$$x \equiv 43 \bmod 100 = 10^2 \qquad (43 = 4 \cdot 10^1 + 3 \cdot 10^0)$$

a:

$$13n \equiv 4 \cdot 7^1 + 3 \cdot 7^2 \bmod 7^2 = 49$$
$$13n \equiv 31 \bmod 49$$

49	x	1	0
13	x	0	1
10	3		-3
3	1		4
1 $\Longrightarrow$ 1 db inkongurens megoldas van	3		(-15)
0	3		49

$$x_1 = \frac{31}{1} \cdot (-15) + \underbrace{k \cdot \frac{49}{1}}_{0} = 31 \cdot (-15) = (-465) \Longrightarrow n \equiv (-465) \bmod 49$$

$$n \equiv 25 \bmod 49$$
$$n \equiv 74 \bmod 49$$

b:

$$12n \equiv 2 \cdot 8 + 1 \bmod 8^2$$
$$12n \equiv 17 \bmod 64$$

64	x	1	0
13	x	0	1
(4)	5		-3
0	3		4

$$4 \nmid 17 \Longrightarrow \text{nincs megoldas}$$

8

$$x \equiv 7^{3^{47}} \bmod 100$$

harom tetel all rendelkezesunkre

1. $a, n \in \mathbb{Z}, (a, n) = 1 : a^{\varphi} \equiv 1 \bmod n$
2. p prim, $a \in \mathbb{Z} : a^p \equiv a \bmod p$
3.

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$
$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5$$

$$\varphi(100) = 100 \prod_{i=1}^{2} \left(1 - \frac{1}{p_i}\right) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10(2-1)(5-1) = 10 \cdot 1 \cdot 4 = 40 \Longrightarrow 7^{40} \equiv 1 \bmod 100 \Longrightarrow$$

$$\Longrightarrow 7^{40n+k} \equiv 7^k \bmod 100 \Longrightarrow 7^n \equiv 7^{n \bmod 40} \Longrightarrow 7^{3^{47}} \equiv 7^{3^{47} \bmod 40} \bmod 100$$
$$3^{47} \bmod 40 = 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^2 \cdot 3^1 \bmod 40 = 1 \cdot 1 \cdot 1 \cdot 9 \cdot 3 \bmod 40 = 27$$

mert
$3^1 \bmod 40 = 3$
$3^2 \bmod 40 = 9$
$3^4 \bmod 40 = 81 \bmod 40 = 1$
$3^8 \bmod 40 = 3^4 \cdot 3^4 \bmod 40 = 1 \cdot 1 \bmod 40$
$3^{16} \bmod 40 = 1$
$3^{32} \bmod 40 = 1$
$7^{3^{47}} \bmod 100 = 7^{3^{47} \bmod 40} \bmod 100 = 7^{27} \bmod 100 = 1 \cdot 1 \cdot 49 \cdot 7 \bmod 100 = 343 \bmod 100 =$
$43 \bmod 100$

mert

$7^{27} \bmod 100 = 7^{16} \cdot 7^8 \cdot 7^2 \cdot 7 \bmod 100$
$7^1 \bmod 100 = 7$
$7^2 \bmod 100 = 49$
$7^4 \bmod 100 = 2401 \bmod 100 = 1$
$7^8 \bmod 100 = 1^2 \bmod 100 = 1$
$7^{16} \bmod 100 = ... = 1$

2/a

$$27x + 35y = 3$$
$$ax \equiv b \bmod n \iff ax + ny = b$$
$$27x \equiv 3 \bmod 35 \iff 35y \equiv 3 \bmod 27$$

35	x	1	0
27	x	0	1
8	1	1	−1
3	3	−3	4
2	2	7	−9
1	1	−10	13
0	2	27	−35

$$\left.\begin{array}{ll} \text{negyedik sorbol latszodik hogy} & 3 - (-3) \cdot 35 + 4 \cdot 27 \\ \text{utolso sorbol} & 0 = 27 \cdot 35 + (-35) \cdot 27 \end{array}\right\} \Longrightarrow 3 = (-3 + 27k) \cdot 35 + (4 - 35k) \cdot 27$$

2/d

$$18x + 14y = 16$$

18	x	1	0
14	x	0	1
4	1	1	−1
2	3	−3	4
0	2	7	−9

$$\left.\begin{array}{ll} \text{harmadik sorbol} & 1 \cdot 18 + (-1) \cdot 14 = 4 \iff 4 \cdot 18 + (-4) \cdot 14 = 16 \\ \text{utolso sorbol} & 0 = 7 \cdot 18 - 9 \cdot 14 \end{array}\right\} \Longrightarrow (4 + 7k) \cdot 18 + (-4 - 9k) \cdot 14 = 16$$

3

$$4 \text{ ill. } 5 \text{ hatvanyai } \bmod 7$$

$$\begin{aligned}
4^0 \bmod 7 &= 1 \\
4^1 \bmod 7 &= 4 \\
4^2 \bmod 7 &= 2 \\
4^3 \bmod 7 &= 1 \\
4^4 \bmod 7 &= 4 \\
4^5 \bmod 7 &= 2 \\
4^6 \bmod 7 &= 1
\end{aligned}$$

a maradek “korbeer” es ismetlodik