XXXIV.

Über den Zellerschen Beweis des quadratischen Reziprozitätssatzes.

[Festschrift Heinrich Weber zu seinem siebzigsten Geburtstag am 5. März 1912 gewidmet von Freunden und Schülern. Leipzig und Berlin 1912, S. 23—36.]

Das Lemma, auf welches Gauß seinen dritten und fünften Beweis des Reziprozitätssatzes gegründet hat, ist später der Ausgangspunkt für viele andere Beweise desselben Satzes geworden[1]). Unter allen diesen Beweisen scheint mir der einfachste der zu sein, welchen Chr. Zeller[2]) mir in einem Briefe vom 8. Juli 1872 mitgeteilt hat; dieser Brief schließt mit den durchaus zutreffenden Worten: „Man braucht also jene Hilfsgrößen nicht, welche bisher bei dem Beweise unseres Satzes verwendet worden sind und denselben umständlich gemacht haben.“ In der Tat vermeidet Zeller gänzlich die in dem dritten Beweise von Gauß eingeführten größten Ganzen $[x]$ und gelangt zum Ziele, indem er zwei neue Betrachtungen mit dem Lemma von Gauß verbindet. Einige Monate später hat Zeller (in dem Sitzungsberichte der Berliner Akademie vom 16. Dezember 1872) einen sehr ähnlichen Beweis veröffentlichen lassen, in welchem an Stelle der zweiten Betrachtung eine dritte tritt, wodurch aber die Einfachheit nach meiner Ansicht ein wenig gelitten hat. Mag nun diese Abänderung noch so geringfügig scheinen, so glaube ich doch Zellers Verdienst in ein helleres Licht zu rücken, wenn ich den wesentlichen Inhalt des genannten Briefes in freier Umarbeitung und geänderter Bezeichnung jetzt bekannt mache.

Hierzu ist es freilich nötig, die bekannten Tatsachen, auf denen das Lemma von Gauß beruht, kurz in Erinnerung zu bringen, und

---

[1]) Eine sehr eingehende Darstellung dieser Beweise findet man bei P. Bachmann (Niedere Zahlentheorie, erster Teil, 1902, Seite 212—286).

[2]) Damals Pfarrer und Bezirks-Schulinspektor zu Weiler bei Schorndorf (Württemberg), später Seminarrektor in Markgröningen, wo er im Jahre 1899 als Oberschulrat verstorben ist.

zwar in der Form, daß unter dem Reste einer ganzen Zahl in bezug auf einen ungeraden Modulus $p > 1$ immer ihr absolut kleinster, also zwischen den Grenzen $\pm\frac{p}{2}$ gelegener Rest verstanden werden soll. Läßt man nun, wenn q relative Primzahl zu p ist, den Faktor h alle ganzen Zahlen

$$1, 2, \cdots, \frac{p-1}{2}$$

des Intervalles $0 < h < \frac{p}{2}$ durchlaufen, und bildet man die Reste a und die Quotienten y für die Produkte

$$hq = a + yp \equiv a \pmod{p}, \tag{1}$$

so sind diese Reste a alle von Null und auch voneinander verschieden, weil zwei verschiedene Faktoren h immer zwei inkongruente Produkte hq erzeugen; da ferner auch die Summe von zwei Produkten hq niemals durch p teilbar ist, so sind sogar die absoluten Werte aller Reste a verschieden und stimmen folglich in ihrem Komplex mit den Faktoren h völlig überein; jeder Faktor h ist auch der absolute Wert von einem und nur einem Reste a. Bedeutet daher P das Produkt aller Faktoren h, und m die Anzahl derjenigen Reste a, welche negativ sind, so ist $P(-1)^m$ das Produkt aller Reste a, und durch Multiplikation aller Kongruenzen (1) ergibt sich

$$Pq^{\frac{p-1}{2}} \equiv P(-1)^m \pmod{p}.$$

Wird jetzt angenommen, daß die ungerade Zahl p eine Primzahl ist, so ist das Produkt P nicht teilbar durch p, mithin

$$q^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}.$$

Das nach Euler benannte Kriterium besteht bekanntlich darin, daß die Potenz linker Hand $\equiv +1$ oder $\equiv -1 \pmod{p}$ ist, je nachdem q quadratischer Rest oder Nichtrest von p ist, und wenn man diese positive oder negative Einheit nach Legendre durch das Symbol $\left(\frac{q}{p}\right)$ bezeichnet, so kann das Resultat der vorhergehenden Betrachtung durch die Gleichung

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

ausgedrückt werden[1]). Hierin besteht das obenerwähnte Lemma von Gauß.

Ist q ebenfalls eine ungerade positive Primzahl, so wird der zu beweisende Reziprozitätssatz bekanntlich durch die Gleichung

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

ausgedrückt, welche jetzt mit Hilfe des Lemma von Gauß eine einfachere Gestalt annimmt. Durchläuft nämlich der Faktor k alle ganzen Zahlen

$$1, 2, \cdots, \frac{q-1}{2}$$

des Intervalls $0 < k < \frac{q}{2}$, und bildet man wie in (1) die Reste b und die Quotienten x für die Produkte

$$kp = b + xq \equiv b \pmod{q}, \tag{2}$$

so sind die absoluten Werte der Reste b wieder alle verschieden, und ebenso wird

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

wo n die Anzahl derjenigen Reste b bedeutet, die negativ sind; hierdurch verwandelt sich der zu beweisende Satz offenbar in die Kongruenz

$$m + n \equiv \frac{p-1}{2}\,\frac{q-1}{2} \pmod{2}, \tag{3}$$

welche auch so ausgesprochen werden kann: Die Summe $m + n$ ist stets und nur dann ungerade, wenn $p \equiv q \equiv -1 \pmod{4}$ ist.

Nachdem diese Umformung des Reziprozitätssatzes, welche die Grundlage für den dritten und fünften Beweis von Gauß bildet, in Erinnerung gebracht ist, will ich jetzt die beiden Hauptpunkte hervorheben, auf denen Zellers Beweis beruht. Hierbei setze ich lediglich voraus, es seien p, q relative[2]) Primzahlen, beide ungerade, positiv

---

[1]) E. Schering hat bemerkt, daß dieselbe auch für das von Jacobi verallgemeinerte Symbol von Legendre gilt (Monatsbericht der Berliner Akademie vom 22. Juni 1876).

[2]) Der folgende Beweis gilt daher zufolge der vorhergehenden Anmerkung auch für den verallgemeinerten Reziprozitätssatz.

und > 1; auch soll (wie in der Berliner Darstellung) p die kleinere dieser beiden Zahlen bedeuten.

Die erste Bemerkung Zellers geht aus einer Vergleichung der beiden Reihen (1) und (2) hervor und besteht darin, daß alle Gleichungen (1) aus ebenso vielen Gleichungen (2) nur durch Umsetzung ihrer Glieder entspringen. Ist z. B. $p = 11$, $q = 27$, so erhält man die Reihe (2) und daraus die Reihe (1) in der folgenden Tabelle:

$1 \cdot p = +11 + 0 \cdot q$	
$2 \cdot p = -5 + 1 \cdot q$	$1 \cdot q = +5 + 2 \cdot p$
$3 \cdot p = +6 + 1 \cdot q$	
$4 \cdot p = -10 + 2 \cdot q$	
$5 \cdot p = +1 + 2 \cdot q$	$2 \cdot q = -1 + 5 \cdot p$
$6 \cdot p = +12 + 2 \cdot q$	
$7 \cdot p = -4 + 3 \cdot q$	$3 \cdot q = +4 + 7 \cdot p$
$8 \cdot p = +7 + 3 \cdot q$	
$9 \cdot p = -9 + 4 \cdot q$	
$10 \cdot p = +2 + 4 \cdot q$	$4 \cdot q = -2 + 10 \cdot p$
$11 \cdot p = +13 + 4 \cdot q$	
$12 \cdot p = -3 + 5 \cdot q$	$5 \cdot q = +3 + 12 \cdot p$
$13 \cdot p = +8 + 5 \cdot q$	

Um diese Beziehung zwischen den beiden Reihen allgemein zu beweisen, setze man jede Gleichung (1) in die Form

$$yp = -a + hq;$$

aus der Definition der Zahlen a, h und aus unserer Annahme $p < q$ folgt

$$-\frac{p}{2} < -a < +\frac{p}{2}, \quad p < hq < \frac{p}{2}q,$$

hieraus durch Addition und Division durch p

$$+\frac{1}{2} < y < \frac{q+1}{2},$$

mithin auch $0 < y < \frac{q}{2}$. Also ist jeder in der Reihe (1) auftretende Quotient y auch einer der Faktoren k in der Reihe (2), und da jede Zahl $-a$ zwischen den Grenzen $\pm\frac{p}{2}$, also gewiß auch zwischen $\pm\frac{q}{2}$ liegt, so ist $-a$ der diesem Faktor $k = y$ entsprechende Rest b des Produktes kp in (2), und der Quotient $x = h$, w. z. b. w.

Mit diesen Resten $b = -a$, deren Anzahl $= \frac{p-1}{2}$ ist, sind aber alle zwischen den Grenzen $\pm\frac{p}{2}$ liegenden Reste b in (2) erschöpft, weil, wie oben bemerkt, die absoluten Werte aller Reste b voneinander verschieden sind. Die Anzahl m der negativen Reste a in (1) ist daher zugleich die Anzahl derjenigen positiven Reste b in (2), welche $< \frac{p}{2}$ sind; fügt man zu diesen m positiven Resten b noch alle n negativen Reste b hinzu, so ist die Summe $m + n$ die Anzahl aller Reste b in (2), welche in dem Intervalle

$$-\frac{q}{2} < b < +\frac{p}{2} \tag{4}$$

liegen.

In dem obigen Beispiel $p = 11$, $q = 27$, wo $m = 2$, $n = 5$, liegen im Intervalle (4) die sieben Reste $b = -10, -9, -5, -4, -3, +1, +2$; die übrigen sechs Reste sind $b = 6, 7, 8, 11, 12, 13$.

Nachdem hiermit die Bedeutung der Summe $m + n$ für die Reihe (2) festgestellt ist, beantwortet Zeller die Hauptfrage nach ihrer Parität, ob sie gerade oder ungerade ist, durch eine zweite Betrachtung, deren einfacher Grundgedanke in Folgendem besteht. Wenn es in einem endlichen System von Elementen b ein Gesetz gibt, das jedem b ein bestimmtes Element b' desselben Systems zuordnet, und zwar so symmetrisch, daß umgekehrt $(b')' = b$ wird, so hat die Anzahl aller b offenbar dieselbe Parität wie die Anzahl der Fälle, in denen $b' = b$ ist. Für unsere Untersuchung, wo es sich um die Reste b in der Reihe (2) handelt, gewinnt Zeller eine solche Verteilung in symmetrische Paare b, b' auf folgende Weise.

Durchläuft der Faktor k alle seine Werte, und setzt man

$$k + k' = \frac{q+1}{2}, \tag{5}$$

so durchläuft k' offenbar dieselben Werte in umgekehrter Folge, und jedem solchen Faktorenpaar k, k' entspricht ein Restepaar

$$b \equiv kp, \quad b' \equiv k'p \pmod{q}.$$

Da jeder Rest b durch einen und nur einen Faktor k erzeugt wird, so ist durch b vermöge (5) auch der Faktor k', mithin auch der zugehörige Rest b' vollständig bestimmt, und aus der Symmetrie der Gleichung (5) in bezug auf k, k' folgt, daß umgekehrt $(b')' = b$ ist.

Durch Addition der beiden vorstehenden Kongruenzen mit Rücksicht auf (5) folgt die Kongruenz

$$b + b' \equiv \frac{q+1}{2} p \pmod{q},$$

welche die gegenseitige Abhängigkeit der beiden, ein symmetrisches Paar bildenden Reste b, b' vollständig ausdrückt. Dies läßt sich aber noch genauer verfolgen. Zufolge der Definition der Reste b, b' liegt einerseits ihre Summe $b + b'$ gewiß zwischen den Grenzen $\pm q$; andererseits ist das ihr kongruente Produkt

$$(6) \qquad \frac{q+1}{2} p = \frac{p-q}{2} + \frac{p+1}{2} q = \frac{p+q}{2} + \frac{p-1}{2} q,$$

mithin

$$b + b' \equiv \frac{p-q}{2} \equiv \frac{p+q}{2} \pmod{q},$$

und da zufolge unserer Annahme $p < q$ die beiden Zahlen $\frac{p \mp q}{2}$ ebenfalls zwischen den Grenzen $\pm q$ liegen, so ist

$$\text{entweder } b + b' = \frac{p-q}{2}$$

$$\text{oder } b + b' = \frac{p+q}{2}.$$

Im ersten Fall sind beide Reste b, b' algebraisch $< \frac{p}{2}$; wäre nämlich einer derselben, z. B. $b' > \frac{p}{2}$, so wäre der andere $b < -\frac{q}{2}$, was der Definition von b widerspricht. Im zweiten Fall sind beide Reste $> \frac{p}{2}$; wäre nämlich z. B. $b' < \frac{p}{2}$, so wäre $b > \frac{q}{2}$, was abermals unmöglich ist. Mithin sondern sich die beiden Fälle in folgender Weise scharf voneinander:

$$(7) \qquad \text{I.} \quad b + b' = \frac{p-q}{2}, \; -\frac{q}{2} < b, \, b' < +\frac{p}{2},$$

$$(8) \qquad \text{II.} \quad b + b' = \frac{p+q}{2}, \; +\frac{p}{2} < b, \, b' < +\frac{q}{2},$$

und zugleich leuchtet ein, daß b' in jedem dieser beiden Intervalle dieselben Werte wie b, aber in umgekehrter Größenfolge durchläuft.

Wir betrachten jetzt nur noch das erste Intervall (7), welches identisch mit dem obigen in (4) ist und folglich genau $m + n$ Reste b enthält. Diese Summe $m + n$ wird daher immer gerade sein, wenn jedes symmetrische Restpaar in (7) aus zwei ungleichen Resten b, b' besteht. Da ferner der Fall $b = b'$ immer und nur dann eintrifft, wenn zugleich $k = k'$ ist, so geschieht dies in (7) gewiß und nur in dem einzigen Fall, wenn gleichzeitig

$$b = b' = \frac{p-q}{4}, \quad k = k' = \frac{q+1}{4},$$

also

$$p \equiv q \equiv -1 \pmod 4 \tag{9}$$

ist, und da alle anderen, etwa in (7) enthaltenen Restpaare aus zwei ungleichen Resten b, b' bestehen, so ist die Summe $m + n$ in diesem und nur in diesem Falle (9) ungerade.

Hiermit ist die Kongruenz (3), also auch der Reziprozitätssatz wirklich bewiesen.

Zur Erläuterung bemerke ich noch folgendes. Ist $q \equiv 1 \pmod 4$, so folgt aus (5), daß der Fall $k = k'$ niemals eintreten kann; es wird daher jedes Restpaar sowohl in (7) wie in (8) aus zwei ungleichen Resten b, b' bestehen, und folglich ist sowohl die Anzahl $m + n$ der Reste b in (7), wie die Anzahl $\frac{q-1}{2} - m - n$ der Reste b in (8) gerade. Ist dagegen $q \equiv -1 \pmod 4$, so tritt der Fall $k = k'$, also auch $b = b'$, gewiß einmal ein, nämlich in (7) oder (8), je nachdem $p \equiv -1$ oder $\equiv +1 \pmod 4$ ist.

In dem obigen Beispiel $p = 11$, $q = 27$, wo $m = 2$, $n = 5$, ordnen sich die sieben Reste des Intervalles (7) in die vier Paare

$$(b, b') = (-10, +2), (-9, +1), (-5, -3), (-4, -4)$$

mit der Summe $b + b' = -8$, und die sechs Reste des Intervalles (8) zerfallen in die drei Paare

$$(b, b') = (6, 13), (7, 12), (8, 11)$$

mit der Summe $b + b' = +19$. Da dieses Beispiel den Bedingungen (9) genügt, so entspricht dem Faktor $k = k' = 7$ das im Intervall (7) liegende, aus zwei gleichen Resten bestehende Paar $b = b' = -4$.

Im vorstehenden habe ich Zellers scharfsinnigen Beweis (auf Grund des Briefes vom 8. Juli 1872) etwas ausführlicher dargestellt, weil er mit geringstem Aufwande von Rechnung eine sehr deutliche

Einsicht in den Bau und den Zusammenhang der beiden Reihen (1), (2) gibt und deshalb besonders geeignet zum Vortrage vor Anfängern erscheint. Um ihn mit der sehr kurz gefaßten Berliner Darstellung (vom 16. Dezember 1872) bequem zu vergleichen, ändere ich die in der letzteren gewählte Bezeichnung so ab, daß sie mit unserer obigen übereinstimmt, und außerdem will ich zur Abkürzung die Anzahl der Reste b innerhalb des Intervalles

$$(10) \qquad -\frac{q}{2} < b < -\frac{p}{2}$$

mit t bezeichnen. Durch eine Betrachtung, die nahezu mit dem ersten Teile des obigen Beweises übereinstimmt, ergibt sich zunächst die Zerlegung

$$(11) \qquad m + n = \frac{p-1}{2} + t,$$

und handelt sich es daher jetzt noch um die Frage, wann die Anzahl t gerade oder ungerade ist. Dazu dient wieder eine Verteilung der Reste b in symmetrische Paare, die aber von der obigen, durch (5) bestimmten wesentlich abweicht und deshalb hier näher behandelt werden soll. Schließt man in (2) den größten Faktor $k = \frac{q-1}{2}$ aus, dem zufolge (6) nach Subtraktion von p der positive Rest $b = \frac{q-p}{2}$ entspricht, und setzt man

$$(12) \qquad k + k'' = \frac{q-1}{2},$$

so durchläuft k'' dieselben $\frac{q-3}{2}$ Faktoren wie k, und jedes Paar von Resten $b \equiv kp$, $b'' \equiv k''p \pmod{q}$ liefert eine zwischen den Grenzen $\pm q$ liegende Summe

$$b + b'' \equiv \frac{q-1}{2} p \equiv -\frac{p+q}{2} \equiv \frac{q-p}{2} \pmod{q}.$$

Verfährt man ähnlich wie oben, so erhält man wieder zwei scharf getrennte Intervalle

$$\text{III.} \quad b + b'' = -\frac{p+q}{2}; \quad -\frac{q}{2} < b,\ b'' < -\frac{p}{2}$$

$$\text{IV.} \quad b + b'' = +\frac{q-p}{2}; \quad -\frac{p}{2} < b,\ b'' < +\frac{q}{2},$$

in denen b'' immer dieselben Werte wie b durchläuft. Da das Intervall III mit dem in (10) identisch ist und folglich t Reste b enthält (weil der einzige ausgeschlossene Rest $b = \frac{q-p}{2}$ außerhalb dieses Intervalles liegt), so ergibt sich durch deren Verteilung in symmetrische Paare b, b'', daß diese Anzahl t stets und nur dann ungerade ist, wenn der Fall

$$k = k'' = \frac{q-1}{4},\ b = b'' = -\frac{p+q}{4}$$

eintritt, was immer und nur dann geschieht, wenn $q \equiv 1$, $p \equiv -1$ (mod. 4) ist. Durch Kombination dieses Resultates mit der obigen Zerlegung (11) gelangt schließlich die Berliner Darstellung, indem sie die einzelnen Fälle der Reste von p, q (mod. 4) durchgeht, ebenfalls zu dem Endergebnis, daß die Summe $m + n$ dann und nur dann ungerade ist, wenn $p \equiv q \equiv -1$ (mod. 4) ist, w. z. b. w.

Aus mehreren Gründen verdient wohl der frühere Beweis den Vorzug vor diesem zweiten. Da der Charakter der Summe $m + n$ (mod. 2) das einzige Ziel der Untersuchung bildet, so erscheint ihre Zerlegung (11) in zwei Bestandteile von vornherein als ein Umweg, der sich am Schluß nochmals fühlbar macht; außerdem ist die hier benutzte, durch (12) bestimmte Verteilung der Reste b in symmetrische Paare weniger einfach als die frühere, schon weil sie den Ausschluß eines Faktors k und des entsprechenden Restes b erfordert.

Als Zeller mir seinen Beweis mitteilte, kannte er den dritten Beweis von Gauß nur in der schon vereinfachten Darstellung, wie sie sich in §§ 43, 44 der Vorlesungen über Zahlentheorie von Dirichlet (zweite Auflage 1871) findet. In meiner Antwort (vom 13. Juli 1872) drückte ich ihm meine Freude über seinen Beweis aus, der so geradenwegs auf das Ziel zusteuert, und fügte eine kurze Darstellung des fünften Beweises von Gauß hinzu, der ihm augenscheinlich noch unbekannt war. Dies hat Zeller veranlaßt, mir noch einmal zu schreiben (am 7. Oktober 1872); auch in diesem Briefe findet sich noch keine Spur von der eben besprochenen zweiten Symmetrie der Reihe (2), die den Nerv des Beweises in der Berliner Darstellung bildet; er enthält aber noch zwölf Formeln, die von gewissen Summen der Reste a, b und der Quotienten x, y in den Reihen (1), (2) handeln und damals, wie ich glaube, noch unbekannt waren. Diese

Formeln, deren Beweise Zeller zum Teil andeutet, sind eigentlich nur Kombinationen von sechs verschiedenen Relationen, die ich jetzt im Anschluß an den ersten Beweis von Zeller noch ableiten will. Hierbei bezeichne ich die Reste a, b bzw. mit a_1, b_1 oder mit a_2, b_2, je nachdem sie negativ oder positiv sind, und die Summen der Zahlen

$$h,\ a,\ a_1,\ a_2,\ y;\ k,\ b,\ b_1,\ b_2,\ x$$

bzw. mit

$$H,\ A,\ A_1,\ A_2,\ Y;\ K,\ B,\ B_1,\ B_2,\ X.$$

Da die absoluten Werte $-a_1$, a_2 aller Reste a mit den Faktoren h, ebenso die absoluten Werte $-b_1$, b_2 aller Reste b mit den Faktoren k übereinstimmen, so erhält man zunächst

$$(13) \qquad -A_1 + A_2 = H = \frac{1}{2}\frac{p+1}{2}\frac{p-1}{2},$$

$$(14) \qquad -B_1 + B_2 = K = \frac{1}{2}\frac{q+1}{2}\frac{q-1}{2}.$$

Zwei neue Gleichungen folgen aus der Betrachtung der beiden Intervalle (7), (8). Während die $m+n$ Reste b in (7) aus den n negativen Resten b_1 und den m positiven Zahlen $-a_1$ bestehen, so verbleiben nach Entfernung der letzteren aus den Resten b_2 die $\frac{q-1}{2} - m - n$ Reste b in (8), und da b' in jedem der beiden Intervalle dieselben Werte wie b durchläuft, so folgt durch Summation

$$(15) \qquad 2\,(B_1 - A_1) = \frac{p-q}{2}(m+n),$$

$$(16) \qquad 2\,(B_2 + A_1) = \frac{p+q}{2}\left(\frac{q-1}{2} - m - n\right).$$

Durch Auflösung dieser vier Gleichungen ergibt sich

$$(17) \qquad -4A_1 = p(m+n) - \frac{p-1}{2}\frac{q-1}{2},$$

$$(18) \qquad -4B_1 = q(m+n) - \frac{p-1}{2}\frac{q-1}{2},$$

$$(19) \qquad +4A_2 = \frac{2p+q+1}{2}\frac{p-1}{2} - p(m+n),$$

$$(20) \qquad +4B_2 = \frac{2q+p+1}{2}\frac{q-1}{2} - q(m+n),$$

woraus auch noch

$$2A = 2(A_1 + A_2) = \frac{p+q}{2}\,\frac{p-1}{2} - p(m+n), \tag{21}$$

$$2B = 2(B_1 + B_2) = \frac{p+q}{2}\,\frac{q-1}{2} - q(m+n) \tag{22}$$

folgt.

Es leuchtet ein, daß aus jeder dieser Formeln auch die Kongruenz (3), also der Reziprozitätssatz folgt; außerdem will ich bemerken, daß diese Kongruenz durch die schärfere

$$m + n \equiv -\frac{p-1}{2}\,\frac{q-1}{2} \pmod 4 \tag{23}$$

ersetzt werden kann, die man leicht erhält, wenn man z. B. die Gleichung (17) mit p multipliziert und bedenkt, daß $p^2 \equiv 1$, also $p(p-1) \equiv -(p-1) \pmod 8$ ist.

Besonders hervorzuheben ist aber, daß alle diese Formeln, obwohl sie auf der ausdrücklichen Annahme $p < q$ beruhen, augenscheinlich auch für die entgegengesetzte Annahme $p > q$ gelten, weil die Ausdrücke für B_1, B_2 und B aus denen für A_1, A_2 und A durch gleichzeitige Vertauschung von p mit q (und von m mit n) hervorgehen.

Um endlich die Summen X, Y der Quotienten x, y ebenfalls durch p, q, m, n auszudrücken, kann man verschiedene Wege einschlagen. Da die Ausdrücke für H, A, K, B schon bekannt sind, so liegt es nahe, hierzu die beiden Gleichungen

$$Hq = A + Yp, \quad Kp = B + Xq \tag{24}$$

zu benutzen, die aus (1), (2) durch Summation entstehen, und zufolge der eben hervorgehobenen Bemerkung genügt es, nur eine der beiden Summen, z. B. X zu berechnen, weil hieraus die andere Y durch Vertauschung von p mit q hervorgehen muß. Aus (14) und (22) folgt nun

$$2(Kp - B) = \frac{q+1}{2}\,p\,\frac{q-1}{2} - \frac{p+q}{2}\,\frac{q-1}{2} + q(m+n)$$

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

und da die in der Klammer rechts enthaltene Summe bei Vertauschung von p mit q ungeändert bleibt, so folgt aus (24) die Doppelgleichung

$$2X = 2Y = \frac{p-1}{2}\,\frac{q-1}{2} + m + n, \tag{25}$$

worin abermals der Reziprozitätssatz enthalten ist. Zugleich ergibt sich aus der Kongruenz (23), daß die Summe $X = Y$ stets gerade ist.

Ein anderer Weg, die Summe X zu bestimmen, ergibt sich aus der durch (5) bestimmten Verteilung der Reste b in symmetrische Paare. Bezeichnet man mit x, x' die den Faktoren k, k' entsprechenden Quotienten, so ist

$$kp = b + xq, \quad k'p = b' + x'q,$$

also

$$(b + b') + (x + x')q = \frac{q+1}{2}\,p,$$

und aus (6), (7), (8) folgt

$$x + x' = \frac{p+1}{2} \text{ im Intervalle (7)},$$

$$x + x' = \frac{p-1}{2} \text{ im Intervalle (8)}.$$

Da nun x' sowohl in (7) wie in (8) dieselben Werte wie x durchläuft, deren Anzahl bzw. $m + n$ und $\frac{q-1}{2} - m - n$ ist, so erhält man im ganzen

$$2X = \frac{p+1}{2}(m+n) + \frac{p-1}{2}\left(\frac{q-1}{2} - m - n\right),$$

was mit (25) übereinstimmt.

Hiermit ist das Wesentliche der Formeln erschöpft, die Zeller mir in seinem zweiten Briefe (vom 7. Oktober 1872) mitgeteilt hat, wo er auch beiläufig bemerkt, daß die Größen X, $X - n$, $X - m$ bzw. mit den auf ganz andere Weise definierten Anzahlen α, β, γ im fünften Beweise von Gauß übereinstimmen (wo die Zeichen m, M, n, N durch die ihnen hier entsprechenden p, q, m, n zu ersetzen sind); doch wird der Zusammenhang zwischen den beiden verschiedenen Definitionen nicht untersucht.

Die Gleichheit der beiden Quotientensummen X, Y ist hier auf einem Wege erkannt, der alle früheren Resultate voraussetzt. Diese Gleichheit besteht, wie ich noch bemerken will, selbst dann, wenn die beiden ungeraden Zahlen p, q irgendeinen gemeinsamen Teiler haben; der kürzeste Weg, sie zu beweisen, scheint der folgende zu sein, wobei es auch gleichgültig bleibt, welche der Zahlen p, q die

kleinere ist. Läßt man die Faktoren h, k alle ihre Werte durchlaufen, so kann die Anzahl α der Fälle, in denen die Produktsumme

$$hq + kp > \frac{pq}{2}$$

wird, auf zwei verschiedene Arten bestimmt werden. Wählt man zuerst einen bestimmten Faktor k und setzt $kp = b + xq$ wie in (2), so findet man leicht, daß dieser Quotient x zugleich die Anzahl aller derjenigen Faktoren h ist, welche für diesen Wert k der vorstehenden Forderung genügen, und hieraus folgt offenbar $\alpha = X$. Wählt man aber zuerst einen bestimmten Faktor h und setzt $hq = a + yp$ wie in (1), so erhält man auf dieselbe Weise die Antwort $\alpha = Y$; mithin ist $X = Y$, w. z. b. w.