DAS RECIPROCITÄTSGESETZ IN DER THEORIE DER QUADRATISCHEN RESTE[1]

VON

JULIUS KÖNIG
in BUDAPEST.

In diesen Zeilen beabsichtige ich einen Beweis des Reciprocitätsgesetzes der quadratischen Reste vorzutragen, der — mit Ausschluss eines jeden andern Hülfsmittels — nur jene Eigenschaften des Legendre'schen, beziehungsweise Jacobi'schen Symbols benutzt, die unmittelbar aus der Definition entspringen. Damit erhält der neue Beweis gegenüber der langen Reihe bekannter Beweise eine ganz besondere Stellung und es ist damit auch sein formaler Gang festgelegt. Denn wo immer aus der Definition eines Operationssymbols dessen allgemeine Eigenschaften entwickelt werden sollen, kann dies im Wesen nicht anders, als mittels vollständiger Induction geschehn. Der mitzutheilende Beweis wird daher ebenso auf der vollständigen Induction beruhen, wie der erste Gauss'sche Beweis, der sich in der IV. Section der »Disquisitiones arithmeticae» findet; *er benützt aber jenes berühmte Gauss'sche Lemma nicht,* nach welchem, wenn p eine Primzahl von der Form $8n + 1$ ist, es immer unterhalb $2\sqrt{p} + 1$ eine Primzahl q gibt, von welcher p quadratischer Nichtrest ist.

Die Quelle dieses Lemma's findet sich in Wahrheit erst in den Tiefen der Theorie der quadratischen Formen, und sein elementarer Beweis hat GAUSS bekanntlich grossen Schwierigkeiten verursacht; »demonstratio satis diu operam nostram elusit» — berichtet er selbst darüber, während KRONECKER[2] GAUSS' Gedankengang seinerzeit mit folgenden Worten charak-

[1] Der ungarischen Akademie der Wissenschaften vorgelegt am 18 November 1895.

[2] Mon. Ber. d. k. p. Akad. d. Wiss. zu Berlin, 1876, pag. 341.

Acta mathematica. 22. Imprimé le 6 juillet 1898.

terisirte: »Jene merkwürdige und scharfsinnige Deduction, welche ganz direct mit Überwindung aller Schwierigkeiten auf das Ziel losgehend fast wie eine Art Kraftprobe Gauss'schen Geistes erscheint.»

Die mathematische öffentliche Meinung hat — soviel ich weiss — bei dem inductiven Beweise des Reciprocitätsgesetzes bisher jene Kraftprobe für unerlässlich gehalten und schon darum dürfen die folgenden Betrachtungen einiges Interesse beanspruchen. Doch abgesehen hievon ist für das System der Arithmetik die Thatsache nicht ohne Wichtigkeit, dass das Reciprocitätzgesetz in der That eine ausschliessliche Folge der Definition des Legendre'schen Symbols ist, und aus der Theorie der höheren Congruenzen nicht das geringste, also auch weder die Fermat'sche Congruenz, noch das Euler'sche Kriterium, noch irgend ein anderes äquivalentes Hülfsmittel vorwegnimmt.

Um dies ganz klar zu legen, sollen zuerst die als Prämissen zu verwendenden Sätze vollständig zusammengestellt werden.

Die Prämissen des Beweises. Ist p irgend eine ungerade Primzahl, und a durch p nicht theilbar, so bedeute das Zeichen $\left(\frac{a}{p}\right)$ die positive oder negative Einheit, je nachdem die Congruenz $x^2 \equiv a \pmod{p}$ eine Wurzel besitzt oder nicht, der gebräuchlichen Terminologie nach also je nachdem a Rest oder Nichtrest von p ist. Wenn aber a durch p theilbar ist, soll $\left(\frac{a}{p}\right)$ gleich Null sein.

Die Multiplicationsregel des so definirten Legendre'schen Symbols lautet:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

und ist eine unmittelbare Folge der Definition, wenn sowohl a, als b Reste von p sind. In den übrigen Fällen sind bekanntlich nur noch jene beiden ganz elementaren Sätze zu verwenden, nach denen

erstens mit x auch ax ein vollständiges System incongruenter Zahlen $\bmod. p$ durchläuft und

zweitens die Anzahl sowohl der Reste, wie der Nichtreste von p gleich $\frac{1}{2}(p-1)$ ist.

Das Jacobi'sche Symbol ist nun nichts anderes, als eine rein formale Verallgemeinerung des Legendre'schen; ist nämlich P irgend eine positive,

ungerade ganze Zahl — weiter gehn wir hier überhaupt nicht — und hat P in Primfactoren zerlegt die Form:

$$P = p_1 p_2 \cdots p_r,$$

so lautet die Definition des Jacobi'schen Symbols:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right),$$

und die Multiplicationsregel des Legendre'schen Symbols bleibt demnach auch für dieses erhalten.

Zu den Prämissen gehört endlich noch der auf den quadratischen Restcharakter von -1 bezügliche Satz, nach welchem:

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

(Im folgenden soll nämlich der Kürze wegen statt $(-1)^{\frac{n-1}{2}}$ immer ε_n geschrieben werden.) Ein von EULER stammender Beweis dieses Satzes, der sich im 109. Art. der »Disquisitiones» reproducirt findet, bewegt sich ausschliesslich in dem angegebenen elementaren Gedankenkreise. Um dem Leser hierüber am bequemsten ein klares Bild zu geben, soll dieser Beweis — in aller Kürze und zweckentsprechend formulirt — hier eingefügt werden.

Die Reste der ungeraden Primzahl p,

$$a_1, a_2, \ldots, a_{\frac{p-1}{2}}$$

werden in zwei Classen eingereiht.

In die erste Classe mögen jene Reste a gehören, für welche $a^2 \equiv 1 \pmod{p}$ ist. Nun ist $a^2 - 1 = (a-1)(a+1)$ nur dann durch p theilbar, wenn $a-1$ oder $a+1$ theilbar ist, also nur dann, wenn $a \equiv 1$ oder $a \equiv -1 \pmod{p}$. In diese erste Classe gehören demnach ein oder zwei Reste, je nachdem -1 Rest oder Nichtrest ist; da doch $+1$ immer ein Rest ist.

In die zweite Classe gehören alle übrigen Reste. In dieser Classe findet sich zu jedem Reste a ein und nur ein zweiter Rest b, so dass $ab \equiv 1 \pmod{p}$, und zwar ist b von a verschieden, da sonst a der ersten

Classe angehören würde. Zu b gehört nun ebenso wieder a; es vertheilen sich demnach die Reste der zweiten Classe in Paare, ihre Anzahl ist gerade.

Ist nun $p = 4n + 1$, und demnach die Anzahl sämmtlicher Reste, $\frac{p-1}{2}$, gerade, so müssen die der ersten Classe angehörigen Reste auch in gerader Zahl vorhanden sein, und dann ist -1 Rest von p.

Ist hingegen $p = 4n + 3$, also $\frac{p-1}{2}$ ungerade, so müssen die Reste erster Classe in ungerader Zahl vorhanden sein; es ist also -1 Nichtrest von p.

Damit ist aber bekanntlich der Inhalt des Satzes $\left(\frac{-1}{p}\right) = \varepsilon_p$ erschöpft.

Nach dieser Einleitung wenden wir uns zu unserem eigentlichen Gegenstande. Der zu betretende Weg ist ein wesentlich anderer, als in Gauss' erstem Beweise, oder der Dirichlet'schen Umarbeitung (Crelle, Journal, 47. Bd.). Eine Unterscheidung verschiedener Fälle je nach dem Charakter der vorkommenden Primzahlen findet überhaupt nicht statt, sondern wir zerlegen den Reciprocitätssatz entsprechender Massen in von einander unabhängige Theilsätze, die entweder mit Hülfe der vollständigen Induction leicht direct zu beweisen sind, oder durch Umkehrung aus den schon bewiesenen Theilsätzen entspringen.

Satz I. *Sind q und r zwei positive, ungerade Primzahlen, und ist ferner $q < r$, so folgt aus $\left(\frac{\varepsilon_q q}{r}\right) = 1$ immer auch $\left(\frac{r}{q}\right) = 1$.*

Da der Satz für die kleinsten Primzahlen, z. B. diejenigen unterhalb 11, richtig ist, so kann der allgemeine Beweis so geführt werden, dass wir den Satz für die Zusammenstellung zweier Primzahlen die kleiner als r sind, als richtig voraussetzen, und dann nachweisen, dass er auch für die Zusammenstellung einer Primzahl unterhalb r mit r selbst richtig bleibt.

Im Sinne unsrer Voraussetzung hat die Congruenz

$$x^2 - \varepsilon_q q \equiv 0 \pmod{r}$$

Wurzeln; sei a eine Wurzel, die positiv und kleiner als r ist; dann ist $r-a$ eine ebensolche; und zwar ist von den beiden Wurzeln die eine gerade, die andere ungerade. Wir bezeichnen die gerade Wurzel mit ξ; dann ist

$$\xi^2 - \varepsilon_q q = r\varphi, \tag{1}$$

und φ ist jedenfalls ungerade, weil ξ gerade; φ ist ferner positiv, denn selbst im ungünstigen Falle, wenn $\varepsilon_q = 1$, kann die links stehende Differenz nicht negativ sein; sonst wäre ja $q - \xi^2$ positiv, und diese positive Zahl kleiner als q, und trotzdem durch die Primzahl r, die grösser als q ist, theilbar. Ferner hat man

$$r\varphi \leqq \xi^2 + q < (r-1)^2 + r,$$

und hieraus unmittelbar

$$\varphi < r.$$

a) Wenn nun φ nicht durch q theilbar ist, so erhält man für jeden Primfactor π_i von φ

$$\left(\frac{\varepsilon_q q}{\pi_i}\right) = 1,$$

und da $\pi_i \leqq \varphi < r$, im Sinne der Voraussetzung auch

$$\left(\frac{\pi_i}{q}\right) = 1,$$

und endlich durch Multiplication $\left(\frac{\varphi}{q}\right) = 1$. Andrerseits ergibt aber die fundamentale Identität (1)

$$\left(\frac{r\varphi}{q}\right) = 1$$

und schliesslich

$$\left(\frac{r}{q}\right) = \left(\frac{\varphi}{q}\right) = 1.$$

b) Ist aber φ durch q theilbar, so setzen wir $\varphi = q\psi$; dann ist nach (1) auch ξ durch q theilbar, also $\xi = q\eta$; durch diese Substitutionen geht (1) in

$$q^2\eta^2 - \varepsilon_q q = rq\psi$$

oder

$$\varepsilon_q q\eta^2 - 1 = \varepsilon_q r\psi \tag{2}$$

über, wo ψ wieder kleiner als r, positiv und ungerade ist, den Theiler q aber, wie die linke Seite zeigt, nicht mehr enthält. Diese Identität zeigt nun wieder, dass $\varepsilon_q q$ Rest von jedem Primfactor π_i der Zahl ψ, also $\left(\frac{\varepsilon_q q}{\pi_i}\right) = 1$, und hieraus nach unsern Voraussetzungen $\left(\frac{\pi_i}{q}\right) = 1$ also schliesslich auch $\left(\frac{\psi}{q}\right) = 1$.

Andrerseits folgt aus (2)

$$r\psi \equiv -\varepsilon_q \pmod{q};$$

also $\left(\frac{r\psi}{q}\right) = \left(\frac{-\varepsilon_q}{q}\right)$, was wie man leicht sieht, immer $+1$ ergibt, hieraus endlich

$$\left(\frac{r}{q}\right) = \left(\frac{\psi}{q}\right) = 1,$$

womit unser Satz auch für diesen Fall bewiesen ist.

Satz II. *Sind q und r zwei positive, ungerade Primzahlen, und ist ferner $q < r$, so folgt aus $\left(\frac{q}{r}\right) = 1$ immer auch $\left(\frac{\varepsilon_q r}{q}\right) = 1$.*

Dem bei Satz I. benutzten Gedankengange abermals folgend, hat nun die Congruenz

$$x^2 - q \equiv 0 \pmod{r}$$

Wurzeln; und es sei wieder ξ eine solche, die positiv, gerade und kleiner als r ist. Dann erhält man

$$\xi^2 - q = r\varphi \tag{3}$$

und φ ist wieder positiv, ungerade und kleiner als r.

a) Wenn nun φ nicht durch q theilbar ist, so hat man für jeden Primfactor π_i von φ die Relation $\left(\frac{q}{\pi_i}\right) = 1$, und also, da der Satz für

die Zusammenstellung zweier Primzahlen unterhalb r als richtig angenommen wird, hieraus $\left(\frac{\varepsilon_{\pi_i}\pi_i}{q}\right) = 1$, und endlich durch Multiplication

$$\left(\frac{\varepsilon_\varphi \varphi}{q}\right) = 1,$$

da ja bekanntlich $\varepsilon_a \varepsilon_b = \varepsilon_{ab}$ ist.

Andrerseits erhält man aus der Identität (3)

$$\left(\frac{r\varphi}{q}\right) = 1$$

und demnach

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_r \varphi}{q}\right).$$

Ist nun $q \equiv 1 \pmod 4$, so sind $+\varphi$ und $-\varphi$ zugleich Reste oder Nichtreste von q; es ist also auch

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_\varphi \varphi}{q}\right) = 1.$$

Für den zweiten Fall, $q \equiv 3 \pmod 4$, bemerken wir, dass

$$r\varphi = \xi^2 - q \equiv 1 \pmod 4$$

ist, also $\varepsilon_{r\varphi} = 1$, oder $\varepsilon_r = \varepsilon_\varphi$ und hienach wieder

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_\varphi \varphi}{q}\right) = 1,$$

was zu beweisen war.

b) Ist nun wieder zweitens φ durch q theilbar, dann gehn wir — grade so, wie früher bei Satz I. — zur Identität

$$q\eta^2 - 1 = r\psi \tag{4}$$

über. Auch diese zeigt, dass, wenn π_i irgend einen Primfactor von ψ bedeutet, q Rest von π_i ist, also $\left(\frac{q}{\pi_i}\right) = 1$, und hieraus wieder $\left(\frac{\varepsilon_{\pi_i}\pi_i}{q}\right) = 1$, oder endlich durch Multiplication $\left(\frac{\varepsilon_\psi \psi}{q}\right) = 1$.

Andrerseits hat man

$$r\psi \equiv -1 \pmod q$$

also $\left(\frac{r\psi}{q}\right) = \left(\frac{-1}{q}\right) = \varepsilon_q$. Und hieraus wieder:

$$\left(\frac{\varepsilon_r r}{q}\right) = \varepsilon_q \left(\frac{\varepsilon_r \psi}{q}\right) = \left(\frac{-\varepsilon_r \psi}{q}\right),$$

welche Symbole sich gleich $+1$ ergeben. Denn, da η gerade, wird $r\psi \equiv 3 \pmod 4$, also $\varepsilon_{r\psi} \equiv -1$, oder $\varepsilon_\psi = -\varepsilon_r$, und hienach

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_\psi \psi}{q}\right) = 1,$$

was zu beweisen war.

Satz III. *Sind q und r zwei positive, ungerade Primzahlen und ist ferner $q < r$, so folgt aus $\left(\frac{\varepsilon_r r}{q}\right) = 1$ immer auch $\left(\frac{q}{r}\right) = 1$.*

Unsere Voraussetzung nach ist die Congruenz

$$x^2 - \varepsilon_r r \equiv 0 \pmod q$$

lösbar. Sei nun a irgend eine ihrer geraden Wurzeln; dann ist $a + 2qu$ eine ebensolche und man hat

$$(a + 2qu)^2 - \varepsilon_r r = q\varphi,$$

wo φ ungerade und, wenn nur u positiv und gross genug genommen wird, auch positiv ist.

Der Wert von u soll nun noch so festgelegt werden, dass φ nur solche Primzahlen als Theiler enthalte, die grösser als r sind.

Damit zuerst

$$\varphi = \frac{a^2 - \varepsilon_r r}{q} + 4au + 4qu^2$$

nicht durch q theilbar sei, genügt es u der Congruenz

$$\text{(a)} \qquad \frac{a^2 - \varepsilon_r r}{q} + 4au \equiv 1 \pmod q$$

entsprechend zu wählen, was natürlich immer möglich ist, da ja a nicht durch q theilbar ist.

Seien nun $q_1, q_2, \ldots$ die sämmtlichen Primzahlen, die nicht grösser als r sind, mit Ausschluss von q; und unter diesen $q_1', q_2', \ldots, r$ die-

jenigen, die in $1 - \varepsilon_r r$ nicht als Theiler enthalten sind. Wählt man dann u den Congruenzen

(b) $$a + 2qu \equiv 1 \pmod{q_i'}$$

entsprechend, so wird

$$q\varphi \equiv 1 - \varepsilon_r r \pmod{q_i'},$$

und mit $1 - \varepsilon_r r$ ist also auch φ nicht durch q_i' theilbar.

Seien nun ferner $q_1'', q_2'', \ldots$ jene Primzahlen die nicht grösser als r sind, aber in $1 - \varepsilon_r r$ enthalten sind, ohne jedoch Theiler von $4 - \varepsilon_r r$ zu sein. (Sollte keine solchen vorhanden sein, so fallen natürlich die aufzustellenden Bedingungen ganz fort.) Dem entsprechend unterwerfen wir u noch den eventuellen Bedingungscongruenzen:

(c) $$a + 2qu \equiv 2 \pmod{q_i''}$$

und dann zeigt wieder

$$q\varphi \equiv 4 - \varepsilon_r r \pmod{q_i''},$$

dass φ durch keine der Primzahlen q_i'' theilbar sein kann.

Nun bleiben aber von den Primzahlen unterhalb r nur solche, die sowohl in $1 - \varepsilon_r r$, als in $4 - \varepsilon_r r$ als Theiler enthalten sind; eine solche kann nur die 3 sein. Sollte sich nun keine der Bedingungen (a), (b), (c) auf die 3 beziehen, beschränken wir die Wahl von u von neuem durch die Congruenz:

(d) $$a + 2qu \equiv 0 \pmod{3},$$

und dann ist

$$q\varphi \equiv -\varepsilon_r r \pmod{3},$$

also φ keinesfalls durch 3 theilbar, da r Primzahl und jedenfalls > 3.

Die linearen Congruenzen (a), (b), (c), (d) soweit sie in Anwendung kommen, besitzen immer gemeinschaftliche Lösungen; denn die Moduln sind durchaus verschiedene ungerade Primzahlen, während Coefficient der Unbekannten und Modul immer relative Primzahlen sind. Dabei kann natürlich u immer noch positiv und beliebig gross gewählt werden. Dann

ist auch φ positiv; mit dem so fixirten Werte von u sei nun $\xi = a + 2qu$, das mit a zugleich gerade ist, so erhält man endlich

$$\xi^2 - \varepsilon_r r = q\varphi, \tag{5}$$

und hier enthält φ nur solche Primtheiler, die grösser als r sind.

Nun hat man wieder nach (5) für jeden solchen Primtheiler π_i

$$\left(\frac{\varepsilon_r r}{\pi_i}\right) = 1$$

und hieraus, da $\pi_i > r$ ist, nach Satz I. $\left(\frac{\pi_i}{r}\right) = 1$, oder endlich durch Multiplication

$$\left(\frac{\varphi}{r}\right) = 1.$$

Andrerseits ergiebt sich aus (5) auch $\left(\frac{q\varphi}{r}\right) = 1$, also schliesslich

$$\left(\frac{q}{r}\right) = \left(\frac{\varphi}{r}\right) = 1,$$

was zu beweisen war.

Das Reciprocitätsgesetz wird nun in der aller einfachsten Weise durch Zusammenstellung des II. und III. Satzes erschlossen. Man hat nämlich, wenn wieder $r > q$, nach II. aus $\left(\frac{q}{r}\right) = 1$ immer auch $\left(\frac{\varepsilon_r r}{q}\right) = 1$, und umgekehrt nach III. aus $\left(\frac{\varepsilon_r r}{q}\right) = 1$ immer auch $\left(\frac{q}{r}\right) = 1$; die beiden Symbole haben demnach gleichzeitig den Wert $+1$ oder -1. Es ist also:

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{q}{r}\right),$$

oder anders geschrieben

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

die bekannte Form des Reciprocitätsgesetzes, in welcher q und r mit einander vertauscht werden können, und demnach also schliesslich auch die bisherige Einschränkung $(q < r)$ wegfällt.

Zur Vervollständigung dieser Darstellung möge noch bemerkt werden, dass der auf die Zahl 2 bezügliche Ergänzungssatz, wenn einmal das Reciprocitätsgesetz festgestellt und demnach auch auf das Jacobi'sche Symbol ausgedehnt ist, nach einer von KRONECKER in seinen Vorlesungen gegebenen Bemerkung in zwei Zeilen erledigt werden kann.

Ist nämlich $P > 1$, positiv und ungerade, also eine der beiden Zahlen P und $P-2$ von der Form $4n+1$, so hat man

$$\left(\frac{2}{P}\right) = \left(\frac{-1}{P}\right)\left(\frac{P-2}{P}\right) = \left(\frac{-1}{P}\right)\left(\frac{P}{P-2}\right) = (-1)^{\frac{P-1}{2}}\left(\frac{2}{P-2}\right);$$

also bei Fortsetzung dieser Reduction schliesslich:

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P-1}{2}+\frac{P-3}{2}+\ldots+1} = (-1)^{\frac{P^2-1}{8}}.$$