Galois Fields work sheet.

$$GCD(a,b) = d$$

$$\exists (s,t) \mid d = s \cdot a + t \cdot b.$$

GCD exists:

Let $S = \{ s\,a + t\,b \mid a, b \in \mathbb{D} \}$

Pick $d \in S$, s.t. $f(d)$ is least.

$$d = sa + tb$$

$a \div d$: $\quad a = q \cdot d + r$

$f(r) < f(d)$, but $f(d) =$ least.

$r = 0$. $\quad a = q \cdot d$

$\quad b = q \cdot d.$

d divides both a, b.

let $a = q'e$, $b = q''e$

$e \mid a, b$

$d = s \cdot a + t \cdot b$

$= s \cdot q'e + t \cdot q''e$

$= e(\qquad)$

$d =$ multiple of e.

So $d = \underline{\underline{G}}CD$.

$GCD(s,t) = GCD(s, t-rs)$

$= GCD(s, t-s) = d$

Compute inverses.

$a \in \mathbb{Z}_p$. $\quad a \cdot \underline{\underline{a^{-1}}}_{?} = 1$

$GCD(a, p) = 1$

$s \cdot a + t \cdot p = 1 \pmod{p}$

$\Rightarrow \underline{\underline{s}} \cdot a = 1 \pmod{p}$

$\underline{\underline{F_2[x]}} \pmod{\underline{x^2 + x + 1}}$

$\S$ $\quad ax + b, \quad a, b \in F_2$

a	b
0	0
0	1
1	0
1	1

D = Euclidean Domain

p = prime $\in D$

$D \pmod{p} = \mathbb{F}$ field

$D = \mathbb{R}[x] \quad p = x^2+1$

$\mathbb{R}[x] \pmod{x^2+1} = \mathbb{C}$

= Complex numbers

Note. $\mathbb{R}[x]$ = polynomial ring.

x^2+1 = prime/irreducible poly.

$\mathbb{R}[x] \pmod{x^2+1} = \mathbb{C}$

set of "constants" numbers

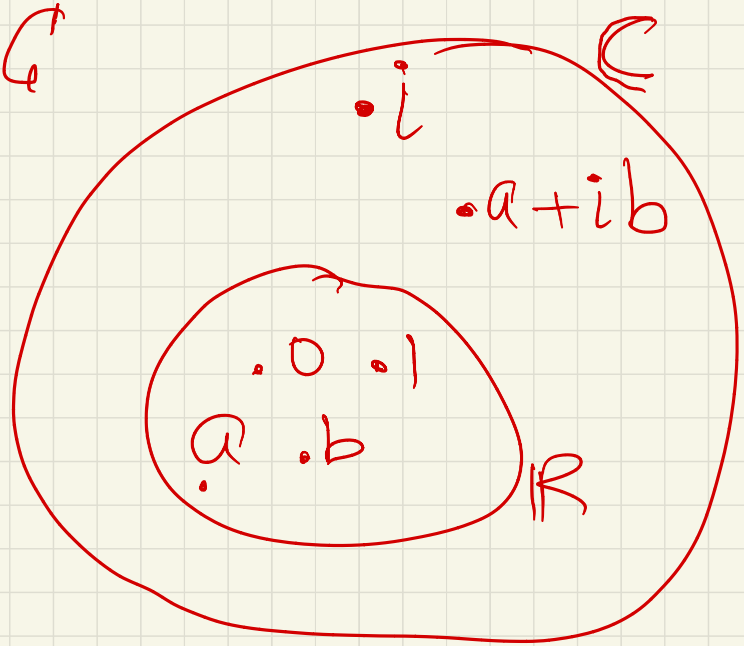
$(x^2+1=0) \Rightarrow x^2=-1$

$x=\sqrt{-1}=i$

$$\left.\begin{array}{l} p(x)=x^2+1 \\ p(i)=i^2+1=0 \end{array}\right\} \begin{array}{l} i = \text{root} \\ \text{of } p(x). \end{array}$$

root $i \notin \mathbb{R}$, root in $\mathbb{C}$

$\mathbb{R} \subset \mathbb{C}$



Construction of finite fields $\mathbb{F}_{2^k}$

$$\mathbb{F}_{2^k} = \mathbb{F}_2[x] \pmod{p(x)}$$

$\mathbb{F}_2 = \{0,1\} = \mathbb{Z}_2 =$ base field

$\mathbb{F}_2[x] =$ Univariate polynomial ring w/ coefficients in $\mathbb{F}_2 = \{0,1\}$

$p(x) =$ irreducible poly

$p(x) \in \mathbb{F}_2[x]$, degree $= k$

$p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$

$p(0) = 1 \neq 0 \pmod 2$

$p(1) = 3 \pmod 2 = 1 \neq 0$

$x^2 + x + 1$ has no roots in $\mathbb{F}_2$

$=$ irreducible in $\mathbb{F}_2$.

$$\frac{\mathbb{F}_2[x] \pmod{x^2+x+1} = \mathbb{F}_{2^2}}{x^2 + x + 1 = 0}$$

$\Rightarrow \quad x^2 = -(x+1)$

$= (x+1)$

$-1 = +1 \pmod 2$

degree of $p(x) = k$

$\mathbb{F}_{2^2} = \mathbb{F}_2[x] \pmod{x^2+x+1}$

$\Rightarrow$ Take <u>any</u> polynomial in $\mathbb{F}_2[x]$, coeff $= 0, 1$, any degree, divide by x^2+x+1, and take the remainder $\underline{r}$

$\underbrace{\deg(r)}_{=1} < \deg(x^2+x+1)$

$ax+b$, $\quad a, b \in \mathbb{F}_2 = \{0, 1\}$.

Let α = root of $p(x) = x^2+x+1$

$p(\alpha) = 0$

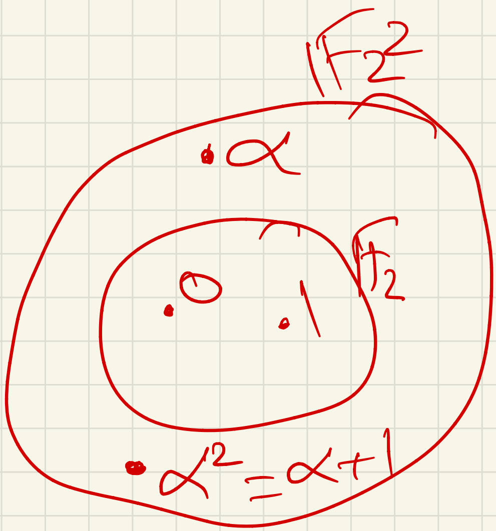
$\alpha^2+\alpha+1 = 0$

$\alpha^2 = \alpha+1$

a	b	
0	0	0
0	1	1
1	0	α
1	1	$\alpha+1 = \alpha^2$

$\mathbb{F}_{2^k} \supset \mathbb{F}_2$

$\alpha \approx i$ in complex numbers.



$p(\alpha) = 0 \Rightarrow \alpha \in \mathbb{F}_{2^2}$

$\alpha \notin \mathbb{F}_2$

$\alpha^2 = \alpha + 1$

$$\begin{aligned}
\alpha^3 &= \underbrace{\alpha^2 + \alpha}_{\text{mod}(\alpha^2+\alpha+1)} = \alpha + 1 + \alpha \\
&= 2\alpha + 1 \\
&= 0 + 1
\end{aligned} \Bigg\} (\text{mod } 2)$$

$= 1$

In $\mathbb{F}_2 K = \mathbb{F}_2[x] \pmod{p(x)}$

Coefficients are reduced (mod 2), because base field $= \mathbb{F}_2$.

AND

All computations reduced $\pmod{p(\alpha)}$

$\alpha^2 + \alpha + 1$

$\alpha^2 \pmod{\alpha^2+\alpha+1} = \alpha + 1$

$\alpha^3 \pmod{\alpha^2+\alpha+1} = \alpha(\alpha+1)$

$\mod \alpha^2+\alpha+1$

$= 1$

$\mathbb{F}_{2^3} = \mathbb{F}_2[x] \pmod{\underbrace{x^3+x+1}_{p(x)}}$

$p(\beta)=0 \quad \beta^3+\beta+1=0$

or $\beta^3 = \beta+1$

$\to ax^2+bx+c, \quad a,b,c \in \mathbb{F}_2$

a	b	c	
0	0	0	0
0	0	1	$1 \to \beta^7$
0	1	0	β
0	1	1	$\beta+1 \to \beta^3$
1	0	0	β^2
1	0	1	$\beta^2+1 = \beta^6$
1	1	0	$\beta^2+\beta = \beta^4$
1	1	1	$\beta^2+\beta+1 = \beta^5$

$$\beta^3 = \beta + 1$$

$$\beta^4 = \beta^2 + \beta$$

$$\beta^5 = \beta^3 + \beta^2 = (\beta+1) + \beta^2$$
$$= \beta^2 + \beta + 1$$

$$\beta^6 = \beta(\beta^2 + \beta + 1)$$
$$= \beta^3 + \beta^2 + \beta$$
$$= (\beta+1) + \beta^2 + \beta$$
$$= \beta^2 + 1$$

$$\beta^7 = \beta(\beta^2 + 1) = \beta^3 + \beta$$
$$= (\cancel{\beta} + 1) + \cancel{\beta}$$
$$= 1.$$

$A = \{a_{k-1}, \ldots, a_1, a_0\}$

k-bit vector.

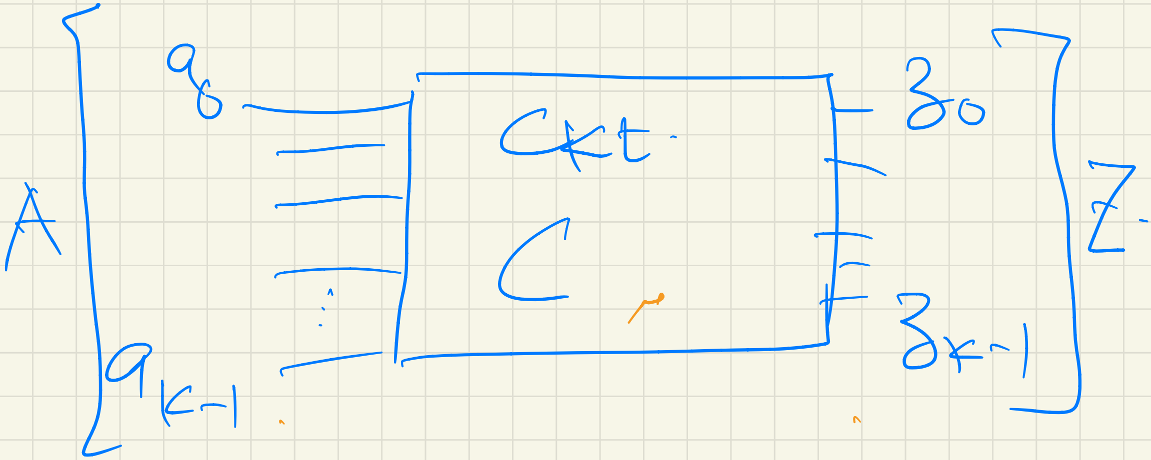
$A \in \mathbb{Z}$ $\quad A = a_0 + 2a_1 + 4a_2 + \cdots + 2^{k-1} a_{k-1}$

$\sum_{i=0}^{k-1} 2^i a_i \Leftarrow$

$A \in \mathbb{F}_{2^k}$ $\quad P(\alpha) = 0$.

$$A = a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + \cdots + a_{k-1} \alpha^{k-1}$$

$$= \sum_{i=0}^{k-1} \alpha^i a_i$$



Model ckt C in $\mathbb{F}_{2^k}$.

$$A = \sum_{i=0}^{k-1} a_i \alpha^i$$

$p(\alpha) = 0$, $\quad p(x) \in \mathbb{F}_2[x]$ irreducible poly.

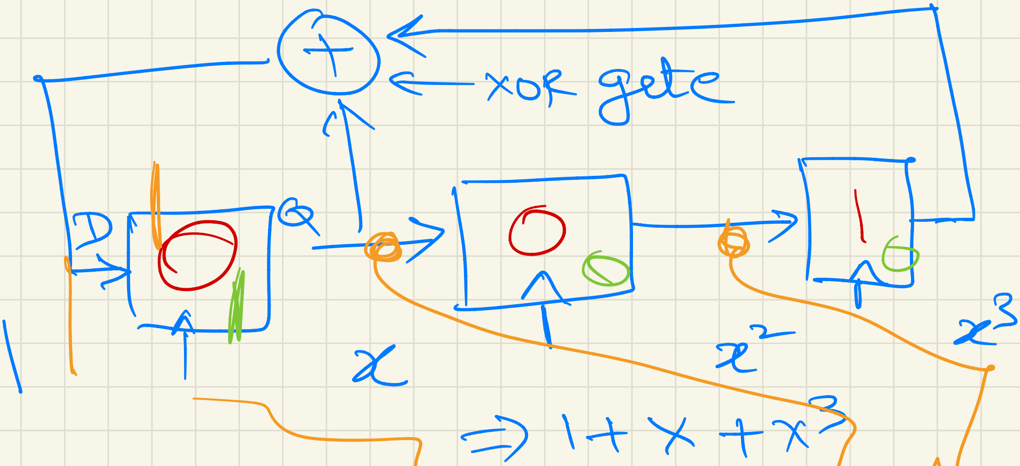
$\Rightarrow$ given

$\mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$

$\mathbb{F}_{2^k} \cong \mathbb{F}_2[x] \pmod{p(x)}$

as a pseudo-random number generator ckt.

Linear Feedback Shift register.
(LFSR).



0 0 1 $= \alpha^2$

1 0 0

1 1 0