Über das quadratische Reziprozitätsgesetz.

Von G. Frobenius.

Die vom Gaussischen Lemma ausgehenden Beweise des Reziprozitätsgesetzes erfordern eine Abzählung von Gitterpunkten, die sich durch Zerschneiden und Zusammensetzen von Figuren in ähnlicher Weise ausführen läßt wie die zahlreichen Beweise des pythagoreischen Lehrsatzes. Die größte Bewunderung hat mit Recht die Art erregt, wie Zeller (Monatsber. 1874, S. 846) diese Abzählung ganz direkt ausführt. Aber auch seine Schlüsse lassen sich noch durch passende Anwendung jenes Verfahrens und konsequentere Benutzung seines Symmetrieprinzips vereinfachen. Für die Behauptung, daß

$$\varkappa = \frac{1}{4}(p-1)(q-1)+\lambda+\mu$$

gerade ist, erhält man so einen überaus anschaulichen und der geometrischen Deutung unmittelbar zugänglichen Beweis, der die Vorzüge des fünften Beweises von Gauss mit denen des dritten vereinigt. Seine von keiner Rechnung getrübte Durchsichtigkeit läßt deutlich erkennen, daß der Schluß, der in den meisten Darstellungen als der Nerv des Beweises erscheint, für die Herleitung des Reziprozitätsgesetzes selbst ganz überflüssig ist. Notwendig ist er, um zu zeigen, daß $\varkappa$ durch 4 teilbar ist, was noch nirgends bemerkt worden zu sein scheint. Jene Behauptung begründe ich näher durch Vergleichung des Beweises mit dem fünften und dritten Beweise von Gauss.

Voraus schicke ich einige Bemerkungen über die Definition, die Zolotareff für das Jacobische Zeichen gegeben hat.

§ 1.

Das Zeichen von Zolotareff.

Ist p eine positive ungerade Zahl, so bezeichne ich mit $\Re(x)$ den kleinsten positiven Rest der ganzen Zahl x (mod p). Ist q relativ prim zu p, so stimmen die Zahlen

$$\Re(q),\ \Re(2q),\ \cdots\ \Re((p-1)q) \tag{1.}$$

abgesehen von der Reihenfolge mit den Zahlen

$$1\ ,\ 2\ ,\ \cdots\ p-1 \tag{2.}$$

überein, bilden also eine Permutation derselben. Je nachdem diese gerade oder ungerade ist, hat das JACOBI-LEGENDREsche Zeichen $\left(\frac{q}{p}\right)$ den Wert $+1$ oder -1. Diese Definition hat für den Fall, wo p eine Primzahl ist, ZOLOTAREFF gegeben in einer Arbeit über das Reziprozitätsgesetz, *Nouv. Ann.* (2) *tom. XI, p. 354*. Darüber habe ich in den Fortschritten der Mathematik, Bd. 4 (1872), S. 75, berichtet, und ich habe jene Definition schon damals auf den Fall ausgedehnt, wo p irgendeine ungerade Zahl ist. Die Ausdehnung, die ich wiederholt in meinen Vorlesungen vorgetragen habe, ist seither auch von LERCH und anderen gefunden worden. Daß das JACOBIsche Zeichen ein *Gruppencharakter* ist, tritt durch diese Definition am deutlichsten in Erscheinung. Dabei wird der Umstand benutzt, daß sich jede Gruppe als Gruppe von Permutationen darstellen läßt. Ist $q \equiv r \pmod p$, so ist

$$\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right). \tag{3.}$$

Die Permutation (1.) ist gerade oder ungerade, je nachdem darin die Anzahl $\varkappa$ der Inversionen gerade oder ungerade ist. Sind x und y zwei verschiedene Zahlen der Reihe (2.), so entsteht eine Inversion, wenn

$$x<y\ ,\qquad \Re(xq) > \Re(yq) \tag{4.}$$

ist. Ersetzt man q durch $-q$, so enthält die Permutation

$$\Re(-q)\ ,\ \Re(-2q),\ \cdots \Re\big(-(p-1)q\big)$$

$$\frac{1}{2}(p-1)(p-2)-\varkappa$$

Inversionen, und folglich ist, weil $p-2$ ungerade ist,

$$\left(\frac{-q}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left(\frac{q}{p}\right) \tag{5.}$$

und insbesondere für $q=1$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}. \tag{6.}$$

Für $q=2$ enthält die Permutation

$$2,\ 4,\ \cdots p-1,\ 1,\ 3,\ \cdots p-2$$

$$1+2+3+\cdots+\frac{1}{2}(p-1) = \frac{1}{8}(p^2-1)$$

Inversionen, und mithin ist

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}. \tag{7.}$$

Ist allgemein

$$x+y' = p\ , \qquad y+x' = p,$$

so ist auch

$$\Re(xq)+\Re(y'q) = p, \qquad \Re(yq)+\Re(x'q) = p.$$

Unter den Bedingungen (4.) ist auch

$$x' < y'\ , \qquad \Re(x'q) > \Re(y'q).$$

Demnach können die Inversionen einander paarweise zugeordnet werden, und wenn die beiden Inversionen eines Paares verschieden sind, so können sie unberücksichtigt bleiben, weil es nur darauf ankommt, ob $\varkappa$ gerade oder ungerade ist. Es braucht also nur die Anzahl λ der Inversionen gezählt zu werden, wofür $x = x'$, also auch $y = y'$ ist. Für solche ist

$$x+y = p\ , \quad \Re(xq)+\Re(yq) = p,$$

und folglich nach (4.)

$$x < \frac{1}{2}p\ , \quad \Re(xq) > \frac{1}{2}p.$$

Demnach ist

$$\left(\frac{q}{p}\right) = (-1)^{\lambda}, \tag{8.}$$

wo λ angibt, wie oft der kleinste positive Rest von

$$q,\ 2q, \cdots \frac{1}{2}(p-1)q \qquad (\mathrm{mod}\ p)$$

größer als $\frac{1}{2}p$, oder der absolut kleinste Rest negativ ist (Gauss, Schering).

Aus dieser Eigenschaft des Zeichens von Zolotareff ergibt sich (§ 2) das Reziprozitätsgesetz

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}. \tag{9.}$$

In Verbindung mit $\left(\frac{1}{p}\right) = 1$ genügen die Formeln (3.), (5.) und (9.) vollständig zur Berechnung des Zeichens $\left(\frac{q}{p}\right)$. Nach (3.) ist $\left(\frac{q}{p}\right) = \left(\frac{\pm r}{p}\right)$, wo $\pm r$ der absolut kleinste Rest von q (mod $2p$), also $r < p$ und ungerade ist. Ist dieser Rest negativ, so führt (5.) das Zeichen auf $\left(\frac{+r}{p}\right)$, und dann (9.) auf $\left(\frac{p}{r}\right)$ zurück. Bei Fortsetzung dieses Verfahrens werden Zähler und Nenner immer kleiner, bis man auf $\left(\frac{1}{p}\right) = 1$ kommt. (Auf diesem Wege findet man auch $\left(\frac{2}{p}\right) = \left(\frac{2-p}{p}\right)$.) Da nun das Jacobische Zeichen dieselben Eigenschaften besitzt, so muß es mit dem Zeichen von Zolotareff übereinstimmen.

§ 2.

Das Reziprozitätsgesetz.

Sei x eine Veränderliche, deren *Bereich* auf die Werte

$$1, 2, \cdots \frac{1}{2}(p-1) \qquad (x)$$

beschränkt ist. Der absolut kleinste Rest von $qx \pmod p$ ist $qx - py$, falls y so gewählt wird, daß diese Differenz zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ liegt, was stets und nur in einer Weise möglich ist. Demnach gibt λ an, für wie viele Wertepaare x, y

$$0 > qx - py > -\frac{1}{2}p \qquad (\lambda)$$

ist. Hier entspricht nicht jedem der $\frac{1}{2}(p-1)$ Werte von x ein Wert von y, sondern nur λ von ihnen, und jedem dieser λ Werte nur ein Wert y. Da für diesen

$$py > qx > 0, \quad py < qx + \frac{1}{2}p < \frac{1}{2}qp + \frac{1}{2}p$$

ist, so kann y auf die Werte

$$1, 2, \cdots \frac{1}{2}(q-1) \qquad (y)$$

beschränkt werden, deren Bereich ich mit (y) bezeichne.

Ebenso gibt μ an, für wieviel Stellen

$$0 > py - qx > -\frac{1}{2}q \qquad (\mu)$$

ist, wenn x die Werte $1, 2, \cdots \frac{1}{2}(p-1)$ und y die Werte $1, 2, \cdots \frac{1}{2}(q-1)$ durchläuft. Solcher Wertepaare x, y gibt es

$$\rho = \frac{1}{2}(p-1)(q-1),$$

deren Bereich ich mit (x, y) bezeichne.

Für jede dieser ρ Stellen ist entweder

(1.) $$py - qx > \frac{1}{2}p \qquad (\delta)$$

oder

(2.) $$\frac{1}{2}p > py - qx > 0 \qquad (\lambda)$$

oder

(3.) $$0 > py - qx > -\frac{1}{2}q \qquad (\mu)$$

oder

(4.) $$-\frac{1}{2}q > py - qx. \qquad (\delta').$$

An keiner Stelle ist[1] $py - qx = 0$. Der Bedingung (1.) mögen δ, der Bedingung (4.) δ' Stellen genügen. Dann ist

$$\rho = \lambda + \mu + \delta + \delta'. \tag{5.}$$

Nun ist aber

$$\delta' = \delta. \tag{6.}$$

Denn die Ungleichheit (1.) geht durch die Substitutionen

$$x = \frac{1}{2}(p+1) - x' \ , \quad y = \frac{1}{2}(q+1) - y' \tag{7.}$$

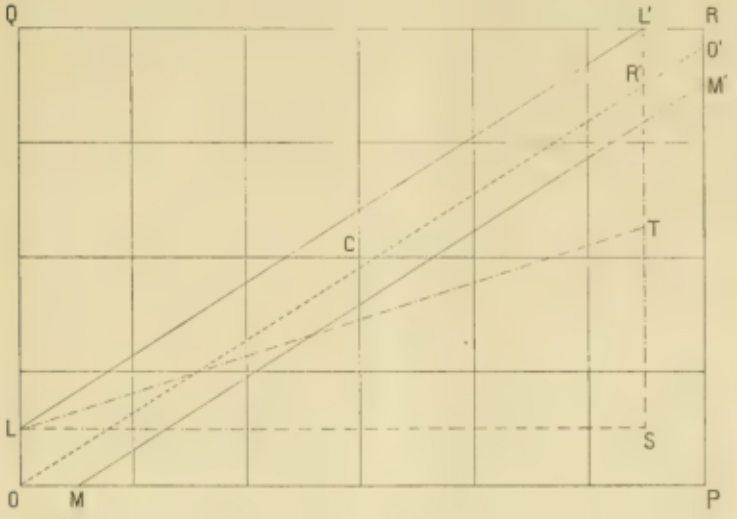
in (4.) über, und wenn x die Werte $1, 2, \cdots \frac{1}{2}(p-1)$ durchläuft, so durchläuft x' dieselben Werte. Ebenso stimmt der Bereich (y) mit (y') überein. Mithin ist

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}. \tag{8.}$$

Daß für ebenso viele Werte $p(2y-1) > q\,2x$ ist, wie $p\,2y < q(2x-1)$ erkennt man noch unmittelbarer, wenn man die Substitutionen (7.) auf die Gestalt

$$\begin{array}{llll} 2x & = p-(2x'-1) \ , & 2y & = q-(2y'-1) \\ 2x-1 & = p-\ 2x' & , \ 2y-1 & = q-\ 2y' \end{array} \tag{9.}$$

bringt.



[1] Haben p und q den größten gemeinsamen Divisor d, so sind hier noch die $\frac{1}{2}(d-1)$ Lösungen der Gleichung $py = qx$ zu berücksichtigen, $x = p', 2p', \cdots \frac{1}{2}(d-1)p'$, wo $p = dp'$ ist (vgl. FIELDS, *Amer. J. Bd. 13, S. 189*).

Die geometrische Bedeutung dieser Schlüsse ist klar. In der Figur ist $p = 11$, $q = 7$. R hat die Koordinaten $\frac{1}{2}(p+1)$, $\frac{1}{2}(q+1)$, L, L', M, M' sind die Mitten der Seiten der betreffenden Quadrate. Die 3 parallelen Geraden OO', LL', MM' haben die Gleichungen

$$py = qx, \quad py = qx + \frac{1}{2}p, \quad py = qx - \frac{1}{2}q.$$

Die Substitution (7.) ordnet je zwei Punkte einander zu, die zum Zentrum C des Rechtecks

$$a = \frac{1}{4}(p+1), \quad b = \frac{1}{4}(q+1)$$

symmetrisch liegen. Ich werde sie *symmetrische* Punkte im Rechteck nennen.

Innerhalb des Rechtecks $OPQR$ liegen ρ Gitterpunkte, λ zwischen OO' und LL', μ zwischen OO' und MM'. Entfallen δ Punkte auf das Dreieck $LL'Q$, so entfallen auf das kongruente Dreieck $MM'P$ ebenso viele, und mithin ist

$$\rho = \lambda + \mu + 2\delta. \tag{10.}$$

Diesen anschaulichen Beweis hätte man längst gefunden, hätte nicht Eisenstein (*Crelles Journal Bd. 28, S. 246*) seine Nachfolger irre geführt durch Zeichnen eines Rechtecks $OP'Q'R'$, worin R' die Koordinaten $\frac{1}{2}p$, $\frac{1}{2}q$ besitzt, also auf OO' liegt. Übrigens hat Eisenstein nicht, wie häufig gesagt wird, durch geometrische Betrachtungen das Reziprozitätsgesetz bewiesen, sondern nur die Formel (15.) aber nicht die Formel (6.) oder (16.).

Um die Beziehungen des obigen Beweises zu anderen Darstellungen klarer darlegen zu können, bringe ich ihn noch auf folgende Form. Wenn an λ' Stellen des Bereiches (x, y)

$$py - qx < 0 \tag{11.}$$

$$(\lambda')$$

ist, so ist nach (2.) an $\lambda + \lambda'$ Stellen

$$py - qx < \frac{1}{2}p \tag{12.}$$

$$(\lambda + \lambda').$$

Auf diese Weise wird die Grenze 0 (die Grenzlinie OO') entfernt, die allein die volle Symmetrie der Figur stört. Wenn an μ' Stellen

$$py - qx > 0 \tag{13.}$$

$$(\mu')$$

ist, so ist nach (3.) an $\mu + \mu'$ Stellen

$$qx - py < \frac{1}{2}q \tag{14.}$$

$$(\mu + \mu').$$

Da $py-qx$ an jeder der ε Stellen entweder positiv oder negativ ist, so ist nach (11.) und (13.)

$$\lambda' + \mu' = \varepsilon. \tag{15.}$$

Weil die Bedingung (12.) durch die Substitutionen (7.) in (14.) übergeht, so ist

$$\lambda + \lambda' = \mu + \mu'. \tag{16.}$$

Mithin ist

$$\lambda + \mu \equiv \lambda' + \mu' = \frac{1}{4}(p-1)(q-1) \pmod 2.$$

Macht man in der Ungleichheit (12.) nur die eine der beiden Substitutionen (7.), so erkennt man, daß $\lambda + \lambda' = \mu + \mu'$ die Anzahl der Stellen ist, die der symmetrischen Bedingung

$$\frac{2x}{p} + \frac{2y}{q} > 1 \tag{17.}$$

genügen; oder auch der Bedingung

$$\frac{2x-1}{p} + \frac{2y-1}{q} < 1. \tag{18.}$$

Nun kann man auch dem Beweise von ZELLER eine Form geben, die seinem Mangel an Symmetrie abhilft. Nach (2.) und (3.) ist $\lambda + \mu$ die Anzahl der Stellen x, y, die der Bedingung

$$\frac{1}{2}p > py - qx > -\frac{1}{2}q \qquad (\lambda + \mu)$$

genügen[1]. Diese aber geht durch die Substitution (7.) in sich selbst über. Gehört x, y zu den $\lambda + \mu$ Stellen, so gehört dazu auch x', y'. Daher ist $\lambda + \mu$ gerade, außer wenn

$$x = x' = \frac{1}{4}(p+1) \quad , \quad y = y' = \frac{1}{4}(q+1)$$

ganze Zahlen sind, wenn also p und q beide von der Form $4n-1$ sind. Dann und nur dann ist $\lambda + \mu$ ungerade.

Liegt der Punkt x, y auf dem Streifen zwischen LL' und MM' (dem Sechseck $OLL'RM'M$, oder dem Parallelogramm $LL'M'M$, dessen Diagonalen sich in C schneiden), so liegt der symmetrische

[1] Erst nach Abschluß dieser Arbeit ist mir die Mitteilung von DEDEKIND über die ursprüngliche Form des ZELLERschen Beweises in der Festschrift für HEINRICH WEBER zu Gesicht gekommen. Bis zu dieser Stelle stimmt dieser Beweis mit dem obigen überein, nur daß $p < q$ vorausgesetzt wird. Dies liegt daran, daß die im Anfang dieses Paragraphen bestimmten Grenzen für y nicht aus der Ungleichheit (2.), sondern aus $\frac{1}{2}p > py - qx > -\frac{1}{2}p$ erhalten sind. Daß $y > 0$ ist, kann man aber daraus nur schließen, wenn $p < 2q$ ist.

Punkt x', y' auch darauf. Dieser Streifen nebst allen seinen Gitterpunkten kommt durch eine halbe Umdrehung um den Mittelpunkt C des Rechtecks mit sich selbst zur Deckung. Daher ist die Anzahl $\lambda + \mu$ dieser Gitterpunkte gerade, außer wenn das Zentrum der Symmetrie

$$a = \frac{1}{4}(p+1) \quad , \quad b = \frac{1}{4}(q+1)$$

selbst ein Gitterpunkt ist. Bei diesem Beweise ist die Hinzunahme fremder Gitterpunkte gänzlich vermieden worden.

§ 3.

Der fünfte Beweis von Gauss.

Gauss benutzt in seinem *dritten* Beweise ebenfalls die Zahlen $\lambda + \lambda'$ und $\mu + \mu'$, die er in § 7 mit L und M bezeichnet. Leider ist ihm die Beziehung $L = M$ entgangen; sonst hätte er uns viele Beweise des Reziprozitätsgesetzes erspart. Statt dessen zeigt er, daß $L = \lambda + \lambda'$ gerade ist. Aus denselben Gründen ist auch $\mu + \mu'$ gerade, und mithin ist

$$\lambda + \mu \equiv \lambda' + \mu' = \rho \pmod 2 .$$

Demnach können die Beweise in zwei Klassen geteilt werden, je nachdem sie darauf ausgehen zu zeigen, daß $L = M$ ist, oder daß L gerade ist. Den letzteren Weg halte ich für einen Umweg. Eine ähnliche Einteilung macht Schering (*Gött. Nachr. 1879, S. 217*), der in dieses Gebiet nach Gauss am tiefsten eingedrungen ist.

Aus dem Prinzip der Symmetrie abzuleiten, daß $\lambda + \lambda'$ gerade ist, ist mir nur durch die Deutung gelungen, die Gauss in seinem *fünften* Beweise für diese Zahl entwickelt hat.

Er ordnet dort jeder Stelle u, v eine Zahl z zu, die zwischen $-\frac{1}{2}pq$ und $+\frac{1}{2}pq$ liegende Zahl, die den beiden Kongruenzen

$$z \equiv u \pmod p \quad , \quad z \equiv v \pmod q$$

genügt. Unter den Zahlen z, die den ε Stellen x, y entsprechen, seien α positiv, δ negativ. Unter den Zahlen z, die den ε Stellen $-x, y$ entsprechen, seien β positiv, δ negativ. Dann ist

$$\rho = \alpha + \delta = \beta + \gamma .$$

Ist x eine *bestimmte* der Zahlen $1, 2, \cdots \frac{1}{2}(p-1)$, so sind $\frac{1}{2}(q-1)$ der Zahlen $1, 2, \cdots \frac{1}{2}(pq-1)$ kongruent $-x \pmod p$, nämlich

$$-x+p, \; -x+2p, \; \cdots -x+\frac{1}{2}(q-1)p .$$

*Irgend*einem der $\frac{1}{2}(p-1)$ Werte von $-x$ sind daher $\frac{1}{2}(p-1)\frac{1}{2}(q-1) - \rho$ jener $\frac{1}{2}(pq-1)$ Zahlen (mod p) kongruent. Von diesen ρ Zahlen sind β irgendeinem der Werte von y (mod q) kongruent, δ irgendeinem der Werte von $-y$, und λ sind $\equiv 0$ (mod q). Dies sind die λ Zahlen aus der Reihe

$$q,\quad 2q,\quad \cdots \frac{1}{2}(p-1)q,$$

die einem $-x$ (mod p) kongruent sind. Daher ist

$$\rho - \beta + \delta + \lambda = \gamma + \delta + \mu.$$

Aus diesen vier Gleichungen ergeben sich die Formeln

$$(1.)\quad \begin{array}{llll} 2\alpha = \rho+\lambda+\mu, & \alpha = \lambda+\lambda' = \mu+\mu', & LL'P \simeq MM'Q, \\ 2\beta = \rho-\lambda+\mu, & \beta = \lambda' & , & OO'P \quad , \\ 2\gamma = \rho+\lambda-\mu, & \gamma = \mu' & , & OO'Q \quad , \\ 2\delta = \rho-\lambda-\mu, & \delta = \lambda'-\mu = \mu'-\lambda, & LL'Q \simeq MM'P. \end{array}$$

In der ersten Spalte stehen die Formeln von GAUSS, die Bedeutung der beiden anderen Spalten erläutere ich unten. Jede der vier Formeln beweist das Reziprozitätsgesetz. Ganz besonders deutlich zeigen sie, wie unnötig es für den Beweis dieses Satzes zu wissen, daß α gerade ist.

Der fünfte Beweis von GAUSS ist (aber nicht in der Darstellung von KRONECKER) ebenso einfach wie der des § 2, aber nicht so durchsichtig und anschaulich. Dafür hat er den Vorzug, daß man aus der darin benutzten Definition von α leicht erkennen kann, daß α gerade ist.

Ist das Zentrum der Symmetrie

$$a = \frac{1}{4}(p+1) \quad , \quad b = \frac{1}{4}(q+1)$$

ein Gitterpunkt, so ist $p \quad q \quad -1$, also $pq \quad 1$ (mod 4), und folglich ist

$$c = -\frac{1}{4}(pq-1)$$

die ihm entsprechende Zahl z, und diese ist negativ.

Entspricht aber dem Punkte x, y eine positive Zahl z, so entspricht dem symmetrischen Punkte x', y' nach (7.) § 2 die Zahl

$$(2.)\qquad z' = \frac{1}{2}(pq+1) - z,$$

die ebenfalls positiv ist. Folglich zerfällen die α *positiven* Punkte x, y, (denen ein positiver Wert von z entspricht), in $\frac{1}{2}\alpha$ Paare symmetri-

scher Punkte. (Ist z negativ, so ist $z' = -\frac{1}{2}(pq-1)-z$ ebenfalls negativ.)

Die zweite Spalte der obigen Tabelle erhält man, indem man die Formeln von Gauss mit den Relationen (15.) und (16.), § 2 vergleicht. In der dritten Spalte habe ich mit $OO'P$ und $OO'Q$ die beiden Figuren bezeichnet, in die das Rechteck durch die Gerade OO' geteilt wird. Der Punkt O' liegt nämlich auf der Seite PR oder QR, je nachdem $p > q$ oder $p < q$ ist. (Ist also $p > q$, so ist $\lambda' \leq \mu'$ und $\lambda \geq \mu$.) In ähnlicher Weise bezeichne ich die Figuren, in die das Rechteck durch LL' oder MM' geteilt wird. Demnach ist $LL'P$ das Fünfeck $OLL'RP$, und enthält α Gitterpunkte.

Mit voller Absicht habe ich hier das Zeichen und den Begriff der größten ganzen Zahl unter einer gegebenen Größe vermieden, weil er den Sinn der Beweise des Reziprozitätsgesetzes mehr verdunkelt als erhellt. (Vgl. z. B. den Beweis von Hacks, *Acta Math. Bd. 12, S. 109*, der mit dem Beweise in § 2 nahe verwandt ist.) Dieser Ansicht scheint auch Dedekind zu sein. Dagegen werde ich mich im folgenden einer Zeichensprache bedienen, die eine Vereinfachung der von Schering benutzten ist. Sind die Variabeln x und y so beschränkt wie oben, so bezeichne ich die Anzahl der Stellen des Bereiches (x, y), an denen $f(x,y) < g(x,y)$ ist mit $[f(x,y) < g(x,y)]$. Ist nirgends $f(x,y) = g(x,y)$, so ist, wie in der Formel (15.) § 2

$$(3.) \qquad [f(x,y) < g(x,y)] + [f(x,y) > g(x,y)] = \rho.$$

Die Zahlen $\lambda', \mu', \lambda, \mu$ sind dann durch die Gleichungen

$$(4.) \qquad \lambda' = [py < qx] \quad , \qquad \mu' = [py > qx],$$

$$(5.) \qquad \lambda + \lambda' = [p(2y-1) < q2x] = \mu + \mu' = [p2y > q(2x-1)]$$

definiert, die Zahlen von Gauss durch

$$(6.) \quad \begin{array}{llll} \alpha = [p(2y-1) < q2x] & = [p2y & > q(2x-1)], \\ \beta = [p2y & < q2x] & = [p(2y-1) > q(2x-1)], \\ \gamma = [p(2y-1) < q(2x-1)] & = [p2y & > q2x], \\ \delta = [p2y & < q(2x-1)] & = [p(2y-1) > q2x]. \end{array}$$

Die zweite Formel geht jedesmal durch die Substitution (9.) § 2 aus der ersten hervor.

Die Verteilung der δ *negativen* Punkte im Rechteck läßt sich genauer beschreiben: Ist ξ, η ein solcher (im Innern oder auch am Rande des Rechtecks, aber die 4 Ecken O, P, Q, R ausgeschlossen), so ist der entsprechende negative Wert $z = \xi - py = \eta - qx$. Die Zahl δ ist die Anzahl der Lösungen der Gleichung

$$(7.) \qquad py - qx = \xi - \eta,$$

wenn jeder der beiden Punkte x, y und ξ, η das Innere des Rechtecks durchläuft.

Die Bedingung hängt nur von $\xi - \eta$ ab. Ist also ξ', η' ein Punkt des Rechtecks, für den $\xi' - \eta' = \xi - \eta$ ist, so ist er auch ein negativer Punkt (dagegen ist $\xi = \frac{1}{2}(p-1)$, $\eta = \frac{1}{2}(q-1)$, $z = \frac{1}{2}(pq-1)$ positiv, und $\xi' = \frac{1}{2}(p+1)$, $\eta' = \frac{1}{2}(q+1)$, $z' = -\frac{1}{2}(pq-1)$ negativ). Daher braucht man nur die negativen Punkte auf dem Rande zu suchen (mit Ausschluß der Ecken). Sei wieder x auf das Gebiet (x), y auf (y), § 2 beschränkt. Von den absolut kleinsten Resten der Zahlen $-qx \pmod p$ [bzw. $-py \pmod q$] seien λ [μ] positiv, $\xi_1, \xi_2, \cdots \xi_\lambda$ [$\eta_1, \eta_2, \cdots \eta_\mu$]. Man nehme auf OP die λ Punkte mit den Abszissen $\xi_1, \xi_2, \cdots \xi_\lambda$ und auf OQ die μ Punkte mit den Ordinaten $\eta_1, \eta_2, \cdots \eta_\mu$, und ziehe durch jeden dieser $\lambda + \mu$ (negativen) Punkte eine Parallele zur Geraden $y = x$, die den Winkel POQ halbiert. Die Punkte im Innern des Rechtecks, die auf diesen $\lambda + \mu$ (zu C symmetrischen) Geraden liegen, sind die δ negativen Punkte.

Ist $p > q$, so ist $\lambda \geqq \mu$ und

$$\frac{1}{2}(q-1) \leqq \lambda + \mu \leqq \frac{1}{2}(p-1). \tag{8.}$$

Beide Grenzen werden erreicht, z. B. die untere für $p - 2 = q = 4n + 1$, die obere für $p - 2 = q = 4n - 1$. Denn die $\lambda + \mu$ positiven Zahlen $\xi_1, \cdots \xi_\lambda, \eta_1, \cdots \eta_\mu$ sind alle untereinander verschieden, die Zahlen $1, 2, \cdots \frac{1}{2}(q-1)$ kommen alle unter ihnen vor, von den Zahlen zwischen $\frac{1}{2}q$ und $\frac{1}{2}p$ fehlen $\nu = \frac{1}{2}(p-1) - \lambda - \mu$. Sind dies $\tau_1, \tau_2, \cdots \tau_\nu$, so ist

$$\tau_1 + \tau_\nu = \tau_2 + \tau_{\nu-1} = \cdots = \frac{1}{2}(p+q), \tag{9.}$$

und in derselben Beziehung stehen die zwischen $\frac{1}{2}q$ und $\frac{1}{2}p$ liegenden Werte unter den Zahlen $\xi_1, \xi_2, \cdots \xi_\lambda$. Denn ist $py - qx = \xi$, so ist $qx < py \leqq \frac{1}{2}(q-1)p < \frac{1}{2}(p-1)q$, also $x \leqq \frac{1}{2}(p-3)$. Daher ist auch

$$\xi' = p\left(\frac{1}{2}(q+1) - y\right) - q\left(\frac{1}{2}(p-1) - x\right) = \frac{1}{2}(p+q) - \xi \tag{10.}$$

eine der Zahlen $\xi_1, \cdots \xi_\lambda$. Wenn $\frac{1}{4}(p+q)$ eine ganze Zahl ist, so ist sie ein ξ oder τ, d. h. ist die Gleichung $py - qx = \frac{1}{4}(p+q)$ möglich oder nicht, je nachdem $q \equiv -1$ oder $+1 \pmod 4$ ist; und dasselbe gilt für $\frac{1}{4}(p-q)$. Aus diesen Überlegungen kann man nach

Zeller schließen, daß $\lambda + \mu$ nur dann ungerade ist, wenn $p \equiv q \equiv -1 \pmod 4$ ist. Man hat aber immer umständliche Betrachtungen anzustellen, wenn man sich, wie in Gleichung (10.) einer anderen Symmetrie bedient, als der durch (7.), § 2 ausgedrückten. Solcher Symmetrien kann man übrigens leicht noch andere aufstellen, wenn man $p > mq$ voraussetzt.

Ist $\xi_1 > \xi_2 > \cdots > \xi_\lambda$ und $\eta_1 > \eta_2 > \cdots \eta_\mu$, so ergeben sich mit Hilfe von (7.), § 2 die Relationen

$$(11.) \qquad \xi_1 - \eta_1 = \cdots = \xi_\alpha - \eta_\alpha = \xi_{\alpha+1} + \xi_\lambda = \xi_{\alpha+2} + \xi_{\lambda-1} = \cdots = \frac{1}{2}(p-q),$$

demnach $\xi_\alpha > \frac{1}{2}(p-q) > \xi_{\alpha+1}$. Endlich führt die am Ende des § 4 besprochene Methode von Dirichlet (vgl. Dedekind a. a. O. S. 33) zu den Gleichungen

$$(12.) \quad 4(\xi_1 + \xi_2 + \cdots + \xi_\lambda) = p(\lambda+\mu) - \rho, \; 4(\eta_1 + \eta_2 + \cdots + \eta_\alpha) = q(\lambda+\mu) - \rho.$$

Da die $\lambda - \mu$ verschiedenen Zahlen $\xi_\lambda, \cdots \xi_{\alpha+1} < \frac{1}{2}(p-q)$ sind, so ist

$$(13.) \qquad \lambda - \mu < \frac{1}{2}(p-q), \qquad \frac{1}{2}(p-1) - \lambda > \frac{1}{2}(q-1) - \mu.$$

Zum Schluß erwähne ich noch eine Deutung der Formel (17.), § 2 in Verbindung mit den Formeln (11.) und (13.), § 2. Ordnet man jeder Stelle u, v eine Zahl t zu, den absolut kleinsten Rest von $-pv - qu \equiv -(p+q)z \pmod{pq}$, so sind unter den Zahlen, die den ρ Stellen x, y entsprechen, α positiv und δ negativ; und unter den Zahlen, die den ρ Stellen $-x, y$ entsprechen, β positiv und γ negativ.

§ 4.

Der dritte Beweis von Gauss.

Durchläuft x_0 die geraden, x_1 die ungeraden Werte von x, so ist der Bereich $(x) = (x_0) + (x_1)$ und analog $(y) = (y_0) + (y_1)$. Ist $p = 4n \pm 1$, so durchläuft x_1 die n Werte $1, 3, \cdots 2n-1$. Dann gibt Gauss in seinem *dritten* Beweise § 4, VIII, die Formel

$$\frac{1}{2}(\lambda + \lambda') = \frac{1}{2}(q-1)n - [py < qx_1].$$

Hier muß also unterschieden werden, ob p die Form $4n+1$ oder $4n-1$ hat. Diesem Schönheitsfehler ist aber leicht abzuhelfen. Es ist nämlich $\frac{1}{2}(q-1)n$ die Anzahl der Punkte im Rechteck, deren Ab-

zisse ungerade ist. Daher erhält man, indem man das Rechteck durch OO' teilt, die Relation

$$\frac{1}{2}(\lambda+\lambda') = [py > qx_1] = [py > q(2x-1)].$$

Denn wenn $q(2x-1) < py < \frac{1}{2}pq$ ist, so ist $2x-1 < \frac{1}{2}p$, gehört also dem Bereiche (x_1) an.

Nimmt man dazu die Gleichung $\lambda+\lambda' = \mu+\mu'$, so erhält man die folgenden Sätze (vgl. Schering, Sitzungsber. 1885, S. 116 u. 117):

(1.) $$\frac{1}{2}(\lambda'-\lambda) = [py_0 < qx] = [2py < qx]$$

ist die Anzahl der Punkte in $OO'P$ mit geradem y.

(2.) $$\frac{1}{2}(\mu'-\mu) = [py > qx_0] = [py > 2qx]$$

ist die Anzahl der Punkte in $OO'Q$ mit geradem x.

(3.) $$\frac{1}{2}(\lambda+\lambda') = [py > qx_1] = [py > q(2x-1)]$$
$$= \frac{1}{2}(\mu+\mu') = [py_1 < qx] = [p(2y-1) < qx]$$

ist die Anzahl der Punkte in $OO'P$ mit ungeradem y und zugleich die Anzahl der Punkte in $OO'Q$ mit ungeradem x.

Nach der Methode des § 2 lassen sich diese Sätze so erhalten: Durchläuft v die Werte $1, 2, \cdots q-1$, so ist der Bereich

$$(v) = (2y) + (2y-1) \qquad (y) + (q-y)$$

und entsprechend ist $[pv < q2x]$ gleich

$$[p2y < q2x] + [p(2y-1) < q2x] = [py < q2x] + [p(q-y) < q2x].$$

Ersetzt man in dem letzten Ausdruck $2x$ durch $p-(2x-1)$, so geht er in $[py > q(2x-1)]$ über. Wendet man ferner auf zwei jener Ausdrücke die Formel (3.) § 3 an, so erhält man

$$\varepsilon - [py > qx] + [p(2y-1) < q2x] = \varepsilon - [py > q2x] + [py > q(2x-1)]$$

oder nach (12.) und (13.), § 2

$$[py > q(2x-1)] - [py > q2x] = \lambda + \lambda' - \mu'.$$

Durchläuft u die Werte $1, 2, \cdots p-1$, so ist

$$[py > q(2x-1)] + [py > q2x] = [py > qu] = [py > qx] = \mu'.$$

Denn wenn $qu < py < \frac{1}{2}pq$ ist, so ist $u < \frac{1}{2}p$, gehört also dem Bereich (x) an. Mithin ist

$$\frac{1}{2}(\lambda + \lambda') = [py > q(2x-1)].$$

Die Gleichungen

$$(4.)\quad (\lambda + \lambda') = [p(2y-1) < q2x], \quad \frac{1}{2}(\lambda + \lambda') = [p(2y-1) < qx]$$

lassen die interessante geometrische Deutung zu:

Das rechtwinklige Dreieck $LL'S$ mit den Katheten $\frac{1}{2}p$ und $\frac{1}{2}q$ wird durch seine Mittellinie LT (deren Gleichung $p(2y-1) = qx$ ist) in zwei Dreiecke geteilt, die gleich viele Gitterpunkte enthalten. Wird dagegen die Ordinate $P'R'$ des Punktes R' in V halbiert, so enthält nach (1.) das Dreieck $OP'V$ nur $\frac{1}{2}(\lambda' - \lambda)$, das Dreieck OVR' aber $\frac{1}{2}(\lambda' + \lambda)$ Gitterpunkte, so daß λ Gitterpunkte auf dem Streifen zwischen den beiden Parallelen LT und OV liegen, d. h. von den absolut kleinsten Resten der Zahlen

$$q, \qquad 2q, \qquad \frac{1}{2}(p-1)q \qquad (\mathrm{mod}\ 2p)$$

sind λ negativ.

Zu einer anderen Deutung der Zahl $\frac{1}{2}(\lambda + \lambda')$ führt der Beweis, den Dirichlet in seinen Vorlesungen entwickelt hat:

Unter den $\lambda + \lambda'$ Gitterpunkten in der Figur $LL'P$ gibt es ebenso viele, an denen die Zahl $py - qx$ gerade ist, wie solche, an denen sie ungerade ist.

Denn durchläuft x, y die Stellen, für die $p(2y-1) < q2x$ ist, so ist

$$\sum (-1)^{py-qx} = 0.$$

Ist nämlich $g(x)$ die Anzahl der Werte von y, die einem bestimmten Werte x entsprechen, so ist

$$p\,g(x) - qx = \pm x',$$

wo x' zugleich mit x die Werte $1, 2, \cdots \frac{1}{2}(p-1)$ durchläuft (Gauss, Beweis des Lemma). Dann ist die Partialsumme

$$\sum (-1)^y = \frac{1}{2}((-1)^{g(x)} - 1),$$

also, weil (vgl. Kronecker, Sitzungsber. 1884, S. 252)

$$g(x) + x \equiv x^l \pmod 2$$

ist,

$$2\sum(-1)^{x+y} = \sum(-1)^x\left((-1)^{g(x)}-1\right) = \sum(-1)^{x'} - \sum(-1)^x = 0.$$

Alle diese feineren Einteilungen sind aber, wie ich nochmals bemerke, zum Beweise des Reziprozitätsgesetzes selbst nicht notwendig. Dazu braucht man nicht zu wissen, daß die Zahl $\varepsilon + \lambda + \mu$ durch 4 teilbar ist, sondern nur, daß sie gerade ist.