FFC 28.4.08

Berlekamp erlaubt uns quadratfreie Polynome

$f = f_1 \cdots f_s$ (f_i irred $P \in \mathbb{F}_q[x]$) zu faktorisieren:

Wenn $\deg f = n$, dann x^{qk} $0 \le k < \deg f$ mit Rest durch f dividieren

$x^{qk} = h_k(x) f(x) + r_k(x)$ $\quad r_k(x) = \sum_{j=0}^{n-1} b_{kj} x^j$. $B = (b_{kj})_{0 \le j \le n-1}^{0 \le k \le n-1}$; Lineares Gl sys.

$(c_0, \ldots, c_{n-1})(B - I) = 0$ lösen: dim als $\mathbb{F}_q$-VR des Lösungsraums ist s = Anzahl der versch. irred Faktoren von f; $(c_0 c_1 \ldots c_{n-1}) \neq (c_0, 0, \ldots, 0)$ falls verschied $s > 1$ liefert f reduzierende Polyn. $g = \sum_{i=0}^{k} c_i x^i$ $\quad f = \prod_{c \in \mathbb{F}_q} \operatorname{ggT}(f, g - c)$ ist nicht triv. Faktorisierung iterieren falls f noch nicht komplett faktorisiert. Jetzt müssen ~~wir~~ wir noch die Faktorisierung eines bel. $f \in \mathbb{F}_q[x]$ auf Faktorisierung von quadratfreien Polyn. zurückführen.

Sei f. zuerst f' bilden. Wenn $f' = 0$ ($f = \sum a_k x^k$, $f' = \sum k a_k x^{k-1} = 0 \Rightarrow$ jedes k mit $a_k \neq 0$ ist Vielfaches von p). Dann $f = \sum_k a_k x^{pk}$, f ist eine p-te Potenz: sei $b_k \in \mathbb{F}_q$ mit $b_k^p = a_k$ dann $f = \sum a_k x^{pk} = \sum b_k^p x^{pk} = (\sum b_k x^k)^p$. p-te Wurzel aus $f = \sum a_k x^{pk}$ ziehen erfordert finden von $b \in \mathbb{F}_q$ mit $b^p = a$ für bel $a \in \mathbb{F}_q$. Für $a = 0$, $b = 0$ v Für $a \neq 0$ $\operatorname{ggT}(p, q-1) = 1$ finde $\alpha, \beta \in \mathbb{Z}$ $\quad \alpha p + \beta(q-1) = 1$ $\quad b := a^\alpha$ denn $b^p = a^{\alpha p} = a^{\alpha p} \cdot 1 = a^{\alpha p} \cdot a^{(q-1)\beta} = a^1 = a$. Also wenn $f' = 0$ die p-te ~~Potenz~~ Wurzel aus f berech (iteriere bis $f' \neq 0$)

Sei f mit $f' \neq 0$; bilde $\operatorname{ggT}(f, f') = d$ und $\frac{f}{d}$ quadratfrei.

$g = \frac{f}{d}$ mit Berlekamp faktorisieren, irred. Faktorisierung von g aus f wegdividieren (zur höchst mögl. Potenz) man erhält eine p-te Potenz, iterieren.

Wenn nämlich $f = h^p f_1^{k_1} \cdots f_s^{k_s}$ $\quad 1 \le k_i < p$ dann $f' = h^p (f_1^{k_1} \cdots f_s^{k_s})'$

$\operatorname{ggT}(f, f') = h^p f_1^{k_1 - 1} \cdots f_s^{k_s - 1}$ und $\frac{f}{\operatorname{ggT}(f, f')} = f_1 \cdots f_s$

Bem: Man kann (Berlekamp-Zassenhaus) ein Alg zur Faktorisierung von Polyn. in $\mathbb{Z}_p[x]$ auch zum Faktorisieren von Polyn. $\in \mathbb{Z}[x]$ verwenden (z.B. in Mignotte/Stefanescu) irreduzible Polynome in $\mathbb{F}_q[x]$

Zur Erinnerung: $\forall f$ irred $\in \mathbb{F}_q[x]$ ist der Zerfällungskörper über $\mathbb{F}_q$ derselbe, nämlich der eind. bestimmte Körper mit q^n El. (der Zerf. kö aller irred Polyn. $\in \mathbb{F}_q$ vom Grad n enthält nur einen Körper der Ord. q^n).

Außerdem reicht es eine Nst α ein irred $f \in \mathbb{F}_q[x]$ zu adjungieren, $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^n}$, wo f und alle anderen irred Polyn. vom Grad n über $\mathbb{F}_q$ zerfallen.

Lemma: $x^{q^n} - x \in \mathbb{F}_q[x]$. Dann $x^{q^n}-x$ ist Produkt aller normierten irred Polyn. $\in \mathbb{F}_q[x]$, deren Grad n teilt.

Bew: in $\mathbb{F}_{q^n}[x]$ zerfällt $x^{q^n}-x = \prod_{c\in\mathbb{F}_{q^n}}(x-c)$. Kein mehrf. Nst, also in $\mathbb{F}_q[x]$ keine mehrfachen Faktoren. Jedes irred $f \in \mathbb{F}_q[x]$ mit deg $f = d | n$ hat Nst in $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$, daher teilt f (Minipoly $\in \mathbb{F}_q[x]$ ein der $c \in \mathbb{F}_{q^n}$) in $\mathbb{F}_q[x]$ das Polyn. $x^{p^n}-x$. Kein anderen irred Faktoren als die Minimalpoly der $c \in \mathbb{F}_{q^n}$ in $\mathbb{F}_q[x]$, und die Elemente von $\mathbb{F}_{q^n}$ haben ein Minimalpoly deren Grad $[\mathbb{F}_q[c]:\mathbb{F}_q]$ n teilt, da $\mathbb{F}_q[c] \subseteq \mathbb{F}_{q^n}$
$\Rightarrow$ $\mathbb{F}_q[c]$ hat q^d El für ein $d|n$ da $[\mathbb{F}_q[c]:\mathbb{F}_q] = d | n$.
Anders ausgedrückt: $\prod_{c\in\mathbb{F}_{q^n}}(x-c)$ ist, da in $\mathbb{F}_q[x]$, Prod aller Minimalpoly aller $c \in \mathbb{F}_{q^n}$ über $\mathbb{F}_q$ (je einer). Diese Minimalpoly sind genau die irred normierten Poly $\in \mathbb{F}_q[x]$ mit deg $| n$. $\square$

Notation: Sei $I(q,n)(x)$ = Prod. aller normierten irred Polyn. $\in \mathbb{F}_q[x]$ mit deg $= n$.

Dann 1) $x^{q^n}-x = \prod_{d|n} I(q,d)(x)$ und $N_q(d)$ die Anzahl der versch normierten irred Polyn. $\in \mathbb{F}_q[x]$ mit deg $= d$.

und 2) $q^n = \sum_{d|n} d\, N_q(d)$

Daraus können wir mit Möbius Inversion Formeln für $I(n,q)(x)$ und $N_q(d)$ erhalten.

Zahlentheoretische Möbius Funktion und Möbius Inversion.

Def: für $n \in \mathbb{N} = \{1,2,\dots\} = \{n \in \mathbb{Z} \mid n>0\}$. def $\mu(n) = \begin{cases} (-1)^s & n = p_1 \cdots p_s \text{ quadratfrei } p_i \text{ prim} \\ 0 & \text{sonst (n nicht quadratfrei)} \end{cases}$

Bem: n heißt quadratfrei, wenn $\nexists\, p$ prim : $p^2 \mid n$. (nicht Prod von s versch. PZ $n = p_1 \cdots p_s$, 1 gilt als Prod von 0 Primzahlen)

Lemma: $\sum_{d \mid n} \mu(d) = \begin{cases} 0 & n \neq 1 \\ 1 & n = 1 \end{cases}$ (d|n im Summationsindex heißt summieren über alle $d \in \mathbb{N}$ mit $1 \le d \le n$ und $d \mid n$)

Bew: $n=1$ ✓ $n>1$: $\sum_{d \mid n} \mu(d) = \sum_{\substack{d \mid n \\ d \text{ quadratfrei}}} \mu(d) = \sum_{k=0}^{s} \binom{s}{k} (-1)^k = (1-1)^s = 0$ wobei

$n = p_1 \cdots p_s$ und es $\binom{s}{k}$ quadratfreie Teiler $d = p_{i_1} \cdots p_{i_k}$ mit k versch. Primzahlen gibt, die jeweils $\mu(d) = (-1)^k$ beitragen

Satz (Möbius-Inversion)

Seien f, g Funktionen $: \mathbb{N} \to (G,+)$ (kom. Gruppe) sodass $g(n) = \sum_{d \mid n} f(d)$ dann

$$g(n) = \sum_{d \mid n} \mu\left(\tfrac{n}{d}\right) f(d) = \sum_{\substack{(c,d) \\ cd = n \\ 1 \le c,d \le n}} \mu(c) f(d).$$

Dasselbe multiplikativ geschrieben, wenn $f, g : \mathbb{N} \to (G, \cdot)$ kom. Gruppe ist.

$g(n) = \prod_{d \mid n} f(d)$, dann $f(n) = \prod_{d \mid n} g(d)^{\mu(\frac{n}{d})} = \prod_{\substack{(c,d) \\ 1 \le c,d \le n \\ c \cdot d = n}} g(d)^{\mu(c)}$

Bew: zeige $g(n) = \sum_{d \mid n} f(d) \Rightarrow f(n) = \sum_{d \mid n} g(d) \mu\left(\frac{n}{d}\right)$ [$\Leftarrow$ Ü]

$$\sum_{d \mid n} g\left(\tfrac{n}{d}\right) \mu(d) = \sum_{d \mid n} \Big(\sum_{c \mid \frac{n}{d}} g(c) \Big) \mu(d) = \sum_{\substack{(c,d) \\ c \cdot d \mid n}} g(c) \mu(d) = \sum_{c \mid n} g(c) \underbrace{\sum_{d \mid \frac{n}{c}} \mu\left(\tfrac{n}{c}\right)}_{= 0 \text{ außer } n = c} = g(n)$$

[Möbius Inversion angewendet auf]

Kor: $I(q,n)(x) = \prod_{d \mid n} \left(x^{q^d} - x\right)^{\mu(\frac{n}{d})} = \prod_{\substack{(c,d) \\ c \cdot d = n \\ 1 \le c,d \le n}} \left(x^{q^d} - x\right)^{\mu(c)}$

und $N_q(n) = \frac{1}{n} \sum_{d \mid n} q^d \mu\left(\frac{n}{d}\right) = \frac{1}{n} \sum_{\substack{(c,d) \\ c \cdot d = n}} q^d \mu(c)$

Bew: Möbius Inversion angewendet auf $x^{q^n}-x=\prod_{d|n} I(q,n)(x)$ und auf $q^n=\sum_{d|n} d\, N_q(d)$

mit $g(n)=q^n$, $f(n)=n\,N_q(n)$.

Außerdem: $I(q,n)(x)$

Prop: $\cancel{x^{q^n}-x} = \prod_{\substack{m|q^n-1 \\ m\nmid q^k-1 \text{ f. } 1\le k<n}} \varphi_m(x)$ für $n>1$, ~~...~~

Bew: im Zerfällungskörper von $x^{q^n}-x$, welcher der Zerf.kö von $x^{q^n-1}-1$ ist

$x^{q^n-1}-1=\prod_{\substack{c\in\mathbb{F}_{q^n}\\ c\neq 0}}(x-c)$. Die El. $c\in\mathbb{F}_{q^n}\setminus\{0\}$ sind d-te Einheitswurzeln

jeweils für ein $d|q^n-1$ (d die Ordnung von c in $(\mathbb{F}_{q^n}\setminus\{0\},\cdot)$).

$\prod_{\substack{c\in\mathbb{F}_{q^n}\\ c\ d\text{-te EW}}}(x-c)=\varphi_d(x)$. Der kleinste Oberkörper von $\mathbb{F}_q$, der alle d-ten EW enthält ist $\mathbb{F}_{q^l}$ mit l minimal sod $d|q^l-1$

D.h. Prod über alle $(x-c)$ mit c primitive d-te EW in $\mathbb{F}_{q^n}$, die keinen kleineren Erweiterungskörper von $\mathbb{F}_q$ enthalten, ist, ist einerseits $\prod_{\substack{d|q^n-1\\ d\nmid q^k-1\ 1\le k<n}}\varphi_d(x)$ und andererseits das Prod aller irred Polyn., deren Grad n ist. jedes El $\neq 0$ von $\mathbb{F}_{q^n}$ ist primitive d-te EW für ein $d|n$ und genau dann erzeugt c den Körper $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ d.h. $\mathbb{F}_{q^n}=\mathbb{F}_q[c]$ wenn entweder das Min.poly von c über $\mathbb{F}_q$ $\deg = n$ hat oder äquiv. der kleinste exponent von q ist, sod $\mathbb{F}_{q^n}$ ein primitive d-te EW hat d.h. $d|q^n-1$ $d\nmid q^k-1$ $1\le k<n$.