

GYA KORLAT

→ leírni lehet ezt

1.) a) $6x + 5 = 6$ $\div 3 \rightarrow + (3^{-1}) = +4$

$6x = 10 = 3$

$6x = 3 \quad | \cdot (6^{-1})$

$x = 4$

=

$6 \cdot 4 = 24$ 7-tel osztva maradék

$\hookrightarrow 6 \cdot 4 = 3$

$3 + 3 = 6$

$6 \cdot N / 7$

N						
1	2	3	4	5	6	7
6	5	4	3	2	1	

maradék

b) $7x + 4 = 2$

$7x + 7 = 2 \quad | + (7^{-1}) = +4$

$7 \cdot N$ mod 11

$7x = 6 \quad | \cdot 7^{-1}$

1	2	3	4	5	6	7	8	9	10
7	3	10	6	2	9	5	1	8	4

$x = 6 \cdot 8 = 48$
 $(\text{mod } 11) = 4$

↑

Até levetve, ahol
 ahol 1 van

$7 \cdot 4 = 6$

$6 - 4 = 6 + 7 = 13 = 2$

2. $t = 2 \quad q = 7 \Rightarrow (n = q - 1) \Rightarrow n = 6$

a)

$G_{k \times n}$

$H_{(n-t) \times n}$

$t = 2 = \left\lfloor \frac{\text{dim} - 1}{2} \right\rfloor \Rightarrow \text{dim} = 5$

$MDS \Rightarrow \text{dim} - 1 = n - t \Rightarrow t = 2$

Minimum

$$G_{k \times n} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \dots & \alpha_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \dots & \alpha_{n-1}^{k-1} \end{bmatrix} \text{ u. d. r. r.}$$

$$\begin{matrix} 2 & 3 & 4 & 5 & 6 & \text{mod } 7 \end{matrix}$$

$$\begin{matrix} 2 & 4 & 1 & 2 & 4 & 1 & \times \end{matrix}$$

$$\begin{matrix} 3 & 2 & 6 & 4 & 5 & 1 & \times \end{matrix}$$

$$\begin{matrix} 4 & 2 & 1 & 4 & 2 & 1 & \times \end{matrix}$$

$$\begin{matrix} 5 & 4 & 6 & 2 & 3 & 1 & \leftarrow \end{matrix}$$

$$\begin{matrix} 6 & 1 & 6 & 1 & 6 & 1 & \times \end{matrix}$$

mod 7

störte es also nicht, dass wir alle x nicht

PRIMITIV ELEM

AHOL MINDEN NEM KIZÖN

$$\alpha = 5$$

$$G_{2 \times 6} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix}$$

paritós elemek relatív.

prim. elem (5)

$$H_{(n-k) \times n} = \begin{bmatrix} 1 & \alpha^1 & \dots & \alpha^{(n-1) \cdot 1} \\ 1 & \alpha^2 & \dots & \alpha^{(n-1) \cdot 2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \dots & \alpha^{(n-1) \cdot (n-k)} \end{bmatrix}$$

$$4 \ 4 \times 6 = \begin{bmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{bmatrix}$$