ACTA ARITHMETICA
XI (1965)

Eine Bemerkung zur Fermatschen Vermutung

von

M. EICHLER (Basel)

Diese Zeilen enthalten einen Beweis für die folgende Tatsache, wobei auf frühere Ansätze nicht zurückgegriffen wird:

Es sei $l > 3$ eine Primzahl. Die Gleichung

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

besitzt keine Lösung in ganzen rationalen zu 1 *teilerfremden Zahlen, wenn die genaue im* 1. *Faktor der Klassenzahl des l-ten Kreiskörpers enthaltene Potenz*

$$l^H < l^r, \quad r = [\sqrt{l}] - 1 \tag{2}$$

ist.

Unter der Voraussetzung sind bekanntlich $(x + \zeta^i y) = \mathfrak{a}_i^l$ l-te Potenzen ganzer Ideale des Kreiskörpers, wo ζ eine primitive l-te Einheitswurzel bedeutet. Man bildet nun die l^r Potenzprodukte $\mathfrak{a}_1^{a_1} \ldots \mathfrak{a}_r^{a_r}$ mit $0 \leqslant a_i < l$. Sie verteilen sich auf die l^H Relativklassen bzgl. des größten reellen Unterkörpers, deren Ordnungen Potenzen von l sind; und die Anzahl der Relativklassen ist bekanntlich der erste Faktor der Klassenzahl. Mittels des Schubfachprinzips entnimmt man der Voraußetzung (2): es gibt ganze rationale a_i, welche nicht sämtlich Null sind und den Ungleichungen $|a_i| < l$ genügen, sodaß $\mathfrak{a}_1^{a_1} \ldots \mathfrak{a}_r^{a_r}$ mit einem Ideal des reellen Unterkörpers äquivalent ist. Das läßt sich wegen der Bedeutung der $\mathfrak{a}_i$ so formulieren:

$$\prod_{i=1}^{r} (x + \zeta^i y)^{a_i} = \zeta^\mu \varepsilon \alpha \varrho^l \tag{3}$$

mit einer Zahl ϱ des Kreiskörpers, einer Zahl α des reellen Unterkörpers, welche beide in Zähler und Nenner zu l teilerfremd sind, und mit einer Einheit ε. Nach dem Dirichletschen Einheitensatz sind alle Einheiten Produkte reeller Einheiten mit Potenzen von ζ. Man darf daher in (3) ε als reell voraussetzen.

In (3) wendet man den Automorphismus $\zeta \to \bar{\zeta} = \zeta^{-1}$ an und dividiert (3) durch die so entstehende Gleichung. Da $\varrho^l \bmod l$ einer rationalen Zahl kongruent ist, erhält man

$$\prod_{i=1}^{r} \left(\frac{x+\zeta^i y}{y+\zeta^i x}\right)^{a_i} \equiv \zeta^{\nu} \bmod l, \qquad \nu = 2\mu - \sum_{i=1}^{r} i a_i. \tag{4}$$

Man setzt hier

$$x_i = \begin{cases} y & \text{für} \quad a_i < 0, \\ x & \text{für} \quad a_i \geqslant 0, \end{cases} \qquad y_i = \begin{cases} x & \text{für} \quad a_i < 0, \\ y & \text{für} \quad a_i \geqslant 0, \end{cases}$$

$$F(\zeta) = \prod_{i=1}^{r} (x_i + \zeta^i y_i)^{|a_i|}, \qquad G(\zeta) = \prod_{i=1}^{r} (y_i + \zeta^i x_i)^{|a_i|}.$$

und kann dann (4) so schreiben:

$$F(\zeta) \equiv \zeta^{\nu} G(\zeta) \bmod l. \tag{5}$$

Weil $1, \zeta, \ldots, \zeta^{l-1}$ eine Ganzheitsbasis bilden, bedeutet (5)

$$F(\zeta) = \zeta^{\nu} G(\zeta) + l K(\zeta)$$

mit einem ganzzahligen Polynom $(l-1)$-ten Grades $K(\zeta)$. Diese Gleichung läßt sich als eine Identität zwischen Polynomen in einer Unbestimmten ξ schreiben:

$$F(\xi) = \xi^{\nu} G(\xi) + (1 + \xi + \ldots + \xi^{l-1}) H(\xi) + l K(\xi). \tag{6}$$

Wendet man den Gausschen Satz auf das Produkt $(1+\ldots+\xi^{l-1})H(\xi)$ an, so erkennt man, daß $H(\xi)$ ganze rationale Koeffizienten hat.

Man multipliziert beide Seiten von (6) mit $1-\xi$ und differenziert sie nach ξ. Das liefert zunächst die Kongruenz für Polynome

$$\begin{aligned}(1-\xi)F'(\xi) - F(\xi) \\ \equiv (1-\xi)\xi^{\nu} G'(\xi) - \xi^{\nu} G(\xi) + \nu(1-\xi)\xi^{\nu-1} G(\xi) + (1-\xi^l) H'(\xi) \bmod l\end{aligned}$$

und sodann

$$(1-\zeta)F'(\zeta) - F(\zeta) \equiv (1-\zeta)\zeta^{\nu} G'(\zeta) - \zeta^{\nu} G(\zeta) + \nu(1-\zeta)\zeta^{\nu-1} G(\zeta) \bmod l.$$

Nach Division durch (5) erhält man hieraus

$$(1-\zeta) \sum_{i=1}^{r} i a_i \left(\frac{y}{y+\zeta^i x} - \frac{x}{x+\zeta^i y}\right) \equiv \nu(1-\zeta) \bmod l. \tag{7}$$

Durch formales Ausmultiplizieren mit

$$f(\zeta) = \prod_{i=1}^{r} (x+\zeta^i y)(y+\zeta^i x)$$

entstehen auf beiden Seiten von (7) Polynome in ζ, deren Grad voraussetzungsgemäß $r(r+1)+1 < l-1$ ist. Aus dem Grunde entsteht so eine Kongruenz, welche für eine Unbestimmte ξ anstelle von ζ gilt, und dann ist auch (7) mit einer Unbestimmten ξ anstelle von ζ richtig.

Entwickelt man nun die linke Seite in eine Potenzreihe nach ξ, so kommt man unter Benutzung der Abkürzung $u = xy^{-1}$ auf

$$\begin{aligned}(1-\xi)(u-u^{-1})\{s a_s(-\xi^s + (u+u^{-1})\xi^{2s} + \ldots) + (s+1) a_{s+1}(-\xi^{s+1} + \ldots)\} \\ \equiv (1-\xi)\nu \bmod l,\end{aligned}$$

wo s den kleinsten Index bedeutet, für welchen $a_s \neq 0$ ist. Daraus entnimmt man $\nu \equiv u - u^{-1} \equiv 0 \bmod l$ oder

$$x \equiv \pm y \bmod l.$$

Aus Symmetriegründen ist auch $y \equiv \pm z \bmod l$. Für $l > 3$ ist das nicht möglich.

Reçu par la Rédaction le 23. 9. 1964