Matyáš Lerch
Über den fünften Gauss'schen Beweis des Reziprozitätsgesetzes für die quadratischen Reste

Zprávy Král. Čes. spol. nauk, II. tř., 1903, č. 3, 1–19

Persistent URL: http://dml.cz/dmlcz/501556

III.

Ueber den fünften Gauss'schen Beweis des Reziprozitätsgesetzes für die quadratischen Reste.

Von M. Lerch in Freiburg (Schweiz).

Vorgelegt am 9. Januar 1903.

Wir bezeichnen in üblicher Weise mit $E(x)$ oder mit $[x]$ die ganze Zahl, welche mit der positiven oder negativen reellen Grösse x in dem durch die Ungleichungen

$$E(x) \leqq x < E(x) + 1$$

charakterisierten Zusammenhange steht. Diese an den Stellen $x = 0, \pm 1, \pm 2, \ldots$ unstetige Funktion der reellen Veränderlichen x genügt der Gleichung

$$E(x) + E(-x) = -1, \tag{1}$$

falls x keine ganze Zahl ist. Ferner ist für jede positive oder negative ganze Zahl k

$$E(x+k) = E(x) + k. \tag{2}$$

Aus diesen beiden Eigenschaften (1) und (2) der Funktion $E(x)$ folgert man bei *ungeraden* λ die Kongruenz

$$E(x) \equiv E(\lambda - x) \pmod 2. \tag{3}$$

Ausser der Funktion $E(x)$ spielt auch die folgende

$$R(x) = x - E\left(x + \frac{1}{2}\right) \tag{4}$$

eine bedeutende Rolle in der Arithmetik. Sie wird als der absolut kleinste Rest der reellen Grösse x bezeichnet, während $E(x)$ den Namen des grössten Ganzen von x trägt. Es ist nämlich $R(x)$ eine Grösse, welche den Ungleichungen

$$-\frac{1}{2} \leqq R(x) < \frac{1}{2}$$

genügt, und sich von x nur um eine ganze Zahl unterscheidet; letztere hat den Wert

$$E\left(x + \frac{1}{2}\right)$$

und wird als die der Grösse x nächst liegende ganze Zahl gekennzeichnet.

Wir bedürfen ferner, um einige arithmetischen Resultate bequem durch Formeln auszudrücken, eines Symbols, das das *Vorzeichen* (signum) einer reellen Grösse s bedeutet Wir schreiben demgemäss nach Vorgang von Kronecker

$$\text{sgn. } s = \begin{cases} 1, & \text{wenn } s > 0, \\ 0, & \quad " \quad s = 0, \\ -1, & \quad " \quad s < 0. \end{cases}$$

Uns wird namentlich die Funktion sgn. $R(x)$ interessieren. Für diese gelten bei *gebrochenen* x die Relazionen

$$(5) \quad \frac{1 - \text{sgn. } R(x)}{2} = E\left(x + \frac{1}{2}\right) - E(x) = E(2x) - 2E(x),$$

da alle drei Grössen Null oder Eins bedeuten, je nachdem der Rest $R(x)$ positiv oder negativ ausfällt, wenn er nur von Null verschieden bleibt. Unter derselben Bedingung ist schliesslich

$$(6) \quad \text{sgn. } R(x) = (-1)^{E\left(x+\frac{1}{2}\right)+E(x)} = (-1)^{E(2x)}$$

Dies vorausgeschickt, sei n eine *ungerade positive*, m eine beliebige ganze Zahl, und man bilde die arithmetische Funktion

$$(7) \quad \left(\frac{m}{n}\right) = \text{sgn.} \prod_{k=1}^{\frac{n-1}{2}} R\left(\frac{km}{n}\right).$$

Dieselbe verschwindet, wenn m und n einen von 1 verschiedenen gemeinsamen Teiler haben. Ist derselbe gleich n, so ist offenbar die rechte Seite gleich Null, ist er aber eine Zahl $d < n$, so ist $d \geqq 2$, daher wird

$$\frac{n}{d} \leqq \frac{n-1}{2},$$

und es wird dann der Faktor $R\left(\frac{km}{n}\right)$, welcher dem Wert $k = \frac{n}{d}$ entspricht, offenbar verschwinden.

Dagegen sind alle Faktoren des Produktes (7) von Null verschieden, wenn m, n relativ prim sind. In diesem Falle sind die Darstellungen (6) anwendbar, und man erhält

$$(8)\quad \left(\frac{m}{n}\right) = (-1)^{\sum_k \left[\frac{2km}{n}\right]} = (-1)^{\sum_k \left[\frac{km}{n}\right] + \sum_k \left[\frac{km}{n} + \frac{1}{2}\right]},$$

wobei k die Werte $k = 1, 2, 3, \ldots \frac{n-1}{2}$ durchlaufen soll.

Für den Fall $n = 1$ versagt die Definizion, und man setzt

$$(7^0)\qquad \left(\frac{m}{1}\right) = 1.$$

Es ist ferner leicht zu sehen, dass

$$(9)\qquad \left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}},$$

ferner verifiziert man leicht mit Hilfe von (8), dass

$$(10)\qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

indem man die Fälle $n \equiv 1, 3, 5, 7 \pmod 8$ unterscheidet.

Ausserdem liefert die Definizion (7) mit Berücksichtigung von (9) die Relazion:

$$\left(\frac{-m}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{m}{n}\right),$$

weil allgemein

$$R(-x) = -R(x)$$

ist.

Wenn nun P und Q zwei positive ungerade ganze Zahlen ohne gemeinsamen Teiler bedeuten, so besteht das sogenannte Reziprozitätsgesetz

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

Es bietet keine Schwierigkeiten, diese Relazion mit Hilfe der Darstellung (7) oder (8) zu beweisen. Wir schlagen dazu einen Weg ein, der sich an den fünften Gauss'schen Beweis desselben Satzes [1]) nahe anschliesst, jedoch werden dabei zu gleicher Zeit die anderen fundamentalen Beziehungen

$$\left(\frac{m}{P}\right)\left(\frac{m'}{P}\right) = \left(\frac{m\,m'}{P}\right), \quad \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{PQ}\right)$$

ans Licht treten.

Zuvörderst bemerken wir jedoch, dass die Periodizitätseigenschaft der Funktion $R(x)$, d. h.

$$R(x+1) = R(x)$$

die des Zeichens $\left(\frac{m}{n}\right)$ nach sich zieht:

$$\left(\frac{m+kn}{n}\right) = \left(\frac{m}{n}\right), \tag{11}$$

[1]) Wegen Literatur verweise ich auf das vortreffliche Werk Bachmann's, „Niedere Zahlentheorie", I. Teil; Leipzig, Tb. 1902.

was man auch so formulieren kann, dass

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right),$$

sobald

$$m \equiv m' \pmod{n}$$

ist.

Ferner ist für relativ prime m, n das Zeichen (7) offenbar $(-1)^{\mu}$, wenn es unter den Faktoren $R\left(\frac{km}{n}\right)$ μ negative giebt; bedeutet daher $\mu\ (m, n)$ die Anzahl der negativen absolut kleinsten Reste der Grössen

$$\frac{m}{n}, \quad \frac{2m}{n}, \quad \frac{3m}{n}, \quad \ldots \quad \frac{\frac{n-1}{2}\, m}{n},$$

oder, anders ausgedrückt,

$$(12) \qquad \mu\ (m, n) = \sum_{k=1}^{\frac{n-1}{2}} \frac{1 - \operatorname{sgn.} R\left(\frac{km}{n}\right)}{2},$$

so wird

$$(13) \qquad \left(\frac{m}{n}\right) = (-1)^{\mu\ (m, n)}$$

Dies vorausgeschickt, seien P, Q zwei positive, ungerade und relativ prime Zahlen; ferner seien m und m' zwei beliebige ganze Zahlen, die resp. zu P und Q relativ prim sind. Die ersten $\frac{PQ-1}{2}$ Zahlen der natürlichen Zahlenreihe

$$g = 1,\ 2,\ 3 \ldots . \frac{PQ-1}{2}$$

werden in acht Klassen eingeteilt, und zwar so, dass alle Zahlen g derselben Klasse die gleichen *Charaktere*

$$\operatorname{sgn.} R\left(\frac{mg}{P}\right), \quad \operatorname{sgn.} R\left(\frac{m'g}{Q}\right),$$

besitzen; weil dieselben nur die Werte 1, -1, 0 haben können, so sind nur folgende acht Klassen vorhanden:

$$I\ (1,\ 1),\ II\ (1,\ -1),\ III\ (-1,\ 1),\ IV\ (-1,\ -1).$$
$$V\ (0,\ 1),\ VI\ (0,\ -1),\ VII\ (1,\ 0),\ VIII\ (-1,\ 0).$$

Die Zahlen der *III.* Klasse z. B. werden demnach durch die Gleichungen

$$\text{sgn. } R\left(\frac{mg}{P}\right) = -1,\ \text{sgn. } R\left(\frac{m'g}{Q}\right) = 1$$

charakterisiert. Die Anzahlen der Elemente der Klassen *I*, *II*, *III* und *IV* werden resp. mit α, β, γ, δ angedeutet. Die Anzahl der Elemente der *V.* Klasse (u. s. w.) werden wir kurz mit *V* (etc.) bezeichnen.

Die Klassen *V* und *VI* umfassen alle Zahlen g der Reihe $1, 2, \ldots . \frac{PQ-1}{2}$, für welche

$$R\left(\frac{gm}{P}\right) = 0;$$

da m zu P relativ prim ist, so kann dies nur für $g \equiv 0 \pmod{P}$ zutreffen, also für die Zahlen $g = kP$, wobei $k = 1,\ 2, \ldots \frac{Q-1}{2}$ sein kann. Deswegen ist

$$V + VI = \frac{Q-1}{2}.$$

Da die Klasse *VI* alle Zahlen $g = kP$ umfasst, für welche

$$\text{sgn. } R\left(\frac{m'g}{Q}\right) = -1$$

ist, so ist ihre Anzahl offenbar

$$\sum_{k=1}^{\frac{Q-1}{2}} \frac{1 - \text{sgn. } R\left(\frac{m'kP}{Q}\right)}{2} = \mu\ (m'P,\ Q),$$

d. h.

$$(a) \quad VI = \mu\,(m'P,\ Q),\quad V = \frac{Q-1}{2} - \mu\,(m'P,\ Q).$$

In ähnlicher Weise ergiebt sich

$$(a') \quad VIII = \mu\,(mQ,\ P),\quad VII = \frac{P-1}{2} - \mu\,(mQ,\ P).$$

Man sieht leicht ein, dass sich Eigenschaften unserer Symbole ergeben müssen, wenn wir die Summen

$$(b) \qquad \begin{cases} S = \sum_{g=1}^{\frac{PQ-1}{2}} \text{sgn. } R\left(\frac{gm}{P}\right), \\ T = \sum_{g=1}^{\frac{PQ-1}{2}} \text{sgn. } R\left(\frac{gm'}{Q}\right) \end{cases}$$

auf zwei verschiedene Arten ermitteln.

Um die erste Summe umzuformen, spalte ich sie in zwei Teile, wovon der erste die Glieder $g = 1, 2, \ldots . P\,\frac{Q-1}{2}$ enthält, der zweite dagegen Glieder enthält, für welche

$$P\frac{Q-1}{2} < g \leqq \frac{PQ-1}{2} = P\frac{Q-1}{2} + \frac{P-1}{2}.$$

Im ersten Teile setze ich dann $g = \varrho + P\gamma$, im zweiten $g = P\,\frac{Q-1}{2} + h$. Für die ersteren g ist

$$R\left(\frac{gm}{P}\right) = R\left(\frac{\varrho m}{P}\right)$$

und es wird demnach der erste Teil der Summe den Wert

$$\frac{Q-1}{2} \sum_{\varrho=0}^{P-1} \text{sgn. } R\left(\frac{\varrho m}{P}\right) = 0$$

haben; der zweite Teil ist offenbar

$$\sum_{h=1}^{\frac{P-1}{2}} \text{sgn. } R\left(\frac{hm}{P}\right).$$

Dass der vorletzte Ausdruck verschwindet, ist leicht zu sehen, da die Grössen $R\left(\frac{\varrho m}{P}\right)$ für $\varrho = h$ und für $\varrho = P - h$ entgegengesetzt sind. Man hat daher

$$S = \sum_{h=1}^{\frac{P-1}{2}} \text{sgn. } R\left(\frac{hm}{P}\right),$$

und in ähnlicher Weise

$$T = \sum_{h=1}^{\frac{Q-1}{2}} \text{sgn. } R\left(\frac{hm'}{Q}\right).$$

Mit Rücksicht auf (12) lassen sich diese Resultate wie folgt schreiben

$$(c) \qquad \begin{cases} S = \dfrac{P-1}{2} - 2\,\mu\,(m,\ P), \\ T = \dfrac{Q-1}{2} - 2\,\mu\,(m',\ Q). \end{cases}$$

Andererseits bestimmt man S und T direkt, wenn man in den Aggregaten (b) die Glieder in die entsprechenden Klassen verteilt. So kommt

$$S = \alpha + \beta - \gamma - \delta + VII - VIII,$$
$$T = \alpha - \beta + \gamma - \delta + V \quad - VI,$$

oder wenn man die Ausdrücke (a) benützt, und für S und T die Werte (c) einsetzt:

$$(d) \qquad \begin{cases} 2\,\mu\,(mQ,\ P) - 2\,\mu\,(m,\ P) = \alpha + \beta - \gamma - \delta. \\ 2\,\mu\,(m'P,\ Q) - 2\,\mu\,(m',\ Q) = \alpha - \beta + \gamma - \delta. \end{cases}$$

Ferner beachte man, dass die sämmtlichen $\frac{PQ-1}{2}$ Zahlen sich in die acht Klassen verteilen, und daher

$$\alpha + \beta + \gamma + \delta + (V + VI) + (VII + VIII) = \frac{PQ-1}{2},$$

oder da die eingeklammerten Ausdrücke die Werte $\frac{P-1}{2}$ und $\frac{Q-1}{2}$ haben,

$$(e) \qquad \alpha+\beta+\gamma+\delta=\frac{(P-1)\,(Q-1)}{2}$$

sein muss.

Schliesslich ergiebt die Betrachtung der Produkte

$$\text{sgn. } R\left(\frac{gm}{P}\right) . \text{ sgn. } R\left(\frac{gm'}{Q}\right),$$

die in den vier letzten Klassen Null sind, die Beziehung

$$\sum_{g=1}^{\frac{PQ-1}{2}} \text{sgn. } R\left(\frac{gm}{P}\right) . \text{ sgn. } R\left(\frac{gm'}{Q}\right)=\alpha-\beta-\gamma+\delta.$$

Nun werden die Glieder dieser Summe nicht geändert, wenn man das Zeichen von g ändert, und deshalb ist dieselbe mit der folgenden

$$\frac{1}{2}\sum_{g} \text{sgn. } R\left(\frac{gm}{P}\right) . \text{ sgn. } R\left(\frac{gm'}{Q}\right), \quad \left(g=0, \pm 1, \pm 2, \ldots \pm\frac{PQ-1}{2}\right)$$

identisch. Anstelle des verwendeten Wertsystems der Zahlen g kann man ein beliebiges vollständige Restensystem mod. PQ treten lassen, also auch das folgende:

$$g=hQ+kP, \begin{pmatrix} h=0, \pm 1, \pm 2, \ldots \pm\frac{P-1}{2} \\ k=0, \pm 1, \pm 2, \ldots \pm\frac{Q-1}{2} \end{pmatrix}.$$

Alsdann wird aber

$$\text{sgn. } R\left(\frac{gm}{P}\right) . \text{ sgn. } R\left(\frac{gm'}{P}\right) = \text{sgn. } R\left(\frac{hmQ}{P}\right) . \text{ sgn. } R\left(\frac{km'P}{Q}\right),$$

und die Summe nimmt die Gestalt

$$\frac{1}{2}\sum_{h=\frac{P-1}{-2}}^{\frac{P-1}{2}} \text{sgn. } R\left(\frac{hmQ}{P}\right) \sum_{k=\frac{Q-1}{-2}}^{\frac{Q-1}{2}} \text{sgn. } R\left(\frac{km'P}{Q}\right)$$

an.

Sie ist demnach gleich Null und unsere letzte Beziehung wird wie folgt

$$(f) \qquad \alpha-\beta-\gamma+\delta=0$$

lauten.

Nun ergiebt sich aus (*e*) und (*f*)

$$\alpha + \delta = \frac{P-1}{2} \cdot \frac{Q-1}{2};$$

wenn man dann die Gleichungen (*d*) addiert, und vom letzten Resultat Gebrauch macht, so ergiebt sich

$$\mu\,(mQ,\ P) - \mu\,(m,\ P) + \mu\,(m'P,\ Q) - \mu\,(m',\ Q) =$$

$$2\alpha - \frac{P-1}{2} \cdot \frac{Q-1}{2},$$

und hieraus folgt, wenn man beide Seiten als Exponenten von -1 benützt, mit Rücksicht auf (13) das Lemma

$$(A)\quad \left(\frac{mQ}{P}\right)\left(\frac{m'P}{Q}\right) \cdot \left(\frac{m}{P}\right)\left(\frac{m'}{Q}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

Dasselbe liefert für $m = m' = 1$ sofort das Reziprozitätsgesetz

$$(14)\qquad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

Setzt man darin dagegen bloss $m' = 1$, so wird

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

wenn man mit $\left(\frac{P}{Q}\right)$ reduziert und mit $\left(\frac{m}{P}\right)$ multipliziert, da offenbar

$$\left(\frac{m}{P}\right)^2 = 1,$$

so kommt

$$(g)\qquad \left(\frac{mQ}{P}\right) = \left(\frac{m}{P}\right)\left(\frac{Q}{P}\right).$$

Sei nun m' eine beliebige zu P prime Zahl, so kann man immer die positive Zahl h so wählen, dass die Zahl

$$Q = m' + hP$$

ungerade und positiv wird. Alsdann ist aber

$$Q \equiv m', \; mQ \equiv mm' \pmod{P},$$

und daher

$$\left(\frac{Q}{P}\right) = \left(\frac{m'}{P}\right), \left(\frac{mQ}{P}\right) = \left(\frac{mm'}{P}\right),$$

sodass die Gleichung (g) die Gestalt

$$\left(\frac{mm'}{P}\right) = \left(\frac{m}{P}\right)\left(\frac{m'}{P}\right) \tag{15}$$

annimmt, womit also eine zweite Fundamentaleigenschaft des Zeichens $\left(\frac{m}{n}\right)$ bewiesen wird.

Es seien nun m, n, n' positive ungerade Zahlen, und zwar m zu nn' relativ prim. Um das Zeichen

$$\left(\frac{m}{nn'}\right)$$

zu ermitteln, benützen wir das Reziprozitätsgesetz (14), wonach

$$\left(\frac{m}{nn'}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{nn'-1}{2}} \left(\frac{nn'}{m}\right)$$

ist; die rechte Seite ist nun nach (15)

$$(-1)^{\frac{m-1}{2}\cdot\frac{nn'-1}{2}} \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right),$$

oder wenn man beide Faktoren vermöge des Gesetzes (14) umformt,

$$(-1)^{\frac{m-1}{2}\cdot\frac{nn'-1}{2} - \frac{m-1}{2}\cdot\frac{n-1}{2} - \frac{m-1}{2}\cdot\frac{n'-1}{2}} \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right),$$

d. h., da

$$\frac{nn'-1}{2}-\frac{n-1}{2}-\frac{n'-1}{2}=\frac{(n-1)(n'-1)}{2}$$

notwendig gerade ist,

$$\left(\frac{m}{nn'}\right)=\left(\frac{m}{n}\right)\left(\frac{m}{n'}\right). \tag{16}$$

Wenn dieses Gesetz für positive ungerade m bewiesen ist, so lässt es sich mit Hilfe der Substitution $m=m'+hnn'$ auf beliebige Zahlen m ausdehnen.

Das bescheidene Lemma (A), dass wir durch eine leichte Modifikazion des fünften Gauss'schen Beweises des Reziprozitätsgesetzes gewonnen haben, erweist sich somit als ein Gesetz, aus welchem alle Fundamentaleigenschaften (14), (15) und (16) direkt fliessen.

Dieselben gestatten aber auch den Zusammenhang des Zeichens $\left(\frac{m}{n}\right)$ mit der Theorie der quadratischen Reste zu ergründen. Es folgt in der Tat aus (15) für $m=m'$

$$\left(\frac{m^2}{n}\right)=\left(\frac{m}{n}\right)^2=1,$$

solange m und n relativ prim sind. Demnach ist unter der gleichen Bedingung

$$\left(\frac{m^2r}{n}\right)=\left(\frac{r}{n}\right).$$

Es sei nun p eine ungerade Primzahl; alsdann zerfallen*) die Zahlen $1, 2, 3, \ldots . p-1$ in $\frac{p-1}{2}$ quadratische Reste a, und in ebenso viele Nichtreste b. Für die Reste a ist die Congruenz

$$x^2\equiv a \pmod{p}$$

lösbar, und somit folgt

$$\left(\frac{a}{p}\right)=\left(\frac{x^2}{p}\right).$$

*) Wegen der näheren Begründung vergl. z. B. das zitierte Buch von Bachmann.

also hat man für sämmtliche Reste a

$$\left(\frac{a}{p}\right)=1.$$

Sind ferner b, b' zwei Nichtreste, so ist ihr Produkt ein Rest, folglich

$$\left(\frac{bb'}{p}\right)=1,$$

und hieraus

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

d. h. das Zeichen $\left(\frac{b}{p}\right)$ hat für sämmtliche Nichtreste denselben Wert.

Existiert daher eine Zahl m, für welche

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

ist, so ist sie ein Nichtrest und es ist alsdann für alle Nichtreste

$$\left(\frac{b}{p}\right)=-1.$$

In diesem Falle hat also das Zeichen $\left(\frac{k}{p}\right)$ den Wert $+1$, wenn k ein quadratischer Rest von p ist, dagegen ist jenes Zeichen -1, wenn k ein Nichtrest ist.

Nun sind in den Fällen, wann entweder $p \equiv 3 \pmod 4$, oder $p \equiv 5 \pmod 8$ solche Zahlen m, für die $\left(\frac{m}{p}\right)=-1$ ist, immer vorhanden, u. zw. ist im ersten Falle

$$\left(\frac{p-1}{p}\right)=\left(\frac{-1}{p}\right)=-1, \text{ also } m=p-1,$$

im zweiten Falle wieder

$$\left(\frac{2}{p}\right)=-1, \text{ also } m=2.$$

Es bleibt nur ein Fall übrig, nämlich wenn $p \equiv 1 \pmod 8$.

Immer dann, wenn $\left(\frac{b}{p}\right) = -1$, wird

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) = 0,$$

und umgekehrt ist diese Gleichung nur dann möglich, wenn einige $\left(\frac{\nu}{p}\right)$ negativ sind. Also kommt alles auf den Beweis dieser letzten Relazion; dieselbe findet aber unter viel allgemeineren Bedingungen statt, es ist nämlich immer

$$\sum_{\nu=1}^{n-1} \left(\frac{\nu}{n}\right) = 0, \tag{17}$$

solange n keine Quadratzahl ist. Für $n = s^2$ folgt nämlich aus (16)

$$\left(\frac{\nu}{n}\right) = \left(\frac{\nu}{s^2}\right) = \left(\frac{\nu}{s}\right)^2,$$

und dies ist gleich $+1$ oder 0, je nachdem ν und s relativ prim sind oder nicht; ist daher n ein vollständiges Quadrat, so hat die linke Seite von (17) den Wert $\varphi(n)$, d. h. die Anzahl aller zu n relativ primen inkongruenter Zahlen $< n$.

Ein Mittel, die Gleichung (17) zu beweisen, giebt uns die Goniometrie. Man beachte, dass offenbar

$$\text{sgn. } R(x) = \text{sgn. } \sin 2x\pi,$$

und daher nach (7)

$$\left(\frac{m}{n}\right) = \text{sgn.} \prod_{k=1}^{\frac{n-1}{2}} \sin \frac{2km\pi}{n}$$

Solange m relativ prim zu n bleibt, ist der absolute Betrag des Produktes auf der rechten Seite offenbar gleich

$$\prod_{k=1}^{\frac{n-1}{2}} \sin \frac{2k\pi}{n};$$

man hat daher die folgende Darstellung des Zeichens $\left(\frac{m}{n}\right)$

$$(18)\quad \left(\frac{m}{n}\right)=\frac{\prod^{k} \sin \frac{2km\pi}{n}}{\prod_{k} \sin \frac{2k\pi}{n}},\quad \left(k=1,\ 2,\ \ldots .\ \frac{n-1}{2}\right),$$

welche von Eisenstein herrührt.

Beachtet man, dass, wie leicht zu sehen

$$2^{\frac{n-1}{2}} \prod_{k} \sin \frac{2k\pi}{n}=\sqrt{n},$$

wo die Quadratwurzel positiv zu nehmen ist, so folgt aus (18)

$$(18^0)\qquad \left(\frac{m}{n}\right)\sqrt{n}=2^{\frac{n-1}{2}} \prod_{k=1}^{\frac{n-1}{2}} \sin \frac{2km\pi}{n}$$

Hierdurch ist der Zusammenhang der Kreisteilung mit der Theorie der quadratischen Reste in einfachster Weise dargelegt und auch ein Weg zur Einführung der Gauss'schen Summen gewonnen; für unsere Zwecke sind jedoch diese Theorien entbehrlich, und wir gelangen zum Beweise der Gleichung (17), wenn wir in irgend welcher Weise die rechte Seite von (18^0) in eine Summe verwandeln, in welcher sich dann die Summazion nach m ausführen lässt. Setzen wir der Kürze wegen

$$2^{r-1} \sin x \sin 2x \sin 3x \ldots . \sin rx=\Phi_r\ (x),$$

so erhalten wir successive

$$\begin{aligned}
\Phi_2\ (x) &= \cos x-\cos 3x,\\
\Phi_3\ (x) &= \sin 2x+\sin 4x-\sin 6x,\\
\Phi_4\ (x) &= 1-\cos 6x-\cos 8x+\cos 10x,\\
\Phi_5\ (x) &= \sin x+\sin 3x+\sin 5x-\sin 11x-\sin 13x\\
&\quad +\sin 15x,\\
\Phi_6\ (x) &= \cos x+\cos 3x-2\cos 7x-\cos 11x+\cos 17x\\
&\quad +\cos 19x-\cos 21x,
\end{aligned}$$

und allgemein

$$(19)\quad \begin{cases} \Phi_{2r}(x) = A_0 + A_1 \cos x + A_2 \cos 2x + \ldots + \\ \qquad A_{r(2r+1)} \cos r\,(2r+1)\,x, \\ \Phi_{2r-1}(x) = B_1 \sin x + B_2 \sin 2x + \ldots + \\ \qquad B_{r(2r-1)} \sin r\,(2r-1)\,x, \end{cases}$$

wobei die Koeffizienten A und B ganze Zahlen sind. Die Gleichung (18^0) lautet alsdann

$$(18^1)\quad \left(\frac{m}{n}\right)\sqrt{n} = 2\,\Phi_{\frac{n-1}{2}}\left(\frac{2m\pi}{n}\right),$$

und sie bleibt auch dann richtig, wenn m und n einen von Eins verschiedenen gemeinsamen Teiler haben, da im solchen Falle beide Seiten gleich Null sind. Ersetzen wir in (18^1) die rechte Seite durch den aus (19) fliessenden Summenausdruck, so lässt sich die Summazion nach $m = 0, 1, 2, \ldots n-1$ leicht ausführen, da

$$\sum_{m=0}^{n-1} \sin \frac{2mk\pi}{n} = 0,$$

$$\sum_{m=0}^{n-1} \cos \frac{2mk\pi}{n} = 0 \text{ oder } n,$$

und es ergiebt sich hieraus, dass

$$\sum_{m=0}^{n-1} \Phi\left(\frac{2m\pi}{n}\right) = S$$

eine gewöhnliche ganze Zahl ist; da alsdann wegen (18^1)

$$\sqrt{n} \sum_{m=0}^{n-1} \left(\frac{m}{n}\right) = 2S$$

sein muss, so ist hieraus zu schliessen, dass der razionale Faktor der linken Seite

$$\sum_{m=0}^{n-1} \left(\frac{m}{n}\right)$$

immer dann verschwinden muss, wenn $\sqrt{n}$ irrazional ist, d. h. wenn n keine Quadratzahl ist. Da aber $\left(\frac{0}{n}\right) = 0$ ist, so hat man schliesslich die Gleichung (17), und die Bedeutung des Zeichens für die Theorie der quadratischen Reste ist damit vollständig klargelegt.

Das Symbol $\left(\frac{m}{n}\right)$ wurde für primzahliges n durch Legendre eingeführt; die allgemeine Fassung desselben stammt von Jacobi her, der auch vermöge der Definizion

$$\left(\frac{m}{-n}\right) = \left(\frac{m}{n}\right)$$

negative „Nenner" einführte. Ihren Ursprung nehmen alle die mitgeteilten Begriffe und Darstellungen des *Legendre-Jacobischen Zeichens* — wie das Zeichen $\left(\frac{m}{n}\right)$ genannt wird — in den Arbeiten Gauss', namentlich in dessen Abhandlung *Summatio quarundam serierum singularium;* da jedoch Gauss, wahrscheinlich wegen Animosität gegen Legendre, den Gebrauch des Zeichens $\left(\frac{m}{n}\right)$ vermieden hat, so stammt die formale Ausbildung dieser Theorie eigentlich von Eisenstein, Schering und Kronecker her.

Es soll hier noch erörtert werden, wie im Falle $p \equiv 1 \pmod 8$, die Existenz einer Primzahl $q < p$ dargelegt werden kann, für welche

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

Für kleine Primzahlen q lässt sich die Gleichung $\left(\frac{b}{q}\right) = -1$ unmittelbar erledigen, und man kann annehmen, dass bis zu einer gewissen Grenze für jede Primzahl q das Legendre'sche Zeichen ein Unterscheidungsmerkmal für die quadratischen Reste und Nichtreste bildet. Es sei daher p die erste Primzahl, für welche immer

$$\left(\frac{k}{p}\right) = 1,$$

solange k durch p nicht teilbar ist. Ist dann q eine ungerade Primzahl $< p$, so ergiebt sich hieraus mit Hilfe des Reziprozitätsgesetzes die Gleichung

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

und daher wird p ein Rest des Moduls q sein.

Setzt man die Theorie der Kongruenz

$$x^2 \equiv h \pmod{n}$$

für zusammengesetzte Moduli als bekannt voraus, so würde man hieraus schliessen, dass die Kongruenz

$$(a) \quad x^2 \equiv p \pmod{M} \text{ für } M = 1 \cdot 2 \cdot 3 \ldots (2m+1)$$

möglich ist, sobald $2m+1 < p$ ist. Die Unmöglichkeit dieser Kongruenz lässt sich aber nach Gauss (ein Ergänzungssatz vom 1. Gauss'schen Beweise des Reziprozitätsgesetzes) wie folgt dartun.

Es sei x eine positive Lösung der Kongruenz (a); da $2m+1 < p$ ist, und p eine Primzahl, so ist p und daher auch x relativ prim zu M. Nun ist aber wegen (a) für den Modul M

$$x\,(p-1^2)\,(p-2^2) \ldots (p-m^2) \equiv x\,(x^2-1^2)\,(x^2-2^2) \ldots (x^2-m^2)$$

die rechte Seite hat den Wert

$$(x+m)\,(x+m-1) \ldots (x+1)\,x\,(x-1) \ldots (x-m)$$

und ist daher durch M teilbar; demnach muss auch

$$x\,(p-1^2)\,(p-2^2) \ldots (p-m^2)$$

durch M teilbar sein, oder da x relativ prim zu M ist, so wird

$$(b) \quad \frac{1}{m+1} \cdot \frac{p-1^2}{(m+1)^2-1^2} \cdot \frac{p-2^2}{(m+1)^2-2^2} \cdots \frac{p-m^2}{(m+1)^2-m^2}$$

eine ganze Zahl sein. Wählt man aber

$$m = E(\sqrt{p}),$$

was mit der Bedingung $2m+1<p$ verträglich ist, so wird $(m+1)^2>p$ und alle Faktoren des Produkts sind echte Brüche. Dasselbe ist daher keine ganze Zahl und die Kongruenz (a) ist einfach unmöglich. Daher muss es unter den Primfaktoren des Moduls M, d. h. zwischen 1 und $2\sqrt{p}+1$, mindestens eine Primzahl q geben, für welche

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

Damit wird die übliche Bedeutung des Legendre'schen Zeichens auch für den Fall $p\equiv 1 \pmod 8$ erledigt.