12.3.2021 VORMITTAG

$p$ Primzahl $\Rightarrow \prod_{i=0}^{p-1}(x-i) = x^p - x$ in $\mathbb{F}_p[x]$

Bws Sei $f$ Linkspolynom $\deg f = p$ $f$ monisch
Sei $g$ Rechtspolynom. $\deg g = p$ $g$ monisch

$\forall a \in \mathbb{F}_p$ $f(a) = 0$ $g(a) = 0$ (kleiner Satz von Fermat)

$\{\text{Nullstellen von } f\} = \{\text{Nullstellen von } g\} = \mathbb{F}_p$

---

Satz $A$ Ring mit Char. $p$, $h \in A \Rightarrow$

$$\prod_{i=0}^{p-1}(h-i) = h^p - h$$

Satz (Berlekamp) $p$ Primzahl, $f \in \mathbb{F}_p[x]$ monisch, $\deg(f) = d \geq 1$.
$Q \in M_d(\mathbb{F}_p)$ Abbildungsmatrix des Frobeniushom. von $\mathbb{F}_p[x]/(f)$.

- $\dim_{\mathbb{F}_p} \ker(Q-I) = \#$ verschiedene irreduzible Faktoren von $f$
- $\dim_{\mathbb{F}_p} \ker(Q-I) \geq 2 \Rightarrow$ wählen Sie $b \in \ker(Q-I) \setminus \mathrm{Span}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$

$h = b_0 + b_1 x + \dots + b_{d-1} x^{d-1}$, $f = \prod_{i=0}^{p-1} \gcd(f, h-i)$ nicht triviale Zerlegung!

Eine wiederholte Benutzung dieses Satzes gibt eine Zerlegung von $f$, wo jeder Faktor eine Potenze eines einzigen irreduziblen Faktors ist.

Bemerkung $h, h-1, \dots, h-(p-1)$ paarweise teilerfremd (relativisch prim)
$\Rightarrow \gcd(f,h), \gcd(f,h-1), \dots, \gcd(f, h-(p-1))$ paarweise teilerfremd.

<u>Beispiel</u> $f \in \mathbb{F}_p[x]$ monisch.

$\dim_{\mathbb{F}_p} \ker(Q - I) = 3 \implies$ # irreduzible Faktore von f $= 3$

$f_1, f_2, f_3$ paarweise verschiedene irred. monisch Polynome $\qquad f = f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3}$

$\alpha_1, \alpha_2, \alpha_3 \in \mathbb{N}^+$

Eine Basis von $\ker(Q-I)$ : $\left[\begin{array}{c|c|c} 1 & & \\ 0 & b & \bar{b} \\ \vdots & & \\ 0 & & \end{array}\right]$

- $b \rightsquigarrow h \rightsquigarrow$ 3 unten $\{\gcd(f, h-i) \mid 0 \le i < p\}$ sind nich trivial
  $\implies$ Sie müßen $f_1^{\alpha_1}, f_2^{\alpha_2}, f_3^{\alpha_3}$ sein.
- $\bar{b} \rightsquigarrow \bar{h} \rightsquigarrow$ 2 unten $\{\gcd(f, \bar{h}-i) \mid 0 \le i < p\}$ sind nicht trivial
  $\implies$ Sie müßen $f_1^{\alpha_1} f_2^{\alpha_2}$, $f_3^{\alpha_3}$ sein
  oder Permutationen

**Satz**[4.5] $\mathbb{K}$ Körper mit $\operatorname{char} \mathbb{K} = 0$ oder $\mathbb{K} = \mathbb{F}_p$.
$f \in \mathbb{K}[x]$ mit $\deg f \geq 1$. $g = \gcd(f, f') \in \mathbb{K}[x]$.
Genau eine von den folgenden Aussagen gilt:

1) $\deg g = 0$, $g = 1$, $f$ quadratfrei
2) $0 < \deg g < \deg f$, $f = g \cdot \left(\frac{f}{g}\right)$ nicht triviale Zerlegung
3) $\deg g = \deg f$, $\mathbb{K} = \mathbb{F}_p$, $f' = 0$, $\exists\, a_1, \dots, a_r \in \mathbb{F}_p$ mit

$$f = \sum_{i=0}^{r} a_i x^{ip} = \left(\sum_{i=0}^{r} a_i x^i\right)^p$$

Eine wiederholte Benutzung dieses Satzes gibt eine Zerlegung, wo jeder Faktor quadratfrei ist.

Um in $\mathbb{F}_p[x]$ zu faktorisieren, sollen Sie beide Sätze benutzen!

Beispiel 4.7 $f = x^7 + 3x^5 + 4x^4 + 3x^3 - 3x^2 + x + 1 \in \mathbb{F}_{11}[x]$

hat 2 irreduzible Faktore.

Berlekamp $\rightsquigarrow$ $h = x^2 + 2x^4 + x^6$

$$f = \underbrace{(x^4 + 2x^2 + 1)}_{= f_1} \cdot \underbrace{(x^3 + x + 4)}_{= f_2}$$

$\Rightarrow$ $f_1, f_2$ Potenzen von irreduziblen Polynomen

Man kann nicht mit $f_1, f_2$ Berlekamp verwenden.

Satz 4.5 mit $f_1$: $\gcd(f_1, f_1') = x^2 + 1$ $\quad \dfrac{f_1}{\gcd(f_1, f_1')} = x^2 + 1$

so $f_1 = (x^2+1)^2$ $\quad x^2 + 1 \in \mathbb{F}_{11}[x]$ irr.

Satz 4.5 mit $f_2$: $\gcd(f_2, f_2') = 1 \Rightarrow f_2$ quadratfrei

$\Rightarrow$ $f = (x^2+1)^2 (x^3 + x + 4)$

Beispiel 4.8 $f =$ gleiches Polynom in $\mathbb{F}_{11}[x]$ $\deg(f) = 7$

Satz 4.5 : $a_1 = \gcd(f, f') = x^2+1$ $a_2 = \frac{f}{a_1} = x^5 + 2x^3 + 4x^2 + x + 4$

Satz 4.5 mit $a_1$ : $\gcd(a_1, a_1') = 1 \Rightarrow a_1$ quadratfrei.

Satz 4.5 mit $a_2$ : $\gcd(a_2, a_2') = 1 \Rightarrow a_2$ " "

Berlekamp mit $a_1$ : $a_1$ hat 1 irr. Faktor $\Rightarrow a_1$ irreduzibel

Berlekamp mit $a_2$ : $a_2$ hat 2 irr. Faktor $\Rightarrow$ Wählen

$b_1 \in \ker(Q_{a_2} - I) \sim \operatorname{Span}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ $h_1 = x + x^3$

die nicht trivialen Elemente in $\{\gcd(a_1, h_1 - i) \mid 0 \leq i < 11\}$

sind $x^2+1$ und $x^3+x+4$ ($\Rightarrow$ sie sind irr.)

$a_2 = (x^2+1) \cdot (x^3+x+4)$

$f = a_1 \cdot a_2 = (x^2+1) \cdot \left((x^2+1)(x^3+x+4)\right) = (x^2+1)^2 (x^3+x+4)$

$\dim_{\mathbb{F}_p} \ker(Q - I) = \#$ irr. Faktor von $f$

$\gcd(f, f') = 1 \iff f$ quadratfrei

$$\left\{\begin{array}{l} \dim_{\mathbb{F}_p} \ker(Q-I) = 1 \\ \gcd(f, f') = 1 \end{array}\right. \iff f \text{ irr.}$$

Ist Irreduzibel

$$f = 3x^{34} + 5x^{17} + 2 \in \mathbb{F}_{17}[x]$$

Satz 4.5 mit $f$? $\quad f' = 3 \cdot 34 x^{33} + 5 \cdot 17 x^{16} = 0$

$$\gcd(f, f') = \gcd(f, 0) = f$$

$$f = 3^{17} x^{34} + 5^{17} x^{17} + 2^{17} = (3x^2)^{17} + (5x)^{17} + 2^{17}$$

$$= (3x^2 + 5x + 2)^{17}$$

Ist $3x^2 + 5x + 2$ irreduzibel?

Aufgabe 4.3.1 – 4.3.4

Aufgabe 3.3.3.

Die Faktorisierung-Aufgabe
in der Prüfung
ist ähnlich zu
Beispiel 4.7, 4.8

$\boxed{\S 5}$

Lesen Sie den Anfang von § 5 !