92. Über die Fermatsche Vermutung, V.

Von Taro MORISHIMA.
Furitsu Kotogakko, Tokyo.

(Rec. and Comm. by T. TAKAGI, M.I.A., Oct. 13, 1930.)

In der vorliegenden Note bedienen wir uns durchgehend der folgenden Bezeichnungen:

l eine ungerade Primzahl,
ζ die primitive l-te Einheitswurzel,
k der Kreiskörper von ζ,
k_0 der reelle Unterkörper vom $\frac{l-1}{2}$-ten Grade von k,
$h=h_1l^t$ die Klassenzahl von k, $l \nmid h_1$,
$\bar{\alpha}$ die zu α konjugiert komplexe Zahl.

Satz: Für $n \geqq \sigma+t$ ist

$$\alpha^l+\beta^l=\varepsilon\gamma^{l^n}, \qquad (\alpha, \beta, \gamma, l)=1 \tag{1}$$

in ganzen Zahlen α, β, γ von k_0 unlösbar, wo ε Einheit, $\sigma=\frac{l-3}{2}$, $l>31$, für $l \leqq 31$ $n=1$.

Beweis: Bestände (1), so folgte, da $h=h_1l^t$ $(l \nmid h_1)$,

$$\frac{\alpha+\zeta^i\beta}{1+\zeta^i}=\varepsilon_i\omega_i^{l^{n-t}}\equiv\varepsilon_i c \qquad (\text{mod } \lambda^l), \tag{2}$$

$$\frac{\alpha+\zeta^{-i}\beta}{1+\zeta^{-i}}=\bar{\varepsilon}_i\bar{\omega}_i^{l^{n-t}}\equiv\zeta^{m_i}\varepsilon_i c \qquad (\text{mod } \lambda^l), \tag{3}$$

$$\alpha+\beta=\varepsilon_0\omega_0^{l^{n-t}}, \tag{4}$$

wo $\lambda=1-\zeta$, $\bar{\varepsilon}_i=\zeta^{m_i}\varepsilon_i$ Einheit und c rational, also

$$\alpha\zeta^i+\beta\equiv\zeta^{m_i}\alpha+\zeta^{m_i+i}\beta \qquad (\text{mod } \lambda^l). \tag{5}$$

Daher wäre

$$a(1-i\lambda)+b\equiv a(1-m_i\lambda)+b(1-(m_i+i)\lambda) \qquad (\text{mod } \lambda^2),$$

wo $\alpha\equiv a$, $\beta\equiv b$ (mod λ^2), a und b rational, also

$$m_i\equiv\frac{a-b}{a+b}i \qquad (\text{mod } l), \qquad (l \nmid a+b), \tag{6}$$

folglich nach (5) und (6)

$$\beta+\alpha\zeta^{i}-\zeta^{\frac{a-b}{a+b}i}\alpha-\zeta^{\left(\frac{a-b}{a+b}+1\right)i}\beta\equiv 0 \pmod{\lambda^{l}}. \tag{7}$$

Hieraus folgte

$$\varepsilon_i=\bar{\varepsilon}_i\,; \tag{8}$$

denn i) $l=3$: $\frac{a-b}{a+b}\not\equiv 1,\ -1 \pmod 3$,

also $a\equiv b \pmod 3$, d.h. nach (6) $m_i\equiv 0 \pmod 3$.

ii) $l=5$: $\frac{a-b}{a+b}\not\equiv 1,\ -1 \pmod 5$

und ferner $\frac{a-b}{a+b}\not\equiv 2,\ 3$[1] $\pmod 5$, denn sonst wäre wegen (7)

$$\beta(1-\zeta^{3i})+\alpha\zeta^{i}(1-\zeta^{i})\equiv 0 \pmod{\lambda^{5}},$$

also für $i=1, 2, 3$

$$\beta+(\alpha+\beta)\zeta^{i}+\beta\zeta^{2i}\equiv 0 \pmod{\lambda^{4}},$$

folglich

$$\begin{vmatrix} 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta^4 \\ 1 & \zeta^3 & \zeta^6 \end{vmatrix}\equiv 0 \pmod{\lambda^{4}}.$$

Daher wäre $a\equiv b \pmod 5$.

iii) $l\geqq 7$: Aus (7) folgte mit $i=0, 1, 2, 3$

$$(1-\zeta)(1-\zeta^{\frac{a-b}{a+b}})(1-\zeta^{\frac{a-b}{a+b}+1})(\zeta-\zeta^{\frac{a-b}{a+b}})(\zeta-\zeta^{\frac{a-b}{a+b}+1})(1-\zeta)\equiv 0 \pmod{\lambda^{7}},$$

also $a\equiv b \pmod l$.

Folglich wäre nach (2), (3), (4) und (8)

$$\omega_i^{l^{n-t}}+\bar{\omega}_i^{l^{n-t}}=\varepsilon'\omega_0^{l^{n-t}},$$

also

$$2\omega_i^{l^{n-t}}\equiv\varepsilon'\omega_0^{l^{n-t}} \pmod{\lambda l^{n-t}},$$

$$2c_i^{l^{n-t}}\equiv\varepsilon' c_0^{l^{n-t}} \pmod{\lambda l^{n-t}},$$

wo ε' Einheit und c rational, also

$$2^{l-1}c_i^{(l-1)l^{n-t}}\equiv N\varepsilon' c_0^{(l-1)l^{n-t}} \pmod{l^{n-t+1}},$$

$$2^{l-1}\equiv 1 \pmod{l^{n-t+1}},$$

was unmöglich ist.

Speziell für $l\leqq 31$ $t=0$, $2^{l-1}\not\equiv 1 \pmod{l^2}$.

---

1) $\frac{a-b}{a+b}\not\equiv 3$: wie im Beweis zu $\frac{a-b}{a+b}\not\equiv 2$.

Bemerkung: I) Für $n \geqq \max(\sigma, t+1)$ ist

$$\alpha^{l^n}+\beta^{l^n}=\varepsilon\gamma^{l^n}, \qquad (\alpha\beta\gamma, l)=1$$

in ganzen Zahlen α, β, γ von k unlösbar, wo ε Einheit, $\sigma=\frac{l-3}{2}$.

Beweis: Wie im Beweis zu Satz.

Speziell II) für $t=0$, $2^{l-1} \not\equiv 1 \pmod{l^2}$

$$\alpha^l+\beta^l=\varepsilon\gamma^l, \qquad (\alpha\beta\gamma, l)=1$$

in ganzen Zahlen α, β, γ von k unlösbar.