Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 24 (1950)

Artikel: Eulersche Zahlen und großer Fermat'scher Satz.
Autor: Gut, Max
DOI: https://doi.org/10.5169/seals-20301

Eulersche Zahlen und großer Fermat'scher Satz

Von Max Gut, Zürich

1. Inhaltsangabe

D. Mirimanoff hat im Jahre 1905 in einer Arbeit [4][1]) gezeigt, daß die Gleichung

$$x^l + y^l = z^l \,, \tag{1.1}$$

wo l eine ungerade Primzahl bedeutet, keine Lösung in ganzen rationalen, zu l teilerfremden Zahlen x, y und z hat, wenn wenigstens eine der Bernoullischen Zahlen B_{l-3}, B_{l-5}, B_{l-7} und B_{l-9} nicht durch l teilbar ist.

In einer weiteren Arbeit, auf die mich Herr Professor *H. S. Vandiver* in freundlichster Weise aufmerksam machte, wurde diese Aussage von *T. Morishima* [5] im Jahre 1932 auf B_{l-11} und unter der Voraussetzung, daß $20579903 \cdot 75571 \not\equiv 0 \pmod{l}$ ist, weiter auf B_{l-13} ausgedehnt.

Bekanntlich hat aber *B. Rosser* [7] im Jahre 1939 gezeigt, daß der erste Fall des großen Fermatschen Satzes nur möglich ist, wenn $l \geqq 8332403$ und in einer weiteren Arbeit [8] schon 1940, wenn $l > 41000000$ ist, so daß die Restriktion bezüglich B_{l-13} bei der eben erwähnten Arbeit von *T. Morishima* dahinfällt.

Weiter zeigten *D. H. Lehmer* und *Emma Lehmer* [3] im Jahre 1941, daß der erste Fall des großen Fermatschen Satzes nur möglich ist, wenn $l > 253747889$ ist.

Mit Rücksicht auf den engen Zusammenhang zwischen den Bernoullischen und den Eulerschen Zahlen kann man sich fragen, welche Bedeutung die letzteren für den großen Fermatschen Satz haben. Im folgenden zeige ich, daß wenn die Gleichung

$$X^{2l} + Y^{2l} = Z^{2l} \tag{1.2}$$

eine Lösung in ganzen rationalen zu l teilerfremden Zahlen hat, zu den *Kummer-Mirimanoff*schen Kongruenzen in einer der drei Formen[2])

[1]) Vergleiche die entsprechenden Nummern im Literaturverzeichnis am Ende der vorliegenden Arbeit.

[2]) Vergleiche die Formeln in der vorliegenden Arbeit in Abschnitt 9 und 10.

(9.4) bzw. (9.5) und (9.6) bzw. (10.1) ganz analoge Kongruenzen treten, nämlich (9.8) bzw. (9.7) bzw. (10.2), wobei in den beiden ersten Formen analog die Eulerschen an Stelle der Bernoullischen Zahlen auftreten.

Ferner beweise ich den zum erwähnten Satze von *Mirimanoff* analogen *Satz*: Die Gleichung (1.2) hat keine Lösung in ganzen rationalen zu l teilerfremden Zahlen X, Y und Z, wenn wenigstens eine der Eulerschen Zahlen E_{l-3}, E_{l-5}, E_{l-7}, E_{l-9} und E_{l-11} nicht durch l teilbar ist.

In bezug auf die Teilbarkeit der Zahlen X, Y und Z durch 2 beachte man, daß wenn für (1.2) eine Lösung in nicht verschwindenden ganzen rationalen zueinander teilerfremden Zahlen existiert, notwendigerweise eine der beiden Zahlen X und Y gerade, die andere und übrigens auch Z ungerade sind.

Zu unserem Satze sind aber sofort zwei Bemerkungen zu machen.

Erstens hat *E. E. Kummer* [2] in einer im Oktober 1835 geschriebenen und im Jahre 1837 publizierten Arbeit schon gezeigt, daß der erste Fall bei der Gleichung (1.2) höchstens dann möglich ist, wenn $l \equiv 1 \pmod 8$ ist. Ich werde aber im folgenden von dieser Erkenntnis *Kummer*s keinen Gebrauch machen, d. h. l soll in der vorliegenden Arbeit eine beliebige ungerade Primzahl bedeuten dürfen, da sich mir eine Fallunterscheidung nicht aufdrängte, und eine Reihe von Relationen an sich von Interesse und vielleicht bei anderen Untersuchungen von Nutzen sind, wo man nicht wünscht, die erwähnte Restriktion für l vorauszusetzen.

Zweitens hat *H. S. Vandiver* [11] im Jahre 1940 schon gezeigt, daß sogar die Gleichung (1.1) keine Lösung in ganzen rationalen Zahlen x, y, z, mit $xyz \not\equiv 0 \pmod l$ haben kann, wenn E_{l-3} nicht durch l teilbar ist.

2. Bezeichnungen

In der ganzen vorliegenden Arbeit bedeute immer l eine beliebige ungerade Primzahl, k_0 den Körper der rationalen Zahlen, $\zeta = e^{\frac{2\pi i}{l}}$ die primitive l-te Einheitswurzel und $k = k_0(\zeta)$ den Körper der l-ten Einheitswurzeln. Die Zahlen von k bezeichne ich mit griechischen Minuskeln, die Ideale von k mit Frakturminuskeln. Ferner bedeute r eine Primitivzahl mod. l, S den erzeugenden Automorphismus von k, also $\zeta^S = \zeta^r$, $\lambda = 1 - \zeta$ den Primteiler von l in k und $\mathfrak{l}$ das Primideal von k, das λ teilt, so daß $l = \mathfrak{l}^{l-1}$.

Den erzeugenden Automorphismus des Gaußschen Zahlkörpers $k_0(i)$ bezeichne ich mit Σ, also $i^\Sigma = -i$, das Kompositum von k und $k_0(i)$ mit $K = k(i) = k_0(i, \zeta)$. Die Zahlen von K seien durch griechische Ma-

juskeln, die Ideale von K durch Frakturmajuskeln angedeutet. Im Falle $l \equiv 1 \pmod 4$ seien $\mathfrak{L}_1$ und $\mathfrak{L}_2$ die voneinander verschiedenen Primideale von K, die $\mathfrak{l}$ teilen, so daß $\mathfrak{l} = \mathfrak{L}_1 \cdot \mathfrak{L}_2$, im Falle $l \equiv 3 \pmod 4$ sei $\mathfrak{L}$ das Primideal von K, das $\mathfrak{l}$ teilt, so daß $\mathfrak{l} = \mathfrak{L}$.

Ist M eine zum Ideal $\mathfrak{J}$ bzw. μ eine zum Ideal $\mathfrak{j}$ teilerfremde Zahl, wo $(\mathfrak{J}, l) = (\mathfrak{j}, l) = 1$ ist, so bedeute $\left(\frac{M}{\mathfrak{J}}\right)_K$ den l-ten Potenzcharakter in K, $\left(\frac{\mu}{\mathfrak{j}}\right)_k$ den l-ten Potenzcharakter in k. Für beliebiges $\mathfrak{J}$ bzw. $\mathfrak{j}$ sei das Hilbertsche Normenrestsymbol in K mit $\left(\frac{N, M}{\mathfrak{J}}\right)_K$, das Hilbertsche Normenrestsymbol in k mit $\left(\frac{\nu, \mu}{\mathfrak{j}}\right)_k$ bezeichnet.

3. Die *Takagi*sche Form des Reziprozitätsgesetzes der l-ten Potenzreste in K

Für zu l teilerfremde Zahlen M, N bzw. μ, ν sei

$$\left.\begin{aligned} \{M, N\}_K &= \left(\frac{N, M}{\mathfrak{L}_1}\right)_K \left(\frac{N, M}{\mathfrak{L}_2}\right)_K, \quad \text{falls } l \equiv 1 \pmod 4 \\ \{M, N\}_K &= \left(\frac{N, M}{\mathfrak{L}}\right)_K, \quad \text{falls } l \equiv 3 \pmod 4 \end{aligned}\right\} \tag{3.1}$$

$$\{\mu, \nu\}_k = \left(\frac{\nu, \mu}{\mathfrak{l}}\right)_k .$$

Fehlt bei einer geschweiften Klammer der Index, so ist immer das Symbol in K gemeint:

$$\{M, N\} = \{M, N\}_K .$$

Dann gelten, vergleiche generell *Takagi* [9], die Rechenregeln:

$$\begin{aligned} &\{M, M\}_K = 1 \\ &\{M, N\}_K = \{N, M\}_K^{-1} \\ &\{MM', N\}_K = \{M, N\}_K \cdot \{M', N\}_K \\ &\{M, NN'\}_K = \{M, N\}_K \cdot \{M, N'\}_K . \end{aligned} \tag{3.2}$$

Für zwei zueinander und zu l teilerfremde Zahlen M, N von K bzw. μ, ν von k ist weiter

$$\{M, N\}_K = \left(\frac{M}{N}\right)_K \left(\frac{N}{M}\right)_K^{-1} \tag{3.3}$$

$$\{\mu, \nu\}_k = \left(\frac{\mu}{\nu}\right)_k \left(\frac{\nu}{\mu}\right)_k^{-1}, \tag{3.4}$$

endlich gemäß Satz 10, *Takagi* [9], S. 24, für zueinander und zu l teilerfremde Zahlenpaare M, N bzw. M', N':

$$\{M', N'\}_K = \{M, N\}_K \ , \quad \text{falls} \begin{Bmatrix} M' \equiv M \\ N' \equiv N \end{Bmatrix} (\text{mod. } \lambda^l) \ .$$

Analog zu *Takagi* [10], S. 231, führen wir die $2(l-1)$ Basisgrößen für die Restklassen mod λ^l von K:

$$\left.\begin{array}{l} K_u \equiv 1 - \lambda^u \,(\text{mod } \lambda^{u+1}) \ , \quad K_u^{S-r^u} \equiv 1 \,(\text{mod } \lambda^l) \\ \text{und} \\ K_u^* \equiv 1 - i\lambda^u \,(\text{mod } \lambda^{u+1}) \ , \quad K_u^{*S-r^u} \equiv 1 \,(\text{mod } \lambda^l) \end{array}\right\} u = 1, 2, \ldots, l-1 \ ,$$

ein, die zum Beispiel durch

$$\left.\begin{array}{l} K_u \equiv (1 - \lambda^u)^{-r^u \frac{S^{l-1} - r^{l-1}}{S - r^u}} \\ K_u^* \equiv (1 - i\lambda^u)^{-r^u \frac{S^{l-1} - r^{l-1}}{S - r^u}} \end{array}\right\} (\text{mod } \lambda^l) \ , \ u = 1, 2, \ldots, l-1 \ ,$$

gegeben werden können, wobei man für $u = 1$ direkt $K_1 = \zeta$ und für $u = l - 1$ direkt $K_{l-1} = 1 + l$ und $K_{l-1}^* = 1 + il$ nehmen darf. Da diese Basisgrößen nur mod. λ^l bestimmt sind, kann man immer erreichen, daß sie je zu zweit zueinander teilerfremd sind; übrigens sind sie mod λ^l eindeutig bestimmt.

Wir bestimmen nun zunächst unter Anwendung der eben angegebenen Rechenregeln für das Symbol $\{M, N\}_K$ den Wert dieses Symbols für je zwei Basisgrößen.

Sind u und v zwei beliebige Zahlen der Reihe $1, 2, \ldots, l-1$, so ist $\{K_u, K_v\}_K = 1$, wenn $u = v$ ist. Für $u \neq v$ ist gemäß den Definitionen (3.3) und (3.4) und Satz 5 oder 6, S. 9—10, *Takagi* [9], falls man K_u und K_v in k wählt:

$$\{K_u, K_v\}_K = \left(\frac{K_u}{K_v}\right)_K \left(\frac{K_v}{K_u}\right)_K^{-1} = \left(\frac{K_u}{K_v}\right)_k^2 \left(\frac{K_v}{K_u}\right)_k^{-2} = \{K_u, K_v\}_k^2 \ .$$

Mithin gilt allgemein, vergleiche Formeln (6) und (7), *Takagi* [10], S. 231:

$$\left.\begin{aligned}\{K_u, K_v\}_K &= \zeta^{2v},\ u+v=l\\ \{K_u, K_v\}_K &= 1\quad ,\ u+v\neq l\end{aligned}\right\} u, v = 1, 2, \ldots, l-1\ . \tag{3.5}$$

Für beliebiges u und v aus der Reihe $1, 2, \ldots, l-1$ wird weiter:

$$\{K_u^S, K_v^{*S}\}_K = \{K_u, K_v^*\}_K^r = \{K_u, K_v^*\}_K^{r^{u+v}},$$

mithin ist dieses Symbol gleich 1, wenn $u+v \neq l$ ist.

Ferner ist, da man K_u in k annehmen darf:

$$\{K_u, K_{l-u}^*\}_K^2 = \{K_u, K_{l-u}^*\}_K \cdot \{K_u, K_{l-u}^{*\Sigma}\}_K = \{K_u, K_{l-u}^{*1+\Sigma}\}_K =$$

$$= \left\{ K_u, (1+\lambda^{2l-2u})^{-r^{l-u}\frac{S^{l-1}-r^{l-1}}{S-r^{l-u}}} \right\}_K .$$

Da man, wie eben bemerkt, annehmen darf, daß K_u in k liegt, kann dieses Symbol gemäß (3.5) höchstens dann einen von 1 verschiedenen Wert haben, wenn für nicht negatives ganzes rationales x die Gleichung besteht:

$$u + 2l - 2u + x = l\ .$$

Das bedeutet aber $x = u - l$, welche Gleichung nicht erfüllt ist.

Folglich ist

$$\left.\begin{aligned}\{K_u, K_v^*\}_K = \{K_u, K_v^{*\Sigma}\}_K = \{K_u, K_v^{*1+\Sigma}\}_K = \{K_u, K_v^{*1-\Sigma}\}_K = 1\\ \text{für beliebiges } u, v = 1, 2, \ldots, l-1\ .\end{aligned}\right\} \tag{3.6}$$

Ferner ist

$$\{K_u^{*S}, K_v^{*S}\}_K = \{K_u^*, K_v^*\}_K^r = \{K_u^*, K_v^*\}_K^{r^{u+v}},$$

so daß

$$\{K_u^*, K_v^*\}_K = 1, \text{ wenn } u+v \neq l \text{ ist.} \tag{3.7}$$

Es ist mithin nur noch der Wert dieses Symbols für $u+v=l$ zu bestimmen.

Wir bestimmen zuerst $\{K_1^*, K_{l-1}^*\}_K$. Um die Betrachtungen weiter unten nicht unterbrechen zu müssen, schicken wir folgende Bemerkungen voraus.

Es sei zur Abkürzung

$$l \cdot u(x) = \binom{l}{1} x^{\frac{l-3}{2}} + \binom{l}{3} x^{\frac{l-5}{2}} + \cdots + \binom{l}{l-4} x + \binom{l}{l-2}$$

und

$$l \cdot g(x) = \binom{l}{2} x^{\frac{l-3}{2}} + \binom{l}{4} x^{\frac{l-5}{2}} + \cdots + \binom{l}{l-3} x + \binom{l}{l-1} \tag{3.8}$$

gesetzt, so daß $u(x)$ und $g(x)$ ganzrationalzahlige Polynome sind. Dann hat das normierte ganzrationalzahlige Polynom:

$$[(x-1)^{\frac{l-1}{2}} + l \cdot g(x-1)]^2 - (x-1)[l \cdot u(x-1)]^2$$

vom Grade $l-1$ die Nullstelle $\xi = 1 + \lambda^2 = 1 + (1-\zeta)^2$.

In der Tat wird

$$\begin{aligned}
&[(\xi-1)^{\frac{l-1}{2}} + l \cdot g(\xi-1)]^2 - (\xi-1)[l \cdot u(\xi-1)]^2 \\
&= [\lambda^{l-1} + l \cdot g(\lambda^2)]^2 - \lambda^2 [l \cdot u(\lambda^2)]^2 \\
&= [\lambda^{l-1} + l \cdot g(\lambda^2) + \lambda l \cdot u(\lambda^2)]\,[\lambda^{l-1} + l \cdot g(\lambda^2) - \lambda l \cdot u(\lambda^2)] \\
&= \frac{1}{\lambda^2}[\lambda^l + \lambda l \cdot g(\lambda^2) + \lambda^2 l \cdot u(\lambda^2)]\,[\lambda^l + \lambda l \cdot g(\lambda^2) - \lambda^2 l \cdot u(\lambda^2)] \\
&= \frac{1}{\lambda^2}[(\lambda+1)^l - 1]\,[(\lambda-1)^l + 1]
\end{aligned}$$

und hier ist der zweite Faktor gleich 0.

Bedeutet daher n die absolute Norm in k, so wird

$$n(\xi) = n(1+\lambda^2) = [(-1)^{\frac{l-1}{2}} + l \cdot g(-1)]^2 + [l \cdot u(-1)]^2 ,$$

also

$$n(1+\lambda^2) \equiv 1 + 2(-1)^{\frac{l-1}{2}} l \cdot g(-1) \pmod{l^2}$$

und daher

$$\frac{n(1+\lambda^2)-1}{l} \equiv 2(-1)^{\frac{l-1}{2}} \cdot g(-1) \pmod{l} .$$

Folglich wird wegen:

$$\left(\frac{\zeta}{1+\lambda^2}\right)_k = \zeta^{\frac{n(1+\lambda^2)-1}{l}}$$

$$\left(\frac{\zeta}{1+\lambda^2}\right)_k = \zeta^{2(-1)^{\frac{l-1}{2}} \cdot g(-1)} . \tag{3.9}$$

Wir betrachten die echte Erweiterung von K zu $K(\sqrt[l]{1-\lambda+il})$.

Bedeutet N die Relativnorm von $K(\sqrt[l]{1-\lambda+il})$ zu K, so wird

$$N(1-i^l+i^l\cdot\sqrt[l]{1-\lambda+il}) = (1-i^l)^l + i(1-\lambda+il)$$
$$= 1-i\lambda-l+[(1-i^l)^l-1+i]$$

oder

$$N(1-i^l+i^l\sqrt[l]{1-\lambda+il}) = 1-i\lambda-l+(A+Bi)\,l\ , \quad (3.10)$$

mit ganzen rationalen A und B.

Hierbei interessiert uns nur der Wert von A. Es ist

$$2lA = (1-i^l)^l - 1 + i + (1+i^l)^l - 1 - i\ ,$$

also

$$lA = -\binom{l}{2}+\binom{l}{4}-\binom{l}{6}+-\cdots+(-1)^{\frac{l-1}{2}}\binom{l}{l-1}.$$

Gemäß Formel (3.8) wird

$$lA = (-1)^{\frac{l-1}{2}}\cdot l\cdot g(-1)\ ,$$

mithin

$$A = (-1)^{\frac{l-1}{2}}\, g(-1)\ ,$$

so daß sich (3.9) mit Hilfe der in (3.10) definierten ganzen rationalen Zahl A so schreiben läßt:

$$\left(\frac{\zeta}{1+\lambda^2}\right)_k = \zeta^{2A}\ . \quad (3.11)$$

Aus (3.10) und dem allgemeinen Reziprozitätsgesetz folgt:

$$\{1-\lambda+il\ ,\ 1-i\lambda-l+(A+Bi)\,l\}_K = 1\ ,$$

und daraus läßt sich jetzt vermöge (3.11) leicht der Wert von $\{K_1^*, K_{l-1}^*\}_K$ bestimmen[3]). In der Tat folgt unter Benutzung der schon hergeleiteten Formeln (3.5), (3.6) und (3.7):

---

[3]) Vergleiche zur letzten Formel und dem folgenden die Ausführungen bei *Takagi* [10].

$$\{\zeta K_{l-1}^*, (1-i\lambda)(1-l)(1+Al)(1+Bil)\}_K = 1 ,$$

also

$$\{\zeta, (1-i\lambda)(1-l)(1+Al)(1+Bil)\}_K \times$$

$$\times \{K_{l-1}^*, (1-i\lambda)(1-l)(1+Al)(1+Bil)\}_K = 1 ,$$

d. h.

$$\{\zeta, 1-i\lambda\}_K \cdot \zeta^2 \cdot \zeta^{-2A} \cdot \{K_{l-1}^* , 1-i\lambda\}_K = 1 ,$$

oder

$$\left(\frac{\zeta}{1-i\lambda}\right)_K \cdot \zeta^{2-2A} \cdot \{K_{l-1}^* , K_1^*\}_K = 1 .$$

Folglich wird wegen Satz 5, S. 9—10, *Takagi* [9]:

$$\{K_1^* , K_{l-1}^*\}_K = \zeta^{2-2A} \cdot \left(\frac{\zeta}{1+\lambda^2}\right)_k ,$$

also vermöge (3.11):

$$\{K_1^* , K_{l-1}^*\}_K = \zeta^2 = \zeta^{-2(l-1)} . \tag{3.12}$$

Aus dieser Formel erhält man jetzt aber sofort den Wert von $\{K_u^*, K_{l-u}^*\}_K$ für jeden Wert von u.

Es sei zunächst im folgenden $1 < u < \frac{l}{2}$, $u+v=l$, also $\frac{l}{2} < v < l-1$.

Es sei ferner Λ eine beliebige ganze Zahl von K mit der Eigenschaft

$$\Lambda \equiv \lambda \pmod{\lambda^2} ,$$

und wir betrachten die echte Körpererweiterung von K zu $K(\sqrt[l]{1-i\Lambda})$.

Bedeutet N die Relativnorm von $K(\sqrt[l]{1-i\Lambda})$ zu K, so wird

$$N(1-\sqrt[l]{1-i\Lambda}) = i\Lambda ,$$

und daher ist die Zahl $(1-\sqrt[l]{1-i\Lambda})^l$, falls $l \equiv 1 \pmod 4$ ist, genau durch $\mathfrak{L}_1$ und $\mathfrak{L}_2$, falls $l \equiv 3 \pmod 4$ ist, genau durch $\mathfrak{L}$ und durch keine höhere Potenz dieser Ideale teilbar. Es wird mithin:

$$N\left(1 - i^{l(1-v)}(1-\sqrt[l]{1-i\Lambda})^v\right) \equiv 1 - i^{l(1-v)}\, l - i\Lambda^v \pmod{\lambda^l} .$$

Folglich wird:

$$\{1-i\Lambda , 1 - i^{l(1-v)}\, l - i\Lambda^v\}_K = 1 . \tag{3.13}$$

Insbesondere wird erstens für $\Lambda = \lambda$:

$$\{1 - i\lambda\ ,\ 1 - i\lambda^v - i^{l(1-v)}\, l\}_K = 1\ . \tag{3.14}$$

Zweitens wird für ein durch

$$1 - i\Lambda \equiv (1 - i\lambda)\, K_u^* \pmod{\lambda^l}$$

bestimmtes ganzzahliges Λ:

$$1 - i\Lambda \equiv (1 - i\lambda)(1 - i\lambda^u) \pmod{\lambda^{u+1}}\ ,$$

also

$$1 - i\Lambda \equiv 1 - i\lambda - i\lambda^u \pmod{\lambda^{u+1}}\ ,$$

folglich

$$\Lambda \equiv \lambda(1 + \lambda^{u-1}) \pmod{\lambda^{u+1}}\ ,$$

mithin für geeignetes ganzes Γ aus K:

$$\Lambda \equiv \lambda(1 + \lambda^{u-1} + \Gamma\lambda^u) \pmod{\lambda^l}\ .$$

Daher wird

$$\Lambda^v \equiv \lambda^v(1 + v\,\lambda^{u-1}) \equiv \lambda^v + v\,\lambda^{l-1} \equiv \lambda^v - vl \pmod{\lambda^l}\ .$$

Folglich wird nach (3.13):

$$\{(1 - i\lambda)\, K_u^*\ ,\ 1 - i\lambda^v - i^{l(1-v)}\, l + ivl\}_K = 1\ ,$$

also

$$\{(1 - i\lambda)\, K_u^*\ ,\ (1 - i\lambda^v - i^{l(1-v)}\, l)\,(1 + ivl)\}_K = 1\ .$$

Wegen (3.14) wird:

$$\{1 - i\lambda,\ 1 + ivl\}_K\, \{K_u^*,\ 1 - i\lambda^v - i^{l\,(1-v)}\, l\}_K\, \{K_u^*,\ 1 + ivl\}_K = 1\ ,$$

und weiter:

$$\{1 - i\lambda, K_{l-1}^*\}_K^v\, \{K_u^*, 1 - i\lambda^v\}_K\, \{K_u^*, 1 - i^{l(1-v)}\, l\}_K\, \{K_u^*, K_{l-1}^*\}_K^v = 1\ .$$

Wegen (3.6) und (3.7) wird

$$\{K_1^*, K_{l-1}^*\}_K^v\, \{K_u^*, K_v^*\}_K = 1\ ,$$

und mithin wegen (3.12):

$$\zeta^{2v}\, \{K_u^*, K_v^*\}_K = 1\ .$$

Da also

$$\{K_u^*, K_v^*\}_K = \zeta^{-2v} \quad \text{für} \quad 1 \leqq u < \frac{l}{2} , \quad u + v = l ,$$

ist auch

$$\{K_v^*, K_u^*\}_K = \zeta^{2v} \quad \text{für} \quad \frac{l}{2} < v \leqq l - 1 , \quad u + v = l .$$

Mithin ist

$$\left.\begin{aligned} \{K_u^*, K_v^*\}_K &= \zeta^{-2v} , \quad u + v = l \\ \{K_u^*, K_v^*\}_K &= 1 , \quad u + v \neq l \end{aligned}\right\} u, v = 1, 2, \ldots, l - 1 . \tag{3.15}$$

Ist allgemein für zu l teilerfremdes M:

$$M \equiv M^{l^2} K_1^{G_1(M)} K_2^{G_2(M)} \ldots K_{l-1}^{G_{l-1}(M)} K_1^{*\,G_1^*(M)} K_2^{*\,G_2^*(M)} \ldots K_{l-1}^{*\,G_{l-1}^*(M)} (\mathrm{mod}\ \lambda^l) , \tag{3.16}$$

so erhält auf Grund der Formeln (3.5), (3.6) und (3.15) das Reziprozitätsgesetz, falls N zu M und zu l teilerfremd ist, die Form:

$$\{M, N\}_K = \zeta^{-2 \sum_{w=1}^{l-1} w G_w(M) G_{l-w}(N) + 2 \sum_{w=1}^{l-1} w G_w^*(M) G_{l-w}^*(N)} . \tag{3.17}$$

Wie man sofort erkennt, wird weiter

$$\{M, N\}_K = \{M^2, N^2\}_K^{\frac{1-l^2}{4}} = \left\{M M^{\Sigma} \cdot \frac{M}{M^{\Sigma}}, \quad N N^{\Sigma} \cdot \frac{N}{N^{\Sigma}}\right\}_K^{\frac{1-l^2}{4}} ,$$

$$\{M, N\}_K = \{M M^{\Sigma}, N N^{\Sigma}\}_K^{\frac{1-l^2}{4}} \cdot \left\{\frac{M}{M^{\Sigma}}, \quad \frac{N}{N^{\Sigma}}\right\}_K^{\frac{1-l^2}{4}} , \tag{3.18}$$

und hiebei ist

$$\left\{M M^{\Sigma}, \quad N N^{\Sigma}\right\}_K^{\frac{1-l^2}{4}} = \zeta^{-2 \sum_{w=1}^{l-1} w G_w(M) G_{l-w}(N)} , \tag{3.19}$$

$$\left\{\frac{M}{M^{\Sigma}}, \quad \frac{N}{N^{\Sigma}}\right\}_K^{\frac{1-l^2}{4}} = \zeta^{2 \sum_{w=1}^{l-1} w G_w^*(M) G_{l-w}^*(N)} . \tag{3.20}$$

4. Die *Kummer*sche Form für das Reziprozitätsgesetz der l-ten Potenzreste in K

Es sei M eine ganze Zahl von K, die der Kongruenz $M \equiv 1 \pmod{\lambda}$ genügt. Setzt man

$$M = c_0 + c_1 \zeta + c_2 \zeta^2 + \cdots + c_{l-2} \zeta^{l-2} ,$$

wo die c_u, $u = 0, 1, 2, \ldots, l-2$, ganze Zahlen des Gaußschen Zahlkörpers sind, so ist also

$$c_0 + c_1 + c_2 + \cdots + c_{l-2} \equiv 1 \pmod{l} .$$

Setzt man daher

$$M(\xi) = c_0 + c_1 \xi + \cdots + c_{l-2} \xi^{l-2} - \frac{c_0 + c_1 + c_2 + \cdots + c_{l-2} - 1}{l} \times \\ \times (1 + \xi + \xi^2 + \cdots + \xi^{l-1}) ,$$

so gilt für dieses ganzzahlige Polynom des Gaußschen Zahlkörpers vom Grade $l-1$, dessen freie Variable wir mit ξ bezeichnen, um in späteren Formeln eine Verwechslung mit der Größe x der Gleichung (1.1) zu vermeiden:

$$M(1) = 1 , \quad M(\zeta) = M , \quad M^{\Sigma}(1) = 1 , \quad M^{\Sigma}(\zeta) = M^{\Sigma} .$$

Für reelles v führen wir die beiden reellen Funktionen[4]

$$F(M\ ;\ v) = \tfrac{1}{2} \log M(e^v)\, M^{\Sigma}(e^v)$$

und

$$F^*(M\ ;\ v) = \operatorname{arc\,tg} \frac{-i\,[M(e^v) - M^{\Sigma}(e^v)]}{M(e^v) + M^{\Sigma}(e^v)}$$

ein, so daß

$$\log M(e^v) = F(M\ ;\ v) + i\, F^*(M\ ;\ v) ,$$

und setzen für $w = 1, 2, \ldots, l-1$:

$$L_w(M) = \left[\frac{d^w F(M\ ;\ v)}{dv^w}\right]_{v=0} \quad \text{und} \quad L_w^*(M) = i\left[\frac{d^w F^*(M\ ;\ v)}{dv^w}\right]_{v=0} .$$

Die ersten $l-1$ Größen sind ganze rationale Zahlen, die zweiten $l-1$ Größen sind von der Form: i multipliziert mit einer ganzen rationalen Zahl.

[4]) Die zweite dieser Funktionen ist zwar unendlich vieldeutig, aber wir brauchen im folgenden überall nur ihre Ableitungen nach v.

Sind die Koeffizienten von $v, v^2, \ldots, v^{l-1}$ der beiden Potenzreihen $F(v)$ und $G(v)$ Zahlen des Gaußschen Zahlkörpers mit zu l teilerfremden Nennern, und ist jeder der Koeffizienten von $v, v^2, \ldots, v^{l-1}$ der einen Reihe je kongruent mod. l zu dem entsprechenden der andern Reihe, so schreiben wir

$$F(v) \cong G(v) \ .$$

Wird die ganze Zahl M von K mit der Kongruenzeigenschaft $M \equiv 1$ (mod. λ) auf irgendeine Weise in die Gestalt

$$M = a_0 + a_1 \zeta + a_2 \zeta^2 + \cdots + a_t \zeta^t$$

gebracht, wo $a_0, a_1, a_2, \ldots, a_t$ ganze Zahlen des Gaußschen Zahlkörpers sind, so wird im allgemeinen das Polynom

$$\overline{M}(\xi) = a_0 + a_1 \xi + a_2 \xi^2 + \cdots + a_t \xi^t$$

nicht mehr der Gleichung

$$\overline{M}(1) = 1$$

genügen, aber jedenfalls der Kongruenz

$$\overline{M}(1) \equiv 1 \pmod{l} \ ,$$

und es ist

$$M(\xi) = \overline{M}(\xi) - \frac{\overline{M}(1) - 1}{l}(1 + \xi + \xi^2 + \cdots + \xi^{l-1}) + Q(\xi) \cdot (\xi^l - 1) \ ,$$

wo $Q(x)$ ein Polynom von x ist, dessen Koeffizienten ganze Zahlen des Gaußschen Zahlkörpers sind.

Mithin wird

$$M(e^v) \cong \overline{M}(e^v) + \frac{\overline{M}(1) - 1}{l} \cdot \frac{v^{l-1}}{(l-1)!}$$

und

$$\log M(e^v) \cong \log \overline{M}(e^v) + \frac{\overline{M}(1) - 1}{l} \cdot \frac{v^{l-1}}{(l-1)!} \ .$$

Führt man analog die beiden reellen Funktionen

$$F(\overline{M}; v) = \tfrac{1}{2} \log \overline{M}(e^v)\, \overline{M}^{\Sigma}(e^v)$$

und

$$F^*(\overline{M}; v) = \operatorname{arc\,tg} \frac{-i[\overline{M}(e^v) - \overline{M}^{\Sigma}(e^v)]}{\overline{M}(e^v) + \overline{M}^{\Sigma}(e^v)}$$

ein, so daß

$$\log \overline{M}(e^v) = F(\overline{M}\,;v) + iF^*(\overline{M}\,;v)\ ,$$

so folgt für $w = 1, 2, \ldots, l-2$:

$$L_w(M) \equiv \left[\frac{d^w F(\overline{M}\,;v)}{dv^w}\right]_{v=0} \pmod{l}\ ,$$

$$L_w^*(M) \equiv i\left[\frac{d^w F^*(\overline{M}\,;v)}{dv^w}\right]_{v=0} \pmod{l}\ ,$$

und

$$L_{l-1}(M) \equiv \left[\frac{d^{l-1} F(\overline{M}\,;v)}{dv^{l-1}}\right]_{v=0} + \frac{\overline{M}(1) + \overline{M}^{\Sigma}(1) - 2}{2l} \pmod{l}\ ,$$

$$L_{l-1}^*(M) \equiv i\left[\frac{d^{l-1} F^*(\overline{M}\,;v)}{dv^{l-1}}\right]_{v=0} + \frac{\overline{M}(1) - \overline{M}^{\Sigma}(1)}{2l} \pmod{l}\ .$$

Für $M \equiv N \equiv 1 \pmod{\lambda}$ und $w = 1, 2, \ldots, l-1$ erkennt man leicht:

1. Ist $M \equiv N \pmod{\lambda^l}$, so ist

$$\log M(e^v) \cong \log N(e^v)$$

und daher

$$L_w(M) \equiv L_w(N), \quad L_w^*(M) \equiv L_w^*(N) \pmod{l}\ .$$

2. Es ist $\log M(e^v)N(e^v) \cong \log M(e^v) + \log N(e^v)$, falls

$$M(1) = M^{\Sigma}(1) = N(1) = N^{\Sigma}(1) = 1\ ,$$

und daher

$$L_w(MN) \equiv L_w(M) + L_w(N)\,;\ L_w^*(MN) \equiv L_w^*(M) + L_w^*(N) \pmod{l}\ ^{5})\ .$$

3. Für $u = 1, 2, \ldots, l-2$ wird:

$$L_w(M^{S^u}) \equiv r^{wu} L_w(M)\,;\ L_w^*(M^{S^u}) \equiv r^{wu} L_w^*(M) \pmod{l}\ .$$

Da, wie man auf übliche Weise nachrechnet, für $u = 1, 2, \ldots, l-1$, $w = 1, 2, \ldots, l-1$:

$$L_w(K_u) \equiv L_w^*(K_u) \equiv L_w(K_u^*) \equiv L_w^*(K_u^*) \equiv 0 \pmod{l},\ u \neq w\ ,$$

ferner

$$L_w^*(K_w) \equiv L_w(K_w^*) \equiv 0 \pmod{l}\ ,$$

---

[5]) Auf Grund der letzten beiden Formeln sind die *Kummer*schen Exponenten $L_w(M)$ und $L_w^*(M)$ (mod. l) definiert für irgendeine ganze oder *gebrochene* Zahl M des Strahles $M \equiv 1 \pmod{\lambda}$.

dagegen:

$$L_w(K_w) \equiv (-1)^{w-1}\, w\,! \;, \quad L_w^*(K_w^*) \equiv i(-1)^{w-1}\, w\,! \pmod{l} \;,$$

so wird, vergleiche Formel (3.16) für $M \equiv 1 \pmod{\lambda}$:

$$G_w(M) \equiv \frac{(-1)^{w-1}}{w!} L_w(M) \;, \; G_w^*(M) \equiv -i\frac{(-1)^{w-1}}{w!} L_w^*(M) \pmod{l} \;. \tag{4.1}$$

Folglich wird, vergleiche Formeln (3.19) und (3.20), für zueinander teilerfremde M, N mit $M \equiv N \equiv 1 \pmod{\lambda}$:

$$\left\{ M M^{\Sigma}, N N^{\Sigma} \right\}^{\frac{1-l^2}{4}} = \zeta^{2 \sum_{w=1}^{l-1} (-1)^w L_w(M)\, L_{l-w}(N)}$$

und

$$\left\{ \frac{M}{M^{\Sigma}}, \frac{N}{N^{\Sigma}} \right\}^{\frac{1-l^2}{4}} = \zeta^{2 \sum_{w=1}^{l-1} (-1)^w L_w^*(M) L_{l-w}^*(N)}$$

und damit wegen (3.18):

$$\left\{ M, N \right\} = \zeta^{2 \sum_{w=1}^{l-1} (-1)^w L_w(M) L_{l-w}(N) + 2 \sum_{w=1}^{l-1} (-1)^w L_w^*(M) L_{l-w}^*(N)}$$

5. Das Symbol $\{M, N\}$ für Einheiten und l-te Idealpotenzen von K

Sind M und N Einheiten,

oder eine der beiden Größen eine Einheit und die andere eine zu l teilerfremde l-te Idealpotenz,

oder M und N zu l teilerfremde l-te Idealpotenzen und die absolute Norm von M zur Relativnorm von N in bezug auf k teilerfremd,

oder $M = N$ eine zu l teilerfremde l-te Idealpotenz und die von MM^{Σ} verschiedenen zu MM^{Σ} absolut konjugierten Größen zu MM^{Σ} teilerfremd,

so wird gemäß (3.3) und (3.2):

$$\left\{ \left(M M^{\Sigma} \right)^{S^n}, N N^{\Sigma} \right\} = 1 \;, \left\{ \left(\frac{M}{M^{\Sigma}} \right)^{S^n}, \frac{N}{N^{\Sigma}} \right\} = 1 \;; \; n = 0, 1, 2, \ldots, l-2 \;.$$

Nun ist entsprechend den Definitionen für K_u und K_u^* und Formel (3.16):

$$M^{S^n} \equiv M^{l^2 S^n} K_1^{r^n G_1(M)} K_2^{r^{2n} G_2(M)} \ldots$$

$$\ldots K_{l-1}^{r^{(l-1)n} G_{l-1}(M)} K_1^{*r^n G_1^*(M)} K_2^{*r^{2n} G_2^*(M)} \ldots K_{l-1}^{*r^{(l-1)n} G_{l-1}^*(M)} \pmod{\lambda^l},$$

folglich wird gemäß (3.19) und (3.20):

$$\left.\begin{aligned} \sum_{w=1}^{l-1} w r^{wn} G_w(M) G_{l-w}(N) &\equiv 0 \pmod{l} \\ \sum_{w=1}^{l-1} w r^{wn} G_w^*(M) G_{l-w}^*(N) &\equiv 0 \pmod{l} \end{aligned}\right\} n = 0, 1, 2, \ldots, l-2 .$$

Da die Determinante

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ r & r^2 & r^3 & \ldots & r^{l-1} \\ r^2 & r^4 & r^6 & \ldots & r^{2(l-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ r^{l-2} & r^{2(l-2)} & r^{3(l-2)} & \ldots & r^{(l-1)(l-2)} \end{vmatrix} \not\equiv 0 \pmod{l}$$

ist, so wird

$$\left.\begin{aligned} G_w(M) G_{l-w}(N) &\equiv 0 \pmod{l} \\ G_w^*(M) G_{l-w}^*(N) &\equiv 0 \pmod{l} \end{aligned}\right\} w = 1, 2, \ldots, l-1 ,$$

also auch für $M \equiv N \equiv 1 \pmod{\lambda}$ gemäß (4.1):

$$\left.\begin{aligned} L_w(M) L_{l-w}(N) &\equiv 0 \pmod{l} \\ L_w^*(M) L_{l-w}^*(N) &\equiv 0 \pmod{l} \end{aligned}\right\} w = 1, 2, \ldots, l-1 . \qquad (5.1)$$

Speziell wird für $M = N \equiv 1 \pmod{\lambda}$ mit der für diesen Fall oben erwähnten Beschränkung für M:

$$\left.\begin{aligned} L_w(M) L_{l-w}(M) &\equiv 0 \pmod{l} \\ L_w^*(M) L_{l-w}^*(M) &\equiv 0 \pmod{l} \end{aligned}\right\} w = 1, 2, \ldots, l-1 . \qquad (5.2)$$

Im übrigen ist klar, daß wenn M eine Einheit oder eine zu l teilerfremde l-te Idealpotenz ist, gemäß (3.3)

$$\left\{ M, \zeta \right\}_K = \left(\frac{M}{\zeta}\right)_K \left(\frac{\zeta}{M}\right)_K^{-1} = 1 ,$$

also $G_{l-1}(M) \equiv 0 \pmod{l}$, und falls $M \equiv 1 \pmod{\lambda}$ ist:

$$L_{l-1}(M) \equiv 0 \pmod{l} \tag{5.3}$$

ist.

6. Die *Kummer*schen Exponenten für die Einheit H

Wir schicken voraus, daß wir Vorzeichen und Indexbezeichnung der Bernoullischen und Eulerschen Zahlen so wählen, daß

$$e^{Bv} = \sum_{m=0}^{\infty} B_m \frac{v^m}{m!} = \frac{ve^v}{e^v - 1} , \tag{6.1}$$

so daß also außer $B_1 = \frac{1}{2}$ alle B_m mit ungeradem Index m gleich 0 sind, dagegen $B_0 = 1$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, usw. Aus Gleichung (6.1) folgt übrigens nach Division durch v und Integration nach v sofort, daß

$$\log \frac{e^v - 1}{v} = \sum_{m=1}^{\infty} \frac{B_m}{m} \cdot \frac{v^m}{m!} . \tag{6.2}$$

Ferner sei

$$e^{Ev} = \sum_{m=0}^{\infty} E_m \frac{v^m}{m!} = \frac{2}{e^v + e^{-v}} , \tag{6.3}$$

so daß alle E_m mit ungeradem Index m gleich 0 sind, dagegen $E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$ usw. Durch Differentiation nach v erkennt man die Richtigkeit der Formel

$$2 \log (1 - ie^v) = \log (1 + e^{2v}) - i\left(\sum_{m=1}^{\infty} E_{m-1} \frac{v^m}{m!} + \frac{\pi}{2} \right) \tag{6.4}$$

bei geeigneter Wahl der Determination der auf der linken Seite dieser Gleichung stehenden Funktion, wo unter $\log(1 + e^{2v})$ der Hauptwert verstanden sein soll.

Für die Einheit[6])

$$H = \left(1 - i\zeta^{\frac{l+1}{2}}\right)^{2(l^2-1)} \prod_{g=3}^{l-1} \left(\frac{1 - \zeta^g}{1 - \zeta}\right)^{l^2-1} =$$

$$= \left(1 - i\zeta^{\frac{l+1}{2}}\right)^{2(l^2-1)} \prod_{g=3}^{l-1} (1 + \zeta + \zeta^2 + \cdots + \zeta^{g-1})^{l^2-1}$$

ist

[6]) Für den zweiten Faktor vergleiche *Hasse* [1], p. 112/113.

$$\overline{H}(\xi) = \left(1 - i\xi^{\frac{l+1}{2}}\right)^{2(l^2-1)} \prod_{g=3}^{l-1} (1 + \xi + \xi^2 + \cdots + \xi^{g-1})^{l^2-1} ,$$

also

$$\overline{H}(1) = (1 - i)^{2(l^2-1)} \prod_{g=3}^{l-1} g^{l^2-1} = [(l-1)!]^{l^2-1} = \overline{H}^{\Sigma}(1)$$

und

$$\log \overline{H}(e^v) = 2(l^2 - 1) \log \left(1 - ie^{\frac{l+1}{2}v}\right) +$$

$$+ (l^2 - 1) \sum_{g=3}^{l-1} \log (1 + e^v + e^{2v} + \cdots + e^{(g-1)v}) .$$

Es wird auf Grund der Formel (6.4)

$$\log \overline{H}(e^v) \cong - \sum_{g=3}^{l-1} \log \frac{e^{gv} - 1}{e^v - 1} - \log (1 + e^{(l+1)v}) + i \sum_{w=1}^{\infty} E_{w-1} \left(\frac{l+1}{2}\right)^w \cdot \frac{v^w}{w!}$$

oder

$$\log \overline{H}(e^v) \cong - \sum_{g=3}^{l-1} \log \frac{e^{gv} - 1}{e^v - 1} - \log \frac{e^{2v} - 1}{e^v - 1} + i \sum_{w=1}^{\infty} \frac{E_{w-1}}{2^w} \cdot \frac{v^w}{w!}$$

$$= - \sum_{g=1}^{l-1} \log \frac{e^{gv} - 1}{gv} \cdot \frac{v}{e^v - 1} - \log [(l-1)!] + i \sum_{w=1}^{\infty} \frac{E_{w-1}}{2^w} \cdot \frac{v^w}{w!} ,$$

mithin unter Benutzung der Formel (6.2):

$$\log \overline{H}(e^v) \cong - \sum_{g=1}^{l-1} \sum_{w=1}^{\infty} (g^w - 1) \frac{B_w}{w} \cdot \frac{v^w}{w!} + i \sum_{w=1}^{\infty} \frac{E_{w-1}}{2^w} \cdot \frac{v^w}{w!} .$$

Daher ist für $w = 1, 2, \ldots, l-2$:

$$L_w(H) \equiv - \frac{B_w}{w} \pmod{l} ,$$

und, vergleiche die Bemerkung am Ende von Abschnitt 5:

$$L_{l-1}(H) \equiv 0 \pmod{l} ,$$

ferner für $w = 1, 2, \ldots, l-1$:

$$L_w^*(H) \equiv \frac{i}{2^w} E_{w-1} \pmod{l} .$$ [7])

[7]) Will man eine Einheit haben, bei welcher bei der *Kummer*schen Entwicklung nur die Eulerschen Zahlen erscheinen, so kann man zum Beispiel $\frac{i+\zeta}{1+i\zeta}$ nehmen.

7. Die erste Form der *Kummer*schen Exponenten für die Idealpotenz A

Wenn die Gleichung (1.2) eine Lösung in ganzen rationalen nicht verschwindenden Zahlen X, Y, Z hat, so hat sie auch immer eine solche Lösung, für welche X, Y und Z je zu zweit zueinander teilerfremd sind. Wir nehmen daher in der Folge zum indirekten Beweise unseres Satzes in Abschnitt 1 an, daß die Gleichung (1.2) eine Lösung besitzt, für welche die ganzen rationalen Zahlen X, Y, Z je zu zweit zueinander teilerfremd und (*erster* Fall des großen Fermatschen Satzes!) alle drei zu l teilerfremd sind. Dann sind auch alle $2l$ Faktoren der linken Seite der Gleichung

$$\prod_{m=0}^{l-1}(X + i\zeta^m Y)\prod_{n=0}^{l-1}(X - i\zeta^n Y) = X^{2l} + Y^{2l} = Z^{2l}$$

zueinander teilerfremd, mithin zueinander und zu l teilerfremde l-te Idealpotenzen von K. Denn wenn ein Primideal $\mathfrak{P}$ von K in zwei verschiedenen dieser $2l$ Faktoren aufgehen würde, so wäre zunächst $\mathfrak{P}$ ein Teiler von Z. Von den beiden Zahlen X und Y ist eine gerade, die andere ungerade und Z ungerade. Also würde $\mathfrak{P}$ jedenfalls weder Teiler von 2 noch von l sein. $\mathfrak{P}$ würde auch die Differenz der beiden Faktoren, mithin auch Y, und daher auch X teilen, was einen Widerspruch ergibt.

Insbesondere ist auch

$$A = \frac{X + i\zeta Y}{X + iY}$$

eine l-te Idealpotenz von K, deren Zähler und Nenner zu l teilerfremd sind.

Es wird

$$\overline{A}(\xi) = \frac{X + i\xi Y}{X + iY}\ ,\quad \overline{A}(1) = \overline{A}^{\Sigma}(1) = 1\ ,$$

ferner

$$F(\overline{A}\,;\,v) = \tfrac{1}{2}\log\frac{X^2 + e^{2v}Y^2}{X^2 + Y^2}\ ,$$

also

$$\frac{dF(\overline{A}\,;\,v)}{dv} = \frac{Y^2 e^{2v}}{X^2 + Y^2 e^{2v}} \tag{7.1}$$

und mithin für $w = 1, 2, \ldots, l-1$:

$$\left[\frac{d^w F(\overline{A}\,;\,v)}{dv^w}\right]_{v=0} = 2^{w-1}\frac{P_w(X^2, Y^2)}{(X^2 + Y^2)^w}\ ,$$

wo $P_w(\xi;\eta)$ ein homogenes Polynom vom Grade w in ξ und η mit ganzen rationalen Zahlkoeffizienten ist. Die Bezeichnung für diese Polynome stimmt genau überein mit der von *Mirimanoff* [4], S. 46—47.

Für $w = 1, 2, \ldots, l-1$ ist folglich:

$$L_w(A) \equiv 2^{w-1} \frac{P_w(X^2, Y^2)}{(X^2+Y^2)^w} \pmod{l} .$$

Weiter wird

$$F^*(\overline{A}; v) = \operatorname{arc\,tg} \frac{XY(e^v-1)}{X^2+Y^2 e^v} ,$$

also

$$\frac{dF^*(\overline{A}; v)}{dv} = \frac{XY}{X^2 e^{-v} + Y^2 e^v} . \tag{7.2}$$

Vertauscht man im Ausdrucke auf der rechten Seite der Gleichung (7.2) X und Y und gleichzeitig v mit $-v$, so ändert er sich nicht. Mithin ist *für ungerades* w die Größe

$$(X^2+Y^2)^w \cdot \left[\frac{d^w F^*(\overline{A}; v)}{dv^w}\right]_{v=0} \tag{7.3}$$

das Produkt von XY und eines homogenen Polynoms in $\xi = X^2$ und $\eta = Y^2$, das in ξ und η vom Grade $w-1$ und in ξ und η symmetrisch ist. *Für gerades* w ist der Ausdruck (7.3) das Produkt von $XY(X^2-Y^2)$ und eines homogenen Polynoms in $\xi = X^2$ und $\eta = Y^2$, das in ξ und η vom Grade $w-2$ und in ξ und η symmetrisch ist.

Setzt man für $w = 1, 2, \ldots, l-1$:

$$\left[\frac{d^w F^*(\overline{A}; v)}{dv^w}\right]_{v=0} = \frac{X}{Y} \cdot \frac{Q_w(X^2, Y^2)}{(X^2+Y^2)^w} ,$$

und

$$\frac{Y^2}{X^2} = t ,$$

so ist

$$Q_w(X^2, Y^2) = X^{2w} Q_w(1, t) .$$

Setzt man weiter

$$Q_w(1, t) = Q_w^*(t) ,$$

so ist für $w = 1, 2, \ldots, l-1$:

$$\left[\frac{d^w F^*(\overline{A}; v)}{dv^w}\right]_{v=0} = \frac{X}{Y} \cdot \frac{Q_w^*(t)}{(1+t)^w}$$

und

$$L_w^*(A) \equiv i \frac{X}{Y} \cdot \frac{Q_w^*(t)}{(1+t)^w} \pmod{l} .$$

$Q_w^*(t)$ ist ein ganzrationalzahliges Polynom vom Grade w in t. Für ungerades w ist $Q_w^*(t)$ durch t teilbar und $\frac{Q_w^*(t)}{t}$ ist ein symmetrisches Polynom in t vom Grade $w-1$. Für gerades w ist $Q_w^*(t)$ durch $t(1-t)$ teilbar und $\frac{Q_w^*(t)}{t(1-t)}$ ein symmetrisches Polynom in t vom Grade $w-2$.

Die Rechnung liefert

$$Q_2^*(t) = t(1-t)$$

$$Q_4^*(t) = t(1-t)\,(1-22t+t^2)$$

$$Q_6^*(t) = t(1-t)\,(1-236t+1\,446t^2-236t^3+t^4)$$

$$Q_8^*(t) = t(1-t)\,(1-2\,178t+58\,479t^2-201\,244t^3+58\,479t^4-2\,178t^5+t^6)$$

$$Q_{10}^*(t) = t(1-t)\,(1-19\,672t+1\,736\,668t^2-19\,971\,304t^3+$$
$$+49\,441\,990t^4-19\,971\,304t^5+1\,736\,668t^6-19\,672t^7+t^8)\,.$$

8. Die zweite Form der *Kummer*schen Exponenten für die Idealpotenz A

In $A = \frac{X+i\zeta Y}{X+iY}$ setzen wir für die beiden ganzen rationalen und zu l teilerfremden Zahlen X und Y:

$$\frac{Y}{X} = T$$

und nehmen in der Folge wesentlich an (*erster* Fall des großen Fermatschen Satzes!), daß $T^2 \not\equiv -1 \pmod{l}$ ist. Gemäß den Formeln (7.1) und (7.2) wird:

$$L_1(A) \equiv \frac{T^2}{1+T^2} \qquad \text{und} \qquad L_1^*(A) \equiv i\frac{T}{1+T^2} \pmod{l}\,.$$

Im folgenden möge daher $w = 2, 3, \ldots, l-1$ sein.

Zur Abkürzung setzen wir vorübergehend

$$U = \frac{iT}{1+iT}\,,$$

so daß

$$T = \frac{iU}{U-1}$$

wird und

$$A = \frac{1+i\zeta T}{1+iT} = 1 - \frac{iT(1-\zeta)}{1+iT} = 1 - U(1-\zeta)\,.$$

Es wird

$$\overline{A}(\xi) = 1 - U(1-\xi)\ , \qquad \overline{A}(1) = \overline{A}^{\Sigma}(1) = 1\ ,$$

und formal [8])

$$\log \overline{A}(e^v) = \log\left[1 - U(1-e^v)\right] = -\sum_{n=1}^{\infty} \frac{1}{n} U^n (1-e^v)^n$$

$$= -\sum_{n=1}^{\infty} \frac{U^n}{n} \sum_{m=0}^{n} (-1)^m \binom{n}{m} e^{vm} = -\sum_{n=1}^{\infty} \frac{U^n}{n} \sum_{m=0}^{n} (-1)^m \binom{n}{m} \sum_{w=0}^{\infty} m^w \cdot \frac{v^w}{w!}.$$

Mithin wird für $w = 2, 3, \ldots, l-1$:

$$\left[\frac{d^w \log \overline{A}(e^v)}{dv^w}\right]_{v=0} = -\sum_{n=1}^{\infty} \frac{U^n}{n} \sum_{m=0}^{n} (-1)^m \binom{n}{m} m^w\ .$$

In der Summe über m verschwindet der Summand für $m = 0$ und die innere Summe verschwindet für $n > w$. Folglich wird für $w = 2, 3, \ldots, l-1$:

$$\left[\frac{d^w \log \overline{A}(e^v)}{dv^w}\right]_{v=0} = -\sum_{n=1}^{l-1} \frac{U^n}{n} \sum_{m=1}^{n} (-1)^m \binom{n}{m} m^w\ . \tag{8.1}$$

Für $w = 2, 3, \ldots, l-1$ betrachten wir den Ausdruck:

$$\frac{-1}{(1+iT)^l} \sum_{m=1}^{l-1} (-i)^m\, m^{w-1} T^m\ . \tag{8.2}$$

Führt man in ihm die Größe U ein, so wird er gleich

$$\sum_{m=1}^{l-1} m^{w-1} U^m (U-1)^{l-m}$$

$$= \sum_{m=1}^{l-1} m^{w-1}\, U^m \left[\sum_{h=0}^{l-m} (-1)^h \binom{l-m}{h} U^{l-m-h}\right]$$

$$= \sum_{m=1}^{l-1} m^{w-1} \sum_{h=0}^{l-m} (-1)^h \binom{l-m}{h} U^{l-h}\ .$$

Summiert man hier zuerst über m und dann über h, so wird der Ausdruck (8.2) gleich

$$\sum_{h=1}^{l-1} (-1)^h\, U^{l-h} \sum_{m=1}^{l-h} \binom{l-m}{h} m^{w-1} + U^l \sum_{m=1}^{l-1} m^{w-1}\ .$$

---

[8]) Vergleiche zum folgenden die Ausführungen auf S. 116/117 bei *Hasse* [1].

Der Koeffizient von U^l verschwindet mod l. Setzt man noch $h = l - n$, so ist der Ausdruck (8.2) mod. l gleich

$$-\sum_{n=1}^{l-1}(-1)^n \frac{U^n}{n} \sum_{m=1}^{n} m^w \cdot \frac{n}{m}\binom{l-m}{l-n} .$$

Nun ist mod l

$$\begin{aligned}\frac{n}{m}\binom{l-m}{l-n} &= \frac{n}{m} \cdot \frac{(l-m)(l-m-1)\cdots(l-(n-1))}{(n-m)!} \\ &\equiv (-1)^{n-m}\frac{n}{m} \cdot \frac{m(m+1)\ldots(n-1)}{(n-m)!} \\ &= (-1)^{n-m}\frac{n(n-1)(n-2)\ldots(m+1)}{(n-m)!} \\ &= (-1)^{-n+m}\binom{n}{m} .\end{aligned}$$

Der Ausdruck (8.2) wird mithin mod l

$$-\sum_{n=1}^{l-1}\frac{U^n}{n}\sum_{m=1}^{n}(-1)^m\binom{n}{m}m^w .$$

Folglich wird gemäß (8.1) und (8.2) für $w = 2, 3, \ldots, l-1$:

$$L_w(A) + L_w^*(A) \equiv \frac{-1}{(1+iT)^l}\sum_{m=1}^{l-1}(-i)^m m^{w-1} T^m \pmod{l} . \quad (8.3)$$

Trennt man in der letzten Formel reelles und imaginäres und setzt wie in Abschnitt 7

$$\frac{Y^2}{X^2} = T^2 = t ,$$

so folgt für $w = 2, 3, \ldots, l-1$:

$$L_w(A) \equiv 2^{w-1}\frac{\varphi_w(t)}{(1+t)^l} \pmod{l}$$

und

$$L_w^*(A) \equiv i\frac{X}{Y} \cdot \frac{\varphi_w^*(t)}{(1+t)^l} \pmod{l} ,$$

wo

$$\varphi_w(t) = \sum_{m=1}^{l-1}(-1)^{m-1} m^{w-1} t^m \quad (8.4)$$

die von *Mirimanoff* [4] S. 57, Formel (12) eingeführten Polynome sind und

$$\varphi_w^*(t) = \sum_{m=1}^{l} (-1)^{m-1}(2m-1)^{w-1}\, t^m \tag{8.5}$$

ist.

9. Beweis des Hauptsatzes

Aus den im Eingang zum Abschnitt 7 gemachten Annahmen folgt gemäß Abschnitt 5, vergleiche Formeln (5.1) und (5.3), daß für $w = 1, 2, \ldots, l-2$:

$$L_w(A)\, L_{l-w}(H) \equiv 0 \pmod{l} ,$$

ferner

$$L_{l-1}(A) \equiv 0 \pmod{l} ,$$

endlich für $w = 1, 2, \ldots, l-1$:

$$L_w^*(A)\, L_{l-w}^*(H) \equiv 0 \pmod{l} .$$

Gemäß Abschnitt 6 sind diese Kongruenzen, da es immer auf einen zu l teilerfremden Faktor nicht ankommt, äquivalent zu den folgenden:

$$L_w(A)\cdot B_{l-w} \equiv 0 \pmod{l}, \quad w = 3, 5, \ldots, l-2 , \tag{9.1}$$

$$L_{l-1}(A) \equiv 0 \pmod{l}, \tag{9.2}$$

$$L_w^*(A)\cdot E_{l-1-w} \equiv 0 \pmod{l}, \quad w = 2, 4, \ldots, l-1 . \tag{9.3}$$

Die Kongruenzen (9.1) setzen auf jeden Fall voraus, daß $l > 3$ ist, was wir in der Folge immer annehmen.

Beachtet man, daß $X^2 + Y^2$ jedenfalls zu l teilerfremd ist, so ergeben sich aus den Formeln des Abschnittes 7 die zu den Kongruenzen (9.1) äquivalenten Kongruenzen:

$$P_w(X^2, Y^2)\cdot B_{l-w} \equiv 0 \pmod{l} , \quad w = 3, 5, \ldots, l-2 . \tag{9.4}$$

Die Kongruenzen (9.4) entsprechen genau den Kongruenzen (2), S. 47 in der Arbeit [4] von *Mirimanoff*.

In der Folge beachte man, daß $t \not\equiv 0 \pmod{l}$ ist, ferner ist die Kongruenz $t \equiv -1 \pmod{l}$ nicht möglich, da sonst $Z \equiv 0 \pmod{l}$ wäre gegen Annahme. Mithin sind die Kongruenzen (9.1) und (9.2) gemäß Abschnitt 8 äquivalent zu den folgenden:

$$\varphi_w(t)\cdot B_{l-w} \equiv 0 \pmod{l}, \quad w = 3, 5, \ldots, l-2, \tag{9.5}$$

$$\varphi_{l-1}(t) \equiv 0 \pmod{l}. \tag{9.6}$$

Die Kongruenzen (9.3) sind äquivalent zu den folgenden:

$$\varphi_w^*(t)\cdot E_{l-1-w} \equiv 0 \pmod{l}, \quad w = 2, 4, \ldots, l-1. \tag{9.7}$$

Die Polynome $\varphi_w(t)$ und $\varphi_w^*(t)$ sind in den Formeln (8.4) und (8.5) definiert.

Endlich sind die Kongruenzen (9.3) gemäß Abschnitt 7 äquivalent zu den folgenden:

$$Q_w^*(t)\cdot E_{l-1-w} \equiv 0 \pmod{l}, \quad w = 2, 4, \ldots, l-1, \tag{9.8}$$

denn X und Y sind nach Annahme zu l teilerfremd.

Der in Abschnitt 1 behauptete Satz wird mithin bewiesen sein, wenn wir zeigen können, daß die Kongruenz $Q_w^*(t) \equiv 0 \pmod{l}$ nicht möglich ist, falls $w = 2, 4, 6, 8, 10$ ist.

Aus den Ausführungen von *Mirimanoff* [4], S. 48 und 51, geht aber hervor, daß mit einer Lösung $t \equiv \tau$, $t \not\equiv 0 \pmod{l}$, $t \not\equiv -1 \pmod{l}$ der Kongruenz

$$Q_w^*(t) \equiv 0 \pmod{l}$$

diese Kongruenz notwendigerweise auch die Lösungen

$$\tau, \frac{1}{\tau}, \quad -1-\tau, \quad -\frac{1}{1+\tau}, \quad -1-\frac{1}{\tau}, \quad -\frac{\tau}{1+\tau}$$

haben muß.

Diese sechs Wurzeln brauchen mod l nicht notwendigerweise voneinander verschieden zu sein. Man hat folgende drei Fälle zu untersuchen:

I. Die sechs Wurzeln bilden im ganzen nur zwei mod l inkongruente Wurzeln, wenn $t^2 + t + 1 \equiv 0 \pmod{l}$ ist, und dieser Fall kann nur eintreten, wenn $l \equiv 1 \pmod{6}$ ist.

Nun hat *Pollaczek* [6] gezeigt, daß wenn die Kongruenzen (9.5) und (9.6) gelten, dieser Fall nicht eintreten kann.

II. Diese sechs Wurzeln bilden im ganzen genau nur drei mod l inkongruente Wurzeln, wenn t mod l kongruent einer der drei Zahlen 1, -2, $-\frac{1}{2}$ ist.

Mithin muß $t \equiv -2 \pmod{l}$ Wurzel der Kongruenz

$$\frac{Q_w^*(t)}{t(1-t)} \equiv 0 \pmod{l}$$

sein. Für $w = 2$ ist nichts zu beweisen. Für die weiteren Werte von w hat der Quotient $\dfrac{Q_w^*(t)}{t(1-t)}$ für $t = -2$ die Primzahlpotenz-Produkt-Zerlegung:

$$\begin{aligned} w &= 4: \quad 7^2 \\ w &= 6: \quad 8161 \\ w &= 8: \quad 983 \cdot 2903 \\ w &= 10: \quad 7 \cdot 109 \cdot 173 \cdot 12959 \ . \end{aligned}$$

Aber für diese Primzahlen hat die Gleichung (1.1), also a fortiori (1.2) im ersten Falle des großen Fermatschen Satzes keine Lösung [9]).

III. Wenn diese sechs Wurzeln mod. l inkongruent sind, so muß das Polynom $\dfrac{Q_w^*(t)}{t(1-t)} \bmod l$ durch ein normiertes Polynom von der Form

$$1 + 3t + at^2 + (2a - 5)t^3 + at^4 + 3t^5 + t^6 \qquad (9.9)$$

teilbar sein, wo a ganzrationalzahlig ist und $a \not\equiv -\frac{3}{4} \pmod l$, ferner, wenn $l \equiv 1 \pmod 6$, auch $a \not\equiv 6 \pmod l$ ist. Dieser Fall kann höchstens für $w \geqq 8$ eintreten.

Für $w = 8$ würde $-2178 \equiv 3 \pmod l$, mithin müßte, da $l = 3$ zu verwerfen ist, $l = 727$ sein. Für $l = 727$ würde $a \equiv 319 \pmod l$, also $a \not\equiv -\frac{3}{4} \pmod l$ und $a \not\equiv 6 \pmod l$; aber die Kongruenz

$$2a - 5 \equiv 135 \pmod{727}$$

ist nicht erfüllt.

Für $w = 10$ müßte $\dfrac{Q_w^*(t)}{t(1-t)}$ außer einem Faktor von der Form (9.9) mod. l noch einen Faktor von der Form $1 + bt + t^2$ mit ganzrationalzahligem b haben (welcher Faktor dann $\not\equiv 0 \pmod l$ wäre!). Aus den Koeffizienten von t und t^2 des entstehenden Polynoms vom 8. Grade in t würde aber folgen, daß

$$b \equiv -19675 \pmod l \qquad \text{und} \qquad a \equiv 1795692 \pmod l \ .$$

---

[9]) Dies erkennt man auf Grund bekannter Kriterien entweder sofort direkt oder dann folgt es jedenfalls aus den Arbeiten von *B. Rosser* [7] und [8] und *D. H. Lehmer* und *Emma Lehmer* [3], sowie natürlich früherer diesbezüglicher Arbeiten anderer Autoren.

Eliminiert man das Produkt ab aus den Koeffizienten von t^3 und t^4, so müßte

$$-2a - 5b \equiv 89384594 \pmod{l}$$

sein. Das würde aber bedeuten, daß

$$3 \cdot 7 \cdot 13 \cdot 340211 \equiv 0 \pmod{l} .$$

Aber für diese Primzahlen hat die Gleichung (1.1), also a fortiori (1.2) im ersten Falle des großen Fermatschen Satzes keine Lösung.

Damit ist aber der Beweis unseres Satzes in Abschnitt 1 geleistet.

10. Eine weitere notwendige Bedingung für die Lösbarkeit der Gleichung (1.2)

Mirimanoff hat in seiner Arbeit [4] noch eine weitere notwendige Bedingung für die Lösbarkeit der Gleichung (1.1) im ersten Falle aufgestellt. Wir geben zum Schlusse die entsprechenden Bedingungen für die Lösbarkeit der Gleichung (1.2) im ersten Falle an.

Aus den Formeln (5.2) und (5.3) folgt, falls man $M = A$ setzt und die zweite Form der *Kummer*schen Exponenten für die Idealpotenz A gemäß Abschnitt 8 einführt:

$$\left.\begin{aligned} \varphi_w(t)\,\varphi_{l-w}(t) &\equiv 0 \pmod{l} , \quad w = 2, 3, \ldots, \frac{l-1}{2} , \\ \varphi_{l-1}(t) &\equiv 0 \pmod{l} , \end{aligned}\right\} \tag{10.1}$$

$$\left.\begin{aligned} \varphi^*_w(t)\,\varphi^*_{l-w}(t) &\equiv 0 \pmod{l} , \quad w = 2, 3, \ldots, \frac{l-1}{2} , \\ \varphi^*_{l-1}(t) &\equiv 0 \pmod{l} . \end{aligned}\right\} \tag{10.2}$$

Dabei sind die Polynome $\varphi_w(t)$ und $\varphi^*_w(t)$ in den Formeln (8.4) und (8.5) definiert. Um Relationen zwischen diesen Polynomen aufzustellen — worauf ich hier nicht weiter eingehen will — ist möglicherweise die Relation (8.3) geeigneter.

(Eingegangen den 17. Juni 1949.)

LITERATUR

[1] *Hasse, H.*, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II, Reziprozitätsgesetz, Jahresbericht der Deutschen Mathematiker-Vereinigung, Sonderdruck, Leipzig und Berlin 1930, B. G. Teubner.

[2] *Kummer, E. E.*, De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda, Journ. f. d. reine und angew. Math., vol. 17, p. 203/209 (1837).

[3] *Lehmer, D. H.* and *Lehmer, Emma*, On the first case of Fermat's last theorem. Bull. Amer. Math. Soc., vol. 47, p. 139/142 (1941).

[4] *Mirimanoff, D.*, L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de *Kummer*, Journ. f. d. reine und angew. Math., vol. 128, p. 45/68 (1905).

[5] *Morishima, T.*, Über die Fermatsche Vermutung VII., Proc. Acad., Tokyo, vol. 8, p. 63/66 (1932).

[6] *Pollaczek, F.*, Über den großen Fermatschen Satz. Sitzungsber. Akad. Wissen. Wien, Math.-naturw. Kl., Abt. IIa, vol. 126, p. 45/59 (1917).

[7] *Rosser, B.*, On the first case of Fermat's last theorem, Bull. Amer. Math. Soc. vol. 45, p. 636/640 (1939).

[8] *Rosser, B.*, A new lower bound for the exponent in the first case of Fermat's last theorem, Bull. Amer. Math. Soc., vol. 46, p. 299/304 (1940).

[9] *Takagi, T.*, Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper, Journ. Coll. Science Imp. Univ. Tokyo, vol. 44, Art. 5 (1922/23).

[10] *Takagi, T.*, Zur Theorie des Kreiskörpers. Journ. f. d. reine und angew. Math., vol. 157, pg. 230/238, (1927).

[11] *Vandiver, H. S.*, Note on Euler Number criteria for the first case of Fermat's last theorem. Amer. Journ. Math., vol. 62, p. 79/82 (1940).