16
40

$9 | 8$

$4 \quad -8$

$8 = 40 - 2 \cdot 16$

$2 \equiv 6 \ (4)$

$\cancel{1 \equiv 3 \ (4)}$

$1 \equiv 3 \ (2)$

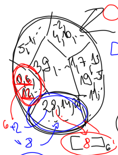
$3x \equiv 6 \ (5)$

$x \equiv \cancel{3}\,2 \ (5)$

$x^n + y^n = z^n$

$x^2 + y^2 = z^2$

$n \geq 3 \quad x^n + y^n = z^n$



$\mathbb{Z} \quad \bigcirc + \bigcirc = \bigcirc$

$m = 6$

$[0]_6 + [2]_6 = [2]_6$

$\mathbb{Z}_6$

$\mathbb{Z}_m$

$6 + 2 = 8$

$[8]_6$

-5

$-5 = k \cdot 6 + b$

$(-1) + 1 \quad 0 \leq |b| < 5$

2 22-15:47

$[a]_m \cdot [b]_m = [a \cdot b]_m$

$[2]_5 \cdot [3]_5 = [6]_5 = [1]_5$

$[a]_m \cdot [b]_m = [1]_m$

$[3]_5$ je m. b $[2]_5$ ✓ inverzní $[a]_m$

$\varphi(5) = 4 \qquad \varphi(6) = 2$

1, 2, 3, 4 $\quad$ 5 $\qquad$ 1, $\cancel{2}$, $\cancel{3}$, $\cancel{4}$, 5, $\cancel{6}$

$\varphi(40) = \varphi(2^3 \cdot 5) = 1 \cdot 2^2 \cdot 4 = 16$

2 22-16:28

$(113, 50)$

$113 : 50 = 2$ zb. $13 \ldots \quad 113 = 2 \cdot 50 + 13$

$50 : 13 = 3$ zb. $11 \qquad 50 = 3 \cdot 13 + 11$

$13 : 11 = 1$ zb. $2 \qquad 13 = 1 \cdot 11 + 2$

$11 : 2 = 5$ zb. $1 \qquad 11 = 5 \cdot 2 + 1$

$2 : 1 = 2$ zb. 0

$1 = 11 - 5 \cdot 2 = 11 - 5(13 - 1 \cdot 11)$

$= 6 \cdot 11 - 5 \cdot 13 = 6(50 - 3 \cdot 13) - 5 \cdot 13 =$

$= 6 \cdot 50 - 23 \cdot 13 = 6 \cdot 50 - 23(113 - 2 \cdot 50)$

$= 52 \cdot 50 - 23 \cdot 113$

2 22-16:35

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

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

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

$3^{56} - 1$

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

$3^{35} - 1$

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

zb. $3^{14} - 1$

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

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

$-(3^{21} - 3^7)$

$3^7 - 1$

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

$-(3^{14} - 3^7)$

$3^7 - 1$

0

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

$= (3^{21} - 1) - 3^7 \cdot \big((3^{77} - 1) - (3^{56} + 3^{35} + 3^{14})(3^{21} - 1)\big)$

$= (3^{21} - 1)\big(1 + 3^7(3^{56} + 3^{35} + 3^{14})\big) - 3^7(3^{77} - 1)$

2 22-16:41

$3x \equiv 5 \ (17)$

$3x \equiv 12 \ (17)$

$x \equiv -4 \ (17)$

$x = -4 + 17t \qquad t \in \mathbb{Z}$

2 22-16:52

$13^{24} + 12^{11} + 11^{10} \equiv \qquad (\text{mod } 9)$

$4^{12} + 3^{11} + 2^{10} \equiv 2^{24} + 3^{11} + 2^{10}$

$2^3 = 8 \qquad \equiv (2^3)^8 + (3^2)^5 \cdot 3 + (2^3)^3 \cdot 2$

$2^3 \equiv -1 \ (9) \qquad \equiv (-1)^8 + 0 - 2$

$3^2 = 9 \qquad \equiv 1 - 2 \equiv -1 \ (9)$

$3^2 \equiv 0 \ (9)$

zbytek je 8

2 22-16:54

$$*\ 2^{15}+3^{14}+5^{13}+2^{12}$$

$$2^{15}+3^{14}+5^{13}+2^{12} \equiv 0+1+1+0$$
$$\equiv 2 \equiv 0\ (2)$$

$$2^{15}+3^{14}+5^{13}+2^{12} \overset{?}{\equiv} 0\ (11)$$

$$2^{10} \equiv 1\ (11) \qquad 5^{10} \equiv 1\ (11)$$
$$3^{10} \equiv 1\ (11)$$

$$2^{10}\cdot 2^5 + 3^{10}\cdot 3^4 + 5^{10}\cdot 5^3 + 2^{10}\cdot 4 \equiv$$
$$\equiv 2^5+3^4+5^3+4 \qquad a^{p-1}\equiv 1\ (p)$$
$$(a,p)=1$$
$$\equiv -1+4+5\cdot 3+4$$
$$\equiv 22 \equiv 0\ (11)$$

2 22-17:02

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

$$[17]_{78}\cdot[a]_{78} = [1]_{78}$$
$$17a \equiv 1 \pmod{78}$$
$$1 = 17a + 78k$$

$78:17 = 4$ zb 10 $\qquad 78 = 4\cdot 17 + 10$
$17:10 = 1$ zb 7 $\qquad 17 = 1\cdot 10 + 7$
$10:7 = 1$ zb 3 $\qquad 10 = 1\cdot 7 + 3$
$7:3 = 2$ zb 1 $\qquad 7 = 2\cdot 3 + 1$

$$1 = 7-2\cdot 3 = 7-2(10-1\cdot 7) =$$
$$= 3\cdot 7 - 2\cdot 10 = 3\cdot(17-1\cdot 10) - 2\cdot 10$$
$$= 3\cdot 17 - 5\cdot 10 = 3\cdot 17 - 5(78-4\cdot 17)$$
$$= 23\cdot 17 - 5\cdot 78$$
$$a = 23$$
$$[17]^{-1}_{78} = [23]_{78}$$

2 22-17:10

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

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

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

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

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

2 22-17:19

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

$$735 = 5\cdot 147 = 35\cdot 21$$
$$= 3\cdot 5\cdot 7\cdot 7$$

2 22-17:25

$$4x \equiv 3\ (7)$$
$$4x \equiv -4\ (7)$$
$$x \equiv -1$$
$$\boxed{x = -1+7t}$$

2 22-17:29

2 22-17:30

1) $x \equiv 8 \ (11)$

$x \equiv 5 \ (8)$

$x \equiv 1 \ (3)$

$x = 8 + 11t$

2) $8 + 11t \equiv 5 \ (8)$

$3t \equiv 5 \ (8)$

$3t \equiv -3 \ (8)$

$t \equiv -1 \ (8)$

$t = -1 + 8s$

$x = 8 + 11(-1 + 8s) =$

$= -3 + 88s$

$-3 + 88s \equiv 1 \ (3)$

$s \equiv 1 \ (3)$

$s = 1 + 3k$

$x = -3 + 88(1 + 3k)$

$\boxed{x = 85 + 264k}$

2 22-17:30

$13^{11^{97}} \equiv \quad (10)$

$\equiv 3^{11^{97}} \quad (10)$

$3^4 \equiv 1 \ (10)$

$\underbrace{\overbrace{3\cdot3\cdot3\cdot3}^{1}\overbrace{3\cdot3\cdot3\cdot3}^{1}3\cdot\ \ldots\ \cdot3\overbrace{3\cdot3\cdot3}^{3^?}}_{11^{97}}$

$11^{97} \equiv ? \quad (4)$

$(-1)^{97} \equiv -1 \equiv 3 \ (4)$

$3\cdot3\cdot3 = 2\underline{\underline{7}}$

2 22-17:35