COMPOSITIO MATHEMATICA

KLAUS LANGMANN

Eindeutigkeit der Lösungen der Gleichung $x^d + y^d = ap$

Compositio Mathematica, tome 88, n° 1 (1993), p. 25-38

<http://www.numdam.org/item?id=CM_1993__88_1_25_0>

Compositio Mathematica **88**: 25–38, 1993.

Eindeutigkeit der Lösungen der Gleichung $x^d + y^d = ap$

KLAUS LANGMANN
Mathematisches Institut, Einsteinstr. 62, D 4400 Münster

Received 21 February 1992; accepted 6 July 1992

Seit langer Zeit weiß man, daß bei festem $a \in \mathbb{N}$ die Gleichung $x^2+y^2=ap$ für unendlich viele Primzahlen p mehr als eine Lösung $(x, y) \in \mathbb{N}^2$ mit $x > y$ haben kann (z.B. für $a=5$). Von daher mag es interessant sein, daß für $d \geqslant 4$ die analoge Gleichung $x^d+y^d=ap$ für *fast alle* Primpotenzen p höchstens eindeutig lösbar ist (Folgerung 4). Hierbei kann natürlich nicht eine solche Eindeutigkeit für *alle* Primzahlen p erwartet werden (denn z.B. ist $133^4+134^4=ap=158^4+59^4$ mit geeignetem $a \in \mathbb{N}$ und geeigneter Primzahl p). Diese Eindeutigkeitsaussage ist Spezialfall einer Abschätzung für die Anzahl der Lösungen der Thue-Gleichung (Satz 3), die in gewisser Weise die Ergebnisse von [4] verschärft (vergl. dazu auch [1, 2, 5]).

Weiter weiß man, daß die Gleichung $x^2+y^2=p=u^2+uv+v^2$ für unendlich viele Primzahlen lösbar ist. Von daher ist wohl nicht klar, daß gewisse Gleichungen der Form $x^4+y^4=p=u^4+\alpha u^2v^2+\beta v^4$ nur für endlich viele Primpotenzen p lösbar sind (Folgerung 7). Diese Aussage ist Spezialfall von Satz 6, der für gewisse homogene Polynome P, Q die Unlösbarkeit von $P(x, y)=p=Q(u, v)$ zeigt.

An dieser Stelle sei dem Referenten für wertvolle Hinweise (die insbesondere zur Formulierung von Satz 3 führten) gedankt.

Zunächst beweisen wir folgenden "3-Werte-Satz", der das zahlentheoretische Analogon zu einem entsprechenden funktionentheoretischem Satz ist (weshalb die Sätze dieser Arbeit auch entsprechend funktionentheoretisch formuliert werden können, vergl. Satz 2 in [4]. Die Numerierung b_2, b_3, b_4 in diesem Lemma 1 erfolgt mit Rücksicht auf die Anwendung in Beweis von Satz 2)

LEMMA 1. *Sei K ein fester Zahlkörper und S eine feste endliche Menge von Bewertungen, die alle archimedischen Bewertungen enthalten soll. R bezeichne den Ring der S-ganzen Zahlen von K. Für $f \in K^*$ bedeute $\mathscr{D}_S(f)$ der Divisor $\Sigma_{\not\in S} \operatorname{ord}_{\not}(f)\not$. Weiter seien b_2, b_3, b_4 (bzw. $\tilde{b}_2, \tilde{b}_3, \tilde{b}_4$) drei paarweise verschiedene Zahlen aus K. Seien $\{z_h\}$ und $\{\tilde{z}_h\}$ zwei Folgen aus K mit $z_h \neq z_k$, $\tilde{z}_h \neq \tilde{z}_k$ für alle $h \neq k$ und mit*

$$\mathscr{D}_S(z_h - b_w) = \mathscr{D}_S(\tilde{z}_h - \tilde{b}_w) \quad \text{für } 2 \leqslant w \leqslant 4 \text{ und für alle } h. \tag{1}$$

Dann ist nach Teilfolgenbildung der z_h und $\tilde{z}_h$ stets

$$(z_h - b_2)/(b_3 - b_2) = (\tilde{z}_h - \tilde{b}_2)/(\tilde{b}_3 - \tilde{b}_2$$

und

$$(b_4 - b_2)/(b_3 - b_2) = (\tilde{b}_4 - \tilde{b}_2)/(\tilde{b}_3 - \tilde{b}_2) \tag{2}$$

oder aber es gibt zwei (von h unabhängige) gebrochen-lineare Funktionen R_1, $R_2 \in K(T)$, so daß nach eventueller fester Vergrößerung von S für gewisse (von h abhängende) Einheiten $e \in R^*$ gilt

$$(z_h, \tilde{z}_h) = (R_1(e), R_2(e)) \tag{3}$$

Beweis. OBdA $b_i - b_j \in R^*$ und $\tilde{b}_i - \tilde{b}_j \in R^*$ für $i \neq j$. Setze

$$u_h := (z_h - b_2)/(b_3 - b_2), \qquad a := (b_4 - b_2)/(b_3 - b_2)$$

und definiere entsprechend $\tilde{u}_h, \tilde{a}$. Es ist $a \neq 0, 1 \neq \tilde{a}$. Aus (1) folgt

$$\mathscr{D}_S(u_h) = \mathscr{D}_S(\tilde{u}_h),\ \mathscr{D}_S(u_h - 1) = \mathscr{D}_S(\tilde{u}_h - 1),\ \mathscr{D}_S(u_h - a) = \mathscr{D}_S(\tilde{u}_h - \tilde{a}).$$

Wir haben also Einheiten $e_{ih} \in R^*$ mit

$$u_h e_{1h} = \tilde{u}_h,\ (u_h - 1)e_{2h} = \tilde{u}_h - 1,\ (u_h - a)e_{3h} = \tilde{u}_h - \tilde{a}. \tag{4}$$

Wir lassen jetzt der Einfachheit den Index h fort. Wenn für eine unendliche Teilfolge der h (also *oBdA* wieder für alle h, da die Aussage im Lemma sich ja nur auf Teilfolgen bezieht) stets $e_1 = \alpha$ und $e_2 = \beta$ unabhängig von h wäre, so erhalten wir aus (4) im Fall $\alpha \neq \beta$, daß u nur einen einzigen Wert annähme. Der Fall $\alpha = \beta$ führt auf $u = \tilde{u}$ und damit im Fall $a = \tilde{a}$ auf die Behauptung (2) und im Fall $a \neq \tilde{a}$ auf $u = (ae_3 - \tilde{a})/(e_3 - 1) = \tilde{u}$ und damit auf die Behauptung (3). Entsprechendes ergibt sich, wenn $e_1 = \alpha$ und $e_3 = \beta$ bzw. $e_2 = \alpha$ und $e_3 = \beta$ ist.

Jetzt behandeln wir den Fall, daß e_2 und e_3 bei laufendem h in jeder Teilfolge unendlich viele Werte annehmen und $e_1 = \alpha =$ konstant ist. Wir erhalten aus (4)

$$e_3(\alpha^{-1} - a) + e_2(1 - \tilde{\alpha}\alpha^{-1}) + e_2 e_3(\alpha^{-1}(a - 1)) = 1 - \tilde{a}. \tag{5}$$

Wir benutzen jetzt den Einheitensatz von Evertse-Laurent-van der Poorten-Schlickewei (im folgendem nach dem alphabetisch erstgenannten zitiert; siehe z.B. [3]): Ist m eine feste Zahl und sind $e^*_{ih} \in R^*$ Einheiten mit $\Sigma_{i=1}^{m} e^*_{ih} = 1$ für alle laufenden h, so ist nach Teilfolgenbildung der h für einen festen Index $j \leqslant m$

entweder e_{jh}^* unabhängig von h, oder e_{jh}^* taucht in einer Teilsumme $\Sigma_{i\in I} e_{ih}^*=0$ auf (also $j\in I$).

Da e_2, e_3 bei laufendem h in jeder Teilfolge unendlich viele Werte annehmen, erhalten wir aus (5) deswegen nach erneuter Teilfolgenbildung

$$e_3(\alpha^{-1}-a)+e_2(1-\tilde{a}\alpha^{-1})=0 \quad \text{und} \quad e_2e_3(\alpha^{-1}(a-1))=1-\tilde{a}. \tag{6}$$

Setzt man die 1. Gleichung von (6) in die 2. Gleichung ein, so erhält man, falls nicht $a\alpha=1=\tilde{a}\alpha^{-1}$ ist, einen Widerspruch dazu, daß e_2, e_3 unendlich viele Werte annehmen. Im Fall $a\alpha=1=\tilde{a}\alpha^{-1}$ erhalten wir $a\tilde{a}=1$, $e_1=\tilde{a}$, $e_3=-e_2^{-1}\tilde{a}(1-\tilde{a})/(1-a)$ und $u=(e_2-1)/(e_2-\tilde{a})$, $\tilde{u}=\tilde{a}(e_2-1)/(e_2-\tilde{a})$ und damit wieder die in (3) behauptete Form. Entsprechendes ergibt sich, wenn e_1 und e_3 bei laufendem h unendlich viele Werte annehmen (wir erhalten dann $(1-a)(1-\tilde{a})=1$) bzw. wenn e_1 und e_2 unendlich viele Werte annehmen (wir erhalten dann $a+\tilde{a}=1$).

Jetzt müssen wir noch den Fall behandeln, daß alle e_i mit laufendem h jeweils unendlich viele Werte annehmen für jede unendliche Teilfolge der h. Aus (4) folgt die Identität

$$e_3e_1^{-1}+(-e_3a)+e_1^{-1}e_2e_3(a-1)+e_2+(-\tilde{a}e_2e_1^{-1})=1-\tilde{a}. \tag{7}$$

Wir betrachten in dieser Summe $\Sigma_{i=1}^5 e_i^*=1-\tilde{a}$ maximale Indexmengen J mit $\Sigma_{i\in J} e_i^*=0$ für eine gewisse unendliche Teilfolge der h. Wir müssen Fallunterscheidungen treffen:

Fall 1. $(e_3e_1^{-1})$ und $(-\tilde{a}e_2e_1^{-1})$ gehören nicht zu den e_i^* mit $i\in J$. Dann nimmt also nach Evertse für eine Teilfolge der h stets $e_3e_1^{-1}$ einen festen Wert α und $e_2e_1^{-1}$ einen festen Wert β an. Aus (4) folgt

$$u(\tilde{a}\beta-\tilde{a}+1-\alpha)=(\tilde{a}\beta-a\alpha).$$

Da u ja unendlich viele Werte annehmen soll, muß $\alpha=(\tilde{a}-1)/(a-1)$ und $\beta=a(\tilde{a}-1)/\tilde{a}(a-1)$ sein. Dies führt auf $u=[(a\tilde{a}-\tilde{a})+e_1(a-a\tilde{a})]/[e_1(a-\tilde{a})]$, womit $(z,\tilde{z})$ wieder die Form (3) hat.

Fall 2. $(e_3e_1^{-1})$ und $(-\tilde{a}e_2e_1^{-1})$ gehören beide zu den e_i^* mit $i\in J$.

Dann müssen natürlich die Summanden $(-e_3a)$ und e_2 in der Summe (7) ebenfalls zu den e_i^* mit $i\in J$ gehören (da sonst nach Evertse e_3 oder e_2 nur endlich viele Werte bei laufendem h annehmen würden). Also haben wir im Fall 2

$$e_1^{-1}e_2e_3(a-1)=1-\tilde{a} \quad \text{und} \quad e_1^{-1}+(-\tilde{a}e_2e_1^{-1}e_3^{-1})+e_2e_3^{-1}=a. \tag{8}$$

Da e_1 ja unendlich viele Werte annehmen muß, folgt aus der 2. Gleichung von

(8) wieder nach Evertse, daß einer der beiden Fälle auftreten muß:

Fall 2(*a*). $e_1^{-1}+e_2e_3^{-1}=0$ und $-\tilde{a}e_2e_1^{-1}e_3^{-1}=a$.

Fall 2(*b*). $e_1^{-1}+(-\tilde{a}e_2e_1^{-1}e_3^{-1})=0$ und $e_2e_3^{-1}=a$.

Fall 2(a) führte auf $e_1^{-2}=a/\tilde{a}$ und würde deshalb nur endlich viele Werte für e_1 implizieren. Fall 2(b) führt mittels der 1. Gleichung von (8) auf $a\tilde{a}=1$ und $u=-1/ae_3$, $\tilde{u}=-ae_3$, womit wir wieder eine Darstellung (3) bekommen.

Fall 3. $(e_3e_1^{-1})$ gehört zu den e_i^* mit $i\in J$, und $(-\tilde{a}e_2e_1^{-1})$ gehört nicht dazu.

Wir erhalten dann [da wieder nach Evertse sowohl $(-e_3a)$ als e_2 als auch $e_1^{-1}e_2e_3(a-1)$ in der Teilsumme $\Sigma_{i\in J}e_i^*$ von (7) auftauchen muß]:

$$-\tilde{a}e_2e_1^{-1}=(1-\tilde{a}) \quad \text{und} \quad e_3e_2^{-1}e_1^{-1}+(a-1)e_3e_1^{-1}+(-ae_3e_2^{-1})=-1 \tag{9}$$

Jetzt betrachten wir maximale Indexmengen I mit $\Sigma_{i\in I}\bar{e}_i^*=0$, wobei $\Sigma_{i=1}^{3}\bar{e}_i^*=-1$ die zweite Summe aus (9) ist.

Fall (3*a*) I ist leer. Dann würden nach Evertse $e_3e_2^{-1}e_1^{-1}$, $e_3e_1^{-1}$ und $e_3e_2^{-1}$ alle nur endlich viele Werte bei laufendem h annehmen, womit auch e_1 nur endlich viele Werte annähme.

Fall 3(*b*) $e_3e_2^{-1}e_1^{-1}+(a-1)e_3e_1^{-1}=0$. In diesem Fall nähme also e_2 nur einen Wert an.

Fall 3(*c*) $e_3e_2^{-1}e_1^{-1}+(-ae_3e_2^{-1})=0$. Dann nähme also e_1 nur einen Wert an.

Fall (3*d*) $(a-1)e_3e_1^{-1}+(-ae_3e_2^{-1})=0$. Aus der zweiten Gleichung von (9) folgt dann $e_3e_2^{-1}e_1^{-1}=-1$; mit der ersten Gleichung von (9) ergibt sich daraus $a+\tilde{a}=1$, $u=[(1-\tilde{a})e_1+\tilde{a}]/e_1$ und $\tilde{u}=(1-\tilde{a})e_1+\tilde{a}$. Wieder haben wir also eine Darstellung der Form (3) erhalten.

Fall 4. $(-\tilde{a}e_2e_1^{-1})$ gehört zu den e_i^* mit $i\in J$ und $e_3e_1^{-1}$ gehört nicht dazu.

Dieser Fall wird analog Fall 3 mit vier Unterfällen geführt und ergibt schließlich eine Darstellung $(1-a)(1-\tilde{a})=1$, $u=(e_1+1)/e_1$ und $\tilde{u}=e_1+1$. Damit ist Lemma 1 gezeigt.

Die Formulierung in Lemma 1 ist ineffektiv. Wenn jedoch der Satz von Evertse in effektiver Form ausgesprochen werden könnte, so könnte man auch Lemma 1 (und damit die weiteren Sätze dieser Arbeit) effektiv formulieren. Denn wie der Beweis von Lemma 1 zeigt, sind die unendlichen Lösungsscharen von (4) *genau* durch folgende 11 Fälle gegeben:

1. $a=\tilde{a}$, $u=\tilde{u}$,
2. $u=(ae_3-\tilde{a})/(e_3-1)$, $e_1=1$, $e_2=1$,
3. $u=(ae_2-a)/(ae_2-\tilde{a})$, $e_1=\tilde{a}/a$, $e_3=\tilde{a}/a$,
4. $u=(\tilde{a}-a)/[(\tilde{a}-1)-(a-1)e_1]$, $e_2=(\tilde{a}-1)/(a-1)$, $e_3=(\tilde{a}-1)/(a-1)$,
5. $a\tilde{a}=1$, $u=(e_2-1)/(e_2-\tilde{a})$, $e_1=\tilde{a}$, $e_3=e_2^{-1}\tilde{a}^2$,
6. $a+\tilde{a}=1$, $u=1/(1+e_1)$, $e_2=e_1^{-1}$, $e_3=-1$,
7. $(1-a)(1-\tilde{a})=1$, $u=-\tilde{a}/(1-\tilde{a}-e_1)$, $e_2=1-\tilde{a}$, $e_3=\tilde{a}^2a^{-2}e_1^{-1}$,
8. $u=[(a\tilde{a}-\tilde{a})+e_1(a-\tilde{a}a)]/e_1(a-\tilde{a})$, $e_2=a(\tilde{a}-1)e_1/\tilde{a}(a-1)$, $e_3=(\tilde{a}-1)e_1/(a-1)$,

9. $a\tilde{a} = 1$, $u = -1/ae_3$, $e_2 = e_3 a$, $e_1 = e_3^2 a^2$,
10. $a + \tilde{a} = 1$, $u = (ae_1 + \tilde{a})/e_1$, $e_2 = -a\tilde{a}^{-1}e_1$, $e_3 = a\tilde{a}^{-1}e_1^2$,
11. $(1-a)(1-\tilde{a}) = 1$, $u = (e_1 + 1)/e_1$, $e_2 = e_1^2$, $e_3 = (1-\tilde{a})e_1$.

Mit diesen 11 Fällen können also die in (3) auftauchenden gebrochen-linearen Funktionen R_1, R_2 explezit angegeben werden, so daß dann in den jetzt folgenden Beweisen effektiv weitergeschlossen werden kann. In dem sich anschließendem Satz 2 haben wir oft bessere Schranken als in [4] Folgerung 4 (im Gegensatz zu [4] Satz 3 darf sich aber jetzt $P(x, y)$ nur um eine feste S-Einheit von h unterscheiden):

LEMMA 2. *Sei* $P(X, Y) \in \mathbb{Z}[X, Y]$ *ein festes irreduzibeles homogenes Polynom vom* Grad $d \geqslant 4$. *Weiter sei* c *eine feste natürliche Zahl und* $c_1, \ldots, c_v$ *feste paarweise verschiedene rationale Zahlen. Dann gibt es zu fast allen* $h \in \mathbb{Z}$ *höchstens* Ad^{t-1} *viele verschiedene Quotienten* x/y, *so daß* $(cs, cy) \in \mathbb{Z}^2$, $ggT(cx, cy) \leqslant c^2$ *und so daß* $P(x, y) \in \{c_1 h, \ldots, c_v h\}$ *ist. Dabei bedeutet* t *die Anzahl der verschiedenen Primfaktoren* p_i *von* h *mit* $p_i \geqslant c$ *und* A *die Anzahl der verschiedenen Quotienten* $L_1(T)/L_2(T) \in \mathbb{Q}(T)$ *mit linearen Polynomen* $L_1(T)$, $L_2(T) \in \mathbb{C}[T]$ *und mit*

$$P(T, 1) = P(L_1(T), L_2(T))$$

(*wobei der triviale Fall* $L_1(T) = T$, $L_2(T) = 1$ *mitgezählt wurde*)

Beweis. Angenommen, für unendlich viele h wäre die behauptete Abschätzung falsch. Sei dann $P(x_{jh}, y_{jh}) = c_{\mu(j,h)} h$ für $0 \leqslant j \leqslant Ad^{t-1}$ mit $x_{jh}/y_{jh} \neq x_{ih}/y_{ih}$ für $i \neq j$. Schreibe $c_\mu = \tilde{c}_\mu / \tilde{\tilde{c}}_\mu$ mit $\tilde{c}_\mu, \tilde{\tilde{c}}_\mu \in \mathbb{Z}$. Weiter schreibe

$$P(X, Y) = \alpha_0 \prod_{w=1}^{d} (X - \alpha_w Y)$$

und setze $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$. Sei $R \subset K$ eine endlich erzeugte $\mathbb{Z}$-Algebra, so daß $\tilde{c}_\mu, \tilde{\tilde{c}}_\mu, c!, \alpha_0, \alpha_1, \ldots, \alpha_d \in R^*$ und $\alpha_m - \alpha_n \in R^*$ für $1 \leqslant m \neq n \leqslant d$ ist. *OBdA* ist R faktoriell (wegen der Endlichkeit der Klassenzahl ist stets die Lokalisation nach einem geeignetem Element schon faktoriell). Mit $\mathscr{D}(z)$ bezeichne wieder die Divisoren $\Sigma_{\mathfrak{p} \subset R} \operatorname{ord}_{\mathfrak{p}}(z)\mathfrak{p}$, wobei $\mathfrak{p}$ alle Primideale in R durchläuft. Wir haben also für $0 \leqslant j \leqslant Ad^{t-1}$

$$\mathscr{D}\left(\prod_{w=1}^{d} (x_{jh} - \alpha_w y_{jh})\right) = \mathscr{D}(h). \tag{11}$$

Setze $\tilde{c} := c! \prod \tilde{c}_\mu \tilde{\tilde{c}}_\mu$ und betrachte die Lokalisation $\mathbb{Z}_{\tilde{c}}$. Schreibe $h\mathbb{Z}_{\tilde{c}} = \bigcap_{i=1}^{t} (p_i \mathbb{Z}_{\tilde{c}})^{n_i}$ mit Primzahlen $p_i \in \mathbb{Z}$, $p_i \notin R^*$ (hierbei wird eventuell t kleiner als in der Behauptung unseres Satzes). Fixiere zu jedem $i \leqslant t$ ein Primideal $\mathfrak{p}_i \subset R$ mit $\mathfrak{p}_i \supset p_i R$. Dann ist $hR = \bigcap_i \bigcap_{\sigma \in G} (\sigma(\mathfrak{p}_i))^{n_i}$, wobei G die Galoisgruppe

von K über $\mathbb{Q}$ bedeutet. Nun gibt es bei festem $0 \leqslant j \leqslant Ad^{t-1}$ zu jedem $1 \leqslant i \leqslant t$ ein $\sigma_{ji} \in G$ (das natürlich von x_{jh}, y_{jh} abhängt) mit $(x_{jh} - \alpha_1 y_{jh}) \subset \sigma_{ji}(\mathfrak{p}_i)$ [denn sonst wäre $(x_{jh} - \sigma^{-1}(\alpha_1) y_{jh})R \not\subset \mathfrak{p}_i$ für alle $\sigma \in G$, also $(x_{jh} - \alpha_w y_{jh})R \not\subset \mathfrak{p}_i$ für alle $1 \leqslant w \leqslant d$ und damit $\prod_{w=1}^{d} (x_{jh} - \alpha_w y_{jh}) \not\subset \mathfrak{p}_i$]. Ist ferner $(x_{jh} - \alpha_1 y_{jh})R \subset \sigma_r(\mathfrak{p}_i) \cap \sigma_s(\mathfrak{p}_i)$, so ist $(x_{jh} - \sigma_q^{-1}(\alpha_1) y_{jh})R \subset \mathfrak{p}_i$ für $q \in \{r, s\}$. Dann muß wegen $(x_{jh} - \alpha_m y_{jh}, x_{jh} - \alpha_n y_{jh})R = R$ für $m \neq n$ schon $\sigma_r^{-1}(\alpha_1) = \sigma_s^{-1}(\alpha_1)$ sein. Bezeichnet U die Untergruppe von G, die $\mathbb{Q}(\alpha_1)$ festläßt, so ist also $\sigma_r \in \sigma_s U$. Damit ist $(x_{jh} - \alpha_1 y_{jh})R \subset \sigma(\mathfrak{p}_i)$ genau dann, wenn $\sigma \in \sigma_{ji} U$ ist. Es folgt

$$(x_{jh} - \alpha_1 y_{jh})R = \bigcap_{i=1}^{t} \bigcap_{\sigma \in \sigma_{ji} U} (\sigma(\mathfrak{p}_i))^{n_i}. \tag{12}$$

Damit gilt bei $\tilde{\sigma}_j := \sigma_{o1} \sigma_{j1}^{-1}$ für $0 \leqslant j \leqslant Ad^{t-1}$

$$(x_{jh} - \tilde{\sigma}_j(\alpha_1) y_{jh})R = \bigcap_{i=1}^{t} \bigcap_{\sigma \in \sigma_{o1} \sigma_{j1}^{-1} \sigma_{ji} U} (\sigma(\mathfrak{p}_i))^{n_i}. \tag{13}$$

Nun gibt es für die Nebenklassen von U genau d viele Möglichkeiten. Also gibt es für die rechte Seite von (13) insgesammt höchstens d^{t-1} viele Möglichkeiten (da ja bei $i = 1$ schon die Nebenklasse $\sigma_{o1} \sigma_{j1}^{-1} \sigma_{j1} U$ unabhängig vom laufendem j ist). Da j aus der Menge $\{0, 1, \ldots, Ad^{t-1}\}$ ist, gibt es also $A+1$ viele Indizes j ($oBdA$ wieder $0 \leqslant j \leqslant A$), so daß für jedes dieser j die rechte Seite von (13) bei festhaltenem h stets dasselbe Ideal ist. Somit gilt für $0 \leqslant j \leqslant A$

$$(x_{oh} - \alpha_1 y_{oh})R = (x_{jh} - \tilde{\sigma}_j(\alpha_1) y_{jh})R. \tag{14}$$

Wähle jetzt Galoisautomorphismen $\bar{\sigma}_1, \ldots, \bar{\sigma}_d$ mit $\bar{\sigma}_w(\alpha_1) = \alpha_w$ für $1 \leqslant w \leqslant d$. Dann folgt aus (14) bei $\tilde{\alpha}_j := \tilde{\sigma}_j(\alpha_1)$ (womit also insbesondere $\tilde{\alpha}_0 = \alpha_1$ ist) für $0 \leqslant j \leqslant A$ und für $1 \leqslant w \leqslant d$

$$(x_{oh} - \alpha_w y_{oh})R = (x_{jh} - \bar{\sigma}_w(\tilde{\alpha}_j) y_{jh})R. \tag{15}$$

Dabei ist für $m \neq n \leqslant d$ auch $\bar{\sigma}_m(\tilde{\alpha}_j) \neq \bar{\sigma}_n(\tilde{\alpha}_j)$ [denn sonst wäre $(x_{oh} - \alpha_m y_{oh})R = (x_{oh} - \alpha_n y_{oh})R$, woraus wegen $(x_{oh}, y_{oh})R = R$ und $\alpha_m - \alpha_n \in R^*$ schon $(x_{oh} - \alpha_m y_{oh})R = R$ folgte. Darauf können wir alle Automorphismen $\bar{\sigma}_w$ amwenden und erhalten über Produktbildung $P(x_{oh}, y_{oh})R = R$. Diese Gleichung hat aber nach Siegel-Mahler nur endlich viele verschiedene Lösungsquotienten (x_{oh}/y_{oh}) mit $x_{oh}, y_{oh} \in R$. Wegen $(cx_{oh}, cy_{oh}) \in \mathbb{Z}^2$ und $ggT(cx_{oh}, cy_{oh}) \leqslant c^2$ kommen dann auch nur endlich viele Paare (x_{oh}, y_{oh}) und damit auch nur endlich viele Werte für h in Frage.]

Setze nun für $0 \leqslant j \leqslant A$ und für $2 \leqslant w \leqslant d$

$$z_{jh} := x_{jh}/(x_{jh} - \tilde{\alpha}_j y_{jh}), \qquad b_{jw} := \tilde{\sigma}_w(\tilde{\alpha}_j)/(\bar{\sigma}_w(\tilde{\alpha}_j) - \tilde{\alpha}_j). \tag{16}$$

Bei festem j sind die b_{jw} paarweise verschieden. Da $\tilde{\alpha}_0 = \alpha_1$ und somit $\bar{\sigma}_w(\tilde{\alpha}_0) = \alpha_w$ ist, haben wir dann die Identität

$$\frac{z_{oh} - b_{ow}}{z_{jh} - b_{jw}} = \frac{(x_{oh} - \alpha_w y_{oh})/(x_{jh} - \bar{\sigma}_w(\tilde{\alpha}_j) y_{jh})}{(x_{oh} - \alpha_1 y_{oh})/(x_{jh} - \tilde{\alpha}_j y_{jh})} \cdot \frac{\alpha_1(\bar{\sigma}_w(\tilde{\alpha}_j) - \tilde{\alpha}_j)}{\tilde{\alpha}_j(\alpha_w - \alpha_1)}.$$

Nach (15) ist dieser Ausdruck in R^*. Somit wird für $0 \leqslant j \leqslant A$ und $2 \leqslant w \leqslant d$

$$\mathscr{D}(z_{oh} - b_{ow}) = \mathscr{D}(z_{jh} - b_{jw}). \tag{17}$$

Da $d \geqslant 4$ ist, können wir auf (17) unser Lemma 1 anwenden, wenn wir jetzt h laufen lassen (die b_{jw} hängen zwar auch von h ab, aber da sie aus einer endlichen Menge stammen, können wir nach Teilfolgenbildung der h annehmen, daß diese Zahlen unabhängig von h für $0 \leqslant j \leqslant A$, $2 \leqslant w \leqslant d$ sind). Da die Menge $\{z_{oh}\}$ bei laufendem h nicht endlich sein kann [wie nach (15) gezeigt wurde] ergeben sich mit Lemma 1 folgende Aussagen (18) und (19):

Nach Teilfolgenbildung der h gibt es eine feste Umordnung der j, so daß danach für eine gewisse Zahl $0 \leqslant r \leqslant A+1$ stets

$$\begin{aligned} &(z_{oh} - b_{o2})/(b_{o3} - b_{o2}) = (z_{jh} - b_{j2})/(b_{j3} - b_{j2}) \quad \text{für } 0 \leqslant j \leqslant r \\ &(b_{ow} - b_{o2})/(b_{o3} - b_{o2}) = (b_{jw} - b_{j2})/(b_{j3} - b_{j2}) \quad \text{für } 0 \leqslant j \leqslant r \text{ und } 2 \leqslant w \leqslant d \end{aligned} \tag{18}$$

ist und für $r+1 \leqslant j \leqslant A$ stets ein nichtkonstantes Funktionenpaar $(R_{1j}(T), R_{2j}(T))$ mit gebrochen-linearen Funktionen R_{1j}, R_{2j} existiert, so daß für gewisse (von j und h abhängende Einheiten $e \in R^*$) gilt

$$(z_{oh}, z_{jh}) = (R_{1j}(e), R_{2j}(e)) \quad \text{für } r+1 \leqslant j \leqslant A. \tag{19}$$

Im Fall (18) gilt für $0 \leqslant j \leqslant r$ und $2 \leqslant w \leqslant d$, daß

$$\frac{z_{oh} - b_{o2}}{b_{o3} - b_{o2}} - \frac{b_{ow} - b_{o2}}{b_{o3} - b_{o2}} = \frac{z_{jh} - b_{j2}}{b_{j3} - b_{j2}} - \frac{b_{jw} - b_{j2}}{b_{j3} - b_{j2}}$$

ist. Setzen wir hierin jetzt (16) ein, so ergibt sich für $1 \leqslant w \leqslant d$ und $0 \leqslant j \leqslant r$

$$(x_{oh} - \alpha_w y_{oh})/(x_{oh} - \alpha_1 y_{oh}) = [(x_{jh} - \bar{\sigma}_w(\tilde{\alpha}_j) y_{jh})/(x_{jh} - \tilde{\alpha}_j y_{jh})] \cdot \gamma_{jw} \tag{20}$$

wobei $\gamma_{j1} := 1$ und für $2 \leqslant w \leqslant d$

$$\gamma_{jw} := [(b_{o3} - b_{o2})/(b_{j3} - b_{j2})] \cdot [\tilde{\alpha}_j(\alpha_w - \alpha_1)/\alpha_1(\bar{\sigma}_w(\tilde{\alpha}_j) - \tilde{\alpha}_j)]$$

ist. Bilde das Produkt aus allen Gleichungen in (20) für $1 \leqslant w \leqslant d$. Da nach dem im Anschluß von (15) Gesagten die $\bar{\sigma}_w(\tilde{\alpha}_j)$ alle Wurzeln $\alpha_1, \ldots, \alpha_d$ durchlaufen, und da $P(x_{oh}, y_{oh}) = c_{\mu(o,h)}/c_{\mu(j,h)} P(x_{jh}, y_{jh})$ ist, folgt

$$(c_{\mu(j,h)}/c_{\mu(o,h)})(x_{oh} - \alpha_1 y_{oh})^d = (x_{jh} - \tilde{\alpha}_j y_{jh})^d \Big/ \prod_{w=1}^{d} \gamma_{jw}.$$

Hierauf wenden wir den Galoisautomorphismus $\bar{\sigma}_w$ an, dividieren durch y_{oh}^d und ziehen anschließend die d. Wurzel, so daß nach Teilfolgenbildung der h ein von h unabhängiges $\varepsilon_{jw} \in K$ existiert mit

$$(x_{oh}/y_{oh} - \bar{\sigma}_w(\alpha_1)) = (x_{jh}/y_{oh} - \bar{\sigma}_w(\tilde{\alpha}_j) y_{jh}/y_{oh}) \varepsilon_{jw}. \tag{21}$$

Nun ist (21) ein aus d linearen Gleichungen bestehendes System in den 3 Variabeln $t_1 := x_{oh}/y_{oh}$, $t_2 := x_{jh}/y_{oh}$, $t_3 := y_{jh}/y_{oh}$. Da dieses Gleichungssystem nicht eindeutig lösbar sein kann (sonst wäre ja x_{oh}/y_{oh} eindeutig festgelegt, und damit wäre wieder h eindeutig bestimmt), muß der Lösungsraum eindimensional sein. Somit gibt es also lineare Polynome $L_{1j}(T)$, $L_{2j}(T)$, so daß (21) die Identitäten

$$(T - \bar{\sigma}_w(\alpha_1)) = (L_{1j}(T) - \bar{\sigma}_w(\tilde{\alpha}_j) L_{2j}(T)) \varepsilon_{jw} \tag{22}$$

für $1 \leqslant w \leqslant d$ und für $0 \leqslant j \leqslant r$ impliziert. Aus (22) ergibt sich durch Produktbildung über alle w bei $\varepsilon_j := [\Pi_{w=1}^{d} \varepsilon_{jw}]^{1/d} \in \mathbb{C}$ (wobei eine beliebige d. Wurzel zu nehmen ist)

$$P(T, 1) = P(\varepsilon_j L_{1j}(T), \varepsilon_j L_{2j}(T)) \tag{23}$$

wobei noch galt

$$L_{1j}(x_{oh}/y_{oh})/L_{2j}(x_{oh}/y_{oh}) = x_{jh}/y_{jh}. \tag{24}$$

Wir müssen jetzt die j mit $r+1 \leqslant j \leqslant A$ betrachten. Mit der Definition (16) ergibt sich aus (19) die Existenz zweier gebrochen-linearer Funktionen Q_{1j}, Q_{2j} mit

$$(x_{oh}/y_{oh}, x_{jh}/y_{jh}) = (Q_{1j}(e), Q_{2j}(e)) \tag{25}$$

mit einer von j, h abhängenden Einheit $e \in R^*$. Es kann nicht $Q_{1j}(T)$ konstant sein (sonst wäre ja wieder x_{oh}/y_{oh} unabhängig von h). Dann ist also bei $S_j := Q_{2j} \circ Q_{1j}^{-1}$ schon

$$x_{jh}/y_{jh} = S_j(x_{oh}/y_{oh}). \tag{26}$$

Schreibe jetzt $S_j(T) = L_{1j}(T)/L_{2j}(T)$ mit linearen Funktionen L_{1j}, L_{2j}. Wir treffen jetzt Fallunterscheidung:

Fall (1). $P(T, 1)/P(L_{1j}(T), L_{2j}(T))$ ist konstant. Schreibe diese Konstante in der Form $(\varepsilon_j)^d$. Dann ist also für $r+1 \leqslant j \leqslant A$

$$P(T, 1) = P(\varepsilon_j L_{1j}(T), \varepsilon_j L_{1j}(T)). \tag{27}$$

Dieselbe Gleichung hatten wir schon in (23) gesehen, nur damals für $0 \leqslant j \leqslant r$. Da außerdem in beiden Fällen $\varepsilon_j L_{1j}(x_{oh}/y_{oh})/\varepsilon_j L_{2j}(x_{oh}/y_{oh}) = x_{jh}/y_{jh}$ gilt, müssen auch alle Quotienten $L_{1j}(T)/L_{2j}(T)$ verschieden sein für $0 \leqslant j \leqslant A$. Da $x_{jh}/y_{jh} \in \mathbb{Q}$ war und $x_{oh}/y_{oh} \in \mathbb{Q}$ eine unendliche Folge durchläuft, müssen alle Quotienten $L_{1j}(T)/L_{2j}(T)$ in $\mathbb{Q}(T)$ liegen. Dies ist ein Widerspruch zur Definition von A und somit kann der Fall (1) nicht auftreten.

Fall (2). Es gibt ein $j \in \{r+1, \ldots, A\}$, so daß $P(T, 1)/P(L_{1j}(T), L_{2j}(T))$ nicht konstant ist. Der gekürzte Bruch hat dann die Gestalt

$$\prod_{i \in I_1} (T - \alpha_i) \Big/ \prod_{i \in I_2} (L_{1j}(T) - \alpha_i L_{2j}(T)) \tag{28}$$

mit $|I_1| = |I_2| \geqslant 1$, so daß $T - \alpha_{i_1}$ teilerfremd $zu (L_{1j}(T) - \alpha_{i_2} L_{2j}(T))$ für $i_1 \in I_1$, $i_2 \in I_2$ ist. Wird in (28) jetzt $T = x_{oh}/y_{oh}$ eingesetzt, so ist dies gleich

$$P(x_{oh}/y_{oh}, 1)/[P(x_{jh}/y_{jh}, 1)(L_{2j}(x_{oh}/y_{oh}))^d].$$

Wegen

$$P(x_{oh}, y_{oh}) = [c_{\mu(0,h)}/c_{\mu(j,h)}] P(x_{jh}, y_{jh})$$

ist diese Zahl bis auf eine Einheit eine d. Potenz. Andererseits war ja $x_{oh}/y_{oh} = Q_{1j}(e)$ mit einer gewissen (von j und h abhängenden) Einheit $e \in R^*$. Wird $Q_{1j}(T) = \tilde{L}_{1j}(T)/\tilde{L}_{2j}(T)$ mit linearen Funktionen $\tilde{L}_{1j}, \tilde{L}_{2j}$ gesetzt, so ist die Gleichung (28) für $T = x_{oh}/y_{oh}$ gleich

$$\prod_{i \in I_1} (\tilde{L}_{1j}(e) - \alpha_i \tilde{L}_{2j}(e)) \Big/ \prod_{i \in I_2} (L_{1j}(\tilde{L}_{1j}(e)/\tilde{L}_{2j}(e))\tilde{L}_{2j}(e) - \alpha_i L_{2j}(\tilde{L}_{1j}(e)/\tilde{L}_{2j}(e))\tilde{L}_{2j}(e)). \tag{29}$$

Damit ist (29) bis auf eine Einheit eine d. Potenz. Indem wir jetzt R lokalisieren, sind *oBdA* $L_{1j}, L_{2j}, \tilde{L}_{1j}, \tilde{L}_{2j} \in R[T]$. Da der Bruch in (28) nicht weiter kürzbar war, sind alle linearen Ausdrücke in (29) als Funktion der *Variabeln* e paarweise teilerfremd. Indem wir R noch einmal nach einer festen Zahl lokalisieren, sind auch alle Faktoren mit der oben betrachteten *Zahl* $e \in R^*$ teilerfremd. Somit sind alle Faktoren von (29) bis auf Einheiten schon d. Potenzen. Also haben wir

mindestens zwei lineare Polynome L_1^*, L_2^* vor uns, so daß stets $L_1^*(e)$ und $L_2^*(e)$ bis auf Einheiten $d.$ Potenzen sind und L_1^*, L_2^* modulo K^* verschieden sind. Bilde jetzt eine endlich erzeugte $\mathbb{Z}$-Algebra $\bar{R} \supset R$, so daß jede Einheit aus R^* in $\bar{R}$ schon eine $d.$ Potenz ist (dies geht nach dem Direchletschen Einheitensatz). Dann sind also $L_1^*(e)$ und $L_2^*(e)$ in $\bar{R}$ jedesmal eine $d.$ Potenz. Nach dem Satz von Siegel kommen jetzt für e nur endlich viele Werte in Frage. Dann kommen nach (25) auch nur endlich viele Werte für x_{oh}/y_{oh} in Frage. Damit haben wir endgültig einen Widerspruch.

Sei jetzt $P(X, Y)$ ein festes homogenes Polynom vom Grad $d \geqslant 4$ und sei G die (endliche) Gruppe

$$\left\{\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix} \in \mathrm{Gl}_2(\mathbb{Q});\ P(X, Y) = P(\alpha X + \beta Y, \gamma X + \delta Y)\right\}.$$

Wir sagen, daß zwei Paare (x, y), $(u, v) \in \mathbb{Q}^2$ "äquivalent" seien, wenn es ein $\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix} \in G$ gibt mit $(u, v) = (\alpha x + \beta y, \gamma x + \delta y)$. Wenn $(x, y) \in \mathbb{Q}^2$ eine Lösung von $P(x, y) = h$ ist, so ist auch jedes dazu äquivalente (u, v) eine Lösung. In dieser Terminologie gilt

SATZ 3. *Sei $P(X, Y) \in \mathbb{Z}[X, Y]$ ein irreduzibeles homogenes Polynom vom* Grad $d \geqslant 4$. *Weiter sei c eine feste natürliche Zahl. Dann hat für fast alle $h \in \mathbb{Z}$ die Gleichung*

$$P(x, y) = h$$

höchstens d^{t-1} viele untereinander nicht äquivalente Lösungen $(x, y) \in \mathbb{Z}^2$ mit $ggT(x, y) = 1$, wobei t die Anzahl der verschiedenen Primfaktoren p_i von h mit $p_i \geqslant c$ bedeutet.

Genauer gilt diese Abschätzung sogar für die Anzahl der untereinander nicht äquivalenten Lösungen $P(x, y) = h$ mit $(xc, yc) \in \mathbb{Z}^2$ und $ggT(xc, yc) \leqslant c^2$.

Beweis. Die Zahl A aus Lemma 2 kann auch als Mächtigkeit der Menge

$$M := \left\{\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix} \in \mathrm{Gl}_2(\mathbb{Q});\ \exists 1 \leqslant \mu \leqslant \nu \text{ mit } c_\mu P(X, Y) = P(\alpha X + \beta Y, \gamma X + \delta Y)\right\}$$

gedeutet werden für gewisse feste paarweise verschiedene rationale Zahlen $c_i \in \mathbb{Q}$ mit $\sqrt[d]{c_i/c_j} \notin \mathbb{Q}$ [dies sieht man, wenn man in Lemma 2 bei den Linearfunktionen $L_{1i}(T)$, $L_{2i}(T)$ mit $L_{1i}(T)/L_{2i}(T) \in \mathbb{Q}(T)$ und mit $P(T, 1) = P(L_{1i}(T), L_{2i}(T))$ einen geeigneten Faktor von der Form $\sqrt[d]{1/c_i}$ mit $c_i \in \mathbb{Q}$ herauszieht, so daß wir die gewünschten Linearfunktionen $\alpha_i T + \beta_i, \gamma_i T + \delta_i$ mit $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{Q}$ bekommen].

Dabei sind die c_i zwar nicht kanonisch durch $P(X, Y)$ bestimmt, aber wir können irgendein solches feste System $c_1, \ldots, c_v$ betrachten. Da die Matrizen $\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}\in \mathrm{Gl}_2(\mathbb{Q})$ mit $P(\alpha X+\beta Y, \gamma X+\delta Y)=c_iP(X, Y)$ bei festem c_i eine Nebenklasse von G bilden, ist also $A=v$ ord G.

Wir zeigen nun die letzte Aussage von Satz 3. Sei $\tilde{c}$ eine so große Fakultät $\tilde{c}=\kappa!$, so daß für alle $(xc, yc)\in\mathbb{Z}^2$ mit $ggT(xc, yc)\leqslant c^2$ und für alle $\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}\in M$ auch

$$((\alpha x+\beta y)\tilde{c}, (\gamma x+\delta y)\tilde{c})\in\mathbb{Z}^2 \quad \text{und} \quad ggT((\alpha x+\beta y)\tilde{c}, (\gamma x+\delta y)\tilde{c})\leqslant \tilde{c}^2$$

ist (dies geht, da M endlich ist). Somit führt jede betrachtete Lösung von $P(x, y)=h$ mit $(xc, yc)\in\mathbb{Z}^2$, $ggT(xc, yc)\in c^2$ zu insgesammt $|M|=v$ ord G vielen verschiedenen Lösungen $(u, v):=(\alpha x+\beta y, \gamma x+\delta y)$ mit $(u\tilde{c}, v\tilde{c})\in\mathbb{Z}^2$, $ggT(u\tilde{c}, v\tilde{c})\leqslant\tilde{c}^2$ und $P(u, v)=c_ih$ für ein $i\leqslant v$. [Dabei sind die so erhaltenen Paare (u, v), die aus einem festen (x, y) konstruiert werden, auch alle *oBdA* verschieden: Weil es nur endlich viele Zahlen u/v mit $u/v=(\alpha u+\beta v)/(\gamma u+\delta v)$ für ein von der Einheitsmatrix verschiedenes $\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}\in G$ gibt, gibt es wegen $(uc, vc)\in\mathbb{Z}^2$ und $ggT(uc, vc)\leqslant c^2$ auch nur endlich viele Ausnahmetupel (u, v) und damit auch nur endlich viele Ausnahmezahlen h].

Wenn es nun mehr als d^{t-1} viele untereinander nicht äquivalente Lösungen (x, y) mit $P(x, y)=h$, $(xc, yc)\in\mathbb{Z}^2$ und $ggT(xc, yc)\leqslant c^2$ gäbe, gäbe es dann auch mehr als Ad^{t-1} viele verschiedene Lösungsquotienten x/y mit $(x\tilde{c}, y\tilde{c})\in\mathbb{Z}^2$, $ggT(x\tilde{c}, y\tilde{c})\leqslant\tilde{c}^2$ und $P(x, y)=c_ih$ für ein $i\leqslant v$. Dies widerspricht Lemma 2 [hierbei wurde natürlich noch benutzt, daß aus $c_{\mu_1}h=P(x_1, y_1)$, $c_{\mu_2}h=P(x_2, y_2)$ und $x_1/y_1=x_2/y_2$ schon "$(x_1, y_1)=\pm(x_2, y_2)$" folgt. Im Fall "d gerade" muß bei der gesammten Argumentation die Matrix $\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}$ mit $\begin{pmatrix}-\alpha & -\gamma\\ -\beta & -\delta\end{pmatrix}$ identifiziert werden.]

FOLGERUNG 4. Seien a, b, $c\in\mathbb{Z}$-$\{0\}$ und $d\geqslant 4$ feste Zahlen. Ist dann die Gleichung

$$ax^d+by^d=cp$$

mit einer genügend großen Primpotenz p durch ganze Zahlen x, y mit $ggT(x, y)=1$ lösbar, so hat sie genau

1 Lösung im Fall d ungerade, a/b keine d. Potenz, (30)

4 Lösungen im Fall d gerade, a/b keine d. Potenz, (31)

8 Lösungen im Fall d gerade, $a = b$. (32)

Beweis. Ist $T^d + \frac{b}{a} = (P_1(T))^d + \frac{b}{a}(P_2(T))^d$ mit linearen Polynomen P_1, P_2, so folgt durch Differenzieren

$$1 = P_1'(0)(P_1(T)/T)^{d-1} + \frac{b}{a} P_2'(0)(P_2(T)/T)^{d-1}.$$

Da es keine nichttrivialen Parametrisierungen der Fermatkurve gibt, folgt $(P_1(T))^d = T^d$ oder $((P_1(T))^d = \frac{b}{a}$. Damit folgt die Behauptung aus Satz 3.

FOLGERUNG 5. Seien a, b, $c \in \mathbb{N}$ mit $a^2 + b^2 = c^2$. Gegeben sei die Homogenisierung einer elliptischen Kurve in der Form

$$X = \mathrm{Var}(ax_1^2 + bx_2^2 - cx_3^2,\ cx_1^2 + bx_4^2 - ax_3^2) \subset \mathbb{C}^4.$$

Ist $x_i \in X \cap \mathbb{Z}^4$ eine Folge mit $x_i \neq x_j$ für $i \neq j$ und mit $ggT(x_{1i}, x_{2i}) = 1$, so hat für großes i die Zahl $x_{1i}^4 + x_{2i}^4$ mindestens zwei verschiedene Primfaktoren p_{1i}, p_{2i} mit $p_{vi} \to \infty$ für $v = 1, 2$ und $i \to \infty$.

Beweis. Angenommen, es gäbe eine Zahl $b \in \mathbb{N}$ und eine Teilfolge der x_i, so daß $x_{1i}^4 + x_{2i}^4$ für alle i dieser Teilfolge höchstens einen Primfaktor $p_i \geqslant b$ hat. Da $(x_1, x_2, x_3, x_4) \in X$ die Identität $x_1^4 + x_2^4 = x_3^4 + x_4^4$ erfüllen, ergibt sich mit Folgerung 4 die Aussage.

Nachdem in Folgerung 5 die Gleichung $x_1^4 + x_2^4 = x_3^4 + x_4^4$ über eine elliptische Kurve parametrisiert worden ist, können wir auch die nach Euler existierenden Parametrisierungen über rationale Kurven betrachten. Eine Überlegung wie in Beweis Satz 3 zeigt jedoch, daß bei einer nichttrivialen Parametrisierung $f_1^4 + f_2^4 = f_3^4 + f_4^4$ mit $f_i(t) \in \mathbb{Z}(t)$ stets das Polynom $f_1^4 + f_2^4$ reduzibel ist, so daß wir damit nur triviale Ergebnisse erhalten.

SATZ 6. *Seien* α, β *algebraische Zahlen mit* $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. *Bezeichne mit* $P(X, Y) \in \mathbb{Z}[X, Y]$ *und* $Q(U, V) \in \mathbb{Z}[U, V]$ *zwei homogene Polynome vom* Grad $d := [\mathbb{Q}(\alpha) : Q]$ *mit* $P(\alpha, 1) = 0 = Q(\beta, 1)$. *Es gebe keine Darstellung*

$$P(T, 1) = Q(L_1(T), L_2(T))$$

mit linearen Polynomen $L_1(T), L_2(T) \in \mathbb{C}[T]$ *und* $L_1(T)/L_2(T) \in \mathbb{Q}(T)$. *Ist dann c eine feste natürliche Zahl, so hat für fast alle ganzen Zahlen h, die höchstens einen Primfaktor (mit beliebiger Vielfachheit) größer als c enthalten, die Gleichung*

$$|P(x, y)| = h = |Q(u, v)|$$

keine Lösung $(x, y)\in\mathbb{Z}^2$, $(u, v)\in\mathbb{Z}^2$ *mit* $ggT(x, y)=1=ggT(u, v)$.

Beweis. Schreibe

$$P(X, Y)=\alpha_0\prod_{w=1}^{d}(X-\alpha_w Y)=\beta_0\prod_{w=1}^{d}(U-\beta_w V)=Q(U, V).$$

Setze $K:=\mathbb{Q}(\alpha_1,\ldots,\alpha_d)=\mathbb{Q}(\beta_1,\ldots,\beta_d)$ und sei $R\subset K$ eine endlich erzeugte $\mathbb{Z}$-Algebra, so daß $c!$, α_0, $\alpha_1,\ldots,\alpha_d$, $\alpha_m-\alpha_n$, β_o, $\beta_1,\ldots,\beta_d$, $\beta_m-\beta_n\in R^*$ für $m\neq n\leqslant d$ ist. Der Beweis verläuft jetzt analog Beweis Satz 2. Setze also $\tilde{c}:=c!$ und schreibe $h\mathbb{Z}_{\tilde{c}}=p^n\mathbb{Z}_{\tilde{c}}$ mit einer von h abhängenden Primzahl p (wobei eventuell $n=0$ ist). Ist dann (x_h, y_h) und (u_h, v_h) eine Lösung von $|P(x_h, y_h)|=h=|Q(u_h, v_h)|$, so folgt wie in (14)

$$(x_h-\alpha_1 y_h)R=(u_h-\tilde{\sigma}(\beta_1)v_h)R \tag{33}$$

für einen gewissen, von h abhängenden Galoisautomorphismus $\tilde{\sigma}\in G:=\mathrm{Gal}(K:\mathbb{Q})$. Setze dann wie in (16) für $2\leqslant w\leqslant d$

$$\begin{aligned} &z_h:=x_h/(x_h-\alpha_1 y_h),\quad \tilde{z}_h:=u_h/(u_h-\tilde{\sigma}(\beta_1)v_h)\\ &b_w:=\bar{\sigma}_w(\alpha_1)/(\bar{\sigma}_w(\alpha_1)-\alpha_1),\ \tilde{b}_w:=\tilde{\sigma}_w(\tilde{\sigma}(\beta_1))/[\bar{\sigma}_w(\tilde{\sigma}(\beta_1))-\tilde{\sigma}(\beta_1)], \end{aligned} \tag{34}$$

wobei $\bar{\sigma}_w\in G$ sein soll mit $\bar{\sigma}_w(\alpha_1)=\alpha_w$ für $2\leqslant w\leqslant d$. Dann folgt wie in (17)

$$\mathscr{D}(z_h-b_w)=\mathscr{D}(\tilde{z}_h-\tilde{b}_w). \tag{35}$$

Hierauf wenden wir jetzt bei laufendem h das Lemma 1 an und schließen wie in Beweis Satz 2 Ziffer (18) ff weiter (wobei jetzt $x_{oh}, y_{oh}, z_{oh}, b_{ow}$ durch x_h, y_h, z_h, b_w und entsprechend $x_{jh}, y_{jh}, z_{jh}, b_{jw}$ durch $u_h, v_h, \tilde{z}_h, \tilde{b}_w$ ersetzt wird). Es folgt dann entsprechend (23) bzw. entsprechend (27) eine Gleichung

$$P(T, 1)=Q(\varepsilon L_1(T), \varepsilon L_2(T)), \tag{36}$$

welche nach Voraussetzung unlösbar ist, oder wir bekommen entsprechend dem nach (28) Gesagten einen Widerspruch.

In der Regel wird die Gleichung $P(T, 1)=Q(L_1(T), Q_2(T))$ nicht mit linearen Polynomen L_1, L_2 lösbar sein: Denn wir haben ja 4 Variabeln (nämlich die Koeffizienten von L_1 und L_2) und $d+1$ viele Gleichungen für diese 4 Variabeln (da ja $P(T, 1)$ vom Grad d ist). Ein konkretes Beispiel für diesen Sachverhalt liefert

FOLGERUNG 7. Seien $a\neq b$ und c feste natürliche Zahlen. Dann hat für fast alle Primpotenzen p die Gleichung

$$x^4+y^4=cp=u^4+4(b^2-a^2)u^2v^2+(a^2+b^2)^2v^4$$

keine Lösung $(x, y, u, v) \in \mathbb{Z}^4$ mit $ggT(x, y) = 1 = ggT(u, v)$.

Beweis. Setze $P(X, Y) = X^4 + 4(b^2 - a^2)X^2Y^2 + 4(a^2 + b^2)^2Y^4$ und $Q(U, V) = U^4 + V^4$. Offensichtlich ist für $\alpha := \sqrt{2}a + i\sqrt{2}b$ und $\beta := (\sqrt{2} + i\sqrt{2})/2$ schon $P(\alpha, 1) = 0 = Q(\beta, 1)$. Wäre $P(T, 1) = Q(L_1(T), L_2(T))$ bei $L_1(T) = \bar{\alpha}_1 T + \bar{\beta}_1$, $L_2(T) = \bar{\alpha}_2 T + \bar{\beta}_2$, so folgten die Gleichungen

$$\bar{\alpha}_1^4 + \bar{\alpha}_2^4 = 1,\ \bar{\alpha}_1^3\bar{\beta}_1 + \bar{\alpha}_2^3\bar{\beta}_2 = 0,\ \bar{\alpha}_1^2\bar{\beta}_1^2 + \bar{\alpha}_2^2\bar{\beta}_2^2 = \tfrac{2}{3}(b^2 - a^2),$$
$$\bar{\alpha}_1\bar{\beta}_1^3 + \bar{\alpha}_2\bar{\beta}_2^3 = 0,\ \bar{\beta}_1^4 + \bar{\beta}_2^4 = 4(a^2 + b^2)^2. \tag{37}$$

Zunächst muß $\bar{\alpha}_1\bar{\beta}_1\bar{\alpha}_2\bar{\beta}_2 \neq 0$ sein. Es folgt, wenn die 3. Potenz der 2. Gleichung durch die 4. Gleichung dividiert wird, daß $\bar{\alpha}_1^8 = \bar{\alpha}_2^8$ ist. Wegen der 1. Gleichung von (37) ist dann $\bar{\alpha}_1 = \gamma_1\bar{\alpha}_2 = \gamma_2\sqrt[4]{1/2}$ mit $\gamma_1^4 = \gamma_2^4 = 1$. Aus der 2 und 5. Gleichung folgt damit $\bar{\beta}_1 = -\bar{\beta}_2\gamma_1 = \gamma_3\sqrt[4]{2}\sqrt{a^2 + b^2}$. Dann würde aus der 3. Gleichung schon $(a^2 + b^2)E = \frac{2}{3}(b^2 - a^2)$ folgen, wobei $E \in \{-2, 0, 2\}$ ist. Dies ist wegen $a, b \in \mathbb{N}$ unmöglich.

References

1. Bombieri, E.: Schmidt, W. M.: On Thue's equation. *Invent. Math.* 88 (1987), 69–81.
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 (1984), 225–244.
4. Langmann, K.: Lösungsanzahl der Thue-Gleichung. Eingereicht bei *Compos. Math.*
5. Stewart, C. L.: On the number of solutions of polynomial congruences and Thue equations. Erscheint in Journal of the AMS.