Johannes Gutenberg–Universität Mainz

Die L-Reihen einiger symmetrischer Quintiken

Diplomarbeit

vorgelegt dem Fachbereich Mathematik
im August 2000
von

Christian Meyer
Erbacher Str. 19 b
55262 Heidesheim

Das Thema stellte
Herr Prof. D. van Straten

Inhaltsverzeichnis

Einleitung

Stellen wir uns eine Hyperfläche im n-dimensionalen projektiven Raum über $\mathbb{C}$ vor, die durch eine Gleichung gegeben ist, deren Koeffizienten in $\mathbb{Z}$ liegen. Dann können wir durch Reduktion dieser Koeffizienten modulo einer Primzahl p die Hyperfläche als Varietät im n-dimensionalen projektiven Raum über dem endlichen Körper $\mathbb{F}_p$ betrachten. Dort enthält sie natürlich nur endlich viele Punkte, und wir können uns fragen, wieviele es denn nun genau sind. Der erste Ansatz mag sein, polynomielle Abhängigkeit von p zu vermuten. Das ist oft eine gute Näherung, aber selten genau richtig. Man wird häufig Formeln der Art

$$\begin{aligned} \text{Anzahl Punkte bei Reduktion modulo } p \quad &= \\ \text{Polynom in } p \text{ vom Grad } (n-1) \quad &+ \quad \text{ein Rest } a_p \end{aligned}$$

finden, so daß der "Rest" a_p klein ist gegenüber p^{n-1}. Das Erstaunliche ist nun, daß die a_p, wenn das Polynom in $p-1$ richtig gewählt ist, oft eine Interpretation haben, die ein ganz anderes Gebiet der Mathematik eröffnet. Die "richtige Wahl" hängt mit den eventuell vorhandenen Singularitäten der Hyperfläche sowie einigen Invarianten wie ihrer Kohomologie zusammen; bei "richtiger Wahl" wollen wir die a_p als Koeffizienten einer Reihe auffassen, der *L-Reihe* der Hyperfläche.

Das "ganz andere Gebiet der Mathematik" ist das der *modularen Formen*. Das sind analytische Funktionen mit sehr speziellen Symmetrieeigenschaften. Modulare Formen haben eine Reihenentwicklung "in ∞" mit Koeffizienten b_n; und zwar derart, daß es ausreicht, die Koeffizienten b_p für alle Primzahlen zu kennen, da die Koeffizienten bei b_n durch Multiplikation der Koeffizienten zu den Primfaktoren von n entstehen.

Häufig scheint es nun so zu sein, daß sich die a_p als Koeffizienten der Reihenentwicklung einer modularen Form (oder eventuell als Linearkombination der Koeffizienten der Reihenentwicklungen mehrerer modularer Formen) auffassen lassen, d.h. die L-Reihe der Hyperfläche ist gleich einer Reihe, die durch modulare Formen bestimmt wird. In diesem Fall wird die Hyperfläche dann *modular* genannt.

Üblicherweise stellt man eine Modularitätsvermutung auf, indem man die Punkte auf der gegebenen Hyperfläche für einige Primzahlen zählt und dann versucht, "passende" modulare Formen zu finden. Das kann schon schwierig genug sein. Noch schwieriger ist es meistens, Gleichheit für *alle* (oder zumindest fast alle) Primzahlen zu zeigen. Es gibt aber erstaunliche Resultate, die im Prinzip besagen, daß die Gleichheit für fast alle Primzahlen folgt, wenn sie für eine geschickt gewählte *endliche* Teilmenge feststeht.

Für eine ganz bestimmte Klasse von Hyperflächen, nämlich einige *elliptische Kurven*, war der Nachweis, daß sie modular sind, stark genug, um die berühmte Fermatsche Vermutung zu beweisen.

Wir wollen Untersuchungen auf Modularität für gewisse Hyperflächen, nämlich einige Mitglieder einer Familie von Quintiken im 4-dimensionalen Raum, anstellen. Wir gehen dabei folgendermaßen vor:

Kapitel 1: Wir stellen die erwähnte Familie vor. Sie enthält ein besonders interessantes Mitglied $\mathcal{M}$, um das wir uns in den folgenden Kapiteln zunächst bemühen.

Kapitel 2: Wir untersuchen die Singularitäten von $\mathcal{M}$ über den endlichen Körpern $\mathbb{F}_p$. Natürlich hängt es von p ab, welche Singularitäten vorkommen. Wir lösen dann die Singularitäten über $\mathbb{C}$ durch Blow-Up auf (d.h. wir verschaffen uns ein glattes Modell $\tilde{\mathcal{M}}$ von $\mathcal{M}$) und überlegen, für welche p auf diese Weise auch die Singularitäten von $\mathcal{M}$ über $\mathbb{F}_p$ aufgelöst werden. Wir benötigen $\tilde{\mathcal{M}}$ später zum Beweis der Modularität von $\mathcal{M}$.

Kapitel 3: Wir wollen für einige Primzahlen p die Punkte auf den Quintiken über $\mathbb{F}_p$ zählen. Dazu müssen wir den Computer benutzen. Es ist sehr leicht, einen einfachen Zählalgorithmus zu implementieren. Wir geben uns etwas mehr Mühe und sparen insbesondere viel Rechenzeit durch Ausnutzen von Symmetrie.

Kapitel 4: Wir wollen die Modularität von $\mathcal{M}$ zeigen und führen die dazu nötigen Werkzeuge ein, insbesondere Galois-Darstellungen, étale-Kohomologie, die Weil-Vermutungen, modulare Formen und nicht-kubische Teilmengen von Vektorräumen. Wir rechnen unterwegs die Kohomologie von $\tilde{\mathcal{M}}$ mit einer Methode aus, die ausnutzt, daß wir Punkte über endlichen Körpern zählen können. Schließlich können wir für $\mathcal{M}$ die Modularität zeigen.

Kapitel 5: Wir wenden die Methoden aus Kapitel 2 und Kapitel 4 in komprimierter Form auf einige andere außergewöhnliche Mitglieder der Familie von Quintiken an und können hier jeweils mindestens die Modularität mit Begründung vermuten und in einigen Fällen auch beweisen.

Ich setze in dieser Arbeit Kenntnisse aus der Algebraischen Geometrie voraus, insbesondere über Singularitäten von Hyperflächen und deren Auflösung durch Blow-Up. Ich versuche, spezielle Konzepte aus der algebraischen Zahlentheorie wie Frobeniuselemente und Galois-Darstellungen zu erklären. Die Theorie der modularen Formen wird nur so weit vorgestellt, wie nötig. Viele der verwendeten Methoden sind sehr tiefliegend und schwer in wenigen Worten zu vermitteln. Ich vereinfache daher gelegentlich und führe die Methoden nur für die benötigten Spezialfälle vor. Ich habe mich bemüht, dann erklärende Literatur anzugeben. Gerade das Gebiet der Modularitätsvermutungen ist jedoch noch wenig erforscht, und die vorhandene Literatur ist sehr schwierig zu lesen. Trotzdem (oder vielleicht gerade deswegen) habe ich das Thema sehr interessant gefunden, auch weil es so verschiedene Gebiete der Mathematik miteinander verbindet.

Ich möchte mich daher bei Herrn Prof. van Straten für das interessante Thema und für die gute Betreuung, insbesondere die ständige Ansprechbarkeit, bedanken. Ich danke auch allen, denen ich einmal eine Frage zu dieser Arbeit gestellt habe; die Antwort hat mir immer weitergeholfen. Besonders möchte ich auch meinen Eltern danken, die mir durch ihre Unterstützung das Studium erst ermöglicht haben.

In dieser Version der Arbeit habe ich einige Fehler behoben. Vielen Dank an den Zweitkorrektor, Herrn Prof. Pfister, der mich auf die meisten aufmerksam gemacht hat.

Darüberhinaus habe ich das Literaturverzeichnis ergänzt. Der Artikel [21] ist inzwischen im *Journal of Number Theory* erschienen. In Kapitel 2 wird des Weiteren eine Arbeit von M. Saito und N. Yui erwähnt. Diese ist jetzt als Preprint veröffentlicht ([14]).

Die in Kapitel 5 behandelte L-Reihe der Barth-Nieto-Quintik $\mathcal{M}_{(1:0)}$ ist auch ein Gegenstand der inzwischen ebenfalls als Preprint verfügbaren Arbeit von K. Hulek, J. Spandaw, B. van Geemen und D. van Straten in [9].

Notationen

Standardbezeichnungen

Symbol	Bedeutung
$\mathbb{P}$	die Menge aller Primzahlen
$\mathbb{N}$	die Menge der natürlichen Zahlen
$\mathbb{Q}$	der Körper der rationalen Zahlen
$\mathbb{R}$	der Körper der reellen Zahlen
$\mathbb{C}$	der Körper der komplexen Zahlen
$\mathbb{H}$	die obere Halbebene von $\mathbb{C}$
$\mathbb{F}_p$	der Körper mit p Elementen für ein $p \in \mathbb{P}$
$\mathbb{P}^i(\mathbb{K})$	der i-dimensionale projektive Raum über dem Körper $\mathbb{K}$
$\overline{\mathbb{K}}$	ein algebraischer Abschluß des Körpers $\mathbb{K}$
$\#A$	Mächtigkeit der (endlichen) Menge A

Wir wollen Varietäten über $\mathbb{C}$ betrachten, die durch Gleichungen gegeben sind, deren Koeffizienten in $\mathbb{Z}$ liegen. Solche Gleichungen können wir modulo p reduzieren und uns die Varietät über dem endlichen Körper $\mathbb{F}_p$ anschauen. Wir wollen dabei immer dasselbe Symbol für die Varietät benutzen. Es ergibt sich dann aus dem Zusammenhang, welcher Körper gemeint ist. Genauso schreiben wir $\mathbb{P}^i$ statt $\mathbb{P}^i(\mathbb{K})$, wenn klar ist, um welchen Körper es sich handelt.

Elementar-symmetrische Funktionen

Sei $\mathbb{K}$ ein Körper, und seien $X_0, X_1, \ldots, X_n$ Variablen mit Werten in $\mathbb{K}$. Wir bezeichnen mit

$$S_i(X_0, X_1, \ldots, X_n) := \sum_{0 \le j_1 < \cdots < j_i \le n} X_{j_1} X_{j_2} \cdots X_{j_i}$$

die i-te *elementar-symmetrische Funktion* in den X_j. Wir wollen die Formeln meistens für $n = 5$ benutzen und kürzen deswegen ab:

$$S_i := S_i(X_0, X_1, \ldots, X_5).$$

Kapitel 1

Die Quintiken

Sei $\mathbb{K}$ ein Körper. Die Gleichung

$$S_1 = X_0 + X_1 + X_2 + X_3 + X_4 + X_5 = 0$$

definiert einen $\mathbb{P}^4(\mathbb{K}) \subset \mathbb{P}^5(\mathbb{K})$, auf dem die symmetrische Gruppe Σ_6 durch Permutation der Koordinaten operiert. Durch

$$\begin{aligned} S_1 &= 0 \\ \alpha S_5 + \beta S_2 S_3 &= 0 \quad \text{mit } (\alpha : \beta) \in \mathbb{P}^1(\mathbb{K}) \end{aligned}$$

ist daher eine Familie von Quintiken $\mathcal{M}_{(\alpha:\beta)} \subset \mathbb{P}^4(\mathbb{K})$ gegeben, die invariant sind unter der Operation von Σ_6.

In [19] wurde diese Familie über $\mathbb{C}$ untersucht. Für allgemeines $(\alpha : \beta) \in \mathbb{P}^1$ hat $\mathcal{M}_{(\alpha:\beta)}$ genau 100 (isolierte) Singularitäten, die alle gewöhnliche Doppelpunkte ("nodes") sind, nämlich:

Die "Segre nodes": Die Σ_6-Bahn von

$$(1 : 1 : 1 : -1 : -1 : -1), \qquad \text{insgesamt 10 Punkte}$$

Die "Moving nodes": Die Σ_6-Bahn von

$$(1 : 1 : -1 : -1 : z : -z), \qquad \text{insgesamt 90 Punkte}$$

z ist hierbei eine Lösung der Gleichung $\beta z^2 + (\alpha + 2\beta) = 0$.

Die Bezeichung "Segre nodes" rührt daher, daß diese Punkte auch die singulären Punkte der *Segre-Kubik*

$$S_1 = S_3 = 0$$

sind (vgl. [15]). Der Name "Moving nodes" entstand aus der Tatsache, daß sich diese Punkte bei wechselndem $(\alpha : \beta)$ über die 45 Geraden bewegen, die die 10 "Segre nodes" verbinden.

Für 6 Punkte $(\alpha : \beta) \in \mathbb{P}^1$ ist der singuläre Ort anders:

$(\alpha : \beta)$	sing. Ort	Punkt auf der Σ_6-Bahn	#Punkte
$(25 : 1)$	106 nodes	$(1 : 1 : 1 : -1 : -1 : -1)$	10 nodes
		$(1 : 1 : -1 : -1 : 3\sqrt{-3} : -3\sqrt{-3})$	90 nodes
		$(1 : 1 : 1 : 1 : 1 : -5)$	6 nodes
$(1 : 1)$	130 nodes	$(1 : 1 : 1 : -1 : -1 : -1)$	10 nodes
		$(1 : 1 : -1 : -1 : \sqrt{-3} : -\sqrt{-3})$	90 nodes
		$(1 : 1 : 1 : 1 : \sqrt{-3} - 2 : -\sqrt{-3} - 2)$	30 nodes
$(-3 : 1)$	10 "Del Pezzo" nodes	$(1 : 1 : 1 : -1 : -1 : -1)$	
$(0 : 1)$	Die Fläche $S_2 = S_3 = 0$		
$(-2 : 1)$	10 nodes und 15 Geraden	$(1 : 1 : 1 : -1 : -1 : -1)$	10 nodes
		$(x : x : y : y : z : z)$	15 Geraden
		$x + y + z = 0$	
$(1 : 0)$	10 nodes und 20 Geraden	$(1 : 1 : 1 : -1 : -1 : -1)$	10 nodes
		$(0 : 0 : 0 : x : y : z)$	20 Geraden
		$x + y + z = 0$	

Besonders interessant ist das Familienmitglied

$$\mathcal{M} := \mathcal{M}_{(1:1)}.$$

Diese Quintik hat genau 130 gewöhnliche Doppelpunkte. Eine Quintik in $\mathbb{P}^4$ kann höchstens 135 gewöhnliche Doppelpunkte aufweisen (vgl. [20]); und $\mathcal{M}$ ist zur Zeit das Beispiel, das dieser Schranke am nächsten kommt. Außer den "Segre nodes" und den "Moving nodes" verfügt $\mathcal{M}$ noch über 30 "Extra nodes", nämlich die Σ_6-Bahn des Punktes

$$(1 : 1 : 1 : 1 : \sqrt{-3} - 2 : -\sqrt{-3} - 2).$$

Die Quintik $\mathcal{M}_{(1:0)}$ ist auch als *Barth-Nieto-Quintik* bekannt. Viele Informationen darüber finden sich in [1], neuerdings auch in [9].

Bei der Quintik $\mathcal{M}_{(-3:1)}$ fallen jeweils 9 "Moving nodes" mit einem "Segre node" zusammen. Die entstehende Singularität ist lokal isomorph zu dem Kegel über der (glatten) kubischen Fläche in $\mathbb{P}^3$, daher der Name "Del Pezzo node".

Kapitel 2

Singularitäten von $\mathcal{M}$ und ihre Auflösung

2.1 Singularitäten von $\mathcal{M}$ über $\mathbb{F}_p$

Wir wollen nun den singulären Ort von $\mathcal{M}$, jeweils aufgefasst als Varietät über den endlichen Körpern $\mathbb{F}_p, p \in \mathbb{P}$ untersuchen. Die Fälle $p = 2$ und $p = 3$ werden dabei eine Sonderstellung einnehmen.

2.1.1 Wann ist -3 ein Quadrat?

Über $\mathbb{C}$ hat $\mathcal{M}$ Singularitäten, deren Koordinaten algebraisch von $\sqrt{-3}$ abhängen. Wir werden daher bei der Untersuchung der Singularitäten von $\mathcal{M}$ über den $\mathbb{F}_p$ wissen müssen, in welchen $\mathbb{F}_p$ die Zahl -3 ein Quadrat ist.

2.1 Definition
Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, p) = 1$. *Das* Legendre-Symbol *zu a und p ist definiert als*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls es ein } b \in \mathbb{Z} \text{ gibt mit } a \equiv b^2 \pmod{p} \\ -1 & \text{sonst} \end{cases}$$

Wir geben zwei bekannte Eigenschaften des Legendre-Symbols an (vgl. [7], Kapitel 6):

2.2 Lemma
1. *Sei $p \in \mathbb{P}$ ungerade. Dann gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

2. Quadratisches Reziprozitätsgesetz:

Seien $p \neq q \in \mathbb{P}$ ungerade. Dann gilt

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \textit{falls } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \textit{sonst} \end{cases}$$

Damit können wir die Frage beantworten, in welchen Körpern $\mathbb{F}_p$ die Zahl -3 ein Quadrat ist:

2.3 Satz
Sei $p \in \mathbb{P}, p \geq 5$. Dann gilt

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \textit{falls } p \equiv 1, -5 \pmod{12} \\ -1 & \textit{falls } p \equiv -1, 5 \pmod{12} \end{cases}.$$

Beweis:

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 3 \\ -1 & \text{falls } p \equiv -1 \pmod 3 \end{cases}$$

$$\begin{aligned} \text{Also } \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) &= \begin{cases} (-1)^{\frac{p-1}{2}} & \text{falls } p \equiv 1 \pmod 3 \\ -(-1)^{\frac{p-1}{2}} & \text{falls } p \equiv -1 \pmod 3 \end{cases} \\ &= \begin{cases} 1 & \text{falls } p \equiv \pm 1 \pmod{12} \\ -1 & \text{falls } p \equiv \pm 5 \pmod{12} \end{cases}. \end{aligned}$$

$$\begin{aligned} \text{Wegen } \left(\frac{-3}{p}\right) &\equiv (-3)^{\frac{p-1}{2}} \pmod p, \\ \left(\frac{3}{p}\right) &\equiv 3^{\frac{p-1}{2}} \pmod p \\ \text{und } (-3)^{\frac{p-1}{2}} &= \begin{cases} 3^{\frac{p-1}{2}} & \text{falls } p \equiv 1 \pmod 4 \\ -3^{\frac{p-1}{2}} & \text{falls } p \equiv 3 \pmod 4 \end{cases} \\ \text{folgt } \left(\frac{-3}{p}\right) &= \begin{cases} 1 & \text{falls } p \equiv 1, -5 \pmod{12} \\ -1 & \text{falls } p \equiv -1, 5 \pmod{12} \end{cases}. \end{aligned}$$

2.1.2 Singularitäten im Fall $p \geq 5$

Es ist gelegentlich angenehm, die S_i mit Hilfe der Potenzsummen

$$C_k := C_k(X_0, X_1, \ldots, X_5) := \sum_{i=0}^{5} {X_i}^k$$

auszudrücken. Modulo S_1 gilt nämlich:

$$\begin{aligned} S_2 &= -\frac{1}{2}C_2 \\ S_3 &= \frac{1}{3}C_3 \\ S_4 &= -\frac{1}{4}C_4 + \frac{1}{8}{C_2}^2 \\ S_5 &= \frac{1}{5}C_5 - \frac{1}{6}C_2C_3 \end{aligned}$$

Über $\mathbb{F}_2$ und $\mathbb{F}_3$ sind nicht alle dieser Gleichungen definiert. Wir werden daher diese beiden Fälle gesondert betrachten. Sei also im Folgenden $p \geq 5$ fest. Um den Fall $p = 5$ nicht auch auszuschließen (die Rechnungen werden zeigen, daß es dafür auch keinen Grund gibt), werden wir die angegebene Gleichung für S_5 nicht benutzen. Sei

$$F := S_5 + S_2S_3$$

das $\mathcal{M}$ definierende Polynom. Ein Punkt $\eta := (\eta_0 : \eta_1 : \ldots : \eta_5) \in \mathbb{P}^4(\mathbb{F}_p) \subset \mathbb{P}^5(\mathbb{F}_p)$ (d.h. $S_1(\eta) = 0$) auf $\mathcal{M}$ ist singulär genau dann, wenn die Differentiale der beiden definierenden Gleichungen in $\mathbb{P}^5(\mathbb{F}_p)$ linear abhängig sind, wenn also für ein $(\nu : \mu) \in \mathbb{P}^1(\mathbb{F}_p)$ gilt:

$$\nu\partial_i F(\eta) = \mu\partial_i S_1(\eta)$$

Es gilt $\mu\partial_i S_1(\eta) = \mu$, also können wir $\nu \neq 0$ annehmen und daher $\nu = 1$ setzen. Wir erhalten

$$\begin{aligned} \mu &= \partial_i F(\eta) \\ &= \partial_i S_5(\eta) + (\partial_i S_2(\eta))S_3(\eta) + S_2(\eta)(\partial_i S_3(\eta)) \\ &= S_4(\eta) - \eta_i(S_3(\eta) - \eta_i(S_2(\eta) - \eta_i(S_1(\eta) - \eta_i))) \\ &\quad +(S_1(\eta) - \eta_i)S_3(\eta) + S_2(\eta)(S_2(\eta) - \eta_i(S_1(\eta) - \eta_i)) \\ &= S_4(\eta) - \eta_i(S_3(\eta) - \eta_i(S_2(\eta) + {\eta_i}^2)) - \eta_i S_3(\eta) + S_2(\eta)(S_2(\eta) + {\eta_i}^2) \\ &= S_4(\eta) + {\eta_i}^4 + 2{\eta_i}^2 S_2(\eta) - 2\eta_i S_3(\eta) + S_2(\eta)^2 \\ &= {\eta_i}^4 - {\eta_i}^2 C_2(\eta) - \frac{2}{3}C_3(\eta)\eta_i - \frac{1}{4}C_4(\eta) + \frac{3}{8}C_2(\eta)^2 \end{aligned}$$

Wir summieren über alle i, um μ zu eliminieren:

$$\begin{aligned} 6\mu &= \sum_{i=0}^{5}\Big(S_4(\eta) + {\eta_i}^4 + 2{\eta_i}^2 S_2(\eta) - 2\eta_i S_3(\eta) + S_2(\eta)^2\Big) \\ &= 6S_4(\eta) + C_4(\eta) + 2C_2(\eta)S_2(\eta) + 6S_2(\eta)^2 \\ &= -\frac{1}{2}C_4(\eta) + \frac{5}{4}C_2(\eta)^2 \end{aligned}$$

Also muß jede Koordinate η_i von η der Gleichung

$$P(X) := X^4 - C_2X^2 - \frac{2}{3}C_3X - \frac{1}{6}(C_4 - C_2^2) = 0$$

genügen, wobei $C_i = C_i(\eta)$.

Wir fassen nun C_2, C_3, C_4 als variable Konstanten auf und bezeichnen die Nullstellen von P in $\overline{\mathbb{F}_p}$ mit x, y, z, t. Da der Koeffizient von P bei X^3 gleich Null ist, gilt $x + y + z + t = 0$. A priori gibt es neun Möglichkeiten, wie die Koordinaten η_i eines singulären Punktes η von $\mathcal{M}$ über diese vier Nullstellen verteilt sein können:

Fall 1 :	$6x$	Fall 4 :	$3x, 3y$	Fall 7 :	$2x, 2y, 2z$
Fall 2 :	$5x, y$	Fall 5 :	$4x, y, z$	Fall 8 :	$3x, y, z, t$
Fall 3 :	$4x, 2y$	Fall 6 :	$3x, 2y, z$	Fall 9 :	$2x, 2y, z, t$

Wir untersuchen die einzelnen Fälle:

Fall 1: kann nicht auftreten, da aus $0 = S_1(\eta) = S_1(x : x : \ldots : x)$ für $p \geq 5$ folgen würde, daß $x = 0$.

Fall 2: Wir können annehmen, daß $\eta = (1 : 1 : 1 : 1 : 1 : -5)$. Damit ist $C_2 = 30, C_3 = -120, C_4 = 630$ und

$$P(X) = X^4 - 30X^2 + 80X + 45.$$

Damit haben wir $P(1) = 96 = 3 \cdot 2^5$; deshalb kann auch dieser Fall für $p \geq 5$ nicht auftreten.

Fall 3: Wir können annehmen, daß $\eta = (1 : 1 : 1 : 1 : -2 : -2)$. Damit ist $C_2 = 12, C_3 = -12, C_4 = 36$ und

$$P(X) = X^4 - 12X^2 + 8X + 18.$$

Damit haben wir $P(1) = 15$ und $P(-2) = -30$; deshalb kann auch dieser Fall für $p > 5$ nicht auftreten. Für $p = 5$ liegt η nicht auf $\mathcal{M}$.

Fall 4: Wir können annehmen, daß $\eta = (1 : 1 : 1 : -1 : -1 : -1)$. Damit ist $C_2 = 6, C_3 = 0, C_4 = 6$ und

$$P(X) = X^4 - 6X^2 + 5.$$

Für alle $p \geq 5$ ist $P(1) = P(-1) = 0$.

Fall 5: Wir können annehmen, daß

$$\eta = (x : x : x : x : u - 2x : -u - 2x).$$

Im Fall $x = 0, u = 1$ folgt $P(X) = X^4 - 2X^2 + \frac{1}{3}$; wegen der Forderung $P(0) = 0$ kommt dieser Fall nicht vor.

Wir nehmen also an, daß $\eta = (1 : 1 : 1 : 1 : u - 2 : -u - 2)$. Damit ist $C_2 = 12 + 2u^2, C_3 = -12 - 12u^2, C_4 = 36 + 48u^2 + 2u^4$. Auswertung von P bei $X = 1, X = u - 2, X = -u - 2$ liefert folgende Gleichungen:

$$\begin{aligned} u^4 + 18u^2 + 45 &= 0 \\ u^4 - 12u^3 + 18u^2 - 36u + 45 &= 0 \\ u^4 + 12u^3 + 18u^2 + 36u + 45 &= 0. \end{aligned}$$

Addition der letzten beiden Gleichungen liefert die erste, Subtraktion hingegen

$$u^3 + 3u = 0.$$

Die Lösung $u = 0$ würde in Fall 3 zurückführen, wir nehmen also $u \neq 0$ an. Wir erhalten als weitere Lösungen:

$$u = \pm\sqrt{-3}.$$

Fall 6: Wir können annehmen, daß

$$\eta = (x : x : x : u - x : u - x : -2u - x).$$

Im Fall $x = 0, u = 1$ folgt $P(X) = X^4 - 6X^2 + 4X + 3$; wegen der Forderung $P(0) = 0$ kommt dieser Fall nicht vor.

Wir nehmen also an, daß $\eta = (1 : 1 : 1 : u - 1 : u - 1 : -2u - 1)$. Damit ist $C_2 = 6(u^2 + 1), C_3 = -6u^2(u + 3), C_4 = 6(3u^4 + 4u^3 + 6u^2 + 1)$. Auswertung von P bei $X = 1, X = u - 1$ liefert:

$$\begin{aligned} 3u^2(u^2 + 4) &= 0 \\ u(u^3 + 6u^2 - 6u + 4) &= 0 \end{aligned}$$

Die Lösung $u = 0$ führt zurück in Fall 4. Wir nehmen also $u \neq 0$ an. Einsetzen der ersten Gleichung in die zweite liefert dann:

$$u^2 + 5u - 6 = 0, \text{ also } u \in \{1, -6\}$$

Es ist $1^2 + 4 = 5$ und $(-6)^2 + 4 = 40$, daher erhalten wir für $p > 5$ keine weiteren Lösungen.

Für $p = 5$ ergeben sich die beiden Punkte $(1 : 1 : 1 : 0 : 0 : -3)$ und $(1 : 1 : 1 : -2 : -2 : 1)$. Ersterer liegt nicht auf $\mathcal{M}$, letzterer führt zurück in Fall 3.

Fall 7: Wir können annehmen, daß

$$\eta = (x : x : y : y : z : z) \text{ mit } x + y + z = 0.$$

Insbesondere muß auch die vierte Nullstelle t von P gleich Null sein. Damit muß $P(0) = 0$ gelten. Daraus folgt wiederum

$$P(X) = X^4 - C_2 X^2 - \frac{2}{3} C_3 X$$

sowie

$$0 = {C_2}^2 - C_4 = 4x^4 + 4y^4 + 4z^4 + 8x^2y^2 + 8x^2z^2 + 8y^2z^2.$$

Nehmen wir $x = 0$ an, so folgt sofort $y^4 + z^4 + 2y^2z^2 = 0$ und mit $y = -z$ dann $y = z = 0$. Also können wir jetzt $x = 1$ annehmen. Dann:

$$\begin{aligned} P(x) = P(1) &= 1 - C_2 - \frac{2}{3} C_3 \\ &= 1 - (2 + 2y^2 + 2(1+y)^2) - \frac{2}{3}(2 + 2y^3 - 2(1+y)^3) \\ &= 1 - 4(1 + y + y^2) - \frac{4}{3}(-3y - 3y^2) \\ &= -3 \end{aligned}$$

Also kommt dieser Fall nicht vor.

Fall 8: Wir können annehmen, daß

$$\eta = (x : x : x : y : z : t) \quad \text{mit} \quad 3x + y + z + t = 0.$$

Wegen $x + y + z + t = 0$ folgt sofort $x = 0, y + z + t = 0$. Wie in Fall 7 muß gelten:

$$P(X) = X^4 - C_2 X^2 - \frac{2}{3} C_3 X$$

sowie

$$0 = C_4 - {C_2}^2 = 2(y^2z^2 + y^2t^2 + z^2t^2).$$

Aus $t = 0$ folgt wieder $yz = 0$ und damit $y = z = 0$. Also können wir $t = 1$ annehmen. Dann:

$$\begin{aligned} P(t) = P(1) &= 1 - C_2 - \frac{2}{3} C_3 \\ &= 1 - (1 + y^2 + (1+y)^2) - \frac{2}{3}(1 + y^3 - (1+y)^3) \\ &= 1 - 2(1 + y + y^2) - \frac{2}{3}(-3y - 3y^2) \\ &= -1 \end{aligned}$$

Also kommt auch dieser Fall nicht vor.

Fall 9 Wir haben $2x + 2y + z + t = 0$ sowie $x + y + z + t = 0$ und können daher annehmen, daß

$$\eta = (x : x : -x : -x : z : -z).$$

Die Annahme $x = 0$ führt zurück in Fall 5, also setzen wir $x = 1$. Damit ist $C_2 = 4 + 2z^2, C_3 = 0, C_4 = 4 + 2z^4$ und

$$P(X) = X^4 - (4 + 2z^2)X^2 - \frac{1}{6}(-12 - 16z^2 - 2z^4).$$

Die Gleichungen $P(1) = P(-1) = P(z) = P(-z) = 0$ reduzieren sich auf

$$z^4 + 2z^2 - 3 = (z^2 + 3)(z^2 - 1) = 0$$

Mit $z^2 - 1 = 0$ sind wir wieder in Fall 4. Wir erhalten also zwei neue Lösungen:

$$z = \pm\sqrt{-3}$$

Wir fassen die Ergebnisse in folgendem Satz zusammen:

2.4 Satz
Sei $p \in \mathbb{P}, p \geq 5$. Dann hat $\mathcal{M}$ über $\mathbb{F}_p$ die folgenden Singularitäten:

Segre nodes: *Die Σ_6-Bahn von*

$$(1 : 1 : 1 : -1 : -1 : -1), \qquad \textit{insgesamt 10 Punkte}$$

Moving nodes: *Falls $p \equiv 1, -5 \pmod{12}$: Die Σ_6-Bahn von*

$$(1 : 1 : -1 : -1 : \sqrt{-3} : -\sqrt{-3}), \qquad \textit{insgesamt 90 Punkte}$$

Extra nodes: *Falls $p \equiv 1, -5 \pmod{12}$: Die Σ_6-Bahn von*

$$(1 : 1 : 1 : 1 : \sqrt{-3} - 2 : -\sqrt{-3} - 2), \qquad \textit{insgesamt 30 Punkte}$$

Dies sind die Fälle 4, 9 und 5 in der vorausgegangenen Untersuchung.

2.1.3 Singularitäten im Fall $p = 2$

Wir zeigen, daß in diesem Fall alle Punkte aus $\mathbb{P}^4$ auf $\mathcal{M}$ liegen. Sei dazu $\eta \in \mathbb{P}^5(\mathbb{F}_2)$ ein Punkt. Die Bedingung $\eta \in \mathbb{P}^4$ (d.h. $S_1(\eta) = 0$) liefert, daß eine gerade Anzahl der Koordinaten von η gleich Eins ist. Es gibt also (bis auf Vertauschung von Koordinaten) nur 3 Fälle:

Fall 1 $\eta = (1 : 1 : 0 : 0 : 0 : 0)$. In diesem Fall gilt offenbar $S_5(\eta) = S_3(\eta) = 0$ und damit $\eta \in \mathcal{M}$.

Fall 2 $\eta = (1 : 1 : 1 : 1 : 0 : 0)$. Es gilt $S_5(\eta) = S_2(\eta) = 0$ und damit wieder $\eta \in \mathcal{M}$.

Fall 3 $\eta = (1 : 1 : 1 : 1 : 1 : 1)$. Es gilt $S_5(\eta) = S_3(\eta) = 0$ und daher auch hier $\eta \in \mathcal{M}$.

2.1.4 Singularitäten im Fall $p = 3$

Sei wieder $\eta := (\eta_0 : \eta_1 : \ldots : \eta_5)$ ein singulärer Punkt von $\mathcal{M}$. Dann gilt wie im Fall $p \geq 5$ für ein $\mu \in \mathbb{F}_3$ und jedes $i \in \{0, \ldots, 5\}$

$$\begin{aligned} \mu &= S_4(\eta) + \eta_i^4 + 2\eta_i^2 S_2(\eta) - 2\eta_i S_3(\eta) + S_2(\eta)^2 \\ &= S_4(\eta) + S_2(\eta)^2 + \eta_i^2 - \eta_i^2 S_2(\eta) + \eta_i S_3(\eta) \\ &= -C_4(\eta) + \eta_i^2(1 - C_2(\eta)) + \eta_i S_3(\eta). \end{aligned}$$

Addition dreier solcher Gleichungen liefert, daß jedes η_i der Gleichung

$$\begin{aligned} 0 = P(X) &:= (1 - C_2)X^2 + S_3 X - 1 + C_2 - S_3 \\ &= (X - 1)((X + 1)(1 - C_2) + S_3) \end{aligned}$$

genügt, wobei wir $C_j = C_j(\eta)$ und $S_j = S_j(\eta)$ wieder als variable Konstanten auffassen. Der Koordinatenvektor eines singulären Punktes kann also höchstens zwei verschiedene Einträge enthalten. Wir können außerdem $\eta_0 = \eta_1 = 1$ annehmen. Wir betrachten die möglichen Fälle:

Fall 1 $\eta = (1 : 1 : 1 : 1 : 1 : 1)$ ist auf jeden Fall singulär.

Fall 2 $\eta = (1 : 1 : 1 : 0 : 0 : 0)$ ist nicht singulär, da in diesem Fall $S_3 = 1, C_2 = 0$ und $P(X) = (X - 1)^2$ folgt.

Fall 3 $\eta = (1 : 1 : 1 : -1 : -1 : -1)$ ist singulär. Hier gilt $S_3 = C_2 = 0$ und $P(X) = (X - 1)(X + 1)$.

$\tilde{\mathcal{M}}$ hat also über $\mathbb{F}_3$ genau 11 Singularitäten, nämlich den Punkt

$$(1 : 1 : 1 : 1 : 1 : 1)$$

und die "Segre-Nodes", die 10 gewöhnlichen Doppelpunkte auf der Σ_6-Bahn von

$$(1 : 1 : 1 : -1 : -1 : -1).$$

Im Punkt $(1 : 1 : 1 : 1 : 1 : 1)$ finden wir hier eine kompliziertere Singularität; der Tangentialkegel ist die durch

$$\begin{aligned} 0 &= 2(X_0^4 + X_1^4 + X_2^4 + X_3^4) \\ &+ 10(X_0^3X_1 + X_0X_1^3 + X_0^3X_2 + X_0X_2^3 + X_0^3X_3 + X_0X_3^3 + \\ &\qquad X_1^3X_2 + X_1X_2^3 + X_1^3X_3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3) \\ &+ 15(X_0^2X_1^2 + X_0^2X_2^2 + X_0^2X_3^2 + X_1^2X_2^2 + X_1^2X_3^2 + X_2^2X_3^2) \\ &+ 28(X_0^2X_1X_2 + X_0X_1^2X_2 + X_0X_1X_2^2 + X_0^2X_1X_3 + \\ &\qquad X_0X_1^2X_3 + X_0X_1X_3^2 + X_0^2X_2X_3 + X_0X_2^2X_3 + \\ &\qquad X_0X_2X_3^2 + X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2) \\ &+ 48X_0X_1X_2X_3 \end{aligned}$$

gegebene symmetrische Quartik in $\mathbb{P}^3$.

2.2 Auflösung der Singularitäten

2.2.1 Wie lösen wir auf?

Wir möchten nun die Singularitäten von $\mathcal{M}$ auflösen. Dazu blasen wir $\mathcal{M}$ (als Varietät über $\mathbb{C}$) entlang des singulären Orts auf. Die entstehende Varietät bezeichnen wir mit $\tilde{\mathcal{M}}$. Wir werden sehen, daß die Reduktion von $\tilde{\mathcal{M}}$ auf $\mathbb{F}_p$ für $p \geq 5$ wieder glatt ist, da alle Singularitäten von $\mathcal{M}$ in diesen Charakteristiken gewöhnliche Doppelpunkte sind, die auch schon über $\mathbb{C}$ auftreten. In den Fällen $p = 2$ und $p = 3$ gibt es zusätzliche Singularitäten, die auf diese Weise nicht aufgelöst werden. Wir sagen, daß 2 und 3 *Primzahlen von schlechter Reduktion* sind.

2.2.2 Um wieviel wird $\mathcal{M}$ dadurch größer?

Wir werden uns später für die Anzahl der Punkte interessieren, die auf $\tilde{\mathcal{M}}$ über $\mathbb{F}_p$ liegen, zumindest für die Primzahlen von guter Reduktion. Die Anzahl der Punkte auf $\mathcal{M}$ werden wir mit dem Computer bestimmen. Wir benötigen also die Zahl $\#\tilde{\mathcal{M}} - \#\mathcal{M}$ für jedes $p \in \mathbb{P}, p \geq 5$.

Wir bestimmen dazu für je einen Vertreter der Σ_6-Bahnen der Singularitäten von $\mathcal{M}$ die exceptionelle Menge des Blow-Up, also den Tangentialkegel. Dieser ist jeweils eine glatte Quadrik in $\mathbb{P}^3$, d.h. die Singularitäten sind tatsächlich gewöhnliche Doppelpunkte und werden durch den Blow-Up aufgelöst. Eine glatte Quadrik in $\mathbb{P}^3$ über einem algebraisch oder zumindest quadratisch abgeschlossenen Körper ist isomorph zu $\mathbb{P}^1 \times \mathbb{P}^1$ (d.h. sie verfügt über ein Regelsystem aus zwei Systemen von Geraden). Wir untersuchen, welche der Geraden auf der Quadrik rational über $\mathbb{F}_p$ sind und können daraus schließen, wieviele Punkte sie über $\mathbb{F}_p$ enthält.

Die Berechnung der definierenden Gleichungen der Tangentialkegel lassen wir jeweils vom Computer durchführen.

Die "Segre nodes"

Wir betrachten den Vertreter $P = (-1 : -1 : -1 : 1 : 1)$ in der affinen Karte $X_4 = 1$. Dann ist der Tangentialkegel gegeben durch

$$0 = S_2(X_0, \ldots, X_3) + X_3^2.$$

Diese Gleichung beschreibt offenbar eine glatte Quadrik in $\mathbb{P}^3$. Darauf liegen unter anderem die Punkte

$$P_1 = (1 : -1 : 0 : 1) \qquad \text{und} \qquad P_2 = (1 : -1 : 0 : -1).$$

Die Tangentialräume an P_1 und P_2 sind gegeben durch

$$2X_1 + X_2 + 2X_3 = 0 \qquad \text{und} \qquad 2X_0 + X_2 + 2X_3 = 0.$$

Wir erhalten als Schnitt der Tangentialräume mit der Quadrik die Geradenpaare

$$\begin{aligned} G_1 &= \{(a : b : 2a + 2b : -a - 2b) | (a : b) \in \mathbb{P}^1\}, \\ G_2 &= \{(a : b : 0 : -b) | (a : b) \in \mathbb{P}^1\} \end{aligned}$$

und

$$\begin{aligned} G_3 &= \{(a : b : 2a + 2b : -2a - b) | (a : b) \in \mathbb{P}^1\}, \\ G_4 &= \{(a : b : 0 : -a) | (a : b) \in \mathbb{P}^1\}. \end{aligned}$$

Wegen

$$det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 2 & 2 & 0 & 0 \\ 1 & 2 & 1 & 0 \end{pmatrix} = -4$$

gilt $G_1 \cap G_4 = \emptyset$.

Wir nehmen nun einen beliebigen Punkt auf G_4 und schneiden den Tangentialraum dort mit G_1. Der Tangentialraum an $(a : b : 0 : -a) \in G_4$ ist gegeben durch

$$(b - a)X_0 + bX_2 + (b - a)X_3 = 0.$$

Einsetzen von $(c : d : 2c + 2d : -c - 2d) \in G_1$ ergibt

$$bc + ad = 0.$$

G_1 und G_4 sind rational über $\mathbb{F}_p$, nach obigen Berechnungen aber auch jede der Geraden auf der Quadrik, die G_1 und G_4 schneiden. Damit sind alle Geraden des Regelsystems rational über $\mathbb{F}_p$, d.h. die Quadrik enthält dort genau $(p + 1)^2 = p^2 + 2p + 1$ Punkte.

Die "Moving nodes"

Wir betrachten den Vertreter $Q = (\sqrt{-3} : -\sqrt{-3} : -1 : -1 : 1)$ in der affinen Karte $X_4 = 1$. Dann ist der Tangentialkegel gegeben durch

$$\begin{aligned} 0 &= X_0X_1 + X_0X_2 + X_0X_3 + X_1X_2 + X_1X_3 - X_2X_3 \\ &+ \frac{1 - \sqrt{-3}}{2}X_0^2 + \frac{1 + \sqrt{-3}}{2}X_1^2. \end{aligned}$$

Auch diese Gleichung beschreibt eine glatte Quadrik in $\mathbb{P}^3$. Darauf liegen offenbar die Punkte

$$\begin{aligned} Q_1 &= (0:0:1:0) \text{ und} \\ Q_2 &= (0:0:0:1). \end{aligned}$$

Die Tangentialräume an Q_1 und Q_2 sind gegeben durch

$$X_0 + X_1 - X_3 = 0 \qquad \text{und} \qquad X_0 + X_1 - X_2 = 0.$$

Der Schnitt der beiden Tangentialräume und der Quadrik besteht aus den Punkten

$$\begin{aligned} Q_3 &= (1:-1:0:0) \text{ und} \\ Q_4 &= (\sqrt{-3}-1:2:\sqrt{-3}+1:\sqrt{-3}+1). \end{aligned}$$

Damit erhalten wir zwei Geraden auf der Quadrik, die sich nicht schneiden:

$$\begin{aligned} G_1 &= Q_1Q_3 \\ &= \{(a:-a:b-a:0) | (a:b) \in \mathbb{P}^1\} \quad \text{und} \\ G_2 &= Q_2Q_4 \\ &= \{((\sqrt{-3}-1)c:2c:(\sqrt{-3}+1)c:d+\sqrt{-3}c) | (c:d) \in \mathbb{P}^1\} \end{aligned}$$

Der Tangentialraum an $(a:-a:b-a:0) \in G_1$ ist gegeben durch

$$0 = (b - a(1+\sqrt{-3}))(X_0 + X_1) + (a-b)X_3.$$

Einsetzen von $((\sqrt{-3}-1)c:2c:(\sqrt{-3}+1)c:d+\sqrt{-3}c) \in G_2$ liefert

$$(2-\sqrt{-3})ac + bc + ad - bd = 0.$$

Die Quadrik verfügt also über ein Regelsystem, das dann rational über $\mathbb{F}_p$ ist, wenn $\sqrt{-3} \in \mathbb{F}_p$ gilt. Also enthält sie über $\mathbb{F}_p$ genau $(p+1)^2$ Punkte, wenn $p \equiv 1, -5 \pmod{12}$, sonst keine Punkte.

Die "Extra nodes"

Wir betrachten den Vertreter $R = (1:1:1:\sqrt{-3}-2:1)$ in der affinen Karte $X_4 = 1$. Dann ist der Tangentialkegel gegeben durch

$$\begin{aligned} 0 &= \sqrt{-3}\,((X_0 + \ldots + X_3)^2 - X_3^2) \\ &- 4X_3(X_0 + \ldots + X_3) \\ &- (X_0^2 + X_1^2 + X_2^2). \end{aligned}$$

Auch diese Gleichung beschreibt eine glatte Quadrik in $\mathbb{P}^3$. Der Ansatz

$$X_3 = 0, \qquad X_0 + X_1 + X_2 = 0$$

liefert die auf der Quadrik liegenden Punkte

$$\begin{aligned} R_1 &= (1+\sqrt{-3} : 1-\sqrt{-3} : -2 : 0) \text{ und} \\ R_2 &= (\sqrt{-3}-1 : \sqrt{-3}+1 : -2 : 0). \end{aligned}$$

Der Tangentialraum an R_1 ist gegeben durch

$$0 = (1+\sqrt{-3})X_0 + (1-\sqrt{-3})X_1 - 2X_2.$$

Der Ansatz

$$X_0 + X_1 - 2X_2 = 0, \qquad X_0 - X_1 = 0$$

liefert auf dem Schnitt des Tangentialraums an R_1 mit der Quadrik die Punkte

$$\begin{aligned} R_3 &= (2 : 2 : 2 : \sqrt{-3}-3) \text{ und} \\ R_4 &= (2 : 2 : 2 : 2\sqrt{-3}-3). \end{aligned}$$

Die Tangentialräume an R_3 und R_4 sind gegeben durch

$$\begin{aligned} 0 &= (2\sqrt{-3}+2)(X_0+X_1+X_2) + \sqrt{-3}X_3 \text{ und} \\ 0 &= (\sqrt{-3}+2)(X_0+X_1+X_2) - \sqrt{-3}X_3. \end{aligned}$$

Addition der Gleichungen liefert

$$X_3 = 0, \qquad X_0 + X_1 + X_2 = 0.$$

Wir erhalten also als Schnitt der beiden Tangentialräume und der Quadrik gerade die Punkte R_1 und R_2. Damit erhalten wir auf der Quadrik zwei Geraden, die sich nicht schneiden:

$$G_1 = R_1R_3 : \mathbb{P}^1 \to \mathbb{P}^3$$

$$(a:b) \mapsto (2a+b(\sqrt{-3}-1) : 2a-b(\sqrt{-3}+1) : 2a-4b : (a-b)(\sqrt{-3}-3)),$$

$$G_2 = R_2R_4 : \mathbb{P}^1 \to \mathbb{P}^3$$

$$(c:d) \mapsto (2c+d(\sqrt{-3}-3) : 2c+d(\sqrt{-3}-1) : 2c-4d : (c-d)(2\sqrt{-3}-3)).$$

Der Tangentialraum an

$$(2a+b(\sqrt{-3}-1) : 2a-b(\sqrt{-3}+1) : 2a-4b : (a-b)(\sqrt{-3}-3)) \in G_1$$

ist gegeben durch

$$\begin{aligned} 0 &= (2a+b(\sqrt{-3}-1))X_0 + (2a-b(\sqrt{-3}+1))X_1 \\ &+ (2a-4b)X_2 + (a-b)(\sqrt{-3}-3)X_3. \end{aligned}$$

Einsetzen von

$$(2c + d(\sqrt{-3} - 3) : 2c + d(\sqrt{-3} - 1) : 2c - 4d : (c - d)(2\sqrt{-3} - 3)) \in G_2$$

liefert

$$(9\sqrt{-3} + 15)ac - (9\sqrt{-3} - 19)ad - (15\sqrt{-3} + 27)bc + (4\sqrt{-3} + 6)bd = 0.$$

Die Quadrik verfügt also über ein Regelsystem, das dann rational über $\mathbb{F}_p$ ist, wenn $\sqrt{-3} \in \mathbb{F}_p$ gilt. Also enthält sie über $\mathbb{F}_p$ genau $(p+1)^2$ Punkte, wenn $p \equiv 1, -5 \pmod{12}$, sonst keine Punkte.

2.2.3 Zusammenfassung

Wir fassen die Untersuchungen in einem Satz zusammen:

2.5 Satz
Für $p \in \mathbb{P}, p \geq 5$ ist die Reduktion von $\tilde{\mathcal{M}}$ auf $\mathbb{F}_p$ wieder eine glatte Varietät. Darüber hinaus gilt:

- *Falls $p \equiv 1, -5 \pmod{12}$: Alle 130 Singularitäten und die Regelsysteme der Tangentialkegel sind rational über $\mathbb{F}_p$, und*

$$\#\tilde{\mathcal{M}} - \#\mathcal{M} = 130((p+1)^2 - 1) = 130(p^2 + 2p).$$

- *Falls $p \equiv -1, 5 \pmod{12}$: Nur die 10 Segre-Nodes (sowie die Regelsysteme ihrer Tangentialkegel) sind rational über $\mathbb{F}_p$, und*

$$\#\tilde{\mathcal{M}} - \#\mathcal{M} = 10((p+1)^2 - 1) = 10(p^2 + 2p).$$

Kapitel 3

Geschicktes Zählen von Punkten

Wir möchten zählen, wieviele Punkte $\mathcal{M}$ über $\mathbb{F}_p$ enthält. Dazu müssen wir eine bestimmte Menge von Punkten aus $\mathbb{P}^5(\mathbb{F}_p)$ in die $\mathcal{M}$ definierenden Gleichungen einsetzen. Wir sind daran interessiert, diese Menge möglichst klein zu halten, ohne den Aufwand für ihre Bestimmung zu groß geraten zu lassen. Wir nutzen natürlich die Symmetrie von $\mathcal{M}$ unter der Operation von Σ_6 aus.

3.1 Darstellungen von Σ_6-Bahnen

Sei $B \subset \mathbb{P}^5(\mathbb{F}_p)$ eine Bahn unter der Operation von Σ_6 durch Vertauschung der Koordinaten. Sei $k \in \{0, \ldots, 5\}$ maximal gewählt, so daß es einen entsprechend normierten Punkt $P = (X_0 : X_1 : \cdots : X_5) \in B$ mit den folgenden Eigenschaften gibt:

- Die Koordinaten von P werden durch positive Zahlen $< p$ repräsentiert, also
$$X_0, X_1, \ldots, X_5 \in \{0, \ldots, p-1\}.$$
- Die Koordinaten von P sind aufsteigend geordnet, also
$$X_0 \leq X_1 \leq \cdots \leq X_5.$$
- Die ersten k Koordinaten von P sind ≤ 1, also
$$\begin{aligned} X_0, \ldots, X_i &= 0, \\ X_{i+1}, \ldots, X_k &= 1. \end{aligned}$$
mit einem passenden $i \in \{0, \ldots, k-1\}$.

Wir nennen dann das Tupel

$$[X_0, X_1, \ldots, X_5]$$

(in eckigen Klammern) eine *Darstellung* der Bahn B. Diese ist allerdings nicht immer eindeutig, so lässt sich etwa über $\mathbb{F}_{23}$ der Punkt

$$(1:1:2:5:7:7)$$

auch auf

$$(10:10:20:4:1:1)$$

normieren. Seine Σ_6-Bahn hat damit mindestens zwei zulässige Darstellungen, nämlich

$$[1,1,2,5,7,7] \quad \text{und} \quad [1,1,4,10,10,20]$$

Zwei unterschiedliche Bahnen können aber keine gleiche Darstellung haben.

Wir ordnen nun die Menge aller den obigen Bedingungen genügenden Darstellungen der Bahn B lexikographisch durch

$$[X_0, X_1, \ldots, X_5] < [Y_0, Y_1, \ldots, Y_5] :\Longleftrightarrow X_i = Y_i \text{ für } i < j \text{ und } X_j < Y_j.$$

Sie enthält dann bezüglich dieser Ordnung ein eindeutiges minimales Element.

Wenn wir nun die Punkte in $\mathbb{P}^5(\mathbb{F}_p)$ (auf-)zählen wollen, so können wir stattdessen untersuchen, wieviele minimale Darstellungen es gibt und wieviele Punkte jeweils auf den Σ_6-Bahnen liegen, die diesen Darstellungen zugeordnet sind. Dazu wollen wir (minimale) Darstellungen in Typen einteilen.

3.1.1 Typen von Darstellungen

Sei $[X_0, X_1, \ldots, X_5]$ (nicht unbedingt minimale) Darstellung einer Σ_6-Bahn über $\mathbb{F}_p$. Wir bezeichnen mit a_i, $0 \leq i \leq p-1$, die Anzahl der X_j, für die $X_j = i$ gilt. Nach Konstruktion steht

$$a_1 \geq a_i \quad \text{für} \quad i > 1$$

fest. Als den *Typ* der Darstellung bezeichnen wir das absteigend sortierte Tupel $(a_0, a_1, \ldots, a_{p-1})$, wobei wir Nullen weglassen. Dann gibt es genau 11 verschiedene Typen:

(6)	$(3,3)$	$(2,2,1,1)$
$(5,1)$	$(3,2,1)$	$(2,1,1,1,1)$
$(4,2)$	$(3,1,1,1)$	$(1,1,1,1,1,1)$
$(4,1,1)$	$(2,2,2)$	

3.1.2 Wieviele Punkte liegen auf den Bahnen?

A priori können auf den Σ_6-Bahnen, deren minimale Darstellungen von einem gewissen Typ sind, folgende Anzahlen von Punkten liegen:

(6)	1	$(3,1,1,1)$	120
$(5,1)$	6	$(2,2,2)$	90
$(4,2)$	15	$(2,2,1,1)$	180
$(4,1,1)$	30	$(2,1,1,1,1)$	360
$(3,3)$	20	$(1,1,1,1,1,1)$	720
$(3,2,1)$	60		

Die tatsächliche Anzahl von Punkten auf der Bahn muß ein Teiler der angegebenen Zahl sein. Wir möchten letztendlich die Anzahl der Punkte auf $\mathcal{M}$ bestimmen und sind daher nur an den Bahnen von Punkten $P \in \mathbb{P}^5(\mathbb{F}_p)$ interessiert, für die $S_1(P) = 0$ gilt. Sei also B Bahn eines solchen Punktes. Wir unterscheiden nach dem Typ der minimalen Darstellung von B. Seien für diese Darstellung a_i, $0 \leq i \leq p-1$ wie oben gegeben.

(6): Dieser Typ kann für $p \geq 5$ nicht auftreten.

(5,1): $a_0 = 5$ ist unmöglich, also $a_1 = 5$ und $\#B = 6$.

(4,2): Wieder muß $a_1 = 4$ gelten und daher $\#B = 15$.

(4,1,1): Es gilt $a_0 = 4$ oder $a_1 = 4$. Im ersten Fall folgt $\#B = 15$, sonst $\#B = 30$.

(3,3): $a_0 = 3$ ist für $p \neq 3$ unmöglich, also ist $a_1 = 3$ und B die Bahn des Punktes $(1:1:1:-1:-1:-1)$. Deshalb ist $\#B = 10$.

(3,2,1): Alle a_i, die nicht Null sind, sind paarweise verschieden. Also muß $\#B = 60$ gelten.

(3,1,1,1): Gilt $a_1 = 3$, so $\#B = 120$. Sei also $a_0 = 3, a_1 = 1$. Dann ist B die Bahn eines Punktes der Form $(0:0:0:1:a:b)$. Ist $ab \equiv 1 \pmod{p}$ und a (oder äquivalent dazu b) dritte Einheitswurzel, so folgt $\#B = 40$, sonst $\#B = 120$.

(2,2,2): Gilt $a_0 = 0$, so ist B die Bahn des Punktes $(0:0:1:1:-1:-1)$ und damit $\#B = 45$. Sei also $a_0 \neq 0$. Dann ist B die Bahn eines Punktes der Form $(1:1:a:a:b:b)$. Ist (wie oben) $ab \equiv 1 \pmod{p}$ und a (oder äquivalent dazu b) dritte Einheitswurzel, so folgt $\#B = 30$, sonst $\#B = 90$.

(2,2,1,1): Es gilt $a_1 = 2$. Gilt dazu $a_{p-1} = 2$, so ist B die Bahn eines Punktes der Form $(1:1:-1:-1:a:-a)$ und damit $\#B = 90$. In allen anderen Fällen gilt $\#B = 180$.

(2,1,1,1,1): Gilt $a_1 = 2$, so $\#B = 360$. Sei also $a_1 = 1, a_0 = 2$. B ist dann Bahn eines Punktes der Form $(0 : 0 : 1 : a : b : c)$. Gilt $a \equiv -1$ oder $b \equiv -1$ oder $c \equiv -1 \pmod{p}$, so ist $\#B = 180$. Sind a, b, c unterschiedliche Potenzen derselben vierten (aber nicht zweiten) Einheitswurzel, so ist $\#B = 90$. In allen anderen Fällen ist $\#B = 360$.

(1,1,1,1,1,1): Sei zunächst $a_0 = 1$. B ist dann Bahn eines Punktes der Form $(0 : 1 : a : b : c : d)$. Sind a, b, c, d unterschiedliche Potenzen derselben fünften Einheitswurzel, so ist $\#B = 144$, sonst $\#B = 720$.

Sei jetzt $a_0 = 0$. Dann liegt auch ein Punkt der Form $(1 : a : b : c : d : e)$ auf B. Sind a, b, c, d, e unterschiedliche Potenzen derselben sechsten (aber nicht zweiten oder dritten) Einheitswurzel, so $\#B = 120$.

Liegt hingegen auch ein Punkt der Form $(1 : a : a^2 : b : ba : ba^2)$ auf B, so daß a eine dritte Einheitswurzel ist, und ist $b, ba, ba^2 \not\equiv -1$, so $\#B = 240$.

Liegt hingegen auch ein Punkt der Form $(1 : -1 : a : -a : b : -b)$ auf B, so $\#B = 360$.

In allen anderen Fällen ist $\#B = 720$.

3.1.3 Wann ist eine gegebene Darstellung minimal?

Wir können also jetzt, wenn wir eine minimale Darstellung gefunden haben, bestimmen, wieviele Punkte auf der zugehörigen Σ_6-Bahn liegen. Ein letztes Problem besteht noch darin, zu entscheiden, ob eine gegebene Darstellung minimal ist. Sei wieder B Bahn eines Punktes $P \in \mathbb{P}^5(\mathbb{F}_p)$ mit $S_1(P) = 0$. Sei irgendeine Darstellung von B gegeben. Wir unterscheiden wieder nach dem Typ der Darstellung:

(6): Dieser Typ kann für $p \geq 5$ nicht auftreten.

(5,1) oder (4,2) oder (3,2,1): In diesen Fällen gilt stets

$$a_1 > a_i \quad \text{für} \quad i > 1.$$

Deswegen ist die Darstellung schon eindeutig und damit minimal. (Wir können durch Multiplikation mit Körperelementen keine kleinere Darstellung errreichen.)

(4,1,1): Gilt $a_1 = 4$, so ist die Darstellung mit demselben Argument wie oben eindeutig. Gilt hingegen $a_0 = 4$, so ist die Darstellung gleich $[0, 0, 0, 0, 1, p-1]$ und daher auch eindeutig.

(3,3): Die Darstellung muß gleich $[1, 1, 1, p-1, p-1, p-1]$ sein und ist daher eindeutig.

(2,1,1,1,1): Ist $a_1 = 2$, so ist die Darstellung eindeutig. Ist dagegen $a_0 = 2$, so muß sie nicht minimal sein.

(2,2,1,1): Ist $a_0 = a_1 = 2$, so ist die Darstellung eindeutig. Ist $a_0 \neq 2$, so muß sie nicht minimal sein.

(2,2,2): Ist $a_0 = a_1 = 2$, so ist die Darstellung gleich $[0, 0, 1, 1, p-1, p-1]$ und damit eindeutig. Ist $a_0 \neq 2$, so muß sie nicht minimal sein.

(1,1,1,1,1,1): Man sieht es keinem Fall an, ob die Darstellung minimal ist.

In den Fällen, in denen wir nicht a priori sagen können, ob die Darstellung minimal ist, müssen wir es ausrechnen. Wir können dazu die Einträge der Darstellung mit Elementen aus $\mathbb{F}_p$ durchmultiplizieren, das so gewonnene Tupel sortieren und untersuchen, ob wir wieder eine Darstellung und vielleicht sogar eine kleinere erhalten. Alle zulässigen Darstellungen zu einer Bahn entstehen so.

Wir führen die Vorgehensweise an dem schon verwendeten Beispiel vor. Sie also B die Bahn des Punktes $(10 : 10 : 20 : 4 : 1 : 1) \in \mathbb{P}^5(\mathbb{F}_{23})$. Sei die zulässige Darstellung $[1, 1, 4, 10, 10, 20]$ vom Typ $(2, 2, 1, 1)$ gegeben. Es gilt also $a_0 = 0, a_1 = 2, a_4 = 1, a_{10} = 2, a_{20} = 1$, und die Darstellung muß nicht a priori minimal sein. Nur für $j = 10$ gilt $a_1 = a_j$. Wir können also höchstens durch Multiplikation mit $10^{-1} = 7$ eine andere zulässige Darstellung finden. Wir erhalten das Tupel $[7, 7, 5, 1, 1, 2]$, nach Sortieren $[1, 1, 2, 5, 7, 7]$. Dies ist tatsächlich eine zulässige und sogar minimale Darstellung.

Der Nachteil dieser Vorgehensweise ist die Notwendigkeit der Berechnung von multiplikativen Inversen in endlichen Körpern.

3.2 Die Zählmethode

Wir wollen die erarbeiteten Methoden verwenden, um zu ermitteln, wieviele Punkte $\mathcal{M}$ (oder eine andere der Σ_6-invarianten Quintiken) über $\mathbb{F}_p$ enthält. Wir gehen wie folgt vor:

- Zähle alle zulässigen Darstellungen über $\mathbb{F}_p$ auf, die zu Bahnen von Punkten gehören, für die $S_1 = 0$ gilt. Dies ist leicht durch 5 geschachtelte Zählschleifen (for-Schleifen) zu realisieren.
- Ermittle zu jeder Darstellung, ob sie minimal ist. (Abschnitt 3.1.3)
- Falls ja, setze einen Punkt aus der zugehörigen Bahn in die jeweilige Gleichung ein. Liegt der Punkt auf der Quintik, ermittle die Anzahl der Punkte auf seiner Bahn. (Abschnitt 3.1.2)

3.3 Ergebnisse

3.3.1 Wieviele Punkte müssen getestet werden?

Die folgende Tabelle listet für alle Primzahlen $p < 100$ die Zahl d_p der minimalen Darstellungen auf, die zu Σ_6-Bahnen von Punkten gehören, in denen S_1 verschwindet; dann die Zahl der Elemente in $\mathbb{P}^4(\mathbb{F}_p)$ und den Quotienten dieser beiden Zahlen, also die durchschnittliche Anzahl von Elementen auf den Σ_6-Bahnen.

p	d_p	$\#\mathbb{P}^4(\mathbb{F}_p)$	Quotient
2	3	31	10
3	6	121	20
5	13	781	60
7	27	2801	103
11	79	16105	203
13	129	30941	239
17	285	88741	311
19	409	137561	336
23	761	292561	384
29	1681	732541	435
31	2127	954305	448
37	3981	1926221	483
41	5757	2896405	503
43	6849	3500201	511
47	9473	4985761	526
53	14757	8042221	544
59	21995	12326281	560
61	24925	14076605	564
67	35449	20456441	577
71	44109	25774705	584
73	49005	28792661	587
79	66123	39449441	596
83	79787	48037081	602
89	104145	63455221	609
97	144833	89451461	617

Man erkennt den erwarteten Effekt, daß nämlich der Anteil der Bahnen mit minimalen Darstellungen vom Typ $(1,1,1,1,1,1)$ mit wachsendem p zunimmt. So muß also beispielsweise für $p = 97$ nur für etwa $1/617$ aller Punkte aus $\mathbb{P}^4(\mathbb{F}_{97})$ überhaupt getestet werden, ob sie auf $\mathcal{M}$ liegen.

3.3.2 Und wieviele Punkte liegen nun auf $\mathcal{M}$?

Die folgende Tabelle listet für alle Primzahlen $5 \leq p \leq 199$ die Anzahl $\#\mathcal{M}$ der Punkte auf $\mathcal{M}$ über $\mathbb{F}_p$ auf und auch, wieviele davon singulär sind. Letzteres bestätigt die Ergebnisse aus Kapitel 2.

p	$\#\mathcal{M}$	singulär	p	$\#\mathcal{M}$	singulär
5	370	10	97	1184090	130
7	1130	130	101	1132930	10
11	2530	10	103	1400570	130
13	5930	130	107	1341010	10
17	7930	10	109	1639370	130
19	15770	130	113	1571050	10
23	17290	10	127	2522090	130
29	32770	10	131	2417410	10
31	55610	130	137	2759770	10
37	87770	130	139	3250970	130
41	85690	10	149	3528370	10
43	130730	130	151	4109450	130
47	126010	10	157	4593050	130
53	176770	10	163	5113370	130
59	240850	10	167	4938490	10
61	333050	130	173	5475250	10
67	427850	130	179	6056290	10
71	407530	10	181	6892490	130
73	541370	130	191	7335370	10
79	672890	130	193	8289530	130
83	641170	10	197	8029090	10
89	783370	10	199	9050330	130

Die Primzahlen von schlechter Reduktion sind 2 und 3. Über $\mathbb{F}_2$ gilt $\mathcal{M} = \mathbb{P}^4$; über $\mathbb{F}_3$ enthält $\mathcal{M}$ 91 Punkte, von denen 11 singulär sind.

3.3.3 Kosten-Nutzen-Rechnung

Es stellt sich natürlich die Frage, ob der verwendete Algorithmus eine Zeitersparnis bringt, die den theoretischen Aufwand dieses Kapitels rechtfertigt. Zu Vergleichszwecken habe ich deshalb noch den "dummen" Algorithmus implementiert, der alle Punkte aus $\mathbb{P}^4$ durchläuft und in die Gleichung einsetzt. Die folgende Tabelle enthält für einige Primzahlen die Laufzeiten in Sekunden (auf Sun Ultra 10, 300 MHz, Solaris 5.6) beider Algorithmen und

den Unterschiedsfaktor.

p	"schlau"	"dumm"	Faktor
37	0.4	18.5	46
47	1.1	48	43
59	3.0	119	39
67	5.9	198	33
97	33.4	869	26

Der Zeitgewinn ist also wesentlich, nimmt aber mit wachsendem p relativ gesehen ab. Ein entscheidender Faktor dafür ist die Notwendigkeit der Berechnung von multiplikativen Inversen. Sicherlich ist es auch noch möglich, den Algorithmus zu optimieren. Für unsere Zwecke reicht es jedoch meistens aus, Anzahlen von Punkten für Primzahlen $p < 100$ zu kennen; und diese werden mit den in diesem Kapitel entwickelten Methoden jedenfalls schnell genug berechnet.

Kapitel 4

Die L-Reihe von $\mathcal{M}$

Wir haben durch Auflösung der Singularitäten von $\mathcal{M}$ eine glatte Varietät $\tilde{\mathcal{M}}$ erhalten. Wir zeigen, daß die mittlere Kohomologie von $\tilde{\mathcal{M}}$ 2-dimensional ist; wir bestimmen deren L-Reihe und zeigen, daß sie bis auf eventuelle Euler-Faktoren bei den Primzahlen von schlechter Reduktion gleich der L-Reihe der modularen Form $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ ist, der eindeutigen Cusp-Form vom Gewicht 4 und Level 6.

4.1 Galois-Darstellungen

Wir müssen später die Wirkung linearer Abbildungen auf $\mathbb{F}_p$-Vektorräume (nämlich der Frobenius-Abbildungen auf die Kohomologie von $\tilde{\mathcal{M}}$) untersuchen. Das Werkzeug dazu sind die im Folgenden vorgestellten Galois-Darstellungen.

Sei $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ die Gruppe der Automorphismen von $\overline{\mathbb{Q}}$. G ist eine kompakte Gruppe bezüglich der Krull-Topologie. Sei $l \in \mathbb{P}$ und V ein n-dimensionaler $\mathbb{Q}_l$-Vektorraum. Die volle lineare Gruppe

$$\mathrm{Aut}(V) = \mathrm{Aut}_{\mathbb{Q}_l}(V) = \mathrm{GL}_n(\mathbb{Q}_l)$$

der Automorphismen von V ist eine l-adische Lie-Gruppe bezüglich der von $\mathrm{Hom}_{\mathbb{Q}_l}(V,V)$ induzierten natürlichen Topologie. Eine *(l-adische) Galois-Darstellung* (von G) ist nun ein stetiger Gruppenhomomorphismus

$$\rho : G \longrightarrow \mathrm{Aut}(V).$$

Das Bild von ρ in $\mathrm{Aut}(V)$ ist dabei stets abgeschlossen.

Die Theorie der Galois-Darstellungen wird in [16] entwickelt.

Wir wollen zunächst die (riesige) Gruppe G besser verstehen und führen dazu den Begriff des *Frobenius-Elements* ein. Wir halten uns dabei an [13].

Sei zunächst K eine beliebige endliche galoissche Erweiterung von $\mathbb{Q}$. Die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ lässt den Ring $\mathcal{O}_K$ der ganzen Zahlen in K invariant, so daß wir eine induzierte Wirkung von $\mathrm{Gal}(K/\mathbb{Q})$ auf der Menge der Ideale in $\mathcal{O}_K$ erhalten. Speziell wird die Menge der Primideale $\mathfrak{p}$ von $\mathcal{O}_K$, die die Primzahl p enthalten, permutiert. Die Untergruppe $D_\mathfrak{p}$ von $\mathrm{Gal}(K/\mathbb{Q})$, die $\mathfrak{p}$ fest lässt, heißt *Zerlegungsgruppe* von $\mathfrak{p}$ in $\mathrm{Gal}(K/\mathbb{Q})$.

Der endliche Körper $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ ist eine Erweiterung des Körpers $\mathbb{F}_p$ und heißt der *Restklassenkörper* von $\mathfrak{p}$. Die Erweiterung $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$ ist galoissch; ihre Galoisgruppe ist die zyklische Gruppe, die von dem Frobeniusautomorphismus $\phi_p : x \mapsto x^p$ von $\mathbb{F}_\mathfrak{p}$ erzeugt wird. Wir erhalten einen natürlichen surjektiven Homomorphismus $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$, indem wir ein $\delta \in D_\mathfrak{p}$ mit dem durch δ induzierten Automorphismus von $\mathcal{O}_K/\mathfrak{p}$ assoziieren. Ist er injektiv für ein $\mathfrak{p}$, so auch für alle $\mathfrak{p}$. Wir sagen dann, daß die Primzahl p *unverzweigt* ist für die Erweiterung $K/\mathbb{Q}$ (Dies gilt stets für fast alle Primzahlen p.). In diesem Fall hat ϕ_p also für jedes $\mathfrak{p}$ ein eindeutiges Urbild $\mathrm{Frob}_\mathfrak{p}$ in $D_\mathfrak{p}$, genannt der Frobeniusautomorphismus für $\mathfrak{p}$. Die $\mathrm{Frob}_\mathfrak{p}$ sind konjugiert in $\mathrm{Gal}(K/\mathbb{Q})$. Es ist daher üblich, sie alle mit Frob_p zu bezeichnen (was also ein bis auf Konjugation wohldefiniertes Element von $\mathrm{Gal}(K/\mathbb{Q})$, das *Frobenius-Element bei* p, liefert).

Wir möchten das Konzept von Frobenius-Elementen gerne auf unendliche algebraische Erweiterungen $K/\mathbb{Q}$ (insbesondere auf $\overline{\mathbb{Q}}/\mathbb{Q}$ ausdehnen. Sei wieder $p \in \mathbb{P}$, und sei $\mathfrak{p}$ eine Primstelle von $\overline{\mathbb{Q}}$, die über p liegt (Das ist eine geeignete Auswahl von Primidealen, die über p liegen, aus den $\mathcal{O}_K$ für alle endlichen Erweiterungen K von $\mathbb{Q}$).

Wir assoziieren zu $\mathfrak{p}$ analog einen Restklassenkörper $\mathbb{F}_\mathfrak{p}$ und eine Zerlegungsgruppe $D_\mathfrak{p} \leq \mathrm{Gal}(K/\mathbb{Q})$. Es gibt wieder einen surjektiven Gruppenhomomorphismus $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. Der Frobeniusautomorphismus $\phi_p : x \mapsto x^p$ erzeugt $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ topologisch, d.h. sein Erzeugnis ist dicht in $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. Wir bezeichnen den Kern der Abbildung $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ mit $I_\mathfrak{p}$. Da die $\mathfrak{p}$ alle konjugiert sind durch Elemente aus $\mathrm{Gal}(K/\mathbb{Q})$, sind auch alle die $I_\mathfrak{p}$ konjugiert. Wir können also die Primzahl p wieder *unverzweigt* für die Erweiterung $K/\mathbb{Q}$ nennen, wenn eines der $I_\mathfrak{p}$ trivial ist.

Ist nun $\rho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow H$ ein Gruppenhomomorphismus, so enthält der Kern von ρ eines der $I_\mathfrak{p}$ genau dann, wenn er alle $I_\mathfrak{p}$ enthält. Ist ρ speziell eine Galois-Darstellung, so heißt sie in diesem Fall *unverzweigt bei* p. Dies ist gleichbedeutend mit der Aussage, daß p unverzweigt ist für die Erweiterung $L/\mathbb{Q}$, die dem Kern von ρ als Untergruppe von G zugeordnet wird.

Wir nennen nun für $p \in \mathbb{P}$ jedes Urbild der Abbildung $D_\mathfrak{p} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ für ein $\mathfrak{p}$ über p ein *Frobenius-Element* für p in $\mathrm{Gal}(K/\mathbb{Q})$. Ein solches bezeichnen wir wieder mit Frob_p. Diese Bezeichnung wird (im für uns interessanten Fall $K = \overline{\mathbb{Q}}$) dadurch gerechtfertigt, daß wir nicht die Gruppe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ direkt anschauen, sondern eine Galois-Darstellung davon. Ist nämlich die

Galois-Darstellung ρ unverzweigt bei p, so sind nach den obigen Ausführungen die Bilder der Frobenius-Elemente für p bis auf Konjugation gleich. Insbesondere sind Spur und Determinante gleich.

Eine wichtige Anwendung des Dichtesatzes von Tchebotarev ist es, daß die Frobenius-Elemente für die unverzweigten Primzahlen eine dichte Teilmenge von $\mathrm{Gal}(K/\mathbb{Q})$ bilden. Insbesondere können wir Aussagen über das Verhalten der Frobenius-Elemente unter stetigen Abbildungen (wie etwa der Spur einer Galois-Darstellung) auf die ganze Gruppe ausdehnen.

Wir möchten Galois-Darstellungen miteinander vergleichen können. Dazu benötigen wir einen Gleichheitsbegriff, der schwach genug ist. Zunächst einmal sind alle Galois-Darstellungen ρ, denen wir im Folgenden begegnen werden, *rational* (bzw. *ganz*), d.h. ρ ist unverzweigt außerhalb einer endlichen Menge $S \subset \mathbb{P}$, und für $p \in \mathbb{P}, p \notin S$ haben die ("charakteristischen") Polynome $\det(1 - \rho(\mathrm{Frob}_p)t)$ Koeffizienten in $\mathbb{Q}$ (bzw. $\mathbb{Z}$). Ist ρ' eine weitere rationale Darstellung mit derselben Menge S und $\det(1 - \rho(\mathrm{Frob}_p)t) = det(1 - \rho'(\mathrm{Frob}_p)t)$ für alle $p \notin S$, so heißen ρ und ρ' *kompatibel*.

Sei nun $\rho : G \longrightarrow \mathrm{Aut}(V)$ eine rationale Galois-Darstellung. Dann hat V eine Kompositionsreihe

$$V = V_0 \supset V_1 \supset \cdots \supset V_q = 0$$

maximaler Länge von ρ-invarianten Unterräumen. Wir gewinnen daraus eine neue Galois-Darstellung

$$\rho' : G \longrightarrow \mathrm{Aut}(V') \qquad \text{mit } V' = \sum_{i=0}^{q-1} V_i/V_{i+1}.$$

Diese ist wieder rational und heißt (eine) *Halbvereinfachung* von ρ. Dieser Begriff erklärt sich daher, daß das Bild von ρ' in V die Struktur einer halbeinfachen Lie-Gruppe hat. Es gilt, daß es zu jeder rationalen l-adischen Galois-Darstellung ρ genau eine (bis auf Isomorphismus eindeutige) mit ρ kompatible und halbeinfache l-adische Darstellung gibt (genannt "die" Halbvereinfachung von ρ).

4.2 Arithmetische Eigenschaften von Varietäten

Wir wollen nun die (bewiesenen) Weil-Vermutungen über die Zeta-Funktion einer Varietät formulieren, die direkt mit den Anzahlen von Punkten über endlichen Körpern auf der Varietät zu tun haben, und im Zusammenhang damit die l-adische Kohomologie einer Varietät einführen. Die zugehörige Theorie wird in [12] ausführlich und in [8], Anhang C, sehr übersichtlich dargestellt.

Sei X eine glatte projektive Varietät der Dimension n über $\mathbb{C}$, die durch Gleichungen gegeben ist und modulo p für $p \in \mathbb{P}$ reduziert werden kann (wie z.B. $\tilde{\mathcal{M}}$). Die folgenden Aussagen gelten zwar allgemeiner, wir benötigen aber nur diesen Spezialfall.

4.2.1 Zeta-Funktionen, die Weil-Vermutungen und l-adische Kohomologie

Sei $p \in \mathbb{P}$ fest. Wir bezeichnen mit ν_{p^r} die Anzahl der Punkte, die X über $\mathbb{F}_{p^r}$ enthält. Die *Zeta-Funktion* von X zur Primzahl p ist dann definiert als

$$Z_p(t) = \exp\left(\sum_{r=1}^{\infty} \nu_{p^r} \frac{t^r}{r}\right).$$

Die (bewiesenen) Weil-Vermutungen besagen nun unter anderem die folgenden Tatsachen:

$Z_p(t)$ ist eine rationale Funktion in t und lässt sich schreiben als

$$Z_p(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}.$$

Die $P_i = P_{p,i}$ sind Polynome mit ganzzahligen Koeffizienten und zerfallen in

$$P_i(t) = \prod_j (1 - \omega_{ij} t),$$

wobei die ω_{ij} von l unabhängige algebraische Zahlen sind. Schließlich gilt

$$|\omega_{ij}| = p^{i/2}.$$

Bis auf die letzte folgen diese Eigenschaften relativ leicht, wenn man eine "gute" Kohomologietheorie (oder auch *Weil-Kohomologietheorie*) auf X hat. Die erste solche Theorie war die von Grothendieck entdeckte l-adische Kohomologie. Die letzte Eigenschaft wurde dann später von Deligne bewiesen.

Sei jetzt $l \in \mathbb{P}$, $l \neq p$ und $\mathbb{Z}_l = \varprojlim \mathbb{Z}/l^r\mathbb{Z}$ der Ring der l-adischen Zahlen mit Quotientenkörper $\mathbb{Q}_l$. Dann ist die (i-te) *l-adische Kohomologie* von X definiert durch

$$H^i(X, \mathbb{Q}_l) = (\varprojlim H^i_{\text{ét}}(X, \mathbb{Z}/l^r\mathbb{Z})) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l,$$

wobei $H^i_{\text{ét}}$ (die ebenfalls von Grothendieck gefundene) étale-Kohomologie bezüglich der étale-Topologie bezeichnet (siehe [12]). Die Gruppen $H^i(X, \mathbb{Q}_l)$

sind Vektorräume über $\mathbb{Q}_l$. Sie sind endlich-dimensional für $0 \leq i \leq 2n$, sonst Null. Wir werden uns vor allem für die Zahlen

$$h^i := \dim_{\mathbb{Q}_l} H^i(X, \mathbb{Q}_l)$$

interessieren. Daher ist für uns wichtig, daß Poincaré-Dualität gilt, d.h. es gibt perfekte Paarungen

$$H^i(X, \mathbb{Q}_l) \times H^{2n-i}(X, \mathbb{Q}_l) \to H^{2n}(X, \mathbb{Q}_l)$$

für $0 \leq i \leq 2n$. Insbesondere ergibt sich

$$h^i = h^{2n-i}, \qquad 0 \leq i \leq 2n.$$

Nur mit der Definition sind die h^i schlecht auszurechnen; es gilt jedoch der Vergleichssatz

$$H^i(X, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \mathbb{C} \cong H^i(X, \mathbb{C}),$$

wobei X auf der rechten Seite als Varietät über $\mathbb{C}$ betrachtet wird. Es ist also auch möglich, die h^i über "normale" (topologische) Kohomologie zu berechnen.

Es gilt außerdem der *Fixpunktsatz von Lefschetz*: Sei $f : X \longrightarrow X$ ein Morphismus. Dadurch werden Vektorraumhomomorphismen $f^* : H^i(X, \mathbb{Q}_l) \longrightarrow H^i(X, \mathbb{Q}_l)$ induziert. Seien alle Fixpunkte von f isoliert mit "Multiplizität 1" (d.h. der Schnitt des Graphen von f mit der Diagonale in $X \times X$ ist transversal), und sei $N(f, X)$ die Anzahl der Fixpunkte von f. Dann gilt

$$N(f, X) = \sum_{i=0}^{2n} (-1)^i \operatorname{Spur}(f^* | H^i(X, \mathbb{Q}_l)).$$

Wir wollen diesen Satz speziell auf die Frobeniusabbildung $F_p : X \longrightarrow X$ anwenden, die einem Punkt (X_i) den Punkt (X_i^p) zuordnet; denn es ist ν_{p^r} gerade die Anzahl der Fixpunkte der r-ten Iterierten F_p^r, also

$$\nu_{p^r} = \sum_{i=0}^{2n} (-1)^i \operatorname{Spur}((F_p^r)^* | H^i(X, \mathbb{Q}_l)).$$

Die induzierte Abbildung $F_p^* : H^i(X, \mathbb{Q}_l) \longrightarrow H^i(X, \mathbb{Q}_l)$ können wir auffassen als das Bild eines Frobeniuselements Frob_p in $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Da die Frobeniuselemente nach dem Dichtesatz von Tchebotarev dicht in $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ liegen, können wir so l-adische Galois-Darstellungen

$$\rho_{l,i} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_{h^i}(\mathbb{Q}_l)$$

mit

$$\rho_{l,i}(\operatorname{Frob}_p) = (F_p)^* | H^i(X, \mathbb{Q}_l)$$

definieren, und zwar so, daß sie unverzweigt sind außerhalb der Primzahlen von schlechter Reduktion von X und mit den Paarungen

$$H^i(X, \mathbb{Q}_l) \times H^{2n-i}(X, \mathbb{Q}_l) \to H^{2n}(X, \mathbb{Q}_l)$$

verträglich sind. Wir schreiben auch

$$\mathrm{Frob}_p \,|H^i(X, \mathbb{Q}_l) \qquad \text{statt} \qquad (F_p)^*|H^i(X, \mathbb{Q}_l).$$

Mit all diesen Voraussetzungen gilt dann für die Faktoren der Zeta-Funktion

$$P_i(t) = det((1 - \mathrm{Frob}_p\, t)|H^i(X, \mathbb{Q}_l)).$$

Die ω_{ij} sind also gerade die Eigenwerte von $\mathrm{Frob}_p\,|H^i(X, \mathbb{Q}_l)$.

Insbesondere ist der Grad von P_i gleich h^i. Es gilt $h^0 = h^{2n} = 1$, und die Wirkung von Frob_p auf $H^0(X, \mathbb{Q}_l)$ bzw. $H^{2n}(X, \mathbb{Q}_l)$ ist die Identität bzw. Multiplikation mit p^n (vgl. [12], §12). Also gilt

$$P_0(t) = 1 - t \quad \text{und} \quad P_{2n}(t) = 1 - p^n t.$$

4.2.2 L-Reihen

In der von den Frobeniuselementen induzierten Wirkung auf die l-adische Kohomologie ist also die Information über die Anzahl der Punkte auf X über endlichen Körpern codiert. Die *L-Reihe* oder *L-Funktion* von X (eigentlich von $H^n(X, \mathbb{Q}_l)$) ist nun die formale Dirichlet-Reihe

$$L(s, X) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}.$$

Hierbei ist $a_1 = 1$, $a_p = \mathrm{Spur}(\mathrm{Frob}_p\,|H^n(X, \mathbb{Q}_l))$ für $p \in \mathbb{P}$, und für $q \notin \mathbb{P}$ ist a_q das Produkt der a_p zu den Primfaktoren p von q.

Wir haben nach den Weil-Vermutungen die Abschätzungen

$$|a_p| = |\,\mathrm{Spur}(\mathrm{Frob}_p\,|H^n(X, \mathbb{Q}_l))| \leq h^n \cdot p^{n/2}$$

und daher nach einem allgemeinen Resultat über Dirichlet-Reihen (absolute) Konvergenz von $L(s, X)$ für genügend großen Realteil von s. In diesem Fall hat $L(s, X)$ die Euler-Produktentwicklung

$$L(s, X) = \prod_{p \in \mathbb{P}} \frac{1}{P_{p,n}(p^{-s})}.$$

Es gibt eine Vermutung, daß $L(s, X)$ sich immer als Linearkombination von L-Reihen modularer Formen (s. Abschnitt 4.4) darstellen läßt, daß also ein

direkter Zusammenhang besteht zwischen den Anzahlen von Punkten auf X über endlichen Körpern und zwischen modularen Formen. Diese Vermutung ist Teil des Langlands-Programms. Ich habe keine Quelle gefunden, in der sie für unsere Zwecke sinnvoll aufgeschrieben ist. S. Bloch hat sich damit beschäftigt, aber wohl nie etwas veröffentlicht. Darüberhinaus ist in [21] eine Arbeit von M. H. Saito und N. Yui angekündigt, die aber auch noch nicht erschienen ist. Wir werden deshalb die Ergebnisse für unsere Familie von Quintiken nur vorstellen, ohne sie in den großen Kontext einzuordnen.

4.3 Anwendung auf $\tilde{\mathcal{M}}$

Wir wollen die Ergebnisse aus dem vorigen Abschnitt auf die Varietät $\tilde{\mathcal{M}}$ anwenden. Um die Zeta-Funktion von $\tilde{\mathcal{M}}$ zu bestimmen, benötigen wir zunächst die noch fehlenden $h^i, 1 \leq i \leq 5$. Da $\mathcal{M}$ eine Hyperfläche ist, gilt $H^1(\mathcal{M}, \mathcal{O}_X) = 0$ (vgl. [8], Theorem III.3.5). Aus der Exponentialsequenz können wir dann die exakte Sequenz

$$0 \longrightarrow H^1(\mathcal{M}, \mathbb{Z}) \longrightarrow H^1(\mathcal{M}, \mathcal{O}_X) \longrightarrow H^1(\mathcal{M}, \mathcal{O}_X^*) \longrightarrow \cdots$$

herleiten (vgl. [8], Anhang B.5). Also gilt

$$H^1(\mathcal{M}, \mathbb{Z}) = 0.$$

Sei $\mathbb{Z}_{\tilde{\mathcal{M}}}$ bzw. $\mathbb{Z}_{\mathcal{M}}$ die konstante Garbe auf $\tilde{\mathcal{M}}$ bzw. $\mathcal{M}$ und $f_*\mathbb{Z}_{\tilde{\mathcal{M}}}$ die direkte Bildgarbe von $\mathbb{Z}_{\tilde{\mathcal{M}}}$ auf $\mathcal{M}$ für den Blow-Up $f : \tilde{\mathcal{M}} \longrightarrow \mathcal{M}$. Sei weiterhin $R^1 f_*$ der erste rechts-abgeleitete Funktor von f_*. Der Anfang der Leray-Spektralsequenz für f ist dann

$$0 \longrightarrow H^1(\mathcal{M}, f_*\mathbb{Z}_{\tilde{\mathcal{M}}}) \longrightarrow H^1(\tilde{\mathcal{M}}, \mathbb{Z}_{\tilde{\mathcal{M}}}) \longrightarrow H^0(\mathcal{M}, R^1 f_*\mathbb{Z}_{\tilde{\mathcal{M}}}) \longrightarrow \cdots$$

Die Fasern $f^{-1}(P)$ der Punkte P aus $\mathcal{M}$ sind (Punkte oder) Quadriken, also zusammenhängend; deshalb gilt

$$f_*\mathbb{Z}_{\tilde{\mathcal{M}}} = \mathbb{Z}_{\mathcal{M}}.$$

Sie sind sogar einfach zusammenhängend; deshalb gilt außerdem

$$R^1 f_*\mathbb{Z}_{\tilde{\mathcal{M}}} = 0.$$

Daraus folgt sofort

$$H^1(\tilde{\mathcal{M}}, \mathbb{Z}) = H^1(\tilde{\mathcal{M}}, \mathbb{Z}_{\tilde{\mathcal{M}}}) = 0,$$

also $h^1 = h^5 = 0$ und deswegen $P_1(t) = P_5(t) = 1$.

Sei für den Moment X eine projektive Varietät. Wir bezeichnen mit $\beta_i(X) := \dim H^i(X, \mathbb{Q})$ ihre *i-te Betti-Zahl* und nennen noch $d(X) := \dim H^4(X, \mathbb{Q}) -$

1 ihren *Defekt*. Ist X speziell eine Hyperfläche vom Grad n in $\mathbb{P}^4$ mit insgesamt s Singularitäten, die alle gewöhnliche Doppelpunkte seien, so finden wir in [22] für die Betti-Zahlen von X und einer (großen) Auflösung $\tilde{X}$ von X die Formeln:

$$\begin{aligned}
\beta_2(X) &= 1 \\
\beta_3(X) &= n^4 - 5n^3 + 10n^2 - 10n + 4 - s + d(X) \\
\beta_2(\tilde{X}) &= \beta_4(\tilde{X}) \quad = \quad 1 + s + d(X) \\
\beta_3(\tilde{X}) &= n^4 - 5n^3 + 10n^2 - 10n + 4 - 2s + 2d(X)
\end{aligned}$$

Speziell für $X = \mathcal{M}$ mit Auflösung $\tilde{X} = \tilde{\mathcal{M}}$ ist $\beta_i(\tilde{\mathcal{M}}) = h^i$, und mit $d := d(\mathcal{M})$ ergibt sich:

$$\begin{aligned}
h^3 &= 204 - 2 \cdot 130 + 2d \quad = \quad 2d - 56 \qquad \text{und} \\
h^2 &= h^4 \quad = \quad d + 131.
\end{aligned}$$

Also können wir, wenn wir den Defekt d kennen, h^2 und h^3 ausrechnen. In [22] ist eine Methode dazu angegeben, die allerdings (zum Beispiel) das Berechnen des Koranges einer 126×130-Matrix erfordert (Das Ergebnis ist $d = 29$, was schon in [19] erwähnt wurde.). Wir verwenden stattdessen die aus den Weil-Vermutungen stammende Abschätzung

$$|\operatorname{Spur}(\operatorname{Frob}_p | H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l))| \leq p^{3/2} h^3$$

und unsere Ergebnisse über das Zählen von Punkten auf $\mathcal{M}$ über endlichen Körpern. Diese Methode wurde u.a. von B. van Geemen entwickelt und zum Beispiel in [18] angewendet.

Sei $p \in \mathbb{P}, p \geq 5$. Wählen wir $p \equiv 1, -5 \pmod{12}$, so ist $\#\tilde{\mathcal{M}} = \#\mathcal{M} + 130(2p + p^2)$, und alle Singularitäten von $\mathcal{M}$ sowie die Regelsysteme der Tangentialkegel sind rational über $\mathbb{F}_p$. In diesem Fall wird $H^2(\tilde{\mathcal{M}}, \mathbb{Q})$ von Divisorklassen aufgespannt (vgl. [18]). Deswegen ist die Wirkung von Frob_p auf $H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l)$ einfach Multiplikation mit p, und es folgt

$$P_2(t) = (1 - pt)^{h^2} \quad \text{und} \quad \operatorname{Spur}(\operatorname{Frob}_p | H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l)) = ph^2.$$

Aufgrund der Poincaré-Dualität ist die Wirkung von Frob_p auf $H^4(\tilde{\mathcal{M}}, \mathbb{Q}_l)$ Multiplikation mit p^2, und es folgt

$$P_4(t) = (1 - p^2 t)^{h^4} \quad \text{und} \quad \operatorname{Spur}(\operatorname{Frob}_p | H^4(\tilde{\mathcal{M}}, \mathbb{Q}_l)) = p^2 h^4.$$

Der Fixpunktsatz von Lefschetz liefert uns

$$\begin{aligned}
\#\tilde{\mathcal{M}} &= \sum_{i=0}^{6} (-1)^i \operatorname{Spur}(\operatorname{Frob}_p | H^i(\tilde{\mathcal{M}}, \mathbb{Q}_l)) \\
&= 1 + ph^2 - \operatorname{Spur}(\operatorname{Frob}_p | H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l)) + p^2 h^4 + p^3 \\
&= 1 + p^3 + p(p+1)h^2 - \operatorname{Spur}(\operatorname{Frob}_p | H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l)).
\end{aligned}$$

Wegen der schon erwähnten Abschätzung

$$|\operatorname{Spur}(\operatorname{Frob}_p | H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l))| \leq p^{3/2} h^3$$

folgt

$$\begin{aligned} |\#\tilde{\mathcal{M}} - 1 - p^3 - p(p+1)h^2| &\leq p^{3/2} h^3 \\ &= p^{3/2}(2d - 56) = p^{3/2}(2h^2 - 318). \end{aligned}$$

Speziell für $p = 13$ erhalten wir die Ungleichung

$$|29082 - 182h^2| \leq 13^{3/2}(2h^2 - 318)$$

und daraus $h^2 = h^4 = 160$ und $h^3 = 2$ (und wieder $d = 29$). In diesem Fall hat also die Zeta-Funktion von $\mathcal{M}$ die Form

$$Z_p(t) = \frac{P_3(t)}{(1-t)(1-pt)^{160}(1-p^2t)^{160}(1-p^3t)}.$$

Betrachten wir nun noch den Fall $p \equiv -1, 5 \pmod{12}$. Hier kann die Wirkung von Frob_p auf $H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l)$ komplizierter sein. Es gilt jedoch

$$P_2(t) = 1 - t \cdot \operatorname{Spur}(\operatorname{Frob}_p | H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l)) + O(t^2),$$

und da nach den Weil-Vermutungen $P_2(t)$ ein Polynom mit ganzzahligen Koeffizienten ist, ist auch $\operatorname{Spur}(\operatorname{Frob}_p | H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l))$ eine ganze Zahl. Da sich jeder Eigenwert von $\operatorname{Frob}_p | H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l)$ als p-faches einer Einheitswurzel darstellen lässt, muß sogar

$$\operatorname{Spur}(\operatorname{Frob}_p | H^2(\tilde{\mathcal{M}}, \mathbb{Q}_l)) = p \cdot k$$

für ein $k \in \mathbb{Z}, |k| \leq h^2$ gelten. Wegen der Poincaré-Dualität ist entsprechend

$$\operatorname{Spur}(\operatorname{Frob}_p | H^4(\tilde{\mathcal{M}}, \mathbb{Q}_l)) = p^2 \cdot k.$$

Es gilt $\#\tilde{\mathcal{M}} = \#\mathcal{M} + 10(2p + p^2)$. Wir berechnen den Wert von k durch eine ähnliche Abschätzung wie oben:

$$|\#\tilde{\mathcal{M}} - 1 - p^3 - k(p + p^2)| \leq p^{3/2} h^3 = 2p^{3/2}$$

Speziell für $p = 17$ erhalten wir die Ungleichung

$$|6246 - 306k| \leq 34\sqrt{17}$$

und daraus $k = 20$.

Wir definieren für $p \in \mathbb{P}, p \geq 5$

$$a_p := \operatorname{Spur}(\operatorname{Frob}_p | H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l)).$$

Nach den obigen Berechnungen haben wir also jetzt die Formeln

$$a_p = 1 - 100p + 30p^2 + p^3 - \#\mathcal{M}, \qquad \text{falls } p \equiv 1, -5 \pmod{12}$$

und

$$a_p = 1 + 10p^2 + p^3 - \#\mathcal{M}, \qquad \text{falls } p \equiv -1, 5 \pmod{12}.$$

Wir erhalten beispielsweise:

p	5	7	11	13	17	19	23
a_p	6	-16	12	38	-126	20	168

4.4 Modulare Formen

4.4.1 Modulare Formen für $\Gamma_0(N)$

Wir führen jetzt modulare Formen ein. Das sind analytische Funktionen mit speziellen Symmetrieeigenschaften, die eine Reihen- bzw. Produktexpansion "in ∞" haben. Die Theorie wird zum Beispiel in [10] ausführlich dargestellt.

Sei $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ die *volle modulare Gruppe*. Die Gruppen

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \;\middle|\; c \equiv 0 \pmod{N} \right\} \qquad \text{für } N \in \mathbb{N}$$

haben endlichen Index in Γ und heißen *Hecke-Untergruppen* von Γ.

Eine *uneingeschränkte modulare Form* vom *Gewicht* $k \in \mathbb{Z}$ und *Level* $N \in \mathbb{N}$ ist eine analytische Funktion f auf $\mathbb{H}$ mit

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \qquad \text{für alle } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), \quad \tau \in \mathbb{H}.$$

Hierbei ist natürlich $\gamma\tau = (a\tau + b)/(c\tau + d)$ das Bild von τ unter der γ zugeordneten Möbius-Transformation. f hat stets eine *q-Expansion*

$$f(\tau) = \sum_{n=-\infty}^{\infty} c_n q^n \qquad \text{mit } q = e^{2\pi i \tau / N}.$$

Gilt $c_n = 0$ für $n < 0$, so heißt f eine *modulare Form*. Gilt außerdem noch $c_0 = 0$, so heißt f eine *Cusp-Form*.

Die Menge $M_k(\Gamma_0(N))$ der modularen Formen vom Gewicht k und Level N ist ein endlich-dimensionaler Vektorraum. Die Cusp-Formen vom Gewicht k und Level N bilden einen Unterraum $S_k(\Gamma_0(N)) \leq M_k(\Gamma_0(N))$.

$S_k(\Gamma_0(N))$ ist orthogonale Summe simultaner(!) Eigenräume für gewisse Operatoren, die *Hecke-Operatoren*. Eine Cusp-Form, die ein Eigenvektor

für die Hecke-Operatoren ist, heißt *Eigenform*; zwei Eigenformen, die in dem selben Eigenraum liegen, heißen *äquivalent*. Ist $r_1 r_2 | N$ und $f(\tau)$ eine Eigenform für $\Gamma_0(N/r_1 r_2)$, dann ist $f(r_2\tau)$ eine Eigenform für $\Gamma_0(N)$ mit denselben Eigenwerten. Solch eine Eigenform wird *Oldform* genannt. Die Oldforms spannen einen Unterraum $S_k^{old}(\Gamma_0(N)) \leq S_k(\Gamma_0(N))$ auf. Das orthogonale Komplement dazu wird als $S_k^{new}(\Gamma_0(N))$ bezeichnet und eine Eigenform darin als *Newform*. Die Äquivalenzklasse einer Newform ist eindimensional, und $S_k^{new}(\Gamma_0(N))$ ist orthogonale Summe dieser Klassen.

Sei $f \in S_k(\Gamma_0(N))$ eine Cusp-Form mit q-Expansion $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$. Die *L-Funktion* (oder *L-Reihe*) von f ist die Dirichlet-Reihe

$$L(s, f) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}, \qquad s \in \mathbb{C}.$$

Wir erhalten die L-Funktion aus f, indem wir eine *Mellin-Transformation* anwenden:

$$\int_0^{\infty} f(i\sigma)\sigma^s \frac{d\sigma}{\sigma} = (2\pi)^{-s}\Gamma(s)L(s, f)$$

Hierbei bezeichnet $\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}dt$ die *Gamma-Funktion*.

Ist f speziell eine Newform und durch $c_1 = 1$ normiert, so hat $L(s, f)$ eine (für Re $s > k/2 + 1$ konvergente) Euler-Produktexpansion der Form

$$L(s, f) = \prod_{p \in \mathbb{P}, p|N} \left(\frac{1}{1 - c_p p^{-s}}\right) \prod_{p \in \mathbb{P}, p \nmid N} \left(\frac{1}{1 - c_p p^{-s} + p^{k-1-2s}}\right).$$

Insbesondere gilt für $n \notin \mathbb{P}$

$$c_n = c_{p_1} \cdots c_{p_r},$$

wenn $n = p_1 \cdots p_r$ die Primfaktorzerlegung von n ist.

Die *Dedekindsche η-Funktion* ist definiert durch

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n \in \mathbb{N}} (1 - q^n), \qquad \text{wobei } q = e^{2i\pi\tau}.$$

Der Raum $S_4^{new}(\Gamma_0(6))$ ist eindimensional mit der eindeutigen normierten Newform

$$\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$$

$= q - 2q^2 - 3q^3 + 4q^4 + 6q^5 + 6q^6 - 16q^7 - 8q^8 + 9q^9 - 12q^{10} + 12q^{11} - 12q^{12} + 38q^{13} + 32q^{14} - 18q^{15} + 16q^{16} - 126q^{17} - 18q^{18} + 20q^{19} + \ldots + 168q^{23} + \ldots$
(vgl. die Tabellen unter [17]).

Soweit angegeben, stimmen die Koeffizienten dieser Newform bei q^p für Primzahlen $p \geq 5$ mit den in der Tabelle in Abschnitt 4.3 berechneten Werten für $a_p = \text{Spur}(\text{Frob}_p \,|H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l))$ überein. Es ist unser Ziel, die Gleichheit für alle Primzahlen $p \geq 5$ zu zeigen, d.h. die Übereinstimmung der L-Reihen bis auf eventuelle Euler-Faktoren bei den Primzahlen von schlechter

Reduktion. Das Methode dazu ist ein Vergleich der Galois-Darstellung zur Kohomologie von $\tilde{\mathcal{M}}$ mit der im Folgenden vorgestellten Galois-Darstellung zu der erwähnten Newform.

4.4.2 Galois-Darstellung zu einer modularen Form

Sei $f \in S_k^{new}(\Gamma_0(N)), k \geq 2$ eine Newform. Die q-Expansion

$$f(\tau) = \sum_{n=1}^{\infty} c_n q^n$$

von f habe rationale Koeffizienten. Sei $l \in \mathbb{P}$ eine Primzahl. Dann gibt es eine l-adische halbeinfache Galoisdarstellung

$$\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Q}_l),$$

die unverzweigt ist außerhalb (der Teiler von) $N \cdot l$ und für die gilt:

$$\mathrm{Spur}(\rho_l(\mathrm{Frob}_p)) = c_p \quad \text{und} \quad \det(\rho_l(\mathrm{Frob}_p)) = p^{k-1}, \qquad \text{wenn } p \nmid N \cdot l$$

Dadurch ist ρ_l bis auf Isomorphie bestimmt.

Diese Tatsachen wurden von Deligne in [2] bewiesen. Eine lesbare Formulierung (allerdings nur der Existenzaussage, nicht der Konstruktion) findet sich auch in [3], Theorem 6.1.

4.5 Nicht-kubische Mengen

Wir wollen gleich einen Satz aus [11] verwenden und müssen vorher die dort verwendeten Notationen erklären. (Zu diesem Abschnitt siehe [11], Abschnitt 4, insbesondere Definition 4.1 und Behauptung 4.11)

Sei T eine nicht-leere Teilmenge des n-dimensionalen $\mathbb{K}$-Vektorraums V. T heißt *nicht-kubisch*, wenn jedes homogene Polynom vom Grad $d = 3$ aus $\mathbb{K}[X_1, \ldots, X_n]$, das auf T verschwindet, auch auf ganz V verschwindet. Die Menge $V - \{0\}$ ist in jedem Fall nicht-kubisch; und der Nullvektor kann natürlich aus jeder nicht-kubischen Menge entfernt werden (sofern sie dadurch nicht leer wird).

Ist K ein *endlicher* Körper mit q Elementen, so können wir von einer nicht-kubischen Menge minimaler Größe sprechen und versuchen, die Zahl ihrer Elemente abzuschätzen. Es gibt in V außer dem Nullvektor noch die Vektoren

$$v_i, \qquad 1 \leq i \leq q^n - 1.$$

Weiterhin gibt es

$$d := \begin{pmatrix} n+2 \\ 3 \end{pmatrix}$$

Monome vom Grad 3 in $\mathbb{K}[X_1, \ldots, X_n]$. Wir bezeichnen sie mit

$$P_i, \qquad 1 \leq i \leq d.$$

Nun kann ein homogenes Polynom P vom Grad 3 in $\mathbb{K}[X_1, \ldots, X_n]$ dargestellt werden als

$$P = \sum_{i=1}^{d} \lambda_i P_i \qquad \text{mit } \lambda_i \in \mathbb{K}.$$

Betrachten wir jetzt die Matrix

$$A := \begin{pmatrix} P_1(v_1) & \cdots & P_d(v_1) \\ \vdots & \ddots & \vdots \\ P_1(v_{q^n-1}) & \cdots & P_d(v_{q^n-1}) \end{pmatrix},$$

so ist die Anzahl der Elemente einer minimalen nicht-kubischen Menge in V höchstens gleich dem Rang von A.

Sei speziell $V = (\mathbb{F}_2)^3$, also $d = 10$. Bei geeigneter Vertauschung der Vektoren v_i und der Monome P_i ergibt sich

$$A = \begin{pmatrix} 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ & & 1 & & & & & & & \\ 1 & 1 & & 1 & 1 & & & & & \\ & 1 & 1 & & & 1 & 1 & & & \\ 1 & & 1 & & & & & 1 & 1 & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Diese Matrix hat vollen Zeilenrang. Wir können also auf diese Weise keine kleinere nicht-kubische Menge in V als $V - \{0\}$ bestimmen.

Wir zeigen direkt, daß es tatsächlich keine kleinere gibt. Dazu reicht es, für jeden Vektor in $V - \{0\}$ ein homogenes Polynom vom Grad 3 anzugeben, das nur in diesem Vektor nicht verschwindet. Für den Vektor $(1,1,1)$ wählen wir das Polynom $X_1X_2X_3$, für den Vektor $(1,0,0)$ das Polynom $X_1^3 + X_1^2X_2 + X_1^2X_3 + X_1X_2X_3$ und für den Vektor $(1,1,0)$ das Polynom $X_1^2X_2 + X_1X_2X_3$. Der Rest folgt mit Symmetrie.

Sei jetzt noch $V = (\mathbb{F}_2)^4$, also $d = 20$. Dann erhalten wir

$$A = \begin{pmatrix}
 & & & 1 & & & & & & & & & & & & & & & & \\
 & & 1 & & & & & & & & & & & & & & & & & \\
 & & 1 & 1 & & & & & & & & 1 & & & 1 & & & & & \\
 & 1 & & & & & & & & & & & & & & & & & & \\
 & 1 & & 1 & & & & & 1 & & & & & 1 & & & & & \\
 & 1 & 1 & & & & & 1 & & & 1 & & & & & & & & \\
 & 1 & 1 & 1 & & & & 1 & 1 & & 1 & 1 & & 1 & 1 & & & & 1 \\
1 & & & & & & & & & & & & & & & & & & & \\
1 & & & 1 & & & 1 & & & & & & 1 & & & & & & & \\
1 & & 1 & & & 1 & & & & 1 & & & & & & & & & & \\
1 & & 1 & 1 & & 1 & 1 & & & 1 & & 1 & 1 & & 1 & & & 1 & & \\
1 & 1 & & & 1 & & & 1 & & & & & & & & & & & & \\
1 & 1 & & 1 & 1 & & 1 & 1 & & 1 & & & & 1 & 1 & & & 1 & & \\
1 & 1 & 1 & & 1 & 1 & & 1 & 1 & & 1 & 1 & & & & & 1 & & & \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}.$$

Diese Matrix hat über $\mathbb{F}_2$ Rang 14 (Die Summe über alle Zeilen ist Null, die Summe über weniger Zeilen ist stets ungleich Null.). Wir können also aus der Menge $V - \{0\}$ noch einen beliebigen Vektor herausnehmen, und die Menge bleibt nicht-kubisch.

Die beiden Beispiele sind natürlich so gewählt, daß wir sie auch anwenden können. Sei dazu eine endliche Menge $S = \{s_1, \ldots, s_k\}$ von Primzahlen gegeben. Sei $\mathbb{Q}_S$ das Kompositum aller quadratischen Erweiterungen von $\mathbb{Q}$, die außerhalb von S unverzweigt sind. Es gilt

$$\mathbb{Q}_S = \mathbb{Q}[\sqrt{-1}, \sqrt{s_1}, \ldots, \sqrt{s_k}].$$

Sei für $s \in S \cup \{-1\}$

$$\chi_s : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \longrightarrow \mathbb{Z}/2\mathbb{Z}, \qquad \chi_s(g) = \begin{cases} 1 & \text{falls } g\ \mathbb{Q}[\sqrt{s}] \text{ fest lässt} \\ -1 & \text{sonst} \end{cases}$$

der quadratische Galois-Charakter, der $\sqrt{s}$ ausschneidet. Die Abbildung

$$F : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{k+1}, \qquad F(g) = \begin{pmatrix} (\chi_{s_1}(g)+1)/2 \\ \vdots \\ (\chi_{s_k}(g)+1)/2 \\ (\chi_{-1}(g)+1)/2 \end{pmatrix}$$

ist dann bijektiv. Wir können also auf diese Weise $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ als $\mathbb{Z}/2\mathbb{Z}$-Vektorraum auffassen. Speziell für Frobeniuselemente können wir die χ_s

ausrechnen durch

$$\begin{aligned}\chi_s(\mathrm{Frob}_p) &= \left(\frac{s}{p}\right) \qquad \text{für } s \in S, p \in \mathbb{P}, p \notin S,\\ \chi_s(\mathrm{Frob}_\infty) &= \left(\frac{-1}{s}\right) \qquad \text{für } s \in S,\\ \chi_{-1}(\mathrm{Frob}_\infty) &= -1.\end{aligned}$$

Frob_∞ ist dabei eine gängige Bezeichnung für komplexe Konjugation, also ein Element von Ordnung 2 in $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$.

4.6 Identifikation der L-Reihe

Wir wollen jetzt beweisen, daß die L-Reihe von $\tilde{\mathcal{M}}$ bis auf eventuelle Euler-Faktoren bei den Primzahlen von schlechter Reduktion gleich der L-Reihe der modularen Form $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ ist. Das Erstaunliche daran ist, daß es im Prinzip reicht, endlich viele Koeffizienten zu vergleichen. Diese Erkenntnis basiert auf den Resultaten von G. Faltings in [6] über das Vergleichen zweier l-adischer Darstellungen. Die Grundlage dabei ist der Dichtesatz von Tchebotarev (vgl. auch [4]). J. P. Serre hat auf diese Ergebnisse aufbauend einen Satz bewiesen, den R. Livné in [11] als Theorem 4.3 aufgeschrieben hat. Wir verwenden einen Spezialfall dieses Satzes:

4.1 Satz
Sei S eine endliche Menge von Primzahlen, und seien $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_2)$ Galois-Darstellungen, die außerhalb von S unverzweigt sind. Sei $\mathbb{Q}_S$ das Kompositum aller quadratischen Erweiterungen von $\mathbb{Q}$, die außerhalb von S unverzweigt sind. Es gelte:

1. $\mathrm{Spur}\,\rho_1 \equiv \mathrm{Spur}\,\rho_2 \equiv 0 \pmod 2$ *und* $\det\rho_1 \equiv \det\rho_2 \pmod 2$.
2. *Es gibt eine endliche Menge T von Primzahlen, disjunkt zu S, für die gilt:*
   (a) *Das Bild der Menge $\{\mathrm{Frob}_t \,|\, t \in T\}$ in $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ (aufgefaßt als $\mathbb{Z}/2\mathbb{Z}$-Vektorraum wie in Abschnitt 4.5) ist nicht-kubisch.*
   (b) *Für alle $t \in T$ ist*
   $$\mathrm{Spur}\,\rho_1(\mathrm{Frob}_t) = \mathrm{Spur}\,\rho_2(\mathrm{Frob}_t)$$
   und
   $$\det\rho_1(\mathrm{Frob}_t) = \det\rho_2(\mathrm{Frob}_t).$$

Dann haben ρ_1 und ρ_2 isomorphe Halbvereinfachungen. Insbesondere gilt $\mathrm{Spur}\,\rho_1(\mathrm{Frob}_p) = \mathrm{Spur}\,\rho_2(\mathrm{Frob}_p)$ für alle Primzahlen $p \notin S$.

Die Darstellung ρ_1 sei gegeben durch die Wirkung von $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ auf der 2-adischen Kohomologie $H^3(\tilde{\mathcal{M}}, \mathbb{Q}_2))$, die nach den bisherigen Ausführungen ein 2-dimensionaler Vektorraum ist. Die Darstellung ρ_2 soll die 2-adische Darstellung sein, die nach Deligne der Eigenform $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ zugeordnet wird.

Wir weisen für ρ_1 und ρ_2 die Voraussetzungen von Satz 4.1 nach. Zunächst einmal wird in [21] als Lemma 3.11. Folgendes bewiesen:

4.2 Lemma
Sei die Galois-Darstellung $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_2)$ *unverzweigt außerhalb von 2 und 3, und sei* $\mathrm{Spur}\,\rho(\mathrm{Frob}_5) \equiv \mathrm{Spur}\,\rho(\mathrm{Frob}_7) \equiv \mathrm{Spur}\,\rho(\mathrm{Frob}_{11}) \equiv \mathrm{Spur}\,\rho(\mathrm{Frob}_{13}) \equiv 0 \pmod 2$. *Dann gilt* $\mathrm{Spur}\,\rho(\mathrm{Frob}_p) \equiv 0 \pmod 2$ *für alle Primzahlen* $p \geq 5$.

Um festzustellen, daß die Spuren unserer Galois-Darstellungen gerade sind, reicht es also, Frobeniuselemente für endlich viele Primzahlen zu untersuchen. Auch das folgt allgemein aus den Resultaten von Faltings in [6].

Wir können jetzt zeigen:

4.3 Lemma

$$\mathrm{Spur}\,\rho_1 \equiv \mathrm{Spur}\,\rho_2 \equiv 0 \pmod 2$$

Beweis:
Wir wollen zunächst das vorige Lemma auf ρ_1 und ρ_2 anwenden. Für $p = 7, 13$ gilt $a_p = 1 - 100p + 30p^2 + p^3 - \#\mathcal{M}$, für $p = 5, 11$ gilt $a_p = 1 + 10p^2 + p^3 - \#\mathcal{M}$. $\#\mathcal{M}$ ist dabei in jedem Fall gerade. Also haben wir $a_5 \equiv a_7 \equiv a_{11} \equiv a_{13} \equiv 0 \pmod 2$ und nach Anwendung des Lemmas

$$\mathrm{Spur}\,\rho_1(\mathrm{Frob}_p) \equiv 0 \pmod 2$$

für alle Primzahlen $p \geq 5$.

Die Koeffizienten der modularen Form $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ bei q^5, q^7, q^{11} und q^{13} sind gerade, also haben wir auch

$$\mathrm{Spur}\,\rho_2(\mathrm{Frob}_p) \equiv 0 \pmod 2$$

für alle Primzahlen $p \geq 5$. Da $\mathrm{Spur} \circ \rho_1$ und $\mathrm{Spur} \circ \rho_2$ stetige Abbildungen sind und die Menge $\{\mathrm{Frob}_p \,|\, p \geq 5\}$ dicht ist in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, folgt die Behauptung als Anwendung des Dichtesatzes von Tchebotarev (vgl. Abschnitt 4.1). □

4.4 Lemma

$$\det\rho_1 = \det\rho_2, \qquad \textit{insbesondere} \qquad \det\rho_1 \equiv \det\rho_2 \pmod 2$$

Beweis:
Sei $p \geq 5$. Es gilt $\det \rho_2(\mathrm{Frob}_p) = p^3$. Die Poincaré-Dualität besagt unter anderem, daß die Paarung

$$(\cdot,\cdot) : H^3(\tilde{\mathcal{M}}, \mathbb{Q}_2) \times H^3(\tilde{\mathcal{M}}, \mathbb{Q}_2) \to H^6(\tilde{\mathcal{M}}, \mathbb{Q}_2) \cong \mathbb{Q}_2,$$

perfekt ist und die Galois-Wirkung respektiert. Die Wirkung von Frob_p auf $H^6(\tilde{\mathcal{M}}, \mathbb{Q}_2)$ ist Multiplikation mit p^3. Sind ω_1, ω_2 die Eigenwerte von Frob_p auf $H^3(\tilde{\mathcal{M}}, \mathbb{Q}_2)$ mit jeweiligen Eigenvektoren v_1, v_2, dann folgt

$$\begin{aligned} \omega_1\omega_2(v_1, v_2) &= (\omega_1 v_1, \omega_2 v_2) \\ &= (\mathrm{Frob}_p(v_1), \mathrm{Frob}_p(v_2)) = \mathrm{Frob}_p((v_1, v_2)) \\ &= p^3(v_1, v_2) \end{aligned}$$

und daher $\det \rho_1(\mathrm{Frob}_p) = \omega_1\omega_2 = p^3$.

Also gilt $\det \rho_1(\mathrm{Frob}_p) = \det \rho_2(\mathrm{Frob}_p)$.

Da auch $\det \circ \rho_1$ und $\det \circ \rho_2$ stetige Abbildungen sind, erhalten wir wie in Lemma 4.3

$$\det \rho_1 = \det \rho_2$$

und insbesondere

$$\det \rho_1 \equiv \det \rho_2 \pmod 2$$

als Anwendung des Dichtesatzes von Tchebotarev. □

4.5 Satz
Bis auf eventuelle Euler-Faktoren bei 2 und 3 ist die L-Reihe der mittleren Kohomologie $H^3(\tilde{\mathcal{M}}, \mathbb{Q}_l)$ von $\tilde{\mathcal{M}}$ gleich der L-Reihe der modularen Form

$$\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2,$$

der eindeutigen Newform vom Gewicht 4 und Level 6.

Beweis:
Die Primzahlen von schlechter Reduktion von $\tilde{\mathcal{M}}$ sind 2 und 3, der Level von $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ ist 6. Also sind die beiden Darstellungen ρ_1 und ρ_2 unverzweigt außerhalb von $S = \{2, 3\}$. Der Körper $\mathbb{Q}_S$, der für die Anwendung von Satz 4.1 benötigt wird, ist $\mathbb{Q}[i, \sqrt{2}, \sqrt{3}]$. Es gilt $\mathbb{Q}_S = \mathbb{Q}[\xi_{24}]$, wobei ξ_{24} eine primitive 24te Einheitswurzel ist, also $\#\,\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) = 8$. Die nichttrivialen Elemente von $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ sind gegeben durch

$$\xi_{24} \mapsto \xi_{24}^t, \qquad t \in T := \{5, 7, 11, 13, 17, 19, 23\}.$$

Das heißt gerade, daß das Bild der Menge $\{\mathrm{Frob}_t \,|\, t \in T\}$ in $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ nicht-kubisch ist. Nach Lemma 4.4 gilt $\det \rho_1(\mathrm{Frob}_p) = p^3 = \det \rho_2(\mathrm{Frob}_p)$

und nach der Tabelle in Abschnitt 4.3 außerdem $\mathrm{Spur}\,\rho_1(\mathrm{Frob}_p) = a_p = \mathrm{Spur}\,\rho_2(\mathrm{Frob}_p)$ für alle $p \in T$. Lemma 4.3 liefert die erforderliche Bedingung über die Spuren, Lemma 4.4 die über die Determinanten. Durch Anwendung von Satz 4.1 folgt schließlich die Behauptung. □

Es hat also ausgereicht, die Punkte auf $\mathcal{M}$ für alle Primzahlen $5 \leq p \leq 23$ zu zählen. Mit weniger Primzahlen können wir nicht auskommen (zumindest, wenn wir Satz 4.1 verwenden wollen), da es keine nicht-kubische Menge mit weniger als 7 Elementen in $(\mathbb{Z}/2\mathbb{Z})^3$ gibt.

Verzichten wir auf die Theorie nicht-kubischer Mengen und ersetzen die entsprechende Bedingung in Satz 4.1 durch die schwächere Forderung

$$\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) = \{\mathrm{Frob}_t \,|t \in T\},$$

so müssen wir noch eine Primzahl p zu der Menge T hinzunehmen, für die $p \equiv 1 \pmod{24}$ gilt. Das kleinste mögliche p ist dann 73. Diese Methode wurde z.B. in [21] verwendet.

In [4] wird noch eine Abschätzung angegeben, die allgemein besagt, für welche Primzahlen man Koeffizienten vergleichen muß, um die L-Reihen zu zwei rationalen l-adischen Galois-Darstellungen als gleich zu erkennen, nämlich für alle Primzahlen kleiner als

$$70 \cdot (l^{2d^2}(\log l^{2d^2} + \sum_{p \in S} \log p))^2.$$

Hierbei ist S die Menge der Primzahlen von schlechter Reduktion und d die Dimension des Zielraums der Galois-Darstellungen. Allerdings gilt die Abschätzung nur unter der verallgemeinerten Riemannschen Hypothese.

In unserem Fall ergibt sich mit $l = 2$, $d = h^3 = 2$ und $S = \{2, 3\}$:

$$70 \cdot (2^8(\log 2^8 + \log 2 + \log 3))^2 \approx 246949150$$

Dieses Ergebnis ist natürlich für praktische Zwecke völlig ungeeignet.

Kapitel 5

Die kleinen Brüder von $\mathcal{M}$

Wir wollen nun einige andere interessante Mitglieder der in Kapitel 1 vorgestellten Familie von Quintiken auf ihre L-Reihen untersuchen. Dabei können wir viele Methoden aus den vorigen Kapiteln völlig analog verwenden. Wir werden deshalb aus Gründen der Übersichtlichkeit nicht jedes Detail aufschreiben, sondern markante Wegpunkte setzen.

5.1 Die Barth-Nieto-Quintik $\mathcal{M}_{(1:0)}$

5.1.1 Singularitäten und Auflösung

Über $\mathbb{C}$ hat $\mathcal{M}_{(1:0)}$ folgende Singularitäten:

- Die Σ_6-Bahn des Punktes $(1:1:1:-1:-1:-1)$; das sind 10 gewöhnliche Doppelpunkte (die "Segre nodes").
- Die Gerade $\{(0:0:0:x:y:z), \quad x+y+z=0\}$ und ihre Σ_6-Bahn; das sind 20 singuläre Geraden. Jeweils 4 dieser Geraden schneiden sich in den 15 Punkten der Σ_6-Bahn von $(0:0:0:0:1:-1)$; weitere Schnittpunkte gibt es nicht.

Der Tangentialkegel in den Punkten der Σ_6-Bahn von $(0:0:0:0:1:-1)$ ist isomorph zu der *Cayley-Kubik*

$$X_0X_1X_2 + X_0X_1X_3 + X_0X_2X_3 + X_1X_2X_3 = 0.$$

Nach [1] lassen sich die Singularitäten von $\mathcal{M}_{(1:0)}$ in drei Schritten auflösen, so daß wir ein glattes Modell $\tilde{\mathcal{M}}_{(1:0)}$ von $\mathcal{M}_{(1:0)}$ erhalten:

Schritt 1: Wir ersetzen die 15 Schnittpunkte der singulären Geraden jeweils durch eine Cayley-Kubik. (Dadurch werden die singulären Geraden getrennt.)

Schritt 2: Wir ersetzen die 20 singulären Geraden jeweils durch Quadriken (d.h. $\mathbb{P}^1 \times \mathbb{P}^1$).

Schritt 3: Wir ersetzen die 10 Doppelpunkte durch Geraden ($\mathbb{P}^1$). Hier wird also eine kleine Auflösung gewählt.

Eine Untersuchung wie in Kapitel 2 zeigt, daß in allen Charakteristiken $p \geq 5$ genau die erwähnten Singularitäten auftreten und dort die Reduktion von $\tilde{\mathcal{M}}_{(1:0)}$ auf $\mathbb{F}_p$ wieder glatt ist. Die Primzahlen von schlechter Reduktion sind auch hier wieder 2 und 3.

5.1.2 Die L-Reihe

Nach [1] ist die Eulerzahl $\chi(\mathcal{M}_{(1:0)})$ von $\mathcal{M}_{(1:0)}$ gleich -10, die von $\tilde{\mathcal{M}}_{(1:0)}$ gleich 100. Sei

$$h^i := h^i(\tilde{\mathcal{M}}_{(1:0)})$$

die i-te Betti-Zahl von $\tilde{\mathcal{M}}_{(1:0)}$. Wir erhalten wieder $h^0 = h^6 = 1$ und, da die Fasern des Blow-Up auch hier einfach zusammenhängend sind, $h^1 = h^5 = 0$. Es ergibt sich

$$\begin{aligned} 100 = \chi(\tilde{\mathcal{M}}_{(1:0)}) &= h^0 - h^1 + h^2 - h^3 + h^4 - h^5 + h^6 \\ &= 1 - 0 + h^2 - h^3 + h^4 - 0 + 1 \\ &= 2 + 2h^2 - h^3, \end{aligned}$$

also

$$h^3 = 2h^2 - 98.$$

Wir wollen den Wert von h^3 wieder mit Hilfe einer Abschätzung, die wir aus dem Fixpunktsatz von Lefschetz und den Weil-Vermutungen erhalten, ermitteln. Da in allen Charakteristiken $p \geq 5$ alle Singularitäten von $\mathcal{M}_{(1:0)}$ und die exceptionellen Mengen der Blow-Ups rational über $\mathbb{F}^p$ sind, ist die Wirkung von Frob_p auf $H^2(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q})$ Multiplikation mit p und die Wirkung auf $H^4(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q})$ Multiplikation mit p^2. Wir erhalten

$$\begin{aligned} \#\tilde{\mathcal{M}}_{(1:0)} &= \sum_{i=0}^{6} (-1)^i \,\mathrm{Spur}(\mathrm{Frob}_p \,|H^i(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q}_l)) \\ &= 1 + ph^2 - \mathrm{Spur}(\mathrm{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q}_l)) + p^2 h^4 + p^3 \\ &= 1 + p^3 + p(p+1)h^2 - \mathrm{Spur}(\mathrm{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q}_l)). \end{aligned}$$

Wegen $|\,\mathrm{Spur}(\mathrm{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q}_l))| \leq p^{3/2} h^3$ folgt

$$\begin{aligned} |\#\tilde{\mathcal{M}}_{(1:0)} - 1 - p^3 - p(p+1)h^2| &\leq p^{3/2} h^3 \\ &= p^{3/2}(2h^2 - 98). \end{aligned}$$

Wenn wir also jetzt noch die Punkte auf $\tilde{\mathcal{M}}_{(1:0)}$ für genügend große p zählen, können wir h^2 bestimmen.

Wir zählen zunächst mit dem Computer und den Methoden aus Kapitel 3 die Punkte auf $\mathcal{M}_{(1:0)}$. Wir erhalten:

p	$\#\mathcal{M}_{(1:0)}$
5	370
7	920
11	2860
13	4370
17	8950
19	11780
23	19360

Im ersten Schritt der Singularitätenauflösung werden 15 Punkte durch Cayley-Kubiken ersetzt. Wir müssen also wissen, wieviele Punkte auf dieser Kubik liegen. Sei $(X_0 : X_1 : X_2 : X_3) \in \mathbb{P}^3(\mathbb{F}_p)$ mit

$$X_0X_1X_2 + X_0X_1X_3 + X_0X_2X_3 + X_1X_2X_3 = 0.$$

Das ist äquivalent zu

$$X_0(X_1X_2 + X_1X_3 + X_2X_3) = -X_1X_2X_3.$$

Wir unterscheiden zwei Fälle:

Fall 1: Es gilt $X_1X_2+X_1X_3+X_2X_3 = 0$. In diesem Fall ist auch $X_1X_2X_3 = 0$. Es gilt also entweder $X_1 = X_2 = X_3 = 0 \neq X_0$, oder genau eine der drei Koordinaten X_1, X_2, X_3 ist $\neq 0$. Im letzten Fall ist X_0 beliebig. Es gibt also

$$1 + 3 \cdot p$$

solche Punkte.

Fall 2: Es gilt $X_1X_2 + X_1X_3 + X_2X_3 \neq 0$. Dann ist X_0 durch

$$X_0 = \frac{-X_1X_2X_3}{X_1X_2 + X_1X_3 + X_2X_3}$$

bestimmt. Die Gleichung $X_1X_2 + X_1X_3 + X_2X_3 = 0$ beschreibt eine glatte Quadrik in $\mathbb{P}^2$, auf der immer $\#\mathbb{P}^1 = p + 1$ Punkte liegen. Also gibt es

$$\#\mathbb{P}^2 - \#\mathbb{P}^1 = p^2 + p + 1 - (p + 1) = p^2$$

Punkte, die $X_1X_2 + X_1X_3 + X_2X_3 \neq 0$ erfüllen.

Auf der Cayley-Kubik liegen also p^2+3p+1 Punkte.

Wir können jetzt zusammenzählen:

$$\begin{aligned}
\#\tilde{\mathcal{M}}_{(1:0)} &= \#\mathcal{M}_{(1:0)} \\
&+ 15(\#\text{Cayley-Kubik } - 1) \\
&+ 20(\#\mathbb{P}^1 \times \mathbb{P}^1 - \#\mathbb{P}^1) \\
&+ 10(\#\mathbb{P}^1 - 1) \\
&= \#\mathcal{M}_{(1:0)} + 15(p^2+3p) + 20(p^2+p) + 10p \\
&= \#\mathcal{M}_{(1:0)} + 35p^2 + 75p
\end{aligned}$$

Wir haben also nun die Abschätzung

$$|\#\mathcal{M}_{(1:0)} + 35p^2 + 75p - 1 - p^3 - p(p+1)h^2| \leq p^{3/2}(2h^2 - 98).$$

Speziell für $p = 13$ ergibt sich

$$|4531 - 91h^2| \leq 13^{3/2}(h^2 - 49)$$

und daraus

$$h^2 = 50 \quad \text{und (wie bei } \tilde{\mathcal{M}}) \quad h^3 = 2.$$

Wir definieren wieder

$$a_p := \text{Spur}(\text{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q}_l)).$$

Dann haben wir

$$\begin{aligned}
a_p &= 1 + p^3 + 50p(p+1) - 35p^2 - 75p - \#\mathcal{M}_{(1:0)} \\
&= 1 + p^3 + 15p^2 - 25p - \#\mathcal{M}_{(1:0)}.
\end{aligned}$$

Wir rechnen einige Werte aus:

p	5	7	11	13	17	19	23
a_p	6	-16	12	38	-126	20	168

Soweit berechnet, stimmen also die a_p wieder mit den Koeffizienten der modularen Form $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ überein. Wir können nun (da insbesondere $h^2 = 2$ gilt, die Primzahlen von schlechter Reduktion die gleichen sind wie bei $\mathcal{M}$ und es sich um dieselbe modulare Form handelt) den letzten Abschnitt aus Kapitel 4 wörtlich übernehmen und folgenden Satz beweisen:

5.1 Satz
Bis auf eventuelle Euler-Faktoren bei 2 und 3 ist die L-Reihe der mittleren Kohomologie $H^3(\tilde{\mathcal{M}}_{(1:0)}, \mathbb{Q}_l)$ von $\tilde{\mathcal{M}}_{(1:0)}$ gleich der L-Reihe der modularen Form

$$\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2,$$

der eindeutigen Newform vom Gewicht 4 und Level 6.

Beweis:
siehe Satz 4.5. □

5.2 Die Quintik $\mathcal{M}_{(-3:1)}$

5.2.1 Singularitäten und Auflösung

Über $\mathbb{C}$ hat $\mathcal{M}_{(-3:1)}$ genau 10 Singularitäten, nämlich die Σ_6-Bahn des Punktes $(1:1:1:-1:-1:-1)$. Die Tangentialkegel dort sind jeweils isomorph zu der glatten kubischen Fläche $\mathcal{D}$, die durch

$$\begin{aligned} 0 &= X_0^2X_1 + X_0X_1^2 + X_0^2X_2 + X_0X_2^2 \\ &+ X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 \\ &+ X_2^2X_3 + X_2X_3^2 + 2X_0X_1X_2 + 2X_1X_2X_3 \\ &+ 3X_0^2X_3 + 3X_0X_3^2 + 4X_0X_1X_3 + 4X_0X_2X_3. \end{aligned}$$

gegeben ist. In [19] erhielten diese Singularitäten deshalb den Namen "Del Pezzo nodes".

Wir können die Singularitäten von $\mathcal{M}_{(-3:1)}$ auflösen und ein glattes Modell $\tilde{\mathcal{M}}_{(-3:1)}$ von $\mathcal{M}_{(-3:1)}$ erhalten, wenn wir die singulären Punkte jeweils durch den Tangentialkegel ersetzen.

Wir müssen nun untersuchen, für welche Primzahlen p die Reduktion von $\tilde{\mathcal{M}}_{(-3:1)}$ wieder glatt ist (und welche Singularitäten in diesen Charakteristiken überhaupt auftreten). Die Fälle $p = 2$ und $p = 3$ können wir a priori ausklammern, denn für $p = 2$ sieht $\mathcal{M}_{(-3:1)}$ aus wie $\mathcal{M}$ und für $p = 3$ wie $\mathcal{M}_{(0:1)}$. Für $p \geq 5$ können wir eine Fallunterscheidung wie bei der Varietät $\mathcal{M}$ durchführen. Wir erhalten zunächst, daß die Koordinaten eines singulären Punktes der Gleichung

$$P(X) := X^4 - \frac{1}{3}C_2(\eta)X^2 - \frac{2}{9}C_3(\eta)X - \frac{1}{6}C_4(\eta) + \frac{1}{18}C_2^2(\eta) = 0$$

genügen müssen. Alle Fälle der nachfolgenden Fallunterscheidung verhalten sich wie bei der Untersuchung von $\mathcal{M}$, außer dem

Fall 3: Wir können annehmen, daß $\eta = (1:1:1:1:1:-5)$. Damit ist $C_2 = 30, C_3 = -120, C_4 = 630$ und

$$P(X) = X^4 - 10X^2 + \frac{80}{3}X - 55.$$

Damit haben wir

$$\begin{aligned} P(1) &= -7 \cdot \frac{2^4}{3} \\ P(-5) &= 7 \cdot \frac{5 \cdot 2^4}{3} \end{aligned}$$

Tatsächlich treten also in Charakteristik $p = 7$ weitere 6 Singularitäten auf, nämlich die Σ_6-Bahn des Punktes $(1 : 1 : 1 : 1 : 1 : -5)$. Wir können das auch daraus erkennen, daß $\mathcal{M}_{(-3:1)}$ für $p = 7$ aussieht wie die Varietät $\mathcal{M}_{(25:1)}$, die schon über $\mathbb{C}$ über diese 6 Singularitäten verfügt, die gewöhnliche Doppelpunkte sind.

Die Primzahlen von schlechter Reduktion sind also 2,3 und 7. In allen anderen Charakteristiken sind die Singularitäten von $\mathcal{M}_{(-3:1)}$ genau die, die auch über $\mathbb{C}$ auftreten, und die Reduktion von $\tilde{\mathcal{M}}_{(-3:1)}$ ist glatt.

5.2.2 Die L-Reihe

Wir wollen uns zunächst um die Kohomologie von $\tilde{\mathcal{M}}_{(-3:1)}$ kümmern und benötigen dazu als erstes die Eulerzahl. Wir fassen dazu $\mathcal{M}_{(-3:1)}$ als singuläres Mitglied einer Familie von glatten Quintiken $\{X_t\}$ auf. Dann gilt (vgl. [5], Korollar 2.3.)

$$\begin{aligned}\chi(\mathcal{M}_{(-3:1)}) &= \chi(X_t) + 10 \cdot \text{Milnorzahl(Del Pezzo Node)} \\ &= -200 + 10 \cdot 16 \\ &= -40.\end{aligned}$$

$\tilde{\mathcal{M}}_{(-3:1)}$ entsteht aus $\mathcal{M}_{(-3:1)}$ durch Ersetzen von 10 Punkten durch kubische Flächen, also

$$\begin{aligned}\chi(\tilde{\mathcal{M}}_{(-3:1)}) &= \chi(\mathcal{M}_{(-3:1)}) + 10 \cdot (\chi(\text{kubische Fläche}) - 1) \\ &= -40 + 10 \cdot (\chi(\mathbb{P}^2 \text{ aufgeblasen in 6 Punkten}) - 1) \\ &= -40 + 10 \cdot (9 - 1) \\ &= 40.\end{aligned}$$

Setzen wir wieder

$$h^i := h^i(\tilde{\mathcal{M}}_{(-3:1)}),$$

so haben wir $h^0 = h^6 = 1, h^1 = h^5 = 0$ und die Beziehung

$$40 = \chi(\tilde{\mathcal{M}}_{(-3:1)}) = 2 + 2h^2 - h^3.$$

Für $p \neq 2, 3, 7$ sind alle Singularitäten von $\mathcal{M}_{(-3:1)}$ und die exceptionellen Mengen der Blow-Ups rational über $\mathbb{F}_p$, und wir erhalten wie gehabt aus dem Fixpunktsatz von Lefschetz

$$\#\tilde{\mathcal{M}}_{(-3:1)} = 1 + p^3 + p(p+1)h^2 - \text{Spur}(\text{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(-3:1)}, \mathbb{Q}_l))$$

und wegen $|\,\text{Spur}(\text{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(-3:1)}, \mathbb{Q}_l))| \leq p^{3/2}h^3$

$$\begin{aligned}|\#\tilde{\mathcal{M}}_{(-3:1)} - 1 - p^3 - p(p+1)h^2| &\leq p^{3/2}h^3 \\ &= p^{3/2}(2h^2 - 38).\end{aligned}$$

Es gilt

$$\#\tilde{\mathcal{M}}_{(-3:1)} = \#\mathcal{M}_{(-3:1)} + 10 \cdot (\#\mathcal{D} - 1).$$

Dabei ist $\mathcal{D}$ eine glatte kubische Fläche, also liegen über $\mathbb{F}_p$ darauf nach dem Fixpunktsatz von Lefschetz

$$\begin{aligned} \#\mathcal{D} &= \sum_{i=0}^{4} (-1)^i \operatorname{Spur}(\operatorname{Frob}_p | H^i(\mathcal{D}, \mathbb{Q}_l)) \\ &= 1 - 0 + \operatorname{Spur}(\operatorname{Frob}_p | H^2(\mathcal{D}, \mathbb{Q}_l)) - 0 + p^2 \\ &= 1 + p^2 + \operatorname{Spur}(\operatorname{Frob}_p | H^2(\mathcal{D}, \mathbb{Q}_l)) \end{aligned}$$

Punkte. Man sieht der Gleichung von $\mathcal{D}$ nicht an, wieviele Punkte nun genau darauf liegen, deshalb benutzen wir zum Zählen auch den Computer.

p	$\#\mathcal{M}_{(-3:1)}$	$\#\mathcal{D}$	p	$\#\mathcal{M}_{(-3:1)}$	$\#\mathcal{D}$
5	430	51	113	1639060	13335
11	2590	177	127	2283800	17019
13	4340	261	131	2498800	17817
17	9250	375	137	2853160	19455
19	10940	495	139	2962460	20295
23	19570	645	149	3630400	22947
29	36580	987	151	3772700	23859
31	42860	1179	157	4234400	25749
37	68660	1629	163	4718960	27711
41	92950	1887	167	5080180	28725
43	106100	2151	173	5631130	30795
47	135460	2445	179	6214450	32937
53	187840	3075	181	6435500	34029
59	252460	3777	191	7519990	37437
61	280040	4149	193	7739780	38601
67	362840	4959	197	8198560	39795
71	432430	5397	199	8440100	40995
73	468500	5841	211	10048700	45999
79	588680	6795	223	11809460	51291
83	677560	7305	227	12473020	52665
89	827590	8367	229	12802220	54045
97	1041980	10089	233	13467640	55455
101	1173490	10707	239	14475250	58317
103	1244900	11331	241	14857820	59769
107	1393870	11985	251	16774300	64257
109	1478240	12645	257	17918470	67335

Nach den Zahlen scheint

$$\operatorname{Spur}(\operatorname{Frob}_p | H^2(\mathcal{D}, \mathbb{Q}_l)) = p \cdot \begin{cases} 5 & \text{falls } p \equiv 2 \pmod 3 \\ 7 & \text{falls } p \equiv 1 \pmod 3 \end{cases}$$

zu gelten; es gibt für uns aber keine Notwendigkeit, das zu beweisen.

Für $p = 17$ liefert die Abschätzung aus dem Fixpunktsatz von Lefschetz zum ersten Mal $h^2 > 24$, für $p = 59$ zum ersten Mal $h^2 < 26$. Also haben wir

$$h^2 = 25, \qquad h^3 = 12.$$

Wir wollen wieder untersuchen, ob die L-Reihe von $\mathcal{M}_{(-3:1)}$ modular ist. Sei dazu

$$a_p := \mathrm{Spur}(\mathrm{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(-3:1)}, \mathbb{Q}_l)).$$

Wir listen jetzt a_p auf, dann die Koeffizienten b_p einer Newform vom Gewicht 4 für $\Gamma_0(21)$ und dann die Koeffizienten c_p einer Newform vom Gewicht 2 für $\Gamma_0(21)$. Beide modularen Formen sind unter [17] tabelliert.

p	a_p	b_p	c_p	p	a_p	b_p	c_p
5	−54	−4	−2	71	−678	−678	0
11	282	62	4	73	−2832	−642	−6
13	−192	−62	−2	79	−5580	740	−16
17	−426	84	−6	83	−4512	468	−12
19	480	100	4	89	−6030	200	−14
23	−42	−42	0	97	7464	−1266	18
29	−300	−10	−2	101	7302	232	14
31	−48	−48	0	103	2328	−1792	8
37	864	−246	6	107	234	−1906	4
41	162	−248	2	109	−9900	−90	−18
43	−792	68	−4	113	−7452	458	−14
47	324	324	0	127	804	804	0
53	1848	258	6	131	3432	812	4
59	3660	120	12	137	−3696	414	−6
61	12	622	−2	139	6720	−1620	12
67	2244	904	4	149	6840	2370	6

Soweit berechnet, gilt stets

$$a_p - b_p - 5 \cdot p \cdot c_p = 0.$$

Tatsächlich scheint sich also die L-Reihe von $\mathcal{M}_{(-3:1)}$ als Summe von L-Reihen modularer Formen darstellen zu lassen. Der Raum $S_4^{new}(\Gamma_0(21))$ ist 4-dimensional, $S_2^{new}(\Gamma_0(21))$ nur 1-dimensional (s. Tabelle unter [17]). Es ist also unwahrscheinlich, daß die gefundene Linearkombination lediglich zufällig für die angegebenen Primzahlen verschwindet.

Nun habe ich leider nicht die Möglichkeit, die Gültigkeit der Gleichung für alle $p \neq 2, 3, 7$ zu zeigen. Der Satz von Livné aus [11] ist nur für Galois-Darstellungen nach $\mathrm{GL}_2(\mathbb{Q}_2)$, nicht aber nach $\mathrm{GL}_{12}(\mathbb{Q}_2)$ ausgelegt, und ich weiß auch nicht, ob die Darstellung, die wir aus der Wirkung von $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

auf $H^3(\tilde{\mathcal{M}}_{(-3:1)}, \mathbb{Q}_l)$ erhalten, etwa in kleinere Blöcke zerfällt (also z.B. schon halbeinfach ist). Sollte es aber einen vergleichbaren Satz geben, der auch ähnliche Voraussetzungen hat, haben wir einige Vorarbeit geleistet. Es gibt 3 Primzahlen von schlechter Reduktion, und wir können eine nicht-kubische Menge (mit 14 Elementen) in $(\mathbb{Z}/2\mathbb{Z})^4$ angeben, also im Prinzip sagen, wieviele Primzahlen getestet werden müssen, um Gleichheit für alle Primzahlen von guter Reduktion sicherzustellen.

Die Formel aus [4], die wir (unter Annahme der verallgemeinerten Riemannschen Hypothese) benutzen könnten, um die Modularität zu beweisen, liefert, daß wir alle Primzahlen kleiner als

$$70 \cdot (2^{288}(\log 2^{288} + \log 2 + \log 3 + \log 7))^2 \approx 7 \cdot 10^{90}$$

testen müssten - das sind natürlich viel zu viele.

5.3 Die Quintik $\mathcal{M}_{(25:1)}$

5.3.1 Singularitäten und Auflösung

Über $\mathbb{C}$ hat $\mathcal{M}_{(25:1)}$ genau 106 isolierte Singularitäten, nämlich

Die "Segre nodes": Die Σ_6-Bahn von

$$(1:1:1:-1:-1:-1), \qquad \text{insgesamt 10 Punkte}$$

Die "Moving nodes": Die Σ_6-Bahn von

$$(1:1:-1:-1:3\sqrt{-3}:-3\sqrt{-3}), \qquad \text{insgesamt 90 Punkte}$$

Zusätzliche Singularitäten: Die Σ_6-Bahn von

$$(1:1:1:1:1:-5), \qquad \text{insgesamt 6 Punkte}$$

Letztere Singularitäten sind ebenfalls gewöhnliche Doppelpunkte; der Tangentialkegel dort ist isomorph zu der glatten Quadrik

$$2(X_0^2 + X_1^2 + X_2^2 + X_3^2) - S_2(X_0, \ldots, X_3) = 0.$$

Die Singularitäten können also wieder durch Blow-Up aufgelöst werden, und wir erhalten ein glattes Modell $\tilde{\mathcal{M}}_{(25:1)}$ von $\mathcal{M}_{(25:1)}$.

Über $\mathbb{F}_2$ und $\mathbb{F}_3$ sieht $\mathcal{M}_{(25:1)}$ aus wie $\mathcal{M}$, über $\mathbb{F}_5$ wie $\mathcal{M}_{(0:1)}$ und über $\mathbb{F}_7$ wie $\mathcal{M}_{(-3:1)}$. In den anderen Charakteristiken p zeigt eine Untersuchung wie in Kapitel 2, daß die "Segre nodes" und ihre Tangentialkegel immer rational

über $\mathbb{F}_p$ sind, die "Moving nodes" und ihre Tangentialkegel hingegen nur dann, wenn $p \equiv 1, -5 \pmod{12}$.

Die sechs zusätzlichen Singularitäten sind ebenfalls rational über $\mathbb{F}_p$; ihre Tangentialkegel jedoch nur, wenn $p \equiv 1, 4 \pmod 5$. In diesem Fall enthalten sie also jeweils $(p+1)^2 = p^2 + 2p + 1$ Punkte. Ist hingegen $p \equiv 2, 3 \pmod 5$, so liegen nur $p^2 + 1$ Punkte auf den Tangentialkegeln. In diesem Fall sind vermutlich zwei sich schneidende Geraden des Regelsystems bis auf den Schnittpunkt nicht rational über $\mathbb{F}_p$. Ich gebe keinen Beweis dazu an, da dieser ähnlich funktionieren würde wie die Untersuchungen zu den Tangentialkegeln der Singularitäten von $\mathcal{M}$ und da wir die Behauptung für die wenigen p, zu denen wir sie benötigen, von Hand überprüfen können.

Die Primzahlen von schlechter Reduktion sind also 2, 3, 5 und 7.

5.3.2 Die L-Reihe

Sei d der Defekt von $\mathcal{M}_{(25:1)}$ und $h^i := \dim H^i(\mathcal{M}_{(25:1)}, \mathbb{Q})$ wie üblich. Dann gilt nach den Formeln aus [22], die wir schon für $\mathcal{M}$ angewendet haben:

$$\begin{aligned} h^3 &= 204 - 2 \cdot 106 + 2d \qquad \text{und} \\ h^2 &= h^4 = d + 107. \end{aligned}$$

Wir zählen wieder die Punkte auf $\tilde{\mathcal{M}}_{(25:1)}$:

$$\#\tilde{\mathcal{M}}_{(25:1)} = \#\mathcal{M}_{(25:1)} + \begin{cases} 106(p^2+2p) & \text{falls } p \equiv 1, -5 \pmod{12}, p \equiv 1, 4 \pmod 5 \\ 16(p^2+2p) & \text{falls } p \equiv -1, 5 \pmod{12}, p \equiv 1, 4 \pmod 5 \\ 106p^2 + 200p & \text{falls } p \equiv 1, -5 \pmod{12}, p \equiv 2, 3 \pmod 5 \\ 16p^2 + 20p & \text{falls } p \equiv -1, 5 \pmod{12}, p \equiv 2, 3 \pmod 5 \end{cases}$$

Wir haben also für den Fall $p \equiv 1, -5 \pmod{12}$ die Abschätzung

$$\begin{aligned} |\#\tilde{\mathcal{M}}_{(25:1)} - 1 - p^3 - p(p+1)h^2| &\leq p^{3/2}h^3 \\ &= p^{3/2}(2h^2 - 222). \end{aligned}$$

Ausrechnen für $p = 31$ liefert $h^2 > 120$; für $p = 139$ erhalten wir $h^2 < 122$. Damit folgt

$$h^2 = 121, \qquad h^3 = 20.$$

Im Fall $p \equiv -1, 5 \pmod{12}$ gilt

$$|\#\tilde{\mathcal{M}}_{(25:1)} - 1 - p^3 - p(p+1)k| \leq p^{3/2}h^3$$

für ein $k \in \mathbb{Z}$ mit $|k| \leq h^2$. Der Fall $p = 23$ liefert $k > 30$; für $p = 83$ erhalten wir $k < 32$. Wir definieren wieder die Koeffizienten der L-Reihe durch

$$a_p := \mathrm{Spur}(\mathrm{Frob}_p \,|H^3(\tilde{\mathcal{M}}_{(25:1)}, \mathbb{Q}_l))$$

Wir haben also

- falls $p \equiv 1, -5 \pmod{12}, p \equiv 1, 4 \pmod{5}$:

$$\begin{aligned} a_p &= 1 + p^3 + 121p(p+1) - \#\tilde{\mathcal{M}}_{(25:1)} \\ &= 1 + p^3 + 121p(p+1) - \#\mathcal{M}_{(25:1)} - 106(2p + p^2) \\ &= 1 + p^3 + 15p^2 - 91p - \#\mathcal{M}_{(25:1)} \end{aligned}$$

- falls $p \equiv -1, 5 \pmod{12}, p \equiv 1, 4 \pmod{5}$:

$$\begin{aligned} a_p &= 1 + p^3 + 31p(p+1) - \#\tilde{\mathcal{M}}_{(25:1)} \\ &= 1 + p^3 + 31p(p+1) - \#\mathcal{M}_{(25:1)} - 16(2p + p^2) \\ &= 1 + p^3 + 15p^2 - p - \#\mathcal{M}_{(25:1)} \end{aligned}$$

- falls $p \equiv 1, -5 \pmod{12}, p \equiv 2, 3 \pmod{5}$:

$$\begin{aligned} a_p &= 1 + p^3 + 121p(p+1) - \#\tilde{\mathcal{M}}_{(25:1)} \\ &= 1 + p^3 + 121p(p+1) - \#\mathcal{M}_{(25:1)} - 100(2p + p^2) - 6p^2 \\ &= 1 + p^3 + 15p^2 - 79p - \#\mathcal{M}_{(25:1)} \end{aligned}$$

- falls $p \equiv -1, 5 \pmod{12}, p \equiv 2, 3 \pmod{5}$:

$$\begin{aligned} a_p &= 1 + p^3 + 31p(p+1) - \#\tilde{\mathcal{M}}_{(25:1)} \\ &= 1 + p^3 + 31p(p+1) - \#\mathcal{M}_{(25:1)} - 10(2p + p^2) - 6p^2 \\ &= 1 + p^3 + 15p^2 + 11p - \#\mathcal{M}_{(25:1)} \end{aligned}$$

Wir listen in der folgenden Tabelle für einige Werte von p zunächst die Anzahl $\#\tilde{\mathcal{M}}_{(25:1)}$ der Punkte auf $\tilde{\mathcal{M}}_{(25:1)}$ über $\mathbb{F}_p$ auf, dann a_p, dann die Koeffizienten b_p einer Newform vom Level $210 = 2 \cdot 3 \cdot 5 \cdot 7$ und Gewicht 4. Diese Newform ist aufgrund des hohen Levels in den Tabellen, die man unter [17] findet, nicht erfaßt; ihre Koeffizienten lassen sich aber mit dem Programm HECKE, das dort heruntergeladen werden kann, bestimmen.

HECKE ist eine von W. A. Stein erstellte freie Software. Sie ist unter Unix und Linux lauffähig und beherrscht den Umgang mit modularen Formen zu beliebigen Levels und Gewichten. Insbesondere kann sie Dimensionen von Räumen modularer Formen und Koeffizienten modularer Formen ausrechnen.

Soweit berechnet, ist $a_p - b_p$ durch $9 \cdot p$ teilbar. Wir geben daher auch die Werte $\frac{a_p - b_p}{9 \cdot p}$ an.

p	$\#\mathcal{M}_{(25:1)}$	a_p	b_p	$\frac{a_p - b_p}{9 \cdot p}$
11	2716	420	24	4
13	3926	−220	14	−2
17	9076	360	54	2
19	11186	−640	44	−4
23	21856	−1500	156	−8
29	35236	1740	174	6
31	43706	−2320	−88	−8
37	68966	−700	−34	−2
41	93496	600	−138	2
43	108326	−4480	164	−12
47	141076	−3600	−216	−8
53	188416	3180	318	6
59	255616	1920	−204	4
61	278786	−1540	−442	−2
67	355886	6920	−316	12
71	428596	4860	−252	8
73	472286	−9100	98	−14
79	580466	−1000	−1000	0
83	666556	9480	516	12
89	822616	1080	−522	2
97	1037726	8420	−310	10
101	1176376	6840	1386	6
103	1237286	6440	−976	8
107	1417336	−19380	−120	−20
109	1464866	−1540	422	−2
113	1647736	−12060	2178	−14
127	2282486	−2200	−2200	0
131	2493256	12120	−2028	12
137	2839456	14940	2610	10
139	2938106	24680	−340	20
149	3666796	−25980	−1842	−18

Die Werte in der letzten Spalte sind für die angegebenen p die Koeffizienten c_p einer Newform vom Level 210 und Gewicht 2, die ebenfalls mit HECKE ausgerechnet werden können. Es gilt also für alle angegebenen p

$$a_p = b_p + 9 \cdot p \cdot c_p.$$

Der Raum $S_4^{new}(\Gamma_0(21))$ ist (laut HECKE) 12-dimensional, $S_2^{new}(\Gamma_0(21))$ nur 5-dimensional. Es ist also auch hier unwahrscheinlich, daß die gefun-

dene Linearkombination lediglich zufällig für die angegebenen Primzahlen verschwindet.

Wie bei $\mathcal{M}_{(-3:1)}$ kann ich die Gleichheit für alle Primzahlen von guter Reduktion allerdings auch hier nicht beweisen. Gäbe es einen Satz wie den Satz von Livné aus [11], der nicht-kubische Mengen verwendet, müssten (da es 4 Primzahlen von schlechter Reduktion gibt) soviele Primzahlen getestet werden, wie eine nicht-kubische Menge in $(\mathbb{Z}/2\mathbb{Z})^5$ Elemente enthalten muß, also höchstens 31, wahrscheinlich aber weniger.

Die Formel aus [4], die wir (unter Annahme der verallgemeinerten Riemannschen Hypothese) benutzen könnten, um die Modularität zu beweisen, liefert hier, daß wir alle Primzahlen kleiner als

$$70 \cdot (2^{800}(\log 2^{800} + \log 2 + \log 3 + \log 5 + \log 7))^2 \approx 2 \cdot 10^{487}$$

testen müssten - das sind natürlich auch wieder viel zu viele.

5.4 Die Quintik $\mathcal{M}_{(-2:1)}$

5.4.1 Singularitäten und Auflösung

Über $\mathbb{C}$ hat $\mathcal{M}_{(-2:1)}$ folgende Singularitäten:

- Die Σ_6-Bahn des Punktes $(1 : 1 : 1 : -1 : -1 : -1)$; das sind 10 gewöhnliche Doppelpunkte (die "Segre nodes").
- Die Gerade $\{(x : x : y : y : z : z), \quad x + y + z = 0\}$ und ihre Σ_6-Bahn; das sind 15 singuläre Geraden. Jeweils 3 dieser Geraden schneiden sich in den 15 Punkten der Σ_6-Bahn von $(1 : 1 : 1 : 1 : -2 : -2)$; weitere Schnittpunkte gibt es nicht.

Genau diese Singularitäten treten in allen Charakteristiken $p \geq 5$ auf; die Primzahlen von schlechter Reduktion sind 2 und 3.

Wir führen den Prozeß der Singularitätenauflösung für $\mathcal{M}_{(-2:1)}$ nicht durch, sondern gehen stattdessen einen anderen Weg: Wir stellen eine Vermutung über die L-Reihe von $\mathcal{M}_{(-2:1)}$ auf und können daraus Rückschlüsse auf die Auflösung der Singularitäten ziehen.

5.4.2 Die L-Reihe

Wir zählen die Punkte auf $\mathcal{M}_{(-2:1)}$ über $\mathbb{F}_p$ und vergleichen die Werte mit den Koeffizienten a_p der modularen Form $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$, der auch

schon bei $\mathcal{M}$ und $\mathcal{M}_{(1:0)}$ aufgetretenen einzigen Newform vom Level 6 und Gewicht 4.

p	$\#\mathcal{M}_{(-2:1)}$	a_p	p	$\#\mathcal{M}_{(-2:1)}$	a_p
5	295	6	71	429895	792
7	815	−16	73	465815	218
11	2695	12	79	584015	−520
13	4175	38	83	672295	−492
17	8695	−126	89	819415	810
19	11495	20	97	1048775	1154
23	19015	168	101	1179895	−618
29	35815	30	103	1247615	128
31	43055	−88	107	1393975	−1476
37	69455	254	109	1467695	1190
41	92455	42	113	1630375	−462
43	105575	−52	127	2287775	−2536
47	135175	−96	131	2497975	2292
53	188695	198	137	2848135	−726
59	255895	−660	139	2969495	380
61	280895	−538	149	3633415	1590
67	364535	884	151	3776495	2432

Soweit angegeben, gilt stets

$$\#\mathcal{M}_{(-2:1)} - 1 - p^3 - 15p^2 + 40p + a_p = 0.$$

Wir können jetzt vermuten, daß es ein glattes Modell von $\mathcal{M}_{(-2:1)}$ gibt, dessen mittlere Kohomologie 2-dimensional ist (denn es taucht nur eine modulare Form vom Gewicht 4 auf), und daß die L-Reihe von $\mathcal{M}_{(-2:1)}$ gleich der L-Reihe der modularen Form $\eta(\tau)^2\eta(2\tau)^2\eta(3\tau)^2\eta(6\tau)^2$ ist. Es ist sicherlich möglich, das auch zu beweisen. Dazu sind die Singularitäten von $\mathcal{M}_{(-2:1)}$ durch Blow-Up aufzulösen, die Eulerzahl zu bestimmen und die Frobenius-Wirkung auf die Kohomologie zu untersuchen. Dann kann wieder der Satz von Livné aus [11] angewendet werden.

Literaturverzeichnis

[1] W. Barth, I. Nieto, *Abelian surfaces of type (1,3) and quartic surfaces with 16 skew lines*, J. of Alg. Geometry Vol. 3, No. 2, pp. 173-222, 1994.

[2] P. Deligne, *Formes modulaires et représentations l-adiques*, Sem. Bourbaki 355 (1968/69), Lect. Notes 349, pp. 139-172, Springer, 1971.

[3] P. Deligne, J. P. Serre, *Formes modulaires de poids 1*, Ann.Sci.Ec.Norm. Sup. 7, pp. 507-530, 1974.

[4] P. Deligne, *Représentations l-adiques*, Astérisque 127, pp. 249-255, Société Mathématique de France, 1985.

[5] A. Dimca, *On the homology and cohomology of complete intersections with isolated singularities*, Compositio Mathematica Vol. 58, pp. 321-339, 1986.

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. math. 73, pp. 349-366, 1983.

[7] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, 4. Auflage, 1960.

[8] R. Hartshorne, *Algebraic Geometry*, Graduate texts in mathematics 52, Springer, 1977.

[9] K. Hulek, J. Spandaw, B. van Geemen, D. van Straten, *The modularity of the Barth-Nieto quintic and its relatives*, preprint, AG/0010049, 2000.

[10] A. W. Knapp, *Elliptic Curves*, Princeton Mathematical Notes 40, Princeton University Press, 1993.

[11] R. Livné, *Cubic exponential sums and Galois representations*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), pp. 247-261, Contemp.Math. 67, Amer.Math.Soc., Providence, R.I., 1987.

[12] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series 33, Princeton University Press, 1980.

[13] K. A. Ribet, *Galois representations and modular forms*, Bull. of the AMS Vol. 32, No. 4, pp. 375-402, 1995.

[14] M. Saito, N. Yui, *The modularity conjecture for rigid Calabi-Yau threefolds over* $\mathbb{Q}$, preprint, AG/0009041, 2000.

[15] C. Segre, *Sulla varietà cubica con dieci punti doppi dello spazio a quattro dimensioni*, Atti Acc., Torino, Vol. 22, pp. 791-801, 1887.

[16] J. P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, W. A. Benjamin, 1968.

[17] W. A. Stein, *Modular forms database*, `http://shimura.math.berkeley.edu/~was/Tables/`, Stand: 1.8.2000.

[18] B. van Geemen, J. Werner, *Nodal quintics in* $\mathbb{P}^4$, Arithmetic of complex manifolds (Erlangen, 1988), pp. 48-59, Lect. Notes 1399, Springer, 1989.

[19] D. van Straten, *A quintic hypersurface in* $\mathbb{P}^4$ *with 130 nodes*, Topology Vol. 32, No. 4, pp. 857-864, 1993.

[20] A. Varchenko, *On semi-continuity of the spectrum and an upperbound for the number of singular points of projective hypersurfaces*, Dokl. Akda. Nauk. USSR 270, pp. 735-739, 1983.

[21] H. A. Verrill, *The L-series of certain rigid Calabi-Yau threefolds*, J. Number Theory 81, pp. 310-334, 2000.

[22] J. Werner, *Kleine Auflösungen spezieller dreidimensionaler Varietäten*, Bonner mathematische Schriften 186, 1987.