Zu Eisensteins transzendentem Beweis des quadratischen Reziprozitätsgesetzes.

Autor(en): **Koschmieder, L.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **37 (1962-1963)**

PDF erstellt am: **11.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-28620

L. KOSCHMIEDER, Tübingen

Zu Eisensteins transzendentem Beweis des quadratischen Reziprozitätsgesetzes

Herrn Max Müller zum sechzigsten Geburtstag am 9. Mai 1961

1. G. EISENSTEIN hat einen Beweis des quadratischen Reziprozitätsgesetzes geführt, dessen Gang von dem üblichen abweicht[1]): er bedient sich einer transzendenten Hilfsfunktion, des Sinus, dessen Multiplikation er heranzieht. Wie er sagt, liefe der Beweis noch glatter, wenn man statt des Sinus den Tangens benutzte. Das scheint bisher nicht geschehen zu sein; ich hoffe, hier zu zeigen, daß es sich lohnt, diesem Hinweise zu folgen.

2. Das Reziprozitätsgesetz handelt von zwei ungeraden Primzahlen; es sei zunächst p eine solche. Ein Restsystem (mod. p), das $\mathfrak{R}$ heiße, zerfällt, wenn man von der durch p teilbaren Zahlenklasse absieht, in zwei halbe Restsysteme R und $\overline{R}$, so daß, wenn r die zu R gehörigen Reste sind, $\overline{R}$ aus den Resten $-r$ besteht. Man kann für $\mathfrak{R}$ das System der absolut kleinsten Reste wählen; dann wird R von den Zahlen $1, 2, \ldots, \frac{p-1}{2}$ gebildet, $\overline{R}$ von denselben Zahlen mit negativem Zeichen. Vervielfacht man die Reste r mit einer durch p nicht teilbaren Zahl q, so kann ein Produkt qr zu R oder zu $\overline{R}$ gehören; entweder ist

$$qr \equiv r' \,(\text{mod. } p) \qquad (1) \qquad \text{oder} \qquad qr \equiv -r' \,(\text{mod. } p)\,, \qquad (\overline{1})$$

wo r' in R liegt. Die zwei Formeln (1), ($\overline{1}$) lassen sich bei Gebrauch der ungeraden und mit π periodischen Tangensfunktion durch *eine* ersetzen,

$$qr \equiv r' \frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r'\pi}{p}} \,(\text{mod. } p)\,. \qquad (2)$$

Vervielfacht man alle $\frac{p-1}{2}$ Kongruenzen (2) über R, so erhält man

$$q^{\frac{p-1}{2}} \Pi r \equiv \Pi r' \, \Pi \frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r'\pi}{p}} \,(\text{mod. } p)\,.$$

Πr links und $\Pi r'$ rechts stimmen überein, da auch r' die Gesamtheit R durch-

[1]) J. reine angew. Math. *29*, 177–179 (1845).

läuft. Man darf die Kongruenz durch diese zu p teilerfremde Zahl teilen, dann bleibt (mod. p)

$$q^{\frac{p-1}{2}} \equiv \Pi \frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r'\pi}{p}} = \Pi \frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r\pi}{p}} . \tag{3}$$

Nach dem EULERschen Kennzeichen in der Lehre von den quadratischen Resten gilt aber

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \text{(mod. } p) ,$$

wo $\left(\frac{q}{p}\right)$ das LEGENDREsche Symbol bedeutet,

$$\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{wenn } q \text{ quadratischer Rest,} \\ -1, & \text{wenn } q \text{ quadratischer Nichtrest} \end{cases}$$

(mod. p) ist. Also kann man statt (3) schreiben

$$\left(\frac{q}{p}\right) \equiv \Pi \frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r\pi}{p}} \text{ (mod. } p) .$$

Nun ist aber die rechte Seite, wie man aus dem Mittelgliede von (3) und dem zu (2) Gesagten ersieht, eine «Einheit», das heißt gleich ± 1, wie die linke. Da Einheiten verschiedenen Zeichens nicht kongruent (mod. p) sein können, folgt

$$\left(\frac{q}{p}\right) = \Pi_{r} \frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r\pi}{p}} . \tag{4}$$

Ist jetzt auch q eine ungerade Primzahl, so ergibt sich ebenso

$$\left(\frac{p}{q}\right) = \Pi_{s} \frac{\operatorname{tg} \frac{ps\pi}{q}}{\operatorname{tg} \frac{s\pi}{q}} , \tag{5}$$

wo s ein halbes Restsystem des Moduls q durchläuft.

3. Die Formeln (4), (5) zeigen, daß hier die sogenannte *Multiplikation der trigonometrischen Funktionen*, und zwar des Tangens, eingreift. Wir befassen uns daher kurz mit dieser. Man erkennt sogleich, daß $\operatorname{tg} mx$ bei ganzem m eine rationale Funktion von $\operatorname{tg} x$ ist, und zwar für $m > 0$ durch vollständige Induktion: Für $m = 2$ trifft es zu, und gilt es für $m = n$, so nach dem Summensatz

$$\operatorname{tg}(n+1)x = \frac{\operatorname{tg} nx + \operatorname{tg} x}{1 - \operatorname{tg} nx \operatorname{tg} x}$$

gleichfalls für $m = n + 1$. — Auch $\operatorname{tg} mx / \operatorname{tg} x$ ist eine rationale Funktion von

$\operatorname{tg} x$; wir wollen jetzt ihre Gestalt bestimmen, und zwar bei *ungeradem* m. Das Gebiet der Veränderlichen x ist $0 \leqq x < \pi$. Die Funktion $\operatorname{tg} mx / \operatorname{tg} x$ ist das Verhältnis zweier Polynome in $\operatorname{tg} x$. Das Zählerpolynom hat seine Nullstellen dort, wo sie verschwindet; das sind die Punkte

$$mx = h\pi, \quad x_h = h\frac{\pi}{m}, \quad h = 1, 2, \ldots, m-1. \tag{6}$$

Die Nullstellen des Nennerpolynoms liegen dort, wo sie unendlich wird, also in den $m-1$ Punkten

$$mx = (2H+1)\frac{\pi}{2}, \quad x_H = (2H+1)\frac{\pi}{2m}, \quad H = 0, 1, \ldots, m-1 \tag{7}$$

ohne $H = \dfrac{m-1}{2}$. Daher ist

$$\frac{\operatorname{tg} mx}{\operatorname{tg} x} = C\,\Pi\,\frac{\operatorname{tg} x - \operatorname{tg} x_h}{\operatorname{tg} x - \operatorname{tg} x_H} \tag{8}$$

mit einem von x unabhängigen Werte C.

Die Nullstellen (6) des Zählers lassen sich übersichtlich paaren, zu

$$x_h = h\frac{\pi}{m} \text{ und } x_{m-h} = (m-h)\frac{\pi}{m} = \pi - x_h, \quad \operatorname{tg} x_{m-h} = -\operatorname{tg} x_h;$$

der Zähler wird also $\Pi(\operatorname{tg}^2 x - \operatorname{tg}^2 x_h)$, wo über ein halbes Restsystem mod. m zu vervielfachen ist, das heißt über die Werte $h = 1, 2, \ldots, \dfrac{m-1}{2}$. — Auch die Pole (7) der Funktion (8) kann man zu Paaren zusammenfassen, nämlich

$$x_H = (2H+1)\frac{\pi}{2m} \text{ mit } x_{m-H-1} = [2(m-H-1)+1]\frac{\pi}{2m} = \pi - x^H;$$

der Nenner wird daher $\Pi(\operatorname{tg}^2 x - \operatorname{tg}^2 x_H)$, $H = 0, 1, \ldots, \dfrac{m-3}{2}$, und somit der Bruch (8)

$$\frac{\operatorname{tg} mx}{\operatorname{tg} x} = C\,\Pi\,\frac{\operatorname{tg}^2 x - \operatorname{tg}^2 x_h}{\operatorname{tg}^2 x - \operatorname{tg}^2 x_H}. \tag{9}$$

Schließlich lassen sich die Nullstellen x_H des Nenners zu denen x_h des Zählers in Beziehung bringen; nach (6) und (7) ist nämlich

$$x_H + x_h = (2H+1)\frac{\pi}{2m} + h\frac{\pi}{m} = [2(H+h)+1]\frac{\pi}{2m}.$$

Wählt man $2(H+h) = m-1$, was wegen der Ungeradheit von m möglich ist, so wird

$$x_H + x_h = \frac{\pi}{2}, \quad \operatorname{tg} x_H = \operatorname{ctg} x_h, \quad H = \frac{m-1}{2} - h.$$

In (9) eingesetzt, ergibt dies

$$\frac{\operatorname{tg} m x}{\operatorname{tg} x} = C \prod \frac{\operatorname{tg}^2 x - \operatorname{tg}^2 x_h}{\operatorname{tg}^2 x - \operatorname{ctg}^2 x_h} = c \prod \frac{\operatorname{tg}^2 x - \operatorname{tg}^2 x_h}{1 - \operatorname{tg}^2 x \operatorname{tg}^2 x_h} . \tag{10}$$

c ist wiederum ein fester Wert, den man leicht findet, indem man

$$x = \frac{\pi}{4}, \quad \operatorname{tg} x = 1, \quad \operatorname{tg} m x = \operatorname{tg} m \frac{\pi}{4} = (-1)^{\frac{m-1}{2}}$$

setzt; das liefert $c = (-1)^{\frac{m-1}{2}}$, also endgültig

$$\frac{\operatorname{tg} m x}{\operatorname{tg} x} = (-1)^{\frac{m-1}{2}} \prod_h \frac{\operatorname{tg}^2 x - \operatorname{tg}^2 x_h}{1 - \operatorname{tg}^2 x \operatorname{tg}^2 x_h} , \tag{11}$$

wo, wie gesagt, h ein halbes Restsystem (mod. m) durchläuft.

4. Bedeutet m eine der Primzahlen q und p, so ist demnach

$$\frac{\operatorname{tg} q x}{\operatorname{tg} x} = (-1)^{\frac{q-1}{2}} \prod_s \frac{t^2 - \beta^2}{1 - \beta^2 t^2} , \quad s = 1, 2, \ldots, \frac{q-1}{2} , \tag{12}$$

$$\frac{\operatorname{tg} p x}{\operatorname{tg} x} = (-1)^{\frac{p-1}{2}} \prod_r \frac{t^2 - \alpha^2}{1 - \alpha^2 t^2} , \quad r = 1, 2, \ldots, \frac{p-1}{2} \tag{13}$$

mit den Abkürzungen $\operatorname{tg} x = t$, $\operatorname{tg} \frac{s\pi}{q} = \beta$, $\operatorname{tg} \frac{r\pi}{p} = \alpha$.

Setzt man $x = \frac{r\pi}{p}$ in (12) und $x = \frac{s\pi}{q}$ in (13), so erhält man

$$\frac{\operatorname{tg} \frac{qr\pi}{p}}{\operatorname{tg} \frac{r\pi}{p}} = (-1)^{\frac{q-1}{2}} \prod_s \frac{\alpha^2 - \beta^2}{1 - \beta^2 \alpha^2} , \quad \frac{\operatorname{tg} \frac{ps\pi}{q}}{\operatorname{tg} \frac{s\pi}{q}} = (-1)^{\frac{p-1}{2}} \prod_r \frac{\beta^2 - \alpha^2}{1 - \alpha^2 \beta^2} ;$$

(4) und (5) nehmen daher die Gestalt an

$$\left(\frac{q}{p}\right) = \prod_r (-1)^{\frac{q-1}{2}} \prod_s \frac{\alpha^2 - \beta^2}{1 - \alpha^2 \beta^2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{r,s} \frac{\alpha^2 - \beta^2}{1 - \alpha^2 \beta^2} , \tag{14}$$

$$\left(\frac{p}{q}\right) = \prod_s (-1)^{\frac{p-1}{2}} \prod_r \frac{\beta^2 - \alpha^2}{1 - \alpha^2 \beta^2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{r,s} \frac{\beta^2 - \alpha^2}{1 - \alpha^2 \beta^2} . \tag{15}$$

Diese beiden Ausdrücke unterscheiden sich nur durch die Vorzeichen der Faktoren im Zähler, deren es $\frac{p-1}{2}\frac{q-1}{2}$ gibt; also folgt aus (14), (15) wirklich

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

— das Reziprozitätsgesetz.

5. Ich reiche diesen am 20. September 1961 in Oberwolfach auf einer Tagung über Geschichte der Mathematik gehaltenen Vortrag[1]) zum Druck ein, obwohl seit meinen in den Math. Ann. *83*, 280–285 (1921) und in den Monatsh. Math. *54*, 265–283 (1950) veröffentlichten Arbeiten zwei Abhandlungen von T. KUBOTA erschienen sind, die den Zusammenhang der Reziprozitätsgesetze mit transzendenten Funktionen betreffen[2]) [J. reine angew. Math. *208*, 35–50 (1961); Nagoya math. J. *19*, 1–13 (1961); meine soeben genannten Arbeiten über das kubische und biquadratische Reziprozitätsgesetz sind dort nicht erwähnt]. Zum Beweise des quadratischen Reziprozitätsgesetzes, bei dem KUBOTA sich nicht auf Primzahlen p und q beschränkt, benutzt er wie EISENSTEIN den Sinus, und er macht vom GAUSSschen Lemma Gebrauch, das ich hier nicht herangezogen habe.

Eingegangen den 20. August 1962

Note on Cross-sections in STIEFEL Manifolds

by GEORGE W. WHITEHEAD

(Extract from a letter to B. ECKMANN)

For which values of n, m, r $(n \geqq m > r)$ does the fibration $V_{n,m} \to V_{n,r}$ have a cross-section? The case $r = 1$ has recently been settled by ADAMS [2]. The remaining cases can easily be settled with the aid of your paper [4].

Theorems. Among the fibrations $V_{n,m} \to V_{n,r}$ $(n \geqq m > r \geqq 2)$, only the following have cross-sections:

$$V_{n,n} \to V_{n,n-1}, \quad V_{7,3} \to V_{7,2}, \quad V_{8,4} \to V_{8,3}.$$

Proof. Obviously, if $V_{n,m} \to V_{n,r}$ has a cross-section and $r < k < m$, so does $V_{n,k} \to V_{n,r}$. According to [4. p. 328, Hilfsatz], if $V_{n,m} \to V_{n,r}$ has a cross-section, so does $V_{n-1,m-1} \to V_{n-1,r-1}$. Moreover, [4, p. 337], if $V_{q,3} \to V_{q,2}$ has a cross-section, then R^{q+1} has a continuous multiplication $(x, y) \to xy$ such that $||xy|| = ||x|| \cdot ||y||$, and therefore [1] $q = 3$ or $q = 7$. Thus, if $V_{n,m} \to V_{n,r}$

[1]) Schon früher (im Studienjahr 1955/56) hatte ich im Mathematischen Colloquium der Universität Bagdad darüber vorgetragen, und, davon angeregt, hat Herr RAFIQ HUSSEIN bei der Prüfung für den Grad eines B. Sc. eine Thesis darüber verfaßt.

[2]) Den Hinweis auf sie verdanke ich Herrn P. ROQUETTE.