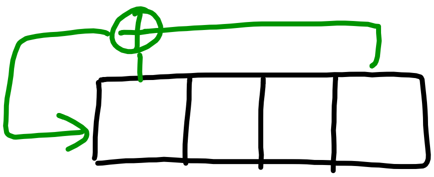
Stromchiffren

↗

LFSR → $P(X)$ Polynome in $\mathbb{F}_2[X]$



→ $\underbrace{X^4+X^3+1}$

Ziel:

irreduzibel → Nullstellen?

primitiv $X^i \bmod P(X)$

Irreduzible Polynome vom Grad 4

$$P(X) = X^4 + p_3 X^3 + p_2 X^2 + p_1 X + \underbrace{p_0}_{=1}$$

$p_0 = 0 \to$ reduzibel

von p_1, p_2, p_3 zwei koeff $= 1$ → reduzibel

z.B. $X^4 + X^3 + X^2 + 1$

$1 + 1 + 1 + 1 = 0 \to (X+1)$ Faktor von P

Insgesamt: ein koeff $= 1$ oder alle drei

⇒ kandidaten

$P(x) = x^4 + x^3 + 1$ ✓

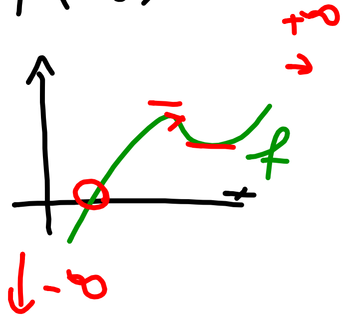
$(x^4 + x^2 + 1)$ s.u.

$x^4 + x + 1$ ✓

$x^4 + x^3 + x^2 + x + 1$ ✓

x_0 ist Nullstelle von $P(x)$

$\Leftrightarrow P(x_0) = 0$



Vorüberlegung :

$$P(x) = \underbrace{\overset{\substack{1\\2}}{g(x)}}_{\text{Grad 1}} \cdot \overset{\substack{3\\2}}{h(x)}$$

✓ Nullstelle

Grad2 Grad 2

welche Grad 2 - Polynome sind irreduzibel

$\boxed{x^2 + x + 1}$ einziges irreduzibles vom Grad 2

$x^2 + 1 = (x+1)^2$

welches Polynom P vom Grad 4 zerfällt

in

$$P(x) = (x^2+x+1)\cdot(x^2+x+1) \quad ?$$

$$(x^2+x+1)\cdot(x^2+x+1) = x^4+x^2+1$$

drei irreduzible Polynome, die auf Primitivität zu prüfen sind

Hierzu:

$$X^{i} \bmod \hat{P}(X) \qquad i = 1, 2, 3, \ldots, 2^{n} - 1$$

ausrechnen.

Wenn erst bei $i = 2^{n} - 1$ das Ergebnis $= 1$ ist dann heißt $P(X)$ primitiv.

Beispiel:

wir testen $P(X) = X^4+X^3+X^2+X+1$

$X^4 = X^3+X^2+X+1$

i	$X^i \bmod P(X)$
1	X
2	X^2
3	X^3
4	$X^4 = X^3+X^2+X+1$
5	$X^4+X^3+X^2+X = X^3+X^2+X+1+X^3+X^2+\cancel{X} = \textcircled{1}$

schon bei $i=5$

$\Rightarrow$ nicht prim.

primitives Polynom:

$P(x) = X^4 + X + 1$ $\rightsquigarrow$ $X^4 = X + 1$

i	X^i
1	x
2	x^2
3	x^3
4	$x^4 = x + 1$
5	$x^2 + x$
$\vdots$	

i	
10	$x^2 + x + 1$
$\vdots$	
14	$x^3 + 1$
15	1

↳ erst bei $i = 15$

$\Rightarrow$ $P(X)$ primitiv

$\Rightarrow$ LFSR mit max. Periode

Fakten zu primitiven Polynomen

- irreduzibel, konstanter Term $\neq 0$
- Anzahl primitiver Polynome vom Grad n

$$\frac{\varphi(2^n-1)}{n}$$

12
15
7
25

Euler'sche φ-Funktion

(engl. totient function)

$$\varphi(n) = \left|\left\{ a \mid ggT(a,n)=1,\ 1 \le a \le n-1 \right\}\right|$$

$$\varphi(6) = \left|\left\{ a \mid ggT(a,6)=1,\ 1 \le a < 5 \right\}\right|$$

a	1	2	3	4	5
	✓	✗	✗	✗	✓

$$\Rightarrow \varphi(6) = 2$$

Übung:

$$\varphi(12) = |\{1,5,7,11\}| = 4$$

$$\varphi(15) = |\{1,2,4,7,8,11,13,14\}| = 8$$

$$\varphi(7) = |\{1,2,3,4,5,6\}| = 6$$

$$\varphi(25) = 20$$

Berechnung von $\varphi(n)$:

① $n \in \mathbb{P}$ ← Menge der Primzahlen

$\varphi(n) = n-1$ bzw $\varphi(p) = p-1$

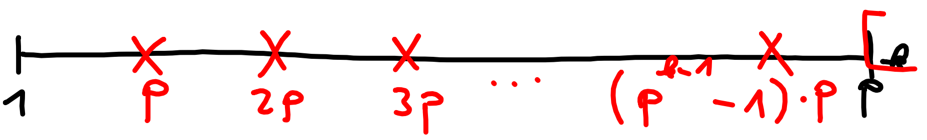
② $n = p^k$, $p \in \mathbb{P}$

$$p^k - 1 - (p^{k-1} - 1)$$

$$= p^k - p^{k-1}$$

$p^k - p$

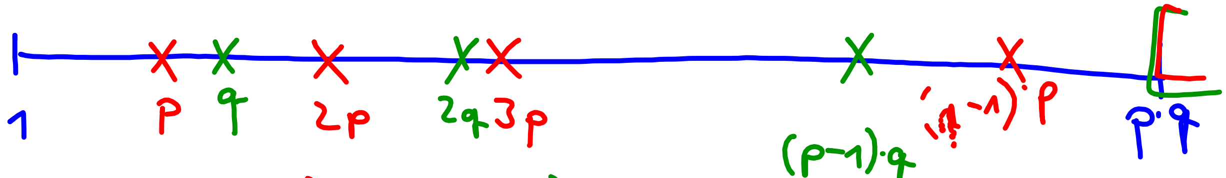
$(p^{k-1} - 1) \cdot p$



$$\Rightarrow \varphi(p^k) = p^k - p^{k-1}$$

[Beispiel: $\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$]

③ $\varphi(p \cdot q)$, $p, q \in \mathbb{P}$, $p \neq q$



$$p \cdot q - 1 - (q-1) - (p-1) = pq - p - q + 1$$

$$\boxed{\begin{aligned} \varphi(pq) &= pq - p - q + 1 \\ &= \underbrace{(p-1)}_{\varphi(p)} \cdot \underbrace{(q-1)}_{\varphi(q)} \end{aligned}}$$

allgemein:

es gilt sogar $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$

falls $ggT(m_1, m_2) = 1$