165. Über die Fermatsche Vermutung, X.

Von Taro MORISHIMA.
Furitu Kotogakko, Tokyo.
(Comm. by T. TAKAGI, M.I.A., Dec. 12, 1933.)

Die folgende Arbeit ist eine Untersuchung über die Fermatsche Vermutung im ersten Fall. Es seien

l eine ungerade Primzahl,
k der Kreiskörper der l-ten Einheitswurzel,
$h=l^n q$, $q \not\equiv 0 \pmod{l}$, die Klassenzahl von k,
r eine primitive Wurzel mod l,
ζ eine primitive l-te Einheitswurzel,
s die Substitution $(\zeta : \zeta^r)$ in k.

Wir legen einen allgemeineren Äquivalenzbegriff zugrund und nennen zwei Ideale $\mathfrak{j}$, $\mathfrak{j}'$ in k äquivalent ($\mathfrak{j} \sim \mathfrak{j}'$), wenn im absoluten Sinne $\mathfrak{j}^q$, $\mathfrak{j}'^q$ äquivalent sind; unter „Klasse eines Ideals $\mathfrak{j}$ innerhalb der irregulären Gruppe" können wir einfach die Klasse von $\mathfrak{j}^{qq'}$ ($qq' \equiv 1 \pmod{l^n}$) im absoluten Sinne verstehen. In diesem Sinne gilt:

Satz A.[1] In k läßt sich für die Gruppe der q-ten Potenzen der Idealklassen eine Basis

$$\mathfrak{j}_1, \mathfrak{j}_2, \ldots\ldots, \mathfrak{j}_e,$$

$$\mathfrak{j}_i^{l^{n_i}} \sim 1, \qquad \mathfrak{j}_i^{l^{n_i-1}} \nsim 1 \qquad (i=1,2,\ldots\ldots,e)$$

wählen, derart, daß zugleich auch

$$\mathfrak{j}_i^{s-a_i} \sim 1$$

gilt, wobei a_i gewisse ganze rationale Zahl bedeutet und die der Klasse $\mathfrak{j}_i$ zugehörige Zahl genannt werden soll.

Es seien ferner $\mathfrak{p}_1, \mathfrak{p}_2, \ldots\ldots$ die Ideale derjenigen Klassen $\mathfrak{j}_i$ in Satz A, deren a_i quadratische Nichtreste mod l sind, $\mathfrak{q}_1, \mathfrak{q}_2, \ldots\ldots$ die Ideale der übrigen Klassen aber, deren a_i quadratische Reste mod l sind, und

$$\mathfrak{p}_i^{l^{m_i}} = (\rho_i), \qquad \mathfrak{q}_i^{l^{n_i}} = (\rho_i'),$$

dann sind

$$\rho_i^{s-a_i} = \alpha_i^{l^{m_i}}, \qquad \rho_i'^{s-a_i'} = \alpha_i'^{l^{n_i}}, \tag{1}$$ [2]

---

1) F. Pollaczek: Math. Zeit., **21**, S. 11; T. Morishima: Jap. Journ. Math., Vol. **10** (1933).

2) F. Pollaczek: a.a.O., S. 20.

wobei $a_i = r^{(2k+1)l^{m_i-1}}$, $a'_i = r^{2k'l^{n_i-1}}$ sind.

Nun sei für ganze rationale Zahlen x, y, z

$$x^l + y^l + z^l = 0\,, \qquad (x, y, z, l) = 1\,,$$

dann ist

$$(x + \zeta y) = \mathfrak{a}^l\,,$$

wobei ζ die primitive l-te Einheitswurzel und $\mathfrak{a}$ ein Ideal in k ist. Nach Satz A ist

$$\mathfrak{a}^q = (\alpha) \prod_{i=1}^{t_1} \mathfrak{p}_i^{b_i} \prod_{i=1}^{t_0} \mathfrak{q}_i^{c_i}\,,$$

wobei t_1, t_0 die Anzahl der Klassen $\mathfrak{p}$ bzw. $\mathfrak{q}$ bedeuten, also

$$(x + \zeta y)^q = \varepsilon \prod_{i=1}^{t_1} \rho_i^{b'_i} \prod_{i=1}^{t_0} \rho_i'^{c'_i} \alpha^l\,, \tag{2}$$

wobei ε eine Einheit in k ist.

Nun ist $t' = t_1 - t_0$ die Anzahl[3] der Nichtprimärzahlen aus ρ_i in (1) und es seien

$$\rho_1,\ \rho_2,\ \ldots\ldots,\ \rho_{t'} \tag{3}$$

diese Nichtprimärzahlen, deren zugehörige Zahlen

$$r^{d_i} \qquad (i = 1, 2, \ldots\ldots, t') \tag{4}$$

sind. Ist $t' < 6$, so gibt es in r^3, r^5, r^7, r^9, r^{11}, r^{13} mindestens eine Zahl r^j, welche mit keiner der diesen Klassen in (3) zugehörigen Zahlen r^{d_i} mod l kongruent ist, d.h.

$$r^j \not\equiv r^{d_i} \qquad (\mathrm{mod}\ l) \qquad (i = 1, 2, \ldots\ldots, t') \tag{5}$$

ist.

Aus (1) und (2) folgt

$$(x + \zeta y)^{q\Pi(s - r^{d_i})} \equiv \zeta^f \rho'' a \qquad (\mathrm{mod}\ l)\,.$$

wobei das Produkt sich auf alle d_i aus (4) bezieht, ρ'' reelle Zahl in k und a ganze rationale Zahl ist. Folglich ist für $3 \leqq j \leqq 13$

$$q \Pi (r^j - r^{d_i}) \left[\frac{d^j \log (x + e^{\nu} y)}{d\nu^j} \right]_0 \equiv 0 \qquad (\mathrm{mod}\ l)\,,$$

da j ungerade Zahl ist, also nach (5)

$$\left[\frac{d^j \log (x + e^{\nu} y)}{d\nu^j} \right]_0 \equiv 0 \qquad (\mathrm{mod}\ l)$$

für $3 \leqq j \leqq 13$, was aber unmöglich[4] ist.

3) T. Takagi: Crelles Journ., **157**.

4) T. Morishima: Proc. **8** (1932), S. 64–65.
D. H. Lehmer: Bull. Amer. Math. Soc., **38**, S. 723–724 (1932).

Hieraus folgt der Satz:

Satz. *Es seien t_1, t_0 die Range der Gruppen der q-ten Potenzen der Klassen des Kreiskörpers $R(\zeta)$ bzw. des reellen Unterkörpers $R(\zeta+\zeta^{-1})$ von $R(\zeta)$, wobei R rationalen Körper darstellt. Ist $t_1-t_0<6$, so ist*

$$x^l+y^l+z^l=0\,, \qquad (x, y, z, l)=1$$

durch ganze rationale Zahlen x, y, z unlösbar.