$F_{2^k} = F_2[x] \pmod{P(x)}$ $\quad P(\alpha) = 0$

$\deg(P(x)) = k$

$P(x)$

irreducible & primitive

$F_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$

$\alpha^{q-1} = 1$

$\alpha^q = \alpha$

α = primitive element or root

irreducible but not primitive

$\alpha, \alpha^2, \alpha^3, \ldots, \underline{\underline{\alpha^n = 1}}$

$n < \cancel{k}\, q-1$

$\alpha \neq$ primitive root

$$(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$$

$$*\,(b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0)$$

$$- a_0 b_0 + a_1 b_0 \alpha + a_2 b_0 \alpha^2$$

$$+ a_3 b_0 \alpha^3 + b_1 a_0 \alpha$$

$$+ b_1 a_1 \alpha^2$$

Design of a 2-bit multiplier in $\mathbb{F}_4$

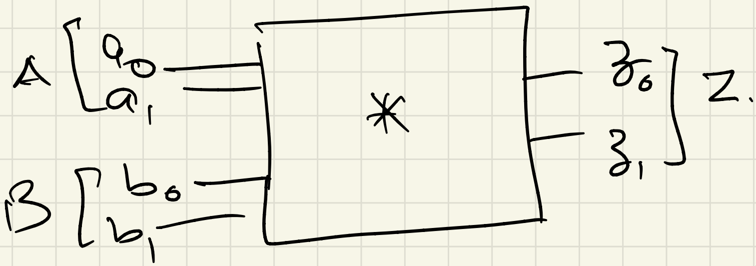
$$\mathbb{F}_4 = \mathbb{F}_2[x] \pmod{x^2+x+1} \rightarrow P(x)$$

$$\alpha^2+\alpha+1=0$$

$$Z = A \cdot B \pmod{P(x)}$$

Spec: $Z - A\cdot B \Rightarrow Z + A\cdot B$.

$A = a_0 + a_1\alpha \qquad B = b_0 + b_1\alpha$



$z_0 + z_1\alpha$

$$A\cdot B = (a_0+a_1\alpha)(b_0+b_1\alpha)$$
$$= a_0b_0 + a_0b_1\alpha + a_1b_0\alpha + \underline{\underline{a_1b_1\alpha^2}}$$

$(\alpha^2 = \alpha+1)$

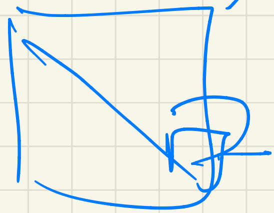
$$A\cdot B = \underline{a_0b_0} + (a_0b_1+a_1b_0)\alpha + a_1b_1(\alpha+1)$$

$$= (a_0b_0+a_1b_1) + (a_0b_1+a_1b_0+a_1b_1)\alpha$$

$$z_0 \quad + \quad z_1\alpha$$

$X = \{A, B, Z, t, q_1, q_2, b, \dots\}$

$$\left.\begin{array}{l} f_1(x) = 0 \\ f_2(x) = 0 \\ \vdots \\ f_{12}(x) = 0 \end{array}\right\} \xrightarrow{\text{gaussian elim.}} \text{G.B.} \left.\begin{array}{l} g_1(x) \\ g_2(x) \\ \vdots \\ g_{12}(x) \end{array}\right\} = 0$$



Common roots?

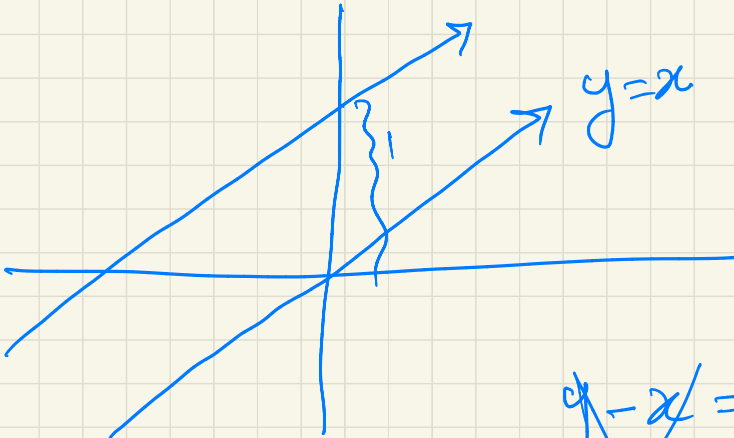
✓ f g

$2(3x + 2y = 5)$ f_1

$3(2x + 3y = 7)$ f_2

$y = \square$ f_3

f_1, f_3



$$y - x = 0$$

$$y - x = 1$$