FLAG - TD

03.27.2023

$$B_D = \sum_{i=0}^{D-1} b_i x^{D-1-i}$$

$$V = x^d + \sum_{i=0}^{d} v_i x^i$$

- We only consider reccurence relation up to i, but assume it will be the same for all i (infiniety)

$$B_D V = r_0 + r_1 x + \cdots + r_{d-1} x^{d-1} \mod x^D$$

$$x^D u + B_D V = R \qquad \deg(R) < d$$

EEA until the $\deg(R) < \deg(V)$

Input: D terms of sequence $b = (b_i)_{i \in \mathbb{N}}$

Out: $V = (V_i)_{0 \le i \le d}$ $\quad d \le D/2$

- EEA (X^D, B_D)
- Stop when $\deg(R) < \deg(V)$

Example

$\underline{\mathbb{F}_{13}}$, $d = 4$, $D = 8$

$b = (6, 7, 7, 1, 2, 1, 6, 9)$

$$B_D = \sum_{i=0}^{D-1} b_i x^{D-i-1}$$

$$B_D = 9 + 6x + x^2 + 2x^3 + x^4 + 7x^5 + 7x^6 + 6x^7$$

$EEA(x^8, B_D)$

A	B_D	Q	R	U	V
x^8	$6x^7 + 7x^6 + 7x^5 \ldots\ldots$	$11x + 11$	$2x^6 + 3x^5 + 6x^4 + 6x^3 + x^2 + 4x + 5$		
		$\vdots$			

Example

$\mathbb{F}_{13}$, $d=2$, $D=4$

$b=(6,7,7,1)$

$$B_D = \sum_{i=0}^{D-1} b_i x^{D-i-1}$$

$$B_D = 1 + 7x + 7x^2 + 6x^3$$

$EEA(X^4, B_D)$

R	Q	u	v
x^4		1	0
$6x^3+7x^2+7x+1$	$11x+11$	0	1
$2x^2+3x+2$	$3x+12$	1	$2x+2$
$4x+3$		$10x+1$	$7x^2+9x+2$

$$X^D u + B_D V = R$$

$$B_D V = r_0 + \cdots + r^{d-1} x^{d-1}$$

$$V = x^d + \sum_{i=0}^{d-1} v_i x^i = 2 + 9x + 7x^2$$

we assume leading coefficient is 1, so $V/7$

$$V = x^2 + 5x + 4$$

there is some mistakes

Wiedemann Algo

$\Leftarrow$ theory based question on exam. (most likely)

Inputs: $M \in \mathbb{K}^{n \times n}$

Output: $u \in \mathbb{K}^n$ s.t. $M \cdot u = 0$

random: $x_0, y \in \mathbb{K}^n$

$x = Mx_0 \in \mathbb{K}^n$

$S = (S_i)_{i \in \mathbb{N}}$, $S_i = M^i x$ $\quad (x, Mx, M^2x, \dots)$

$b = (b_i)_{i \in N} = (y^T S_i) = (y^T M^i x)$

minimal poly. of M

$P_r = P_r x^r + \text{—} + P_0 \quad r \leq n$

$P_r(M) = 0$

$\sum_{i=0}^{r} P_i M^i = 0 \in \mathbb{K}^{n \times n}$

$\sum_{i=0}^{r} (P_i M^i) x = 0 \longrightarrow P_r(S) = 0$

$\sum_{i=0}^{r} y^T [(P_r M^i) x] = 0 \longrightarrow P_r(b) = 0$

$\sum_{i=0}^{r} P_r (y^T S_i) = 0$