BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

SITZUNGSBERICHTE

JAHRGANG
1975

MÜNCHEN 1976

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN
In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung München

Eine diophantische Aufgabe des Leonardo von Pisa

Von **Hermann Schmidt** in Würzburg

Vorgelegt am 7. Februar 1975

Noch in jüngster Zeit wurde mehrfach hervorgehoben (Hofmann [4] S. 95/96, King [5] S. 18, Cassels [2] S. 207–208), daß Leonardo von Pisa bereits im 13. Jahrhundert Systeme quadratischer Gleichungen in rationalen Unbekannten folgender Gestalt betrachtet hat ([7] S. 253, 271)

$$z^2 = x^2 + c = y^2 - c, \quad c \in N, x, y, z \in Q. \tag{1}$$

Er gibt in der Tat in seinem Liber quadratorum a. a. O. für $c = 5$ die Lösung 12 $(x, y, z) = (31, 49, 41)$ an. Daß (1) für $c = 1$ unlösbar ist, war schon Fermat bekannt; einen unmittelbar an das System (1) anknüpfenden Beweis gibt z. B. Cassels a. a. O. Eine Übersicht über alle Lösbarkeitsfälle hat man aber auch heute nicht, und die weitergehende Frage nach der Gesamtheit aller Lösungen ist anscheinend nur im Fibonaccischen Falle $c = 5$ behandelt worden. Wir zeigen hier durch Zurückführung auf eine kubische Gleichung in zwei rationalen Unbekannten, daß im Lösbarkeitsfalle stets unendlich viele verschiedene Lösungen vorhanden sind; für $c = 5$ ist eine weitere zahlenmäßig angegeben (10)[1]. Ferner gewinnen wir unter Benutzung neuerer Ergebnisse über rationale Punkte auf kubischen Kurven (vgl. besonders Lind [9]) hinreichende Bedingungen für Unlösbarkeit.

Wir gehen aus von dem mit (1) gleichwertigen System

$$x^2 + y^2 - 2z^2 = 0 \tag{2a}$$

$$x^2 - y^2 + 2c = 0. \tag{2b}$$

Es handelt sich demnach, wenn x, y, z als rechtwinkelige Koordinaten angesehen werden, um die Ermittlung der rationalen

[1] Schon bekannt, vgl. Mordell [15] S. 71/72, wo auch Hinweis auf Uspensky-Heaslet [16].

Punkte auf einer Raumkurve 4. Ordnung, die durch (1) als Schnitt zweier (bzw. dreier) hyperbolischer Zylinder, durch (2)a b als Schnitt eines solchen mit einem Drehkegel gegeben ist. Da die Unbekannten nicht notwendig ganzzahlig zu sein brauchen, ist es keine Einschränkung, von vornherein

$$(2)\,\mathrm{c} \qquad c \text{ quadratfrei}$$

anzunehmen.

Für die Gesamtheit der Lösungen von (2)a findet man unter Benützung der Lösung (1, 1, 1) nach dem bekannten Verfahren der stereographischen Projektion (vgl. z. B. Dickson [3] 44, 47 oder Nagell [11] 216) die Darstellung

$$(3) \quad \begin{cases} x = \varrho(u^2 + 2uv - v^2) \;\;\;= \varrho(2u^2 - (u-v)^2) \\ y = \varrho(-u^2 + 2uv + v^2) = \varrho(2v^2 - (u-v)^2) \\ z = \varrho(u^2 + v^2), \end{cases}$$

worin $u, v \in \boldsymbol{Z}$, $(u, v) = 1$, $\varrho \in Q$.

Hieraus oder unmittelbar durch Betrachtungen im Gaussschen Zahlenkörper ergibt sich die komplexe Form

$$(3)' \qquad Z := x + iy = \varrho(1-i)(u+iv)^2$$
$$z = \varrho(u+iv)(u-iv), \text{ woraus noch folgt (bei } Z \neq 0)$$

$$(3)'' \qquad Z = (1-i)\, z\, \frac{u+iv}{u-iv}.$$

Einsetzen in (2)b, etwa unter Benutzung von

$x^2 - y^2 = \varrho^2\, \Re\,(-2i\,(u+iv)^4) = 8\,\varrho^2\, uv\,(u^2 - v^2)$ gibt

(4) $4\varrho^2 uv\,(u^2 - v^2) + c = 0$; für die in Frage kommenden Parameterwerte ist also $\varrho \neq 0$ und

$$(4)' \qquad uv\,(v^2 - u^2) > 0,$$

und mit

$$(4)'' \qquad w := \frac{1}{2\varrho}$$

erhält man schließlich die Bedingung

(5) $c w^2 = uv\,(v^2 - u^2)$, $(u, v) = 1$. Hier ist wegen (2)c jetzt auch $w \in \boldsymbol{Z}$.

Man hat damit

Satz 1. *Genau dann ist die Aufgabe* (1) *bei der Annahme* (2) c *lösbar, wenn die ganze Zahl c quadratfreier Kern einer durch die biquadratische Form $uv\,(v^2 - u^2)$ ganzzahlig dargestellten, natürlichen Zahl ist.*

Demnach können zu einem beliebigen Paare (u, v), das die Bedingung (4)′ erfüllt, die zugehörigen Werte c und $\pm w$, damit alle Lösungen berechnet werden; dabei genügt es – etwa für die Herstellung einer Tafel –[2], da es nur auf die Beträge $|x|$, $|y|$ ankommt, $0 < u < v$ anzunehmen. Denn falls $uv < 0$, kommt man durch eine Drehung $W^* = \pm iW$ der $W (= u + iv)$-Ebene, bei der $Z^* = -Z$ wird, auf einen schon berücksichtigten Fall zurück.

Hiermit ist natürlich die Frage nach der Lösbarkeit von bei vorgegebenem c nicht erledigt. Setzt man nun noch

(6) $v = \xi u$, $w = \eta u^2$, so sieht man, daß alles auf die Lösbarkeit in rationalen Zahlen mit $\eta \neq 0$ von

(7) $c\eta^2 = \xi(\xi^2 - 1)$ oder auch (vermöge (6′) $c\xi = \xi'$, $c^2\eta = \eta'$) von

(7)′ $\eta'^2 = \xi'(\xi'^2 - c^2)$ in rationalen Zahlen mit $\eta' \neq 0$ hinauskommt.

Zwischen den (etwa vorhandenen) gesuchten Punkten der Kurve (1) und den entsprechenden von (7) bzw. (7)′ besteht die Kette eineindeutiger Abbildungen

$$(8) \qquad (x, y, z) \leftrightarrow (\pm W, w) \leftrightarrow (\xi, \eta) \leftrightarrow (\xi', \eta')$$

(vermittelt durch (3)′ (3)″ (4)″ (6) (6)′).

Die schon eingangs erwähnte klassische Unlösbarkeit für $\underline{c = 1}$ folgt jetzt aus der Unlösbarkeit von (5). Wegen $(u, v) = 1$ müßten jetzt u und v Quadrate sein, und $\omega^2 = \tau^4 - \sigma^4$ ist in N ja bekanntlich unlösbar (vgl. z.B. Nagell [11], S. 227, Th. 114).

Für das weitere ziehen wir das altbekannte Tangentenverfahren heran: der dritte Schnittpunkt der Tangente in einem Punkte $(\xi_0, \eta_0 \neq 0)$ von (7) mit der Kurve hat die Abszisse

[2] Vgl. hierfür und für umfassende geschichtliche Angaben Dickson [14] 459 ff.

(9) $\xi_1 = \frac{(\xi_0^2+1)^2}{4\xi_0(\xi_0^2-1)}$ (vgl. z.B. Lind [9] S. 19, Satz 2),

und man hat weiter vermöge (6) (3) (4) (5) (1)

$$\xi_1 = \frac{z_0^2}{c}, \quad \eta_1 = \frac{x_0 y_0 z_0}{c^2}.$$

So erhält man z.B. im Fibonaccischen Falle

$$c = 5, (u_0, v_0, w_0) = (4, 5, 6)$$

die weitere Lösung [1])

(10) $1\,494\,696\,(x_1, y_1, z_1) = (113\,279, 4\,728\,001, 3\,344\,161)$, und

im Falle $c = 6$ zu der Lösung $2\,(x_0, y_0, z_0) = (1, 7, 5)$ noch

$$140\,(x_1, y_1, z_1) = (1\,151, 1\,249, 1\,201) \text{ vgl.}^2, 468 \text{ u.}).$$

Nunmehr beweisen wir

Satz 2. *Besitzt* (1) *eine Lösung, so auch unendlich viele verschiedene, und zwar entsteht eine Folge von solchen durch fortgesetzte Anwendung des Tangentenverfahrens bei der Kurve* (7).

Daß es genügt, (7) zu betrachten (bei $\eta \neq 0$) folgt aus (8); wir verwenden weiterhin eine schon bei Schmidt [12] S. 11, Hilfssatz 3 in einem etwas schwierigeren Fall benützte Methode.

Hilfssatz. *Die Iterierten der rationalen Funktion* $\varphi(\xi) = \frac{(\xi^2+1)^2}{4\xi(\xi^2-1)}$ (*vgl.* (9)) *sind für* $\xi \in Q, \xi(\xi^2-1) > 0$ *sämtlich vorhanden und voneinander verschieden.*

Zum Beweis ist zunächst zu bemerken, daß für $\xi\,(\xi^2-1) > 0$ stets $\varphi\,(\xi) > 1$ ausfällt, abgesehen von den irrationalen Stellen $\xi = 1 \pm \sqrt{2}$ (Berührabszissen der nicht vertikalen Tangenten vom Punkte (1, 0) an die Kurve). Das folgt sofort aus

$(\xi^2+1)^2 - 4\,\xi\,(\xi^2-1) = (\xi^2-2\,\xi-1)^2 > 0$. Die Folge der Nachfolger eines solchen Wertes ξ_0, nämlich $\xi_{\nu+1} = \varphi\,(\xi_\nu)$, $\nu = 0, 1, \ldots$ bricht also nicht ab, und zwar ist $\xi_\nu > 1$ für $\nu \geq 1$. Nunmehr sei $\xi = \frac{a}{b}$, $a > b$, $(a, b) = 1$. Dann ist mit

$G := a^2 + b^2, F := ab\,(a^2 - b^2)$

$\varphi(\xi) = \frac{G^2}{4F} =: \frac{g}{h}, (g, h) = 1$, also $g = \frac{G^2}{D}$, $h = \frac{4F}{D}$, wenn

$D := (G^2, 4F)$. Nun ist zunächst $(ab, a^2 + b^2) = 1$ wegen $(a, b) = 1$,

ferner

$$(a^2 - b^2, (a^2 + b^2)^2) = (a^2 - b^2, (a^2 - b^2)^2 + 4b^2(a^2 - b^2) + 4b^4) = \\ = (a^2 - b^2, 4b^4)$$

ein Teiler von 4, also D eine Potenz von 2. Ist nun $a^2 + b^2$ gerade, so $a \equiv b \equiv 1\ (2)$, $a^2 + b^2 \equiv 2\ (4)$, $G^2 \equiv 4\ (8)$, also $D \leq 4$. Ferner ist $F \geq 2.3 = 6$. Somit wird schließlich

$$(11) \qquad g^2 + h^2 \geq \frac{G^4}{4^2} + \frac{4^2 6^2}{4^2} > G^2 > G = a^2 + b^2$$

da das Polynom

$$T^2 - 16\,T + 16.36 = (T - 8)^2 + 16.32$$

positiv definit ist. Durch wiederholte Anwendung von (11) folgt daher nun die Behauptung, daraus dann sofort Satz 2.

Ein anderer Beweis desselben wird bei Laub [6], 39 (42) ff. angegeben, wobei allerdings sehr ins einzelne gehende Ergebnisse von B. Levi [8] über den Aufbau des Moduls der rationalen Punkte auf einer Kurve 3. Ordnung als bekannt vorausgesetzt werden.

Besonders reich an Beispielen für c-Werte der in Satz 2 geforderten Art ist die Arbeit Wiman [13], wo im übrigen tiefgehende Untersuchungen über den Rang des soeben erwähnten Moduls für Kurven der Gleichungsform (7)′ durchgeführt sind.

Auf der anderen Seite gilt

Satz 3. *Unlösbar ist* (1), *wenn* (7) *nur exzeptionelle rationale Punkte besitzt.*

Dabei heißt ein Punkt einer Kurve 3. Ordnung nach Nagell exzeptionell, wenn das Tangentenverfahren periodisch wird oder abbricht, so daß, wenn es ein rationaler Punkt ist, höchstens endlich viele weitere solche geliefert werden.

Der Beweis folgt sofort daraus, daß es jetzt auf (7) überhaupt keinen rationalen Punkt mit $\eta \neq 0$ geben kann, da ein solcher nach Satz 2 ja zu unendlich vielen solchen führen würde, also ein „ordinärer" (d.h. nicht exzeptioneller) Punkt wäre. Damit werden nun die Ergebnisse von Nagell und Lind [9], 10, 76ff. über exzeptionelle Kurven (7)′ anwendbar, und diese ergeben z.B. die Unlösbarkeit von (7) für folgende Fälle (p, q voneinander verschiedene Primzahlen):

$$c = p \equiv 3\ (8);\ c = pq,\ p \equiv q \equiv 3\ (8)$$

$$c = 2p,\ p \equiv -3, 5, -7\ (16);\ c = 2pq,\ p \equiv q \equiv \pm 3\ (8).$$

Der bei Beha-eddin [1] Schluß, S. 55,2. (vgl. auch Moritz [10] 284) als Aufgabe angeführte Fall $c = 10$ ist damit insbesondere als unmöglich erledigt, wie es der Herausgeber Nesselmann [1] 72, 35) schon ohne Beweis behauptet. – Für die Vermittlung des Buches [1] in Aufklärung einer irreführenden Angabe bei Moritz a. a. O. habe ich den Herren Hermelink und H. Gericke in München zu danken.

Nicht enthalten ist hier der Fall $\underline{c = 2}$, wo die Unlösbarkeit aber bekannt ist.[3]

Schriftenverzeichnis

[1] Beha-eddin Mohammed ben Alhossain, Essenz der Rechenkunst, arabisch und deutsch herausgegeben von G. H. F. Nesselmann, Berlin 1843.

[2] Cassels J. W. S., Diophantine Equations with special reference to elliptic curves, J. London Math. Soc. 41 (1966) 193–291.

[3] Dickson L. E., Introduction to the theory of numbers. Chicago 1946.

[4] Hofmann J. E., Geschichte der Mathematik I, Sammlung Göschen 226/226a. De Gruyter 1963.

[5] King, Ch., Leonardo Fibonacci. The Fibonacci Quarterly 1 (1963) Nr. 4, 15–19.

[6] Laub H., Rationale Punkte auf den kubischen Kurven $y^2 = x(x+a)(x+b)$. Prüfungsarbeit Würzburg 1966 (maschinenschriftlich).

[7] Leonardo Pisano, Liber quadratorum 1225. Scritti, Publ. da B. Boncampagni Roma 1857, II, 253–283.

[8] Levi B., Saggio per una teoria aritmetica delle forme cubiche ternarie. Atti R. Accad. Scienze Torino 41 (1906), 43 (1908).

[3] Vgl. Dickson [14] 465 oben (Barlow), auch 468/9 (Lucas).

[9] Lind C.-E., Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlechte eins.
Inaugural-Dissertation Uppsala 1940.

[10] Moritz R. E., On Mathematics and Mathematicians. New York, Dover 1958.

[11] Nagell T., Introduction to Number Theory. Stockholm-New York 1951.

[12] Schmidt Hermann, Über einige diophantische Aufgaben 3. und 4. Grades. Jahresbericht der Deutschen Math., Ver. 67 (1964) 2–13, mit Nachtrag ebenda 70 (1967) 51/52.

[13] Wiman A., Über rationale Punkte auf Kurven $y^2 = x(x^2 - c^2)$. Acta Math. Uppsala 77 (1945) 281–320.

[14] Dickson L. E., History of the Theory of Numbers II. Diophantine Analysis. Chelsea Publ. Comp. New York 1952, Ch. XVI.

[15] Mordell L. J., Diophantine Equations. Academic Press 1969.

[16] Uspensky J. V. und Heaslet M. A., Elementary Number Theory. Mac Graw Hill London 1939 (Verf. nicht zugänglich gewesen).