102. Über die Fermatsche Vermutung, XII.

Von Taro MORISHIMA.
Prefectural Higher School of Tokyo.
(Comm. by T. TAKAGI, M.I.A., Oct. 12, 1935.)

Es seien

l eine ungerade Primzahl,
ζ eine primitive l-te Einheitswurzel,
k der Kreiskörper von ζ,
k' der reelle Unterkörper vom μ-ten Grade von k, $\mu=\frac{l-1}{2}$,
r eine primitive Wurzel mod. l,
s die Substitution $(\zeta\to\zeta^r)$ in k,
B_i die Bernoullische Zahl,
$\varepsilon(\zeta)=\sqrt{\frac{1-\zeta^r}{1-\zeta}\,\frac{1-\zeta^{-r}}{1-\zeta^{-1}}}$ die Kreiseinheit in k,
$E_n=\varepsilon(\zeta)^{f(s)}$ (symbolische Potenz), $f(s)=\sum_{i=0}^{\mu-1} r^{2(\mu-in)}s^i$.

In meiner früheren Arbeit[1] habe ich den Satz bewiesen:
Satz A. *Wenn die Gleichung*

$$\alpha^l+\beta^l+\gamma^l=0 \tag{1}$$

durch ganzen, zu l relativprime Zahlen α, β, γ aus dem reellen Unterkörper k' vom μ-ten Grade vom Kreiskörper k lösbar ist, so ist

$$E_{\mu-j}=\tilde{\varepsilon}_j^l\,, \qquad (j=1, 2, 3, 4, 5, 6)\,,$$

wobei $\tilde{\varepsilon}_j$ reelle Einheit in k ist.

Es sei $\eta_1, \eta_2, \ldots\ldots, \eta_{\mu-1}$ ein Fundamentalsystem reeller Einheiten mit der Eigenschaft[2]

$$\eta_i^{s-r^{a_i}}=\tilde{\eta}_i^{l^c}\,, \qquad a_i=2il^{c-1}\,, \qquad (i=1, 2, \ldots\ldots, \mu-1)\,, \tag{2}$$

wobei $\tilde{\eta}_i$ gewisse reelle Einheiten in k bedeuten, und

$$\eta_i^{n_i}=\varepsilon(\zeta)^{F_i(s)} \text{ (symbolische Potenz)}, \qquad F_1(s)=\sum_{j=1}^{\mu-1} b_{ij}s^{j-1}\,,$$
$$(i=1, 2, \ldots\ldots, \mu-1)\,,$$

wobei n_i, b_{ij} ganze rationale Zahlen sind und $(n_i, b_{i1}, b_{i2}, \ldots\ldots, b_{i\mu-1})=1$. Setzt man die Determinante $|b_{ij}|=\triangle$, so ist $\triangle\not\equiv 0 \pmod{l}$.[3] Ferner sei h_2 der zweite Faktor der Klassenzahl von k, d.h. die Klassenzahl von k'. Dann gilt

$$h_2=\frac{n_1 n_2\cdots\cdots n_{\mu-1}}{\triangle}\,, \qquad (\triangle, l)=1\,.$$

Wenn E_i l-te Potenz einer Einheit aus k ist, so ist n_i durch l teilbar.[4]

---

1) T. Morishima: Jap. Journ. Math., **11** (1935), Satz 5 (zitiert als T. M.).
2) F. Pollaczek: Math. Zeitschr., **21**, S. 9.
3) H. S. Vandiver: Proc. Nat. Acad. Scie., **16** (1930), S. 747.
4) Ditto.

Hieraus folgt nach Satz A

Satz 1. *Wenn die Gleichung* (1) *durch ganze, zu l relativprime Zahlen α, β, γ aus k' lösbar ist, so ist der zweite Faktor h_2 der Klassenzahl von k durch l^6 teilbar.*

Nun seien x, y, z in $x^l+y^l+z^l=0$ ganze rationale Zahlen und

$$-t\equiv\frac{y}{x},\ \frac{x}{y},\ \frac{z}{y},\ \frac{y}{z},\ \frac{x}{z},\ \frac{z}{x}\qquad (\mathrm{mod}\ l).$$

Dann gilt für hinreichend grosses l und für geeignetes t

$$\left[\frac{d^n\log(1-te^\nu)}{d\nu^n}\right]_{\nu=0}\equiv 0\,,\qquad (n=2, 3, \ldots\ldots, 2[\sqrt[3]{\log l}]+1\qquad (\mathrm{mod}\ l)\tag{3}$$

nicht mehr.[5] Diese Ergebnisse gelten such für t aus der Gleichung (1), wobei

$$-t\equiv\frac{b}{a},\ \frac{a}{b},\ \frac{c}{b},\ \frac{b}{c},\ \frac{a}{c},\ \frac{c}{a}\qquad (\mathrm{mod}\ l)\,,\tag{4}$$

und $\alpha\equiv a$, $\beta\equiv b$, $\gamma\equiv c$ (mod $1-\zeta$) sind.[6] Folglich erhält man

Satz 2.[6] *Wenn für hinreichend grosses l die Gleichung* (1) *durch ganze, zu l relativprime Zahlen α, β, γ aus dem Kreiskörper k lösbar ist, so ist*

$$B_{\mu-i}\equiv 0\,,\qquad (i=1, 2, \ldots\ldots, [\sqrt[3]{\log l}])\,,\qquad (\mathit{mod}\ l)\,.$$

Nun ist[7]

$$(-1)^{i-1}\frac{2^{2i}-1}{2i}B_i=\left[\frac{d^{2i}\log(1+e^\nu)}{d\nu^{2i}}\right]_{\nu=0}=-(1-\theta)\sum_{j=1}^{2i-1}(-1)^j\Delta^j o^{2i-1}\theta^j\,,$$

wobei $\Delta^j o^i=\sum_{k=1}^{j}(-1)^{j-k}\binom{j}{k}k^i$ und $\theta=\frac{1}{2}$ ist, also

$$\frac{2^{2i-1}(2^{2i}-)}{i}B_1=\left|\sum_{j=1}^{2i-1}(-1)^j\Delta^j o^{2i-1}2^{2i-j-1}\right|$$

eine positive ganze Zahl. Es ist aber $\Delta^j o^{2i-1}<2^j j^{2i-1}$, also

$$\left|\sum_{j=1}^{2i-1}(-1)^j\Delta^j o^{2i-1}2^{2i-j-1}\right|<\sum_{j=1}^{2i-1}2^{2i-1}j^{2i-1}<(4i)^{2i}<e^{i^2}<l\,,$$

wenn $6<i<\sqrt{\log l}$ ist. Folglich ist für alle $i\leqq[\sqrt{\log l}]$

$$B_i\not\equiv 0\qquad (\mathrm{mod}\ l)\,,\tag{5}$$

falls l hinreichend gross ist. Nach (3), (4), (5) und Satz 2 kann man in analoger Weise folgenden Satz beweisen, wie bei Satz A:

Satz 3.[8] *Wenn für hinreichend grosses l die Gleichung* (1) *durch ganze, zu l relativprime Zahlen α, β, γ aus k' lösbar ist, so ist für alle $j\leqq[\sqrt[3]{\log l}]$*

$$E_{\mu-j}=\tilde{\varepsilon}_j^l\,,$$

wobei $\tilde{\varepsilon}_j$ reelle Einheit in k ist.

---

5) M. Krasner: C. R. Acad. Sci., Paris, **199** (1934), 256–258. $[\sqrt[3]{\log l}]$ ist die grösste ganze Zahl $<\sqrt[3]{\log l}$.

6) T. M.: 245, Satz 3.

7) M. Krasner: a. a. O., 256–257.

8) T. M.: 246–251.

Nach Satz 3 kann man also in analoger Weise folgenden Satz beweisen, wie bei Satz 1:

Satz 4 (Hauptsatz). *Hat die Gleichung* (1) *für hinreichend grosses l eine Auflösung in ganzen, zu l relativprimen Zahlen α, β, γ vom reellen Unterkörper k' von k, so ist der zweite Faktor h_2 der Klassenzahl von k durch $l^{[\sqrt[3]{\log l}]}$ teilbar.*

Nun kann man in analoger Weise folgenden Satz beweisen, wie bei Hilfssatz 1 und Satz 3 in meiner früheren Arbeit (T. M.)[9]: Ist die Gleichung (1) im Falle I lösbar, so ist für t aus (4)

$$\left[\frac{d^{2n}\log\eta_n(e^\nu)}{d\nu^{2n}}\right]_{\nu=0}\cdot\left[\frac{d^{l-2n}\log(1-te^\nu)}{d\nu^{l-2n}}\right]_{\nu=0}\equiv 0 \pmod{l}, \tag{6}$$

$$(n=1,2,\ldots\ldots,\mu-1).$$

Für $n=\mu-1, \mu-2, \mu-3, \mu-4, \mu-5, \mu-6$ ist der zweite Faktor dieser Formel (6) zu l prim,[10] also nach (6)

$$\left[\frac{d^{2n}\log\eta_n(e^\nu)}{d\nu^{2n}}\right]_{\nu=0}\equiv 0 \pmod{l}. \tag{7}$$

Andererseits ist nach (2) für $m\neq 2n$

$$\left[\frac{d^{m}\log\eta_n(e^\nu)}{d\nu^{m}}\right]_{\nu=0}\equiv 0 \pmod{l}. \tag{8}$$

Nach (7) und (8) ist also η_n primär, wobei $n=\mu-1, \mu-2, \mu-3, \mu-4, \mu-5, \mu-6$ ist. Für hinreichend grosses l gilt die Formel (7) nach (3), (4) und (6) für $n=\mu-1, \mu-2, \ldots\ldots, \mu-[\sqrt[3]{\log l}]$. Hieraus folgt der Satz:

Satz 5. *Ist die Gleichung* (1) *im Falle I durch ganze Zahlen vom Kreiskörper k lösbar, so ist $\eta_{\mu-i}$ für $i=1,2,3,4,5,6$ primär, wobei $\eta_1, \eta_2, \ldots\ldots, \eta_{\mu-1}$ ein Fundamentalsystem reeller Einheiten mit der Eigenschaft* (2) *ist. Dies gilt auch für $i=1,2,\ldots\ldots,[\sqrt[3]{\log l}]$, falls l hinreichend gross ist.*

---

9) Man erhält diesen Satz, indem man ε in der Formel auf T. M. 243 durch η_n ersetzt.
10) T. M.: 246.