Über eine Verallgemeinerung eines Satzes von Fermat.

Von
ERNST TROST (Zürich).

(Als Manuskript eingegangen am 13. Februar 1940.)

Von FERMAT [1]) stammt der Satz, dass es mit Ausnahme von 1 und 7 keine ganzen Zahlen von der Form $2X^2-1$ gibt, deren Quadrat dieselbe Form hat, d.h. die einzigen nichtnegativen Lösungen der diophantischen Gleichung

$$(2X^2-1)^2=2Y^2-1 \tag{1}$$

sind durch $X=0$, $Y=1$; $X=1$, $Y=1$; $X=2$, $Y=5$ gegeben. Ein Beweis dieses Satzes ist kürzlich von WACHS[2]) veröffentlicht worden.

Man kann sich fragen, ob noch weitere Formen MX^2-N mit positiven ganzen Koeffizienten M und N die Eigenschaft haben, dass das Quadrat von genau zwei der durch die Form dargestellten Zahlen wieder durch die Form dargestellt wird. Es soll hier eine einparametrige Schar solcher Formen angegeben werden.

Die diophantische Gleichung

$$(MX^2-N)^2=MY^2-N \tag{2}$$

besitzt die triviale Lösung $X=0$, $Y=1$, wenn $M=N(N+1)$. Man überzeugt sich sofort, dass in diesem Fall stets auch $X=2$, $Y=4N+1$ eine Lösung in natürlichen Zahlen ist. Diese Lösung ist somit ebenfalls als triviale Lösung anzusehen, insbesondere also auch die Lösung $X=2$, $Y=5$ von (1). Setzt man in (2) $M=N(N+1)$,

[1]) Oeuvres de FERMAT, ed. P. Tannery et CH. Henry, t. II, p. 434, 441.

[2]) S. WACHS: Démonstration d'un théorème de Fermat. Bull. Soc. math. France *66* (1938), 164—170. Derselbe Beweis ist schon von A. GENOCCHI (Nouv. Ann. Math., (3) *2* (1883), 306—310) angegeben worden. Vgl. auch L. E. DICKSON, History of the theory of numbers, Washington 1920, vol. II, p. 488.

so erhebt sich die Frage, für welche $N>1$ die dann mit (2) äquivalente Gleichung

$$N[(N+1)X^2-1]^2=(N+1)Y^2-1$$

nur die beiden trivialen Lösungen besitzt. Wir wollen zeigen, dass dies jedenfalls für $N=D^2$ ($D\neq 1$) der Fall ist[3]). Zum Beweis verwenden wir einen von LJUNGGREN[4]) mit Hilfe der Einheitentheorie hergeleiteten allgemeinen Satz über die Lösungen der Gleichungen $Ax^4-By^4=\pm 1$.

Wir beweisen zunächst drei Hilfssätze.

Hilfssatz 1. Sind D_1 und F natürliche Zahlen, $D_1F\neq 1$ und D_1 quadratfrei, so besitzt die diophantische Gleichung

$$4D_1^2(D_1^2F^4+1)X^4+1=Y^2 \tag{3}$$

ausser $X=0$, $Y=1$ und $X=F$, $Y=2D_1^2F^4+1$ keine Lösung in nichtnegativen ganzen Zahlen.

Beweis: Bekanntlich[5]) werden alle ganzzahligen teilerfremden Lösungen der Gleichung $Ax^2+y^2=z^2$, wo A eine quadratfreie Zahl bedeutet, durch folgende Formeln gegeben:

$$x=2\varrho uv,\quad y=\varrho(\alpha u^2-\beta v^2),\quad z=\varrho(\alpha u^2+\beta v^2),\quad \alpha\beta=A. \tag{4}$$

Hierbei sind u und v positive teilerfremde Zahlen und ϱ ist $=\frac{1}{2}$, wenn A,u,v alle ungerade sind und $=1$ sonst. Setzt man $P=D_1^2F^4+1=k^2A$, wo A quadratfrei ist, so ist in (3) $x=2kD_1X^2$, somit $kD_1X^2=uv$, weil $\varrho=1$ sein muss. Hieraus folgt $u=k_1d_1U^2$, $v=k_2d_2V^2$ mit $k_1k_2=k$, $d_1d_2=D_1$, $(k_1,k_2)=(d_1,d_2)=(k,D_1)=1$. Aus der zweiten Formel in (4) erhält man jetzt

$$\alpha k_1^2d_1^2U^4-\beta k_2^2d_2^2V^4=\pm 1,\quad \alpha\beta=A. \tag{5}$$

Wir dürfen dabei annehmen, dass α ungerade ist. Die Zahl $e=(k_1d_1U^2\sqrt{\alpha}+k_2d_2V^2\sqrt{\beta})^2=2\alpha k_1^2d_1^2U^4\mp 1+2D_1U^2V^2\sqrt{P}$ ist eine

[3]) Für $D=1$ sind einige leichte Modifikationen notwendig.

[4]) W. LJUNGGREN: Einige Eigenschaften der Einheiten reeller quadratischer und rein biquadratischer Zahlkörper. Oslo Vid. akad. Skrifter I, 1936, Nr. 12.

[5]) Vgl. L. E. DICKSON: Einführung in die Zahlentheorie, Berlin, B. G. Teubner, 1931, p. 37.

Einheit mit positiver Norm im Ring $r(\sqrt{P})$. Weil $\varepsilon = D_1F^2 + \sqrt{P}$ offenbar die Fundamentaleinheit (>1) in diesem Ring sein muss, ergibt sich $e = \varepsilon^{2n}$. Somit ist

$$2\alpha k_1^2 d_1^2 U^4 \mp 1 = D_1^{2n}F^{4n} + n(2n-1)D_1^{2n-2}F^{4n-4}P + \cdots + P^n .$$

Da $D_1^{2n}F^{4n} \pm 1$ für $D_1F \neq 1$ entweder durch P teilbar ist oder mit P nur den Teiler 1 oder 2 gemeinsam hat, ist $\alpha k_1^2 = 1$ oder $= P$ und man erhält aus (5)

$$d_1^2 PU^4 - d_2^2 V^4 = \pm 1 . \tag{6}$$

Nach LJUNGGREN gibt es nun unter allen Gleichungen $Ax^4 - By^4 = \pm 1$, für die die reellen biquadratischen Körper $k\left(\sqrt[4]{\frac{A}{B}}\right)$ identisch sind, höchstens eine einzige, die in ganzen nichtverschwindenden Zahlen x und y lösbar ist, und diese Gleichung hat höchstens eine Lösung in natürlichen Zahlen x und y[6]). Allen Gleichungen (6) entspricht derselbe Körper $k(\sqrt[4]{D_1^2P})$. $PU^4 - D_1^2V^4 = 1$ mit der Lösung $U=1$, $V=F$ ist somit die einzige in natürlichen Zahlen lösbare Gleichung (6) und die angegebene Lösung ist die einzige. Die andern Gleichungen können höchstens noch eine triviale Lösung mit $U=0$ besitzen. Hieraus ergibt sich leicht die Behauptung.

Hilfssatz 2. Die diophantische Gleichung

$$4D_1^2(D_1^2D_2^2F^4 + 1)X^4 + 1 = Y^2 \quad (D_2 \neq 1)$$

besitzt keine Lösung in natürlichen Zahlen X, Y, wobei $(2X, D_2) = 1$.

Beweis: Setzt man $D_1^2D_2^2F^4 + 1 = Q$, so ist $\eta = D_1D_2F^2 + \sqrt{Q}$ die Fundamentaleinheit in $r(\sqrt{Q})$. Die Behauptung folgt nun unmittelbar aus $Y + 2D_1X^2\sqrt{Q} = (D_1D_2F^2 + \sqrt{Q})^{2t}$, weil der irrationale Teil der rechten Seite durch $D_1D_2F^2$ teilbar ist.

Hilfssatz 3. Die diophantische Gleichung

$$D_1^2(D_1^2D_2^2F^4 + 1)X^4 + 2 = Y^2 \quad (D_1D_2F \neq 1)$$

besitzt keine Lösung in ganzen Zahlen.

---

[6]) Vgl. T. SKOLEM: Diophantische Gleichungen. Ergeb. d. Math. Bd. V, Heft 4, 1938, p. 113, Satz 30. Zum Beweis von Hilfssatz 1 kann man auch Satz 32 verwenden.

Beweis: Aus Kongruenzbetrachtungen mod 4 folgt, dass eine Lösung X, Y nur möglich ist, wenn $Q \equiv 2 (\mathrm{mod}\ 4)$. Dann sind $D_1 D_2 F$ und X ungerade. Ferner ist $g = \frac{1}{2}(Y + D_1 X^2 \sqrt{Q})^2 = D_1^2 Q X^4 + 1 + D_1 Y X^2 \sqrt{Q}$ eine Einheit mit positiver Norm in $r(\sqrt{Q})$.

Aus $g = \eta^{2m}$ ergibt sich

$$D_1^2 Q X^4 + 1 = D_1^{2m} D_2^{2m} F^{4m} + m(2m-1) D_1^{2m-2} D_2^{2m-2} F^{4m-4} Q + \cdots + Q^m. \quad (7)$$

Somit ist $(D_1^2 D_2^2 F^4)^m - 1$ durch Q teilbar. Wegen $D_1 D_2 F \neq 1$ muss m gerade sein. Dann ist aber in (7) die rechte Seite $\equiv 1 (\mathrm{mod}\ 4)$, während die linke $\equiv 3 (\mathrm{mod}\ 4)$ ist. Also führt die Annahme einer Lösung auf einen Widerspruch.

Wir beweisen nun den

Satz. Ist $D \neq 1$ eine natürliche Zahl, dann besitzt die diophantische Gleichung

$$D^2[(D^2+1)X^2 - 1]^2 = (D^2+1)Y^2 - 1 \quad (8)$$

ausser $X=0$, $Y=1$ und $X=2$, $Y=4D^2+1$ keine Lösung in nichtnegativen ganzen Zahlen.

Beweis: Wir schreiben (8) in der einfacheren Form

$$(D^2X^2 - 1)^2 + D^2 X^4 = Y^2. \quad (9)$$

Bei der Anwendung von (4) auf (9) kann man annehmen, dass u und v verschiedene Parität haben. Man erhält so folgende zwei Fälle:

$DX^2 = 2uv$	(10.1)	$D^2X^2 - 1 = u^2 - v^2$	(10.2)
$DX^2 = u^2 - v^2$	(11.1)	$D^2X^2 - 1 = 2uv$	(11.2)

Setzt man $D = D_3 F^2$, wo D_3 quadratfrei ist, so folgt aus (10.1), weil v nicht gerade sein kann, $u = 2D_1 U^2$, $v = D_2 V^2$ mit $D_1 D_2 = D_3$ und $(D_1, D_2) = (D_2, 2U) = 1$.

Aus (10.2) findet man unter Berücksichtigung von (10.1)

$$4D_1^2(D_1^2 D_2^2 F^4 + 1) U^4 + 1 = D_2^2 (V^2 + 2D_1^2 F^2 U^2)^2.$$

Nach Hilfssatz 1 und 2 ist $U=0$ oder $U=F$, somit $X=0$ oder $X=2$.

Aus (11.1) ergibt sich $u+v=D_1U^2$, $u-v=D_2V^2$, so dass $u=\frac{1}{2}(D_1U^2+D_2V^2)$, $v=\frac{1}{2}(D_1U^2-D_2V^2)$. Unter Berücksichtigung von (11.1) erhält man aus (11.2)

$$D_1^2(D_1^2D_2^2F^4+1)U^4+2=D_2^2(V^2+D_1^2F^2U^2)^2.$$

Nach Hilfssatz 3 kann also dieser Fall nicht auftreten. Damit ist der Satz bewiesen.