19. Über die Fermatsche Vermutung, VIII.

Von Taro MORISHIMA.
Furitsu Kotogakko, Tokyo.

(Comm. by T. TAKAGI, M.I.A., March 12, 1932.)

Hat die Gleichung

$$x^l+y^l+z^l=0 \tag{1}$$

eine Auflösung in ganzen, durch l nicht teilbaren, relativ primen Zahlen x, y, z, so müssen die sechs Verhältnisse

$$-t=\frac{x}{y},\ \frac{y}{x},\ \frac{z}{x},\ \frac{x}{z},\ \frac{y}{z},\ \frac{z}{y} \tag{2}$$

den Kongruenzen

$$b_i\cdot f_{l-i}(t)\equiv 0 \qquad (i=1, 2, \ldots\ldots, l-2) \qquad \pmod{l}$$

Genüge leisten, wo $f_i(t)=\sum_{r=0}^{l-1} r^{i-1}t^r$, $b_0=1$, $b_1=-\frac{1}{2}$, $b_{2i}=(-1)^{i-1}B_i$, $b_{2i+1}=0$ und B_i die Bernoullischen Zahlen sind; was das sogenannte Kummersche Kriterium und wichtiger Satz ist. Ich will diese Ergebnisse erweitern und den Satz beweisen:

Ist die Gleichung (1) *im Falle I lösbar, so müssen die sechs Verhältnisse* (2) *den Kongruenzen*

$$b_{2i}\cdot f_{2i}(t)\cdot\left[\frac{d^{l(l-2i)}\log\left(1-e^{\nu}(1-t)\right)}{d\nu^{l(l-2i)}}\right]_{\nu=0}\equiv 0 \qquad \pmod{l^2}$$

$$(i=1, 2, \ldots\ldots, \frac{l-3}{2})$$

Genüge leisten.

Es bezeichne nun $\zeta=e^{\frac{2\pi i}{l}}$, und r eine primitive Wurzel (mod l), und $r_i\equiv r^i$ (mod l) den kleinsten positiven Rest von r^i, und $\mathfrak{p}(\zeta)=\mathfrak{p}$ den Primidealteiler der Primzahl $p=1+lk$. Kummer[1] hat gezeigt, dass das Produkt

$$\prod_i \mathfrak{p}(\zeta^{r^i}), \tag{3}$$

ausgedehnt über alle Werte des Index i aus der Reihe $0, 1, \ldots\ldots, l-2$,

1) Vgl. Journal f. Math., **35**, S. 364.

für welche $r_{\frac{l-1}{2}-i}+r_{\frac{l-1}{2}-i+\mathrm{ind}\,d}>l$ ist, unter d einen beliebigen Wert aus der Reihe $1, 2, \ldots\ldots, l-2$ und unter $\mathrm{ind}\,d$ den auf die primitive Wurzel r bezüglichen Index $(\mathrm{mod}\ l)$ verstanden, einem Hauptideale $\psi_d(\zeta)$ gleich ist.

Es ist nach (1)

$$(x+\zeta^i y)=\mathfrak{a}_1^l, \qquad (x+\zeta z)=\mathfrak{a}_2^l, \tag{4}$$

$$x+y=\mathfrak{a}^l, \tag{5}$$

wo $\mathfrak{a}$ ein Ideal des Kreiskörpers $\mathrm{P}(\zeta)$ ist, und nach dem Reziprozitätsgesetz[1]

$$\left(\frac{x+\zeta^i y}{\psi_d(\zeta)}\right)\left(\frac{\psi_d(\zeta)}{x+\zeta^i y}\right)^{-1}=\zeta^{\sum\limits_{s=1}^{l-1}(-1)^s \mathfrak{l}_s(x+\zeta^i y)^{l-1}\cdot\mathfrak{l}_{l-s}(\psi_d(\zeta))^{l-1}}, \tag{6}$$

wo $\left(\frac{\alpha}{\beta}\right)$ der l-te Potenzrestcharakter und

$$\mathfrak{l}_s(\varphi(\zeta))=\left[\frac{d^s\log\varphi(e^v)}{dv^s}\right]_{v=0} \qquad (s=1, 2, \ldots\ldots, l-2),$$

$$\mathfrak{l}_{l-1}(\varphi(\zeta))=\left[\frac{d^{l-1}\log\varphi(e^v)}{dv^{l-1}}\right]_{v=0}+\frac{\varphi(1)-1}{l}$$

ist. Aus (3), (4) und (6) folgt

$$\left(\frac{x+\zeta^i y}{\prod\limits_i \mathfrak{p}(\zeta^{r^i})}\right)=\zeta^{\sum\limits_{s=1}^{l-2}(-1)^s i^s \mathfrak{l}_s(x+\zeta y)\cdot\mathfrak{l}_{l-s}(\psi_d)}, \tag{7}$$

da $\mathfrak{l}_{l-1}(x+\zeta^i y)^{l-1}\equiv 0\ (\mathrm{mod}\ l)$. Wenn $y\equiv 0\ (\mathrm{mod}\ p)$, so ist

$$\left(\frac{x+\zeta^i y}{\prod\limits_i \mathfrak{p}(\zeta^{r^i})}\right)=\left(\frac{x}{\prod\mathfrak{p}}\right),$$

und nach (5)

$$\left(\frac{x+\zeta^i y}{\prod\mathfrak{p}}\right)=\left(\frac{a^l}{\prod\mathfrak{p}}\right)=1.$$

Nach (7) und (8) ist für $i=1, 2, \ldots\ldots, l-1$

$$\sum_{s=1}^{l-2}(-1)^s i^s \mathfrak{l}_s(x+\zeta y)\cdot\mathfrak{l}_{l-s}(\psi_d)\equiv 0 \qquad (\mathrm{mod}\ l),$$

also

$$\mathfrak{l}_s(x+\zeta y)\cdot\mathfrak{l}_{l-s}(\psi_d)\equiv 0 \qquad (s=1, \ldots\ldots, l-2) \qquad (\mathrm{mod}\ l). \tag{9}$$

---

1) Vgl. Hasse, Jahresber. d. D. M. V., Ergänzungsband VI (1930).

Setzt man nun

$$\varepsilon=\sqrt{\frac{1-\zeta^r}{1-\zeta}\cdot\frac{1-\zeta^{-r}}{1-\zeta^{-1}}}, \qquad E_s=\prod_{i=0}^{\frac{l-3}{2}}\varepsilon(\zeta^{r^i})^{r^{-2is}},$$

$$\left(\frac{E_s}{\mathfrak{p}}\right)=\zeta^{\operatorname{ind}_{\mathfrak{p}}E_s}, \qquad D_i=\left[\frac{d^i\log(x+e^\nu y)}{d\nu^i}\right]_{\nu=0},$$

so ist für $s=1, 2, \ldots\ldots, \frac{l-3}{2}$

$$(r^{2s}-1)\mathfrak{l}_{l-2s}(\psi_d)\equiv 2\operatorname{ind}_{\mathfrak{p}}E_s\cdot(1+d^{l-2s}-(d+1)^{l-2s}) \pmod{l}^{1)}$$

also nach (9)

$$D_{2s}\cdot\operatorname{ind}_{\mathfrak{p}}E_s\equiv 0 \pmod{l}$$

da $1+d^{l-2s}-(d+1)^{l-2s}\not\equiv 0 \pmod{l}$. Also ist für $s=1, 2, \ldots\ldots, \frac{l-3}{2}$

$$D_{2s}\cdot\operatorname{ind}_{\mathfrak{a}_2}E_s\equiv 0 \pmod{l} \tag{10}$$

und ferner nach Vandiver[1]

$$(r^{2s}-1)b_{(2s-1)l+1}\cdot\left[\frac{d^{l(l-2s)}\log(x+e^\nu z)}{d\nu^{l(l-2s)}}\right]_{\nu=0}\equiv 2l\operatorname{ind}_{\mathfrak{a}_2}E_s \pmod{l^2} \tag{11}$$

also nach (10) und (11)

$$b_{(2s-1)l+1}\cdot D_{2s}\left[\frac{d^{l(l-2s)}\log(x+e^\nu z)}{d\nu^{l(l-2s)}}\right]_{\nu=0}\equiv 0 \pmod{l^2},$$

folglich

$$b_{2s}\cdot D_{2s}\cdot\left[\frac{d^{l(l-2s)}\log(x+e^\nu z)}{d\nu^{l(l-2s)}}\right]_{\nu=0}\equiv 0 \pmod{l^2},$$

da

$$D_{2s}\cdot\left[\frac{d^{l(l-2s)}\log(x+e^\nu z)}{d\nu^{l(l-2s)}}\right]_{\nu=0}\equiv 0 \pmod{l}.^{2)}$$

---

1) Vgl. Vandiver, Annals of Math., (2), **26** (1925).
2) Vgl. Vandiver, Proc. Nat. Acad. Sci., **11** (1925).