Zeitschrift: Mitteilungen der Naturforschenden Gesellschaft Luzern
Herausgeber: Naturforschende Gesellschaft Luzern
Band: 14 (1943)

Artikel: Neues über die Pell'sche Gleichung
Autor: Bucher, J.
DOI: https://doi.org/10.5169/seals-523525

Neues über die Pell'sche Gleichung

VON
J. BUCHER
LUZERN

I.

Den folgenden Betrachtungen ist der quadratische Zahlenkörper $k(\sqrt{pq})$ zugrundegelegt, wo entweder p und q Primzahlen der Form $4n+1$ sind, oder $q=2$ ist. Unsere Entwicklungen beziehen sich zunächst auf den ersten Fall, in Ergänzungssätzen werden wir jeweils den zweiten Fall berücksichtigen.

Ist $\left(\frac{p}{q}\right) = 1$, so existieren über die Norm der Grundeinheit die Sätze von *Dirichlet* (Werke 1. Bd., S. 219), die später mehrfach ergänzt wurden, so von mir (Dissertation, Zürich 1919), von Herrn *L. Rédei* (Journal für Mathematik Bd. 171), von Herrn *A. Scholz* (Mathematische Zeitschrift Bd. 39). Wir wissen folgendes: Ist der gegenseitige biquadratische Restcharakter der Zahlen p und q bekannt, so läßt sich daraus schließen, ob die Klassenzahl in $k(\sqrt{pq})$ — stets Äquivalenz im engern Sinn vorausgesetzt — durch 8 teilbar ist oder nicht; ferner läßt sich im letzteren Fall die Norm der Grundeinheit genau charakterisieren.

In der folgenden Arbeit wird gezeigt, daß, wenn der biquadratische Restcharakter gewisser irrationaler Primfaktoren in quadratischen Zahlenkörpern bekannt ist, ferner die Anzahl der quadratischen Reste in bestimmten Intervallen, wir daraus schließen können, ob die Klassenzahl in $k(\sqrt{pq})$ durch 16 teilbar ist oder nicht; im letztern Falle läßt sich die Norm der Grundeinheit genau charakterisieren. Die Resultate von *Dirichlet* werden also wesentlich erweitert.

II.

Mit den bisher bekannten Resultaten stehen gewisse Kongruenzen in Zusammenhang. Es sei $\varsigma = \frac{t - u\sqrt{pq}}{2}$, wobei t und

u die kleinsten positiven ganzen Zahlen sind, für welche die Gleichung $\frac{t^2 - pqu^2}{4} = 1$ erfüllt ist. Aus der Definition folgt: ς ist positiv und $\frac{t}{2} \equiv \pm 1 \pmod{p}$ und $\pmod{q}$. ς ist das Quadrat einer Einheit und zwar der Grundeinheit ε' ($\varepsilon > 1$) in $k(\sqrt{pq})$, wenn $N(\varepsilon) = -1$ ist oder einer Einheit im erweiterten Körper $k(\sqrt{p}, \sqrt{q})$ von der Form $\eta = \frac{x\sqrt{p} - y\sqrt{q}}{2}$, wenn die Norm der Grundeinheit in $k(\sqrt{pq}) = 1$ ist. Der besondern Form von $N(\varepsilon)$, bzw. $N(\eta)$ entsprechend, können drei Fälle unterschieden werden:

1. Fall. $N(\varepsilon) = \frac{x^2 - pqy^2}{4} = -1$;

2. Fall. $N(\eta) = \frac{px^2 - qy^2}{4} = -1$;

3. Fall. $N(\eta) = \frac{px^2 - qy^2}{4} = 1$.

Diesen drei Normen sind, wie man sofort sieht, folgende drei Kongruenzen umkehrbar eindeutig zugeordnet:

1. Fall. $\frac{t}{2} = \frac{x^2 + pqy^2}{4} \equiv -1 \pmod{p} \equiv -1 \pmod{q}$;

2. Fall. $\frac{t}{2} = \frac{px^2 + qy^2}{4} \equiv 1 \pmod{p} \equiv -1 \pmod{q}$;

3. Fall. $\frac{t}{2} = \frac{px^2 + qy^2}{4} \equiv -1 \pmod{p} \equiv 1 \pmod{q}$.

Ist $q = 2$ betrachten wir entsprechend die Einheit: $\varsigma = t - u\sqrt{2p}$ und unterscheiden, wie oben die drei Fälle:

1. Fall. $N(\varepsilon) = x^2 - 2py^2 = -1$; $t = x^2 + 2py^2 \equiv -1 \pmod{p} \equiv -1 \pmod{4}$;

2. Fall. $N(\eta) = px^2 - 2y^2 = -1$; $t = px^2 + 2y^2 \equiv 1 \pmod{p} \equiv -1 \pmod{4}$;

3. Fall. $N(\eta) = px^2 - 2y^2 = 1$; $t = px^2 + 2y^2 \equiv -1 \pmod{p} \equiv 1 \pmod{4}$.

Betrachten wir statt ς allgemein die Einheit $\varsigma^n = \frac{T - U\sqrt{pq}}{2}$, wo $\frac{T}{2} \equiv \left(\frac{t}{2}\right)^n \pmod{pq}$. Ist n gerade, dann ist $\frac{T}{2} \equiv 1 \pmod{pq}$, ist n ungerade, dann ist $\frac{T}{2} \equiv \frac{t}{2} \pmod{pq}$. Entsprechendes gilt für den Körper $k(\sqrt{2p})$, so daß folgender Satz gilt:

1. Satz. *Ist* $\varsigma^n = \frac{T - U\sqrt{pq}}{2}$, *bzw.* $= T - U\sqrt{2p}$ *und sind die absolut kleinsten Reste von* $\frac{T}{2}$, *bzw.* T *nach den Moduln* p *und* q, *bzw. nach den Moduln* p *und* 4 : $(-1; -1)$, $(1; -1)$ *oder* $(-1; 1)$, *so liegt in bezug auf* $N(\sqrt{\varsigma})$ *der erste, zweite oder dritte Fall vor und* n *ist ungerade; sind aber diese Reste gleich* $(1; 1)$, *so ist* n *gerade.*

Auf Grund dieses Satzes können nun die Sätze von *Dirichlet* so formuliert werden:

Ist die Klassenzahl h *durch* 4 *teilbar, so ist:*

$$\left(\frac{p}{q}\right)_4 \equiv \left(\frac{t}{2}\right)^{\frac{h}{4}} \pmod{p}; \quad \left(\frac{q}{p}\right)_4 \equiv \left(\frac{t}{2}\right)^{\frac{h}{4}} \pmod{q} \text{ und für } q = 2$$

$$\left(\frac{p}{2}\right)_4 \equiv t^{\frac{h}{4}} \pmod{p}; \quad \left(\frac{2}{p}\right)_4 \equiv t^{\frac{h}{4}} \pmod{4}.$$

Dabei bedeutet $\left(\frac{p}{2}\right)_4 = 1$, daß p von der Form: $16n + 1$ und $\left(\frac{p}{2}\right)_4 = -1$, daß p von der Form: $16n + 9$ ist.

III.

A. Wir setzen im folgenden stets voraus, daß $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, bzw. $\left(\frac{p}{2}\right)_4 = \left(\frac{2}{p}\right)_4 = 1$ ist, daß also die Klassenzahl durch 8 teilbar ist.

Nehmen wir zuerst p und q ungerade an. Ich definiere dann als x-Zahlen jene $\frac{p-1}{4}$ Zahlen $x < \frac{p}{2}$, für welche $\left(\frac{x}{p}\right) = 1$ ist und als y-Zahlen jene $\frac{q-1}{4}$ Zahlen $y < \frac{q}{2}$, für welche $\left(\frac{y}{q}\right) = 1$ ist. Ferner betrachte ich die Funktionen:

$$(1) \quad \varphi(u) \equiv \Pi\left(u - 4\sin^2\frac{x\pi}{p}\right) \equiv u^{\frac{p-1}{4}} + a_1 u^{\frac{p-5}{4}} + \ldots + a_{\frac{p-1}{4}}$$

$$(2) \quad \psi(u) \equiv \Pi\left(u - 4\sin^2\frac{y\pi}{q}\right) \equiv u^{\frac{q-1}{4}} + b_1 u^{\frac{q-5}{4}} + \ldots + b_{\frac{q-1}{4}}$$

und ihre Resultante, das Doppelprodukt:

$$(3) \qquad R_{p,q} = \Pi\left(4\sin^2\frac{x\pi}{p} - 4\sin^2\frac{y\pi}{q}\right) \text{ bzw.}$$

$$(4) \qquad R_{q,p} = \Pi\left(4\sin^2\frac{y\pi}{q} - 4\sin^2\frac{x\pi}{p}\right) .$$

Ich definiere ferner die Zahlen λ folgendermaßen:

$$(5) \qquad \lambda_{p,q}\, R_{p,q} = |\, R_{p,q}\,|; \quad \lambda_{q,p}\, R_{q,p} = |\, R_{q,p}\,| .$$

Ist n die Anzahl der negativen Faktoren in $R_{p,q}$, so ist

$$(6) \qquad \lambda_{p,q} = (-1)^n .$$

Weil $R_{q,p}$ aus $R_{p,q}$ hervorgeht, wenn alle Faktoren das Zeichen ändern, so folgt:

$$(7) \qquad \lambda_{q,p} = (-1)^{\frac{(p-1)(q-1)}{16}} \lambda_{p,q} .$$

Beispiel. Wir berechnen $\lambda_{101,5}$, indem wir die Anzahl der negativen Faktoren im Produkt $\Pi\left(4\sin^2\frac{x\pi}{101} - 4\sin^2\frac{\pi}{5}\right)$ abzählen. Die Anzahl ist gleich der Anzahl der x-Zahlen $< \frac{101}{5}$ und die Zahl beträgt 11. Es ist also nach (6) : $\lambda_{101,5} = -1$ und nach (7) : $\lambda_{5,101} = 1$.

Ich bezeichne die Grundeinheit $\varepsilon > 1$ in $k(\sqrt{p})$ mit ε_p und die entsprechende Einheit in $k(\sqrt{q})$ mit ε_q, bilde die Produkte: $e_p = -\sqrt{p}\,\varepsilon_p'$ und $e_q = -\sqrt{q}\,\varepsilon_q'$, wobei e_p und e_q total positive Zahlen sind. Ferner zerlege ich p in $k(\sqrt{q})$ in $\mathfrak{p}\mathfrak{p}'$ und q in $k(\sqrt{p})$ in $\mathfrak{q}\mathfrak{q}'$ und betrachte die biquadratischen Restsymbole: $\left(\frac{e_p}{\mathfrak{q}}\right)_4$ und $\left(\frac{e_q}{\mathfrak{p}}\right)_4$. Ersteres ist z. B. so definiert: $\left(\frac{e_p}{\mathfrak{q}}\right)_4 \equiv e_p^{\frac{q-1}{4}}$ (mod $\mathfrak{q}$). Wie sich später zeigen wird, können sie nur die Werte $+1$ und -1 annehmen, und es ist $\left(\frac{e_p}{\mathfrak{q}}\right)_4 = \left(\frac{e_p}{\mathfrak{q}'}\right)_4 ; \left(\frac{e_q}{\mathfrak{p}}\right)_4 = \left(\frac{e_q}{\mathfrak{p}'}\right)_4 .$ Nach diesen Vorbereitungen können wir folgenden Satz für ungerade p und q aussprechen:

Hauptsatz. *Ist die Klassenzahl in $k(\sqrt{pq})$ durch 8 teilbar, dann ist* $\lambda_{q,p}\left(\frac{e_q}{\mathfrak{p}}\right)_4 \equiv \left(\frac{t}{2}\right)^{\frac{h}{8}}$ *(mod p);* $\lambda_{p,q}\left(\frac{e_p}{\mathfrak{q}}\right)_4 \equiv \left(\frac{t}{2}\right)^{\frac{h}{8}}$ *(mod q).*

Zusammen mit dem 1. Satz läßt sich aus $\left(\frac{e_q}{\mathfrak{p}}\right)_4$, $\left(\frac{e_p}{\mathfrak{q}}\right)_4$ und λ bestimmen, ob die Klassenzahl in $k(\sqrt{pq})$ durch 16 teilbar ist oder nicht, und im letzteren Fall, welche Form $N(\sqrt{\varsigma})$ hat.

Bemerkung. Da nach dem Ideal $\mathfrak{p}$ die irrationale Zahl e_q einer rationalen Zahl kongruent ist, so kommt es bei der Bestimmung von $\left(\frac{e_q}{\mathfrak{p}}\right)_4$ darauf an, ob eine rationale Zahl biquadratischer Rest nach dem Modul p ist oder nicht.

Zahlenbeispiele. Die folgende Tabelle ist aufgestellt für die 5 kleinsten Primzahlen p, für welche die Klassenzahl in $k(\sqrt{5p})$ durch 8 teilbar ist. Ferner ist n und daraus $\lambda_{p,5}$ und $\lambda_{5,p}$ berechnet. Bei der Berechnung von $\mathfrak{p}$ ist $\omega = \frac{1+\sqrt{5}}{2}$, ferner ist $\mathfrak{q} = \left(5, \frac{1+\sqrt{p}}{2}\right)$. Die Zahlen e_p sind teilweise nur nach dem Modul 5 angegeben. Ferner ist $e_5 = -\sqrt{5}\left(\frac{1-\sqrt{5}}{2}\right) = \frac{5-\sqrt{5}}{2}$.

p	n	$\lambda_{p,5}$	$\lambda_{5,p}$	$\mathfrak{p}$	e_p	$\left(\frac{e_p}{\mathfrak{q}}\right)_4$	$\left(\frac{e_5}{\mathfrak{p}}\right)_4$	$\lambda_{p,5}\left(\frac{e_p}{\mathfrak{q}}\right)_4$	$\lambda_{5,p}\left(\frac{e_5}{\mathfrak{p}}\right)_4$	$N(\sqrt{\varsigma})$
101	11	-1	1	$(101, 22+\omega)$	$101-10\sqrt{101}$	1	1	-1	1	II. Fall
181	18	1	-1	$(181, 13+\omega)$	$\equiv 1 \pmod 5$	1	1	1	-1	III. „
401	43	-1	-1	$(401, 111+\omega)$	$401-20\sqrt{401}$	1	-1	-1	1	II. „
461	48	1	-1	$(461, 21+\omega)$	$\equiv 1 \pmod 5$	1	-1	1	1	16/h
521	56	1	1	$(521, 99+\omega)$	$\equiv -1 \pmod 5$	-1	-1	-1	-1	I. Fall

B. Für $q = 2$ betrachten wir an Stelle von (3):

(8) $R_{p,2} = \Pi\left(4\sin^2\frac{x\pi}{p} - 4\sin^2\frac{\pi}{8}\right)$. Die Anzahl der negativen Faktoren n ist gleich der Anzahl der x-Zahlen, die kleiner als $\frac{p}{8}$ sind. Der Formel (6) entspricht:

(9) $\lambda_{p,2} = (-1)^n$. Da in $R_{p,2}$ $\frac{p-1}{4}$ Faktoren vorkommen und p die Form $16n+1$ hat, so ist:

(10) $\lambda_{p,2} = \lambda_{2,p} = \lambda$. Ferner ist $e_2 = -\sqrt{2}(1-\sqrt{2}) = 2-\sqrt{2}$. $\left(\frac{e_p}{2}\right)_4$ ist in besonderer Weise zu definieren. $e_p = -\sqrt{p}\,\varepsilon_p'$ hat die Form $a - b\sqrt{p}$, wobei, wie später bewiesen wird, a die Form $8n+1$, b die Form $8n$ hat. Wir definieren nun $\left(\frac{e_p}{2}\right)_4 = 1$, wenn $a+b \equiv 1 \pmod{16}$ und $\left(\frac{e_p}{2}\right)_4 = -1$, wenn $a+b \equiv 9 \pmod{16}$.

Wir erhalten dann folgenden:

Ergänzungssatz zum Hauptsatz: *Ist die Klassenzahl in $k(\sqrt{2p})$ teilbar durch 8, dann ist:*

$$\lambda\left(\frac{e_2}{\mathfrak{p}}\right)_4 \equiv t^{\frac{h}{8}}\ (mod\ p);\ \lambda\left(\frac{e_p}{2}\right)_4 \equiv t^{\frac{h}{8}}\ (mod\ 4)\quad .$$

Zahlenbeispiele. Unter den Primzahlen p, für welche in $k(\sqrt{2p})$ die Klassenzahl durch 8 teilbar ist, haben wir die ersten 3 gewählt und dazu noch $p = 1217$, weil dieses die kleinste Primzahl ist, für welche die Klassenzahl in $k(\sqrt{2p})$ durch 16 teilbar ist. e_p ist mit einer Ausnahme nach dem Modul 16 angegeben.

p	n	λ	$\mathfrak{p}$	e_p	$\left(\frac{e_p}{2}\right)_4$	$\left(\frac{e_2}{\mathfrak{p}}\right)_4$	$\lambda\left(\frac{e_p}{2}\right)_4$	$\lambda\left(\frac{e_2}{\mathfrak{p}}\right)_4$	N $(\sqrt{\varsigma}$
113	9	—1	$(113, 51+\sqrt{2})$	$\equiv 9+8\sqrt{113}$ (mod 16)	1	1	— 1	— 1	I. Fal
257	20	1	$(257, 60+\sqrt{2})$	$257-16\sqrt{257}$	1	— 1	1	— 1	III. Fal
337	25	—1	$(337, 26+\sqrt{2})$	$\equiv 9+8\sqrt{337}$ (mod 16)	1	— 1	— 1	1	II. Fal
1217	84	1	$(1217, 591+\sqrt{2})$	$\equiv 1$ (mod 16)	1	1	1	1	16/h

IV.

Wir gehen zu den Beweisen über und beweisen zunächst folgenden

2. Satz. *Ist die Klassenzahl in $k(\sqrt{pq})$: $h = 8h_1$, so ist:*

$$(11)\qquad \varsigma^{h_1} = \left(\frac{t - u\sqrt{pq}}{2}\right)^{h_1} = |\,R_{p,\,q}\,| = \lambda_{p,\,q}\,R_{p,\,q} = \lambda_{q,\,p}\,R_{q,\,p}\quad .$$

Beweis. Wir teilen die zu p und q teilerfremden Zahlen $< \frac{pq}{2}$ in 4 Klassen ein:

1. die α-Zahlen, für welche gilt: $\left(\frac{\alpha}{p}\right) = \left(\frac{\alpha}{q}\right) = 1$
2. die β-Zahlen, für welche gilt: $\left(\frac{\beta}{p}\right) = \left(\frac{\beta}{q}\right) = -1$
3. die γ-Zahlen, für welche gilt: $\left(\frac{\gamma}{p}\right) = -\left(\frac{\gamma}{p}\right) = 1$
4. die δ-Zahlen, für welche gilt: $\left(\frac{\delta}{p}\right) = -\left(\frac{\delta}{p}\right) = -1$.

Die α- und β-Zahlen zusammengefaßt bezeichnen wir als A-Zahlen, die γ- und δ-Zahlen als B-Zahlen und schließlich die A- und B-Zahlen zusammengefaßt als C-Zahlen.

Die allgemeine Klassenzahlformel (*E. Hecke*, Theorie der algebraischen Zahlen, S. 209) ergibt für h — Äquivalenz im engern Sinn vorausgesetzt — mit unsern Bezeichnungen:

$$h = \frac{2}{\log \varsigma} \log \frac{\Pi \sin \frac{A\pi}{pq}}{\Pi \sin \frac{B\pi}{pq}} \tag{12}$$

oder, wenn wir von den Logarithmen zu den Grundzahlen übergehen, $h = 8h_1$ setzen und radizieren:

$$\varsigma^{4h_1} = \frac{\Pi \sin \frac{A\pi}{pq}}{\Pi \sin \frac{B\pi}{pq}} \; . \tag{13}$$

Für das Folgende brauchen wir verschiedene Formeln der Winkelteilung, und entnehmen sie Webers Algebra, I. Bd., 2. Aufl. Nach Formel 20, S. 478, gilt für jede ungerade Zahl n:

$$2^{\frac{n-1}{2}} \Pi \sin \frac{2\pi\nu}{n} = \sqrt{n} \; . \qquad \left(\nu = 1, 2, \ldots \frac{n-1}{2}\right). \tag{14}$$

Die Wurzel hat das positive Vorzeichen, weil alle Faktoren links positiv sind. Setzen wir $n = pq$ und beachten, daß die $\frac{pq-1}{2}$ Zahlen, die kleiner als $\frac{pq}{2}$ sind, sich zusammensetzen aus den $\frac{(p-1)(q-1)}{2}$ zu p und q teilerfremden Zahlen (C-Zahlen), aus den $\frac{p-1}{2}$ Zahlen λq $\left(\lambda = 1, 2, \ldots \frac{p-1}{2}\right)$ und aus den $\frac{q-1}{2}$ Zahlen μp $\left(\mu = 1, 2, \ldots \frac{q-1}{2}\right)$. Es gilt daher $2^{\frac{pq-1}{2}} \Pi \sin \frac{2\pi\nu}{pq} = 2^{\frac{(p-1)(q-1)}{2}} \Pi \sin \frac{2\pi C}{pq} \cdot 2^{\frac{p-1}{2}} \Pi \sin \frac{2\pi\lambda}{p} \cdot$ $\cdot 2^{\frac{q-1}{2}} \Pi \sin \frac{2\pi\mu}{q}$. Die linke Seite ist wegen (14) $= \sqrt{pq}$, der zweite und dritte Faktor rechts sind aus gleichem Grunde $\sqrt{p}$ und $\sqrt{q}$. Daraus folgt:

$$2^{\frac{(p-1)(q-1)}{2}} \Pi \sin \frac{2\pi C}{pq} = 1 \; , \tag{15}$$

welche Gleichung sich auch schreiben läßt:

$$2^{\frac{(p-1)(q-1)}{2}} \Pi \sin \frac{\pi C}{pq} = 1 \; . \tag{16}$$

Diejenigen C-Zahlen in der Formel (15) nämlich, für welche $2C < \frac{pq}{2}$, ergeben in der Formel (16) die geraden C-Zahlen, diejenigen C-Zahlen in der Formel (15), für welche $2C > \frac{pq}{2}$ ist, ersetzen wir durch die C-Zahlen: $pq - 2C$ und diese ergeben in der Formel (16) die ungeraden C-Zahlen. Multiplizieren wir (16) und (13) und radizieren, so folgt:

$$\varsigma^{2h_1} = 2^{\frac{(p-1)(q-1)}{4}} \Pi \sin \frac{\pi A}{pq} \tag{17}$$

Wir betrachten nun folgende vier positiven Produkte:

$$P_1 = 2^{\frac{(p-1)(q-1)}{8}} \Pi \sin \frac{\alpha \pi}{pq}; \qquad P_2 = 2^{\frac{(p-1)(q-1)}{8}} \Pi \sin \frac{\beta \pi}{pq};$$

$$P_3 = 2^{\frac{(p-1)(q-1)}{8}} \Pi \sin \frac{\gamma \pi}{pq}; \qquad P_4 = 2^{\frac{(p-1)(q-1)}{8}} \Pi \sin \frac{\delta \pi}{pq}.$$

Vergleichen wir die α-Zahlen mit den Zahlen der Linearform: $L: qx + py$, die entstehen, wenn x die früher definierten x- und y die positiven und negativen y-Zahlen durchläuft. Wir bemerken, daß die Zahlen der Linearform eindeutig den α-Zahlen zugeordnet sind, in dem Sinne, daß jede Zahl der Linearform einer und nur einer α-Zahl, mit positivem oder negativem Vorzeichen nach dem Modul pq kongruent ist. Es folgt daraus:

$$P_1 = \left| 2^{\frac{(p-1)(q-1)}{8}} \Pi \sin \frac{(qx + py)\pi}{pq} \right|. \quad \text{(Doppelprodukt.)} \tag{18}$$

Wegen der trigonometrischen Identität: $\sin(\alpha + \beta)\sin(\alpha - \beta) = \sin^2 \alpha - \sin^2 \beta$ folgt, wenn wir noch die Potenzen von 2 in das Produkt hineinnehmen:

$$P_1 = \left| \Pi \left(4\sin^2 \frac{x\pi}{p} - 4\sin^2 \frac{y\pi}{q} \right) \right|. \tag{19}$$

Vergleichen wir in gleicher Weise die γ-Zahlen mit den Zahlen der Linearform: $qx + pz$, wo z die positiven und negativen quadratischen Nichtreste mod q durchläuft, deren absoluter Betrag $< \frac{q}{2}$ ist. Die Zahlen sind quadratische Reste mod p und quadratische Nichtreste mod q. Wie oben erhalten wir entsprechend:

$$P_3 = \left| \Pi \left(4 \sin^2 \frac{x\pi}{p} - 4 \sin^2 \frac{z\pi}{q} \right) \right| . \tag{20}$$

Multiplizieren wir P_1 und P_3, so ergibt sich:

$$P_1 P_3 = \left| \Pi \left(4 \sin^2 \frac{x\pi}{p} - 4 \sin^2 \frac{u\pi}{q} \right) \right| , \tag{21}$$

wo die u-Zahlen sämtliche Zahlen von 1 bis $\frac{q-1}{2}$ durchlaufen. Wir multiplizieren nun zuerst über die u-Zahlen und dieses Produkt gibt nach Weber, Formel 29, S. 480, für ein festes x: $= \dfrac{\sin \frac{xq\pi}{p}}{\sin \frac{x\pi}{p}}$. Multiplizieren wir noch über die x-Zahlen, dann ist: $P_1 P_3 = \left| \dfrac{\Pi \sin \frac{xq\pi}{p}}{\Pi \sin \frac{x\pi}{p}} \right| = 1$. Weil nämlich q quadratischer Rest mod p ist, durchläuft qx mit x die halben Reste mod p. Weil qx nicht kongruent einer Zahl $-qx$ nach dem Modul p sein kann, so sind die Faktoren des Zählers und Nenners, vom Vorzeichen und der Reihenfolge abgesehen, gleich. Es ist also $P_1 P_3 = 1$; vertauschen wir p und q so folgt: $P_1 P_4 = 1$ und schließlich wegen $P_1 P_2 P_3 P_4 = 1 : P_2 P_3 = 1$ und $P_2 P_4 = 1$, woraus folgt: $P_1 = P_2$; $P_3 = P_4$. Die rechte Seite der Gleichung (17) gibt $P_1 P_2 = P_1^2$, und durch Radizieren ergibt sich, wenn wir für P_1 Gleichung (19) setzen:

$$\varsigma^{h_1} = \left(\frac{t - u\sqrt{pq}}{2} \right)^{h_1} = | R_{p,q} | = \lambda_{p,q} R_{p,q} = \lambda_{q,p} R_{q,p}, \tag{22}$$

was zu beweisen war.

Ergänzungssatz zum 2. Satz. *Ist die Klassenzahl in $k(\sqrt{2p})$ $h = 8h_1$, so ist:*

$$\varsigma^{h_1} = (t - u\sqrt{2p})^{h_1} = \left| \Pi \left(4 \sin^2 \frac{\pi x}{p} - 4 \sin^2 \frac{\pi}{8} \right) \right| = \tag{23}$$

$$= | R_{p,2} | = \lambda R_{p,2} = \lambda R_{2,p} .$$

Beweis. Wir teilen die zur Diskriminante $d = 8p$ teilerfremden Zahlen $< 4p$ in 4 Klassen ein:

1. die α-Zahlen, für welche gilt: $\left(\frac{2}{\alpha}\right) = 1; \quad \left(\frac{p}{\alpha}\right) = \left(\frac{\alpha}{p}\right) = 1$
2. die β-Zahlen, für welche gilt: $\left(\frac{2}{\beta}\right) = -1; \left(\frac{p}{\beta}\right) = \left(\frac{\beta}{p}\right) = -1$
3. die γ-Zahlen, für welche gilt: $\left(\frac{2}{\gamma}\right) = -1; \left(\frac{p}{\gamma}\right) = \left(\frac{\gamma}{p}\right) = 1$
4. die δ-Zahlen, für welche gilt: $\left(\frac{2}{\delta}\right) = 1; \quad \left(\frac{p}{\delta}\right) = \left(\frac{\delta}{p}\right) = -1.$

Die A-, B-, C-Zahlen definieren wir entsprechend wie oben. Die allgemeine Klassenzahlformel ergibt, Äquivalenz im engern Sinne vorausgesetzt, wenn wir zu den Grundzahlen übergehen, $h = 8h_1$ setzen und radizieren, der Formel (13) entsprechend:

$$\varsigma^{4h_1} = (t - u\sqrt{2p})^{4h_1} = \frac{\Pi \sin \frac{\pi A}{8p}}{\Pi \sin \frac{\pi B}{8p}} \quad . \tag{24}$$

Setzen wir in (14) $n = p$, so ergibt sich:

$$2^{\frac{p-1}{2}} \Pi \sin \frac{2\pi\nu}{p} = \sqrt{p} \left(\nu = 1, 2, \ldots \frac{p-1}{2}\right) \tag{25}$$

und nach einer ähnlichen Überlegung wie bei der Ableitung der Gleichung (16) aus (15) ergibt sich:

$$2^{\frac{p-1}{2}} \Pi \sin \frac{\nu\pi}{p} = \sqrt{p} \ . \quad \left(\nu = 1, 2 \ldots \frac{p-1}{2}\right). \tag{26}$$

Dividieren wir (25) durch (26) so ergibt sich wegen der Identität:

$$2 \sin \alpha = 2 \sin \frac{\alpha}{2} \, 2 \sin \frac{\pi - \alpha}{2}$$

$$2^{\frac{p-1}{2}} \Pi \sin \frac{(p - 2\nu)\pi}{8p} = 1 \ . \tag{27}$$

Durch weitere zweimalige Anwendung der obigen Identität auf (27) folgt:

$$2^{2(p-1)} \Pi \sin \frac{C\pi}{8p} = 1 \, . \tag{28}$$

Multiplizieren wir (24) und (28) und radizieren, so erhalten wir:

$$\varsigma^{2h_1} = 2^{p-1} \Pi \sin \frac{A\pi}{8p} \quad . \tag{29}$$

Es sei wieder, wie oben, $P_1 = 2^{\frac{p-1}{2}} \Pi \sin \frac{\alpha\pi}{8p}$, usw. Vergleichen wir die Zahlen der Linearform: $8x + py$, wo diesmal y die Werte $+1$ und -1 annehmen kann, mit den α-Zahlen, so bemerken wir, daß die Zahlen der Linearform, vom Vorzeichen abgesehen, den α-Zahlen nach dem Modul $8p$ kongruent sind. Es folgt daraus ähnlich wie früher:

$$P_1 = \left| \Pi \left(4 \sin^2 \frac{\pi x}{p} - 4 \sin^2 \frac{\pi}{8} \right) \right| . \tag{30}$$

Die γ-Zahlen entsprechen den Zahlen der Linearform: $8x + pz$, wo z die Werte $+3$ und -3 annehmen kann. Es ist deshalb:

$$P_3 = \left| \Pi \left(4 \sin^2 \frac{x\pi}{p} - 4 \sin^2 \frac{3\pi}{8} \right) \right| , \tag{31}$$ woraus hervorgeht: $P_1 P_3 = \left| \Pi \left(16 \sin^4 \frac{x\pi}{p} - 16 \sin^2 \frac{x\pi}{p} + 2\right) \right| = \left| \Pi 2 \cos \frac{4\pi x}{p} \right| =$

$$= \left| \frac{\Pi\, 2 \sin \frac{8\pi x}{p}}{\Pi\, 2 \sin \frac{4\pi x}{p}} \right| = 1,$$ weil 2 quadratischer Rest mod p ist.

Ähnlich wie vorhin, ergibt sich schließlich: $P_1 P_2 = P_1^2$ und aus (29) folgt durch Radizieren:

$$\varsigma^{h_1} = (t - u\sqrt{2p})^{h_1} = \lambda \Pi \left(4 \sin^2 \frac{x\pi}{p} - 4 \sin^2 \frac{\pi}{8} \right) , \tag{32}$$

womit der Ergänzungssatz bewiesen ist.

V.

In (1) haben wir die Funktion $\varphi(u)$ aufgestellt. Für die Koeffizienten dieser Funktion beweisen wir folgenden

3. Satz. *Die Koeffizienten a_ν der Funktion $\varphi(u)$ sind ganze Zahlen in $k(\sqrt{p})$ und durch $\sqrt{p}$ teilbar.*

Beweis. Die Zahlen $4 \sin^2 \frac{x\pi}{p}$ sind ganze algebraische Zahlen vom Grade $\frac{p-1}{2}$. Die irreduzible Gleichung vom $\frac{p-1}{2}$ Grade, denen sie genügen, mit ganzzahligen rationalen Koeffizienten, und dem Koeffizienten der höchsten Potenz $= 1$, ist in Webers Algebra (S. 480, Formel 28) aufgestellt. Es sind deshalb auch die Zahlen, die aus den Zahlen $4\sin^2\frac{x\pi}{p}$ durch Addition und Multiplikation entstehen, ganze Zahlen.

Nach *Gauß* ist $\Sigma\, 2\cos\frac{2x\pi}{p} = \frac{-1+\sqrt{p}}{2}$, ferner $\Sigma\, 2\cos\frac{2z\pi}{p} = \frac{-1-\sqrt{p}}{2}$, wo z die Nichtreste mod p bedeuten, die $< \frac{p}{2}$ sind. Aus der trigonometrischen Identität: $4\sin^2\alpha = 2 - 2\cos\alpha$ folgt:

$$(33) \qquad \Sigma\, 4\sin^2\frac{x\pi}{p} = \frac{p-1}{2} - \left(\frac{-1+\sqrt{p}}{2}\right) = \frac{p-\sqrt{p}}{2}$$

$$(34) \qquad \Sigma\, 4\sin^2\frac{z\pi}{p} = \frac{p+\sqrt{p}}{2} .$$

Zwischen $x = 2\cos\varphi$ und $A_n(x) = 2\cos n\varphi$ existiert nach *Weber* (S. 475) das System von Gleichungen:

I. $A_1(x) \quad = x;$

II. $A_2(x) \quad = x^2 - 2$ usw., mit der Rekursionsformel:

$A_{n+1}(x) = x A_n(x) - A_{n-1}(x).$

Führen wir in das System dieser Gleichungen die Werte: $y = 4\sin^2\frac{\varphi}{2}$ und $C_n(y) = 4\sin^2\frac{n\varphi}{2}$ ein, so folgt wegen $x = 2 - y$ und $A_n(x) = 2 - C_n(y)$ das neue System von Gleichungen:

I. $C_1(y) \quad = y;$

II. $C_2(y) \quad = -y^2 + 4y$ usw. mit der Rekursionsformel:

$C_{n+1}(y) = (2-y)\, C_n(y) + 2y - C_{n-1}(y) .$

Die Rekursionsformel zeigt, daß auf der rechten Seite der Reihe nach Funktionen vom 1., 2., usw. Grade vorkommen, wobei — was wesentlich ist — kein von y unabhängiger Summand vorkommt. Wir setzen nun in der ersten Gleichung für y: $y_1 = 4\sin^2\frac{x_1\pi}{p}$; $y_2 = 4\sin^2\frac{x_2\pi}{p}$; usw. und addieren über alle $\frac{p-1}{4}$ Werte von y. Dasselbe machen wir bei der zweiten Gleichung, bei der dritten usw. Die linken Seiten haben nach

(33) und (34) die Werte $\dfrac{p-\left(\frac{n}{p}\right)\sqrt{p}}{2}$, auf der rechten Seite kommen der Reihe nach die Potenzsummen: $s_1 = \Sigma y_\nu$; $s_2 = \Sigma y_\nu^2$ usw. vor. Wir erhalten dann das System von Gleichungen:

$$\text{I.}\quad \frac{p-\sqrt{p}}{2} = s_1;$$

$$\text{II.}\quad \frac{p-\left(\frac{2}{p}\right)\sqrt{p}}{2} = -s_2 + 4s_1;$$

$$\text{III.}\quad \frac{p-\left(\frac{3}{p}\right)\sqrt{p}}{2} = s_3 - 6s_2 + 9s_1; \text{ usw.}$$

Aus der ersten Gleichung folgt, daß s_1 durch $\sqrt{p}$ teilbar ist, aus der zweiten Gleichung das nämliche für s_2, usw. Die Rekursionsformel zeigt, daß alle Potenzsummen durch $\sqrt{p}$ teilbar sind.

Die Potenzsummen hängen mit den Koeffizienten durch die *Newton*'schen Gleichungen zusammen.

$$\begin{aligned} 0 &= s_1 + a_1 \\ 0 &= s_2 + a_1 s_1 + 2a_2 \\ 0 &= s_3 + a_1 s_2 + a_2 s_1 + 3a_3 \text{ usw.,} \end{aligned}$$

woraus wir erkennen, daß alle Koeffizienten a_ν durch $\sqrt{p}$ teilbar sind.

Gleicherweise läßt sich natürlich auch beweisen, daß in (2) die Koeffizienten b_ν durch $\sqrt{q}$ teilbar sind.

VI.

Es seien $\varphi(u)$, $\psi(u)$ [vergl. (1), (2)] gegeben und ihre Resultante (3). Dann ist bekanntlich $R_{p,q}$ eine Summe von Produkten der Koeffizienten a_ν und b_ν. Wie aus der Darstellung der Resultante (3) hervorgeht, gibt es nur einen Summanden, der nicht von den b_ν abhängt, nämlich $X^{\frac{q-1}{4}}$, wo $X = \Pi 4 \sin^2 \dfrac{x\pi}{p}$

und einen Summanden, der nicht von den a_ν abhängt, nämlich $(-1)^{\frac{(p-1)(q-1)}{16}} Y^{\frac{p-1}{4}}$, wo $Y = \Pi 4 \sin^2 \frac{y\pi}{q}$. Alle übrigen Summanden sind Multipla, sowohl der Zahlen a_ν als auch der Zahlen b_ν, und mit Rücksicht auf den 3. Satz können wir ihre Summe schreiben: $Z\sqrt{pq}$. Multiplizieren wir die Resultante mit $\lambda_{p,q}$, so folgt wegen Satz 2 und Formel (7):

$$(35) \qquad \left(\frac{t - u\sqrt{pq}}{2}\right)^{h_1} = \lambda_{p,q} X^{\frac{q-1}{4}} \pm Z\sqrt{pq} + \lambda_{q,p} Y^{\frac{p-1}{4}}.$$

Vermittels der Klassenzahlformel und wegen (14) ergibt sich für $X = -\sqrt{p}\,\varepsilon_p'^{h_p}$, wo h_p die ungerade Klassenzahl in $k(\sqrt{p})$ ist und ebenso für $Y = -\sqrt{q}\,\varepsilon_q'^{h_q}$, wo h_q die ungerade Klassenzahl in $k(\sqrt{q})$ ist. Wir können (35) in zwei Kongruenzen nach den Moduln $\sqrt{p}$ und $\sqrt{q}$ zerlegen und erhalten:

$$(36) \qquad \left(\frac{t}{2}\right)^{h_1} \equiv \lambda_{q,p} Y^{\frac{p-1}{4}} \pmod{\sqrt{p}}; \left(\frac{t}{2}\right)^{h_1} \equiv \lambda_{p,q} X^{\frac{q-1}{4}} \pmod{\sqrt{q}}.$$

Bei der ersten Kongruenz steht links eine rationale Zahl, rechts eine ganze Zahl aus $k(\sqrt{q})$, folglich muß die Kongruenz auch nach dem Modul p gelten. Die irrationale Zahl $Y^{\frac{p-1}{4}}$ kann aber nur dann *einer* rationalen Zahl nach dem Modul p kongruent sein, wenn die Differente der Zahl durch p teilbar ist, d. h. wenn $Y^{\frac{p-1}{4}}$ die Form hat: $a + bp\omega \cdot \left(\omega = \frac{1-\sqrt{q}}{2}\right)$.
Dann gilt die Kongruenz sowohl nach dem Modul $\mathfrak{p}$, als auch nach dem Modul $\mathfrak{p}'$, wo $p = \mathfrak{p} \cdot \mathfrak{p}'$ eine Zerlegung von p in $k(\sqrt{q})$ ist. Gehören nun die Zahl α und das Ideal $\mathfrak{p}$ dem gleichen Zahlenkörper an, und ist $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$, ferner $N(\mathfrak{p}) = p$, so definieren wir das biquadratische Restsymbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_4 = +1$ oder $= -1$, je nachdem $\alpha^{\frac{p-1}{4}} \equiv +1$ oder $\equiv -1 \pmod{\mathfrak{p}}$ ist. Wir können also die erste Kongruenz schreiben:

$$(37) \qquad \left(\frac{t}{2}\right)^{h_1} \equiv \lambda_{q,p} \left(\frac{Y}{\mathfrak{p}}\right)_4 \equiv \lambda_{q,p} \left(\frac{Y}{\mathfrak{p}'}\right)_4 \pmod{p}.$$

Nun ist noch nachzuweisen, daß $\left(\frac{Y}{\mathfrak{p}}\right)_4 = \left(\frac{e_q}{\mathfrak{p}}\right)_4$ ist, wobei $e_q = -\sqrt{q}\,\varepsilon_q'$ ist. Aus (37) folgt $\left(\frac{Y}{\mathfrak{p}}\right) = \left(\frac{-\sqrt{q}\,\varepsilon'^{h_q}}{\mathfrak{p}}\right) = 1$. Ferner folgt aus $\left(\frac{\pm\sqrt{q}}{\mathfrak{p}}\right) = 1$ der Reihe nach: $\left(\frac{\varepsilon_q'^{h_q}}{\mathfrak{p}}\right) = 1$, $\left(\frac{\varepsilon_q'}{\mathfrak{p}}\right) = 1$, $\left(\frac{\varepsilon_q'^2}{\mathfrak{p}}\right)_4 = 1$ und schließlich: $\left(\frac{Y}{\mathfrak{p}}\right)_4 = \left(\frac{e_q}{\mathfrak{p}}\right)_4$. Ebenso folgt aus der zweiten Kongruenz (36) $\left(\frac{t}{2}\right)^{h_1} = \lambda_{p,q}\left(\frac{e_p}{\mathfrak{q}}\right)_4 \pmod{q}$, womit der Hauptsatz bewiesen ist.

Um den Ergänzungssatz für $q = 2$ zu beweisen, schreiben wir die Gleichung (32) als eine Kongruenz nach dem Modul $\sqrt{p}$ oder, was wir dürfen, nach dem Modul p an und wir erhalten:

$$t^{h_1} \equiv \lambda\left(4\sin^2\frac{\pi}{8}\right)^{\frac{p-1}{4}} \pmod{p}\,. \tag{38}$$

Nun ist $4\sin^2\frac{\pi}{8} = 2 - \sqrt{2} = e_2$, und mit Benützung des biquadratischen Restsymbols erhalten wir:

$$t^{h_1} \equiv \lambda\left(\frac{e_2}{\mathfrak{p}}\right)_4 \pmod{p}, \tag{39}$$

womit die Hälfte des Ergänzungssatzes bewiesen ist.

Um den zweiten Teil zu beweisen, berechnen wir die Funktion 5. Grades mit den Nullstellen: 0, $4\sin^2\frac{\pi}{8}$, $4\sin^2\frac{2\pi}{8}$, $4\sin^2\frac{3\pi}{8}$, $4\sin^2\frac{4\pi}{8}$. Sie heißt: $t(u) \equiv u^5 - 10u^4 + 34u^3 - 44u^2 + 16u$. Wir dividieren die in (1) definierte Funktion $\varphi(u)$ durch $t(u)$ und der Rest $r(u)$ ist dann eine eindeutig bestimmte Funktion vom 4. Grade. Die Koeffizienten von $r(u)$ sind ganze Zahlen in $k(\sqrt{p})$. Der Algorithmus der Division zeigt nämlich, daß die Koeffizienten von $r(u)$ aus den Koeffizienten von $\varphi(u)$ und von $t(u)$ nur durch die Operationen der Addition, Subtraktion und Multiplikation hervorgehen. Aus $\varphi(u) \equiv t(u) \cdot q(u) + r(u)$ folgt für die Nullstellen u_ν von $t(u)$: $\varphi(u_\nu) = r(u_\nu)$. Man findet so:

$r(0) = \Pi 4 \sin^2 \frac{x\pi}{p} = X = -\sqrt{p}\,\varepsilon_p'^{h_p} = A - B\sqrt{p}$ (A und B ganz und positiv)

$r\left(4 \sin^2 \frac{\pi}{8}\right) = \lambda(t - u\sqrt{2p})^{h_1} = \lambda(T - U\sqrt{2p})$, wegen (32)

$r\left(4 \sin^2 \frac{3\pi}{8}\right) = \lambda(t + u\sqrt{2p})^{h_1} = \lambda(T + U\sqrt{2p})$, (statt $\sqrt{2}, -\sqrt{2}$)

$r\left(4 \sin^2 \frac{2\pi}{8}\right) = 1$ und $r\left(4 \sin^2 \frac{4\pi}{8}\right) = 1$ nach leichter Ausrechnung. Durch Interpolation läßt sich $r(u)$ bestimmen und man findet als Koeffizienten von u^4: $\frac{A - B\sqrt{p} - 4\lambda T + 3}{16}$. Weil dieser Ausdruck als ganze Zahl in $k(\sqrt{p})$ von der Form $\frac{M + N\sqrt{p}}{2}$, $M \equiv N \pmod 2$ ist, folgt: $B \equiv 0 \pmod 8$, $A \equiv 1 \pmod 8$. Ferner folgt aus $\lambda T \equiv 1 \pmod 4$: $A + B \equiv 1 \pmod{16}$ und umgekehrt, aus $\lambda T \equiv -1 \pmod 4$ $A + B \equiv 9 \pmod{16}$ und umgekehrt. Setzen wir $-\sqrt{p}\,\varepsilon_p' = a - b\sqrt{p}$, so folgt, weil h_p ungerade ist $A \equiv a \pmod{16}$; $B \equiv b \pmod{16}$. Das Symbol $\left(\frac{e_p}{2}\right)_4$ soll nun $+1$ sein, wenn $a + b \equiv 1 \pmod{16}$ und -1, wenn $a + b \equiv 9 \pmod{16}$. Es ist dann: $\lambda T \equiv \left(\frac{e_p}{2}\right)_4 \pmod 4$ oder $T \equiv \lambda \left(\frac{e_p}{2}\right)_4 \pmod 4$. Andererseits folgt aus der Gleichung $(t - u\sqrt{2p})^{h_1} = T - U\sqrt{2p}$, weil u und U gerade Zahlen sind: $t^{h_1} \equiv T \pmod{2\sqrt{2}}$, bzw. $t^{h_1} \equiv T \pmod 4$. Aus den beiden Kongruenzen für T folgt:

(40) $\qquad t^{h_1} \equiv \lambda \left(\frac{e_p}{2}\right)_4 \pmod 4$, womit auch der zweite Teil des Ergänzungssatzes bewiesen ist.