Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 16 (1943-1944)

Artikel: Kurze Darstellung des fünften Gauß'schen Beweises für den Quadratischen Reziprozitätssatz.

Autor: Rédei, L.

DOI: https://doi.org/10.5169/seals-15561

Kurze Darstellung des fünften Gauß'schen Beweises für den Quadratischen Reziprozitätssatz

Von L. Rédei in Szeged, Ungarn

Gauß' (auf seinem Lemma beruhender) fünfter Beweis des quadratischen Reziprozitätssatzes

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)} \tag{1}$$

(p, q verschiedene positive ungerade Primzahlen) läßt sich mit passender Symbolik wie folgt sehr leicht führen.

Für eine reelle Zahlenmenge M deuten wir die Symbole $\mathrm{p}^+\mathrm{q}^-$, $\mathrm{p}^-\mathrm{q}^-$, q^-, $\mathrm{p}^0\mathrm{q}^-$ so, daß z. B. $\mathrm{p}^0\mathrm{q}^- M$ die Anzahl der ganzen Zahlen in M ist, deren absolut kleinster Rest mod p und mod q die 0 bzw. negativ ist. Dabei wird für M immer nur ein Intervall (a, b) oder eine Folge $(a_1, a_2, \ldots, a_n)$ in Betracht kommen. Wir setzen noch $S[f(p, q)] = f(p, q) + f(q, p)$ für irgendeine Funktion $f(p, q)$ von p, q.

Offenbar ist

$$\mathrm{p}^+\mathrm{q}^-(0, pq) = \tfrac{1}{4}(p-1)(q-1)$$

d. h.

$$\mathrm{p}^+\mathrm{q}^-\left(0, \frac{pq}{2}\right) + \mathrm{p}^+\mathrm{q}^-\left(\frac{pq}{2}, pq\right) = \tfrac{1}{4}(p-1)(q-1).$$

Nach Umformung des zweiten Gliedes gemäß

$$\mathrm{p}^+\mathrm{q}^-(a, b) = \mathrm{q}^+\mathrm{p}^-(-b, -a) = \mathrm{q}^+\mathrm{p}^-(pq-b, pq-a)$$

ergibt sich

$$S\left[\mathrm{p}^+\mathrm{q}^-\left(0, \frac{pq}{2}\right)\right] = \tfrac{1}{4}(p-1)\ (q-1),$$

also

$$S\left[\mathrm{p}^+\mathrm{q}^-\left(0, \frac{pq}{2}\right) + \mathrm{p}^-\mathrm{q}^-\left(0, \frac{pq}{2}\right)\right] \equiv \tfrac{1}{4}(p-1)(q-1) \pmod 2,$$

da das neu angefügte Glied symmetrisch in p, q ist. Der Ausdruck in [ ] ist

$$\mathfrak{q}^-\left(0,\frac{pq}{2}\right) - \mathfrak{p}^0\mathfrak{q}^-\left(0,\frac{pq}{2}\right) = \tfrac{1}{4}(p-1)(q-1) - \mathfrak{q}^-\left(p, 2p, \ldots, \frac{q-1}{2}p\right),$$

und somit folgt

$$S\left[\mathfrak{q}^-\left(p, 2p, \ldots, \frac{q-1}{2}p\right)\right] \equiv \tfrac{1}{4}(p-1)(q-1) \pmod 2 .$$

Nach Übergehen zu Potenzen von -1 entsteht (1) wegen des Lemmas von Gauß.

(Eingegangen den 15. Oktober 1943.)