Markoffzahlen

Diplomarbeit

von

Volker Senkel

vorgelegt
an der Universität Bielefeld
Fakultät für Mathematik

im November 1997

Inhaltsverzeichnis

1 Markoffzahlen **13**

1.1 Elementare Eigenschaften . . . 13

1.2 Ketten und die Invariante $q(p)$ . . . 18

1.3 Die Erweiterungen $q_{\pm}(p)$ . . . 21

1.4 Anwendungen von $q(p)$ und $q_{\pm}(p)$ . . . 24

2 Markoffzahlen in verschiedenen Kontexten **29**

2.1 Markoff-Formen . . . 29

2.2 Markoffspektrum . . . 36

2.3 Arithmetische Flächen . . . 42

3 Abschätzungen von $q(p)$ **49**

Einleitung

A. Hurwitz [1] beschäftigte sich 1905, meines Wissens als erster, in seiner Arbeit *'Über eine Aufgabe der unbestimmten Analysis'* mit diophantischen Gleichungen der Art :

$$\sum_{i=1}^{n} x_i^2 = a \prod_{i=1}^{n} x_i, \quad a \in \mathbb{N}.$$

Die Lösungen einer speziellen Gleichung bekamen durch die Arbeiten von Markoff über diophantische Approximation eine besondere Bedeutung und werden Thema des vorliegenden Textes sein.

Definition 0.0.1 *Eine Zahl $p \in \mathbb{N}$ zu der Zahlen p_1, $p_2 \in \mathbb{N}$ existieren, so daß (p,p_1,p_2) Lösung der diophantischen Gleichung*

$$x_1^2 + x_2^2 + x_3^2 = 3x_1x_2x_3$$

ist, heißt **Markoffzahl**. *(zur Notation siehe Definition 1.1.1 (S. 13))*

Eine bislang ungeklärte Frage im Zusammenhang mit Markoffzahlen ist die sogenannte Eindeutigkeitsvermutung.

Eindeutigkeitsvermutung : *Ein Markofftripel (p,p_1,p_2) ist bereits durch $p = max(p,p_1,p_2)$ bestimmt, das heißt, es kann kein Markofftripel (p,p_1',p_2') existieren mit $p = max(p,p_1,p_2,p_1',p_2')$.*

Mit diesem Text möchte ich zwei Ziele verfolgen :

1. Den Kenntnisstand bzw. neue Erkenntnisse in Bezug auf die Eindeutigkeitsvermutung vorzustellen, diese zu erweitern und alternative Beweise aufzuzeigen.

2. Die Ergebnisse der oben genannten Arbeiten von Markoff darzustellen.

In Kapitel 1 *(S. 13)* wird zunächst der Aufbau und elementare Eigenschaften sowie die Notation von Markoffzahlen vorgestellt. Die Ergebnisse sind weitestgehend Cassels [5] und Frobenius [4] entnommen. Demnach läßt eine Markoffzahl p die Berechnung gewisser Invarianten $q = q(p)$ zu, die der Kongruenz

$$q^2 \equiv -1 \; mod(p)$$

genügen. Mit dieser Invarianten kann man folgende Aussage bezüglich der Eindeutigkeitsvermutung machen. Existieren zu einer Markoffzahl p zwei Tripel (p, p_1, p_2) und (p, p_1', p_2') mit $p = max(p, p_1, p_2, p_1', p_2')$, so entsprechen diesen Tripeln auch zwei Lösungen der Kongruenz :

$$q^2 \equiv -1 \; mod(p)$$

Umgekehrt läßt sich daraus folgern, daß bei eindeutiger Lösbarkeit der Kongruenz, das Tripel (p, p_1, p_2) durch $p = \max(p,p_1,p_2)$ eindeutig bestimmt ist. Die Aussage findet sich bereits bei Frobenius [4], allerdings ohne Beweis. Schmutz [11] gibt einen einfachen Beweis im Kontext arithmetischer Flächen an. Darüber hinaus werde ich mit den Ergebnissen von Cassels [5] im Kontext indefiniter binärer quadratischer Formen, eine geeignete Transformation angeben, aus der die Aussage folgt. Neben dieser Invarianten möchte ich noch für gerade p, zwei weitere Invarianten q_- und q_+ definieren, die den Kongruenzen :

$$q_-^2 \equiv -1 \; mod(3p-2) \text{ und } q_+^2 \equiv -1 \; mod(3p+2)$$

genügen. Man kann die entsprechende Aussage zeigen und entsprechend folgern, daß bei eindeutiger Lösbarkeit einer der Kongruenzen das Markofftripel (p, p_1, p_2) eindeutig durch p bestimmt ist.
Darüber hinaus haben Schmutz [11] und Baragar [15] unabhängig voneinander Teilbarkeitskriterien für eine Markoffzahl p aufgestellt, aus deren Erfüllung die Richtigkeit der Eindeutigkeitsvermutung für dieses p folgt. Die Kriterien von Schmutz stellen einen Spezialfall von Baragar dar, die er mit Hilfe der Invarianten q beweist. Mit den Invarianten q_+ und q_- kann man nun den Beweis von Schmutz erweitern und damit weitere Teile der Teilbarkeitskriterien von Baragar zeigen.

Kapitel 2 *(S. 29)* stellt die Ergebnisse der Arbeiten von Markoff vor. In diesen beschäftigte er sich mit der Frage, inwieweit eine irrationale Zahl θ durch rationale Brüche $\frac{r}{s}$ approximiert werden kann, das heißt, inwieweit zu einer Zahl $\theta \in \mathbb{R} \backslash \mathbb{Q}$ Zahlen $\kappa \in \mathbb{R}$ existieren, so daß :

$$\left| \theta - \frac{r}{s} \right| < \frac{\kappa}{s^2} \tag{0.1}$$

unendlich viele Lösungen $r, s \in \mathbb{Z}$ besitzt. Ein einfaches Ergebnis aus der Zahlentheorie besagt, daß für $\kappa = 1$ stets unendlich viele $r, s \in \mathbb{Z}$ existieren, die die Ungleichung 0.1 *(S. 6)* lösen (vergleiche : 2.2.1 *(S. 37)*). Man kann zunächst einmal $s > 0$ annehmen. In diesem Fall ist das r bereits bestimmt und die Aussage ist äquivalent zu der Aussage, daß zwischen den Funktionen :

$$s\theta - \frac{1}{s} \quad \text{und} \quad s\theta + \frac{1}{s} \tag{0.2}$$

unendlich viele Gitterpunkte aus $\mathbb{Z} \times \mathbb{Z}$ liegen (vergleiche Abbildung 0.1 *(S. 7)*). Mit Hilfe

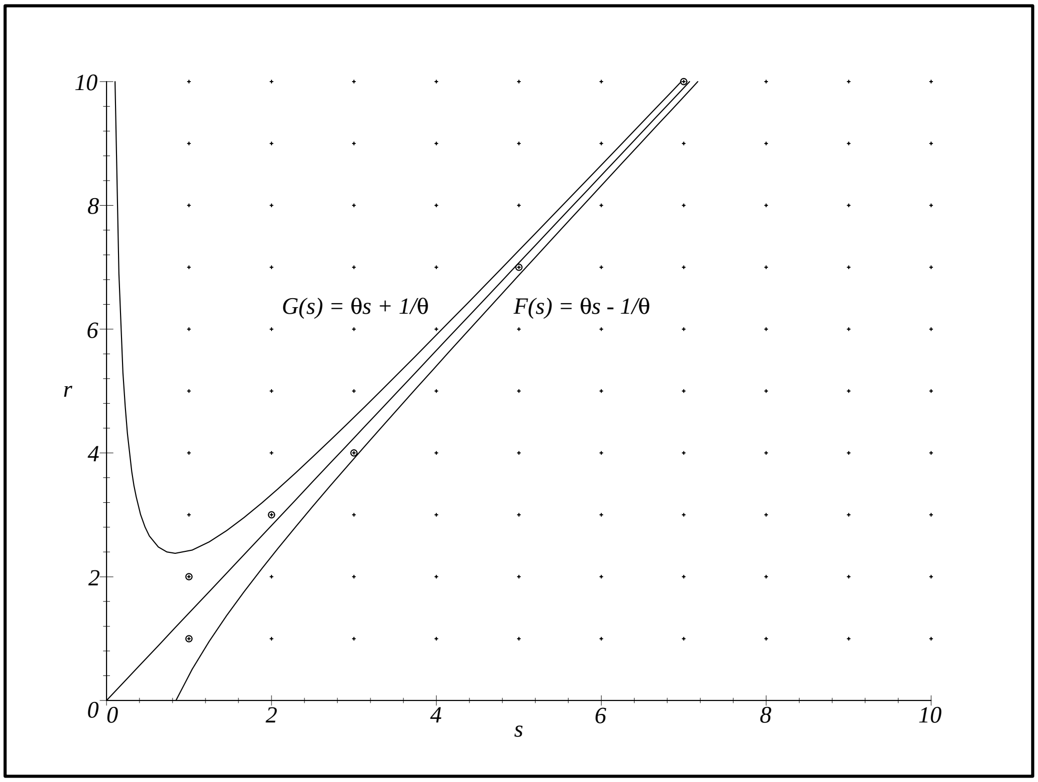

Abbildung 0.1: $\theta s - \frac{1}{s} \leq \theta s \leq \theta s + \frac{1}{s}$

der Theorie der Kettenbrüche läßt sich zeigen, daß $\kappa = 1$ durch $\kappa = 5^{-\frac{1}{2}}$ ersetzt werden kann. Markoff hat gezeigt, daß die Konstante $\kappa = 5^{-\frac{1}{2}}$ zwar nicht für alle $\theta \in \mathbb{R}\backslash\mathbb{Q}$ aber für bestimmte Klassen von $\theta \in \mathbb{R}\backslash\mathbb{Q}$ weiter verbessert werden kann. Dazu definiert man für ein $\theta \in \mathbb{R}\backslash\mathbb{Q}$:

$$\nu(\theta) := inf \left\{ \kappa : \; \left| \theta - \frac{r}{s} \right| \; < \frac{\kappa}{s^2}, \; \textit{für unendlich viele } r, s \in \mathbb{Z} \right\},$$

und

$$\mathfrak{M}_{\mathfrak{s}} := \left\{ \nu(\theta) : \; \nu(\theta) > \frac{1}{3}; \; \theta \in \mathbb{R} \right\}$$

Die Menge $\mathfrak{M}_{\mathfrak{s}}$ heißt Markoffspektrum und wirft die folgenden zwei Fragen auf :

1. Wie ist das Markoffspektrum bzw. sind die Elemente m des Markoffspektrums aufgebaut?

2. Wie sehen die Klassen $\Theta_m := \{\theta \in \mathbb{R}\backslash\mathbb{Q} \ : \ \nu(\theta) = m \ ; \ m \in \mathfrak{M}_{\mathfrak{H}}\}$ für ein festes Element m des Markoffspektrums aus ?

Diese beiden Fragen lassen sich nicht mehr mit elementaren Eigenschaften von Markoffzahlen klären und führen zu indefiniten binäre quadratischen Formen und den Markoff-Formen. Markoff-Formen sind indefinite binäre quadratische Form, mit gewissen ganzzahligen Koeffizienten. Diese Koeffizienten lassen sich mit Hilfe der Invarianten $q = q(p)$ und einer weiteren Invarianten $r = r(p)$ berechnen. Für eine Markoffzahl p hat die entsprechende Markoff-Form f_p folgende Gestalt :

$$f_p(x,y) = px^2 + (3p - 2q)xy - (3q - r)y^2 \ , \quad p \text{ Markoffzahl.}$$

Es wird sich zeigen, daß man mit Hilfe der Wurzel $f_p(\zeta_p, 1) = 0$ einer Markoff-Form, die Menge Θ_m beschreiben kann. Sei :

$$PSL_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - cd = \pm 1; a, b, c, d \in \mathbb{Z} \right\}$$

und

$$S \circ \theta := \frac{a\theta + b}{c\theta + d} \ , \quad S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) \ \ , \ \theta \in \mathbb{R} \ .$$

Dann ist

$$\Theta_{\nu(\zeta_p)} = \{S \circ \zeta_p : S \in PSL_2(\mathbb{Z})\}$$

gerade der Bahnenraum von ζ_p in $\mathbb{R}$. Darüber hinaus kann man mit Hilfe von Markoffzahlen und Markoff-Formen das Markoffspektrum $\mathfrak{M}_{\mathfrak{H}}$ konkret angeben. Sei zunächst f eine indefinite binäre quadratische Form

$$f(xy) = \alpha x^2 + \beta xy + \gamma y^2 \ ; \ \alpha, \beta, \gamma \in \mathbb{R}$$

mit Diskriminante

$$D(f) = \beta^2 - 4\alpha\gamma > 0.$$

Für eine solche Form sei:

$$\mu(f) = inf \ \{ \ |f(m,n)| \ : \ (m,n) \ \in \mathbb{Z} \times \mathbb{Z}\backslash(0,0)\} \ .$$

Dann gilt für eine Markoffzahl p, deren Markoff-Form f_p und den Wurzeln $f_p(\zeta_p, 1) = f_p(\zeta_p', 1) = 0$ der Markoff-Form :

$$\mu(f_p) = p \ \text{ und } \ \sqrt{D(f_p)} = \sqrt{9p^2 - 4}.$$

Mit diesen Werten kann man nun das Markoffspektrum angeben :

$$\frac{\mu(f_p)}{\sqrt{D(f_p)}} = \frac{p}{\sqrt{9p^2-4}} = \nu(\zeta_p) \in \mathfrak{M}_{\mathfrak{5}} \ .$$

Umgekehrt existiert zu jedem Element $m \in \mathfrak{M}_{\mathfrak{5}}$ eine Markoffzahl p mit :

$$m = \frac{p}{\sqrt{9p^2-4}} \ .$$

Damit ist das Markoffspektrum $\mathfrak{M}_{\mathfrak{5}}$ diskret und hat als einzigen Häufungspunkt $\frac{1}{3}$. Weiter gilt :

$$\frac{1}{3} < m < \frac{1}{\sqrt{5}} \quad \text{für alle} \quad m \in \mathfrak{M}_{\mathfrak{5}}.$$

Insgesamt stellt sich natürlich die Frage, was indefinite binäre quadratische Formen mit Lösungen der Ungleichung :

$$|s\theta - r| < \frac{\kappa}{s}$$

zu tun haben. Diese Frage ist nicht einfach zu beantworten und wird im Kapitel 2 *(S. 29)* genauer behandelt. Allerdings ist es möglich geometrisch eine Analogie feststellen. Dazu betrachte man zunächst die Menge $N_p = \{(x,y) \in \mathbb{R}^2 \ : \ f_p(x,y) = 0\}$. Offensichtlich kann man diese Menge als Vereinigung der Mengen

$$N_p = \{(s\zeta_p, s) \ : \ s \in \mathbb{R}, f_p(\zeta_p, 1) = 0\} \cup \{(s\zeta_p', s) \ : \ s \in \mathbb{R}, f_p(\zeta_p', 1) = 0\}$$

darstellen. Betrachtet man nun den Wert $\mu(f_p)$, also

$$\mu(f_p) = inf\ \{\ |f_p(m,n)| \ : \ (m,n) \ \in \mathbb{Z} \times \mathbb{Z} \backslash (0,0)\}\ ,$$

so liegt dessen Urbild (m,n), soweit es denn explizit existiert, sicherlich in der 'Nähe' der Menge N_p. Für eine Markoff-Form kann man das Urbild des Infimums angeben. Es gilt :

$$\mu(f_p) = f_p(q,p) = p.$$

Betrachtet man nun die 'Höhenlinien' H_p, also :

$$H_p = \left\{(x,y) \in \mathbb{R}^2 \ : \ |f_p(x,y)| = p\right\} \ ,$$

so gilt $(q,p) \in H_p$. Existiert ein weiteres Tupel $(r',s') \in \mathbb{Z} \times \mathbb{Z}\backslash(0,0)$ innerhalb der durch H_p berandeten Menge, so gilt aufgrund der Stetigkeit von f_p :

$$|f_p(r',s')| < |f_p(q,p)| = inf\ \{\ |f_p(m,n)| \ : \ (m,n) \ \in \mathbb{Z} \times \mathbb{Z}\backslash(0,0)\}$$

(siehe Abbildung 0.2 *(S. 10)*). Ist andererseits $\mu(f_p)$ ein 'echtes' Infimum, so existiert eine Folge $(r_n, s_n)_{n\in\mathbb{N}} \subset \mathbb{Z} \times \mathbb{Z}\backslash(0,0)$ mit :

$$|f_p(r_n, s_n)| \to |f_p(q,p)|.$$

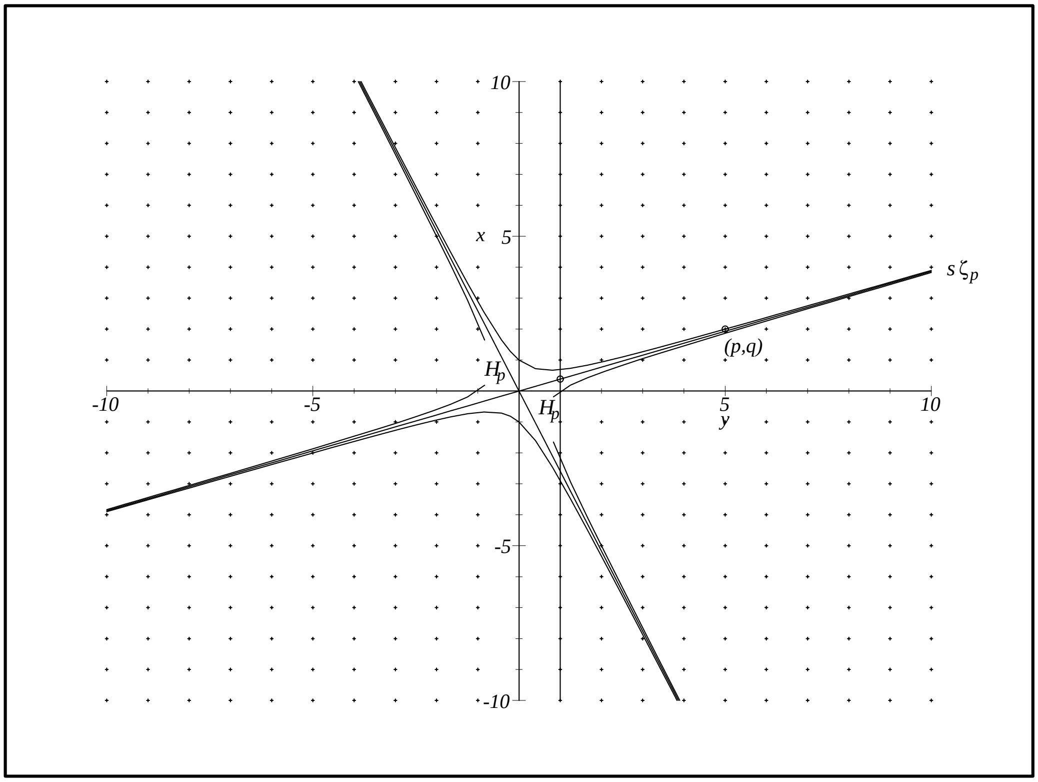

Abbildung 0.2: $f_p(x,y) = 0$ mit $f_p(q,p) = \mu(f_p) = p$ und 'Höhenlinien' H_p

Damit liegen zu jedem $\varepsilon > 0$ unendlich viele Tupel $(r_m, s_m)_{m\in\mathbb{N}} \subset (r_n, s_n)_{n\in\mathbb{N}}$ innerhalb der durch $H_{p+\varepsilon}$ berandeten Menge. Vergleicht man nun die Abbildung 0.2 *(S. 10)* mit der Abbildung 0.1 *(S. 7)* , so wird die Analogie sichtbar.

Die Ergebnisse der Arbeiten von Markoff sind die beiden Theoreme *The Markoff chain for forms* 2.1.4 *(S. 31)* und *The Markoff chain for approximations* 2.2.9 *(S. 42)* . Die Aussagen sind umfangreicher, als meine bisherigen Ausführungen und werden im Kapitel 2 *(S. 29)* ausführlich dargestellt. Die Beweise von Markoff basieren im wesentlichen auf der Theorie der Kettenbrüche. 1913 gelang es Frobenius [4], der die umfangreichste Arbeit über Markoffzahlen geschrieben hat, Teile des Satzes mittels indefiniter binärer quadratischer Formen zu beweisen, die Cassels [5] 1959 vervollständigte.

Neben den Zusammenhängen zur diophantischen Approximation und den indefiniten binären quadratischen Formen bzw. Minimalformen (siehe : Remak [6]) existiert ein Zusammenhang zur hyperbolischen Geometrie (siehe : Cohn [7, 8] 1955, Lehner/Sheingorn [9] 1984, Haas [10] 1986) und speziell zu den Längenspektren arithmetischer Flächen (siehe Schmutz

[11]).

Kapitel 3 *(S. 49)* beschäftigt sich noch einmal mit der Eindeutigkeitsvermutung von Markoffzahlen und nutzt dabei die Ergebnisse aus Kapitel 2 *(S. 29)* aus. Dabei wird die Frage gestellt, welche Werte die Invariante $q = q(p)$ annehmen kann. Schmutz [11] gibt eine untere Schranke $\zeta(p)$ an, bei der aus der eindeutigen Lösbarkeit von

$$q^2 \equiv -1 \; mod(p) \quad , \quad \text{für} \quad \zeta(p) \; \leq \; q,$$

die Richtigkeit der Vermutung für p folgt. Mit den Ergebnissen von Frobenius [4] kann man zum einen eine obere Schranke $\xi(p)$ angeben und zum anderen nachweisen, daß beide nicht verbesserbar sind.

Für Markoffzahlen läßt sich eine Fülle von Invarianten und Konstanten definieren, die in einer ebensolchen Fülle von, meist elementaren, Gleichungen und Kongruenzen miteinander verbunden sind, was schnell dazu führen kann, daß man, schon bei einfachen Rechnungen, den Überblick verliert. Deshalb habe ich mich bemüht einerseits die Definitionen auf das Nötigste zu beschränken und andererseits die jeweiligen Rechnungen ausführlich darzustellen.

Bemerkung 0.0.2 *Leider gibt es bei Markoffzahlen und deren Invarianten und Konstanten keine eindeutige Notation. So kann man zum Beispiel folgende Bezeichnungen für ein Markofftripel finden :*

$$(x, y, z), \;\; (p, q, r), \;\; (m, m_1, m_2), \;\; (p, p_1, p_2).$$

Ich habe im vorliegenden Text die Notation (p, p_1, p_2) *für ein Markofftripel von Frobenius [4] und Remak [6] übernommen. Leider kann man dabei vermuten, daß es sich bei einer Markoffzahl* p *um eine Primzahl handelt. Dies ist im allgemeinen nicht so. Primzahlen werden in diesem Text mit* $\tilde{p}$ *bezeichnet.*

Einen herzlichen Dank möchte ich Herrn Prof. Dr. Helling für die interessante Themenstellung und die hilfreiche Betreuung meiner Diplomarbeit aussprechen.

Kapitel 1

Markoffzahlen

1.1 Elementare Eigenschaften

Definition 1.1.1 *Eine Zahl $p \in \mathbb{N}$ † zu der Zahlen $p_1, p_2 \in \mathbb{N}$ existieren, so daß (p,p_1,p_2) Lösung der diophantischen Gleichung*

$$x_1^2 + x_2^2 + x_3^2 = 3x_1x_2x_3 \tag{1.1}$$

ist, heißt **Markoffzahl**. *(Markoffzahlen : Siehe Abbildung 1.1 (S. 16))*

Mit p sind natürlich auch p_1 und p_2 Markoffzahlen. Innerhalb eines Markofftripels (p,p_1,p_2) ist p nicht gegenüber p_1 oder p_2 ausgezeichnet. Im weiteren wird jedoch p die zu betrachtende Markoffzahl sein, an die meist eine Bedingung wie zum Beispiel $p = max(p, p_1, p_2)$, oder p ist Erzeugende einer Markoffkette (vgl. Abschnitt 1.2 *(S. 18)*). Die mögliche Bedingung wird im jeweiligen Fall angegeben. Eine Markoffzahl p ist nicht notwendig eine Primzahl.

Definition 1.1.2 *Eine* **singuläre Lösung** *der diophantischen Gleichung (1.1 (S. 13)) ist ein Markofftripel, bei dem zwei Markoffzahlen übereinstimmen.*

† Für die folgenden Ausführungen sind nur Lösungen $p, p_1, p_2 \in \mathbb{N}$ relevant, obwohl natürlich auch eine allgemeinere Betrachtung für $p, p_1, p_2 \in \mathbb{Z}$ möglich wäre. Eine solche, allgemeinere Betrachtung findet sich beispielsweise bei Cassels [5].

Singuläre Lösungen :
Sei also:

$$\begin{array}{rcl} p_1 & = & p_2 \\ \Rightarrow \quad p^2+p_1^2+p_2^2 & = & 3pp_1p_2 \\ \Leftrightarrow \quad p^2+2p_1^2 & = & 3pp_1^2 \\ \Rightarrow \quad p_1 \ \text{teilt}\ p & & \\ \text{Sei } d \in \mathbb{N} \ \text{mit}\ p & = & dp_1 \end{array}$$

$$\begin{array}{rcl} \Rightarrow \quad d^2p_1^2+2p_1^2 & = & 3dp_1^3 \\ \Leftrightarrow \quad d^2+2 & = & 3dp_1 \\ \Leftrightarrow \quad \frac{2}{d} & = & \underbrace{3p_1-d}_{\in\mathbb{Z}} \\ \Rightarrow \quad d \text{ teilt } 2 & & \\ \Rightarrow \quad d=1 & \text{oder} & d=2. \end{array}$$

Die einzigen singulären Lösungen sind (1,1,1), und (1,1,2).

Benachbarte Lösungen :
Sei (p,p_1,p_2) ein nicht-singuläres Markofftripel und

$$\Phi_p(x) = x^2 - x(3p_1p_2) + (p_1^2+p_2^2). \tag{1.2}$$

Offensichtlich ist p Wurzel von Φ_p und für die Diskriminante $D(\Phi_p)$ gilt :

$$D(\Phi_p) = \left(\frac{-3p_1p_2}{2}\right)^2 - (p_1^2+p_2^2).$$

Sei nun $p_1 > p_2$

$$\Rightarrow \quad \frac{D(\Phi_p)}{p_1^2} = \underbrace{\frac{9}{4}p_2^2}_{>2} - \underbrace{\left(\frac{p_2^2}{p_1^2}+1\right)}_{<2}$$

$\Rightarrow D(\Phi_p) > 0$ und Φ_p besitzt eine zweite Wurzel p'.

$$\begin{array}{rcl} \Rightarrow \quad \Phi_p(x) & = & (x-p)(x-p') \\ & = & x^2 - x(p+p') + pp'. \end{array}$$

Ein Koeffizientenvergleich mit (1.2 *(S. 14)*) ergibt :

$$\begin{array}{ccc} p+p' = 3p_1p_2 & & pp' = p_1^2+p_2^2 \\ \Rightarrow \quad p' \text{ ist ganz} & \text{und} & \Rightarrow p' > 0 \\ & \Rightarrow \quad p' \text{ ist Markoffzahl.} & \end{array}$$

Bemerkung 1.1.3 *Aus jedem Tripel (p,p_1,p_2), das keine singuläre Lösung ist, erhält man drei neue Tripel :*

$$\begin{array}{c} (p',p_1,p_2), \qquad (p,p_1',p_2), \qquad (p,p_1,p_2') \\ \textit{mit } p' = 3p_1p_2 - p, \quad p_1' = 3pp_2 - p_1, \quad p_2' = 3pp_1 - p_2. \end{array} \tag{1.3}$$

Sei $p_1 = max(p_1, p_2)$. Es ist :

$$\begin{aligned} \Phi_p(x) &= x^2 - x(3p_1p_2) + (p_1^2 + p_2^2) \\ &= (x-p)(x-p'). \end{aligned}$$

Entsprechend gilt :

$$\begin{aligned} (p_1 - p)(p_1 - p') &= \Phi_p(p_1) \\ &= p_1^2 - p_1(3p_1p_2) + (p_1^2 + p_2^2) \\ &< 3p_1^2 - 3p_1^2p_2 \\ &= 3p_1^2 \underbrace{(1-p_2)}_{\leq 0} \end{aligned} \tag{1.4}$$

$$\Rightarrow \Phi_p(p_1) < 0.$$

Aus (1.4 *(S. 15)*) folgt :

$$\begin{aligned} p &> max(p_1, p_2) > p' \\ \text{oder} \quad p' &> max(p_1, p_2) > p. \end{aligned}$$

Sei nun $p = max(p, p_1, p_2)$. Mit entsprechenden Überlegungen, wie oben, erhält man :

$$p_2' > p \;, \quad p_1' > p, \quad max(p_1, p_2) > p'$$

Bemerkung 1.1.4 *Jedes Tripel besitzt somit zwei Nachbartripel; eines mit einem größeren maximalen Element und eines mit einem kleineren maximalen Element :*

$$\begin{array}{c} (p', p_1, p_2) \\ \uparrow \\ (p, p_1, p_2) \\ \swarrow \searrow \\ (p, p_1', p_2) \quad (p, p_1, p_2'). \end{array}$$

Bemerkung 1.1.5 *Beginnt man mit einem beliebigen Tripel und berechnet jeweils das benachbarte Tripel mit dem kleineren maximalen Element, so muß der Prozeß irgendwann stoppen, und dies kann nur bei einem singulären Tripel sein.*
Andererseits kann man, ausgehend von einem singulären Tripel in umgekehrter Richtung, zu jedem beliebigen Tripel gelangen.

Lemma 1.1.6 *Alle Lösungen können in einem Baum, ausgehend von (1,1,1), berechnet werden und es gilt :*

$$ggT(p, p_1) = ggT(p, p_2) = ggT(p_1, p_2) = 1.$$

Beweis :

Der erste Teil des Lemmas ergibt sich aus der Bemerkung 1.1.5 *(S. 15)* .

Angenommen : $ggT(p, p_1) = d \neq 1$

$$\begin{aligned} p^2 + p_1^2 + p_2^2 = 3pp_1p_2 \quad &\Rightarrow \quad d \;\text{ teilt } p_2 \\ p' = 3p_1p_2 - p \qquad &\Rightarrow \quad d \;\text{ teilt } p'. \end{aligned}$$

Das heißt, d teilt den ggT von allen benachbarten Lösungen und damit auch von deren benachbarten, u.s.w.

$$\Rightarrow d \text{ teilt } ggT(1, 1, 1).$$

□

Abbildung 1.1 *(S. 16)* beschreibt den Aufbau von Markoffzahlen. Für die nächsten Ab-

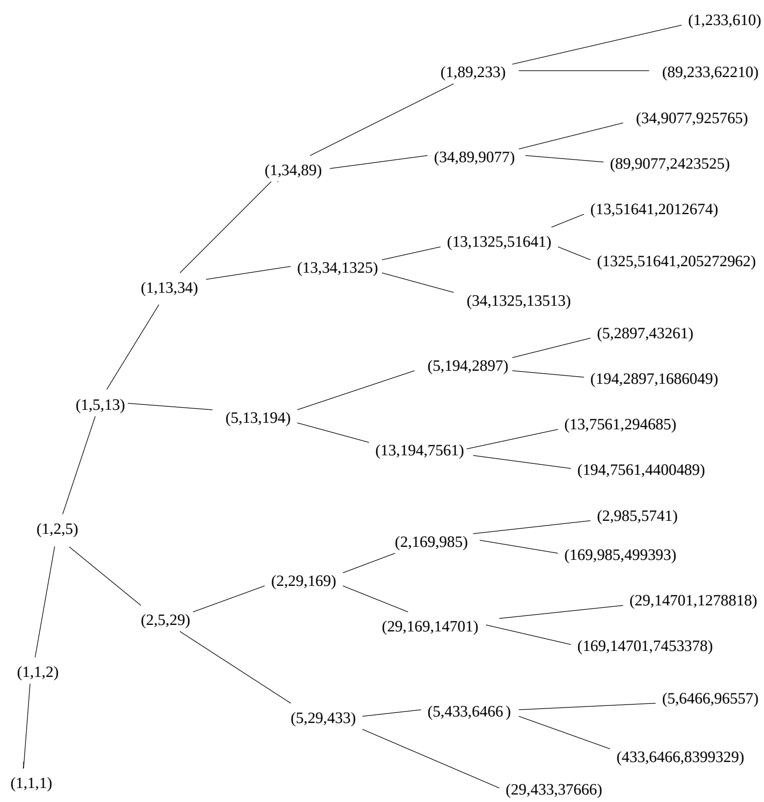

Abbildung 1.1: Markofftripel

schnitte sind neben der Markoffzahl p auch die Zahlen $(3p \pm 2)$ von Interesse. Der Rest dieses Abschnittes beschäftigt sich mit elementaren Teilbarkeitskriterien von p und $(3p \pm 2)$.

Bemerkung 1.1.7

$$p \not\equiv 0 \; mod(4)$$

Beweis :

$$\text{Annahme}: \quad p \equiv 0 \; mod(4) \quad \Rightarrow \quad p_1, p_2 \text{ sind ungerade}$$
$$\Rightarrow \quad p_1^2, p_2^2 \text{ sind entweder}:$$

$$\begin{aligned} \Rightarrow \quad (4n+1)^2 &= 16n^2 + 8n + 1 &= 8n^* + 1 \\ \text{oder} & & \\ (4n'+3)^2 &= 16n'^2 + 24n' + 9 &= 8n'^* + 1 \end{aligned}$$

für geeignete n, n', n^*, n'^*

$$\begin{aligned} \Rightarrow 0 \equiv 3pp_1p_2 &= p^2 + p_1^2 + p_2^2 \\ &\equiv 0 + 1 + 1 \quad mod(4). \end{aligned}$$

Bemerkung 1.1.8 *Ist p eine Markoffzahl, so ist jeder ungerade Primfaktor von p,(3p - 2), (3p + 2) von der Form (4n + 1).*

Beweis :

1.) Für p wegen :

$$\begin{aligned} p^2 + p_1^2 + p_3^2 &= 3pp_1p_2 \\ \Rightarrow \quad p(3p_1p_2 - p) &= p_1^2 + p_2^2. \end{aligned}$$

2.) Für $(3p \pm 2)$ wegen :

$$\begin{aligned} p_1p_2(3p \pm 2) &= 3pp_1p_2 \pm 2p_1p_2 \\ &= p^2 + p_1^2 + p_2^2 \pm 2p_1p_2 \\ &= p^2 + (p_1 \pm p_2)^2. \end{aligned}$$

□

Andererseits besitzen diese Eigenschaften auch Zahlen wie 37 und 61, die keine Markoffzahlen sind.

Bemerkung 1.1.9

$$\begin{array}{lll} a.) & (3p \pm 2) \not\equiv 2 \; mod(4), & (folgt\ direkt\ aus\ Bem.\ 1.1.7\ (S.\ 16)\ ) \\ b.) & (3p \pm 2) \neq 2\tilde{p}\ , & \tilde{p}\ Primzahl, \tilde{p} \neq 2. \end{array}$$

Beweis : b.) Wegen Bemerkung 1.1.8 *(S. 17)* gilt:

$$\begin{array}{rcll} \tilde{p} &=& (4n+1) & , \; n \in \mathbb{N} \\ \Rightarrow \quad 2\tilde{p} &\equiv& 2 \; mod(4) & \\ \Rightarrow \quad (3p \pm 2) &\equiv& 2 \; mod(4) & \text{Widerspruch zu Bemerkung 1.1.9 } (S.\ 17) \text{ a.).} \end{array}$$

1.2 Ketten und die Invariante $q(p)$

Definition 1.2.1 *Sei* (p,p_1,p_2) *ein Markofftripel mit* $p = max(p,p_1,p_2)$. *Berechnet man ausgehend von* (p,p_1,p_2) *fortwährend Tripel mit größeren maximalen Elementen, mit der Beschränkung, p festzuhalten, so nennt man diese Lösungen* $\{(p,p_i,p_{i+1})_{i\in\mathbb{N}}\}$ *eine* **Kette** *bezüglich p.*

Bemerkung 1.2.2 *Sei nun* (p,p_1,p_2) *ein Markofftripel mit* $p = max(p,p_1,p_2)$.

a) *Je zwei der Markoffzahlen sind teilerfremd.*

Somit gilt :

$$p^2 + p_1^2 + p_2^2 = 3pp_1p_2$$
$$\Rightarrow p_1^2 + p_2^2 \equiv 0 \; mod(p)$$

b) $$\Rightarrow \tfrac{p_1}{p_2} \equiv -\tfrac{p_2}{p_1}$$

Definition 1.2.3 *Sei* (p,p_1,p_2) *nicht-singuläres Markofftripel, mit* $p = max(p,p_1,p_2)$. *Man wähle* $\varepsilon = \pm 1$ *, so daß für* q,q_1,q_2 *mit*

$$\begin{array}{lllll} \varepsilon q & \equiv & \frac{p_1}{p_2} & \equiv -\frac{p_2}{p_1} & mod(p) \\ \varepsilon q_1 & \equiv & \frac{p_2}{p} & \equiv -\frac{p}{p_2} & mod(p_1) \\ \varepsilon q_2 & \equiv & \frac{p}{p_1} & \equiv -\frac{p_1}{p} & mod(p_2) \end{array}$$

$$0 < q < \frac{p}{2} \quad und \quad 0 < q_i < \frac{p_i}{2} \; , \; i = 1,2 \; gilt. \tag{1.5}$$

Man kann, für ein q, die Reihenfolge von p_1 und p_2 bzw. das Vorzeichen ε ändern und die Kongruenz in Definition 1.2.3 *(S. 18)* bleibt trotzdem richtig. Entsprechend kann man nun das Vorzeichen bzw. die Reihenfolge so wählen, daß $\pm q$ der absolut kleinste Rest von :

$$\frac{p_1}{p_2} \text{ oder } \frac{p_2}{p_1} \; mod(p)$$

ist. Geht man, bei festgehaltenem p, zu einer benachbarten Lösung (p,p_3,p_2) über :

$$\begin{array}{llcl} \text{lt. (1.3 } (S.\ 14) \text{)} & p_3 & = & 3pp_2 - p_1 \\ \Rightarrow & \frac{p_3}{p_2} & = & \frac{3pp_2}{p_2} - \frac{p_1}{p_2} \\ & & = & 3p - \frac{p_1}{p_2} \\ & & \equiv & -\frac{p_1}{p_2} \; mod(p) \; , \end{array}$$

so bleibt q bis auf das Vorzeichen unverändert. Wiederholt man dies beliebig oft und kommt man zu der Lösung (p,p_i,p_{i+1}), so gilt entsprechend :

$$\frac{p_i}{p_{i+1}} \equiv \pm q \; mod(p).$$

Damit ist q Invariante der Kette $\{(p, p_i, p_{i+1})_{i\in\mathbb{N}}\}$. Entsprechend sind auch q_1 und q_2 Invarianten der Ketten $\{(p_1, p_{1_j}, p_{1_{j+1}})_{j\in\mathbb{N}}\}$ bzw. $\{(p_2, p_{2_k}, p_{2_{k+1}})_{k\in\mathbb{N}}\}$. Die Invariante q ist gegenüber q_1 und q_2 nur dadurch ausgezeichnet, daß $p = max(p, p_1, p_2)$ gilt.
Es ist :

$$p_1^2(1+q^2) \equiv p_1^2 + p_2^2 \equiv 0 \ mod(p)$$

$$\Rightarrow q^2 \equiv -1 \ mod(p).$$

Insgesamt gilt damit :

Bemerkung 1.2.4

$$q^2 \equiv -1 \ mod(p) \ , \quad q_1^2 \equiv -1 \ mod(p_1) \ , \quad q_2^2 \equiv -1 \ mod(p_2).$$

Mit diesen Kongruenzen kann man ein weiteres Zahlentripel (r,r_1,r_2) definieren.

Definition 1.2.5 *Für ein Markofftripel (p,p_1,p_2) mit den Invarianten (q,q_1,q_2) sei das Tripel (r,r_1,r_2) definiert als :*

$$pr - q^2 = 1 \ , \ p_1r_1 - q_1^2 = 1 \ , \ p_2r_2 - q_2^2 = 1.$$

Bemerkung 1.2.6 *Die Definition der Invarianten q besitzt die Einschränkung, daß (p,p_1,p_2) nicht-singuläres Markofftripel ist. Allerdings ist es sinnvoll auch für die singulären Tripel $(1,1,1)$, und $(2,1,1)$ die Werte q und r zu definieren, um später auch Markoff-Formen für $p = 1$ und $p = 2$ definieren zu können. Bei Frobenius [4] finden sich hierfür folgende Werte :*

$$\begin{aligned} p = 1 \ &: \ q = 0, \ r = 1, \\ p = 2 \ &: \ q = 1, \ r = 1. \end{aligned}$$

Leider erhält man mit diesen Werten keine sinnvollen Markoff-Formen.

Bezüglich der Tripel (p,p_1,p_2), (q,q_1,q_2) und (r,r_1,r_2) gelten unter anderem folgende Relationen .

Lemma 1.2.7 *Für ein nicht-singuläres Tripel (p,p_1,p_2), mit $p = max(p, p_1, p_2)$ gilt :*

$$pq_2 - p_2q = p_1 \tag{1.6}$$

$$p_1q - pq_1 = p_2 \tag{1.7}$$

$$p_1q_2 - p_2q_1 = p' = 3p_1p_2 - p. \tag{1.8}$$

Da sich die Beweise ähneln, möchte ich nur die erste Gleichung zeigen.
Beweis :
Es gilt :

$$\begin{array}{rrcl}
 & pq_2 - p_2q & \equiv & pq_2 \\
 & & \equiv & p_1 \; mod(p_2) \\
\text{nach Def. } 1.2.3 \; (S. \; 18) \text{ ist :} & \varepsilon q_2 & \equiv & -\frac{p_1}{p} \; mod(p_2) \\
\text{und :} & pq_2 - p_2q & \equiv & -p_2q \\
 & & \equiv & p_1 \; mod(p) \\
\text{wg. } ggT(p, p_2) = 1 \text{ :} & pq_2 - p_2q & \equiv & p_1 \; mod(p_2p) \\
\text{aber :} & pq_2 - p_2q - p_1 & < & pq_2 \\
 & & \leq & pp_2 \\
\text{aus } (\; 1.5 \; (S. \; 18) \;) \text{ folgt :} & pq_2 - p_2q - p_1 & \geq & p - p_2(p-1) - p_1 \\
 & & = & \underbrace{(p + p_2 - p_1)}_{>0} - pp_2 \\
\Rightarrow & & > & -pp_2
\end{array}$$

$$\Rightarrow pq_2 - p_2q = p_1.$$

□

Mit der Definition von q hat man eine Invariante von Ketten gefunden, die eine zentrale Stellung in der Theorie der Markoffzahlen einnimmt. Die Invariante q wird für alle wesentlichen Konstruktionen in Kapitel 2 *(S. 29)* , bei Markoff-Formen, beim Markoffspektrum und im Kontext arithmetischer Flächen, benötigt.
Darüber hinaus läßt sich mit Hilfe von q zwar nicht die Eindeutigkeitsvermutung bestätigen, aber man kann mit $q = q(p)$ Kriterien für eine Markoffzahl p angeben, aus deren Erfüllung die Richtigkeit der Vermutung für eben jenes p folgt. Ein solches Kriterium hat Schmutz [11] bewiesen.

Theorem 1.2.8 *Würden mehrere Ketten bezüglich p existieren, so würden ihnen auch mehrere Lösungen q der Kongruenz :*

$$q^2 \equiv -1 \; mod(p) \tag{1.9}$$

entsprechen.

Das Theorem läßt sich sehr leicht, allerdings nicht mit den bisherigen Mitteln, beweisen. Im Abschnitt 2.1 *(S. 29)* , im Kontext indefiniter binärer quadratischer Formen, werde ich zeigen, daß sich eine geeignete Transformation angeben läßt, aus der die Aussagen direkt folgen.

Kommen wir nun zur Aussage des Theorems. Wenn ein Markofftripel (p,p_1,p_2) nicht eindeutig durch $p = max(p,p_1,p_2)$ bestimmt ist, also ein weiteres Tripel (p,p'_1,p'_2) mit $p = max(p,p'_1,p'_2)$ existiert, würden auch zwei Ketten $\{(p,p_i,p_{i+1})_{i\in\mathbb{N}}\}$ und $\{(p,p'_i,p'_{i+1})_{i\in\mathbb{N}}\}$ bezüglich dieser Markoffzahl p existieren. Theorem 1.2.8 *(S. 20)* besagt, daß in solch einem Fall die beiden Ketten unterschiedliche Invarianten q und q' definieren.
Umgekehrt folgt aus der eindeutigen Lösbarkeit der Kongruenz $q^2 \equiv -1\ mod(p)$, für ein p, die Richtigkeit der Eindeutigkeitsvermutung für dieses p. In Kapitel 3 *(S. 49)* wird gezeigt, daß für eine Markoffzahl p nur ein bestimmter Bereich von Lösungen q der Kongruenz $q^2 \equiv -1\ mod(p)$ relevant ist (Theorem 3.0.1 *(S. 49)*) , und zwar :

$$0 \leq \zeta(p) \leq q \leq \xi(p) \leq \frac{p}{2}.$$

Das heißt, man kann die Aussage von Theorem 1.2.8 *(S. 20)* mit Hilfe des Theorems 3.0.1 *(S. 49)* der Art erweitern, daß aus der eindeutigen Lösbarkeit der Kongruenz $q^2 \equiv -1\ mod(p)$, für $\zeta(p) \leq q \leq \xi(p)$ folgt, daß das Tripel (p,p_1,p_2) eindeutig durch $p = max(p,p_1,p_2)$ bestimmt ist.
Alle mir sonst bekannten Kriterien, aus denen die Richtigkeit der Eindeutigkeitsvermutung für ein p folgt, setzen einen konkreten Aufbau von p bzw. $(3p \pm 2)$ voraus (vgl. Theorem 1.4.4 *(S. 25)*).
Dies sollte Anlaß genug sein, nach weiteren Invarianten $q_\pm$ zu suchen, die ähnliche Eigenschaften wie die Invariante q besitzen, und für die eine ähnliche Aussage wie Theorem 1.2.8 *(S. 20)* möglich ist.

1.3 Die Erweiterungen $q_\pm(p)$

Bei der Konstruktion der Erweiterungen $q_\pm(p)$ wollen wir uns an der Konstrukion der Invarianten q orientieren. Dessen Ausgangspunkt ist die Bemerkung 1.2.2 *(S. 18)*. Demnach benötigt man zunächst eine Gleichung, die der Gleichung

$$p^2 + p_1^2 + p_2^2 \quad = \quad 3pp_1p_2$$

ähnelt. Bei Bemerkung 1.1.8 *(S. 17)* 2.) findet man folgende Gleichung :

$$p^2 + (p_1 \pm p_2)^2 = p_1p_2(3p \pm 2). \tag{1.10}$$

In Bemerkung 1.2.2 *(S. 18)* wird als nächstes sichergestellt, daß je zwei der Zahlen p, p_1 und p_2 teilerfremd sind. Damit erhält man :

$$\tfrac{p_1}{p_2} \quad \equiv \quad -\tfrac{p_2}{p_1}\ mod(p).$$

Also wäre nun zu zeigen, daß je zwei der Zahlen $p, (p_1 \pm p_2)$ und $(3p \pm 2)$ teilerfremd sind. Dies ist allerdings nicht ohne weiteres richtig.

Bemerkung 1.3.1 *Für ein Markofftripel (p,p_1,p_2), mit $p = max(p,p_1,p_2)$, gilt :*

$$\begin{array}{rcll} ggT(p,(p_1 \pm p_2)) & = & 1 \textit{ oder } 2 & , \\ ggT(p,(3p \pm 2)) & = & 1 \textit{ oder } 2 & \textit{und} \\ ggT((p_1 \pm p_2),(3p \pm 2)) & = & 1 \textit{ oder } 2. & \end{array}$$

Beweis :

Sei im weiteren $p_1 > p_2$ und damit $(p_1 \pm p_2) > 0$. Angenommen, es ist : $ggT(p, p_1 \pm p_2) = a > 1, a \in \mathbb{N}$. Somit gilt, mit geeigneten $a_p, a_{p_1,p_2} \in \mathbb{N}$:

$$\begin{array}{lc} \Rightarrow & p = aa_p \text{ und } p_1 \pm p_2 = aa_{p_1,p_2} \\ & \text{Zusammen mit Gleichung (1.10 } (S.\ 21) \text{) erhält man :} \\ \Rightarrow & p_1p_2(3p \pm 2) = a^2(a_p^2 \pm a_{p_1,p_2}^2) \\ & \text{Wegen } ggT(p,p_1) = ggT(p,p_2) = 1 \text{ gilt :} \\ & a^2 \text{ teilt } (3p \pm 2) \\ \Rightarrow & ggT(p,(3p \pm 2)) = a \\ & \text{Mit geeigneten } a_{(3p\pm 2)}, a_p \in \mathbb{N} \text{ ist :} \\ & p = aa_p \text{ und } (3p \pm 2) = a^2 a_{(3p\pm 2)} \\ \Rightarrow & 3p \pm 2 = 3aa_p \pm 2 = a^2 a_{(3p\pm 2)} \\ \Rightarrow & \frac{\pm 2}{a} = \underbrace{aa_{(3p\pm 2)} - 3a_p}_{\in \mathbb{N}} \\ \Rightarrow & a = 1 \text{ oder } 2. \end{array}$$

Damit hat man auch gezeigt $ggT(p,(3p \pm 2)) = 1$ oder 2. Mit denselben Überlegungen folgt: $ggT(p_1 \pm p_2, (3p \pm 2)) = 1$ oder 2.

Bemerkung 1.3.2 *Für jedes $q_\pm = q_\pm(p)$ sei p und damit auch $(3p \pm 2)$ als ungerade angenommen.*

Mit dieser Annahme sind je zwei der Zahlen $p, (p_1 \pm p_2)$ und $(3p \pm 2)$ teilerfremd, und man erhält (vgl. Bem. 1.2.2 *(S. 18)* b)) :

$$\begin{array}{rrcl} & p^2 + (p_1 \pm p_2)^2 & = & p_1p_2(3p \pm 2) \\ \Rightarrow & p^2 + (p_1 \pm p_2)^2 & \equiv & 0 \; mod(3p \pm 2) \\ \Rightarrow & \frac{p}{p_1 \pm p_2} & \equiv & -\frac{p_1 \pm p_2}{p} \; mod(3p \pm 2). \end{array}$$

Jetzt kann man sich entsprechend zu dem obigen q, zwei $q_\pm$ definieren.

Definition 1.3.3 *Sei (p,p_1,p_2) ein Markofftripel, mit $p = max(p,p_1,p_2)$ und p ungerade. Man wähle $\varepsilon = \pm 1$, so daß für $q_\pm$ mit :*

$$q_\pm := \varepsilon \frac{p}{p_1 \pm p_2} \; mod(3p \pm 2)$$

$$0 < q_\pm < \frac{(3p \pm 2)}{2} \; gilt.$$

Für die beiden Erweiterungen $q_\pm$ gilt wieder :

$$\begin{array}{rrcl} & (p_1 \pm p_2)^2(1+q_\pm^2) & = & (p_1 \pm p_2)^2 + p^2 \\ & & = & p_1 p_2 (3p \pm 2) \\ & & \equiv & 0 \;\; mod(3p \pm 2) \\ \Rightarrow & q_\pm^2 & \equiv & -1 \; mod(3p \pm 2). \end{array}$$

Geht man jedoch bei festgehaltenem p zu einer benachbarten Lösung (p, p_3, p_2) mit $p_3 = 3pp_2 - p_1$ über, so kann man leicht nachrechnen, daß die definierten $q_\pm(p)$ im Normalfall keine Invarianten der Kette $\{(p, p_i, p_{i+1})_{i \in \mathbb{N}}\}$ sind †. Dies ist allerdings für die nachfolgenden Überlegungen auch nicht notwendig.
Als nächstes benötigt man noch zwei einfache Abschätzungen. Aus Bemerkung 1.1.3 *(S. 14)* folgt für ein nicht-singuläres Tripel :

$$\begin{array}{rcll} p & = & 3p_1p_2 - p' & \text{mit } : p > max(p_1, p_2) > p' \\ \Rightarrow & > & 3p_1p_2 - p_1p_2 & \\ \Rightarrow & > & p_1 + p_2. & \end{array}$$

Darüber hinaus gilt :

$$\begin{array}{rrcll} & 2p + p \pm 2 & = & (3p \pm 2) & \\ \Rightarrow & p & < & \frac{(3p\pm2)}{2} & \text{mit } (3p-2) > 2. \end{array}$$

Da $(3p - 2) > 2$ für ein ungerades $(3p \pm 2)$ (Bem. 1.3.2 *(S. 22)*) keine Einschränkung darstellt, gilt insgesamt für ein Tripel mit $p > p_1 > p_2$:

$$(p_1 \pm p_2) < \frac{(3p \pm 2)}{2}. \tag{1.11}$$

Theorem 1.3.4 *Würden mehrere Tripel (p, p_1, p_2) und (p, p_1', p_2') bezüglich einer ungeraden Markoffzahl p existieren, so würden dieser Markoffzahl auch mehrere Lösungen $q_\pm$ der beiden Kongruenzen :*

$$q_\pm^2 \equiv -1 \; mod(3p \pm 2) \tag{1.12}$$

entsprechen.

Beweis :
Angenommen es existieren zu einer Markoffzahl p zwei Tripel (p, p_1, p_2) und (p, p_1', p_2') mit $q_\pm = q_\pm'$, also :

$$\begin{array}{rrcl} & \varepsilon \frac{p}{p_1 \pm p_2} & \equiv & \varepsilon' \frac{p}{p_1' \pm p_2'} \; mod(3p \pm 2) \\ \Rightarrow & \varepsilon(p_1 \pm p_2) & \equiv & \varepsilon'(p_1' \pm p_2') \; mod(3p \pm 2). \end{array}$$

† Daher auch die Bezeichnung : 'Erweiterungen $q_\pm$'

Angenommen es gilt $\varepsilon \neq \varepsilon'$:

$$\begin{array}{rcl} \Rightarrow -(p_1 \pm p_2) & \equiv & (p_1' \pm p_2') \; mod(3p \pm 2) \\ \Rightarrow \underbrace{(3p \pm 2) - \underbrace{(p_1 \pm p_2)}_{< \frac{(3p \pm 2)}{2}}}_{> \frac{(3p \pm 2)}{2}} & = & \underbrace{(p_1' \pm p_2')}_{< \frac{(3p \pm 2)}{2}}. \qquad \text{lt. 1.11 } (S.\ 23) \end{array}$$

Also haben wir $\varepsilon = \varepsilon'$ und somit :

$$\begin{array}{rcl} (p_1 \pm p_2) & \equiv & (p_1' \pm p_2') \; mod(3p \pm 2) \\ \Rightarrow \; (p_1 \pm p_2) & = & (p_1' \pm p_2'). \end{array}$$

Da für beide Tripel folgende Gleichung gilt :

$$\begin{array}{ccccc} & & p_1 p_2 (3p \pm 2) & = & p^2 + (p_1 \pm p_2)^2 \\ \text{folgt} & : & p_1 p_2 & = & p_1' p_2' \\ \text{mit} & : & (p_1 \pm p_2) & = & (p_1' \pm p_2') \\ \text{ergibt sich} & : & p_1 = p_1' & \text{oder} & p_1 = p_2'. \end{array}$$

□

1.4 Anwendungen von $q(p)$ und $q_\pm(p)$

Faßt man nun die bisherigen Überlegungen zusammen, so ergibt sich folgende Bemerkung :

Bemerkung 1.4.1 *Aus Theorem 1.3.4 (S. 23) und Theorem 1.2.8 (S. 20) folgt, bei eindeutiger Erfüllung mindestens einer der drei Kongruenzen :*

$$q_\pm^2 \equiv -1 \; mod(3p \pm 2), \; \text{ und } q^2 \equiv -1 \; mod(p),$$

die Richtigkeit der Eindeutigkeitsvermutung für das p.

Beispiel 1.4.2 *Für die Markoffzahl $p = 51641$ besitzen die Kongruenzen die Lösungen :*

$$\begin{array}{rclcrcl} q^2 & \equiv & -1 \; mod(p) & : & x_1 & = & 19760 \\ & & & : & x_2 & = & 22502 \\ q_+^2 & \equiv & -1 \; mod(3p+2) & : & x_{+_1} & = & 2007 \\ q_-^2 & \equiv & -1 \; mod(3p-2) & : & x_{-_1} & = & 1968 \\ & & & : & x_{-_2} & = & 27204 \\ & & & : & x_{-_3} & = & 45700. \end{array}$$

Aus der eindeutigen Lösung für q_+ folgt die Eindeutigkeitsvermutung für das p.

Allerdings gibt es auch Markoffzahlen bei denen alle drei Kongruenzen mindestens zwei Lösungen haben.

Beispiel 1.4.3 *Dies ist zum Beispiel für $p = 1325$ und $p = 9077$ der Fall :*

$$\begin{array}{rclrcl}
p & = & 1325 & x_1 & = & 182 \\
 & & & x_2 & = & 507 \\
3p+2 & = & 3977 & x_{+_1} & = & 1239 \\
 & & & x_{+_2} & = & 1918 \\
3p-2 & = & 3973 & x_{-_1} & = & 1607 \\
 & & & x_{-_2} & = & 1955
\end{array} \quad \text{, und} \quad \begin{array}{rclrcl}
p & = & 9077 & x_1 & = & 2216 \\
 & & & x_2 & = & 3468 \\
3p+2 & = & 27233 & x_{+_1} & = & 13319 \\
 & & & x_{+_2} & = & 13432 \\
3p-2 & = & 22681 & x_{-_1} & = & 5482 \\
 & & & x_{-_2} & = & 11069
\end{array}$$

Im Kapitel 3 *(S. 49)* wird mit dem Theorem 3.0.1 *(S. 49)* die Richtigkeit der Eindeutigkeitsvermutung für $p = 1325$ (Beispiel 3.0.2 *(S. 52)*) und mit der Bemerkung 3.0.6 *(S. 54)* entsprechend für $p = 9077$ (Beispiel 3.0.7 *(S. 54)*) gezeigen werden.

Die eigentliche Motivation zur Definition der Erweiterungen $q_\pm$ waren die Theoreme 1.4.4 *(S. 25)* von A.Baragar [15] und 1.4.5 *(S. 26)* von Schmutz [11]. Beide haben unabhängig voneinander Kriterien für die Richtigkeit der Eindeutigkeitsvermutung für eine Markoffzahl p gezeigt, die mit dem Aufbau von p und $(3p \pm 2)$ zusammenhängen. Die Aussagen von A. Baragar sind die umfangreicheren. Schmutz[11] hat eine der Aussagen mit Hilfe elementarer Eigenschaften der Invariante q gezeigt. Im weiteren werde ich versuchen die restlichen Aussagen mit ähnlichen Eigenschaften von q und den Erweiterungen $q_\pm$ zu zeigen.
1994 hat A. Baragar in [15] folgendes Theorem bewiesen.

Theorem 1.4.4 *Ein Markofftripel (p,p_1,p_2) ist durch p bestimmt, wenn p oder $(3p \pm 2)$ von der Form $2^k\tilde{p}$, $\tilde{p}$ Primzahl, $k = 0,1,2$, sind.*

Das Theorem gilt, wegen Bemerkung 1.1.7 *(S. 16)* und 1.1.9 *(S. 17)* , nur mit den Einschränkungen:

$$p \not\equiv 0 \; mod(4) \text{ und } (3p \pm 2) \not\equiv 2 \; mod(4).$$

Es ist erweiterbar für die Fälle, daß p von der Form $2^k\tilde{p}^n$, $\tilde{p}$ Primzahl, $k = 0, 1$, $n \in \mathbb{N}$, ist, und daß $(3p \pm 2)$ von der Form $2^k\tilde{p}^n$, $\tilde{p}^n$ ungerade Potenz einer Primzahl, $k = 0, 2$, $n \in \mathbb{N}$, ist. Die Überlegungen gehen auf Don Zagier und Harvey Cohn zurück. Man faßt, für eine ungerade Markoffzahl p, die Gleichung :

$$x^2 + y^2 - 3pxy = -p^2$$

als Norm

$$N_{K/\mathbb{Q}}(x + \omega y) = -p^2 \quad , \; K = \mathbb{Q}(\omega)$$

auf, wobei ω die größere der Lösungen

$$\omega^2 + 3p\omega + 1 = 0$$

ist. So erhält man eine Bijektion der Kette $\{(p_i, p_{i+1}, p)_{i\in\mathbb{N}}\}$ und Lösungen $\beta \in \mathbb{Z} \times \omega\mathbb{Z}$ mit :

$$N_{K/\mathbb{Q}}(\beta) = -p^2.$$

Für eine nähere Betrachtung dieser Beziehungen sei auf A.Baragar [15] verwiesen.

Bei Schmutz [11] findet sich, unabhängig davon, ein einfacher Beweis des Spezialfalls $p = \tilde{p}^n, \tilde{p}$ Primzahl, von Theorem 1.4.4 *(S. 25)* . Dieser Beweis basiert auf elementaren Eigenschaften der Invarianten q.

Theorem 1.4.5 *Ein Markofftripel (p,p_1,p_2) ist durch p bestimmt, wenn p Potenz einer Primzahl $\tilde{p}$ ist.*

Bemerkung 1.4.6 *Für die Markoffzahl 169, gilt $169 = 13 \cdot 13$.*

Beweis :
a) Für $\tilde{p} = 2$ ist die Aussage wegen Bemerkung 1.1.7 *(S. 16)* offensichtlich.
b) Sei also $p = \tilde{p}^n, \tilde{p} \neq 2$, Primzahl. Angenommen das Markofftripel (p,p_1,p_2) sei nicht durch p bestimmt. Wegen Theorem 1.2.8 *(S. 20)* existieren dann q, q' mit $(0 < q, q' < \frac{p}{2})$. Sei $q' > q$, dann gilt :

$$\begin{array}{rccll}
 & (q'^2 - q^2) & \equiv & 0 & mod(p) \\
\Rightarrow & \underbrace{(q'+q)}_{<\tilde{p}^n}\underbrace{(q'-q)}_{<\tilde{p}^n} & \equiv & 0 & mod(\tilde{p}^n) \\
\Rightarrow & (q'+q) \equiv \ (q'-q) & \equiv & 0 & mod(\tilde{p}) \\
\Rightarrow & q & \equiv & 0 & mod(\tilde{p}) \\
\Rightarrow & \text{lt.(1.5 } (S.\ 18)\text{) } \frac{p_1}{p_2} & \equiv & 0 & mod(\tilde{p}) \\
\Rightarrow & ggT(p, p_1) & \neq & 1. &
\end{array}$$

Widerspruch zu Lemma 1.1.6 $(S.\ 15)$

□

Nun kann man versuchen die fehlenden Aussagen von Theorem 1.4.5 *(S. 26)* ähnlich zu beweisen. Zunächst einmal müßte sich der obige Beweis für den Fall $p = 2\tilde{p}^n$ erweitern lassen.

Theorem 1.4.7 *Ein Markofftripel (p,p_1,p_2) ist durch p bestimmt, wenn gilt :*

$$p = 2\tilde{p}^n,\ \tilde{p}\ Primzahl.$$

Beweis :
Es gilt, wegen $q' > q$:

$$\begin{aligned}\underbrace{(q'+q)}_{<2\tilde{p}^n}\underbrace{(q'-q)}_{<\tilde{p}^n} &\equiv 0\ mod(2\tilde{p}^n)\\ &= a2\tilde{p}^n \qquad a \in \mathbb{N}.\end{aligned}$$

Entsprechend zu oben ist zu zeigen, daß eine Aufteilung :

$$(q'+q) = \tilde{p}^n < 2\tilde{p}^n = p \text{ und } (q'-q) = 2a$$

nicht möglich ist. Mit einer solchen Aufteilung wäre :

$$\begin{aligned} & (q'-q) \equiv 0\ mod(2)\\ \Rightarrow\ & (q'+q) = \tilde{p}^n \equiv 0\ mod(2)\\ \Rightarrow\ & p = 2\tilde{p}^n \equiv 0\ mod(4). \quad \text{Widerspruch zu Bem. 1.1.7 } (S.\ 16)\end{aligned}$$

Wegen $(q'-q) < \tilde{p}^n$ folgt :

$$\Rightarrow (q'+q) \equiv (q'-q) \equiv 0\ mod(\tilde{p}).$$

Mit diesen Überlegungen kann man wie bei Theorem 1.4.5 *(S. 26)* argumentieren. □

Für die restlichen Aussagen von Theorem 1.4.4 *(S. 25)* können wir nun auf die Erweiterungen $q_\pm$ zurückgreifen, die ähnliche Eigenschaften wie die Invariante q besitzen.

Theorem 1.4.8 *Sei p eine Markoffzahl. Gilt für ein Vorzeichen $(3p \pm 2)$ ist ungerade Potenz einer Primzahl $\tilde{p}$, so ist das Markofftripel (p, p_1, p_2), mit $p = max(p, p_1, p_2)$, eindeutig durch p bestimmt.*

Beweis :
Da $(3p\pm2)$ als ungerade Potenz einer Primzahl $\tilde{p}$ vorausgesetzt ist, gilt $(3p\pm2) \neq 2^n$, $n \geq 2$. Sei also $(3p\pm2) = \tilde{p}^n$, $\tilde{p} \neq 2$ Primzahl, und $n \geq 2$. Angenommen das Markofftripel (p,p_1,p_2) sei nicht durch p bestimmt. Wegen Theorem 1.3.4 *(S. 23)* existieren dann $q_\pm$, $q'_\pm$ mit :

$$\left(0 < q_\pm, q'_\pm < \frac{(3p \pm 2)}{2}\right).$$

Sei $'q_\pm > q_\pm$, Dann gilt :

$$(q'^2_\pm - q^2_\pm) \equiv 0\ mod(3p \pm 2).$$

Mit der gleichen Argumentation wie beim Beweis von Theorem 1.4.5 *(S. 26)* b), für $q_\pm = q$, erhält man :

$$\begin{aligned} & q_\pm \equiv 0\ mod(\tilde{p})\\ \Rightarrow\ & \tfrac{p}{p_1 \pm p_2} \equiv 0\ mod(\tilde{p}).\end{aligned}$$

Dies ist ein Widerspruch zu $ggT(p, (3p \pm 2)) = 1$. $\square$

Damit konnten wir Theorem 1.4.4 *(S. 25)*, bis auf den Fall $(3p \pm 2) = 4\tilde{p}^n$, $(3p \pm 2)$ ungerade Potenz einer Primzahl, beweisen.

Kapitel 2

Markoffzahlen in verschiedenen Kontexten

2.1 Markoff-Formen

Mit Hilfe von Markoffzahlen lassen sich gewisse Koeffizienten für indefinite binäre quadratische Formen definieren, den sogenannten Markoff-Formen. Es wird sich zeigen, daß man mit den Nullstellen dieser Formen einen guten Überblick über das Markoffspektrum $\mathfrak{M}_{\mathfrak{S}}$ bekommen kann. Sei also f eine indefinite binäre quadratische Form,

$$f(x,y) = \alpha x^2 + \beta xy + \gamma y^2 \ , \quad \alpha, \beta, \gamma \in \mathbb{R}$$

mit Diskriminante

$$D(f) = \beta^2 - 4\alpha\gamma > 0.$$

Für eine solche Form sei:

$$\mu(f) = inf \left\{ \ |f(m,n)| \ : \ (m,n) \ \in \mathbb{Z} \times \mathbb{Z} \backslash (0,0) \right\} \ .$$

Mit Hilfe von

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - cd = 1; a, b, c, d \in \mathbb{Z} \right\}$$

definiert man für indefinite binäre quadratische Formen f und f' die folgende Äquivalenzrelation :

$$f(x,y) \sim f'(x,y)$$

$$\Leftrightarrow \text{es existiert } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ , mit } f'(ax+by, cx+dy) = f(x,y).$$

Definition 2.1.1 *Sei f eine indefinite binäre quadratische Form,*

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2, \quad \alpha, \beta, \gamma \in \mathbb{R}.$$

Sind α, β, γ ganzzahlig und teilerfremd und gilt :

$$\frac{\mu(f)}{\sqrt{D(f)}} > \frac{1}{3} \; ,$$

so heißt f **Markoff-Form**.

Dies ist natürlich eine sehr allgemeine Definition von Markoff-Formen. Sie beinhaltet weder Markoffzahlen, noch gibt sie darüber Aufschluß , wie eine solche Form letztlich aufgebaut ist. Die einzig außergewöhnliche Forderung an eine Markoff-Form ist $\frac{\mu(f)}{\sqrt{D(f)}} > \frac{1}{3}$. Betrachten wir also zunächst den Bruch $\frac{\mu(f)}{\sqrt{D(f)}}$. Seien f und f' zwei äquivalente Formen . Wegen $a, b, c, d \in \mathbb{Z}$ und

$$f'(ax + by, cx + dy) = f(x, y)$$

nehmen beide Formen auf $\mathbb{Z} \times \mathbb{Z}$ dieselben Werte an. Also gilt:

$$\mu(f) = \mu(f') \text{ , für } f \sim f'.$$

Darüber hinaus gilt für eine Zahl $\tau \in \mathbb{R} \backslash \{0\}$:

$$\mu(\tau f) = |\tau| \mu(f) \text{ , und } D(\tau f) = \tau^2 D(f).$$

Weiter gilt :

$$D(f) = D(f') \text{ , für } f \sim f'.$$

Diese Aussage kann man durch einfaches Nachrechnen zeigen.

Definition 2.1.2 *Für eine indefinite binäre quadratische Form g sei*

$$[g] = \{f : f \textit{ indefinite binäre quadratische Form, mit : } \tau f \sim g, \ \tau \in \mathbb{R} \backslash \{0\}\} \tag{2.1}$$

die 'erweiterte' Äquivalenzklasse von g bezüglich $SL_2(\mathbb{Z})$.

Faßt man die bisherigen, allgemeinen Überlegungen zusammen, so ergibt sich die folgende Bemerkung.

Bemerkung 2.1.3 *Sei $[g]$ die 'erweiterte' Äquivalenzklasse von g bezüglich $SL_2(\mathbb{Z})$, dann gilt:*

$$\frac{\mu(f)}{\sqrt{D(f)}} = \frac{\mu(g)}{\sqrt{D(g)}}, \text{ für jedes } \; f \in [g].$$

In Definition 2.1.1 *(S. 30)* wurden Markoff-Formen allgemein, ohne Markoffzahlen oder das Markoffspektrum, definiert. Bei Cassels [5] finden sich die beiden Theoreme 2.1.4 *(S. 31)* und 2.2.9 *(S. 42)*, die genau diese Zusammenhänge herstellen. *'The Markoff chain for forms'* (Theorem 2.1.4 *(S. 31)*), stellt den Zusammenhang von Markoff-Formen und Markoffzahlen, und *'The Markoff chain for approximations'* (Theorem 2.2.9 *(S. 42)*) stellt den Zusammenhang von Markoff-Formen und dem Markoffspektrum her.

Theorem 2.1.4 (The Markoff chain for forms) *Sei*

$$g(x,y) = \alpha x^2 + \beta xy + \gamma y^2, \quad \alpha,\beta,\gamma \in \mathbb{R}$$

eine indefinite binäre quadratische Form mit $D(g) > 0$ und

$$\frac{\mu(g)}{\sqrt{D(g)}} > \frac{1}{3},$$

dann ist g äquivalent zum Vielfachen einer Markoff-Form. Darüber hinaus existiert ein Markofftripel (p,p_1,p_2) mit (p,q,r) wie in Definition 1.2.3 (S. 18) und Definition 1.2.5 (S. 19), so daß g äquivalent zum Vielfachen der Form :

$$f_p(x,y) = px^2 + (3p-2q)xy - (3q-r)y^2 \tag{2.2}$$

ist und es gilt $\mu(f_p) = p$.

Anders ausgedrückt, jede 'erweiterte' Äquivalenzklasse $[g]$ indefiniter binärer quadratischer Formen, mit $\frac{\mu(g)}{\sqrt{D(g)}} > \frac{1}{3}$, enhält eine Markoff-Form f_p. Da dies für alle 'erweiterten' Äquivalenzklassen $[g]$ mit $\frac{\mu(g)}{\sqrt{D(g)}} > \frac{1}{3}$ gilt, bilden die Markoff-Formen f_p ein Repräsentantensystem, der 'erweiterten' Äquivalenzklassen. Darüber hinaus ergibt sich aus Theorem 2.1.4 *(S. 31)* die folgende Bemerkung.

Bemerkung 2.1.5 *Die in Definition 2.1.1 (S. 30) beschriebenen Markoff-Formen sind gerade die Formen:*

$$f_p(x,y) = px^2 + (3p-2q)xy - (3q-r)y^2, \ p \text{ Markoffzahl.}$$

Für eine Markoff-Form f_p ist der Abstand der Nullstellen von $f_p(x,1)$ gerade $\sqrt{D(f_p)} = \sqrt{9p^2-4}$. Das Infimum von f_p auf dem Gitter $\mathbb{Z}\times\mathbb{Z}\setminus(0,0)$ ist nach Theorem 2.1.4 *(S. 31)* gerade $\mu(f_p) = p$ und wird laut Lemma 2.1.9 *(S. 34)* bei (q,p) angenommen (siehe Abbildung 2.1 *(S. 32)*). Damit gilt für eine Markoff-Form f_p:

$$\frac{\mu(f_p)}{\sqrt{D(f_p)}} = \frac{p}{\sqrt{9p-4}}.$$

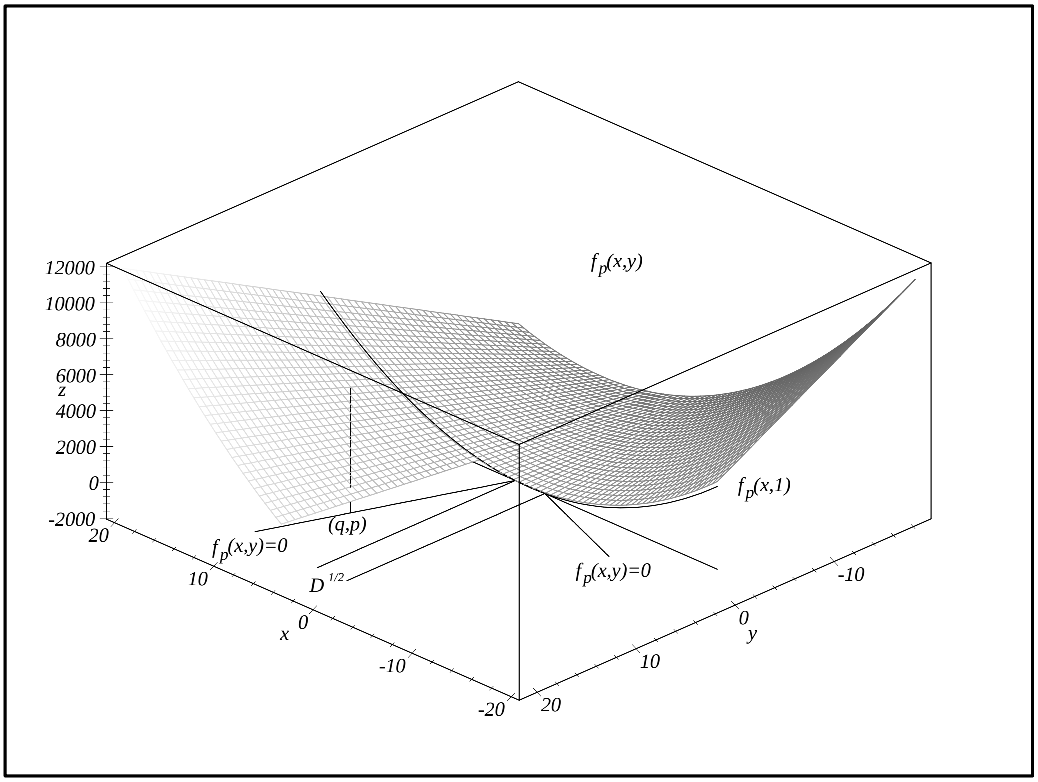

Abbildung 2.1: $\quad f_p(x,y) = px^2 + (3p-2q)xy - (3q-r)y^2$.

Bemerkung 2.1.5 *(S. 31)* führt dazu, daß teilweise die Gleichung 2.2 *(S. 31)* direkt als Definition einer Markoff-Form f_p benutzt wird. Bei Cassels [5] findet sich eine solche Definition (Definition 2.1.6 *(S. 32)*). Allerdings definiert er über $\mu(f_p) = p$, normierte Markoff-Formen F_p, mit $\mu(F_p) = 1$. Dies macht aber innerhalb der 'erweiterten' Äquivalenzklasse keinen Unterschied. In diesem Kapitel möchte ich die Definition von F_p, mit $\mu(F_p) = 1$ benutzen. Im Kapitel 3 *(S. 49)* ist die oben genannte Definition vorteilhafter, da man mit :

$$| f_p(x_0,y_0) | \geq p \ , \text{ für geeignete } (x_0,y_0) \in \mathbb{Z} \times \mathbb{Z},$$

einige nützliche Ungleichungen herleiten kann. Ansonsten bemühe ich mich die Notationen f_p und F_p für Formen der jeweiligen Definition beizubehalten.

Definition 2.1.6 *Sei (p,p_1,p_2) ein Markofftripel mit $p = max(p,p_1,p_2)$ und (p,q,r) wie in Definition 1.2.3 (S. 18) und Definition 1.2.5 (S. 19) . Dann heißt :*

$$pF_p(x,y) = px^2 + (3p-2q)xy + (r-3q)y^2$$

Markoff-Form mit

$$D(F_p) = 9p^2 - 4 > 0$$
$$\textit{und } \mu(F_p) = 1.$$

Ein zentrales Theorem über Markoff-Formen ist ein Theorem, das Cassels in [5] benutzt, um Theorem 2.1.4 *(S. 31)* zu beweisen. Dieses Theorem, das uns noch beim Markoffspektrum begegnen wird, läßt sich relativ einfach zeigen und besagt :

$$F_p(x,y) \sim -F_p(x,y).$$

Dabei ist zu zeigen:

$$F_p(q_1x - r_1y, p_1x - q_1y) = -F_p(x,y), \quad \begin{pmatrix} q_1 & r_1 \\ p_1 & q_1 \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Der Nachweis durch Nachrechnen führt leider zu ausgesprochen langen und unübersichtlichen Ausdrücken. Um dies zu vermeiden, kann man die Aussage auch zeigen, indem man nachweist, daß $F_p(q_1x-r_1y, p_1x-q_1y)$ und$-F_p(x,y)$ in drei Punkten übereinstimmen und somit $F_p(q_1x-r_1y, p_1x-q_1y) - F_p(x,y)$, nach einer geeigneten Substitution, ein Polynom mit drei Nullstellen ist. Eine weitere Möglichkeit die Rechnungen übersichtlich zu halten, besteht darin, eine symmetrische Form φ_p zu definieren.

Definition 2.1.7

$$\varphi_p(y,z) = p^2 F_p(x,y)$$
$$\textit{mit } z = px - qy$$
$$\textit{und } \varphi_p(y,z) = y^2 + 3pyz + z^2.$$

Für diese Form gelten folgende Identitäten.

Lemma 2.1.8

$$\begin{aligned} \varphi_p(y,z) &= \varphi_p(z,y) \\ &= \varphi_p(-z, y+3pz) \qquad (2.3) \\ &= \varphi_p(z+3py, -y)). \qquad (2.4) \end{aligned}$$

Beweis :

Nicht offensichtlich ist nur Gleichung (2.3 *(S. 33)*), also :

$$\begin{aligned} \varphi_p(-z, y+3pz) &= (-z)^2 + 3p(-z)(y+3pz) + (y+3pz)^2 \\ &= z^2 - 3pzy - (3pz)^2 + y^2 + 6pzy + (3pz)^2 \\ &= z^2 + 3pzy + y^2 \\ &= \varphi_p(z,y). \end{aligned}$$

□

Nun können wir die in Kapitel 1 *(S. 13)* definierten Zahlen zu benutzen.

Lemma 2.1.9 *Für ein nicht-singuläres Tripel* (p,p_1,p_2)*, mit* $p = max(p,p_1,p_2)$*, gilt :*

$$\begin{array}{rcll} F_p(q,p) & = & F_p(q-3p,p) & = 1 \\ F_p(q_1,p_1) & = & F_p(q_2-3p_2,p_2) & = -1 \end{array}$$

Beweis :

$$\begin{array}{lccccc} 1.) & \text{z.z.} & p^2F_p(q,p) & = & \varphi_p(p,0) & = & p^2 \\ & (\text{Def. } 2.1.7\ (S.\ 33)\ ) & p^2F_p(x,y) & = & \varphi_p(y,z) & & \\ & \text{und} & z & = & px-qy & & \\ & \Rightarrow & z & = & pq-pq & = & 0 \end{array}$$

$$\begin{array}{lcccc} 2.) & \text{z.z.} & p^2F_p(q-3p,p) & = & \varphi_p(p,-3p^2) \\ & & & = & \varphi_p(0,-p) = p^2 \\ & \text{wg.} & z & = & px-qy \\ & \Rightarrow & z & = & p(q-3p)-qp \\ & \Rightarrow & z & = & -3p^2 \\ & \text{wg. } (\ 2.4\ (S.\ 33)\ ) & \varphi_p(y,z) & = & \varphi_p(z+3py,-y) \\ & \Rightarrow & \varphi_p(p,-3p^2) & = & \varphi_p(-3p^2+3p^2,-p) \\ & & & = & \varphi_p(0,-p) \end{array}$$

$$\begin{array}{lcccc} 3.) & \text{wg.} & z & = & px-qy \\ & \text{und} & (x,y) & = & (q_1,p_1) \\ & \Rightarrow & z & = & pq_1-qp_1 \\ & \text{wg. } (\ 1.7\ (S.\ 19)\ ) & & = & -p_2 \\ & \Rightarrow & p^2F_p(q_1,p_1) & = & \varphi_p(p_1,-p_2) \\ & & & = & p_1^2-3pp_1p_2+p_2^2 \\ & & & = & -p^2 \end{array}$$

$$\begin{array}{lcccc} 4.) & \text{wg.} & z & = & px-qy \\ & \text{und} & (x,y) & = & (q_2-3p_2,p_2) \\ & \Rightarrow & z & = & p(q_2-3p_2)+qp_2 \\ & \text{wg. } (\ 1.6\ (S.\ 19)\ ) & & = & \underbrace{pq_2+qp_2}_{=p_1}-3pp_2 \\ & \Rightarrow & p^2F_p(q_2-3p_2,p_2) & = & \varphi_p(p_2,p_1-3pp_2) \\ & & & = & \varphi_p(p_1,-p_2) \\ & & & = & -p^2 \end{array}$$

$\square$

Lemma 2.1.10 *Für ein nicht-singuläre Tripel (p, p_1, p_2) gilt :*

$$F_p(x,y) \sim -F_p(x,y)$$

$$b.z.w. \quad F_p(q_1x - r_1y, p_1x - q_1y) = -F_p(x,y).$$

Beweis :
Wir betrachten die Gleichung in den drei Punkten $(1,0), (q_1,p_1), (p,q)$:

$$\begin{array}{lrcl}
1.) \quad \text{Sei} & (x,y) & = & (1,0) \\
\text{lt. Lemma 2.1.9 } (S.\ 34) & F_p(q_1,p_1) & = & -F_p(1,0) \\
 & & = & -1
\end{array}$$

$$\begin{array}{lrcl}
2.) \quad \text{Sei} & (x,y) & = & (q_1,p_1) \\
\text{dann ist} & q_1x - r_1y & = & q_1^2 - r_1p_1 \\
 & & = & 1 \\
 & & & \text{lt. (1.2.5 } (S.\ 19) \text{)} \\
\text{und} & p_1x - q_1y & = & p_1q_1 - q_1p_1 \\
 & & = & 0 \\
\Rightarrow & F_p(q_1q_1 - r_1p_1, p_1q_1 - q_1p_1) & = & F_p(1,0) \\
 & & = & -F_p(q_1,p_1)
\end{array}$$

$$\begin{array}{lrcl}
3.) \quad \text{Sei} & (x,y) & = & (q,p) \\
\text{dann ist} & p_1x - q_1y & = & p_1q - q_1p \\
 & & = & p_2 \\
 & & & \text{lt. (1.7 } (S.\ 19) \text{)} \\
 & & & \\
\text{Es ist} & p_1(q_1x - r_1y) & = & p_1(q_1q - r_1p) \\
\text{lt. (1.2.5 } (S.\ 19) \text{)} & & = & p_1q_1q - (1+q_1^2)p \\
\text{lt. (1.7 } (S.\ 19) \text{)} & & = & q_1 \underbrace{(p_1q - q_1p)}_{=p_2} - p \\
 & & = & q_1p_2 - p \\
\text{lt.Lemma 1.8 } (S.\ 19) & & = & p_1q_2 - 3p_1p_2 \\
 & & = & p_1(q_2 - 3p_2) \\
\Leftrightarrow & (q_1q - r_1p) & = & (q_2 - 3p_2) \\
\Rightarrow & F_p(q_1q - r_1p, p_1q - q_1p) & = & F_p(q_2 - 3p_2, p_2) \\
\text{lt.Lemma 2.1.9 } (S.\ 34) & & = & -F_p(q,p)
\end{array}$$

Also stimmen die Formen in den drei Punkten (1,0), (q_1,p_1) und (q,p) überein. Somit besitzt :

$$F_p(q_1x - r_1y, p_1x - q_1y) - F_p(x,y) = 0, \quad \begin{pmatrix} q_1 & r_1 \\ p_1 & q_1 \end{pmatrix} \in SL_2(\mathbb{Z}),$$

aufgefaßt als eine quadratische Gleichung nach einer Substitution $z = \frac{y}{x}$, drei Nullstellen . Daher müssen die Formen gleich sein. $\square$

Kommen wir nun zu dem im Kapitel 1 *(S. 13)* erwähnten Theorem 1.2.8 *(S. 20)* :

Würden mehrere Ketten bezüglich p existieren, so würden diesen Ketten auch mehrere Lösungen q der Kongruenz :

$$q^2 \equiv -1 \; mod(p)$$

entsprechen.

Mit Lemma 2.1.10 *(S. 35)* hat man eine geeignete Transformation gefunden, aus der die obere Aussage direkt folgt.

Beweis :
Annahme : Es existieren zu p zwei Ketten, und damit zwei Tripel (p,p_1,p_2) und (p,p_1',p_2'), mit $p = max(p,p_1,p_2,p_1',p_2')$ und es gilt :

$$\varepsilon\frac{p_1}{p_2} \equiv \varepsilon'\frac{p_1'}{p_2'} \equiv q \; mod(p)$$

Mit diesen Annahmen bestimmen die Ketten nach (1.2.5 *(S. 19)*) dieselben Zahlen (p,q,r), also auch dieselbe Form :

$$pF_p(x,y) = px^2 + (3p-2q)xy + (r-3q)y^2 \; .$$

Lemma 2.1.10 *(S. 35)* besagt, daß beide Tripel (p_1,q_1,r_1) und (p_1',q_1',r_1') die Form F_p wie folgt transformieren :

$$\begin{aligned} F_p(q_1x - r_1y, p_1x - q_1y) &= -F_p(x,y) \\ &= F_p(q_1'x - r_1'y, p_1'x - q_1'y). \end{aligned}$$

$$\begin{aligned} \text{Daraus folgt :} \quad (p_1,q_1,r_1) &= (p_1',q_1',r_1') \\ \Rightarrow \quad (p,p_1,p_2) &= (p,p_1',p_2'). \end{aligned}$$

$\square$

2.2 Markoffspektrum

Eine Betrachtung des Markoffspektrums führt zunächst zu der Frage, wie eine irrationale Zahl θ duch rationale Brüche $\frac{r}{s}$ approximiert werden kann. Ein einfaches Beispiel hierzu ist das nachfolgende Theorem.

Theorem 2.2.1 *Sei $\theta \in \mathbb{R} \backslash \mathbb{Q}$, dann besitzt die Gleichung :*

$$\left|\theta - \frac{r}{s}\right| < \frac{1}{s^2} \tag{2.5}$$

unendlich viele Lösungen $s \in \mathbb{N}$ † und $r \in \mathbb{Z}$.

Will man Theorem 2.2.1 *(S. 37)* für ein $\theta \in \mathbb{R}$ erweitern, so muß '$<$' durch '$\leq$' ersetzt werden. Doch zunächst sind nur die $\theta \in \mathbb{R}\backslash\mathbb{Q}$ von Interesse. Es sei $[\theta] \in \mathbb{Z}$ der ganzzahlige, und $\{\theta\}$ der 'gebroche' Anteil von θ, also :

$$[\theta] \leq \theta < [\theta] + 1 \text{ und } 0 < \{\theta\} < 1 \text{ mit } : \\ [\theta] + \{\theta\} = \theta.$$

Beweis : (Dirichlet)
Sei $n \in \mathbb{N}$ beliebig aber fest. Dann erfüllen die $(n+1)$ Zahlen :

$$x_0 = 0,\ x_i = \{i\theta\}, x_n = 1\ ; \quad 0 < i < n$$

die Ungleichung $0 \leq x_i \leq 1$. Betrachtet man nun die Verteilung der $(n+1)$ Zahlen x_i in den n Intervallen

$$\frac{j}{n} \leq x_i < \frac{j+1}{n}\ ;\ 0 \leq j < n, \tag{2.6}$$

wobei für $j = n-1$ '$\leq$' statt '$<$' zu lesen ist, so muß eine Intervall zwei x_i enthalten. Daher kann man Zahlen $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ finden mit :

$$\begin{array}{rrcl} & |\ (s_1\theta - r_1) - (s_2\theta - r_2)\ | & \leq & \frac{1}{n} \\ \Rightarrow & |\ (s_1 - s_2)\theta - (r_1 - r_2)\ | & \leq & \frac{1}{n}. \end{array}$$

Sei ohne Beschränkung der Allgemeinheit $s_2 < s_1$ und $s = (s_1 - s_2), r = (r_1 - r_2)$, dann gilt wegen 2.6 *(S. 37)* $s < n$. Insgesamt kann man nun zu jedem $\theta \in \mathbb{R}\backslash\mathbb{Q}$ und jedem $n \in \mathbb{N}$ ein $s \in \mathbb{N}$ und ein $r \in \mathbb{Z}$ finden mit :

$$\begin{array}{rrcl} & |\ s\theta - r\ | & \leq & \frac{1}{n} < \frac{1}{s} \\ \Rightarrow & |\ \theta - \frac{r}{s}\ | & < & \frac{1}{s^2} \end{array}$$

□

Nun kann man sich die Frage stellen, unter welchen Bedingungen zu einem $\theta \in \mathbb{R}\backslash\mathbb{Q}$ eine Konstante $\kappa < 1$ existiert, so daß die Ungleichung

$$|\ \theta - \tfrac{r}{s}\ | < \tfrac{\kappa}{s^2}$$

unendlich viele Lösungen $s \in \mathbb{N}$ und $r \in \mathbb{Z}$ besitzt. Mit Hilfe der Theorie der Kettenbrüche kann man zeigen, daß für ein $\theta \in \mathbb{R}\backslash\mathbb{Q}$ die Konstante $\kappa = 1$ durch $\kappa = 5^{-\frac{1}{2}}$ ersetzt werden

†Im folgenden wird teilweise die zu 2.5 *(S. 37)* äquivalente Darstellung $s \mid s\theta - r \mid < 1$ benutzt.

kann (siehe z.B. Cassels [5]). Diese Konstante kann weiter verbessert werden, allerdings nicht für alle $\theta \in \mathbb{R}\backslash\mathbb{Q}$, sondern nur für bestimmte Klassen von θ. Diese Klassen führen zu folgender Äquivalenzrelation auf der Hyperbolischen Ebene $\mathbb{H}^2 = \{z \in \mathbb{C} : \; Im(z) > 0\}$, die sich auf $\mathbb{R}$ erweitern läßt.

Definition 2.2.2 *Seien $\theta, \theta' \in \mathbb{R}$, und*

$$PSL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; : ad - bc = \pm 1 \; ; a, b, c, d \in \mathbb{Z} \right\}.$$

θ und θ' sind genau dann äquivalent, wenn eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z})$ existiert mit :

$$\theta = \frac{a\theta' + b}{c\theta' + d} \quad b.z.w \quad \theta' = \frac{-d\theta + b}{c\theta - a} \; .$$

Markoff hat in [2] und [3] gezeigt, daß eine ganze Kette von Aussagen über die Konstante κ bei der Approximation einer Zahl $\theta \in \mathbb{R}\backslash\mathbb{Q}$ durch rationale Brüche $\frac{r}{s}$ möglich ist. Diese umfangreichen Ergebnisse werden in Theorem 2.2.9 *(S. 42)* 'The Markoff chain for approximations' zusammengefaßt. Einen weniger umfangreichen aber dafür anschaulicheren Ansatz bietet folgende Bemerkung.

Bemerkung 2.2.3 (The Markoff chain) *Für alle $\theta \in \mathbb{R}\backslash\mathbb{Q}$ besitzt die Ungleichung*

$$\mid \theta - \tfrac{r}{s} \mid < \tfrac{5^{-\frac{1}{2}}}{s^2}$$

unendlich viele Lösungen $s \in \mathbb{N}$ und $r \in \mathbb{Z}$. Wenn θ zu $\frac{1}{2}(5^{\frac{1}{2}} - 1)$, das heißt zu einer der Wurzeln von

$$\theta^2 + \theta - 1 = 0,$$

äquivalent ist, so kann die Konstante $\kappa = 5^{-\frac{1}{2}}$ nicht verbessert werden. Wenn nicht, so gibt es unendlich viele Lösungen zu

$$\mid \theta - \tfrac{r}{s} \mid < \tfrac{2^{-\frac{3}{2}}}{s^2}$$

wobei die Konstante $\kappa = 2^{-\frac{3}{2}}$ nicht verbessert werden kann, wenn θ zu einer der Wurzeln von

$$\theta^2 + 2\theta - 1 = 0,$$

äquivalent ist. Anderenfalls gibt es unendlich viele Lösungen zu

$$\mid \theta - \tfrac{r}{s} \mid < \tfrac{5}{(221)^{\frac{1}{2}}} \tfrac{1}{s^2}$$

wobei die Konstante $\kappa = \frac{5}{(221)^{\frac{1}{2}}}$ *nicht verbessert werden kann, wenn* θ *zu einer der Wurzeln von*

$$5\theta^2 + 11\theta - 5 = 0,$$

äquivalent ist. Anderenfalls gibt es unendlich viele Lösungen zu

$$\mid \theta - \tfrac{r}{s} \mid < \tfrac{13}{(1517)^{\frac{1}{2}}} \tfrac{1}{s^2}$$

wobei die Konstante $\kappa = \frac{13}{(1517)^{\frac{1}{2}}}$ *nicht verbessert werden kann, wenn* θ *zu einer der Wurzeln von*

$$13\theta^2 + 29\theta - 13 = 0,$$

äquivalent ist, und so weiter ... . Für die Folge der Konstanten κ *gilt :*

$$5^{-\frac{1}{2}},\ 2^{-\frac{3}{2}},\ \tfrac{5}{(221)^{\frac{1}{2}}},\ \tfrac{13}{(1517)^{\frac{1}{2}}},\ \ldots\ \rightarrow\ \tfrac{1}{3}.$$

Wir wollen nun versuchen an Hand einiger Überlegungen, die Aussagen der obigen Bemerkung zu verstehen. Zunächst einmal ist es sicherlich sinnvoll einerseits für die Zahlen $\theta \in \mathbb{R}\backslash\mathbb{Q}$ die entsprechenden Approximationskonstanten κ, und andererseits die Menge aller möglichen Konstanten κ zu definieren.

Definition 2.2.4 *Für ein* $\theta \in \mathbb{R}\backslash\mathbb{Q}$ *sei :*

$$\nu(\theta) := inf \left\{ \kappa : \ \left| \theta - \frac{r}{s} \right| \ < \frac{\kappa}{s^2}, \ \text{für unendlich viele } r, s \in \mathbb{Z} \right\},$$

und

$$\mathfrak{M}_{\mathfrak{S}} := \left\{ \nu(\theta) : \ \nu(\theta) > \frac{1}{3}; \ \theta \in \mathbb{R} \right\}.$$

Die Menge $\mathfrak{M}_{\mathfrak{S}}$ *heißt* **Markoffspektrum**.

Nun kann man untersuchen, worin der Zusammenhang zwischen der Äquivalenz zweier Zahlen θ und $\theta' \in \mathbb{R}\backslash\mathbb{Q}$ und den Elementen $\nu(\theta)$ und $\nu(\theta')$ des Markoffspektrums liegt.

Theorem 2.2.5 *Seien* $\theta, \theta' \in \mathbb{R}\backslash\mathbb{Q}$, *dann gilt :*

$$\theta \sim \theta' \Rightarrow \nu(\theta) = \nu(\theta').$$

Da $PSL_2(\mathbb{Z})$ bekanntlich durch die Matrizen:

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ und } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

erzeugt wird und offensichtlich $\nu(\theta) = \nu(T(\theta))$ gilt. genügt es zu zeigen, daß :

$$\nu(\theta) = \nu(S(\theta)).$$

Beweis :
Sei also $\kappa > \nu(\theta)$, κ fixiert, dann gibt es unendlich viele Lösungen $s \in \mathbb{N}$ und $r \in \mathbb{Z}$ zu :

$$s \mid s\theta - r \mid < \kappa.$$

Es gilt :

$$\begin{aligned} \mid -r \mid\mid -rS(\theta) - s \mid &= \mid -r \mid\mid -r\left(-\tfrac{1}{\theta}\right) - s \mid \\ &= \mid -r + s\theta - s\theta \mid\mid \tfrac{s\theta - r}{\theta} \mid \\ &\leq (\mid s\theta - r \mid + \mid -s\theta \mid) \mid \tfrac{s\theta - r}{\theta} \mid \\ &= \mid \tfrac{1}{\theta} \mid \underbrace{\mid s\theta - r \mid^2}_{<\left(\frac{\kappa}{s}\right)^2} + \underbrace{s \mid s\theta - r \mid}_{<\kappa} \\ &< \kappa' \end{aligned}$$

für ein fixiertes $\kappa' > \kappa$ und ein geeignet großes s. Sei nun $u = -r$ und $v = s$. Dann besitzt die Ungleichung

$$\mid u \mid\mid uS(\theta) - v \mid < \kappa'$$

unendlich viele Lösungen $u, v \in \mathbb{Z}$ für ein beliebiges $\kappa' > \kappa$. Damit gilt

$$\nu(S(\theta)) \leq \nu(\theta).$$

Die umgekehrte Argumentation liefert $\nu(\theta) \leq \nu(S(\theta))$. □

Kommen wir nun zu den in Bemerkung 2.2.3 *(S. 38)* beschriebenen quadratischen Gleichungen und deren Wurzeln. Dies führt uns wieder zu indefiniten binären quadratischen Formen :

$$f(x,y) = \alpha x^2 + \beta xy + \gamma y^2 \;, \quad \alpha, \beta, \gamma \in \mathbb{R}.$$

Es gibt folgenden Zusammenhang zwischen der Äquivalenz von indefiniten binären quadratischen Formen und der Äquivalenz von Zahlen θ und $\theta' \in \mathbb{R}$. Seien f, f' indefinite binäre quadratische Formen mit :

$$f'(ax + by, cx + dy) = f(x,y) \;, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

und θ Nullstelle von $f(x,1)$.

$$\begin{aligned} \Rightarrow \quad f(\theta,1) = \quad 0 &= f'(a\theta + b, c\theta + d) \\ \Leftrightarrow \quad 0 &= \alpha'(a\theta + b)^2 + \beta'(a\theta + b)(c\theta + d) + \gamma'(c\theta + d)^2 \\ \Rightarrow \quad &= f'(\theta', 1) \\ \Leftrightarrow \quad \theta' &= \tfrac{a\theta + b}{c\theta + d}, \end{aligned}$$

wobei θ' eine der Nullstellen von f' ist. Die gleiche Argumentation gilt natürlich auch für die Formen f, f' mit $f \sim \tau f'$, $\tau \in \mathbb{R}\backslash\{0\}$. Insgesamt erhält man die folgende Bemerkung.

Bemerkung 2.2.6 *Sei $[g]$ die 'erweiterte' Äquivalenzklasse von g und $f \in [g]$. Ist θ eine Nullstelle von $f(x,1)$, dann ist θ äquivalent zu einer der Nullstellen von $g(x,1)$.*

In diesem Kontext besitzen die Wurzeln der Markoff-Formen eine Besonderheit.

Theorem 2.2.7 *Die Wurzeln ζ_p und ζ_p' einer Markoff-Form $F_p(x,1)$ sind äquivalent.*

Beweis :
Nach Theorem 2.1.10 *(S. 35)* gilt $F_p \sim -F_p$. Seien ζ_p und ζ_p' die Wurzeln von $-F_p$. Dann gilt :

$$F_p(q_1\zeta_p - r_1, p_1\zeta_p - q_1) = -F_p(\zeta_p, 1) = 0.$$

Sei nun ζ_p'' die Wurzel von F_p, mit $\zeta_p'' \sim \zeta_p$ dann gilt

$$F_p(\zeta_p'', 1) = 0 \ , \ \zeta_p'' = \frac{q_1\zeta_p - r_1}{p_1\zeta_p - q_1}.$$

Annahme : $\zeta_p'' = \zeta_p$, dann wäre :

$$p_1\zeta_p^2 - 2q_1\zeta_p + r_1 = 0.$$

Damit würde für die Determinante gelten :

$$4q_1^2 - 4p_1r_1 = -4 < 0 \quad \text{lt. (1.2.5 } \textit{(S. 19)} \text{)}$$

Also $\zeta_p'' = \zeta_p'$. □

Bemerkung 2.2.6 *(S. 41)* besagt lediglich, daß für zwei äquivalente indefinite binäre quadratische Formen f und f' und für die Wurzeln θ_1 und θ_2 von f gilt :
θ_1 ist äquivalent zu *einer* der Wurzeln von f' und θ_2 ist äquivalent zu *einer* der Wurzeln von f', aber nicht notwendig θ_1 und θ_2 sind jeweils äquivalent zu *beiden* Wurzeln von f'. Genau diese Besonderheit besitzen Markoff-Formen. Ist f äquivalent zu einer Markoff-Form, so ist jede Wurzel der Markoff-Form äquivalent zu *beiden* Wurzeln von f. Nun enthält nach Theorem 2.1.4 *(S. 31)* jede 'erweiterte' Äquivalenzklasse $[g]$ mit $\frac{\mu(g)}{\sqrt{D(g)}} > \frac{1}{3}$ eine Markoff-Form. Also sind alle Wurzeln dieser 'erweiterten' Äquivalenzklasse $[g]$ äquivalent. Aus Theorem 2.2.5 *(S. 39)* folgt damit die folgende Bemerkung.

Bemerkung 2.2.8 *Sei $[g]$ die 'erweiterte' Äquivalenzklasse von g, mit $\frac{\mu(g)}{\sqrt{D(g)}} > \frac{1}{3}$. Dann gilt für alle Wurzeln θ, θ' von indefiniten binären quadratischen Formen $f, f' \in [g]$:*

$$\theta \sim \theta' \quad \textit{und damit : } \nu(\theta) = \nu(\theta').$$

Betrachtet man die quadratischen Gleichungen in Bemerkung 2.2.3 *(S. 38)* , so stellt man fest, daß es sich dabei um Markoff-Formen handelt :

$$f_1(\theta,1)=0\ ,\quad f_2(\theta,1)=0\ ,\quad f_3(\theta,1)=0\ ,\quad f_4(\theta,1)=0\ ,\quad f_5(\theta,1)=0$$

Mit dem zuvor schon erwähnten Theorem *'The Markoff chain for approximations'* erhält man die Rückrichtung der obigen Bemerkung und einen genauen Überblick über die Werte von $\nu(\theta)$. Leider sind die Beweise der fehlenden Aussagen nicht mehr so einfach zu zeigen und darüber hinaus sehr umfangreich. Für diese sei auf Cassels [5]) verwiesen.

Theorem 2.2.9 (The Markoff chain for approximations) *Sei θ irrational und*

$$\nu(\theta) := inf\left\{\kappa :\ \left|\theta - \frac{r}{s}\right| < \frac{\kappa}{s^2},\ \textit{für unendlich viele } r,s\in\mathbb{Z}\right\}.$$

A: *Ist $\nu(\theta) > \frac{1}{3}$, so ist θ äquivalent zu einer Wurzel, einer Markoff-Form $F_p(x,1)=0$.*
B: *Ist, umgekehrt, θ äquivalent zu einer Wurzel einer Markoff-Form $F_p(x,1)=0$, so ist :*

$$\nu(\theta) = \frac{p}{\sqrt{9p^2-4}} > \frac{1}{3}.$$

Die bisherigen Überlegungen betrafen Approximationskonstanten im Markoffspektrum, für die per Definition $\nu(\theta) > \frac{1}{3}$ gilt. Allerdings sind auch Werte $\nu(\theta) \leq \frac{1}{3}$ möglich. Eine weitergehende Betrachtung dazu findet sich zum Beispiel bei Cusick und Flahive [19].

2.3 Arithmetische Flächen

In diesem Abschnitt möchte ich einen kurzen Überblick über den Zusammenhang zwischen Markoffzahlen bzw. dem Markoffspektrum und einfach geschlossenen Geodätischen auf arithmetischen Flächen geben.

Sei $\mathbb{H}^2 = \{z\in\mathbb{C} :\ Im(z) > 0\}$ die hyperbolische Ebene und

$$SL_2(\mathbb{R}) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} :\ ad-bc=1;\ a,b,c,d\in\mathbb{R}\right\}.$$

Für ein $\gamma\in SL_2(\mathbb{R})$ sei $tr(\gamma)$ die Spur von γ. Eine diskrete Untergruppe von $SL_2(\mathbb{R})$ heißt Fuchssche Gruppe. Im weiteren benötigen wir spezielle Gruppen. Für $N\geq 2$ sei

$$\Gamma(N) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \equiv \begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix} mod(N);\ \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})\right\} \tag{2.7}$$

die Hauptkongruenzgruppe der Stufe N. Das folgende Theorem stellt einige bekannte Tatsachen dar.

Theorem 2.3.1 *Sei Γ eine Fuchsschen Gruppe, dann gilt :*

a)

$$M = \mathbb{H}^2/\Gamma$$

ist Riemannsche Fläche.

b) *Sei $\gamma \in \Gamma$, mit $|tr(\gamma)| > 2$, dann enthält M eine korrespondierende geschlossene Geodätische u, so daß für ein $n \in \mathbb{N}$ gilt:*

$$|tr(\gamma)| = 2cosh\left(n\frac{L(u)}{2}\right),$$

wobei $L(u)$ die Länge der Geodätischen u darstellt.

Bemerkung 2.3.2 *Im weiteren betrachten wir geschlossene Geodätische als orientierungslos und primitiv, also mit nur einem Umlauf.*

Der Rest des Kapitels beschäftigt sich im wesentlichen mit der Hauptkongruenzgruppe der Stufe 3, also $\Gamma(3)$. Ein Fundamentalbereich F_3 von $\Gamma(3)$ wird in Abbildung 2.2 *(S. 44)* dargestellt. Sei also :

$$S = \mathbb{H}^2/\Gamma(3),$$

die Sphäre mit vier Löchern und

$$\pi : \mathbb{H}^2 \to S$$

die Projektion der hyperbolischen Ebene auf die punktierte Sphäre (siehe Abbildung 2.3 *(S. 45)*) . Sei nun $\gamma \in \Gamma(3)$ mit $|tr(\gamma)| > 2$. Somit ist γ hyperbolisch und besitzt die beiden reellen Fixpunkte, ζ_γ und ζ'_γ. Sei A_γ die hyperbolische Gerade durch ζ_γ und ζ'_γ (Siehe Abbildung 2.2 *(S. 44)*). Über die Projektion π wird A_γ auf die (nicht notwendig einfach) geschlossene Geodätische $\pi(A_\gamma)$ abgebildet. Umgekehrt entspringt jede geschlossene Geodätische v einer solchen Projektion.

Bevor wir uns der Frage zuwenden, wann eine Projektion einfach geschlossen ist, sollte man zunächst $\gamma \in \Gamma(N)$ mit einer speziellen Bauart betrachten, mit denen man, auf eine etwas unkonventionelle Weise, Matritzen in $\Gamma(3)$ konstruieren kann.

$$\gamma = \begin{pmatrix} 1+aN & bN \\ cN & 1+dN \end{pmatrix}, \text{mit} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Wegen $\gamma \in \Gamma(N)$, sollte gelten:

$$det(\gamma) = 1 = 1 + aN + dN + N^2\underbrace{(ad-bc)}_{=1}$$
$$\Rightarrow d = -a - N.$$

Also hat γ die Form :

$$\gamma = \begin{pmatrix} 1+aN & bN \\ cN & 1-aN-N^2 \end{pmatrix}.$$

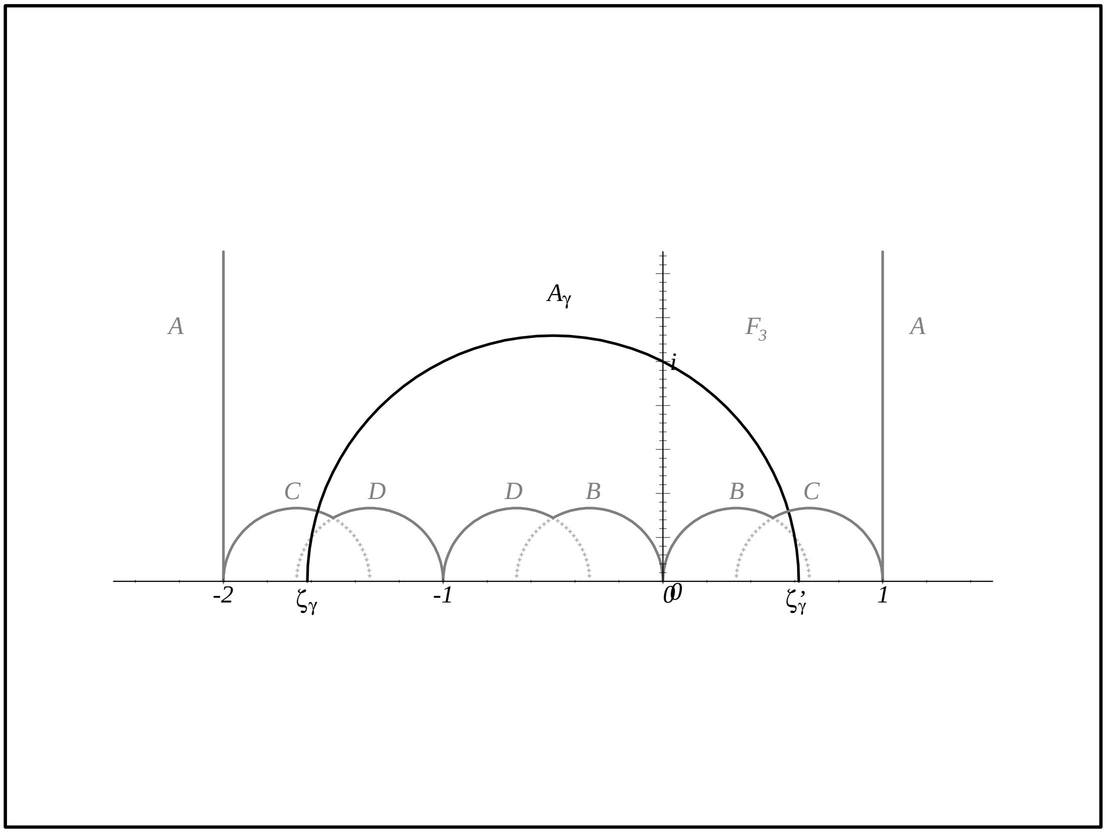

Abbildung 2.2: Hyperbolische Gerade A_γ durch die Punkte ζ_γ und ζ'_γ und ein Fundamentalbereich F_3 von $\Gamma(3)$ mit den Identifikationen : AA BB CC und DD.

Darüber hinaus gilt:

$$|tr(\gamma)| = |2 - N^2|,\ N > 2.$$

Somit ist ein solches γ hyperbolisch. Sei p Markoffzahl und (p, q, r) definiert wie in (1.2.5 *(S. 19)*). Man kann nun die Einträge der Matrix wie folgt definieren:

$$N = 3p\ ,\ a = -q\ ,\ b = 3q - r\ ,\ c = p$$
$$(\Rightarrow d = q - 3p).$$

Mit der Wahl dieser Matrixeinträge hat γ_{3p} die Form :

$$\gamma_{3p} = \begin{pmatrix} 1 - 3pq & 9pq - 3pr \\ 3p^2 & 1 + 3pq - 9p^2 \end{pmatrix}.$$

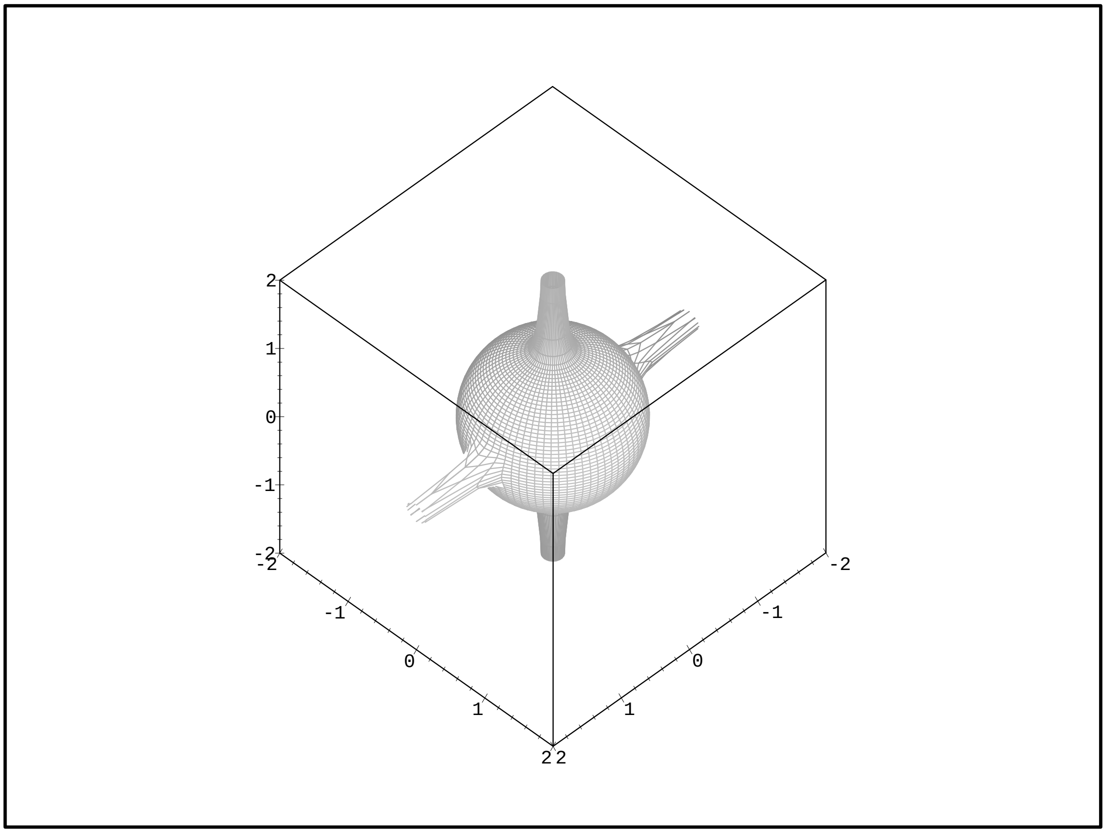

Abbildung 2.3: $S = \mathbb{H}^2/\Gamma(3)$.

Die Definition von N macht Sinn, da $\Gamma(3p)$ Normalteiler von $\Gamma(3)$ ist. Es ist :

$$\begin{aligned} ad - bc &= -q^2 + 3pq - 3pq + rp \\ &= -q^2 + rp \\ &= 1 \qquad \text{lt.(1.2.5 (}S.\ 19\text{))} \end{aligned}$$

Somit gilt : $\gamma_{3p} \in \Gamma(3p) \lhd \Gamma(3)$.

Nun kann man die Fixpunkte $\zeta_{\gamma_{3p}}$ und ${\zeta'}_{\gamma_{3p}}$ von γ_{3p} berechnen :

$$\begin{array}{rcl} & \gamma_{3p}(z) = z & \\ \Leftrightarrow & (1-3pq)z + 3pq - 3pr - z(3p^2z + 1 + 3pq - 9p^2) & = 0 \\ \Leftrightarrow & -3p^2z^2 + (1 - 3pq - 1 - 3pq + 9p^2)z + 9pq - 3pr & = 0 \\ \Leftrightarrow & -3p^2z^2 + 3p(3p-q)z + 3p(3q-r) & = 0 \\ \Leftrightarrow & \underbrace{pz^2 - (3p-q)z - (3q-r)}_{=f_p(z,1) \text{ vg.(2.2 } (S.\ 31)\text{)}} & = 0 \end{array}$$

Bemerkung 2.3.3 *Die reellen Fixpunkte $\zeta_{\gamma_{3p}}$ und $\zeta'_{\gamma_{3p}}$ der hyperbolischen Matrix*

$$\gamma_{3p} = \begin{pmatrix} 1-3pq & 9pq-3pr \\ 3p^2 & 1+3pq-9p^2 \end{pmatrix}$$

stimmen mit den Nullstellen ζ_p und ${\zeta'}_p$ der Markoff-Form

$$f_p(x,y) = px^2 - (3p-q)xy - (3q-r)y^2$$

überein (Siehe Abbildung 2.4 (S. 47)).

Kommen wir nun wieder zu den Geodätischen auf $\mathbb{H}^2/\Gamma(3)$. Bei Lehner/Sheingorn [9] findet sich ein Kriterium dafür, wann die Projektion $\pi(A_\gamma)$ einer hyperbolischen Geraden A_γ, mit reellen Fixpunkten ζ_γ und ${\zeta'}_\gamma$, einfach geschlossen ist. Dies führt uns zurück zum Markoffspektrum. Für ein $\theta \in \mathbb{R}$ sei :

$$\nu(\theta) := inf\left\{\kappa :\ \left|\theta - \frac{r}{s}\right|\ < \frac{\kappa}{s^2},\ \textit{für unendlich viele } r,s \in \mathbb{Z}\right\}$$

und

$$\mathfrak{M}_{\mathfrak{s}} = \left\{\nu(\theta) :\ \nu(\theta) > \frac{1}{3};\ \theta \in \mathbb{R}\right\}$$

das Markoffspektrum.

Theorem 2.3.4 *Sei $\gamma \in \Gamma(3)$ hyperbolisch. $\pi(A_\gamma)$ ist genau dann einfach, wenn $\nu(\zeta_\gamma) = \nu({\zeta'}_\gamma) \in \mathfrak{M}_{\mathfrak{s}}$ gilt .*

Nun gilt aber, wegen Theorem 2.2.5 *(S. 39)* und Theorem 2.2.7 *(S. 41)* , für die Wurzeln ζ_p und ${\zeta'}_p$ einer Markoff-Form f_p, und damit für die gesamten Wurzeln θ, θ' der 'erweiterten' Äquivalenzklasse $[f_p]$:

$$\nu(\zeta_p) = \nu(\zeta'_p) = \nu(\theta) = \nu(\theta') \in \mathfrak{M}_{\mathfrak{s}}.$$

Damit ergibt sich zusammen mit Theorem 2.3.4 *(S. 46)* , daß alle

$$\gamma_{3p} = \begin{pmatrix} 1-3pq & 9pq-3pr \\ 3p^2 & 1+3pq-9p^2 \end{pmatrix}$$

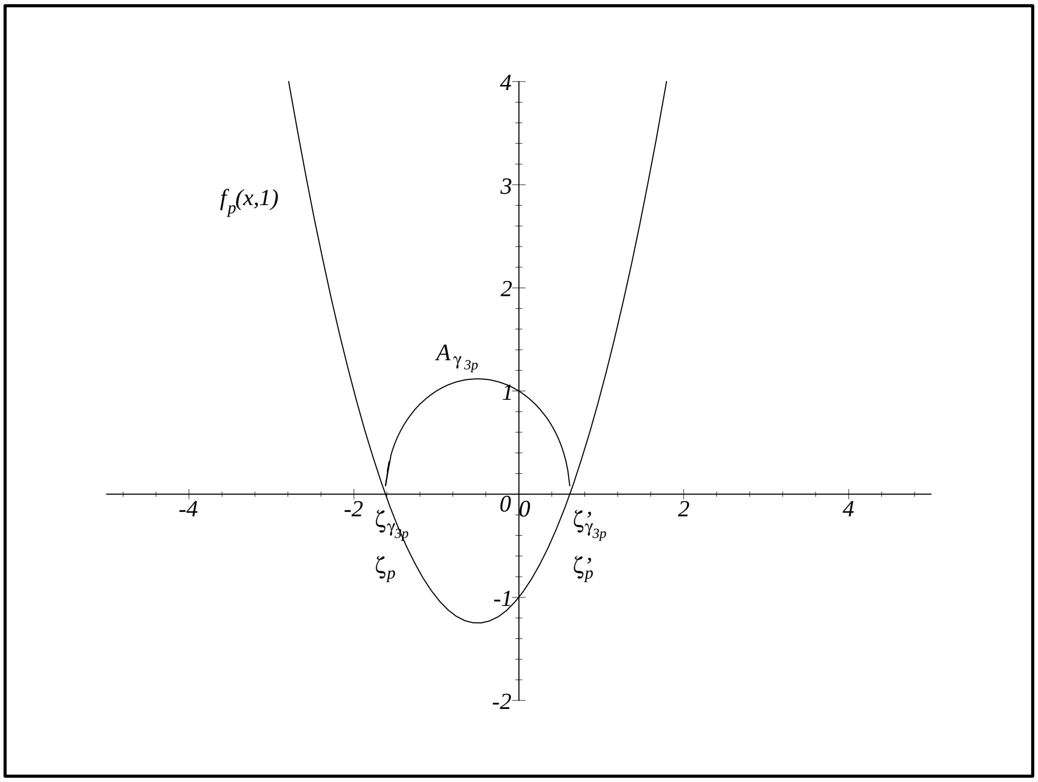

Abbildung 2.4: Markoff-Form $f_p(x,1)$ mit Nullstellen ζ_p und ζ'_p und hyperbolische Gerade $A_{\gamma_{3p}}$ mit Fixpunkten $\zeta_{\gamma_{3p}}$ und $\zeta'_{\gamma_{3p}}$.

mit einfach geschlossenen Geodätischen auf $\mathbb{H}^2/\Gamma(3)$ korrespondieren. Der Hauptsatz bei Lehner/Sheingorn [9] stellt eine Erweiterung dieses Sachverhalts, dar, und zwar eine Identifikation von Markoffzahlen mit dem Längenspektrum einfach geschlossener Geodätischer auf $\mathbb{H}^2/\Gamma(3)$.

Theorem 2.3.5 *Sei u eine einfach geschlossene Geodätische in $\mathbb{H}^2/\Gamma(3)$. Dann existiert eine Markoffzahl p, so daß :*

$$3p = 2cosh\left(\frac{L(u)}{2}\right),$$

wobei L(u) die Länge von u ist. Sei umgekehrt p Markoffzahl. Dann existiert eine einfach geschlossene Geodätische u in $\mathbb{H}^2/\Gamma(3)$, so daß :

$$3p = 2cosh\left(\frac{L(u)}{2}\right)$$

ist. Darüber hinaus sei :

$$w = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

eine Matrix, die mit einer geschlossenen Geodätischen u in $\mathbb{H}^2/\Gamma(3)$ korrespondiert. Die Geodätische u ist genau dann einfach, wenn

$$\gamma x^2 - (\alpha - \delta)xy - \beta y^2$$

Vielfaches einer Markoff-Form ist.

Kommen wir nun zu der Frage, welche Konsequenzen die Erfüllung bzw. die Nicht-Erfüllung der Eindeutigkeitsvermutung mit sich bringt. Für Markoff-Formen besteht die einzige Konsequenz, meines Wissens, in der Notation, und zwar darin, daß eine Markoff-Form, im Falle der Nicht-Erfüllung, $F_{(p,p_1,p_2)}$ statt F_p heißen muß. Im Kontext von arithmetischen Flächen ergeben sich weitreichendere Auswirkungen. Dazu muß man zunächst noch erweiterte Isometrieklassen definieren.

Definition 2.3.6 *Sei u eine einfach geschlossene Geodätische in $\mathbb{H}^2/\Gamma(3)$. Die* **erweiterte Isometrieklasse** *von u enthält eine einfach geschlossene Geodätische $v \subset \mathbb{H}^2/\Gamma(3)$ genau dann, wenn die Fläche einen (möglicherweise orientierungsumkehrenden) Automorphismus Φ besitzt, mit :*

$$\Phi(u) = v.$$

Nun kann man die Eindeutigkeitsvermutung im Rahmen von arithmetischen Flächen formulieren.

Bemerkung 2.3.7 *Die Eindeutigkeitsvermutung ist äquivalent zu der Vermutung, daß zwei einfach geschlossene Geodätische, mit derselben Länge, in derselben erweiterten Isometrieklasse liegen.*

Neben den Zusammenhängen von Markoffzahlen und Markoff-Formen wie auch arithmetischen Flächen, haben Markoffzahlen noch Bedeutung bei freien Halbgruppen, mit zwei Erzeugenden [17] und bei 4-Mannigfaltigkeiten [18]. Über die Auswirkungen der Eindeutigkeitsvermutung in diesen Bereichen sei auf Cohn [17] und Zagier [18] verwiesen. Darüber hinaus hat die Erfüllung der Vermutung Konsequenzen für die Abschätzung des Wachstums von Markoffzahlen (siehe Zagier [14]).

Kapitel 3

Abschätzungen von $q(p)$

In Abschnitt 1.2 *(S. 18)* , Theorem 1.2.8 *(S. 20)* , wurde gezeigt, daß ein Markofftripel (p,p_1,p_2) mit :

$$\varepsilon q \equiv \frac{p_1}{p_2} \equiv -\frac{p_2}{p_1} \; mod(p), \qquad \varepsilon = \pm 1$$

und

$$0 \leq q \leq \frac{p}{2} \; ,$$

bei eindeutiger Lösbarkeit von

$$q^2 \equiv -1 \; mod(p),$$

eindeutig durch p bestimmt ist. Im folgenden wird untersucht, welche Werte ein $q = q(p)$ überhaupt annehmen kann. Es wird sich zeigen, daß nur ein Bereich

$$0 \leq \zeta(p) \leq q \leq \xi(p) \leq \frac{p}{2}$$

für die Betrachtungen relevant ist, und somit schon aus der eindeutigen Lösbarkeit von

$$q^2 \equiv -1 \; mod(p)$$

für

$$\zeta(p) \leq q(p) \leq \xi(p)$$

folgt, daß (p,p_1,p_2) durch p eindeutig bestimmt ist. Eine Herleitung der unteren Schranke $\zeta(p)$ findet sich bei Schmutz [11].

Theorem 3.0.1 *Sei (p,p_1,p_2) ein Markofftripel und*

$$\zeta(p) = \frac{3p - \sqrt{5p^2-4}}{2} \; , \; \xi(p) = -p + \sqrt{2p^2-1}.$$

Sei weiter

$$Q(p) = \{n \in \mathbb{N} \; : \; \zeta(p) \leq \; n \leq \xi(p) \; , \; n^2 \equiv -1 \; mod(p)\} \; .$$

Ist

$$card\{Q(p)\} = 1,$$

so ist (p, p_1, p_2) *eindeutig durch* p *bestimmt.*

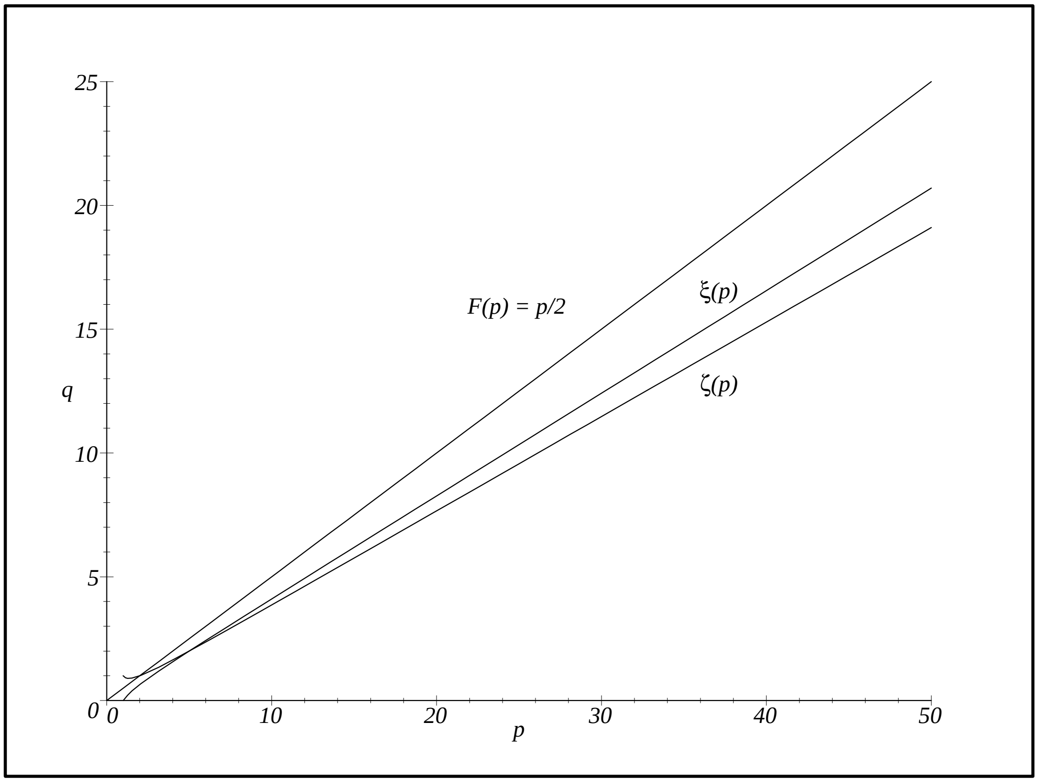

Abbildung 3.1: $\zeta(p) \leq\ q \leq \xi(p) \leq \frac{p}{2}$

Beweis :

In diesem Kapitel betrachten wir wieder nicht-normierte Markoff-Formen, also :

$$f_p(x,y) = px^2 - (3p-2q)xy - (3q-r)y^2$$

und

$$p = \mu(f_p) = inf\ \{\ |f_p(m,n)|\ :\ (m,n)\ \in \mathbb{Z} \times \mathbb{Z} \backslash (0,0)\}$$

Über $\mu(f_p)$ kann man einige Ungleichungen bezüglich (p,q,r) herleiten. Für den Punkt (0,1) gilt :

$$\begin{array}{rccll}
 & \mid f_p(0,1) \mid & = & \mid -(3q-r) \mid & \geq p \geq 0 \\
\text{Annahme :} & 3q-r & \leq & 0 & \\
\Rightarrow & 3q & \leq & r & \\
\text{lt. (1.2.5 } (S.\ 19) \text{)} & q^2+1 & = & rp & \\
\Rightarrow & q^2+1 & \geq & 3qp & \\
\text{lt. (1.5 } (S.\ 18) \text{)} & \frac{1}{2}p & \geq & q & \\
\Rightarrow & q^2+1 & \geq & 6q^2 & \text{Widerspruch} \quad \text{zu } q \in \mathbb{N}.
\end{array}$$

$$\Rightarrow -f_p(0,1) = 3q - r \geq p \geq 0. \tag{3.1}$$

Als nächstes kann man zeigen, daß $q \geq \zeta(p)$ gilt.

$$\text{Es ist } p \leq 3q - r \text{ und } pr - q^2 = 1 \tag{3.2}$$

$$\begin{array}{rccll}
\Rightarrow & p & \leq & 3q - \frac{1+q^2}{p} & \\
\Leftrightarrow & 0 & \geq & q^2 - 3qp + 1 + p^2 & =: \ P(q) \\
\Rightarrow & q_{+/-} & = & \frac{3p \pm \sqrt{5p^2-4}}{2} &
\end{array}$$

$$\text{wg. } P(0) = 1 + p^2 > 0 \text{ und } 0 < q_- < q_+ \text{ folgt :}$$

$$q \geq \frac{3p - \sqrt{5p^2-4}}{2} =: \zeta(p). \tag{3.3}$$

Betrachten wir nun die obere Schranke :

$$\begin{array}{rccl}
\text{Es ist} & |f_p(-5,-2)| & = & |-5p + 8q + 4r| \\
 & & \geq & p \geq 0 \\
\text{Annahme} & p & \leq & -5p + 8q + 4r \\
\Leftrightarrow & 0 & \geq & 2 \underbrace{(p-2q)}_{\geq 0 \ lt.\ (\ 1.5\ (S.\ 18)\ )} + (p-2r) \\
\Rightarrow & p & \leq & 2r \\
\text{lt. (3.1 } (S.\ 51) \text{)} & p & \leq & 3q - r \\
\Rightarrow & p & \leq & 3q - \frac{1}{2}p \\
 & & & \text{Widerspruch zu (1.5 } (S.\ 18) \text{)}
\end{array}$$

$$\Rightarrow f_p(-5,-2) = -5p + 8q + 4r \leq -p$$

$$\Rightarrow 2q + r \leq p.$$

Nun kann man $\xi(p)$ wie oben berechnen.

$$\begin{array}{rccll}
 & p & \geq & 2q + r \ , \ q^2 + 1 & = \quad pr \\
\Rightarrow & p & \geq & 2q + \frac{1+q^2}{p} & \\
\Leftrightarrow & 0 & \geq & q^2 + 2qp + 1 - p^2 & =: \ P(q) \\
\Rightarrow & q_{+/-} & = & -p \pm \sqrt{2p^2-1} &
\end{array}$$

wg. $P(0) = 1 - p^2 \leq 0$ und $q_- < 0 < q_+$ folgt :

$$0 < q \leq -p + \sqrt{2p^2 - 1} =: \xi(p).$$

Insgesamt gilt für jede Lösung :

$$\begin{array}{rl} & \pm q \equiv \frac{p_1}{p_2} \; mod(p) \\ \text{mit} & q^2 \equiv -1 \; mod(p) \\ \text{erfüllt} & \zeta(p) \leq q \leq \xi(p). \end{array}$$

Zusammen mit Theorem 1.2.8 *(S. 20)* folgt die Aussage. □

Beispiel 3.0.2 *Mit diesen Grenzen kann man nun die Eindeutigkeit für Beispiel 1.4.3 (S. 25) , mit $p = 1325$ zeigen, bei dem sowohl q als auch $q_\pm$, jeweils zwei Lösungen der Kongruenzen besaßen. Die Kongruenz $q^2 \equiv -1 \; mod(1325)$ hatte die Lösungen :*

$$q' = 182 \quad \text{und } q = 507.$$

Innerhalb der Grenzen ζ und ξ hat die Kongruenz die eindeutige Lösung q :

$$q' < \zeta(1325) = 506.1 < q < \xi(1325) = 548.8 \; .$$

Beispiel 3.0.3 *Allerdings gibt es Zahlen $n \in \mathbb{N}$ mit:*

$$card Q(n) > 1, \text{ wie zB.}$$

$$\begin{array}{rcl} Q(1130) & = & \{437, 467\}, \; \zeta \; = \; 431.6, \; \xi \; = \; 468.0, \\ Q(2005) & = & \{782, 822\}, \; \zeta \; = \; 765.8, \; \xi \; = \; 830.4. \end{array}$$

Andererseits sind 1130 und 2005 keine Markoffzahlen.

Bei Frobenius [4] findet sich folgende Abschätzung :

Theorem 3.0.4 *Die Werte $\zeta(p)$ und $\xi(p)$ werden unendlich oft angenommen und es gilt :*

$$\frac{1}{2}(3 + \sqrt{5}) > \frac{p}{q} > (1 + \sqrt{2}). \tag{3.4}$$

Für den nachfolgenden Beweis möchte ich die Notation etwas vereinfachen. Es sei $(p, p_1, 1) = \{(p_{i+1}, p_i, 1)_{i \in \mathbb{N}}\}$ die Kette bezüglich 1, und $(p, 2, p_2) = \{(p_{i+1}, p_i, 2)_{i \in \mathbb{N}}\}$ die Kette bezüglich 2, mit $p > p_1$ bzw. $p > p_2$.

Beweis :

1.) Für die Kette $(p, p_1, 1)$ gilt :

$$\zeta(p) = q(p) \; , \; p > p_1.$$

Wegen $\underbrace{p = 3p_1 \cdot 1 - p_1'}_{(siehe->\ (\ 1.3\ (S.\ 14)\ ))}$ und $p_1 > p_1'$ folgt :

$$\begin{array}{rccc} & \frac{1}{2}p & \geq & p_1 \\ \text{Es ist} & q & \equiv & \frac{p_1}{1}\ mod(p) \\ \Rightarrow & q & = & p_1 \leq \frac{1}{2}p \\ \text{wg.} & q^2+1 & = & rp \\ \text{folgt} & p_1^2+1 & = & rp. \end{array}$$

Nun erfüllt $(p, p_1, 1)$ die Gleichung :

$$\begin{array}{rccc} & p^2+p_1^2+1 & = & 3pp_1 \cdot 1 \\ \Rightarrow & 3pp_1 - p^2 & = & rp \\ \Leftrightarrow & 3p_1 - p & = & r \\ \Leftrightarrow & 3q - r & = & p. \end{array}$$

Somit gilt in Ungleichung (3.2 *(S. 51)*) Gleichheit, also auch in (3.3 *(S. 51)*) . Daraus folgt $\zeta(p) = q(p)$ für die Kette $(p, p_1, 1)$ und $\zeta(p)$ ist nicht verbesserbar.

2.) Für die Kette $(p, 2, p_2)$ gilt $\xi(p) = q(p)$. Mit dem gleichen Argument wie oben ist zu zeigen, daß :

$$\begin{array}{rccc} & p & = & 2q+r \\ \text{Also} & q & \equiv & \frac{2}{p_2}\ mod(p) \\ \Leftrightarrow & -2q & \equiv & p_2\ mod(p) \\ \text{lt. (1.5 } (S.\ 18) \text{)} & 0 & \leq & p-2q \end{array}$$

$$\Rightarrow p - 2q = p_2 \tag{3.5}$$

$$\begin{array}{rccc} \Rightarrow & q & = & \frac{p-p_2}{2} \\ \text{Nun ist} & q^2+1 & = & pr \\ \Leftrightarrow & p^2-2pp_2+p_2^2+4 & = & 4pr \\ \Leftrightarrow & \underbrace{p^2+p_2^2+4}_{=3\cdot 2pp_2} & = & 4pr+2pp_2 \\ \Rightarrow & p_2 & = & r. \end{array}$$

Zusammen mit (3.5 *(S. 53)*) folgt die Aussage.

3.) Nun ergibt sich für $(p, p_1, 1)$ und $q = q(p)$ aus 1.) :

$$\begin{array}{rcll} \frac{p}{q} & = & \frac{p}{\frac{1}{2}(3p-\sqrt{5p^2-4})} & \\ & = & \frac{1}{\frac{3}{2}-\frac{1}{2}\sqrt{5-\frac{4}{p^2}}} & \text{monoton steigende Folge} \\ & \xrightarrow{p\to\infty} & \frac{1}{\frac{1}{2}(3-\sqrt{5})} & \\ & = & \frac{1}{2}(3+\sqrt{5}). & \end{array}$$

Die Rechnung für die andere Schranke ist entsprechend. □

Die Beweise der Abschätzungen von Theorem 3.0.1 *(S. 49)* und Theorem 3.0.4 *(S. 52)* basieren beide auf den Überlegungen von Frobenius [4], der damit allerdings nur die etwas gröbere Abschätzung 3.4 *(S. 52)* gezeigt hat. Die Grenzen $\zeta(p)$ und $\xi(p)$ tauchen bei Frobenius in einem anderen Zusammenhang auf. Die Zahlen der Ketten sind vielleicht aus einem anderen Kontext bekannt.

Bemerkung 3.0.5 *Die Elemente der Kette $\{(1, p_i, p_{i+1})_{i \in \mathbb{N}}\}$ sind Fibonacci Zahlen und die der Kette $\{(2, p_i, p_{i+1})_{i \in \mathbb{N}}\}$ sind Pellsche bzw. Duprésche Zahlen.*

Bemerkung 3.0.6 *Die Ungleichung aus Theorem 3.0.4 (S. 52) läßt sich, mit Theorem 3.0.1 (S. 49), in folgender Form darstellen. Sei :*

$$\Upsilon(p) := \frac{3-\sqrt{5}}{2}p \text{ und } \Xi(p) := (-1+\sqrt{2})p,$$

dann ist :

$$\Upsilon(p) < \zeta(p) \leq q \leq \xi(p) < \Xi(p)$$

und es gilt :

$$|\Upsilon(p) - \zeta(p)| < 1 \text{ und } |\Xi(p) - \xi(p)| < 1.$$

Da man mit der Ungleichung $q \in \mathbb{N}$ abschätzt, entsteht nur dann ein Fehler , wenn eine Zahl $q' \in \mathbb{N}$ existiert, die der Kongruenz :

$$q'^2 \equiv -1 \; mod(p)$$

genügt und für die gilt :

$$\Upsilon(p) < q' < \zeta(p) \text{ oder } \xi(p) < q' < \Xi(p).$$

Kommen wir nun noch einmal zum Beispiel 1.4.3 *(S. 25)* , bei dem für die Markoffzahl $p = 9077$ die drei Kongruenzen jeweils zwei Lösungen besaßen und damit keine Aussage über die Eindeutigkeitsvermutung für das p gemacht werden konnte. Versucht man nun, die Grenzen $\xi(9077)$ und $\zeta(9077)$ zu berechnen, so stellt man schnell fest, daß dabei Zwischenergebnisse entstehen, die für normale Computerprogramme zu groß sind (long integer), so daß man $\xi(9077)$ und $\zeta(9077)$ auf numerischem Weg ermitteln müßte. Mit den Grenzen $\Upsilon(9077)$ und $\Xi(9077)$ kann man nun die Eindeutigkeitsvermutung für $p = 9077$ einfach zeigen.

Beispiel 3.0.7 *In Beispiel 1.4.3 (S. 25) besaß die Kongruenz $q^2 \equiv -1 \; mod(9077)$, für die Markoffzahl $p = 9077$, die Lösungen :*

$$q' = 2216 \quad \text{und } q = 3468.$$

Innerhalb der Grenzen $\Upsilon(9077)$ *und* $\Xi(9077)$ *hat die Kongruenz die eindeutige Lösung* q *:*

$$q' < \Upsilon(1325) = 3467.1 < q < \Xi(1325) = 3759.8 \ .$$

Neben den bisherigen Überlegungen bezüglich der Eindeutigkeitsvermutung kann man versuchen, mit dem Computer Markoffzahlen zu berechnen, um möglicherweise einen Widerspruch zur Vermutung zu finden. Dies bietet sich insofern an, da man wegen :

$$(p, p_1, p_2) \text{ mit } p > max(p_1, p_2)$$

$$\text{und } p_2' = 3pp_1 - p_2 \ , \ p_1' = 3pp_2 - p_1 \text{ vgl. } 1.3 \ \textit{(S. 14)}$$

einen genauen Überblick über die Markoffzahlen hat. Die ersten Berechnungen machten 1971 D. Rosen und G.S Patterson Jr. [13], die 30-stellige Markoffzahlen berechneten. A. Baragar [15] testete 1996 140-stellige Markoffzahlen. Ich selber habe 140-stellige Markoffzahlen berechnet und konnte die in Baragar [15] angegebene Anzahl von 18906 Markoffzahlen und die Aussage, daß bis dahin kein Widerspruch zur Eindeutigkeitsvermutung besteht, bestätigen. † Die umfangreichsten Berechnungen stellte D. Zagier [14] an, dessen Datenmaterial bis 10^{1300} reicht und die Vermutung bis dorthin bestätigte, was die Richtigkeit sehr wahrscheinlich macht.

†Leider passen 140-stellige Zahlen nicht auf die Titelseite, deshalb sind dort die 74 schönsten 100-stelligen Markoffzahlen zu sehen.

Literaturverzeichnis

[1] A. Hurwitz. *Über eine unbestimmte Aufgabe der Analysis* (1905), Archiv der Mathematik und Physik, Reihe 3, Bd. **11**, S. 186.

[2] A. Markoff. *Sur les formes binaires indéfines.* (1879), Mathematische Annalen **15**, S. 381-406.

[3] A. Markoff. *Sur les formes binaires indéfines. (Second mémoire)* (1880), Mathematische Annalen **17**, S. 379-399.

[4] G. Frobenius. *Über die Markoffschen Zahlen.* (1968), Gesammelte Abhandlungen, Bd. **3**, Springer , Berlin Heidelberg New York, S. 598-627.

[5] J. Cassels. *An introduction to Diophantine approximation.* (1959), Cambrige, Cambrige Univ. Press.

[6] Remak *Über indefinite binäre quadratische Minimal formen.* (1924) Math. Annalen **92** s.155-182

[7] H. Cohn. *Approch to Markoff's minimal forms through modular functions.* (1955), Annals of Math. **61**, S. 1-12.

[8] H. Cohn. *Approch to Markoff's minimal forms by geodesics on a perforated torus.* (1971), Annals of Math. **18**, S. 125-136.

[9] J. Lehner/ M. Sheingorn. *Simple closed geodesics on* $\Gamma(3)$ *arise from the Markoff spectrum.* (1984), Bulletin AMS **11**, S.359-362.

[10] A. Haas. *Diophantine approximation on hyperbolic Riemann surface.* (1986), Acta Math. **156**, S. 33-82.

[11] P. Schmutz. *Systoles of arithmetic surfaces and the Markoff spectrum.*

[12] P. Buser. *Geometry and spectra of compact Riemann surfaces.* (1992), Birkhäuser, Boston Basel Berlin.

[13] D. Rosen/ G. S. Patterson Jr. *Some Numerical Evidence Concerning the Uniqueness of the Markov Numbers.* (1971), Mathematics of computation, Vol. **25**, Number 116, S. 919-921.

[14] D. Zagier. *On the Number of Markoff Numbers Below a Given Bond.* (1982), Mathmatics of computation, Vol. **39**, Number 160, S. 709-723.

[15] A. Baragar. *On the unicity conjectuere for Markoff Numbers.* (1996), Canadian Math. Bulletin Vol.**39**(1), S. 3-9.

[16] R. C. Gunning *Lectures on Modular Forms* (1962), Princeton University Press.

[17] H. Cohn *Markoff numbers and primitive words* (1972), Math. Ann. v.196 S.8-22.

[18] F. Hirzebruch/ D. Zagier *The Atiyah-Singer Theorem and Elementary Number Theory* (1974), Publish or Perish, Boston, Mass. Chap. 8

[19] T. W. Cusick/M. E. Flahive *The Markoff and Lagrange Spectra* (1989), Mathematical surveys and monographs, No. 30.