Université
franco-allemande
Deutsch-Französische
Hochschule

Zusammenfaßung:

Diese Doktorarbeit untersucht einige Verfahren zur Behandlung von Diophantischen Gleichungen. Wir behandeln insbesondere den Zusammnehang zwischen Diophantischer Analysis und der Theorie von Kreisteilungskörper.

In Kapitel 2 wird eine kurze Einführung in den Methoden der Diophantischen Approximation, die wir in dieser Arbeit verwendeten, gegeben. Insbesondere werden die Begriffe von Höhe und logarithmischen grössten geminsamen Teiler eingeführt.

Im darauffolgenden Kapitel 3, wird eine Vermutung von Thoralf Skolem aus dem Jahr 1937 behandelt, betreffend einer Diophantischen Gleichung. Sei $\mathbb{K}$ ein Zahlkörper, $\alpha_1, \ldots, \alpha_m, \lambda_1, \ldots, \lambda_m$ nicht verschwindende algebraische Zahlen aus $\mathbb{K}$ und S eine endliche Menge von Stellen aus $\mathbb{K}$, die alle unendlichen Stellen enthält und so, dass der Ring der S-ganzen Zahlen

$$\mathcal{O}_S = \mathcal{O}_{\mathbb{K},S} = \{\alpha \in \mathbb{K} : |\alpha|_v \leq 1 \text{ für Stellen } v \notin S\}$$

auch $\lambda_1, \ldots, \lambda_m, \alpha_1, \ldots, \alpha_m, \alpha_1^{-1}, \ldots, \alpha_m^{-1}$ enthält.

Für jedes $n \in \mathbb{Z}$, sei $A(n) = \lambda_1\alpha_1^n + \cdots + \lambda_m\alpha_m^n \in \mathcal{O}_S$. Skolem vermutete [S1]:

Conjecture 0.1 (Exponential Local-Global Principle)**.** *Angenommen, dass für*
jedes nicht triviale Ideal $\mathfrak{a}$ im Ganzheitsring $\mathcal{O}_S$, ein $n \in \mathbb{Z}$ existiert, so dass $A(n) \equiv 0 \bmod \mathfrak{a}$; dann existiert ein $n \in \mathbb{Z}$, so dass $A(n) = 0$.

Sei Γ die durch $\alpha_1, \ldots, \alpha_m$ erzeugte multiplicative Gruppe. Dann ist Γ Produkt einer endlichen abelschen Gruppe mit einer freien abelschen Gruppe von endlichem Rang. Wir beweisen die Vermutung für den Fall in dem der freie Teil den Rang eins hat.

Im Kapitel 4 wird ein früheres Ergebnis von Abouzaid ([A]) verallgemeinert. Sei $F(X,Y) \in \mathbb{Q}[X,Y]$ ein $\mathbb{Q}$-unzerlegbares Polynom. In 1929 bewies Skolem [S2] folgenden schönen Satz:

Theorem 0.2 (Skolem)**.** *Sei*

$$F(0,0) = 0.$$

Dann ist die Menge der Lösungen $L_d = \{F(X,Y) = 0 : \; X, Y \in \mathbb{Z} \text{und} (X,Y) = d\}$ endlich, für jeden $d > 0$.

In 2008, verallgemeinerte Abouzaid [A] dieses Ergebnis, indem er in Zahlenkörper arbeitete. Er bewies folgenden Satz:

Theorem 0.3 (Abouzaid)**.** *Sei $(0,0)$ ein nicht - singurlärer Punkt der ebenen Kurve $F(X,Y) = 0$. Sei $m = \deg_X F, \quad n = \deg_Y F, \quad M = \max\{m,n\}$*

und ε *genüge den Ungleichungen* $0 < \varepsilon < 1$. *Dann gilt für jede Lösung* $(\alpha, \beta) \in \bar{\mathbb{Q}}^2$ *von* $F(X, Y) = 0$*, entweder*

$$\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \leq 56M^8\varepsilon^{-2}\mathrm{h}_p(F) + 420M^{10}\varepsilon^{-2}\log(4M),$$

oder

$$\begin{aligned}\max\{|\mathrm{h}(\alpha) - n\mathrm{lgcd}(\alpha, \beta)|, |\mathrm{h}(\beta) - m\mathrm{lgcd}(\alpha, \beta)|\} \leq{} & \varepsilon \max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} + \\ & + 742M^7\varepsilon^{-1}\mathrm{h}_p(F) + 5762M^9\varepsilon^{-1}\log(2m + 2n).\end{aligned}$$

Die Bedingung, dass $(0, 0)$ ein nicht singulärer Punkt sei, ist eine Einschränkung in diesem Ergebnis. Wir konnten diese Einschränkung aufheben, in dem wir eine leicht veränderte Version des "absoluten" Lemma von Siegel und des Eisenstein-Lemmas verwendeten. Folgender Satz ergibt sich:

Theorem 0.4. *Sei* $F(X, Y) \in \bar{\mathbb{Q}}[X, Y]$ *ein total unzerlegbarer Polynom mit* $F(0, 0) = 0$*. Sei* $m = \deg_X F$, $n = \deg_Y F$ *und* $r = \min\left\{i + j : \frac{\partial^{i+j}F}{\partial^i X \partial^j Y}(0, 0) \neq 0\right\}$*. Sei* $\varepsilon \in \mathbb{R}$ *mit* $0 < \varepsilon < 1$*. Dann gilt für jede Lösung* $\alpha, \beta \in \bar{\mathbb{Q}}$ *von* $F(X, Y) = 0$*, entweder:*

$$\mathrm{h}(\alpha) \leq 200\varepsilon^{-2}mn^6(\mathrm{h}_p(F) + 5)$$

oder

$$\begin{aligned}\left|\frac{\mathrm{lgcd}(\alpha,\beta)}{r} - \frac{\mathrm{h}(\alpha)}{n}\right| \leq \frac{1}{r}(\varepsilon\mathrm{h}(\alpha) & + 4000\varepsilon^{-1}n^4(\mathrm{h}_p(F) + \log(mn) + 1) + \\ & + 30n^2m(\mathrm{h}_p(F) + \log(nm))).\end{aligned}$$

Im Kapitel 5 werden einige Ergebnisse aus der Theorie der Kreisteilungskörper bewiesen, um einen systematischen Lösungsvorgang für bestimmte exponentielle Diophantische Gleichungen darzustellen. Wir besprechen auch einige Eigenschaften von Gruppenringe und von Jacobi-Summen. Darauf basierend wird in Kapitel 6 eine interessante Anwendung entwickelt. Wir betrachten die Diophantische Gleichung

$$X^n - 1 = BZ^n, \tag{1}$$

wobei $B \in \mathbb{Z}$ als Parameter zu verstehen ist. Sei $\varphi^*(B) := \varphi(\mathrm{rad}\ (B))$, mit $\mathrm{rad}\ (B)$ dem Radikal von B, und nehme an, dass

$$(n, \varphi^*(B)) = 1. \tag{2}$$

Zudem definieren wir für festen $B \in \mathbb{N}_{>1}$

$$\mathcal{N}(B) = \{n \in \mathbb{N}_{>1} \mid \exists\, k > 0 \text{ such that } n|\varphi^*(B)^k\}.$$

Falls p eine ungerade Primzahl ist, dann bezeichnen wir mit CF das Bedingungspaar

I Die Vermutung von Vandiver ist wahr für p: somit ist die Klassenzahl h_p^+ des maximalen reellen Teilkörpers des p-ten Kreisteilungskörpers $\mathbb{Q}[\zeta_p]$ nicht durch p teilbar.

II Der irregularitätsindex ist beschränkt durch $i_r(p) < \sqrt{p} - 1$; es gibt also höchstens $\sqrt{p}-1$ ungerade $k < p$ für denen der Zähler der Bernoullizahl $B_k \equiv 0 \bmod p$.

Die besten Ergebnisse sind zur Zeit auf Parameter B eingeschränkt, die durch Primzahlen $q \leq 13$ teilbar sind [BGMP] und es sind vollständige Lösungen für $B < 235$ ([BBGP]) bekannt.

Wenn man von der Erwartung ausgeht, dass die Gleichung keine Lösungen besitzt, ist es natürlich vom Falle auszugehen, in dem der Exponent n eine Primzahl ist: die Existenz von Lösungen für einen zusammengesetzten Exponent n impliziert die Existenz von Lösungen für dessen Primteiler, als Exponent.

Das Hauptergebnis der Arbeit besteht darin, die Gleichung (1), unter Voraussetzung dass n prim ist und (2) gilt, auf dem besser verstandenen Diagonalfall der Gleichung von Nagell – Ljunggren zu beziehen:

$$\frac{X^n - 1}{X - 1} = n^e Y^n, \quad e = \begin{cases} 0 & \text{Falls } X \not\equiv 1 \bmod n, \\ 1 & \text{sonst.} \end{cases}$$

Damit können Ergebnisse aus [M] verwendet werden und wir beweisen

Theorem 0.5. *Sei n prim und $B > 1$ eine ganze Zahl mit $(\varphi^*(B), n) = 1$. Angenommen, die Gleichung (1) habe eine nicht-triviale Lösung, die verschieden ist von $n = 3$ und $(X, Z; B) = (18, 7; 17)$, sei $X \equiv u \bmod n, 0 \leq u < n$ mit $e = 1$ falls $u = 1$ and $e = 0$ sonst. Dann gilt:*

1. *$n > 163 \cdot 10^6$.*
2. *$X - 1 = \pm B/n^e$ und $B < n^n$.*
3. *Falls $u \notin \{-1, 0, 1\}$, dann wird die Bedingung CF (II) durch n nicht erfüllt und*

$$\begin{array}{rcll} 2^{n-1} & \equiv & 3^{n-1} \equiv 1 \mod n^2, & \textit{und} \\ r^{n-1} & \equiv & 1 \mod n^2 & \textit{für alle } r | X(X^2-1). \end{array}$$

Falls $u \in \{-1, 0, 1\}$, dann ist die Bedingung CF (I) für n falsch.

Aus diesem Satz folgern wir:

Theorem 0.6. *Falls die Gleichung (1) für ein festes B, das die Bedingungen (2) erfüllt, eine Lösung besitzt, dann ist entweder $n \in \mathcal{N}(B)$ oder es gibt eine Primzahl p, die zu $\varphi^*(B)$ teilerfremd ist und ein $m \in \mathcal{N}(B)$, so dass $n = p \cdot m$. Zudem bilden X^m, Y^m eine Lösung von (1) für den primen Exponent p und erfüllen somit die Bedingungen in Satz 0.5.*

Dies verbessert die aktuelle Ergebnisse wesentlich.

Im Appendix wird eine ausführliche Beweisführung des Theorems 3 in [M] angegeben, das im Kapitel 6 eine wesntliche Rolle spielt.

KEYWORDS

Diophantine Equations, Cyclotomic Fields, Nagell-Ljunggren Equation, Skolem, Abouzaid, Exponential Diophantine Equation, Baker's Inequality, Subspace Theorem.

REFERENCES

[A] M. ABOUZAID, *Heights and logarithmic gcd on algebraic curves*, *Int. J. Number Th.* **4**, pp. 177–197 (2008).

[BBGP] A.BAZSO AND A.BÉRCZES AND K.GYÖRY AND A.PINTÉR, *On the resolution of equations $Ax^n - By^n = C$ in integers x , y and n $\geq$ 3, II*, *Publicationes Mathematicae Debrecen* **76**, pp. 227 – 250 (2010).

[BGMP] M. A. BENNETT, K. GYŐRY, M. MIGNOTTE AND Á. PINTÉR, *Binomial Thue equations and polynomial powers*, *Compositio Math.* **142**, pp. 1103–1121 (2006).

[M] P. MIHĂILESCU *Class Number Conditions for the Diagonal Case of the Equation of Nagell and Ljunggren*, *Diophantine Approximation*, Springer Verlag, Development in Mathematics **16**, pp. 245–273 (2008).

[S1] TH. SKOLEM, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, *Avhdl. Norske Vid. Akad. Oslo I* **12**, pp. 1–16 (1929).

[S2] T. SKOLEM, *Lösung gewisser Gleichungssysteme in ganzen Zahlen oder ganzzahligen Polynomen mit beschrnktem gemeinschaftlichen Teiler*, *Oslo Vid. Akar. Skr. I*, **12** (1929).