COMPOSITIO MATHEMATICA

KLAUS LANGMANN

Lösungsanzahl der Thue-Gleichung

Compositio Mathematica, tome 86, n° 1 (1993), p. 101-105
<http://www.numdam.org/item?id=CM_1993__86_1_101_0>

Compositio Mathematica **86**: 101–105, 1993.

Lösungsanzahl der Thue- Gleichung

KLAUS LANGMANN
Mathematisches Institut, Universität Münster, Einsteinstraße 62, D-4400 Münster

Received 12 November 1991; accepted in revised form 25 March 1991

Sei $P(X, Y) \in \mathbb{Z}[X, Y]$ ein homogenes irreduzibeles Polynom vom Grad d. Thue bewies 1909, daß die Gleichung $P(X, Y) = \mathbf{h}$ bei festem $h \in \mathbb{Z}$ nur endlich viele Lösungen $(x, y) \in \mathbb{Z}^2$ mit $(x, y) = 1$ hat, falls $d \geqslant 3$ ist. Die Lösungsanzahl dieser Gleichung wurde 1983 von Evertse [2] abgeschätzt. Die dabei erhaltene Schranke wurde 1987 von Bombieri und W. M. Schmidt [1] verbessert: Es gibt eine universelle Konstante K, so daß diese Lösungsanzahl $\leqslant K d^{t+1}$ ist, wobei t die Anzahl der Primfaktoren von h ist. Es wird vermutet, daß der Exponent $t + 1$ dabei nicht verbessert werden kann. Nun hat man in der Zahlentheorie oft Aussagen, in denen Abschätzungen nicht verschärft werden können, weil für einige "kleine" Zahlen die Abschätzung wirklich genau ist (ein typisches Beispiel ist das Waringsche Problem). Somit können wir uns auch hier fragen, ob die Abschätzung der Lösungsanzahl der Gleichung $P(x, y) = h$ nicht verbessert werden kann, wenn wir jetzt nur noch fast alle $h \in \mathbb{Z}$ betrachten. Dies ist für $d \geqslant 4$ möglich (Folgerung 4): Dann haben wir für fast alle h höchstens $2d^t$ viele Lösungspaare (x, y), wobei jetzt t die Anzahl der verschiedenen Primfaktoren von h bedeutet. Eine ähnliche Aussage ("diese Lösungsanzahl ist höchstens gleich $4d^t$") hat vor kurzem Stewart ([6] Theorem 4) unter einer schwächeren Voraussetzung hergeleitet (Für diesen und anderen Hinweisen möchte ich dem Referenten an dieser Stelle Dank sagen).

Der Beweis dieser Aussage beruht auf einen 3-Werte-Satz (Satz 1). Dieser läßt sich sowohl funktionentheoretisch als auch zahlentheoretisch formulieren, so daß auch das Ergebnis über die Lösungsanzahl der Thue-Gleichung sowohl funktionentheoretisch (Satz 2) als auch zahlentheoretisch (Satz 3) formulierbar ist. Der funktionentheoretischen Variante des 3-Werte-Satzes liegt beweistechnisch der Satz von Picard-Borel zu Grunde, der zahlentheoretischen Fassung der dazu analoge Einheitensatz von Evertse-Laurent-van der Poorten-Schlickewei (siehe etwa [3]. Falls dieser Satz effektiv gemacht werden könnte, ergäbe sich auch eine effektive Schranke für die Größe der eventuellen Ausnahmezahlen h in Folgerung 4).

SATZ 1. ("3-Werte-Satz"). *Seien a_1, a_2, a_3 drei verschiedene komplexe Zahlen,*

die keine arithmetische Progression bilden (d.h. $a_i \neq \frac{1}{2}(a_j + a_k)$ *für* $\{i, j, k\} = \{1, 2, 3\}$*). Dann gilt:*

Analytische Version: *Sind f, g auf ganz* $\mathbb{C}$ *meromorphe Funktionen und gilt für die (durch alle Null- und Polstellen auf* $\mathbb{C}$ *gebildeten) Divisoren die Gleichheit* $\mathscr{D}(f - a_v) = \mathscr{D}(g - a_v)$ *für* $1 \leqslant v \leqslant 3$*, so ist* $f = g$ *oder* f, g *konstant.*

Zahlentheoretische Version: *Sei L ein fester Zahlkörper und S eine feste endliche Menge von Bewertungen, die alle archimedischen Bewertungen enthalten soll. Für* $f \in L^*$ *bedeute* $\mathscr{D}_S(f)$ *der Divisor* $\Sigma_{\mathfrak{p} \notin S} \operatorname{ord}_{\mathfrak{p}}(f)\mathfrak{p}$*. Dann gibt es nur endlich viele Ausnahmepaare* $(f, g) \in L^2$ *mit* $f \neq g$ *und* $\mathscr{D}_S(f - a_v) = \mathscr{D}_S(g - a_v)$ *für* $1 \leqslant v \leqslant 3$.

Beweis. Zur analytischen Version vergl. [4], zur zahlentheoretischen siehe [5].

SATZ 2. *Sei* $P(X, Y) = a \prod_{v=1}^{d} (X + a_v Y)$ *ein homogenes Polynom* $\in \mathbb{C}[X, Y]$ *mit paarweise verschiedenen* $a_1, \ldots, a_d$*. Sei* $d \geqslant 4$*. Falls* $d = 4$ *ist, mögen die Zahlen* $1/(a_2 - a_1)$, $1/(a_3 - a_1)$, $1/(a_4 - a_1)$ *keine arithmetische Progression bilden. Mit R bezeichne den Ring aller auf ganz* $\mathbb{C}$ *holomorphen Funktionen. Ist dann* $\mathscr{D}(h)$ *ein Hauptdivisor mit* $t := \#$ *Träger* $\mathscr{D}(h) < \infty$*, so gibt es höchstens* 16^t *viele Paare* $(f, g) \in R^2$ *mit Var* $f \cap$ *Var* $g = \varnothing$ *und*

$$\mathscr{D}(P(f, g)) = \mathscr{D}(h)$$

(wenn man die unendlich vielen trivialen Fälle, die aus (f, g) *durch Multiplikation* (fe, ge) *mit einer Einheit* $e \in R^*$ *entstehen, sowie die trivialen Fälle* $(f, g, h) = (\lambda e, \mu e, \tilde{e})$ *mit* $\lambda, \mu \in \mathbb{C}$, $e, \tilde{e} \in R^*$ *nicht beachtet).*

Beweis. Ordne die a_v so an, daß $1/(a_2 - a_1)$, $1/(a_3 - a_1)$, $1/(a_4 - a_1)$ keine arithmetische Progression bilden (für $d = 4$ geht dies nach Voraussetzung, für $d \geqslant 5$ kann wegen $1/(a_v - a_1) \neq 1/(a_u - a_1)$ für $v \neq u$ dies stets durch Umnumerierung erreicht werden, vergl. Beweis von [5] Folgerung 2).

Jetzt teilt für $1 \leqslant v \leqslant d$ der Divisor $\mathscr{D}(f + a_v g)$ den Divisor $\mathscr{D}(h)$. Da $\mathscr{D}(f + a_v g)$ und $\mathscr{D}(f + a_u g)$ für $v \neq u$ teilerfremd sind und da $\mathscr{D}(h)$ aus t vielen Trägerelementen besteht, gibt es bei festem v für $\mathscr{D}(f + a_v g)$ höchstens 2^t viele Möglichkeiten. Somit gibt es für die Quadrupel $(\mathscr{D}(f + a_v g))_{1 \leqslant v \leqslant 4}$ höchstens 16^t viele Möglichkeiten. Wenn wir mehr als 16^t viele modulo Einheiten verschiedene Paare $(f, g) \in R^2$ mit $\mathscr{D}(P(f, g)) = \mathscr{D}(h)$ hätten, wären also zwei solcher Quadrupel gleich. Das bedeutet also, daß es zwei modulo Einheiten verschiedene Paare (f_1, g_1) und (f_2, g_2) gäbe mit

$$\frac{f_1 + a_v g_1}{f_2 + a_v g_2} \in R^* \quad \text{für } 1 \leqslant v \leqslant 4 \tag{1}$$

Falls $a_1 = 0$ ist, so betrachte für $2 \leqslant v \leqslant 4$

$$\frac{g_1/f_1 - (-1/a_v)}{g_2/f_2 - (-1/a_v)} = \frac{(f_1 + a_v g_1)/(f_2 + a_v g_2)}{f_1/f_2}$$

Wegen (1) ist für $2 \leqslant v \leqslant 4$

$$\mathscr{D}(g_1/f_1 - (-1/a_v)) = \mathscr{D}(g_2/f_2 - (-1/a_v))$$

Nach der analytischen Version des 3-Werte-Satzes ist dann $g_1/f_1 = g_2/f_2$ oder g_1/f_1 konstant. Wegen $\operatorname{Var} g_i \cap \operatorname{Var} f_i = \varnothing$ führt $g_1/f_1 = g_2/f_2$ auf $(f_1, g_1) = e(f_2, g_2)$. g_1/f_1 konstant führt wegen $\operatorname{Var} f_1 \cap \operatorname{Var} g_1 = \varnothing$ auf $f_1, g_1 \in R^*$, und wir erhalten wieder einen der ausgeschlossenen trivialen Fälle.

Falls $a_1 \neq 0$ ist, so ist wegen (1) für $2 \leqslant v \leqslant 4$

$$\frac{f_1/(f_1 + a_1 g_1) - a_v/(a_v - a_1)}{f_2/(f_2 + a_1 g_2) - a_v/(a_v - a_1)} = \frac{(f_1 + a_v g_1)/(f_2 + a_v g_2)}{(f_1 + a_1 g_1)/(f_2 + a_1 g_2)} \in R^*$$

Nun bilden auch $\{a_v/(a_v - a_1)\}_{2 \leqslant v \leqslant 4}$ keine arithmetische Progression, und die Aussage folgt wie im Fall $a_1 = 0$.

Übrigens ist die Voraussetzung im Fall $d = 4$ invariant gegenüber Permutationen: Bildet $\{1/(a_v - a_1)\}_{2 \leqslant v \leqslant 4}$ eine arithmetische Progression, so auch $\{1/(a_v - a_4)\}_{1 \leqslant v \leqslant 3}$. Ist $P(X, Y)$ irreduzibel über $\mathbb{Q}$, so hat dann notwendigerweise die zugehörige Galois-gruppe höchstens 8 Elemente. Ein Beispiel für diese Situation liefert $P(X, Y) = X^4 + cY^4$.

SATZ 3. *Sei* $P(X, Y) \in \mathbb{Z}[X, Y]$ *ein homogenes irreduzibeles Polynom vom* Grad $d \geqslant 4$. *Im Fall* $d = 4$ *möge* $\{1/(a_v - a_1)\}_{2 \leqslant v \leqslant 4}$ *keine arithmetische Progression bilden, wobei die* a_v *die Nullstellen von* $P(X, 1)$ *sein sollen. S sei wie in Satz* 1. *Dann gibt es für fast alle Hauptdivisoren* $\mathscr{D}_S(h)$ *bei* $t := \#$ *Träger* $\mathscr{D}_S(h)$ *höchstens* $2d^t$ *viele Paare* $(f, g) \in \mathbb{Z}^2$ *mit* $ggt(f, g) = 1$ *und*

$$\mathscr{D}_S(P(f, g)) = \mathscr{D}_S(h)$$

Beweis. Sei L der Zerfällungskörper von $P(X, Y)$. $\tilde{S} \supset S$ sei eine Menge von Bewertungen, so daß bei $P(X, Y) = a \prod_{v=1}^{d} (X - a_v Y)$ alle Zahlen a, a_v, $a_v - a_u$ für $v \neq u$ stets $\tilde{S}$-Einheiten sind. Schließlich soll jede Primzahl p, die in $\mathcal{O}(L)$ nicht in verschiedene Primideale zerfällt, noch eine $\tilde{S}$-Einheit werden. (Dies geht, weil es nur endlich viele solcher p gibt). Wegen $(f, g) = 1$ sind dann $(f - a_v g)$ und $(f - a_u g)$ für $v \neq u$ im Ring $\mathcal{O}$ der $\tilde{S}$-ganzen Zahlen von L teilerfremd. Sei $h\mathbb{Z} = \bigcap_{i=1}^{t} p_i^{n_i} \mathbb{Z}$. Dabei kann durch Weglassen aller S-Einheiten p_i (für das

dadurch abgeänderte neue h ändert sich der Divisor $\mathscr{D}_S(h)$ nicht) *oBdA* angenommen werden, daß stets $p_i\mathcal{O} \neq \mathcal{O}$ ist. Fixiere zu jedem $i \leqslant t$ ein Primideal $\mathfrak{p}_i \subset \mathcal{O}$ mit $\mathfrak{p}_i \supset p_i\mathcal{O}$. Dann ist $h\mathcal{O} = \bigcap_i \bigcap_{\sigma \in G} \sigma(\mathfrak{p}_i)^{n_i}$, wobei G die Galoisgruppe von L über $\mathbb{Q}$ bedeutet. Nun gibt es zu jedem $i \leqslant t$ ein $\sigma_i \in G$ mit $(f - a_1 g)\mathcal{O} \subset \sigma_i(\mathfrak{p}_i)$ (denn sonst wäre $(f - \sigma^{-1}(a_1)g)\mathcal{O} \not\subset \mathfrak{p}_i \; \forall \sigma \in G$, also $(f - a_v g)\mathcal{O} \not\subset \mathfrak{p}_i$ für $1 \leqslant v \leqslant d$ und damit $\prod_{v=1}^{d}(f - a_v g)\mathcal{O} \not\subset \mathfrak{p}_i$). Ist ferner $(f - a_1 g)\mathcal{O} \subset \sigma_u(\mathfrak{p}_i) \cap \sigma_v(\mathfrak{p}_i)$, so ist $(f - \sigma_w^{-1}(a_1)g)\mathcal{O} \subset \mathfrak{p}_i$ für $w \in \{u, v\}$; dann muß wegen der oben erwähnten Teilerfremdheit schon $\sigma_u^{-1}(a_1) = \sigma_v^{-1}(a_1)$ sein. Bezeichnet U die Untergruppe von G, die $\mathbb{Q}(a_1)$ fest läßt, so ist also $\sigma_u \in \sigma_v U$. Damit ist $(f - a_1 g)\mathcal{O} \subset \sigma_j(\mathfrak{p}_i)$ genau dann, wenn $\sigma_j \in \sigma_i U$ ist. Es folgt

$$(f - a_1 g)\mathcal{O} = \bigcap_{i=1}^{t} \bigcap_{\sigma \in \sigma_i U} (\sigma(\mathfrak{p}_i))^{n_i} \tag{2}$$

Nun gibt es für die Nebenklassen $\sigma_i U$ für festes $i \leqslant t$ genau d viele Möglichkeiten. Damit gibt es bei festem h für die rechte Seite von (2) höchstens d^t viele Möglichkeiten. Falls es jetzt mehr als $2d^t$ viele Paare $(f, g) \in \mathbb{Z}^2$ mit $(f, g)\mathbb{Z} = \mathbb{Z}$ und $\mathscr{D}_S(P(f, g)) = \mathscr{D}_S(h)$ gibt, ist demnach für zwei Paare $(f_1, g_1) \neq \pm(f_2, g_2)$ schon $(f_1 - a_1 g_1)\mathcal{O} = (f_2 - a_1 g_2)\mathcal{O}$. Indem wir darauf die Galoisautomorphismen σ_v anwenden, folgt

$$(f_1 - a_v g_1)/(f_2 - a_v g_2) \in \mathcal{O}^* \quad \text{für } 1 \leqslant v \leqslant 4 \tag{3}$$

Diese Gleichung (3) entspricht (1) im Beweis von Satz 2. Genau wie dort zeigen wir mit dem zahlentheorethischen 3-Werte-Satz, daß aus der Beziehung (3) schon $f_1/g_1 = f_2/g_2$ bis auf endlich viele Ausnahmepaare $(f_1/g_1, f_2/g_2)$ folgt. Wegen $(f_1, g_1) \neq \pm(f_2, g_2)$ und $(f_1, g_1)\mathbb{Z} = \mathbb{Z} = (f_2, g_2)\mathbb{Z}$ ist aber $f_1/g_1 = f_2/g_2$ nicht möglich. Jedes dieser endlich vielen Ausnahmepaare $(f_1/g_1, f_2/g_2)$ führt wieder auf endlich viele Ausnahmequadrupel (f_1, g_1, f_2, g_2). Da diese Ausnahmequadrupel von dem jetzt laufenden $\mathscr{D}_S(h)$ nicht abhängen, können somit für $\mathscr{D}_S(h)$ nur endlich viele Möglichkeiten auftreten, für die die Gleichung $\mathscr{D}_S(P(f, g) = \mathscr{D}_S(h)$ mehr als $2d^t$ viele Lösungen $(f, g) \in \mathbb{Z}^2$ mit $(f, g) = 1$ hat.

FOLGERUNG 4. *Sei $P(X, Y)$ wie in Satz 3. Dann hat für fast alle $h \in \mathbb{Z}$ die Gleichung $|P(X, Y)| = h$ höchstens $2d^t$ viele Lösungen $(f, g) \in \mathbb{Z}^2$ mit $(f, g) = 1$, wobei t die Anzahl der verschiedenen Primfaktoren von h bedeutet.*

Den "3-Werte-Satz" können wir sowohl in der analytischen als auch in der zahlentheoretischen Version verschärfen. Damit werden wir an anderer Stelle zeigen: Es gibt eine durch algebraische Eigenschaften des Polynoms $P(X, Y)$ definierte Zahl A, so daß für fast alle $h \in \mathbb{Z}$ die Gleichung $|P(X, Y)| = h$ höchstens Ad^{t-1} viele Lösungen hat. Da oft $A < 2d$ ist, bekommen wir hier in vielen Fällen bessere Abschätzungen als in Folgerung 4. Insbesondere folgt, daß bei festem

$a \in \mathbb{Z}$ für fast alle Primpotenzen h die Gleichung $x^d + y^d = ah$ höchstens eine Lösung (x, y) mit $ggt(x, y) = 1$ und mit $x > y > 0$ hat.

Literatur

1. Bombieri, E. and Schmidt, W. M., On Thue's equation. *Invent. Math.* 88, 69–81 (1987).
2. Evertse, J.H., Upper bounds for the number of solutions of diophantine equations. *Math. centrum Amsterdam* 1987, pp. 1–127.
3. Evertse, J. H., On sums of S-units and linear recurrences. *Compos. Math.* 53, 225–244 (1984).
4. Langmann, K., Anwendungen des Satzes von Picard. *Math. Ann.* 266, 369–390 (1984).
5. Langmann, K., Der 4-Werte-Satz in der Zahlentheorie. Compos. Math. 82, 137–142 (1992).
6. Stewart, C. L., On the number of solutions of polynomial congruences and Thue equations. Erscheint in Journal of the AMS.