Infocode gyakorlat

10.19.

$2\cdot 7 = \,?$ $GF(8) = GF(2^3)$

polinomok	vektor	szám
0	000	0
1	001	1
y	010	2
$y+1$	011	3
y^2	100	4
y^2+1	101	5
y^2+y	110	6
y^2+y+1	111	7

← ez csak jelölés

$3+3 = y+1 + y+1 = 0$

$2(y+1) = 2y+2$

GF(2) miatt 0

Bitek összeadása ugyanúgy 0

$4-2 = 4+(2^{-1}_{+}) = 4+2 = y^2+y = \underline{\underline{6}}$

$GF(7)$ $4-2=2$ $4+(2^{-1}_{+}) = 4+5 = 9 = 2$ $2\cdot 4 = 8 = 1$

$2\cdot 7 = y(y^2+y+1) = y^3+y^2+y$

ez lesz $\Rightarrow$ $\boxed{\text{IRREDUCIBILIS P.} \quad p(y) = y^3+y+1}$

$$\begin{array}{l} y^3+y^2+y : y^3+y+1 = 1 \\ -\;y^3+y+1 \\ \hline y^2+y \end{array}$$

miért nem $-$???
nem értem

$2\cdot 7 = 5$

hatványtábla

y^0	1
y^1	y
y^2	y^2
y^3	$y+1$
y^4	y^2+y
y^5	y^2+y+1
y^6	y^2+1
y^7	1

$\to y^3+y^2+y = y+1+y^2+y = y^2+1 = \underline{\underline{5}}$

$2\cdot 7 = y(y^2+y+1)$

$7\cdot\alpha = 7(\alpha_2 y^2 + \alpha_1 y + \alpha_0)$

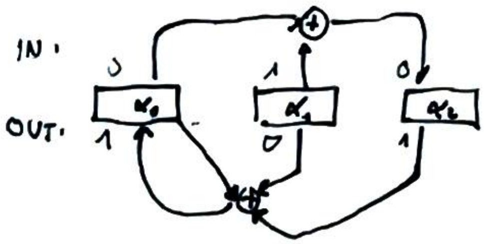
$(y^2+y+1)(\alpha_2 y^2 + \alpha_1 y + \alpha_0) = \ldots = \alpha_2 y^4 + (\alpha_2+\alpha_1) y^3 + (\alpha_2+\alpha_1+\alpha_0) y^2 +$

$+(\alpha_1+\alpha_0) y + \alpha_0 = \alpha_2(y^2+y) + (\alpha_2+\alpha_1)(y+1) + (\alpha_2+\alpha_1+\alpha_0) y^2 + (\alpha_1+\alpha_0) y + \alpha_0 =$

$= (\alpha_1+\alpha_0) y^2 + \alpha_0 y + \alpha_2 + \alpha_1 + \alpha_0$

behelyettesítéssel a hatványtáblából

$$\begin{array}{l|l} \alpha_0 & \alpha_2+\alpha_1+\alpha_0 \\ \alpha_1 \Rightarrow & \alpha_0 \\ \alpha_2 & \alpha_1+\alpha_0 \end{array}$$



$\boxed{2\cdot 7 = y^2+1}$

$g(x) = \prod_{i=0}^{n-k} (x-\alpha^i)$

$h(x) =$