

NEUER UND ELEMENTARER BEWEIS DES LEGENDRESCHEN
RECIPROCITÄTS-GESETZES

GOTTHOLD EISENSTEIN

Crelle's Journal für die Reine und Angewandte Mathematik **27** H. 4 (1844) 322-
329
Math. Werke I, 100-107

Skon kserokopii artykułu z Crelle's, po edycji

25.

Neuer und elementarer Beweis des Legendreschen Reciprocitäts-Gesetzes.

(Von Herrn Stud. G. Eisenstein zu Berlin.)

Nicht leicht möchte die Geschichte eines mathematischen Satzes ein größeres Interesse darbieten, als die des berühmten Fundamentaltheorems für die quadratischen Reste. Man weiß, daß alle Bemühungen der größten Mathematiker vor *Gauß* an dieser steilen Klippe gescheitert sind, bis es endlich diesem Einzigen gelang, den verborgenen Pfad zu entdecken und bis zum Ziele vorzudringen. Er ist aber auch der Einzige geblieben, der in dieser Hinsicht etwas geleistet hat. Seit einer Reihe von fast dreißig Jahren ist den sechs Beweisen, welche *Gauß* von dem Satze gegeben hat, kein neuer hinzugefügt worden; und dies scheint weniger darin seinen Grund gehabt zu haben, daß man den Gegenstand als abgethan betrachtete, sondern vielmehr in der Schwierigkeit, die sich, selbst nach dem bereits Geleisteten, der Auffindung eines neuen Weges entgegenstellte.

Der neue Beweis, den wir in dieser Abhandlung mittheilen wollen, ist ganz elementarer Art. Er dürfte, aufser der Einfachheit, besonders Das als einen Vorzug in Anspruch nehmen, daß eine Operation, von deren Ausführbarkeit die Richtigkeit des Satzes abhängt, durch eine rein analytische Transformation allgemein ausführbar gemacht wird.

Wenn nämlich p und q irgend zwei ungerade Primzahlen bezeichnen, und $\left(\frac{q}{p}\right)$ das bekannte Legendresche Zeichen ist, so kommt der ganze Beweis darauf hinaus, die angezeigte Division

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

wirklich auszuführen, d. h. den Dividendus so umzuformen, daß er in der That durch den Divisor theilbar wird, oder die ganze Zahl \textcircled{C} allgemein so

zu bestimmen, daß der Ausdruck (A)

$$(-1)^{k(p-1) \cdot k(q-1)} \cdot p^{k(q-1)} - \left(\frac{q}{p}\right) = \mathfrak{G} q \text{ wird.}$$

I. Es seien $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_\mu$ allgemeine Glieder der Reihe

$$(\omega.) \quad 1, 2, 3, \dots, p-1.$$

Man bilde den Ausdruck

$$\left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_\mu}{p}\right) = E,$$

dessen Werth offenbar nur die *Einheit* mit dem positiven oder negativen Zeichen sein kann, und bezeichne die Summe

$$2. \quad \sum \left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_\mu}{p}\right),$$

welche sich über alle Werthe von

$$(\alpha.) \quad \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_\mu$$

erstreckt, durch $\psi(\mu)$. Da diese Summe nichts anders ist als die Potenz

$$\left[\sum_{\sigma=1}^{\sigma=p-1} \left(\frac{\sigma}{p}\right) \right]^\mu,$$

und da $\sum_{\sigma=1}^{\sigma=p-1} \left(\frac{\sigma}{p}\right) = 0$ ist, so hat man

$$3. \quad \psi(\mu) = 0.$$

II. Die Glieder der Summe $\psi(\mu)$ lassen sich in eine Anzahl p von Partialgruppen zerlegen. Da nämlich für jedes Glied E derselben die Summe

$$\alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_\mu = s$$

einer der p Zahlen $0, 1, 2, \dots, p-1$ nach dem mod. p congruent werden muß, so rechnen wir in die erste Partialgruppe alle diejenigen Glieder E , für welche $s \equiv 0 \pmod{p}$ ist; in die zweite Partialgruppe alle diejenigen, für welche $s \equiv 1 \pmod{p}$ ist, u. s. w.: allgemein, in die $\nu+1$ te Partialgruppe alle diejenigen Glieder E , für welche

$$4. \quad \alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_\mu \equiv \nu \pmod{p}$$

ist. Wir bezeichnen die p Partialreihen, in welche auf diese Weise $\psi(\mu)$ zerfällt, der Reihe nach durch

$$5. \quad \psi(\mu, 0), \psi(\mu, 1), \psi(\mu, 2), \dots, \psi(\mu, \nu), \dots, \psi(\mu, p-1).$$

III. Die Reihen $\psi(\mu, \nu)$ besitzen mehrere merkwürdige Eigenschaften. Man hat zunächst offenbar

$$6. \quad \psi(\mu, 0) + \psi(\mu, 1) + \dots + \psi(\mu, p-1) = \psi(\mu) = 0.$$

Ich behaupte ferner, daß für jeden *nicht durch p theilbaren* Werth von k ,

$$7. \quad \psi(\mu, k) = \left(\frac{k}{p}\right)^\mu \psi(\mu, 1) \text{ ist.}$$

In der That genügt es, in die für $\psi(\mu, k)$ stattfindende Bedingungscongruenz

$$\alpha_1 + \alpha_2 + \dots + \alpha_\mu \equiv k \pmod{p}$$

und in das allgemeine Glied der Summe selbst,

$$\alpha_i \equiv k\beta_i, \quad \alpha_2 \equiv k\beta_2, \quad \dots \quad \alpha_\mu \equiv k\beta_\mu \pmod{p}$$

zu substituiren, und zu bedenken, daß $\beta_1, \beta_2, \dots, \beta_\mu$ dann selbst wieder allgemeine Glieder der Reihe (ω) werden, um sich von der Richtigkeit der Formel (7.) zu überzeugen. Es ergibt sich hieraus, daß für einen *geraden Werth* von μ ,

$$8. \quad \psi(\mu, 1) = \psi(\mu, 2) = \text{etc.} \dots = \psi(\mu, p-1),$$

also auch, wegen (6.),

$$9. \quad \psi(\mu, 0) + (p-1)\psi(\mu, 1) = 0 \text{ und}$$

$$10. \quad \psi(\mu, 0) - \psi(\mu, 1) = -p\psi(\mu, 1),$$

dagegen für einen *ungeraden Werth* von μ ,

$$11. \quad \psi(\mu, k) = \left(\frac{k}{p}\right) \psi(\mu, 1),$$

$$12. \quad \psi(\mu, 1) + \psi(\mu, 2) + \dots + \psi(\mu, p-1) = 0 \text{ und}$$

$$13. \quad \psi(\mu, 0) = 0 \text{ ist.}$$

IV. Um den Werth der Summen $\psi(\mu, \nu)$ vollständig bestimmen zu können, bilde man eine Recursionsformel, durch welche die Summen $\psi(\mu, \nu)$ in die einfacheren $\psi(\mu-1, \nu)$ ausgedrückt werden.

Man erhält nach der Definition:

$$\psi(\mu, \nu) = \sum \left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_{\mu-1}}{p}\right) \left(\frac{\alpha_\mu}{p}\right) \\ \{\alpha_1 + \alpha_2 + \dots + \alpha_{\mu-1} + \alpha_\mu \equiv \nu \pmod{p}\}.$$

Schreibt man das allgemeine Glied E der Summe so:

$$\left(\frac{\alpha_\mu}{p}\right) \times \left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_{\mu-1}}{p}\right),$$

und die Bedingungscongruenz so:

$$\alpha_1 + \alpha_2 + \dots + \alpha_{\mu-1} \equiv \nu - \alpha_\mu \pmod{p},$$

so zeigt sich auf der Stelle, dafs die Relation

$$14. \quad \psi(\mu, \nu) = \sum \left(\frac{\alpha_\mu}{p} \right) \psi(\mu-1, \nu - \alpha_\mu)$$

Statt findet, wo das Σ zur Rechten eine *einfache* Summe anzeigt, die sich auf die Werthe von α_μ bezieht. Es sei, um diese Recursionsformel anzuwenden, zuerst $\nu=0$. Für diesen Fall giebt die Formel

$$\psi(\mu, 0) = \sum \left(\frac{\alpha_\mu}{p} \right) \psi(\mu-1, -\alpha_\mu).$$

Da $-\alpha_\mu$ nicht durch p theilbar ist, so hat man nach (7.)

$$\psi(\mu-1, -\alpha_\mu) = \left(\frac{-\alpha_\mu}{p} \right)^{\mu-1} \psi(\mu-1, 1).$$

Setzt man diesen Werth hinein, so kommt

$$\psi(\mu, 0) = \sum \left(\frac{-\alpha_\mu}{p} \right)^\mu \cdot \left(\frac{-1}{p} \right) \psi(\mu-1, 1).$$

Aber $\sum \left(\frac{-\alpha_\mu}{p} \right)^\mu$ ist offenbar $\equiv p-1$ oder $\equiv 0$, je nachdem μ *gerade* oder *ungerade* ist: also erhält man endlich

$$15. \quad \psi(\mu, 0) = \left(\frac{-1}{p} \right) (p-1) \psi(\mu-1, 1), \text{ oder } = 0,$$

je nachdem μ *gerade* oder *ungerade* ist.

Um ebenso $\psi(\mu, k)$ zu bestimmen, wenn k nicht durch p theilbar ist, bemerke ich, dafs für einen *geraden* Werth von μ diese Summe schon durch (15.) mitgegeben ist. In der That, die Formel (9.) giebt

$$\psi(\mu, k) = \frac{-1}{p-1} \psi(\mu, 0),$$

also erhält man aus (15.)

$$16. \quad \psi(\mu, k) = - \left(\frac{-1}{p} \right) \psi(\mu-1, 1); \quad \mu \text{ gerade.}$$

Um endlich den Werth von $\psi(\mu, k)$ auszudrücken, wenn μ *ungerade* ist, bedienen wir uns wieder der Recursionsformel (14.). Sie giebt

$$\psi(\mu, k) = \sum \left(\frac{\alpha_\mu}{p} \right) \psi(\mu-1, k - \alpha_\mu).$$

Dasjenige Glied der Reihe zur Rechten, welches dem Werthe $\alpha_\mu = k$ entspricht, liefert $\left(\frac{k}{p} \right) \psi(\mu-1, 0)$; für alle übrigen Glieder ist $k - \alpha_\mu$ *nicht*.

durch p theilbar, und da $\mu - 1$ eine *gerade* Zahl ist, so kann man die Gleichungen (8.) benutzen, und man sieht, daß alle Glieder der obigen Reihe, mit Ausnahme des schon erhaltenen, gefunden werden, wenn man den gemeinschaftlichen Factor $\psi(\mu - 1, 1)$ nach und nach mit

$$\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots \left(\frac{k-1}{p}\right), \left(\frac{k+1}{p}\right), \dots \left(\frac{p-1}{p}\right)$$

multiplicirt, so daß sich die Reihe folgendermaßen schreiben läßt:

$$\begin{aligned} \left(\frac{k}{p}\right) \psi(\mu-1, 0) + \sum_{\sigma=1}^{\sigma=p-1} \left(\frac{\sigma}{p}\right) \psi(\mu-1, 1) - \left(\frac{k}{p}\right) \psi(\mu-1, 1) \\ = \left(\frac{k}{p}\right) [\psi(\mu-1, 0) - \psi(\mu-1, 1)] \\ = -\left(\frac{k}{p}\right) p \psi(\mu-1, 1) \quad (\text{nach (10.)}). \end{aligned}$$

Wir erhalten also

$$17. \quad \psi(\mu, k) = -\left(\frac{k}{p}\right) p \psi(\mu-1, 1); \quad \mu \text{ ungerade};$$

und namentlich für $k=1$,

$$18. \quad \psi(\mu, 1) = -\left(\frac{-1}{p}\right) \psi(\mu-1, 1), \text{ oder } = -p \psi(\mu-1, 1),$$

je nachdem μ *gerade* oder *ungerade* ist.

V. Die Formel (18.) liefert nach und nach das System von Gleichungen

$$\begin{aligned} \psi(2\lambda+1, 1) &= -p \psi(2\lambda, 1), \\ \psi(2\lambda, 1) &= -\left(\frac{-1}{p}\right) \psi(2\lambda-1, 1), \\ \psi(2\lambda-1, 1) &= -p \psi(2\lambda-2, 1), \\ \psi(2\lambda-2, 1) &= -\left(\frac{-1}{p}\right) \psi(2\lambda-3, 1), \\ &\dots \dots \dots \\ \psi(3, 1) &= -p \psi(2, 1), \\ \psi(2, 1) &= -\left(\frac{-1}{p}\right) \psi(1, 1). \end{aligned}$$

Multiplicirt man alle diese Gleichungen mit einander, hebt auf beiden Seiten den gemeinschaftlichen Factor

$$\psi(2\lambda, 1) \psi(2\lambda-1, 1) \dots \psi(2, 1)$$

heraus, und bemerkt, daß $\psi(1, 1) = \left(\frac{1}{p}\right) = 1$ und $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ ist,

so erhält man

$$19. \quad \psi(2\lambda + 1, 1) = (-1)^{\frac{1}{2}(p-1)\lambda} \cdot p^\lambda,$$

und hieraus noch nach (18.)

$$20. \quad \psi(2\lambda, 1) = -(-1)^{\frac{1}{2}(p-1)\lambda} \cdot p^{\lambda-1}.$$

VI. Ist jetzt q eine zweite, von p verschiedene ungerade Primzahl, so hat man nach (19.)

$$21. \quad \psi(q, 1) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} \cdot p^{\frac{1}{2}(q-1)}.$$

Wir wollen nun untersuchen, ob in der Summe

$$\psi(q, 1) = \sum \left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_q}{p}\right) \\ \{\alpha_1 + \alpha_2 + \dots + \alpha_q \equiv 1 \pmod{p}\}$$

Glieder vorkommen können, für welche gleichzeitig

$$22. \quad \alpha_1 = \alpha_2 = \alpha_3 = \text{etc.} = \alpha_q \text{ ist.}$$

Diese Bedingungen erfordern die folgende,

$$q\alpha_1 \equiv 1 \pmod{p};$$

eine Congruenz, welche nur für einen einzigen Werth $\alpha_1 = r$ erfüllt wird. Es existirt also nur ein einziges Glied in $\psi(q, 1)$, für welches alle Elemente α einander gleich sind, und der Werth dieses Gliedes ist

$$\left(\frac{r}{p}\right)^q = \left(\frac{r}{p}\right) = \left(\frac{q}{p}\right).$$

Schliessen wir dieses Glied von der Summe $\psi(q, 1)$ aus, so kommt

$$23. \quad (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} \cdot p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right) = \mathcal{A} = \sum \left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_q}{p}\right),$$

wo in der Summe zur Rechten $\alpha_1, \alpha_2, \dots, \alpha_q$ sämtlich allgemeine Glieder der Reihe 1, 2, 3, $\dots, p-1$ vorstellen, und wo alle Combinationen genommen werden müssen, für welche den beiden Bedingungen genügt wird, dafs erstens

$$24. \quad \alpha_1 + \alpha_2 + \dots + \alpha_q \equiv 1 \pmod{p},$$

und dafs zweitens

$$25. \quad \text{nicht gleichzeitig } \alpha_1 = \alpha_2 = \text{etc.} = \alpha_q \text{ sei.}$$

Der Ausdruck \mathcal{A} erscheint hier in der *elementarsten* Weise dargestellt, in welcher man überhaupt eine ganze Zahl zerfallen kann; nämlich als *ein Aggregat von positiven und negativen Einheiten*. Sehen wir jetzt, ob sich unter dieser Form die *Division* durch die Primzahl q wird verrichten lassen.

VII. Es sei

$$\alpha_1 = m_1, \alpha_2 = m_2, \dots \alpha_q = m_q$$

irgend ein System von Werthen, welches den Bedingungen genügt, denen die Elemente α in (24.) und (25.) unterworfen sind, so dafs

26. $m_1 + m_2 + \dots + m_q \equiv 1 \pmod{p},$

27. und dafs nicht zugleich $m_1 = m_2 = \text{etc.} = m_q.$

Dann genügen offenbar die folgenden q Systeme, welche durch cyclische Permutation der Elemente aus einander entstehen und von denen das erste das vorgelegte ist, nemlich

$$28. \begin{cases} m_1, & m_2, & m_3, & \dots & m_{q-1}, & m_q, \\ m_2, & m_3, & m_4, & \dots & m_q, & m_1, \\ m_3, & m_4, & m_5, & \dots & m_1, & m_2, \\ \dots & \dots & \dots & \dots & \dots & \dots \\ m_q, & m_1, & m_2, & \dots & m_{q-2}, & m_{q-1}, \end{cases}$$

allen den Bedingungen (24.) und (25.); wie unmittelbar aus der symmetrischen Natur von (26.) und (27.) in Beziehung auf ihre Elemente klar ist. Diese q Systeme sind alle von einander *verschieden*, weil q eine Primzahl ist und *nicht* alle Elemente einander gleich sind; sie ertheilen aber dem allgemeinen Gliede der Summe (23.) alle genau *denselben* Werth. Es folgt hieraus, dafs die Totalsumme (23.) in eine Anzahl von Gruppen getheilt werden kann, so dafs jede Gruppe q *einander gleiche* Glieder enthält; und somit ist die Theilbarkeit unseres Ausdrucks \mathcal{A} durch q erwiesen. Es ist leicht, hiernach den Quotienten selbst hinzuschreiben. Derselbe ist

$$29. \frac{(-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right)}{q} = \mathfrak{S} = \sum \left(\frac{\alpha_1}{p}\right) \left(\frac{\alpha_2}{p}\right) \dots \left(\frac{\alpha_q}{q}\right);$$

wo sich die Summe über alle Werthe der verschiedenen α erstreckt, welche den in (24.) und (25.) ausgesprochenen Bedingungen genügen, wo aber noch die Beschränkung hinzutritt, dafs von je q Systemen, welche auseinander durch *cyclische* Permutation der Elemente wie in (28.) entstehen, immer *nur ein einziges* genommen werden mufs.

VIII. Das Legendresche Reciprocitätsgesetz ist eine unmittelbare Folgerung der eben veranstalteten Umformung. In der That, wie eben gezeigt wurde, ist

$$(-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right) \text{ durch } q \text{ theilbar;}$$

aufserdem ist aber

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

folglich ist auch

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

durch q theilbar, was nicht anders geschehen kann, als wenn

$$30. \quad \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)} \left(\frac{q}{p}\right)$$

ist; was zu beweisen war.

Berlin im April 1844.