Bachelorarbeit

Untersuchungen zur Supersingularität von Drinfeldschen Invarianten

27. August 2009

Autorin: Sarah Detzler
Betreuer: Prof. Ernst-Ulrich Gekeler
Sommersemester 2009

Erklärung

Hiermit versichere ich, die Arbeit eigenständig und nur unter Verwendung der angegebenen Hilfsmittel durchgeführt zu haben.

Saarbrücken, den 27.08.2009

Sarah Detzler

Inhaltsverzeichnis

Vorwort

Die vorliegende Arbeit mit dem Titel „Untersuchungen zur Supersingularität von Drinfeldschen Invarianten“ zur Erlangung des Bachelorabschlusses in Mathematik ist in der Zeit vom 1. Juni 2009 bis zum 31. August 2009 am Lehrstuhl von Prof. Ernst-Ulrich Gekeler entstanden.
In dieser Zeit habe ich mich mit einer Rekursionsformel g_k der Tiefe zwei über dem Polynomring A in der Variablen T über dem endlichen Körper $\mathbb{F}_q$ mit q Elementen beschäftigt. In diese Rekursionsformel setzt man zwei Polynome g und Δ ein. Ist $g_d(g, \Delta)$ kongruent zu 0 modulo eines irreduziblen Polynoms f aus diesem Polynomring, so heißt das Paar (g, Δ) supersingulär bezüglich f.
Ist $g_d(d, \Delta)$ supersingulär bezüglich f, so hat der von (g, Δ) über dem Restkörper $A/(f)$ erzeugte Drinfeld Modul spezielle Eigenschaften. Deshalb ist es für die mathematische Forschung interessant zu untersuchen wie oft und in welchen Fällen diese Supersingularität vorkommt. Der Wert $g_d(g, \Delta)$ ist eine sogenannte Drinfeldsche Invariante, daher auch der Name der Arbeit. Auf die Theorie der Drinfeld-Moduln wird in dieser Arbeit gänzlich verzichtet, da es den Rahmen der Arbeit übersteigen würde und für die angestellten Untersuchungen nicht benötigt wurde.
Im ersten Schritt lässt man g und Δ fest gewählt und variiert f. Dann interessiert man sich für die Frage, wie oft (g, Δ) supersingulär bezüglich f ist für alle irreduziblen normierten Polynome f, deren Grad unterhalb einer gewissen Schranke liegt.
Im nächsten Schritt sei f fest gewählt vom Grad d. In diesem Fall ist die Frage interessant, wie viele supersinguläre Paare (g, Δ) es für ein f gibt.

Beginnen werde ich jedoch mit den für das Verständnis benötigten Grundlagen. Anschließend möchte ich eine Beschreibung der Situation geben, die für die ganze Arbeit gültig ist.

Die Arbeit richtet sich an Leser, die bereits einige Vorkenntnisse auf dem Gebiet der Algebra und Zahlentheorie besitzen. Es werden zusätzlich noch einige grundlegende Begriffe aus der Körpertheorie, der Galoistheorie sowie der algebraischen Zahlentheorie benötigt. Die wichtigsten Begriffe und Aussagen werden im Kapitel 1 zusammengestellt.

Die Berechnungen, die zu den in dieser Arbeit getroffenen Vermutungen führten, wurden mit Hilfe der Software *MAGMA Computational Algebra System* durchgeführt.

An dieser Stelle sage ich allen Dank, die mich während meines Studiums und vor allem beim Anfertigen dieser Arbeit unterstützt haben. Mein ganz besonderer Dank gilt Prof. Ernst-Ulrich Gekeler, der die vorliegende Arbeit nicht nur betreut, sondern für meine Anliegen stets ein offenes Ohr und mir bei Fragen immer als hilfreicher Berater zur Seite gestanden hat.
Ganz herzlich danke ich zudem Michael Hein, meiner Familie, meine Kommulitonen Anne Wald und Bernadette Hahn und den Assistenten von Professor Gekeler, Johannes Lengler und Bernd Mehnert.

Saarbrücken, im August 2009 Sarah Detzler

Kapitel 1

Grundlagen

In diesem Kapitel werden Grundlagen behandelt, die im Verlauf der Arbeit benötigt werden und auf die an verschiedenen Stellen verwiesen wird. Leser, denen diese bekannt sind, können gleich zum nächsten Kapitel übergehen. Die folgende Notation ist für die gesamte Arbeit gültig:

- $\mathbb{N} := \{1, 2, 3, ...\}$ ist die Menge der natürlichen Zahlen,
- $\lfloor x \rfloor := max\,\{n\mathbb{Z} \in |n \leq x\}$ ist die Gauß-Klammer,
- mit $|G|$ wird die Kardinalität einer Menge G bezeicnet,
- p ist immer eine Primzahl.

1.1 Körpererweiterungen

1.1.1 Bemerkung:
Ist K ein endlicher Körper, so hat er $q = p^r$ viele Elemente, wobei p eine Primzahl ist und $r \in \mathbb{N}$. Zu jeder Primzahlpotenz $q = p^r$ existiert (bis auf Isomorphie) genau ein endlicher Körper mit q Elementen. Die Charakteristik dieses Körpers ist p und für alle $a \in K$ gilt $a^q = a$. Des Weiteren ist die Einheitengruppe $(K)^*$ zyklisch und (nicht-kanonisch) isomorph zu $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$. Der endliche Körper mit q Elementen wird im Folgenden mit $\mathbb{F}_q$ bezeichnet.

1.1.2 Definition:
Die Abbildung

$$\begin{array}{rccl} \varphi: & \mathbb{N} & \longrightarrow & \mathbb{N}, \\ & n & \longmapsto & \varphi(n) \;=\; \#\{a \in \{1, ..., n\} \mid ggT(n, a) = 1\} \end{array}$$

wird als Eulersche Phi-Funktion bezeichnet. Sie ist schwach multiplikativ, d.h. für zwei teilerfremde natürliche Zahlen n und m gilt $\varphi(nm) = \varphi(n)\varphi(m)$.
Im Spezialfall $n = p^r,\ r \in \mathbb{N},\ p \in \mathbb{P}$, ist

$$\varphi(p^r) = (p-1)p^{r-1}. \tag{1.1}$$

(Siehe [SP07], Seite 75, Definition und Korollar 4.20.)

1.1.3 Definition:
Sind K und L Körper mit $K \subset L$, so nennt man K einen Unterkörper von L bzw. L einen Erweiterungskörper von K. Diese Körpererweiterung bezeichnet man mit $L|K$.
L kann als K-Vektorraum aufgefasst werden. Man definiert den Grad der Körpererweiterung $[L : K]$ als Dimension des K-Vektorraums L.
Die Erweiterung $L|K$ heißt endlich, falls $[L : K]$ endlich ist.

1.1.4 Bemerkung:
Die endlichen Körpererweiterungen des Körpers $\mathbb{F}_q$ sind die Körper $\mathbb{F}_{q^d}$, für $d \in \mathbb{N}$.

1.1.5 Proposition:
Der Körpergrad ist multiplikativ:
Sei K der Grundkörper und L eine Erweiterung von K, sowie M ein Zwischenkörper, d.h. $K \subset M \subset L$. Es gilt:

$$[L : K] = [L : M] \cdot [M : K]$$

(siehe [Bos06a], Seite 90, Satz 2).

1.1.6 Definition:
Ist $\alpha \in L := \mathbb{F}_{q^d}$, so ist die Spur *von α über $K := \mathbb{F}_q$ definiert durch:*

$$Tr_K^L(\alpha) := \alpha + \alpha^q + ... + \alpha^{q^{d-1}}.$$

$Tr_{\mathbb{F}_p}^K(\alpha)$ *bezeichnet die* absolute Spur *von α (siehe [LN94], Seite 51, Definition 2.22).*

1.1.7 Satz:
Sei $K := \mathbb{F}_q$ und $L := \mathbb{F}_{q^d}$, so besitzt die Spurfunktion Tr_K^L folgende Eigenschaften:

1. $Tr_K^L(\alpha + \beta) = Tr_K^L(\alpha) + Tr_K^L(\beta)$ *für alle $\alpha, \beta \in L$.*
2. $Tr_K^L(c \cdot \alpha) = c \cdot Tr_K^L(\alpha)$ *für alle $\alpha \in L$ und $c \in K$.*
3. $Tr_K^L(c) = d \cdot c$ *für alle $c \in K$.*
4. $Tr_K^L(\alpha^q) = Tr_K^L(\alpha)$ *für alle $\alpha \in L$.*

(Siehe [LN94], Seite 52, Theorem 2.23.)

1.1.8 Satz (Transitivität der Spur):
Sei K ein endlicher Körper, L eine endliche Körpererweiterung von K und M eine endliche Körpererweiterung von L. Dann gilt für alle $\alpha \in M$:

$$Tr_K^M(\alpha) = Tr_K^L(Tr_L^M(\alpha))$$

(siehe [LN94], Seite 53, Theorem 2.26).

1.1.9 Satz:
Das charakteristische Polynom $f = \sum_{i=0}^{n} a_i T^i$ einer Matrix $A \in K^{n \times n}$ ist normiert vom Grad n. Es gilt: die Spur von f entspricht $-a_{n-1}$ (siehe [Bos06b], Seite 201, Satz 3).

1.2 Polynomringe über endlichen Körpern

Nun betrachten wir den Polynomring $\mathbb{F}_q[T]$ in der Variablen T über dem endlichen Körper $\mathbb{F}_q$ mit q Elementen. In dieser Arbeit wird er mit A bezeichnet. Der Polynomring A ist insbesondere nullteilerfrei. Besonders interessieren wir uns für die irreduziblen Polynome, d.h. die Elemente aus A, die nicht weiter faktorisiert werden können. Die Anzahl und das Produkt aller normierten irreduziblen Polynome kann man leicht angeben.

1.2.1 Bemerkung:
Die Primideale in $\mathbb{F}_q[T]$ sind diejenigen Ideale, die von den irreduziblen Polynomen erzeugt werden. Man kann einen endlichen Körper mit q^d vielen Elementen konstruieren, indem man aus dem Polynomring $\mathbb{F}_q[T]$ das von einem irreduzibles Polynom f vom Grad d erzeugte Primideal ausdividiert. Es gilt also $\mathbb{F}_q[T]/(f)$ ist ein endlicher Körper mit q^d vielen Elementen (siehe [Bos06a], Seite 26-27). Ist $q = 3$ und $f(T) = T^3 - T + 1$, so hat der Körper $\mathbb{F}_3[T]/(T^3 - T + 1)$ 27 Elemente.

1.2.2 Definition:
Die Möbiusfunktion *ist eine Funktion auf* $\mathbb{N}$*, definiert durch die Vorschrift*

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n \text{ ist das Produkt von } k \text{ verschiedenen Primzahlen} \\ 0 & n \text{ ist nicht quadratfrei} \end{cases}$$

(siehe [LN94], Seite 85, Definition 3.22).

1.2.3 Satz (Möbius-Inversionsformel):

1. *Additiver Fall: Seien h und H zwei Funktionen von $\mathbb{N}$ in eine additiv geschriebene abelsche Gruppe. Dann gilt für alle $n \in \mathbb{N}$*

$$H(n) = \sum_{d|n} h(d)$$

genau dann, wenn für alle $n \in \mathbb{N}$

$$h(n) = \sum_{d|n} \mu(\frac{n}{d}) H(d) = \sum_{d|n} \mu(d) H(\frac{n}{d})$$

gilt.

2. *Multiplikativer Fall: Seien h und H zwei Funktionen von $\mathbb{N}$ in eine multiplikativ geschriebene abelsche Gruppe. Dann gilt für alle $n \in \mathbb{N}$*

$$H(n) = \prod_{d|n} h(d)$$

genau dann, wenn für alle $n \in \mathbb{N}$

$$h(n) = \prod_{d|n} H(d)^{\mu(\frac{n}{d})} = \prod_{d|n} H(\frac{n}{d})^{\mu(d)}$$

gilt.

(Siehe [LN94], Seite 85, Theorem 3.24.)

1.2.4 Definition:
Das Produkt aller irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k wird im Folgenden mit $I(q,k;T)$ bezeichnet.
Die Anzahl aller irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k wird im Folgenden durch $N_q(k)$ bezeichnet.

1.2.5 Satz:
Das Produkt $I(q,k;T)$ aller normierten irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k ist durch folgende Formel gegeben:

$$I(q,k;T) = \prod_{d|k}(T^{q^d} - T)^{\mu(\frac{k}{d})} = \prod_{d|k}(T^{q^{\frac{k}{d}}} - T)^{\mu(d)}$$

(siehe [LN94], Seite 87, Theorem 3.29).

1.2.6 Definition:
Wir definieren das Polynom $[k]$ in $\mathbb{F}_q[T]$ durch die Formel:

$$[k] := T^{q^k} - T$$

1.2.7 Bemerkung:
Das Produkt $I(q,k;T)$ aller irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k ist ein Teiler von:

$$[k] = T^{q^k} - T = \prod_{\substack{f \text{ irreduzibel, normiert} \\ grad(f)|k}} f.$$

Ist p die Charakteristik von $\mathbb{F}_q$, so gilt für alle $\mathbb{F}_q[T]$:

$$(f(T))^p = f(T^p)$$

1.2.8 Satz:
Die Anzahl $N_q(k)$ aller irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k ist durch folgende Formel gegeben:

$$N_q(k) = \frac{1}{n}\sum_{d|k}\mu(\frac{k}{d})q^d = \frac{1}{n}\sum_{d|k}\mu(d)q^{\frac{n}{d}}$$

(siehe [LN94], Seite 86, Theorem 3.25).

1.2.9 Definition:
Für alle $a \in \mathbb{F}^*$ und $b \in \mathbb{F}$ heißen Abbildungen der Form

$$\begin{array}{ccc} \mathbb{F}_q[T] & \longleftrightarrow & \mathbb{F}_q[T] \\ f(T) & \longrightarrow & f(a \cdot T + b) \end{array}$$

affine Transformationen.

Die Gruppe der affinen Transformationen operiert auf der Menge der irreduziblen Polynome.

1.3 Auszüge der Galoistheorie

An dieser Stelle sollen einige Erklärungen sowie wichtige Sätze aus der Galoistheorie, aufgeführt werden. Dabei wird jedoch darauf verzichtet, den Begriff *galoissch* zu erklären. Da in dieser Arbeit nur endliche Körper betrachtet werden, ist die Eigenschaft *galoissch* bei den betrachteten endlichen Körpererweiterung immer gegeben. Die Leserinnen und Leser dieser Arbeit, die eine Einführung in die Galoistheorie wünschen, können diese beispielsweise in ([Bos06a], Kapitel 3 und 4) nachlesen.

1.3.1 Definition:
Unter einem Körperautomorphismus *versteht man eine bijektive Abbildung* $\sigma : L \to L$ *von einem Körper auf sich selbst mit den folgenden Eigenschaften:*
Für alle $\alpha, \beta \in L$ *gilt*

$$\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta),$$
$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta).$$

Die Körperautomorphismen bilden eine Gruppe bezüglich Hintereinanderausführung.
Dabei bilden die Automorphismen, die einen Körper $K \subset L$ *festlassen, eine Untergruppe. Diese Untergruppe heißt* Galoisgruppe *der Körpererweiterung* $L|K$*. Sie wird bezeichnet mit* $Gal(L|K)$*.*

1.3.2 Satz:
Sei $\mathbb{F}_q$ *ein endlicher Körper,* $q = p^r$*, sowie* $\mathbb{F}$ *eine endliche Körpererweiterung vom Grad* n*. Dann ist* $\mathbb{F} \cong \mathbb{F}_{p^{nr}}$ *und* $Gal(\mathbb{F}_q|\mathbb{F})$ *zyklisch von der Ordnung* n *und wird erzeugt vom Frobenius-Automorphismus,* $\mathbb{F}_q \to \mathbb{F}_q$*,* $a \to a^q$ *(siehe [Bos06a], Seite 37-38 und 129).*

1.3.3 Satz:
Es sei L *ein Körper und* G *eine Untergruppe der Automorphismengruppe* $Aut(L)$ *von* L*. Weiter setze man*

$$K = L^G := \{a \in L; \sigma(a) = a \text{ für alle } \sigma \in G\}.$$

Dies ist der sogenannte Fixkörper *unter* G*.*
Ist G *endlich, so ist auch* $L|K$ *eine endliche Galois-Erweiterung vom Grad* $[L : K] = |G|$ *mit Galoisgruppe* $Gal(L|K) = G$ *([Bos06a], Seite 140, Satz 4).*

Wie bereits erwähnt, ist eine Körpererweiterung unter bestimmten Voraussetzungen, die bei uns immer erfüllt sind, *galoissch*. Ist dies für eine Körpererweiterung der Fall, so gilt der Hauptsatz der Galoistheorie:

1.3.4 Satz (Hauptsatz der Galoistheorie, siehe ([Bos06a], Seite 142, Theorem 6)):
Sei $L|K$ *eine endliche galoissche Erweiterung mit Galoisgruppe* $G := Gal(L|K)$*. Dann sind die Zuordnungen*

$$\begin{array}{ccc} \{\text{Teilkörper } M,\ K \subset M \subset L\} & \longleftrightarrow & \{\text{Untergruppen } H \subset G\} \\ M & \longrightarrow & Gal(L|M) \\ L^H & \longleftarrow & H \end{array}$$

welche einer Untergruppe $H \subset G$ *den Fixkörper* L^H*, bzw. einem Zwischenkörper* M *von* $L|K$ *die Galoisgruppe* $Gal(L|M)$ *der Galoiserweiterung zuordnet, bijektiv und invers zueinander.*

Die Körpererweiterung $L|M$ ist ebenfalls galoissch und hat die Galoisgruppe H.
Des Weiteren ist L^H genau dann galoissch, wenn H ein Normalteiler in G ist, also wenn für alle $g \in G$ gilt: $gHg^{-1} = H$. Ist dies der Fall, so induziert die Abbildung $\sigma \mapsto \sigma|_M$ einen Isomorphismus von G/H nach $Gal(M|K)$.

1.3.5 Satz:
Sei $L|K$ eine endliche galoissche Erweiterung mit Galoisgruppe $G := Gal(L|K)$.
Dann gilt $[L : K] = |G|$. ([Bos06a], Seite 141)

1.4 Auszüge der Verzweigungstheorie von Galoiserweiterungen

An dieser Stelle sollen einige Auszüge sowie wichtige Sätze aus der Verzweigungstheorie von Galoiserweiterungen aufgeführt werden. Da in dieser Arbeit nur Galoiserweiterungen behandelt werden, möchte ich auf den allgemeinen Fall nicht eingehen. Auf die Grundlagen sowie die Einzelheiten der Verzweigungstheorie möchte ich auch größtenteils verzichten. Dies ist nachzulesen in ([Neu07], § 8 und 9).

Sei K ein rationaler Funktionenkörper über einem endlichen Körper und $L|K$ eine endliche Galoiserweiterung vom Grad n mit Galoisgruppe $G := Gal(L|K)$. Es sei $\mathcal{O}$ der Ganzheitsring zu L und o der zu K, sowie $\mathfrak{p}$ ein Primideal in o. G operiert auf $\mathcal{O}$. Ist $\sigma \in G$ und $\mathfrak{q}$ ein Primideal über $\mathfrak{p}$(d.h. $\mathfrak{q} \cap o = \mathfrak{p}$), so gilt dies auch für $\sigma(\mathfrak{p})$.

1.4.1 Satz:
Die Galoisgruppe G operiert transitiv auf der Menge der über $\mathfrak{p}$ liegenden Primideale $\mathfrak{q}$ in $\mathcal{O}$, d.h. ist $\mathfrak{q}$ ein Primpolynom in $\mathcal{O}$ über $\mathfrak{p}$ so auch $\sigma(\mathfrak{p})$ für alle $\sigma \in G$. Diese Primideale heißen alle zueinander konjugiert. ([Neu07], Seite 56, Satz 9.1)

1.4.2 Satz:
Ein Primideal $\mathfrak{p}$ von o zerlegt sich in $\mathcal{O}$ in eindeutiger Weise in ein Produkt von Primidealen,

$$\mathfrak{p}\mathcal{O} = (\mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_g)^e.$$

Die auftretenden Primideale $\mathfrak{q}_i$ sind genau diejenigen Primideale von $\mathcal{O}$, die über $\mathfrak{p}$ liegen.
([Neu07], Seite 48)

1.4.3 Definition:
Der Exponent e heißt der Verzweigungsindex. *Der* Trägheitsgrad *f ist definiert als*
$f = [\mathcal{O}/\mathfrak{q}_i : o/\mathfrak{p}]$, wobei $\mathcal{O}/\mathfrak{q}_i$ und $o/\mathfrak{p}$ die Restkörper der Ganzheitsringe modulo der entsprechenden Primideale sind. ([Neu07], Seite 58)

1.4.4 Satz:
Die Restkörper $\mathcal{O}/\mathfrak{q}_i$ sind alle isomorph zueinander. Zudem gilt die fundamentale Gleichung:

$$e \cdot f \cdot g = n.$$

([Neu07], Seite 58)

Kapitel 2

Situation

Betrachtet wird der Polynomring A in der Variablen T über dem endlichen Körper $\mathbb{F}_q$ mit q Elementen. $\mathfrak{p} = (f)$ ist das von f erzeugte Primideal zum irreduziblen normierten Primpolynom vom Grad $grad(f) = d$. Im Folgenden wird mit der Körpererweiterung $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$ über $\mathbb{F}_q$ gearbeitet. Wählt man ein $g \in \mathbb{F}_\mathfrak{p}$ und ein $\Delta \in \mathbb{F}_\mathfrak{p}^*$, so kann man rekursiv eine Folge g_0, g_1, g_2,... in $\mathbb{F}_\mathfrak{p}$ wie folgt definieren:

$$g_0 := 1$$

$$g_1 := g$$

$$g_k(g, \Delta) := -[k-1]g_{k-2}\Delta^{q^{k-2}} + g_{k-1}g^{q^{k-1}}.$$

Dies gilt für alle $k \geq 2$. Des Weiteren wird $[k-1]$ als Element von $\mathbb{F}_\mathfrak{p}$ betrachtet.
Wir bezeichnen ein Paar (g, Δ) als *supersingulär* genau dann, wenn $g_d = 0$ ist in $\mathbb{F}_\mathfrak{p}$.

Das besondere Augenmerk in dieser Arbeit wird auf die beiden folgenden Fragestellungen gelegt:

- Seien g und Δ fest gewählt. Wie oft ist (g, Δ) supersingulär mod $\mathfrak{p}$ für alle $\mathfrak{p}$ unterhalb einer gewissen Schranke, d.h. für alle $\mathfrak{p}$ mit $grad(\mathfrak{p}) \leq x$?
- Die Polynome $\mathfrak{p}$ seien fest gewählt vom Grad d. Wie viele supersinguläre Paare (g, Δ) gibt es modulo $\mathfrak{p}$? Lässt man $\mathfrak{p}$ alle Primideale vom Grad d durchlaufen, so stellt sich die Frage, welchen Wert
  $\sum_{\mathfrak{p}\ grad(\mathfrak{p})=d} |\{(g, \Delta) \mid (g, \Delta) \text{ ist supersingulär mod } \mathfrak{p}\}|$ hat?

Dazu wurden theoretische Überlegungen und numerische Rechnungen mit Hilfe des Computeralgebraprogramms Magma angestellt. Die Berechnungen wurden mit der Magma-Version 2.11 auf dem Server Pyramis der Universität des Saarlandes durchgeführt.
In dieser Arbeit werden die einzelnen $\mathfrak{p}$, für die ein festes j supersingulär ist, als supersinguläre Stellen von j bezeichnet. Für ein festes $\mathfrak{p}$ werden die einzelnen j, die in $\mathbb{F}_\mathfrak{p}$ supersingulär sind, als supersinguläre j-Werte oder supersiguläre Werte bezeichnet.

Kapitel 3

Allgemeine Vorüberlegungen

In diesem Kapitel beschäftigen wir uns mit der Frage, ob es möglich ist, die Supersingulärität eines Paares (g, Δ) schneller als durch die Berechnung von g_k zu überprüfen. Wollen wir die Supersingularität für alle Paare (g, Δ) überprüfen, so müssen wir g_d für $q^d(q^d - 1)$ viele Paare (g, Δ) berechnen. Wie wir sehen werden, ist dies nicht nötig.
Betrachten wir also im Folgenden die Rekursion in $\mathbb{F}_\mathfrak{p}$:

$$g_0 := 1$$

$$g_1 := g$$

$$g_k(g, \Delta) := -[k-1]g_{k-2}\Delta^{q^{k-2}} + g_{k-1}g^{q^{k-1}}. \tag{3.1}$$

3.1.5 Bemerkung:
Man kann jeder Variablen eines Polynoms einen bestimmten Zahlenwert, das sogenannte *Gewicht*, zuordnen. Will man aus einer Variablen mit Gewicht m eine Konstante ausklammern, so muss man diese Konstante in die m-te Potenz erheben. Ein Polynom heißt dann *isobar* vom Gewicht m, wenn jeder Summand dasselbe Gewicht m hat. Isobare Polynome stellen eine Verallgemeinerung von homogenen Polynomen dar. Bei homogenen Polynomen vom Grad n ist 1 das Gewicht jeder Variablen und wenn man eine Konstante aus jeder Variablen ausklammert, so wird diese in die n-te Potenz erhoben. Will man bei einem isobaren Polynom aus jeder Variablen eine Konstante ausklammern, so wird sie in die m-te Potenz erhoben.

3.1.6 Beispiel:
Ordnet man X das Gewicht 2 und Y das Gewicht 3 zu, so ist $f(X;Y) = X^6 + Y^4 + X^3 \cdot Y^2$ ein isobares Polynom vom Gewicht $m = 12$.

$$f(cX;cY) = (cX)^6 + (cY)^4 + (cX)^3 \cdot (cY)^2 = c^{12}X^6 + c^{12}Y^4 + c^6X^3 \cdot c^6Y^2 = c^{12}f(X,Y)$$

3.1.7 Satz:
Ordnet man g das Gewicht $w(g) = 1$ und Δ das Gewicht $w(\Delta) = q + 1$ zu, so ist g_k isobar vom Gewicht $\frac{q^k-1}{q-1}$.

Beweis: Mittels Induktion nach k.
Induktionsanfang:

$$\begin{aligned} k=0: \quad & g_0 = 1 \quad w(g_0) = 0 = q^0 - 1 \\ k=1: \quad & g_1 = g \quad w(g_1) = 1 = \frac{q^1-1}{q-1} \end{aligned}$$

Induktionsvoraussetzung: Die Behauptung sei erfüllt für alle $n \in \mathbb{N}$ mit $n < k$.
Induktionsschritt: $(k-1) \to k$

$$\begin{aligned} w(-[k-1] \cdot g_{k-2}(g,\Delta) \cdot \Delta^{q^{k-2}}) &= w(g_{k-2}(g,\Delta)) + w(\Delta^{q^{k-2}}) \\ &\overset{\text{IV}}{=} \frac{q^{k-2}-1}{q-1} + (q+1) \cdot q^{k-2} \\ &= \frac{q^k - 1}{q-1} \end{aligned}$$

$$\begin{aligned} w(g_{k-1} \cdot g^{q^{k-1}}) &= w(g_{k-1}) + w(g^{q^{k-1}}) \\ &\overset{\text{IV}}{=} \frac{q^{k-1}-1}{q-1} + q^{k-1} \\ &= \frac{q^k-1}{q-1} \end{aligned}$$

Die einzelnen Summanden von g_k haben das Gewicht $\frac{q^k-1}{q-1}$, somit ist g_k isobar vom Gewicht $\frac{q^k-1}{q-1}$.□

3.1.8 Satz:
Es gilt die Gleichung:

$$g_k(c \cdot g, c^{q+1} \cdot \Delta) = c^{\frac{q^k-1}{q-1}} \cdot g_k(g,\Delta).$$

Beweis: Dies folgt direkt aus der Definition von isobar. □

3.1.9 Bemerkung:
Diese Identität beweist, dass die Supersingularität von (g,Δ) nur von $j := \frac{g^{q+1}}{\Delta}$ abhängt. Für ein festes j gibt es insgesamt (q^d-1) viele Paare (g,Δ), für die in $\mathbb{F}_\mathfrak{p}$ gilt $j = \frac{g^{q+1}}{\Delta}$.

3.1.10 Definition:
Wir definieren im Folgenden:

$$\varphi_0 = 1$$
$$\varphi_1 = 1$$
$$\varphi_k(X) = X^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(X) - [k-1] \cdot \varphi_{k-2}(X)$$
$$\chi(k) = \begin{cases} 1, & k \textit{ ungerade} \\ 0, & k \textit{ gerade.} \end{cases}$$

3.1.11 Satz:
Es gilt:

$$g_k(g,\Delta) = \varphi_k(j) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)}.$$

Beweis: Mittels Induktion nach k.
Induktionsanfang: Die Behauptung ist für $k = 0$ und $k = 1$ erfüllt:

$$\begin{aligned} k = 0: \quad g_0 = 1 &= \varphi_0 \cdot \Delta^{\frac{q^0 - q^{\chi(0)}}{q^2-1}} \cdot g^{\chi(0)} \\ k = 1: \quad g_1 &= \varphi_1 \cdot \Delta^{\frac{q^1 - q^{\chi(1)}}{q^2-1}} \cdot g^{\chi(1)} \end{aligned}$$

Induktionsvoraussetzung: Die Behauptung sei erfüllt für alle $n \in \mathbb{N}$ mit $n < k$.
Induktionsschritt: $(k-1) \to k$

$$\begin{aligned}
g_k(g,\Delta) &= -[k-1]g_{k-2}(g,\Delta)\Delta^{q^{k-2}} + g_{k-1}(g,\Delta)g^{q^{k-1}} \\
&\overset{\text{IV}}{=} -[k-1]\varphi_{k-2}(j) \cdot \Delta^{\frac{q^{k-2} - q^{\chi(k-2)}}{q^2-1} + q^{k-2}} \cdot g^{\chi(k-2)} + \varphi_{k-1}(j) \cdot \Delta^{\frac{q^{k-1} - q^{\chi(k-1)}}{q^2-1}} \cdot g^{q^{k-1} + \chi(k-1)} \\
&= -[k-1]\varphi_{k-2}(j) \cdot \Delta^{\frac{q^{k-2} - q^{\chi(k-2)} + q^{k-2}\cdot(q^2-1)}{q^2-1}} \cdot g^{\chi(k-2)} + \varphi_{k-1}(j) \cdot \Delta^{\frac{q^{k-1} - q^{\chi(k-1)}}{q^2-1}} \cdot g^{q^{k-1} + \chi(k-1)} \\
&= -[k-1]\varphi_{k-2}(j) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} + \varphi_{k-1}(j) \cdot \Delta^{\frac{q^{k-1} - q^{\chi(k-1)}}{q^2-1}} \cdot g^{q^{k-1} + \chi(k-1)} \\
&= \left(-[k-1]\varphi_{k-2}(j) + \varphi_{k-1}(j) \cdot \Delta^{\frac{q^{k-1} - q^{\chi(k-1)}}{q^2-1} - \frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{q^{k-1} + \chi(k-1) - \chi(k)} \right) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} \\
&= \left(-[k-1]\varphi_{k-2}(j) + \varphi_{k-1}(j) \cdot \Delta^{\frac{-q^k + q^{k-1} + (-1)^{k-1} q + (-1)^k}{q^2-1}} \cdot g^{q^{k-1} + (-1)^k} \right) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} \\
&= \left(-[k-1]\varphi_{k-2}(j) + \varphi_{k-1}(j) \cdot \Delta^{\frac{-(q-1)(q^{k-1} + (-1)^k)}{q^2-1}} \cdot g^{q^{k-1} + (-1)^k} \right) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} \\
&= \left(-[k-1]\varphi_{k-2}(j) + \varphi_{k-1}(j) \cdot \Delta^{\frac{q^{k-1} + (-1)^k}{q+1}} \cdot g^{q^{k-1} + (-1)^k} \right) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} \\
&= \left(-[k-1]\varphi_{k-2}(j) + \varphi_{k-1}(j) \cdot \left(\frac{g^{q+1}}{\Delta} \right)^{\frac{q^{k-1} + (-1)^k}{q+1}} \right) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} \\
&= \left(-[k-1]\varphi_{k-2}(j) + \varphi_{k-1}(j) \cdot j^{\frac{q^{k-1} + (-1)^k}{q+1}} \right) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)} \\
&= \varphi_k(j) \cdot \Delta^{\frac{q^k - q^{\chi(k)}}{q^2-1}} \cdot g^{\chi(k)}
\end{aligned}$$

□

3.1.12 Korollar:
g_k ist genau dann 0, wenn $\varphi_k(j) = 0$ oder $g = 0$ modulo $\mathfrak{p}$. Beides zusammen kann nicht vorkommen. Ist $\varphi_k(j) = 0$ für genau l verschiedene j, so ist $g_k = 0$ für genau $l \cdot (q^d - 1)$ Paare $(g,\Delta) \in \mathbb{F}_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}^*$ mit $g \neq 0$.

Beweis: Die Behauptung das g_k ist genau dann 0, wenn $\varphi_k(j) = 0$ oder $g = 0$ modulo $\mathfrak{p}$, folgt direckt aus Satz 3.1.11.
Bleibt noch zu, dass $\varphi_k(j) \neq 0$, wenn $g = 0$. Ist $g = 0$, so ist $j = \frac{0}{\Delta} = 0$. Mittels Induktion nach k zeigt man, dass $\varphi_k(0)$ bis auf Vorzeichen mit $\prod_{i=1}^{k-1} \chi(k+i) \cdot [i]$ übereistimmt. Da keiner der Faktoren ein irreduzibles Polynom vom Grad k enthält, ist $\varphi_k(0) \neq 0$ in $\mathbb{F}_\mathfrak{p}$. Dies gilt für alle $\mathfrak{p}$ vom Grad k. □

Betrachten wir nun den Spezialfall $g = 0$.

3.1.13 Korollar:
Ist $g = 0$, so gilt für alle Primideale $\mathfrak{p}$ mit $grad(\mathfrak{p}) = k$ in $\mathbb{F}_\mathfrak{p}$:

$$\begin{aligned} g_k &= 0, \quad \textit{falls } k \textit{ ungerade} \\ g_k &\neq 0, \quad \textit{falls } k \textit{ gerade} \end{aligned}$$

Beweis: Für ungerade k folgt die Behauptung direkt aus Satz 3.1.11.
Für gerade k und $g = 0$ gilt:

$$g_k = (-1)^{\frac{k}{2}} \prod_{i=2}^{k} [i-1] \cdot \Delta^{q^{i-2}}$$

Induktionsanfang: Die Behauptung ist für $k = 0$ und $k = 1$ erfüllt.

$$\begin{aligned} k = 0: &\quad g_0 = 1 \\ k = 2: &\quad g_2 = -[1]\Delta \end{aligned}$$

Induktionsvoraussetzung: Die Behauptung sei erfüllt für alle $n \in \mathbb{N}$ mit $n < k$.
Induktionsschritt: $(k-2) \to k$
k gerade:

$$\begin{aligned} g_k(0,\Delta) &= -[k-1]g_{k-2}(g,\Delta)\Delta^{q^{k-2}} + g_{k-1}(g,\Delta)g^{q^{k-1}} \\ &= -[k-1]g_{k-2}(g,\Delta)\Delta^{q^{k-2}} \\ &\overset{\text{IV}}{=} -[k-1](-1)^{\frac{k-2}{2}} \prod_{i=2}^{k-2} [i-1] \cdot \Delta^{q^{i-2}} \cdot \Delta^{q^{k-2}} \\ &= (-1)^{\frac{k}{2}} \prod_{i=2}^{k} [i-1] \cdot \Delta^{q^{i-2}} \end{aligned}$$

Da keiner dieser Faktoren kongruent zu Null ist modulo eines Primideals $\mathfrak{p}$ für alle $\mathfrak{p}$ mit $grad(\mathfrak{p}) = k$, folgt $g_k \neq 0$ modulo $\mathfrak{p}$, da $\mathbb{F}_\mathfrak{p}$ insbesondere nullteilerfrei ist. □

Daher ist es im Folgenden ausreichend, φ_k anstelle von g_k zu betrachten. Wollen wir die Supersingularität für alle Paare (g, Δ) überprüfen, so müssen wir nicht g_k für $q^d(q^d-1)$ viele Paare (g, Δ) berechnen, sondern lediglich φ_k für $q^d - 1$ viele j.
Zunächst stellt sich die Frage nach dem Grad von φ_k.
Der folgende Satz hat für die theoretischen Überlegungen keine große Bedeutung, ist aber für die Laufzeitanalysen notwendig.

3.1.14 Satz:
Sei $j \in A$ vom Grad d. Dann gilt:

$$grad(\varphi_k(j)) \leq \begin{cases} \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i & \text{für } d \leq q \\ \sum_{i=1}^{k-1} \chi(k+i) \cdot d \cdot q^{i-1} & \text{für } d > q. \end{cases}$$

Beweis: Mittels Induktion nach k.
Induktionsanfang:
Für $\varphi_0(j) = \varphi_1(j) = 1$ ist der Grad jeweils 0.
Da $\varphi_2(j) = -(T^q - T) + j$ ist der $grad(\varphi_2(j)) \leq max(d, q)$.
Induktionvoraussetzung: Die Behauptung sei erfüllt für alle $n \in \mathbb{N}$ mit $n < k$
Man unterscheidet die beiden Fälle $q \geq d$ und $q < d$.
Induktionsschritt: $(k-1) \to k$
1. Fall: $q \geq d$

$$\begin{aligned} grad(\varphi_k(j)) &= grad(j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j) - [k-1] \cdot \varphi_{k-2}(j)) \\ &\leq max(grad(j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j)), grad(-[k-1] \cdot \varphi_{k-2}(j))) \\ &\overset{\text{IV}}{\leq} max(d \cdot \frac{q^{k-1}+(-1)^k}{q+1} + \sum_{i=1}^{k-2} \chi(k-1+i) \cdot q^i, q^{k-1} + \sum_{i=1}^{k-3} \chi(k+i) \cdot q^i) \\ &= \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i \end{aligned}$$

2. Fall: $q < d$

$$
\begin{aligned}
grad(\varphi_k(j)) &= grad(j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j) - [k-1] \cdot \varphi_{k-2}(j)) \\
&\leq max(grad(j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j)), grad(-[k-1] \cdot \varphi_{k-2}(j))) \\
&\overset{\text{IV}}{\leq} max(d \cdot \frac{q^{k-1}+(-1)^k}{q+1} + \sum_{i=1}^{k-2} \chi(k-1+i) \cdot d \cdot q^{i-1}, q^{k-1} + \sum_{i=1}^{k-3} \chi(k+i) \cdot d \cdot q^{i-1}) \\
&= d \cdot \frac{q^{k-1}+(-1)^k}{q+1} + \sum_{i=1}^{k-2} \chi(k-1+i) \cdot d \cdot q^{i-1} \\
&= d \cdot (-1)^{\chi(k)} \cdot \sum_{i=1}^{k-2} (-1)^i q^i + \sum_{i=1}^{k-2} \chi(k-1+i) \cdot d \cdot q^{i-1} \\
&= \sum_{i=1}^{k-1} \chi(k+i) \cdot d \cdot q^{i-1} \qquad \square
\end{aligned}
$$

Kapitel 4

Wachstum der Anzahl supersingulärer Stellen für feste j

Wie auch in den vorangegangenen Kapiteln ist $\mathfrak{p}$ das von einem irreduziblen Polynom f erzeugte Primideal. Von grundlegender Bedeutung für die vorliegende Arbeit ist die Fragestellung, wie oft (g, Δ) für fest gewählte g und Δ supersingulär modulo $\mathfrak{p}$ ist, wobei f alle irreduziblen Polynome mit $grad(f) \leq x$ durchläuft. Wie wir in Kapitel 2 bereits gesehen haben, können wir $\varphi_k(j)$ statt $g_k(g, \Delta)$ betrachten. Wir definieren eine Funktion $H_j(x)$ durch

$$H_j(x) := \sum_{i=2}^{x} \left| \left\{ f \;\middle|\; \begin{array}{c} f \text{ ist normiertes, irreduzibles Polynom, mit } grad(f) \leq x \\ \text{und } j \text{ ist supersingulär mod } \mathfrak{p} \end{array} \right\} \right|.$$

Im Folgenden wird der Wert $H_j(x)$ für ein vorgegebenes j berechnet und somit für alle Paare (g, Δ), für die $\frac{g^{q+1}}{\Delta} = j$ gilt. In unserem Fall durchläuft j die Polynome aus A vom Grad < 2. Wir können uns auf die j aus A beschränken, da wir nur am asymptotischen Verhalten von H_j interessiert sind. Für Paare (g, Δ) mit $g, \Delta \in A$, für die $\frac{g^{q+1}}{\Delta} = j$ ist, müssen wir diejenigen $\mathfrak{p}$ ausschließen für die $\Delta \equiv 0$ ist. Da dies jedoch nur endlich viele sind, ändert dies das asymptotische Verhalten von H_j nicht.

4.1 Vorüberlegungen

In diesem Abschnitt werden Überlegungen angestellt, wie H_j effektiv berechnet werden kann. Zunächst kann man feststellen, dass man das Berechnen aller irreduziblen Polynome, deren Grad unterhalb einer gewissen Schranke liegt, geschickt umgehen kann.
Nach Satz 1.2.5 ist das Produkt $I(q, k; T)$ aller irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k durch folgende Formel gegeben:

$$I(q, k; T) = \prod_{d|k} (T^{q^d} - T)^{\mu(\frac{k}{d})} = \prod_{d|k} (T^{q^{\frac{k}{d}}} - T)^{\mu(d)}.$$

Unser j wurde so gewählt, dass es in A liegt. Dann liegt auch $\varphi_k(j)$ in A und wir können die folgenden Rechnungen zunächst in diesem Polynomring durchführen.
Da $I(q,k;T)$ jedes irreduzible Polynom vom Grad k genau einmal als Faktor enthält, kann man durch Berechnung von $\varphi_k(j)$ in dem Polynomring A und anschließender Bildung des größten gemeinsamen Teilers von $\varphi_k(j)$ und $I(q,k;T)$ feststellen, welche verschiedenen irreduziblen Polynome $\varphi_k(j)$ als Faktoren enthält. Somit kann auch berechnet werden, für welche $\mathfrak{p}$ das Polynom $\varphi_k(j)$ in $\mathbb{F}_\mathfrak{p}$ supersingulär ist. Da jedoch nur die Anzahl von Interesse ist und nicht, für welche f vom Grad k das Paar (g,Δ) supersingulär modulo $\mathfrak{p}$ ist, sind alle benötigten Informationen im Grad von $ggT(\varphi_k(j), I(q,k;T))$ enthalten. Für alle $x \geq 2$ berechnet sich $H_j(x)$ durch $H_j(x) = \sum_{i=2}^{k} grad\frac{ggT(\varphi_i(j),I(q,i;T))}{i}$. Diese Summe startet mit $i=2$, da $\varphi_1 = 1$ ist und somit keinen Beitrag zu H_j liefert.

Die Gruppe der affinen Transformationen operiert auf der Menge der irreduziblen Polynome; dadurch ergibt sich ein Invarianzkriterium.

4.1.1 Satz:
Sei $j \in A$ sowie $b \in \mathbb{F}_q$. Dann gilt:
$j(T)$ ist genau dann supersingulär modulo $\mathfrak{p}(T)$, wenn $j(T+b)$ supersingulär modulo $\mathfrak{p}(T+b)$ ist. Somit haben $j(T)$ und $j(T+b)$ gleichviele supersinguläre Stellen eines festen Grades k.

Beweis: Zunächst stellen wir fest, dass φ_k invariant unter Transformationen der Art $T \to T+b$ ist, da sowohl die Anfangswerte $\varphi_0 = \varphi_1$ als auch $[k-1]$ invariant unter diesen Tranformationen sind. Ein $j(T) \in A$ mit $j \neq 0$ wird unter der Transformation auf $j(T+b)$ abgebildet. Durch Ausmultiplizieren kann $j(T+b)$ in ein Polynom $j'(T)$ umgeformt werden. Ebenso können wir mit einem Primideal $\mathfrak{p}(T)$ verfahren. Man kann $\mathfrak{p}(T)$ auf ein $\mathfrak{p}(T+b)$ abbilden und in ein $\mathfrak{p}'(T)$ umformen. Man überlegt sich leicht, dass $\mathfrak{p}(T)$ genau dann prim ist, wenn $\mathfrak{p}(T+b)$ prim ist. Somit ist $j(T)$ genau dann supersingulär modulo $\mathfrak{p}(T)$, wenn $j'(T)$ supersingulär modulo $\mathfrak{p}'(T)$ ist. □

Weitere Invarianzkriterien ergeben sich aus folgenden Überlegungen:
Zunächst nutzen wir, dass die Rekursion invariant unter Galoistransformationen ist.

4.1.2 Satz:
Sei $q := p^r$, wobei p eine Primzahl und $r \in \mathbb{N}$ mit $r > 1$ ist, $j \in A$ und σ ein Element der Galoisgruppe von $\mathbb{F}_q|\mathbb{F}_p$. Dann gilt:
$j(T)$ ist genau dann supersingulär modulo $\mathfrak{p}(T)$, wenn $\sigma(j(T))$ supersingulär modulo $\sigma(\mathfrak{p}(T))$ ist. Somit haben $j(T)$ und $\sigma(j(T))$ gleichviele supersinguläre Stellen eines festen Grades k. Dabei setzen wir in dieser Situation die Operationen von $Gal(\mathbb{F}_q|\mathbb{F}_p)$ auf $\mathbb{F}_q[T]$ fort.

Beweis:

$$\begin{array}{c} \mathbb{F}_q \\ r \Big| \\ \mathbb{F}_p \end{array}$$

Zunächst stellen wir fest, dass φ_k invariant unter Galoistransformationen ist. Sowohl die Anfangswerte $\varphi_0 = \varphi_1$ als auch $[k-1]$ sind invariant unter diesen Tranformationen, da sowohl $\varphi_0 = \varphi_1$ als

auch $[k-1]$ Polynome mit Koeffizienten in $\mathbb{F}_p$ sind. Für Polynome f gilt, dass $f(T)$ genau dann irreduzibel ist, wenn $\sigma(f(T))$ irreduzibel ist. Somit ist $j(T)$ genau dann supersingulär modulo $\mathfrak{p}(T)$, wenn $\sigma(j(T))$ supersingulär modulo $\sigma(\mathfrak{p}(T))$ ist. □

4.1.3 Satz:
Das Polynom $\varphi_k(X) \in A[X] = \mathbb{F}_q[T, X]$ erfüllt für $0 \neq c \in \mathbb{F}_q$ die Gleichung:

$$\varphi_k(cT; cX) = c^{\lfloor \frac{k}{2} \rfloor} \cdot \varphi_k(T; X).$$

Dies zeigt, dass insbesondere die olgende Identität gilt:

$$\varphi_k(T; c) = c^{\lfloor \frac{k}{2} \rfloor} \cdot \varphi_k(\frac{T}{c}; 1).$$

Beweis: Mittels Induktion nach k
Induktionsanfang: Für $\varphi_0 = \varphi_1 = 1$ ist die Behauptung wahr.
Induktionsbehauptung: Die Behauptung sei erfüllt für alle $n \in \mathbb{N}$ mit $n < k$.
Induktionsschritt: $k - 1 \to k$
Wir unterscheiden die beiden Fälle k gerade bzw. k ungerade.
1. Fall: k ungerade
In dieser Situation ist $k-1$ gerade und $c^{\frac{q^{k-1}+(-1)^k}{q+1}} = 1$, sowie $\lfloor \frac{k-1}{2} \rfloor = \lfloor \frac{k}{2} \rfloor$.
Damit gilt:

$$\begin{aligned}
\varphi_k(cT; cX) &= -((cT)^{q^{k-1}} - (cT))\varphi_{k-2}(cT; cX) + (cX)^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(cT; cX) \\
&\overset{\text{IV}}{=} -((cT)^{q^{k-1}} - (cT)) \cdot c^{\lfloor \frac{k-2}{2} \rfloor}\varphi_{k-2}(T; X) + 1 \cdot c^{\lfloor \frac{k-1}{2} \rfloor} \cdot \varphi_{k-1}(T; X) \\
&= c^{\lfloor \frac{k}{2} \rfloor} \cdot (-(T^{q^{k-1}} - T) \cdot \varphi_{k-2}(T; X) + \varphi_{k-1}(T; X)) \\
&= c^{\lfloor \frac{k}{2} \rfloor} \cdot \varphi_k(T; X).
\end{aligned}$$

2. Fall: k gerade
In dieser Situation ist $k-1$ ungerade und $c^{\frac{q^{k-1}+(-1)^k}{q+1}} = c$, sowie $\lfloor \frac{k-1}{2} \rfloor = \lfloor \frac{k}{2} \rfloor - 1$.
Damit gilt:

$$\begin{aligned}
\varphi_k(cT; cX) &= -((cT)^{q^{k-1}} - (cT))\varphi_{k-2}(cT; cX) + (cX)^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(cT; cX) \\
&\overset{\text{IV}}{=} -((cT)^{q^{k-1}} - (cT)) \cdot c^{\lfloor \frac{k-2}{2} \rfloor}\varphi_{k-2}(T; X) + c \cdot c^{\lfloor \frac{k-1}{2} \rfloor} \cdot \varphi_{k-1}(T; X) \\
&= c^{\lfloor \frac{k}{2} \rfloor} \cdot (-(T^{q^{k-1}} - T) \cdot \varphi_{k-2}(T; X) + \varphi_{k-1}(T; X)) \\
&= c^{\lfloor \frac{k}{2} \rfloor} \cdot \varphi_k(T; X).
\end{aligned}$$

□

4.1.4 Satz:
Ist $k \in \mathbb{N}$, so gilt:
Für alle $0 \neq j \in \mathbb{F}_q$ gibt es gleichviele supersinguläre Stellen f vom Grad k.

Beweis: Ist $\mathfrak{p}(T)$ ein Primideal in $\mathbb{F}_q[T]$, so ist $\mathfrak{p}(\frac{T}{c})$ ein Primideal in $\mathbb{F}_q[\frac{T}{c}]$ und umgekehrt. $\mathfrak{p}(\frac{T}{c})$ kann durch Ausmultiplizieren und Normieren mit einem Primideal $\mathfrak{p}'(T)$ identifiziert werden. Da $\varphi_k(c)$ als Element in $\mathbb{F}_q[T]$ mit dem Element $\varphi_k(1)$ von $\mathbb{F}_q[\frac{T}{c}]$ identifiziert wird, gilt dass $\varphi_k(c)$ genau dann supersingulär modulo $\mathfrak{p}(T)$ ist, wenn dies für $\varphi_k(1)$ modulo $\mathfrak{p}'(T)$ gilt. □

4.1.5 Satz:
Die Primideale $\mathfrak{p}(T)$ und $\mathfrak{p}(a(T+b))$ haben gleichviele supersinguläre j-Werte.

Beweis: Betrachten wir zunächt das Primideal $\mathfrak{p}(T+b)$. Dieses hat nach Satz 4.1.1 genauso viele supersinguläre Werte, wie $\mathfrak{p}(T)$. Sei $j_1 \in A$ ein supersingulärer Wert von $\mathfrak{p}(T)$. Dann ist $\varphi_k(T; j_1)$ ein Vielfaches von $\mathfrak{p}(T)$.
Nach Satz 4.1.3 gilt $a^{\lfloor \frac{k}{2} \rfloor} \cdot \varphi_k(T+b; j_1) = \varphi_k(a(T+b); aj_1)$, diese Gleichung zeigt, dass $\mathfrak{p}(T+b)$ und $\mathfrak{p}(a(T+b))$ die gleiche Anzahl an supersingulären Werten haben. Insgesamt zeigen diese Argumente, das $\mathfrak{p}(T+b)$ und $\mathfrak{p}(T)$ genauso wie $\mathfrak{p}(T+b)$ und $\mathfrak{p}(a(T+b))$ gleichviele supersinguläre Werte haben. Somit gilt dies auch für $\mathfrak{p}(T)$ und $\mathfrak{p}(a(T+b))$. □

Ingesamt haben wir also festgestellt, dass wir die irreduziblen Polynome nicht berechnen müssen, was nicht nur die Rechenzeit, sondern auch den Speicherplatz, den unser Programm benötigt, reduziert. Sonst hätten alle irreduziblen Polynome in einer Liste gespeichert und diese ins Programm eingebunden werden müssen. Es ist jedoch nur notwendig, $grad(ggT(\varphi_k, I(q,k;T)))$ zu berechnen, so dass man nur noch eine Zahl anstelle einer Liste von Strings mit jeweils k Einträgen betrachten muss.
Da wir drei Invarianzkriterien für j gefunden haben, reicht es für unsere Zwecke H_j für $j = 1$ sowie $j = a \cdot T$ berechnen, wobei $a \in \mathbb{F}_q{}^*$ ist. Ist q eine Primzahlpotenz mit Exponent größer 1, so können wir uns darauf beschränken, a die Vertreter jeder Bahn der Galoisguppe durchlaufen zu lassen. Unser j durchläuft nur dei Polynome vom Grad < 2, somit decken diese Fälle alle j ab, die nicht aufgrund der angegebenen Gruppenoperationen die gleiche Anzahl an supersingulären Stellen haben.

4.2 Programm

Eingabe der Parameter:
Einlesen von q;
Einlesen von j;
Setzen der Startwerte:
$\varphi_0 := 1$;
$\varphi_1 := 1$;
$H(k) := 0$;
Berechnung von $H(k)$:
Schleife von $k = 2$ bis x;
$\lambda := \frac{q^{k-1}+(-1)^k}{q+1}$;
$\varphi_k := j^{\lambda} \cdot \varphi_1(j) - [k-1] \cdot \varphi_0(j)$;
$\varphi_0 := \varphi_1$;

$\varphi_1 := \varphi_k$;
y:=Grad des größten gemeinsamen Teilers von φ_k und $I(q,k;T)$, geteilt durch k;
$H(k) := H(k-1) + y$;
Gib $H(k)$ aus;
Beende Schleife;

4.3 Laufzeitanalyse

Ich möchte nicht im Detail auf die von mir verwendeten Algorithmen eingehen. Eine ausfürhliche Beschreibung hierzu findet man in der jeweils angegebene Quelle.
In unseren Rechnungen gilt j ist ein Polynom vom Grad 0 oder 1. Somit hat nach Satz 3.1.14 $\varphi_k(j)$ maximal den Grad $\sum_{i=1}^{k-1} \chi(k+i) \cdot q^i$.
Da alle Berechnungen in einem Polynomring über einem endlichen Körper mit weniger als zehn Elementen stattfinden, können wir annehmen, dass Addition und Multiplikation von Elementen in unserem Grundkörper $\mathbb{F}_q$ dieselbe Rechenzeit in Anspruch nehmen. Wir zählen also jede Addition und Multiplikation in $\mathbb{F}_q$ als eine Operation. Hieraus können wir alle weiteren Berechnungen zusammensetzen.
Für die Grundrechenarten von Polynomen gilt dann: Möchte man zwei Polynome vom Grad n und m mit $n \leq m$ addieren, so benötigt man dazu n Operationen.
Im Zuge des Programms berechnen wir $H_j(k)$ für alle k unterhalb einer gewissen Schranke x. Um $H(k)$ zu berechnen müssen wir zunächst φ_k berechnen und anschließend den Grad des größten gemeinsamen Teilers mit $I(k,q;T)$ bestimmen. Nach einer Addition erhalten wir schließlich $H_j(k)$.
Zunächst beschäftigen wir uns mit der Laufzeitanalyse zur Berechnung von φ_k:

$$\varphi(j) = j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j) - [k-1] \cdot \varphi_{k-2}(j)$$

$j^{\frac{q^{k-1}+(-1)^k}{q+1}}$ würde man normalerweise mittels Repeated Squaring berechnen. Im schlechtesten Fall müsste man $a_k := \left\lfloor log_2(\frac{q^{k-1}+(-1)^k}{q+1}) \right\rfloor$ Quadraturen berechnen. Da jedoch in diesem Fall $j = a \cdot T$ ist, kann man den Wert von $j^{\frac{q^{k-1}+(-1)^k}{q+1}}$ sofort angeben. Es gilt nähmlich: Ist $k-1$ gerade, so ist $a^{\frac{q^{k-1}+(-1)^k}{q+1}} = 1$ und somit $j^{\frac{q^{k-1}+(-1)^k}{q+1}} = T^{\frac{q^{k-1}+(-1)^k}{q+1}}$. Ist $k-1$ ungerade so ist $a^{\frac{q^{k-1}+(-1)^k}{q+1}} = a$ und somit $j^{\frac{q^{k-1}+(-1)^k}{q+1}} = a \cdot T^{\frac{q^{k-1}+(-1)^k}{q+1}}$. Dies zeigt, dass man die Berechnung von $j^{\frac{q^{k-1}+(-1)^k}{q+1}}$ vernachlässigen kann.
Die Multiplikation von $[k-1]$ mit $\varphi_{k-2}(j)$ benötigt weniger Operationen als die üblichen Multiplikationen, da $[k-1]$ nur aus zwei Summanden besteht. Es werden $2 \cdot \sum_{i=1}^{k-3} \chi(k+i) \cdot q^i + 1$ Operationen benötigt.
Hinzu kommen noch $\sum_{i=1}^{k-2} \chi(k+i) \cdot q^i + \frac{q^{k-1}+(-1)^k}{q+1} + 1$ Operationen für die Berechung von $j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j)$ sowie $\sum_{i=1}^{k-1} \chi(k+i) \cdot q^i$ Operationen für die Subtraktion $j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j) - [k-1] \cdot \varphi_{k-2}(j)$.
Zur Berechnung von $\varphi_k(j)$ benötigt man also insgesamt, wenn φ_{k-1} und φ_{k-2} bereits berechnet

sind,

$$2 \cdot \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i + 1 + \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i + \frac{q^{k-1} + (-1)^k}{q+1} + 1 + \frac{q^{k-1} + (-1)^k}{q+1} + \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i$$

Rechenoperationen.
Kommen wir nun zur Berechnung des größten gemeinsamen Teilers. Eine untere Schranke für diese Berechung ist durch den Theoretischen Knut-Schönhage Algorithmus gegeben. Man kann den größten gemeinsamen Teiler also im allgemeinen Fall nicht schneller als mit $O(n \cdot log(n))$ Operationen berechnen(siehe [BCS97] Seite 61-74). Der von Magma benutzte Algorithmus benötigt $O(n \cdot log(n) \cdot log(log(n)))$ Operationen. Der verwendete Algorithmus ist der sogenannte „half-GCD“ Algorithmus (vgl. [AHU75] Seite 303-310). Dieser benötigt eine Laufzeit, die mit $O(M(n))$ anwächst. Hierbei ist $M(n)$ die Komplexität der Polynommultiplikation. Magma benutzt die schnelle Fouriertransformation (fast fourier transformation, FFT) zur Multiplikation zweier Polynome (siehe [BCS97] Seite 32-34). Dieser hat eine Komplexität von $M(n) = n \cdot log(n) \cdot log(log(n))$.
Diese Überlegungen zeigen, dass dieses Programm im Mittel $\sum_{k=2}^{x}(2 \cdot \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i + 1 + \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i + \frac{q^{k-1}+(-1)^k}{q+1} + 1 + \frac{q^{k-1}+(-1)^k}{q+1} + \sum_{i=1}^{k-1} \chi(k+i) \cdot q^i + O(q^k \cdot log(q^k) \cdot log(log(q^k))))$ Operationen benötigt. Folglich wächst die Laufzeit mit $O(q^x \cdot log(q^x) \cdot log(log(q^x)))$ an. Stoppt man die Laufzeit des Programm läuft, so stellt man fest, dass es für kleine k nur wenige Sekunden zur Berechnung von $H(k)$ benötigt, während für große k die Berechnung eines Funktionswertes von $H(k)$ bis zu 20 Minuten dauern kann. Ein k heißt in diesem Fall groß, wenn $q^k \approx 1.000.000$.

4.4 Ergebnisse und Hypothesen

In diesem Abschnitt möchte ich meine berechneten Ergebnisse in Form von Graphen darstellen. Dazu wird $H_j(x)$ in Abhängigkeit von $x := grad(f)$ aufgetragen. Die Werte werden mit einer Bestkurve angenähert. Diese ist in den Graphen rot eingezeichnet. In den Kästchen im oberen linken Rand steht für jeden Graphen die Formel der Bestkurve und die Werte der einzelnen Pararmeter A_1, $t1$ und y_0 mit den zugehörige Standardabweichung. Die Bestkurve ist in unserem Fall immer von der Form $A_1 \cdot e^{(\frac{x}{t1})} + y_0$. Diese Graphen wurden mit der Software OrignPro 7.5 erstellt, die Bestkurven sowie die Extrapolationen am Ende des Kapitels wurden ebenfalls mit diesem Programm berechnet.

Hypothesen:

4.4.1 Bemerkung:
Magma bezeichnet für nicht prime q den Erzeuger der zyklischen Gruppe $\mathbb{F}_q^*$ mit $F.1$. Diese Bezeichnung möchte ich im Folgenden auch verwenden.

Sei j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik 2.
Nach unseren Berechnungen gibt es supersinguläre Paare (j, f) nur, wenn $grad(f)$ gerade ist. Zu

geraden k gibt es immer $\mathbb{F}_q$ vom Grad k, für die j supersingulär ist. Man kann jedoch kein spezielles Muster erkennen, wie viele supersinguläre Stellen bei jedem Zweierschritt hinzukommen.

4.4.2 Vermutung:

Ist j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik 2, dann gibt es supersinguläre Paare (j, f) genau dann, wenn $grad(f)$ gerade ist.

Trägt man H_j in Abhängigkeit von $x := grad(f)$ auf, so stellt man fest, dass man H_j relativ gut durch eine Exponentialfunktion der Form $A_1 \cdot e^{(\frac{x}{t1})} + y_0$ annähern kann, wie die Abbildungen 4.1 bis 4.3 zeigen.

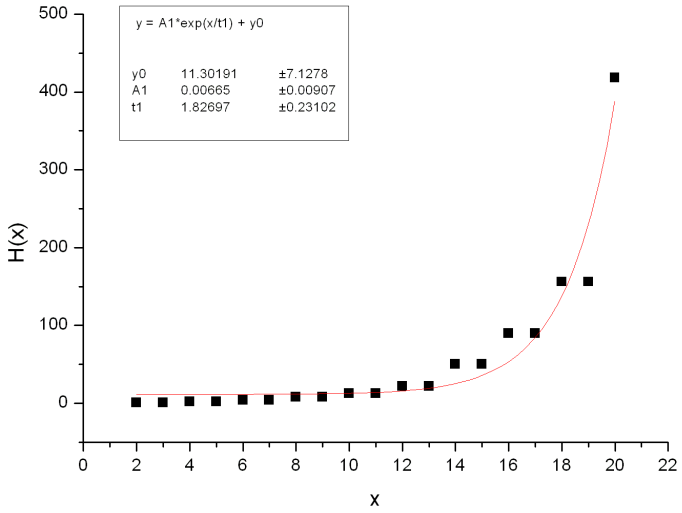

Abbildung 4.1: $q = 2$, $j = 1$

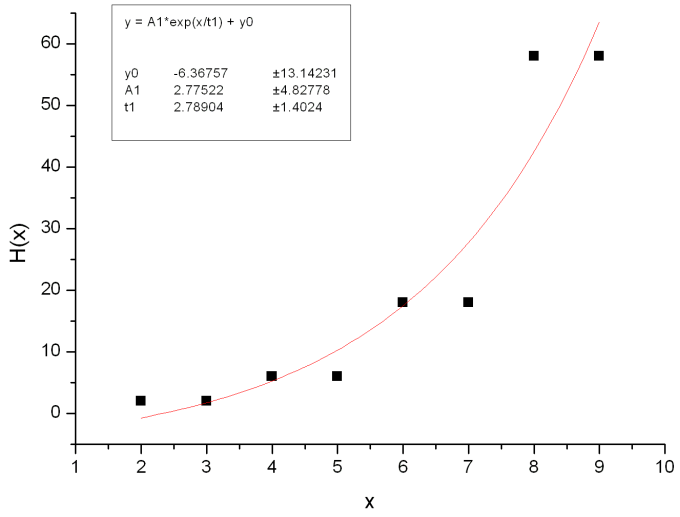

Abbildung 4.2: $q = 4$, $j = 1$

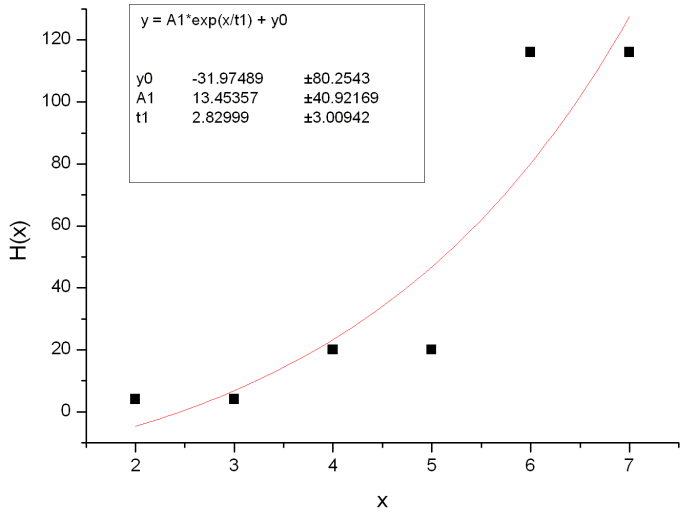

Abbildung 4.3: $q = 8$, $j = 1$

Trägt man jedoch nur die geraden Funktionswerte auf, so wird die Approximation viel besser. Dies belegen die Graphen 4.4 bis 4.6.

4.4.3 Vermutung:

Ist j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik 2, so wächst die Funktion H_j exponentiell, wenn man nur die geraden Funktionswerte betrachtet.

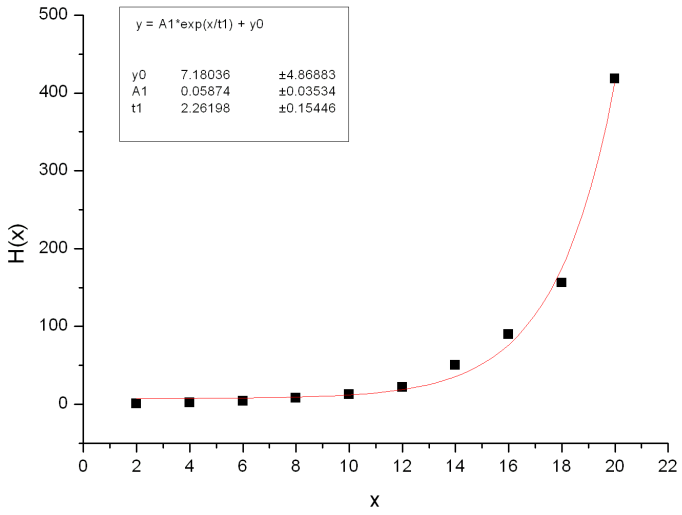

Abbildung 4.4: $q = 2$, $j = 1$

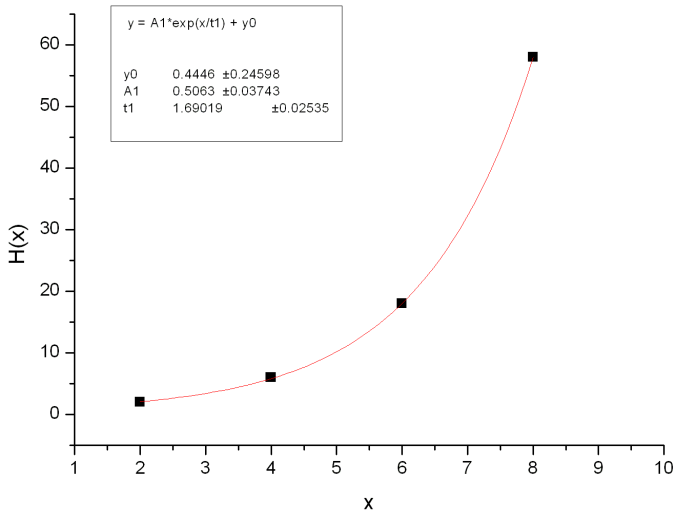

Abbildung 4.5: $q = 4$, $j = 1$

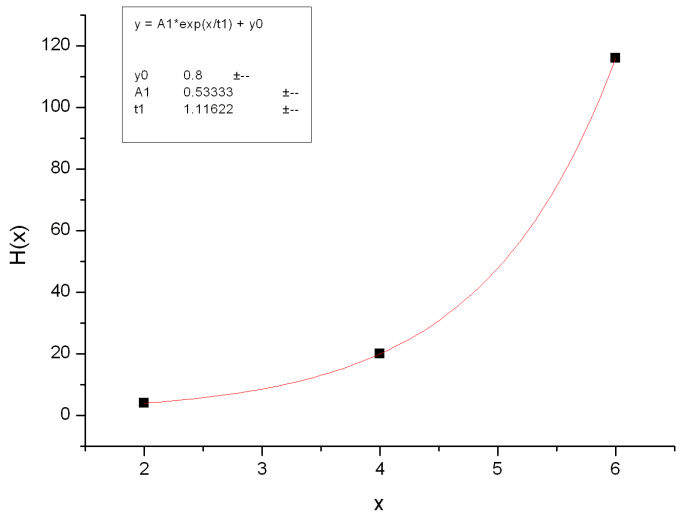

Abbildung 4.6: $q = 8$, $j = 1$

Sei j konstant und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik > 2. Wie die Graphen 4.7 bis 4.9 zeigen, kommen im Fall Charakteristik 3 erst ab $x = 3$ supersinguläre Stellen hinzu. Bei Charakteristik 5 sind die ersten supersingulären Stellen bei $x = 5$ und bei Charakteristik 7 bei $x = 7$. Für den Fall $q = 3$ gibt es einen erneuten Sprung bei $x = 9$. Es lässt sich vermuten, dass in Körpern mit Charakteristik $\neq 2$ nur bei Vielfachen der Charakteristik supersinguläre Stellen hinzukommen. Wahrscheinlich sogar nur bei Potenzen der Charakteristik. Leider konnten keine Berechnungen durchgeführt werden, die diese Aussage unterstützen, da dies die Rechenkapazität von Magma übersteigt.

4.4.4 Vermutung:

Ist j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik > 2, so kommen nur supersinguläre Stelle hinzu, wenn x ein Vielfaches der Charakteristik ist.

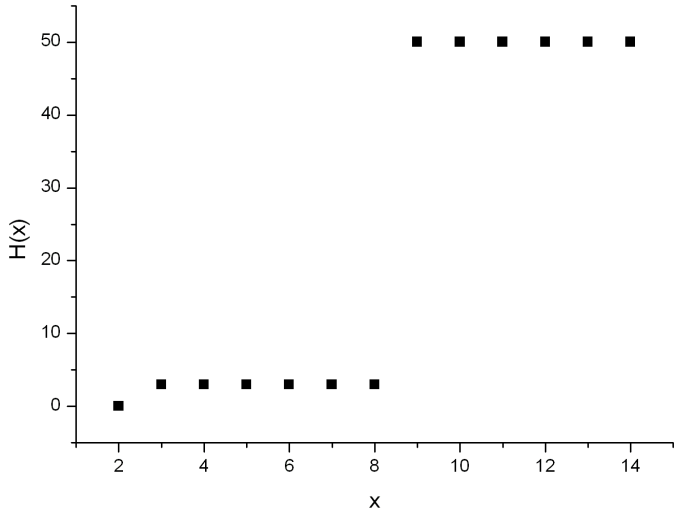

Abbildung 4.7: $q = 3$, $j = 1$

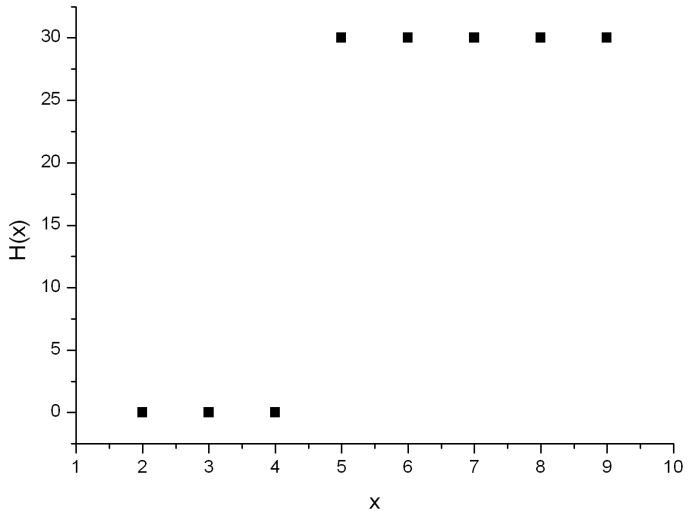

Abbildung 4.8: $q = 5$, $j = 1$

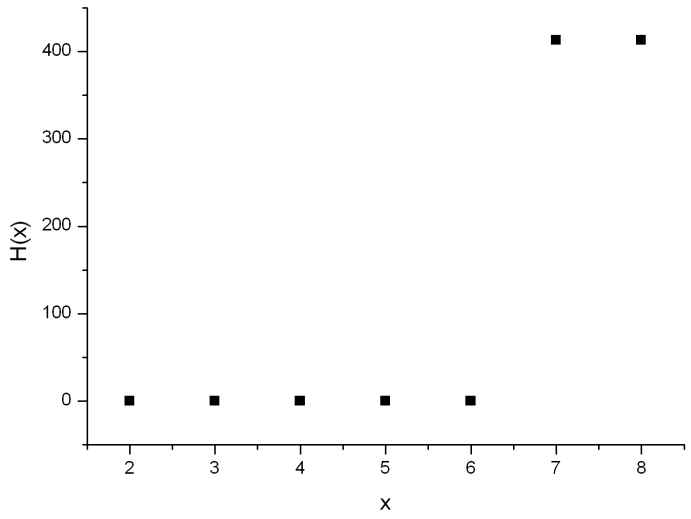

Abbildung 4.9: $q = 7$, $j = 1$

4.4.5 Vermutung:
Allgemein kann man feststellen, dass für konstante j gilt:
$\varphi_k(j) \neq 0$ *modulo* $\mathfrak{p}$ *für alle* $\mathfrak{p}$*, wenn* $k \leq char(\mathbb{F}_q) - 1$.

Trägt man für nicht konstantes j und feste q die Werte von H für alle $j = a \cdot T$ mit $a \in \mathbb{F}_q^*$ in einem Koordinatensystem auf, so stellt man fest, dass H für manche j schneller wächst als für andere. Man kann vermuten, dass es sich hierbei nicht nur um eine statistische Abweichung handelt, sondern dass sich dieser Trend auch für $x \to \infty$ fortsetzt. Für welche a unser H schneller wächst kann man jedoch nicht so leicht vermuten. Was man vermuten kann ist, dass $j = a \cdot T$ für $a = \pm 1$ tendenziell zu der schneller wachsenden Gruppe gehört.

4.4.6 Vermutung:
Ist $j = a \cdot T$, so wächst H_j für manche $a \in \mathbb{F}_q$ schneller als für andere.

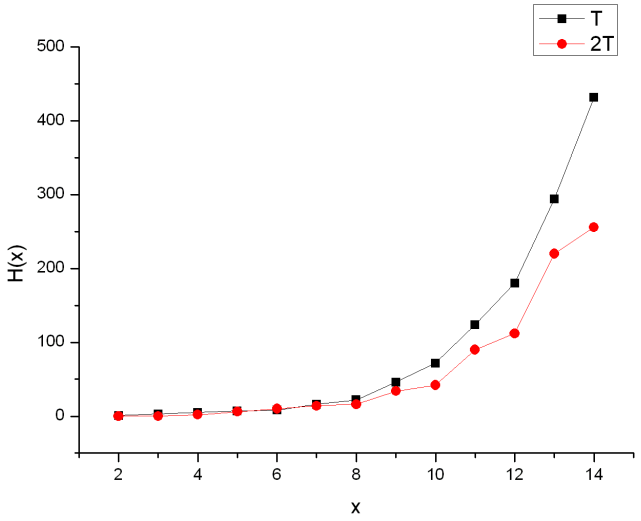

Abbildung 4.10: $q = 3$

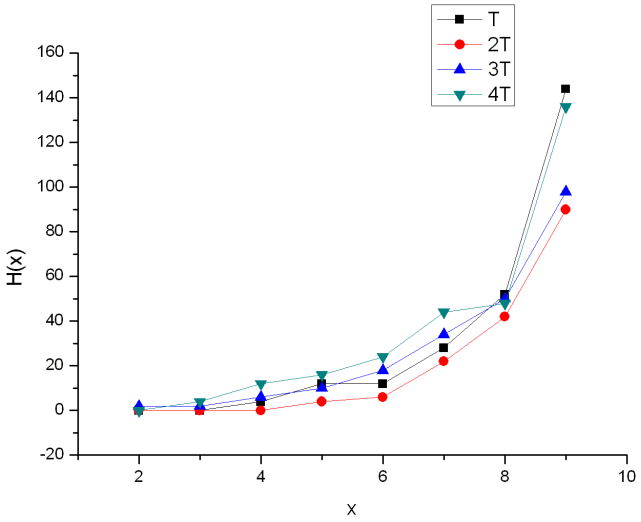

Abbildung 4.11: $q = 5$

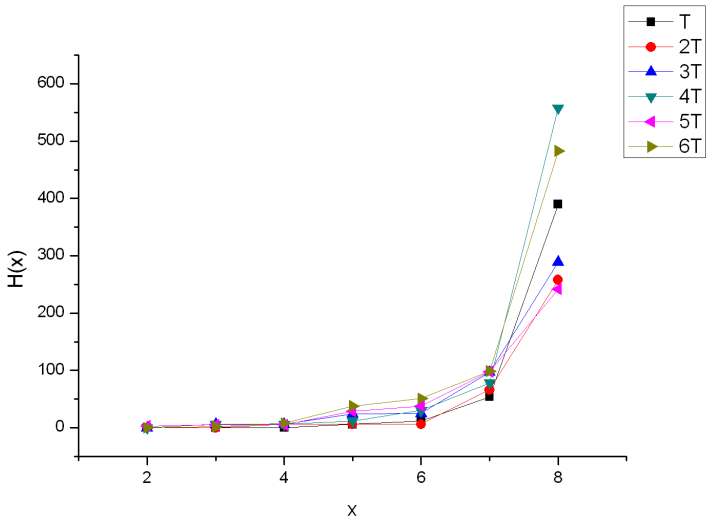

Abbildung 4.12: $q = 7$

Trägt man wie eben alle Werte in denselben Graphen ein, so kann man ein obere und untere Schranke ermitteln. Diese erhält man, indem man in jedem Wert x das Minimum und das Maximum bildet. Diese Minimums- bzw. Maximumsfunktionen lassen sich gut durch eine Exponentialfunktion approximieren, wie die Graphen 4.13 bis 4.22 zeigen.

4.4.7 Vermutung:

Die Funktion H_j verläuft für alle nicht konstanten j zwischen zwei Exponentialfunktionen.

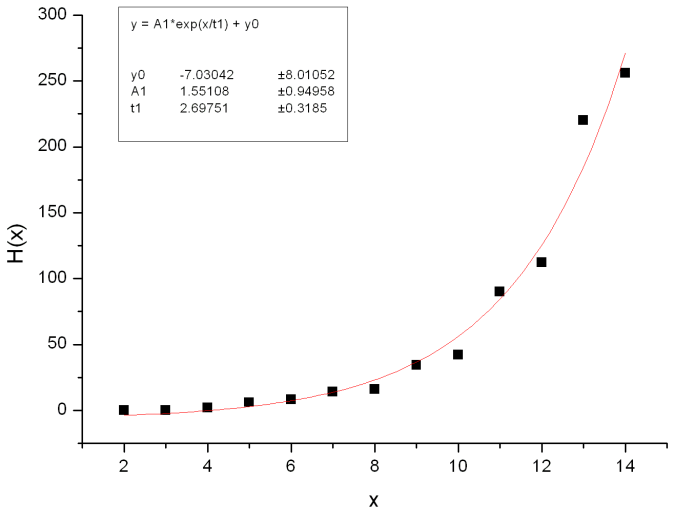

Abbildung 4.13: $q = 3$, Minimum

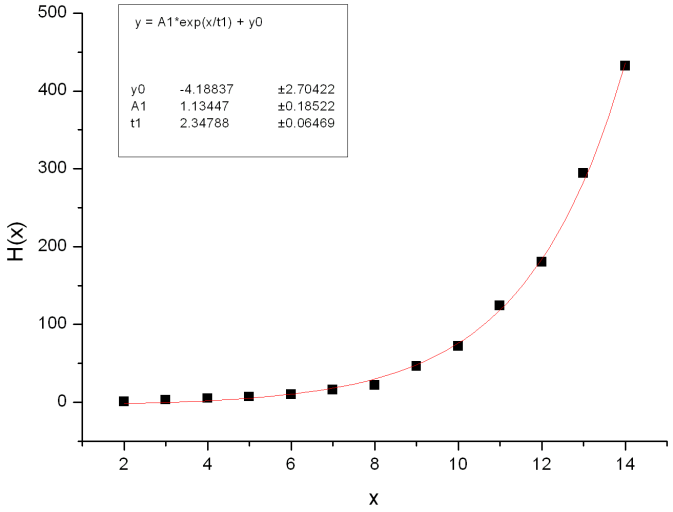

Abbildung 4.14: $q = 3$, Maximum

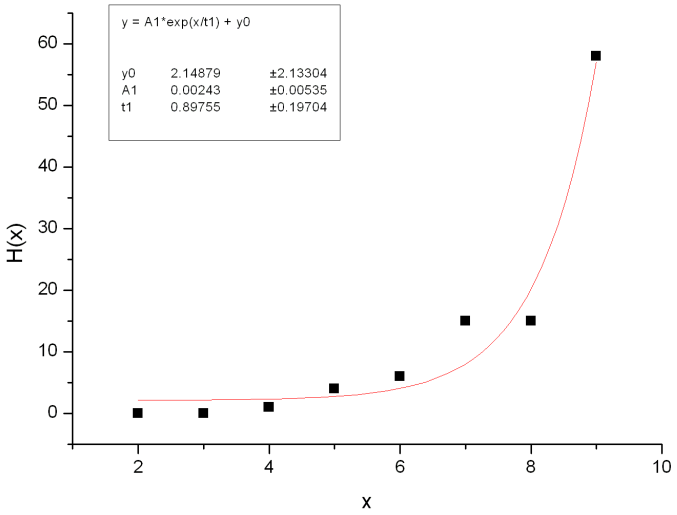

Abbildung 4.15: $q = 4$, Minimum

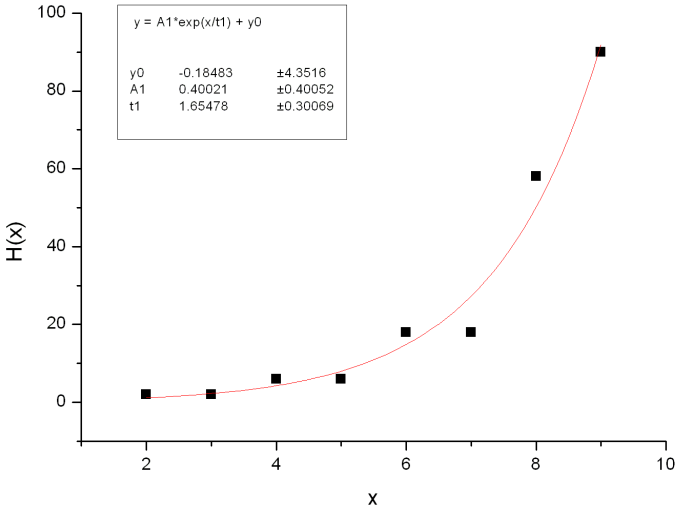

Abbildung 4.16: $q = 4$, Maximum

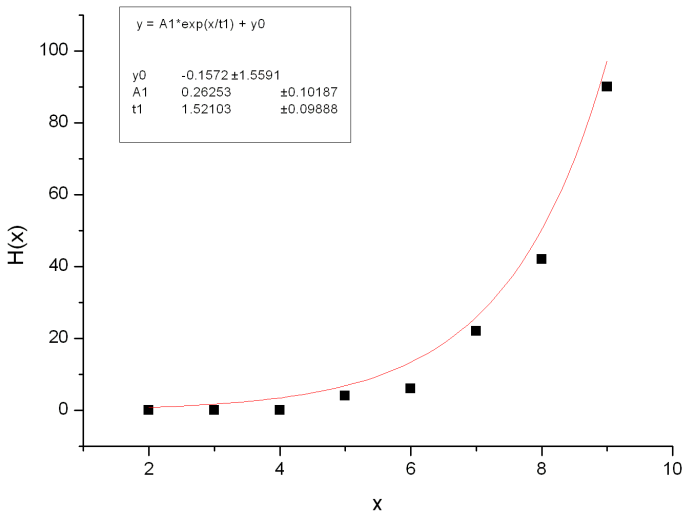

Abbildung 4.17: $q = 5$, Minimum

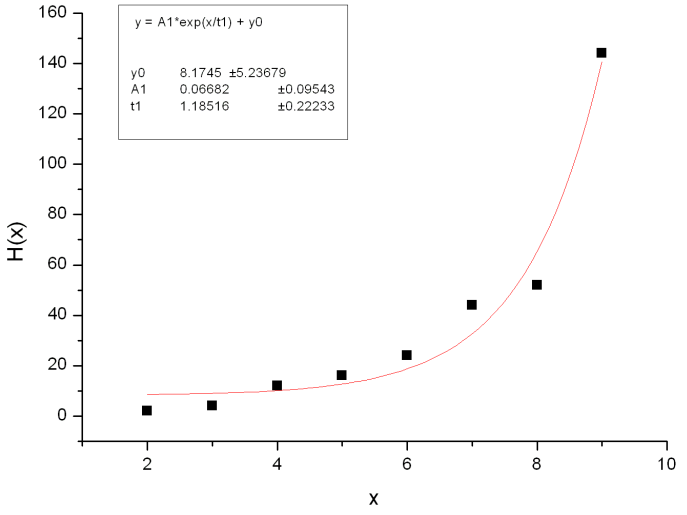

Abbildung 4.18: $q = 5$, Maximum

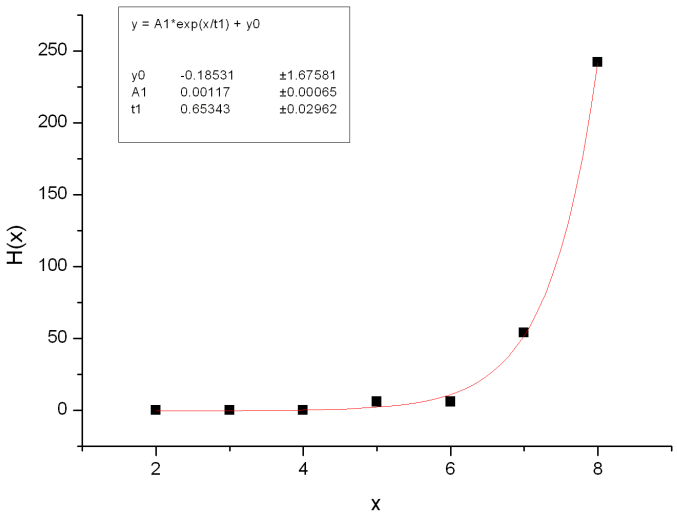

Abbildung 4.19: $q = 7$, Minimum

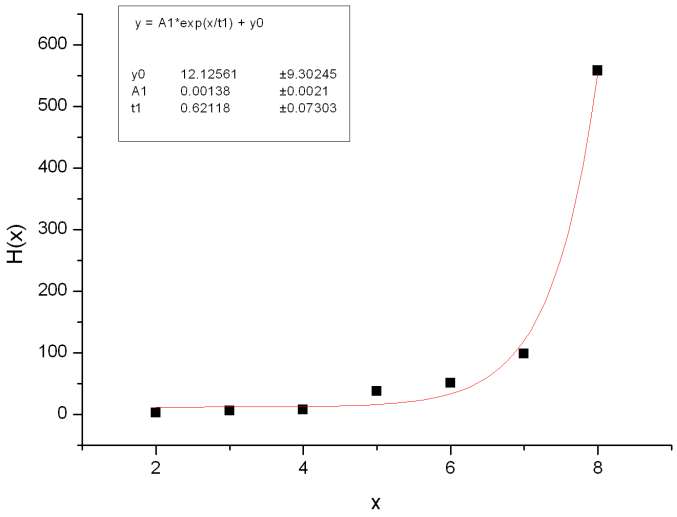

Abbildung 4.20: $q = 7$, Maximum

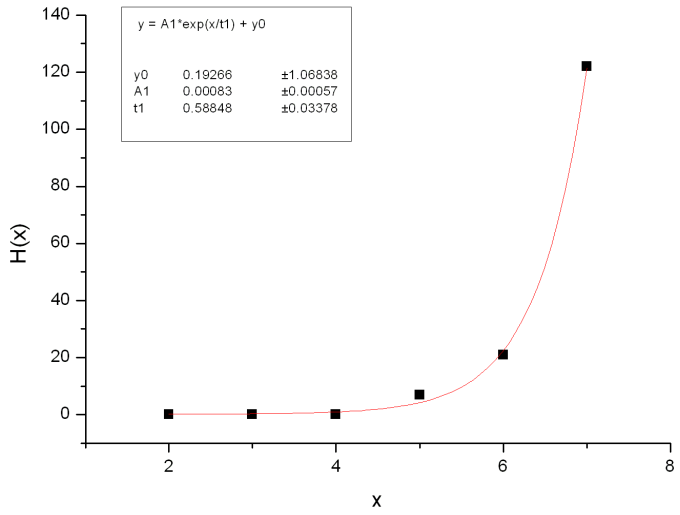

Abbildung 4.21: $q = 8$, Minimum

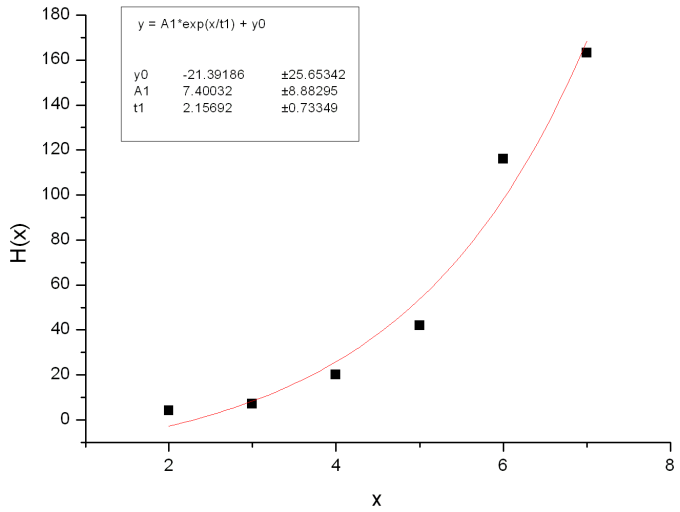

Abbildung 4.22: $q = 8$, Maximum

Ist weiterhin j nicht konstant, so kann man $H(x)$ gut durch eine Exponentialfunktion der Form $A_1 \cdot e^{(\frac{x}{t1})} + y_0$ annähern, wie die Graphen 4.23 bis 4.40 zeigen.

4.4.8 Vermutung:

Für nicht konstantes j wächst H_j exponentiell. Es gilt: t_1 ist unabhängig von j.

Man kann vermuten, dass t_1 nur von q abhängt und y_0 für große x keine Rolle mehr spielt. Je größer q wird, desto schneller wächst H_j, somit ist t_1 streng monoton fallend mit q. Die genaue Abbhängigkeit wird später näher untersucht.

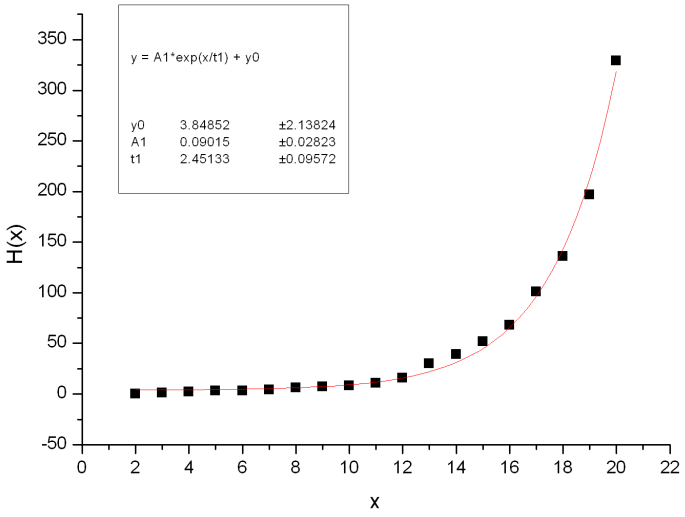

Abbildung 4.23: $q = 2$, $j = T$

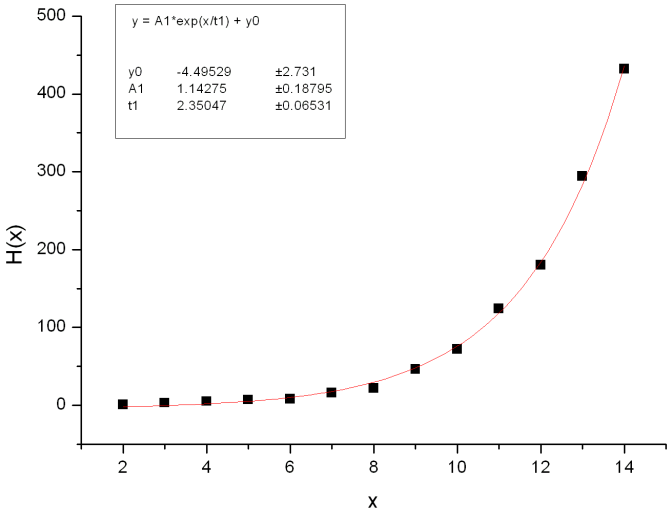

Abbildung 4.24: $q = 3$, $j = T$

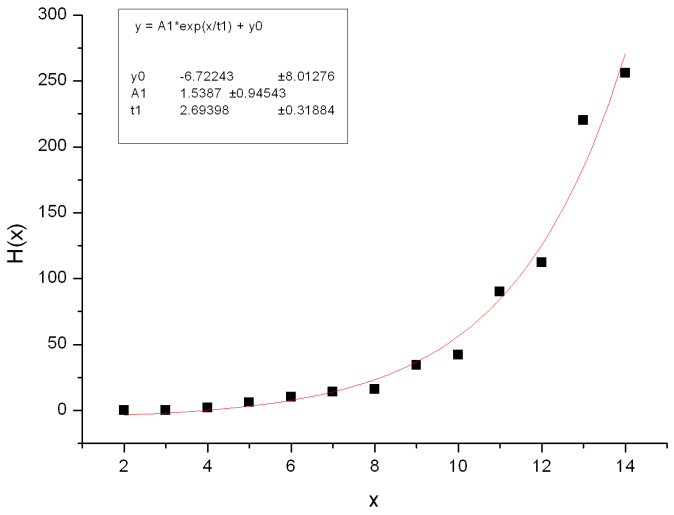

Abbildung 4.25: $q = 3$, $j = 2 \cdot T$

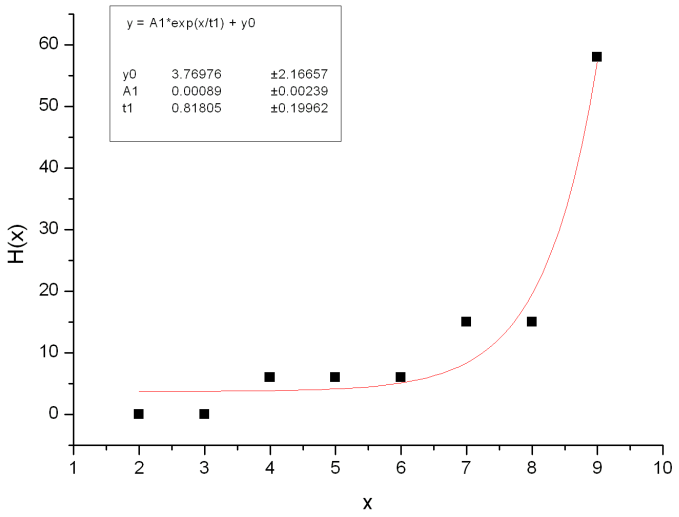

Abbildung 4.26: $q = 4$, $j = T$

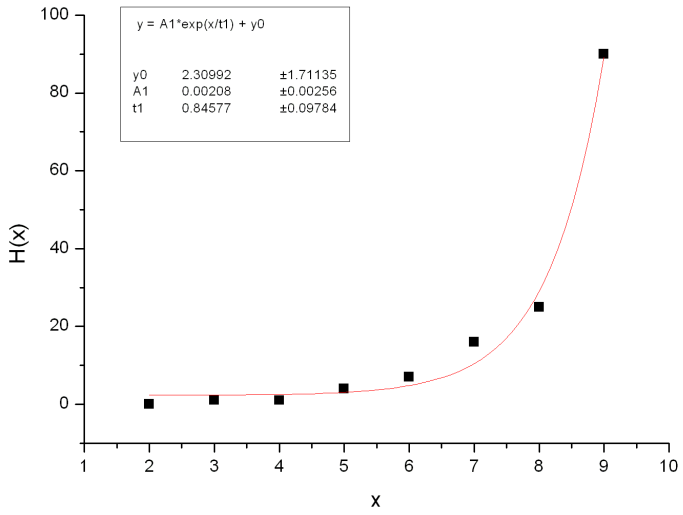

Abbildung 4.27: $q = 4$, $j = F.1 \cdot T$

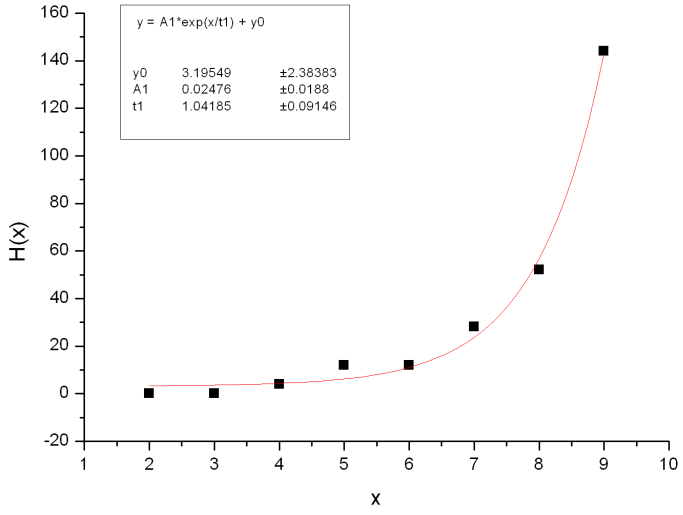

Abbildung 4.28: $q = 5$, $j = T$

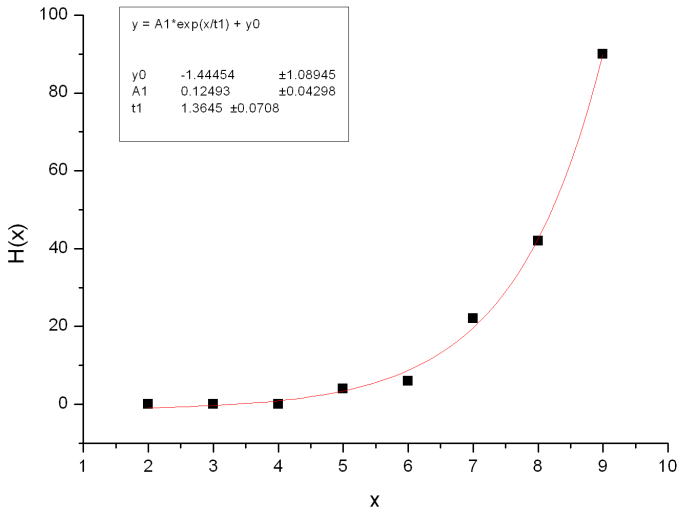

Abbildung 4.29: $q = 5$, $j = 2 \cdot T$

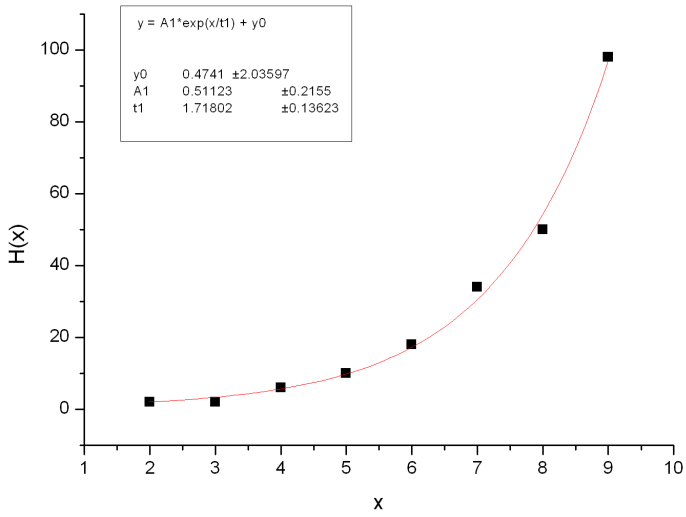

Abbildung 4.30: $q = 5$, $j = 3 \cdot T$

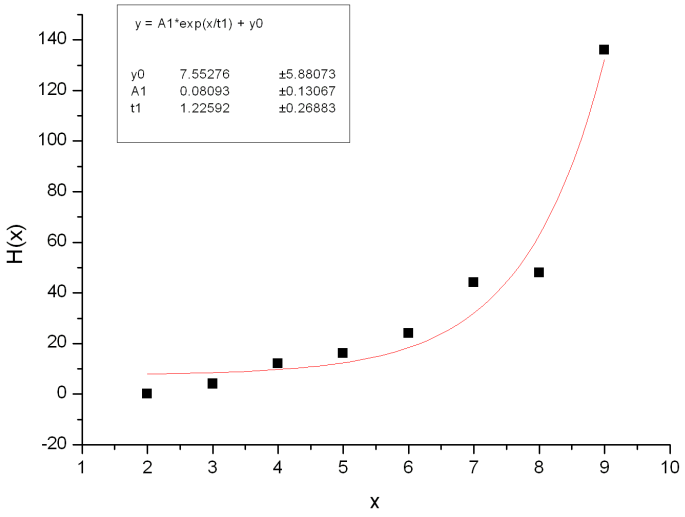

Abbildung 4.31: $q = 5$, $j = 4 \cdot T$

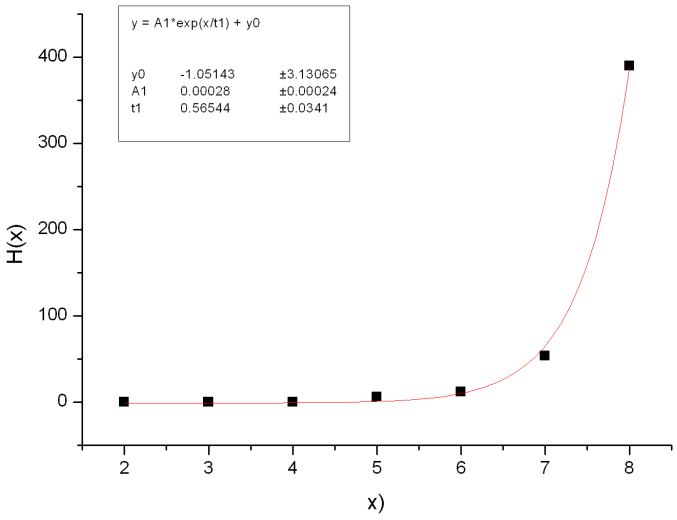

Abbildung 4.32: $q = 7$, $j = T$

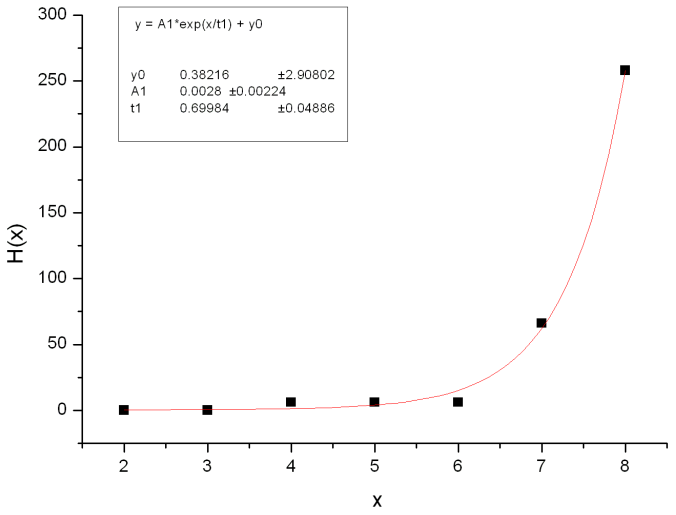

Abbildung 4.33: $q = 7$, $j = 2 \cdot T$

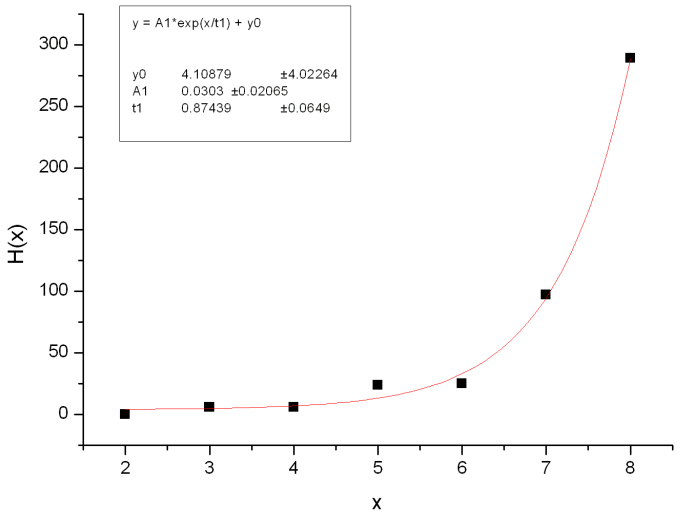

Abbildung 4.34: $q = 7$, $j = 3 \cdot T$

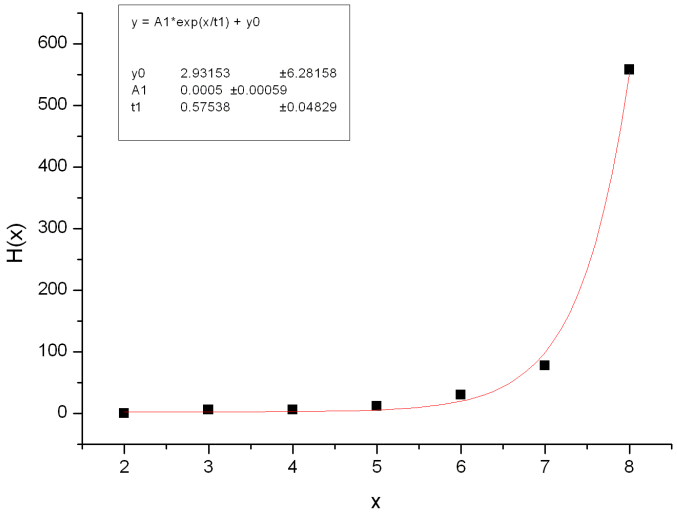

Abbildung 4.35: $q = 7$, $j = 4 \cdot T$

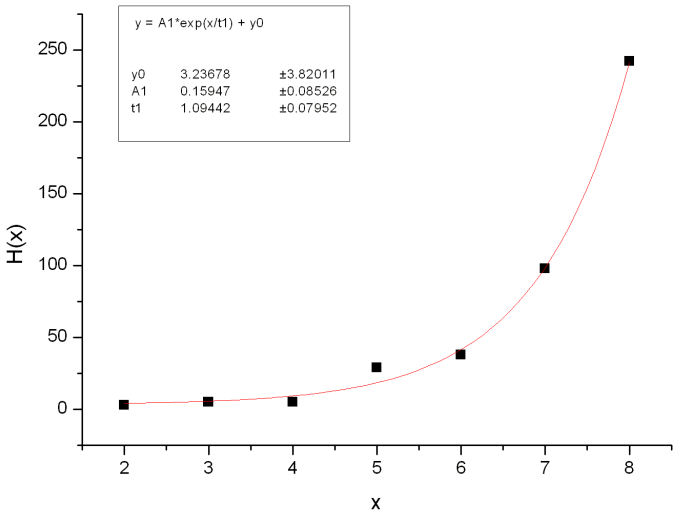

Abbildung 4.36: $q = 7$, $j = 5 \cdot T$

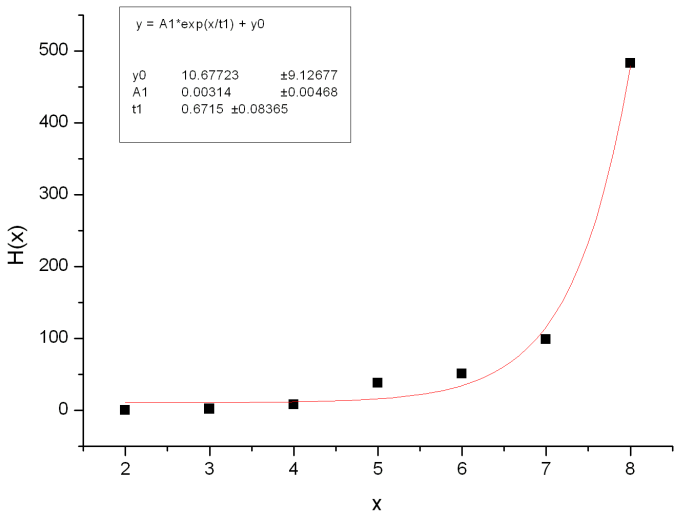

Abbildung 4.37: $q = 7$, $j = 6 \cdot T$

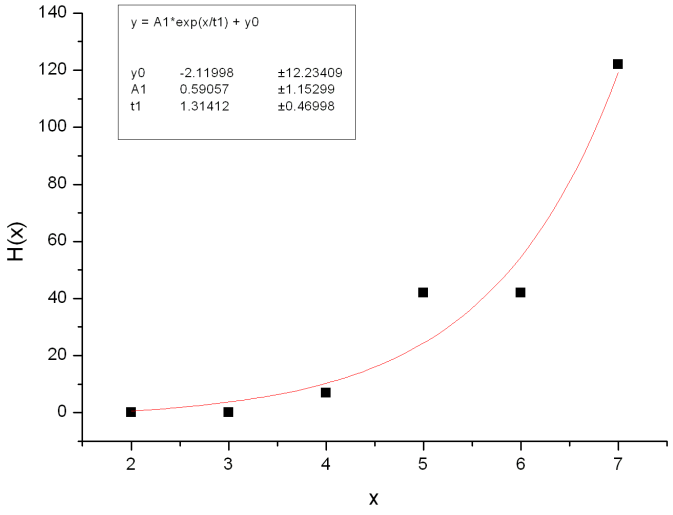

Abbildung 4.38: $q = 8$, $j = T$

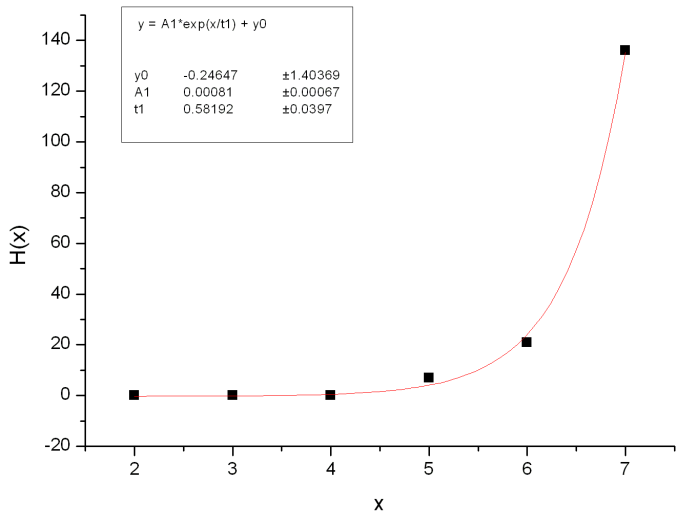

Abbildung 4.39: $q = 8$, $j = F.1^2 \cdot T$

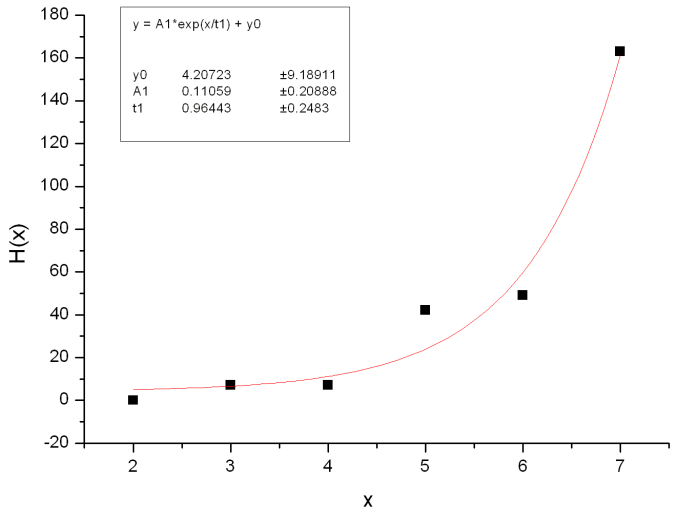

Abbildung 4.40: $q = 8$, $j = F.1^3 \cdot T$

4.4.9 Vermutung:

Die Funktion H_j ist von der Form $A_1 \cdot e^{(\frac{x}{t_1})}$, wobei $t_1 = \frac{c}{ln(q)}$ für eine Konstante c ist.

Wie diese Tabelle zeigt, ist der Mittelwert über alle t_1 für ein festes q ungefähr $t_1 = \frac{c}{ln(q)}$, wobei $c \in [1; 2,771]$. Bei der Mittelwertbildung wurden diejenigen t_1, die wegen der Galoisinvarianz 4.1.2 mehrfach vorkommen, einfach gezählt.

q	Mittelwert von t_1 für festes q	t_1 als Funktion von q
2	$2,45133$	$\frac{1,699}{ln(2)}$
3	$2,522225$	$\frac{2,771}{ln(3)}$
4	$0,72$	$\frac{1,000}{ln(4)}$
5	$1,3375725$	$\frac{2,150}{ln(5)}$
7	$0,746825$	$\frac{1,453}{ln(7)}$
8	$0,8605$	$\frac{1,789}{ln(8)}$

Es lässt sich vermuten, dass t_1 nur von $ln(q)$ abhängt, wenn man $H(x)$ für $x \to \infty$ betrachtet. Man kann nun noch H_j anhand der berechneten Daten extrapolieren, um einen Einblick zu erhalten wie H_j für $x \to \infty$ weiterverläuft, wenn man annimmt, dass die Funktion sich weiterhin wie auf dem berechneten Intervall verhält. Für $q = 2$ und $j = 1$ ergibt die Extrapolation $H(x) = 0,02196 \cdot e^{0,4928 \cdot x}$.

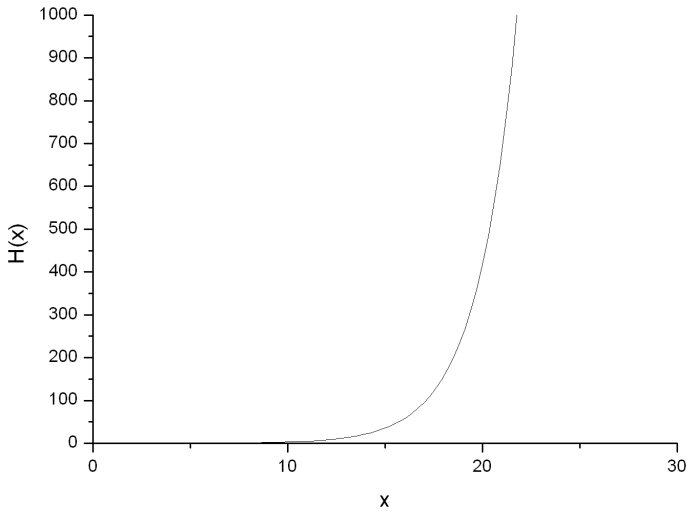

Abbildung 4.41: $q = 2$ $j = 1$

Die Extrapolation berechneten Werte für alle betrachteten j kann man folgender Tabelle entnehmen:

q	j	A_1	t_1
2	T	$0,436$	$3,134$
3	T	$0,554$	$2,074$
3	$2T$	$0,488$	$2,174$
4	T	$0,732$	$2,332$
4	$F.1 \cdot T$	$0,0746$	$2,331$
4	$F.1^3 \cdot T$	$0,0037$	2.0688
5	T	$0,3002$	$1,52$
5	$2T$	$0,0596$	$2,069$
5	$3T$	$0,5447$	$1,7098$
5	$4T$	0.886	$1,94943$
7	T	$0,0038$	$0,713$
7	$2T$	$0,0535$	$1,007$
7	$3T$	$0,371$	$1,261$
7	$4T$	$0,211$	$1,1883$
7	$5T$	$0,48665$	$1,324$
7	$6T$	$0,1321$	0.992
8	T	$0,314$	$0,768$
8	$F.1 \cdot T$	$0,0037$	$0,6744$
8	$F.1^3 \cdot T$	$0,45$	$1,2133$

Man stellt fest, dass die Werte für t_1 für ein festes q, im Vergleich zu den Werten von A_1, relativ dicht zusammenliegen. Die berechneten Werte von t_1 weichen stark von $\frac{1}{ln(q)}$ ab. Um die Abhängigkeit von t_1 von q zu bestimmen, müssten also weitere Untersuchungen für größere x durchgeführt werden. Größere Werte für x würden jedoch die Rechenleistung der von mir verwendeten Magma-Version übersteigen.

In diesem Kapitel haben wir also gesehen, dass sich H_j für nicht konstante j vermutlich asymptotisch wie eine Exponentialfunktion verhält. Des Weiteren wächst H_j für manche j schneller als für andere. Bei der genauen Bestimmung von der Koeffizienten A_1 und t_1 besteht noch Forschungsbedarf.

Kapitel 5

Supersinguläre Stellen Irreduzibler Polynome

In diesem Kapitel beschäftigen wir uns mit den folgenden Fragestellungen:

- Welchen Wert hat $\sum_{\mathfrak{p}\ grad(\mathfrak{p})=d} |\{(g,\Delta) \mid (g,\Delta) \text{ ist supersingulär mod } \mathfrak{p}\}|$?
- Sei $\mathfrak{p}$ fest gewählt vom Grad d. Wie viele supersinguläre Paare (g,Δ) gibt es mod $\mathfrak{p}$?

5.1 Vorüberlegungen

Die Berechnungen mit Magma haben ergeben, dass relativ viele irreduzible Polynome gleichviele supersinguläre j-Werte haben. Um dies etwas besser zu verstehen, zunächst ein paar Vorüberlegungen.

5.1.1 Satz:
Die Gruppe G operiert auf der Menge X, es sei $x \in X$. Dann gilt:
$|G| = |O_x| \cdot |G_x|$, *wobei $|O_x|$ die Bahn von x unter G ist und G_x die Untergruppe von G, die x invariant lässt (siehe [SP07], Seite 121, Satz 6.5).*

Die Gruppe der affinen Transformationen operiert auf der Menge der Primideale. Insbesondere operieren somit auch ihre Untergruppen auf dieser Menge. Die Fixkörper dieser Untergruppen sind für das weitere Vorgehen von großem Interesse. Haben wir diese bestimmt, so können wir die Länge der einzelnen Bahnen bestimmen und angeben, welche Polynome diese Länge haben. Gibt man sich etwas mehr Mühe, so kann man sogar die Anzahl der Bahnen einer bestimmten Länge angeben.

5.1.2 Satz:
Sei $q = p^m$ und $r \in \mathbb{N}$ ein Teiler von m, sowie n ein Teiler von $(q-1)$.
Betrachtet man den Polynomring $\mathbb{F}_q[T]$, so gilt:
Der Fixring der Untergruppe $G_{p^r} := \{f$ ist affine Transformation $\mid f(T) = T + b,\ b \in \mathbb{F}_q$ mit $b^{p^r} = b\}$ der affinen Gruppe ist $\mathbb{F}_q[T^{p^r} - T]$.
Der Fixring der Untergruppe $G_n := \{f$ ist affine Transformation $\mid f(T) = a \cdot T,\ a \in \mathbb{F}_q$ mit $a^n = 1\}$

der affinen Gruppe ist $\mathbb{F}_q[T^n]$.
Der Fixring der Untergruppe
$G_{np^r} := \{f \text{ ist affine Transformation} \mid f(T) = a \cdot T + b,\ a, b \in \mathbb{F}_q \text{ mit } b^{p^r} = b,\ a^{p^r} = a \text{ und } a^n = 1\}$
der affinen Gruppe ist $\mathbb{F}_q[(T^{p^r} - T)^n]$.

Beweis:

$$\begin{array}{c} \mathbb{F}_q(T) \\ | \\ \mathbb{F}_q(T)^{G_{p^r}} \\ | \\ \mathbb{F}_q(T^{p^r} - T) \end{array}$$

Offensichtlich bleiben die Elemente von $\mathbb{F}_q[T^{p^r} - T]$ unter den Transformationen von G_{p^r} fix. Somit ist der Fixkörper $\mathbb{F}_q(T)^{G_{p^r}}$ eine Körpererweiterung des zu $\mathbb{F}_q[T^{p^r} - T]$ gehörigen Quotientenkörpers $\mathbb{F}_q(T^{p^r} - T)$. Der Körper $\mathbb{F}_q(T)$ hat als Körpererweiterung von $\mathbb{F}_q(T^{p^r} - T)$ den Grad p^r und als Körpererweiterung von $\mathbb{F}_q(T)^{G_{p^r}}$ nach Satz 1.3.3 Grad $|(G_{p^r})| = p^r$. Somit hat $\mathbb{F}_q(T)$ als Körpererweiterung beider Körper denselben Grad, deshalb stimmen diese überein. Da die Quotientenkörper übereinstimmen, muss dies auch für die Ganzheitsringe gelten und es folgt, dass $\mathbb{F}_q[T^{p^r} - T]$ der Fixring der Gruppe G_{p^r} ist, wie folgendes Argument zeigt:

$$\begin{array}{cc} \mathbb{F}_q[T] & L := \mathbb{F}_q(T) \\ | & | \\ \mathbb{F}_q[T^{p^r} - T] & K := \mathbb{F}_q(T^{p^r} - T) \end{array}$$

$\mathbb{F}_q[T]$ ist ganz über $\mathbb{F}_q[T^{p^r} - T]$, da das Minimalpolynom von T Koeffizienten in $\mathbb{F}_q[T^{p^r} - T]$ hat. Also ist $\mathbb{F}_q[T]^G = \mathbb{F}_q(T^{p^r} - T) \cap \mathbb{F}_q[T]$ ganz über $\mathbb{F}_q[T^{p^r} - T]$. Da $\mathbb{F}_q[T^{p^r} - T]$ ganz abgeschlossen ist, ist $\mathbb{F}_q[T^{p^r} - T] = \mathbb{F}_q[T]^G$. □

Man überlegt sich leicht, dass die im Satz behandelten Gruppen die einzigen Untergruppen der affinen Gruppe sind. Dann zeigt Satz 5.1.1, dass die Bahnen unter den affinen Transformationen der irreduziblen Polynome, die in keinem dieser Fixkörper vorkommen, die volle Länge $q \cdot (q-1)$ haben, während die Polynome, die in einem dieser Fixkörper liegen, eine kürzere Länge besitzen. Elemente des Rings $\mathbb{F}_q[(T^{p^r} - T)^n]$ haben die Bahnlänge $\frac{q \cdot (q-1)}{n \cdot p^r}$, Elemente des Rings $\mathbb{F}_q[T^n]$, die nicht in $\mathbb{F}_q[(T^{p^r} - T)^n]$ enthalten sind, haben Bahnlänge $\frac{q \cdot (q-1)}{n}$ und Elemente, die in $\mathbb{F}_q[T^{p^r} - T]$ aber nicht in $\mathbb{F}_q[(T^{p^r} - T)^n]$ enthalten sind, haben die Länge $\frac{q \cdot (q-1)}{p^r}$. Die meisten Elemente von $\mathbb{F}_q[T]$ haben jedoch volle Bahnlänge. Ist der Grad s der irreduziblen Polynome kein Teiler von $q \cdot (q-1)$, so haben alle irreduziblen Polynome volle Länge, da sie sich weder als Polynome in der Variablen T^n noch in $T^{p^r} - T$ schreiben lassen. Ist $q \cdot (q-1)$ nur durch ein n oder p^r teilbar, so muss man nur einen Fall betrachten.
Nun bleibt noch die Frage zu beantworten, wie viele Bahnen einer bestimmten Länge es gibt. Wie

wir gerade gesehen haben, ist dies gleichbedeutend mit der Fragestellung, wie viele irreduziblen Polynome $f(T)$ vom Grad s es gibt, die sich als ein Primideal $h(T^{p^r}-T)$, bzw. $h(T^n)$ oder $h((T^{p^r}-T)^n)$ schreiben lassen.
Da die irreduziblen Polynome von $\mathbb{F}_q[T]$ die Primideale von $\mathbb{F}_q[T]$ erzeugen, kann man diese Frage auch anders formulieren. Wie viele Primideale vom Grad s in $\mathbb{F}_q[T^{p^r}-T]$ bzw. $\mathbb{F}_q[T^n]$ bzw. $\mathbb{F}_q[(T^{p^r}-T)^n]$ sind in $\mathbb{F}_q[T]$ prim?
Sei im Folgenden **s der Grad des irreduziblen Polynoms** $f(T)$.

Situation 1

Wir haben also folgende Situation: Wir betrachten die Körpererweiterung $L \mid K$ vom Grad n mit den zugehörigen Ganzheitsringen, wobei $Y := T^n$.

$$\begin{array}{ll} \mathbb{F}_q[T] & L := \mathbb{F}_q(T) \\ \Big| & \Big|{\scriptstyle n} \\ \mathbb{F}_q[Y] & K := \mathbb{F}_q(Y) \end{array}$$

Da Y für $Y = 0$ oder ∞ verzweigt ist, sei unser Primideal $\mathfrak{p} = (f(Y))$ aus $\mathbb{F}_q[Y]$ von der Form $\mathfrak{p} \neq 0, \infty$ und vom Grad $d := \frac{s}{n}$.

5.1.3 Heuristik:
Es gibt $N_q(d) - \sum_{n'|n} \frac{\varphi(n')}{d}$ *viele Primideale von Grad d, die nicht zerfallen.*

Begründung: In L lässt sich $\mathfrak{p}$ als $\mathfrak{p} = \prod_{1 \leq i \leq g} \mathfrak{q}_i$ schreiben. Dabei sind die auftretenden Primideale $\mathfrak{q}_i$ genau diejenigen Primideale von $\mathbb{F}_q[T]$, die über $\mathfrak{p}$ liegen, vgl. Satz 1.4.2. $K_\mathfrak{p}$ sei im Folgenden $\mathbb{F}_q(Y)/\mathfrak{p}$, y ist die Restklasse von Y in $K_\mathfrak{p}$ und $K_\mathfrak{q}$ die Körpererweiterung zu $K_\mathfrak{p}$, die durch ziehen der n-ten Wurzel aus $0 \neq y \in K_\mathfrak{p}$ entsteht. Es gilt die Gleichung $n = e \cdot f \cdot g = f \cdot g$ mit den Bezeichnungen aus Satz 1.4.4.
Wie wir in Satz 1.4.4 gesehen haben, sind die Restklassenkörper der $\mathfrak{q}_i$ über dem Restklassenkörper von $\mathfrak{p}$ alle isomorph. Deshalb reicht es einen dieser Körper $\mathfrak{q}_i = \mathfrak{q}$ zu betrachten. Der Körper $K_\mathfrak{p}$ stellt den Restkörper $K_\mathfrak{p} = \mathbb{F}_q[Y]/\mathfrak{p}$ dar und $K_\mathfrak{q}$ ist die Körpererweiterung, die durch ziehen der n-ten Wurzel aus $0 \neq y \in K_\mathfrak{p}$ hervorgeht. Da f der Grad der Körpererweiterung $K_\mathfrak{p}(\sqrt[n]{y})|K_\mathfrak{p}$ ist (vgl. 1.4.3), hängt f nur von der Ordnung von y in $(K_\mathfrak{p})^*$ ab. $(K_\mathfrak{p})^*$ ist zyklisch vom Grad $q^d - 1$. Sei m_p die Ordnung von y. Dann ist $l := \frac{q^d-1}{m_p}$ der größte Teiler der Ordnung $q^d - 1$, so dass y eine l-te Potenz in $K_\mathfrak{p}$ ist. Ist $l = 1$ oder allgemein $ggt(l, n) = 1$, so ist y keine n'-te Potenz für ein n' mit $1 \leq n'|n$. In diesem Fall ist $f = n$. Allgemein ist $f = \frac{n}{ggt(l,n)}$. Es bleibt also noch die Frage, für wie viele $\mathfrak{p}$ die Restklasse y keine n'-te Potenz ist. Die Ordnung von y ist gleich der Ordnung von unseres Polynoms $f(Y)$ (vgl. [LN94] Seite 82, Lemma 3.17). Es gibt für jedes n' genau $\frac{\varphi(n')}{d}$ viele irreduzible Polynome des Grades d mit Ordnung n' (vgl. [LN94] Seite 78, Theorem 3.5). Somit gibt es insgesamt $\sum_{n'|n} \frac{\varphi(n')}{d}$ viele normierte irreduzible Polynome aus $\mathbb{F}_q[Y]$, die in $\mathbb{F}_q[T]$ zerfallen. Folglich gibt es $N_q(d) - \sum_{n'|n} \frac{\varphi(n')}{d}$ viele Primideale, die nicht zerfallen, wobei $N_q(d)$ die Anzahl der normierten irreduziblen Polynome vom Grad d über $\mathbb{F}_q$ ist. □

Es gibt also

$$N_q(\frac{s}{n}) - \sum_{n'|n} \frac{\varphi(n')}{\frac{s}{n}}$$

viele irreduzible Polynome vom Grad s, deren Bahnen die Länge $\frac{q\cdot(q-1)}{n}$ haben. Hierbei ist noch zu beachten, dass jeweils $\frac{q-1}{|G_n|} = \frac{q-1}{n}$ viele dieser Polynome in einer Bahn liegen.

Situation 2

Da wir abgesehen von $\mathbb{F}_4$ nur den Fall betrachten, dass q eine Primzahl ist, reicht es, uns in dieser Situation auf den Fall $r = 1$ zu beschränken. In den berechneten Beispielen kann die Situation $r > 1$ nur bei Polynomen über $\mathbb{F}_4$ vom Grad vier auftreten, diesen Fall kann man aber sehr schnell von Hand berechnen.

Sei p die Charakteristik von $\mathbb{F}_q$. Betrachten wir nun die Körpererweiterung $L \mid K$ vom Grad p mit den zugehörigen Ganzheitsringen, wobei $Y := T^p - T$.

$$\begin{array}{ll} \mathbb{F}_q[T] & L := \mathbb{F}_q(T) \\ \Big| & {\scriptstyle p}\Big| \\ \mathbb{F}_q[Y] & K := \mathbb{F}_q(Y) \end{array}$$

Die Galoisgruppe dieser Körpererweiterung ist isomorph zu $(\mathbb{F}_p, +)$. Es gilt: Y ist genau dann verzweigt, wenn $Y = \infty$. Für alle anderen Fälle gilt $Y = T^p - T = \prod_{a\in\mathbb{F}_p}(T-a)$. Für ein Primideal $\mathfrak{p} = (f(Y))$ vom Grad $d := \frac{s}{p}$ gibt es zwei Möglichkeit: Es kann in der Körpererweiterung träge bleiben, d.h. $f = p$, oder in p verschiedene Primideale zerfallen, d.h. $g = p$. Dies sind die einzigen Fälle, die vorkommen können, da $\mathfrak{p}(Y)$ invariant unter Transformationen der Form $T \to T + a$ mit $a \in \mathbb{F}_p$. Ist $\mathfrak{q}(T)$ ein Primideal über $\mathfrak{p}(Y)$, so gilt dies auch für $\mathfrak{q}(T + a)$ für alle $a \in \mathbb{F}_p$ ist. Somit gibt es entweder nur ein Primpolynom $\mathfrak{q}(Y)$ über $\mathfrak{p}(Y)$, das invariant unter Galoistransformationen ist, oder $\mathfrak{p} = \prod_{a\in\mathbb{F}_p} \mathfrak{q}(T + a)$.
Des Weiteren betrachten wir die Abbildung

$$\begin{array}{rcl} \alpha : K_\mathfrak{p} & \to & K_\mathfrak{p} \\ T & \to & T^p - T. \end{array}$$

Dann können wir folgende Aussage treffen:

5.1.4 Satz:
In der eben beschriebenen Situation gelten die folgenden Äquivalenzen:

$$\begin{array}{rcl} \mathfrak{p} \textit{ zerfällt in } \mathbb{F}_q(T) & \iff & y := (Y \textit{ mod } \mathfrak{p}) \textit{ liegt im Bild von } \alpha \\ & \iff & Tr_{\mathbb{F}_p}^{K_\mathfrak{p}}(y) = 0, \textit{ d.h. } f(Y) = Y^d + a_{d-2}\cdot Y^{d-2} + ... + a_0 \end{array}$$

Beweis: Es ist zu zeigen: $\mathfrak{p}$ zerfällt in $\mathbb{F}_p(T) \Longleftrightarrow y := (Y \bmod \mathfrak{p})$ liegt im Bild von α
Liegt y im Bild von α, so lässt sich y als $z^p - z$ schreiben für ein $z \in K_\mathfrak{p}$, d.h die zugehörige Restkörpererweiterung $K_\mathfrak{q}$ hat Grad 1. Somit ist auch $f = 1$ und deshalb zerfällt $\mathfrak{p}$. Gilt umgekehrt: y liegt nicht im Bild von α, so lässt sich y für kein $z \in K_\mathfrak{p}$ als $z^p - z$ schreiben. Die Restkörpererweiterung $K_\mathfrak{q}$ hat also Grad p. Somit ist auch $f = p$ und $\mathfrak{p}$ zerfällt nicht.
Bleibt noch zu zeigen:
$(Y \bmod \mathfrak{p})$ liegt im Bild von $\alpha \Longleftrightarrow Tr_{\mathbb{F}_p}^{K_\mathfrak{p}}(y) = 0$, d.h. $f(Y) = Y^d + a_{d-2} \cdot Y^{d-2} + a_{d-3} \cdot Y^{d-3} + ... + a_0$
Liegt y im Bild von α, d.h. es gibt ein $\beta \in K_\mathfrak{p}$, so dass $y = \beta^p - \beta$, dann gilt $\beta^{p^{rd}} - \beta = 0$ und es folgt

$$\begin{aligned} Tr_{\mathbb{F}_q}^{K_\mathfrak{p}}(y) &= Tr_{\mathbb{F}_q}^{K_\mathfrak{p}}(\beta^q - \beta) \\ &= (\beta^p - \beta) + (\beta^p - \beta)^p + ... + (\beta^p - \beta)^{p^{d-1}} \\ &= (\beta^p - \beta) + (\beta^{p^2} - \beta^q) + ... + (\beta^{p^d} - \beta^{p^{d-1}}) \\ &= \beta^{p^d} - \beta \\ &= 0. \end{aligned}$$

Sei $y \in K_\mathfrak{p}$ mit $Tr_{\mathbb{F}_p}^{K_\mathfrak{p}}(y) = 0$ und β eine Wurzel des Polynoms $T^q - T - y$ in einer Körpererweiterung von $K_\mathfrak{p}$, dann ist $\beta^p - \beta = y$ und

$$\begin{aligned} 0 &= Tr_{\mathbb{F}_p}^{K_\mathfrak{p}}(y) \\ &= y + y^p + ... + y^{p^{d-1}} \\ &= (\beta^p - \beta) + (\beta^p - \beta)^p + ... + (\beta^p - \beta)^{p^{d-1}} \\ &= (\beta^p - \beta) + (\beta^{p^2} - \beta^p) + ... + (\beta^{p^d} - \beta^{p^{d-1}}) \\ &= \beta^{p^d} - \beta. \end{aligned}$$

Dies zeigt, dass β schon in $K_\mathfrak{p}$ liegt. □

Stellt sich nun noch die Frage, wie viele irreduzible Polynome vom Grad d mit verschwindender Spur existieren. Bei der folgenden Beweisführung habe ich mich an [MG90] orientiert.

5.1.5 Definition:

1. *Für $\delta \in \mathbb{F}_q$ definieren wir die* Spurpolynome *durch*

$$T_{q,d}(X, \delta) = \begin{cases} \delta, & d = 0 \\ \delta + \sum_{i=0}^{d-1} X^{q^i}, & d > 0 \end{cases}$$

2. *$F_{q,d}(X, \delta)$ sei das Produkt aller normierten irreduziblen Polynome vom Grad d über $\mathbb{F}_q$, deren zweithöchter Koeffizient δ ist.*

5.1.6 Lemma:
Ist $q = p^m$ und $\delta \in \mathbb{F}_q$, gilt

$$T_{q,d}(X,\delta) = \prod_{\substack{d_1|d \\ \gamma \in \mathbb{F}_q,\, \frac{d}{d_1}\cdot\gamma = \delta(mod\, p)}} F_{q,d_1}(X,\gamma)$$

5.1.7 Bemerkung:
Diese Produktdarstellung von $T_{q,d}(X,\delta)$ zeigt, dass jeder Primfaktor von $T_{q,d}(X,\delta)$ nur mit der Vielfachheit 1 vorkommt, die Polynome F_{q,d_1} jedes irreduzible Polynom mit Spur d_1 genau einmal als Faktor enthalten und sie für verschieden d_1 unterschiedliche Faktoren enthalten.

Beweis: Zunächst gilt, dass die Ableitung von $T_{q,d}(X,\delta)$ die Konstante 1 ist. Deshalb hat es keine mehrfachen Faktoren. Daher genügt es, die Primfaktoren beider Seite zu vergleichen.
„$\supset$“ Ist $f(X)$ ein irreduzibles Polynom der Form $f(X) = X^{d_1} + \gamma \cdot X^{d_1-1} + ... +$ und α eine Nullstelle von f in $\mathbb{F}_{q^{d_1}}$, dann folgt mit der Transitivität der Spur:

$$Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^d}}(\alpha) = Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^{d_1}}}(Tr_{\mathbb{F}_{q^{d_1}}}^{\mathbb{F}_{q^d}}(\alpha)) = Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^{d_1}}}(\frac{d}{d_1}\cdot\alpha) = \frac{d}{d_1}\cdot(-\gamma) = -\delta(mod\, p)$$

Deshalb ist f ein Teiler von $T_{q,d}(X,\delta)$.
„$\subset$“ Ist $g(X)$ irreduzibel vom Grad d_1 und $g(X)|T_{q,d}(X,\delta)$, dann ist d_1 ein Teiler von d, da $(T_{q,d}(X,\delta))^q - T_{q,d}(X,\delta) = X^{q^d} - X$. Für eine Wurzel α von g definiert man $\gamma := -Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^{d_1}}}(\alpha)$. Dann ist $\frac{d}{d_1}\cdot\gamma = \delta(mod\, p)$ und somit ist $g(X)$ ein Faktor von $F_{q,d_1}(X,\gamma)$. □

5.1.8 Satz:
Ist $p \nmid d$, so gilt

$$F_{q,d}(X,0) = \prod_{d_1|d}(T_{q,\frac{d}{d_1}}(X,0))^{\mu(d_1)}.$$

Ist $\delta \neq 0$ so gilt

$$F_{q,d}(X,\delta) = \prod_{d_1|d \wedge p\nmid d_1}(T_{q,\frac{d}{d_1}}(X, d^{-1}(mod\, p)\cdot\delta))^{\mu(d_1)}.$$

Ist $p|d$ so gilt

$$F_{q,d}(X,0) = \prod_{d_1|d \wedge p\nmid d_1}(T_{q,\frac{d}{d_1}}(X,0)/(X^{q^{\frac{d}{pd_1}}} - X))^{\mu(d_1)}.$$

Beweis: Die erste beiden Gleichungen folgen aus dem eben bewiesenen Lemma und der Möbiusinversion. Die dritte Gleichung egibt sich aus dem eben bewiesenen Lemma und der Tatsache das

$$\begin{aligned} F_{q,d}(X,0) &= I(q,k;X)/\left(\prod_{\delta\neq 0} F_{q,d}(X,\delta)\right) \\ &= \prod_{d|k}(X^{q^{\frac{k}{d}}} - X)^{\mu(d)}/\left(\prod_{d_1|d\wedge p\nmid d_1}(T_{q,\frac{d}{d_1}}(X, d^{-1}(mod\, p)\cdot\delta))^{\mu(d_1)}\right) \end{aligned}$$

□

5.1.9 Satz:
Die Anzahl der irreduziblen Polynome vom Grad d mit Spur 0 ist:
für $p \nmid d$:

$$N_q(d,0) = \frac{1}{d} \cdot \sum_{d_1|d} (q^{\frac{d}{d_1}-1})^{\mu(d_1)}.$$

für $p|d$:

$$N_q(d,0) = \frac{1}{d} \cdot \sum_{d_1|d \wedge p\nmid d_1} (q^{\frac{d}{d_1}-1} - q^{\frac{d}{p\cdot d_1}})^{\mu(d_1)}.$$

Es gibt also $N_q(d,0) = N_q(\frac{s}{p},0)$ viele irreduzible Polynome mit Bahnlänge $\frac{(q-1)\cdot q}{p}$.
Hierbei ist noch zu beachten, dass jeweils $p-1$ viele dieser Polynome in einer Bahn liegen, nämlich diejenigen normierten irreduziblen Polynome f, die durch die Trabsformationen $T \to aT$ ineinander überführt werden, wobei $a \in \mathbb{F}_p^*$.

Situation 3

Es bleibt noch die letzte Fragestellung, wie viele irreduzible Polynome aus $\mathbb{F}_q[(T^p-T)^n]$ in $\mathbb{F}_q[T]$ irreduzibel sind. Diesen Fall können wir aber wie folgt durch die beiden eben betrachteten Fälle behandeln, indem wir sie nacheinander anwenden:

$$\begin{array}{cc} \mathbb{F}_q[T] & L := \mathbb{F}_q(T) \\ \Big| & \Big|_n \\ \mathbb{F}_q[T^n] & M := \mathbb{F}_q(T^n) \\ \Big| & \Big|_p \\ \mathbb{F}_q[(T^p-T)^n] & K := \mathbb{F}_q((T^p-T)^n) \end{array}$$

Bei dem Schritt von K nach M bleiben $N_q(\frac{s}{pn},0)$ viele Primideale prim, bei dem Schritt von M nach L bleibt etwa jedes $\frac{N_q(\frac{s}{pn})}{N_q(\frac{s}{pn}) - \sum_{n'|n} \frac{\varphi(n')}{\frac{s}{pn}}}$-te Primideal prim. Da die Grade der Körpererweiterungen multiplikativ sind, gibt es ungefähr $N_q(\frac{s}{pn},0) \cdot \frac{N_q(\frac{s}{pn}) - \sum_{n'|n} \frac{\varphi(n')}{\frac{s}{pn}}}{N_q(\frac{s}{pn})}$ viele solcher Polynome. Diese haben Bahnlänge $\frac{(q-1)\cdot q}{pn}$. Hierbei ist noch zu beachten, dass jeweils $\frac{(q-1)}{|G_{np}|} = \frac{(q-1)}{n}$ viele dieser Polynome in einer Bahn liegen.

Eine weitere Gruppe, die auf der Menge der irreduziblen Polynome operiert, ist die Galoisgruppe. Dies führt uns zu folgender Situation:

Situation 4

Sei $q := p^m$, wobei p eine Primzahl und $r \in \mathbb{N}$ mit $m > 1$ ist, $j \in A$ und σ ein Element der Galoisgruppe von $\mathbb{F}_q|\mathbb{F}_p$. Es gilt:

Ein irreduzibles Polynom ist genau dann invariant σ, wenn alle Koeffizienten invariant unter σ sind. Insbesondere gilt:
Hat ein irreduzibles Polynom nur Koeffizienten in $\mathbb{F}_p$, so ist es invariant unter der Galoisgruppe.
Nach dem Hauptsatz der Galoistheorie gibt es zu jeder Untergruppe der Galoisgruppe einen entsprechenden Körper K, so dass $\mathbb{F}_q|K$ galoissch ist. Dies zeigt, dass ein irreduzibles Polynom genau dann invariant unter einer Untergruppe der Galoisgruppe ist, wenn es nur Koeffizienten aus einem Zwischenkörper K besitzt für den gilt $\mathbb{F}_p \subset K \subset \mathbb{F}_q$. Der Körper K ist also von der Form $\mathbb{F}_{p^r}$, wobei r ein Teiler von m ist. Wir haben also ein Verfahren gefunden, um die Galoisinvarianz zu überprüfen. Der folgende Satz gibt an, wie viele Polynome dieser Art es gibt.

5.1.10 Satz:
Ein irreduzibles Polynom über $\mathbb{F}_{p^r}[T]$ von Grad n bleibt genau dann irreduzibel über $\mathbb{F}_{p^m}[T]$, wenn $ggT(n, \frac{m}{r}) = 1$.

Beweis: Siehe [LN94], Seite 99-100. □

Da wir nun Informationen über die einzelnen Bahnen und deren Länge haben, hilft uns dies herauszufinden, welche irreduziblen Polynome automatisch nach Satz 4.1.5 und Satz 4.1.2 gleichviele supersinguläre Stellen eines festen Grades haben. In der Statistik würde man sagen, die Polynome in einer Bahn sind nicht unabhängig voneinander, während die einzelnen Bahnen paarweise unabhängig sind.

5.2 Programm

Eingabe der Parameter:
Einlesen von q;
Einlesen von d;
Einlesen der Liste S der irreduziblen Polynome;
Schleife 1 von $l := 1$ bis Anzahl der irreduziblen Polynome vom Grad d
Setze f gleich dem l-ten Element von S;
i:=0;
Schleife 2 über alle Polynome j, deren Grad kleiner als d ist;
Setzen der Startwerte:
$\varphi_0 := 1$;
$\varphi_1 := 1$;
Berechnung von $\varphi_d(j)$:
Schleife 3 von $k = 2$ bis d
$\lambda := \frac{q^{k-1}+(-1)^k}{q+1}$;
$\varphi_k := j^{\lambda} \cdot \varphi_1(j) - [k-1] \cdot \varphi_0(j) \bmod (f)$;
$\varphi_0 := \varphi_1$;
$\varphi_1 := \varphi_k$;
end Schleife 3;
wenn $\varphi_k(j) = 0$ dann setze $i := i + 1$;
end Schleife 2;

Ausgabe von i; end Schleife 1;

5.3 Laufzeitanalyse

Ich möchte nicht im Detail auf die von mir verwendeten Algorithmen eingehen, eine ausfühliche Beschreibung hierzu findet man in den angegebnen Quellen.
Zunächst muss man alle irreduziblen Polynome vom Grad d berechnen. Der Algorithmus, den Magma dazu verwendet, benötigt $O(q^d d^2)$ Rechenoperationen. Der Algorithmus konstruiert zunächst eine Körpererweiterung vom Grad d über $\mathbb{F}_q$. Anschließend berechnet man die Minimalpolynome aller Elemente dieses Körpers, die verschiedene Minimalpolynome haben. Dies liefert alle irreduziblen Polynome über $\mathbb{F}_q$ vom Grad d. Die Theorie, die hinter diesem Algorithmus steckt, kann in [LN94] (Kapitel 3, Seite 76-100) nachgelesen werden.
Da alle Berechnungen in einem Polynomring über einem endlichen Körper mit weniger als zehn Elementen stattfinden, können wir annehmen, dass Addition und Multiplikation von Elementen in unserem Grundkörper $\mathbb{F}_q$ dieselbe Rechenzeit in Anspruch nehmen. Wir zählen also jede Addition und Multiplikation in $\mathbb{F}_q$ als eine Operation. Hieraus können wir alle weiteren Berechnungen zusammensetzen.
Für die Grundrechenarten von Polynomen gilt dann:
Da j in diesem Fall einen Grad ≤ 8 hat, macht es kaum einen Unterschied, wenn man einen schlechteren Algorithmus zur Polynommultiplikation verwendet. Das naive Multiplizieren von zwei Polynomen vom Grad n und m benötigt $(n+m)(n+m-1)$ Rechenopereationen.
Dividiert man ein Polynom von Grad n mit Rest durch ein Polynom mit Grad m, so kann dies mit $O(M(n-m)+M(m))$ vielen arithmetischen Operationen berechnet werden (siehe [BCS97] Seite 47). Hierbei bezeichnet M die Komplexität der Polynommultiplikation. Magma benötigt dafür mittels der schneller Fouriertransformezion (der sog. FFT Methode) $M(n) = n \cdot log(n) \cdot log(log(n))$ Rechenschritte (siehe [BCS97] Seite 32-34).
Im Zuge des Programms berechnen wir $\varphi_d(j)$ für alle irreduziblen Polynome vom Grad d in $\mathbb{F}_\mathfrak{p}$ und alle $j \in \mathbb{F}_\mathfrak{p}^*$. Deshalb beschäftigen wir uns zunächst mit der Laufzeitanalyse zur Berechnung von φ_k für ein festes k, wenn φ_{k-2} und φ_{k-1} bereits berechnet sind. Dann ergibt sich $\varphi_k(j)$ wie folgt.

$$\varphi_k(j) = j^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(j) - [k-1] \cdot \varphi_{k-2}(j)$$

Zunächst können wir feststellen, dass alle Faktoren einen Grad echt kleiner als d haben, da wir stets modulo $\mathfrak{p}$ rechnen. Somit haben alle Produkte bevor sie erneut reduziert werden Grad kleiner als $2d-2$.
$j^{\frac{q^{k-1}+(-1)^k}{q+1}}$ berechnet man mit Repeated Squaring. Im schlechtesten Fall muss man
$a_k := \left\lfloor log_2(\frac{q^{k-1}+(-1)^k}{q+1}) \right\rfloor$ Quadraturen mit anschließendem Teilen mit Rest durch $\mathfrak{p}$ berechnen. Da der Grad von j echt kleiner als d ist, hat j^2 höchstens Grad $2d-2$. Insgesamt benötigt man zur Berechnung von $j^{\frac{q^{k-1}+(-1)^k}{q+1}}$ etwa $a_k \cdot (2(d-1)(2(d-1)-1) + O(M(2d-2-d)+M(d)))$. Die anschließende Multiplikation mit $\varphi_{k-1}(j)$ und Reduktion modulo $\mathfrak{p}$ braucht $(2(d-1)(2(d-1)-1)) + O(M(2d-2-d)+M(d))$

Die Reduktion von $[k-1]$ modulo $\mathfrak{p}$ kostet weitere $O(M(q^{k-1}-d)+M(d))$ Operationen und die anschließende Multiplikation mit $\varphi_{k-2}(j)$ benötigt $(2(d-1)(2(d-1)-1))$ und die Reduktion modulo $\mathfrak{p}$ benötigt nochmal $O(M(2d-2-d)+M(d))$.
Hinzu kommen noch d Operationen für die Addition der beiden Summanden. Für die insgesamte Berechnung von $\varphi_k(j)$ benötigt man

$$a_k \cdot (2(d-1)(2(d-1)-1)+O(M(2d-2-d)+M(d)))+(2(d-1)(2(d-1)-1))+O(M(2d-2-d)+M(d))$$

$$+O(M(q^{k-1}-d)+M(d))+(2(d-1)(2(d-1)-1))+O(M(2d-2-d)+M(d))$$

Zur Berechnung von $\varphi_d(j)$ benötigt man also insgesamt

$$\sum_{k=2}^{d}\left(\left\lfloor log_2\left(\frac{q^{k-1}+(-1)^k}{q+1}\right)\right\rfloor \cdot (2(d-1)(2(d-1)-1)+O(M(2d-2-d)+M(d)))+(2(d-1)(2(d-1)-1))\right.$$

$$+O(M(2d-2-d)+M(d))+O(M(q^{k-1}-d)+M(d))+(2(d-1)(2(d-1)-1))+O(M(2d-2-d)+M(d)))$$

Rechenoperationen.
Diese Rechnung führen wir für alle irreduziblen normierten Polynome vom Grad d durch. Da es ungefähr $\frac{q^d}{d}$ viele solcher Polynome gibt brauchen wir insgesamt

$$\frac{q^d}{d}\cdot\sum_{k=2}^{d}\left(\left\lfloor log_2\left(\frac{q^{k-1}+(-1)^k}{q+1}\right)\right\rfloor\right)\cdot(2(d-1)(2(d-1)-1)+O(M(2d-2-d)+M(d)))+(2(d-1)(2(d-1)-1))$$

$$+O(M(2d-2-d)+M(d))+O(M(q^{k-1}-d)+M(d))+(2(d-1)(2(d-1)-1))+O(M(2d-2-d)+M(d)))$$

Rechenoperationen.
Diese Überlegungen zeigen, dass nur die Laufzeit des Programm, (ohne vorherige Berechnung der Irreduziblen Polynome) im Mittel mit einer Komplexität

$$O(\frac{q^d}{d}(M((q^{d-1}-d)+M(d))))=O(\frac{q^d}{d}((q^{d-1}-d)\cdot log(q^{d-1}-d)\cdot log(log(q^{d-1}-d))+d\cdot log(d)\cdot log(log(d))))$$

wächst.
Stoppt man die Zeit, während der das Programm läuft, so stellt man fest, dass es für eine kleine Anzahl an irreduziblen Polynomen wenige Minuten zur Berechnung benötigt, während es für große Anzahlen an irreduziblen Polynomen, d.h. größer als 600 mehrere Stunden zur die Berechnung aller Werte benötigt.

5.4 Ergebnisse und Hypothesen

Für kleine Grade, d.h. für d von 1 bis 3, gibt es eine Formel für die Summe

$$\sum_{\mathfrak{p}\ grad(\mathfrak{p})=d} |\{(g,\Delta) \mid (g,\Delta) \text{ ist supersingulär mod } \mathfrak{p}\}|$$

5.4.1 Satz:
$\sum_{\mathfrak{p}\ grad(\mathfrak{p})=d} |\{(g,\Delta) \mid (g,\Delta)$ *ist supersingulär mod* $\mathfrak{p}\}|$ *ist durch folgende Formel gegeben:*

$$\begin{aligned} d=1: &\quad (q-1)q \\ d=2: &\quad (q^2-1)(\tfrac{q^2-q}{2}) \\ d=3: &\quad (q^3-1)(q+1)(\tfrac{q^3-q}{3}) \end{aligned}$$

Beweisidee: Für $d=1$ ist die Formel klar; da $g_1 = g$ ist, sind die Paare $(0,\Delta)$ die einzigen supersinguläre Werte für alle Primideale $\mathfrak{p}$ vom Grad 1. Es gibt insgesamt q viele $\mathfrak{p}$.
Für $d=2$ hat das Polynom $\varphi_2(T) = T - [1]$ genau eine Nullstelle in $\mathbb{F}_{\mathfrak{p}}[T]$ für alle Primideale $\mathfrak{p}$ vom Grad 2. Die Anzahl der supersingulären Paare (g,Δ) von g_2 erhält durch Multiplikation mit (q^2-1)(nach Korollar 3.1.12). Da es $(\frac{q^2-q}{2})$ viele $\mathfrak{p}$ vom Grad zwei gibt erhält man die angegebene Formel.
Für $d=3$ zeigt man, dass das Polynom $\varphi_3(T) = T^q - [1]T^{q-1} - [2]$ genau q viele Nullstellen in $\mathbb{F}_{\mathfrak{p}}[T]$ für alle Primideale $\mathfrak{p}$ vom Grad 3 hat. Die Anzahl der supersingulären Paare (g,Δ) von g_3 erhält durch Multiplikation der Anzahl der Nullstellen mit (q^3-1)(nach Korollar 3.1.12). Für $k=3$ sind nach Satz 3.1.13 alle Paare $(0,\Delta)$ supersingulär für alle Primideale $\mathfrak{p}$ vom Grad 3, es gibt insgesamt q^3-1 solche Paare. Da es $(\frac{q^3-q}{3})$ viele $\mathfrak{p}$ vom Grad 3 gibt, erhält man die angegebene Formel. □

Diese Formeln kommen daher, dass jedes irreduzible Polynom von einem festen Grad $d<4$ gleichviele supersinguläre Werte (g,Δ) hat. Meine Berechnungen zeigen, dass dies für Grade ≥ 4 nicht mehr gilt. Allerdings kann man versuchen, eine Näherungsformel für den Mittelwert der supersingulären Werte j zu jedem irreduziblen Polynom von einem festen Grad d zu finden. Multipliziert man dies mit (q^d-1) so erhält man den Mittelwert der supersingulären Werte (g,Δ).

5.4.2 Vermutung:
Jedes irreduzible Polynom vom Grad d gibt es im Mittel

$$\begin{aligned} &c(q)\frac{q}{q-1}q^{\frac{d}{2}-1} \quad \text{, falls } d \text{ gerade} \\ &c(q)\frac{q}{q-1}q^{\frac{d-1}{2}} \quad \text{, falls } d \text{ ungerade} \end{aligned}$$

viele supersinguläre j-Werte. Hierbei ist $c(q)$ *ein Korrekturfaktor, der für* $q \to \infty$ *gegen* 1 *läuft.*

Diese Formel soll im Folgenden überprüft werden. Dazu setze man $c(q)=1$ und vergleiche das Ergebnis mit den berechneten Werten. Wie die folgende Tabelle zeigt, stimmen die mit der Formel berechneten Werte bis auf Ausnahmen in den Körpern mit 2 bzw. 3 Elementen für $d=6,8$ sehr gut überein. Die mittels Magma berechneten Werte unterstützen also die Hypothese.

q	d	Rechnerisch ermittelter Mittelwert	Theoretischer Mittelwert
2	4	$1,75$	4
2	5	6	8
2	6	5	8
2	7	14	16
2	8	$10,333$	16
3	4	$3,333$	$4,5$
3	5	12	$13,5$
3	6	$10,103$	$13,5$
3	7	39	$40,5$
3	8	$30,37$	$40,5$
4	4	$4,2$	$5,\overline{3}$
4	5	$22,765$	$21,\overline{3}$
5	4	$5,2$	$6,25$
5	5	30	$31,25$
7	4	$7,143$	$8,1\overline{6}$

Tabelle 5.1

Nun stellt sich die Frage, wie die supersingulären Werte auf die einzelnen irreduziblen Polynome verteilt sind. Dazu möchte ich zunächst herausfinden, wie viele irreduzible Polynome eine bestimmte Anzahl an supersingulären j-Werten haben. Dies wird im Folgenden graphisch aufgetragen. Diese Graphen wurden mit der Software Excel 2003 erstellt.

Zunächst stellt man fest, dass in allen betrachteten Körpern jedes irreduzible Polynom vom Grad 4 eine gerade Anzahl an supersingulären Werten hat. Außerdem lässt sich bei den Körpern $\mathbb{F}_5$ und $\mathbb{F}_7$ eine gewisse Symmetrie zur Mitte erahnen. Im Fall $\mathbb{F}_5$ wird das Maximum in der Mitte angenommen und nach außen hin fällt die Anzahl der irreduziblen Polynome, die diese Anzahl an supersingulären Werten hat, ab. Die Werte fallen jedoch nicht gleichmäßig ab. Das Maximum wird in $\mathbb{F}_3$ am Rand angenommen. Der Graph fällt von dort regelmäßig ab. In Körpern mit Charakteristik 2 steigt der Graph an. Die Abstände zwischen den erreichten supersingulären Werten ist immer 2, nur bei $\mathbb{F}_4$ ist er 4. (vgl. Abbildung 5.1 und 5.5)

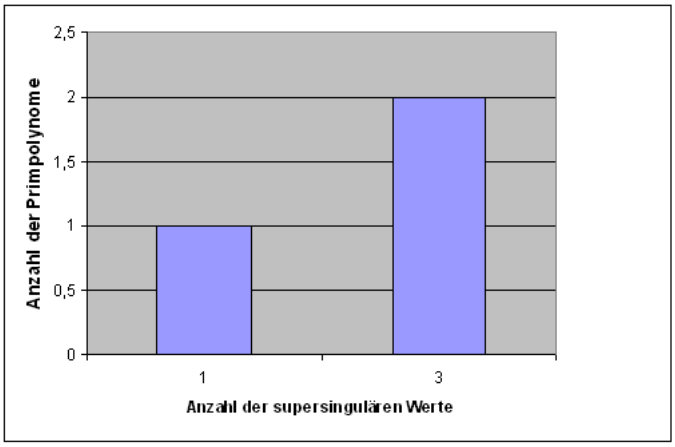

Abbildung 5.1: $q = 2$, $d = 4$

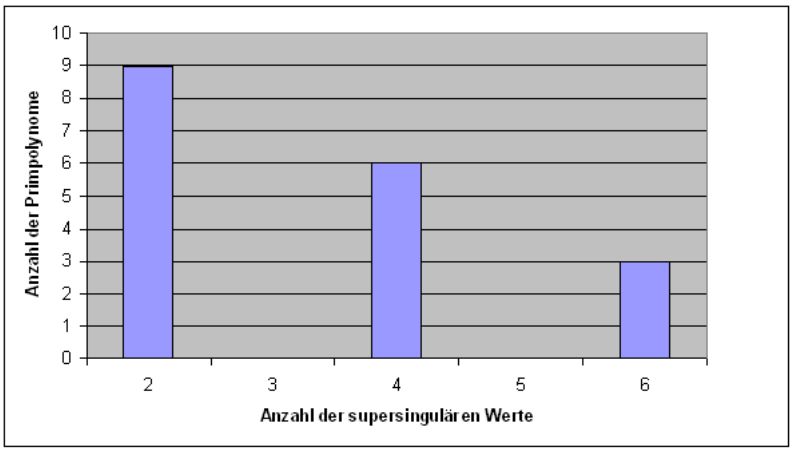

Abbildung 5.2: $q = 3$, $d = 4$

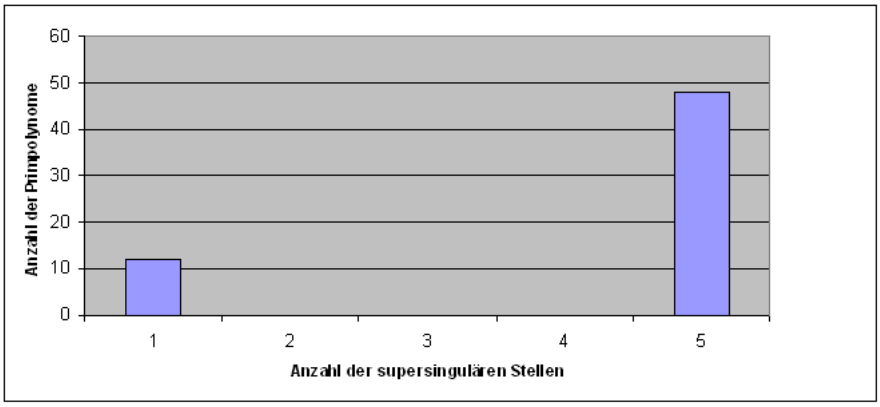

Abbildung 5.3: $q = 4$, $d = 4$

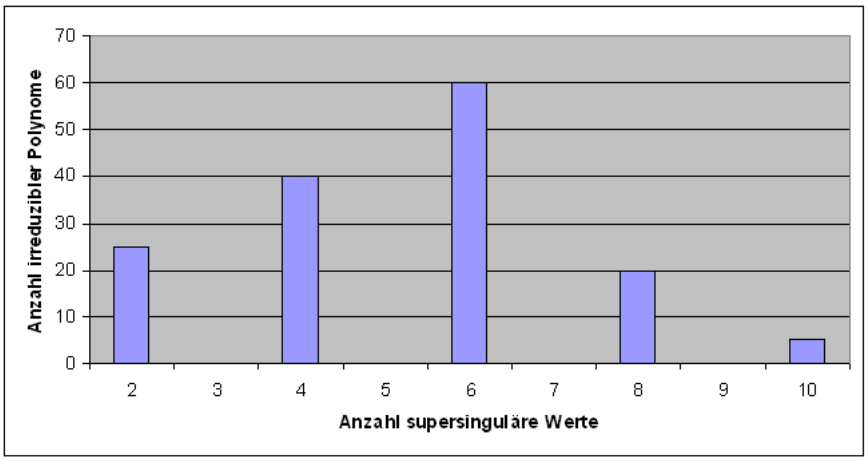

Abbildung 5.4: $q = 5$, $d = 4$

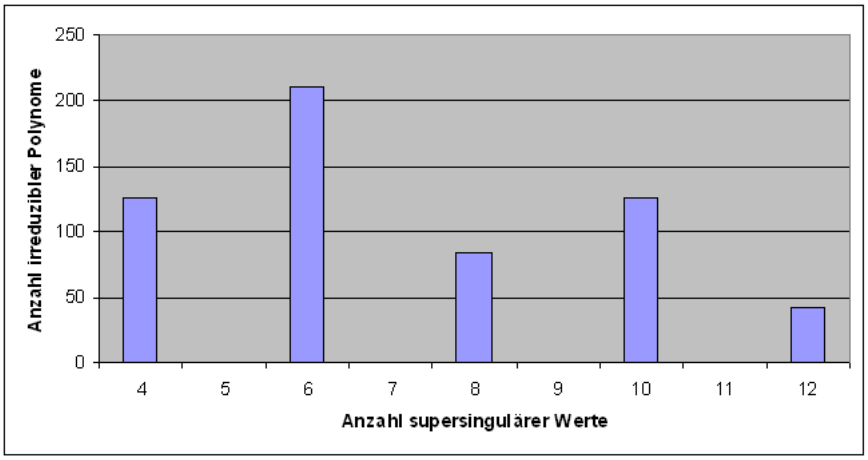

Abbildung 5.5: $q = 7$, $d = 4$

Auch hier stellt man fest, dass in allen betrachteten Körpern jedes irreduzible Polynom vom Grad 5 eine gerade Anzahl an supersingulären Werten hat. Bis auf den Fall $\mathbb{F}_5$ weisen die Graphen eine perfekte Symmetrie zur Mitte auf. Im Fall $\mathbb{F}_2$ haben wir sogar eine Gleichverteilung. Genau wie im Fall Grad 4 sind die Abstände zwischen den erreichten supersingulären Werten immer 2, nur bei $\mathbb{F}_4$ sind sie 4. (vgl. Abbildung 5.6 und 5.9)

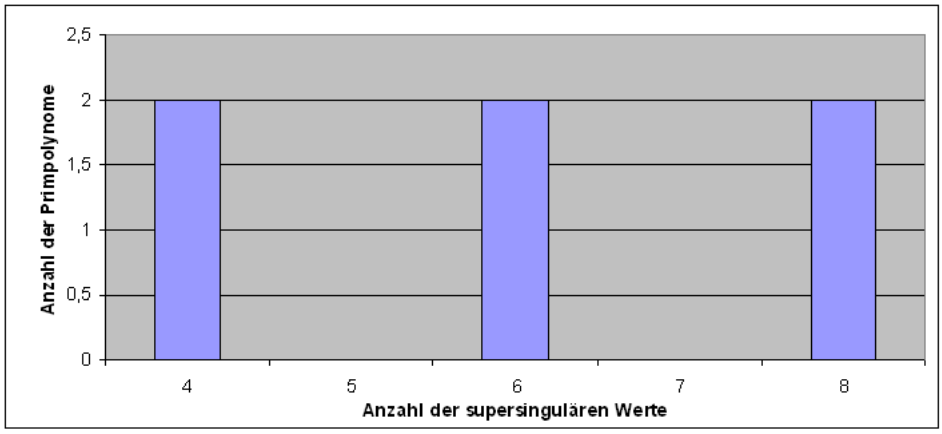

Abbildung 5.6: $q = 2$, $d = 5$

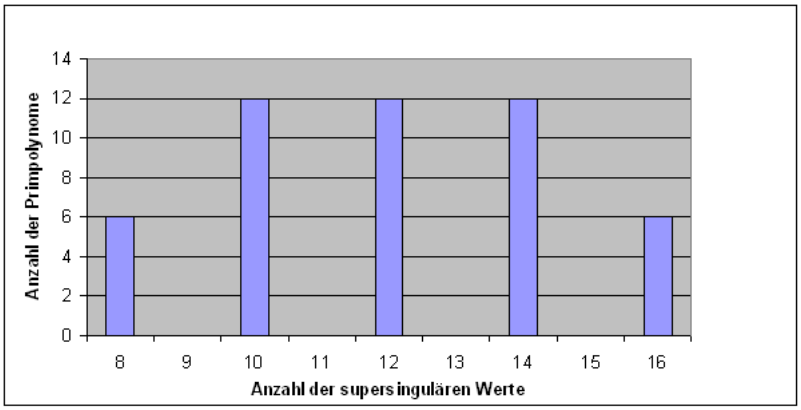

Abbildung 5.7: $q = 3$, $d = 5$

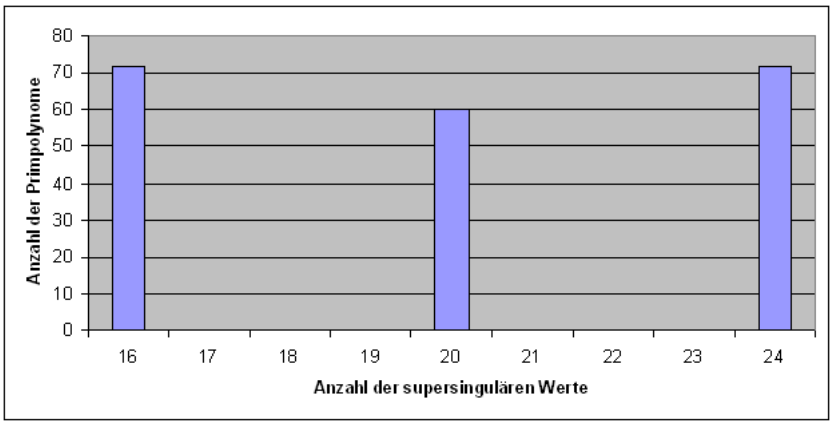

Abbildung 5.8: $q = 4$, $d = 5$

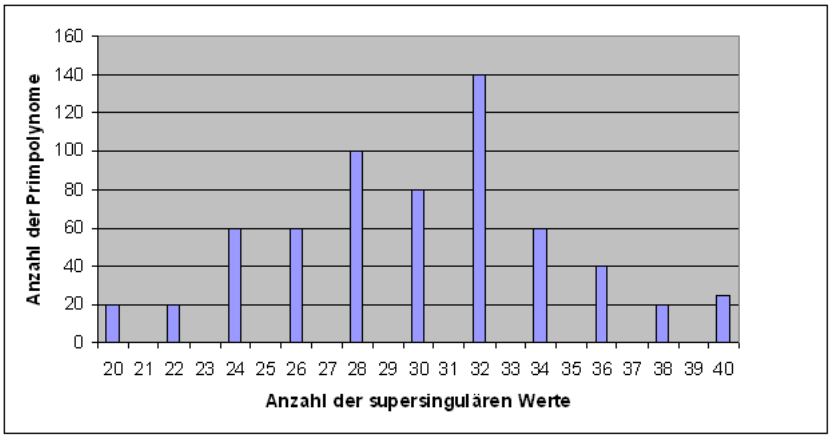

Abbildung 5.9: $q = 5$, $d = 5$

Zunächst stellt man fest, dass in allen betrachteten Körpern jedes irreduzible Polynom vom Grad 6 eine gerade Anzahl an supersingulären Werten hat. Es lässt sich jedoch keine Symmetrie erahnen. Das Maximum wird weder in der Mitte noch am Rand angenommen. Die Abstände zwischen den ereichten supersingulären Werten sind nicht immer gleich, es kommen die Werte 2 und 4 vor. (vgl. Abbildung 5.10 und 5.11)

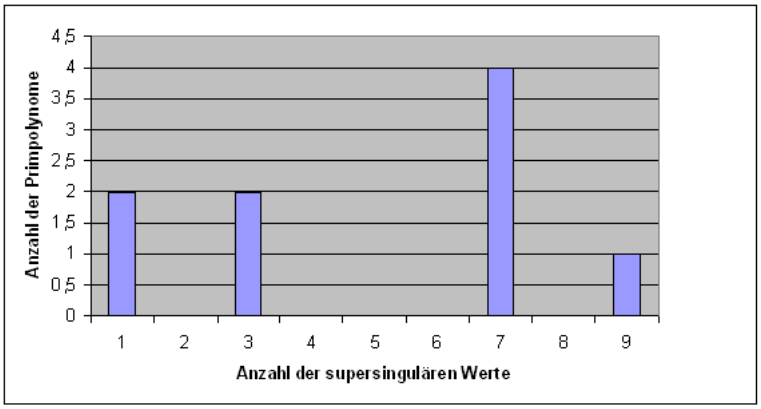

Abbildung 5.10: $q = 2$, $d = 6$

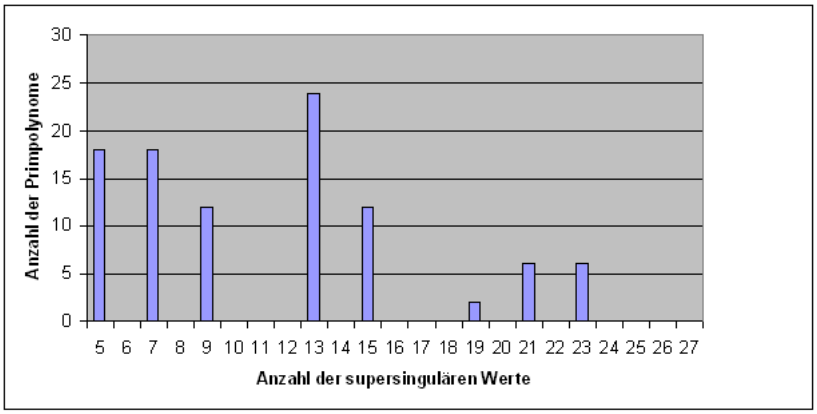

Abbildung 5.11: $q = 3$, $d = 6$

Für Grad 7 gilt: In $\mathbb{F}_2$ haben alle irreduziblen Polynome eine gerade Anzahl an supersingulären Werte. Die Abstände sind regelmäßig von der Größe 6 und der Graph ist symmetrisch zum Mittelpunkt; während in $\mathbb{F}_3$ alle irreduziblen Polynome eine ungerade Anzahl an supersingulären Werten haben, die Abstände regelmäßig von der Größe 8 sind und der Graph unsymmetrisch ist.(vgl. Abbildung 5.12 und 5.13)

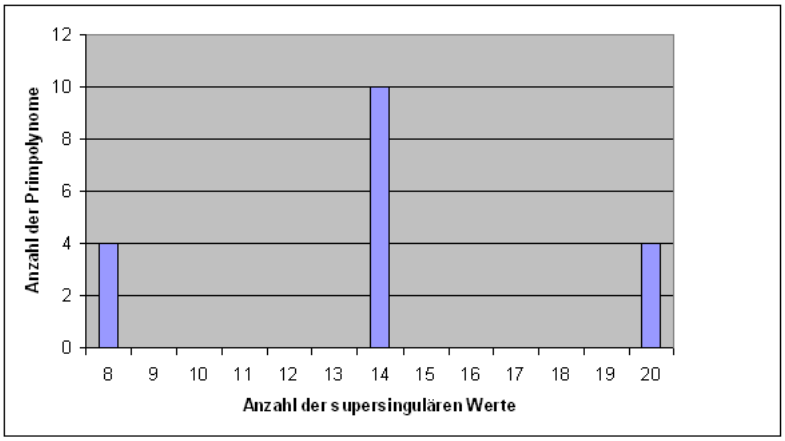

Abbildung 5.12: $q = 2$, $d = 7$

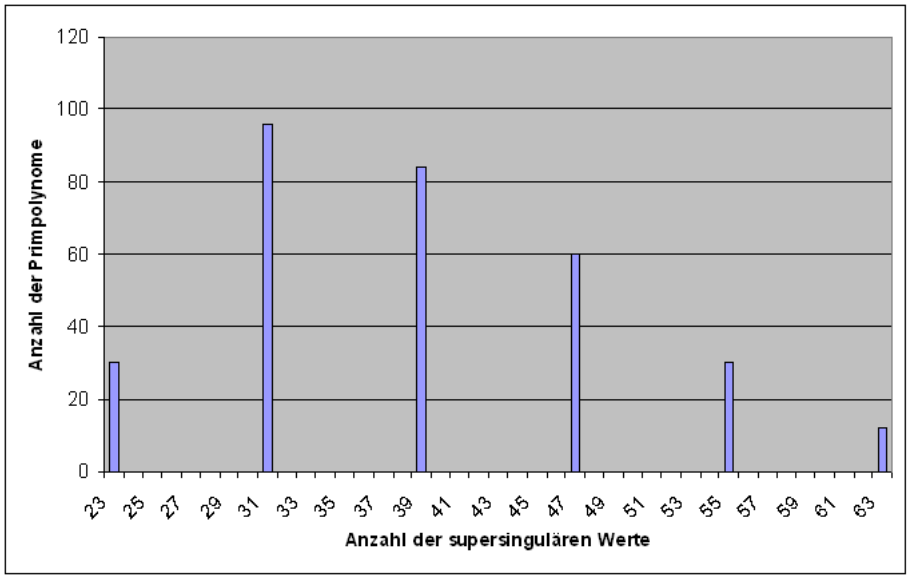

Abbildung 5.13: $q = 3$, $d = 7$

Für Grad 8 gilt: In $\mathbb{F}_2$ haben alle irreduziblen Polynome eine ungerade Anzahl an supersingulären Stellen, während in $\mathbb{F}_3$ alle irreduziblen Polynome eine gerade Anzahl an supersingulären Stellen haben. Es ist keine Symmetrie erkennbar und die Abstände sind unregelmäßig von der Größe 2, 6 und 8. (vgl. Abbildung 5.14 und 5.15)

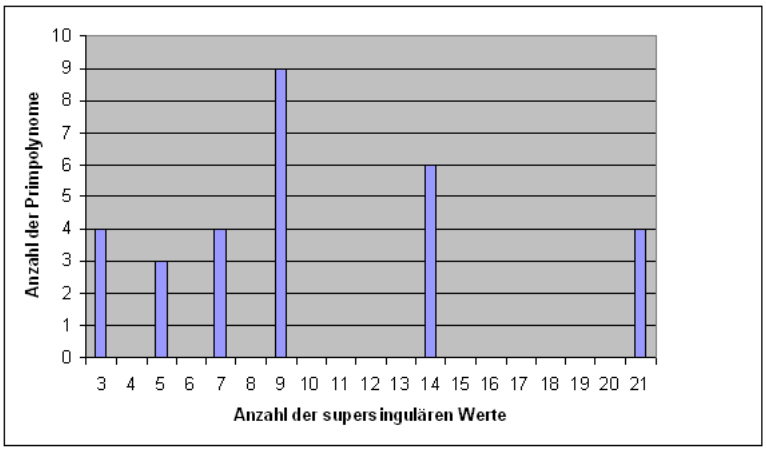

Abbildung 5.14: $q = 2$, $d = 8$

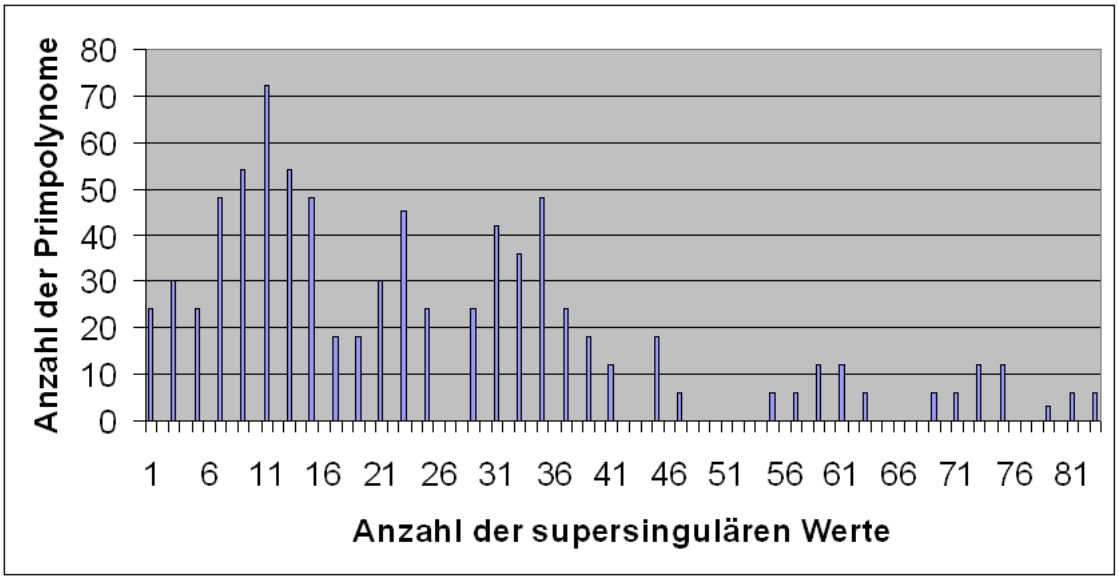

Abbildung 5.15: $q = 3$, $d = 8$

Bis zum Grad 5 kommen nur gerade Zahlen als Anzahl an supersigulären Werten in Frage und für Grad 5 und 7 lässt sich bis auf zwei Ausnahmen eine gewisse Symmetrie erkennen. Für Grad 6 und 8 ist keine deutliche Symmetrie mehr zu erkennen. Für Grad 6 kommen nur ungerade Zahlen als Anzahl an supersigulären Werten vor. Für größerer Werte kommen beide Fälle vor in einem Körper haben alle ireduziblen Polynome eine gerade Zahlen als Anzahl an supersingulären Werten in einem anderen eine ungerade Anzahl. Es lassen sich auch sonst keine Gemeinsamkeiten finden, die Grund zu einer Verallgemeinerung wären. Das Maximum ist nicht immer an derselben Stelle. Man kann auch für ein festes q keine Symmetrie finden. Die Abstände sind zwar immer gerade, aber nich immer regelmäßig oder gleich groß. Es bleibt nur folgende Vermutung aufzustellen:

5.4.3 Vermutung:
Die irreduziblen Polynome vom Grad d über einem festen Körper $\mathbb{F}_q$ haben entweder alle eine gerade oder alle eine ungerade Anzahl an supersingulären Stellen.

Es lässt sich kein festes Muster einer statistischen Verteilung erkennen; manche nehmen ihr Maximum am Rand an, andere genau in der Mitte und wieder andere irgendwo dazwischen. Auch die Tatsache, dass manche eine gewisse Symmetrie aufweisen und andere nicht, lässt nicht darauf schließen, dass man eine feste Verteilung für alle findet.
Da für die Grade kleiner als 4 die Anzahl der supersingulären Werte gleichverteilt ist, kann man vermuten, dass die Verteilung der supersingulären Werte für größere Grade ebenfalls von einer statistichen Gleichverteilung kommt. Eine Methode dies zu überprüfen ist der χ^2-Test. Bei diesem Test berechnet man $V^2 = \sum_{i=1}^{n} \frac{(x_i - E)^2}{E}$, wobei n die Anzahl der unabhängigen Ereignisse und x_i der zum unabhängigen Ereignis i gehörige Messwert ist. Mit E wird der rechnerisch bestimmte Mittelwert bezeichnet, den man der obigen Tabelle (5.1)entnehmen kann. Für große E geht V^2 gegen eine χ^2_{n-1}-Verteilung. Eine Faustregel besagt, dass $E \geq 3$ sein sollte, damit diese Näherung gültig ist. Der Index $n-1$ steht für die Anzahl der Freiheitsgrade. Da wir n unabhängige Ereignisse

haben und den Mittelwert anhand unserer Daten berechnet haben, haben wir lediglich $n-1$ Freiheitsgrade. Man bestimmt nun aus der Tabelle der χ^2_{n-1}-Verteilung das $(1-\alpha)$-Quantil $Q_{1-\alpha}$. Die Zahl $Q_{1-\alpha}$ ist so definiert, dass (nach Zugrundelegung einer χ^2-Verteilung fr V^2) ein „zufälliges“ V^2 mit einer Wahrscheinlichkeit mit $1-\alpha$ einen Wert $\leq Q_{1-\alpha}$ besitzt. In den meisten Fällen wird $\alpha = 0.05$ gewählt, so auch in dieser Arbeit. Den Leserinnen und Lesern, die eine ausführlichere Beschreibung dieser Theorie wünschen, empfehle ich als Quelle ([Kre05] Seite 181-186).
Wie wir bereits gesehen haben, operiert die Menge der affinen Transformationen auf der Menge der irreduziblen Polynome. Ist q eine Primzahl, so ist dies die einzige Gruppe, die wir betrachten müssen. In den anderen Fällen müssen wir noch die Galoisgruppe betrachten. Da zwei irreduzible Polynome, wenn sie durch solche Transformationen ineinander übergehen, nach Satz 4.1.5 und Satz 4.1.2gleichviele supersinguläre Werte haben, sind sie nicht unabhängig voneinander. Wir wollen im Folgenden annehmen, dass die Anzahl der einzelnen supersingulären Werte längs der $\mathfrak{p}$ unabhängig voneiander sind, was nicht immer zwangsläufig der Fall ist. Unter dieser Annahme sind im primen Fall unsere unabhängigen Ereignisse die Bahnen der affinen Transformation, im nicht primen Fall muss noch die Galoisgruppe berücksichtigt werden, wie in Situation 4. Mit dem am Anfang dieses Kapitels erworbenen Wissen können wir nun die Bahnen für die berechneten Beispiele angeben.

5.4.4 Beispiel:
Betrachtet man zum Beispiel die irreduziblen Polynome vom Grad 4 über $\mathbb{F}_3$ so ergeben sich folgende Rechenergebnisse.

Anzahl der supersingulären j-Werte	Anzahl irreduzibler Polynome
2	9
4	6
6	3

Da $3-1=2$ ein Teiler des Grades ist müssen wir die Operationen der Untergruppe der affinen Transformationen G_2 (vgl. Satz 5.1.2) betrachten. Wie in Situation 1 gezeigt, gibt es

$$N_3(2) - \sum_{n'|2} \frac{\varphi(n')}{2} = 2$$

viele irreduzible Polynome vom Grad 4, deren Bahnen die Länge $\frac{6}{2}=3$ haben. Da 3 kein Teiler von 4 ist, ist G_2 die einzige Untergruppe, die wir betrachten müssen, d.h alle anderen Bahnen haben die Länge 1. Es ergibt sich also die Tabelle

Anzahl der supersingulären j-Werte	Anzahl Bahnen
2	2
4	1
6	1

Trägt man zu jeder Bahn die entsprechende Anzahl von supersingulären Werte auf, so ergeben sich folgende Graphen:

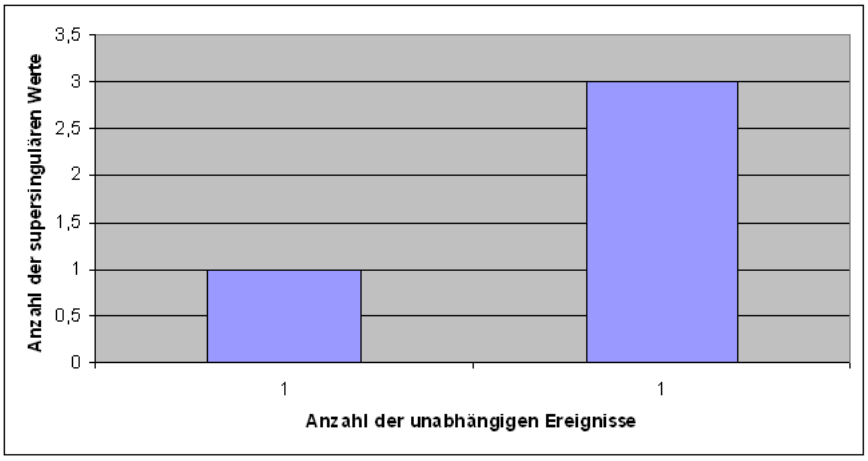

Abbildung 5.16: $q = 2$, $d = 4$

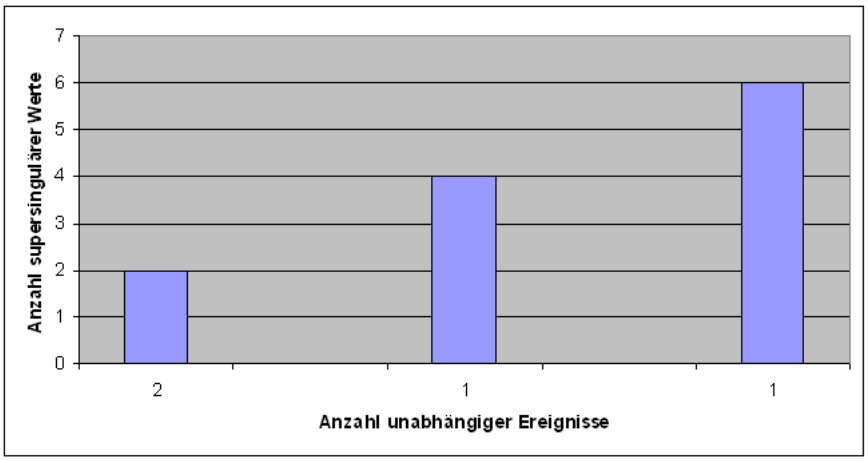

Abbildung 5.17: $q = 3$, $d = 4$

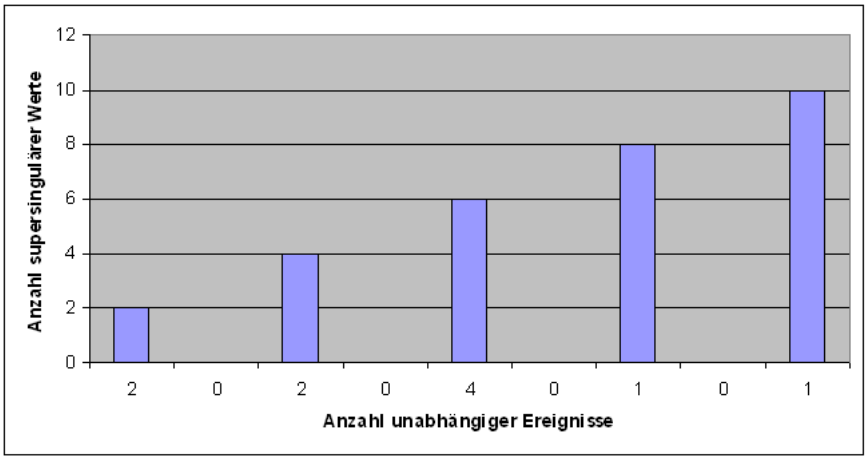

Abbildung 5.18: $q = 5$, $d = 4$

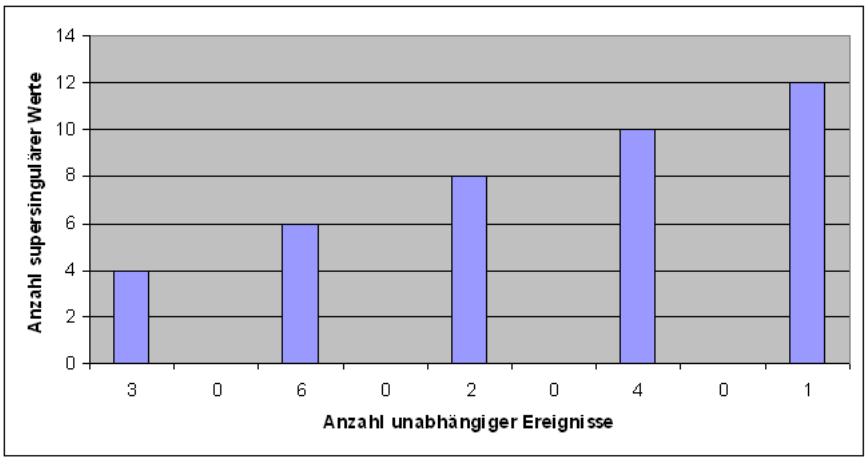

Abbildung 5.19: $q = 7$, $d = 4$

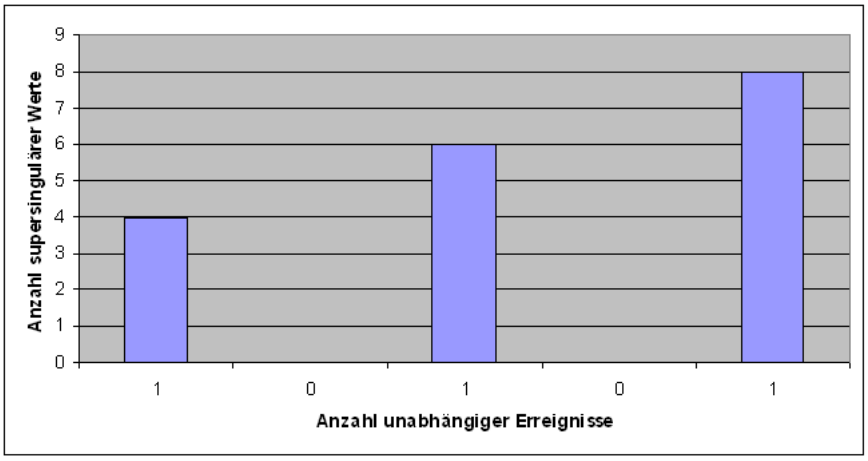

Abbildung 5.20: $q = 2$, $d = 5$

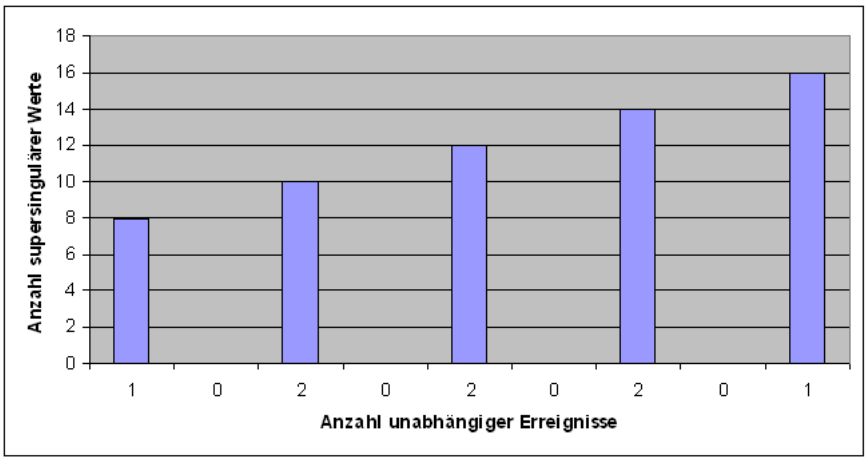

Abbildung 5.21: $q = 3$, $d = 5$

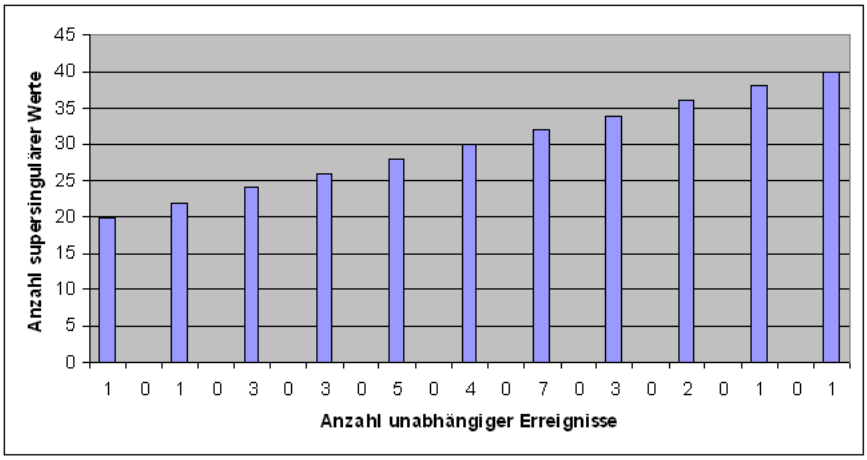

Abbildung 5.22: $q = 5$, $d = 5$

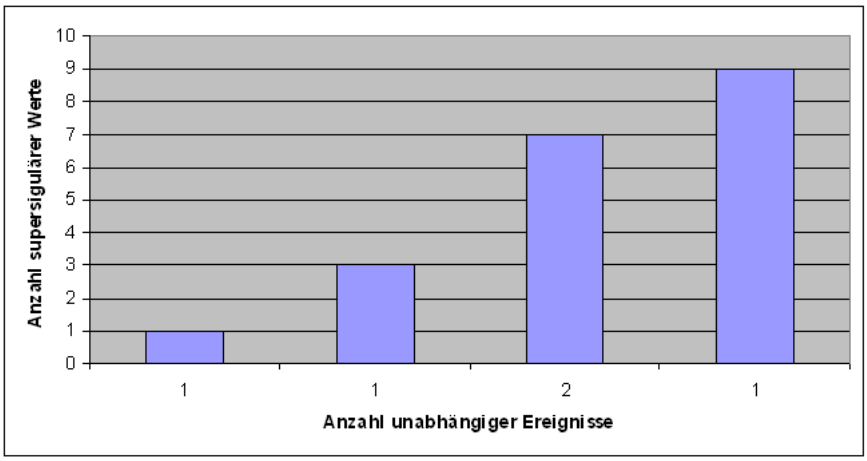

Abbildung 5.23: $q = 2$, $d = 6$

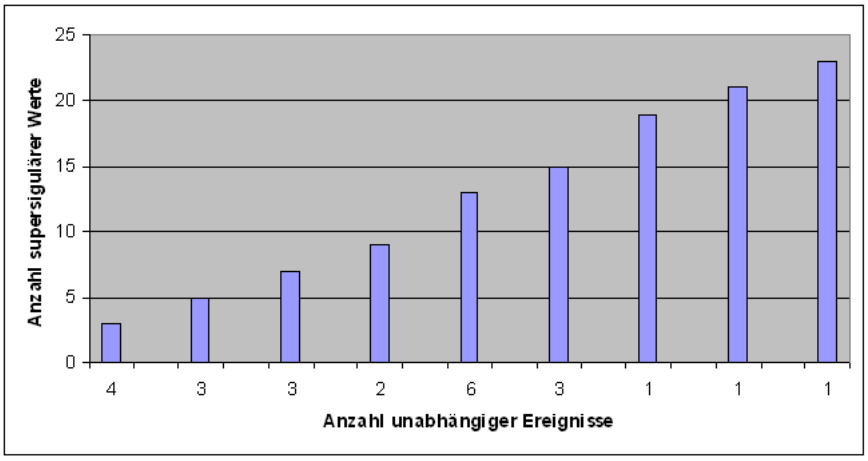

Abbildung 5.24: $q = 3$, $d = 6$

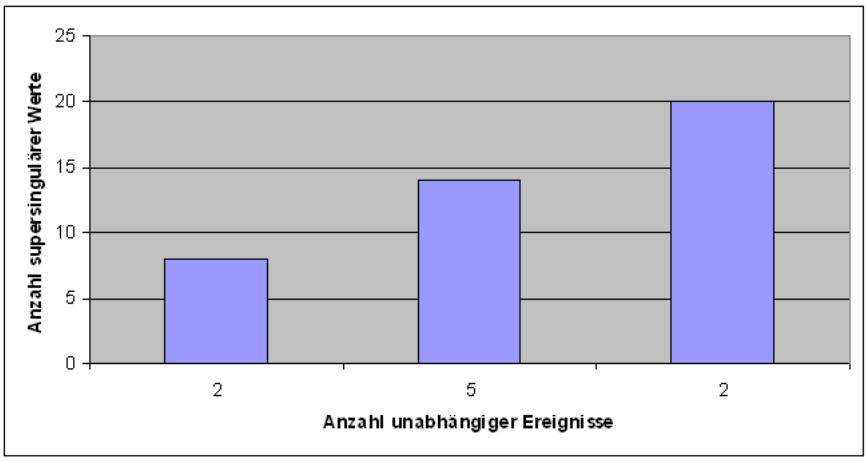

Abbildung 5.25: $q = 2$, $d = 7$

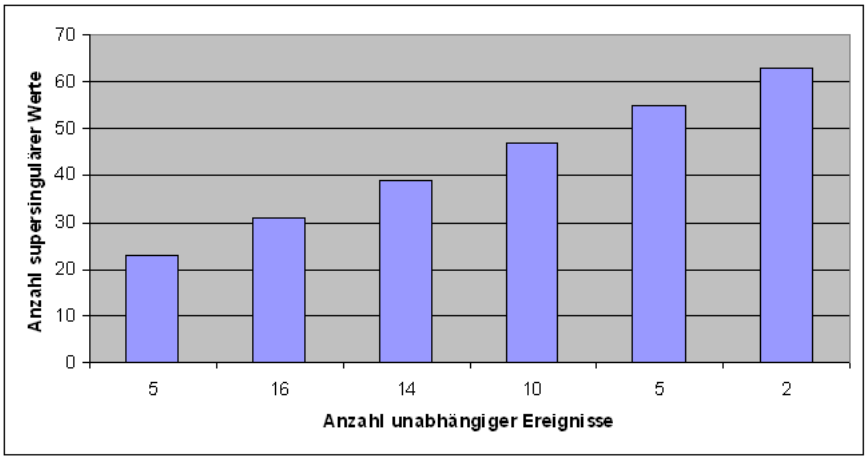

Abbildung 5.26: $q = 3$, $d = 7$

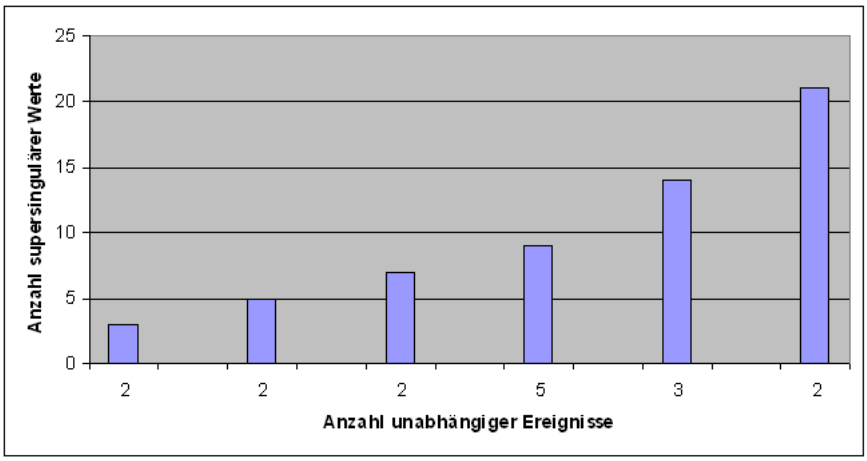

Abbildung 5.27: $q = 2$, $d = 8$

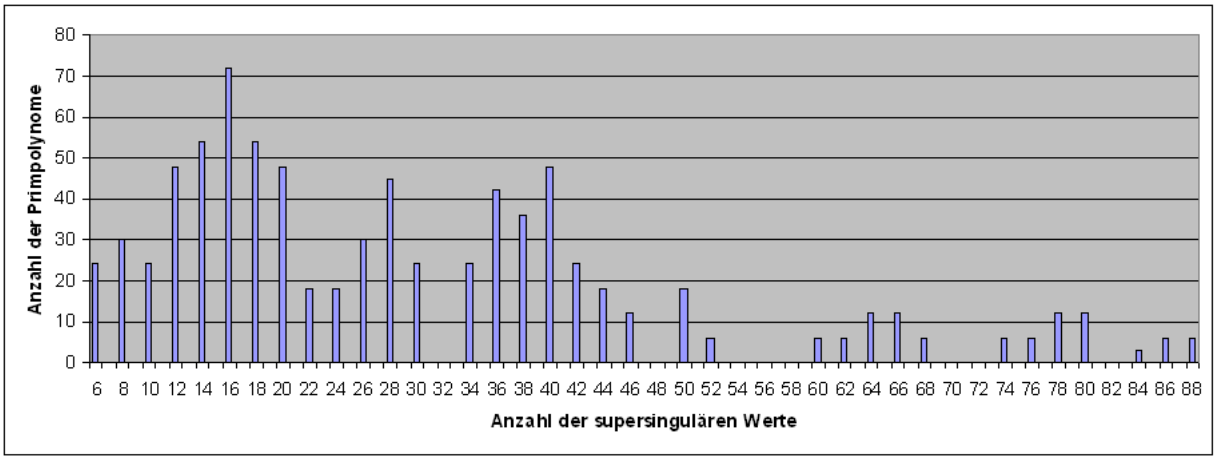

Abbildung 5.28: $q = 3$, $d = 8$

Die Graphen 5.16 bis 5.28 zeigen, dass die mittleren supersingulären Werte tendenziell öfter vorkommen, während die größeren supersingulären Werte tendenziell seltener vorkommen.
Mit diesen Daten können wir nun den χ^2-Test Test durchführen. Die Tabellenwerte der $0,95$-Quantile der χ^2-Verteilung für die entsprechenden Freiheitsgrade ≤ 100 stammen von [INT09a] und die Abschätzung für die 129 Freiheitsgrade [INT09b]

d	q	C	Freiheitgrade	Tabellenwerte der $0,95$-Quantile der χ^2-Verteilung
4	3	$3,33$	3	$7,85$
4	4	$3,047$	4	$9,488$
4	5	$10,92$	9	$16,919$
4	7	$13,332$	15	$24,996$
5	2	$1,3$	2	$5,991$
5	3	4	7	$14,067$
5	4	13	16	$27,587$
5	5	26	30	$38,885$
6	2	$8,8$	4	$9,488$
6	3	$79,99$	23	$35,172$
7	2	$10,28$	8	$15,507$
7	3	$137,85$	34	$48,602$
8	2	$46,1$	15	$26,296$
8	3	> 537	129	< 234

Diese Tabelle zeigt, dass man für die Grade 4 und 5 die Hypothese einer Gleichverteilung annehmen würde. Während sie für größere Grade abgelehnt werden muss. Die Tatsache, dass der Wert für V stärker von dem Tabellenwerte der χ^2-Verteilung abweicht je größer d wird, ist ein Indiz dafür, dass die Verteilung mit steigendem Grad immer stärker von einer Gleichverteilung abweicht. Dies deutet darauf hin, dass keine einheitliche Verteilung für alle Fälle q und d vorliegt. Dies macht

es schwer, eine einheitliche Formel für alle d wie für $d < 4$ zu finden. Ich vermute, dass dies nur näherungsweise möglich ist. Um mehr Erkenntnisse zu gewinnen und vielleicht weitere Vermutungen aufzustellen, müssten weitere Untersuchungen durchgeführt werden, die aber den Rahmen dieser Arbeit übersteigen.

Kapitel 6

Zusammenfassung und Ausblick

Abschließend sollen noch einmal die Ergebnisse dieser Arbeit zusammen gefasst werden.
In Kapitel 3 haben wir gezeigt, dass die Rekursionsforel $\varphi_k(j)$ anstatt die Rekursionsformel $g_k(g, \Delta)$ zu betrachten, vorausgesetzt dass $g \neq 0$ und $j = \frac{g^{q+1}}{\Delta}$. Dies hat den Rechenaufwand erheblich reduziert.
Der Spezialfall $g = 0$ wurde im dritten Kapiteln seperat behandelt.
In Kapitel 4 haben wir zunächst bewiesen, dass diejenigen j, die durch affinen Transformationen oder Galoistransformationen ineinander übergehen, gleich viele supersinguläre Stellen haben und somit auch alle (g, Δ) für die gilt $j = \frac{g^{q+1}}{\Delta}$.
Anschließend wurde für ein festes j die Funktion H_j berechnet. Anhand der Daten ließen sich eine Reihe von Vermutungen aufstellen:

- Ist j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik 2, dann gibt es supersinguläre Paare (j, p) genau dann, wenn $grad(p)$ gerade ist.
- Ist j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik 2, so wächst die Funktion H_j exponentiell, wenn man nur die geraden Funktionswerte betrachtet.
- Ist j ein konstantes Polynom und $\mathbb{F}_q$ ein endlicher Körper mit der Charakteristik > 2, so kommen nur supersinguläre Stelle hinzu, wenn x ein Vielfaches der Charakteristik ist.
- Ist $j = a \cdot T$, so wächst H_j für manche $a \in \mathbb{F}_q$ schneller als für andere.
- Die Funktionrn H_j verläuft für alle nicht konstanten j zwischen zwei Exponentialfuktionen.
- Für nicht konstantes j wächst H_j exponentiell. Zudem gilt t_1 ist unabhängig von j.
- Die Funktion H_j ist von der Form $A_1 \cdot e^{(\frac{x}{t1})}$, wobei $t_1 = \frac{c}{ln(q)}$ für eine Kontsante c ist.

In Kapitel 5 wurde zunächst beobachtet, dass man für Grade $d < 4$ Formeln für $\sum_{\mathfrak{p}\ grad(\mathfrak{p})=d} |\{(g, \Delta) \mid (g, \Delta) \text{ ist supersingulär mod } \mathfrak{p}\}|$ angeben kann. Zudem haben in diesem Fall alle irreduziblen normierten Polynome eines festen Grades < 4 gleichviele supersinguläre Werte, während dies für höhere Grade nicht mehr der Fall ist. Für größere Grade läßt sich keine Formel dieser Art finden. Mithilfe des χ^2-Tests wurde nachgewiesen, dass für wachsende d die Verteilung der supersingulären Werte auf alle irreduziblen Polynome immer stärker von einer Gleichverteilung

abweicht.
Mit den ermittelten Daten wurde die folgende Näherung als recht präzise bestätigt. Jedes irreduzible Polynom vom Grad d hat im Mittel

$$c(q)\frac{q}{q-1}q^{\frac{d}{2}-1} \quad \text{, falls } d \text{ gerade}$$
$$c(q)\frac{q}{q-1}q^{\frac{d-1}{2}} \quad \text{, falls } d \text{ ungerade}$$

viele supersinguläre Werte. Hierbei ist $c(q)$ ein Korrekturfaktur, der für $q \to \infty$ gegen 1 läuft.

In dieser Arbeit wurden mit Hilfe numerischer Berechnungen Vermutungen aufgestellt, von denen die Mehrzahl jedoch noch unbewiesen ist. Diese Vermutungen ließen sich wahrscheinlich nur mit Hilfe der Theorie der Drinfeld-Moduln bewiesen, da es mit den in dieser Arbeit verwendeten Grundlagen kaum möglich ist. Ergänzend zu Kapitel 4 könnte man noch weitere Untersuchen dazu anstellen, für welche j die Funktion H_j schneller wächst.
Mit Hilfe eines leistungfähigeren Servers könnte auch der weitere Velauf von H_j für konstante j über Köper mit Charakteristik > 2 ermittelt werden. Des Weiteren bleibt noch zu bestimmen, wie genau t_1 von q abhängt.
Vor allem in Kapitel 5 besteht noch viel Forschungsbedarf. Durch Anstellen weiterer Berechnungen an einem leistungsfähigeren Server ließe sich eventuell herausfinden, ob die Verteilung der supersingulären Werte einer statistischen Verteilung folgt. Möglicherweise ließe sich dann auch für größere Grade eine exakte Formel für $\sum_{\mathfrak{p}\ grad(\mathfrak{p})=d} |\{(g,\Delta) \mid (g,\Delta) \text{ ist supersingulär mod } \mathfrak{p}\}|$ finden.

Dieses Gebiet bietet also noch viele Forschungsmöglichkeiten und lässt noch sehr viele offene Fragestellungen und Probleme zu.

Symbolverzeichnis

$[k] := T^{q^k} - T$, , Seite 10

$\chi(k)$ ergibt 1, wenn k ungerade ist und 0 wenn k ungerade ist , Seite 16

Δ, ein Element aus A ohne $\mathfrak{p}$ bzw. $\mathbb{F}_{\mathfrak{p}}^*$, Seite 13

$\mathbb{F}_{\mathfrak{p}}$ der Restköreper $A/\mathfrak{p}$, Seite 13

$\mathbb{F}_q$, der endliche Körper mit q Elementen , Seite 7

$\mathfrak{p}$, das von einem irreduziblen Polynom f in A erzeugte Primideal , Seite 13

$\mu(n)$, Möbiusfunktion , Seite 9

$\varphi_k(X)$, die durch die Formel $\varphi_k(X) = X^{\frac{q^{k-1}+(-1)^k}{q+1}} \cdot \varphi_{k-1}(X) - [k-1] \cdot \varphi_{k-2}(X)$ und die Startwerte $\varphi_0 = \varphi_1 = 1$ definierte Rekursionsformel , Seite 16

A der Polynomring in einer Variablen T über dem endlichen Körper $\mathbb{F}_q$, Seite 9

g, ein Element aus A bzw. $\mathbb{F}_{\mathfrak{p}}$, Seite 13

g_k, die durch die Foremel $g_k(g, \Delta) := -[k-1]g_{k-2}\Delta^{q^{k-2}} + g_{k-1}g^{q^{k-1}}$ und die Startwerte $g_0 := 1$, $g_1 := g$ definierte Rekursionsformel , Seite 13

$I(q, k; T)$, Produkt aller normierten irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k , Seite 10

j, $\frac{g^{q+1}}{\Delta}$, Seite 15

L^G der Fixkörper unter der Gruppe G , Seite 11

$N_q(k)$, Anzahl aller normierten irreduziblen Polynome in $\mathbb{F}_q[T]$ vom Grad k , Seite 10

Tr_K^L, die Spur eines Elements aus L über K , Seite 8

Literaturverzeichnis

[AHU75] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1975, Second printing, Addison-Wesley Series in Computer Science and Information Processing. MR MR0413592 (54 #1706)

[BCS97] Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi, *Algebraic complexity theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 315, Springer-Verlag, Berlin, 1997, With the collaboration of Thomas Lickteig. MR MR1440179 (99c:68002)

[Bos06a] Siegfried Bosch, *Algebra*, 6. ed., Springer-Verlag, Berlin, Heidelberg, 2006.

[Bos06b] ———, *Lineare Algebra*, 6. ed., Springer-Verlag, Berlin, Heidelberg, 2006.

[INT09a] *http://psydok.sulb.uni-saarland.de/volltexte/2004/268/html/chivert.htm*, 21.08.2009.

[INT09b] *http://www.faes.de/basis/basis-statistik/basis-statistik-chi-quad-test/basis-statistik-chi-quad-tabel/basis-statistik-chi-quad-tabel.html*, 21.08.2009.

[Kre05] Ulrich Krengel, *Einführung in die Wahrscheinlichkeitstheorie und Statistik*, 8. ed., Vieweg Verlag, Wiesbaden, 2005.

[LN94] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994. MR MR1294139 (95f:11098)

[MG90] Helmut Meyn and Werner Götz, *Self-reciprocal polynomials over finite fields*, Séminaire Lotharingien de Combinatoire (Oberfranken, 1990), Publ. Inst. Rech. Math. Av., vol. 413, Univ. Louis Pasteur, Strasbourg, 1990, pp. 82–90. MR MR1126955 (92k:11141)

[Neu07] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, Heidelberg, 2007.

[SP07] Rainer Schulze-Pillot, *Elementare Algebra und Zahlentheorie*, 1. ed., Springer-Verlag, Berlin, Heidelberg, 2007.