NIEDERSÄCHSISCHE STAATS- UND
UNIVERSITÄTSBIBLIOTHEK GÖTTINGEN

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_0146
LOG Titel: VI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.
LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

VI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.

§. 132.

Der allgemeine Beweis dieses Satzes*) stützt sich auf die Betrachtung einer Classe von unendlichen Reihen von der Form

$$L = \Sigma\, \psi(n),$$

wo der Buchstabe n alle ganzen positiven Zahlen durchlaufen muss, und die reelle oder complexe Function $\psi(n)$ der Bedingung

$$\psi(n)\,\psi(n') = \psi(nn')$$

genügt. Hieraus folgt für $n = n' = 1$, dass $\psi(1) = 1$ oder $= 0$ ist; da aber im letztern Fall $\psi(n) = \psi(1)\,\psi(n)$ für alle Werthe von n verschwinden würde, so nehmen wir immer an, dass $\psi(1) = 1$ ist. Wir nehmen ferner an, die Function $\psi(n)$ sei so beschaffen, dass die Summe der analytischen Moduln aller Werthe $\psi(n)$ *endlich* ist, woraus folgt, dass die Reihe L einen von der Anordnung ihrer Glieder unabhängingen endlichen Werth besitzt. Man überzeugt sich dann leicht von der Richtigkeit der folgenden Gleichung

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma\, \psi(n), \tag{I}$$

*) *Dirichlet:* Abhandlungen der Berliner Akademie aus dem Jahre 1837.

wo das Productzeichen sich auf alle, in beliebiger Ordnung auf einander folgenden, Primzahlen q bezieht*).

Zunächst leuchtet ein, da die Reihe L die Glieder

$$\psi(1) = 1, \quad \psi(q) = z, \quad \psi(q^2) = z^2 \ldots$$

enthält, und die Summe derselben für sich einen endlichen Werth hat, dass der Modulus von $\psi(q) < 1$, und folglich

$$\frac{1}{1 - \psi(q)} = 1 + \psi(q) + \psi(q^2) + \cdots$$

ist. Sind ferner $q_1, q_2, q_3 \ldots$ die sämmtlichen Primzahlen q, wie sie in dem Producte linker Hand aufeinander folgen, so wird das Product Q der ersten m Factoren

$$\frac{1}{1 - \psi(q_1)}, \ \frac{1}{1 - \psi(q_2)} \cdots \frac{1}{1 - \psi(q_m)},$$

wenn man jeden derselben nach der vorstehenden Gleichung in eine unendliche Reihe entwickelt und die Multiplication ausführt, gleich $\Sigma\psi(l)$, wo die Summation über alle die ganzen positiven Zahlen l auszudehnen ist, in welchen keine andern als die Primzahlen $q_1, q_2 \ldots q_m$ aufgehen. Ist daher h irgend eine positive ganze Zahl, und nimmt man m so gross, dass unter den Primzahlen $q_1, q_2 \ldots q_m$ sich alle diejenigen finden, welche $< h$ sind, so enthält $\Sigma\psi(l)$ alle Glieder der Reihe $\Sigma\psi(n)$, in welchen $n < h$ ist, und ausserdem noch unendlich viele andere, in denen $n > h$ ist. Mithin unterscheidet sich das Product Q von der Summe $\Sigma\psi(n)$ um eine Summe von der Form $\Sigma\psi(n')$, in welche aber nur noch Zahlen n' eingehen, welche $\geqq h$ sind. Da nun die Summe der Moduln aller Glieder $\psi(n)$ endlich ist, so kann man h, und also auch m so gross wählen, dass die Summe der Moduln aller Glieder $\psi(n')$, und folglich auch der Modul der Differenz $Q - \Sigma\psi(n)$ kleiner wird als jede vorher gegebene Grösse; d. h. mit unbegrenzt wachsendem m nähert sich Q dem Grenzwerth $\Sigma\psi(n)$, was zu beweisen war.

Ausser diesen Reihen von der Form $L = \Sigma\psi(n)$ haben wir noch diejenigen Reihen zu betrachten, welche durch die Entwick-

---

*) Unter dieser Classe von Reihen sind auch diejenigen enthalten, welche im fünften Abschnitt betrachtet sind. Vergl. §§. 124, 135. Der Werth einer solchen Function ψ ist offenbar für alle Zahlen vollständig bestimmt, sobald er für alle Primzahlen willkürlich angenommen ist. Die ältesten Untersuchungen über solche Reihen und Producte finden sich bei *Euler: Introductio in analysin infinitorum.* Cap. XV.

lung ihrer natürlichen Logarithmen entstehen. Wenn der Modulus von z ein echter Bruch ist, so ist bekanntlich

$$z + \tfrac{1}{2} z^2 + \tfrac{1}{3} z^3 + \tfrac{1}{4} z^4 + \cdots = \log \frac{1}{1-z},$$

und zwar ist der imaginäre Bestandtheil des Logarithmen rechter Hand stets zwischen den Grenzen $-\frac{1}{2}\pi i$ und $+\frac{1}{2}\pi i$ zu nehmen. Setzt man hierin $z = \psi(q)$ und für q alle Primzahlen, so erhält man zufolge der Gleichheit (I)

$$\Sigma\, \psi(q) + \tfrac{1}{2} \Sigma\, \psi(q^2) + \tfrac{1}{3} \Sigma\, \psi(q^3) + \cdots = \log L, \tag{II}$$

und offenbar hat die aus unendlich vielen unendlichen Reihen bestehende linke Seite einen von der Anordnung der Summationen unabhängigen endlichen Werth, weil selbst die Summe der Moduln aller ihrer Glieder einen endlichen Werth besitzt. Der imaginäre Theil des Logarithmen rechter Hand ist die Summe aller imaginären Theile der Logarithmen der einzelnen Factoren, aus denen das obige unendliche Product besteht.

Wir fügen zu diesem Resultat noch einige Bemerkungen hinzu. Ist zunächst $\psi(n)$ eine reelle Function, so sind alle Factoren des unendlichen Productes positiv, also ist $\log L$ reell, und da die Reihe $\log L$ einen endlichen Werth hat, so ist L ein positiver von Null verschiedener Werth. Ist aber $\psi(n)$ imaginär, und $\psi'(n)$ der jedesmal mit $\psi(n)$ conjugirte complexe Werth, so ist auch $\psi'(n)\, \psi'(n') = \psi'(nn')$, und die über alle ganzen positiven Zahlen n ausgedehnte Summe $L' = \Sigma\, \psi'(n)$ ist die mit $L = \Sigma\, \psi(n)$ conjugirte Zahl. Zugleich wird

$$\Sigma\, \psi'(q) + \tfrac{1}{2} \Sigma\, \psi'(q^2) + \tfrac{1}{3} \Sigma\, \psi'(q^3) + \cdots = \log L',$$

und zwar ist $\log L'$ conjugirt mit $\log L$, so dass die Summe $\log L + \log L' = \log(LL')$ reell wird.

Ist endlich der Werth der Function ψ für alle in einer bestimmten Zahl k aufgehenden Primzahlen $= 0$, so ist $\psi(n)$ jedesmal $= 0$, wenn n keine relative Primzahl zu k ist, und die Gleichungen (I) und (II) bleiben richtig, wenn man n alle relativen Primzahlen zu k, und q alle in k nicht aufgehenden Primzahlen durchlaufen lässt.

§. 133.

Es sei nun (wie in §. 131) k eine beliebige positive ganze Zahl, und zwar

$$k = 2^\lambda p^\pi p'^{\pi'} \ldots,$$

wo $p, p' \ldots$ von einander verschiedene ungerade Primzahlen bedeuten; wir geben ferner den Buchstaben

$$a, \ b, \ c, \ c' \ldots$$

ihre frühere Bedeutung (§. 131) und bezeichnen entsprechend mit

$$\theta, \ \eta, \ \omega, \ \omega' \ldots$$

irgend welche Wurzeln der Gleichungen

$$\theta^a = 1, \ \eta^b = 1, \ \omega^c = 1, \ \omega'^{c'} = 1 \ldots$$

Ist nun n irgend eine positive ganze Zahl und zugleich relative Primzahl zu k, und sind ihre Indices

$$\alpha \,(\text{mod. } a), \ \beta \,(\text{mod. } b), \ \gamma \,(\text{mod. } c), \ \gamma' \,(\text{mod. } c') \ldots,$$

so genügt, wie man leicht sieht, der Ausdruck

$$\psi(n) = \frac{\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots}{n^s}$$

der Bedingung $\psi(n)\psi(n') = \psi(nn')$ *); wenn ferner der Exponent $s > 1$ ist, was wir im Folgenden annehmen wollen, so ist die Summe der Moduln n^{-s} aller Glieder $\psi(n)$ endlich (§. 117), und folglich gelten die Gleichungen (I) und (II) des vorigen Paragraphen

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma \, \psi(n) = L$$

$$\Sigma \, \psi(q) + \tfrac{1}{2} \Sigma \, \psi(q^2) + \tfrac{1}{3} \Sigma \, \psi(q^3) + \cdots = \log L$$

in welchen q alle in k nicht aufgehenden Primzahlen, n alle relativen Primzahlen zu k durchlaufen muss; beide Reihen haben, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder un-

---

*) Der Zähler $\chi(n) = \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots$ besitzt die charakteristischen Eigenschaften $\chi(n)\chi(n') = \chi(nn')$ und, wenn $n' \equiv n''$ (mod. k) ist, $\chi(n') = \chi(n'')$. Umgekehrt, wenn eine Function $\chi(n)$ die erste Eigenschaft hat, und wenn sie ausserdem nur eine *endliche* Anzahl m (von Null verschiedener) Werthe $\omega_1, \omega_2 \ldots \omega_m$ besitzt, so sind diese letzteren nothwendig die sämmtlichen Wurzeln der Gleichung $\omega^m = 1$.

abhängige Summen. Wir können hinzufügen, dass beide Reihen auch *stetige* Functionen von s sind, so lange $s > 1$ ist; wir beweisen diese Behauptung für alle Werthe von s, welche grösser als ein beliebiger unechter Bruch σ sind, weil hieraus offenbar die Stetigkeit dieser Reihen für alle Werthe von $s > 1$ (excl. 1) folgt.

Jede der beiden Reihen L und $\log L$ ist von der Form

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots,$$

wo die Moduln der Coefficienten $\alpha_1, \alpha_2, \alpha_3 \ldots$ sämmtlich eine endliche Grösse $A (= 1)$ nicht übertreffen. Um die Stetigkeit einer Function von s innerhalb eines gewissen Intervalls ($s \geqq \sigma$) zu beweisen, genügt es darzuthun, dass, wie klein auch eine positive gegebene Grösse δ sein mag, die Function jedesmal in einen ersten und zwar stetigen, und in einen zweiten Bestandtheil zerlegt werden kann, dessen Modulus innerhalb des ganzen Intervalls ($s \geqq \sigma$) $< \delta$ ist; denn hieraus folgt, dass der Modulus einer plötzlichen Werthänderung der ganzen Function, die doch nur von dem zweiten Bestandtheil herrühren kann, kleiner als 2δ, und folglich, da die gegebene Grösse δ beliebig klein sein darf, nothwendig $= 0$ sein muss (vergl. §§. 101, 143). In unserm Falle ergiebt sich die Möglichkeit einer solchen Zerlegung auf folgende Weise; ist n eine beliebige ganze Zahl, so ist die Summe der ersten n Glieder

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \cdots + \frac{\alpha_n}{n^s}$$

eine stetige Function; der Modulus der Summe aller folgenden Glieder ist kleiner als

$$A\left(\frac{1}{(n+1)^s} + \frac{1}{(n+2)^s} + \cdots\right)$$

und folglich für *alle* Werthe $s \geqq \sigma$ auch kleiner als

$$A\left(\frac{1}{(n+1)^\sigma} + \frac{1}{(n+2)^\sigma} + \cdots\right);$$

da nun σ ein unechter Bruch ist, und folglich (nach §. 117) die Reihe

$$\frac{1}{1^\sigma} + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \cdots$$

convergirt, so kann für jede gegebene Grösse δ entsprechend n so gross gewählt werden, dass

$$A\left(\frac{1}{(n+1)^\sigma}+\frac{1}{(n+2)^\sigma}+\cdots\right)<\delta$$

wird; hiermit ist für jede gegebene Grösse δ die Möglichkeit einer Zerlegung unserer Reihe in zwei Bestandtheile von der obigen Art, und also auch die Stetigkeit der Reihen L und $\log L$ für jeden Werth $s > 1$ nachgewiesen.

Der Beweis des Satzes über die arithmetische Progression gründet sich nun auf die Untersuchung des Verhaltens der Reihen L und $\log L$ bei unbegrenzter Annäherung des Exponenten s an den Werth 1. Wir bemerken zunächst, dass diese Reihen je nach der Wahl der in dem Ausdrucke $\psi(n)$ vorkommenden Einheits-Wurzeln $\theta, \eta, \omega, \omega' \ldots$ ein ganz verschiedenes Verhalten zeigen; da diese Wurzeln resp. $a, b, c, c' \ldots$ verschiedene Werthe haben können, so sind in der Form L im Ganzen

$$a\,b\,c\,c' \ldots = \varphi(k)$$

verschiedene besondere Reihen enthalten; wir theilen diese Reihen L in drei Classen ein:

In die *erste* Classe nehmen wir nur eine einzige Reihe L_1 auf, und zwar diejenige, in welcher alle Einheits-Wurzeln $\theta, \eta, \omega, \omega' \ldots$ den Werth $+1$ haben.

In die *zweite* Classe nehmen wir alle übrigen Reihen L_2 auf, in welchen alle Einheits-Wurzeln reelle Werthe, also die Werthe ± 1 haben.

In die *dritte* Classe nehmen wir alle übrigen Reihen L_3 auf, d. h. alle diejenigen, in welchen wenigstens eine der Einheits-Wurzeln imaginär ist. Die Anzahl dieser Reihen ist jedenfalls gerade, und sie sind paarweise mit einander conjugirt; denn entspricht eine solche Reihe L_3 den Wurzeln $\theta, \eta, \omega, \omega' \ldots$, so entspricht immer eine zweite solche Reihe L'_3 den Wurzeln θ^{-1}, $\eta^{-1}, \omega^{-1}, \omega'^{-1} \ldots$, und diese beiden Systeme von Wurzeln sind nicht identisch.

Wir wollen nun das Verhalten aller dieser Reihen genau untersuchen, wenn der Exponent $s = 1 + \varrho$ sich dem Werthe 1 nähert, d. h. also, wenn die positive Grösse ϱ unendlich klein wird.

§. 134.

Betrachten wir zunächst das Verhalten der ersten Reihe

$$L_1 = \Sigma \frac{1}{n^s} = \Sigma \frac{1}{n^{1+\varrho}},$$

in welcher n alle relativen Primzahlen zu k durchlaufen muss, so leuchtet ein, dass dieselbe als ein Aggregat von $\varphi(k)$ Partialreihen von der Form

$$\frac{1}{\nu^{1+\varrho}} + \frac{1}{(\nu+k)^{1+\varrho}} + \frac{1}{(\nu+2k)^{1+\varrho}} + \cdots$$

angesehen werden kann, wo ν relative Primzahl zu k und $\leqq k$ ist. Da nun (nach §. 117) das Product aus einer solchen Reihe und aus ϱ mit unendlich abnehmendem ϱ sich einem endlichen positiven, von Null verschiedenen Grenzwerth k^{-1} nähert, so können wir

$$L_1 = \frac{l}{\varrho}$$

setzen, wo l mit unendlich abnehmendem ϱ sich ebenfalls einem endlichen, positiven, von Null verschiedenen Grenzwerth nähert.

Ganz anders verhalten sich aber die Reihen L der zweiten und dritten Classe; wir haben gesehen, dass alle diese Reihen, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder unabhängige Werthe besitzen; von jetzt an wollen wir aber ihre Glieder $\psi(n)$ so anordnen, dass die Zahlen n ihrer Grösse nach wachsend auf einander folgen; die so geordneten Reihen L der zweiten und dritten Classe *convergiren* dann für *alle positiven* Werthe von s und sind nebst ihren Derivirten auch *stetige* Functionen des positiven Exponenten s.

Um dies nachzuweisen, betrachten wir zunächst die ganze rationale Function

$$f(x) = \Sigma\, \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots x^\nu$$

der Variabeln x, wo das Summenzeichen sich auf diejenigen $\varphi(k)$ positiven ganzen Zahlen ν bezieht, die relative Primzahlen zu k und $< k$ sind, und wo $\alpha, \beta, \gamma, \gamma' \ldots$ die Indices der Zahl ν bedeuten. Setzt man $x = 1$, so erhält man

$$f(1) = \Sigma\, \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots,$$

wo die Indices α, β, γ, γ' ... unabhängig von einander vollständige Restsysteme resp. in Bezug auf die Moduln a, b, c, c' ... durchlaufen müssen; es ist daher

$$f(1) = \Sigma\, \theta^\alpha . \Sigma\, \eta^\beta . \Sigma\, \omega^\gamma . \Sigma\, \omega'^{\gamma'} \ldots$$

Da nun nach unserer Voraussetzung die Reihe L eine Reihe der zweiten oder dritten Classe und folglich mindestens eine der Einheitswurzeln θ, η, ω, ω' ... *nicht* $= +1$ ist, so ist auch mindestens eine der Summen

$$\Sigma\, \theta^\alpha,\quad \Sigma\, \eta^\beta,\quad \Sigma\, \omega^\gamma,\quad \Sigma\, \omega'^{\gamma'} \ldots$$

gleich Null, und hieraus folgt

$$f(1) = 0.$$

Mit Hülfe dieses Resultates kann man nun die oben behaupteten Eigenschaften der Reihen L auf verschiedene Arten nachweisen. Die eine besteht darin, dass man die Reihe L in ein bestimmtes Integral verwandelt. Nach der von *Legendre* eingeführten Bezeichnung ist

$$\Gamma(s) = \int_0^1 \left(\log \frac{1}{x}\right)^{s-1} dx$$

eine für alle positiven Werthe von s endliche und stetige Function von s; bedeutet ferner n irgend einen positiven Werth, und ersetzt man x durch x^n, so ergiebt sich

$$\frac{\Gamma(s)}{n^s} = \int_0^1 x^{n-1} \left(\log \frac{1}{x}\right)^{s-1} dx;$$

und hieraus folgt leicht (ähnlich wie in den §§. 103, 105), dass die Summe der *ersten* $m\varphi(k)$ Glieder der Reihe L gleich

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x}\, \frac{f(x)}{1-x^k} \left(\log \frac{1}{x}\right)^{s-1} (1 - x^{mk})\, dx$$

ist. Da nun $f(x)$ eine durch x theilbare ganze Function von x ist, welche für $x = 1$ verschwindet, so bleibt innerhalb des ganzen Integrationsgebietes der Modulus der Function

$$\frac{1}{x}\, \frac{f(x)}{1-x^k}$$

unterhalb einer angebbaren endlichen Grösse, und hieraus folgt leicht, wenn man m unendlich wachsen lässt, dass

$$L = \frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} \left(\log \frac{1}{x}\right)^{s-1} dx$$

ist. Es zeigt sich also in der That, dass die unendliche Reihe L der zweiten oder dritten Classe, wenn ihre Glieder in der angegebenen Weise geordnet sind, für jeden positiven Werth von s *convergirt*; beachtet man ferner, dass $\Gamma(s)$ für alle positiven Werthe von s ebenfalls positiv und von Null verschieden, sowie, dass die Derivirte von $\Gamma(s)$ eine stetige Function von s ist, so folgt aus dem vorstehenden geschlossenen Ausdruck für die Reihe L, dass dieselbe nebst ihrer Derivirten eine *stetige* Function von s ist, so lange s positiv bleibt.

Zu demselben Resultate gelangt man aber auch auf anderm Wege, nämlich mit Hülfe des weiter unten in §. 143 bewiesenen allgemeinen Satzes. Denn da zufolge der Gleichung $f(1) = 0$ die Summe der Coefficienten

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots$$

von je $\varphi(k)$ auf einander folgenden Gliedern der Reihe L den Werth Null hat, so bildet die Reihe L eine solche unendliche Reihe, wie sie in §. 143 betrachtet wird; man braucht dort nur unter $k_1, k_2, k_3 \ldots$ die Werthe der successiven Zahlen n zu verstehen, so ergeben sich unmittelbar unsere obigen Behauptungen über die Convergenz und Stetigkeit der Reihe L und ihrer Derivirten.

Aus diesem Resultat ergiebt sich nun, dass jede Reihe L der zweiten oder dritten Classe, wenn der Exponent $s = 1 + \varrho$ abnehmend dem Werth 1 unendlich nahe kommt, sich einem völlig bestimmten *endlichen* Grenzwerth, nämlich dem Werth

$$\int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} dx$$

nähert, welchen die Reihe L bei der oben angegebenen Anordnung ihrer Glieder für $s = 1$ annimmt.

§. 135.

Es hat nun zwar gar keine Schwierigkeit, den Werth des vorstehenden Integrals mit Hülfe von Logarithmen und Kreisfunctionen darzustellen*); dass aber dieser endliche Grenzwerth einer Reihe L der zweiten oder dritten Classe *von Null verschieden* ist — und gerade hierin besteht der Hauptpunct der ganzen nachfolgenden Untersuchung — würde sich aus diesem Ausdrucke schwer oder gar nicht erkennen lassen. Es ist nun von dem höchsten Interesse, dass dieser Nachweis für die Reihen L_2 der zweiten Classe sich mit Hülfe der Untersuchungen des fünften Abschnitts über die Classenanzahl der quadratischen Formen führen lässt; ja wir können hinzufügen, dass historisch jene Untersuchungen ihren Ausgangspunct an dieser Stelle genommen haben.

Wir betrachten eine bestimmte Reihe L_2 der zweiten Classe, welche den Wurzeln

$$\theta = \pm 1, \quad \eta = \pm 1, \quad \omega = \pm 1, \quad \omega' = \pm 1 \ldots$$

entspricht; es sei P das Product aller der in k aufgehenden ungeraden Primzahlen p, denen eine negative Wurzel $\omega = -1$ entspricht, und S das Product der übrigen in k aufgehenden ungeraden Primzahlen (falls in der einen oder andern dieser beiden Gruppen gar keine Primzahl enthalten sein sollte, ist P oder $S = 1$ zu setzen); da nun eine Zahl n quadratischer Rest oder Nichtrest einer Primzahl ist, je nachdem ihr Index γ gerade oder ungerade ist (§. 129), so leuchtet ein, dass

$$\omega^\gamma \omega'^{\gamma'} \ldots = \left(\frac{n}{P}\right)$$

ist; wenn ferner $\theta = -1$, also $a = 2$, und $k \equiv 0 \pmod{4}$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\theta^\alpha = (-1)^\alpha = (-1)^{\frac{1}{2}(n-1)};$$

*) Bei der wirklichen Ausführung der Rechnung durch Zerlegung in Partialbrüche (ähnlich wie in den §§. 103, 105) würde man auf die in der Theorie der Kreistheilung vorkommenden Summen $f(r)$ stossen, wo r irgend eine Wurzel der Gleichung $r^k = 1$ bedeutet.

ebenso, wenn $\eta = -1$, also $b > 1$, und $k \equiv 0 \pmod{8}$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\eta^\beta = (-1)^\beta = (-1)^{1/8(n^2-1)}.$$

Diese Bemerkungen veranlassen uns (vergl. §§. 101, 123), je nach den vier verschiedenen Zeichencombinationen θ, η vier verschiedene Determinanten D zu betrachten; wir setzen nämlich, mit gehöriger Rücksicht auf das Zeichen ± 1:

$$\begin{array}{llll}
D = \pm\ PS^2 \equiv 1 \pmod{4}, & \text{wenn} & \theta = +1, & \eta = +1 \\
D = \pm\ PS^2 \equiv 3 \pmod{4}, & \text{wenn} & \theta = -1, & \eta = +1 \\
D = \pm 2PS^2 \equiv 2 \pmod{8}, & \text{wenn} & \theta = +1, & \eta = -1 \\
D = \pm 2PS^2 \equiv 6 \pmod{8}, & \text{wenn} & \theta = -1, & \eta = -1.
\end{array}$$

Nun sind alle ungeraden Zahlen n auch relative Primzahlen zu $2D$, und umgekehrt, alle relativen Primzahlen zu $2D$ sind auch ungerade Zahlen n, und gleichzeitig ist

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots = \theta^{1/2(n-1)} \eta^{1/8(n^2-1)} \left(\frac{n}{P}\right) = \left(\frac{D}{n}\right);$$

ist daher k gerade, so stimmen die sämmtlichen Zahlen n mit den sämmtlichen relativen Primzahlen zu $2D$ überein, und es ist

$$L_2 = \Sigma\, \psi(n) = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s};$$

ist aber k ungerade, so sind unter den Zahlen n auch gerade Zahlen; da in diesem Falle aber nothwendig $\theta = +1$, $\eta = +1$, also $D \equiv 1 \pmod{4}$ ist, so ist (vergl. §. 102)

$$L_2 = \Sigma \left(\frac{n}{P}\right) \frac{1}{n^s} = \frac{1}{1 - \left(\frac{2}{P}\right) \frac{1}{2^s}} \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo in der letzten Summe rechter Hand der Buchstabe n nur noch alle ungeraden relativen Primzahlen zu k, d. h. alle relativen Primzahlen zu $2D$ zu durchlaufen hat.

Um daher zu beweisen, dass die Reihe L_2 sich einem von Null verschiedenen Grenzwerth nähert, braucht man dasselbe nur von der Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

nachzuweisen. Nun leuchtet ein, dass die Zahl D nie eine *Quadratzahl* sein kann; denn da eine Quadratzahl niemals $\equiv 3 \pmod{4}$, oder $\equiv 2 \pmod{8}$ oder $\equiv 6 \pmod{8}$ ist, so bleibt nur die einzige Möglichkeit $D \equiv 1 \pmod{4}$; da aber in diesem Falle $\theta = +1$, $\eta = +1$ ist, so muss, da L_2 eine Reihe der zweiten Classe ist, wenigstens eine der Wurzeln $\omega, \omega' \ldots = -1$ sein, und folglich P mindestens durch eine ungerade Primzahl p theilbar, also nicht $= 1$ sein; mithin ist D in keinem Falle eine Quadratzahl. Wir haben nun (in §§. 96 und 98) gesehen, dass die Anzahl h der Classen nicht äquivalenter ursprünglicher Formen von der (nicht quadratischen) Determinante D ein Product aus mehreren Factoren ist, von denen der eine der Grenzwerth der obigen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

ist; da nun immer mindestens eine Form $(1, 0, -D)$ existirt, also h niemals $= 0$ ist, und da ferner die übrigen in dem Ausdruck von h vorkommenden Factoren nicht unendlich gross sind, so ist auch dieser Grenzwerth von Null verschieden. Und hieraus folgt, dass auch der Grenzwerth einer jeden Reihe L_2 der zweiten Classe ein von Null verschiedener und folglich positiver Werth ist, was zu beweisen war.

In dem einfachsten Falle, wo k eine Potenz einer ungeraden Primzahl p oder das Doppelte einer solchen Potenz ist, existirt nur eine Reihe

$$L_2 = \Sigma \left(\frac{n}{p}\right) \frac{1}{n^s}$$

der zweiten Classe; in diesem Falle bedarf es nicht der Zuziehung der Theorie der quadratischen Formen, um nachzuweisen, dass der Grenzwerth

$$\Sigma \left(\frac{n}{p}\right) \frac{1}{n}$$

dieser Reihe von Null verschieden ist; für diese Summe haben wir nämlich in §. 103 einen Ausdruck gefunden, welcher neben solchen Factoren, die offenbar von Null verschieden sind, noch den Factor

$$\Sigma \left(\frac{m}{p}\right) m \quad \text{oder} \quad \Sigma \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p}$$

enthält, je nachdem $p \equiv 3$ oder $\equiv 1 \pmod{4}$ ist, und wo m alle Zahlen $1, 2, 3 \ldots (p-1)$ durchlaufen muss. Im ersten Fall ist aber Σm und folglich auch

$$\sum \left(\frac{m}{p}\right) m$$

ungerade, also von Null verschieden; im zweiten Fall ist (§. 107)

$$-\sum \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p} = \log \frac{y + z\sqrt{p}}{y - z\sqrt{p}},$$

wo die ganzen Zahlen y, z der Gleichung $y^2 - pz^2 = 4p$ genügen; es kann folglich z, und also auch der vorstehende Ausdruck nicht $= 0$ sein.

§. 136.

Um nun dasselbe auch für jede Reihe L_3 der dritten Classe zu beweisen, addiren wir alle $\varphi(k)$ Gleichungen von der Form

$$\sum \psi(q) + \tfrac{1}{2} \sum \psi(q^2) + \tfrac{1}{3} \sum \psi(q^3) + \cdots = \log L,$$

welche den verschiedenen Wurzel-Systemen θ, η, ω, ω' ... entsprechen. Bedeutet q irgend eine in k nicht aufgehende Primzahl, und μ irgend eine positive ganze Zahl, so liefert die linke Seite einer jeden solchen Gleichung ein Glied

$$\frac{1}{\mu} \psi(q^\mu),$$

in welchem

$$\frac{1}{\mu} \frac{1}{q^{\mu s}}$$

mit dem Coefficienten

$$\theta^{\alpha\mu} \eta^{\beta\mu} \omega^{\gamma\mu} \omega'^{\gamma'\mu} \ldots$$

behaftet ist, wo α, β, γ, γ' ... die Indices von q bedeuten. Die Summe aller dieser den verschiedenen Wurzelsystemen θ, η, ω, ω' ... entsprechenden Coefficienten wird daher gleich dem Product

$$\sum \theta^{\alpha\mu} \sum \eta^{\beta\mu} \sum \omega^{\gamma\mu} \sum \omega'^{\gamma'\mu} \ldots,$$

wo die Summenzeichen sich der Reihe nach auf die a, b, c, c' ... verschiedenen Werthe von θ, η, ω, ω' ... beziehen. Bekanntlich ist nun die Summe aller gleich hohen Potenzen der Wurzeln von einer Gleichung der Form $x^m = 1$ nur dann von Null verschieden, und zwar $= m$, wenn der Exponent dieser Potenzen durch m theilbar ist; mithin ist das vorstehende Product nur dann von Null verschieden, und zwar $= a\,b\,c\,c' \ldots = \varphi(k)$, wenn die Exponenten $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ resp. durch a, b, c, $c' \ldots$ theilbar sind; da nun $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ die Indices von q^μ sind, so wird dies nur dann und immer dann eintreten, wenn

$$q^\mu \equiv 1 \pmod{2^\lambda}, \quad q^\mu \equiv 1 \pmod{p^\pi}, \quad q^\mu \equiv 1 \pmod{p'^{\pi'}} \ldots,$$

d. h. also, wenn

$$q^\mu \equiv 1 \pmod{k}$$

ist. Mithin wird die Summe aller jener Gleichungen folgende Form annehmen

$$\varphi(k) \left\{ \Sigma \frac{1}{q^s} + \tfrac{1}{2} \Sigma \frac{1}{q^{2s}} + \cdots + \frac{1}{\mu} \Sigma \frac{1}{q^{\mu s}} + \cdots \right\}$$
$$= \log L_1 + \Sigma \log L_2 + \Sigma \log (L_3 L'_3),$$

wo auf der linken Seite das erste, zweite Summenzeichen u. s. f. sich auf alle die in k nicht aufgehenden Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv 1$, $q^2 \equiv 1 \pmod{k}$ u. s. f. Genüge leisten; auf der rechten Seite bezieht sich das erste Summenzeichen auf alle Reihen L_2 der zweiten Classe, das zweite auf alle verschiedenen Paare $L_3 L'_3$ conjugirter Reihen dritter Classe. Mit Hülfe dieser Gleichung sind wir im Stande zu beweisen, dass der endliche Grenzwerth, welchem sich irgend eine Reihe L_3 der dritten Classe nähert, von Null verschieden ist.

Dieser Beweis stützt sich auf das schon früher (§. 134) erhaltene Resultat, dass jede solche Reihe L_3 für alle positiven Werthe von s eine stetige Function von s ist, und dass dasselbe auch von ihrer Derivirten gilt. Wir können daher

$$L_3 = f(s) + iF(s)$$
$$L'_3 = f(s) - iF(s)$$

setzen, wo $f(s)$, $F(s)$ und die Derivirten $f'(s)$, $F'(s)$ stetige Functionen von s sind, so lange s positiv bleibt; da also der Grenzwerth von $L_3 = f(1) + iF(1)$ ist, so muss, falls derselbe $= 0$ ist, nothwendig $f(1) = 0$ und $F(1) = 0$ sein; hieraus folgt nach einem bekannten Satze der Differentialrechnung, dass für jeden Werth $s = 1 + \varrho$, welcher > 1 ist,

$$L_3 = \varrho\ \{f'(1+\delta\varrho) + iF'(1+\varepsilon\varrho)\}$$
$$L'_3 = \varrho\ \{f'(1+\delta\varrho) - iF'(1+\varepsilon\varrho)\}$$

sein wird, wo δ und ε zwischen den Grenzen 0 und 1 liegen; mithin wird

$$L_3 L'_3 = \varrho^2\ \{f'(1+\delta\varrho)^2 + F'(1+\varepsilon\varrho)^2\} = \varrho^2 R,$$

wo R (in Folge der Endlichkeit und Stetigkeit der Derivirten $f'(s)$, $F'(s)$) mit unendlich abnehmendem positiven ϱ sich einem endlichen (nicht negativen) Grenzwerth

$$f'(1)^2 + F'(1)^2$$

nähert. Hieraus folgt nun

$$\log(L_3 L'_3) = -2\log\frac{1}{\varrho} + \log R,$$

wo $\log R$ mit unendlich abnehmendem ϱ sich entweder einem endlichen Grenzwerth nähert oder negativ über alle Grenzen wächst, falls R unendlich klein wird.

Sind im Ganzen m solche Paare von Reihen dritter Classe vorhanden, welche gleichzeitig mit ϱ unendlich klein werden, so ist folglich

$$\Sigma \log(L_3 L'_3) = -2m\log\frac{1}{\varrho} + t,$$

wo t jedenfalls nicht positiv über alle Grenzen wachsen kann, sondern entweder endlich bleibt, oder negativ über alle Grenzen wächst; denn da jedes Product $L_3 L'_3$ sich einem endlichen nicht negativen Werth nähert, so kann auch kein Glied $\log(L_3 L'_3)$ positiv über alle Grenzen wachsen.

Da ferner schon gezeigt ist, dass der Grenzwerth einer jeden Reihe L_2 der zweiten Classe von Null verschieden ist, so nähert sich die Summe

$$\Sigma \log L_2$$

der (jedenfalls reellen) Reihen $\log L_2$ einem endlichen Grenzwerth.

Ausserdem ist schon bewiesen, dass das Product ϱL_1 sich einem endlichen von Null verschiedenen Werth nähert; mithin ist

$$\log L_1 = \log\frac{1}{\varrho} + t',$$

wo t' endlich bleibt; folglich ist die ganze rechte Seite der obigen Gleichung von der Form

$$-(2m-1)\log\frac{1}{\varrho}+T,$$

wo T mit unendlich abnehmendem ϱ jedenfalls nicht positiv über alle Grenzen wachsen kann. Existirte also mindestens eine Reihe L_3 dritter Classe, welche mit ϱ unendlich klein würde, d. h. wäre m mindestens $=1$, so würde die ganze rechte Seite unserer Gleichung mit unendlich abnehmendem positiven ϱ *negativ* unendlich wachsen. Dies ist aber unmöglich, da die linke Seite für alle Werthe von ϱ positiv bleibt. Mithin ist $m=0$, d. h. jede Reihe der dritten Classe nähert sich einem von Null verschiedenen Grenzwerth, was zu beweisen war.

Hieraus folgt endlich noch, dass auch jede der Reihen $\log L_3$ einen endlichen Grenzwerth haben muss, wenn man berücksichtigt, dass nach dem früher Bewiesenen (§. 133) jede solche Reihe sich stetig mit s ändert, so lange $s>1$ ist.

§. 137.

Das Resultat der vorhergehenden Untersuchungen besteht darin, dass bei dem unendlichen Abnehmen der positiven Grösse $\varrho=s-1$ die Reihe $\log L_1$ positiv über alle Grenzen wächst, während alle übrigen Reihen $\log L$ sich endlichen Grenzwerthen nähern. Mit Hülfe desselben sind wir im Stande, den Satz über die arithmetische Progression vollständig zu beweisen.

Es sei nämlich m irgend eine relative Primzahl zu k, so multipliciren wir jede der $\varphi(k)$ Reihen von der Form

$$\Sigma\,\psi(q)+\tfrac{1}{2}\,\Sigma\,\psi(q^2)+\tfrac{1}{3}\,\Sigma\,\psi(q^3)+\cdots=\log L,$$

welche einem bestimmten System von Einheits-Wurzeln θ, η, ω, ω' ... entspricht, mit dem correspondirenden Werth

$$\theta^{-\alpha_1}\,\eta^{-\beta_1}\,\omega^{-\gamma_1}\,\omega'^{-\gamma_1'}\ldots=\chi,$$

wo α_1, β_1, γ_1, γ_1' ... die Indices der Zahl m bedeuten, und addiren alle Producte; dann wird, wenn wieder α, β, γ, γ' ... die Indices einer bestimmten Primzahl q sind, das Glied

$$\frac{1}{\mu}\,\frac{1}{q^{\mu s}}$$

den Coefficienten

$$\sum \theta^{\alpha\mu-\alpha_1}\,\eta^{\beta\mu-\beta_1}\,\omega^{\gamma\mu-\gamma_1}\,\omega'^{\gamma'\mu-\gamma_1'}\ldots$$

erhalten, wo sich das Summenzeichen auf alle $\varphi(k)$ Wurzel-Systeme bezieht; dieser Coefficient ist daher auch gleich dem Product aus den einzelnen Summen

$$\sum \theta^{\alpha\mu-\alpha_1},\ \sum \eta^{\beta\mu-\beta_1},\ \sum \omega^{\gamma\mu-\gamma_1},\ \sum \omega'^{\gamma'\mu-\gamma_1'}\ldots,$$

in welchen die Buchstaben $\theta, \eta, \omega, \omega' \ldots$ resp. ihre $a, b, c, c' \ldots$ verschiedenen Werthe durchlaufen müssen; dieser Coefficient wird folglich nur dann von Null verschieden, und zwar $= a\,b\,c\,c' \ldots = \varphi(k)$ sein, wenn die Exponenten $\alpha\mu-\alpha_1$, $\beta\mu-\beta_1$, $\gamma\mu-\gamma_1$, $\gamma'\mu-\gamma_1' \ldots$ resp. durch $a, b, c, c' \ldots$ theilbar sind, d. h. wenn

$$q^\mu \equiv m \pmod{k}$$

ist. Die Summation aller Producte $\chi \log L$ giebt daher das Resultat

$$\varphi(k)\left\{\sum \frac{1}{q^s} + \tfrac{1}{2}\sum \frac{1}{q^{2s}} + \tfrac{1}{3}\sum \frac{1}{q^{3s}} + \cdots\right\}$$
$$= \sum \chi \log L,$$

wo auf der linken Seite das erste, zweite, dritte Summenzeichen u. s. f. sich auf alle Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv m$, $q^2 \equiv m$, $q^3 \equiv m \pmod{k}$ u. s. f. genügen, während das Summenzeichen auf der rechten Seite sich auf die sämmtlichen $\varphi(k)$ verschiedenen Wurzel-Systeme $\theta, \eta, \omega, \omega' \ldots$ bezieht. Bezeichnet man nun mit z alle positiven ganzen Zahlen mit Ausnahme von 1, so ist offenbar

$$\tfrac{1}{2}\sum \frac{1}{q^{2s}} + \tfrac{1}{3}\sum \frac{1}{q^{3s}} + \tfrac{1}{4}\sum \frac{1}{q^{4s}} + \cdots = Q$$

kleiner als

$$\tfrac{1}{2}\sum \frac{1}{z^2} + \tfrac{1}{2}\sum \frac{1}{z^3} + \tfrac{1}{2}\sum \frac{1}{z^4} + \cdots,$$

wo in jeder Summe z alle seine Werthe durchläuft; da nun, sobald $z \geqq 2$, immer

$$\frac{1}{z^3} \leqq \frac{1}{2}\,\frac{1}{z^2},\quad \frac{1}{z^4} \leqq \frac{1}{4}\,\frac{1}{z^2},\quad \frac{1}{z^5} \leqq \frac{1}{8}\,\frac{1}{z^2} \ldots$$

ist, so ergiebt sich

$$Q < \sum \frac{1}{z^2};$$

während daher s abnehmend sich dem Werthe 1 nähert, bleibt Q fortwährend unterhalb einer endlichen Grösse. Da ferner alle Glieder $\chi \log L$ sich endlichen Grenzwerthen nähern, mit Ausnahme des einzigen Gliedes $\log L_1$, welches über alle Grenzen wächst, so muss auch die Summe

$$\Sigma \frac{1}{q^s}$$

über alle Grenzen wachsen; dies wäre aber nicht möglich, wenn diese Summe aus einer endlichen Anzahl von Gliedern bestände, und folglich muss es unendlich viele Primzahlen q geben, welche $\equiv m$ (mod. k) sind; d. h. also:

Jede unbegrenzte arithmetische Progression $kx + m$, deren Anfangsglied m und Differenz k relative Primzahlen sind, enthält unendlich viele positive Primzahlen q *).

---

*) Ueber die Ausdehnung dieses Satzes auf Linearformen mit complexen Coefficienten, sowie auf quadratische Formen siehe *Dirichlet: Untersuchungen über die Theorie der complexen Zahlen*, Abhandlungen der Berliner Akademie aus dem Jahre 1841; Monatsbericht der Berliner Akademie (März 1840) oder Crelle's Journal XXI; Comptes rendus der Pariser Akademie 1849, T. X, p. 285.