Ein neuer Beweis des quadratischen Reziprocitätssatzes.

Von Ladislaus Rédei in Budapest.

Den nachfolgenden Beweis des quadratischen Reziprocitätssatzes möchte in veröffentlichen, da dieser sich von den bekannten meines Wissens principiell unterscheidet. Wir könnten alle Paare (p, q) der ungeraden Primzahlen gleichzeitig behandeln, doch wollen wir den Fall $p \equiv q \equiv 3 \pmod 4$ vorausschicken, da er besonders interressant ist und auch den Beweis des allgemeinen Falles beleuchtet.

1°. Es seien p, q verschiedene ungerade Primzahlen und $p \equiv q \equiv 3 \pmod 4$. Es sei $\left(\frac{a}{p}\right)$ das Symbol von Legendre und $\left(\frac{a}{p}\right) = 0$, wenn $a \equiv 0 \pmod p$. Es bedeute n_{pq} die Anzahl der mod. pq quadratischen Reste in der ersten Hälfte des kleinsten nichtnegativen Restsystems von pq. Dann hat man:

$$n_{pq} = \sum_{i=1}^{(pq)'} \frac{1+\left(\frac{i}{p}\right)}{2} \frac{1+\left(\frac{i}{q}\right)}{2},$$

wo $(pq)'$ anstatt $\frac{pq-1}{2}$ gesetzt ist und der Strich neben Σ die Auslassung der zu pq nicht relativ primen Werte bedeutet.

Für die in der Rede stehenden Summationswerte hat man $\sum' 1 = \frac{(p-1)(q-1)}{2}$ und $\sum' \left(\frac{i}{p}\right)\left(\frac{i}{q}\right) = 0$, da $\left(\frac{pq-i}{p}\right) = \left(\frac{-i}{p}\right) = -\left(\frac{i}{p}\right)$ und $\sum_{i=1}^{pq-1}{}' \left(\frac{i}{p}\right)\left(\frac{i}{q}\right) = 0$. Es ist also:

$$n_{pq} = \frac{(p-1)(q-1)}{8} + \frac{1}{4}\sum_{i=1}^{(pq)'}{}' \left(\frac{i}{p}\right) + \frac{1}{4}\sum_{i=1}^{(pq)'}{}' \left(\frac{i}{q}\right).$$

Man sieht leicht, dass

$$\sum_{i=1}^{(pq)'}{}' \left(\frac{i}{p}\right) = \sum_{i=1}^{(pq)'} \left(\frac{i}{p}\right) - \sum_{i=1}^{\frac{q-1}{2}} \left(\frac{p \cdot i}{p}\right) - \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{q \cdot i}{p}\right). \qquad (A)$$

Des erste Glied der rechten Seite:

$$\sum_{i=1}^{(pq)'} \left(\frac{i}{p}\right) = \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right),$$

da $(pq)' = \frac{pq-1}{2} \equiv \frac{p-1}{2} \pmod{p}$ wegen $\sum_{i=a+1}^{a+p} \left(\frac{i}{p}\right) = 0$, das zweite Glied ist gleich Null, das dritte ist offenbar das $\left(\frac{q}{p}\right)$-fache des ersten. Man hat also, wenn man das dritte Glied so umgeformt hat, wie das zweite:

$$n_{pq} = \frac{(p-1)(q-1)}{8} + \frac{1-\left(\frac{q}{p}\right)}{4} \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{i}{p}\right) + \frac{1-\left(\frac{p}{q}\right)}{4} \sum_{i=1}^{\frac{q-1}{2}} \left(\frac{i}{q}\right).^{1})$$

Die hier auftretende beide Summen sind ungerade Zahlen, da so $\frac{p-1}{2}$, wie $\frac{q-1}{2}$ ungerade sind. Mit n_{pq} ist also auch $\frac{(p-1)(q-1)}{8} + \frac{1-\left(\frac{q}{p}\right)}{4} + \frac{1-\left(\frac{p}{q}\right)}{4}$ eine ganze Zahl und damit ist der Satz für den jetzt behandelten Fall bewiesen.[2])

2^0. Es sei p, q ein beliebiges Paar der verschiedenen Primzahlen (wir wollen also den vorher behandelten Fall nicht ausschliessen). Es sei $\frac{p-1}{2^e}$ eine ungerade Zahl, g eine primitive

---

[1]) Auf diese Formel bzw. auf ihre Verallgemeinerung gedenke ich an anderer Stelle zurückzukommen.

[2]) Es sei nämlich der zuletzt vorgekommene Ausdruck eine ganze Zahl, also $\frac{(p-1)(q-1)}{4} \equiv \frac{\left(\frac{q}{p}\right) - \left(\frac{p}{q}\right)}{2} \pmod{2}$. Quadriert man die rechte Seite (es ist $a^2 \equiv a \pmod{2}$), formt man die linke Seite nach $x \equiv \frac{1-(-1)^x}{2} \pmod{2}$ um und multipliziert man mit 2, so bekommt man:

$1-(-1)^{\frac{(p-1)(q-1)}{4}} \equiv 1 - \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \pmod{4}$, also: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. Diese ist die gewöhnliche Form des quadratischen Reziprozitätssatzes.

Wurzel der Kongruenzgleichung $x^{p-1} \equiv 1 \pmod{p}$ und α eine (komplexe) primitive Einheitswurzel 2^e-ten Grades. Wir definieren das Symbol $\left[\frac{a}{p}\right]$ für jede razionale ganze Zahl a folgendermassen: Es sei $\left[\frac{a}{p}\right] = \alpha^{\text{ind. } a}$, wo $g^{\text{ind. } a} \equiv a \pmod{p}$, wenn $a \not\equiv 0 \pmod{p}$ und $\left[\frac{p\,a}{p}\right] = 0$. Dann gilt: $\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] = \left[\frac{a\,b}{p}\right]$ und $\left[\frac{a}{p}\right]^{2^{e-1}} = (-1)^{\text{ind. } a} = \left(\frac{a}{p}\right)$. Übrigens hat man $\left[\frac{a}{p}\right] = 1$ dann und nur dann, wenn a ein Potenzwert 2^e-ten Grades ist.

Als e, g, α zu p gehören, so sollen f, h, β zu q gehören.

Das Zahlenpaar $\left(\left[\frac{a}{p}\right], \left[\frac{a}{q}\right]\right)$ werden wir den Karakter von a nennen.

Bedeutet $n_{p,q}^{r,s}$ die Anzahl der Zahlen mit dem Karakter $(\alpha^{-r}, \beta^{-s})$ in der ersten Hälfte des kleinsten nichtnegativen Restsystems der Zahl pq, so sieht man leicht, dass

$$n_{p,q}^{r,s} = \sum_{i=1}^{(pq)'}{}' \left(\frac{1}{2^e}\sum_{\mu=0}^{2^e-1}(\alpha^r\left[\frac{i}{p}\right])^\mu\right)\left(\frac{1}{2^f}\sum_{\nu=0}^{2^f-1}(\beta^s\left[\frac{i}{q}\right])^\nu\right) =$$

$$= \frac{1}{2^{e+f}}\sum_{\mu=0}^{2^e-1}\sum_{\nu=0}^{2^f-1}\alpha^{\mu r}\beta^{\nu s}\sum_{i=1}^{(pq)'}{}'\left[\frac{i}{p}\right]^\mu\left[\frac{i}{q}\right]^\nu. \qquad (1)$$

Abgesehen vom Falle $\mu = \nu = 0$, gibt es immer eine rationale ganze Zahl c, die zu pq relativ prim ist und für welche $\left[\frac{c}{p}\right]^\mu\left[\frac{c}{q}\right]^\nu = \gamma \neq 1$ (z. B. wenn $\mu \neq 0$, so wähle man $c \equiv g \pmod{p}$, $c \equiv 1 \pmod{q}$) und also in diesem Falle $\sigma = \sum_{i=1}^{pq-1}{}'\left[\frac{i}{p}\right]^\mu\left[\frac{i}{q}\right]^\nu = 0$, denn die Summe ändert sich nicht, wenn man ci an Stelle von i setzt, während sie sich mit γ multipliziert. Ferner hat man in diesem Falle:

$$\sigma = \sum_{i=1}^{(pq)'}{}'\left[\frac{i}{p}\right]^\mu\left[\frac{i}{q}\right]^\nu + \sum_{i=1}^{(pq)'}{}'\left[\frac{pq-i}{p}\right]^\mu\left[\frac{pq-i}{q}\right]^\nu =$$

$$= (1+(-1)^{\mu+\nu})\sum_{i=1}^{(pq)'}{}'\left[\frac{i}{p}\right]^\mu\left[\frac{i}{q}\right]^\nu = 0. \qquad (B)$$

In dem Ausdrucke (1) von $n_{p,q}^{r,s}$ verschwinden also die Glieder, die zu einem solchen Indizespaare (μ, ν) gehören, bei dem $\mu+\nu$ gerade und von Null verschieden ist. Folglich:

$$n_{p,q}^{r,s} = \frac{(p-1)(q-1)}{2^{e+f+1}} + \frac{1}{2^{e+f}} \sum_{\substack{\mu=0 \\ (\mu+\nu \text{ ungerade})}}^{2^{e}-1} \sum_{\nu=0}^{2^{f}-1} \alpha^{\mu r} \beta^{\nu s} \sum_{i=1}^{(pq)'} \left[\frac{i}{p}\right]^{\mu} \left[\frac{i}{q}\right]^{\nu}.$$

Nun summiere man nach r von 0 bis $2^{e-1}-1$ und nach s von 0 bis $2^{f-1}-1$, dann verschwinden wegen der Summation nach r und s, nach einer bekannten Eigenschaft der Einheitswurzeln, die Glieder, die zu einem solchen Indicespaare (μ, ν) gehören, bei dem entweder μ gerade und $\neq 0$, oder ν gerade und $\neq 0$; es können also nur Glieder mit den Indices $(0, 1)$, $(0, 3), \ldots$; $(1, 0)$, $(3, 0), \ldots$ bleiben, also

$$n_{pq} = \Sigma n_{p,q}^{r,s} = \frac{(p-1)(q-1)}{2^{3}} + \\ + \frac{1}{2^{e+f}} \sum_{\substack{\mu \\ (\mu \text{ ungerade})}}^{2^{e}-1} \sum_{r=0}^{2^{e-1}-1} \sum_{s=0}^{2^{f-1}-1} \alpha^{\mu r} \sum_{i=1}^{(pq)'} \left[\frac{i}{p}\right]^{\mu} + (\ldots),$$

wo $(\ldots)$ das bedeutet, was man aus dem ihn vorhergehenden Gliede enthält, wenn man statt p und statt die zu p gehörigen Zahlen bzw. q und die zu q gehörigen Zahlen schreibt.

Vollführt man die Summation nach s, formt man die Summe nach i so um, wie im vorigen Paragraphen bei (A), [N. b. $\sum_{i=a+1}^{a+p} \left[\frac{i}{p}\right]^{\mu} = 0$ ergibt sich so, wie bei (B)] so bekommt man:

$$n_{pq} = \frac{(p-1)(q-1)}{8} + \frac{1}{2^{e+1}} \sum_{\substack{\mu=1 \\ (\mu \text{ ungerade}}}^{2^{e}-1} \sum_{r=0}^{2^{e-1}-1} \alpha^{\mu r} \left(1 - \left[\frac{q}{p}\right]^{\mu}\right) \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{i}{p}\right]^{\mu} + (\ldots).$$

Man vollführe die Summation nach r, (Rücksicht genommen auf $\alpha^{2^{e-1}} = -1$), setzen wir ind. $q = x$, also $\left[\frac{q}{p}\right] = \alpha^{x}$, so bekommt man:

$$n_{pq} = \frac{(p-1)(q-1)}{8} + \frac{1}{2^{e}} \sum_{\substack{\mu=1 \\ (\mu \text{ ungerade})}}^{2^{e}-1} \frac{1-\alpha^{\mu x}}{1-\alpha^{\mu}} \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{i}{p}\right]^{\mu} + (\ldots).$$

Es bedeute a_m bzw. a'_m die Anzahl derjenigen Zahlen a in der Folge $1, \ldots, \frac{p-1}{2}$ bzw. $\frac{p+1}{2}, \ldots, p-1$, für welche $\left[\frac{a}{p}\right] = \alpha^{m}$,

so ist:

$$\sum_{l=1}^{\frac{p-1}{2}} \left[\frac{l}{p}\right]^{\mu} = \sum_{m=0}^{2^{e}-1} a_m \alpha^{\mu m}.^{3})$$

Setzt man das in die vorige Formel ein und führt man im so erhaltenen Ausdrucke die Division aus, so bekommt man:

$$n_{pq} = \frac{(p-1)(q-1)}{8} + \frac{1}{2^e} \sum_{r=0}^{x-1} \sum_{m=0}^{2^{e-1}-1} \sum_{\substack{\mu=1 \\ \mu \text{ ungerade}}}^{2^{e}-1} a_m \alpha^{(r+m)\mu} + (\ldots).$$

Hier ist das Glied mit dem Indizespaare (r, m) gleich Null, abgesehen vom Falle, als 2^{e-1} in $r+m$ aufgeht; diese letzte Bedingung ordnet zu einem jeden r zwei Werte $-m_r, m_r + 2^{e-1}$ — von m zu, und so bekommen wir nach der Summation nach μ:

$$n_{pq} = \frac{(p-1)(q-1)}{8} + \frac{1}{2} \sum_{r=0}^{x-1} (\varepsilon a_{m_r'} + \eta a_{m_r + 2^{e-1}}) + (\ldots),$$

wo $\varepsilon, \eta = \pm 1$. Da n_{pq} eine ganze Zahl ist, so steht an der rechten Seite eine ganze Zahl auch dann, wenn man $\varepsilon = \eta = 1$ setzt. Der Summand ist dann nach der dritten Fussnote ersichtlich eine ungerade Zahl, es ist also

$$\frac{(p-1)(q-1)}{8} + \frac{x}{2} + (\ldots)$$

eine ganze Zahl. Da $x \equiv \frac{1-(-1)^x}{2} \equiv \frac{1-(-1)^{\text{ind. } q}}{2} \equiv \frac{1-\left(\frac{q}{p}\right)}{2}$ (mod. 2), so ist

$$\frac{(p-1)(q-1)}{8} + \frac{1-\left(\frac{q}{p}\right)}{4} + \frac{1-\left(\frac{p}{q}\right)}{4}$$

ganz, woraus der Satz folgt, nach der zweiten Fussnote.

---

[3]) Offenbar ist $a_m + a_m'$ gleich der Anzahl derjenigen Glieder in der Folge $1, \ldots, p-1$, für welchen $\left[\frac{a}{p}\right] = \alpha^m$; d. h. $a_m + a_m' = \frac{p-1}{2^e}$. Anderseits ist $a_m' = a_{m+2^{e-1}}$, da $\left[\frac{p-i}{p}\right] = -\left[\frac{i}{p}\right] = \alpha^{2^{e-1}} \left[\frac{i}{p}\right]$, es ist also $a_m + a_{m+2^{e-1}} = \frac{p-1}{2^e}$ eine ungerade Zahl.