A N W E N D U N G E N

D E R

S K O L E M S C H E N M E T H O D E

Diplomarbeit zur Erlangung des Mag.rer.nat.
eingereicht von Thomas Backmeister
an der Universität Innsbruck
im Mai 1987

Begutachter: Univ.Doz. Dr.Kurt Girstmair

I N H A L T S V E R Z E I C H N I S Seite

Bezeichnungen

$\mathbb{Z}$	Ring der ganz-rationalen Zahlen
$\mathbb{Q}$	Körper der rationalen Zahlen
K	ein algebraischer Zahlkörper
$\mathfrak{o}_K$	Ring der ganzen algebraischen Zahlen in K
$\mathbb{Z}_p$	Ring der ganzen p-adischen Zahlen über $\mathbb{Q}$
$\mathbb{Q}_p$	Körper der p-adischen Zahlen über $\mathbb{Q}$
$\mathfrak{o}_{\mathfrak{p}}$	Ring der ganzen $\mathfrak{p}$-adischen Zahlen über K
$K_{\mathfrak{p}}$	Körper der $\mathfrak{p}$-adischen Zahlen über K
$\mathbb{Z}_g$	Ring der ganzen g-adischen Zahlen über $\mathbb{Q}$
$\mathbb{Q}_g$	Ring der g-adischen Zahlen über $\mathbb{Q}$
$\mathfrak{o}_{\mathfrak{a}}$	Ring der ganzen $\mathfrak{a}$-adischen Zahlen über K
$K_{\mathfrak{a}}$	Ring der $\mathfrak{a}$-adischen Zahlen über K
$\mathbb{Z}_g^{\times}$	Gruppe der Einheiten in $\mathbb{Z}_g$
$\mathfrak{o}_{\mathfrak{a}}^{\times}$	Gruppe der Einheiten in $\mathfrak{o}_{\mathfrak{a}}$
$\mathfrak{o}_{\mathfrak{p}}[[X_1,\ldots,X_n]]$	Potenzreihenring über $\mathfrak{o}_{\mathfrak{p}}$ in den Unbestimmten $X_1,\ldots,X_n$
$\mathfrak{o}_{\mathfrak{p}}[X_1,\ldots,X_n]$	Polynomring über $\mathfrak{o}_{\mathfrak{p}}$ in den Unbestimmten $X_1,\ldots,X_n$
$\overline{\mathfrak{o}_{\mathfrak{p}}[X_1,\ldots,X_n]}$	topologische Hülle von $\mathfrak{o}_{\mathfrak{p}}[X_1,\ldots,X_n]$ in $\mathfrak{o}_{\mathfrak{p}}[[X_1,\ldots,X_n]]$ bez. $\mathfrak{p}$-Topologie

Eine Abkürzung: Lit. = Literaturverzeichnis

I. E I N L E I T U N G

In dieser Arbeit geht es um die Darstellung einer von dem norwegischen Mathematiker Thoralf A. Skolem (1887 - 1963) in den Jahren 1933 - 1937 entwickelten Methode zur Lösung diophantischer Gleichungen eines bestimmten Typus.

Diese Methode wird heute als Skolemsche (p-adische) Methode bezeichnet. Wie der Name schon andeutet, stützt sie sich wesentlich auf die Theorie der p-adischen Zahlen und deren Funktionen. Somit gebe ich zunächst einen kurzen Überblick über den Aufbau der p-adischen Zahlen, wobei ich auf Beweise verzichte. Die Definitionen und Behauptungen entnahm ich den Werken 3, 10 und 14 des Literaturverzeichnisses.

1) p-adische Grundlagen

Sei K ein algebraischer Zahlkörper.
Für den Ring $\mathfrak{O}_K$ der ganzen algebraischen Zahlen in K existiert eine sogenannte Divisorentheorie. Darunter versteht man einen Homomorphismus $\alpha \longrightarrow \langle\alpha\rangle$ von $\mathfrak{O}_K \setminus \{0\}$ in eine multiplikative Halbgruppe $\mathfrak{J}$ mit eindeutiger Primfaktorzerlegung, der folgenden drei Bedingungen genügt:

1) β/α in $\mathfrak{O}_K \setminus \{0\} \Longleftrightarrow \langle\beta\rangle/\langle\alpha\rangle$ in $\mathfrak{J}$ für alle $\alpha, \beta \in \mathfrak{O}_K \setminus \{0\}$
2) $\mathfrak{a}/\langle\alpha\rangle$ und $\mathfrak{a}/\langle\beta\rangle$ für ein $\mathfrak{a} \in \mathfrak{J} \Rightarrow \mathfrak{a}/\langle\alpha+\beta\rangle$ für alle $\alpha, \beta \in \mathfrak{O}_K$
3) Für alle $\mathfrak{a}, \mathfrak{b} \in \mathfrak{J}$ mit $\{\alpha \in \mathfrak{O}_K;\ \mathfrak{a}/\langle\alpha\rangle\} = \{\beta \in \mathfrak{O}_K;\ \mathfrak{b}/\langle\beta\rangle\}$ $\Rightarrow \mathfrak{a} = \mathfrak{b}$

Die Elemente $\mathfrak{a}$ von $\mathfrak{J}$ werden als Divisoren von $\mathfrak{O}_K$ bezeichnet. Divisoren der Form $\langle\alpha\rangle, \alpha \in \mathfrak{O}_K \setminus \{0\}$, heißen Hauptdivisoren. $0 \in \mathfrak{O}_K$ wird per Definition durch alle Divisoren aus $\mathfrak{J}$ geteilt.

Zwei Hauptdivisoren $\langle\alpha\rangle$ und $\langle\beta\rangle$ sind genau dann gleich, wenn α und β in $\mathcal{O}_K$ assoziiert sind. Eine Divisorentheorie ist bis auf Isomorphie der entsprechenden Halbgruppen eindeutig gegeben. Für den algebraischen Zahlkörper K ist $\mathfrak{D}$ isomorph zur Halbgruppe aller von 0 verschiedenen Ideale von $\mathcal{O}_K$.

Eine Abbildung $\nu: K \longrightarrow \mathbb{Z} \cup \{\infty\}$ heißt Exponent des Körpers K, wenn folgende drei Eigenschaften erfüllt sind:

1) $\nu(\alpha) = \infty \iff \alpha = 0$

2) $\nu(\alpha\cdot\beta) = \nu(\alpha) + \nu(\beta)$ für alle $\alpha,\beta \in K$

3) $\nu(\alpha+\beta) \geq \min\{\nu(\alpha),\nu(\beta)\}$ für alle $\alpha,\beta \in K$

Jeder Primdivisor $\mathfrak{p}$ von $\mathcal{O}_K$ bestimmt durch

$$\nu_{\mathfrak{p}}(\alpha) := \begin{cases} \max\{n\in\mathbb{Z};\ \mathfrak{p}^n/\langle\alpha\rangle\} & \text{für } \alpha\neq 0 \\ \infty & \text{für } \alpha = 0 \end{cases}$$

einen eindeutig gegebenen ($\mathfrak{p}$-adischen) Exponenten auf K, wobei zwei verschiedene Primdivisioren verschiedene Exponenten bestimmen.

Mit einem beliebigen Divisor $\mathfrak{a}$ läßt sich ebenfalls ein "Exponent" definieren, der anstatt Bedingung 2 der schwächeren Bedingung

2') $\nu_{\mathfrak{a}}(\alpha\cdot\beta) \geq \nu_{\mathfrak{a}}(\alpha) + \nu_{\mathfrak{a}}(\beta)$ für alle $\alpha,\beta \in K$

genügt.

Ein Exponent $\nu_{\mathfrak{p}}$ definiert eine ($\mathfrak{p}$-adische) Bewertung auf K: Das ist eine Abbildung

$$|\ |_{\mathfrak{p}} : K \longrightarrow \mathbb{R}^+ \cup \{0\}$$
$$\alpha \longrightarrow |\alpha|_{\mathfrak{p}} := \rho^{-\nu_{\mathfrak{p}}(\alpha)},$$

wobei ρ eine reelle Zahl größer als 1 ist, und die Eigenschaften 1), 2), 3) erfüllt sind:

1) $/\alpha/_{\mathfrak{p}} = 0 \iff \alpha = 0$

2) $/\alpha\cdot\beta/_{\mathfrak{p}} = /\alpha/_{\mathfrak{p}} \cdot /\beta/_{\mathfrak{p}}$ für alle $\alpha,\beta \in K$

3) $/\alpha\pm\beta/_{\mathfrak{p}} \leq \max\{/\alpha/_{\mathfrak{p}}, /\beta/_{\mathfrak{p}}\}$ für alle $\alpha,\beta \in K$

(wegen 3) heißt die Bewertung nicht-archimedisch).

Verwendet man statt eines Primdivisors einen beliebigen Divisor $\mathfrak{a}$, so schwächt sich 2) ab zu

2') $/\alpha\beta/_{\mathfrak{a}} \leq /\alpha/_{\mathfrak{a}} \cdot /\beta/_{\mathfrak{a}}$ für alle $\alpha,\beta \in K$

Mit Hilfe einer Bewertung läßt sich K zu einem eindeutig bestimmten Körper bzw. Ring vervollständigen, je nachdem ob ein Primdivisor oder ein gewöhnlicher Divisor zugrunde liegt.

Ich beschreibe den Vervollständigungsprozeß an einem gewöhnlichen Divisor $\mathfrak{a} \in \mathfrak{D}$:

Eine Folge $\{\alpha_n\}_{n\in\mathbb{N}}$ von Zahlen aus K heißt ($\mathfrak{a}$-adische) Nullfolge (in Zeichen: $\mathfrak{a}\text{-}\lim\limits_{n\to\infty}\alpha_n = 0$),

wenn $\lim\limits_{n\to\infty} /\alpha_n/_{\mathfrak{a}} = 0$.

$\{\alpha_n\}_{n\in\mathbb{N}}$ heißt ($\mathfrak{a}$-adische) Cauchyfolge, wenn

$$\mathfrak{a}\text{-}\lim_{\substack{n\to\infty\\ m\to\infty}} (\alpha_n-\alpha_m) = \lim_{\substack{n\to\infty\\ m\to\infty}} /\alpha_n-\alpha_m/_{\mathfrak{a}} = 0.$$

Das heißt: für alle $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$, so daß für alle $n \geq N$, $m \geq N$ $/\alpha_n-\alpha_m/_{\mathfrak{a}} < \varepsilon$.

Auf der Menge der Cauchyfolgen aus K kann folgendermaßen eine Äquivalenzrelation eingeführt werden:

$\{\alpha_n\}_{n\in\mathbb{N}} \sim \{\beta_n\}_{n\in\mathbb{N}} :\Longleftrightarrow \{\alpha_n-\beta_n\}_{n\in\mathbb{N}}$ ist eine Nullfolge.

Die Menge aller Äquivalenzklassen $\mathfrak{U}$-adischer Cauchyfolgen in K bezeichnen wir mit $K_{\mathfrak{U}}$.

Sind $\{\alpha_n\}_{n\in\mathbb{N}}$ und $\{\beta_n\}_{n\in\mathbb{N}}$ beliebige Vertreter zweier Äquivalenzklassen $a,b \in K_{\mathfrak{U}}$, so werden Addition und Multiplikation in $K_{\mathfrak{U}}$ eindeutig durch

$$a+b := c_1 \in K_{\mathfrak{U}} \text{ mit } \{\alpha_n+\beta_n\}_{n\in\mathbb{N}} \in c_1$$

$$a\cdot b := c_2 \in K_{\mathfrak{U}} \text{ mit } \{\alpha_n\cdot\beta_n\}_{n\in\mathbb{N}} \in c_2$$

definiert.
Dadurch wird $K_{\mathfrak{U}}$ zu einem kommutativen Ring und $K_{\mathfrak{P}}$ zu einem Körper, genannt $\mathfrak{P}$-adischer Zahlkörper über K, wenn $\mathfrak{P}$ ein Primdivisor ist.

In ihm ist K bis auf Isomorphie enthalten (man identifiziert $\alpha \in K$ mit der Äquivalenzklasse $a \in K_{\mathfrak{U}}$, die die konstante Folge $(\alpha,\alpha,\ldots)$ enthält).

Die Bewertung $/\ /_{\mathfrak{U}}$ läßt sich auf $K_{\mathfrak{U}}$ in natürlicher Weise fortsetzen:

$$\{\alpha_n\}_{n\in\mathbb{N}} \in a \in K_{\mathfrak{U}},\quad /a/_{\mathfrak{U}} := \varrho^{-\lim\limits_{n\to\infty} \nu_{\mathfrak{U}}(\alpha_n)}$$

Fügt man zu $K_{\mathfrak{U}}$ erneut Äquivalenzklassen von Cauchyfolgen aus $K_{\mathfrak{U}}$ hinzu, so läßt sich zeigen, daß dabei kein größerer Ring als $K_{\mathfrak{U}}$ entsteht. Deshalb bezeichnet man $K_{\mathfrak{U}}$ als die Vervollständigung von K bezüglich des Divisors $\mathfrak{U}$.

Der Teilring $O_{\mathfrak{U}} := \{a \in K_{\mathfrak{U}} ;\ /a/_{\mathfrak{U}} \leq 1\}$ von $K_{\mathfrak{U}}$ heißt Ring der ganzen $\mathfrak{U}$-adischen Zahlen über K (die Elemente von $K_{\mathfrak{U}}$ heißen $\mathfrak{U}$-adische Zahlen über K).

Die Einheitengruppe $\underline{\mathfrak{o}_{\mathfrak{U}}^{\times}}$ von $\mathfrak{o}_{\mathfrak{U}}$ ist dann gegeben durch

$$\mathfrak{o}_{\mathfrak{U}}^{\times} = \{a \in \mathfrak{o}_{\mathfrak{U}} \; ; \; /a/_{\mathfrak{U}} = 1\}.$$

$K_{\mathfrak{U}}$ ist vermöge der Metrik $d(a,b) := /a-b/_{\mathfrak{U}}$ ein metrischer Raum. In ihm ist $\mathfrak{o}_{\mathfrak{U}}$ offen-abgeschlossen und kompakt. $\mathfrak{o}_K$ ist eine dichte Teilmenge von $\mathfrak{o}_{\mathfrak{U}}$. Ist $\mathfrak{p}$ ein Primdivisor von $\mathfrak{o}_K$, so ist $\mathfrak{o}_{\mathfrak{p}}$ ein Integritätsbereich und Quot $(\mathfrak{o}_{\mathfrak{p}}) = K_{\mathfrak{p}}$.

$\mathfrak{o}_{\mathfrak{p}}$ besitzt als Ring mit Divisorentheorie nur den Primdivisor $\mathfrak{p}$ (die zu $\mathfrak{o}_{\mathfrak{p}}$ gehörende Divisorenhalbgruppe ist $\mathfrak{H} = \{\mathfrak{p}^n; n \in \mathbb{N}_0\}$).

Ist $a \in \mathfrak{o}_{\mathfrak{p}}$, so heißt $\bar{a} := \{b \in \mathfrak{o}_{\mathfrak{p}} \; ; \; \mathfrak{p}/<b-a>\}$ Restklasse von a mod $\mathfrak{p}$.
Die Menge aller Restklassen mod $\mathfrak{p}$ wird mit $\underline{\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}}$ bezeichnet und ist ein Körper, der

Restklassenkörper von K mod $\mathfrak{p}$.

Sei $\mathfrak{U} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$ die Zerlegung des Divisors $\mathfrak{U}$ von $\mathfrak{o}_K$ in ein Produkt von Primdivisoren mit $\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i \neq j$.

In $\mathfrak{o}_K$ existieren Primelemente $\pi_1, \ldots, \pi_k$ mit
$\mathfrak{p}_i /<\pi_i>$, $\mathfrak{p}_i^2 \nmid <\pi_i>$ für $i = 1, \ldots, k$.

Sei $\alpha := \pi_1 \ldots \pi_k$ und S ein vollständiges Vertretersystem von Restklassen aus $\mathfrak{o}_K/_{\alpha} := \mathfrak{o}_K/\mathfrak{o}_K \cdot \alpha$, das die Null enthält.

Dann läßt sich jedes Element $a \in K_{\mathfrak{U}}$ eindeutig schreiben als

$$\sum_{n=m}^{\infty} a_n \alpha^n \text{ mit } a_i \in S \text{ und } m \in \mathbb{Z}.$$

Ist $a \in \mathcal{O}_{\mathcal{U}}$, so ist $m \geq 0$ und für $a \in \mathcal{O}_{\mathcal{U}}^{\times}$ gilt $m = 0$ mit $\mathcal{O}_K \cdot a_o + \mathcal{O}_K \cdot \alpha = \mathcal{O}_K$.

Die Beziehung zwischen $K_{\mathcal{U}}$ und den Körpern $K\,\varphi_i$ $(i = 1,\ldots,k)$ wird durch folgende Tatsache erhellt (vgl. Lit. 14, Kap. I, § 3 - 5):

(Bezeichne $[\{\alpha_n\}_{n\in\mathbb{N}}]_{\mathcal{U}} \in K_{\mathcal{U}}$ die von $\{\alpha_n\}_{n\in\mathbb{N}}$ erzeugte Äquivalenzklasse in $K_{\mathcal{U}}$, $[\{\alpha_n\}_{n\in\mathbb{N}}]\,\varphi_i \in K\,\varphi_i$ die von derselben Folge erzeugte Äquivalenzklasse in $K\,\varphi_i$.)

Da für $i \neq j$ $K\,\varphi_i \cap K\,\varphi_j = \{0\}$, kann man vom Ring $K\,\varphi_1 \oplus \ldots \oplus K\,\varphi_k$ sprechen, in dem Addition und Multiplikation komponentenweise durchgeführt werden.

Damit ist die Abbildung

$$H : K_{\mathcal{U}} \longrightarrow K\,\varphi_1 \oplus \ldots \oplus K\,\varphi_k$$

$$[\{\alpha_n\}_{n\in\mathbb{N}}]_{\mathcal{U}} \longmapsto \left([\{\alpha_n\}_{n\in\mathbb{N}}]\,\varphi_1, \ldots, [\{\alpha_n\}_{n\in\mathbb{N}}]\,\varphi_k\right)$$

wohldefiniert und ein stetiger Ringisomorphismus.

Die Umkehrabbildung ist gegeben durch

$$H^{-1} : K\,\varphi_1 \oplus \ldots \oplus K\,\varphi_k \longrightarrow K_{\mathcal{U}}$$

$$\left([\{\alpha_n^{(1)}\}_{n\in\mathbb{N}}]\,\varphi_1, \ldots, [\{\alpha_n^{(k)}\}_{n\in\mathbb{N}}]\,\varphi_k\right) \longmapsto [\{\beta_n\}_{n\in\mathbb{N}}]_{\mathcal{U}}$$

wobei $\beta_n := \sum_{i=1}^{k} \alpha_n^{(i)}\, \varepsilon_n^{(i)}$ und die Folgen $\{\varepsilon_n^{(i)}\}_{n\in\mathbb{N}}$ für jedes $i \in \{1,\ldots,k\}$ so gewählte Teilfolgen der Folgen

$$\{E_n^{(i)}\}_{n\in\mathbb{N}} := \left\{ \frac{\left(\frac{\pi_1 \cdots \pi_k}{\pi_i}\right)^n}{\pi_i^n + \left(\frac{\pi_1 \cdots \pi_k}{\pi_i}\right)^n} \right\}_{n\in\mathbb{N}} \text{ sind, daß } \mathfrak{p}_j\text{-}\lim_{n\to\infty} \alpha_n^{(i)} \varepsilon_n^{(i)}$$

$$= \begin{cases} \mathfrak{p}_i\text{-}\lim_{n\to\infty} \alpha_n^{(i)} & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$$

(Es ist $\mathfrak{p}_j\text{-}\lim_{n\to\infty} E_n^{(i)} = \delta_{ij}$ (Kroneckersymbol))

(vgl. Lit. 14, Kap. I, § 5)

Sei p eine natürliche Primzahl

Statt $K_{<p>}$ schreiben wir dann einfach K_p

(statt $O_{<p>}$ O_p, statt $/\ /_{<p>}$ $/\ /_p$ und statt <p>lim p-lim).

Die Elemente von K_p, die Äquivalenzklassen von Folgen mit Gliedern aus $\mathbb{Q}$ sind, bilden einen Teilkörper von K_p, der topologisch isomorph zu $\mathbb{Q}_p$ ist. Wir können deshalb annehmen, daß $\mathbb{Q}_p$ ein Teilkörper des Ringes K_p ist, und vom $\mathbb{Q}_p$-Vektorraum K_p sprechen. (Es ist auch $\mathbb{Z}_p \leq O_p$).
Ebenso sind für $<p> = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$ die $K\mathfrak{p}_i$ und $K\mathfrak{p}_1 \oplus \ldots \oplus K\mathfrak{p}_k$ $\mathbb{Q}_p$-Vektorräume.

Die Abbildung H ist damit auch ein Vektorraumisomorphismus.

Nach (Lit. 3, Kap. IV, § 2, Satz 1) gilt:

Ist $(\omega_1,\ldots,\omega_n)$ eine $\mathbb{Q}$-Basis von K, so ist sie auch eine $\mathbb{Q}_p$-Basis von K_p.

Reihen $\mathfrak{a}$-adischer Zahlen:

Eine Reihe $\sum_{n=0}^{\infty} a_n$ $\mathfrak{a}$-adischer Zahlen aus $K_{\mathfrak{a}}$ konvergiert in $K_{\mathfrak{a}}$ genau dann, wenn $\mathfrak{a}\text{-}\lim_{n\to\infty} a_n = \lim_{n\to\infty} /a_n/_{\mathfrak{a}} = 0$.

Diese Eigenschaft rührt von der Nicht-Archimedizität der $\mathfrak{a}$-adischen Bewertung her und stellt eine bedeutende Vereinfachung gegenüber den reellen und komplexen Zahlen dar.

Weiters kann jede konvergente Reihe $\sum_{n=0}^{\infty} a_n$ in $K_{\mathfrak{a}}$ umgeordnet werden, ohne daß sie ihren Wert dabei ändert.

Die $\mathfrak{p}$-Topologie auf $O_{\mathfrak{p}}[[X_1,\ldots,X_n]]$:

(vgl. G. Preuß, Allgemeine Topologie, 1975, Kap. 10.2)

Sei $\mathfrak{p}$ ein Primdivisor von O_K (bzw. $O_{\mathfrak{p}}$).
Sei $O_{\mathfrak{p}}[[X_1,\ldots,X_n]]$

der Potenzreihenring über $O_{\mathfrak{p}}$ in den Variablen $X_1,\ldots,X_n$.

Für ein $F = \sum_{(i_1,\ldots,i_n)\in \mathbb{N}_o^n} a_{i_1,\ldots,i_n} X_1^{i_1}\ldots X_n^{i_n}$

$\in O_{\mathfrak{p}}[[X_1,\ldots,X_n]]$ und einen Divisor $\mathfrak{a}$

teilt $\mathfrak{a}$ F ($\mathfrak{a}/F$) : $\Leftrightarrow$ $\mathfrak{a}/\langle a_{i_1,\ldots,i_n}\rangle$ für alle

$(i_1,\ldots,i_n) \in \mathbb{N}_o^n$.

Auf $\mathcal{O}_\wp[\![X_1,\dots,X_n]\!]$ läßt sich durch

$$v_\wp(F) := \begin{cases} \max\{n\in\mathbb{N}_0;\ \wp^n \mid F\} & \text{für } F \neq 0 \\ \infty & \text{für } F = 0 \end{cases}$$

ein Exponent definieren und damit eine Bewertung

$$|F|_\wp := \begin{cases} \rho^{-v_\wp(F)} & \text{für } F \neq 0 \\ 0 & \text{für } F = 0. \end{cases} \qquad (\rho > 1 \text{ aus } \mathbb{R})$$

Mit Hilfe der Metrik $d(F,G) := |F-G|_\wp$ auf $\mathcal{O}_\wp[\![X_1,\dots,X_n]\!]$ ist dann die folgende Abbildung h ein Hüllenoperator auf $\mathcal{O}_\wp[\![X_1,\dots,X_n]\!]$:

$$\begin{aligned} h: \mathcal{P}(\mathcal{O}_\wp[\![X_1,\dots,X_n]\!]) &\longrightarrow \mathcal{P}(\mathcal{O}_\wp[\![X_1,\dots,X_n]\!]) \\ \mathcal{A} &\longmapsto h(\mathcal{A}) := \{F\in\mathcal{O}_\wp[\![X_1,\dots,X_n]\!];\\ &\qquad \inf\{|F-G|_\wp;\ G\in\mathcal{A}\}=0\} \end{aligned}$$

($\mathcal{P}$ ... "Potenzmenge")

Dieser Hüllenoperator bestimmt eindeutig eine Topologie auf $\mathcal{O}_\wp[\![X_1,\dots,X_n]\!]$, die $\wp$-Topologie ($\mathcal{T}_\wp$) genannt wird:

$\mathcal{T}_\wp := \{O\subseteq\mathcal{O}_\wp[\![X_1,\dots,X_n]\!];\ h(\complement O)=\complement O\}$

($\complement$ ... "Komplement")

Für ein $\mathcal{A}\in\mathcal{P}(\mathcal{O}_\wp[\![X_1,\dots,X_n]\!])$ ist

$h(\mathcal{A}) = \{F\in\mathcal{O}_\wp[\![X_1,\dots,X_n]\!];\forall n\in\mathbb{N}_0\ \exists F_n\in\mathcal{A}: \wp^{n+1}/(F-F_n)\}$,

und wählt man ein Primelement $\pi\in\mathcal{O}_K$ mit $\wp/\langle\pi\rangle$, $\wp^2\nmid\langle\pi\rangle$, so ist $h(\mathcal{A}) = \{\sum_{n=0}^{\infty}\pi^n F_n\ ;\ F_n\in\mathcal{A}\}$.

Zwei Elemente $\sum_{n=0}^{\infty}\pi^n F_n$ und $\sum_{n=0}^{\infty}\pi^n G_n$ aus $h(\mathcal{A})$ sind genau dann gleich, wenn $\sum_{n=0}^{\nu}\pi^n F_n \equiv \sum_{n=0}^{\nu}\pi^n G_n \mod \wp^{\nu+1}$ für alle $\nu\geq 0$.

Im Verlauf dieser Arbeit interessiert uns nur die Hülle von $\mathcal{O}_p[X_1,\ldots,X_n]$:

$$h(\mathcal{O}_p[X_1,\ldots,X_n]) = \left\{ \sum_{n=0}^{\infty} \pi^n F_n \; ; \; F_n \in \mathcal{O}_p[X_1,\ldots,X_n] \right\} =: \overline{\mathcal{O}_p[X_1,\ldots,X_n]}$$

2) Die Grundidee der Skolemschen Methode

Sei K wieder ein algebraischer Zahlkörper vom Grad n und $\varepsilon_1,\ldots,\varepsilon_r$ ein System von Grundeinheiten von K.
Sei $m \in \mathbb{N}$, $m < n$, eine Zahl so, daß $r \leq n-m$.
Für $\mathbb{Q}$-linear unabhängige Zahlen $\omega_1,\ldots,\omega_m$ aus K bezeichne $M := \langle \omega_1,\ldots,\omega_m \rangle \subseteq \mathcal{O}_K$ den von den ω_i erzeugten $\mathbb{Z}$-Modul.
Wir ergänzen $\omega_1,\ldots,\omega_m$ zu einer $\mathbb{Q}$-Basis $\omega_1,\ldots,\omega_m,\omega_{m+1},\ldots,\omega_n \in K$ und betrachten den Modul $\overline{M} := \mathbb{Z}\langle \omega_1,\ldots,\omega_n \rangle$.
($\overline{M}$ nennt man dann vollständig in K)

In $\overline{M}$ gibt es nur endlich viele paarweise nicht-assoziierte Zahlen $\gamma_1,\ldots,\gamma_h$ mit vorgegebener Norm $c \in \mathbb{Z}$ (vgl.Lit.3, Kap.II,§2,Korollar zu Satz 5).
Alle $\alpha \in \overline{M}$ mit Norm(α) = c lassen sich dann in der Form $\alpha = \gamma_j \zeta \varepsilon_1^{y_1} \cdot \ldots \cdot \varepsilon_r^{y_r}$ darstellen, wobei $\gamma_j \in \{\gamma_1,\ldots,\gamma_h\}$, ζ eine Einheitswurzel aus $\mathcal{O}_K$ und $y_1,\ldots,y_r \in \mathbb{Z}$ (vgl. Lit.3,Kap.II,§5,Satz 1).

Sind $X_1,\ldots,X_m$ Unbestimmte über $\mathbb{Z}$ und $\sigma_1,\ldots,\sigma_n$ die Isomorphismen von K in $\mathbb{C}$ (Körper der komplexen Zahlen), so ist

$$F(X_1,\ldots,X_m) := \text{Norm}(X_1\omega_1+\ldots+X_m\omega_m) := [X_1\sigma_1(\omega_1)+\ldots+X_m\sigma_1(\omega_m)] \cdot \ldots \cdot [X_1\sigma_n(\omega_1)+\ldots+X_m\sigma_n(\omega_m)]$$

eine Form aus $\mathbb{Z}[X_1,\ldots,X_m]$ vom Grad n.
Sie ist irreduzibel über $\mathbb{Q}$, wenn o.E.d.A. $\omega_1 = 1$ und $K = \mathbb{Q}(\omega_2,\ldots,\omega_m)$ (vgl.Lit.3,Kap.II,§1,Satz 2).

Die Methode von Skolem ist nun ein Verfahren, diophantische Gleichungen der Gestalt $F(X_1,\ldots,X_m) = \text{Norm}(X_1\omega_1+\ldots+X_m\omega_m) = c$ (1) $\in \mathbb{Z}$ effektiv zu lösen.

Die Grundidee dabei ist folgende:

Für jede Lösung $(x_1,\dots,x_m)\in\mathbb{Z}^m$ von (1) ist nach dem Vorherigen $x_1\omega_1+\dots+x_m\omega_m \in M\subseteq\overline{M}$ eine Zahl in $\overline{M}$ mit der Norm c.
Sie hat also eine Darstellung $x_1\omega_1+\dots+x_m\omega_m+0\omega_{m+1}+\dots+0\,\omega_n = \gamma_j\zeta\,\varepsilon_1^{y_1}\cdot\dots\cdot\varepsilon_r^{y_r}$ mit $\gamma_j\in\{\gamma_1,\dots,\gamma_h\}$, ζ Einheitswurzel aus σ_K und $y_1,\dots,y_r\in\mathbb{Z}$.

Das bedeutet, daß die i-ten Koordinaten für i=m+1,...,n von $\gamma_j\zeta\varepsilon_1^{y_1}\cdot\dots\cdot\varepsilon_r^{y_r}$ bez. $\omega_{m+1},\dots,\omega_n$ identisch verschwinden müssen.
Ich bezeichne für $k\in\{m+1,\dots,n\}$ die k-te Koordinate von $\gamma_j\zeta\varepsilon_1^{y_1}\cdot\dots\cdot\varepsilon_r^{y_r}$ mit $(\gamma_j\zeta\varepsilon_1^{y_1}\cdot\dots\cdot\varepsilon_r^{y_r})_k$ und schreibe also

$$\begin{aligned}(\gamma_j\zeta\varepsilon_1^{y_1}\cdot\dots\cdot\varepsilon_r^{y_r})_{m+1} &= 0\\ &\cdots\cdots\cdots\cdots\\ &\cdots\cdots\cdots\cdots\\ (\gamma_j\zeta\varepsilon_1^{y_1}\cdot\quad\cdot\varepsilon_r^{y_r})_n &= 0\end{aligned}\qquad(2)$$

Das Problem, die diophantische Gleichung (1) zu lösen, ist damit auf die Lösung des Gleichungssystems (2) in den Unbekannten $y_1,\dots,y_r\in\mathbb{Z}$ zurückgeführt.

Da wir vorausgesetzt haben, daß $r\le n-m$, kann man erwarten, daß das System (2) nur endlich viele Lösungen in $\mathbb{Z}^m$ besitzt.

Skolem läßt als Lösungen auch Zahlen $y_1,\dots,y_r\in\mathbb{Z}_p$ zu und entwickelt die Funktion $\mathbb{Z}_p^{\,r}\longrightarrow K_p$: $(y_1,\dots,y_r)\longmapsto\varepsilon_1^{y_1}\cdot\dots\cdot\varepsilon_r^{y_r}$ in eine gleichmäßig konvergente p-adische Reihe.

Dadurch kann man (2) ersetzen durch ein System der Form

$$\left.\begin{aligned}\sum_{n_1,\dots,n_r=0}^{\infty} a_{m+1,n_1,\dots,n_r}\,y_1^{n_1}\cdot\quad\cdot y_r^{n_r} &= 0\\ \cdots\cdots\cdots\cdots\\ \sum_{n_1,\dots,n_r=0}^{\infty} a_{n,n_1,\dots,n_r}\,y_1^{n_1}\cdot\quad\cdot y_r^{n_r} &= 0\end{aligned}\right\}\qquad(3)$$

mit $a_{i,n_1,\dots,n_r}\in\mathbb{Q}_p$.

Für Systeme der Form (3) bewies Skolem Sätze, in denen unter Erfüllung gewisser Bedingungen kleine obere Schranken für deren Anzahl p-adischer Lösungen aufgestellt werden. Wichtig sind vor allem die Spezialfälle in einer oder zwei Unbekannten, also $\sum_{n_1=0}^{\infty} a_{n,n_1} y^{n_1} = 0$ bzw.

$$\left.\begin{aligned} \sum_{n_1,n_2=0}^{\infty} a_{n-1,n_1,n_2} y_1^{n_1} y_2^{n_2} &= 0 \\ \sum_{n_1,n_2=0}^{\infty} a_{n,n_1,n_2} y_1^{n_1} y_2^{n_2} &= 0 \end{aligned}\right\}$$

3) Kapitelübersicht

Der Hauptteil dieser Arbeit gliedert sich in zwei Kapitel II und III, denen jeweils ein Hauptsatz voransteht; einmal ein Satz von Skolem über die Anzahl ganzer p-adischer Lösungen einer Gleichung der Gestalt $F(X) = 0$ mit $F \in \overline{\mathbb{Q}_p}[X]$, das andere Mal ein Satz von Skolem über die Anzahl ganzer p-adischer Lösungen eines Gleichungssystems der Form

$$\left.\begin{aligned} F_1(X,Y) &= 0 \\ F_2(X,Y) &= 0 \end{aligned}\right\}$$

mit $F_1, F_2 \in \overline{\mathbb{Q}_p}[X,Y]$.

In Kapitel II werden nach dem Hauptsatz stetige Funktionen auf $\mathbb{Z}_p$ behandelt und erläutert, wie diese in gleichmäßig konvergente Funktionenreihen entwickelt werden können (Weierstraßentwicklung) (II.2).

Das diesbezügliche Hauptresultat wird im Hauptsatz für p-adische Funktionen formuliert (II.3).
Anschließend werden die Ergebnisse aus II.2 und II.3 dazu benützt, die Endlichkeit ganzrationaler Lösungen von Gleichungen des Typs $A_1(X)\beta_1^X+\ldots+A_s(X)\beta_s^X = 0$ mit $A_i \in K[X]$ und $\beta_i \in K$ zu beweisen, wobei β_i/β_j für $i\neq j$ keine Einheitswurzel ist, aber den Betrag 1 haben darf (II.4).
In II.5 geht es um lineare rekurrente Folgen und um die Frage, wie oft solche Folgen Werte eines Polynoms aus $K[X]$ annehmen können.
In II.6,II.6.1 und II.6.2 erhalten wir mittels einiger Sätze von Skolem Auskunft über die Lösungsanzahl bestimmter diophantischer Gleichungen (speziell kubische Formen mit negativer Diskriminante), und eine Reihe von Beispielen soll zeigen, wie die Lösungen mit der Skolemschen Methode berechnet werden können.
In Kapitel III werden nach dem Hauptsatz Invarianten und Kovarianten von Formen in zwei Variablen eingeführt (III.2), um anschließend in III.3 einen theoretischen Weg kennenzulernen, wie man elliptische Kurven durch Rückführung auf kubische oder biquadratische Formen und durch Anwendung der Skolemschen Methode lösen kann.
III.4 ist biquadratischen Formen mit negativer Diskriminante gewidmet und III.5 kubischen Formen mit positiver Diskriminante.
Anhand eines weiteren Beispiels soll in III.6 demonstriert werden, wie auch diophantische Gleichungen mit Formen fünften (und höheren) Grades in drei (und mehr) Unbestimmten voll-

kommen mit Skolems Methode gelöst werden können.
Den Schluß bildet eine Zusammenfassung und Beurteilung der Skolemschen Methode sowie ein Anhang mit ergänzenden Beispielen.

II. P-ADISCHE FUNKTIONEN IN EINER UNBESTIMMTEN

II.1 Ein Hauptsatz von Skolem über p-adische Reihen in einer Unbestimmten

Satz 1 (Lit.21, Satz 1):
Sei K ein algebraischer Zahlkörper, p eine Primzahl, $\mathfrak{p}$ ein Primdivisor von $\mathfrak{o}_K$, der p teilt und $\pi \in \mathfrak{o}_K$ mit $\mathfrak{p} \nmid (\pi)$, $\mathfrak{p}^2 \mid (\pi)$. Weiter sei $F := \sum_{i=0}^{\infty} \pi^i f_i(X) \in \overline{\mathfrak{o}_{\mathfrak{p}}}[X]$, wobei $\mathrm{Grad}(f_0)=m$ und der Leitkoeffizient von f_0 aus $\mathfrak{o}_{\mathfrak{p}}^{\times}$ ist.
Dann hat die Gleichung $F = 0$ höchstens m Lösungen in $\mathfrak{o}_{\mathfrak{p}}$, d.h. es gibt höchstens m verschiedene $x \in \mathfrak{o}_{\mathfrak{p}}$, sodaß die Kongruenzen $\sum_{i=0}^{\nu} \pi^i f_i(x) \equiv 0 \bmod \mathfrak{p}^{\nu+1}$ für alle $\nu \geq 0$ simultan erfüllt sind.

Beweis: Wir zeigen zuerst, daß man $\overline{f_i}$ und $g_i \in \mathfrak{o}_{\mathfrak{p}}[X]$, $i \geq 1$, so finden kann, daß $\mathrm{Grad}(\overline{f_i}) < \mathrm{Grad}(f_0)$ und $\sum_{i=0}^{\nu} \pi^i f_i \equiv (f_0 + \sum_{i=1}^{\nu} \pi^i \overline{f_i})(1 + \sum_{i=1}^{\nu} \pi^i g_i) \bmod \mathfrak{p}^{\nu+1}$ für alle $\nu \geq 1$. Somit gibt es Potenzreihen $\overline{F}$ und G aus $\overline{\mathfrak{o}_{\mathfrak{p}}}[X]$ von der Gestalt $\overline{F} = f_0 + \sum_{i=1}^{\infty} \pi^i \overline{f_i}$, $G = 1 + \sum_{i=1}^{\infty} \pi^i g_i$, sodaß $F = \overline{F} \cdot G$.
Bei der Konstruktion von $\overline{F}$ und G verfahren wir induktiv:
Für $\nu=1$ muß also gelten:
$f_0 + \pi f_1 \equiv (f_0 + \pi \overline{f_1})(1 + \pi g_1) \bmod \mathfrak{p}^2$.
Das ist gleichbedeutend mit $f_1 \equiv g_1 f_0 + \overline{f_1} \bmod \mathfrak{p}$.
Da der Leitkoeffizient von f_0 nach Voraussetzung eine $\mathfrak{p}$-adische Einheit ist, existieren nach dem Divisionsalgorithmus g_1 und $\overline{f_1} \in \mathfrak{o}_{\mathfrak{p}}[X]$ so, daß $\mathrm{Grad}(\overline{f_1}) < \mathrm{Grad}(f_0)$ und $f_1 = g_1 f_0 + \overline{f_1}$.
Man setzt $\overline{f_1} := f_1 - g_1 f_0$.
Für $\nu=2$ muß gelten:
$f_0 + \pi f_1 + \pi^2 f_2 \equiv (f_0 + \pi \overline{f_1} + \pi^2 \overline{f_2})(1 + \pi g_1 + \pi^2 g_2) \bmod \mathfrak{p}^3$, was

äquivalent ist zu

$f_1+\pi f_2 \equiv \overline{f_1} + f_0g_1+\pi(\overline{f_2}+f_0g_2+\overline{f_1}g_1) \bmod \mathfrak{p}^3$ und wegen $f_1=\overline{f_1}+g_1f_0$ weiter zu $f_2-\overline{f_1}g_1 \equiv f_0g_2+\overline{f_2} \bmod \mathfrak{p}$.

Wieder existieren nach dem Divisionsalgorithmus solche g_2 und $\overline{f_2}$ in $\mathfrak{o}_\mathfrak{p}[X]$ mit $\mathrm{Grad}(\overline{f_2}) < \mathrm{Grad}(f_0)$.

Man setzt $\overline{f_2} := f_2-\overline{f_1}g_1-f_0g_2$.

Der allgemeine Induktionsschritt verläuft ganz analog, ist jedoch umständlich niederzuschreiben und wird deshalb wegge= lassen.

Da nun $G(x) \in \mathfrak{o}_\mathfrak{p}^x$ für alle $x \in \mathfrak{o}_\mathfrak{p}$, ist $x \in \mathfrak{o}_\mathfrak{p}$ Nullstelle von $F = \overline{F} \cdot G$ genau dann, wenn x Nullstelle von $\overline{F}$ ist.

Wir betrachten also $\overline{F} = 0$ an Stelle von $F = 0$.

Da für $h_\nu := f_0+\sum_{i=1}^{\nu} \pi^i \overline{f_i}$ die Folge $\{h_{\nu+1}-h_\nu\}_{\nu\in\mathbb{N}}$ eine Null= folge im $\mathfrak{o}_\mathfrak{p}$-Modul $\bigoplus_{j=0}^{m} \mathfrak{o}_\mathfrak{p}/\mathfrak{p} X^j = \overline{\bigoplus_{j=0}^{m} \mathfrak{o}_\mathfrak{p}/\mathfrak{p} X^j}$ ist ($m=\mathrm{Grad}(f_0)$), ist $\{h_\nu\}_{\nu\in\mathbb{N}}$ konvergent in diesem Modul, also $\overline{F} \in \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{o}_\mathfrak{p}X \oplus \ldots \ldots \oplus \mathfrak{o}_\mathfrak{p} X^m$.

Damit hat $\overline{F}$ höchstens m Nullstellen in $\mathfrak{o}_\mathfrak{p}$, wodurch der Satz bewiesen ist.

Bemerkung: Der Satz behält seine Gültigkeit auch noch, wenn $\mathfrak{p}$ kein Primdivisor von K ist. Man muß dann nur verlangen, daß der Leitkoeffizient von f_0 eine $\mathfrak{p}$-adische Einheit ist. Wir werden den Satz nur für den Spezialfall $K = \mathbb{Q}$ und $\mathfrak{p} = p$, eine Primzahl, benötigen.

II.2 Stetige Funktionen auf $\mathbb{Z}_g$

Sei g eine natürliche Zahl und $f: \mathbb{Z}_g \longrightarrow K_g$ $(K_g := K_{\langle g \rangle})$ eine auf ganz $\mathbb{Z}_g$ stetige Funktion.

Das heißt per Definition: Für alle $x_o \in \mathbb{Z}_g$ und für alle $\varepsilon > 0$ gibt es ein $\delta > 0$, sodaß für alle $x_o \in \mathbb{Z}_g$ mit $|x-x_o|_g < \delta$ $|f(x)-f(x_o)|_g$ gilt.

Da $\mathbb{Z}_g$ kompakt in $\mathbb{Q}_g$ ist, ist f sogar gleichmäßig stetig auf $\mathbb{Z}_g$, d.h. für alle $\varepsilon > 0$ gibt es ein $\delta > 0$, sodaß für alle $x,y \in \mathbb{Z}_g$ mit $|x-y|_g < \delta$ $|f(x)-f(y)|_g < \varepsilon$.

Für die Funktion f kann man die sogenannten Weierstraßkoeffizienten a_n, $n \in \mathbb{N}_o$, definieren:

$$a_n := \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k)$$

$$\left[\binom{n}{k} := \frac{n(n-1)\ldots(n-1+k)}{k!} \right]$$

Die Reihe $f^{\neq}(X) := \sum_{n=0}^{\infty} a_n \binom{X}{n}$ mit $\binom{X}{n} := \frac{X(X-1)\ldots(X-n+1)}{n!} \in \mathbb{Q}[X]$ heißt die zu f gehörende Interpolationsreihe oder Weierstraßentwicklung.

Ist $x \in \mathbb{N}$, so konvergiert $f^{\neq}(x)$ gegen f(x) (vgl.Lit.14,Kap.II, §9.2).

Hingegen gilt auf $\mathbb{Z}_g$:

$f^{\neq}$ konvergiert genau dann gleichmäßig auf $\mathbb{Z}_g$, wenn $g\text{-}\lim_{n\to\infty} a_n = 0$.

Beweis: "==> ": Konvergiert $\sum_{n=0}^{\infty} a_n \binom{x}{n}$ für alle $x \in \mathbb{Z}_g$, so auch für x=-1. Also existiert

$$\sum_{n=0}^{\infty} a_n \binom{-1}{n} = \sum_{n=0}^{\infty} (-1)^n a_n$$

in K_g, d.h. $g\text{-}\lim_{n\to\infty} a_n = 0$.

"<==" : Zunächst halten wir fest: Für $x \in \mathbb{Z}_g$ und $n \in \mathbb{N}_0$ ist $\binom{x}{n} \in \mathbb{Z}_g$ (d.h. $\left|\binom{x}{n}\right|_g \leq 1$). Dies ist sicher richtig für $x \in \mathbb{Z}$ (sogar: $\binom{x}{n} \in \mathbb{Z}$). Da aber die Abbildung: $\mathbb{Z}_g \longrightarrow \mathbb{Q}_g : x \longmapsto \binom{x}{n}$ stetig und $\mathbb{Z}$ dicht in $\mathbb{Z}_g$ liegt, gilt die Aussage für alle $x \in \mathbb{Z}_g$. Sei nun $g\text{-}\lim_{n\to\infty} a_n = 0$. Wegen $\left|a_n \binom{x}{n}\right|_g \leq |a_n|_g$ ($n \in \mathbb{N}_0$, $x \in \mathbb{Z}_g$), ist f^* gleichmäßig konvergent auf $\mathbb{Z}_g$ nach dem Majoranten=kriterium.

Im Falle $g\text{-}\lim_{n\to\infty} a_n = 0$ stellt also f^* als gleichmäßiger Grenz=wert stetiger Funktionen auf $\mathbb{Z}_g$ eine stetige und wegen der Kompaktheit von $\mathbb{Z}_g$ gleichmäßig stetige Funktion auf $\mathbb{Z}_g$ dar. Da f und f^* auf der in $\mathbb{Z}_g$ dichten Menge $\mathbb{N}$ übereinstimmen, stimmen sie auch auf $\mathbb{Z}_g$ überein.
Die Eindeutigkeit der zu f gehörenden Interpolationsreihe ist leicht einzusehen (Lit.14,Kap.II,§9.4).

Zusammenfassend haben wir also folgenden

Satz 2:

Ist $f: \mathbb{Z}_g \longrightarrow K_g$ eine stetige Funktion und gilt für ihre Weierstraßkoeffizienten a_n $g\text{-}\lim_{n\to\infty} a_n = 0$, so hat f die ein=deutig bestimmte auf $\mathbb{Z}_g$ gleichmäßig konvergente Entwick=lung $\sum_{n=0}^{\infty} a_n \binom{x}{n}$.

II.3 Der Hauptsatz für p-adische Funktionen

Sei p eine Primzahl.

Es gilt:

Satz 3 (Lit.14,Kap.II,§10.1,Theorem 1):

Sei $f: \mathbb{Z}_p \longrightarrow K_p$ stetig.

Dann besitzt f eine eindeutig bestimmte auf $\mathbb{Z}_p$ gleichmäßig konvergente Interpolationsreihe $\sum_{n=0}^{\infty} a_n \binom{x}{n}$, wobei a_n wie bisher die Weierstraßkoeffizienten von f bedeuten.

Beweis:

Wir verwenden hier für die Festsetzung der p-adischen Bewertung auf $\mathbb{Q}_p$ eine spezielle Zahl ρ, nämlich $\rho := p$ (vgl.Seite 2).

Eine Funktion $S: \mathbb{Z}_p \longrightarrow K_p$ nennt man Stufenfunktion, wenn es ein $t \in \mathbb{N}$ gibt, sodaß $S(x) = S(y)$ für alle $x,y \in \mathfrak{o}_p$ mit $x \equiv y \bmod p^t$. Das kleinste solche $t \in \mathbb{N}$ heißt dann die Ordnung von S.

Offensichtlich sind Stufenfunktionen gleichmäßig stetig.

Nach (Lit.14,Kap.II,§8.9) gilt:

Eine Funktion $f: \mathbb{Z}_p \longrightarrow K_p$ ist gleichmäßig stetig auf $\mathbb{Z}_p$ $\Longleftrightarrow$ für alle $s \in \mathbb{N}$ gibt es eine Stufenfunktion $S: \mathbb{Z}_p \longrightarrow K_p$, sodaß $|f(x)-S(x)|_p \leq p^{-s}$ für alle $x \in \mathbb{Z}_p$.

Sei nun $s \in \mathbb{N}$ beliebig und S die gegebene stetige Funktion f bezüglich s approximierende Stufenfunktion.

Also: $|f(x)-S(x)|_p \leq p^{-s}$ für alle $x \in \mathbb{Z}_p$.

Sei $\sum_{n=0}^{\infty} b_n \binom{x}{n}$ die Interpolationsreihe von S mit den Weierstraßkoeffizienten $b_n \in K_p$. Da für die Weierstraßkoeffizienten einer stetigen Funktion f allgemein die wichtige Beziehung

$\sup_{n\in\mathbb{N}} |a_n|_p = \sup_{n\in\mathbb{N}} |f(n)|_p$ gilt (Lit.14,Kap.II,§9.3), so hat man auch hier, wenn $\sum_{n=0}^{\infty} a_n\binom{X}{n}$ die Interpolationsreihe von f ist: $\sup_{n\in\mathbb{N}} |a_n-b_n|_p = \sup_{n\in\mathbb{N}} |f(n)-S(n)|_p \leq p^{-s}$.

Wir zeigen, daß für alle hinreichend großen $n\in\mathbb{N}$ $|b_n|_p \leq p^{-s}$, woraus $|a_n|_p \leq |a_n-b_n+b_n|_p \leq \max\{|a_n-b_n|_p, |b_n|_p\} \leq p^{-s}$ für genügend große $n\in\mathbb{N}$ folgt.

Da $s\in\mathbb{N}$ beliebig gewählt war, folgt daraus $p\text{-}\lim_{n\to\infty} a_n = 0$, womit Satz 3 bewiesen wäre.

Für den Beweis von $|b_n|_p \leq p^{-s}$ für alle hinreichend großen $n\in\mathbb{N}$ gibt es mehrere Versionen, von denen die wohl einfachste und kürzeste die folgende ist:

Seien V und W zwei Unbestimmte über K_p, die durch die folgenden drei äquivalenten Beziehungen miteinander verbunden sind:

$$V = \frac{W}{1+W} \quad ; \quad W = \frac{V}{1-V} \quad , \quad (1-V)(1+W) = 1.$$

Nach (Lit.14,Kap.II,§9.5) gilt dann:

Für $x\in\mathbb{N}$ sind die beiden Gleichungen

$f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ und $a_n = \sum_{k=0}^{n} (-1)^k\binom{n}{k} f(n-k)$ äquivalent zur

formalen Identität $\sum_{n=0}^{\infty} f(n)V^n = (1+W)\sum_{n=0}^{\infty} a_n W^n$.

Also gilt auch hier: $\sum_{n=0}^{\infty} S(n)V^n = (1+W)\sum_{n=0}^{\infty} b_n W^n$.

Sei t die Ordnung von S.

Dann ist S periodisch mit der Periode p^t; d.h. $S(x+p^t)=S(x)$.

Für $n=N+m.p^t\in\mathbb{N}$, $0\leq N\leq p^t-1$ folgt:

$$\sum_{n=0}^{\infty} S(n)V^n = \sum_{m=0}^{\infty}\sum_{N=0}^{p^t-1} S(N+mp^t)V^{N+mp^t} = \sum_{N=0}^{p^t-1} S(N)V^N \sum_{m=0}^{\infty} V^{mp^t} =$$

$$= \sum_{N=0}^{p^t-1} S(N)V^N \frac{1}{1-V^{p^t}} \quad .$$

Wegen (4) wird dadurch

$$\sum_{n=0}^{\infty} b_n W^n = \frac{1}{1+W} \sum_{N=0}^{p^t-1} S(N)\left(\frac{W}{1+W}\right)^N \frac{1}{1-\left(\frac{W}{1+W}\right)^{p^t}} = \frac{A(W)}{B(W)} \quad \text{mit}$$

$$A(W) = \sum_{N=0}^{p^t-1} S(N)W^N(1+W)^{p^t-N-1} \quad , \quad B(W) = (1+W)^{p^t} - W^{p^t} \quad .$$

A und B sind dabei aus $K_p[W]$ und haben höchstens den Grad p^t-1.
Da p eine Primzahl ist, sind die Binomialkoeffizienten $\binom{p}{k}$ für $k=1,\ldots,p-1$ durch p teilbar, sodaß $(X+1)^{p^t} = X^{p^t}+1+p\phi(X)$, wobei $\phi(X) \in \mathbb{Z}[X]$ (Induktion über t).
Deshalb ist $B(W) = 1+p\,\phi(W)$ und $\phi(W) \in \mathbb{Z}[W]$ hat höchstens den Grad p^t-1.
Es ist also $\sum_{n=0}^{\infty} b_n W^n = \frac{A(W)}{1+p\,\phi(W)} = \sum_{k=1}^{\infty} (-1)^{k-1} p^{k-1} A(W)\,\phi(W)^{k-1}$.
Die Polynome $A(W)\,\phi(W)^{k-1}$ haben höchstens den Grad $(p^t-1)+(k-1)(p^t-1) = k(p^t-1)$.
Vergleicht man die Koeffizienten der beiden letzten Reihen (Elemente des Potenzreihenrings $K_p[[W]]$), so sieht man, daß nur die Terme der zweiten Reihe einen Beitrag für b_n geben, in denen $k(p^t-1) \geq n$ oder $k-1 \geq \frac{n}{p^t-1} - 1$.
Also ist b_n auf jeden Fall durch $p^{k-1} = p^{\left(\frac{n}{p^t-1}-1\right)}$ teilbar und deswegen $p\text{-}\lim_{n\to\infty} b_n = 0$.
Die Behauptung folgt nun aus Satz 2.

Satz 3 läßt sich auch für stetige Funktionen
$f: \mathbb{Z}_p \longrightarrow \mathcal{O}_{\mathfrak{P}}$, $\mathfrak{P}$ ein Primdivisor von $\mathcal{O}_K$ mit $\mathfrak{P} \nmid \langle p \rangle$, beweisen. Da dieser Beweis aber verhältnismäßig kompliziert ist, verzichte ich hier auf seine Ausführung und zitiere nur den

von der Qualität der Aussage her zu Satz 3 analogen

Satz 3' (Lit.10,§16,Satz N):

Sei p eine Primzahl und $\mathfrak{p}$ ein Primdivisor von $\mathfrak{o}_K$ mit $\mathfrak{p} / \langle p \rangle$. Jede stetige Funktion $f: \mathbb{Z}_p \longrightarrow \mathfrak{o}_\mathfrak{p}$ besitzt eine eindeutig bestimmte auf $\mathbb{Z}_p$ gleichmäßig konvergente Interpolationsreihe $\sum_{n=0}^{\infty} a_n \binom{X}{n}$, wobei $a_n = \sum_{k=0}^{n} (-1)^k f(n-k) \binom{n}{k} \in \mathfrak{o}_\mathfrak{p}$ wiederum die Weierstraßkoeffizienten von f sind.

Satz 1 und Satz 3' zusammen ergeben

Satz 4 (Lit.10,§16):

Sei p eine Primzahl.

Ist $f: \mathbb{Z}_p \longrightarrow K_p$ stetig und hat f unendlich viele Nullstellen, so ist f schon die Nullfunktion.

Beweis:

Sei $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}$, $\mathfrak{p}_i$ Primdivisoren von $\mathfrak{o}_K$.

Wir nehmen an, daß f nicht die Nullfunktion ist. Nach Satz 3 besitzt f eine auf $\mathbb{Z}_p$ gleichmäßig konvergente Interpolationsreihe $\sum_{n=0}^{\infty} a_n \binom{X}{n}$. Da $p\text{-}\lim_{n \to \infty} a_n = 0$, gibt es ein $b \neq 0$ aus K_p, sodaß $ba_n \in \mathfrak{o}_p$ für alle $n \geq 0$. $b.f = \sum_{n=0}^{\infty} ba_n \binom{X}{n}$ ist dann eine stetige Funktion von $\mathbb{Z}_p$ nach $\mathfrak{o}_p$ mit denselben Nullstellen wie f und wie f nicht die Nullfunktion.

Sei $H: K_p \longrightarrow K_{\mathfrak{p}_1} \oplus \ldots \oplus K_{\mathfrak{p}_k}$ der in der Einleitung definierte stetige Isomorphismus und $H_i := (pr_i \circ H)/_{\mathfrak{o}_p}$ für $i=1,\ldots,k$ die auf $\mathfrak{o}_p$ eingeschränkte Hintereinanderausführung von H und der Projektion von $K_{\mathfrak{p}_1} \oplus \ldots \oplus K_{\mathfrak{p}_k}$ auf $K_{\mathfrak{p}_i}$.

Die H_i sind stetige Funktionen von $\mathfrak{o}_p$ nach $\mathfrak{o}_{\mathfrak{p}_i}$.

Da $b.f : \mathbb{Z}_p \longrightarrow \mathfrak{o}_p$ nicht die Nullfunktion ist, gibt es

mindestens ein $j \in \{1,\dots,k\}$, sodaß $H_j o(bf)$: $\mathbb{Z}_p \longrightarrow \mathfrak{o}_{\mathfrak{p}_j}$ nicht die Nullfunktion ist. $H_j o(bf)$ ist stetig und besitzt deshalb nach Satz 3' eine gleichmäßig konvergente Interpolationsreihe $\sum_{n=0}^{\infty} b_n \binom{X}{n}$ mit $b_n \in \mathfrak{o}_{\mathfrak{p}_j}$ und $\mathfrak{p}_j\text{-}\lim_{n\to\infty} b_n = 0$.
Sei $\pi_j \in \mathfrak{o}_K$ ein Primelement mit $\mathfrak{p}_j \,/\!\langle \pi_j \rangle$, $\mathfrak{p}_j^{\,2} \nmid \langle \pi_j \rangle$.
Dann können wir die letzte Reihe schreiben als $\sum_{n=0}^{\infty} \pi^n f_n(X) \in \overline{\mathfrak{o}_{\mathfrak{p}_j}[X]}$ (vgl. Seite 10).
Nach Satz 1 hat $\sum_{n=0}^{\infty} \pi^n f_n(X)$ höchstens $\mathrm{Grad}(f_o)$ Nullstellen in $\mathbb{Z}_p$, und o.E.d.A. ist der Leitkoeffizient von f_o aus $\mathfrak{o}_{\mathfrak{p}_j}^{\times}$.
Da alle Nullstellen von bf auch Nullstellen von $H_j o(bf)$ sind, ist der Satz hiermit bewiesen.

II.4 Exponentialgleichungen

Mit Hilfe der bisherigen Sätze läßt sich nun ein Satz beweisen, der dazu benützt werden soll, Aussagen über lineare rekurrente Folgen algebraischer Zahlen zu erhalten.

Satz 5 (Lit.10,§17,Satz 0):
Sei K ein algebraischer Zahlkörper und $A_1,\ldots,A_s \in K[X]$ alle ungleich Null.
$\beta_1,\ldots,\beta_s$ seien Zahlen in K ungleich Null, sodaß β_i/β_j für alle $i\neq j$ keine Einheitswurzel ist. Dann hat die Funktion

$f: \mathbb{Z} \longrightarrow K$

$x \longmapsto A_1(x)\beta_1^x+\ldots+A_s(x)\beta_s^x$ nur endlich viele Nullstellen in $\mathbb{Z}$.

Bemerkung: Man kann ein nur wenig schwächeres Resultat als Satz 5 trivial beweisen, indem man statt "β_i/β_j für alle $i\neq j$ keine Einheitswurzel" voraussetzt, daß $|\beta_i/\beta_j| \neq 1$ für alle $i\neq j$ ($|\ |$... "Betrag").

Der relativ lange Beweis von Satz 5 liefert jedoch eine Möglichkeit, die endlich vielen Nullstellen der Funktion f mit der Skolemschen Methode zu berechnen, auch wenn für ein $i\neq j$ $|\beta_i/\beta_j| = 1$ gilt. Ich werde das anschließend an einem Beispiel zeigen.

Beweis von Satz 5:
Sei p eine Primzahl, sodaß alle β_j p-adische Einheiten in K_p sind.

Dann hat jedes β_j eine Darstellung

$a_{o,j} + a_{1,j}p + a_{2,j}p^2 + \ldots$, wobei die $a_{i,j}$ Elemente eines Repräsentantensystems von σ_K/p sind und $\sigma_K \cdot a_{o,j} + \sigma_K \cdot p = \sigma_K$ gilt.

Bezeichnet φ_K die Eulersche φ-Funktion für σ_K, also $\varphi_K(\mathfrak{A}) := |(\sigma_K/\mathfrak{A})^x|$, $\mathfrak{A}$ Ideal in σ_K, so gilt $a_{o,j}^{\varphi_K(p)} \equiv 1 \bmod p$ $(\varphi_K(p) := \varphi_K(\sigma_K \cdot p))$ (siehe Lit.18,Kap.8,Aufg.3).

Daraus folgt aber auch $\beta_j^{\varphi_K(p)} \equiv 1 \bmod p$ für alle $j=1,\ldots,s$.

Somit ist für $M := \varphi_K(p)$ $\beta_j^M = 1+\rho_j$ mit $\rho_j \in \sigma_K \cdot p$.

Wegen $p\text{-}\lim_{n\to\infty} \rho_j^n = 0$ ist die Reihe $g_j(Y) := \sum_{n=0}^{\infty} \rho_j^n \binom{Y}{n}$ gleichmäßig konvergent auf $\mathbb{Z}_p$.

Sie definiert für $y \in \mathbb{Z}_p$ die Funktion

$y \longmapsto (1+\rho_j)^y := \sum_{n=0}^{\infty} \rho_j^n \binom{y}{n}$.

Setzt man für $r=0,\ldots,M-1$ $f_r: \mathbb{Z} \longrightarrow K$

$y \longmapsto f_r(y)$

mit $f_r(y) := \sum_{j=1}^{s} A_j(My+r)\beta_j^{My+r} = \sum_{j=1}^{s} A_j(My+r)\beta_j^r g_j(y) =$

$\sum_{j=1}^{s} B_{r,j}(y) g_j(y)$, $B_{r,j} \in K[Y]$,

so hat f eine Nullstelle in $M\mathbb{Z}+r$ genau dann, wenn f_r eine Nullstelle in $\mathbb{Z}$ hat.

(f hat unendlich viele Nullstellen in $\mathbb{Z}$ $\Leftrightarrow$ $\exists r \in \{0,\ldots,M-1\}$: f_r hat unendlich viele Nullstellen in $\mathbb{Z}$).

Da A_j und $B_{r,j}$ für alle $r=0,\ldots,M-1$ denselben Grad haben und $A_j \neq 0$ ist, so sind auch alle $B_{r,j}$ ungleich Null.

Es kann ohne E.d.A. angenommen werden, daß alle $B_{r,j} \in \sigma_K[Y]$ (ansonsten multipliziere man alle $B_{r,j}$ mit geeignetem $\alpha \in \sigma_K$, was auf die Nullstellen der f_r keinen Einfluß ausübt).

Als Polynome haben die $B_{r,j}$ endliche Interpolationsreihen, d.h. es gilt: $B_{r,j} = \sum_{n=0}^{t} \gamma_{r,j,n} \binom{Y}{n} \neq 0$, $\gamma_{r,j,n} \in \sigma_K$ (hier sei $t = \max_{r,j} \{\mathrm{Grad}(B_{r,j})\}$).

Mit Hilfe der Formel

$$\binom{Y}{m}\binom{Y}{n} = \sum_{k=0}^{\min\{m,n\}} \binom{\min\{m,n\}}{k}\binom{n+m-k}{\min\{m,n\}}\binom{Y}{n+m-k} \qquad \text{(siehe Lit.10,§16)}$$

erhält man für die Produkte $B_{r,j}(y)g_j(y)$ die Reihenentwicklung

$$\sum_{k=0}^{\infty}\Big(\sum_{\nu=0}^{\min\{t,k\}} \beta_{r,j,\nu}\,\varrho_j^{k-\nu}(1+\varrho_j)^{\nu}\binom{k}{\nu}\Big)\binom{y}{k}.$$

Somit ist $f_r(y) = \sum_{j=1}^{s} B_{r,j}(y)g_j(y) =$

$$\sum_{k=0}^{\infty}\Big(\sum_{\nu=0}^{\min\{t,k\}}\binom{k}{\nu}\Big[\sum_{j=1}^{s}\beta_{r,j,\nu}\,\varrho_j^{k-\nu}(1+\varrho_j)^{\nu}\Big]\Big)\binom{y}{k}.$$

Nimmt man an, f habe unendlich viele Nullstellen, so gibt es ein $r\in\{0,\dots,M-1\}$, sodaß f_r unendlich viele Nullstellen besitzt. Nach Satz 4 muß f_r also die Nullfunktion sein. Das bedeutet, daß die Weierstraßkoeffizienten von f_r alle gleich Null sind. Das unendliche System linearer Gleichungen über $\mathbb{C}_p$

$$\sum_{\nu=0}^{\min\{t,k\}}\sum_{j=1}^{s}\binom{k}{\nu}\varrho_j^{k-\nu}(1+\varrho_j)^{\nu}X_{\nu,j} = 0 \quad ; \; k=0,1,2,\dots$$

hat demnach die nichttriviale Lösung $\beta_{r,1,0},\dots,\beta_{r,s,t}$.

Die ersten $s(t+1)$ linearen Gleichungen ergeben das System

$$\begin{array}{l} i\text{-te} \\ \text{Zeile} \end{array}\Bigg\{ \underbrace{\binom{i}{0}\varrho_j^{i}}_{j=1,\dots,s} \quad \underbrace{\binom{i}{1}\varrho_j^{i-1}(1+\varrho_j)}_{j=1,\dots,s} \quad \underbrace{\binom{i}{2}\varrho_j^{i-2}(1+\varrho_j)^2}_{j=1,\dots,s} \quad \dots \quad \underbrace{\binom{i}{t}\varrho_j^{i-t}(1+\varrho_j)^{t}}_{j=1,\dots,s} \Bigg) \begin{pmatrix} X_{0,1} \\ \vdots \\ X_{0,s} \\ X_{1,1} \\ \vdots \\ X_{1,s} \\ \vdots \\ X_{t,1} \\ \vdots \\ X_{t,s} \end{pmatrix} = 0$$

Obige ((t+1)s x (t+1)s) - Matrix werde mit A bezeichnet. Ihre Determinante muß Null sein. Jede Spalte von A besitzt einen Faktor $(1+\varrho_j)^k$, sodaß wegen der Spaltenlinearität der Determinante folgt: $\det(A) = (1+\varrho_j)^{(1+2+\ldots+t)} \det B$ mit

$$B = \left(\begin{array}{c|c|c|c} & & & \\ \binom{i}{0}\varrho_j^{\,i} & \binom{i}{1}\varrho_j^{\,i-1} & \cdots & \binom{i}{t}\varrho_j^{\,i-t} \\ & & & \end{array} \right) \longleftarrow \text{i-te Zeile}$$

$\underbrace{\qquad\qquad}_{j=1,\ldots,s}$

Da $(1+\varrho_j) \neq 0$, ist $\det A = 0 \iff \det B = 0$.

DetB werde mit $\Pi(s(t+1);\varrho_1,\ldots,\varrho_s)$ bezeichnet. Es gilt die Formel $\Pi(N;\varrho_1,\ldots,\varrho_s) = \prod_{j=2} (\varrho_j-\varrho_1)^{\left[\frac{N-2}{2}\right]} \Pi(N-1;\varrho_2,\ldots,\varrho_s,\varrho_1)$ mit $N:=s(t+1)$ (siehe Lit.10,§17).

Durch mehrfache Anwendung kommt man auf

$$\Pi(N;\varrho_1,\ldots,\varrho_s) = +/- \prod_{s>t} (\varrho_s-\varrho_t)^n \quad , \quad n \in \mathbb{N} .$$

Aus detB = 0 folgt also $\varrho_j=\varrho_k$ für mindestens ein $j\neq k$. Wegen $\beta_j^{\,M}=1+\varrho_j=1+\varrho_k=\beta_k^{\,M}$ haben wir dann $\left(\frac{\beta_j}{\beta_k}\right)^M = 1$ für $j\neq k$ im Widerspruch zur Voraussetzung des Satzes.

<u>Bemerkung:</u> Ist speziell s der Grad von K über $\mathbb{Q}$, und sind die Koeffizienten von $A_1,\ldots,A_s$ und $\beta_1,\ldots,\beta_s$ konjugiert zueinander und ganz-algebraisch, dann ist $f(x)=\mathrm{Spur}(A_1(x)\beta_1^{\,x})$ aus $\mathbb{Z}$ für $x\in\mathbb{Z}$, also f eine Funktion von $\mathbb{Z}$ nach $\mathbb{Z}$.

In dieser Form gibt es für den Satz schöne Anwendungsmöglichkeiten und in konkreten Beispielen können für die Reihen

der f_r in Gestalt von Satz 1 kleine obere Schranken für die Lösungsanzahl gefunden werden.

Ein Beispiel zu Satz 5 (aus Lit.10,§17):

Sei $K = \mathbb{Q}(\sqrt{-7})$ und $A_1 := 1$, $A_2 := -1$, $A_3 := -\sqrt{-7}$,

$\beta_1 := 1+\sqrt{-7}$, $\beta_2 := 1-\sqrt{-7}$, $\beta_3 := 2$,

also $f: \mathbb{Z} \longrightarrow K$

$x \longmapsto f(x) = (1+\sqrt{-7})^x - (1-\sqrt{-7})^x - \sqrt{-7}\, 2^x$.

Es ist $|\beta_1/\beta_2| = 1$, jedoch β_1/β_2 keine n-te Einheitswurzel für ein $n \in \mathbb{N}$ ($\beta_1/\beta_2 = \frac{-3+\sqrt{-7}}{4} \notin \mathfrak{o}_K$).

Weiter ist $(1+\sqrt{-7})^8 = -3968-384\sqrt{-7} \equiv 1 \bmod 3$

$(1-\sqrt{-7})^8 = -3968+384\sqrt{-7} \equiv 1 \bmod 3$

$2^8 = 256 \equiv 1 \bmod 3$

f besitzt eine Nullstelle in $8\mathbb{Z}+r$ genau dann, wenn

$f_r: \mathbb{Z} \longrightarrow K$

$y \longmapsto f_r(y) := (1+\sqrt{-7})^{8y+r} - (1-\sqrt{-7})^{8y+r} - \sqrt{-7}\cdot 2^{8y+r}$

eine Nullstelle hat ($r \in \{0,\dots,7\}$).

Wir entwickeln $f_r(Y)$ für $r=0,\dots,7$ in 3-adische Reihen (Y Unbestimmte über $\mathbb{Z}$):

$$f_r(Y) = \sum_{n=0}^{\infty} 3^n(-1323-128\sqrt{-7})^n\binom{Y}{n}(1+\sqrt{-7})^r$$
$$- \sum_{n=0}^{\infty} 3^n(-1323+128\sqrt{-7})^n\binom{Y}{n}(1-\sqrt{-7})^r$$
$$- \sum_{n=0}^{\infty} 3^n \cdot 85^n\binom{Y}{n}\, 2^r \ .$$

Man darf $f_r(Y)$ nach der $\mathbb{Q}$-Basis $(1, \sqrt{-7})$ von K (= $\mathbb{Q}_3$-Basis von K_3) umordnen (siehe Einleitung 1)). Die ersten drei Glieder davon schreiben wir für $r=0,\dots,7$ an:

$$f_0(Y) = [-3.85Y-3^2.85^2(\tfrac{Y}{2})+3^3\ldots] + [-1-3.256Y+3^2.677376(\tfrac{Y}{2})+3^3\ldots]\sqrt{-7}$$

Nach Satz 1 hat die Reihe der ersten Komponente höchstens eine Nullstelle, nämlich y=0 (Grad(85Y) = 1), die der zweiten Komponente aber keine Nullstelle (Grad(-1) = 0), sodaß f_o keine Nullstelle in $\mathbb{Z}$ besitzt.

$$f_1(Y) = [3.170Y+3^2.2.85^2(\tfrac{Y}{2})+3^3\ldots] + [3(-2902)Y+3^2.3948658(\tfrac{Y}{2})+3^3\ldots]\sqrt{-7}$$

Da 170 und -2902 3-adische Einheiten sind und Grad(170Y)= Grad(-2902Y)=1, hat f_1 genau die Nullstelle y=0, woraus sich für f die Nullstelle 8.0+1=1 ergibt.

$$f_2(Y) = [3.4.85Y+3^2.4.85^2(\tfrac{Y}{2})+3^3\ldots] + [3^2(-1252)Y+4.1635641(\tfrac{Y}{2}))+3^3.4.338688(\tfrac{Y}{2})+3^4\ldots]\sqrt{-7}$$

hat wie $f_1(Y)$ nur die Nullstelle 0, was für f die Nullstelle 8.0+2=2 ergibt.

$$f_3(Y) = [-3.8.85Y-3^2.8.85^2(\tfrac{Y}{2})+3^3\ldots] + [-16+3.40.128Y-3^2\ldots]\sqrt{-7}$$

hat keine Nullstelle.

Ebenso haben

$$f_4(Y) = [3.16.85Y-3^2.16.85^2(\tfrac{Y}{2})+\ldots] + [-64-3.16.128Y+3^2\ldots]\sqrt{-7},$$

$$f_5(Y) = [3.32.85Y-3^2.32.85^2(\tfrac{Y}{2})+3^3\ldots] + [-64-3.2.176.128Y+3^2\ldots]\sqrt{-7},$$

$$f_6(Y) = [-3.64.85Y-3^2.64.85^2(\tfrac{Y}{2})+\ldots] + [256+3^2\ldots]\sqrt{-7}$$ und

$$f_7(Y) = \left[-3.85.128Y-3^2.85^2.128\binom{Y}{2}+\ldots\right]$$
$$+ \left[3(256+2.832.128Y)+3^2\ldots.\right] \sqrt{-7}$$

nach Satz 1 keine Nullstellen.

Wir erhalten somit das Ergebnis:
$f(x) = (1+\sqrt{-7})^x - (1-\sqrt{-7})^x - \sqrt{-7}.2^x = 0$ ist nur für $x = 1$ und $x = 2$ erfüllt.

II.5 Lineare rekurrente Folgen

Sei K ein algebraischer Zahlkörper und $\{f(n)\}_{n\in\mathbb{N}_0}$ eine Folge in K.

Man nennt $\{f(n)\}_{n\in\mathbb{N}_0}$ linear rekurrent mod h, $h \geq 1$, wenn es rationale Zahlen $c_0,\dots,c_{h-1}$ gibt, sodaß für alle $n\in\mathbb{N}_0$ $f(n+h) = \sum_{j=0}^{h-1} c_j f(n+j)$ gilt.

Ist dabei h kleinstmöglich gewählt, so sind die Zahlen $c_0,\dots,c_{h-1}$ durch $\{f(n)\}_{n\in\mathbb{N}_0}$ eindeutig bestimmt.

Denn sei $f(n+h) = \sum_{j=0}^{h-1} c_j f(n+j) = \sum_{j=0}^{h-1} d_j f(n+j)$ und angenommen, $r := \max\{j;\ c_j \neq d_j\}$ existiert, so ist $f(n+r) = \sum_{j=0}^{r-1} \frac{c_j-d_j}{c_r-d_r} f(m+j)$ im Widerspruch zur Minimalität von h.

Es ist $c_0 \neq 0$, wenn h minimal ist.

In diesem Fall heißt das wohldefinierte Polynom $G(X) := X^h - c_{h-1}X^{h-1} - \dots - c_0$ Begleitpolynom zur rekurrenten Folge $\{f(n)\}_{n\in\mathbb{N}_0}$.

Es soll im Folgenden eine Beziehung zwischen linearen rekurrenten Folgen und Funktionen des Typs

$$f:\ \mathbb{Z} \longrightarrow K,\quad x \longmapsto A_1(x)\beta_1^x + \dots + A_s(x)\beta_s^x,\ A_j \in K[X] \text{ ungleich Null und } 0 \neq \beta_j \in K,$$

hergestellt werden.

Zur Folge $\{f(n)\}_{n\in\mathbb{N}_0}$ gehört die erzeugende Funktion

$$Y := \sum_{n=0}^{\infty} f(n)Z^n \in K[[Z]] .$$

Setzt man $B(Z) := b_0+b_1Z+\dots+b_{h-1}Z^{h-1}$ mit

$b_0 := f(0)$, $b_1 := f(1)-c_{h-1}f(0)$, $b_2 := f(2)-c_{h-1}f(1)-c_{h-2}f(0)$

u.s.w. bis $b_{h-1} := f(h-1)-c_{h-1}f(h-2)- \dots -c_1 f(0)$,

so ist $Y = \dfrac{B(Z)}{1-c_{h-1}Z- \dots - c_0 Z^h}$ (5)

Beweis:

$$\frac{1}{1-c_{h-1}Z- \dots -c_0 Z^h} B(Z) = \sum_{n=0}^{\infty} (c_{h-1}Z+ \dots +c_0 Z^h)^n B(Z)$$

$$= \sum_{n=0}^{\infty} P(n)Z^n \sum_{k=0}^{h-1} b_k Z^k \qquad (P(n) \in \mathbb{Q})$$

$$= \sum_{n=0}^{\infty} \sum_{k=0}^{h-1} b_k P(n)Z^{n+k} = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{h-1} b_k P(n-k)\Big) Z^n .$$

Die letzte Reihe ist gleich Y genau dann, wenn $f(n) = \sum_{k=0}^{h-1} b_k P(n-k)$ für alle $n \in \mathbb{N}_0$.

Nach dem polynomischen Lehrsatz ist $\sum_{n=0}^{\infty} (c_{h-1}Z+ \dots +c_0 Z^h)^n$

$$= \sum_{n=0}^{\infty} \sum_{\substack{k_1+\dots+k_h=n \\ k_i \geq 0}} \binom{n}{k_1,\dots,k_h} (c_{h-1}Z)^{k_1} \cdot \dots \cdot (c_0 Z^h)^{k_h}$$

$$= \sum_{k_1,\dots,k_h=0}^{\infty} \binom{k_1+\dots+k_h}{k_1,\dots,k_h} c_{h-1}^{k_1} \cdot \dots \cdot c_0^{k_h} Z^{k_1+2k_2+\dots+hk_h}$$

$$= \sum_{n=0}^{\infty} \Big(\sum_{k_1+2k_2+\dots+hk_h=n} \binom{k_1+\dots+k_h}{k_1,\dots,k_h} c_{h-1}^{k_1} \cdot \dots \cdot c_0^{k_h} \Big) Z^n$$

Daraus folgt: $P(n) = \sum_{k_1+\dots+hk_h=n} \binom{k_1+\dots+k_h}{k_1,\dots,k_h} c_{h-1}^{k_1} \cdot \dots \cdot c_0^{k_h}$.

Die Folge $\{P(n)\}_{n \in \mathbb{N}_0}$ aber ist wie $\{f(n)\}_{n \in \mathbb{N}_0}$ eine zu G(X) gehörende lineare rekurrente Folge, also $P(n+h) = \sum_{j=0}^{h-1} c_j P(n+j)$.

denn: $\sum_{j=0}^{h-1} c_j P(n+j) =$

$$= \sum_{j=0}^{h-1} c_j \sum_{k_1+\ldots+hk_h=n+j} \binom{k_1+\ldots+k_h}{k_1,\ldots,k_h} c_{h-1}^{k_1} \cdot \ldots \cdot c_0^{k_h}$$

$$= \sum_{j=0}^{h-1} c_j \sum_{k_1+\ldots+hk_h=n+h-(h-j)} \binom{k_1+\ldots+k_h}{k_1,\ldots,k_h} c_{h-1}^{k_1} \cdot \ldots \cdot c_0^{k_h}$$

$$= \sum_{j=0}^{h-1} \sum_{k_1+\ldots+hk_h=n+h} c_j \binom{k_1+\ldots+k_h-1}{k_1,\ldots,k_{h-j}-1,\ldots,k_h} c_{h-1}^{k_1} \cdot \ldots \cdot c_j^{k_{h-j}-1} \cdot \ldots \cdot c_0^{k_h}$$

$$= \sum_{k_1+\ldots+hk_h=n+h} \underbrace{\sum_{j=0}^{h-1} \binom{k_1+\ldots+k_h-1}{k_1,\ldots,k_{h-j}-1,\ldots,k_h}}_{=\binom{k_1+\ldots+k_h}{k_1,\ldots,k_h}} c_{h-1}^{k_1} \cdot \ldots \cdot c_j^{k_{h-j}} \cdot \ldots \cdot c_0^{k_h}$$

$$= P(n+h) \ .$$

Durch vollständige Induktion über n ergibt sich

$f(n) = \sum_{k=0}^{h-1} b_k P(n-k)$, denn:

n=0: $f(0) = b_0 P(0) = b_0$

n=1: $f(1) = b_0 P(1) + b_1 P(0) = b_0 c_{h-1} + b_1$

Gelte die Induktionsannahme.

$$f(n+1) = f(n+1-h+h) = \sum_{j=0}^{h-1} c_j f(n+1-h+j)$$

$$\overset{(I.A.)}{=} \sum_{j=0}^{h-1} c_j \sum_{k=0}^{h-1} b_k P(n+1-h+j-k)$$

$$= \sum_{k=0}^{h-1} b_k \underbrace{\sum_{j=0}^{h-1} c_j P(n+1-h-k+j)}_{=P(n+1-k)}$$

Insgesamt ist also Gleichung (5) richtig.

Y läßt sich umformen in $Y = \frac{B(Z)}{1-c_{h-1}Z-\ldots-c_0 Z^h} =$

$$= \frac{B(Z)}{Z^h G(Z^{-1})} = \frac{B(Z)}{\prod_{i=1}^{T} \prod_{j=1}^{n_i} (1-\beta_{i,j}Z)^{m_i}} ,$$

wobei $G = \prod_{i=1}^{T} G_i^{m_i}$ die Zerlegung von G in Potenzen verschiedener Primteiler und $\beta_{i,1},\ldots,\beta_{i,n}$ die paarweise verschiedenen Nullstellen der G_i im algebraischen Zahlkörper $L := K(\beta_{1,1},\ldots,\beta_{1,n_1},\ldots,\beta_{T,1},\ldots,\beta_{T,n_T})$ seien (die G_i sind separabel).

Mit Partialbruchzerlegung folgt weiter:

$$Y = \sum_{i=1}^{T} \sum_{j=1}^{n_i} \sum_{r=1}^{m_i} \frac{\gamma_{i,j}}{(1-\beta_{i,j}Z)^r} \quad \text{mit } \gamma_{i,j} \in L.$$

$$\frac{1}{(1-\beta_{i,j}Z)^r} = \Big(\sum_{n=0}^{\infty} (\beta_{i,j}Z)^n \Big)^r =$$

$$= \sum_{n=0}^{\infty} \Big(\sum_{k_1=0}^{n} \sum_{k_2=0}^{k_1} \cdots \sum_{k_{r-1}=0}^{k_{r-2}} (\beta_{i,j}Z)^n \Big)$$

$$= \sum_{n=0}^{\infty} A_{r-1}(n)(\beta_{i,j}Z)^n , \text{ wobei}$$

$A_{r-1} \in \mathbb{Q}[X]$ ein Polynom (r−1)-ten Grades ist ($r \geq 2$, $k_0 = n$).

(Induktion über r; vgl. Lit.10, §18, Seite 64)

Also wird $Y = \sum_{i=1}^{T} \sum_{j=1}^{n_i} \sum_{r=1}^{m_i} \gamma_{i,j} \sum_{n=0}^{\infty} A_{r-1}(n)\beta_{i,j}^n Z^n$

$$= \sum_{n=0}^{\infty} \sum_{i=1}^{T} \sum_{j=1}^{n_i} \underbrace{\sum_{r=1}^{m_i} \gamma_{i,j} A_{r-1}(n)}_{=: B_{i,j}(n),\ \text{wobei } B_{i,j} \in L[X] \text{ vom Grad } m_i-1.} \beta_{i,j}^n Z^n$$

Vergleicht man die Koeffizienten mit $Y = \sum_{n=0}^{\infty} f(n)Z^n$, so wird

$$f(n) = \sum_{i=1}^{r} \sum_{j=1}^{n_i} B_{i,j}(n)\beta_{i,j}^{\,n} .$$

Damit haben wir den

Satz 6 (Lit.10,§18.R):

Sei $\{f(n)\}_{n\in\mathbb{N}_0}$ eine lineare rekurrente Folge in einem algebraischen Zahlkörper K mit dem Begleitpolynom

$G(X) = X^h - c_{h-1}X^{h-1} - \ldots - c_0 \in \mathbb{Q}[X]$, $h \geq 1$.

Seien $\beta_1, \ldots, \beta_s$ die verschiedenen Nullstellen von G mit den Vielfachheiten $m_1,\ldots,m_s$ (also $\sum_{i=1}^{s} m_i = h$ und β_i alle ungleich Null wegen $c_0 \neq 0$).

Dann gibt es Polynome $A_1,\ldots,A_s \in K(\beta_1,\ldots,\beta_s)[X]$ mit den Graden $m_1-1,\ldots,m_s-1$, sodaß für alle $n \in \mathbb{N}_0$:

$$f(n) = \sum_{j=1}^{s} A_j(n)\beta_j^{\,n} .$$

Mit diesem Satz folgt sofort:

Satz 7 (Lit.10,§18.T):

Die Voraussetzungen seien wie in Satz 6.

Zusätzlich seien alle β_i und β_i/β_j für $i\neq j$ keine Einheitswurzeln und P(X) ein Polynom mit algebraischen Koeffizienten.

Dann ist $f(n) = P(n)$ für nur endlich viele $n \in \mathbb{N}_0$.

Beweis:

Sei $L = K(\beta_1,\ldots,\beta_s)$ und M der Körper, der durch Adjunktion der Koeffizienten von P zu L entsteht. Dann hat die Funktion

$$f: \mathbb{Z} \longrightarrow M$$
$$x \longmapsto \sum_{j=1}^{s} A_j(x)\beta_j^{\,x} - P(x).1^x$$

nach Satz 5 nur endlich viele Nullstellen.

Bemerkung (Lit.10,§18):

Ist $\{f(n)\}_{n\in\mathbb{N}_0}$ eine lineare rekurrente Folge mit den Voraussetzungen von Satz 7, so kann man angeblich durch sorgfältige Anwendung von Satz 1 zeigen, daß es eine natürliche Zahl N gibt, sodaß keine algebraische Zahl von der Folge mehr als N mal angenommen wird.

Wie Satz 1 dazu verwendet werden kann, ist mir jedoch nicht bekannt. Es wird vermutet, daß diese Zahl N nur vom Grad des Begleitpolynoms der Folge $\{f(n)\}_{n\in\mathbb{N}_0}$ abhängt. Für Folgen, deren Begleitpolynom zweiten Grades ist, soll möglicherweise N = 5 sein.

Ein Beispiel zu Satz 7:

Sei K ein algebraischer Zahlkörper und $\{f(n)\}_{n\in\mathbb{N}_0}$ eine lineare rekurrente Folge mit $f(0) := a_0 \in K$ und $f(1) := a_1 \in K$, die der Gleichung $f(n+2) = f(n+1) - 2.f(n)$ genügt.

Das Begleitpolynom der Folge lautet $G(X) = X^2 - X + 2$ und hat die beiden Nullstellen $\beta_1 := \frac{1+\sqrt{-7}}{2}$ und $\beta_2 := \frac{1-\sqrt{-7}}{2}$.

Hier ist $B(Z) = b_0+b_1Z = a_0+(a_1-a_0)Z$ und

$$Y = \frac{B(Z)}{1-Z+2Z^2} = \frac{a_0+(a_1-a_0)Z}{(1-\beta_1 Z)(1-\beta_2 Z)} = \frac{\gamma_1}{1-\beta_1 Z} + \frac{\gamma_2}{1-\beta_2 Z} =$$

$$= \sum_{n=0}^{\infty} (\gamma_1\beta_1^n+\gamma_2\beta_2^n)Z^n \quad \text{mit } \gamma_1 = \frac{a_1-a_0\beta_2}{\sqrt{-7}} \text{ und } \gamma_2 = \frac{a_0\beta_1-a_1}{\sqrt{-7}}$$

(vgl.Seite 32).

$$\Longrightarrow \quad f(n) = \gamma_1\beta_1^n + \gamma_2\beta_2^n = \frac{1}{\sqrt{-7}}\left((a_1-a_0\beta_2)\beta_1^n+(a_0\beta_1-a_1)\beta_2^n\right).$$

β_1 und β_2 sind keine Einheitswurzeln, und nach dem Beispiel zu Satz 5 hat β_1/β_2 den Betrag 1, ist aber keine Einheitswurzel.

Nach Satz 7 gibt es also kein Polynom mit algebraischen Koeffizienten, das an unendlich vielen Stellen Werte aus der Folge $\{f(n)\}_{n\in\mathbb{N}_0}$ annimmt.

Ein Spezialfall: $f(0) = 0$ und $f(1) = 1$ mit $f(n+2)=f(n+1)-2.f(n)$.

Dann nimmt die Folge den Wert 1 nur in $n=1$ und $n=2$ an.

denn: $f(n) = \frac{1}{\sqrt{-7}} (\beta_1{}^n-\beta_2{}^n) = \frac{1}{\sqrt{-7}} ((\frac{1+\sqrt{-7}}{2})^n - (\frac{1-\sqrt{-7}}{2})^n)$

Aus dem Beispiel zu Satz 5 wissen wir, daß die Gleichung

$$\frac{(1+\sqrt{-7})^x}{2^x\sqrt{-7}} - \frac{(1-\sqrt{-7})^x}{2^x\sqrt{-7}} = 1 \quad \text{oder} \quad (1+\sqrt{-7})^x-(1-\sqrt{-7})^x-\sqrt{-7}\,2^x = 0$$

in ganzen Zahlen nur für $x=1$ und $x=2$ erfüllt ist.

II.6 Diophantische Gleichungen

Satz 5 dient uns jetzt zur Aufstellung eines weiteren Satzes, der durch seine Gestalt schon etwas besser erkennen läßt, wie die bisherigen Ergebnisse mit der Einheitentheorie von Zahlkörpern zusammenhängen, in denen genau eine Fundamentaleinheit existiert.

Satz 8 (Lit.20,Satz 6 oder Lit.21,Satz 5):
Sei K ein algebraischer Zahlkörper vom Grad n, $(\omega_1,\ldots,\omega_n)$ eine $\mathbb{Q}$-Basis von K und $0\neq\alpha\in K$.
Für $x\in\mathbb{Z}$ seien $x_1,\ldots,x_n\in\mathbb{Q}$ so, daß $\alpha^x = x_1\omega_1+\ldots+x_n\omega_n$.
Ist $0\neq F\in\mathbb{Z}[X_1,\ldots,X_n]$ ein Polynom und $|\{x\in\mathbb{Z};F(x_1,\ldots,x_n)=0\}|=\infty$, so gibt es ein $r\in\{0,\ldots,M-1\}$, sodaß $F(x_1,\ldots,x_n) = 0$ für alle $x \equiv r \bmod M$.

Beweis:
Sei p eine Primzahl und zwar so, daß α eine p-adische Einheit in K_p ist. Wie im Beweis von Satz 5 gibt es dann ein $M\in\mathbb{N}$ mit $\alpha^M\equiv 1 \bmod p$, also $\alpha^M = 1+p\beta$, $\beta\in\mathfrak{o}_p$.
Die Funktion: $\mathbb{Z}_p \longrightarrow K_p: x \longmapsto (\alpha^M)^x$ läßt sich somit über $\mathbb{Z}_p$ in die gleichmäßig konvergente Reihe $\sum_{m=0}^{\infty} (p\beta)^m\binom{X}{m}$ entwickeln. Da $\beta\in\mathfrak{o}_p$, hat $\beta^m\in\mathfrak{o}_p$ eine Basisdarstellung $\sum_{j=1}^{n} b_{m,j}\,\omega_j$ mit $b_{m,j}\in\mathbb{Q}_p$, wobei $|b_{m,j}|_p$ beschränkt bleibt für alle m und j.
Also ist für $x\in\mathbb{Z}$ $(\alpha^M)^x = \sum_{m=0}^{\infty} p^m\left(\sum_{j=1}^{n} b_{m,j}\,\omega_j\right)\binom{x}{m} =$

$$= \sum_{j=1}^{n} \left(\sum_{m=0}^{\infty} p^m b_{m,j} \binom{x}{m} \right) \omega_j \quad \text{mit } p\text{-}\lim_{m\to\infty} p^m b_{m,j} = 0. \qquad (6)$$

Sei $r \in \{0,\ldots,M-1\}$

Wir betrachten alle $x \in \mathbb{Z}$ der Form $x = Mx' + r$, $x' \in \mathbb{Z}$.

Für $\alpha^x = x_1\omega_1 + \ldots + x_n\omega_n$ sei $\alpha^{Mx'} = x'_1\omega_1 + \ldots + x'_n\omega_n$

und $\alpha^r = a_{1,r}\omega_1 + \ldots + a_{n,r}\omega_n$ mit x_i, x'_i und $a_{i,r} \in \mathbb{Q}$.

Es folgt: $\alpha^x = \alpha^{Mx'}\alpha^r = \sum_{j=1}^{n} \sum_{i=1}^{n} a_{i,r} x'_j \omega_i \omega_j =$

$$\sum_{j=1}^{n} \sum_{i=1}^{n} a_{i,r}\, x'_j \sum_{h=1}^{n} \gamma_{i,j,h}\, \omega_h = \sum_{h=1}^{n} \Big(\sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,r} \gamma_{i,j,h}\, x'_j \Big) \omega_h$$

mit $\gamma_{i,j,h} \in \mathbb{Q}$. Wegen (6) ist $x'_j = \sum_{m=0}^{\infty} p^m b_{m,j} \binom{x'}{m}$ und daher

$$x_h = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,r} \gamma_{i,j,h} \sum_{m=0}^{\infty} p^m b_{m,j} \binom{x'}{m}$$

$$= \sum_{m=0}^{\infty} \underbrace{\Big(\sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,r} \gamma_{i,j,h}\, b_{m,j} \Big)}_{=: c_{m,h} \in \mathbb{Q}_p} p^m \binom{x'}{m} \quad \text{mit } p\text{-}\lim_{m\to\infty} c_{m,h} p^m = 0.$$

Somit ist die Abbildung: $\mathbb{Z} \longrightarrow \mathbb{Q} : x' \longmapsto x_h$, $1 \le h \le n$,

stetig fortsetzbar zur Abbildung:

$$\mathbb{Z}_p \longrightarrow \mathbb{Q}_p : x' \longmapsto \sum_{m=0}^{\infty} c_{m,h}\, p^m \binom{x'}{m} \quad \text{und}$$

$f_r : \mathbb{Z} \longrightarrow \mathbb{Q} : x' \longmapsto F(x_1,\ldots,x_n)$ stetig fortsetzbar zur

Abbildung: $f_r : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p : x' \longmapsto F\Big(\sum_{m=0}^{\infty} c_{m,1} p^m \binom{x'}{m}, \ldots$

$$\ldots, \sum_{m=0}^{\infty} c_{m,n} p^m \binom{x'}{m} \Big)$$

Gibt es kein $r \in \{0,\ldots,M-1\}$, sodaß f_r die Nullfunktion ist, dann hat jedes f_r nach Satz 4 nur endlich viele Nullstellen und deswegen auch $f: \mathbb{Z} \longrightarrow \mathbb{Q} : x \longmapsto F(x_1,\ldots,x_n)$ nur endlich viele Nullstellen.

Hat also f unendlich viele Nullstellen in $\mathbb{Z}$, so muß es ein $r \in \{0,\ldots,M-1\}$ geben, sodaß f_r die Nullfunktion ist oder damit gleichbedeutend f auf der Restklasse $\{x \in \mathbb{Z};\ x \equiv r \bmod M\}$ identisch verschwindet.

II.6.1 Gleichungssysteme in drei Unbekannten

In diesem Abschnitt stelle ich zwei Sätze über die Endlichkeit der Lösungsanzahl gewisser Gleichungssysteme auf.
Sie dienen dazu, bei konkreten Beispielen prüfen zu können, ob die Anwendung der Skolemschen Methode zur Berechnung der Lösungen auch sinnvoll ist (Endlichkeit der Lösungsanzahl).

Satz 9 (Lit.20,Satz 7):
Sei $(1, \omega_1, \omega_2)$ $\mathbb{Q}$-Basis eines kubischen Zahlkörpers K mit negativer Diskriminante, wobei $\omega_1, \omega_2 \in \mathcal{O}_K$.
Seien σ_1 und σ_2 die beiden nicht-identischen Isomorphismen von K in $\mathbb{C}$ und $f \in \mathbb{Z}[X,Y,Z]$ ein Polynom, dessen höchster homogener Teil über $\mathbb{Q}$ nicht durch das Polynom
$N(X+Y\omega_1+Z\omega_2) := (X+Y\omega_1+Z\omega_2)(X+Y\sigma_1(\omega_1)+Z\sigma_1(\omega_2))(X+Y\sigma_2(\omega_1)+Z\sigma_2(\omega_2))$
$\in \mathbb{Z}[X,Y,Z]$ teilbar ist.
Dann hat das Gleichungssystem

$$\begin{aligned} N(X+Y\omega_1+Z\omega_2) &= 1 \\ f(X,Y,Z) &= 0 \end{aligned} \qquad (7)$$

nur endlich viele Lösungen in $\mathbb{Z}$.

Beweis:
Der Satz stammt von Skolem aus dem Jahr 1933. Der Beweis ist verhältnismäßig langwierig und nicht konstruktiv (indirekte Schlüsse). Er ist deshalb für die Anwendung nicht zu gebrauchen. Aus diesem Grund möchte ich mich auf eine Skizze beschränken:

Es gibt ein algebraisches $t \in \mathbb{C}$, sodaß $K = \mathbb{Q}(t)$ (Satz vom primitiven Element). Nach (Lit.18,Kap.2) ist die Diskriminante von K bis auf einen quadratischen Faktor gleich der Diskrimante des Minimalpolynoms g von t. Das kubische Polynom g hat also eine reelle und zwei komplexe Nullstellen, sodaß K einen reellen und zwei konjugiert komplexe Isomorphismen nach $\mathbb{C}$ besitzt. Nach dem Dirichletschen Einheitensatz gibt es somit in K genau eine Fundamentaleinheit ε. Wir nehmen o.E.d.A. an, daß K und damit ε reell ist.

Das Gleichungssystem (7) führt also zu einem System

$$\begin{aligned} X+Y\omega_1+Z\omega_2 &= \varepsilon^n \\ f(X,Y,Z) &= 0 \quad , \end{aligned} \tag{8}$$

wobei n eine Unbestimmte über $\mathbb{Z}$ ist.

Nach Satz 8 gilt: Ist obiges Gleichungssystem für unendlich viele $(x,y,z,n_o) \in \mathbb{Z}^4$ erfüllt, so gibt es ein $M \in \mathbb{N}$ und ein $r \in \{0,\ldots,M-1\}$, sodaß das System für alle $(x,y,z,n_o) \in \mathbb{Z}^4$ mit $n_o \equiv r \bmod M$ erfüllt ist.

Letzteres kann Skolem jedoch ausschließen.

Er zeigt zunächst mit Hilfe der Tatsache, daß der höchste homogene Teil von f und $N(X+Y\omega_1+Z\omega_2)$ teilerfremd sind, daß die Folge $\left\{\frac{\varepsilon^{n_o}\sigma_1(\varepsilon^{n_o})}{\varepsilon^{n_o}\sigma_2(\varepsilon^{n_o})}\right\}_{n_o \to -\infty}$ nur endlich viele Häufungspunkte (bez. der gewöhnlichen Topologie) besitzt, wenn die n_o eine beliebige Restklasse durchlaufen und $(x,y,z,n_o) \in \mathbb{Z}^4$ Lösungen von (8) sind. Da die Grundeinheit ε größer als 1 gewählt werden kann, geht ε^{n_o} gegen 0 für $n_o \to -\infty$.

Wegen $N(\varepsilon) = \varepsilon\sigma_1(\varepsilon)\sigma_2(\varepsilon) = 1$ gehen dann $\sigma_1(\varepsilon)^{n_o}$ und $\sigma_2(\varepsilon)^{n_o}$ gegen unendlich. Das bedeutet, daß die Folge

$\left\{\frac{\sigma_1(\varepsilon^{n_0})}{\sigma_2(\varepsilon^{n_0})}\right\}_{n_0\to-\infty}$ dieselben endlich vielen Häufungspunkte besitzt wie $\left\{\frac{\varepsilon^{n_0}-\sigma_1(\varepsilon^{n_0})}{\varepsilon^{n_0}-\sigma_2(\varepsilon^{n_0})}\right\}_{n_0\to-\infty}$.

(Begründung: Ist ε_0 Häufungspunkt von $\left\{\frac{\varepsilon^{n_0}-\sigma_1(\varepsilon^{n_0})}{\varepsilon^{n_0}-\sigma_2(\varepsilon^{n_0})}\right\}_{n_0\to-\infty}$

so gibt es eine unendliche Teilmenge $M\subseteq\mathbb{Z}_{<0}$, sodaß ε_0 Grenz=

wert der Teilfolge $\left\{\frac{\varepsilon^m-\sigma_1(\varepsilon^m)}{\varepsilon^m-\sigma_2(\varepsilon^m)}\right\}_{\substack{m\in M\\ m\to-\infty}}$ ist. Dann ist ε_0 aber

auch Grenzwert von $\left\{\frac{-\frac{\varepsilon^m}{\sigma_2(\varepsilon^m)}}{\frac{\varepsilon^m}{\sigma_2(\varepsilon^m)}-1}\right\}_{\substack{m\in M\\ m\to-\infty}}$ + $\left\{\frac{\frac{\varepsilon^m}{\sigma_2(\varepsilon^m)}-\frac{\sigma_1(\varepsilon^m)}{\sigma_2(\varepsilon^m)}}{\frac{\varepsilon^m}{\sigma_2(\varepsilon^m)}-1}\right\}_{\substack{m\in M\\ m\to-\infty}}$

$= \left\{\frac{-\frac{\sigma_1(\varepsilon^m)}{\sigma_2(\varepsilon^m)}}{\frac{\varepsilon^m}{\sigma_2(\varepsilon^m)}-1}\right\}_{\substack{m\in M\\ m\to-\infty}}$ und somit auch von $\left\{\frac{-\frac{\sigma_1(\varepsilon^m)}{\sigma_2(\varepsilon^m)}}{\frac{\varepsilon^m}{\sigma_2(\varepsilon^m)}-1}\right\}_{\substack{m\in M\\ m\to-\infty}}\cdot\left\{\frac{-\varepsilon^m}{\sigma_2(\varepsilon^m)}+1\right\}_{\substack{m\in M\\ m\to-\infty}}$

$= \left\{\frac{\sigma_1(\varepsilon^m)}{\sigma_2(\varepsilon^m)}\right\}_{\substack{m\in M\\ m\to-\infty}}$.

Also ist ε_0 auch Häufungspunkt der Folge $\left\{\frac{\sigma_1(\varepsilon^{n_0})}{\sigma_2(\varepsilon^{n_0})}\right\}_{n_0\to-\infty}$.

Die Umkehrung zeigt man analog.)

Wegen $\left|\frac{\sigma_1(\varepsilon)}{\sigma_2(\varepsilon)}\right| = 1$ liegen alle Folgenglieder auf dem komplexen Einheitskreis. Dabei muß $\frac{\sigma_1(\varepsilon)}{\sigma_2(\varepsilon)}$ sogar eine Einheitswurzel sein, da sich sonst die Folgenglieder dicht auf dem Einheitskreis verteilen würden im Widerspruch zur Endlichkeit der Häufungs= punkte.

Weiter zeigt Skolem, daß als Einheitswurzeln für $\frac{\sigma_1(\varepsilon)}{\sigma_2(\varepsilon)}$ nur $+/-\rho$, $+/-i$ und $+/-i\rho$ in Frage kommen, wobei $\rho^3=1$.

Durch Betrachtung der Körper $\mathbb{Q}(\omega_1)$, $\mathbb{Q}(\omega_1,\sigma_1(\omega_1),\sigma_2(\omega_1))$ und $\mathbb{Q}(\rho)$ und der Diskriminante von $\mathbb{Q}(\omega_1)$ gelangt er zur Fest= stellung, daß $\mathbb{Q}(\omega_1)$ die Gestalt $\mathbb{Q}(\sqrt[3]{d})$ mit $d\in\mathbb{Z}$ haben muß, woraus sich aus der Darstellung von ε in diesem Körper (=K) der Widerspruch ergibt, daß $N(\varepsilon) = d^2c^3 = 1$ mit $c\in\mathbb{Q}$, also

d eine Kubikzahl ist ($\mathbb{Q}(\omega_1)$=K hat den Grad 3).

Der letzte Satz kann noch etwas allgemeiner formuliert werden:

Satz 10 (Lit.20,Satz 8):

Die Bedingungen seien wie in Satz 9 und $0 \neq h \in \mathbb{Z}$.

Dann hat das System

$$N(X+Y\omega_1+Z\omega_2) = h$$
$$f(X,Y,Z) = 0$$

nur endlich viele ganzzahlige Lösungen.

Beweis: Wir führen die Behauptung auf Satz 9 zurück.

Im $\mathbb{Z}$-Modul $M := \langle 1,\omega_1,\omega_2\rangle$ gibt es nur endlich viele nicht-assoziierte Zahlen α mit $N(\alpha) = h$ (siehe Lit.3,Kap.II,§2,Satz 5) ($\{\mathfrak{A}$; $\mathfrak{A}$ Ideal in O_K mit $N(\mathfrak{A}) = |O_K/\mathfrak{A}| = h\}$ ist endlich).

Jede Zahl $\beta \in M$ mit $N(\beta) = h$ läßt sich dann schreiben als $\beta=\alpha\varepsilon$, wo ε eine Einheit in M ist. Sei $\alpha = a+b\omega_1+c\omega_2$ und $\varepsilon = u+v\omega_1+w\omega_2$ mit $a,b,c,u,v,w \in \mathbb{Z}$.

Dann folgt: $\beta = \alpha\varepsilon = (a+b\omega_1+c\omega_2)(u+v\omega_1+w\omega_2) =$

$= (a_1u+a_2v+a_3w)+(b_1u+b_2v+b_3w)\omega_1+(c_1u+c_2v+c_3w)\omega_2 =$

$= x + y\omega_1 + z\omega_2$; $a_i,b_i,c_i \in \mathbb{Z}$.

Man erhält nun alle Lösungen von

$$N(X+Y\omega_1+Z\omega_2) = h$$
$$f(X,Y,Z) = 0,$$

wenn man für jeden Repräsentanten α, $N(\alpha) = h$, das System

$$N(U+V\omega_1+W\omega_2) = 1$$
$$g(U,V,W) = 0$$

mit $g(U,V,W) := f(Ua_1+Va_2+Wa_3, Ub_1+Vb_2+Wb_3, Uc_1+Vc_2+Wc_3)$ (9)
$\in \mathbb{Z}[U,V,W]$ löst.

Die Bedingung des Satzes für g ist erfüllt:

Sei angenommen, daß der höchste homogene Teil g_r von g teilbar ist durch $N(U+V\omega_1+W\omega_2)$, also $g_r(U,V,W) = N(U+V\omega_1+W\omega_2).T(U,V,W)$, $T \in \mathbb{Z}[U,V,W]$.

Die Gleichung läßt sich schreiben als $g_r(U,V,W) = N(U+V\omega_1+W\omega_2).h.\frac{1}{h}.T(U,V,W) = N(U+V\omega_1+W\omega_2)N(a+b\omega_1+c\omega_2)\overline{T}(U,V,W)$ (10)
mit $\overline{T} \in \mathbb{Q}[U,V,W]$.

Die lineare Abbildung: $M \longrightarrow M: \varepsilon \longmapsto \alpha\varepsilon$ ist wegen $\alpha \neq 0$ injektiv, sodaß die zugehörige Matrix $\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}$ invertierbar über $\mathbb{Q}$ und somit die Abbildung $\mathbb{Q}[U,V,W] \longrightarrow \mathbb{Q}[U,V,W]$

$$U \longmapsto a_1U+a_2V+a_3W$$
$$V \longmapsto b_1U+b_2V+b_3W$$
$$W \longmapsto c_1U+c_2V+c_3W$$

ein Ringisomorphismus ist
$\left(\begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}\right)$. Deshalb entspricht dem höchsten homogenen Teil g_r von g nach (9) genau der höchste homogene Teil f_r von f.

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}^{-1} := \begin{pmatrix} a_1' & a_2' & a_3' \\ b_1' & b_2' & b_3' \\ c_1' & c_2' & c_3' \end{pmatrix} \in Gl(3,\mathbb{Q})$$

$$f_r(X,Y,Z) \longmapsto f_r(Ua_1+Va_2+Wa_3, Ub_1+Vb_2+Wb_3, Uc_1+Vc_2+Wc_3) = g_r(U,V,W)$$

$$g_r(U,V,W) \longmapsto g_r(Xa'_1+Ya'_2+Za'_3, Xb'_1+Yb'_2+Zb'_3, Xc'_1+Yc'_2+Zc'_3)$$

Man kommt mit (10) zu dem Widerspruch:

$f_r(X,Y,Z) = N(X+Y\omega_1+Z\omega_2)\ \overline{T}'(X,Y,Z)$, $\overline{T}' \in \mathbb{Q}[X,Y,Z]$.

II.6.2 Zerlegbare Formen in zwei Unbestimmten

Der folgende Satz ist ein Spezialfall des Thueschen Satzes, daß jede irreduzible Form vom Grad ≥ 3 nur endlich viele Lösungen in $\mathbb{Z}$ besitzt. Im Gegensatz zu den Beweisen des allgemeinen Satzes liefert jedoch der hier wiedergegebene Beweis in Verbindung mit Satz 8 eine Methode, in konkret gegebenen Fällen die endlich vielen Lösungen tatsächlich zu berechnen.

Satz 11 (Lit.20,Satz 9):
Sei $F \in \mathbb{Z}[U,V]$ ein homogenes Polynom.
$F(U,1)$ sei irreduzibel über $\mathbb{Q}$, dagegen reduzibel in einem kubischen Zahlkörper K mit negativer Diskriminante. Dann liegen auf den ebenen Kurven $F(U,V) = a$, $0 \neq a \in \mathbb{Z}$, nur endlich viele Punkte (u,v) in $\mathbb{Z}^2$.

Beweis:
Sei $K = \mathbb{Q}(\vartheta)$ und ϑ', ϑ'' die Konjugierten von ϑ.
Dann zerfällt $F(U,1)$ über K in drei konjugierte Faktoren
$F(U,1,\vartheta) \in \mathbb{Z}[\vartheta][U]$,
$F(U,1,\vartheta') \in \mathbb{Z}[\vartheta'][U]$ und
$F(U,1,\vartheta'') \in \mathbb{Z}[\vartheta''][U]$.
Somit läßt sich $F(U,V)$ schreiben als $F(U,V)=N(F(U,V,\vartheta)) := F(U,V,\vartheta)F(U,V,\vartheta')F(U,V,\vartheta'')$, wobei $F(U,V,\vartheta)$ homogen in U und V ist. $F(U,V,\vartheta)$ hat in der Basis $(1,\vartheta,\vartheta^2)$ die Gestalt $f(U,V) + g(U,V)\vartheta + h(U,V)\vartheta^2$, (11)
wobei $f,g,h \in \mathbb{Z}[U,V]$ homogen und alle vom gleichen Grad sind!

Nun ist die Gleichung $F(U,V) = a$ äquivalent zum Gleichungs=system

$$\begin{aligned} N(X+Y\sqrt{n}+Z\sqrt{n}^2) &= a \\ X = f(U,V),\ Y &= g(U,V),\ Z = h(U,V), \end{aligned} \tag{12}$$

wobei X,Y,Z Unbestimmte über $\mathbb{Z}$ sind.

Nach (Lit.17,Satz 56) gilt, daß k+1 Polynome in k Variablen über einem Körper K stets algebraisch abhängig sind (über diesem Körper). Also gibt es ein Polynom $G \in \mathbb{Q}[X,Y,Z]$, $G \neq 0$, sodaß $G(f,g,h)=0$ in U und V.

Es gilt nun: Das Gleichungssystem (12) hat nur endlich viele Lösungen in $\mathbb{Z}^5$ genau dann, wenn das System

$$\begin{aligned} N(X+Y\sqrt{n}+Z\sqrt{n}^2) &= a \\ G(X,Y,Z) &= 0 \end{aligned} \tag{13}$$

nur endlich viele Lösungen in $\mathbb{Z}^3$ besitzt.

Einerseits ist nämlich die Abbildung $(x,y,z,u,v) \longmapsto (x,y,z)$ der Menge der Lösungen von (12) auf die Lösungsmenge von (13) surjektiv. Andererseits gibt es zu einer Lösung $(x,y,z) \in \mathbb{Z}^3$ von (13) nur endlich viele $u,v \in \mathbb{Z}$, sodaß (x,y,z,u,v) eine Lösung von (12) ist. (*)

Der Grund für letzteres liegt darin, daß f,g und h relativ prim zueinander sind. Denn wäre dem nicht so, so hätten also f,g und h einen gemeinsamen Teiler, der keine Konstante ist und außerdem wegen der Homogenität von f,g und h auch homogen sein müßte. Daraus würde aber wegen (11) folgen, daß $F(U,V) = NF(U,V,\sqrt{n})$ einen homogenen Teiler vom Grad ≥ 1 hätte, sodaß $F(U,1)$ reduzibel über $\mathbb{Q}$ wäre im Widerspruch zur Voraussetzung.

Es sind also o.E.d.A. f und g teilerfremd. Nach (Lit.9, Kap.IV,§6) gibt es dann zwei Polynome $P_1,P_2 \in \mathbb{K}[U,V]$ und

$0 \neq Q \in \mathbb{Q}[V]$, sodaß $P_1 f + P_2 g = Q$.
Jede gemeinsame Lösung $(u,v) \in \mathbb{Z}^2$ von $f=0, g=0$ ergibt damit eine Lösung v von $Q=0$.
Analog gibt es P_1', $P_2' \in \mathbb{Q}[U,V]$ und $0 \neq Q' \in \mathbb{Q}[U]$, sodaß $P_1' f + P_2' g = Q'$. Da Q und Q' nur endlich viele Nullstellen haben, hat auch das System $f=0, g=0$ nur endlich viele Lösungen in $\mathbb{Z}^2$. Wegen der Homogenität von f und g gilt dies auch für jedes Gleichungssystem $f=x, g=y$ mit $x,y \in \mathbb{Z}$, womit die Behauptung (*) bewiesen wäre.
Damit nun (13) nur endlich viele Lösungen hat, darf der höchste homogene Teil von G nach Satz 10 nicht durch $N(X+Y\sqrt{\ }+Z\sqrt{\ }^2)$ teilbar sein. G ist aber selbst homogen, sodaß man, wenn notwendig, G so oft durch eine Potenz von $N(X+Y\sqrt{\ }+Z\sqrt{\ }^2)$ dividiert, bis ein Polynom $G_1(X,Y,Z)$ übrigbleibt, das nicht mehr durch $N(X+Y\sqrt{\ }+Z\sqrt{\ }^2)$ teilbar ist.
Die Nullstellen ($\neq(0,0,0)$) von G und G_1 sind dieselben.
Zurückschreitend hat also (13), daraus (12) und deswegen $F(U,V)=a$ nur endlich viele Lösungen.

Beispiele

1)

Mit Satz 11 lassen sich alle irreduziblen kubischen Formen mit negativer Diskriminante behandeln! (zur Definition der Diskriminante siehe III.2)
Diese zerfallen nämlich im kubischen Körper $\mathbb{Q}(\vartheta), \vartheta$ eine Nullstelle der Form, und die Diskriminante von $\mathbb{Q}(\vartheta)$ ist bis auf einen quadratischen Faktor gleich der Diskriminante der kubischen Form (siehe Lit.18,Kap.2).

Es sei hier erwähnt, daß B.Delaunay (1922) und T.Nagell (1928) unabhängig voneinander bewiesen, daß irreduzible kubische Formen mit genau einer reellen Nullstelle (oder äquivalent dazu: negativer Diskriminante) höchstens 5 Lösungen in $\mathbb{Z}^2$ besitzen. Sie benützten jedoch nicht die p-adische Methode in ihren Beweisen.

Für das folgende Beispiel benützte ich eine Tabelle von Fundamentaleinheiten einer Anzahl kubischer Körper mit negativer Diskriminante, die in einer Arbeit von M.Pohst, P.Weiler und H.Zassenhaus 1982 erschien ("On Effective Computation of Fundamental Units I,II", Math.Comp.38,number 157,Jan.1982):

Gegeben ist das den Körper K definierende Polynom
$f = X^3 + 4X^2 + 6X + 1$ mit der negativen Diskriminante -139,
also $K := \mathbb{Q}(\varrho)$, wobei ϱ eine reelle Nullstelle von f ist.
Wir wollen alle ganzzahligen Lösungen der Gleichung

$$X^3 + 4X^2Y + 6XY^2 + Y^3 = 1 \qquad (14)$$

mit der Skolemschen Methode berechnen.
ϱ ist eine Fundamentaleinheit in K, sodaß (14) gleichwertig

ist mit $N(X-\varrho Y) = 1$ oder $X-\varrho Y = +/-\varrho^n$, n Unbestimmte über $\mathbb{Z}$. Es gilt: 44 ist die kleinste natürliche Zahl mit $\varrho^{44} = 1+23\eta$, $\eta \equiv -7-19\varrho-8\varrho^2 \bmod 23$.

Wir setzen $n=44n'+r$ (n' Unbest.über $\mathbb{Z}$) mit $r \in \{0,1,\ldots,43\}$. Die Komponente von $\varrho^{44n'+r}$ in ϱ^2 ist nur für r=0 und r=1 kongruent 0 mod 23, sodaß nur diese beiden Fälle untersucht werden müssen (Computerhilfe).

Wir entwickeln zunächst $\varrho^{44n'}$ in eine gleichmäßig konvergente 23-adische Interpolationsreihe: $\varrho^{44n'} = \sum_{k=0}^{\infty} 23^k \eta^k \binom{n'}{k} = \sum_{k=0}^{\infty} 23^k(-7-19\varrho-8\varrho^2+23\eta')^k\binom{n'}{k}$ $(\eta' \in \mathbb{Z}[\varrho])$ und ordnen diese Reihe nach der Basis $(1, \varrho, \varrho^2)$:

$$\varrho^{44n'} = [1+23(-7)n'+23^2\ldots] + [23(-19)n'+23^2\ldots]\varrho + [23(-8)n'+23^2\ldots]\varrho^2$$

Da $(1, \varrho, \varrho^2)$ auch eine $\mathbb{Q}_{23}$-Basis von K_{23} ist (Lit.3,Kap.IV, §2,Satz 1), folgt

$23(-8)n'+23^2\ldots = 0$ oder $8n'+23\ldots = 0$

Wir suchen also die Nullstellen der Reihe $F = \sum_{i=0}^{\infty} 23^i f_i(X)$ mit $f_0 = 8X$. Da 8 eine 23-adische Einheit ist, können wir Satz 1 anwenden und erhalten, daß F höchstens $\mathrm{Grad}(f_0)$, d.h. eine Nullstelle hat. Eine solche ist $n_0=0$.

Entwickelt man analog $\varrho^{44n'+1}$, so ergibt sich

$$[23.8n'+23^2\ldots] + [1+23.41n'+23^2\ldots]\varrho + [23.13n'+23^2\ldots]\varrho^2$$

und deswegen muß gelten: $13n'+23\ldots = 0$.

Diese Reihe hat wie vorhin auch nur $n_0=0$ als Lösung.

Wir erhalten also insgesamt $X-\varrho Y = +/-\varrho^0, +/-\varrho^1$, woraus sich durch Koeffizientenvergleich die einzigen beiden ganzzahligen Lösungen $\underline{(1,0)}$ und $\underline{(0,1)}$ von (14) ergeben.

Für weitere Beispiele dieser Art verweise ich auf den Anhang.

Ich habe dort mit Hilfe der erwähnten Tabelle von Fundamental=einheiten zahlreiche Gleichungen mit derselben Methode und unter Benützung eines Computers gelöst. Es war so nicht schwierig, relativ schnell eine "günstige" Primzahl zu finden.

B.Delaunay und T.Nagell bewiesen 1922 bzw. 1928 unabhängig voneinander, daß für eine irreduzible kubische Form $f \in \mathbb{Z}[X,Y]$ mit negativer Diskriminante die Gleichung $f=1$ höchstens 5 ganzzahlige Lösungen besitzt. Sie benützten jedoch nicht die Skolemsche Methode in ihren Beweisen (Lit.10,§19).

2)

Ein allgemeineres Beispiel kubischer Formen mit negativer Diskriminante ist die Gleichung $X^3 - dY^3 = 1$, wobei $d \in \mathbb{Z}$ kubikfrei ist. Sie hat außer (1,0) höchstens eine weitere Lösung in $\mathbb{Z}^2$. Der Beweis ist etwas langwierig, stützt sich aber im Prinzip auf dieselben Ideen, die eben demonstriert wurden. Hat $X^3 - dY^3 = 1$ eine nichttriviale Lösung $(x,y) \in \mathbb{Z}^2$ und ist ε eine Grundeinheit von $\mathbb{Q}(\sqrt[3]{d})$ mit der Norm 1, so gilt: $x+y\sqrt[3]{d} = \varepsilon$ oder ε^2. Dieses genauere Resultat wurde 1925 von T.Nagell ebenfalls mit anderen Methoden als die Skolemsche gefunden (Lit.10,§20).

3)

Mit Hilfe der letzten Sätze lösen wir jetzt die Gleichung $F(U,V) := U^6 + 10U^3V^3 - 2V^6 = 1$, die von Skolem in (Lit.20) angegeben wurde: $F(U,1)$ ist irreduzibel über $\mathbb{Q}$, wie man in $\mathbb{Z}/5$ leicht prüfen kann. Sie hat in $\mathbb{Q}(\sqrt[3]{2})$ die Zerlegung

$(U^2-\vartheta+\vartheta^2U)(U^2-\vartheta'+\vartheta'^2U)(U^2-\vartheta''+\vartheta''^2U)$, wobei $\vartheta := \sqrt[3]{2}$,

$\vartheta' := -\frac{\vartheta}{2} + i\frac{\sqrt{3\vartheta^2}}{2}$, $\vartheta'' := -\frac{\vartheta}{2} - i\frac{\sqrt{3\vartheta^2}}{2}$ ($\mathbb{Q}(\vartheta)$ hat eine negative Diskriminante). Es folgt: $F(U,V)=N(U^2-V^2\vartheta+UV\vartheta^2)$

$F(U,V) = 1$ wird also gleichwertig mit

$$\begin{aligned} N(X+Y\vartheta+Z\vartheta^2) &= 1 \\ X = U^2,\ Y = -V^2,\ Z &= UV \end{aligned} \qquad (15)$$

Die Polynome U^2, $-V^2$ und UV sind algebraisch abhängig vermöge der Relation $G = XY+Z^2 \in \mathbb{Z}[X,Y,Z]$ $(G(U^2,-V^2,UV) = 0)$.

Wir lösen also zunächst das System

$$\begin{aligned} N(X+Y\vartheta+Z\vartheta^2) &= 1 \\ XY + Z^2 &= 0 \end{aligned} \qquad (16)$$

$\mathbb{Q}(\vartheta)$ hat die Fundamentaleinheit $\varepsilon := \vartheta-1$ mit $N(\varepsilon)=1$ (siehe Lit.24). Somit wird das Gleichungssystem (16) zu

$$\begin{aligned} X+Y\vartheta+Z\vartheta^2 &= \varepsilon^n \\ XY + Z^2 &= 0 \end{aligned} \qquad (17)$$

Wir haben $\varepsilon^3 = (\vartheta-1)^3 = 1+3\vartheta-3\vartheta^2 \equiv 1 \bmod 3$ und setzen für $n=3n'+r$, $0 \le r < 3$, $\varepsilon^{3n'} = X'+Y'\vartheta+Z'\vartheta^2$; $\varepsilon^0=1$, $\varepsilon^1 = -1+\vartheta$, $\varepsilon^2 = 1-2\vartheta+\vartheta^2$. Durch Koeffizientenvergleich in $\varepsilon^n = \varepsilon^{3n'}\varepsilon^r$ bekommt man für r=0: $X=X'$, $Y=Y'$, $Z=Z'$

r=1: $X= -X'+2Z'$, $Y=X'-Y'$, $Z=Y'-Z'$

r=2: $X=X'+2Y'-4Z'$, $Y= -2X'+Y'+2Z'$, $Z=X'-2Y'+Z'$.

Aus $XY+Z^2$ wird also für

r=0: $X'Y'+Z'^2 =: G_0(X',Y',Z')$

r=1: $-X'^2+Y'^2+Z'^2+2X'Z'+X'Y'-4Y'Z' =: G_1(X',Y',Z')$

r=2: $-X'^2+6Y'^2-7Z'^2-7X'Y'+12X'Z'-4Y'Z' =: G_2(X',Y',Z')$

Wir lösen jetzt die drei Systeme

1) $$\begin{aligned} X'+Y'\vartheta+Z'\vartheta^2 &= (\varepsilon^3)^{n'} \\ G_0(X',Y',Z') &= 0 \end{aligned}$$

2) $X'+Y'\nu'+Z'\nu'^2 = (\varepsilon^3)^{n'}$

$G_1(X',Y',Z') = 0$

3) $X'+Y'\nu'+Z'\nu'^2 = (\varepsilon^3)^{n'}$

$G_2(X',Y',Z') = 0$

$$(\varepsilon^3)^{n'} = (1+3(\nu'-\nu'^2))^{n'} = \sum_{i=0}^{\infty} 3^i(\nu'-\nu'^2)^i\binom{n'}{i}$$

$$= [1+3^2(-4)\binom{n'}{2}+3^3(-2)\binom{n'}{3}+3^4\ldots]$$
$$+ [3n'+3^2\cdot 2\binom{n'}{2}+3^3(-6)\binom{n'}{3}+3^4\ldots]\nu'$$
$$+ [-3n'+3^2\binom{n'}{2}+3^4\cdot 2\binom{n'}{3}+3^5\ldots]\nu'^2 .$$

Koeffizientenvergleich ergibt somit:

$$X' = 1+3^2(-4)\binom{n'}{2}+3^3(-2)\binom{n'}{3}+\ldots$$

$$Y' = 3n'+3^2\cdot 2\binom{n'}{2}+3^3(-2)\binom{n'}{3}+\ldots$$

$$Z' = -3n'+3^2\binom{n'}{2}+3^4\cdot 2\binom{n'}{3}+\ldots$$

Einsetzen in $G_o(X',Y',Z')=0$ erzeugt die Reihe
$3n'+3^2(n'^2+2\binom{n'}{2})+3^3(-4)n'\binom{n'}{2}+\ldots = 0$, die nach Satz 1 höchstens eine Lösung und zwar $n_o' = 0$ besitzt.
Analog erhält man für $G_1(X',Y',Z')=0$ eine Reihe, die kongruent 1 mod 3 ist, also keine Lösung haben kann.
Das Gleiche gilt für $G_2(X',Y',Z')=0$.
Insgesamt ergibt sich also für (17) die einzige Lösung $n_o=0$.
Somit ist in (15) $X=1, Y=Z=0$, woraus sich für $F(U,V)=1$ die einzigen Lösungen $\underline{(+/-1,0)}$ ergeben.

III. P-ADISCHE FUNKTIONEN IN ZWEI UNBESTIMMTEN

III.1 Ein Hauptsatz von Skolem über p-adische Reihen in zwei Unbestimmten

Um auch diophantische Gleichungen lösen zu können, die mit Hilfe der Einheitentheorie algebraischer Zahlkörper auf Exponentialgleichungen mit zwei unbestimmten Exponenten zurückgeführt werden können, bewies Skolem einen zu Satz 1 analogen Satz über Gleichungssysteme in p-adischen Reihen mit zwei Variablen. Es geht hauptsächlich darum, ausreichende und leicht überprüfbare Bedingungen dafür zu finden, daß ein solches System in einer gewissen Weise zu einem Gleichungssystem gleichwertig ist, das aus teilerfremden Polynomen aus $\mathfrak{o}_{\mathfrak{p}}[X,Y]$ besteht, also nur endlich viele Lösungen haben kann.

Satz 12 (Lit.20,Satz 14 und Lit.21,Satz 11):
Sei p eine Primzahl, K ein algebraischer Zahlkörper, $\mathfrak{p}$ ein Primdivisor von $\mathfrak{o}_K$ mit $\mathfrak{p}/\langle p\rangle$ und $\pi \in \mathfrak{o}_K$ ein Primelement mit $\mathfrak{p}/\langle\pi\rangle$, $\mathfrak{p}^2 \nmid \langle\pi\rangle$. Seien $F_1 := \sum_{i=0}^{\infty} \pi^i f_i(X,Y)$ und

$F_2 := \sum_{i=0}^{\infty} \pi^i g_i(X,Y)$ aus $\overline{\mathfrak{o}_{\mathfrak{p}}[X,Y]}$, wobei die Leitkoeffizienten von f_0 und g_0 in $\mathfrak{o}_{\mathfrak{p}}^{\times}$ liegen.
Außerdem gelte: es gibt $P_1,P_2,Q_1,Q_2 \in \mathfrak{o}_{\mathfrak{p}}[X,Y]$ und $\overline{f_0} \in \mathfrak{o}_p[X]$, $\overline{g_0} \in \mathfrak{o}_p[Y]$ mit $\overline{f_0},\overline{g_0} \not\equiv 0 \bmod \mathfrak{p}$, sodaß

$$f_o P_1 + g_o Q_1 \equiv \overline{f_o} \mod \mathfrak{p}$$

und $$f_o P_2 + g_o Q_2 \equiv \overline{g_o} \mod \mathfrak{p}.$$

Dann hat das Gleichungssystem

$$\begin{aligned} F_1(X,Y) &= 0 \\ F_2(X,Y) &= 0 \end{aligned} \tag{18}$$

höchstens $\mathrm{Grad}(\overline{f_o}).\mathrm{Grad}(\overline{g_o})$ Lösungen in $\mathbb{Z}_p^{\,2}$.

Zunächst eine Definition, die wir im Beweis benötigen (Lit.9,Kap.IV,§5): Seien $f = a_o + a_1 X + \ldots + a_n X^n$ und $g = b_o + b_1 X + \ldots + b_m X^m \in K_{\mathfrak{p}}[X]$ zwei Polynome. Dann nennt man

$$\mathrm{Res}(f,g) := \det \begin{pmatrix} a_n, \ldots, a_o, 0, \ldots, 0 \\ \ldots\ldots\ldots\ldots\ldots \\ 0, \ldots, 0, a_n, \ldots, a_o \\ b_m, \ldots, b_o, 0, \ldots, 0 \\ \ldots\ldots\ldots\ldots\ldots \\ 0, \ldots, 0, b_m, \ldots, b_o \end{pmatrix} \begin{matrix} \} \\ \\ \} \\ \} \\ \\ \} \end{matrix} \begin{matrix} m \text{ Zeilen} \\ \\ \\ n \text{ Zeilen} \end{matrix}$$

$= a_n^{\,m} b_m^{\,n} \prod_{i,k} (\alpha_i - \beta_k) \in K_{\mathfrak{p}}$, wobei $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f und $\beta_1, \ldots, \beta_m$ die Nullstellen von g (in einer Erweiterung von $K_{\mathfrak{p}}$) sind, <u>Resultante</u> von f und g. Sie ist Null genau dann, wenn f und g eine Nullstelle gemeinsam haben.

Beweis von Satz 12:

O.E.d.A. nehmen wir an, daß weder f_o noch g_o aus $O_{\mathfrak{p}}^{\,x}$ sind (sonst wäre der Satz trivial). Wir betrachten das System

$$\begin{aligned} \overline{F_1} &:= F_1 P_1 + F_2 Q_1 = 0 \\ \overline{F_2} &:= F_1 P_2 + F_2 Q_2 = 0 \end{aligned} \tag{19}$$

Wegen $f_oP_1+g_oQ_1 = \overline{f_o} + \pi h$ und

$f_oP_2+g_oQ_2 = \overline{g_o} + \pi h'$ $(h,h' \in \mathfrak{o}_{\mathfrak{p}}[X,Y])$,

lassen sich $\overline{F_1},\overline{F_2}$ $\overline{\mathfrak{o}_{\mathfrak{p}}[X,Y]}$ schreiben in der Gestalt

$$\overline{f_o}(X) + \sum_{i=1}^{\infty} \pi^i \overline{f_i}(X,Y) \quad \text{bzw.}$$

$$\overline{g_o}(Y) + \sum_{i=1}^{\infty} \pi^i \overline{g_i}(X,Y) \ , \quad \overline{f_i},\overline{g_i} \in \mathfrak{o}_{\mathfrak{p}}[X,Y].$$

Da jede Lösung von (18) eine Lösung von (19) ist, können wir den Satz für das System (19) beweisen.

Wir nehmen o.E.d.A. an, daß die Leitkoeffizienten von $\overline{f_o}$ und $\overline{g_o}$ aus $\mathfrak{o}_{\mathfrak{p}}^{\times}$ sind, und setzen $\mathrm{Grad}(\overline{f_o}) =: n \geqslant 1$ und $\mathrm{Grad}(\overline{g_o}) =: m \geqslant 1$. Für alle $k \in \mathbb{N}_o$ läßt sich X^{n+k} nach dem Divisionsalgorithmus durch $X^{n+k} = q_k(X)\overline{f_o}(X) + r_k(X)$ darstellen, wobei $q_k,r_k \in \mathfrak{o}_{\mathfrak{p}}[X]$ und $\mathrm{Grad}(r_k) < \mathrm{Grad}(\overline{f_o})$. Dasselbe gilt in Analogie für alle Y^{m+k}, $k \in \mathbb{N}_o$.

Ist $(x,y) \in \mathbb{Z}_p^{\,2}$ eine Lösung von (19), so gilt demnach:

$$\begin{aligned} x^{n+k} &= q_k(x)\overline{f_o}(x) + r_k(x) \\ &= -q_k(x) \sum_{i=1}^{\infty} \pi^i f_i(x,y) + r_k(x) \quad \text{für alle } k \in \mathbb{N}_o, \end{aligned}$$

$$\begin{aligned} y^{m+l} &= q_l(y)\overline{g_o}(y) + r_l(y) \\ &= -q_l(y) \sum_{i=1}^{\infty} \pi^i \overline{g_i}(x,y) + r_l(y) \quad \text{für alle } l \in \mathbb{N}_o \end{aligned}$$

mit $\mathrm{Grad}(r_k) < \mathrm{Grad}(\overline{f_o})$ und $\mathrm{Grad}(r_l) < \mathrm{Grad}(\overline{g_o})$.

Ersetzen wir also in $\overline{f_1}$ und $\overline{g_1}$ alle X^{n+k} und Y^{m+l} durch

$$-q_k(X) \sum_{i=1}^{\infty} \pi^i \overline{f_i}(X,Y) + r_k(X) \quad \text{bzw.}$$

$$-q_l(Y) \sum_{i=1}^{\infty} \pi^i \overline{g_i}(X,Y) + r_l(Y) \quad \text{für } k,l \in \mathbb{N}_o, \text{ so wird}$$

aus (19) ein Gleichungssystem

$$\begin{aligned} \overline{f_o}(X) + \pi \tilde{f}_1(X,Y) + \sum_{i=2}^{\infty} \pi^i f_i'(X,Y) &= 0 \\ \overline{g_o}(Y) + \pi \tilde{g}_1(X,Y) + \sum_{i=2}^{\infty} \pi^i g_i'(X,Y) &= 0 \ , \end{aligned} \tag{20}$$

wo $f_1, g_1, f_i', g_i' \in \mathcal{O}_{\mathcal{P}}[X,Y]$ und $\mathrm{Grad}_X(\tilde{f}_1)$, $\mathrm{Grad}_X(\tilde{g}_1) < \mathrm{Grad}(\overline{f_o})$ und $\mathrm{Grad}_Y(\tilde{f}_1)$, $\mathrm{Grad}_Y(\tilde{g}_1) < \mathrm{Grad}(\overline{g_o})$.
Dabei hat (20) ebenfalls die Lösung $(x,y) \in \mathbb{Z}_p^{\,2}$.
Wiederholt man die gleichen Substitutionen in f_2' und g_2', so erhält man ein Gleichungssystem mit (x,y) als Lösung von der Gestalt

$$\begin{aligned} \overline{f_o}(X) + \pi \tilde{f}_1(X,Y) + \pi^2 \tilde{f}_2(X,Y) + \sum_{i=3}^{\infty} \pi^i f_i''(X,Y) &= 0 \\ \overline{g_o}(Y) + \pi \tilde{g}_1(X,Y) + \pi^2 \tilde{g}_2(X,Y) + \sum_{i=3}^{\infty} \pi^i g_i''(X,Y) &= 0 \end{aligned}$$

mit $f_2, g_2, f_i'', g_i'' \in \mathcal{O}_{\mathcal{P}}[X,Y]$ und $\mathrm{Grad}_X(\tilde{f}_2)$, $\mathrm{Grad}_X(\tilde{g}_2) < \mathrm{Grad}(\overline{f_o})$ und $\mathrm{Grad}_Y(\tilde{f}_2)$, $\mathrm{Grad}_Y(\tilde{g}_2) < \mathrm{Grad}(\overline{g_o})$.

Dieser Prozeß läßt sich ad infinitum fortsetzen (ich erspare mir die umständliche Schreibarbeit des Induktionsschrittes), sodaß das System (19) schließlich die Gestalt

$$\begin{aligned} \overline{F_1} &= \overline{f_o}(X) + \sum_{i=1}^{\infty} \pi^i \tilde{f}_i(X,Y) = 0 \\ \overline{F_2} &= \overline{g_o}(Y) + \sum_{i=1}^{\infty} \pi^i \tilde{g}_i(X,Y) = 0 \end{aligned}$$

annimmt, wobei die Grade der $\tilde{f}_i$ und $\tilde{g}_i$ in X und Y kleiner als die von $\overline{f_o}$ bzw. $\overline{g_o}$ sind.
Setzt man für jedes $\nu \in \mathbb{N}$

$$\overline{f_o}(X) + \sum_{i=1}^{\nu} \pi^i \tilde{f}_i(X,Y) = \overline{f_o}(X) + A_{\nu,1}(X)Y + \ldots + A_{\nu,m-1}(X)Y^{m-1}$$

$\in \mathcal{O}_{\mathcal{P}}[X,Y]$, so sind die Folgen $\left\{A_{\nu+1,1} - A_{\nu,1}\right\}_{\nu \in \mathbb{N}}$, ... , $\left\{A_{\nu+1,m-1} - A_{\nu,m-1}\right\}_{\nu \in \mathbb{N}}$ $\mathcal{P}$-adische Nullfolgen im $\mathcal{O}_{\mathcal{P}}$-Modul $\mathcal{O}_{\mathcal{P}} \oplus \mathcal{O}_{\mathcal{P}} X \oplus \ldots \oplus \mathcal{O}_{\mathcal{P}} X^{n-1}$, sodaß also die Folgen

$\{A_{\nu,1}\}_{\nu\in\mathbb{N}}, \ldots, \{A_{\nu,m-1}\}_{\nu\in\mathbb{N}}$ in diesem Modul konvergieren.

Deswegen ist $\overline{F_1} = \overline{f_o}(X) + A_1(X)Y + \ldots + A_{m-1}(X)Y^{m-1} \in$
$\mathcal{O}_{\mathfrak{p}}[X] \oplus \mathcal{O}_{\mathfrak{p}}[X]Y \oplus \ldots \oplus \mathcal{O}_{\mathfrak{p}}[X]Y^{m-1}$ mit $\mathrm{Grad}(A_1),\ldots,\mathrm{Grad}(A_{m-1}) \leq n-1$.

Analog gilt für $\overline{F_2}$:

$\overline{F_2} = B_o(X) + B_1(X)Y + \ldots + B_{m-1}(X)Y^{m-1} + b_mY^m$ mit $B_i \in \mathcal{O}_{\mathfrak{p}}[X]$, $\mathrm{Grad}(B_i) \leq n$ und $b_m \in \mathcal{O}_{\mathfrak{p}}^{\times}$.

Wir betrachten die Determinante

$$\mathrm{Res}_X(\overline{F_1},\overline{F_2}) := \det \begin{pmatrix} A_{m-1},\ldots,\overline{f_o},0,\ldots,0 \\ \ldots\ldots\ldots\ldots\ldots \\ 0,\ldots,0,A_{m-1},\ldots,\overline{f_o} \\ b_m,B_{m-1},\ldots,B_o,0,\ldots,0 \\ \ldots\ldots\ldots\ldots\ldots \\ 0,\ldots,0,b_m,B_{m-1},\ldots,B_o \end{pmatrix} \equiv$$

$$\det \begin{pmatrix} 0,\ldots,0,\overline{f_o},0,\ldots,0 \\ \ldots\ldots\ldots\ldots\ldots \\ 0,\ldots\ldots\ldots\ldots,0,\overline{f_o} \\ b_m,B_{m-1},\ldots,B_o,0,\ldots,0 \\ \ldots\ldots\ldots\ldots\ldots \\ 0,\ldots,0,b_m,B_{m-1},\ldots,B_o \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} m \text{ Zeilen} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} m-1 \text{ Zeilen} \end{matrix} \mod \mathfrak{p}.$$

Entwickelt man die letzte Determinante z.B. nach der ersten Zeile, so ergibt sich:

$\mathrm{Res}_X(\overline{F_1},\overline{F_2}) \equiv \overline{f_o}(X).b_m^{m-1} \mod \mathfrak{p}$.

Daraus folgt: $\mathrm{Res}_X(\overline{F_1},\overline{F_2}) = b_m^{m-1}\overline{f_o}(X) + \sum_{i=1}^{\infty} \pi^i R_i(X) \in \overline{\mathcal{O}_{\mathfrak{p}}[X]}$.

Die Darstellung von $\overline{F_1}$ und $\overline{F_2}$ ist auch analog wie vorher möglich in der Gestalt:

$\overline{F_1} = A_o'(Y) + A_1'(Y)X + \ldots + A_{n-1}'(Y)X^{n-1} + a_n'X^n \in \mathcal{O}_{\mathfrak{p}}[X,Y]$

mit $a_n' \in \mathfrak{o}_{\mathfrak{p}}[X]$,

$$\overline{F_2} = \overline{g_o}(Y) + B_1'(Y)X + \ldots + B_{n-1}'(Y)X^{n-1} \in \mathfrak{o}_{\mathfrak{p}}[X,Y].$$

Es ist dann $\mathrm{Res}_Y(\overline{F_1},\overline{F_2}) := \det$

$$\begin{pmatrix} a_n', A_{n-1}', \ldots, A_o', 0, \ldots, 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 0, \ldots, 0, a_n', A_{n-1}', \ldots, A_o' \\ B_{n-1}, \ldots, \overline{g_o}, 0, \ldots, 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 0, \ldots, 0, B_{n-1}, \ldots, \overline{g_o} \end{pmatrix}$$

$\equiv \overline{g_o}(Y)^n a_n'^{n-1} \bmod \mathfrak{p}$, also

$$\mathrm{Res}_Y(\overline{F_1},\overline{F_2}) = a_n'^{n-1}\overline{g_o}(Y) + \sum_{i=1}^{\infty} \pi^i S_i(Y) \in \overline{\mathfrak{o}_{\mathfrak{p}}[Y]}\ .$$

Jede Lösung $(x,y) \in \mathbb{Z}_p^{\,2}$ von (20) ist auch Lösung von

$$\begin{aligned} \mathrm{Res}_X(\overline{F_1},\overline{F_2}) &= 0 \\ \mathrm{Res}_Y(\overline{F_1},\overline{F_2}) &= 0 \end{aligned} \qquad (21)$$

Nach Satz 1 hat aber die erste Gleichung höchstens $\mathrm{Grad}(b_m^{\,m-1}\overline{f_o})$ $= n$ und die zweite Gleichung höchstens $\mathrm{Grad}(a_n'^{n-1}\overline{g_o}) = m$ Lösungen x bzw. $y \in \mathbb{Z}_p$, wonach (20) also maximal n.m Lösungen in $\mathbb{Z}_p^{\,2}$ besitzen kann.

Ein für Anwendungen wichtiger Spezialfall ist

Satz 13 (Lit.21,Bem.nach Satz 11):

Die Voraussetzungen seien wie in Satz 12.

Außerdem sei f_o linear, also $f_o = aX+bY+c$ mit a oder $b \not\equiv 0$ mod $\mathfrak{p}$. Dann hat das Gleichungssystem

$$\begin{aligned} F_1(X,Y) &= 0 \\ F_2(X,Y) &= 0 \end{aligned} \qquad (22)$$

höchstens $\mathrm{Grad}(g_o)$ Lösungen in $\mathbb{Z}_p^{\,2}$.

Bemerkung:

Der Unterschied des Beweises von Satz 13 zu dem von Satz 12 besteht darin, daß es hier vermöge der Linearität von f_o möglich ist, das System $F_1 = \sum_{i=0}^{\infty} \pi^i f_i = 0$

$$F_2 = \sum_{i=0}^{\infty} \pi^i g_i = 0$$

auf ein System

$$H_1 = h_{1,0}(X) + \sum_{i=1}^{\infty} \pi^i h_{1,i}(X,Y) = 0$$

$$H_2 = Y + \sum_{i=1}^{\infty} \pi^i h_{2,i}(X,Y) = 0$$

zurückzuführen, in dem $h_{1,0} \not\equiv 0 \bmod \mathfrak{p}$ und $\mathrm{Grad}(h_{1,0}) \leq \mathrm{Grad}(g_o)$. Auf $H_1 = 0$, $H_2 = 0$ ist dann Satz 12 anwendbar. Die zusätzliche Beweisarbeit besteht lediglich im Nachweis von $\mathrm{Grad}(h_{1,0}) \leq \mathrm{Grad}(g_o)$.

Beweis von Satz 13:

O.E.d.A.: $g_o \notin O_{\mathfrak{p}}^{\times}$ und $b \not\equiv 0 \bmod \mathfrak{p}$.

Wir betrachten das System

$$\begin{aligned} F_1(X,Y) &= 0 \\ F_1P_1 + F_2Q_1 &= 0 , \end{aligned} \tag{23}$$

wobei $P_1(X,Y)$ und $Q_1(X,Y)$ nach Voraussetzung so existieren, daß $f_oP_1 + g_oQ_1 \equiv \overline{f_o}(X) \bmod \mathfrak{p}$.

(Der Grund für die Wahl von (23) liegt darin, daß wir f_o als linear und $b \not\equiv 0 \bmod \mathfrak{p}$ angenommen haben. In den anderen Fällen arbeitet man analog mit $F_1=0$, $F_1P_2+F_2Q_2=0$ bzw. $F_1P_1+F_2Q_1=0$, $F_2=0$ bzw. $F_1P_2+F_2Q_2=0$, $F_2=0$).

Man darf nun annehmen, daß der Grad von $\overline{f_o}$ nicht größer als der von g_o ist. Das sieht man z.B. so:

Setzt man $g_o(X,Y) := g_{o,o}(X)+g_{o,1}(X)Y+ \dots +g_{o,k}(X)Y^k$, so ist $\mathrm{Res}_X(f_o,g_o) = \mathrm{Res}_X(aX+bY+c, g_{o,o}(X)+ \dots +g_{o,k}(X)Y^k)$

$$= \det \left(\begin{matrix} b, aX+c, 0, \dots, 0 \\ \dots\dots\dots\dots \\ 0, \dots, 0, b, aX+c \\ g_{o,k}, \dots\dots, g_{o,o} \end{matrix} \right) \Bigg\} \text{ k Zeilen}$$

=(nach der 1.Spalte entwickelt)

$$= +/-g_{o,k}(X)(aX+c)^k +/- bg_{o,k-1}(X)(aX+c)^{k-1} +/- \dots +/- b^k g_{o,o}.$$

Hat g_o den Grad m, so haben die $g_{o,i}$ höchstens den Grad m-i, sodaß also $\mathrm{Res}_X(f_o,g_o)$ höchstens den Grad m hat.
Nach (Lit.17,§41,Satz 116) gibt es $P_1', Q_1' \in \mathcal{O}_{\mathfrak{p}}[X,Y]$ derart, daß $\mathrm{Res}_X(f_o,g_o) \equiv f_o P_1' + g_o Q_1' \bmod \mathfrak{p}$. Man kann also $P_1 := P_1'$, $Q_1 := Q_1'$ und $\overline{f_o} := \mathrm{Res}_X(f_o,g_o)$ setzen und hat dann $\mathrm{Grad}(\overline{f_o}) \leq \mathrm{Grad}(g_o)$. Jede Lösung von (22) ist eine Lösung von (23), das sich in der Gestalt

$$aX+bY+c + \sum_{i=1}^{\infty} \pi^i f_i(X,Y) = 0$$

$$\overline{f_o}(X) + \sum_{i=1}^{\infty} \pi^i \overline{f_i}(X,Y) = 0 ,$$

$\overline{f_i} \in \mathcal{O}_{\mathfrak{p}}[X,Y]$, schreiben läßt. Vermöge der Transformation

$$\mathcal{O}_{\mathfrak{p}}[\![X,Y]\!] \longrightarrow \mathcal{O}_{\mathfrak{p}}[\![X,Y]\!]$$
$$X \longmapsto X$$
$$Y \longmapsto b^{-1}(Y-aX-c)$$

wird aus dem letzten System

$$Y + \sum_{i=1}^{\infty} \pi^i f_i'(X,Y) = 0$$
$$\overline{f_o}(X) + \sum_{i=1}^{\infty} \pi^i g_i'(X,Y) = 0 \qquad (24)$$

mit $f_i', g_i' \in \mathcal{O}_{\mathfrak{p}}[X,Y]$.
Nach Satz 12 hat aber (24) höchstens $\mathrm{Grad}(Y).\mathrm{Grad}(\overline{f_o}) = \mathrm{Grad}(\overline{f_o}) \leq \mathrm{Grad}(g_o)$ Lösungen in $\mathbb{Z}_p^{\,2}$.

Bemerkungen:

1)

Sind f_o und g_o beide linear, also $f_o = aX+bY+e_1$, $g_o = cX+dY+e_2$ ($f_o, g_o \not\equiv 0 \bmod \mathfrak{p}$), so ist die Bedingung

$$f_o P_1 + g_o Q_1 \equiv \overline{f_o}(X) \bmod \mathfrak{p}$$
$$f_o P_2 + g_o Q_2 \equiv \overline{g_o}(Y) \bmod \mathfrak{p}$$

erfüllt, wenn die Funktionaldeterminante von f_o und g_o mod $\mathfrak{p}$ nicht verschwindet, d.h.: $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \not\equiv 0 \bmod \mathfrak{p}$.

Dann kann man nämlich $f_o := (ad-bc)X + (de_1-be_2) \not\equiv 0 \bmod \mathfrak{p}$

und $g_o := (ad-bc)Y + (ae_2-ce_1) \not\equiv 0 \bmod \mathfrak{p}$

setzen, und es ist $df_o - bg_o \equiv \overline{f_o} \bmod \mathfrak{p}$,

$-cf_o + ag_o \equiv \overline{g_o} \bmod \mathfrak{p}$.

2)

Der Beweis von Satz 12 stützt sich im wesentlichen auf Satz 1, indem das Gleichungssystem (18) mit Hilfe der Voraussetzungen des Satzes und unter Benützung von Resultanten auf das System (21) zurückgeführt werden kann. Da darin die Variablen X und Y jeweils nur in einer Gleichung auftreten, ist Satz 1 anwendbar.

3)

Durch Induktion über n, der Anzahl der Gleichungen bzw. Unbestimmten, läßt sich Satz 12 mit Hilfe analoger Betrachtungen von Resultanten verallgemeinern zu:

Satz 12' (Lit.21):

K, p, $\mathfrak{p}$ und π seien wie in Satz 12.

Seien $F_1 := \sum_{i=0}^{\infty} \pi^i f_{i,1} \in \overline{\mathfrak{o}_{\mathfrak{p}}[X_1, \ldots, X_n]}$

.....

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$F_n := \sum_{i=0}^{\infty} \pi^i f_{i,n} \in \overline{\mathcal{O}_{\mathcal{P}}[X_1,\ldots,X_n]},$$

wobei die Leitkoeffizienten der $f_{o,i}$ in $\mathcal{O}_{\mathcal{P}}{}^{x}$ liegen und folgende Bedingungen erfüllt sind: es gibt $P_{i,j} \in \mathcal{O}_{\mathcal{P}}[X_1,\ldots,X_n]$ für $i,j=1,\ldots,n$ und $\overline{f_{o,1}} \in \mathcal{O}_{\mathcal{P}}[X_1]$, ... , $\overline{f_{o,n}} \in \mathcal{O}_{\mathcal{P}}[X_n]$ mit $\overline{f_{o,i}} \not\equiv 0 \bmod \mathcal{P}$, sodaß

$$f_{o,1}P_{1,1} + \cdots + f_{o,n}P_{1,n} \equiv \overline{f_{o,1}} \bmod \mathcal{P}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_{o,1}P_{n,1} + \cdots + f_{o,n}P_{n,n} \equiv \overline{f_{o,n}} \bmod \mathcal{P}.$$

Dann hat das Gleichungssystem

$$F_1 = 0, \ \ldots\ , F_n = 0$$

höchstens $\mathrm{Grad}(\overline{f_{o,1}}) \cdot \ldots \cdot \mathrm{Grad}(\overline{f_{o,n}})$ Lösungen in $\mathbb{Z}_p{}^{n}$.

Den Beweis erspare ich mir aufgrund der umständlichen Schreibarbeiten und weil im wesentlichen kein Unterschied zum Beweis von Satz 12 besteht.

Es gibt auch einen zu Satz 13 analogen Spezialfall von Satz 12':

Satz 13' (Lit.26):

Alle Voraussetzungen seien wie in Satz 12'. Außerdem seien $f_{o,1}, \ldots, f_{o,n}$ alle linear. Dann hat das System

$$F_1 = 0, \ \ldots\ , F_n = 0$$

höchstens eine Lösung in $\mathbb{Z}_p{}^{n}$.

Die Bedingungen des Satzes sind erfüllt, wenn die Funktionaldeterminante der $f_{o,i} \bmod \mathcal{P}$ nicht verschwindet.

4)

Aufgrund von Satz 13, in dem eine obere Schranke für die Lösungsanzahl durch das Produkt der Grade von f_o und g_o angegeben werden kann, vermutete Skolem, daß dies auch im allgemeinen Fall (f_o, g_o haben beliebige Grade) gelten müsse. Für beliebige Körper K (z.B. $K = \mathbb{C}$) ist diese Vermutung wahrscheinlich nicht richtig. Man kann nämlich leicht Beispiele von teilerfremden Polynomen $f, g \in K[X,Y]$ angeben, für die es keine $P_1, P_2, Q_1, Q_2 \in K[X,Y]$ und $0 \neq \overline{f} \in K[X]$, $0 \neq \overline{g} \in K[Y]$ gibt, sodaß

$$fP_1 + gQ_1 = \overline{f},$$
$$fP_2 + gQ_2 = \overline{g}$$

und $\mathrm{Grad}(\overline{f}) \leq \mathrm{Grad}(f)$, $\mathrm{Grad}(\overline{g}) \leq \mathrm{Grad}(g)$ erfüllt ist.

III.2 Invarianten und Kovarianten

In den folgenden Paragraphen werden für Überlegungen zur Existenz gewisser kubischer und biquadratischer Formen Begriffe aus der Invariantentheorie solcher Formen benötigt. Diese sollen hier kurz eingeführt werden.
(Lit.9,Kap.V,§§1-4 und Lit.16)

A) Kubische Formen

Wir setzen $\mathbb{Q}[X,Y]_n := \{ f \in \mathbb{Q}[X,Y]$; f homogen vom Grad n$\}$.
Sei $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2,\mathbb{Q})$.
A bestimmt eine Variablentransformation

$$A: \quad \mathbb{Q}[X,Y]_n \longrightarrow \mathbb{Q}[X,Y]_n$$

$$f = \sum_{i+j=n} a_{i,j} X^i Y^j \longmapsto A(f) := \sum_{i+j=n} a_{i,j} (aX+bY)^i (cX+dY)^j$$

$$=: \sum_{i+j=n} \tilde{a}_{i,j} X^i Y^j$$

Damit können wir eine Gruppenoperation der Gruppe $Gl(2,\mathbb{Q})$ auf $\mathbb{Q}[X,Y]_n$ definieren:

$$Gl(2,\mathbb{Q}) \times \mathbb{Q}[X,Y]_n \longrightarrow \mathbb{Q}[X,Y]_n$$

$$(A,f) \longmapsto Aof := A(f)$$

Die Bahn von $f \in \mathbb{Q}[X,Y]_n$ bezüglich $Gl(2,\mathbb{Q})$ werde bezeichnet mit $[f] := \{ Aof;\ A \in Gl(2,\mathbb{Q}) \}$.
Sei $\mathcal{J} \in \mathbb{Q}[A_{i,j};\ i+j=n]$ ($A_{i,j}$ Unbestimmte über $\mathbb{Q}$)
Für $f = \sum_{i+j=n} a_{i,j} X^i Y^j \in \mathbb{Q}[X,Y]_n$ sei $\mathcal{J}(f)$ definiert als

$$\mathcal{J}(f) := \mathcal{J}(a_{i,j};\ i+j=n) \quad .$$

Dann nennt man $\mathcal{J}$ relative Invariante von f vom Gewicht $\lambda \in \mathbb{N}_0$,

wenn für alle $A \in Gl(2,\mathbb{Q})$ $\mathcal{J}(Aof) = (\det A)^{\lambda}\,\mathcal{J}(f)$, d.h. wenn $\mathcal{J}$ auf $[f]$ konstant ist bis auf Faktoren aus $\mathbb{Q}$.

Sei $C \in \mathbb{Q}[X,Y,A_{i,j};\ i+j=n]$ und $C(f) := C(X,Y,a_{i,j}) \in \mathbb{Q}[X,Y]$.

C heißt <u>(relative) Kovariante</u> von f vom Gewicht $\lambda \in \mathbb{N}_0$, wenn für alle $A \in Gl(2,\mathbb{Q})$: $C(Aof) = (\det A)^{\lambda} C(f)$, also C ist auf $[f]$ konstant bis auf Faktoren aus $\mathbb{Q}$.

Sei nun speziell $f := a_{3,0}X^3 + a_{2,1}X^2Y + a_{1,2}XY^2 + a_{0,3}Y^3 \in \mathbb{Q}[X,Y]_3$. Bekanntlich ist die <u>Diskriminante von f</u> definiert als <u>$D(f)$</u> $:= a_{3,0}^4 \prod_{i<k} (\alpha_i - \alpha_k)^2$, wobei α_j die Nullstellen von $f(X,1)$ sind.

Man kann $D(f)$ auch in den Koeffizienten von f schreiben:

$$D(f) = -27a_{3,0}^2a_{0,3}^2+18a_{3,0}a_{2,1}a_{1,2}a_{0,3}+a_{2,1}^2a_{1,2}^2-4a_{3,0}a_{1,2}^3 -4a_{2,1}^3a_{0,3}\,.$$

Es gilt: die <u>Diskriminante D</u> $:= -27A_{3,0}^2A_{0,3}^2+18A_{3,0}A_{2,1}A_{1,2}A_{0,3} +A_{2,1}^2A_{1,2}^2-4A_{3,0}A_{1,2}^3-4A_{2,1}^3A_{0,3} \in \mathbb{Z}[A_{3,0},A_{2,1},A_{1,2},A_{0,3}]_4$ ist eine relative Invariante von f vom Gewicht 6:

Für alle $A \in Gl(2,\mathbb{Q})$ ist $D(Aof) = (\det A)^6 D(f)$.

Die kubische Form f besitzt auch eine in X,Y quadratische Kovariante H und eine in X,Y kubische Kovariante Q:

$$H(X,Y,A_{3,0},A_{2,1},A_{1,2},A_{0,3}) := -\frac{1}{4}\det\begin{pmatrix} \frac{\partial^2 f}{\partial X^2} & \frac{\partial^2 f}{\partial X \partial Y} \\ \frac{\partial^2 f}{\partial X \partial Y} & \frac{\partial^2 f}{\partial Y^2} \end{pmatrix}_{a_{i,j}\to A_{i,j}}$$

$$= (A_{2,1}X+A_{1,2}Y)^2 - (3A_{3,0}X+A_{2,1}Y)(A_{1,2}X+3A_{0,3}Y)$$

$$\in \mathbb{Z}[X,Y,A_{3,0},A_{2,1},A_{1,2},A_{0,3}]\,,$$

$$Q(X,Y,A_{3,0},A_{2,1},A_{1,2},A_{0,3}) := \det \begin{pmatrix} \frac{\partial f}{\partial X} & \frac{\partial f}{\partial Y} \\ \frac{\partial H}{\partial X} & \frac{\partial H}{\partial Y} \end{pmatrix}_{a_{i,j} \to A_{i,j}}$$

$$\in \mathbb{Z}[X,Y,A_{3,0},A_{2,1},A_{1,2},A_{0,3}] .$$

Zwischen f, D(f), H und Q besteht die wichtige Beziehung:

$$\underline{Q^2 + 27D(f)f^2 = 4H^3} .$$

B) Biquadratische Formen

Sei $f(X,Y) := a_{4,0}X^4+4a_{3,1}X^3Y+6a_{2,2}X^2Y^2+4a_{1,3}XY^3+a_{0,4}Y^4 \in \mathbb{Q}[X,Y]_4$. (binomische Schreibweise)

Dann hat f eine Invariante $\mathcal{J}_1$ vom Gewicht 4 und eine Invariante $\mathcal{J}_2$ vom Gewicht 6:

$$\mathcal{J}_1 := A_{4,0}A_{0,4}-4A_{3,1}A_{1,3}+3A_{2,2}^2 \in \mathbb{Z}[A_{4,0},A_{3,1},A_{2,2},A_{1,3},A_{0,4}]$$

$$\mathcal{J}_2 := \det \begin{pmatrix} A_{4,0} & A_{3,1} & A_{2,2} \\ A_{3,1} & A_{2,2} & A_{1,3} \\ A_{2,2} & A_{1,3} & A_{0,4} \end{pmatrix} = A_{4,0}A_{2,2}A_{0,4}+2A_{3,1}A_{2,2}A_{1,3}- A_{2,2}^3-A_{4,0}A_{1,3}^2-A_{3,1}^2A_{0,4}$$

$$\in \mathbb{Z}[A_{4,0},A_{3,1},A_{2,2},A_{1,3},A_{0,4}]$$

Die Diskriminante von f ist gegeben durch $D = 16(\mathcal{J}_1^3-27\mathcal{J}_2^2)$.

Sie ist eine relative Invariante von f vom Gewicht 12.

C) Äquivalenzklassen

Wir betrachten die Gruppenoperation

$$Sl(2,\mathbb{Z}) \times \mathbb{Z}[X,Y]_n \longrightarrow \mathbb{Z}[X,Y]_n$$

$$(A,f) \longmapsto Aof := A(f) ,$$

wobei $Sl(2,\mathbb{Z}) := \{A \in Gl(2,\mathbb{Z});\ detA = 1\}$ und
A: $\mathbb{Z}[X,Y]_n \longrightarrow \mathbb{Z}[X,Y]_n$ analog wie in A) eine Variablen-transformation ist.

Durch die Bahnen von $\mathbb{Z}[X,Y]_n$ bezüglich $Sl(2,\mathbb{Z})$ wird eine Äquivalenzrelation auf $\mathbb{Z}[X,Y]_n$ bestimmt: $f \sim g :\Leftrightarrow [f] = [g]$

Ist $\mathcal{J}$ eine relative Invariante von $f \in \mathbb{Z}[X,Y]_n$, so gilt hier: $\mathcal{J}(Aof) = \mathcal{J}(f) \in \mathbb{Q}$ für alle $A \in Sl(2,\mathbb{Z})$.

Wir definieren also: $\mathcal{J}([f]) := \mathcal{J}(f)$, wobei f ein beliebiger Vertreter der Äquivalenzklasse $[f]$ ist.

Es gelten nun die beiden wichtigen Tatsachen:

1) Sei $\alpha \in \mathbb{Z}$. Dann gibt es nur endlich viele Äquivalenz-klassen in $\mathbb{Z}[X,Y]_3$, deren Diskriminanten den Wert α haben.

2) Es gibt nur endlich viele Äquivalenzklassen in $\mathbb{Z}[X,Y]_4$, deren relative Invarianten $\mathcal{J}_1$ und $\mathcal{J}_2$ fest vorgegebene Zahlen $\alpha \in \mathbb{Z}$ bzw. $\beta \in \mathbb{Z}$ annehmen!

III.3 Elliptische Kurven

Es soll jetzt gezeigt werden, wie eine elliptische Kurve zurückführbar ist auf eine endliche Anzahl kubischer oder biquadratischer Formen mit negativer Diskriminante, die mit der Skolemschen Methode behandelt werden können. Dabei wird aber nur die theoretische Existenz dieser Formen bewiesen und kein allgemein praktischer Weg gezeigt, diese tatsächlich zu finden. Ein solcher kann nur anhand eines Beispiels erläutert werden.

Wir betrachten elliptische Kurven der Form $Y^2 = X^3 + k$ mit $0 \neq k \in \mathbb{Z}$, genannt Mordellgleichungen, und unterscheiden zwei Fälle:
1) $k > 0$ und 2) $k < 0$. Im zweiten Fall sind die auftretenden Schwierigkeiten erheblich größer als bei $k > 0$. So waren bis 1963 alle Gleichungen mit $0 < k \leq 100$ vollständig gelöst, jedoch blieben für negative $k \geq -100$ noch 20 Gleichungen ungelöst (vgl. W.Ljunggren, On the Diophantine Equation $Y^2 = X^3 + k$, Acta Arithmetica,1963).

Sei zuerst $Y^2 = X^3 + k$, $k \in \mathbb{Z}$ positiv: (25)
Ist (p,q) eine ganzzahlige Lösung von (25), also $q^2 = p^3 + k$, so werde damit die binäre kubische Form
$h_{p,q} = X^3 - 3pXY^2 + 2qY^3 \in \mathbb{Z}[X,Y]$ definiert. $h_{p,q}$ hat die negative Diskriminante $27(4p^3 - 4q^2) = -27.4k$ und liegt somit in einer von endlich vielen Äquivalenzklassen von $\mathbb{Z}[X,Y]_3$ (= Bahnen bezüglich $Sl(2,\mathbb{Z})$) mit dieser Diskriminante.

Wir zeigen jetzt folgendes: Ist $h^{(1)}, \ldots, h^{(s)}$ ein Repräsentantensystem aller Formen mit der Diskriminante $-27.4k$, so gibt es zu jedem $j \in \{1,\ldots,s\}$ höchstens endlich viele $(p,q) \in \mathbb{Z}^2$, sodaß $h_{p,q} \in [h^{(j)}]$. Diese (p,q) können auch berechnet werden, und zwar mit der Skolemschen Methode, wenn $h^{(j)}$ irreduzibel ist. Somit kann (25) nur endlich viele Lösungen haben.

Sei nun o.E.d.A. $h_{p,q} \in [h^{(1)}]$. Wir schreiben $h^{(1)} = a_{3,0}X^3+a_{2,1}X^2Y+a_{1,2}XY^2+a_{0,3}Y^3$. Es existiert ein $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2,\mathbb{Z})$, sodaß $Aoh^{(1)} = h_{p,q}$ oder $X^3-3pXY^2+2qY^3 =$

$$a_{3,0}(aX+bY)^3+a_{2,1}(aX+bY)^2(cX+dY)+a_{1,2}(aX+bY)(cX+dY)^2+a_{0,3}(cX+dY)^3$$

Koeffizientenvergleich in X^3 und X^2Y ergibt (26)

$$a_{3,0}a^3+a_{2,1}a^2c+a_{1,2}ac^2+a_{0,3}c^3 = h^{(1)}(a,c) = 1 \quad \text{bzw.}$$

$$b\frac{\partial h^{(1)}}{\partial X}(a,c) + \frac{\partial h^{(1)}}{\partial Y}(a,c) = 0 . \tag{26'}$$

Nun hat $h^{(1)}(X,Y) = 1$ nur endlich viele Lösungen in $\mathbb{Z}^2$, unabhängig davon, ob $h^{(1)}$ reduzibel oder irreduzibel über $\mathbb{Q}$ ist:

Denn sei $h^{(1)}$ zunächst reduzibel angenommen. Da die Diskriminante von $h^{(1)}$ ungleich Null ist, sind alle Linearfaktoren von $h^{(1)}$ verschieden. Das heißt, $h^{(1)}(X,Y) = 1$ ist äquivalent zu zwei Gleichungssystemen der Gestalt

$$b_0X^2+b_1XY+b_2Y^2 = 1 \quad \text{und} \quad b_0X^2+b_1XY+b_2Y^2 = -1$$
$$\alpha X+\beta Y = 1 \qquad\qquad \alpha X+\beta Y = -1$$

$(b_0,b_1,b_2,\alpha,\beta \in \mathbb{Z})$, wobei $b_0X^2+b_1XY+b_2Y^2$ und $\alpha X+\beta Y$ teilerfremd sind. Daraus folgt aber, daß auch $h_1 := b_0X^2+b_1XY+b_2Y^2-1$ und $h_2 := \alpha X+\beta Y-1$ teilerfremd sind.

Durch Betrachtung von $\mathrm{Res}_X(h_1,h_2) := \det \begin{pmatrix} b_2, b_1X, b_0X^2-1 \\ \beta, \alpha X-1, 0 \\ 0, \beta, \alpha X-1 \end{pmatrix} \neq 0$

$\mathrm{Res}_Y(h_1,h_2) := \det \begin{pmatrix} b_0, b_1Y, b_2Y^2-1 \\ \alpha, \beta Y-1, 0 \\ 0, \alpha, \beta Y-1 \end{pmatrix} \neq 0$ (vgl. Beweis zu Satz 12, Seite 58) sieht man dann, daß das Gleichungssystem $h_1 = 0$, $h_2 = 0$ nur endlich viele Lösungen in $\mathbb{Z}^2$ haben kann. Dasselbe gilt, wenn man $h_1 = b_0X^2+b_1XY+b_2Y^2+1$ und $h_2 = \alpha X+\beta Y+1$ setzt. Also hat $h^{(1)}(X,Y) = 1$ im Falle "$h^{(1)}$ reduzibel" nur endlich viele Lösungen, die auch berechenbar sind.

Ist $h^{(1)}$ irreduzibel über $\mathbb{Q}$, so hat $h^{(1)}(X,Y) = 1$ nach Satz 11 und Beispiel 1 auch nur endlich viele Lösungen in $\mathbb{Z}^2$, die mit der Skolemschen Methode gefunden werden können.

Die beiden Gleichungen in (26') sind also nur für endlich viele (a,c) und (b,d) $\in \mathbb{Z}^2$ erfüllt (zu jedem $(a,c)\in\mathbb{Z}^2$ existiert unter Berücksichtigung von detA = ad-bc = 1 ein eindeutig bestimmtes $(b,d) = (-\frac{1}{3}\frac{\partial h^{(1)}}{\partial Y}(a,c), \frac{1}{3}\frac{\partial h^{(1)}}{\partial X}(a,c)) \in \mathbb{Z}^2$).

Deshalb können nach Koeffizientenvergleich in (26) auch nur endlich viele $(p,q)\in\mathbb{Z}^2$ existieren, die auf der elliptischen Kurve (25) liegen.

Man kann somit alle ganzzahligen Punkte (p,q) von (25) bestimmen, wenn es gelingt, ein Vertretersystem der endlich vielen Äquivalenzklassen kubischer Formen mit der vorgegebenen Diskriminante -27.4k zu finden.
Da dieses Problem im allgemeinen jedoch schwer lösbar ist,

versucht man bei konkret gegebenen elliptischen Kurven durch Betrachtung quadratischer Körper auf eine endliche und "ausreichende" Anzahl kubischer Formen mit negativer Diskriminante zu gelangen und deren Lösungen z.B. mit der Skolemschen Methode zu ermitteln.

Dazu ein Beispiel (siehe Lit.5):

Gegeben ist die Kurve $Y^2 = 4X^3 + 13$. (27)

Multipliziert man sie mit 16 und setzt $X = 4X$, $Y = 4Y$, so erhält man $Y^2 = X^3 + 208$, sodaß die besprochene Theorie Gültigkeit hat. Der Körper $K := \mathbb{Q}(\sqrt{13})$ hat die Klassenzahl 1, sodaß $\mathcal{O}_K$ $(= \mathbb{Z} + \mathbb{Z}\frac{1}{2}(1+\sqrt{13}))$ ein ZPE-Ring ist.

Er besitzt die Fundamentaleinheit $\varepsilon := 1 + \frac{1}{2}(1+\sqrt{13})$.

(27) wird über $\mathcal{O}_K$ zu

$$\frac{Y+\sqrt{13}}{2}\cdot\frac{Y-\sqrt{13}}{2} = (a+b\,\frac{1+\sqrt{13}}{2})^3(a+b\,\frac{1-\sqrt{13}}{2})^3 \quad \text{mit } a,b \in \mathbb{Z},$$

woraus folgt: $\frac{Y+\sqrt{13}}{2} = \varepsilon^{\alpha}(a+b\,\frac{1+\sqrt{13}}{2})^3$, und o.E.d.A.

ist $\alpha = 0, +/-1$. $\alpha = 0$ ist dabei nicht möglich, weil $(a+b\,\frac{1+\sqrt{13}}{2})^3 \in \mathbb{Z}[\sqrt{13}]$. Vergleicht man die Koeffizienten von $\sqrt{13}$ in den beiden Fällen $\alpha = 1$ und $\alpha = -1$, so erhält man $a^3+6a^2b+15ab^2+11b^3 = 1$ bzw.

$$a^3-3a^2b+6ab^2-b^3 = 1 .$$

Wir haben also die beiden Gleichungen

$$X^3+6X^2Y+15XY^2-Y^3 = 1 \quad \text{und} \tag{28}$$

$$X^3-3X^2Y+6XY^2-Y^3 = 1 \tag{29}$$

zu lösen. Die linearen Substitutionen $\binom{X}{Y} = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\binom{X}{Y}$ bzw. $\binom{X}{Y} = \begin{pmatrix}1 & -1\\ 0 & -1\end{pmatrix}\binom{X}{Y}$ führen zur Gleichung

$$h(X,Y) := X^3+3XY^2-3Y^3 = 1 . \tag{30}$$

Man findet alle ganzen Lösungen von (28) und (29), indem man die von (30) bestimmt. h hat die negative Diskrimi= nante -27.13 und ist irreduzibel über $\mathbb{Q}$.
In L := $\mathbb{Q}(\lambda)$, λ reelle Nullstelle von h(X,1), ist $1-\lambda$ eine Fundamentaleinheit. Es ist $(1-\lambda)^3 = 1 + 3(-1+\lambda^2)$, sodaß man analog wie in Beispiel 1 (Satz 11) mit der Prim= zahl 3 weiterrechnet. Man erhält für die Gleichung $X-\lambda Y = +/- (1-\lambda)^n$ in n die einzigen Lösungen 0 und 1, sodaß in (30) (1,0) und (1,1) die einzigen ganzen Lösungen sind. Das ergibt für (28) die Lösungen (1,0),(-1,1) und für (29) (1,0),(0,-1) und schließlich für $Y^2 = 4X^3+13$ die einzigen ganzzahligen Punkte <u>(-1,3), (-1,-3), (3,11)</u> und <u>(3,-11)</u>.

Wir kommen jetzt zum zweiten Fall elliptischer Kurven:
$Y^2 = X^3 + k$, wobei $k < 0$.
Multipliziert man die Gleichung mit 4 und transformiert die Variablen vermöge $\binom{X}{Y} = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix} \binom{X}{Y}$, so erhält man
$Y^2 = 4X^3 + 4k$.
Wir studieren noch etwas allgemeiner die Kurve $Y^2=4X^3+aX+b$ (31)
mit $a,b \in \mathbb{Z}$, wobei die Diskriminante von $4X^3+aX+b$ (wie die von $4X^3+4k$) negativ sei.
Ist (s,t) eine ganzzahlige Lösung von (31), also $t^2 = 4s^3+as+b$, so werde damit die biquadratische Form $h_{s,t} = X^4 - 6sX^2Y^2 + 4tXY^3 + (-a-3s^2)Y^4 \in \mathbb{Z}[X,Y]$ definiert. Sie hat die Invarianten $\mathcal{J}_1 = -a-3s^2+3s^2 = -a$ und $\mathcal{J}_2 = -s(-a-3s^2)+s^3-t^2 = 4s^3+as-t^2 = -b$ und liegt somit

in einer der endlich vielen Äquivalenzklassen biquadratischer Formen mit den Invarianten $\mathcal{J}_1 = -a$ und $\mathcal{J}_2 = -b$.
Wir zeigen wiederum: Ist $h^{(1)}, \ldots, h^{(k)}$ ein Repräsentantensystem aller Formen mit den Invarianten -a und -b, so gibt es zu jedem $j \in \{1,\ldots,k\}$ höchstens endlich viele $(s,t) \in \mathbb{Z}^2$, sodaß $h_{s,t} \in [h^{(j)}]$.
Daraus folgt, daß (31) nur endlich viele Lösungen haben kann.
Sei o.E.d.A. $h_{s,t} \in [h^{(1)}]$ mit

$$h^{(1)} = a_{4,0}X^4+a_{3,1}X^3Y+a_{2,2}X^2Y^2+a_{1,3}XY^3+a_{0,4}Y^4 \quad \in \mathbb{Z}[X,Y].$$

Also existiert ein $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Sl(2,\mathbb{Z})$, sodaß $Aoh^{(1)} = h_{s,t}$

oder $X^4-6sX^2Y^2+4tXY^3+(-a-3s^2)Y^4 = a_{4,0}(\alpha X+\beta Y)^4+$

$a_{3,1}(\alpha X+\beta Y)^3(\gamma X+\delta Y)+a_{2,2}(\alpha X+\beta Y)^2(\gamma X+\delta Y)^2+$

$a_{1,3}(\alpha X+\beta Y)(\gamma X+\delta Y)^3+a_{0,4}(\gamma X+\delta Y)^4$. (32)

Koeffizientenvergleich in X^3 und X^2Y ergibt

$$a_{4,0}\alpha^4+a_{3,1}\alpha^3\gamma+a_{2,2}\alpha^2\gamma^2+a_{1,3}\alpha\gamma^3+a_{0,4}\gamma^4 = h^{(1)}(\alpha,\gamma)=1$$

bzw. $\beta \frac{\partial h}{\partial X}(\alpha,\gamma) + \delta \frac{\partial h}{\partial Y}(\alpha,\gamma) = 0$ (32')

$h^{(1)}$ hat die negative Diskriminante $-16(a^3+27b^2) =$
$= D(4X^3+aX+b)$ und kann deswegen über $\mathbb{Q}$ höchstens in ein Produkt zweier teilerfremder quadratischer Formen oder einer kubischen und einer Linearform zerfallen. Durch ähnliche Überlegungen wie auf Seite 70 und 71 kann man erkennen, daß $h^{(1)}(X,Y) = 1$ im Falle "$h^{(1)}$ reduzibel" nur endlich viele Lösungen besitzt.
Ist $h^{(1)}$ irreduzibel über $\mathbb{Q}$, so hat $h^{(1)} = 1$ nach dem

Satz von Thue (siehe z.B. Lit.3,Kap.IV,§6.3) auch nur endlich viele ganzzahlige Lösungen, die mit der Skolemschen Methode berechnet werden können, weil die Diskriminante von $h^{(1)}$ negativ ist (siehe dazu III.4).

Es sind somit die beiden Gleichungen in (32') nur für endlich viele (α, γ) und $(\beta, \delta) \in \mathbb{Z}^2$ erfüllt (zu jedem $(\alpha, \gamma) \in \mathbb{Z}^2$ existiert eindeutig $(\beta, \delta) = (-\frac{1}{4}\frac{\partial h}{\partial Y}(\alpha, \gamma), \frac{1}{4}\frac{\partial h}{\partial X}(\alpha, \gamma))$ mit $\alpha\delta - \beta\gamma = 1$). Nach Koeffizientenvergleich in (32) können deswegen auch nur endlich viele $(s,t) \in \mathbb{Z}^2$ existieren, die auf der elliptischen Kurve (31) liegen.

Da man im allgemeinen nur schwer ein Vertretersystem der endlich vielen Äquivalenzklassen biquadratischer Formen mit vorgegebenen Invarianten aufstellen kann, sucht man in der Praxis nach anderen Wegen, um Gleichung (31) auf eine endliche Anzahl biquadratischer Formen mit negativer Diskriminante zurückzuführen. Deren Lösungen können dann z.B. mit der Skolemschen Methode berechnet werden.

Auf einem dieser Wege benützt man die Arithmetik kubischer Körper:
So führt beispielsweise die Gleichung $Y^2 = 4X^3 - 3$ durch Arbeiten in $\mathbb{Q}(\vartheta')$, $\vartheta'^3 = 6$, ϑ' reell, auf die beiden Formen $-4X^3Y - 3Y^4$ und $X^4 - 6X^2Y^2 - 4XY^3 - 3Y^4$ mit den Invarianten $J_1 = 0$, $J_2 = 3$ und der Diskriminante $-16.9.27$. (siehe Lit.28)
Auch die Gleichung $Y^2 = X^3 - 7X + 10$ kann durch Rechnen in $\mathbb{Q}(\vartheta')$, ϑ' reelle Nullstelle von $X^3 - 7X + 10$, auf 7 biquadratische Formen zurückgeführt werden, von denen zwei die Invarianten

$\mathcal{J}_1 = \frac{7}{4}$, $\mathcal{J}_2 = -\frac{5}{8}$ und die Diskriminante -83 und die übrigen fünf die Invarianten $\mathcal{J}_1 = 28$, $\mathcal{J}_2 = -40$ und die Diskriminante $-16^3.83$ haben (siehe Lit.4).

III.4 Biquadratische Formen mit negativer Diskriminante

Sei $h(X,Y) := a_{4,0}X^4+a_{3,1}X^3Y+a_{2,2}X^2Y^2+a_{1,3}XY^3+a_{0,4}Y^4 \in \mathbb{Z}[X,Y]$ eine irreduzible biquadratische Form mit negativer Diskriminante. Wir wollen die diophantische Gleichung $h(X,Y) = 1$ mit der Skolemschen Methode lösen und multiplizieren sie dazu mit $a_{4,0}^3$.

Vermöge der Transformation $\binom{X}{Y} = \begin{pmatrix} a_{4,0} & 0 \\ 0 & 1 \end{pmatrix} \binom{X}{Y}$ erhalten wir daraus

$$f(X,Y) := X^4+b_{3,1}X^3Y+b_{2,2}X^2Y^2+b_{1,3}XY^3+b_{0,4}Y^4 = a_{4,0}^3 \qquad (33)$$

mit $b_{i,j} \in \mathbb{Z}$.

f ist ebenfalls irreduzibel mit negativer Diskriminante und, $f(X,1)$ hat deswegen zwei reelle und zwei komplexe Nullstellen. Sei ϑ eine der reellen Nullstellen. Über $K := \mathbb{Q}(\vartheta)$ wird dann (33) zu

$$N(X-Y\vartheta) = a_{4,0}^3 . \qquad (34)$$

Nach (Lit.3,Kap.II,§2,Korollar zu Satz 5) gibt es im $\mathbb{Z}$- Modul $\mathbb{Z}[\vartheta] := \mathbb{Z} + \mathbb{Z}\vartheta + \mathbb{Z}\vartheta^2 + \mathbb{Z}\vartheta^3$ nur endlich viele paarweise nicht-assoziierte Zahlen $\gamma_1, \dots, \gamma_h$ mit der Norm $a_{4,0}^3$.

Der Dirichletsche Einheitensatz (Lit.3,Kap.II,§4,Satz 5) besagt, daß es in $\mathbb{Z}[\vartheta]$ genau zwei Fundamentaleinheiten ε_1 und ε_2 gibt, sodaß sich jede Einheit ε in $\mathbb{Z}[\vartheta]$ darstellen läßt als $\varepsilon = +/- \varepsilon_1^{n_o} \varepsilon_2^{m_o}$ mit $n_o, m_o \in \mathbb{Z}$.

Somit hat jede Zahl α in $\mathbb{Z}[\vartheta]$ mit der Norm $a_{4,0}^3$ die

Gestalt $\alpha = +/- \gamma_i \varepsilon_1^{n_o} \varepsilon_2^{m_o}$ mit $n_o, m_o \in \mathbb{Z}$ und $\gamma_i \in \{\gamma_1, \dots, \gamma_h\}$.

Gleichung (34) wird also zu

$$X - Y\nu' = +/- \gamma_i \varepsilon_1^n \varepsilon_2^m \quad . \tag{35}$$

Um diese Gleichung in n und m über $\mathbb{Z}$ zu lösen, wählen wir eine Primzahl p (ob sie die später benötigten Voraus= setzungen für die Anwendung von Satz 12 oder Satz 13 er= füllen wird, bleibt jetzt noch fraglich).

Wie im Beweis zu Satz 5 schon erläutert, gibt es wegen $\varepsilon_1, \varepsilon_2 \in \mathfrak{o}_p^x$ natürliche Zahlen M und N, sodaß $\varepsilon_1^N \equiv 1 \bmod p$ und $\varepsilon_2^M \equiv 1 \bmod p$ ($\varepsilon_1^N = 1 + p\lambda_1$, $\varepsilon_2^M = 1 + p\lambda_2$; $\lambda_1, \lambda_2 \in \mathbb{Z}[\nu]$).

Wir setzen $n = Nn' + r$ und $m = Mm' + s$ mit $r \in \{0, \dots, N-1\}$, $s \in \{0, \dots, M-1\}$ und entwickeln $\gamma_i \varepsilon_1^n \varepsilon_2^m$ für jedes r und s in eine über $\mathbb{Z}_p$ gleichmäßig konvergente Inter= polationsreihe:

$$\gamma_i \varepsilon_1^n \varepsilon_2^m = \gamma_i (\varepsilon_1^N)^{n'} (\varepsilon_2^M)^{m'} \varepsilon_1^r \varepsilon_2^s =$$

$$= \gamma_i \varepsilon_1^r \varepsilon_2^s \sum_{k=0}^{\infty} p^k \lambda_1^k \binom{n'}{k} \sum_{l=0}^{\infty} p^l \lambda_2^l \binom{m'}{l} .$$

Ordnet man diese Reihe nach der $\mathbb{Q}_p$-Basis $(1, \nu', \nu'^2, \nu'^3)$ von K_p, so ergibt Koeffizientenvergleich in ν'^2 und ν'^3 in (35) ein Gleichungssystem

$$\sum_{\tau=0}^{\infty} p^{\nu_\tau} f_{\nu_\tau}^{(i,r,s)}(n',m') = 0$$

$$\sum_{\tau=0}^{\infty} p^{\nu_\tau} g_{\nu_\tau}^{(i,r,s)}(n',m') = 0$$

mit $f_\nu^{(i,r,s)}$, $g_\nu^{(i,r,s)} \in \mathcal{O}_p[n',m']$ für alle

$i \in \{1,\ldots,h\}$, $r \in \{0,\ldots,N-1\}$, $s \in \{0,\ldots,M-1\}$.

Sind für $f_o^{(i,r,s)}$ und $g_o^{(i,r,s)}$ die Bedingungen von Satz 12 erfüllt, so kann eine kleine obere Schranke für die Anzahl der Lösungen in $\mathbb{Z}^2$ angegeben werden. In manchen Fällen ist es sogar möglich, die Lösungen den Reihen direkt "abzulesen", wodurch man also sämtliche ganzen Lösungen von (35) erhält.

Ein Beispiel:

Die für die folgende Gleichung benötigten Fundamentaleinheiten entnahm ich wie im Beispiel 1 zu Satz 11 der 1982 erschienenen Tabelle von M.Pohst, P.Weiler und H.Zassenhaus. Dasselbe gilt für die Ganzheitsbasis des zugehörigen Zahlkörpers K.

Sei $f := X^4 + X^3 + 3X - 1$ mit der Diskriminante -775 die definierende Gleichung für $K := \mathbb{Q}(\rho)$, ρ reelle Nullstelle von f. K besitzt die Ganzheitsbasis $(1, \rho, \rho+\rho^2, \frac{1}{2}(1+2\rho^2+\rho^3))$ und die beiden Fundamentaleinheiten $\varepsilon_1 := \rho$,

$$\varepsilon_2 := 1+\rho+\tfrac{1}{2}(1+2\rho^2+\rho^3) = \tfrac{3}{2} + \rho + \rho^2 + \tfrac{1}{2}\rho^3 .$$

Wir lösen die Gleichung

$$X^4 + X^3Y + 3XY^3 - Y^4 = 1 , \qquad (36)$$

die gleichwertig ist zu

$$X - \rho Y = +/- \varepsilon_1^n \varepsilon_2^m . \qquad (37)$$

Es ist $\varepsilon_1^6 = 1+4(-\rho+\rho^2-\rho^3)$ und

$$\varepsilon_2^6 = 1+4(12+\rho+5\rho^2+4\rho^3) .$$

Wir setzen also $n=6n'+r$, $m=6m'+s$ mit $r,s \in \{0,\dots,5\}$. Dann ist $\varepsilon_1^n \varepsilon_2^m \equiv \varepsilon_1^r \varepsilon_2^s \bmod 4$, und $\varepsilon_1^r \varepsilon_2^s$ hat in der Basis von $\mathcal{O}_K$ eine Darstellung $\varepsilon_1^r \varepsilon_2^s =$

$a+b\rho+c(\rho+\rho^2)+d\,\frac{1}{2}(1+2\rho^2+\rho^3)$ mit $a,b,c,d \in \mathbb{Z}$.

Wir können die Fälle ausschließen, in denen c oder d nicht kongruent 0 mod 4 ist. Schreiben wir $\varepsilon_1^r \varepsilon_2^s$ in der Potenzbasis $(1,\rho,\rho^2,\rho^3)$ von $\mathbb{Z}[\rho]$, so bedeutet das:

$$\varepsilon_1^r \varepsilon_2^s = (a+\tfrac{d}{2}) + (b+c)\rho + (c+d)\rho^2 + \tfrac{1}{2}d\rho^3 \cdot$$

$$= a' + b'\rho + c'\rho^2 + d'\rho^3 \text{ mit } a',b',c',d' \in \mathbb{Q},$$

wo uns nur die Fälle interessieren, in denen $a',b',c',d' \in \mathbb{Z}$ und $c' \equiv 0 \bmod 4$ und $d' \equiv 0 \bmod 2$ gilt.
Ich habe $\varepsilon_1^r \varepsilon_2^s$ für alle $r,s \in \{0,\dots,5\}$ berechnet und gefunden, daß obige Bedingung nur für $(r,s) \in \{(0,0),(1,0),(1,3)\}$ erfüllt ist.

1) $\underline{(r,s) = (0,0)}$

Wir entwickeln $\varepsilon_1^n \varepsilon_2^m = \varepsilon_1^{6n'} \varepsilon_2^{6m'}$ in die auf $\mathbb{Z}_2$ gleichmäßig konvergente Potenzreihe

$$\sum_{k=0}^{\infty} 4^k(-\rho+\rho^2-\rho^3)^k\binom{n'}{k} \sum_{k=0}^{\infty} 4^k(12+\rho+5\rho^2+4\rho^3)^k\binom{m'}{k} \text{ und}$$

ordnen sie nach Potenzen von ρ:

$$\begin{aligned}\varepsilon_1^{6n'} \varepsilon_2^{6m'} = {} & [1+4\cdot 12m'+4^2\dots] \\ & + [4(-n'+m')+4^2\dots]\ \rho \\ & + [4(n'+5m')+4^2\dots]\ \rho^2 \\ & + [4(-n'+4m')+4^2\dots]\ \rho^3\end{aligned}$$

Es folgt:
$$\begin{aligned}(n'+5m') + 4\dots &= 0 \\ (-n'+4m') + 4\dots &= 0 \ .\end{aligned} \qquad (38)$$

Da det $\begin{pmatrix} 1 & 5 \\ -1 & 4 \end{pmatrix} = 9 \not\equiv 0 \bmod 2$, hat das System (38) nach Satz 13 + Bemerkung 1 höchstens eine Lösung in $\mathbb{Z}^2$, nämlich (0,0). Für (37) ergibt sich daraus $X - \rho Y = +/- 1$ und somit die beiden Lösungen (+/- 1,0) von (36) .

2) $\underline{(r,s) = (1,0)}$

Hier ist $\varepsilon_1^{6n'+1} \varepsilon_2^{6m'} = [4(-n'+4m')+4^2\ldots]$
$+ [1+4.3n'+4^2\ldots]\ \rho$
$+ [4(-n'+m')+4^2\ldots]\ \rho^2$
$+ [4(2n'+m')+4^2\ldots]\ \rho^3$,

also
$$\begin{aligned} (-n'+m')+4\ldots &= 0 \\ (2n'+m')+4\ldots &= 0 \ . \end{aligned} \qquad (39)$$

Da det $\begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} = -3 \not\equiv 0 \bmod 2$, hat (39) genau die Lösung (0,0) . Somit ist in (37) $X - \rho Y = +/- \rho$, was aber für (36) keine Lösung ergibt.

3) $\underline{(r,s) = (1,3)}$

$\varepsilon_1^{6n'+1} \varepsilon_2^{6m'+3} = [2+4(-n'+28m')+4^2\ldots]$
$+ [1+4(n'+2m')+4^2\ldots]\ \rho$
$+ [4(n'+11m')+4^2\ldots]\ \rho^2$
$+ [4.9m'+4^2\ldots]\ \rho^3$,

also
$$\begin{aligned} (n'+11m')+4\ldots &= 0 \\ 9m'+4\ldots &= 0 \end{aligned} \qquad (40)$$

Wiederum ist det $\begin{pmatrix} 1 & 11 \\ 0 & 9 \end{pmatrix} = 9 \not\equiv 0 \bmod 2$, sodaß (40) genau eine Lösung, nämlich (0,0) besitzt. Für (37) bedeutet das $X - \rho Y = +/- \varepsilon_1 \varepsilon_2^3 = +/- (2+\rho)$, woraus wir für (36) die beiden Lösungen (2,-1) und (-2,1) erhalten.

Es gilt also insgesamt:

Die Gleichung $X^4 + X^3Y + 3XY^3 - Y^4 = 1$ hat die einzigen ganzzahligen Lösungen $(1,0)$, $(-1,0)$, $(2,-1)$ und $(-2,1)$.

Weitere Beispiele dieser Art finden sich im Anhang.

III.5 Kubische Formen mit positiver Diskriminante

Während wir Gleichungen f = 1, f kubische Form mit negativer Diskriminante, durch eine "direkte" Anwendung des Hauptsatzes 1 (siehe Beispiel 1 zu Satz 11) lösen können, ist dies jedoch für Gleichungen f = 1, f kubische Form mit positiver Diskriminante, nicht möglich. Das liegt daran, daß f in diesem Fall drei reelle Nullstellen besitzt und deswegen der Körper $\mathbb{Q}(\varrho)$, ϱ eine der Nullstellen von f, genau zwei Fundamentaleinheiten hat. Man käme bei der "direkten" Anwendung der Skolemschen Methode auf Gleichungen der Gestalt

$$\sum_{k=0}^{\infty} p^k f_k(n',m') = 0 ,$$

p eine Primzahl und $f_k \in \mathbb{O}_p[n',m']$, die nicht unbedingt endlich viele Lösungen haben müssen. Man hilft sich hier mit der Invariantentheorie kubischer Formen weiter (siehe III.2.A)). Es besteht ja zwischen f, D(f) und den beiden Kovarianten H und Q die Beziehung

$$Q(X,Y)^2 = 4H(X,Y)^3 - 27D(f)f(X,Y)^2 .$$

Man sucht also zuerst die ganzzahligen Punkte auf der elliptischen Kurve $Q^2 = 4H^3 + k$ in H und Q mit $k = -27D(f)1^2 < 0$, wie in III.3 besprochen wurde.

Ist $(H_o,Q_o) \in \mathbb{Z}^2$ eine der Lösungen, so erhält man vermöge des Systems $H(X,Y) = H_o$

$$Q(X,Y) = Q_o$$

Lösungen von $f(X,Y) = 1$ (H ist eine quadratische Form).

Beispiel:

$f(X,Y) = X^3 - 3XY^2 - Y^3$ mit den Kovarianten

$H(X,Y) = 9(X^2 + XY + Y^2) =: 9H'(X,Y)$

$Q(X,Y) = 27(X^3 + 6X^2Y + 3XY^2 - Y^3) =: 27Q'(X,Y)$ und $D(f)=81$.

Wir erhalten mit $f(X,Y) = 1$

$$27^2Q'^2 = 4.9^3H'^3 - 27.81 \quad \text{oder}$$

$$Q'^2 = 4H'^3 - 3 \qquad (41)$$

N.Tzanakis (siehe Lit.28) löste diese elliptische Kurve 1984 durch Rückführung auf die beiden biquadratischen Formen $-4X^3Y - 3Y^4 = 1$ und $X^4 - 6X^2Y^2 - 4XY^3 - 3Y^4 = 1$ mit den Diskriminanten $-16.9.27$ und fand die einzigen ganzen Punkte $(+/- 1,1)$, $(+/- 37,7)$ von (41).

Er kam damit auf die Systeme

$(X^3+6X^2Y+3XY^2-Y^3,\ X^2+XY+Y^2) = (1,1), (-1,1), (37,7), (-37,7)$

und erhielt für $f(X,Y) = 1$ die Lösungen $(1,0)$, $(0,-1)$, $(-1,1)$, $(2,1)$, $(-3,2)$ und $(1,-3)$.

III.6 Formen fünften Grades in drei Unbestimmten

Mit Hilfe der Sätze 12 und 13 lassen sich auch Gleichungen der Gestalt $N(X+Y\sqrt{\gamma}+Z\sqrt{\gamma'}) = 1$ behandeln, wenn $\sqrt{\gamma}$ und $\sqrt{\gamma'}$ zwei $\mathbb{Q}$-linear unabhängige ganze Zahlen eines algebraischen Zahlkörpers K fünften Grades sind, wobei K genau einen reellen konjugierten Körper besitzt. Denn dann gibt es nach dem Dirichletschen Einheitensatz in K zwei Grundeinheiten, sodaß man nach Vervollständigung des $\mathbb{Z}$-Moduls $\mathbb{Z}\langle 1, \sqrt{\gamma}, \sqrt{\gamma'}\rangle$ zu $\mathbb{Z}\langle 1, \sqrt{\gamma}, \sqrt{\gamma'}, \omega_1, \omega_2\rangle$ durch Koeffizientenvergleich in ω_1 und ω_2 analog wie in III.4 zu einem Gleichungssystem

$$\sum_{\nu=0}^{\infty} p^{\nu} f_{\nu}(X,Y) = 0$$

$$\sum_{\nu=0}^{\infty} p^{\nu} g_{\nu}(X,Y) = 0$$

gelangt (p Primzahl, $f_{\nu}, g_{\nu} \in \mathfrak{o}_p[X,Y]$).

So bewies Skolem beispielsweise für $K := \mathbb{Q}(\sqrt{\gamma})$, $\sqrt{\gamma}$ reelle Nullstelle von X^5-2, daß $N(X+Y\sqrt{\gamma}+Z\sqrt{\gamma}^2) = 1$ höchstens 6 Lösungen in $\mathbb{Z}^3$ besitzt (Lit.20). Drei davon waren ihm bekannt und er vermutete, daß man bei geeigneter Wahl der Primzahl p beweisen könnte, daß es nur diese drei Lösungen gibt.

1977 konnte A.Bremner (siehe Lit.6) Skolems Vermutung bestätigen, und zwar durch Verwendung der Primzahl 251. Er stellte fest, daß 251 eine der ersten Primzahlen ist, die in K vollständig in ein Produkt von Primdivisoren ersten Grades zerfällt.

Das heißt: $\langle 251 \rangle = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_k$, wobei die Grade der Restklassenkörper $\sigma_K/\mathfrak{p}_i$ über $\mathbb{Z}/251$ alle gleich 1 sind.

Es ist fraglich, ob dieser Tatsache eine allgemeine tiefere Bedeutung zugrunde liegt oder ob es nur ein "Zufall" ist, daß ausgerechnet mit dieser Primzahl das Problem gelöst werden konnte.

Das Ergebnis von Bremner lautet: die Gleichung

$N(X+Y\sqrt{7}+Z\sqrt{7}^2) = X^5+2Y^5+4Z^5-10XY^3Z+10X^2YZ^2 = 1$ hat die einzigen ganzzahligen Lösungen $(1,0,0)$, $(-1,1,0)$ und $(1,-2,1)$.

In ähnlicher Weise lassen sich vermutlich durch geeignete Wahl von Primzahlen die folgenden zu $K = \mathbb{Q}(\sqrt{7})$ gehörenden Normgleichungen lösen:

$$N(X+Y\sqrt{7}+Z\sqrt{7}^3) = X^5+2Y^5+8Z^5-20XYZ^3+10X^2Y^2Z = 1 \qquad (42)$$

$$N(X+Y\sqrt{7}^2+Z\sqrt{7}^3) = X^5+4Y^5+8Z^5-10X^3YZ+20XY^2Z^2 = 1 \qquad (43)$$

$$N(X+Y\sqrt{7}+Z\sqrt{7}^4) = X^5+2Y^5+16Z^5-10X^3YZ+20XY^2Z^2 = 1 \qquad (44)$$

$$N(X+Y\sqrt{7}^2+Z\sqrt{7}^4) = X^5+4Y^5+16Z^5-20XY^3Z+20X^2YZ^2 = 1 \qquad (45)$$

$$N(X+Y\sqrt{7}^3+Z\sqrt{7}^4) = X^5+8Y^5+16Z^5-40XYZ^3+20X^2Y^2Z = 1 \qquad (46)$$

Skolem (Lit.20) fand für (42) höchstens 4 ganze Lösungen,
für (43) -"- 3 -"- ,
für (44) -"- 3 -"- ,
für (45) -"- 1 ganze Lösung
und für (46) -"- 1 -"- ,

wobei in (42) (1,0,0), (-1,1,0) und (1,1,1),
in (43) (1,0,0) und (-1,1,1)
und in (44) (1,0,0) und (-1,1,0) bekannt sind.

IV. SCHLUSSBEMERKUNGEN UND BEWERTUNG DER SKOLEMSCHEN METHODE

Ich möchte in diesem Kapitel abschließend noch ein paar nennenswerte Gesichtspunkte der Skolemschen Methode erwähnen und über ihren bis heute gebliebenen Wert sprechen. Ich glaube, man kann dabei die Arbeiten Skolems über die p-adische Methode nach zwei Richtlinien unterscheiden:

1) Ihr Einfluß auf Weiterentwicklungen innerhalb der Theorie der diophantischen Gleichungen. Skolem versuchte unter anderem, den berühmten Satz von Thue über die Endlichkeit der Lösungsanzahl binärer Formen auf Formen in mehr als zwei Variablen zu verallgemeinern. In seiner letzten Arbeit über die p-adische Methode (Lit.23) gelangte er dabei zu einem wichtigen Ergebnis, das spätere Mathematiker wie Claude Chabauty und Wolfgang Schmidt zu einer Vermutung veranlaßte, die in einem Satz von Schmidt aus dem Jahre 1971 ihre Bestätigung fand. Ich werde später noch genauer darauf eingehen.

2) Der praktische Nutzen der Skolemschen Methode zur Lösung konkret gegebener diophantischer Gleichungen.
Die Fragen, die sich hier erheben, sind:
Wo liegen die Grenzen der Anwendbarkeit der Methode?
Welche Schwierigkeiten können bei Berechnungen auftreten?
Wodurch zeichnet sich die Methode besonders aus?

Ich versuchte in dieser Arbeit hauptsächlich an Beispielen, einen Einblick in diese Fragen zu geben. Wie der Leser vermutlich schon bemerkt haben wird, mußte in allen Berechnungen von Anfang an eine wichtige Grundvoraussetzung erfüllt sein, nämlich die Kenntnis der Grundeinheiten des in Frage kommenden Körpers. Bei allen Beispielen, die ich in der Literatur finden konnte, waren im Grunde genommen die Rechnungen zur Aufstellung eines Systems von Grundeinheiten die aufwendigsten. Man könnte noch eine sehr große Zahl diophantischer Gleichungen beliebig hohen Grades und in beliebig vielen Variablen mit Skolems Methode lösen, wenn man das Problem der Berechnung von Fundamentaleinheiten in den Griff bekäme!

Eine weitere stillschweigend angenommene Voraussetzung oder Erleichterung, die ich in meinen Beispielen machte, war folgende: die Beispiele waren immer von der Gestalt $N(X_1 \omega_1 + \ldots + X_n \omega_n) = 1$, also mit $\underline{1}$ auf der rechten Seite statt allgemeiner irgendeine ganze Zahl h. Die Schwierigkeiten, die ich dabei umgehen konnte, betrafen die Berechnung eines Systems paarweise nicht-assoziierter Zahlen $\gamma_1, \ldots, \gamma_k$ mit der Norm h im betreffenden $\mathbb{Z}$-Modul. Könnte man auch dieses Problem auf "vernünftige" Weise lösen, böte sich eine noch größere Zahl von Gleichungen zur Lösung an.

Der Einfachheit halber verwendete ich in allen Beispielen ausschließlich reelle Zahlkörper, in denen die Gruppe der Einheitswurzeln E_K nur aus den Elementen +/- 1 besteht.

Es ist aber i.a. nicht allzu schwierig, auch Gleichungen zu lösen, die zurückführbar sind auf Normgleichungen $X_1\omega_1 + \ldots + X_n\omega_n = \varepsilon\,\varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_k^{n_k}$, wobei ε eine komplexe Einheitswurzel eines Zahlkörpers K ist.
Ist K beispielsweise ein biquadratischer Körper, wo das definierende Polynom f ausschließlich komplexe Wurzeln hat, so kann $\mathbb{Q}(E_K)$ mit Hilfe der Galoistheorie relativ leicht identifiziert werden. Für $f = X^4+a_1X^3+a_2X^2+a_3X+a_4$ und ϱ eine Nullstelle von f hat $K = \mathbb{Q}(\varrho)$ in diesem Falle genau eine Grundeinheit ε, und die Gleichung
$X^4 + a_1X^3Y + a_2X^2Y^2 + a_3XY^3 + a_4Y^4 = 1$ führt auf

$X-\varrho Y = \varepsilon\,\varepsilon^n$, die man mit der Skolemschen Methode behandeln kann.
Obwohl man mit der p-adischen Methode viele Gleichungen lösen kann, bleibt natürlich noch eine große Klasse übrig, bei denen dies auf direktem Wege (also ohne den Umweg über die Invariantentheorie) generell nicht möglich ist. Es handelt sich um Gleichungen mit Formen, deren Grad minus die Anzahl der Unbestimmten kleiner ist als die Anzahl der Grundeinheiten des betreffenden Körpers. Dabei würde man nämlich Gleichungssysteme in p-adischen Funktionen=reihen erhalten, wo die Anzahl der Gleichungen kleiner ist als die Anzahl der Variablen. Es wäre dann nicht mit einer endlichen Zahl von Lösungen zu rechnen.
Ein besonderer Vorteil der Skolemschen Methode gegenüber anderen Verfahren zur Lösung diophantischer Gleichungen liegt, so weit ich abschätzen kann, darin, daß die oberen Schranken, die man für die Lösungsanzahl erhält, in der Regel so klein

sind, daß man durch Anschreiben der ersten paar Glieder der auftretenden p-adischen Reihen alle Lösungen direkt "ablesen" kann.
Hingegen nachteilig ist wohl der Umstand, daß die Rechnungen auf dem Prinzip des "Probierens" beruhen: man kann von vornherein nie wissen, ob die gewählte Primzahl geeignet ist, die Bedingungen der Hauptsätze 1 oder 12 zu erfüllen. Selbst wenn man einen Rechner benützt, können deswegen umfangreiche Berechnungen entstehen, ehe man Erfolg hat (vgl.z.B.III.6: p=251).
Zusammenfassend meine ich, daß Skolems Methode ein im Grunde verblüffend einfaches Mittel darstellt, "große" Ergebnisse zu erhalten, vor allem dann, wenn der Grad und die Variablenanzahl der Gleichungen hoch sind. Skolem selbst sah in der Anwendung seines Verfahrens auf Formen fünften Grades in drei Unbestimmten den besten Beweis für die Brauchbarkeit der Methode (vgl.Lit.26).
Die weiteren Fortschritte hängen nicht so sehr von dieser selbst, als vielmehr von der Weiterentwicklung anderer Gebiete der algebraischen Zahlentheorie, wie z.B. der Einheitentheorie, ab.

Ich komme nun zurück zu Punkt 1), der historischen Bedeutung der Arbeiten Skolems, und formuliere zunächst den anfangs erwähnten Satz von Skolem aus dem Jahre 1935 über eine Verallgemeinerung des Thueschen Resultats (Lit.23,Satz9):

Ist K ein algebraischer Zahlkörper fünften Grades, der genau einen reellen konjugierten Körper besitzt, und sind α, β, γ

$\mathbb{Q}$-linear unabhängige ganze Zahlen in K, so hat die Gleichung $N(\alpha X+\beta Y+\gamma Z) = h \in \mathbb{Z}$ nur endlich viele Lösungen in $\mathbb{Z}^3$.

Dieser Satz gab Grund zur Frage, ob nicht ähnliche Sätze für Körper K beliebigen Grades und Moduln M beliebigen Ranges in K gültig sind. Eine notwendige Bedingung für die Endlichkeit der Lösungsanzahl einer Gleichung $N(\alpha) = h$, $\alpha \in M$, M $\mathbb{Z}$-Modul in K, kann leicht gefunden werden: M darf keinen vollständigen Modul in einem Teilkörper $K' \subseteq K$, der ungleich $\mathbb{Q}$ und kein imaginär-quadratischer Körper ist, darstellen. Zur Erklärung zunächst ein paar Definitionen:

Zwei Moduln M_1 und M_2 heißen ähnlich, falls es ein ß aus K gibt, sodaß $M_1 = \beta M_2$.
Ein Modul M in K stellt einen vollständigen Modul in einem Teilkörper $K' \subseteq K$ dar, falls M einen Teilmodul M' besitzt, der einem vollständigen Modul (Def. Seite 10) in K' ähnlich ist.
Sei also jetzt angenommen, daß ein $\mathbb{Z}$-Modul M in K einen vollständigen Modul in einem Teilkörper K' von K darstellt, wobei K' ungleich $\mathbb{Q}$ und nicht imaginär-quadratisch ist. Es gibt dann in K' mindestens eine Fundamentaleinheit, sodaß die Gleichung $N_{K'/\mathbb{Q}}(\varepsilon) = a \in \mathbb{Z}$ jedenfalls für gewisse a unendlich viele Lösungen hat, wobei $\varepsilon \in M'$, M' vollständig in K' und ähnlich zu einem Teilmodul $\overline{M}$ von M, also $\gamma M' = \overline{M}$ mit $\overline{M} \subseteq M$ und $\gamma \in K$ gilt.
Dann folgt: $N_{K/\mathbb{Q}}(\gamma\varepsilon) = N_{K/\mathbb{Q}}(\gamma) N_{K/\mathbb{Q}}(\varepsilon) =$

$N_{K/\mathbb{Q}}(\gamma) N_{K'/\mathbb{Q}}(\varepsilon)^{[K:K']} = N_{K/\mathbb{Q}}(\gamma) \cdot a^{[K:K']} = b \in \mathbb{Z}$

(o.E.d.A.: $b \in \mathbb{Z}$, denn falls $b \in \mathbb{Q}$, also $b = \frac{b_1}{b_2}$, $b_i \in \mathbb{Z}$

$\Longrightarrow N_{K/\mathbb{Q}}(b_2 \gamma^{\varrho}) = b_2^{[K:\mathbb{Q}]} N_{K/\mathbb{Q}}(\gamma^{\varrho}) = b_2^{[K:\mathbb{Q}]} \frac{b_1}{b_2} \in \mathbb{Z}$).

Das bedeutet: $N_{K/\mathbb{Q}}(\eta) = b$ hat unendlich viele Lösungen $\eta \in \overline{M} \subseteq M$. Also ist die erwähnte Bedingung notwendig für die Endlichkeit der Lösungsanzahl von $N(\alpha) = h \in \mathbb{Z}$, $\alpha \in M$.

Im zitierten Satz von Skolem ist sie natürlich auch erfüllt, da ein Körper fünften Grades ja gar keinen echten Teilkörper ungleich $\mathbb{Q}$ haben kann.
Es wurde nun vermutet, daß die Bedingung nicht nur notwendig sondern auch hinreichend ist für die Endlichkeit der Lösungsanzahl. 1938 wurde die Vermutung von C.Chabauty für Zahlkörper K beliebigen Grades und $\mathbb{Z}$-Moduln vom Rang 3 unter der Bedingung bewiesen, daß K mindestens zwei Paare komplexkonjugierter Körper besitzt. W.Schmidt erledigte 1967 den Fall für Moduln vom Rang 3 ohne Zusatzbedingung und 1971 (Lit.19) konnte er schließlich den gewünschten Satz beweisen:

Sei K ein algebraischer Zahlkörper und M ein $\mathbb{Z}$-Modul in K. Genau dann gibt es ein $h \in \mathbb{Z}$, für welches die Gleichung $N(\alpha) = h$ unendlich viele Lösungen $\alpha \in M$ besitzt, falls M einen vollständigen Modul in einem Teilkörper K' von K darstellt, der weder gleich $\mathbb{Q}$ noch ein imaginär-quadratischer Körper ist.

Schmidt benützte nicht die Skolemsche Methode für den Beweis, der keine Möglichkeit liefert, im gegebenen Fall die endlich vielen Lösungen tatsächlich zu bestimmen.

(Aus dem Satz folgt wiederum leicht der Satz von Thue über die Endlichkeit der Lösungsanzahl binärer irreduzibler Formen vom Grad ≥ 3.)

Eine große Menge von Beispielen für den Schmidtschen Satz kann folgendermaßen konstruiert werden:
Sind p und q Primzahlen und $\sqrt{n} := \sqrt[p]{q}$, dann ist der $\mathbb{Z}$-Modul $M := \langle 1, \sqrt{n}, \sqrt{n}^2, \ldots, \sqrt{n}^{p-2} \rangle$ nicht vollständig in $K := \mathbb{Q}(\sqrt{n})$ vom Grad p. Da K nur die trivialen Teilkörper besitzt, stellt M nur in $\mathbb{Q}$ einen vollständigen Modul dar. Somit hat die Gleichung $N(X_1+X_2\sqrt{n}+\ldots+X_{p-1}\sqrt{n}^{p-2}) = h \in \mathbb{Z}$ nur endlich viele Lösungen in $\mathbb{Z}^{p-1}$.
Für p=5 und q=2 lautet die Gleichung:

$$X_1^5+2X_2^5+4X_3^5+8X_4^5-20X_2X_3^3X_4+20X_1X_3^2X_4^2+20X_2^2X_3X_4^2-20X_1X_2X_4^3$$
$$+10X_1^2X_2X_3^2-10X_1^3X_3X_4-10X_1^2X_2^3+10X_1^2X_2^2X_4 = h.$$

V. ANHANG (RECHENBEISPIELE)

Ich habe hier weitere Beispiele diophantischer Gleichungen in kubischen und biquadratischen Formen mit negativer Diskriminante behandelt, wobei die Lösungsmethode dieselbe wie die in Beispiel 1 zu Satz 11 bzw. in Beispiel zu III.4 ist. Für die Gleichungen benützte ich eine Tabelle von Grundeinheiten kubischer und biquadratischer Körper ("On Effective Computation of Fundamental Units I,II", Math.Comp. 38,number 157,Jan.1982).
Die weitläufigen Rechnungen machte ich mit Hilfe eines Computers.

A) Kubische Formen

Die hier auftretenden Körper $\mathbb{Q}(\rho)$ haben alle die Ganzheitsbasis $(1, \rho, \rho^2)$.

Jedes der Beispiele ist in folgender Weise geschrieben:

1) Angabe der Gleichung $X^3+a_1X^2Y+a_2XY^2+a_3Y^3=1$, $a_i \in \mathbb{Z}$.

2) Angabe der Grundeinheit $\varepsilon = a+b\rho+c\rho^2$ des Körpers $\mathbb{Q}(\rho)$, ρ reelle Nullstelle von $X^3+a_1X^2+a_2X+a_3$.

3) Angabe von $\varepsilon^M = 1+p\eta$ mit $M \in \mathbb{N}$, p Primzahl(potenz),
$\eta \in \mathbb{Z}[\rho]$, $\eta = \eta_1+\eta_2\rho+\eta_3\rho^2 \in \mathbb{Z}[\rho]$.

4) Angabe der Zahlen $r \in \{0,\dots,M-1\}$, für die die Komponente von ε^r in ρ^2 kongruent 0 mod p ist.

5) Angabe der p-adischen Reihen $\varepsilon^{Mn'+r} = \varepsilon^r+p\varepsilon^r(\eta_1+\eta_2\rho+\eta_3\rho^2)n'+p^2\dots$
bzw. $\varepsilon^{Mn'+r} = \varepsilon^r+p\varepsilon^r\eta n'+p^2\varepsilon^r\eta^2\binom{n'}{2}+p^3\varepsilon^r\eta^3\binom{n'}{3}+p^4\dots$
für die in 4) angegebenen $r \in \{0,\dots,M-1\}$.

6) Angabe der aus den in 5) angegebenen Reihen folgenden Gleichungen $\sum_{n=0}^{\infty} p^i f_i(n') = 0$, $f_i \in \mathbb{Z}_p[n']$, mit den jeweils einzigen ganzzahligen Lösungen in n' (geschr. n_o).

7) Angabe aller aus 6) vermöge $X - \rho Y = +/- \varepsilon^{Mn'+r}$ resultierenden ganzzahligen Lösungen von $X^3+a_1X^2Y+a_2XY^2+a_3Y^3=1$.

a) 1) $X^3-2X^2Y-2Y^3 = 1$

2) $\varepsilon = 1+2\rho-\rho^2$

3) $\varepsilon^8 = 1+5\eta$, $\eta \equiv -3-4\rho^2 \bmod 5$

4) 0

5) $\varepsilon^{8n'} = 1+5(-3-4\rho^2)n'+5^2\ldots$

6) $-4n'+5\ldots=0$, $n_o=0$

7) (1,0)

b) 1) $X^3+X^2Y+2XY^2-2Y^3 = 1$

2) $\varepsilon = -1+\rho+\rho^2$

3) $\varepsilon^5 = 1+5(6-31\rho+33\rho^2)$

4) 0

5) $\varepsilon^{5n'} = 1+5(6-31\rho+33\rho^2)n'+5^2\ldots$

6) $33n'+5\ldots=0$, $n_o=0$

7) (1,0)

c) 1) $\underline{X^3+X^2Y+XY^2+3Y^3 = 1}$

2) $\varepsilon = -1+\rho+\rho^2$

3) $\varepsilon^2=1+3(-1-2\rho-\rho^2)$

4) 0

5) $\varepsilon^{2n'}=1+3(-1-2\rho-\rho^2)n'+3^2\ldots$

6) $-n'+3\ldots=0$, $n_o=0$

7) $\underline{(1,0)}$

d) 1) $\underline{X^3-2X^2Y-2XY^2-2Y^3 = 1}$

2) $\varepsilon =3-\rho$

3) $\varepsilon^8=1+11(-840-2340\rho+900\rho^2)$

4) 0,1

5) $\varepsilon^{8n'}=1+11(-840-2340\rho+900\rho^2)n'+11^2\ldots$

$\varepsilon^{8n'+1}=3-\rho+11(-4320-7980\rho+3240\rho^2)n'+11^2\ldots$

6) $900n'+11\ldots=0$, $n_o=0$

$3240n'+11\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (3,1)}$

e) 1) $\underline{X^3+XY^2+Y^3 = 1}$

2) $\varepsilon=\rho$

3) $\varepsilon^8=1+3(-1-\rho)$

4) 0,1,3

5) $\varepsilon^{8n'}=1+3(-1-\rho)n'+3^2(1+2\rho+\rho^2)\binom{n'}{2}+3^3(-2\rho-3\rho^2)\binom{n'}{3}+3^4\ldots$

$\varepsilon^{8n'+1}=\rho+3(-\rho-\rho^2)n'+3^2\ldots$

$\varepsilon^{8n'+3}=-1-\rho+3(1+2\rho+\rho^2)n'+3^2\ldots$

6) $\binom{n'}{2}-3\binom{n'}{3}+3\ldots=0$, $n_o=0,1$

$-n'+3\ldots=0$, $n_o=0$

$n'+3\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (0,1),\ (1,-1),\ (-2,3)}$

f) 1) $\underline{X^3+4X^2Y+2XY^2+2Y^3 = 1}$

2) $\varepsilon = 5+5\rho+\rho^2$

3) $\varepsilon^2 = 1+3(4+12\rho+3\rho^2)$

4) 0

5) $\varepsilon^{2n'} = 1+3(4+12\rho+3\rho^2)n'+3^2(-56+6\rho+6\rho^2)\binom{n'}{2}+3^3\ldots$

6) $n'+3.2\binom{n'}{2}+3\ldots=0,\ n_o=0$

7) $\underline{(1,0)}$

g) 1) $\underline{X^3+2XY^2+Y^3 = 1}$

2) $\varepsilon = \rho$

3) $\varepsilon^6 = 1+4(\rho+\rho^2)$

4) 0,1,3

5) $\varepsilon^{6n'} = 1+4(\rho+\rho^2)n'+4^2\ldots$

$\varepsilon^{6n'+1} = \rho+4(-1-2\rho+\rho^2)n'+4^2\ldots$

$\varepsilon^{6n'+3} = -1-2\rho+4(2+3\rho-3\rho^2)n'+4^2\ldots$

6) $n'+4\ldots=0,\ n_o=0$

$n'+4\ldots=0,\ n_o=0$

$-3n'+4\ldots=0,\ n_o=0$

7) $\underline{(1,0),\ (0,1),\ (1,-2)}$

h) 1) $\underline{X^3+X^2Y+XY^2+2Y^3 = 1}$

2) $\varepsilon = 1+\rho$

3) $\varepsilon^6 = 1+8(-1-2\rho-\rho^2)$

4) 0,1

5) $\varepsilon^{6n'} = 1+8(-1-2\rho-\rho^2)n'+8^2\ldots$

$\varepsilon^{6n'+1} = 1+\rho+8(1-2\rho-2\rho^2)n'+8^2\ldots$

6) $-n'+8\ldots=0,\ n_o=0$

$-n'+4\ldots=0,\ n_o=0$

7) $\underline{(1,0),\ (-1,1)}$

i) 1) $\underline{X^3-2X^2Y-XY^2-Y^3 = 1}$

2) $\varepsilon = \rho$

3) $\varepsilon^6 = 1+3(4+6\rho+11\rho^2)$

4) 0,1

5) $\varepsilon^{6n'} = 1+3(4+6\rho+11\rho^2)n'+3^2\ldots$

$\varepsilon^{6n'+1} = \rho+3(11+15\rho+28\rho^2)n'+3^2\ldots$

6) $11n'+3\ldots=0$, $n_o=0$

$28n'+3\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (0,-1)}$

j) 1) $\underline{X^3+X^2Y+3XY^2+2Y^3 = 1}$

2) $\varepsilon = 1+\rho$

3) $\varepsilon^6 = 1+4(2+\rho-3\rho^2)$

4) 0,1,4

5) $\varepsilon^{6n'} = 1+4(2+\rho-3\rho^2)n'+4^2\ldots$

$\varepsilon^{6n'+1} = 1+\rho+4(8+12\rho+\rho^2)n'+4^2\ldots$

$\varepsilon^{6n'+4} = -5-7\rho+4(-52-82\rho-13\rho^2)n'+4^2\ldots$

6) $-3n'+4\ldots=0$, $n_o=0$

$n'+4\ldots=0$, $n_o=0$

$-13n'+4\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (1,-1),\ (-5,7)}$

k) 1) $\underline{X^3+X^2Y+2XY^2+3Y^3 = 1}$

2) $\varepsilon = 1+\rho$

3) $\varepsilon^8 = 1+3(32+33\rho+6\rho^2)$

4) 0,1,6

5) $\varepsilon^{8n'} = 1+3(32+33\rho+6\rho^2)n'+3^2(-56+1284\rho+1041\rho^2)\binom{n'}{2}+3^3\ldots$

$\varepsilon^{8n'+1} = 1+\rho+3(14+53\rho+33\rho^2)n'+3^2(-3179-854\rho+1284\rho^2)\binom{n'}{2}+\ldots$

$\varepsilon^{8n'+6} = 4-16\rho-15\rho^2+3(1631+892\rho-303\rho^2)n'+3^2\ldots$

6) $2n'+3.347\binom{n'}{2}+3\ldots=0$, $n_o=0$

$11n'+3.428\binom{n'}{2}+3\ldots=0$, $n_o=0$

$-5-3.101n'+3\ldots=0$, keine Lösung

7) $\underline{(1,0),\ (-1,1)}$

l) 1) $\underline{X^3+4X^2Y+XY^2+Y^3 = 1}$

2) $\varepsilon = \rho$

3) $\varepsilon^4 = 1+3(1+\rho+5\rho^2)$

4) 0,1

5) $\varepsilon^{4n'} = 1+3(1+\rho+5\rho^2)n'+3^2\ldots$

$\varepsilon^{4n'+1} = \rho+3(-5-4\rho-19\rho^2)n'+3^2\ldots$

6) $5n'+3\ldots=0$, $n_o=0$

$-19n'+3\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (0,1)}$

m) 1) $\underline{X^3+3XY^2+2Y^3 = 1}$

2) $\varepsilon = 1+\rho-\rho^2$

3) $\varepsilon^3 = 1+3(8+11\rho-5\rho^2)$

4) 0

5) $\varepsilon^{3n'} = 1+3(8+11\rho-5\rho^2)n'+3^2\ldots$

6) $-5n'+3\ldots=0$, $n_o=0$

7) $\underline{(1,0)}$

n) 1) $\underline{X^3+3X^2Y+2XY^2+3Y^3 = 1}$

2) $\varepsilon = 1+3\rho+\rho^2$

3) $\varepsilon^2 = 1+3(-3-\rho)$

4) 0

5) $\varepsilon^{2n'} = 1+3(-3-\rho)n'+3^2(9+6\rho+\rho^2)\binom{n'}{2}+3^3(-24-25\rho-6\rho^2)\binom{n'}{3}\ldots$

6) $\binom{n'}{2}+3(-6)\binom{n'}{3}+3^2\ldots=0$, $n_o=0,1$

7) $\underline{(1,0),\ (-8,3)}$

o) 1) $\underline{X^3+XY^2+3Y^3 = 1}$

2) $\varepsilon = 1+\rho$

3) $\varepsilon^8 = 1+7\eta$, $\eta \equiv 2+3\rho-4\rho^2 \bmod 7$

4) 0,1

5) $\varepsilon^{8n'} = 1+7(2+3\rho-4\rho^2)n'+7^2\ldots$

$\varepsilon^{8n'+1} = 1+\rho+7(14+9\rho-\rho^2)n'+7^2\ldots$

6) $-4n'+7\ldots=0$, $n_o=0$

$-n'+7\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (-1,1)}$

p) 1) $\underline{X^3+X^2Y+3Y^3 = 1}$

2) $\varepsilon = 2+\rho$

3) $\varepsilon^6 = 1+9(-29+5\rho+11\rho^2)$

4) 0,1

5) $\varepsilon^{6n'} = 1+9(-29+5\rho+11\rho^2)n'+9^2\ldots$

$\varepsilon^{6n'+1} = 2+\rho+9(-91-19\rho+16\rho^2)n'+9^2\ldots$

6) $11n'+9\ldots=0$, $n_o=0$

$16n'+9\ldots=0$, $n_o=0$

7) $\underline{(1,0),\ (2,-1)}$

q) 1) $\underline{X^3+4XY^2+Y^3 = 1}$

2) $\varepsilon = \rho$

3) $\varepsilon^6 = 1+8(\rho+2\rho^2)$

4) 0,1,3

5) $\varepsilon^{6n'} = 1+8(\rho+2\rho^2)n'+8^2(-4-20\rho-15\rho^2)\binom{n'}{2}+8^3\ldots$

$\varepsilon^{6n'+1} = \rho+8(-2-8\rho+\rho^2)n'+8^2\ldots$

$\varepsilon^{6n'+3} = -1-4\rho+8(8+31\rho-6\rho^2)n'+8^2\ldots$

6) $n'+2^2(-15)\binom{n'}{2}+2^5\ldots=0,\ n_o=0$

$n'+8\ldots=0,\ n_o=0$

$-3n'+2^2\ldots=0,\ n_o=0$

7) $\underline{(1,0),\ (0,1),\ (1,-4)}$

B) Biquadratische Formen

Alle auftretenden Körper $\mathbb{Q}(\varrho)$ haben die Ganzheitsbasis $(1, \varrho, \varrho^2, \varrho^3)$.

Jedes der Beispiele ist in folgender Weise geschrieben:

1) Angabe der Gleichung $X^4+a_1X^3Y+a_2X^2Y^2+a_3XY^3+a_4Y^4=1$, $a_i \in \mathbb{Z}$.

2) Angabe der beiden Grundeinheiten $\varepsilon_1 = a+b\varrho+c\varrho^2+d\varrho^3$ und $\varepsilon_2 = a'+b'\varrho+c'\varrho^2+d'\varrho^3$ des Körpers $\mathbb{Q}(\varrho)$, ϱ reelle Nullstelle von $X^4+a_1X^3+a_2X^2+a_3X+a_4$.

3) Angabe von $\varepsilon_1^N = 1+p\eta$, $\varepsilon_2^M = 1+p\varrho$, p Primzahl, $\eta, \varrho \in \mathbb{Z}[\varrho]$, $\eta \equiv \eta' \bmod p$, $\varrho \equiv \varrho' \bmod p$, $\eta', \varrho' \in \mathbb{Z}[\varrho]$.

4) Angabe der Paare $(r,s) \in \{0,\dots,N-1\} \times \{0,\dots,M-1\}$, für die die Komponenten von $\varepsilon_1^r\varepsilon_2^s$ in ϱ^2 und ϱ^3 kongruent 0 mod p sind.

5) Für (r,s) aus 4) und $\varepsilon_1^r\varepsilon_2^s \equiv \varepsilon_{r,s} \bmod p$ Angabe der Reihenentwicklungen $\varepsilon_1^{Nn'+r}\varepsilon_2^{Mm'+s} = \varepsilon_1^r\varepsilon_2^s +$

$$p[\eta'\varepsilon_{r,s}^{n'} + \varrho'\varepsilon_{r,s}^{m'}] + p^2[\alpha_1 n' + \alpha_2 m' + \alpha_3 n'm' + \alpha_4\binom{n'}{2} + \alpha_5\binom{m'}{2}] + p^3\dots,$$

wobei $\alpha_i \in \mathbb{Z}[\varrho]$ bzw.

Feststellung der Tatsache, daß $X - \varrho Y = \pm\varepsilon_1^{Nn'}\varepsilon_2^{Mm'}\varepsilon_1^r\varepsilon_2^s \equiv \pm\varepsilon_1^r\varepsilon_2^s \bmod p$ für die Gleichung in 1) mod p keine Lösung ergibt.

6) Angabe der aus den Reihenentwicklungen in 5) resultierenden Gleichungssysteme der Gestalt

$$\sum_{i=0}^{\infty} p^i f_i(n',m') = 0$$

$$\sum_{i=0}^{\infty} p^i g_i(n',m') = 0$$

mit $f_i, g_i \in \mathbb{Z}_p[n',m']$, $f_o = b_1 n' + b_2 m' + b_3 \in \mathbb{Z}[n',m']$,

$g_o = c_1 n' + c_2 m' + c_3 \in \mathbb{Z}[n',m']$

und $\det \begin{pmatrix} b_1 & b_2 \\ c_1 & c_2 \end{pmatrix} \not\equiv 0 \bmod p$.

Sind b_3 und c_3 beide gleich Null, so wird die einzige ganzzahlige Lösung $\underline{(0,0)}$ angegeben.

Ist b_3 oder c_3 ungleich Null, dann muß für eine Lösung (n_o, m_o) des Systems gelten:

$b_1 n_o + b_2 m_o + b_3 \equiv 0 \bmod p$, $c_1 n_o + c_2 m_o + c_3 \equiv 0 \bmod p$, und

daraus $\underline{(n_o, m_o) \equiv \left(\frac{b_2 c_3 - b_3 c_2}{b_1 c_2 - b_2 c_1}, \frac{b_3 c_1 - b_1 c_3}{b_1 c_2 - b_2 c_1}\right) =: (d_1, d_2) \bmod p.}$

Mit $(n_o, m_o) = (d_1, d_2) + p(e_1, e_2)$ folgt dann

$$\underline{X - \varrho Y} \equiv +/- \varepsilon_1^{Nn_o+r} \varepsilon_2^{Mm_o+s} = +/- \varepsilon_1^{N(d_1+pe_1)+r} \varepsilon_2^{M(d_2+pe_2)+s}$$

$$\equiv +/- \varepsilon_1^{Nd_1+r} \varepsilon_2^{Md_2+s} \bmod p^2, \text{ weil (in den Beispielen)}$$

$$\varepsilon_1^{Np} \equiv \varepsilon_2^{Mp} \equiv 1 \bmod p^2 .$$

7) Angabe aller der aus den Gleichungssystemen in 6) folgenden Lösungen der Gleichung in 1)

1) vermöge $X - \varrho Y = +/- \varepsilon_1^{N \cdot 0} \varepsilon_2^{M \cdot 0} \varepsilon_1^r \varepsilon_2^s = +/- \varepsilon_1^r \varepsilon_2^s$ bzw.

2) bis auf Kongruenz mod p^2, wenn $X - \varrho Y \equiv$

$$+/- \varepsilon_1^{Nd_1+r} \varepsilon_2^{Md_2+s} \equiv +/- (x_o - y_o \varrho) \in \mathbb{Z} + \mathbb{Z}\varrho \bmod p^2 .$$

a) 1) $\underline{X^4+2X^3Y+XY^3-Y^4 = 1}$

2) $\varepsilon_1=\rho$, $\varepsilon_2=1-\rho-\rho^2$

3) $\varepsilon_1^6=1+3\eta$, $\eta \equiv 1-2\rho+\rho^2 \mod 3$

$\varepsilon_2^6=1+3\xi$, $\xi \equiv \rho^2-\rho^3 \mod 3$

4) (0,0), (1,0), (3,3), (4,3)

5) $\varepsilon_1^{6n'}\varepsilon_2^{6m'}=1+3[(1-2\rho+\rho^2)n'+(\rho^2-\rho^3)m']+3^2\ldots$

$X-\rho Y \equiv +/-\rho \mod 3$ ergibt keine Lösung

$\varepsilon_1^{6n'+3}\varepsilon_2^{6m'+3}=2-6\rho+6\rho^2-3\rho^3$

$+3[(20-31\rho+23\rho^2-57\rho^3)n'+(42-57\rho+20\rho^2-95\rho^3)m']+3^2\ldots$

$X-\rho Y \equiv +/-\varepsilon_1^4\varepsilon_2^3 \equiv +/-\rho \mod 3$ ergibt keine Lösung

6) $(n'+m')+3\ldots=0$

$(\ \ -m')+3\ldots=0$, $(n_o,m_o)=(0,0)$

$(2+23n'+20m')+3\ldots=0$

$(-1-57n'-95m')+3\ldots=0$, $(n_o,m_o)\equiv(1,1) \mod 3$

$X-\rho Y \equiv +/-\varepsilon_1^9\varepsilon_2^9 \equiv +/- 1 \mod 9$

7) $\underline{(1,0), (-1,0),}$

möglicherweise 2 Lösungen kongruent $\underline{(1,0)}$ bzw. $\underline{(-1,0) \mod 9}$.

b) 1) $\underline{X^4+X^3Y+2XY^3+Y^4 = 1}$

2) $\varepsilon_1=\rho$, $\varepsilon_2=1+\rho$

3) $\varepsilon_1^{\,8}=1+5\eta$, $\eta \equiv -1-\rho+\rho^2-\rho^3 \bmod 5$

$\varepsilon_2^{\,24}=1+5\xi$, $\xi \equiv -3-4\rho-\rho^2+3\rho^3 \bmod 5$

4) (0,0), (1,0), (0,1), (1,19), (2,6), (2,7), (3,1), (3,6), (4,12), (4,13), (5,7), (5,12), (6,18), (6,19), (7,13), (7,18)

5) $\varepsilon_1^{\,8n'}\,\varepsilon_2^{\,24m'}=1+5[(-1-\rho+\rho^2-\rho^3)n'+(-3-4\rho-\rho^2+3\rho^3)m']+5^2\ldots$

$\varepsilon_1^{\,8n'+1}\,\varepsilon_2^{\,24m'}=\rho+5[(1+\rho-\rho^2+2\rho^3)n'+(-3-4\rho-4\rho^2-4\rho^3)m']+5^2\ldots$

$X-\rho Y \equiv +/- (1+\rho) \bmod 5$ ergibt keine Lösung

$X-\rho Y \equiv +/- \varepsilon_1\varepsilon_2^{\,19} \equiv +/- (1+2\rho) \bmod 5$ ergibt keine Lösung

$\varepsilon_1^{\,8n'+2}\varepsilon_2^{\,24m'+6}=\varepsilon_1^{\,2}\varepsilon_2^{\,6}+$

$+5[(1+\rho-\rho^2+\rho^3)n'+(3+4\rho+\rho^2-3\rho^3)m']+5^2\ldots$

$X-\rho Y \equiv +/- \varepsilon_1^{\,2}\varepsilon_2^{\,7} \equiv +/- (1+\rho) \bmod 5$ ergibt keine Lösung

$X-\rho Y \equiv +/- \varepsilon_1^{\,3}\varepsilon_2 \equiv +/- (1+2\rho) \bmod 5$ ergibt keine Lösung

$\varepsilon_1^{\,8n'+3}\varepsilon_2^{\,24m'+6}=\varepsilon_1^{\,3}\varepsilon_2^{\,6}+$

$+5[(-1-\rho+\rho^2-2\rho^3)n'+(3+9\rho+4\rho^2+4\rho^3)m']+5^2\ldots$

$\varepsilon_1^{\,8n'+4}\varepsilon_2^{\,24m'+12}=\varepsilon_1^{\,4}\varepsilon_2^{\,12}+$

$+5[(-1-\rho+\rho^2-\rho^3)n'+(-3-4\rho-\rho^2+3\rho^3)m']+5^2\ldots$

$X-\rho Y \equiv +/- \varepsilon_1^{\,4}\varepsilon_2^{\,13} \equiv +/- (1+\rho) \bmod 5$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_1^5 \varepsilon_2^7 \equiv +/- (1+2\varrho) \bmod 5$ ergibt keine Lösung

$$\varepsilon_1^{8n'+5} \varepsilon_2^{24m'+12} = \varepsilon_1^5 \varepsilon_2^{12} + 5[(1+\varrho-\varrho^2+2\varrho^3)n'+(-3-9\varrho-4\varrho^2-4\varrho^3)m'] +5^2\ldots$$

$$\varepsilon_1^{8n'+6} \varepsilon_2^{24m'+18} = \varepsilon_1^6 \varepsilon_2^{18} + 5[(1+\varrho-\varrho^2+\varrho^3)n'+(3+4\varrho+\varrho^2-3\varrho^3)m'] +5^2\ldots$$

$X-\varrho Y \equiv +/- \varepsilon_1^6 \varepsilon_2^{19} \equiv +/- (1+\varrho) \bmod 5$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_1^7 \varepsilon_2^{13} \equiv +/- (1-2\varrho) \bmod 5$ ergibt keine Lösung

$$\varepsilon_1^{8n'+7} \varepsilon_2^{24m'+18} = \varepsilon_1^7 \varepsilon_2^{18} + 5[(-1-\varrho+\varrho^2-2\varrho^3)n'+(3+9\varrho+4\varrho^2+4\varrho^3)m'] +5^2\ldots$$

6) $(n'-m')+5\ldots=0$

$(-n'+3m')+5\ldots=0$, $(n_o,m_o)=(0,0)$

$(-n'-4m')+5\ldots=0$

$(2n'-4m')+5\ldots=0$, $(n_o,m_o)=(0,0)$

$(-n'+m'+b_3)+5\ldots=0$

$(n'-3m'+c_3)+5\ldots=0$, $(n_o,m_o) \equiv (1,1) \bmod 5$ wegen

$$\varepsilon_1^2 \varepsilon_2^6 \equiv 4-15\varrho^3 \bmod 25$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{10} \varepsilon_2^{30} \equiv +/- 1 \bmod 25$$

$(n'+4m'+b_3)+5\ldots=0$

$(-2n'+4m'+c_3)+5\ldots=0$, $(n_o,m_o) \equiv (1,1) \bmod 5$ wegen

$$\varepsilon_1^3 \varepsilon_2^6 \equiv 15+9\varrho-10\varrho^3 \bmod 25$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{11} \varepsilon_2^{30} \equiv +/- \varrho \bmod 25$$

$(n'-m'+b_3)+5\ldots=0$

$(-n'+3m'+c_3)+5\ldots=0$, $(n_o,m_o)\equiv(2,2)$ mod 5 wegen

$$\varepsilon_1^{4}\varepsilon_2^{12}\equiv -9-20\rho^3 \text{ mod } 25$$

$$X-\rho Y\equiv +/-\ \varepsilon_1^{20}\varepsilon_2^{60}\equiv +/-\ 1 \text{ mod } 25$$

$(-n'-4m'+b_3)+5\ldots=0$

$(2n'-4m'+c_3)+5\ldots=0$, $(n_o,m_o)\equiv(2,2)$ mod 5 wegen

$$\varepsilon_1^{5}\varepsilon_2^{12}\equiv 20+6\rho-5\rho^3 \text{ mod } 25$$

$$X-\rho Y\equiv +/-\ \varepsilon_1^{21}\varepsilon_2^{60}\equiv +/-\ \rho \text{ mod } 25$$

$(-n'+m'+b_3)+5\ldots=0$

$(n'+2m'+c_3)+5\ldots=0$, $(n_o,m_o)\equiv(3,3)$ mod 5 wegen

$$\varepsilon_1^{6}\varepsilon_2^{18}\equiv 14-20\rho^3 \text{ mod } 25$$

$$X-\rho Y\equiv +/-\ \varepsilon_1^{30}\varepsilon_2^{90}\equiv +/-\ 1 \text{ mod } 25$$

$(n'-m'+b_3)+5\ldots=0$

$(-2n'-m'+c_3)+5\ldots=0$, $(n_o,m_o)\equiv(3,3)$ mod 5 wegen

$$\varepsilon_1^{7}\varepsilon_2^{18}\equiv 20+4\rho-5\rho^3 \text{ mod } 25$$

$$X-\rho Y\equiv +/-\ \varepsilon_1^{31}\varepsilon_2^{90}\equiv +/-\ \rho \text{ mod } 25$$

7) $\underline{(1,0),\ (-1,0)}$,
$\underline{(0,1),\ (0,-1)}$,

höchstens 3 Lösungen kongruent $\underline{(1,0) \text{ mod } 25}$,
- " - 3 - " - $\underline{(-1,0) \text{ mod } 25}$,
- " - 3 - " - $\underline{(0,1) \text{ mod } 25}$,
- " - 3 - " - $\underline{(0,-1) \text{ mod } 25}$.

c) 1) $\underline{X^4-2X^2Y^2-Y^4 = 1}$

2) $\varepsilon_1 = \varrho$, $\varepsilon_2 = -1+\varrho+\varrho^2$

3) $\varepsilon_1^{24} = 1+5\eta$, $\eta \equiv 3+2\varrho^2 \bmod 5$

$\varepsilon_2^{12} = 1+5\varrho$, $\varrho \equiv 1+2\varrho+4\varrho^2+2\varrho^3 \bmod 5$

4) (0,0), (1,0), (6,0), (7,0), (12,0), (13,0), (18,0), (19,0)

5) $\varepsilon_1^{24n'}\varepsilon_2^{12m'} = 1+5[(3+2\varrho^2)n'+(1+2\varrho+4\varrho^2+2\varrho^3)m'] +5^2\ldots$

$X-\varrho Y \equiv +/- \varepsilon_1 \equiv +/- \varrho \bmod 5$ ergibt keine Lösung

$\varepsilon_1^{24n'+6}\varepsilon_2^{12m'} = 2+5\varrho^2+$

$+5[(16+39\varrho^2)n'+(22+14\varrho+53\varrho^2+34\varrho^3)m'] +5^2\ldots$

$\varepsilon_1^{24n'+7}\varepsilon_2^{12m'} = 2\varrho+5\varrho^3+$

$+5[(16\varrho+39\varrho^3)n'+(34+22\varrho+82\varrho^2+53\varrho^3)m'] +5^2\ldots$

$\varepsilon_1^{24n'+12}\varepsilon_2^{12m'} = 29+70\varrho^2 +$

$+5[(227+548\varrho^2)n'+(309+198\varrho+746\varrho^2+478\varrho^3)m'] +5^2\ldots$

$\varepsilon_1^{24n'+13}\varepsilon_2^{12m'} = 29\varrho+70\varrho^3 +$

$+ 5[(227\varrho+548\varrho^3)n'+(478+309\varrho+1154\varrho^2+746\varrho^3)m'] +5^2\ldots$

$\varepsilon_1^{24n'+18}\varepsilon_2^{12m'} = 408+985\varrho^2 +$

$+5[(3194+7711\varrho^2)n'+(4348+2786\varrho+10497\varrho^2+6726\varrho^3)m'] +5^2\ldots$

$\varepsilon_1^{24n'+19}\varepsilon_2^{12m'} = 408\varrho+985\varrho^3 +$

$+5[(3194\varrho+7711\varrho^3)n'+(6726+4348\varrho+16238\varrho^2+10497\varrho^3)m'] +\ldots$

6) $(2n'+4m')+5\ldots=0$

$2m' +5\ldots=0$, $(n_o,m_o)=(0,0)$

$(39n'+53m'+1)+5\ldots=0$

$34m' +5\ldots=0$, $(n_o,m_o)\equiv(1,0) \bmod 5$

$X-\rho Y \equiv +/- \varepsilon_1^{30} \equiv +/- 7 \bmod 25$

$82m' +5\ldots=0$

$(39n'+53m'+1)+5\ldots=0$, $(n_o,m_o)\equiv(1,0) \bmod 5$

$X-\rho Y \equiv +/- \varepsilon_1^{31} \equiv +/- 7\rho \bmod 25$

ergibt keine Lösung (mod 25)

$(548n'+746m'+14)+5\ldots=0$

$478m' +5\ldots=0$, $(n_o,m_o)\equiv(2,0) \bmod 5$

$X-\rho Y \equiv +/- \varepsilon_1^{60} \equiv +/- 1 \bmod 25$

$1154m' +5\ldots=0$

$(548n'+746m'+14)+5\ldots=0$, $(n_o,m_o)\equiv(2,0) \bmod 5$

$X-\rho Y \equiv +/- \varepsilon_1^{61} \equiv +/- \rho \bmod 25$

ergibt keine Lösung (mod 25)

$(7711n'+10497m'+197)+5\ldots=0$

$6726m' +5\ldots=0$, $(n_o,m_o)\equiv(3,0) \bmod 5$

$X-\rho Y \equiv +/- \varepsilon_1^{90} \equiv +/- 7 \bmod 25$

$16238m' +5\ldots=0$

$(7711n'+10497m'+197)+5\ldots=0$, $(n_o,m_o)\equiv(3,0) \bmod 5$

$X-\rho Y \equiv +/- \varepsilon_1^{91} \equiv +/- 7\rho \bmod 25$

ergibt keine Lösung (mod 25)

7) $\underline{(1,0),\ (-1,0)}$,

höchstens 2 Lösungen kongruent $\underline{(7,0) \bmod 25}$,

- " - 2 - " - $\underline{(-7,0) \bmod 25}$,

- " - 1 Lösung - " - $\underline{(1,0) \bmod 25}$,

- " - 1 - " - $\underline{(-1,0) \bmod 25}$.

d) 1) $\underline{X^4-2X^2Y^2+XY^3-Y^4 = 1}$

2) $\varepsilon_1=\varrho,\quad \varepsilon_2= 1-\varrho$

3) $\varepsilon_1^{16}=1+7\eta\ ,\ \eta \equiv 4-3\varrho-4\varrho^3 \bmod 7$

$\varepsilon_2^{48}=1+7\xi\ ,\ \xi \equiv 3-4\varrho+3\varrho^2-6\varrho^3 \bmod 7$

4) (0,0), (0,1), (1,0), (1,5), (1,35), (2,24), (2,31), (5,20), (8,24), (8,25), (9,11), (9,24), (9,29), (10,0), (10,7), (13,44)

5) $\varepsilon_1^{16n'}\varepsilon_2^{48m'} = 1+7\left[(4-3\varrho-4\varrho^3)n'+(3-4\varrho+3\varrho^2-6\varrho^3)m'\right]+7^2\ldots$

$X-\varrho Y \equiv +/- \varepsilon_1 \equiv +/- \varrho \bmod 7$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_2 \equiv +/- (1-\varrho) \bmod 7$ ergibt keine Lösung

$\varepsilon_1^{16n'+1}\varepsilon_2^{48m'+5} = (-12+18\varrho-35\varrho^2+21\varrho^3) +$

$+7\left[(-351+551\varrho-1024\varrho^2+601\varrho^3)n'+(-585+924\varrho-1710\varrho^2+1001\varrho^3)m'\right]+\ldots$

$\varepsilon_1^{16n'+1}\varepsilon_2^{48m'+35} = \varepsilon_1\varepsilon_2^{35} +$

$+7\left[(10\varrho+22\varrho^2+8\varrho^3)n'+(6-10\varrho+26\varrho^2+6\varrho^3)m'\right]+7^2\ldots$

$\varepsilon_1^{16n'+2}\varepsilon_2^{48m'+24} = \varepsilon_1^2\varepsilon_2^{24} +$

$+7\left[(20-35\varrho+44\varrho^2-4\varrho^3)n'+(27-40\varrho+67\varrho^2-18\varrho^3)m'\right]+7^2\ldots$

$X-\varrho Y \equiv +/- \varepsilon_1^{2}\varepsilon_2^{31} \equiv +/- (1-3\varrho) \bmod 7$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_1^{5}\varepsilon_2^{20} \equiv +/- (1-2\varrho) \bmod 7$ ergibt keine Lösung

$$\varepsilon_1^{16n'+8}\varepsilon_2^{48m'+24} = \varepsilon_1^{8}\varepsilon_2^{24} +$$

$$+7\left[(24-18\varrho-24\varrho^3)n'+(18-24\varrho+18\varrho^2-36\varrho^3)m'\right]+7^2\ldots$$

$X-\varrho Y \equiv +/- \varepsilon_1^{8}\varepsilon_2^{25} \equiv +/- (1-\varrho) \bmod 7$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_1^{9}\varepsilon_2^{11} \equiv +/- (2-2\varrho) \bmod 7$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_1^{9}\varepsilon_2^{24} \equiv +/- \varrho \bmod 7$ ergibt keine Lösung

$$\varepsilon_1^{16n'+9}\varepsilon_2^{48m'+29} = \varepsilon_1^{9}\varepsilon_2^{29} +$$

$$+7\left[(-20+30\varrho-33\varrho^2+8\varrho^3)n'+(-24+35\varrho-54\varrho^2+21\varrho^3)m'\right]+7^2\ldots$$

$$\varepsilon_1^{16n'+10}\varepsilon_2^{48m'} = \varepsilon_1^{10} +$$

$$7\left[(36-42\varrho+33\varrho^2-24\varrho^3)n'+(36-51\varrho+66\varrho^2-45\varrho^3)m'\right]+7^2\ldots$$

$X-\varrho Y \equiv +/- \varepsilon_1^{10}\varepsilon_2^{7} \equiv +/- (1-3\varrho) \bmod 7$ ergibt keine Lösung

$X-\varrho Y \equiv +/- \varepsilon_1^{13}\varepsilon_2^{44} \equiv +/- (1-2\varrho) \bmod 7$ ergibt keine Lösung

6) $3m' +7\ldots=0$

$(-4n'-6m')+7\ldots=0$, $(n_o,m_o)=(0,0)$

$(-1024n'-1710m'-5)+7\ldots=0$

$(601n'+1001m'+3)+7\ldots=0$, $(n_o,m_o)\equiv(3,5) \bmod 7$

$X-\varrho Y \equiv +/- \varepsilon_1^{49}\varepsilon_2^{245} \equiv +/- (23-24\varrho) \bmod 49$

$(22n'+26m'+b_3)+7\ldots=0$

$(8n'+6m'+c_3)+7\ldots=0$, $(n_o,m_o)\equiv(3,2) \bmod 7$ wegen

$$\varepsilon_1\varepsilon_2^{35} \equiv -37+5\varrho-42\varrho^2+42\varrho^3 \bmod 49$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{49}\varepsilon_2^{131} \equiv +/- (2+2\varrho) \bmod 49$$

$(44n'+67m'+b_3)+7\ldots=0$

$(-4n'-18m'+c_3)+7\ldots=0$, $(n_o,m_o) \equiv (6,5) \bmod 7$ wegen

$$\varepsilon_1^2\varepsilon_2^{24} \equiv 36-25\varrho+21\varrho^2-35\varrho^3 \bmod 49$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{98}\varepsilon_2^{264} \equiv +/- (8-4\varrho) \bmod 49$$

$18m'+b_3)+7\ldots=0$

$(-24n'-36m'+c_3)+7\ldots=0$, $(n_o,m_o) \equiv (3,3) \bmod 7$ wegen

$$\varepsilon_1^8\varepsilon_2^{24} \equiv 48+14\varrho^2-14\varrho^3 \bmod 49$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{56}\varepsilon_2^{168} \equiv +/- 1 \bmod 49$$

$(-33n'-54m'+b_3)+7\ldots=0$

$(8n'+21m'+c_3)\ \ +7\ldots=0$, $(n_o,m_o) \equiv (6,1) \bmod 7$ wegen

$$\varepsilon_1^9\varepsilon_2^{29} \equiv -44+38\varrho+7\varrho^3 \bmod 49$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{105}\varepsilon_2^{77} \equiv +/- (23-24\varrho) \bmod 49$$

$(33n'+66m'+b_3)+7\ldots=0$

$(-24n'-45m'+c_3)+7\ldots=0$, $(n_o,m_o) \equiv (2,2) \bmod 7$ wegen

$$\varepsilon_1^{10} \equiv 13-17\varrho+35\varrho^2-14\varrho^3 \bmod 49$$

$$X-\varrho Y \equiv +/- \varepsilon_1^{42}\varepsilon_2^{96} \equiv +/- (8-4\varrho) \bmod 49$$

7) $\underline{(1,0),\ (-1,0)}$,

höchstens 2 Lösungen kongruent $\underline{(23,24) \bmod 49}$,

-"- 2 - " - $\underline{(-23,-24) \bmod 49}$,

-"- 2 - " - $\underline{(8,4) \bmod 49}$,

-"- 2 - " - $\underline{(-8,-4) \bmod 49}$,

-"- 1 Lösung - " - $\underline{(1,0) \bmod 49}$,

-"- 1 - " - $\underline{(-1,0) \bmod 49}$,

-"- 1 - " - $\underline{(2,-2) \bmod 49}$,

-"- 1 - " - $\underline{(-2,2) \bmod 49}$.

VI. L I T E R A T U R V E R Z E I C H N I S

1) R.Alter,K.K.Kubota, The Diophantine Equation $X^2+11=3^n$ and a Related Sequence, J.Number Theory 7,5-10,1975

2) James Ax, On Schanuel's Conjectures and Skolem's Method, Proc.Symp.in Pure Math.20,206-212,1969

3) S.I.Borewicz,I.R.Safarević, Zahlentheorie,1966,Basel

4) A.Bremner,N.Tzanakis, Integer Points on $Y^2=X^3-7X+10$, Math.Comp.41,731-741,1983

5) A.Bremner,P.Morton, The Integer Points on Three Related Elliptic Curves, Math.Comp.41,235-238,1983

6) A.Bremner, Solution of a Problem of Skolem, J.Number Theory 9,499-501,1977

7) C.Chabauty, Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini, Annali di Math.IV,17,127-168,1938

8) C.Chabauty, Démonstration nouvelle d'un théorème de Thue et Mahler sur les formes binaires, Bull.Sci.Math. 65,112-115,1941

9) R.Fricke, Lehrbuch der Algebra I,1924, Braunschweig

10) D.J.Lewis, Diophantine Equations: p-adic methods, Math. Assoc.Amer.Studies in Math.6,25-75,1969

11) W.Ljunggren, Einige Sätze über unbestimmte Gleichungen von der Form $AX^4+BX^2+C=DY^2$, Vid.-Akad.Skrifter I, 9,3-41,1942

12) W.Ljunggren, Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante, Acta Math.75,1-21,1942

13) W.Ljunggren, Thoralf Albert Skolem in memoriam, Math. Scand.13,5-8,1963

14) K.Mahler, p-adic Numbers and Their Functions,1981, Cambridge

15) L.J.Mordell, Note on the Integer Solutions of the Equation $EY^2=AX^3+BX^2+CX+D$, Mess.Math.51,169-171, 1922

16) L.J.Mordell, Diophantine Equations,1969,New York

17) O.Perron, Algebra,1927,Berlin

18) P.Ribenboim, Algebraic Numbers,1972,New York

19) W.M.Schmidt, Linearformen mit algebraischen Koeffizienten II,Math.Ann.191,1-20,1971

20) T.Skolem, Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen, Vid.-Akad.Skrifter I, 6,3-61,1933

21) T.Skolem, Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, 8^{th} Skand.Mat.Kong.Stockholm,163-188,1934

22) T.Skolem, En metode til behandling av ubestemte ligninger, Chr.Michelsens Inst.Beretn. IV,6,3-34,1934

23) T.Skolem, Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen, Math.Ann.111,399-424,1935

24) T.Skolem, Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen, Vid.-Akad.Avh.I,12,3-16,1937

25) T.Skolem, Diophantische Gleichungen, Ergebnisse der Mathe= matik und ihrer Grenzgebiete,114-120,1938

26) T.Skolem, The Use of a p-adic Method in the Theory of Diophantine Equations, Soc.Math.Belg.7,83-95,1955

27) T.Skolem,S.Chowla,D.J.Lewis, The Diophantine Equation $2^{n+2}-7=X^2$ and Related Problems, Proc.Amer.Math. Soc.10,663-669,1959

28) N.Tzanakis, The Diophantine Equation $X^3-3XY^2-Y^3 = 1$ and Related Equations, J.Number Theory 18,192-205, 1984

Lebenslauf des Verfassers

Am 11. April 1961 wurde ich als Sohn des Roland und der Ute Backmeister, geb. Rek, in Mannheim geboren.
Ein Jahr danach zogen meine Eltern mit mir nach Dornbirn (Österreich), wo mein Vater als Fabrikant tätig wurde.
Ich besuchte die Volksschule im benachbarten Ort Schwarzach von 1967 bis 1971 und das Bundesgymnasium in Bregenz, wo ich im Jahre 1979 maturierte. Anschließend durfte ich meine Englischkentnisse durch einen einjährigen U.S.A.-Aufenthalt als Austauschschüler praktizieren und vertiefen. Ich lebte bei einer sehr netten Familie in Kalifornien, besuchte eine highschool und konnte durch zahlreiche Aktivitäten den amerikanischen Lebensstil kennenlernen.
Nach der Rückkehr begann ich im Herbst 1980 in Innsbruck mit dem Studium der Mathematik.