icm©

Soit maintenant $a_1, a_2, \ldots, a_m$ une suite finie quelconque de chiffres du système décimal, $a_1 \neq 0$, et soit a le nombre naturel ayant m chiffres qui sont successivement $a_1, a_2, \ldots, a_m$. D'après notre lemme on a pour x suffisamment grand $\pi'(ax) < \pi'\big((a+1)x\big)$, et il en résulte qu'il existe un nombre naturel s aussi grand que l'on veut et tel que $\pi'(a, 10^s) < \pi'\big((a+1)10^s\big)$. Il existe donc un nombre premier p de la forme $p = 10^n k+b$, tel que

$$a \cdot 10^s < p < (a+1) \cdot 10^s.$$

Or, il s'ensuit de ces inégalités que les premiers m chiffres du nombre p sont respectivement les mêmes que ceux du nombre a; les n derniers chiffres du nombre $p = 10^n k+b$ étant évidemment les mêmes respectivement que ceux du nombre b, notre théorème se trouve démontré.

D'après une remarque de S. Knapowski une legère modification de notre démonstration permettrait de prouver un théorème plus général, où l'on remplacerait la base 10 par une base g, où g est un nombre naturel quelconque >1, la condition $(b_n, 10) = 1$ devant être remplacée par $(b_n, g) = 1$.

Travaux cités

[1] W. Sierpiński, *Sur l'existence des nombres premiers avec une suite arbitraire des chiffres initiaux*, Le Matematiche 6 (1951), p. 135-137.

[2] E. Trost, *Primzahlen*, Basel 1953.

Reçu par la Rédaction le 10. 11. 1958

ACTA ARITHMETICA
V (1959)

Über einen verallgemeinerten Fermatschen Satz

von

B. Stolt (Uppsala)

1. P. Fermat hat den folgenden Satz aufgestellt.

Die Gleichung $x^2+2 = y^3$ *besitzt genau die Lösung* $x = 5$, $y = 3$ *in natürlichen Zahlen* x, y.

Fermat behauptet, er habe den Satz bewiesen, aber der erste bekannte Beweis stammt von Euler.

Es seien $n > 1$ und D natürliche Zahlen. Die allgemeinere Gleichung

$$x^2+D = y^n \tag{1}$$

ist von T. Nagell [5]-[8] und W. Ljunggren [1], [2] behandelt worden. Die meisten Resultate beziehen sich auf die Gleichung

$$x^2+D = y^q, \tag{2}$$

wo q eine ungerade Primzahl ist. Für $D = 1, 2, 3$ ist (1) von Nagell vollständig gelöst worden.

Bei den obigen Untersuchungen wird im allgemeinen vorausgesetzt, daß die Klassenzahl h von $K(\sqrt{-D})$ zu n prim ist. Durch Zerlegung des linken Gliedes von (1) wird dann (1) in eine Gleichung vom Typus $F(u, v) = k$ überführt, wo k eine Konstante und $F(u, v)$ eine binäre ganzzahlige Form ist. Diese neue Gleichung ist so beschaffen, daß man aus ihr leicht einsieht, daß entweder u oder v nur gewisser Werte fähig ist. Für besondere Werte von n und D läßt sich dann zeigen, daß (1) in natürlichen Zahlen x, y unmöglich ist oder genau eine gewisse Lösung hat.

In der vorliegenden Arbeit wird die noch allgemeinere Gleichung

$$Cx^2+D = y^q \tag{3}$$

behandelt, wo C, D natürliche Zahlen sind und q eine ungerade Primzahl ist. Ferner ist CD quadratfrei, $CD \not\equiv 7 \pmod 8$ und $h(\sqrt{-CD})$ prim zu q Nach Thue [11] hat (3) nur endlich viele ganzzahlige Lösungen x, y.

(3) ist in Sonderfällen von Nagell [5], [8] und Ljunggren [3] behandelt worden. Dabei wird (3) genau wie (1) in eine Gleichung vom Typus $F(u,v)=k$ überführt, wo entweder u oder v nur gewisser Werte fähig ist.

In der vorliegenden Arbeit wird gezeigt, daß es möglich ist, aus $F(u,v)=k$ noch weitere Aufschlüsse über die ursprüngliche Gleichung zu erhalten. Zunächst wird $F(u,v)=k$ in eine Gleichung vom Typus $f(y)=0$ überführt, wo y mit der gleichbezeichneten Veränderlichen von (3) identisch ist. Durch einfache Kongruenzbetrachtungen erhält man leicht in Satz 1 eine Reihe von Fällen, wo (3) in natürlichen Zahlen x, y unmöglich ist.

In Satz 2 betrachtet man Klassen von Gleichungen der Form (3), in welchen q und D gegeben sind und C alle diejenigen natürlichen Zahlen durchläuft, die eine gewisse Kongruenz erfüllen. Für $q>3$ läßt sich zeigen, daß höchstens eine Gleichung jeder Klasse in natürlichen Zahlen lösbar ist und genau eine Lösung hat. Für $q=3$ erhält man für gewisse Klassen dasselbe Resultat, aber es gibt auch Klassen, wo höchstens zwei Lösungen möglich sind.

Aus Satz 2 folgt das wichtige Ergebnis, daß die Gleichung

$$x^2+D=y^q \tag{2}$$

im Falle $D\equiv 3 \pmod 8$, $q=3$ höchstens zwei Lösungen, in allen übrigen Fällen höchstens eine Lösung in natürlichen Zahlen x, y hat.

2. Es seien q, C und D gegebene natürliche Zahlen, q eine ungerade Primzahl, CD quadratfrei und $\not\equiv 7 \pmod 8$. Ferner sei die Klassenzahl $h(\sqrt{-CD})$ prim zu q.

Unter diesen Voraussetzungen ist bekannt, daß die diophantische Gleichung

$$Cx^2+D=y^q \tag{3}$$

in folgenden Fällen keine Lösungen in natürlichen Zahlen x, y hat.

$D=1$ mit der Ausnahme von $C=2$, $q=5$, $x=11$, $y=3$, laut Nagell [5], [8], $D=2$ mit der Ausnahme von $C=1$, $q=3$, $x=5$, $y=3$, laut Nagell [8], $C=1$, $D=3$, laut Nagell [5]. Es genügt folglich, $CD\neq 1$ und $CD\neq 3$ anzunehmen.

Es sei x, y eine ganzzahlige Lösung von (3). Unter den obigen Voraussetzungen ist es möglich, (3) in der Form

$$(Cx+\sqrt{-CD})(Cx-\sqrt{-CD})=Cy^q$$

zu schreiben.

Wegen $CD\not\equiv 7 \pmod 8$ ist y ungerade. Dann haben die beiden Hauptideale $(Cx+\sqrt{-CD})$ und $(Cx-\sqrt{-CD})$ den größten gemeinsamen Teiler $(C,\sqrt{-CD})$, denn $(C)=(C,\sqrt{-CD})^2$ und $(x,y)=1$. Dann ergibt sich

$$(Cx+\sqrt{-CD})=(C,\sqrt{-CD})\mathfrak{a}^q, \tag{4}$$

wo $\mathfrak{a}$ ein Ideal des Körpers $K(\sqrt{-CD})$ ist. Ferner gilt

$$(Cx+\sqrt{-CD})^2=(C)\mathfrak{a}^{2q}, \tag{5}$$

wo $\mathfrak{a}^{2q}$ ein Hauptideal ist. Weil h zu q prim ist, erhält man leicht $\mathfrak{a}^2\sim(1)$.

Die einzigen Einheiten des Körpers $K(\sqrt{-CD})$ sind ± 1. Aus (5) folgt dann

$$(Cx+\sqrt{-CD})^2=C(u+v\sqrt{-CD})^q 2^{-q}, \tag{6}$$

wo $\frac{1}{2}(u+v\sqrt{-CD})$ eine ganze Zahl des Körpers $K(\sqrt{-CD})$ ist.

Aus (6) folgt

$$\tfrac{1}{2}(u+v\sqrt{-CD})=(\tfrac{1}{2}(a_1\sqrt{C}+b_1\sqrt{-D}))^2,$$

a_1, b_1 ganz rational, $a_1\equiv b_1 \pmod 2$.

Wegen (6) ergibt sich dann

$$x\sqrt{C}+\sqrt{-D}=(a_2\sqrt{C}+b_2\sqrt{-D})^q 2^{-q},$$

$a_2\equiv b_2 \pmod 2$. Hieraus folgt mit $q=2m+1$

$$2^q=\sum_{r=0}^{m}\binom{q}{2r+1}a_2^{q-1-2r}b_2^{2r+1}C^{m-r}(-D)^r. \tag{7}$$

Aus (7) folgt $b_2=\pm 1$ oder $b_2=\pm 2^m$. Wenn (7) als eine Kongruenz betrachtet wird, erhält man

$$b_2(-D)^m\equiv 2^q\equiv 2 \pmod q$$

oder $b_2\equiv\pm 2 \pmod q$.

$b_2=\pm 1$ ist nur im Falle $q=3$ möglich. Wegen (7) gilt dann

$$D=3Ca_2^2\mp 8$$

oder $CD\equiv 3 \pmod 8$.

In den Fällen $q>3$ oder $q=3$, $CD\not\equiv 3 \pmod 4$ gilt $a_2=2a$, $b_2=2b$. Hieraus folgt

$$x\sqrt{C}+\sqrt{-D}=(a\sqrt{C}+b\sqrt{-D})^q$$

und wie vorher

$$1=\sum_{r=0}^{m}\binom{q}{2r+1}a^{q-1-2r}b^{2r+1}C^{m-r}(-D)^r. \tag{8}$$

Wenn q ein Teiler von D ist, so ist (8) unmöglich. Aus $(D,q)=1$ folgt $b=(-D/q)$ und ferner wegen $y=Na=Ca^2+D$

$$\left(\frac{-D}{q}\right)=\sum_{r=0}^{m}\binom{q}{2r+1}(Ca^2)^{m-r}(-D)^r=\sum_{r=0}^{m}\binom{q}{2r+1}(y-D)^{m-r}(-D)^r. \tag{9}$$

Aus (9) folgt der Reihe nach

$$\left(\frac{-D}{q}\right)=\sum_{r=0}^{m}\binom{q}{2r+1}(-D)^r\sum_{s=0}^{m-r}\binom{m-r}{s}y^s(-D)^{m-r-s}$$

$$=\sum_{s=0}^{m}y^{m-s}(-D)^s\sum_{r=0}^{s}\binom{q}{2r+1}\binom{m-r}{m-s}.$$

Nach E. Netto [9], S. 253, Formel (36), 2. Zeile, gilt mit den Bezeichnungen der vorliegenden Arbeit

$$\sum_{r=0}^{s}\binom{q}{2r+1}\binom{m-r}{m-s}=4^s\frac{q}{m-s}\binom{m+s}{2s+1},\quad s=0,1,\ldots,m-1,\quad \sum_{r=0}^{m}\binom{q}{2r+1}=4^m.$$

Dann folgt

$$\left(\frac{-D}{q}\right)=\sum_{s=0}^{m-1}4^s\cdot\frac{q}{m-s}\binom{m+s}{2s+1}y^{m-s}(-D)^s+4^m(-D)^m. \tag{10}$$

Es ist leicht zu zeigen, daß $\frac{1}{m-s}\binom{m+s}{2s+1}$ ganz ist. Denn $\binom{m+s}{2s}$ und $\binom{m+s}{2s+1}$ sind ganz. Ferner gilt $(2s+1,\,m-s)=1$. Denn wäre $2s+1=ft$, $m-s=gt$, so könnte man s eliminieren. Dann wäre $q=2m+1=(f+2g)t$, woraus $t=1$ folgt.

Aus (10) ergibt sich

$$\sum_{s=0}^{m-1}\frac{4^s}{m-s}\binom{m+s}{2s+1}y^{m-s}(-D)^s+\frac{1}{q}\left[(-4D)^m-\left(\frac{-D}{q}\right)\right]=0.$$

Mit

$$K_0=1,\quad K_s=\frac{4^s}{m-s}\binom{m+s}{2s+1}D^s,\quad s=1,2,\ldots,m-1, \tag{11}$$

erhält man

$$K_m=\frac{1}{q}\left[(4D)^m-\left(\frac{D}{q}\right)\right]$$

$$\sum_{s=0}^{m}(-1)^sK_sy^{m-s}=0. \tag{12}$$

Wegen $K_0=1$ ist jede rationale Lösung von (12) ganz. Ferner sind alle K_s ganz. Wenn x, y eine ganzzahlige Lösung von (3) ist, so ist y eine ganzzahlige ungerade Lösung von (12).

Es seien $y_1,y_2,\ldots,y_m$ die m Wurzeln von (12). Für symmetrische Funktionen der Wurzeln werden folgende Kürzungen benutzt.

$$S_1=\sum_{i=3}^{m}y_i,\quad S_2=\sum_{i,j=3}^{m}y_iy_j,\quad \ldots,\quad S_{m-2}=\prod_{i=3}^{m}y_i.$$

Es sei $q>3$. Wenn (3) zwei ganzzahlige Lösungen x_1,y_1; x_2,y_2 hätte, $y_1\neq y_2$, so hätte (12) zwei ganzzahlige ungerade Lösungen y_1, y_2. Dann hätte man wegen (12) für $m>3$

$$K_1=y_1+y_2+S_1, \tag{13}$$

$$K_2=y_1y_2+(y_1+y_2)S_1+S_2, \tag{14}$$

$$K_\nu=y_1y_2S_{\nu-2}+(y_1+y_2)S_{\nu-1}+S_\nu,\quad \nu=3,4,\ldots,m-2, \tag{15}$$

$$K_{m-1}=y_1y_2S_{m-3}+(y_1+y_2)S_{m-2}, \tag{16}$$

$$K_m=y_1y_2S_{m-2}. \tag{17}$$

Mit $\binom{0}{0}=1$ folgt aus (13)-(15)

$$S_\nu=\sum_{k=0}^{\nu}(-1)^kK_{\nu-k}\sum_{i=0}^{[k/2]}(-1)^i\binom{k-i}{i}(y_1+y_2)^{k-2i}(y_1y_2)^i,\nu=1,2,\ldots,m,-2. \tag{18}$$

Aus (16)-(18) folgt

$$K_{m-1}=\sum_{k=1}^{m-1}(-1)^{k+1}K_{m-1-k}\sum_{i=0}^{[k/2]}(-1)^i\binom{k-i}{i}(y_1+y_2)^{k-2i}(y_1y_2)^i, \tag{19}$$

$$K_m=\sum_{k=0}^{m-2}(-1)^kK_{m-2-k}\sum_{i=0}^{[k/2]}(-1)^i\binom{k-i}{i}(y_1+y_2)^{k-2i}(y_1y_2)^{i+1}. \tag{20}$$

Es ist leicht zu zeigen, daß (19) und (20) auch für $m=2$ und $m=3$ gültig sind.

Es sei x, y eine ganzzahlige Lösung von (3). Wegen (3) ist klar, daß y folgende Bedingungen erfüllen muß.

(21)

$y \equiv 1 \pmod 4$,	wenn	$D \equiv 1 \pmod 4$,	C ungerade,
$y \equiv 3 \pmod 4$,	wenn	$D \equiv 3 \pmod 4$,	C ungerade,
$y \equiv \pm 1 \pmod 8$,	wenn	$D \equiv 1 \pmod 8$,	$C \equiv 6 \pmod 8$,
	„	$D \equiv 7 \pmod 8$,	$C \equiv 2 \pmod 8$,
$y \equiv 1, 3 \pmod 8$,	wenn	$D \equiv 1 \pmod 8$,	$C \equiv 2 \pmod 8$,
	„	$D \equiv 3 \pmod 8$,	$C \equiv 6 \pmod 8$,
$y \equiv \pm 3 \pmod 8$,	wenn	$D \equiv 5 \pmod 8$,	$C \equiv 6 \pmod 8$,
	„	$D \equiv 3 \pmod 8$,	$C \equiv 2 \pmod 8$,
$y \equiv 5, 7 \pmod 8$,	wenn	$D \equiv 5 \pmod 8$,	$C \equiv 2 \pmod 8$,
	„	$D \equiv 7 \pmod 8$,	$C \equiv 6 \pmod 8$,
$y \equiv C+2 \pmod 8$,	wenn	$D \equiv 2 \pmod 8$,	C ungerade,
$y \equiv C-2 \pmod 8$,	wenn	$D \equiv 6 \pmod 8$,	C ungerade.

3. Aus (12) und (21) folgt leicht

Satz 1. *Es seien q, C und D gegebene natürliche Zahlen, q eine ungerade Primzahl, CD quadratfrei, $\not\equiv 7 \pmod 8$, $\neq 1$ und $\neq 3$. Wenn $q = 3$ soll auch $CD \not\equiv 3 \pmod 4$ erfüllt sein. Wenn $h(\sqrt{-CD})$ zu q prim ist, so ist* (3) *in folgenden Fällen in natürlichen Zahlen x, y nicht lösbar.*

$q \equiv 1 \pmod 4$,	$D \equiv 2 \pmod 4$,	C *beliebig*,	
$q \equiv 1 \pmod 4$,	$D \equiv 1 \pmod 2$,	C *beliebig*,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 3 \pmod 4$,	$D \equiv 1 \pmod 4$,	$C \equiv 1 \pmod 2$,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 3 \pmod 4$,	$D \equiv 3 \pmod 4$,	$C \equiv 1 \pmod 2$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 3 \pmod 4$,	$D \equiv 1 \pmod 8$,	$C \equiv 2 \pmod 8$,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 3 \pmod 4$,	$D \equiv 5 \pmod 8$,	$C \equiv 2 \pmod 8$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 3 \pmod 4$,	$D \equiv 5 \pmod 8$,	$C \equiv 6 \pmod 8$,	
$q \equiv 3 \pmod 4$,	$D \equiv 3 \pmod 8$,	$C \equiv 2 \pmod 8$,	
$q \equiv 3 \pmod 4$,	$D \equiv 3 \pmod 8$,	$C \equiv 6 \pmod 8$,	$\left(\frac{D}{q}\right) = -1$,

$q \equiv 3 \pmod 4$,	$D \equiv 7 \pmod 8$,	$C \equiv 6 \pmod 8$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 3 \pmod 8$,	$D \equiv 2 \pmod 8$,	$C \equiv 1 \pmod 8$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 3 \pmod 8$,	$D \equiv 2 \pmod 8$,	$C \equiv 3 \pmod 8$,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 3 \pmod 8$,	$D \equiv 2 \pmod 8$,	$C \equiv 5, 7 \pmod 8$,	
$q \equiv 3 \pmod 8$,	$D \equiv 6 \pmod 8$,	$C \equiv 1, 3 \pmod 8$,	
$q \equiv 3 \pmod 8$,	$D \equiv 6 \pmod 8$,	$C \equiv 5 \pmod 8$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 3 \pmod 8$,	$D \equiv 6 \pmod 8$,	$C \equiv 7 \pmod 8$,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 7 \pmod 8$,	$D \equiv 2 \pmod 8$,	$C \equiv 1, 3 \pmod 8$,	
$q \equiv 7 \pmod 8$,	$D \equiv 2 \pmod 8$,	$C \equiv 5 \pmod 8$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 7 \pmod 8$,	$D \equiv 2 \pmod 8$,	$C \equiv 7 \pmod 8$,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 7 \pmod 8$,	$D \equiv 6 \pmod 8$,	$C \equiv 1 \pmod 8$,	$\left(\frac{D}{q}\right) = +1$,
$q \equiv 7 \pmod 8$,	$D \equiv 6 \pmod 8$,	$C \equiv 3 \pmod 8$,	$\left(\frac{D}{q}\right) = -1$,
$q \equiv 7 \pmod 8$,	$D \equiv 6 \pmod 8$,	$C \equiv 5, 7 \pmod 8$.	

Beweis. Es sei $q = 2m+1$. Wenn die Annahme des Satzes besteht und x, y eine Lösung von (3) in natürlichen Zahlen ist, so muß y eine Lösung von (12) sein.

Wegen (12) ergibt sich

$$y^m - 2Dm(m+1)y^{m-1} + (-1)^{m+1}\left(\frac{D}{q}\right) q \equiv 0 \pmod 8. \tag{22}$$

Wenn $q \equiv 1 \pmod 4$, $\left(\frac{D}{q}\right) = -1$ erhält man aus (22) $y^2+1 \equiv 0 \pmod 4$, was nicht möglich ist.

Um die Unmöglichkeit von $q \equiv 1 \pmod 4$, $D \equiv 2 \pmod 4$, $\left(\frac{D}{q}\right) = +1$

zu beweisen, nehmen wir den Fall $m \equiv 2^n \pmod{2^{n+1}}$, $n > 0$, an. Dann gilt

$$y^m \equiv 1,\ q^2 \equiv 1,\ K_1 \equiv K_2 \dots \equiv K_{m-1} \equiv 0 \pmod{2^{n+2}}.$$

Aus (12) folgt

$$y^m - q \equiv 2^{n+1} \equiv 0 \pmod{2^{n+2}},$$

was einen Widerspruch liefert. Wenn n die Werte $1, 2, \dots$ durchläuft, ergibt sich die Unmöglichkeit der Fälle $q \equiv 5 \pmod 8$, $q \equiv 9 \pmod{16}$, ..., d. h. von $q \equiv 1 \pmod 4$.

Wenn $q \equiv 3 \pmod 4$, $D \equiv 1 \pmod 4$, $C \equiv 1 \pmod 2$, $(D/q) = -1$, erhält man $y - 3 \equiv 0 \pmod 4$, was wegen $y \equiv 1 \pmod 4$ nicht möglich ist.

Wenn $q \equiv 3 \pmod 4$, $D \equiv 3 \pmod 4$, $C \equiv 1 \pmod 2$, $(D/q) = +1$, erhält man $y + 3 \equiv 0 \pmod 4$, was wegen $y \equiv 3 \pmod 4$ nicht möglich ist.

Wenn $q \equiv 3 \pmod 8$, $D \equiv 1 \pmod 2$, $C \equiv 2 \pmod 4$, geht (22) in

$$y + 4 + 3(D/q) \equiv 0 \pmod 8 \tag{23}$$

über. Wenn $q \equiv 7 \pmod 8$, $D \equiv 1 \pmod 2$, $C \equiv 2 \pmod 4$, geht (22) in

$$y + 7(D/q) \equiv 0 \pmod 8 \tag{24}$$

über. Aus (21), (23) und (24) folgt leicht, daß die im Satze gegebenen Fälle unmöglich sind.

Wenn $q \equiv 3 \pmod 4$, $D \equiv 2 \pmod 4$, erhält man

$$y + q(D/q) \equiv 0 \pmod 8. \tag{25}$$

Mit Hilfe der Resultate von (21) und (25) ist es leicht zu bestätigen, daß die im Satze gegebenen Fälle unmöglich sind.

4. Satz 2. *Es seien q und D gegebene natürliche Zahlen, q eine ungerade Primzahl, $D \neq 1$ und $\neq 3$. Man betrachtet alle Gleichungen*

$$Cx^2 + D = y^q, \tag{3}$$

in welchen C eine natürliche Zahl ist, CD quadratfrei, $CD \not\equiv 7 \pmod 8$, $h(\sqrt{-CD})$ prim zu q.

Wenn $q \equiv 3 \pmod 4$, $q > 3$, oder wenn $q = 3$, $CD \not\equiv 3 \pmod 4$, gibt es unter allen Gleichungen (3) höchstens eine, die in natürlichen Zahlen x, y lösbar ist. Wenn sie lösbar ist, hat sie genau eine Lösung.

Wenn $q \equiv 1 \pmod 4$, gibt es unter allen Gleichungen (3), wo C und D einer der folgenden Bedingungen genügen, höchstens eine, die in natürlichen Zahlen x, y lösbar ist. Wenn sie lösbar ist, hat sie genau eine Lösung.

$$D \equiv 1 \pmod 2, \quad C \equiv 1 \pmod 2,$$
$$D \equiv 1 \pmod 4, \quad C \equiv 6 \pmod 8,$$
$$D \equiv 3 \pmod 4, \quad C \equiv 2 \pmod 8.$$

Wenn $q = 3$, $D \equiv 1 \pmod 2$, C beliebig, gibt es unter allen Gleichungen (3) höchstens zwei, die in natürlichen Zahlen x, y lösbar sind. Sie haben zusammen höchstens zwei Lösungen.

Beweis. Es seien, q, C und D gegebene natürliche Zahlen, q eine ungerade Primzahl, CD quadratfrei und $\not\equiv 7 \pmod 8$. Ferner sei $h(\sqrt{-CD})$ prim zu q. Wegen der in **2** genannten Sonderfälle kann man $D \neq 1$ und $\neq 3$ annehmen. Im Falle $q = 3$ sei ferner $CD \not\equiv 3 \pmod 4$.

Nunmehr werden alle Gleichungen der Form (3) betrachtet, in welchen q und D gegeben sind und C diejenigen Werte annimmt, die mit einer der gegebenen Bedingungen des Satzes vertragbar sind. Aus jeder solchen Gleichung kann man wegen **2** dieselbe Gleichung (12) herleiten. Wenn eine der Gleichungen (3) in natürlichen Zahlen x, y lösbar ist, so muß y eine Lösung der Gleichung (12) sein.

Es seien x_1, y_1 und x_2, y_2 natürliche Zahlen, $y_1 \neq y_2$, die Lösungen derselben Gleichung (3) oder verschiedener Gleichungen (3) sind. Dann hat die entsprechende Gleichung (12) zwei ungerade Lösungen y_1, y_2. Für diese gelten (19) und (20). Der Satz wird folglich bewiesen, indem man zeigt, daß (12) in den gegebenen Fällen höchstens eine ungerade Lösung hat.

Wenn $q \equiv 3 \pmod 4$, $q > 3$, folgt aus (19) $K_{m-1} \equiv (y_1 y_2)^{(m-1)/2} \equiv 1 \pmod 2$. Aber wegen (11) ist K_{m-1} gerade, was einen Widerspruch liefert.

Wenn $q = 3$, $CD \not\equiv 3 \pmod 4$, kann man (12) aus (3) herleiten. Sie ist eine Gleichung ersten Grades und hat höchstens eine ganzzahlige Lösung.

Es sei $q \equiv 1 \pmod 4$. Dann ist (3) nur für ungerade D lösbar. Wir nehmen den Fall $q = 2m+1$, $m \equiv 2^n \pmod{2^{n+1}}$, $n > 0$, an. Wegen (11) gilt

$$K_1 \equiv 2^{n+1},\ K_2 \equiv K_3 \equiv \dots \equiv K_{m-1} \equiv 0 \pmod{2^{n+2}}.$$

Aus der Annahme folgt

$$(y_1 + y_2)^{2r+1} \binom{(m+1)/2}{2r+1} \equiv 0 \pmod{2^{n+1}}, \qquad r > 0.$$

Wegen (19) ergibt sich

$$K_{m-1} \equiv 0 \equiv (-y_1 y_2)^{(m-1)/2} \tfrac{1}{2} m (y_1 + y_2) \pmod{2^{n+1}}.$$

Hieraus folgt $y_1 + y_2 \equiv 0 \pmod 4$. Aus (19) folgt dann

$$K_{m-1} \equiv 0 \equiv (-y_1 y_2)^{(m-1)/2} [\tfrac{1}{2} m (y_1 + y_2) - K_1] \pmod{2^{n+2}}.$$

Dann ergibt sich $y_1 + y_2 \equiv 4 \pmod 8$, woraus $y_1 y_2 \equiv 3 \pmod 8$ folgt.

Wenn $D \equiv 1 \pmod 4$, $C \equiv 1 \pmod 2$, folgt aus (21) $y_1 \equiv y_2 \equiv 1 \pmod 4$, was einen Widerspruch liefert.

Wenn $D \equiv 3 (\mathrm{mod}\, 4)$, $C \equiv 1 (\mathrm{mod}\, 2)$, folgt aus (21) $y_1 \equiv y_2 \equiv 3 (\mathrm{mod}\, 4)$, was einen Widerspruch liefert.

Wenn $D \equiv 1 (\mathrm{mod}\, 8)$, $C \equiv 6 (\mathrm{mod}\, 8)$, oder $D \equiv 7 (\mathrm{mod}\, 8)$, $C \equiv 2 (\mathrm{mod}\, 8)$, oder $D \equiv 5 (\mathrm{mod}\, 8)$, $C \equiv 6 (\mathrm{mod}\, 8)$, oder $D \equiv 3 (\mathrm{mod}\, 8)$, $C \equiv 2 (\mathrm{mod}\, 8)$, folgt aus (21) $y_1 y_2 \equiv \pm 1 (\mathrm{mod}\, 8)$, was einen Widerspruch liefert.

Wenn n die Werte $1, 2, \ldots$ durchläuft, ergibt sich die Unmöglichkeit der Fälle $q \equiv 5 (\mathrm{mod}\, 8)$, $q \equiv 9 (\mathrm{mod}\, 16)$, ..., d. h. von $q \equiv 1 (\mathrm{mod}\, 4)$.

Wenn $q = 3$, $D \equiv 1 (\mathrm{mod}\, 2)$, C beliebig, führt jede Gleichung (3) zu einer Gleichung der Form (7), oder

$$8 = b_2(3Ca_2^2 - Db_2^2), \tag{26}$$

$a_2 \equiv b_2 (\mathrm{mod}\, 2)$. Wenn a_2 und b_2 gerade sind, geht (26) in eine Gleichung ersten Grades in y der Form (12) über. Wenn a_2 und b_2 ungerade sind, geht (26) in $3Ca_2^2 - D - 8(D/3) = 0$ über. Aus $y = Na = \frac{1}{4}(Ca_2^2 + D)$ folgt

$$3y - D - 2(D/3) = 0. \tag{27}$$

Jede Gleichung (3) geht folglich in eine der beiden Gleichungen (12) oder (27) über. Diese haben je höchstens eine ganzzahlige ungerade Lösung.

In ähnlicher Weise kann man die Gleichungen $Cx^2 + D = 2y^q$ und $Cx^2 + D = 4y^q$ behandeln (vgl. Ljunggren [4], Stolt [10]).

Literaturverzeichnis

[1] W. Ljunggren, *On the Diophantine equation* $x^2 + p^2 = y^n$, Norske Vid. Selsk. Forhdl. 16 (1943), p. 27-30.

[2] — *On the Diophantine equation* $x^2 + D = y^n$, Ibid. 17 (1944), p. 93-96.

[3] — *On a Diophantine equation*, Ibid. 18 (1945), p. 125-128.

[4] — *Über die Gleichungen* $1 + Dx^2 = 2y^n$ *und* $1 + Dx^2 = 4y^n$, Ibid. 15 (1942), p. 115-118.

[5] T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk matem. forenings skrifter I Nr 13 (1923), p. 6-82.

[6] — *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. 5 (1954), p. 153-159.

[7] — *On the Diophantine equation* $x^2 + 8D = y^n$, Ark. mat. 3 (1955), p. 103-112.

[8] — *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Reg. Soc. Sci. Upsal. IV Ser. 16 (1955), p. 1-38.

[9] E. Netto, *Lehrbuch der Combinatorik*, 2 Aufl. 1927.

[10] B. Stolt, *Die Anzahl von Lösungen gewisser diophantischer Gleichungen*, Arch. Math. 8 (1957), p. 393-400.

[11] A. Thue, *Über die Unlösbarkeit der Gleichung* $ax^2 + bx + c = dy^n$ *in großen ganzen Zahlen* x *und* y, Arch. Math. Naturvid. 24 (1916), p. 1-6.

Reçu par la Rédaction le 24. 12. 1958

ACTA ARITHMETICA
V (1959)

The zeta function and discriminant of a division algebra

by

K. G. Ramanathan (Bombay)

§ 1. Let D be a division algebra of finite rank $g = hf^2$ over the field Γ of rational numbers and Z its centre so that $(D : Z) = f^2$ and $(Z : \Gamma) = h$. Let $\bar{\Gamma}$ be the real number field. Siegel [10] has shown that the tensor product $\bar{D} = D \otimes \bar{\Gamma}$ has, over $\bar{\Gamma}$, an involution $x \to x^*$. Let P be the space of positive elements of $\bar{D}$, that is the set of elements $x = x^*$ all of whose characteristic roots are positive. P is a symmetric Riemannian space with the metric $ds^2 = \sigma(\xi^{-1} d\xi\, \xi^{-1} d\xi)$. Let $[d\xi]$ denote the volume element computed with this metric. We introduce the generalized gamma function

$$\Gamma_D(a, s) = \int_P (N\xi)^{s/2} e^{-\pi\sigma(a\xi)} [d\xi]$$

where $a \in P$, N and σ denote norm and trace in the regular representation of $\bar{D}$ over $\bar{\Gamma}$ and s is a complex variable whose real part is greater than $(f-1)/f$. $\Gamma_D(a, s)$ is a simple generalization of the gamma function introduced by C. L. Siegel [9] in the analytic theory of quadratic forms. Let Λ be a lattice in $\bar{D}$ and $\tilde{\Lambda}$ the complementary lattice. Let ξ be an arbitrary but fixed element of P. The function

$$\vartheta(\Lambda, \xi) = \sum_{a \in \Lambda} e^{-\pi\sigma(a^* \xi a)}$$

is called the *theta function* of the lattice. There exists a transformation formula connecting $\vartheta(\Lambda, \xi)$ and $\vartheta(\tilde{\Lambda}, \xi^{-1})$. By using this theta function and the gamma function above, we shall obtain a simple proof of the functional equation for the zeta function of D. In view of the work of Siegel on the zeta functions of indefinite forms, it seems more natural to use the representation space P of the units of a maximal order of D in the study of the zeta function of D.

For the discriminant d of a totally real algebraic number field C. L. Siegel [6] obtained an identity which shows at once that $|d| > 1$. This identity was generalized to all fields by Müntz [5] and Calloway [1].