Werk

Titel: Mathematische Annalen
Ort: Leipzig
Jahr: 1877
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235181684_0012
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0012

LOG Id: LOG_0019
LOG Titel: Bemerkungen zum analytischen Beweise des cubischen Reciprocitätsgesetzes
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN235181684
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235181684

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Bemerkungen zum analytischen Beweise des cubischen Reciprocitätsgesetzes.

Von V. Dantscher in Wien.

In der Abhandlung „Applications de l'Algèbre à l'Arithmétique transcendante“*), welche die bekannten schönen Beweise des quadratischen und biquadratischen Reciprocitätsgesetzes durch periodische Functionen enthält, bemerkt Herr Eisenstein, dass auch das cubische Reciprocitätsgesetz nach derselben Methode bewiesen werden könne; indessen hat die Ausführung dieses Gedankens doch manches Eigenthümliche für sich, so dass eine kurze Darstellung vielleicht nicht ungerechtfertigt erscheint**), umsomehr, als dieselbe Gelegenheit bietet zu zeigen, dass die Theilbarkeit der Coefficienten der Theilungsgleichung durch einen eingliedrigen Primzahltheiler (worauf sich der Irreductibilitätsbeweis stützt) auch in den Ausnahmefällen ohne umständliche Reihenentwickelungen leicht erschlossen werden kann.

I.

Die Theorie der cubischen Reste erfordert die Einführung der complexen Zahlen $a+b\varrho$***) (a und b reale ganze Zahlen, $\varrho^2+\varrho+1=0$). Die Eigenschaften dieses Zahlensystemes lassen sich nach Analogie jener der gemeinen complexen Zahlen leicht entwickeln und sind, so weit es für den vorliegenden Zweck erforderlich ist, in der Eisenstein'schen Abhandlung „Beweis des Reciprocitätssatzes für die cubischen Reste u. s. w.“ Crelle's J. XXVII, oder in den Vorlesungen „Die Lehre von der Kreistheilung“ von H. Prof. Dr. Paul Bachmann, Leipzig 1872, zusammengestellt.

Bedeutet m eine Primzahl ($1-\varrho$ ausgenommen), μ deren Norm, z eine durch m nicht theilbare Zahl, so ist der cubische Charakter von z in Beziehung auf die Primzahl m, den Eisenstein mit dem

*) Mathm. Abh. von Dr. G. Eisenstein, Berlin 1847, p. 127.

**) In der Jenaer Doctordissertation des H. Paul Hübler (1871), die mir leider erst während der Correctur zur Kenntniss gekommen ist, wird der Beweis des cubischen Reciprocitätsgesetzes (der mir übrigens p. 33 bez. des Nachweises, dass die Coeff. M_μ u. N_μ *ganze* complexe Zahlen seien, nicht vollständig zu sein scheint) nicht durch die Symmetrie der analytischen Darstellung von $\left(\frac{n}{m}\right)$ in Beziehung auf m und n geliefert, und werden ausserdem die oben erwähnten Ausnahmefälle nicht behandelt.

***) Gauss' Werke, Bd. II. theoria resid. biqu. commentatio II. Anm. p. 102.

Symbole $\left[\frac{z}{m}\right]$ bezeichnet, definirt durch die Congruenz $\left[\frac{z}{m}\right] \equiv z^{\frac{\mu-1}{3}} \bmod m$. Bilden die Zahlen $r_1, r_2, \cdots r_{\frac{\mu-1}{3}}$ ein Drittelrestsystem mod m, so bilden auch die Zahlen $zr_1, zr_2, \cdots zr_{\frac{\mu-1}{3}}$ ein solches, und ist daher $zr_h \equiv \varrho^i r_k \bmod m$; erhält dabei $i\alpha$ mal den Werth 0, β mal den Werth 1, γ mal den Werth 2, so ist $z^{\frac{\mu-1}{3}} \equiv \varrho^{\beta+2\gamma} \bmod m$, also kann man geradezu setzen:

$$\left[\frac{z}{m}\right] = \varrho^{\beta+2\gamma}. \tag{1}$$

An dieses Lemma knüpft nun die analytische Behandlung an. Sie beruht einerseits auf der Existenz einer doppelt periodischen Function pu, welche ein primitives Periodenpaar 2ω, $2\omega\varrho$ besitzt, andererseits auf der sogenannten complexen Multiplication derselben in der Art, dass $p(\varrho u) = \varrho pu$ ist. Ist $z = z' + (\alpha + \beta\varrho)m \equiv z' \bmod m$, so ist dann

$$p\left(\frac{z2\omega}{m}\right) = p\left(\frac{z'2\omega}{m} + 2\alpha\omega + 2\beta\omega\varrho\right) = p\left(\frac{z'2\omega}{m}\right)$$

d. h. die Congruenz $z \equiv z' \bmod m$ ersetzt durch die Gleichung $p\left(\frac{z2\omega}{m}\right) = p\left(\frac{z'2\omega}{m}\right)$, und umgekehrt.

Ist ferner $zr_h \equiv \varrho^i r_k$, so ist $p\left(\frac{zr_h 2\omega}{m}\right) = \varrho^i p\left(\frac{r_k 2\omega}{m}\right)$, woraus der Ausdruck von ϱ^i durch den Quotienten $p\left(\frac{zr_h 2\omega}{m}\right) : p\left(\frac{r_k 2\omega}{m}\right)$ folgt; das cubische Symbol lässt sich also darstellen in der Form

$$\left[\frac{z}{m}\right] = \prod_r \frac{p\left(\frac{zr2\omega}{m}\right)}{p\left(\frac{r2\omega}{m}\right)}, \tag{2}$$

wobei r ein Drittelrestsystem mod m durchläuft.

Eine Function pu mit den verlangten Eigenschaften ist nun nach der Theorie des Herrn Weierstrass die specielle p Function $p(u; 0, g_3)$, in der man überdiess noch zur Vereinfachung $g_3 = 1$ setzen kann; im Folgenden wird $p(u; 0, 1)$ kurz mit pu oder p bezeichnet.

Die für die allgemeine Function $p(u; g_2, g_3)$ bestehende Relation $p(mu; m^{-4}g_2, m^{-6}g_3) = \frac{1}{m^2} p(u; g_2, g_3)$ ergiebt für $g_2 = 0$ und $m = \varrho$ $p(\varrho u) = \varrho pu$, und das Additionstheorem für $p(u; 0, 1$

$$p(u+v) = \frac{2pu \cdot pv\,(pu+pv) - 1 - p'u \cdot p'v}{2(pu-pv)^2}$$

lässt mit Rücksicht darauf, dass die Entwickelung von pu in der Um-

gebung des Nullpunktes mit $\frac{1}{u^2}$ anfängt, unmittelbar erkennen, dass $2\omega\varrho$ eine primitive Periode von pu ist, wenn 2ω eine solche ist.

Um nun in dem Falle, wo z und m zwei ungerade primäre*) Primzahlen P und Q sind, die Beziehung zwischen $\left[\frac{Q}{P}\right]$ und $\left[\frac{P}{Q}\right]$, d. h. das Reciprocitätsgesetz unmittelbar aus der analytischen Darstellung zu ersehen, muss die complexe Multiplication der Function pu durch einen ungeraden primären Multiplicator $m = -1 + 3\alpha + 3\beta\varrho$ genauer ausgeführt werden.

Aus dem Additionstheoreme folgt zunächst, dass sich $p(mu)$ rational durch pu ausdrücken lässt; angenommen nämlich, es sei für einen bestimmten Multiplicator n, der eine ganze complexe Zahl von der Form $a + b\varrho$ ist, $p(nu) = R(pu)$, so ist auch $p[(n \pm \varrho^i)u]$ (wegen $p(\pm \varrho^i u) = \varrho^i pu$, $p'(nu) = \frac{1}{n} R'(pu)\, p'u$ und $p'^2 u = 4pu^3 - 1$) eine rationale Function von pu.

Für $n = 1 - \varrho$ und $n = 2$ findet man aber unmittelbar:

$$(3a) \quad p[(1-\varrho)u] = \frac{p^3u - 1}{(1-\varrho)^2 p^2 u}; \qquad (3b) \quad \frac{p(2u)}{pu} = \frac{p^3u + 2}{4p^3u - 1}.$$

Die erstere dieser Gleichungen lässt in den Grössen $\frac{2\omega}{1-\varrho} = \frac{2+\varrho}{3} 2\omega$ und $\frac{1+\varrho}{1-\varrho} 2\omega = \frac{1+2\varrho}{3} 2\omega$, den Dreitheilungspunkten der Diagonale 2ω, $2\omega\varrho$ des Periodenparallelogrammes, die Nullwerthe von pu erkennen.

Setzen wir also

$$(4.) \qquad \frac{p(mu)}{pu} = \frac{\Phi(pu)}{F(pu)},$$

mit Φ und F ganze Functionen ohne gemeinsamen Theiler bezeichnend, so lässt sich zunächst Folgendes aussagen: die linke Seite bleibt zufolge der Gleichung $p(\varrho u) = \varrho pu$ ungeändert, wenn ϱu an die Stelle von u tritt, und erhält für $u = 0$, wofür pu ∞ wird, den Werth $\frac{1}{m^2}$; also sind Φ und F ganze Functionen desselben Grades von p^3u und ist der Coefficient der höchsten Potenz in Φ gleich 1, wenn er in F m^2 ist.

Zur Darstellung der rationalen Function $\frac{\Phi}{F}$ dient nun die Function

---

*) Jede durch $1-\varrho$ nicht theilbare Zahl $a + b\varrho$ lässt sich durch Multiplication mit einer Einheit $(-1)^\sigma \varrho^\tau$ auf die Form $-1 + 3\alpha + 3\beta\varrho$ bringen und zwar ist, wenn $\mathfrak{a}$ und $\mathfrak{b}$ die kleinsten positiven Reste von a und b mod 3 bezeichnen, $\sigma \equiv \mathfrak{a} + \mathfrak{b} \bmod 2$, $\tau \equiv \frac{1}{2}(1 + (-1)^\sigma)(\mathfrak{a} + 2\mathfrak{b} + 1) + \frac{1}{2}(1 - (-1)^\sigma)(2\mathfrak{a} + \mathfrak{b} + 1) \bmod 3$

$\frac{\sigma(mu)}{\sigma^\mu u}$, *) welche für ein ungerades, durch $1-\varrho$ nicht theilbares m, eine ganze Function von p^3u ist, in pu vom Grade $\frac{\mu-1}{2}$, gegeben in der Form:

$$(5)\quad \frac{\sigma(mu)}{\sigma^\mu u} = \Psi(pu) = m\prod_s\left[pu - p\left(\frac{s2\omega}{m}\right)\right] = m\prod_{\mathfrak{m}}\left[p^3u - p^3\left(\frac{\mathfrak{m}2\omega}{m}\right)\right],$$

wobei s ein halbes Restsystem, $\mathfrak{m}$ ein Sechstelrestsystem mod m durchläuft.

Insbesondere ergiebt sich für $m = 1-\varrho$ $\frac{\sigma(\overline{1-\varrho}v)}{\sigma^3 u} = (1-\varrho)pu$.

Die Grössen $\pm\frac{s2\omega}{m}$ bilden ein vollständiges System incongruenter Unendlichkeitswerthe von $\frac{p(mu)}{pu}$, welche sämmtlich die Ordnungszahl 2 haben, also müssen sie zugleich Nullwerthe von $F(pu)$ sein mit der Ordnungszahl 2. Da m als ungerade vorausgesetzt ist, so ist jeder Werth $\frac{s2\omega}{m}$ verschieden von einer Halbperiode und verschwindet daher $\Psi(pu)$ für ihn nur in der ersten Ordnung; $\Psi^2(pu)$ verschwindet also für jede Wurzel von $F(pu)$ in derselben Ordnung, die beiden Functionen $\mu-1^{\text{ten}}$ Grades haben gleiche Coefficienten der höchsten Glieder, also ist

$$(6)\quad F(pu) = \Psi^2(pu) = m^2\prod_{\mathfrak{m}}[p^3u - p^3v_{\mathfrak{m}}]^2$$

wobei $\frac{\mathfrak{m}2\omega}{m}$ zur Abkürzung mit $v_{\mathfrak{m}}$ bezeichnet ist.

Denselben Schluss kann man auch mit Benutzung der bekannten Relation $pu = -\frac{d^2\log\sigma u}{du^2}$ machen; durch sie ergiebt sich aus (5):

$$(7)\quad \frac{p(mu)}{pu} = \frac{\mu\Psi^2 + (4p^3u - 1)[\Psi'^2 - \Psi\Psi''] - 6\Psi\Psi' pu}{m^2\Psi^2};$$

allein diese Darstellung ist zum Beweise des Reciprocitätsgesetzes nicht geeignet.

Eine andere, für den gegenwärtigen Zweck entscheidende Einsicht in den Zusammenhang zwischen den Functionen Φ und Ψ verschaffen die aus dem Additionstheoreme erfliessenden Formeln:

$$(8a)\quad p\left(u - \frac{2\omega}{1-\varrho}\right)p\left(u + \frac{2\omega}{1-\varrho}\right) = \frac{1}{pu};$$

$$(8b)\quad p\left(u - \frac{2\omega}{1-\varrho}\right) + p\left(u + \frac{2\omega}{1-\varrho}\right) = -\frac{1}{p^2u}.$$

Aus ihnen folgt wegen $m \equiv -1 \bmod 1-\varrho$:

---

*) Weierstrass in seinen Vorlesungen; vergl. auch Kiepert, Crelle's J. B. 76. „Wirkliche Ausführung der ganzzahligen Multiplication u. s. w."

$$\frac{p\left[m\left(u-\frac{2\omega}{1-\varrho}\right)\right]p\left[m\left(u+\frac{2\omega}{1-\varrho}\right)\right]}{p\left(u-\frac{2\omega}{1-\varrho}\right)p\left(u+\frac{2\omega}{1-\varrho}\right)}$$

$$= \frac{pu}{p(mu)} = \frac{\Phi\left[p\left(u-\frac{2\omega}{1-\varrho}\right)\right]\Phi\left[p\left(u+\frac{2\omega}{1-\varrho}\right)\right]}{m^4\prod_{\mathrm{m}}\left[p^3\left(u-\frac{2\omega}{1-\varrho}\right)-p^3v_{\mathrm{m}}\right]^2\left[p^3\left(u+\frac{2\omega}{1-\varrho}\right)-p^3v_{\mathrm{m}}\right]^2};$$

nach (8a) und (8b) ist:

$$\left[p^3\left(u-\frac{2\omega}{1-\varrho}\right)-p^3v_{\mathrm{m}}\right]\left[p^3\left(u+\frac{2\omega}{1-\varrho}\right)-p^3v_{\mathrm{m}}\right]$$

$$= \frac{1}{p^6u}\left[p^6v_{\mathrm{m}}p^6u - 3p^3v_{\mathrm{m}}p^3u + p^3u + p^3v_{\mathrm{m}}\right],$$

somit ergiebt sich:

$$\frac{p(mu)}{pu} = m^4\,\frac{\prod_{\mathrm{m}}\left[p^6v_{\mathrm{m}}p^6u - 3p^3v_{\mathrm{m}}p^3u + p^3u + p^3v_{\mathrm{m}}\right]^2}{p^{2\mu-2}u\;\Phi\left[p\left(u-\frac{2\omega}{1-\varrho}\right)\right]\;\Phi\left[p\left(u+\frac{2\omega}{1-\varrho}\right)\right]}.$$

Die Function $\prod_{\mathrm{m}}\left[p^6v_{\mathrm{m}}\,p^6u - 3\,p^3v_{\mathrm{m}}\,p^3u + p^3u + p^3v_{\mathrm{m}}\right]$ verschwindet für jede der $\mu - 1$ von einander verschiedenen Wurzeln von $\Phi(pu)$, ist also mit Rücksicht auf die Grade und ersten Coefficienten gleich $\prod_{\mathrm{m}}p^6v_{\mathrm{m}}\;\Phi(pu)$.

Nach dieser Darstellung des Zählers $\Phi(pu)$ erhält $\frac{p(mu)}{pu}$ die Form:

$$(9)\qquad \frac{(pmu)}{pu} = \frac{1}{m^2\prod_{\mathrm{m}}p^6v_{\mathrm{m}}}\prod_{m}\frac{p^6v_{\mathrm{m}}\,p^6u - 3p^3v_{\mathrm{m}}\,p^3u + p^3u + p^3v_{\mathrm{m}}}{\left[p^3u - p^3v_{\mathrm{m}}\right]^2}.$$

Mit Hilfe der bekannten Gleichung:

$$(10)\qquad \sigma(u + 2\nu\omega + 2\nu'\omega') = (-1)^{\nu\nu'+\nu+\nu'}e^{2(\nu\eta+\nu'\eta')(u+\nu\omega+\nu'\omega')}\,\sigma u$$

und der Gleichung $\eta\omega' - \eta'\omega = \frac{\pi}{2}i$, aus welcher hier wegen $\eta' = \varrho^2\eta$

$$(11)\qquad \eta\omega = \eta'\omega' = \frac{\pi i}{2(1+2\varrho)}$$

hervorgeht, zeigt man nun leicht, dass $m^2\prod_{\mathrm{m}}p^6v_{\mathrm{m}}$ den Werth 1 hat.

Aus (5) folgt nämlich zunächst $\frac{\sigma\left(m\frac{2\omega}{1-\varrho}\right)}{\sigma^{\mu}\left(\frac{2\omega}{1-\varrho}\right)} = (-1)^{\frac{\mu-1}{6}}\,m\prod_{\mathrm{m}}p^3v_{\mathrm{m}}$;

nach (10) ist $\frac{\sigma\left(m\frac{2\omega}{1-\varrho}\right)}{\sigma\left(\frac{2\omega}{1-\varrho}\right)} = -(-1)^{\alpha(\beta+1)+\beta} e^{2\left[\frac{\mu-1}{3}+\beta(1+2\varrho)\right]\eta\omega} = -e^{2\frac{\mu-1}{3}\eta\omega}$,

denn nach der Voraussetzung, dass $m = -1 + 3\alpha + 3\beta\varrho$ ungerade ist, ist $\alpha(\beta+1)$ sicher gerade.

Um $\sigma^{\mu-1}\left(\frac{2\omega}{1-\varrho}\right)$ zu berechnen dient die Gleichung $\frac{\sigma(\overline{1-\varrho}u)}{\sigma^3 u} = (1-\varrho)pu$; aus ihr folgt, mit Rücksicht auf $\sigma'(2\omega) = -e^{2\eta\omega}$, $p'^2\left(\frac{2\omega}{1-\varrho}\right) = -1$, für $u = \frac{2\omega}{1-\varrho}$, $\sigma^6\left(\frac{2\omega}{1-\varrho}\right) = -e^{4\eta\omega}$, also $\sigma^{\mu-1}\left(\frac{2\omega}{1-\varrho}\right) = (-1)^{\frac{\mu-1}{6}} e^{2\frac{\mu-1}{3}\eta\omega}$, und somit ist

$$m\prod_{\mathrm{m}} p^3 v_{\mathrm{m}} = -1. \tag{12}$$

Aus (9) erhalten wir demnach die gesuchte Darstellung von $\frac{p(mu)}{pu}$ in der Form:

$$\frac{p(mu)}{pu} = \prod_{\mathrm{m}} \frac{p^6 v_{\mathrm{m}}\, p^6 u - 3p^3 v_{\mathrm{m}}\, p^3 u + p^3 u + p^3 v_{\mathrm{m}}}{[p^3 u - p^3 v_{\mathrm{m}}]^2}, \tag{13}$$

welche nun zum Beweise des Reciprocitätsgesetzes völlig geeignet ist.

Sind nämlich P und Q zwei ungerade primäre Primzahlen, bezeichnen $\mathfrak{p}$ und $\mathfrak{q}$ beziehungsweise Sechstelrestsysteme mod P und mod Q, und setzt man zur Abkürzung $\frac{\mathfrak{p}2\omega}{P} = \omega_{\mathfrak{p}}$, $\frac{\mathfrak{q}2\omega}{Q} = \omega_{\mathfrak{q}}$, so ist nach (2):

$$\left[\frac{Q}{P}\right] = \prod_{\mathfrak{p}} \left[\frac{p(Q\omega_{\mathfrak{p}})}{p\omega_{\mathfrak{p}}}\right]^2, \quad \left[\frac{P}{Q}\right] = \prod_{\mathfrak{q}} \left[\frac{p(P\omega_{\mathfrak{q}})}{p\omega_{\mathfrak{q}}}\right]^2.$$

Benützen wir nun für $\frac{p(Q\omega_{\mathfrak{p}})}{p\omega_{\mathfrak{p}}}$ die obige Darstellung von $\frac{p(mu)}{pu}$, so ergiebt sich:

$$\left[\frac{Q}{P}\right] = \prod_{\mathfrak{p}}\prod_{\mathfrak{q}} \left\{\frac{p^6\omega_{\mathfrak{q}}\, p^6\omega_{\mathfrak{p}} - 3p^3\omega_{\mathfrak{q}}\, p^3\omega_{\mathfrak{p}} + p^3\omega_{\mathfrak{q}} + p^3\omega_{\mathfrak{p}}}{(p^3\omega_{\mathfrak{p}} - p^3\omega_{\mathfrak{q}})^2}\right\}^2;$$

nun ist aber der Ausdruck rechts vollkommen symmetrisch in Beziehung auf $\omega_{\mathfrak{p}}$ und $\omega_{\mathfrak{q}}$, folglich ist das cubische Reciprocitätsgesetz für zwei ungerade primäre Primzahlen P und Q ausgedrückt durch die Formel

$$\left[\frac{Q}{P}\right] = \left[\frac{P}{Q}\right].$$

Nach der Annahme über P und Q ist die Primzahl 2 ausgeschlossen; es ist aber leicht zu zeigen, dass auch $\left[\frac{2}{P}\right] = \left[\frac{P}{2}\right]$ ist. Die Zahl 1 bildet ein Drittelrestsystem mod 2, also ist nach (2) $\left[\frac{P}{2}\right] = \frac{p(P\omega)}{p\omega}$; benützt man für den Ausdruck rechts wieder die Dar-

stellung (13) und bemerkt, dass $4p^3\omega = 1$, $\frac{p^3\omega_\mathfrak{p} + 2}{4p^3\omega_\mathfrak{p} - 1} = \frac{p(2\omega_\mathfrak{p})}{p\omega_\mathfrak{p}}$ ist [(36)], so erhält man:

$$\left[\frac{P}{2}\right] = \prod_\mathfrak{p} \frac{p^2(2\omega_\mathfrak{p})}{p^2\omega_\mathfrak{p}} = \left[\frac{2}{P}\right].$$

Auch die Bestimmung von $\left[\frac{1-\varrho}{P}\right]$ lässt sich aus den entwickelten Formeln, wie folgt, treffen.

Nach (2) und (3a) ist

$$\left[\frac{1-\varrho}{P}\right] = \prod_\mathfrak{p} \frac{p^2(\overline{1-\varrho}\,\omega_\mathfrak{p})}{p^2\omega_\mathfrak{p}} = \prod_\mathfrak{p} \left[\frac{p^3\omega_\mathfrak{p} - 1}{(1-\varrho)^2 p^1\omega_\mathfrak{p}}\right]^2;$$

nach (12) ist $\prod_\mathfrak{p} p^6\omega_\mathfrak{p} = \frac{1}{P^2}$; bezeichnet man ferner $N(P)$ mit π und bemerkt $(1-\varrho)^{2\frac{\pi-1}{3}} = 3^{\frac{\pi-1}{3}}\varrho^{\frac{\pi-1}{3}}$, so ergiebt sich:

$$\left[\frac{1-\varrho}{P}\right] = 3^{-\frac{\pi-1}{3}}\varrho^{-\frac{\pi-1}{3}} P^2 \prod_\mathfrak{p} [p^3\omega_\mathfrak{p} - 1]^2.$$

Da nun $p^3\left(\frac{2\omega}{3}\right) = 1$ ist, wie man aus (3a) erschliesst, so kann man setzen:

$$P^2 \prod_\mathfrak{p} [p^3\omega_\mathfrak{p} - 1]^2 = P^2 \prod_\mathfrak{p} \left[p^3\omega_\mathfrak{p} - p^3\left(\frac{2\omega}{3}\right)\right]^2 = \frac{\sigma^2\left(\frac{P2\omega}{3}\right)}{\sigma^{2\pi}\left(\frac{2\omega}{3}\right)} \quad [(5)].$$

Nach (10) und (11) ist $\frac{\sigma^2\left(\frac{P2\omega}{3}\right)}{\sigma^2\left(\frac{2\omega}{3}\right)} = e^{4\frac{\pi-1}{9}\eta\omega}\varrho^\beta$; um $\sigma^{2\pi-2}\left(\frac{2\omega}{3}\right)$ zu bestimmen benützen wir die auch für beliebige Invarianten g_2, g_3 giltige Gleichung $\sigma(2u) = -\sigma^4 u \cdot p'u$, und bemerken:

$$\sigma\left(\frac{4\omega}{3}\right) = \sigma\left(-\frac{2\omega}{3} + 2\omega\right) = e^{\frac{2\eta\omega}{3}}\sigma\left(\frac{2\omega}{3}\right), \quad p'^2\left(\frac{2\omega}{3}\right) = 3;$$

also ist

$$(9) \quad \sigma^{-2\pi+2}\left(\frac{2\omega}{3}\right) = 3^{\frac{\pi-1}{3}} e^{-4\frac{\pi-1}{9}\eta\omega}, \text{ und somit } \frac{\sigma^2\left(\frac{P2\omega}{3}\right)}{\sigma^{2\pi}\left(\frac{2\omega}{3}\right)} = 3^{\frac{\pi-1}{3}}\varrho^\beta.$$

Damit ergiebt sich nun

$$\left[\frac{1-\varrho}{P}\right] = \varrho^{\beta - \frac{\pi-1}{3}} = \varrho^{2\alpha},$$

denn $\frac{\pi-1}{3} \equiv \alpha + \beta \bmod 3$.

Ist also P eine primäre Primzahl $A + B\varrho$, so ist der cubische Charakter von $1 - \varrho$ in Beziehung auf P gegeben durch die Formel

$$\left[\frac{1-\varrho}{P}\right] = \varrho^{\frac{2}{3}(A+1)},$$

die offenbar auch für $P = 2$ gilt.

II.

Der Nachweis, dass die Coefficienten der Function

$$\Psi(pu) = mpu^{\frac{\mu-1}{2}} + c_1 pu^{\frac{\mu-r}{2}} + \cdots + c_{\frac{\mu-1}{6}},$$

welche gleich Null gesetzt die Theilungsgleichung darstellt, ganze complexe Zahlen von der Form $a + b\varrho$ sind, und zwar, wenn m eine ungerade primäre Primzahl ist, mit Ausnahme des letzten, für den wir bereits den Werth $(-1)^{\frac{\mu+5}{6}}$ gefunden haben, sämmtlich durch m theilbar sind (worauf sich der Irreductibilitätsbeweis stützt), lässt sich ganz ähnlich so, wie bei der Lemniscatentheilungsgleichung führen.

Um zunächst zu beweisen, dass die Coefficienten ganze Zahlen sind, nehme ich an, dass für ein bestimmtes ungerades primäres m in $\frac{p(mu)}{pu} = \frac{\Phi(pu)}{\Psi^2(pu)}$ Φ eine ganzzahlige Function sei, in welcher der Coefficient von $pu^{\mu-1}$ 1 ist, Ψ eine eben solche Function sei, in welcher der Coefficient von $pu^{\frac{\mu-1}{2}}$ m ist.

Nun ist $p'(mu) = \frac{\Phi\Psi + (\Phi'\Psi - 2\Phi\Psi')p}{m\Psi^3} p'$; halten wir damit zusammen die Gleichung $p'(mu)^2 = 4p^3(mu) - 1$, so folgt

$$(4p^3 - 1)\frac{[\Phi\Psi + (\Phi'\Psi - 2\Phi\Psi')p]^2}{m^2\Psi^6} = \frac{4p^3\Phi^3 - \Psi^6}{\Psi^6},$$

oder

$$[\Phi\Psi + (\Phi'\Psi - 2\Phi\Psi')p]^2 = m^2\frac{4p^3\Phi^3 - \Psi^6}{4p^3 - 1};$$

hieraus erschliesst man sofort, dass die Coefficienten von

$$(1) \qquad \Phi\Psi + (\Phi'\Psi - 2\Phi\Psi')p$$

durch m theilbare ganze Zahlen sind.

Es ist leicht zu sehen, dass man von m aus durch Schritte ± 3 und $\pm 3\varrho$, stets ungerade primäre Zahlen passirend, zu jeder andern Zahl m_1 dieser Art gelangen kann; es genügt also zu zeigen, dass die

angenommene Form der Darstellung von $\frac{p(mu)}{pu}$ auch für $\frac{p(\overline{m\pm 3}\,u)}{pu}$ und für $\frac{p(\overline{m\pm 3\varrho}\,u)}{pu}$ stattfindet.

Bezeichnen wir $\frac{p(\overline{m\pm 3}\,u)}{pu} = \frac{\Phi_{m\pm 3}(pu)}{\Psi^2_{m\pm 3}(pu)}$, $\frac{p(\overline{m\pm 3\varrho}\,u)}{pu} = \frac{\Phi_{m\pm 3\varrho}(pu)}{\Psi^2_{m\pm 3\varrho}(pu)}$,

$$p(3u) = \frac{p^9 + 24p^6 + 3p^3 - 1}{3^2p^2(p^3-2)} = \frac{\varphi}{\psi^2},$$

$$p'(3u) = \frac{(p^9 - 57p^6 + 3p^3 - 1)(p^3+2)}{3^3p^3(p^3-1)^3}\,p' = \frac{\chi}{\psi^3}\,p'$$

so ergiebt das Additionstheorem:

$$(2)\quad p[m\pm 3\,u] = \frac{2p\varphi\Phi(p\Phi\psi^2+\varphi\Psi^2) - \psi'\Psi'\mp\psi\Psi\frac{1}{m}[\Psi(\Phi+p\Phi') - 2\Phi\Psi'p](4p^3-1)}{2[p\Phi\psi^2 - \Psi^2\varphi]^2}.$$

Hierbei sind Zähler und Nenner mit Rücksicht auf (1) ganzzahlige Functionen. Betrachten wir zunächst den Ausdruck $\Psi^2\varphi - p\Phi\psi^2$, der im Nenner auftritt; er muss sowohl Ψ_{m+3} als Ψ_{m-3} als Factor enthalten, und, da diese beiden Functionen zu einander prim sind, wie gleich gezeigt werden soll, auch das Product $\Psi_{m+3}\,\Psi_{m-3}$.

Die Zahlen $m+3$ und $m-3$ sind nämlich nach der Annahme über m offenbar prim; die Wurzeln von Ψ_{m+3} und Ψ_{m-3} sind beziehungsweise dargestellt durch $p\left(\frac{s2\omega}{m+3}\right)$ und $p\left(\frac{r2\omega}{m-3}\right)$, wenn s und r halbe Restsysteme mod $m+3$ und mod $m-3$ bedeuten; soll nun sein $p\left(\frac{r2\omega}{m-3}\right) = p\left(\frac{s2\omega}{m+3}\right)$, so müsste $\frac{r}{m-3} \mp \frac{s}{m+3}$ eine ganze Zahl sein, was nicht möglich ist, da der Werth 0 für r und s ausgeschlossen ist.

Vergleicht man Grade und Anfangscoefficienten, so ergiebt sich:

$$\Psi^2\varphi - p\Phi\psi^2 = \Psi_{m+3}\Psi_{m-3}.$$

Bemerken wir ferner, dass das constante Glied in $\Psi^2\varphi - p\Phi\psi^2$ gleich -1 ist, so können wir nach dem bekannten Satze (Gauss, disq. arithm. 42) sofort erschliessen, dass Ψ_{m+3} und Ψ_{m-3} ganzzahlige Functionen sind, deren constantes Glied den Werth ± 1 hat, und durch Vergleichung mit $\frac{\sigma(\overline{m\pm 3}\,u)}{\sigma^{N(m\pm 3)}u}$, dass die Coefficienten der höchsten Glieder in Ψ_{m+3}, Ψ_{m-3} beziehungsweise $m+3$, $m-3$ sind.

Ferner ist leicht zu zeigen, dass der Zähler in (2) den Factor 2 hat. Setzen wir für einen Augenblick: $p(\overline{m-3}u) = \frac{Z}{2N}$, $p(\overline{m+3}u) = \frac{Z'}{2N'}$, so ist der Ausdruck rechts in (2) für das obere Zeichen $\frac{Z'N}{2NN'}$, für das untere $\frac{ZN'}{2NN'}$; die aus dem Additionstheoreme erfliessenden Formeln:

$$p(u+v)+p(u-v)=\frac{2pu\cdot pv\,(pu+pv)-1}{[pu-pv]^2}$$

und

$$p(u+v)\,p(u-v)=\frac{p^2u\cdot p^2v+pu+pv}{[pu-pv]^2}$$

zeigen aber, dass ZZ' durch 4 und $ZN'+Z'N$ durch 2 theilbar sind; nachdem nun die constanten Glieder in N und $N'\pm 1$ sind, so ist nothwendig sowohl Z als Z' durch 2 theilbar.

Nach der Division durch 2 ist nun der Zähler in (2) $\Phi_{m\pm 3}\,\Psi^2_{m\mp 3}$ und zwar eine ganzzahlige Function.

Da in $\Psi^2_{m\mp 3}$ das constante Glied 1 ist, so erschliesst man nach dem Hilfssatze I, Serret, Algebra, dtsch v. Wertheim, Bd. I. p. 194, leicht, dass auch $\Phi_{m\pm 3}$ eine ganzzahlige Function, deren erster Coefficient 1 sein muss, da der entsprechende Coefficient im Nenner $(m\mp 3)^2$ ist.

In der Darstellung von $\frac{p(m\pm 3u}{pu}$ sind demnach genau dieselben Bedingungen erfüllt, welche für die von $\frac{p(mu)}{pu}$ angenommen werden; dasselbe lässt sich bezüglich $\frac{p(m\pm 3\varrho u)}{pu}$ behaupten, wobei nur $\varrho\psi$ an die Stelle von ψ tritt.

Nun besteht aber die vorausgesetzte Form für $m=-1-3\varrho$, wo sich ergiebt:

$$(3)\quad p[-1-3\varrho u]=\frac{p^6u+(-1-3\varrho)(2-3\varrho)\,p^3u-(-1-3\varrho)}{[(-1-3\varrho)p^3+1]^2}\,pu,$$

folglich besteht sie für jeden ungeraden primären Multiplicator m und sind die Coefficienten von $\Psi(pu)$ ganze Zahlen.

Dass diese Coefficienten mit Ausnahme von $c_{\frac{\mu-1}{6}}$, wenn m eine Primzahl ist, durch m theilbar sind, wird für zweigliedrige Primzahlen vollständig aus dem Umstande erklärt, dass die Coefficienten von $\Phi\Psi+(\Phi'\Psi-2\Phi\Psi')\,p$ sämmtlich durch m theilbar sind.

Zuvörderst bemerke ich noch, dass das constante Glied in Φ gleich $-m$ ist, wie man leicht aus $\frac{p(mu)}{pu}=\frac{\Phi}{\Psi^2}$ ersieht, wenn man u den Werth $\frac{2\omega}{1-\varrho}$ ertheilt.

Setzen wir also:

$$(4)\quad \Phi=p^{\mu-1}+b_1p^{\mu-4}+\cdots+b_hp^{\mu-1-3h}+\cdots-m$$

$$(5)\quad \Psi=mp^{\frac{\mu-1}{2}}+c_1p^{\frac{\mu-7}{2}}+\cdots+c_xp^{\frac{\mu-6x-1}{2}}+\cdots+(-1)^{\frac{\mu+5}{6}},$$

und nehmen an, dass die Coefficienten b_{h+1}, b_{h+2}, $\cdots\, b_{\frac{\mu-1}{3}}$ und c_0,

$c_1, \cdots c_{\varkappa-1}$ durch m theilbar seien, so sind aus dem angegebenen Grunde auch alle Coefficienten des Ausdrucks

$$\left[c_\varkappa p^{\frac{\mu-6\varkappa-1}{2}} + \cdots + (-1)^{\frac{\mu+5}{6}}\right][(\mu-3)\, b_1 p^{3h-3} + \cdots (\mu-3h)\, b_h]$$
$$-[p^{3h} + \cdots b_h]\left[(\mu-6\varkappa-1)c_\varkappa p^{\frac{\mu-6\varkappa-1}{2}} + \cdots + 6c_{\frac{\mu-7}{6}}\, p^3\right]$$

durch m theilbar.

Das constante Glied ergiebt demnach:

$$(\mu - 3h)\, b_h \equiv 0 \bmod m \tag{6}$$

Ist nun m eine zweigliedrige Primzahl, so ist $\mu - 3h$, wenn $0 < h < \mu$ ist, nicht durch m theilbar, folglich ist $b_h \equiv 0 \bmod m$, nun wissen wir aber: $b_{\frac{\mu-1}{3}}$ ist gleich $-m$, also sind $b_1, b_2, \cdots b_{\frac{\mu-1}{3}}$ sämmtlich durch m theilbar.

Der Coefficient der höchsten Potenz ergiebt:

$$(\mu - 6\varkappa - 1)\, c_\varkappa \equiv 0 \bmod m; \tag{7}$$

hier gilt dasselbe: wenn $\varkappa$ kleiner ist als $\frac{\mu-1}{6}$, so muss $c_\varkappa \equiv 0 \bmod m$ sein; c_0 ist aber gleich m, also sind $c_0, c_1, \cdots c_{\frac{\mu-7}{6}}$ sämmtlich durch m theilbar.

Anders aber verhält sich die Sache, wenn m eine eingliedrige Primzahl n (von der Form $6\nu + 5$) ist; dann ist $\mu - 3h$ für die $\frac{n-2}{3}$ Werthe $n, 2n, \cdots \frac{n-2}{3}\, n$ von h, und $n^2 - 6\varkappa - 1$ für die $\frac{n-5}{6}$ Werthe $\frac{5n-1}{6}, \frac{11n-1}{6}, \cdots \frac{n^2-6n-1}{6}$ Werthe von $\varkappa$ durch n theilbar und kann daher die Theilbarkeit der betreffenden Coefficienten b_h und $c_\varkappa$ aus den obigen Congruenzen nicht erschlossen werden.

Aber auch in diesen Ausnahmefällen bleibt die genannte Eigenschaft jener Coefficienten bestehen und lässt sich der Nachweis dafür aus dem bisher Erhobenen ziemlich einfach herstellen; hierzu dient die Bemerkung, dass, mit Rücksicht auf die nachgewiesene Form der rationalen Function $\frac{\Phi}{\psi^2}$, in der Gleichung (7) I. die Coefficienten von $(4p^3 - 1)\,[\psi'^2 - \psi\psi''] - 6p^2\psi\psi'$ sämmtlich durch n^2 theilbar sein müssen.

Aus derselben Gleichung ergiebt sich auch, wenn man im Zähler rechts das constante Glied, welches gleich $-m^3$ sein muss, bestimmt, für $c_{\frac{\mu-7}{6}}$ der Werth $m\frac{m^2+m'}{6}$, wobei m' die zu m conjugirte Zahl bezeichnet; also ist:

$$(8)\quad \Psi = np^{\frac{n^2-1}{2}} + c_1 p^{\frac{n^2-7}{2}} + \cdots + c_\varkappa p^{\frac{n^2-6\varkappa-1}{2}} + \cdots + n^2 \frac{n+1}{6} p^3 - 1.$$

Wenn nun $6\varkappa + 1 \equiv 0 \bmod n$ ist, so sind die $n-1$ Nachbarcoefficienten nach rechts und links sicher durch n theilbar.

Nimmt man an, es sei $\varkappa$ (natürlich kleiner als $\frac{n^2-1}{6}$) der grösste Index, für den die vorstehende Congruenz erfüllt ist, und berechnet den Coefficienten von $p^{\frac{n^2-1}{2}-3\varkappa-2}$ in der Function $(4p^3-1)[\Psi'^2 - \Psi\Psi''] - 6p^2\Psi\Psi''$, und zwar nur mod n^2, so erhält man dafür den Ausdruck $(6\varkappa+6)(6\varkappa+7)c_{\varkappa+1} - \frac{1}{4}(6\varkappa+1)(6\varkappa+3)c_\varkappa$, der, wie man sich leicht überzeugt, seine Bedeutung auch für alle grösseren Werthe von $\varkappa$ und gewiss auch für die Werthe $\varkappa-1$, $\varkappa-2$, $\cdots \varkappa - \frac{n-2}{3}$ behält.

Die Congruenz:

$$(9)\quad 4(6\varkappa+6)(6\varkappa+7)c_{\varkappa+1} - (6\varkappa+1)(6\varkappa+3)c_\varkappa \equiv 0 \bmod n^2,$$

welche sich daraus ergiebt, scheint indess auf den ersten Anblick wenig zu nützen, denn um zu erschliessen, dass $c_\varkappa$ durch n theilbar ist, müsste man zeigen können, dass $c_{\varkappa+1}$ durch n^2 theilbar ist; eine etwas eingehendere Betrachtung zeigt jedoch, dass dies in der That der Fall ist.

Setzen wir in (9) für $\varkappa$ die Werthe $\varkappa+1$, $\varkappa+2$, $\cdots \varkappa + \frac{n-5}{6}$, schreiben zur besseren Uebersicht für $6\varkappa+1$ K, und bilden die Congruenzen:

$$(10)\quad \left.\begin{array}{l} 4(K+5)(K+6)c_{\varkappa+1} - K(K+2)c_\varkappa \equiv 0 \\ 4(K+11)(K+12)c_{\varkappa+2} - (K+6)(K+8)c_{\varkappa+1} \equiv 0 \\ \vdots \qquad\qquad \vdots \\ 4(K+n)(K+n+1)c_{\varkappa+\frac{n+1}{6}} - (K+n-5)(K+n-3)c_{\varkappa+\frac{n-5}{6}} \equiv 0, \end{array}\right\} \bmod n^2$$

so sind die in denselben auftretenden Zahlen $K+\lambda$, mit Ausnahme von K und $K+n$, nicht durch n theilbar, die Coefficienten $c_{\varkappa+1}$, $c_{\varkappa+2}, \cdots c_{\varkappa+\frac{n+1}{6}}$ dagegen, wie bereits angedeutet wurde, sicher durch n theilbar.

Aus der letzten Congruenz folgt nun, dass $c_{\varkappa+\frac{n-5}{6}}$ durch n^2 theilbar ist, aus der vorletzten, dass $c_{\varkappa+\frac{n-11}{6}}$ durch n^2 theilbar ist, u. s. w.; aus der zweiten, dass $c_{\varkappa+1}$ durch n^2 theilbar ist, aus der ersten endlich, dass $c_\varkappa$ durch n theilbar ist.

Denselben Schluss kann man machen, indem man die den Werthen $\varkappa - 1, \varkappa - 2, \cdots \varkappa - \frac{n+1}{3}$ entsprechenden Congruenzen:

$$\left.\begin{array}{c} 4(K-1)Kc_k-(K-6)(K-4)c_{\varkappa-1} \equiv 0 \\ 4(K-7)(K-6)c_{k-1}-(K-12)(K-10)c_{\varkappa-2} \equiv 0 \\ \cdot \qquad\qquad \cdot \\ \cdot \qquad\qquad \cdot \\ \cdot \qquad\qquad \cdot \\ 4(K-2n+3)(K-2n+4)c_{\varkappa-\frac{n-2}{3}}-(K-2n-2)(K-2n)c_{\varkappa-\frac{n+1}{3}} \equiv 0 \end{array}\right\} \bmod n^2$$

aus (9) bildet. Hierbei sind wiederum die Zahlen $K - \lambda'$, mit Ausnahme von K und $K - 2n$, nicht durch n theilbar, dagegen die Coefficienten $c_{\varkappa-1}, \cdots c_{\varkappa-\frac{n-2}{3}}$ sämmtlich durch n theilbar; also sind die Coefficienten $c_{\varkappa-\frac{n-2}{3}}, c_{\varkappa-\frac{n-5}{3}}, \cdots c_{\varkappa-1}$ durch n^2, und $c_\varkappa$ durch n theilbar.

Das Resultat ist daher das folgende: auch wenn $6\varkappa + 1 \equiv 0 \bmod n$ ist, ist $c_\varkappa$ durch n theilbar (ausgenommen $c_{\frac{n^2-1}{6}}$); überdiess sind seine $\frac{n+1}{6}$ Nachbarn nach rechts und $\frac{n-2}{3}$ Nachbarn nach links durch n^2 theilbar.

Dass auch die Coefficienten b_h durch n theilbar sind, wenn $h \equiv 0 \bmod n$, folgt schon aus der in I. angegebenen zweiten Entstehung von Φ aus Ψ.

Wien, am 27. März 1877.