Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0120
LOG Titel: Supplemente. I. Ueber einige Sätze aus der Theorie der Kreistheilung von Gauss.
LOG Typ: chapter

Contact

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

I. Ueber einige Sätze aus der Theorie der Kreistheilung von Gauss.

§. 111.

Wir schicken zunächst ein Lemma aus der Theorie der Fourier'schen Reihen voraus, deren Glieder nach den Cosinus der successiven Vielfachen eines Winkels fortschreiten; es wird in derselben nachgewiesen*), dass für alle reellen Werthe von x zwischen $x = 0$ und $x = \pi$ mit Einschluss dieser Grenzen stets

$$\varphi(x) = \tfrac{1}{2}a_0 + a_1 \cos x + a_2 \cos 2x + a_3 \cos 3x + \cdots$$

ist, wenn $\varphi(x)$ eine innerhalb dieses Intervalles endliche und stetige Function bedeutet, welche nicht unendlich viele Maxima und Minima hat, und wo die Coefficienten $a_0, a_1, a_2 \ldots$ durch die Gleichung

$$a_s = \frac{2}{\pi}\int_0^{\pi} \varphi(x) \cos sx\, dx$$

bestimmt werden. Hieraus folgt für $x = 0$

$$\pi\varphi(0) = \sum_{-\infty}^{+\infty} \int_0^{\pi} \varphi(x) \cos sx\, dx,$$

wo das Summenzeichen sich auf den Buchstaben s bezieht, für welchen Null und alle ganzen positiven und negativen Zahlwerthe der Reihe nach einzusetzen sind. Auf diesen der genannten Theorie entlehnten Satz stützen wir uns im Folgenden.

*) *Dirichlet*: *Sur la convergence des séries etc.* (Crelle's Journal IV); derselbe Beweis ist vereinfacht im Repertorium der Physik von Dove und Moser. Bd. I. Vergl. *B. Riemann: Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe.* 1867.

Zunächst verallgemeinern wir denselben, indem wir das Integral

$$\int_0^{2h\pi} f(x)\cos sx\,dx$$

betrachten, in welchem h eine positive ganze Zahl, s eine positive oder negative ganze Zahl, und $f(x)$ eine Function bedeutet, welche innerhalb des Integrationsgebietes den obigen Bedingungen genügt. Man kann dasselbe in $2h$ Integrale von der Form

$$\int_{r\pi}^{(r+1)\pi} f(x)\cos sx\,dx$$

zerlegen, wo für r der Reihe nach die Zahlen $0, 1, 2 \ldots$ bis $2h-1$ zu setzen sind; je nachdem r eine gerade oder ungerade Zahl ist, ersetzen wir die Integrationsvariabele x durch $r\pi + x$, oder durch $(r+1)\pi - x$; dadurch geht das vorstehende Integral in

$$\int_0^{\pi} f(r\pi + x)\cos sx\,dx, \text{ oder in } \int_0^{\pi} f((r+1)\pi - x)\cos sx\,dx$$

über, und hieraus ergiebt sich zufolge des obigen Satzes entsprechend

$$\sum_{-\infty}^{+\infty} \int_{r\pi}^{(r+1)\pi} f(x)\cos sx\,dx = \pi f(r\pi), \text{ oder } = \pi f((r+1)\pi),$$

wo die Summe links sich wieder auf alle ganzen Zahlen s bezieht. Setzt man hierin für r die ganzen Zahlen $0, 1, 2 \ldots 2h-1$, und addirt die so entstehenden Gleichungen, so erhält man den Satz

$$2\pi\{\tfrac{1}{2}f(0) + f(2\pi) + f(4\pi) + \cdots + f(2(h-1)\pi) + \tfrac{1}{2}f(2h\pi)\} = \sum_{-\infty}^{+\infty} \int_0^{2h\pi} f(x)\cos sx\,dx.$$

§. 112.

Wir beschäftigen uns nun mit den beiden folgenden bestimmten Integralen

$$p = \int_{-\infty}^{+\infty} \cos(x^2)\, dx, \quad q = \int_{-\infty}^{+\infty} \sin(x^2)\, dx;$$

dass dieselben wirklich bestimmte endliche Werthe besitzen, obgleich die Functionen unter den Integralzeichen für unendlich grosse Werthe von x nicht unendlich klein werden, erkennt man leicht durch die Transformationen

$$p = 2\int_0^{\infty} \cos(x^2)\, dx = \int_0^{\infty} \frac{\cos y}{\sqrt{y}}\, dy$$

$$q = 2\int_0^{\infty} \sin(x^2)\, dx = \int_0^{\infty} \frac{\sin y}{\sqrt{y}}\, dy;$$

denn zerlegt man das ganze unendliche Integrationsgebiet der positiven Variabeln y in solche Intervalle, in deren jedem die unter dem Integralzeichen befindliche Function ihr Zeichen nicht ändert, so ergiebt sich, dass die Bestandtheile, welche diesen Intervallen entsprechen, eine unendliche Reihe bilden, deren Glieder abwechselnde Zeichen haben und dem absoluten Werthe nach beständig und zwar ins Unendliche abnehmen; woraus folgt, dass diese Reihe, sowohl bei dem Integrale p, wie bei q, eine convergente ist. Für unsern Zweck genügt dieser Nachweis der Endlichkeit von p und q; die numerischen Werthe dieser Integrale werden sich von selbst aus der folgenden Untersuchung ergeben*).

Beide Integrale bilden nur specielle Fälle des folgenden

---

*) *Dirichlet: Recherches sur diverses appl.* etc. §. 9. Vergl. *Dirichlet: Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies* (Crelle's Journal XVII).

$$\Delta = \int_{-\infty}^{+\infty} \cos(\delta + x^2)\, dx = p\cos\delta - q\sin\delta,$$

wo δ eine beliebige Constante bedeutet; bezeichnen wir ferner mit α eine beliebige positive Constante und mit $\sqrt{\alpha}$ die *positiv* genommene Quadratwurzel aus α, so ergiebt sich, wenn man die Integrationsvariabele x durch $x\sqrt{\alpha}$ ersetzt, folgende Gleichung

$$\frac{\Delta}{\sqrt{\alpha}} = \int_{-\infty}^{+\infty} \cos(\delta + \alpha x^2)\, dx$$

(wäre $\sqrt{\alpha}$ negativ, so müsste man auch in dem Integrale rechter Hand die beiden Grenzen mit einander vertauschen). Wir führen nun eine zweite positive Constante β ein, und zerlegen das vorstehende Integral in unendlich viele Bestandtheile von der Form

$$\int_{s\beta}^{(s+1)\beta} \cos(\delta + \alpha x^2)\, dx,$$

wo für s successive alle ganzen Zahlen von $-\infty$ bis $+\infty$ einzusetzen sind; in jedem einzelnen solchen Integrale ersetzen wir die Integrationsvariabele x durch $s\beta + x$, wodurch es in das folgende übergeht

$$\int_0^{\beta} \cos(\delta + \alpha s^2\beta^2 + 2\alpha s\beta x + \alpha x^2)\, dx.$$

Wir verfügen nun über die beiden bis jetzt ganz willkürlichen positiven Constanten α und β folgendermaassen: unter m verstehen wir irgend eine positive ganze Zahl, und setzen $\alpha\beta^2 = 2m\pi$, $2\alpha\beta = 1$, d. h. also

$$\beta = 4m\pi, \quad \alpha = \frac{1}{8m\pi}.$$

Da nun s eine ganze Zahl ist, so wird

$$\cos(\delta + \alpha s^2\beta^2 + 2\alpha s\beta x + \alpha x^2) = \cos(\delta + sx + \alpha x^2)$$
$$= \cos\left(\delta + \frac{x^2}{8m\pi}\right)\cos sx - \sin\left(\delta + \frac{x^2}{8m\pi}\right)\sin sx,$$

und folglich

$$\int_{s\beta}^{(s+1)\beta} \cos(\delta + \alpha x^2)\, dx$$

$$= \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx - \int_0^{4m\pi} \sin\left(\delta + \frac{x^2}{8m\pi}\right) \sin sx\, dx.$$

Das zweite Integral rechter Hand, welches unter dem Integralzeichen den Factor $\sin sx$ enthält, verschwindet offenbar für $s = 0$, und nimmt für je zwei gleiche, aber entgegengesetzte Werthe von s ebenfalls gleiche, aber entgegengesetzte Werthe an. Summiren wir daher den vorstehenden Ausdruck für alle ganzen Zahlwerthe s von $-\infty$ bis $+\infty$, so ergiebt sich

$$\frac{\Delta}{\sqrt{\alpha}} = \Delta\sqrt{8m\pi} = \sum_{-\infty}^{+\infty} \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx.$$

Die rechte Seite dieser Gleichung ist nun genau so gebaut wie in dem Satze am Schlusse des vorhergehenden Paragraphen; setzen wir zur Abkürzung

$$f(x) = \cos\left(\delta + \frac{x^2}{8m\pi}\right),$$

so erhalten wir

$$\Delta\sqrt{8m\pi} = 2\pi\{\tfrac{1}{2}f(0) + f(2\pi) + \cdots + f(2(2m-1)\pi) + \tfrac{1}{2}f(4m\pi)\},$$

wo links die Quadratwurzel

$$\sqrt{8m\pi} = \frac{1}{\sqrt{\alpha}}$$

positiv zu nehmen ist. Nun ist ferner, wenn s irgend eine ganze Zahl bedeutet,

$$f(4m\pi + 2s\pi) = f(2s\pi),$$

also

$$f(2s\pi) = \tfrac{1}{2}f(2s\pi) + \tfrac{1}{2}f(4m\pi + 2s\pi);$$

mithin kann die in den Parenthesen eingeschlossene Summe auch in die Form

$$\tfrac{1}{2}\sum f(2s\pi)$$

gebracht werden, wo der Buchstabe s die Zahlen

$$0,\ 1,\ 2 \ldots (4m-1)$$

oder irgend ein anderes vollständiges Restsystem in Bezug auf den Modul $4m$ durchlaufen muss; und man erhält also

$$\Delta\sqrt{8m\pi} = \pi \sum \cos\left(\delta + s^2 \frac{\pi}{2m}\right).$$

Setzt man ferner $4m = n$, so dass n irgend eine ganze positive, aber durch 4 theilbare Zahl bedeutet, und bezeichnet man mit $\sqrt{n}$ und $\sqrt{\frac{1}{2}\pi}$ die *positiv* genommenen Quadratwurzeln aus n und $\frac{1}{2}\pi$, so nimmt die Gleichung folgende Gestalt an

$$\Delta\sqrt{n} = \sqrt{\tfrac{1}{2}\pi} \cdot \sum \cos\left(\delta + s^2 \cdot \frac{2\pi}{n}\right),$$

wo s ein vollständiges Restsystem in Bezug auf den Modul n durchlaufen muss. Nun ist

$$\Delta = p\cos\delta - q\sin\delta,$$

wo p, q die obigen Integralwerthe bedeuten, die von n und dem willkürlichen δ ganz unabhängig sind; wir können daher p und q durch eine specielle Annahme für n, am einfachsten durch die Annahme $n = 4$ bestimmen; auf diese Weise erhalten wir

$$2(p\cos\delta - q\sin\delta) = 2(\cos\delta - \sin\delta)\sqrt{\tfrac{1}{2}\pi},$$

und in Folge der Willkürlichkeit von δ

$$p = q = \sqrt{\tfrac{1}{2}\pi}.$$

Nachdem so die Werthe von p und q gefunden sind, nimmt unsere obige Gleichung folgende Gestalt an

$$\sum \cos\left(\delta + s^2 \frac{2\pi}{n}\right) = (\cos\delta - \sin\delta)\sqrt{n},$$

und sie zerfällt in die beiden folgenden:

$$\sum \cos\left(s^2 \frac{2\pi}{n}\right) = \sqrt{n}$$

$$\sum \sin\left(s^2 \frac{2\pi}{n}\right) = \sqrt{n};$$

hierin bedeutet also n jede beliebige ganze positive Zahl, welche $\equiv 0 \pmod 4$ ist, und $\sqrt{n}$ die *positiv* genommene Quadratwurzel aus n. Bezeichnet man zur Abkürzung $\sqrt{-1}$ mit i, und, wie gewöhnlich, mit e die Basis des natürlichen Logarithmensystems, so kann man beide Gleichungen in die eine Gleichung

$$\sum e^{s^2 \cdot \frac{2\pi i}{n}} = (1+i)\sqrt{n}$$

zusammenziehen, in welcher der Buchstabe s ein vollständiges Restsystem (mod. n) zu durchlaufen hat.

§. 113.

Wir wollen jetzt Summen betrachten, welche die vorstehende als speciellen Fall enthalten; wir bezeichnen mit n irgend eine ganze positive Zahl, mit h irgend eine positive oder negative ganze Zahl, und setzen zur Abkürzung

$$\sum e^{s^2 \frac{2h\pi i}{n}} = \varphi(h, n),$$

wo der Summationsbuchstabe s irgend ein vollständiges Restsystem in Bezug auf den Modulus n durchlaufen muss. Mit Hülfe dieser Bezeichnungsweise können wir den im vorigen Paragraphen bewiesenen Satz in folgender Weise ausdrücken:

$$\varphi(1, n) = (1 + i)\sqrt{n}, \quad \text{wenn} \quad n \equiv 0 \pmod 4.$$

Der Ausdruck $\varphi(h,n)$ besitzt nun die folgenden drei Eigenschaften:

1. Ist $h \equiv h' \pmod n$, so ist

$$\varphi(h, n) = \varphi(h', n);$$

dies folgt unmittelbar daraus, dass für jeden ganzzahligen Werth von s stets

$$e^{s^2 \frac{2h\pi i}{n}} = e^{s^2 \frac{2h'\pi i}{n}}$$

ist.

2. Ist a relative Primzahl gegen n, so ist

$$\varphi(ha^2, n) = \varphi(h, n);$$

denn es ist

$$\varphi(ha^2, n) = \sum e^{(as)^2 \frac{2h\pi i}{n}},$$

und wenn s ein vollständiges Restsystem nach dem Modul n durchläuft, so gilt (nach §. 18) dasselbe von as.

3. Sind m, n irgend zwei relative Primzahlen, und beide positiv, so ist

$$\varphi(hm, n)\ \varphi(hn, m) = \varphi(h, mn).$$

Es ist nämlich

$$\varphi(hm, n) = \Sigma\, e^{s^2 \frac{2hm\pi i}{n}}, \quad \varphi(hn, m) = \Sigma\, e^{t^2 \frac{2hn\pi i}{m}},$$

wo die Buchstaben s, t vollständige Restsysteme resp. in Bezug auf die Moduln n, m durchlaufen müssen; und folglich ist

$$\varphi(hm, n)\ \varphi(hn, m) = \Sigma\, e^{\left(\frac{ms^2}{n} + \frac{nt^2}{m}\right) 2h\pi i},$$

wo das Summenzeichen rechter Hand sich auf alle mn Combinationen jedes Werthes von s mit jedem Werthe von t bezieht. Da nun

$$\frac{ms^2}{n} + \frac{nt^2}{m} = \frac{(ms + nt)^2}{mn} - 2st$$

ist, und alle Multipla von $2\pi i$ im Exponenten fortgelassen werden können, so ist auch

$$\varphi(hm, n)\ \varphi(hn, m) = \Sigma\, e^{(ms+nt)^2 \frac{2h\pi i}{mn}},$$

wo das Summenzeichen sich wieder auf sämmtliche Werthe von s und t bezieht. Setzt man nun

$$ms + nt = r,$$

so nimmt r, wenn s und t alle ihnen zukommenden Werthe durchlaufen, im Ganzen mn Werthe an, und zwar sind diese alle incongruent nach dem Modulus mn; denn aus

$$ms + nt \equiv ms' + nt' \pmod{mn}$$

folgt

$$ms \equiv ms' \pmod{n}, \quad nt \equiv nt' \pmod{m}$$

und folglich, da m und n relative Primzahlen sind,

$$s \equiv s' \pmod{n}, \quad t \equiv t' \pmod{m};$$

d. h. die Zahl r nimmt nur dann Werthe an, welche nach dem Modul mn congruent sind, wenn die Werthe von s congruent nach dem Modul n, und gleichzeitig die Werthe von t congruent nach dem Modul m sind. Den mn verschiedenen Combinationen von s und t correspondiren daher mn Werthe von r, welche nach dem Modul mn incongruent sind, und folglich bilden diese Werthe von r ein vollständiges Restsystem nach dem Modul mn. Es ist folglich

$$\varphi(hm, n)\ \varphi(hn, m) = \Sigma\, e^{r^2 \frac{2h\pi i}{mn}} = \varphi(h, mn),$$

was zu beweisen war.

§. 114.

Mit Hülfe dieser Sätze können wir nun den Werth von $\varphi(1,n)$, welcher für den Fall, dass $n \equiv 0 \pmod 4$ ist, schon in §. 112 gefunden ist, auch für alle andern Werthe der Zahl n bestimmen. Ist zunächst n irgend eine *ungerade* Zahl, so nehmen wir in dem letzten Satz des vorigen Paragraphen

$$h = 1, \quad m = 4,$$

und erhalten

$$\varphi(4, n)\ \varphi(n, 4) = \varphi(1, 4n);$$

nun ist nach dem zweiten Satze des vorigen Paragraphen

$$\varphi(4, n) = \varphi(2^2, n) = \varphi(1, n);$$

ferner ist

$$\varphi(n, 4) = 2(1 + i^n),$$

und nach dem in §. 112 gefundenen Resultat

$$\varphi(1, 4n) = (1 + i)\sqrt{4n} = 2(1 + i)\sqrt{n},$$

wo die Quadratwurzel $\sqrt{n}$ wieder positiv genommen werden muss. Hieraus ergiebt sich also

$$\varphi(1, n) \cdot 2(1 + i^n) = 2(1 + i)\sqrt{n}$$

oder

$$\varphi(1, n) = \frac{1 + i}{1 + i^n}\sqrt{n};$$

je nachdem nun $n \equiv 1$ oder $\equiv 3 \pmod 4$ ist, wird

$$i^n = i \quad \text{oder} = -i$$

und folglich

$$\frac{1 + i}{1 + i^n} = 1 \quad \text{oder} = \frac{1 + i}{1 - i} = i,$$

also

$$\varphi(1, n) = \sqrt{n} \quad \text{oder} = i\sqrt{n};$$

diese beiden Fälle lassen sich aber in die eine Formel

$$\varphi(1, n) = i^{\frac{1}{4}(n-1)^2}\sqrt{n}$$

zusammenfassen.

Ist endlich n durch 2, aber nicht durch 4 theilbar, also das Doppelte einer ungeraden Zahl, so setzen wir in dem dritten Satze des vorigen Paragraphen $h = 1$, ferner $m = 2$, und $\frac{1}{2}n$ statt n, wodurch allen Bedingungen desselben Genüge geschieht, und erhalten

$$\varphi(2, \tfrac{1}{2}n)\ \varphi(\tfrac{1}{2}n, 2) = \varphi(1, n);$$

nun ist aber

$$\varphi(\tfrac{1}{2}n, 2) = 0,$$

und folglich auch

$$\varphi(1, n) = 0.$$

Wir wollen die so gewonnenen Resultate in folgender Tabelle zusammenfassen:

$$\begin{aligned}
&\varphi(1, n) = (1+i)\sqrt{n}, && \text{wenn } n \equiv 0 \pmod 4\\
&\varphi(1, n) = i^{\frac{1}{4}(n-1)^2}\sqrt{n}, && \text{wenn } n \equiv 1 \pmod 2\\
&\varphi(1, n) = 0, && \text{wenn } n \equiv 2 \pmod 4.
\end{aligned}$$

Von der grössten Wichtigkeit ist aber die Bemerkung, dass die in den beiden ersten Formeln vorkommende Quadratwurzel $\sqrt{n}$ durchaus *positiv* genommen werden muss, wie es sich bei der Untersuchung in §. 112 herausgestellt hat. Ohne diese nähere Bestimmung würden die vorstehenden Sätze sich auf viel einfachere Art beweisen lassen; *Gauss* wurde zuerst in seiner Theorie der Kreistheilung auf die Betrachtung solcher Summen geführt*); es ergiebt sich dort ohne Schwierigkeit der Werth des Quadrates derselben; der viel tiefer liegenden Bestimmung des Vorzeichens der Quadratwurzel widmete er aber eine besondere Abhandlung**), in welcher er auf einem, von dem hier (in §. 112) eingeschlagenen gänzlich verschiedenen Wege, nämlich durch rein algebraische Zerlegung dieser Summen in Producte, vollständig zum Ziele gelangte.

---

*) *D. A.* art. 356.

**) *Summatio quarumdam serierum singularium.* 1808.

§. 115.

Wir suchen nun den Werth von $\varphi(h, n)$ auch für beliebige Werthe von h zu bestimmen, beschränken uns dabei aber auf den Fall, dass n eine ungerade Primzahl ist, die wir mit p bezeichnen wollen. Bezeichnen wir mit α die sämmtlichen $\frac{1}{2}(p-1)$ incongruenten quadratischen Reste von p, mit β die $\frac{1}{2}(p-1)$ quadratischen Nichtreste, so ist (nach §. 33)

$$\varphi(h, p) = \Sigma\, e^{s^2 \frac{2h\pi i}{p}} = 1 + 2\,\Sigma\, e^{\alpha \frac{2h\pi i}{p}};$$

da ferner

$$1 + \Sigma\, e^{\alpha \frac{2h\pi i}{p}} + \Sigma\, e^{\beta \frac{2h\pi i}{p}} = \Sigma\, e^{s \frac{2h\pi i}{p}} = 0$$

ist, sobald h nicht durch p theilbar ist, so können wir für diesen Fall mit Benutzung des Legendre'schen Symbols

$$\varphi(h, p) = \Sigma\, e^{\alpha \frac{2h\pi i}{p}} - \Sigma\, e^{\beta \frac{2h\pi i}{p}} = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}}$$

setzen, wo s die Werthe $1, 2 \ldots (p-1)$ durchläuft. Da ferner

$$\left(\frac{hs}{p}\right) = \left(\frac{h}{p}\right)\left(\frac{s}{p}\right), \quad \left(\frac{h}{p}\right)\left(\frac{h}{p}\right) = 1$$

ist, so wird

$$\varphi(h,p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{hs}{p}\right) e^{hs \cdot \frac{2\pi i}{p}},$$

oder, da h nicht theilbar durch p ist, und folglich hs gleichzeitig mit s ein vollständiges Restsystem nach dem Modul p durchläuft (mit Ausschluss der Zahl $\equiv 0$),

$$\varphi(h, p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}};$$

für $h = 1$ ergiebt sich

$$\varphi(1, p) = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}}$$

und folglich (nach §. 114)

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

wo die Quadratwurzel $\sqrt{p}$ wieder positiv zu nehmen ist. (Wenn h durch p theilbar ist, so ergiebt sich unmittelbar aus der Definition dieser Summen $\varphi(h, p) = p$.)

Aus dem vorstehenden Resultate in Verbindung mit dem dritten Satze des §. 113 lässt sich nun auf ganz einfache Weise das Reciprocitätsgesetz in der Theorie der quadratischen Reste (§. 42) für je zwei positive ungerade Primzahlen p und q ableiten. Es ist nämlich

$$\varphi(q, p) = \left(\frac{q}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p},$$

und ebenso

$$\varphi(p, q) = \left(\frac{p}{q}\right) i^{\frac{1}{4}(q-1)^2} \sqrt{q},$$

und nach dem vorhergehenden Paragraphen

$$\varphi(1, pq) = i^{\frac{1}{4}(pq-1)^2} \sqrt{pq},$$

und zwar sind alle Quadratwurzeln *positiv* zu nehmen, woraus folgt, dass

$$\sqrt{pq} = \sqrt{p}\sqrt{q}$$

ist. Nach dem dritten Satze des §. 113 ist nun

$$\varphi(p, q)\, \varphi(q, p) = \varphi(1, pq),$$

folglich

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{\frac{1}{4}(p-1)^2 + \frac{1}{4}(q-1)^2} \sqrt{p}\sqrt{q} = i^{\frac{1}{4}(pq-1)^2} \sqrt{pq},$$

und also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\lambda},$$

wo zur Abkürzung λ für

$$\frac{(pq-1)^2-(p-1)^2-(q-1)^2}{4} = \frac{p-1}{2}\,\frac{q-1}{2}\left\{(p+1)(q+1)-2\right\}$$

gesetzt ist; da nun

$$(p+1)(q+1) - 2 \equiv 2 \pmod 4$$

ist, so erhalten wir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\frac{1}{2}(p-1)(q-1)} = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)},$$

womit der Reciprocitätssatz von Neuem bewiesen ist. Dieser Beweis rührt ebenfalls von *Gauss* her*).

*) *Summatio quarumdam serierum singularium.* 1808.

Auf ganz ähnliche Art lassen sich die Sätze (§§. 40, 41) über die Zahlen -1 und 2 beweisen. Aus dem obigen Satze

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}$$

folgt nämlich

$$\varphi(-1, p) = \left(\frac{-1}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p};$$

andererseits ist

$$\varphi(-1, p) = \Sigma\, e^{s^2 \frac{2\pi(-i)}{p}},$$

und hieraus folgt, dass $\varphi(-1, p)$ durch Vertauschung von i mit $-i$ aus $\varphi(1, p)$ hervorgeht, dass also

$$\varphi(-1, p) = (-i)^{\frac{1}{4}(p-1)^2} \sqrt{p}$$

ist; durch Vergleichung dieser beiden Ausdrücke, in denen $\sqrt{p}$ beide Male positiv zu nehmen ist, ergiebt sich aber

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{4}(p-1)^2} = (-1)^{\frac{1}{2}(p-1)}.$$

Setzen wir ferner in dem dritten Satz des §. 113

$$h = 1, \quad m = 8, \quad n = p,$$

so erhalten wir

$$\varphi(8, p)\, \varphi(p, 8) = \varphi(1, 8p);$$

nun ist aber

$$\varphi(1, 8p) = (1 + i)\sqrt{8p} = 4\sqrt{p} \cdot e^{\frac{1}{4}\pi i},$$

ferner

$$\varphi(p, 8) = 4\, e^{\frac{1}{4}p\pi i},$$

ferner (nach dem zweiten Satze des §. 113)

$$\varphi(8, p) = \varphi(2 \cdot 2^2, p) = \varphi(2, p),$$

d. h.

$$\varphi(8, p) = \left(\frac{2}{p}\right) \varphi(1, p) = \left(\frac{2}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p};$$

setzen wir diese Werthe für $\varphi(8, p)$, $\varphi(p, 8)$ und $\varphi(1, 8p)$ in die vorangehende Gleichung ein, so erhalten wir

$$\left(\frac{2}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p} \cdot 4\, e^{\frac{1}{4}p\pi i} = 4\sqrt{p} \cdot e^{\frac{1}{4}\pi i},$$

und hieraus folgt leicht

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

Auf diese Weise sind alle Hauptsätze der Theorie der quadratischen Reste von Neuem bewiesen.

§. 116.

Für den Fall, dass p eine ungerade Primzahl, und h irgend eine durch p nicht theilbare ganze Zahl ist, haben wir im vorigen Paragraphen folgende Gleichung erhalten

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) \varphi(1, p),$$

welche, wenn man den für $\varphi(1, p)$ gefundenen Werth einsetzt, in die folgende übergeht:

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}; \tag{1}$$

soll dieselbe auch für den vorher ausgeschlossenen Fall, in welchem $h \equiv 0 \pmod{p}$ ist, ihre Gültigkeit behalten, so müssen wir übereinkommen, immer

$$\left(\frac{h}{p}\right) = 0$$

zu setzen, wenn h durch p theilbar ist; denn die linke Seite der Gleichung wird

$$\Sigma \left(\frac{s}{p}\right) = 0,$$

weil die Anzahl der quadratischen Reste genau gleich ist der Anzahl der quadratischen Nichtreste. Nach dieser Erweiterung des von Legendre eingeführten Zeichens wird ferner, wenn man an der in §. 46 gegebenen Erklärung des Jacobi'schen Symbols festhält, stets

$$\left(\frac{m}{P}\right) = 0,$$

wenn m keine relative Primzahl zu P ist.

Die Gleichung (1) gilt jetzt allgemein für jede positive ungerade Primzahl p, wenn h irgend eine ganze Zahl bedeutet, und die Summation linker Hand darf auch auf die Zahlclasse $s \equiv 0 \pmod{p}$ ausgedehnt werden. Wir wollen nun zeigen, dass dieser Satz über ungerade positive Primzahlen p sich genau in derselben Fassung

auch auf jede positive ungerade zusammengesetzte Zahl P übertragen lässt, welche durch keine Quadratzahl (ausser 1) theilbar ist. Wir setzen also

$$P = pp'p'' \dots$$

wo $p, p', p'' \dots$ lauter positive ungerade und von einander verschiedene Primzahlen bedeuten, und führen der Bequemlichkeit halber folgende Bezeichnung ein:

$$\frac{P}{p} = Q, \quad \frac{P}{p'} = Q', \quad \frac{P}{p''} = Q'' \dots$$

Schreiben wir nun für jede der Primzahlen $p, p', p'' \dots$ die obige Gleichung (1) auf:

$$\begin{aligned}
\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} &= \left(\frac{h}{p}\right) i^{1/4(p-1)^2} \sqrt{p} \\
\Sigma \left(\frac{s'}{p'}\right) e^{s'\frac{2h\pi i}{p'}} &= \left(\frac{h}{p'}\right) i^{1/4(p'-1)^2} \sqrt{p'} \\
\Sigma \left(\frac{s''}{p''}\right) e^{s''\frac{2h\pi i}{p''}} &= \left(\frac{h}{p''}\right) i^{1/4(p''-1)^2} \sqrt{p''} \\
&\cdots\cdots\cdots\cdots
\end{aligned}$$

und setzen wir zur Abkürzung

$$sQ + s'Q' + s''Q'' + \cdots = m,$$

so ergiebt, da auch nach der neuen Erweiterung des Legendre'schen Symbols stets

$$\left(\frac{h}{p}\right)\left(\frac{h}{p'}\right)\left(\frac{h}{p''}\right)\cdots = \left(\frac{h}{P}\right)$$

ist, die Multiplication aller dieser Gleichungen folgendes Resultat

$$\begin{aligned}
&\Sigma \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\cdots e^{m\frac{2h\pi i}{P}} \\
&= \left(\frac{h}{p}\right) i^{1/4(p-1)^2 + 1/4(p'-1)^2 + 1/4(p''-1)^2 + \cdots} \sqrt{P},
\end{aligned} \tag{2}$$

wo $\sqrt{P}$ wieder positiv zu nehmen ist, und das Summenzeichen linker Hand sich auf alle $pp'p'' \dots = P$ Combinationen aller Werthe von $s, s', s'' \dots$ bezieht. Zunächst leuchtet nun ein, dass je zwei verschiedenen dieser Combinationen auch zwei nach dem Modulus P incongruente Werthe von m entsprechen; denn aus

$$sQ + s'Q' + s''Q'' + \cdots \equiv tQ + t'Q' + t''Q'' + \cdots \pmod{P}$$

würde, da Q', Q'' ... sämmtlich $\equiv 0 \pmod{p}$ sind, folgen, dass

$$sQ \equiv tQ \pmod{p},$$

und, da Q relative Primzahl zu p ist, auch

$$s \equiv t \pmod{p}$$

wäre; ähnlich würde aus derselben Annahme gleichzeitig

$$s' \equiv t' \pmod{p'}; \quad s'' \equiv t'' \pmod{p''} \ldots$$

folgen, so dass also die beiden Combinationen s, s', s'' ... und t, t', t'' ... identisch wären. In der That durchläuft also m ein vollständiges Restsystem in Bezug auf den Modulus P. Ferner ist nun

$$\left(\frac{m}{p}\right) = \left(\frac{sQ + s'Q' + s''Q'' + \cdots}{p}\right) = \left(\frac{sQ}{p}\right) = \left(\frac{s}{p}\right)\left(\frac{Q}{p}\right),$$

und ebenso

$$\left(\frac{m}{p'}\right) = \left(\frac{s'}{p'}\right)\left(\frac{Q'}{p'}\right), \quad \left(\frac{m}{p''}\right) = \left(\frac{s''}{p''}\right)\left(\frac{Q''}{p''}\right)\cdots,$$

folglich auch, wenn man alle diese Gleichungen multiplicirt,

$$\left(\frac{m}{P}\right) = \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\cdots\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots$$

Multiplicirt man daher beide Seiten der obigen Gleichung (2) mit

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots,$$

so erhält man

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots\left(\frac{h'}{P}\right)i^{\Sigma\frac{1}{4}(p-1)^2}\sqrt{P},$$

wo rechts zur Abkürzung

$$\left(\frac{p-1}{2}\right)^2 + \left(\frac{p'-1}{2}\right)^2 + \left(\frac{p''-1}{2}\right)^2 + \cdots = \Sigma\left(\frac{p-1}{2}\right)^2$$

gesetzt ist. Da nun ferner

$$\left(\frac{Q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right)\cdots$$
$$\left(\frac{Q'}{p'}\right) = \left(\frac{p}{p'}\right)\left(\frac{p''}{p'}\right)\cdots$$
$$\left(\frac{Q''}{p''}\right) = \left(\frac{p}{p''}\right)\left(\frac{p'}{p''}\right)\cdots$$
$$\cdots\cdots\cdots\cdots\cdots$$

ist, so erhält man durch Multiplication

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = \Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

wo das Productzeichen Π sich auf alle möglichen Paare von je zwei verschiedenen Primzahlen p, p' bezieht. Da nun nach dem Reciprocitätssatze

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

ist, so erhält man

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = i^{2\Sigma\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)},$$

wo das Summenzeichen rechter Hand sich wieder auf alle Combinationen von je zwei verschiedenen Primzahlen p, p' bezieht; es ist ferner

$$\Sigma\left(\frac{p-1}{2}\right)^2 + 2\,\Sigma\frac{p-1}{2}\frac{p'-1}{2}$$
$$= \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots\right)^2,$$

folglich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)+\cdots]^2}\sqrt{P}.$$

Da endlich (vergl. §. 46)

$$P = (1+(p-1))(1+(p'-1))(1+(p''-1))\cdots$$
$$\equiv 1+(p-1)+(p'-1)+(p''-1)+\cdots \pmod 4$$

und folglich

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots \pmod 2$$

und hieraus

$$\left(\frac{P-1}{2}\right)^2 \equiv \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2}\cdots\right)^2 \pmod 4$$

ist, so ergiebt sich schliesslich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

worin der zu beweisende Satz besteht. Nimmt man $h \equiv 0 \pmod P$, so erhält man wieder den (in §. 52. I. bewiesenen) Satz

$$\Sigma\left(\frac{m}{P}\right) = 0.$$