 : 13 = 3$ zb. 11 $\Rightarrow 11 = 50 - 3 \cdot 13$

$13 : 11 = 1$ zb. 2 $\Rightarrow 2 = 13 - 1 \cdot 11$

$11 : 2 = 5$ zb. 1 $\Rightarrow 1 = 11 - 5 \cdot 2$

$2 : 1 = 2$ zb. 0

$$1 = 11 - 5 \cdot 2$$
$$= 11 - 5(13 - 1 \cdot 11) = -5 \cdot 13 + 6 \cdot 11$$
$$= -5 \cdot 13 + 6(50 - 3 \cdot 13) = 6 \cdot 50 - 23 \cdot 13$$

b) $(3^{77} - 1, 3^{21} - 1)$

$(3^{77} - 1) : (3^{21} - 1) = 3^{56} + 3^{35} + 3^{14}$

$-(3^{77} - 3^{56})$

$3^{56} - 1$

$-(3^{56} - 3^{35})$

$3^{35} - 1$

$3^{35} - 3^{14}$

$3^{14} - 1$ zb.

$$3^7 - 1 = (3^{21} - 1) - 3^7(3^{14} - 1)$$
$$= (3^{21} - 1) - 3^7 \cdot ((3^{77} - 1) - (3^{56} + 3^{35} + 3^{14})(3^{21} - 1))$$
$$= (3^{21} - 1)[3^{63} + 3^{42} + 3^{21} + 1] - 3^7(3^{77} - 1)$$

$(3^{21} - 1) : (3^{14} - 1) = 3^7$

$3^{21} - 3^7$

$3^7 - 1$

$(3^{14} - 1) : (3^7 - 1) = 3^7 + 1$

$3^{14} - 3^7$ zb.

$3^7 - 1$

Příklad 2

$[17]^{-1}_{78}$

$78 : 17 = 4$ zb $10 \Rightarrow 10 = 78 - 4 \cdot 17$

$17 : 10 = 1$ zb $7 \Rightarrow 7 = 17 - 1 \cdot 10$

$10 : 7 = 1$ zb $3 \quad 3 = 10 - 1 \cdot 7$

$7 : 3 = 2$ zb $1 \quad 1 = 7 - 2 \cdot 3$

$1 = 7 - 2 \cdot (10 - 1 \cdot 7) = 3 \cdot 7 - 2 \cdot 10 = 3(17 - 1 \cdot 10) - 2 \cdot 10 = 3 \cdot 17 - 5 \cdot 10$

$= 3 \cdot 17 - 5 \cdot (78 - 4 \cdot 17) = 23 \cdot 17 - 5 \cdot 78$

$[17]^{-1}_{78} = [23]_{78}$

Příklad 3

$(2^{2k}+1)(2^k+1) = 2^k - 1$

$-(2^{2k}+2^k)$

$-2^k + 1$

$-(-2^k - 1)$

2

$(2^k+1) : 2 = 2^{k-1}$

-2^k

1

$1 = (2^k+1) - 2^{k-1} \cdot 2$

$= (2^k+1) - 2^{k-1} \cdot [(2^{2k}+1) - (2^k-1)(2^k+1)]$

$= (2^k+1) \cdot [1 - 2^{k-1}(-(2^k-1))] + \ldots$

$= (2^k+1) \cdot [1 + 2^{2k-1} - 2^{k-1}] + \ldots$

$[2^k+1]^{-1}_{2^{2k}+1} = [1 + 2^{2k-1} - 2^{k-1}]_{2^{2k}+1}$

Příklad 4.

$3x \equiv 5 \quad (17)$

! $\cdot 3^{15}$

$15x \equiv 25 \ (17)$

$-2x \equiv 8 \ (17)$!

$x \equiv -4 \ (17)$

$x \equiv 13 \ (17)$

Příklad 5

$37x \equiv 82 \ (105)$

$37x \equiv 82 \ (3)$

$x \equiv 1 \ (3)$

$6 + 35s \equiv 1 \ (3)$

$2s \equiv 1 \ (3)$

$s \equiv 2 \ (3)$

$s = 2 + 3k$

$37x \equiv 82 \ (5)$

$37 \cdot (6 + 7t) \equiv 82 \ (5)$

$2(6 + 7t) \equiv 2 \ (5)$

$6 + 7t \equiv 1 \ (5)$

$1 + 2t \equiv 1 \ (5)$

$2t \equiv 0 \ (5)$

$t \equiv 0 \ (5)$

$t = 5s$

$37x \equiv 82 \ (7)$

$2x \equiv 5 \ (7)$

$6x \equiv 15$

$x \equiv 6 \ (7)$

$x = 6 + 7t$

$x = 6 + 35s$

$x = 6 + 35 \cdot (2 + 3k)$

$x = 76 + 105k$

Příklad 6

$$x \equiv 10\ (13) \Rightarrow x = 10 + 13k$$
$$x \equiv 3\ (12) \Rightarrow 10 + 13k \equiv 3\ (12)$$
$$x \equiv 0\ (11)$$
$$k \equiv 5\ (12)$$
$$k = 5 + 12s$$
$$x = 10 + 13(5 + 12s) = 75 + 156s$$
$$75 + 156s \equiv 0\ (11)$$
$$= 75 + 156(1 + 11t)$$
$$2s \equiv 2\ (11)$$
$$= \underline{231} + 1716t$$
$$s \equiv 1\ (11)$$
$$s = 1 + 11t$$

Příklad 4

$$\varphi(735)$$
$$735 = 3 \cdot 5 \cdot 7^2$$
$$\varphi(735) = 2 \cdot 4 \cdot 6 \cdot 7 = 336$$

Příklad 8

$$13^{11^{9^7}} \equiv x\ (10)$$
$$3^{11^{9^7}} \equiv x\ (10)$$

$$3^1 = 3$$
$$3^2 = 9$$
$$3^3 \equiv 7\ (10)$$
$$3^4 \equiv 1\ (10)$$
$$\vdots$$

$$11^{9^7} \equiv y\ (4)$$
$$(-1)^{9^7} \equiv y\ (4)$$
$$y \equiv 3\ (4)$$
$$\Rightarrow 3^3 \equiv x\ (10)$$
$$\underline{x \equiv 7\ (10)}$$

Příklad 9

$2^{180} \equiv 1 \ (37)$ - MFV

$3^{180} \equiv 1 \ (37)$ - MFV

$5^{180} \equiv 1 \ (37)$ - MFV

$2^{181} + 3^{181} + 5^{181} \equiv 2+3+5 \equiv \underline{10 \ (37)}$

Příklad 10

$945 = 3^3 \cdot 5 \cdot 7$

$p^{18} \equiv 1 \ (27)$ E.V.

$p^{36} \equiv 1 \ (27)$

$p^4 \equiv 1 \ (5)$ E.V.

$p^{36} \equiv 1 \ (5)$

$p^6 \equiv 1 \ (7)$ E.V.

$p^{36} \equiv 1 \ (7)$

$\Rightarrow p^{36} \equiv 1 \ (945)$

Příklad 11

$\varphi(n) = \frac{n}{4}$

viz cvičení: $\varphi(n) = \frac{n}{2} \Leftrightarrow n = 2^\alpha$

$n = 2^k \cdot m, \quad (2, m) = 1$

$\varphi(2^k \cdot m) = \frac{2^k \cdot m}{4}$

$2^{k-1} \cdot \varphi(m) = \frac{2^k \cdot m}{4}$

$\varphi(m) = \frac{m}{2} \Rightarrow m = 2^\alpha$ ↯

$(m, 2) = 1$!

Příklad 12

$\varphi(n) = 6$

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$\varphi(n) = (p_1 - 1) \cdot p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1) p_k^{\alpha_k - 1}$

$6 = 1 \cdot 6$

$(p_1 - 1) = 6 \Rightarrow p_1 = 7 \Rightarrow n = 7$

$p_1^{\alpha_1 - 1} = 1 \quad \alpha_1 = 1$

větší prvočíslo v rozkladu být menší

$6 = 2 \cdot 3$

$p_1 - 1 = 2 \Rightarrow n = 9$

$p_1 = 3$

$6 = 1 \cdot 1 \cdot 6$

$\Rightarrow p_1 - 1 = 1$

$p_1 = 2$

$p_2 - 1 = 6 \Rightarrow p_2 = 7$

$\Rightarrow n = 14$

$6 = 1 \cdot 2 \cdot 3$

$p_1 - 1 = 1$

$p_1 = 2 \Rightarrow n = 18$

$p_2 - 1 = 2$

$p_2 = 3$

$p_1 - 1 = 3$ ↯

Příklad 13

$$2^x = 11 + 7y$$

$$2^x \equiv 11 + 7y \ (7)$$

$$2^x \equiv 4 \ (7)$$

$2^1 \equiv 2$
$2^2 \equiv 4$
$2^3 \equiv 1$
$2^4 \equiv 2$
$\vdots$

$\Rightarrow x = 2 + 3t$

$$2^{2+3t} = 11 + 7y$$

$$y = \frac{2^{2+3t} + 11}{7}$$

$$\Rightarrow \left(2+3t, \frac{2^{2+3t}+11}{7}\right), \ t \in \mathbb{Z}$$