11.3.2021 NACHMITTAG

Satz (Berlekamp) p Primzahl, $f \in \mathbb{F}_p[x]$ monisches Polynom $d = \deg(f) \geq 1$

$\forall j = 0, \dots, d-1$ sei $r_{0,j} + r_{1,j} x + \dots + r_{d-1,j} x^{d-1}$ der Rest der Teilung von x^{jp} durch f.

$$Q = \begin{bmatrix} r_{0,0} & r_{0,1} & \cdots & r_{0,d-1} \\ r_{1,0} & r_{1,1} & \cdots & r_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{d-1,0} & r_{d-1,1} & \cdots & r_{d-1,d-1} \end{bmatrix} \in M_d(\mathbb{F}_p)$$

Abbildungsmatrix von $Fr_A : A \longrightarrow A$ bezüglich der Basis $\{1, x, \dots, x^{d-1}\}$

$A = \mathbb{F}_p[x]/(f)$

1) Die erste Spalte von Q ist $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ und ist ein Eigenvektor von Q zum Eigenwert 1.

2) $\dim_{\mathbb{F}_p} \ker(Q - I) = \# \{\text{irreduzible monische Faktoren von } f\}$

Zahl

$f = x^2(x+1) \rightsquigarrow \# = 2$

$f = x^7 \rightsquigarrow \# = 1$

3) f irreduzibel $\iff \begin{cases} \gcd(f, f') = 1 \\ \dim_{\mathbb{F}_p} \ker(Q - I) = 1 \end{cases}$

4) Wenn $b = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d-1} \end{pmatrix} \in \ker(Q - I) \setminus \operatorname{Span}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$,

$h = b_0 + b_1 x + \dots + b_{d-1} x^{d-1} \implies$

$f = \gcd(f, h) \cdot \gcd(f, h-1) \cdot \ldots \cdot \gcd(f, h - p + 1)$

nicht triviale Zerlegung

Bws 1) $Fr_A(1) = 1^p = 1$

2) nicht einfach, ist auszulassen.

Let's assume that f is quadratfrei: $f = f_1 \cdots f_r$ paarweise verschiedene irreduzible Polynome

$$A = \mathbb{F}_p[x]/(f) \underset{\substack{\text{Chinese}\\\text{remainder}\\\text{theorem}}}{\simeq} \mathbb{F}_p[x]/(f_1) \times \cdots \times \mathbb{F}_p[x]/(f_r)$$

Körper!

$$\ker(Q - I) = \{ b \in (\mathbb{F}_p)^d \mid Qb = b \}$$

$$\updownarrow$$

$$B = \{ h \in A \mid Fr_A(h) = h \} = \{ h \in A \mid h^p = h \}$$

Unterraum von A

$$\begin{array}{ccc} A & \cong & \prod_{i=1}^{r} \mathbb{F}_p[x]/(f_i) \\ \uparrow & & \uparrow \\ B & \cong & \prod_{i=1}^{r} B_i \end{array}$$

$$B_i = \{ g \in \mathbb{F}_p[x]/(f_i) \mid g^p = g \}$$

$$\left.\begin{array}{l} \# B_i \leq p \\ B_i \supseteq \mathbb{F}_p \end{array}\right\} \Rightarrow B_i = \mathbb{F}_p$$

$A_i = \mathbb{F}_p[x]/(f_i)$ Körper $\quad \mathbb{F}_p \subseteq A_i$

$B_i = \{ g \in A_i \mid g^p = g \} = \left\{ \begin{array}{l} \text{Nullstelle vom Polynom } X^p - X \\ \text{im Körper } A_i \end{array} \right\}$

$\# B_i \leq \deg(X^p - X) = p$

Kleiner Satz von Fermat $\Rightarrow \forall a \in \mathbb{F}_p,\ a^p - a = 0 \Rightarrow$ jedes Element von $\mathbb{F}_p$ ist eine Nullstelle von $X^p - X$

$\Rightarrow \mathbb{F}_p \subseteq B_i$

$$\left. \begin{array}{l} \# B_i \leq p \\ B_i \supseteq \mathbb{F}_p \end{array} \right\} \Rightarrow B_i = \mathbb{F}_p$$

V $\mathbb{F}_p$ - Vektorraum der Dimension d

$\# V = p^d$ weil $V \cong (\mathbb{F}_p)^d$

3) f irreduzibel $\Longleftrightarrow \begin{cases} f \text{ quadratfrei} \\ f \text{ hat einen einzigen irreduziblen Faktor} \end{cases} \overset{2)}{\Longleftrightarrow} \begin{cases} \gcd(f, f') = 1 \\ \dim_{\mathbb{F}_p} \ker(Q - I) = 1 \end{cases}$

4) $b \in \ker(Q-I) \Rightarrow Qb = b \Rightarrow Fr_A(h) = h \Rightarrow h^p = h \Rightarrow$

$0 = h^p - h = \prod_{0 \le i < p} (h - i)$ in $A = \mathbb{F}_p[x]/(f)$

$\Rightarrow f$ teilt $h^p - h \Rightarrow f = \gcd\left(f, \prod_{0 \le i < p} (h-i)\right) = \prod_{0 \le i < p} \gcd(f, h-i)$

$b \notin \operatorname{Span}\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \deg h \geq 1$

$h, h-1, h-2, \dots, h-(p-1)$ paarweise relativisch prim

nicht trivial, weil $\deg \gcd(f, h-i) \le \deg h - i \le d-1 < \deg f$

$\square$

Der Berlekamp-Algorithmus funktioniert nicht wenn $\dim_{\mathbb{F}_p} \ker(Q-I) = 1$.

In diesem Fall:

1) wenn $\gcd(f, f') = 1 \rightsquigarrow f$ irreduzibel

ENDE

2) wenn $g = \gcd(f, f') \neq 1$

2a) $\deg g < \deg f \Rightarrow f = g \cdot \left(\frac{f}{g}\right)$

nicht triviale Zerlegung

2b) $\deg g = \deg f \Rightarrow f' = 0 \Rightarrow f$ ist eine p-te Potenz.