a)

$3x \equiv 1 \bmod 7$

7	x	1	0
3	x	0	1
1	2	1	-2
0	3	-3	7

elso sor: $7 = 1 \cdot 7 + 0 \cdot 3$
masodik sor: $3 = 0 \cdot 7 + 1 \cdot 3$
harmadik sor: $1 = 1 \cdot 7 + (-2) \cdot 3$

$$1 = (1 - 3k) \cdot 7 + (-2 + 7k)3$$

$$3x \equiv \underbrace{(1 - 3k)7}_{0} + (-2 + 7k)3 \quad \bmod 7$$

$$3x \equiv (-2 + 7k)3 \quad \bmod 7$$

$$x \equiv -2 + 7k \quad \bmod \frac{7}{(7,3) = 1} = 7$$

$$x \equiv -2 \quad \bmod 7$$

$$x \equiv 5 + 7k \quad (k \in \mathbb{Z})$$

van ehelyett egy algoritmus:

$$3x \equiv 1 \quad \bmod 7$$

ez illeszkedik erre

$$ax \equiv b \quad \bmod n$$

es igaz hogy

1.

$$ax \equiv b \quad \bmod n \Longleftrightarrow ax + ny = b$$

2.

$$ax + ny = (a, n)$$

3.

$$\text{ha} \;\; (a, n) \mid b \quad (a, n) \text{ megoldas van}$$

4.

$$x_i = \frac{b}{(a, n)} x + k \frac{n}{(a, n)} \quad (k = 0, ..., (a, n) - 1)$$

ezt ugy kell alkalmazni hogy

7	x	0
3	x	1
1	2	-2 = x
0	3	

$$x_i = \frac{1}{1} \cdot (-2) + 0 \cdot ... = -2$$

b

$$3x \equiv 1 \mod 8$$

8	x	1	0
3	x	0	1
2	2	1	-2
1	1	-1	3 (ez)
0	2	-3	-8

$$1 = (-1 + 3k)8 + (3 - 8k)3$$

$$3x \equiv \underbrace{(-1 + 3k)8}_{0} + \underbrace{(3 - 8k)3}_{0} \mod 8$$

$$3x \equiv 3 \cdot 3 \mod 8$$

$$x \equiv 3 \mod 8$$

az algoritmussal:

$$x_i = \frac{1}{1} \cdot 3 + \underbrace{k}_{0} \cdot \frac{8}{1}$$

$$x_1 = 3$$

c

$$2x \equiv 1 \mod 8$$

8	x	1	0
2	x	0	1
0	4	1	-4

szabaly szerint: $(a, n) \mid b$ es 2!| 1 tehat nincs megoldas

e

$$31x \equiv 4 \mod 17$$

31	x	1	0
17	x	0	1
14	1	1	-1
3	1	-1	2
2	4	5	-9
1	1	-6 (ez kell)	11
0	2	17	-31

$$x_i = \frac{4}{1} \cdot (-6) + k \cdot \frac{17}{1}$$
$$x_i = -24 + 17k$$
$$x_1 = -24 \equiv ...$$

2/a

$$a = 2, n = 4$$
$$a^0 = 2^0 = 1 = 1 \mod 4$$
$$a^1 = 2^1 = 2 \mod 4$$
$$2^2 = 4 \equiv 0 \mod 4$$
$$2^3 = 8 \equiv 0 \mod 4$$

2/b

$$a = 3, n = 5$$

$$3^0 = 1 \equiv 1 \mod 5 3^1 = 3 \equiv 3 \mod 5 3^2 = 9 \equiv 4 \mod 5 3^3 \equiv 12 \equiv 2 \mod 5 3^4 \equiv 6 \equiv 1 \mod 5$$

megoldasok: 1, 3, 4, 2

3

euler fele freaky fuggveny

$$\varphi(n) = \#\{1 \leq a \leq n : (a, b) = 1\} = |\{1 \leq a \leq n : (a, b) = 1\}| \quad (n \in \mathbb{N})$$

irjuk fel a $\varphi(n) 1 \leq n \leq 16$

$$\varphi(1) = 1$$
$$\varphi(2) = 2$$
$$\varphi(3) = 2$$
$$\varphi(4) = 2$$
$$\varphi(5) = 4$$
$$\varphi(6) = 2$$
$$\varphi(7) = 6$$
$$\varphi(8) = 4$$
$$\varphi(9) = 6$$
$$\varphi(10) = 4$$
$$\varphi(11) = 10$$
$$\varphi(12) = 4$$
$$\varphi(13) = 12$$
$$\varphi(14) = 6$$
$$\varphi(15) = 8$$
$$\varphi(16) = 8$$

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \Longrightarrow \varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \quad \text{(p az prim) es} \quad \varphi(p) = p = 1$$

Euler-Fernat

$$a, n \in \mathbb{Z}, (a, n) = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 \mod n$$

Fernat tetel

$$\text{p prim}, \;\; a \in \mathbb{Z} \Longrightarrow a^p \equiv a \mod p$$

4/a

$$2^6 \bmod 7$$
$$2^6 \bmod 7 = 2^{\varphi(7)} \bmod 7 = 1$$

4/b

$$2^7 \bmod 7 = 2$$

4/c

$$2^8 \bmod 7 = 2^6 \cdot 2^2 \bmod 7 = 1 \cdot 2^2 \bmod 7 = 4$$

4/f

$$2^{13} \bmod 13 = 2^p \bmod p = 2$$

5

$$n =?, \;\; a = 13n$$
$$13n = a \equiv 4 \cdot 7^1 + 3 \cdot 7^0 \mod 7^2 = 49$$
$$13n \equiv 31 \mod 49$$