2025 DiMat II. Minta ZH 1.

1 $(ca, cb) = c(a, b)$, $a > b \Rightarrow (a, b) = (a - b, b) \Rightarrow (a, b) = (a - qb, b)$

a: $\text{lnko}(11^4 - 1, 11^6 - 1)$

$$\begin{aligned}
\text{lnko}(11^4 - 1, 11^6 - 1) &= \text{lnko}(11^4 - 1, (11^6 - 1) - 11^2(11^4 - 1)) \\
&= \text{lnko}(11^4 - 1, 11^2 - 1) \\
&= \text{lnko}((11^4 - 1) - 11^2(11^2 - 1), 11^2 - 1) \\
&= \text{lnko}(11^2 - 1, 11^2 - 1) \\
&= 11^2 - 1 \\
&= 120 \quad \checkmark \text{ 5 pont}
\end{aligned}$$

b: $\text{lnko}(11^4 + 1, 11^6 + 1)$

$$\begin{aligned}
\text{lnko}(11^4 + 1, 11^6 + 1) &= \text{lnko}(11^4 + 1, (11^6 + 1) - (11^4 + 1)) \\
&= \text{lnko}(11^4 + 1, 11^4(11^2 - 1)) \\
&= \text{lnko}(11^4 + 1, 11^2 - 1) \\
&= \text{lnko}(11^4 + 11^2, 11^2 - 1) \\
&= \text{lnko}(11^2 + 1, 11^2 - 1) \\
&= \text{lnko}(122, 120) \\
&= 2 \quad \checkmark \text{ 5 pont}
\end{aligned}$$

2

a: $11x \equiv 360 \pmod{13} \iff \overset{a}{11}x \equiv \overset{b}{9} \pmod{\overset{n}{13}}$

	$n=$ 13	X	1	0
	$a=$ 11	X	0	1
	2	1	1	-1
$(a,n)=$	1	5	-5	$\boxed{6}=x$
	0	2	11	-13

$(a,n) = 1 \mid 9 = b$

$\Rightarrow$ 1 m.o.

$$x_i = \frac{b}{(a,n)} \cdot x + k \cdot \frac{n}{(a,n)}$$

$$= \frac{9}{1} \cdot x + k \cdot \frac{13}{1}$$

$= 9x$ (k nincs, mert 1 m.o. van)

$= 54$

Szebb megoldás: $54 \bmod 13 = \underline{\underline{2}}$

Ell.:

$11 \cdot 2 \bmod 13 = 22 \bmod 13$

$= 9$ ✓

3] $360 = 11x + 13y$

Bővített euklideszi algoritmus előző oldalon

$1 = (-5) \cdot 13 + 6 \cdot 11 \quad / \cdot 360$

$360 = (-1800) \cdot 13 + 2160 \cdot 11$

$0 = 11 \cdot 13 + (-13) \cdot 11$

$\Rightarrow 360 = (-1800 + 11k) \cdot 13 + (2160 - 13k) \cdot 11$

$\Downarrow \qquad \Downarrow$

$k \geq 164 \qquad k \leq 166$

x: alaszkai malamut

y: szibériai husky

$k = 166$: $x = 4$, $y = 28$

$k = 165$: $x = 15$, $y = 15$

$k = 166$: $x = 26$, $y = 2$

b: $13x \equiv 360 \pmod{11} \iff 13 \equiv 8 \pmod{11}$

a = 13	X	1	0
m = 11	X	0	1
2	1	1	-1
1	5	-5 ← x	6
0	2	11	-13

$(a,m) = 1 \mid 8 = b$

$\Rightarrow$ 1 m.o.

$$x_i = \frac{b}{(a,m)} \cdot x + k \cdot \frac{m}{(a,m)}$$

$$= \frac{8}{1} \cdot (-5) + k \cdot \frac{11}{1}$$

$= 8 \cdot (-5)$ (minus k, -ot 1 m.o.)

$= (-40)$

$(-40) \bmod 11 = \underline{\underline{4}}$

EU.:

$13 \cdot 4 \bmod 11 = 52 \bmod 11$

$= 8$ ✓

4

a: $12^{(11^{10})} \bmod 13$

$\varphi(13) = 12 \Rightarrow 12^{12} \bmod 13 = 1$

$\Rightarrow 12^{(11^{10})} \bmod 13 = 12^{(11^{10} \bmod 12)} \bmod 13$

$11^1 \bmod 12 = 11$
$11^2 \bmod 12 = 1$
$11^4 \bmod 12 = 1$
...

$11^{10} \bmod 12 = 11^8 \cdot 11^2 \bmod 12 =$
$= 1 \cdot 1 \bmod 12$
$= 1$

$\Rightarrow 12^{(11^{10})} \bmod 13 = 12^1 \bmod 13$

$= 12$

b: $11^{45} \bmod 23$

$\varphi(23) = 22 \Rightarrow 11^{22} \bmod 23 = 1 \Rightarrow 11^{45} \bmod 23 = 11^{45 \bmod 22} \bmod 23$

$11^{45 \bmod 22} \bmod 23 = 11^1 \bmod 23 =$

$= 11$

5] RSA, $p=7$, $q=13$, $e=5$, $c=2$, $m=?$

$n = p \cdot q = 7 \cdot 13 = 91$

$\varphi(n) = (7-1)\cdot(13-1) = 6 \cdot 12 = 72$

$\text{ggT}(e, \varphi(n)) = \text{ggT}(5, 72) = 1$ ✓

$d: e \cdot d \equiv 1 \mod \varphi(n)$

$5d \equiv 1 \mod 72$

72	X	1	0
5	X	0	1
2	14	1	-14
1	2	-2	29
0	2	5	-72

$x_i := \frac{b}{(a,n)} \cdot x + b \cdot \frac{n}{(a,n)}$

$= \frac{1}{1} \cdot 29$

$= 29 \Rightarrow d = 29$

$5 \cdot 29 \mod 72 = 145 \mod 72$

$= 1$ ✓

$m = c^d \mod n$

$= 2^{29} \mod 72$

$2^{29} = 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2^1$

$2^1 \mod 72 = 2$

$2^2 \mod 72 = 4$

$2^4 \mod 72 = 16$

$2^8 \mod 72 = 256 \mod 72 = 40$

$2^{16} \mod 72 = 40^2 \mod 72 = 1600 \mod 72 = 16$

$2^{29} \mod 72 = 2^1 \cdot 2^4 \cdot 2^8 \cdot 2^{16} \mod 72$

$= 2 \cdot 16 \cdot 40 \cdot 16 \mod 72$

$= 20480 \mod 72$

$= 32$

$\Rightarrow m = 32$