Colloquium zur Masterarbeit

# Theoretische und experimentelle Untersuchungen zu Normalbasen für Erweiterungen endlicher Körper

Stefan Hackenberg

4. Februar 2015

# 1 Grundlagen

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

Definition (normales Element)

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

## Definition (normales Element)

## Definition (vollständig normales Element)

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

## Definition (normales Element)

## Definition (vollständig normales Element)

## Definition (primitives Element)

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

## Definition (normales Element)

Sei $w \in E$ mit $F(w) = E$. $w$ heißt *normal über* $F$, falls

$$\{\gamma(w) : \gamma \in \mathrm{Gal}(E \mid F)\}$$

eine $F$-Basis von $E$ ist.

## Definition (vollständig normales Element)

## Definition (primitives Element)

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

## Definition (normales Element)

Sei $w \in E$ mit $F(w) = E$. $w$ heißt *normal über $F$*, falls

$$\{\gamma(w) : \gamma \in \mathrm{Gal}(E \mid F)\} = \{w, \sigma(w), \ldots, \sigma^{n-1}(w)\} = \{w, w^q, \ldots, w^{q^{n-1}}\}$$

eine $F$-Basis von $E$ ist. Wobei $\sigma : E \to E,\ v \mapsto v^q$ den *Frobenius-Endomorphismus von $F$* notiert.

## Definition (vollständig normales Element)

## Definition (primitives Element)

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

## Definition (normales Element)

Sei $w \in E$ mit $F(w) = E$. $w$ heißt *normal über $F$*, falls

$$\{\gamma(w) : \gamma \in \mathrm{Gal}(E \mid F)\} = \{w, \sigma(w), \ldots, \sigma^{n-1}(w)\} = \{w, w^q, \ldots, w^{q^{n-1}}\}$$

eine $F$-Basis von $E$ ist. Wobei $\sigma : E \to E,\ v \mapsto v^q$ den *Frobenius-Endomorphismus von $F$* notiert.

## Definition (vollständig normales Element)

$w \in E$ heißt *vollständig normal*, falls $w$ normal über jedem Zwischenkörper $E \mid K \mid F$ ist.

## Definition (primitives Element)

# Definitionen

Sei $F := \mathbb{F}_q$ ein endlicher Körper für eine Primzahlpotenz $q = p^r$ mit $r \geq 1$ mit einem fest gewählten algebraischen Abschluss $\bar{F}$ und $E := \mathbb{F}_{q^n}$ eine Körpererweiterung von Grad $n$.

## Definition (normales Element)

Sei $w \in E$ mit $F(w) = E$. $w$ heißt *normal über $F$*, falls

$$\{\gamma(w) : \gamma \in \mathrm{Gal}(E \mid F)\} = \{w, \sigma(w), \ldots, \sigma^{n-1}(w)\} = \{w, w^q, \ldots, w^{q^{n-1}}\}$$

eine $F$-Basis von $E$ ist. Wobei $\sigma : E \to E,\ v \mapsto v^q$ den *Frobenius-Endomorphismus von $F$* notiert.

## Definition (vollständig normales Element)

$w \in E$ heißt *vollständig normal*, falls $w$ normal über jedem Zwischenkörper $E \mid K \mid F$ ist.

## Definition (primitives Element)

$:= E \setminus \{0\}$

$w \in E$ heißt *primitiv*, falls $\langle u \rangle = E^*$, also $u$ ein Erzeuger der multiplikativen Gruppe $E^*$ ist.

# Der Frobenius

**Definition (Frobenius-Endomorphismus von $F$)**

$$\sigma : \begin{array}{ccc} E & \to & E, \\ v & \mapsto & v^q \end{array}$$

heißt der *Frobenius-Endomorphismus von $F$*.

# Der Frobenius

**Definition (Frobenius-Endomorphismus von $F$)**

$$\sigma : \begin{array}{ccc} E & \to & E, \\ v & \mapsto & v^q \end{array}$$

heißt der *Frobenius-Endomorphismus von $F$*.

**Satz**

Es gilt:

- $\sigma$ ist eine $F$-lineare Abbildung.

# Der Frobenius

**Definition (Frobenius-Endomorphismus von $F$)**

$$\begin{aligned} \sigma: \quad E &\to E, \\ v &\mapsto v^q \end{aligned}$$

heißt der *Frobenius-Endomorphismus von $F$*.

**Satz**

Es gilt:

- $\sigma$ ist eine $F$-lineare Abbildung.
- $\sigma\big|_F = \mathrm{id}_F$.

# Der Frobenius

### Definition (Frobenius-Endomorphismus von $F$)

$$\begin{array}{rccl} \sigma: & E & \to & E, \\ & v & \mapsto & v^q \end{array}$$

heißt der *Frobenius-Endomorphismus von $F$*.

### Satz

Es gilt:

- $\sigma$ ist eine $F$-lineare Abbildung.
- $\sigma\big|_F = \mathrm{id}_F$.
- Das Minimalpolynom $\mu_\sigma(x)$ (also das Polynom $g(x) \in F[x]$ kleinsten Grades mit $f(\sigma) = 0$) von $\sigma$ ist
$$\mu_\sigma(x) = x^n - 1\,.$$

# Idee zur Untersuchung von Normalbasen

## Idee

Betrachte $E$ als $F[x]$-Modul durch

$$\begin{array}{rcl} F[x] \times E & \to & E\,, \\ (f(x), v) & \mapsto & f(x) \cdot v := f(\sigma)(v)\,. \end{array}$$

# Idee zur Untersuchung von Normalbasen

### Idee

Betrachte $E$ als $F[x]$-Modul durch

$$\begin{array}{rcl} F[x] \times E & \to & E\,, \\ (f(x), v) & \mapsto & f(x) \cdot v := f(\sigma)(v)\,. \end{array}$$

### Genauer

Seien $f(x) = f_k x^k + \ldots + f_1 x + f_0$ und $v \in E$, so ist

$$f(x) \cdot v \;=\; f(\sigma)(v) \;=$$

# Idee zur Untersuchung von Normalbasen

### Idee

Betrachte $E$ als $F[x]$-Modul durch

$$\begin{aligned} F[x] \times E &\to E\,, \\ (f(x), v) &\mapsto f(x) \cdot v := f(\sigma)(v)\,. \end{aligned}$$

### Genauer

Seien $f(x) = f_k x^k + \ldots + f_1 x + f_0$ und $v \in E$, so ist

$$f(x) \cdot v \;=\; f(\sigma)(v) \;=\; f_k \sigma^k(v) + \ldots + f_1 \sigma(v) + f_0 \sigma^0(v)$$

## Idee zur Untersuchung von Normalbasen

### Idee

Betrachte $E$ als $F[x]$-Modul durch

$$\begin{array}{rcl} F[x] \times E & \to & E\,, \\ (f(x), v) & \mapsto & f(x) \cdot v := f(\sigma)(v)\,. \end{array}$$

### Genauer

Seien $f(x) = f_k x^k + \ldots + f_1 x + f_0$ und $v \in E$, so ist

$$f(x) \cdot v = f(\sigma)(v) = f_k \sigma^k(v) + \ldots + f_1 \sigma(v) + f_0 \sigma^0(v) = f_k v^{q^k} + \ldots + v^q + f_0 v\,.$$

### Definition/Lemma ($q$-Ordnung)

Sei $v \in E$. Betrachte den $F[x]$-Modulhomomorphismus

$$\begin{array}{rccl} \psi_v : & F[x] & \to & E\,, \\ & f(x) & \mapsto & f(x) \cdot v\,. \end{array}$$

### Definition/Lemma ($q$-Ordnung)

Sei $v \in E$. Betrachte den $F[x]$-Modulhomomorphismus

$$\begin{aligned} \psi_v : \quad F[x] &\to E\,, \\ f(x) &\mapsto f(x) \cdot v\,. \end{aligned}$$

1 Ist $\ker \psi_v = (g(x))$ für ein $g(x) \in F[x]$ normiert, so heißt $g(x)$ die *$q$-Ordnung von $v$*. Schreibe $\mathrm{Ord}_q(v) := g(x)$. Die $q$-Ordnung ist eindeutig.

### Definition/Lemma ($q$-Ordnung)

Sei $v \in E$. Betrachte den $F[x]$-Modulhomomorphismus

$$\begin{aligned} \psi_v : \quad F[x] &\to E\,, \\ f(x) &\mapsto f(x) \cdot v\,. \end{aligned}$$

1. Ist $\ker \psi_v = (g(x))$ für ein $g(x) \in F[x]$ normiert, so heißt $g(x)$ die *$q$-Ordnung von $v$*. Schreibe $\mathrm{Ord}_q(v) := g(x)$. Die $q$-Ordnung ist eindeutig.
2. $F[x] \cdot v := \operatorname{im} \psi_v$ heißt der von $v$ *erzeugte $F[x]$-Teilmodul von $E$*.

### Definition/Lemma ($q$-Ordnung)

Sei $v \in E$. Betrachte den $F[x]$-Modulhomomorphismus

$$\psi_v : \begin{array}{ccc} F[x] & \to & E\,, \\ f(x) & \mapsto & f(x) \cdot v\,. \end{array}$$

1. Ist $\ker \psi_v = (g(x))$ für ein $g(x) \in F[x]$ normiert, so heißt $g(x)$ die *$q$-Ordnung von $v$*. Schreibe $\mathrm{Ord}_q(v) := g(x)$. Die $q$-Ordnung ist eindeutig.
2. $F[x] \cdot v := \operatorname{im} \psi_v$ heißt der von $v$ *erzeugte $F[x]$-Teilmodul von $E$*.

Zu $g(x) \mid x^n - 1$ normiert definiere

$$V_g := \{v \in E : \; g(x) \cdot v = 0\}\,.$$

### Satz

Es gilt:

### Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.

### Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.
2. Alle $F[x]$-Teilmoduln von $E$ sind von dieser Form.

### Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.
2. Alle $F[x]$-Teilmoduln von $E$ sind von dieser Form.
3. Die Erzeuger von $V_g$ sind genau die Elemente $v \in E$ mit $\mathrm{Ord}_q(v) = g(x)$, d.h. für diese gilt $F[x] \cdot v = V_g$.

### Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.
2. Alle $F[x]$-Teilmoduln von $E$ sind von dieser Form.
3. Die Erzeuger von $V_g$ sind genau die Elemente $v \in E$ mit $\mathrm{Ord}_q(v) = g(x)$, d.h. für diese gilt $F[x] \cdot v = V_g$.

### Satz

Sei $g(x) \in F[x]$ mit $g(x) \mid x^n - 1$ normiert und $\Delta \subset F[x]$ eine Zerlegung von $g(x)$, d.h. $g(x) = \prod_{\delta \in \Delta} \delta(x)$ mit $\delta \in \Delta$ paarweise teilerfremd, dann gilt

### Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.
2. Alle $F[x]$-Teilmoduln von $E$ sind von dieser Form.
3. Die Erzeuger von $V_g$ sind genau die Elemente $v \in E$ mit $\mathrm{Ord}_q(v) = g(x)$, d.h. für diese gilt $F[x] \cdot v = V_g$.

### Satz

Sei $g(x) \in F[x]$ mit $g(x) \mid x^n - 1$ normiert und $\Delta \subset F[x]$ eine Zerlegung von $g(x)$, d.h. $g(x) = \prod_{\delta \in \Delta} \delta(x)$ mit $\delta \in \Delta$ paarweise teilerfremd, dann gilt

1. $V_g = \oplus_{\delta \in \Delta} V_\delta$.

## Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.
2. Alle $F[x]$-Teilmoduln von $E$ sind von dieser Form.
3. Die Erzeuger von $V_g$ sind genau die Elemente $v \in E$ mit $\mathrm{Ord}_q(v) = g(x)$, d.h. für diese gilt $F[x] \cdot v = V_g$.

## Satz

Sei $g(x) \in F[x]$ mit $g(x) \mid x^n - 1$ normiert und $\Delta \subset F[x]$ eine Zerlegung von $g(x)$, d.h. $g(x) = \prod_{\delta \in \Delta} \delta(x)$ mit $\delta \in \Delta$ paarweise teilerfremd, dann gilt

1. $V_g = \oplus_{\delta \in \Delta} V_\delta$.
2. Jedes $w \in V_g$ lässt sich eindeutig schreiben als $w = \sum_{\delta \in \Delta} w_\delta$ mit $w_\delta \in V_\delta$. Ferner gilt

$$\mathrm{Ord}_q(w) = \prod_{\delta \in \Delta} \mathrm{Ord}_q(w_\delta)$$

und $\mathrm{Ord}_q(w)$ ist ein normierter Teiler von $g(x)$.

## Satz

Es gilt:

1. Für $g(x) \mid x^n - 1$ normiert ist $V_g$ ein $F[x]$-Teilmodul von $E$.
2. Alle $F[x]$-Teilmoduln von $E$ sind von dieser Form.
3. Die Erzeuger von $V_g$ sind genau die Elemente $v \in E$ mit $\mathrm{Ord}_q(v) = g(x)$, d.h. für diese gilt $F[x] \cdot v = V_g$.

## Satz

Sei $g(x) \in F[x]$ mit $g(x) \mid x^n - 1$ normiert und $\Delta \subset F[x]$ eine Zerlegung von $g(x)$, d.h. $g(x) = \prod_{\delta \in \Delta} \delta(x)$ mit $\delta \in \Delta$ paarweise teilerfremd, dann gilt

1. $V_g = \oplus_{\delta \in \Delta} V_\delta$.
2. Jedes $w \in V_g$ lässt sich eindeutig schreiben als $w = \sum_{\delta \in \Delta} w_\delta$ mit $w_\delta \in V_\delta$. Ferner gilt

   $$\mathrm{Ord}_q(w) = \prod_{\delta \in \Delta} \mathrm{Ord}_q(w_\delta)$$

   und $\mathrm{Ord}_q(w)$ ist ein normierter Teiler von $g(x)$.
3. $w$ ist ein Erzeuger von $V_g \quad \Leftrightarrow \quad \forall \delta \in \Delta: \ w_\delta$ ist Erzeuger von $V_\delta$.

# Zurück zur Normalität

**Lemma**

Für $v \in E$ gilt:

$v$ ist normal über $F$

# Zurück zur Normalität

**Lemma**

Für $v \in E$ gilt:

$$v \text{ ist normal über } F \quad \Leftrightarrow \quad F[x] \cdot v = E$$

# Zurück zur Normalität

### Lemma

Für $v \in E$ gilt:

$$v \text{ ist normal über } F \quad \Leftrightarrow \quad F[x] \cdot v = E \quad \Leftrightarrow \quad \mathrm{Ord}_q(v) = x^n - 1\,.$$

# Zurück zur Normalität

## Lemma

Für $v \in E$ gilt:

$$v \text{ ist normal über } F \quad \Leftrightarrow \quad F[x] \cdot v = E \quad \Leftrightarrow \quad \mathrm{Ord}_q(v) = x^n - 1\,.$$

## Strategie: Arbeite eigenständig auf Teilmoduln

Für eine geeignete Zerlegung $\Delta$ von $x^n - 1$ über $F$ finde für jedes $\delta \in \Delta$ ein Element $w_\delta \in E$ mit $\mathrm{Ord}_q(w_\delta) = \delta$. Dann ist

$$\sum_{\delta \in \Delta} w_\delta$$

normal über $F$.

# Zurück zur Normalität

## Lemma

Für $v \in E$ gilt:

$$v \text{ ist normal über } F \quad \Leftrightarrow \quad F[x] \cdot v = E \quad \Leftrightarrow \quad \mathrm{Ord}_q(v) = x^n - 1\,.$$

## Strategie: Arbeite eigenständig auf Teilmoduln

Für eine geeignete Zerlegung $\Delta$ von $x^n - 1$ über $F$ finde für jedes $\delta \in \Delta$ ein Element $w_\delta \in E$ mit $\mathrm{Ord}_q(w_\delta) = \delta$. Dann ist

$$\sum_{\delta \in \Delta} w_\delta$$

normal über $F$.
Gute Zerlegung:

*d*-tes Kreisteilungspolynom

$$x^n - 1 \;=\; \prod_{d | \bar{n}} \Phi_d(x)^{p^b}$$

für $n = \bar{n}p^b$ mit $p \nmid \bar{n}$.

# 3 Vollständig normale Elemente

# Vollständig normale Elemente

**Definition**

$w \in E$ heißt *vollständig normal*, falls $w$ normal über jedem Zwischenkörper $E \mid K \mid F$ ist.

# Vollständig normale Elemente

**Definition**

$w \in E$ heißt *vollständig normal*, falls $w$ normal über jedem Zwischenkörper $E \mid K \mid F$ ist.

**Definition**

einfach $E$ über $F$ heißt *einfach*, falls jedes normale Element von $E$ über $F$ bereits vollständig normal ist.

# Vollständig normale Elemente

### Definition

$w \in E$ heißt *vollständig normal*, falls $w$ normal über jedem Zwischenkörper $E \mid K \mid F$ ist.

### Definition

einfach $E$ über $F$ heißt *einfach*, falls jedes normale Element von $E$ über $F$ bereits vollständig normal ist.

### Satz

$E$ über $F$ ist einfach, falls

- $n = r$ oder $n = r^2$ für eine Primzahl $r$.
- $\bar{n} \mid q - 1$, wobei $n = n' p^b$ mit $p \nmid n'$,
- $n = p^b$ für $b \geq 0$.

Idee: Nutze wieder Modulstrukturen!

Idee: Nutze wieder Modulstrukturen!

**Definition (verallgemeinertes Kreisteilungspolynom)**

Für $k, t \in \mathbb{N}^*$ mit $p \nmid k$ heißt

$$\Phi_{k,t}(x) := \Phi_k(x^t) \quad \in F[x]$$

*verallgemeinertes Kreisteilungspolynom*.

Idee: Nutze wieder Modulstrukturen!

**Definition (verallgemeinertes Kreisteilungspolynom)**

Für $k, t \in \mathbb{N}^*$ mit $p \nmid k$ heißt

$$\Phi_{k,t}(x) := \Phi_k(x^t) \quad \in F[x]$$

*verallgemeinertes Kreisteilungspolynom*.

**Definition (verallgemeinerter Kreisteilungsmodul)**

Für ein verallgemeinertes Kreisteilungspolynom $\Phi_{k,t}(x)$ heißt

$$\mathcal{C}_{k,t} := \{w \in \bar{F} : \Phi_{k,t}(\sigma)(w) = 0\}$$

*verallgemeinerter Kreisteilungsmodul*. Der Modulcharakter von $\mathcal{C}_{k,t}$ ist $\frac{k\,t}{\nu(k)}$.

Idee: Nutze wieder Modulstrukturen!

**Definition (verallgemeinertes Kreisteilungspolynom)**

Für $k, t \in \mathbb{N}^*$ mit $p \nmid k$ heißt

$$\Phi_{k,t}(x) := \Phi_k(x^t) \quad \in F[x]$$

*verallgemeinertes Kreisteilungspolynom*.

**Definition (verallgemeinerter Kreisteilungsmodul)**

Für ein verallgemeinertes Kreisteilungspolynom $\Phi_{k,t}(x)$ heißt

$$\mathcal{C}_{k,t} := \{w \in \bar{F} : \Phi_{k,t}(\sigma)(w) = 0\}$$

*verallgemeinerter Kreisteilungsmodul*. Der Modulcharakter von $\mathcal{C}_{k,t}$ ist $\frac{k\,t}{\nu(k)}$.

**Definition (vollständiger Erzeuger)**

$w \in \bar{F}$ heißt *vollständiger Erzeuger von* $\mathcal{C}_{k,t}$, falls $w$ ein Erzeuger von $\mathcal{C}_{k,t}$ als $\mathbb{F}_{q^d}[x]$-Modul für alle Teiler $d$ des Modulcharakters ist.

# Problem

Bei Erzeugern gilt: Ist $\Delta$ eine Zerlegung von $x^n - 1$ und hat man für jedes $\delta \in \Delta$ ein $w_\delta \in E$ mit $\mathrm{Ord}_q(w_\delta) = \delta(x)$, so ist $w = \sum_{\delta \in \Delta} w_\delta$ ein Erzeuger von $V_{x^n - 1}$ und $\mathrm{Ord}_q(w) = x^n - 1$.

# Problem

Bei Erzeugern gilt: Ist $\Delta$ eine Zerlegung von $x^n - 1$ und hat man für jedes $\delta \in \Delta$ ein $w_\delta \in E$ mit $\mathrm{Ord}_q(w_\delta) = \delta(x)$, so ist $w = \sum_{\delta \in \Delta} w_\delta$ ein Erzeuger von $V_{x^n - 1}$ und $\mathrm{Ord}_q(w) = x^n - 1$.

Achtung: Dies gilt bei vollständigen Erzeugern im Allgemeinen nicht mehr und muss gefordert werden.

# Problem

Bei Erzeugern gilt: Ist $\Delta$ eine Zerlegung von $x^n - 1$ und hat man für jedes $\delta \in \Delta$ ein $w_\delta \in E$ mit $\mathrm{Ord}_q(w_\delta) = \delta(x)$, so ist $w = \sum_{\delta \in \Delta} w_\delta$ ein Erzeuger von $V_{x^n-1}$ und $\mathrm{Ord}_q(w) = x^n - 1$.

Achtung: Dies gilt bei vollständigen Erzeugern im Allgemeinen nicht mehr und muss gefordert werden.

## Definition (verträgliche Zerlegung)

Sei $\Delta$ eine Zerlegung von $\Phi_{k,t}$ in verallgemeinerte Kreisteilungspolynome über $\mathbb{F}_q$. Dann heißt $\Delta$ *verträgliche Zerlegung*, falls gilt: Für jedes $\Phi_{l,s} \in \Delta$ sei $w_{l,s} \in \bar{\mathbb{F}}_q$ ein vollständiger Erzeuger von $\mathcal{C}_{l,s}$ über $\mathbb{F}_q$, so ist

$$w = \sum_{\Phi_{l,s} \in \Delta} w_{l,s}$$

ein vollständiger Erzeuger von $\mathcal{C}_{k,t}$ über $\mathbb{F}_q$.

# Zerlegungssatz für verallgemeinerte Kreisteilungsmoduln

## Satz (Hachenberger 1997)

Sei $\Phi_{k,t}$ ein verallgemeinertes Kreisteilungspolynom über einem endlichen Körper $\mathbb{F}_q$ mit Charakteristik $p$. Sei $r$ eine Primzahl mit

- $r \mid t$,
- $r \neq p$,
- $r \nmid k$.

Dann ist

$$\Delta_r \ := \ \{\Phi_{k,\frac{t}{r}},\ \Phi_{kr,\frac{t}{r}}\}$$

eine Zerlegung von $\Phi_{k,t}$ in verallgemeinerte Kreisteilungspolynome und diese ist verträglich genau dann, wenn

$$r^a \nmid \mathrm{ord}_{\nu(kt')}(q)$$

mit $a = \max\{b \in \mathbb{N} : r^b \mid t\}$ und $t = t'p^b$ für $\mathrm{ggT}(t', p) = 1$.

# Reguläre Kreisteilungsmoduln

## Definition (regulär)

Ein verallgemeinerter Kreisteilungsmodul $\mathcal{C}_{k,t}$ mit $\mathrm{ggT}(k,t) = 1$ heißt *regulär* über einem endlichen Körper $\mathbb{F}_q$ der Charakteristik $p$, falls $\mathrm{ord}_{\nu(k\,t')}(q)$ und $k\,t$ teilerfremd sind für $t = t'p^b$ mit $\mathrm{ggT}(t', p) = 1$.
Eine Körpererweiterung $\mathbb{F}_{q^m} \mid \mathbb{F}_q$ heißt *regulär*, falls $\mathcal{C}_{1,m}$ regulär ist.

# Reguläre Kreisteilungsmoduln

## Definition (regulär)

Ein verallgemeinerter Kreisteilungsmodul $\mathcal{C}_{k,t}$ mit $\mathrm{ggT}(k,t) = 1$ heißt *regulär* über einem endlichen Körper $\mathbb{F}_q$ der Charakteristik $p$, falls $\mathrm{ord}_{\nu(k\,t')}(q)$ und $k\,t$ teilerfremd sind für $t = t'p^b$ mit $\mathrm{ggT}(t',p) = 1$.
Eine Körpererweiterung $\mathbb{F}_{q^m} \mid \mathbb{F}_q$ heißt *regulär*, falls $\mathcal{C}_{1,m}$ regulär ist.

## Satz (Hachenberger 1997)

Sei $\mathbb{F}_q$ ein endlicher Körper von Charakteristik $p$. Seien $k$ eine positive ganze Zahl teilerfremd zu $q$ und $\mathcal{C}_{k,p^b}$ ein regulärer verallgemeinerter Kreisteilungsmodul. Dann gilt:

1. Ist $\mathcal{C}_{k,p^b}$ nicht ausfallend, so ist $u \in \overline{\mathbb{F}}_q$ genau dann ein vollständiger Erzeuger von $\mathcal{C}_{k,p^b}$, falls
$$\mathrm{Ord}_{q^\tau}(u) = \Phi_{\frac{k}{\tau},\,p^b}\,.$$
2. Ist $\mathcal{C}_{k,p^b}$ ausfallend, so ist $u \in \overline{\mathbb{F}}_q$ genau dann ein vollständiger Erzeuger von $\mathcal{C}_{k,p^b}$, falls
$$\mathrm{Ord}_{q^\tau}(u) = \Phi_{\frac{k}{\tau},\,p^b} \quad \text{und} \quad \mathrm{Ord}_{q^{2\tau}}(u) = \Phi_{\frac{k}{2\tau},\,p^b}\,.$$

# Reguläre Kreisteilungsmoduln

## Definition (regulär)

Ein verallgemeinerter Kreisteilungsmodul $\mathcal{C}_{k,t}$ mit $\mathrm{ggT}(k,t) = 1$ heißt *regulär* über einem endlichen Körper $\mathbb{F}_q$ der Charakteristik $p$, falls $\mathrm{ord}_{\nu(k\,t')}(q)$ und $k\,t$ teilerfremd sind für $t = t'p^b$ mit $\mathrm{ggT}(t',p) = 1$.
Eine Körpererweiterung $\mathbb{F}_{q^m} \mid \mathbb{F}_q$ heißt *regulär*, falls $\mathcal{C}_{1,m}$ regulär ist.

## Satz (Hachenberger 1997)

Sei $\mathbb{F}_q$ ein endlicher Körper von Charakteristik $p$. Seien $k$ eine positive ganze Zahl teilerfremd zu $q$ und $\mathcal{C}_{k,p^b}$ ein regulärer verallgemeinerter Kreisteilungsmodul. Dann gilt:

1. Ist $\mathcal{C}_{k,p^b}$ nicht ausfallend, so ist $u \in \overline{\mathbb{F}}_q$ genau dann ein vollständiger Erzeuger von $\mathcal{C}_{k,p^b}$, falls
$$\mathrm{Ord}_{q^\tau}(u) = \Phi_{\frac{k}{\tau},\,p^b}\,.$$
2. Ist $\mathcal{C}_{k,p^b}$ ausfallend, so ist $u \in \overline{\mathbb{F}}_q$ genau dann ein vollständiger Erzeuger von $\mathcal{C}_{k,p^b}$, falls
$$\mathrm{Ord}_{q^\tau}(u) = \Phi_{\frac{k}{\tau},\,p^b} \quad \text{und} \quad \mathrm{Ord}_{q^{2\tau}}(u) = \Phi_{\frac{k}{2\tau},\,p^b}\,.$$

# 4 Existenz und Enumeration primitiv vollständig normaler Elemente

# Notationen

## Definition

$$\mathcal{N}(q,n) \;:=\; \left|\{u \in \mathbb{F}_{q^n} :\; u \text{ ist normal über } \mathbb{F}_q\}\right|,$$

# Notationen

## Definition

$$\begin{aligned} \mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\ \mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \end{aligned}$$

# Notationen

## Definition

$$\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|,
\end{aligned}$$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|,
\end{aligned}
$$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist normal über } \mathbb{F}_q\}\right|,\\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 :\ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}
$$

# Notationen

## Definition

$$\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist normal über } \mathbb{F}_q\}\right|,\\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 :\ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}$$

## Problemstellungen

$\mathcal{N}(q,n) > 0?$ $\mathcal{CN}(q,n) > 0?$ $\mathcal{PN}(q,n) > 0?$ $\mathcal{PCN}(q,n) > 0?$

$\mathcal{N}(q,n) = ?$ $\mathcal{CN}(q,n) = ?$ $\mathcal{PN}(q,n) = ?$ $\mathcal{PCN}(q,n) = ?$

# Notationen

## Definition

$$\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 :\ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}$$

## Problemstellungen

$\mathcal{N}(q,n) > 0?$ ✓ Satz von der Normalbasis

$\mathcal{CN}(q,n) > 0?$ $\mathcal{PN}(q,n) > 0?$ $\mathcal{PCN}(q,n) > 0?$

$\mathcal{N}(q,n) =?$ $\mathcal{CN}(q,n) =?$ $\mathcal{PN}(q,n) =?$ $\mathcal{PCN}(q,n) =?$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|,\\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}
$$

## Problemstellungen

$\mathcal{N}(q,n) > 0?$ ✓ Satz von der Normalbasis

$\mathcal{CN}(q,n) > 0?$

$\mathcal{PN}(q,n) > 0?$

$\mathcal{PCN}(q,n) > 0?$

$\mathcal{N}(q,n) = ?$ ✓ $\mathcal{N}(q,n) = \phi_q(x^n - 1)$

$\mathcal{CN}(q,n) = ?$

$\mathcal{PN}(q,n) = ?$

$\mathcal{PCN}(q,n) = ?$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}
$$

## Problemstellungen

$\mathcal{N}(q,n) > 0?$ ✓
Satz von der Normalbasis

$\mathcal{CN}(q,n) > 0?$ ✓
Verschärfung des Satzes von der Normalbasis
(Blessenohl und Johnsen 1986)

$\mathcal{PN}(q,n) > 0?$

$\mathcal{PCN}(q,n) > 0?$

$\mathcal{N}(q,n) = ?$ ✓
$\mathcal{N}(q,n) = \phi_q(x^n - 1)$

$\mathcal{CN}(q,n) = ?$

$\mathcal{PN}(q,n) = ?$

$\mathcal{PCN}(q,n) = ?$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|,\\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}
$$

## Problemstellungen

$\mathcal{N}(q,n) > 0$? ✓
Satz von der Normalbasis

$\mathcal{CN}(q,n) > 0$? ✓
Verschärfung des Satzes von der Normalbasis
(Blessenohl und Johnsen 1986)

$\mathcal{PN}(q,n) > 0$? ✓
Satz von der primitiven Normalbasis
(Lenstra, Jr. und Schoof 1987)

$\mathcal{PCN}(q,n) > 0$?

$\mathcal{N}(q,n) = ?$ ✓
$\mathcal{N}(q,n) = \phi_q(x^n - 1)$

$\mathcal{CN}(q,n) = ?$

$\mathcal{PN}(q,n) = ?$

$\mathcal{PCN}(q,n) = ?$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist normal über } \mathbb{F}_q\}\right|,\\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|,\\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} :\ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|,\\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 :\ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}
$$

## Problemstellungen

$\mathcal{N}(q,n) > 0$?
Satz von der Normalbasis

$\mathcal{CN}(q,n) > 0$?
Verschärfung des Satzes von der Normalbasis
(Blessenohl und Johnsen 1986)

$\mathcal{PN}(q,n) > 0$?
Satz von der primitiven Normalbasis
(Lenstra, Jr. und Schoof 1987)

$\mathcal{PCN}(q,n) > 0$?

$\mathcal{N}(q,n) = ?$
$\mathcal{N}(q,n) = \phi_q(x^n - 1)$

$\mathcal{CN}(q,n) = ?$
nur bekannt, falls regulär

$\mathcal{PN}(q,n) = ?$

$\mathcal{PCN}(q,n) = ?$

# Notationen

## Definition

$$
\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}
$$

## Problemstellungen

| | | | |
|---|---|---|---|
| $\mathcal{N}(q,n) > 0?$ ✓<br>Satz von der Normalbasis | $\mathcal{CN}(q,n) > 0?$ ✓<br>Verschärfung des Satzes von der Normalbasis<br>(Blessenohl und Johnsen 1986) | $\mathcal{PN}(q,n) > 0?$ ✓<br>Satz von der primitiven Normalbasis<br>(Lenstra, Jr. und Schoof 1987) | $\mathcal{PCN}(q,n) > 0?$ |
| $\mathcal{N}(q,n) = ?$ ✓<br>$\mathcal{N}(q,n) = \phi_q(x^n - 1)$ | $\mathcal{CN}(q,n) = ?$<br>nur bekannt, falls regulär | $\mathcal{PN}(q,n) = ?$ | $\mathcal{PCN}(q,n) = ?$ |

# Notationen

## Definition

$$\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}$$

## Problemstellungen

| | | | |
|---|---|---|---|
| $\mathcal{N}(q,n) > 0?$<br>Satz von der Normalbasis | $\mathcal{CN}(q,n) > 0?$<br>Verschärfung des Satzes von der Normalbasis<br>(Blessenohl und Johnsen 1986) | $\mathcal{PN}(q,n) > 0?$<br>Satz von der primitiven Normalbasis<br>(Lenstra, Jr. und Schoof 1987) | $\mathcal{PCN}(q,n) > 0?$ |
| $\mathcal{N}(q,n) = ?$<br>$\mathcal{N}(q,n) = \phi_q(x^n-1)$ | $\mathcal{CN}(q,n) = ?$<br>nur bekannt, falls regulär | $\mathcal{PN}(q,n) = ?$ | $\mathcal{PCN}(q,n) = ?$<br>nur Abschätzungen und Einzelfälle |

# Notationen

## Definition

$$\begin{aligned}
\mathcal{N}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist normal über } \mathbb{F}_q\}\right|, \\
\mathcal{CN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und normal über } \mathbb{F}_q\}\right|, \\
\mathcal{PCN}(q,n) &:= \left|\{u \in \mathbb{F}_{q^n} : \ u \text{ ist primitiv und vollständig normal über } \mathbb{F}_q\}\right|, \\
\mathcal{G} &:= \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}.
\end{aligned}$$

## Problemstellungen

| | | | |
|---|---|---|---|
| ✓ $\mathcal{N}(q,n) > 0$? | ✓ $\mathcal{CN}(q,n) > 0$? | ✓ $\mathcal{PN}(q,n) > 0$? | $\mathcal{PCN}(q,n) > 0$? |
| Satz von der Normalbasis | Verschärfung des Satzes von der Normalbasis (Blessenohl und Johnsen 1986) | Satz von der primitiven Normalbasis (Lenstra, Jr. und Schoof 1987) | s. nächste Folie |
| ✓ $\mathcal{N}(q,n) =$? | $\mathcal{CN}(q,n) =$? | $\mathcal{PN}(q,n) =$? | $\mathcal{PCN}(q,n) =$? |
| $\mathcal{N}(q,n) = \phi_q(x^n - 1)$ | nur bekannt, falls regulär | | nur Abschätzungen und Einzelfälle |

## Stand der Forschung und Ziele

**Satz (Hachenberger 2001 und 2014)**

Seien $q$ eine Primzahlpotenz und $n \in \mathbb{N}^*$, so dass $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ eine reguläre Erweiterung ist. Dann existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

## Stand der Forschung und Ziele

**Satz (Hachenberger 2001 und 2014)**

Seien $q$ eine Primzahlpotenz und $n \in \mathbb{N}^*$, so dass $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ eine reguläre Erweiterung ist. Dann existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

**Satz (Hachenberger 2014)**

Sei $n \in \mathbb{N}^*$ mit $n \geq 2$. Dann gilt: Für Primzahlpotenzen $q$ mit $q \geq n^4$ existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

## Stand der Forschung und Ziele

**Satz (Hachenberger 2001 und 2014)**

Seien $q$ eine Primzahlpotenz und $n \in \mathbb{N}^*$, so dass $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ eine reguläre Erweiterung ist. Dann existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

**Satz (Hachenberger 2014)**

Sei $n \in \mathbb{N}^*$ mit $n \geq 2$. Dann gilt: Für Primzahlpotenzen $q$ mit $q \geq n^4$ existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

Ziele:

1. Bestimme $\mathcal{CN}(q,n)$ und $\mathcal{PCN}(q,n)$ für möglichst viele Paare $(q,n)$.

## Stand der Forschung und Ziele

**Satz (Hachenberger 2001 und 2014)**

Seien $q$ eine Primzahlpotenz und $n \in \mathbb{N}^*$, so dass $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ eine reguläre Erweiterung ist. Dann existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

**Satz (Hachenberger 2014)**

Sei $n \in \mathbb{N}^*$ mit $n \geq 2$. Dann gilt: Für Primzahlpotenzen $q$ mit $q \geq n^4$ existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

**Ziele:**

1. Bestimme $\mathcal{CN}(q,n)$ und $\mathcal{PCN}(q,n)$ für möglichst viele Paare $(q,n)$.
2. Versuche $\mathcal{G}$ möglichst groß werden zu lassen, d.h. finde für möglichst viele $n$ für alle $q < n^4$ ein $\mathcal{PCN}$-Element in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$.

## Stand der Forschung und Ziele

### Satz (Hachenberger 2001 und 2014)

Seien $q$ eine Primzahlpotenz und $n \in \mathbb{N}^*$, so dass $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$ eine reguläre Erweiterung ist. Dann existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

### Satz (Hachenberger 2014)

Sei $n \in \mathbb{N}^*$ mit $n \geq 2$. Dann gilt: Für Primzahlpotenzen $q$ mit $q \geq n^4$ existiert ein primitives Element in $\mathbb{F}_{q^n}$, das vollständig normal über $\mathbb{F}_q$ ist.

Ziele:

1. Bestimme $\mathcal{CN}(q,n)$ und $\mathcal{PCN}(q,n)$ für möglichst viele Paare $(q,n)$.
2. Versuche $\mathcal{G}$ möglichst groß werden zu lassen, d.h. finde für möglichst viele $n$ für alle $q < n^4$ ein $\mathcal{PCN}$-Element in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$.

$\mathcal{G} := \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}$

# 5 Implementierung endlicher Körper und Körpererweiterungen

Sei $F := \mathbb{F}_q$ ein endlicher Körper mit $q = p^r$ und $E := \mathbb{F}_{q^n}$ eine Erweiterung von Grad $n$.

Sei $F := \mathbb{F}_q$ ein endlicher Körper mit $q = p^r$ und $E := \mathbb{F}_{q^n}$ eine Erweiterung von Grad $n$.

Beschreibung von Elementen endlicher Körper

Sei $F := \mathbb{F}_q$ ein endlicher Körper mit $q = p^r$ und $E := \mathbb{F}_{q^n}$ eine Erweiterung von Grad $n$.

## Beschreibung von Elementen endlicher Körper

- Ist $q = p$, so nutze
$$F \;\cong\; \mathbb{Z}_p \;=\; \{0, 1, \ldots, p-1\} \bmod p\,.$$

Sei $F := \mathbb{F}_q$ ein endlicher Körper mit $q = p^r$ und $E := \mathbb{F}_{q^n}$ eine Erweiterung von Grad $n$.

### Beschreibung von Elementen endlicher Körper

- Ist $q = p$, so nutze
$$F \cong \mathbb{Z}_p = \{0, 1, \ldots, p-1\} \bmod p\,.$$
- Sonst nutze
$$F \cong \mathbb{F}_p[a]/(f(a))$$
für $f(a) \in \mathbb{F}_p[a]$ irreduzibel, normiert von Grad $n$.

Sei $F := \mathbb{F}_q$ ein endlicher Körper mit $q = p^r$ und $E := \mathbb{F}_{q^n}$ eine Erweiterung von Grad $n$.

## Beschreibung von Elementen endlicher Körper

- Ist $q = p$, so nutze
$$F \;\cong\; \mathbb{Z}_p \;=\; \{0, 1, \dots, p-1\} \bmod p\,.$$
- Sonst nutze
$$F \;\cong\; \mathbb{F}_p[a]\big/(f(a))$$
für $f(a) \in \mathbb{F}_p[a]$ irreduzibel, normiert von Grad $n$.

### Beispiel

$$a^8 + 2a^6 + a^2 + 2 \quad \in \quad \mathbb{F}_{3^{10}} = \mathbb{F}_3[a]\big/(a^{10} + 2a^6 + 2a^5 + 2a^4 + a + 2)$$

Idee: Nutze das Computeralgebrasystem Sage.

Idee: Nutze das Computeralgebrasystem Sage.

Beispiel

```
F = GF(3^10,'a')
  #F.modulus() == x^10 + 2*x^6 + 2*x^5 + 2*x^4 + x + 2
```

Idee: Nutze das Computeralgebrasystem Sage.

**Beispiel**

```
F = GF(3^10,'a')
  #F.modulus() == x^10 + 2*x^6 + 2*x^5 + 2*x^4 + x + 2
w = F('a^8+2a^6+a^2+2')
w + w; 2*w; w*w
```

Idee: Nutze das Computeralgebrasystem Sage.

Beispiel

```
F = GF(3^10,'a')
  #F.modulus() == x^10 + 2*x^6 + 2*x^5 + 2*x^4 + x + 2
w = F('a^8+2a^6+a^2+2')
w + w; 2*w; w*w
```

Problem: Sage ist zu langsam!

Idee: Nutze das Computeralgebrasystem Sage.

Beispiel

```
F = GF(3^10,'a')
  #F.modulus() == x^10 + 2*x^6 + 2*x^5 + 2*x^4 + x + 2
w = F('a^8+2a^6+a^2+2')
w + w; 2*w; w*w
```

Problem: Sage ist zu langsam!

Lösung: Eigenes Library in C für grundlegende Arithmetik erstellen und Sage für übergeordnete Aufgaben (Faktorisierung von Polynomen, Zerlegungssatz,. . . ) nutzen.

## Grundlegende Arithmetik in Primkörpern

Idee: Nutze die `C`-Funktion `%`.
D.h. sind $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, so addiere bzw. multipliziere durch `(a+b) % p` und `(a*b) % p`.

## Grundlegende Arithmetik in Primkörpern

Idee: Nutze die `C`-Funktion `%`.
D.h. sind $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, so addiere bzw. multipliziere durch `(a+b) % p` und `(a*b) % p`.

Problem: Zu langsam!

## Grundlegende Arithmetik in Primkörpern

Idee: Nutze die `C`-Funktion `%`.
D.h. sind $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, so addiere bzw. multipliziere durch `(a+b) % p` und `(a*b) % p`.

Problem: Zu langsam!

Gute Idee: Nutze Additions- und Multiplikationstabellen, d.h. `int`-Arrays, sodass die `(a+b)`-te Stelle der Additions- und die `(a*b)`-te Stelle der Multiplikationstabelle gerade das Ergebnis ist.

# Grundlegende Arithmetik in Primkörpern

Idee: Nutze die C-Funktion %.
D.h. sind $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, so addiere bzw. multipliziere durch `(a+b) % p` und `(a*b) % p`.

Problem: Zu langsam!

Gute Idee: Nutze Additions- und Multiplikationstabellen, d.h. `int`-Arrays, sodass die `(a+b)`-te Stelle der Additions- und die `(a*b)`-te Stelle der Multiplikationstabelle gerade das Ergebnis ist.

### Beispiel

Arithmetik in $\mathbb{F}_3$:

```
addTable[ 2+1 ]
        // == 0
addTable[ 0-2 ]
        // == 1
multTable[ 2*2 ]
        // == 1
```

# Grundlegende Arithmetik in Primkörpern

Idee: Nutze die C-Funktion `%`.
D.h. sind $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, so addiere bzw. multipliziere durch `(a+b) % p` und `(a*b) % p`.

Problem: Zu langsam!

Gute Idee: Nutze Additions- und Multiplikationstabellen, d.h. `int`-Arrays, sodass die `(a+b)`-te Stelle der Additions- und die `(a*b)`-te Stelle der Multiplikationstabelle gerade das Ergebnis ist.

### Beispiel

Arithmetik in $\mathbb{F}_3$:

```
int addTableRaw[] = {2, 0, 1, 2, 0, 1, 2, 0, 1};
int initialAddShift = 4;
int *addTable = addTableRaw+initialAddShift;
int multTableRaw[] = {2, 0, 1, 2, 0, 1, 2, 0, 1};
int initialMultShift = 4;
int *multTable = multTableRaw+initialMultShift;
```

```
addTable[ 2+1 ]
            // == 0
addTable[ 0-2 ]
            // == 1
multTable[ 2*2 ]
            // == 1
```

# Grundlegende Arithmetik in Primkörpern

Idee: Nutze die C-Funktion `%`.
D.h. sind $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, so addiere bzw. multipliziere durch `(a+b) % p` und `(a*b) % p`.

Problem: Zu langsam!

Gute Idee: Nutze Additions- und Multiplikationstabellen, d.h. `int`-Arrays, sodass die `(a+b)`-te Stelle der Additions- und die `(a*b)`-te Stelle der Multiplikationstabelle gerade das Ergebnis ist.

## Beispiel

Länge: $2 \cdot 2(p-1) + 1$

Arithmetik in $\mathbb{F}_3$:

```
int addTableRaw[] = {2, 0, 1, 2, 0, 1, 2, 0, 1};
int initialAddShift = 4;
int *addTable = addTableRaw+initialAddShift;
int multTableRaw[] = {2, 0, 1, 2, 0, 1, 2, 0, 1};
int initialMultShift = 4;
int *multTable = multTableRaw+initialMultShift;
```

Länge: $2 \cdot (p-1)^2 + 1$

```
addTable[ 2+1 ]
            // == 0
addTable[ 0-2 ]
            // == 1
multTable[ 2*2 ]
            // == 1
```

## Elemente endlicher Körper in `C`

Ziel: Schnelle Arithmetik durch `int`-Arrays

# Elemente endlicher Körper in C

Ziel: Schnelle Arithmetik durch int-Arrays

## Elemente endlicher Körper

```
struct FFElem{
    int *el;
    int *idcs;
    int len;
};
```

# Elemente endlicher Körper in C

Ziel: Schnelle Arithmetik durch `int`-Arrays

## Elemente endlicher Körper

```
struct FFElem{
    int *el;
    int *idcs;
    int len;
};
```

## Beispiel

$$\hat{=} \quad w := a^8 + 2a^6 + a^2 + 2 \in \mathbb{F}_{3^{10}}$$

# Elemente endlicher Körper in C

Ziel: Schnelle Arithmetik durch `int`-Arrays

## Elemente endlicher Körper

```
struct FFElem{
    int *el;
    int *idcs;
    int len;
};
```

## Beispiel

```
struct FFElem *w = malloc(sizeof(struct FFElem));
```

$\hat{=}$ $w := a^8 + 2a^6 + a^2 + 2 \in \mathbb{F}_{3^{10}}$

# Elemente endlicher Körper in C

Ziel: Schnelle Arithmetik durch `int`-Arrays

## Elemente endlicher Körper

```
struct FFElem{
    int *el;
    int *idcs;
    int len;
};
```

## Beispiel

```
struct FFElem *w = malloc(sizeof(struct FFElem));
w->el = (int[]) {2, 0, 1, 0, 0, 0, 2, 0, 1, 0};
```

$\hat{=}$ $w := a^8 + 2a^6 + a^2 + 2 \in \mathbb{F}_{3^{10}}$

# Elemente endlicher Körper in C

Ziel: Schnelle Arithmetik durch int-Arrays

## Elemente endlicher Körper

```
struct FFElem{
    int *el;
    int *idcs;
    int len;
};
```

## Beispiel

```
struct FFElem *w = malloc(sizeof(struct FFElem));
w->el = (int[]) {2, 0, 1, 0, 0, 0, 2, 0, 1, 0};
w->idcs = (int[]) {8, 6, 2, 0, 0, 0, 0, 0, 0, 0};
```

$\hat{=}$ $w := a^8 + 2a^6 + a^2 + 2 \in \mathbb{F}_{3^{10}}$

# Elemente endlicher Körper in C

Ziel: Schnelle Arithmetik durch `int`-Arrays

## Elemente endlicher Körper

```
struct FFElem{
    int *el;
    int *idcs;
    int len;
};
```

## Beispiel

```
struct FFElem *w = malloc(sizeof(struct FFElem));
w->el = (int[]) {2, 0, 1, 0, 0, 0, 2, 0, 1, 0};
w->idcs = (int[]) {8, 6, 2, 0, 0, 0, 0, 0, 0, 0};
w->len = 4;
```

$\hat{=}$ $w := a^8 + 2a^6 + a^2 + 2 \in \mathbb{F}_{3^{10}}$

# Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

## Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,

# Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,

# Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,
- Quadratur,

# Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,
- Quadratur,
- Potenzieren via Square-and-Multiply,

## Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,
- Quadratur,
- Potenzieren via Square-and-Multiply,
- Polynome als `struct FFElem **poly`,

# Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,
- Quadratur,
- Potenzieren via Square-and-Multiply,
- Polynome als `struct FFElem **poly`,
- Matrizen und Matrixmultiplikation,

## Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,
- Quadratur,
- Potenzieren via Square-and-Multiply, } Intelligenter Primitivitätstest
- Polynome als `struct FFElem **poly`,
- Matrizen und Matrixmultiplikation,

# Implementierte Methoden

Implementiere auf diese Weise effizient folgende Methoden für `FFElem`s:

- Addition,
- Multiplikation,
- Quadratur,
- Potenzieren via Square-and-Multiply,
- Polynome als `struct FFElem **poly`,
- Matrizen und Matrixmultiplikation,

Intelligenter Primitivitätstest

Frobenius-Auswertung und Test auf vollständige Erzeugereigenschaft

# Ein intelligenter Primitivitätstest

**Lemma**

$$q - 1 \;=\; p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$$

die Primfaktorzerlegung von $q - 1$. Definiere für alle $i = 1, \ldots, l$

$$\bar{p}_i \;:=\; \frac{q-1}{p_i}\,.$$

Dann gilt: $u \in \mathbb{F}_q$ ist primitiv genau dann, wenn

$$u^{\bar{p}_i} \;\neq\; 1 \quad \forall\, i = 1, \ldots, l\,.$$

# Ein intelligenter Primitivitätstest

Lemma (Nutze, was schon berechnet ist!)

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $$\begin{aligned} \bar{p}_1 &= 2^3 \cdot 11^2 &&= 968\,, \\ \bar{p}_2 &= 2^3 \cdot 11 \cdot 61 &&= 5368\,, \\ \bar{p}_3 &= 2^2 \cdot 11^2 \cdot 61 &&= 29524\,. \end{aligned}$$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 \ = \ 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \operatorname{ggT}\{\bar{p}_i : \; i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\, d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 \; = \; 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \operatorname{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 \;=\; 61 \cdot 11^2 \cdot 2^3$.

- $$\begin{aligned} \bar{p}_1 &= 2^3 \cdot 11^2 &&= 968\,, \\ \bar{p}_2 &= 2^3 \cdot 11 \cdot 61 &&= 5368\,, \\ \bar{p}_3 &= 2^2 \cdot 11^2 \cdot 61 &&= 29524\,. \end{aligned}$$
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $$\begin{aligned} u^{\bar{p}_1} &= \\ u^{\bar{p}_2} &= \\ u^{\bar{p}_3} &= \end{aligned}$$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $u^{\bar{p}_1} = v^{\bar{n}_1}$,
  $u^{\bar{p}_2} =$
  $u^{\bar{p}_3} =$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \; i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 \; = \; 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 \qquad = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \;\cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $u^{\bar{p}_1} = v^{\bar{n}_1}$,
  $u^{\bar{p}_2} = w^{\bar{n}_2} \qquad := \; u_2$
  $u^{\bar{p}_3} =$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $u^{\bar{p}_1} = v^{\bar{n}_1}$,
  $u^{\bar{p}_2} = w^{\bar{n}_2} := u_2 := z_2$,
  $u^{\bar{p}_3} =$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $u^{\bar{p}_1} = v^{\bar{n}_1}$,
  $u^{\bar{p}_2} = w^{\bar{n}_2} := u_2 := z_2$,
  $u^{\bar{p}_3} = w^9 \cdot z_2$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $$\begin{aligned} \bar{p}_1 &= 2^3 \cdot 11^2 &&= 968\,, \\ \bar{p}_2 &= 2^3 \cdot 11 \cdot 61 &&= 5368\,, \\ \bar{p}_3 &= 2^2 \cdot 11^2 \cdot 61 &&= 29524\,. \end{aligned}$$
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $$\begin{aligned} u^{\bar{p}_1} &= v^{\bar{n}_1}\,, \\ u^{\bar{p}_2} &= w^{\bar{n}_2} &&:= u_2 &&:= z_2\,, \\ u^{\bar{p}_3} &= w^9 \cdot z_2 &&:= u_3 \cdot z_2 &&:= z_3\,. \end{aligned}$$

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d, \quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}, \quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,
- $u_2 := w^{\bar{n}_2}$ und $u_i := w^{\bar{n}_i - \bar{n}_{i-1}}$ für $i = 3, \ldots, l$.
- $z_i := \prod_{j=2}^{i} u_j$ für $i = 2, \ldots, l$.

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 \ = \ 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}, \quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2, \quad \bar{n}_2 := 2, \quad \bar{n}_3 := 11$
- $u^{\bar{p}_1} = v^{\bar{n}_1}$,
  $u^{\bar{p}_2} = w^{\bar{n}_2} := u_2 := z_2$,
  $u^{\bar{p}_3} = w^9 \cdot z_2 := u_3 \cdot z_2 := z_3$.

# Ein intelligenter Primitivitätstest

## Lemma (Nutze, was schon berechnet ist!)

Sei $q-1 = p_1^{\nu_1} \cdot \ldots \cdot p_l^{\nu_l}$ die absteigend sortierte Primfaktorzerlegung von $q-1$, d.h. $p_1 > p_2 > \ldots > p_l$. Notiere

- $\bar{p}_i := \frac{q-1}{p_i}$,
- $d := \mathrm{ggT}\{\bar{p}_i : \ i = 1, \ldots, l\}$,
  $d' := p_1$ falls $l \geq 2$ sonst $d' := 1$
- $v := u^d$, $\quad w := v^{d'}$,
- $\bar{n}_1 := \frac{\bar{p}_1}{d}$, $\quad \bar{n}_i := \frac{\bar{p}_i}{d\,d'}$ für $i = 2, \ldots, l$,
- $u_2 := w^{\bar{n}_2}$ und $u_i := w^{\bar{n}_i - \bar{n}_{i-1}}$ für $i = 3, \ldots, l$.
- $z_i := \prod_{j=2}^{i} u_j$ für $i = 2, \ldots, l$.

Es gilt: $u \in \mathbb{F}_q$ ist genau dann nicht primitiv, falls eine der nachstehenden Bedingungen erfüllt ist:

1. $v = 1$.
2. $v^{\bar{n}_1} = 1$.
3. $w = 1$.
4. $u_2 = 1$.
5. $u_i \cdot z_{i-1} = 1$ für ein $i = 3, \ldots l$.

## Beispiel

Sei $u \in \mathbb{F}_{3^{10}}$. $3^{10} - 1 = 61 \cdot 11^2 \cdot 2^3$.

- $\bar{p}_1 = 2^3 \cdot 11^2 = 968$,
  $\bar{p}_2 = 2^3 \cdot 11 \cdot 61 = 5368$,
  $\bar{p}_3 = 2^2 \cdot 11^2 \cdot 61 = 29524$.
- $d = \mathrm{ggT}\{\bar{p}_1, \bar{p}_2, \bar{p}_3\} = 2^2 \cdot 11 = 44$,
  $d' = p_1 = 61$
- $v := u^d = u^{44}$, $\quad w := v^{d'} = v^{61}$
- $\bar{n}_1 := 2$, $\quad \bar{n}_2 := 2$, $\quad \bar{n}_3 := 11$
- $u^{\bar{p}_1} = v^{\bar{n}_1}$,
  $u^{\bar{p}_2} = w^{\bar{n}_2} := u_2 := z_2$,
  $u^{\bar{p}_3} = w^9 \cdot z_2 := u_3 \cdot z_2 := z_3$.

# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$

Anwendung des Zerlegungssatzes

# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$

Anwendung des Zerlegungssatzes

# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$

Anwendung des Zerlegungssatzes → Wähle das nächste Element $u \in E$

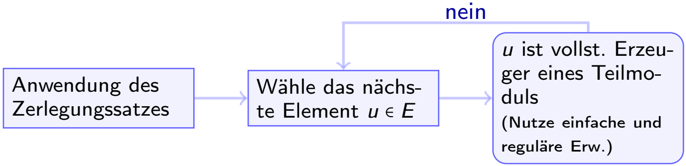
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$

Anwendung des Zerlegungssatzes → Wähle das nächste Element $u \in E$ → $u$ ist vollst. Erzeuger eines Teilmoduls (Nutze einfache und reguläre Erw.)

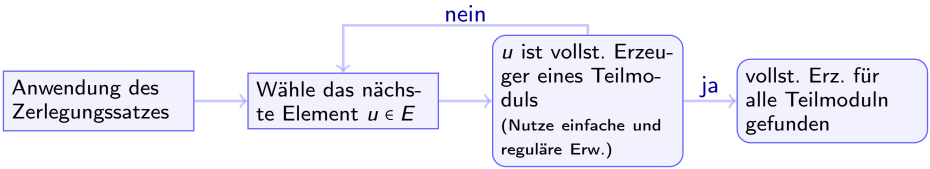
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$

Anwendung des Zerlegungssatzes → Wähle das nächste Element $u \in E$ → $u$ ist vollst. Erzeuger eines Teilmoduls (Nutze einfache und reguläre Erw.)

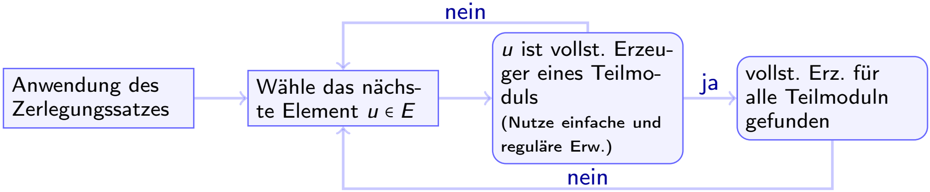
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



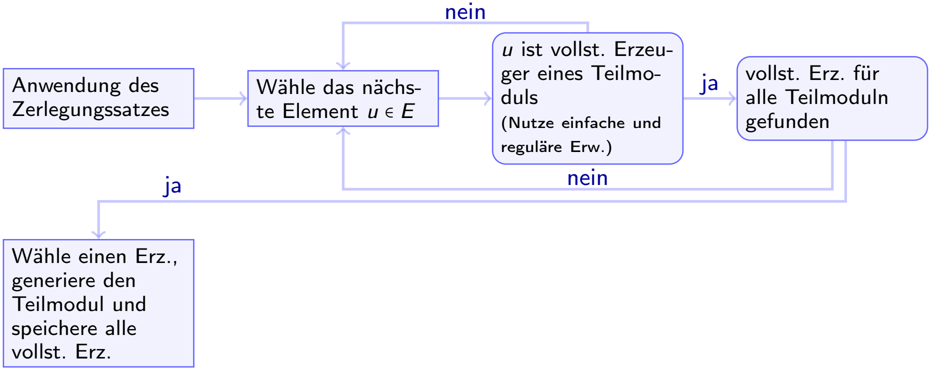
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



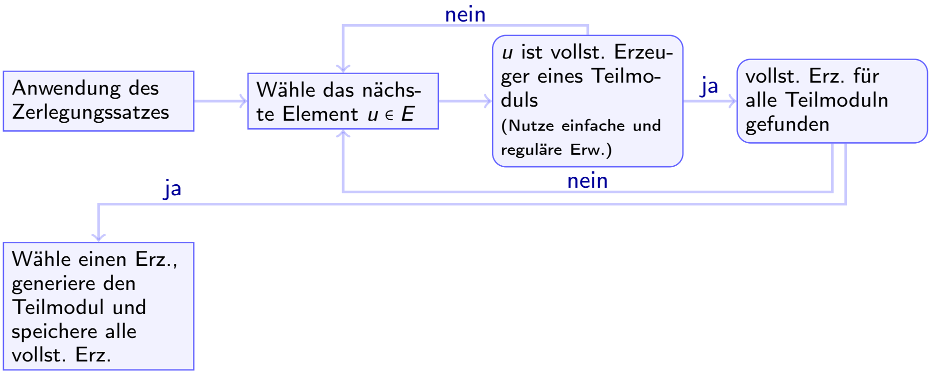
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



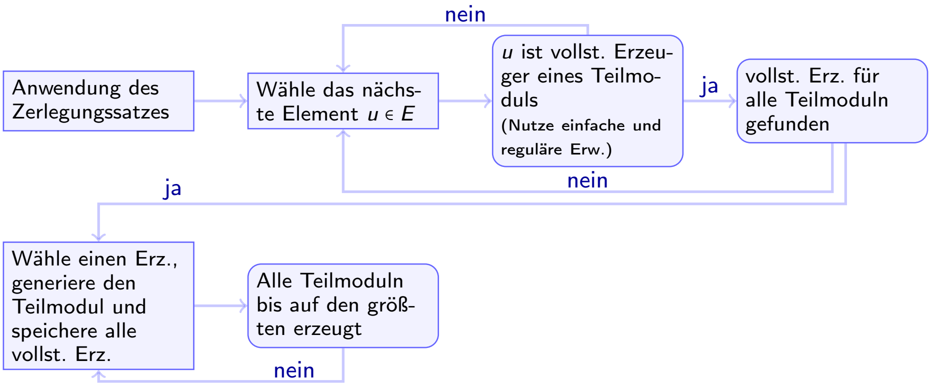
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



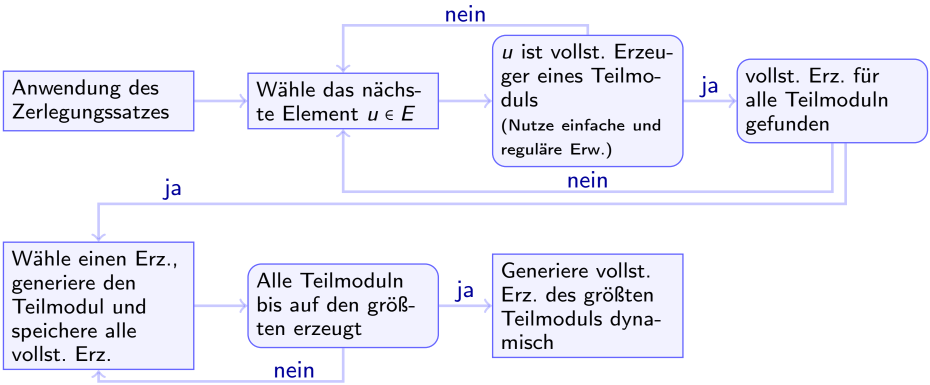
## Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



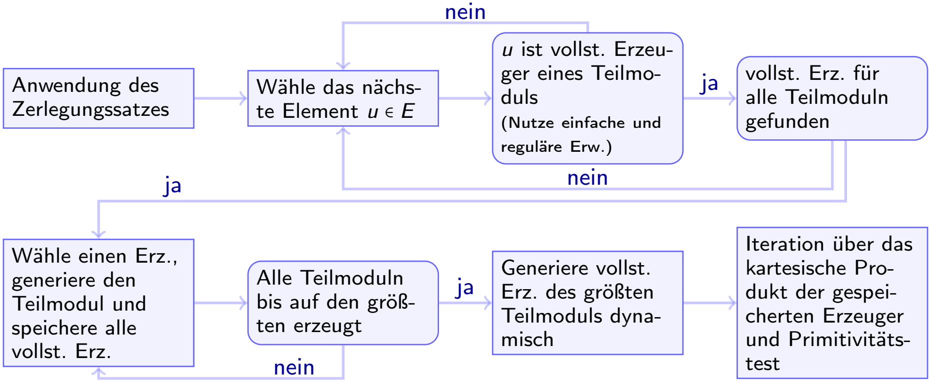
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



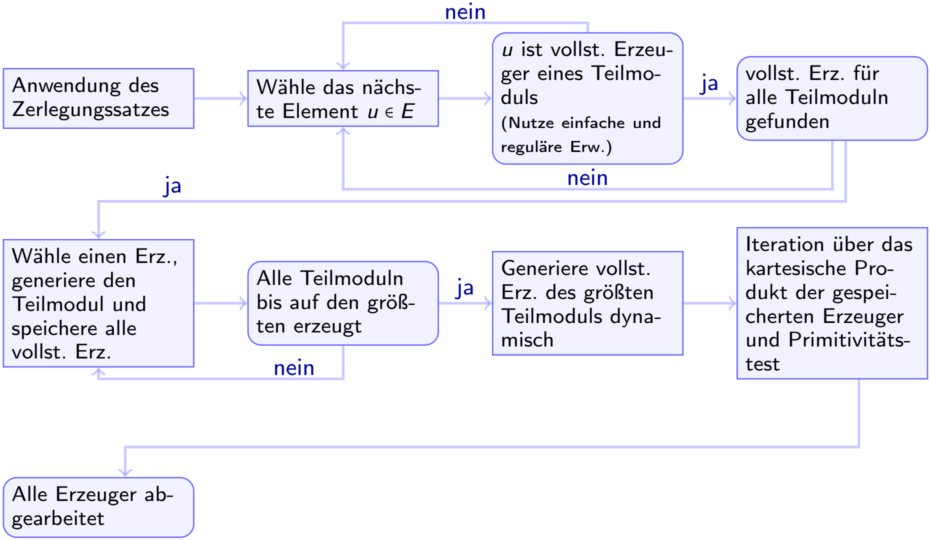
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



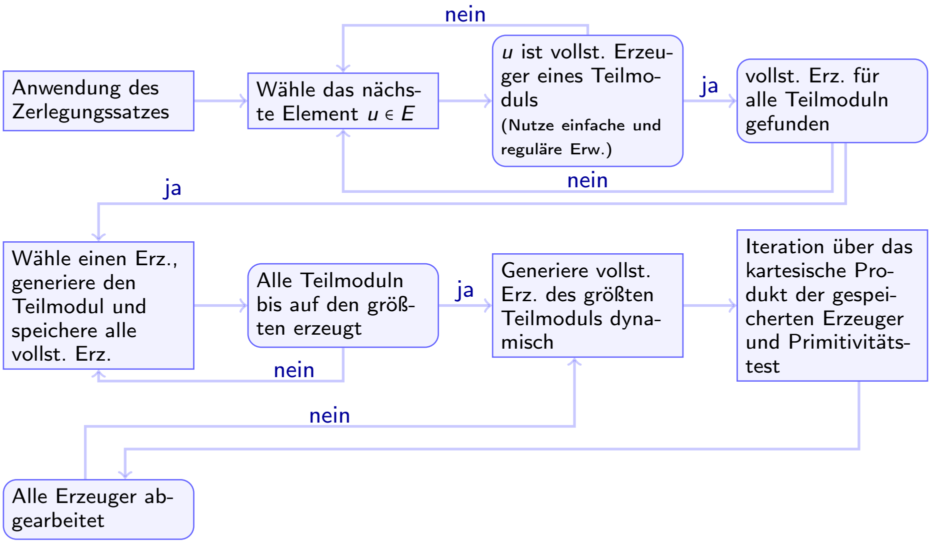
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



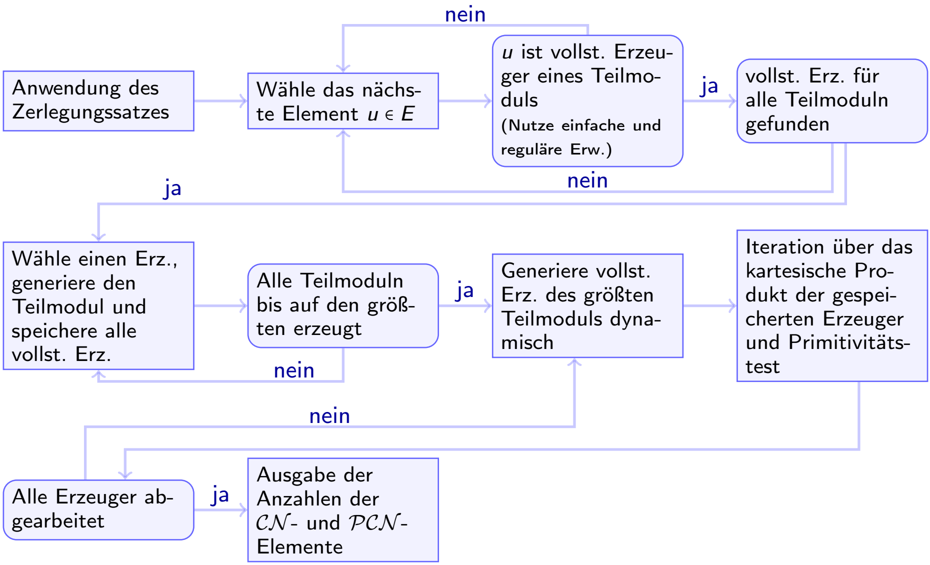
# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



# Algorithmus zur Enumeration von $\mathcal{CN}$- und $\mathcal{PCN}$-Elementen in $\mathbb{F}_{q^n}$ über $\mathbb{F}_q$



# Ergebnisse: $\mathcal{CN}(q,n)$ und $\mathcal{PCN}(q,n)$ berechnet für

Morgan und Mullan (1996),

| $q$ | $n$ |
|---|---|
| 2 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 |
| 3 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 |
| 4 | 2, 3, 4, 5, 6, 7, 8, 9 |
| 5 | 2, 3, 4, 5, 6, 7, 8 |
| 7 | 2, 3, 4, 5, 6 |
| 8 | 2, 3, 4, 5 |
| 9 | 2, 3, 4, 5 |

# Ergebnisse: $\mathcal{CN}(q,n)$ und $\mathcal{PCN}(q,n)$ berechnet für

Morgan und Mullan (1996), SH (2014)

| $q$ | $n$ |
|---|---|
| 2 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31 |
| 3 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 |
| 4 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 |
| 5 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 |
| 7 | 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 |
| 8 | 2, 3, 4, 5, 6, 7, 8, 9 |
| 9 | 2, 3, 4, 5, 6, 7, 8, 9 |
| 11 | 2, 3, 4, 5, 6, 7 |
| 13 | 2, 3, 4, 5, 6, 7 |
| 16 | 2, 3, 4, 5, 6, 7 |
| 17 | 2, 3, 4, 5, 6, 7 |
| 19 | 2, 3, 4, 5, 6, 7 |
| 25 | 2, 3, 4, 5, 6 |
| 27 | 2, 3, 4 |
| 27 | 2, 3, 4, 5, 6, 7 |
| 31 | 2, 3, 4, 5, 6 |
| 31 | 2, 3, 4 |
| 37 | 2, 3, 4, 5, 6 |
| 41 | 2, 3, 4, 5, 6 |
| 43 | 2, 3, 4, 5, 6 |
| 121 | 2, 3, 4 |
| 169 | 2, 3, 4 |
| 361 | 2, 3 |
| 529 | 2, 3 |
| 841 | 2, 3 |
| 961 | 2, 3 |
| 1369 | 2 |
| 1681 | 2 |
| 1849 | 2 |

| $n$ | $q$ |
|---|---|
| 3 | 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59, 61, 64, 67, 71, 73, 79, 81, 83, 89, 97, 121, 125, 128, 169, 243, 256, 289, 343, 361, 512, 529, 625, 729, 841, 961 |
| 4 | 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59, 61, 64, 67, 71, 73, 79, 81, 83, 89, 97, 121, 125, 128, 169, 243 |
| 6 | 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43 |

# 6 | Existenz von $\mathcal{PCN}$-Elementen

# Existenz von $\mathcal{PCN}$-Elementen

# Existenz von $\mathcal{PCN}$-Elementen

Wissen: $\mathcal{PCN}(q, n)$-Elemente existieren, falls

- $\mathbb{F}_{q^n}$ regulär über $\mathbb{F}_q$,
- $q \geq n^4$.

# Existenz von $\mathcal{PCN}$-Elementen

Wissen: $\mathcal{PCN}(q, n)$-Elemente existieren, falls

- $\mathbb{F}_{q^n}$ regulär über $\mathbb{F}_q$,
- $q \geq n^4$.

**Lemma**

Sei $n \in \mathbb{N}^*$ Potenz einer beliebigen Primzahl. Dann gilt: $n$ ist regulär über jeder Primzahlpotenz $q > 1$.

# Existenz von $\mathcal{PCN}$-Elementen

Wissen: $\mathcal{PCN}(q,n)$-Elemente existieren, falls

- $\mathbb{F}_{q^n}$ regulär über $\mathbb{F}_q$,
- $q \geq n^4$.

## Lemma

Sei $n \in \mathbb{N}^*$ Potenz einer beliebigen Primzahl. Dann gilt: $n$ ist regulär über jeder Primzahlpotenz $q > 1$.

## Satz

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq 33$ gilt $n \in \mathcal{G} := \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}$.

# Existenz von $\mathcal{PCN}$-Elementen

Wissen: $\mathcal{PCN}(q,n)$-Elemente existieren, falls

- $\mathbb{F}_{q^n}$ regulär über $\mathbb{F}_q$,
- $q \geq n^4$.

**Lemma**

Sei $n \in \mathbb{N}^*$ Potenz einer beliebigen Primzahl. Dann gilt: $n$ ist regulär über jeder Primzahlpotenz $q > 1$.

**Satz**

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq 33$ gilt $n \in \mathcal{G} := \{n \in \mathbb{N}^*, n \geq 2: \ \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}$.

Vorgehen: Sei $2 \leq n \leq 33$, so dass $n$ keine Primzahlpotenz ist, also

$$n \in \{6, 12, 14, 15, 18, 21, 22, 24, 26, 28, 30\}.$$

Gib dann für alle Primzahlpotenzen $q < n^4$ das „kleinste“ $\mathcal{PCN}$-Polynom an, d.h. ein Polynom von Grad $n$ über $\mathbb{F}_q$, dessen Nullstellen primitiv und vollständig normal sind.

# Existenz von $\mathcal{PCN}$-Elementen

Wissen: $\mathcal{PCN}(q,n)$-Elemente existieren, falls

- $\mathbb{F}_{q^n}$ regulär über $\mathbb{F}_q$,
- $q \geq n^4$.

## Lemma

Sei $n \in \mathbb{N}^*$ Potenz einer beliebigen Primzahl. Dann gilt: $n$ ist regulär über jeder Primzahlpotenz $q > 1$.

## Satz

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq 33$ gilt $n \in \mathcal{G} := \{n \in \mathbb{N}^*, n \geq 2 : \ \forall q$ Primzahlpotenz gilt $\mathcal{PCN}(q,n) > 0\}$.

Vorgeher: Sei $2 \leq n \leq 33$, so dass $n$ keine Primzahlpotenz ist, also

bzgl. Anzahl und Position der Koeffizienten $\neq 0$ und „Größe" der Koeffizienten

$$n \in \{6, 12, 14, 15, 18, 21, 22, 24, 26, 28, 30\}.$$

Gib dann für alle Primzahlpotenzen $q < n^4$ das „kleinste" $\mathcal{PCN}$-Polynom an, d.h. ein Polynom von Grad $n$ über $\mathbb{F}_q$, dessen Nullstellen primitiv und vollständig normal sind.

# Existenz von $\mathcal{PCN}$-Elementen

Wissen: $\mathcal{PCN}(q,n)$-Elemente existieren, falls

- $\mathbb{F}_{q^n}$ regulär über $\mathbb{F}_q$,
- $q \geq n^4$.

**Lemma**

Sei $n \in \mathbb{N}^*$ Potenz einer beliebigen Primzahl. Dann gilt: $n$ ist regulär über jeder Primzahlpotenz $q > 1$.

**Satz**

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq 33$ gilt $n \in \mathcal{G} := \{n \in \mathbb{N}^*, n \geq 2 : \forall q \text{ Primzahlpotenz gilt } \mathcal{PCN}(q,n) > 0\}$.

Vorgeben: Sei $2 \leq n \leq 33$, so dass $n$ keine Primzahlpotenz ist, also

Für $n = 30$ sind 64902 Polynome anzugeben

bzgl. Anzahl und Position der Koeffizienten $\neq 0$ und „Größe“ der Koeffizienten

$$n \in \{6, 12, 14, 15, 18, 21, 22, 24, 26, 28, 30\}.$$

Gib dann für alle Primzahlpotenzen $q < n^4$ das „kleinste“ $\mathcal{PCN}$-Polynom an, d.h. ein Polynom von Grad $n$ über $\mathbb{F}_q$, dessen Nullstellen primitiv und vollständig normal sind.

### Lemma

Sei $u \in \mathbb{F}_{q^n}$ über $\mathbb{F}_q$ ein primitiv vollständig normales Element und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{F}_q[x]$ sein Minimalpolynom. Dann gilt

1. $a_{n-1} = -\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(u) \neq 0$ und
2. $(-1)^n a_0 = \mathrm{Nm}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(u)$ ist primitiv in $\mathbb{F}_q$.

### Lemma

Sei $u \in \mathbb{F}_{q^n}$ über $\mathbb{F}_q$ ein primitiv vollständig normales Element und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{F}_q[x]$ sein Minimalpolynom. Dann gilt

1. $a_{n-1} = -\mathrm{Tr}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(u) \neq 0$ und
2. $(-1)^n a_0 = \mathrm{Nm}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(u)$ ist primitiv in $\mathbb{F}_q$.

### Folgerung

Die kleinsten $\mathcal{PCN}$-Polynome sind Trinome von der Form

$$x^n + a_{n-1}x^{n-1} + a_0 \,.$$

# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$

# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$

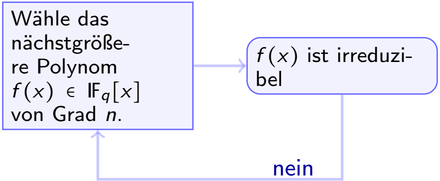
Wähle das nächstgrößere Polynom $f(x) \in \mathbb{F}_q[x]$ von Grad $n$.

# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$

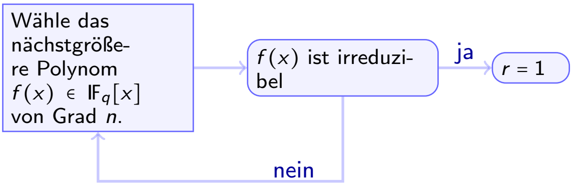
Wähle das nächstgrößere Polynom $f(x) \in \mathbb{F}_q[x]$ von Grad $n$.

→ $f(x)$ ist irreduzibel

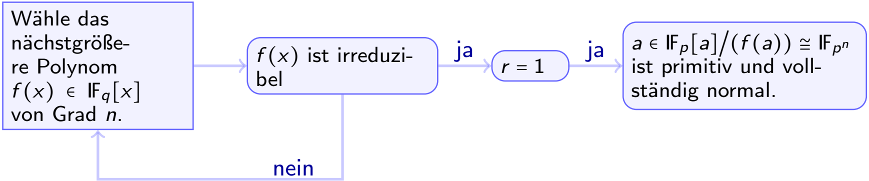
# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



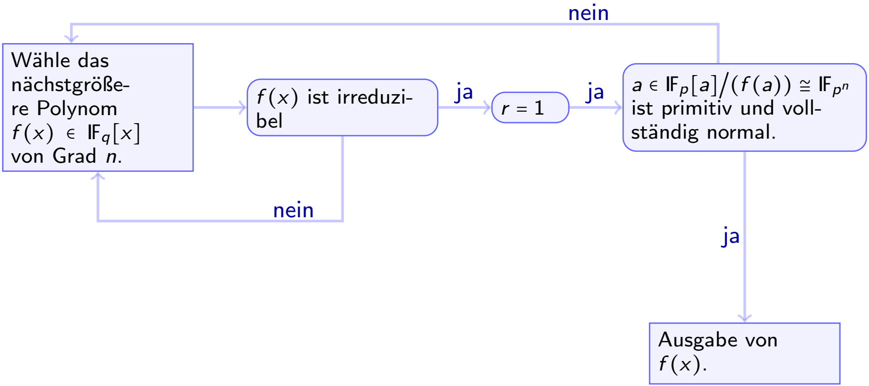
# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



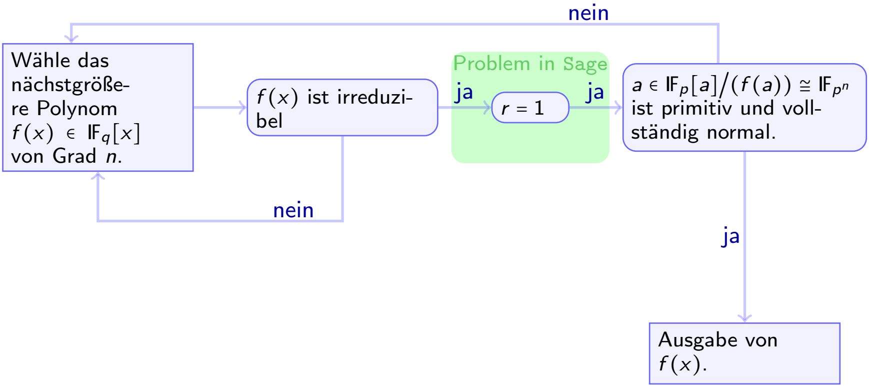
## Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



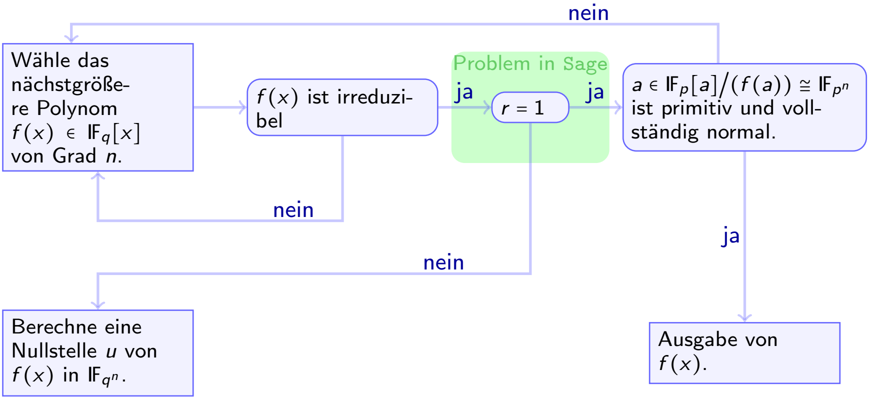
# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



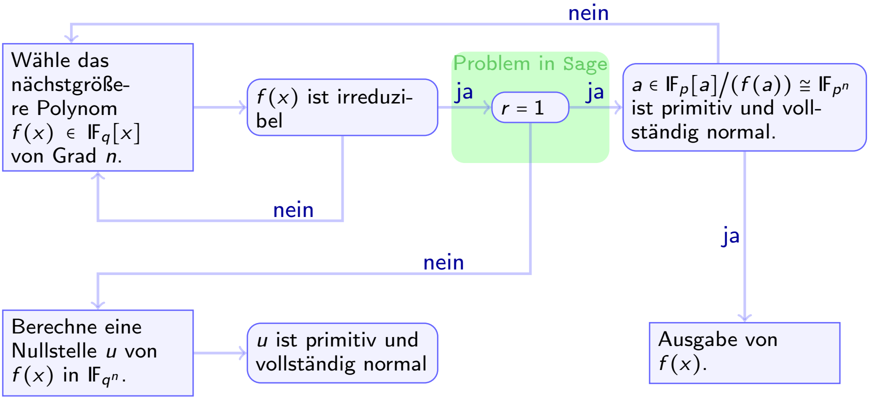
# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



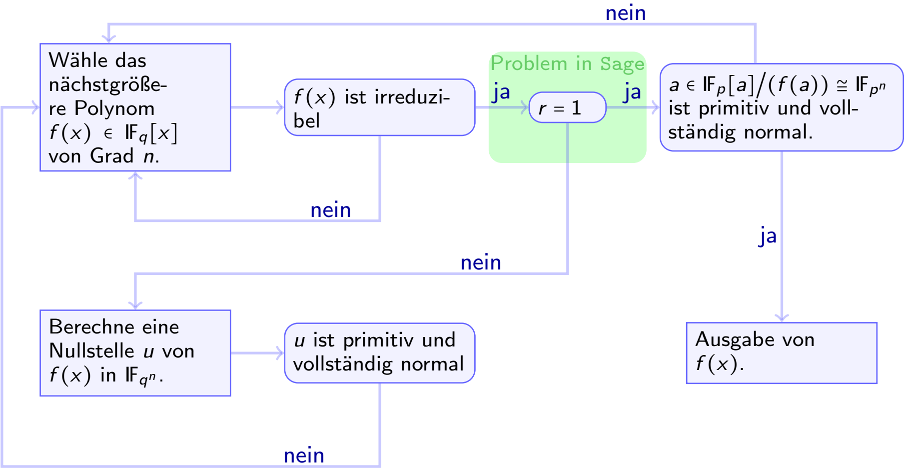
# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



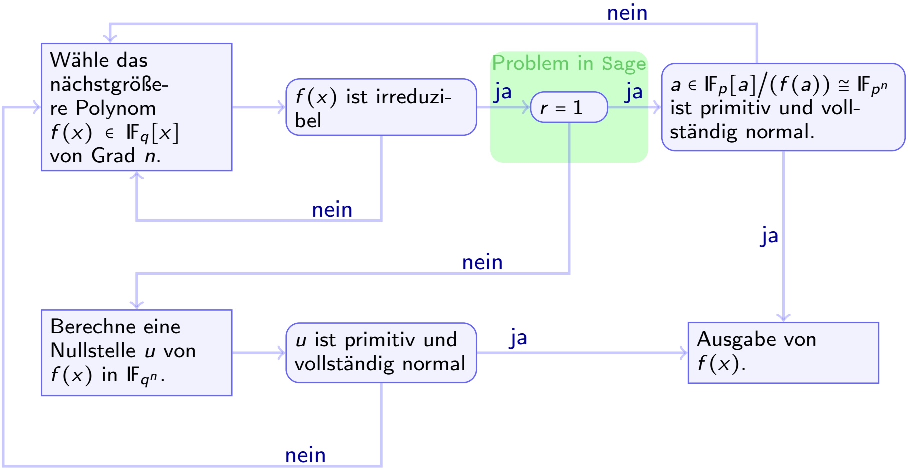
## Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



# Algorithmus zur Findung eines $\mathcal{PCN}$-Polynoms von Grad $n$ über $\mathbb{F}_q$ mit $q = p^r$



Nun bewiesen:

**Satz**

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq 33$ gilt

$$n \in \mathcal{G}\,.$$

Nun bewiesen:

**Satz** (Stand: 03.02.2015)

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq \cancel{33}\ 85$ gilt

$$n \in \mathcal{G}\,.$$

Nun bewiesen:

**Satz**

85 (Stand: 03.02.2015)

Für alle $n \in \mathbb{N}^*$ mit $2 \leq n \leq \cancel{33}$ gilt

$$n \in \mathcal{G}\,.$$

**Vermutung**

Seien $n \in \mathbb{N}^*$ und $r \in \mathbb{N}^*$ beliebig. Dann existiert ein $P_{n,r} \in \mathbb{N}^*$, so dass für alle Primzahlen $p \geq P_{n,r}$ ein primitiv vollständig normales Trinom von Grad $n$ über $\mathbb{F}_{p^r}$ existiert.

Colloquium zur Masterarbeit

# Theoretische und experimentelle Untersuchungen zu Normalbasen für Erweiterungen endlicher Körper

Stefan Hackenberg

4. Februar 2015