Über einige spezielle diophantische Gleichungen.

Von

A. Brauer in Berlin.

Seit Fermat ist die diophantische Gleichung $x^3 + a = y^2$ in einer großen Anzahl von Arbeiten[1]) behandelt worden. Bisher kennt man die Lösungen nur für eine Reihe spezieller Werte von a; insbesondere ist der Fall $a = 2$ nicht erledigt. Die Frage, ob die Gleichung $x^3 + 2 = y^2$ außer den trivialen Lösungen $x = -1$, $y = \pm 1$ noch weitere hat, ist mehrfach[2]) aufgeworfen worden. Daß die Lösung, die E. Fauquembergue[3]) und E. Liminon[4]) gegeben haben, nicht ausreichend ist, hat L. Aubry[5]) gezeigt. Herr E. Landau[6]) hat bewiesen, daß die Lösung der Gleichung $x^3 + 2 = y^2$ gleichbedeutend mit der Lösung der Gleichung

$$\alpha^3 + 3\alpha^2\beta + 6\alpha\beta^2 + 2\beta^3 = 1$$

ist. Ob diese letztere Gleichung nur die Lösung $\alpha = 1$, $\beta = 0$ hat, haben H. Brocard[7]) und Herr E. Landau[8]) als Frage gestellt; diese ist bisher nicht beantwortet worden. A. Boutin[9]), P. Tannery[10]) und

---

[1]) Ausführliche Literaturangaben findet man in L. E. Dickson, History of the theory of numbers 2 (Washington 1920), S. 533–539.

[2]) E. Gerono, Question 599, Nouvelle Correspondance Mathématique 6 (1880), S. 526. — Stenacensis, Question 3359, L'Intermédiaire des Mathématiciens 15 (1908), S. 73. — L. Aubry, Réponse 5085, ibid. (2) 2 (1923), S. 107. — I. L. Riley, The Amerioan Mathematical Monthly 24 (1917), S. 177.

[3]) Mathesis (2) 6 (1896), S. 191.

[4]) L'Intermédiaire des Mathématiciens 15 (1908), S. 191.

[5]) Sur l'équation $x^3 + 2 = y^2$, ibid. 18 (1911), S. 204.

[6]) Sur une démonstration d'Euler d'un théorème de Fermat, ibid. 8 (1901), S. 145–147.

[7]) Question 2241, ibid. 8 (1901), S. 309.

[8]) Question 2915, ibid. 12 (1905), S. 106.

[9]) Ibid. 9 (1902), S. 111.

[10]) Ibid. 9 (1902), S. 283–284.

A. Werebrusow[11]) haben rationale, aber nicht ganzzahlige Lösungen dieser Gleichung angegeben[12]). Herr E. Landau[13]) hat auf Grund eines Satzes von Thue[14]) gezeigt, daß diese Gleichung und daher auch $x^3+2=y^2$ nur endlich viele ganzzahlige Lösungen haben kann. Es soll im folgenden ohne Benutzung des Thueschen Satzes gezeigt werden, daß diese Gleichungen nur die Lösungen $x=-1$, $y=\pm 1$ bzw. $\alpha=1$, $\beta=0$ haben. Es erscheint dies als Spezialfall eines etwas allgemeineren Satzes.

Der Beweis dieses Satzes wird auf Grund der folgenden leichten Verallgemeinerung mehrerer Sätze von Pépin[15]) geführt.

Satz 1. *Ist* $rs \not\equiv -1 \pmod 4$ *und quadratfrei* $(r>0,\ s>0)$, $2m+1\geqq 3$ *und teilerfremd zur Anzahl der Idealklassen des quadratischen Körpers* $\mathsf{P}(\sqrt{-rs})$, *so erhält man alle ganzzahligen teilerfremden Lösungen von*

$$r\xi^2+s\eta^2=\zeta^{2m+1}$$

aus den Gleichungen

$$\xi\sqrt{r}+\eta\sqrt{-s}=(\varkappa\sqrt{r}+\lambda\sqrt{-s})^{2m+1}$$

$$\zeta=r\varkappa^2+s\lambda^2,$$

wo $\varkappa, \lambda$ *teilerfremde, ganze rationale Zahlen sind*[16]).

Während Pépin seine Resultate mittels der Komposition der quadratischen Formen beweist, soll hier der Beweis idealtheoretisch erbracht werden: ξ, η, ζ müssen zu je zweien teilerfremd sein, da rs quadratfrei ist. Ebenso muß r zu ζ teilerfremd sein. Aus $r\xi^2+s\eta^2=\zeta^{2m+1}$ folgt nun

$$(r^{m+1}\xi+r^m\eta\sqrt{-rs})(r^{m+1}\xi-r^m\eta\sqrt{-rs})=r^{2m+1}\zeta^{2m+1}.$$

Man setze

$$\zeta=2^\tau\zeta' \qquad (\tau\geqq 0,\ \zeta' \text{ ungerade}).$$

---

[11]) L'Intermédiaire des Mathématiciens **9** (1902), S. 284.

[12]) Siehe auch A. Werebrusow, Équation $x^3+3x^2y+6xy^2+2y^3=1$, ibid. **13** (1906), S. 196–197.

[13]) Ibid. **20** (1913), S. 154.

[14]) Über Annäherungswerte algebraischer Zahlen. Journal für die reine und angewandte Mathematik **135** (1909), S. 284–305.

[15]) Sur certains nombres complexes de la forme $a+b\sqrt{-c}$, Journal de Mathématiques pures et appliquées (3) **1** (1875), S. 332–335, 339–343. — Sur l'équation indéterminé $X^2+cY^2=Z^3$, Memorie della Pontificia Academia dei Nuovi Lincei **8** (1892), S. 42.

[16]) Ein ähnlicher Satz läßt sich auch für $rs\equiv -1 \pmod 4$ und ungerades ζ beweisen.

Da 2 und r in der Diskriminante des Körpers $\mathsf{P}(\sqrt{-rs})$ aufgehen, ist die Primidealzerlegung von $2^{\tau}r$ von der Form

$$2^{\tau} r \cdot \mathfrak{o} = \mathfrak{q}_1^2 \mathfrak{q}_2^2 \dots \mathfrak{q}_\varrho^2.$$

Nun sind $r^m(r\xi + \eta\sqrt{-rs})\cdot\mathfrak{o}$ und $r^m(r\xi - \eta\sqrt{-rs})\cdot\mathfrak{o}$ konjugierte Ideale des Normalkörpers $\mathsf{P}(\sqrt{-rs})$. Geht daher in dem ersten dieser Ideale ein Ideal $\mathfrak{k}$ auf, so geht in dem zweiten Ideal das zu $\mathfrak{k}$ konjugierte Ideal $\mathfrak{k}'$ auf. Hieraus folgt, da $\mathfrak{q}_\nu = \mathfrak{q}_\nu'$ ist, daß das Ideal $(\mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_\varrho)^{2m+1}$ gleichzeitig in $r^m(r\xi + \eta\sqrt{-rs})\cdot\mathfrak{o}$ und in $r^m(r\xi - \eta\sqrt{-rs})\cdot\mathfrak{o}$ aufgehen muß. Soll ferner in diesen beiden konjugierten Idealen gleichzeitig ein Primideal $\mathfrak{p}$ von ζ' aufgehen, so muß es in $2r^{m+1}\xi$ aufgehen; dies ist unmöglich, da ζ' zu $2r^{m+1}\xi$ teilerfremd ist. Daher sind die Hauptideale

$$r^m(r\xi + \eta\sqrt{-rs})\cdot\mathfrak{o} = (\mathfrak{v}\cdot\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_\varrho)^{2m+1}$$

$$r^m(r\xi - \eta\sqrt{-rs})\cdot\mathfrak{o} = (\mathfrak{w}\cdot\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_\varrho)^{2m+1},$$

wo $\mathfrak{v}\cdot\mathfrak{w} = \zeta'\mathfrak{o}$ und $(\mathfrak{v}, \mathfrak{w}) = \mathfrak{o}$ ist. Gehört nun $\mathfrak{v}\cdot\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_\varrho$ zur Idealklasse A, so muß A^{2m+1} die Hauptklasse sein. Da $2m+1$ zur Klassenanzahl teilerfremd war, muß A selbst die Hauptklasse sein. Also ist $\mathfrak{v}\cdot\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_\varrho$ ein Hauptideal, folglich

$$r^m(r\xi + \eta\sqrt{-rs})\cdot\mathfrak{o} = [(\mu_1 + \lambda_1\sqrt{-rs})\cdot\mathfrak{o}]^{2m+1}.$$

Nun enthält der Körper $\mathsf{P}(\sqrt{-rs})$ nur die Einheiten ± 1, für $rs = 1$ außerdem noch $\pm i$, die sich sämtlich als $(2m+1)$-te Potenzen von ganzen Zahlen des Körpers darstellen lassen; daher ist

$$r^m(r\xi + \eta\sqrt{-rs}) = (\mu + \lambda\sqrt{-rs})^{2m+1} \quad (\mu, \lambda \text{ ganz und rational}).$$

Hieraus folgt, daß μ^{2m+1} durch r teilbar ist. Da r quadratfrei ist, muß $\mu = r\varkappa$ mit ganzem rationalen $\varkappa$ sein. Folglich ist

$$\xi\sqrt{r} + \eta\sqrt{-s} = (\varkappa\sqrt{r} + \lambda\sqrt{-s})^{2m+1}.$$

Man erhält also jedenfalls alle teilerfremden Lösungen ξ, η aus dieser Gleichung.

Satz 2. *Ist $a = 2b^3 > 0$, $6b$ quadratfrei und die Anzahl der Idealklassen des Körpers $\mathsf{P}(\sqrt{-6b})$ zu 3 teilerfremd, so lassen sich alle ganzzahligen Lösungen x, y der Gleichung $x^3 + a = y^2$ angeben*[17]).

[17]) Daß diese Gleichung jedenfalls nur endlich viele Lösungen haben kann, hat Mordell bewiesen („A statement by Fermat", Proceedings of the London Mathematical Society (2) 18 (1920), S. V–VI).

a) Es sollen zunächst die Lösungen mit teilerfremden x, y bestimmt werden. Setzt man $x = u - b$, so geht die Gleichung

$$x^3 + 2b^3 = y^2 \tag{1}$$

über in

$$(u+b)^3 = y^2 + 6bu^2. \tag{2}$$

Hierin sind y und u teilerfremd, da ein gemeinsamer Primteiler in b und daher auch in x aufgehen würde, so daß x und y nicht teilerfremd wären. Alle teilerfremden Lösungen von (2) erhält man aber, da die Voraussetzungen des Satzes 1 erfüllt sind, aus der Gleichung

$$y + u\sqrt{-6b} = (p + q\sqrt{-6b})^3,$$

wo p, q teilerfremde, ganze rationale Zahlen sind. Hieraus folgt

$$y = p^3 - 18bpq^2$$
$$u = 3p^2q - 6bq^3.$$

Andererseits ist

$$(u+b)^3 = y^2 + 6bu^2 = (p^2 + 6bq^2)^3,$$

folglich, da nur reelle Lösungen in Betracht kommen,

$$u + b = p^2 + 6bq^2.$$

Daher ist

$$p^2 + 6bq^2 = 3p^2q - 6bq^3 + b$$

$$p^2(3q-1) = b(6q^3 + 6q^2 - 1). \tag{3}$$

Ein gemeinsamer Teiler von $6q^3 + 6q^2 - 1$ und $3q - 1$ müßte in

$$9(6q^3 + 6q^2 - 1) - (18q^2 + 24q + 8)(3q - 1) = -1$$

aufgehen. Also sind für alle Werte von q die Zahlen $3q - 1$ und $6q^3 + 6q^2 - 1$ teilerfremd, folglich $3q - 1$ ein Teiler von b. Wegen der Teilerfremdheit von y und u muß p zu b teilerfremd sein; also ist

$$3q - 1 = \pm b, \qquad \pm p^2 = 6q^3 + 6q^2 - 1.$$

Da -1 quadratischer Nichtrest (mod 6) ist, ist

$$-p^2 = 6q^3 + 6q^2 - 1, \qquad 3q - 1 = -b.$$

Man erhält also höchstens einen Wert für q, und daher aus

$$y = p^3 - 18bpq^2$$
$$x = 3p^2q - 6bq^3 - b$$

höchstens zwei teilerfremde Lösungspaare x, y.

b) Es müssen nun noch die nicht teilerfremden Lösungen von (1) bestimmt werden. Da $6b$ quadratfrei ist, geht der größte gemeinsame Teiler von x und y in b und daher in u und umgekehrt der von u und y in b und daher in x auf; also haben x und y denselben größten gemeinsamen Teiler wie u und y. Es genügt daher, die nicht teilerfremden Lösungen von (2) zu bestimmen. Es sei $(u, y) = t$; dann ist also t ein Teiler von b, folglich wegen (2) auch t^2 ein Teiler von y. Man setze

$$y = t^2 y_1, \qquad u = t u_1, \qquad b = t b_1.$$

Die Gleichung (2) geht dann über in

$$(u_1 + b_1)^3 = t y_1^2 + 6 b_1 u_1^2. \tag{4}$$

Nun ist $(u_1 + b_1, y_1) = 1$, da ein gemeinsamer Primteiler in b_1 oder in u_1, also in beiden, aufgehen müßte; dies ist unmöglich, da u_1 und y_1 teilerfremd waren. Wegen $6b = 6tb_1$ sind die Voraussetzungen des Satzes 1 erfüllt. Man erhält daher die teilerfremden Lösungen von (4) aus

$$y_1 \sqrt{t} + u_1 \sqrt{-6b_1} = (p_1 \sqrt{t} + q_1 \sqrt{-6b_1})^3;$$

also ist

$$y_1 = t p_1^3 - 18 b_1 p_1 q_1^2,$$
$$u_1 = 3 t p_1^2 q_1 - 6 b_1 q_1^3.$$

Andererseits ist

$$u_1 + b_1 = t p_1^2 + 6 b_1 q_1^2 = 3 t p_1^2 q_1 - 6 b_1 q_1^3 + b_1.$$

Hieraus folgt

$$p_1^2 t (3q_1 - 1) = b_1 (6 q_1^3 + 6 q_1^2 - 1).$$

Diese Gleichung entspricht völlig der Gleichung (3); man kann daher alle für $q_1, p_1, t, u_1, y_1, u, y$ und x überhaupt in Betracht kommenden Werte angeben. Damit ist Satz 2 bewiesen.

Die Voraussetzungen des Satzes sind z. B.[18]) für $b = 1, 5, 7, 11, 13, 17, 19, 23, 35, 43, 47, 55 \ldots$ erfüllt.

Folgerung 1. *$x^3 + 2 = y^2$ hat nur die Lösungen $x = -1$, $y = \pm 1$.*

Es ist nämlich $b = 1$, $q = 0$, $p = \pm 1$, $q_1 = 0$, $t = 1$, $y = \pm 1$, $x = -1$.

Folgerung 2. *Die Gleichung $\alpha^3 + 3\alpha^2\beta + 6\alpha\beta^2 + 2\beta^3 = 1$ hat nur die Lösung $\alpha = 1$, $\beta = 0$.*

---

[18]) Siehe die Tafel der Klassen binärer quadratischer Formen in Gauß' Werken 2 (Göttingen 1863), S. 450–474.

Denn auf Grund der Arbeit von Herrn E. Landau[19]) würde jede andere Lösung α_0, β_0 für $x^3 + 2 = y^2$ die Lösung

$$y = \alpha_0^3 + 6\alpha_0^2\beta_0 + 6\alpha_0\beta_0^2 + 4\beta_0^3,$$
$$x = -(\alpha_0^2 - 2\beta_0^2)$$

ergeben. Daher muß sein

$$\alpha_0^3 + 6\alpha_0^2\beta_0 + 6\alpha_0\beta_0^2 + 4\beta_0^3 = y = \pm 1$$
$$\alpha_0^3 + 3\alpha_0^2\beta_0 + 6\alpha_0\beta_0^2 + 2\beta_0^3 \quad = \quad 1.$$

Also ist entweder

$$3\alpha_0^2\beta_0 + 2\beta_0^3 = 0, \text{ d. h. } \beta_0 = 0, \ \alpha_0 = 1,$$

oder es ist

$$3\alpha_0^2\beta_0 + 2\beta_0^3 = -2, \qquad -x = \alpha_0^2 - 2\beta_0^2 = 1,$$

also

$$8\beta_0^3 + 3\beta_0 + 2 = 0.$$

Diese Gleichung hat aber keine ganze rationale Lösung.

Die gegebene Beweismethode läßt sich auch für eine Reihe weiterer spezieller diophantischer Gleichungen anwenden.

---

[19]) A. a. O. [6]).

(Eingegangen am 31. Juli 1925.)