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

Von

H^rn. LEJEUNE-DIRICHLET.

[Gelesen in der Akademie der Wissenschaften am 27. Juli 1837.]

Die aufmerksame Betrachtung der natürlichen Reihe der Primzahlen läfst an derselben eine Menge von Eigenschaften wahrnehmen, deren Allgemeinheit durch fortgesetzte Induction zu jedem beliebigen Grade von Wahrscheinlichkeit erhoben werden kann, während die Auffindung eines Beweises, der allen Anforderungen der Strenge genügen soll, mit den gröfsten Schwierigkeiten verbunden ist. Eines der merkwürdigsten Resultate dieser Art bietet sich dar, wenn man sämmtliche Glieder der Reihe durch dieselbe übrigens ganz beliebige Zahl dividirt. Nimmt man die Primzahlen aus, die im Divisor aufgehen und mithin unter den ersten Gliedern der Reihe vorkommen, so werden alle übrigen einen Rest lassen, welcher relative Primzahl zum Divisor ist, und das Resultat, welches sich bei fortgesetzter Division herausstellt, besteht darin, dafs jeder Rest der genannten Art unaufhörlich wiederkehrt, und zwar so, dafs das Verhältnifs der Zahlen, welche für irgend zwei solche Reste bezeichnen, wie oft sie bis zu einem gewissen Gliede erschienen sind, bei immer weiter fortgesetzter Division die Einheit zur Grenze hat. Abstrahirt man von der zunehmenden Gleichmäfsigkeit des Vorkommens der einzelnen Reste und beschränkt das Beobachtungsresultat auf die nie aufhörende Wiederkehr eines jeden derselben, so läfst sich dasselbe in dem Satze aussprechen: »dafs jede unbegrenzte arithmetische Reihe, deren »erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, un»endlich viele Primzahlen enthält.«

Für diesen einfachen Satz existirte bis jetzt kein genügender Beweis, wie sehr auch ein solcher wegen der zahlreichen Anwendungen zu wünschen war, welche von dem Satze gemacht werden können. Der einzige Mathematiker, welcher die Begründung dieses Theorems versucht hat, ist, so viel ich weifs, Legendre (1), für den diese Untersuchung aufser dem Reiz, welcher in der Schwierigkeit des Gegenstandes liegt, noch ein ganz besonderes Interesse durch den Umstand haben mufste, dafs er die erwähnte Eigenschaft der arithmetischen Progression bei früheren Arbeiten als Lemma benutzt hatte. Legendre macht den zu beweisenden Satz von der Aufgabe abhängig, die gröfste Anzahl auf einander folgender Glieder einer arithmetischen Reihe zu finden, welche durch gegebene Primzahlen theilbar sein können, löst aber diese Aufgabe nur durch Induction. Versucht man, die auf diese Weise von ihm gefundene, durch die Einfachheit der Form des Resultats höchst merkwürdige Auflösung der Maximumsaufgabe zu beweisen, so stöfst man auf grofse Schwierigkeiten, deren Überwindung mir nicht hat gelingen wollen. Erst nachdem ich den von Legendre eingeschlagenen Weg ganz verlassen hatte, bin ich auf einen völlig strengen Beweis des Theorems über die arithmetische Progression gekommen. Der von mir gefundene Beweis, welchen ich der Akademie in dieser Abhandlung vorzulegen die Ehre habe, ist nicht rein arithmetisch, sondern beruht zum Theil auf der Betrachtung stetig veränderlicher Gröfsen. Bei der Neuheit der dabei zur Anwendung kommenden Principien hat es mir zweckmäfsig geschienen, dem Beweise des Theorems in seiner ganzen Allgmeinheit die Behandlung des besonderen Falles voraus zu schicken, in welchem die Differenz der Progression eine ungerade Primzahl ist.

§. 1.

Es sei p eine ungerade Primzahl und c eine primitive Wurzel derselben, so dafs also die Reste der Potenzen

$$c^0,\ c^1,\ c^2,\ \ldots\ c^{p-2},$$

bei der Division durch p, wenn man von ihrer Ordnung absieht, mit den Zahlen $1, 2, 3, \ldots p-1$ zusammenfallen. Ist n eine nicht durch p theilbare

(1) *Théorie des Nombres. 4ième Partie.* §. IX.

Zahl, so werden wir mit Gaufs den Exponenten $\gamma < p-1$, welcher der Congruenz $c^\gamma \equiv n \pmod{p}$ genügt, den Index von n nennen, und falls es nöthig sein sollte, mit γ_n bezeichnen. Die Wahl der primitiven Wurzel c ist gleichgültig, nur soll angenommen werden, dafs man die einmal gewählte nicht ändere. In Bezug auf die eben definirten Indices gilt der leicht zu beweisende Satz, dafs der Index eines Productes der Summe der Indices der Factoren, um das darin enthaltene Vielfache von $p-1$ vermindert, gleich ist. Ferner bemerke man, dafs immer $\gamma_1 = 0$, $\gamma_{p-1} = \frac{p-1}{2}$, so wie dafs γ_n gerade oder ungerade sein wird, je nachdem n Quadratrest oder Nichtquadratrest von p ist, oder mit Anwendung des Legendreschen Zeichens, je nachdem $\left(\frac{n}{p}\right) = +1$ oder $\left(\frac{n}{p}\right) = -1$ ist.

Es sei nun q irgend eine von p verschiedene Primzahl (2 nicht ausgeschlossen) und s eine positive die Einheit übersteigende Gröfse. Man bezeichne ferner mit ω irgend eine Wurzel der Gleichung

$$\omega^{p-1} - 1 = 0, \tag{1}$$

und bilde die geometrische Reihe

$$\frac{1}{1-\omega^\gamma \frac{1}{q^s}} = 1 + \omega^\gamma \frac{1}{q^s} + \omega^{2\gamma} \frac{1}{q^{2s}} + \omega^{3\gamma} \frac{1}{q^{3s}} + \ldots, \tag{2}$$

in welcher γ den Index von q bedeutet. Denkt man sich für q alle von p verschiedenen Primzahlen gesetzt, und multiplicirt die so entstehenden Gleichungen in einander, so erhält man auf der zweiten Seite eine Reihe, deren Gesetz leicht zu erkennen ist. Ist nämlich n irgend eine nicht durch p theilbare ganze Zahl, und setzt man $n = q'^{m'} q''^{m''} \ldots$, wo q', q'', ... verschiedene Primzahlen bezeichnen, so wird das allgemeine Glied die Form haben

$$\omega^{m'\gamma_{q'} + m''\gamma_{q''} + \ldots} \frac{1}{n^s}.$$

Nun ist aber

$$m'\gamma_{q'} + m''\gamma_{q''} + \ldots \equiv \gamma_n \pmod{p-1},$$

und folglich wegen (1)

$$\omega^{m'\gamma_{q'} + m''\gamma_{q''} + \ldots} = \omega^{\gamma_n}.$$

Man hat daher die Gleichung

$$\Pi \frac{1}{1-\omega^\gamma \frac{1}{q^s}} = \Sigma \omega^\gamma \frac{1}{n^s} = L, \tag{3}$$

wo sich das Multiplicationszeichen auf die ganze Reihe der Primzahlen, mit alleiniger Ausnahme von p, erstreckt, während die Summation sich auf alle ganzen Zahlen von 1 bis ∞ bezieht, welche nicht durch p theilbar sind. Der Buchstabe γ bedeutet auf der ersten Seite γ_q, auf der zweiten dagegen γ_n.

Die eben gefundene Gleichung repräsentirt $p-1$ verschiedene Gleichungen, welche man erhält, wenn man für ω seine $p-1$ Werthe setzt. Bekanntlich lassen sich diese $p-1$ verschiedenen Werthe durch die Potenzen von einem derselben Ω darstellen, wenn dieser gehörig gewählt wird, und sind dann

$$\Omega^0,\ \Omega^1,\ \Omega^2,\ \ldots\ \Omega^{p-2}.$$

Wir werden, dieser Darstellung entsprechend, die verschiedenen Werthe L der Reihe oder des Products mit

$$L_0,\ L_1,\ L_2,\ \ldots\ L_{p-2} \qquad (4)$$

bezeichnen, wobei es einleuchtet daſs L_0 und $L_{\frac{p-1}{2}}$ eine von der Wahl des Werthes Ω unabhängige Bedeutung haben und sich resp. auf $\omega = 1$, $\omega = -1$ beziehen.

Ehe wir weiter gehen, ist es nöthig, den Grund der oben gemachten Voraussetzung anzugeben, nach welcher $s > 1$ sein sollte. Man überzeugt sich von der Nothwendigkeit dieser Beschränkung, wenn man auf den wesentlichen Unterschied Rücksicht nimmt, welcher zwischen zwei Arten von unendlichen Reihen Statt findet. Betrachtet man statt jedes Gliedes seinen Zahlenwerth oder wenn es imaginär ist, seinen Modul, so können zwei Fälle eintreten. Es läſst sich nämlich entweder eine endliche Gröſse angeben, welche die Summe von irgend welchen und noch so vielen dieser Zahlenwerthe oder Moduln stets übertrifft, oder diese Bedingung wird von keiner noch so groſsen aber endlichen Zahl erfüllt. Im ersteren Falle ist die Reihe immer convergirend und hat eine völlig bestimmte Summe, welche von der Anordnung der Glieder ganz unabhängig ist, sei es nun, daſs diese nur nach einer Dimension, sei es, daſs sie nach zwei oder mehr Dimensionen fortschreiten, und eine sogenannte Doppel- oder vielfache Reihe bilden. Im zweiten der eben unterschiedenen Fälle kann zwar die Reihe auch noch convergiren, aber diese Eigenschaft, so wie die Summe der Reihe, werden wesentlich durch die Art der Aufeinanderfolge der Glieder bedingt sein. Findet die Convergenz für eine gewisse Ordnung Statt, so kann sie durch Änderung

dieser Ordnung aufhören, oder es kann, wenn dies nicht der Fall ist, die Summe der Reihe eine ganz andere werden. So ist z. B. von den beiden aus denselben Gliedern gebildeten Reihen

$$1-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}-\frac{1}{\sqrt{4}}+\frac{1}{\sqrt{5}}-\frac{1}{\sqrt{6}}+\ldots$$

$$1+\frac{1}{\sqrt{3}}-\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{5}}+\frac{1}{\sqrt{7}}-\frac{1}{\sqrt{4}}+\ldots$$

nur die erste convergirend, während die folgenden

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\ldots$$

$$1+\frac{1}{3}-\frac{1}{2}+\frac{1}{5}+\frac{1}{7}-\frac{1}{4}+\ldots$$

zwar beide convergiren, aber keinesweges dieselbe Summe haben.

Was nun unsere unendliche Reihe L betrifft, so gehört diese, wie leicht zu sehen ist, nur dann in die erste der beiden eben unterschiedenen Klassen, wenn man $s>1$ annimmt, so dafs also unter dieser Voraussetzung, wenn man $L=\lambda+\mu\sqrt{-1}$ setzt, λ und μ völlig bestimmte endliche Werthe sind. Bezeichnet man nun mit $f_m+g_m\sqrt{-1}$ das Product der m ersten Factoren der Form $\frac{1}{1-\omega^{\gamma}\frac{1}{q^s}}$, diese Factoren in einer beliebigen Ordnung gedacht, so wird man immer m so grofs nehmen können, dafs sich unter diesen m ersten Factoren alle diejenigen befinden, in denen $q<h$ ist, wo h irgend eine ganze Zahl bezeichnet. Sobald m diesen Grad von Gröfse erreicht hat, wird offenbar jede der beiden Differenzen $f_m-\lambda$, $g_m-\mu$, abgesehen vom Zeichen, immerfort kleiner bleiben als $\frac{1}{h^s}+\frac{1}{(h+1)^s}+\ldots$, wie weit man sich auch m noch ferner wachsend denke. Unter der Annahme $s>1$ kann aber $\frac{1}{h^s}+\frac{1}{(h+1)^s}+\ldots$ für ein gehörig grofses h beliebig klein werden. Es ist somit bewiesen, dafs das unendliche Product in (3) einen von der Ordnung seiner Factoren unabhängigen, der Reihe L gleichen Werth hat. Ist hingegen $s=1$ oder $s<1$, so ist dieser Beweis nicht mehr anwendbar, und in der That hat das unendliche Product in diesem Falle im Allgemeinen und unabhängig von der Ordnung der Factoren keinen bestimmten Werth mehr. Liefse sich bei einer gegebenen Art der Aufeinanderfolge der Factoren die Existenz eines Grenzwerthes für die ins Unendliche fortgesetzte Multiplication nachweisen, so würde zwar die Gleichung (3), gehörig verstanden, noch

Statt finden, aber zur Feststellung dieses Werthes keinen wesentlichen Nutzen mehr gewähren. Man müfste nämlich, wenn q', q'', q''', ... die der angenommenen Ordnung entsprechenden Werthe von q sind, die Reihe L als eine so zu ordnende vielfache Reihe betrachten, dafs man zuerst diejenigen Glieder zu nehmen hätte, in denen n nur den Primfactor q' enthält, dann diejenigen der übrigen, in denen n keine anderen Primfactoren als q', q'' enthält, u. s. w. Durch die Nothwendigkeit, den Gliedern diese Ordnung zu geben, würde die Summation der Reihe eben so schwierig, als es die Untersuchung des Productes selbst ist, vor welchem die Reihe nur dann hinsichtlich der Einfachheit etwas voraus hat, wenn die Ordnung ihrer Glieder willkührlich ist, oder sich wenigstens nicht nach den Primfactoren in n richtet.

§. 2.

Setzt man $s = 1+\varrho$, so bleibt die Gleichung (3) gültig, wie klein man auch die positive Gröfse ϱ annehme. Wir wollen nun untersuchen, in welcher Art sich die darin enthaltene Reihe L ändert, wenn man ϱ unendlich klein werden läfst. Das Verhalten der Reihe ist in dieser Beziehung ein ganz verschiedenes, je nachdem ω der positiven Einheit gleich ist oder irgend einen andern Werth hat. Um mit dem ersten Falle oder mit der Untersuchung von L_0 zu beginnen, betrachten wir die Summe

$$S = \frac{1}{k^{1+\ell}} + \frac{1}{(k+1)^{1+\ell}} + \frac{1}{(k+2)^{1+\ell}} + \ldots,$$

in welcher k eine positive Constante bezeichnet. Schreibt man in der bekannten Formel

$$\int_0^1 x^{\ell-1} \log^{\ell}\left(\frac{1}{x}\right) \partial x = \frac{\Gamma(1+\varrho)}{k^{1+\ell}},$$

für k der Reihe nach k, $k+1$, $k+2$, ... und addirt, so kommt

$$S = \frac{1}{\Gamma(1+\varrho)} \int_0^1 \log^{\ell}\left(\frac{1}{x}\right) \frac{x^{k-1}}{1-x} \partial x.$$

Addirt man $\frac{1}{\varrho}$ und subtrahirt zugleich $\frac{1}{\varrho} = \frac{\Gamma(\varrho)}{\Gamma(1+\varrho)} = \frac{1}{\Gamma(1+\varrho)} \int_0^1 \log^{\ell-1}\left(\frac{1}{x}\right) \partial x$, so geht diese Gleichung über in

$$S = \frac{1}{\varrho} + \frac{1}{\Gamma(1+\varrho)} \int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log\left(\frac{1}{x}\right)}\right) \log^{\ell}\left(\frac{1}{x}\right) \partial x,$$

wo das zweite Glied für ein unendlich kleines ϱ sich der endlichen Grenze $\int_0^1 \left(\frac{x^{t-1}}{1-x} - \frac{1}{\log(\frac{1}{x})}\right) \partial x$ nähert.

Betrachtet man statt der Reihe S die allgemeinere, welche zwei positive Constanten a, b enthält,

$$\frac{1}{b^{1+t}} + \frac{1}{(b+a)^{1+t}} + \frac{1}{(b+2a)^{1+t}} + \cdots,$$

so braucht man diese nur in die Form

$$\frac{1}{a^{1+t}}\left(\frac{1}{(\frac{b}{a})^{1+t}} + \frac{1}{(\frac{b}{a}+1)^{1+t}} + \frac{1}{(\frac{b}{a}+2)^{1+t}} + \cdots\right)$$

zu bringen und mit S zu vergleichen, um sogleich zu sehen, dafs sie einem Ausdrucke von folgender Form gleich ist

$$\frac{1}{a}\frac{1}{\varrho} + \phi(\varrho),$$

wo $\phi(\varrho)$ für ein unendlich klein werdendes ϱ sich einer endlichen Grenze nähert. Die zu untersuchende Reihe L_0 besteht aus $p-1$ Partialreihen, wie

$$\frac{1}{m^{1+t}} + \frac{1}{(p+m)^{1+t}} + \frac{1}{(2p+m)^{1+t}} + \cdots,$$

wo man successive $m = 1, 2, \ldots p-1$ zu setzen hat. Man hat mithin

$$L_0 = \frac{p-1}{p}\frac{1}{\varrho} + \phi(\varrho), \qquad (5)$$

wo wieder $\phi(\varrho)$ eine Function von ϱ ist, die für ein unendlich kleines ϱ einen endlichen Werth annimmt, welchen man nach dem Vorigen leicht durch ein bestimmtes Integral ausdrücken könnte, was jedoch zu unserm Zwecke nicht erforderlich ist. Die Gleichung (5) zeigt, dafs L_0 für ein unendlich kleines ϱ den Werth ∞ erhält, und zwar so, dafs $L_0 - \frac{p-1}{p}\frac{1}{\varrho}$ endlich bleibt.

§. 3.

Nachdem wir gefunden haben, nach welchem Gesetze unsere Reihe, wenn darin $\omega = 1$ angenommen wird, für abnehmende der Einheit sich nähernde Werthe von s sich ändert, bleibt uns dieselbe Untersuchung auf die übrigen Wurzeln ω der Gleichung $\omega^{p-1} - 1 = 0$ auszudehnen. Obgleich die Summe der Reihe L, so lange $s > 1$, von der Ordnung der Glieder unabhängig ist, so wird es doch für diese Untersuchung vortheilhaft sein, sich

die Glieder einander so folgend zu denken, daſs die Werthe von n wachsend fortschreiten. Es ist nämlich unter dieser Voraussetzung $\Sigma\omega^{\gamma}\frac{1}{n^s}$ eine Function von s, welche für alle positiven Werthe von s stetig und endlich bleibt, so daſs also namentlich die Grenze, der sich der Werth der Reihe nähert, wenn man darin $s = 1+\rho$ setzt und ρ unendlich klein werden läſst, und welche von der Ordnung der Glieder unabhängig ist, durch $\Sigma\omega^{\gamma}\frac{1}{n}$ ausgedrückt ist, was bei einer andern Ordnung nicht nothwendig der Fall wäre, indem für eine solche $\Sigma\omega^{\gamma}\frac{1}{n}$ von $\Sigma\omega^{\gamma}\frac{1}{n^{1+\rho}}$ um eine endliche Gröſse verschieden sein oder auch gar keinen Werth haben kann. Um die eben ausgesprochene Behauptung zu beweisen, bezeichne man mit h irgend eine ganze positive Zahl und drücke die Summe der $h(p-1)$ ersten Glieder der Reihe mit Hülfe der schon oben gebrauchten für jedes positive s gültigen Formel

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

durch ein bestimmtes Integral aus. Man erhält so für diese Summe

$$\frac{1}{\Gamma(s)}\int_0^1 \frac{\frac{1}{x}f(x)}{1-x^p}\log^{s-1}\left(\frac{1}{x}\right)\partial x - \frac{1}{\Gamma(s)}\int_0^1 \frac{\frac{1}{x}f(x)}{1-x^p}\log^{s-1}\left(\frac{1}{x}\right)x^{hp}\,\partial x,$$

wo man zur Abkürzung gesetzt hat

$$f(x) = \omega^{\gamma_1}x + \omega^{\gamma_2}x^2 + \ldots + \omega^{\gamma_{p-1}}x^{p-1}.$$

Ist nun, wie wir voraussetzen, ω nicht $= 1$, so ist das Polynom $\frac{1}{x}f(x)$ durch $1-x$ theilbar, denn man hat

$$f(1) = \omega^{\gamma_1} + \omega^{\gamma_2} + \ldots + \omega^{\gamma_{p-1}} = 1 + \omega + \ldots + \omega^{p-2} = 0.$$

Befreit man daher Zähler und Nenner des Bruchs unter dem Integralzeichen von dem gemeinschaftlichen Factor $1-x$, so wird derselbe

$$\frac{t+u\sqrt{-1}}{1+x+x^2+\ldots+x^{p-1}},$$

wo t und u Polynome mit reellen Coëfficienten bedeuten. Bezeichnen T und U die gröſsten Zahlenwerthe von t und u zwischen $x = 0$ und $x = 1$, so sind offenbar der reelle und imaginäre Theil des zweiten Integrals respective kleiner als

$$\frac{T}{\Gamma(s)}\int_0^1 x^{hp}\log^{s-1}\left(\frac{1}{x}\right)\partial x = \frac{T}{(hp+1)^s},$$

$$\frac{U}{\Gamma(s)}\int_0^1 x^{hp}\log^{s-1}\left(\frac{1}{x}\right)\partial x = \frac{U}{(hp+1)^s}.$$

Das genannte Integral wird also für $h=\infty$ verschwinden. Die Reihe ist also, bei der angenommenen Ordnung ihrer Glieder, convergirend und man hat für ihre Summe den Ausdruck

$$\Sigma\omega^\nu\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^1 \frac{\frac{1}{x}f(x)}{1-x^\rho}\log^{s-1}\left(\frac{1}{x}\right)\partial x.$$

Diese Function von s bleibt nicht nur selbst, so lange $s>0$, stetig und endlich, sondern dieselbe Eigenschaft kommt auch ihren nach s genommenen Differentialquotienten zu. Es genügt, um sich davon zu überzeugen, nach s zu differentiiren und zu berücksichtigen, dafs $\Gamma(s)$, $\frac{\partial\Gamma(s)}{\partial x}$, ebenfalls stetig und endlich sind, so wie dafs $\Gamma(s)$ nicht Null wird, so lange s positiv bleibt.

Setzen wir daher

$$\frac{1}{\Gamma(s)}\int_0^1 \frac{\frac{1}{x}f(x)}{1-x^\rho}\log^{s-1}\left(\frac{1}{x}\right)\partial x = \psi(s)+\chi(s)\sqrt{-1},$$

wo $\psi(s)$ und $\chi(s)$ reelle Functionen bedeuten, so haben wir nach einem bekannten Satze für ein positives ϱ

$$\psi(1+\varrho)=\psi(1)+\varrho\,\psi'(1+\delta\varrho),\quad \chi(1+\varrho)=\chi(1)+\varrho\,\chi'(1+\varepsilon\varrho), \quad (6)$$

wo zur Abkürzung $\psi'(s)=\frac{\partial\psi(s)}{\partial s}$, $\chi'(s)=\frac{\partial\chi(s)}{\partial s}$ gesetzt ist und δ und ε positive von ϱ abhängige Brüche bedeuten.

Es versteht sich übrigens von selbst, dafs für $\omega=-1$, $\chi(s)=0$ ist, und dafs, wenn man von einer imaginären Wurzel ω zu ihrer conjugirten $\frac{1}{\omega}$ übergeht, $\psi(s)$ denselben Werth behält, $\chi(s)$ aber den entgegengesetzten annimmt.

§. 4.

Wir haben jetzt nachzuweisen, dafs die endliche Grenze, der sich $\Sigma\omega^\nu\frac{1}{n^{1+\tau}}$, unter der Voraussetzung, dafs ω nicht die Wurzel 1 bedeutet, nähert, wenn man das positive ϱ unendlich klein werden läfst, von Null verschieden ist. Diese Grenze ist nach vorigem § durch das Integral gegeben

$$\Sigma\omega^\nu\frac{1}{n} = -\int_0^1 \frac{\frac{1}{x}f(x)}{x^\rho-1}\,\partial x,$$

welches sich leicht durch Logarithmen und Kreisfunctionen ausdrücken läfst.

Irgend ein Linearfactor des Nenners x^p-1 ist $x-e^{\frac{2m\pi}{p}\sqrt{-1}}$, wo m aus der Reihe 0, 1, 2, ... $p-1$ zu nehmen ist. Zerlegt man $\frac{\frac{1}{x}f(x)}{x^p-1}$ in Partialbrüche, so wird nach den bekannten Formeln der Zähler des Bruchs $\frac{A_m}{x-e^{\frac{2m\pi}{p}\sqrt{-1}}}$ durch den Ausdruck $\frac{\frac{1}{x}f(x)}{px^{p-1}}$ gegeben, wo $x=e^{\frac{2m\pi}{p}\sqrt{-1}}$ zu setzen ist. Man hat also $A_m=\frac{1}{p}f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right)$. Substituirt man diesen Werth und bemerkt, dafs $A_0=0$ ist, so erhält man

$$\Sigma\omega^{\gamma}\frac{1}{n}=-\frac{1}{p}\Sigma f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right)\int_0^1\frac{\partial x}{x-e^{\frac{2m\pi}{p}\sqrt{-1}}},$$

wo sich das Summenzeichen auf der zweiten Seite von $m=1$ bis $m=p-1$ erstreckt.

Die Function $f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right)$ ist die bekannte in der Kreistheilung vorkommende und läfst sich leicht auf $f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)$ zurückführen. Es ist nämlich

$$f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right)=\Sigma\omega^{\gamma_g}e^{gm\frac{2\pi}{p}\sqrt{-1}},$$

wo sich das Zeichen von $g=1$ bis $g=p-1$ erstreckt. Setzt man statt gm den jedesmaligen Rest h nach dem Modul p, so sind 1, 2, ... $p-1$, die verschiedenen Werthe von h, und man hat, wegen $gm\equiv h$ (mod. p), $\gamma_g\equiv\gamma_h-\gamma_m$ (mod. $p-1$). Schreibt man also zugleich $\gamma_h-\gamma_m$ für γ_g, was wegen der Gleichung $\omega^{p-1}-1=0$ erlaubt ist, so kommt

$$f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right)=\omega^{-\gamma_m}\Sigma\omega^{\gamma_h}e^{h\frac{2\pi}{p}\sqrt{-1}}=\omega^{-\gamma_m}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right).$$

Die obige Gleichung wird so

$$\Sigma\omega^{\gamma}\frac{1}{n}=-\frac{1}{p}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)\Sigma\omega^{-\gamma_m}\int_0^1\frac{\partial x}{x-e^{\frac{2m\pi}{p}\sqrt{-1}}}.$$

Nun ist für einen positiven Bruch α

$$\int_0^1\frac{\partial x}{x-e^{2\alpha\pi\sqrt{-1}}}=\log(2\sin\alpha\pi)+\frac{\pi}{2}(1-2\alpha)\sqrt{-1},$$

folglich

$$\Sigma\omega^{\gamma}\frac{1}{n}=-\frac{1}{p}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)\Sigma\omega^{-\gamma_m}\left(\log(2\sin\frac{m\pi}{p})+\frac{\pi}{2}(1-\frac{2m}{p})\sqrt{-1}\right).$$

Obgleich dieser Ausdruck für $\Sigma\omega^{\gamma}\frac{1}{n}$, sehr einfach ist, so kann man doch im Allgemeinen nicht daraus schliefsen, dafs $\Sigma\omega^{\gamma}\frac{1}{n}$ einen von Null verschiedenen Werth hat. Es fehlt noch an gehörigen Principien zur Feststellung der Bedingungen, unter denen transcendente Verbindungen, welche unbestimmte ganze Zahlen enthalten, verschwinden können. Die verlangte Nachweisung gelingt jedoch für den besonderen Fall, wo $\omega = -1$. Für die imaginären Werthe von ω werden wir im folgenden § ein anderes Verfahren angeben, welches aber auf den genannten besonderen Fall nicht anwendbar ist. Unter der Voraussetzung, dafs $\omega = -1$, erhält man, mit Berücksichtigung, dafs γ_m gerade oder ungerade ist, je nachdem $\left(\frac{m}{p}\right) = +1$ oder $= -1$, und dafs folglich $(-1)^{-\gamma_m} = \left(\frac{m}{p}\right)$ ist, so wie dafs $(-1)^{\gamma_n} = \left(\frac{n}{p}\right)$, als Grenze von $L_{\frac{p-1}{2}}$ für ein unendlich klein werdendes ϱ

$$\Sigma\left(\frac{n}{p}\right)\frac{1}{n} = -\frac{1}{p}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)\Sigma\left(\frac{m}{p}\right)\left(\log\left(2\sin\frac{m\pi}{p}\right)+\frac{\pi}{2}\left(1-\frac{2m}{p}\right)\sqrt{-1}\right),$$

oder einfacher, da zwischen den Grenzen $m = 1$, $m = p-1$, $\Sigma\left(\frac{m}{p}\right) = 0$ ist,

$$\Sigma\left(\frac{n}{p}\right)\frac{1}{n} = -\frac{1}{p}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)\Sigma\left(\frac{m}{p}\right)\left(\log\left(2\sin\frac{m\pi}{p}\right)-\frac{\pi}{p}m\sqrt{-1}\right).$$

Es sind jetzt zwei Fälle zu unterscheiden, je nachdem die Primzahl p die Form $4\mu+3$ oder $4\mu+1$ hat. Im ersteren Falle ist für zwei Werthe, wie m und $p-m$, die sich zu p ergänzen,

$$\left(\frac{m}{p}\right) = -\left(\frac{p-m}{p}\right) \text{ und } \sin\frac{m\pi}{p} = \sin\frac{(p-m)\pi}{p}.$$

Mithin verschwindet der reelle Theil der Summe, und man erhält, wenn man mit a die Werthe von m bezeichnet, für welche $\left(\frac{m}{p}\right) = 1$, und mit b diejenigen, für welche $\left(\frac{m}{p}\right) = -1$, oder mit anderen Worten, wenn a und b die Quadratreste und Nichtquadratreste von p bedeuten, welche kleiner als p sind,

$$\Sigma\left(\frac{n}{p}\right)\frac{1}{n} = \frac{\pi}{p^2}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)(\Sigma a-\Sigma b)\sqrt{-1}.$$

Ist $p = 4\mu+1$, so verschwindet der imaginäre Theil der Summe, weil alsdann $\left(\frac{m}{p}\right) = \left(\frac{p-m}{p}\right)$, und man erhält

$$\Sigma\left(\frac{n}{p}\right)\frac{1}{n}=\frac{1}{p}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)\log\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}},$$

wo sich das Multiplicationszeichen auf alle a oder b erstreckt.

Bemerkt man jetzt, dafs unter der hier gemachten Annahme von $\omega=-1$, nach bekannten Formeln (1), $f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)$ im ersteren Falle $\sqrt{p}\sqrt{-1}$, im letzteren $\sqrt{p}$ ist, so kommt respective

$$\Sigma\left(\frac{n}{p}\right)\frac{1}{n}=\frac{\pi}{p\sqrt{p}}(\Sigma b-\Sigma a),\quad \Sigma\left(\frac{n}{p}\right)\frac{1}{n}=\frac{1}{\sqrt{p}}\log\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}}.$$

Für den Fall, wo $p=4\mu+3$, sieht man sogleich, dafs $\Sigma\left(\frac{n}{p}\right)\frac{1}{n}$ von Null verschieden ist, indem $\Sigma a+\Sigma b=p\frac{(p-1)}{2}$ ungerade ist und mithin nicht $\Sigma a=\Sigma b$ sein kann. Um dasselbe für $p=4\mu+1$ zu beweisen, nehme man die aus der Kreistheilung bekannten Gleichungen (2) zu Hülfe,

$$2\Pi\left(x-e^{\frac{2a\pi}{p}\sqrt{-1}}\right)=Y-Z\sqrt{p},\quad 2\Pi\left(x-e^{\frac{2b\pi}{p}\sqrt{-1}}\right)=Y+Z\sqrt{p},$$

wo Y und Z Polynome mit ganzen Coëfficienten bedeuten. Setzt man in diesen Gleichungen und der daraus folgenden

$$4\frac{x^p-1}{x-1}=Y^2-pZ^2,$$

$x=1$, und nennt g und h die ganzen Zahlen, welchen Y und Z gleich werden, so kommt, nach einigen leichten Reductionen,

$$2^{\frac{p+1}{2}}\Pi\sin\frac{a\pi}{p}=g-h\sqrt{p},\quad 2^{\frac{p+1}{2}}\Pi\sin\frac{b\pi}{p}=g+h\sqrt{p},\quad g^2-ph^2=4p.$$

Aus der letzten Gleichung folgt, dafs g durch p theilbar ist. Setzt man daher $g=pk$, und dividirt die beiden ersten durch einander, so erhält man

$$\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}}=\frac{k\sqrt{p}+h}{k\sqrt{p}-h},\quad h^2-pk^2=-4.$$

Nach der zweiten dieser Gleichungen kann h nicht Null sein, folglich sind die beiden Seiten der ersten von der Einheit verschieden, woraus so-

---

(1) *Comment. Gotting. rec. Vol. I.* oder die Abhandlungen unserer Akademie, Jahrg. 1835.

(2) *Disq. arith. art.* 357.

gleich, mit Berücksichtigung des oben erhaltenen Ausdruckes folgt, dafs $\Sigma\left(\frac{n}{p}\right)\frac{1}{n}$ nicht den Werth Null haben kann, w. z. b. w. Man kann noch hinzufügen, dafs die Summe $\Sigma\left(\frac{n}{p}\right)\frac{1}{n}$, da sie als Grenzwerth eines Products aus lauter positiven Factoren, nämlich als Grenzwerth von $\Pi\frac{1}{1-\left(\frac{q}{p}\right)\frac{1}{q^{1+\varrho}}}$ für ein unendlich klein werdendes ϱ, auch nicht negativ sein kann, nothwendig positiv sein wird.

Aus dieser Bemerkung folgen unmittelbar zwei wichtige und auf anderem Wege wahrscheinlich sehr schwer zu beweisende Sätze, von denen der auf den Fall $p = 4\mu+3$ bezügliche darin besteht, dafs für eine Primzahl dieser Form immer $\Sigma b > \Sigma a$ ist. Wir wollen uns jedoch bei diesen Folgerungen unserer Methode hier nicht aufhalten, da wir bei einer anderen Untersuchung Gelegenheit finden werden, auf diesen Gegenstand zurückzukommen.

§. 5.

Um für L_m, wenn m weder 0 noch $\frac{p-1}{2}$ ist, nachzuweisen, dafs sein einem unendlich kleinen ϱ entsprechender Grenzwerth von Null verschieden ist, nehme man den Logarithmus von $\Pi\frac{1}{1-\omega^{\gamma}\frac{1}{q^{1+\varrho}}}$, und entwickle den Logarithmus jedes Factors mittelst der Formel

$$-\log(1-x) = x + \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 + \ldots$$

Man findet so

$$\Sigma\,\omega^{\gamma}\frac{1}{q^{1+\varrho}} + \tfrac{1}{2}\Sigma\,\omega^{2\gamma}\frac{1}{(q^2)^{1+\varrho}} + \tfrac{1}{3}\Sigma\,\omega^{3\gamma}\frac{1}{(q^3)^{1+\varrho}} + \ldots = \log L,$$

wo sich die Summationen auf q beziehen und γ den Index von q bedeutet. Setzt man der Reihe nach für ω seine Werthe $1, \Omega, \Omega^2, \ldots \Omega^{p-2}$, addirt und berücksichtigt, dafs die Summe

$$1 + \Omega^{h\gamma} + \Omega^{2h\gamma} + \ldots + \Omega^{(p-2)h\gamma}$$

immer verschwindet, aufser wenn $h\gamma$ durch $p-1$ theilbar ist, in diesem Falle aber den Werth $p-1$ hat, und dafs die Bedingung $h\gamma \equiv 0 \pmod{p-1}$ gleichbedeutend mit $q^h \equiv 1 \pmod{p}$ ist, so erhält man

$$(p-1)\left(\Sigma\frac{1}{q^{1+\varrho}}+\frac{1}{2}\Sigma\frac{1}{q^{2+2\varrho}}+\frac{1}{3}\Sigma\frac{1}{q^{3+3\varrho}}+\ldots\right)=\log(L_0 L_1 \ldots L_{p-2}),$$

wo sich die erste, zweite, ... Summation resp. auf die Werthe von q bezieht, deren erste, zweite, ... Potenzen in der Form $\mu p+1$ enthalten sind. Da die erste Seite reell ist, so folgt, dafs das Product unter dem Zeichen log positiv ist, was auch sonst klar ist, und dafs für den Logarithmus der arithmetische mit keiner Vieldeutigkeit behaftete Werth zu nehmen ist. Die Reihe auf der ersten Seite bleibt stets positiv, und wir werden nun zeigen, dafs die zweite, in Widerspruch hiermit, für ein unendlich kleines ϱ den Werth $-\infty$ haben würde, wenn man die Grenze für L_m als verschwindend annehmen wollte. Die zweite Seite läfst sich in die Form bringen

$$\log L_0+\log L_{\frac{p-1}{2}}+\log L_1 L_{p-2}+\log L_2 L_{p-3}+\ldots,$$

wo $\log L_0$ nach (5) dem Ausdruck

$$\log\left(\frac{p-1}{p}\frac{1}{\varrho}+\phi(\varrho)\right)=\log\left(\frac{1}{\varrho}\right)+\log\left(\frac{p-1}{p}+\varrho\,\phi(\varrho)\right)$$

gleich ist, dessen zweites Glied sich der endlichen Grenze $\log\left(\frac{p-1}{p}\right)$ nähert; eben so bleibt $\log L_{\frac{p-1}{2}}$ endlich, da der Grenzwerth von $L_{\frac{p-1}{2}}$ nach §. 4. von 0 verschieden ist. Irgend einer der übrigen Logarithmen, wie $\log L_m L_{p-1-m}$ ist nach §. 3., $\log(\psi^2(1+\varrho)+\chi^2(1+\varrho))$, welcher Ausdruck, wenn L_m und also auch L_{p-1-m} die Null zur Grenze hätte, so dafs gleichzeitig $\psi(1)=0$, $\chi(1)=0$ wäre, in

$$\log\left(\varrho^2(\psi'^2(1+\delta\varrho)+\chi'^2(1+\varepsilon\varrho))\right)=-2\log\left(\frac{1}{\varrho}\right)+\log(\psi'^2(1+\delta\varrho)+\chi'^2(1+\varepsilon\varrho))$$

übergehen würde. Vereinigt man das Glied $-2\log(\frac{1}{\varrho})$ mit dem ersten Gliede von $\log L_0$, so bleibt $-\log(\frac{1}{\varrho})$, welcher Werth für ein unendlich kleines ϱ in $-\infty$ übergeht, und es ist klar, dafs dieser unendlich grofse negative Werth nicht etwa durch $\log(\psi'^2(1+\delta\varrho)+\chi'^2(1+\varepsilon\varrho))$ aufgehoben werden kann, denn dieser Ausdruck bleibt entweder endlich oder wird selbst $-\infty$, wenn nämlich gleichzeitig $\psi'(1)=0$, $\chi'(1)=0$ wäre. Eben so einleuchtend ist, dafs, wenn man aufser L_m und L_{p-1-m} noch ein anderes oder mehrere andere Paare zusammengehöriger L als verschwindend betrachten wollte, der Widerspruch nur noch verstärkt würde. Es ist somit bewiesen, dafs die einem unendlich klein werdenden ϱ entsprechende Grenze für L_m

(wo m nicht 0 ist) endlich und von der Null verschieden ist, so wie dafs L_0 in demselben Falle ∞ wird, woraus sogleich folgt, dafs die Reihe

$$\Sigma \omega^{\gamma} \tfrac{1}{q^{1+\varrho}} + \tfrac{1}{2} \Sigma \omega^{2\gamma} \tfrac{1}{q^{2+2\varrho}} + \tfrac{1}{3} \Sigma \omega^{3\gamma} \tfrac{1}{q^{3+3\varrho}} + \ldots = \log L \qquad (7)$$

sich immer, wenn nur nicht $\omega = 1$, einer endlichen Grenze nähert, für $\omega = 1$ aber unendlich grofs wird, wenn man ϱ unendlich klein werden läfst.

Wollte man diese endliche Grenze selbst haben, deren Kenntnifs jedoch zu unserem Zwecke nicht erforderlich ist, so würde (wenn ω nicht -1 ist) ihre Bestimmung durch den Ausdruck $\log(\psi(1) + \chi(1)\sqrt{-1})$ mit einer Vieldeutigkeit behaftet sein, die man aber in jedem speciellen Falle, d. h. sobald p und ω numerisch gegeben sind, leicht heben kann. Setzt man die Reihe (7), $= u + v\sqrt{-1}$, und folglich

$$u + v\sqrt{-1} = \log L = \log(\psi(1+\varrho) + \sqrt{-1}\,\chi(1+\varrho)),$$

so hat man

$$u = \tfrac{1}{2} \log(\psi^2(1+\varrho) + \chi^2(1+\varrho)),$$

$$\cos v = \frac{\psi(1+\varrho)}{\sqrt{\psi^2(1+\varrho) + \chi^2(1+\varrho)}}, \quad \sin v = \frac{\chi(1+\varrho)}{\sqrt{\psi^2(1+\varrho) + \chi^2(1+\varrho)}},$$

und folglich ist der Grenzwerth von u ohne Vieldeutigkeit,

$$= \tfrac{1}{2} \log(\psi^2(1) + \chi^2(1)).$$

Um den von v eben so zu erhalten, bemerke man, dafs die Reihe, wie klein auch ϱ sei, stetig mit dieser Gröfse veränderlich ist, wie man leicht nachweisen kann, und dafs mithin auch v eine stetige Function von ϱ sein mufs. Nun wird sich, da nicht zugleich $\psi(1) = 0$, $\chi(1) = 0$ sein kann, aus den oben gegebenen Ausdrücken von $\psi(1+\varrho)$ und $\chi(1+\varrho)$ in Form bestimmter Integrale immer ein positiver endlicher Werth R von solcher Beschaffenheit ableiten lassen, dafs wenigstens eine der Functionen $\psi(1+\varrho)$, $\chi(1+\varrho)$ für jedes ϱ, welches $< R$ ist, dasselbe Zeichen behält. Es wird mithin $\cos v$ oder $\sin v$, sobald ϱ abnehmend kleiner als R geworden ist, sein Zeichen nicht mehr ändern, und also der continuirlich veränderliche Bogen v nicht mehr um π zu- oder abnehmen können. Bestimmt man also den $\varrho = R$ entsprechenden endlichen Werth von v, den wir V nennen wollen, und den man durch numerische Rechnung aus der Reihe (7) selbst leicht finden kann, da diese für

jeden endlichen Werth von ϱ in die erste der in §. 1. unterschiedenen Klassen gehört und also eine völlig bestimmte Summe hat, so ist nun der Grenzwerth v_0 von v durch die Gleichungen

$$\cos v_0 = \frac{\psi(1)}{\sqrt{\psi^2(1)+\chi^2(1)}},\quad \sin v_0 = \frac{\chi(1)}{\sqrt{\psi^2(1)+\chi(1)^2}},$$

mit der Bedingung verbunden, dafs die Differenz $V-v_0$, abgesehen vom Zeichen, $<\pi$ sein mufs, vollständig bestimmt.

§. 6.

Wir sind jetzt im Stande zu beweisen, dafs jede arithmetische Reihe, deren Differenz p ist und deren erstes Glied nicht durch p theilbar ist, unendlich viele Primzahlen enthält, oder mit anderen Worten, dafs es unendlich viele Primzahlen von der Form $\mu p+m$ giebt, wo μ eine unbestimmte ganze Zahl und m eine der Zahlen 1, 2, 3, ... $p-1$ bedeutet. Denkt man sich die in der Gleichung (7) enthaltenen Gleichungen, so wie sie der Reihe nach den Wurzeln $1, \Omega, \Omega^2, \ldots, \Omega^{p-2}$, (4) entsprechen, mit $1, \Omega^{-\gamma_m}, \Omega^{-2\gamma_m}, \ldots \Omega^{-(p-2)\gamma_m}$, multiplicirt und addirt, so erhält man auf der ersten Seite

$$\begin{aligned}
&\Sigma\left(1+\Omega^{\gamma-\gamma_m}+\Omega^{2(\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(\gamma-\gamma_m)}\right)\frac{1}{q^{1+\varrho}}\\
&+\tfrac{1}{2}\Sigma\left(1+\Omega^{2\gamma-\gamma_m}+\Omega^{2(2\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(2\gamma-\gamma_m)}\right)\frac{1}{q^{2+2\varrho}}\\
&+\tfrac{1}{3}\Sigma\left(1+\Omega^{3\gamma-\gamma_m}+\Omega^{2(3\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(3\gamma-\gamma_m)}\right)\frac{1}{q^{3+3\varrho}}\\
&+\ldots,
\end{aligned}$$

wo sich die Summationen auf q beziehen und γ den Index von q bezeichnet. Nun ist aber

$$1+\Omega^{h\gamma-\gamma_m}+\Omega^{2(h\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(h\gamma-\gamma_m)}=0,$$

aufser wenn $h\gamma-\gamma_m=0 \pmod{p-1}$ ist, in welchem Falle diese Summe $=p-1$ ist. Diese Congruenz ist aber gleichbedeutend mit $q^h\equiv m \pmod{p}$. Man hat daher die Gleichung

$$\begin{aligned}
&\Sigma\tfrac{1}{q^{1+\varrho}}+\tfrac{1}{2}\Sigma\tfrac{1}{q^{2+2\varrho}}+\tfrac{1}{3}\Sigma\tfrac{1}{q^{3+3\varrho}}+\ldots\\
&=\frac{1}{p-1}\left(\log L_0+\Omega^{-\gamma_m}\log L_1+\Omega^{-2\gamma_m}\log L_2+\ldots+\Omega^{-(p-2)\gamma_m}\log L_{p-2}\right),
\end{aligned}$$

wo sich die erste Summation auf alle Primzahlen q der Form $\mu p + m$ erstreckt, die zweite auf alle Primzahlen q, deren Quadrate, die dritte auf alle Primzahlen q, deren Cuben, u. s. w. in derselben Form enthalten sind. Denkt man sich nun ϱ unendlich klein werdend, so wird die zweite Seite durch das Glied $\log L_0$ unendlich grofs. Es mufs also auch die erste Seite unendlich werden. Auf dieser Seite bleibt aber die Summe aller Glieder, mit Ausschlufs des ersten, endlich, da bekanntlich $\frac{1}{2}\Sigma\frac{1}{q^2} + \frac{1}{3}\Sigma\frac{1}{q^3} + \ldots$ noch endlich ist, wenn man unter q nicht, wie hier, gewisse Primzahlen, sondern alle ganzen Zahlen, welche > 1 sind, versteht. Folglich mufs die Reihe $\Sigma\frac{1}{q^{1+\varrho}}$ über jede positive Grenze hinaus wachsen, sie mufs mithin unendlich viele Glieder enthalten, d. h. es giebt unendlich viele Primzahlen q der Form $\mu p + m$, w. z. b. w.

§. 7.

Um den im Vorhergehenden geführten Beweis auf eine arithmetische Reihe auszudehnen, deren Differenz irgend eine zusammengesetzte Zahl ist, sind einige Sätze aus der Theorie der Potenzreste erforderlich, die wir hier kurz zusammenstellen wollen, um uns in der Folge leichter darauf berufen zu können. Die Begründung dieser Resultate kann man in den *Disq. arith. sect. III.* nachsehen, wo dieser Gegenstand ausführlich behandelt ist.

I. Die Existenz von primitiven Wurzeln ist nicht auf ungerade Primzahlen p beschränkt, sondern findet auch noch für irgend eine Potenz p^π einer solchen Statt. Ist c eine primitive Wurzel für den Modul p^π, so sind die nach diesem genommenen Reste der Potenzen

$$c^0,\ c^1,\ c^2,\ \ldots,\ c^{(p-1)p^{\pi-1}-1},$$

alle von einander verschieden und fallen mit der Reihe derjenigen Zahlen zusammen, welche $< p^\pi$ und zu p^π relative Primzahlen sind. Hat man nun irgend eine nicht durch p theilbare Zahl n, so ist der Exponent $\gamma_n < (p-1)p^{\pi-1}$, welcher der Congruenz

$$c^{\gamma_n} \equiv n \pmod{p^\pi}$$

genügt, völlig bestimmt und soll der Index von n heifsen. Von solchen Indices gelten wieder die leicht zu beweisenden Sätze, dafs der Index eines Productes der Summe der Indices der Factoren, um das gröfste darin ent-

haltene Vielfache von $(p-1)p^{\pi-1}$ vermindert, gleich, so wie dafs γ_n gerade oder ungerade ist, je nachdem $\left(\frac{n}{p}\right) = +1$ oder -1 ist.

II. Die Primzahl 2 verhält sich in der Theorie der primitiven Wurzeln wesentlich anders, als die ungeraden Primzahlen, und es ist über diese Primzahl Folgendes zu bemerken, wenn wir die erste Potenz 2, welche hier nicht in Betracht kommt, aufser Acht lassen.

1) Für den Modul 2^2 hat man die primitive Wurzel -1. Bezeichnet man den Index für irgend eine ungerade Zahl n mit α_n, so dafs also $(-1)^{\alpha_n} \equiv n \pmod 4$, so ist $\alpha_n = 0$ oder $= 1$, je nachdem n die Form $4\mu+1$ oder $4\mu+3$ hat, und man erhält den Index eines Productes, wenn man von der Summe der Indices der Factoren das gröfste darin enthaltene Vielfache von 2 abzieht.

2) Hat der Modul die Form 2^λ, wo $\lambda \geqq 3$ ist, so giebt es keine primitive Wurzel mehr, d. h. es existirt keine Zahl, für welche die Periode ihrer Potenzreste nach dem Divisor 2^λ alle ungerade Zahlen enthält, welche $< 2^\lambda$ sind. Man kann nur die Hälfte dieser Zahlen als solche Reste darstellen. Wählt man irgend eine Zahl der Form $8\mu+5$ oder speciell 5 zur Basis, so sind die nach dem Modul 2^λ genommenen Reste der Potenzen

$$5^0,\ 5^1,\ 5^2,\ \ldots,\ 5^{2^{\lambda-2}-1},$$

alle von einander verschieden und fallen mit den Zahlen zusammen, welche die Form $4\mu+1$ haben und $< 2^\lambda$ sind. Hat man daher eine Zahl n der Form $4\mu+1$, so läfst sich immer der Congruenz

$$5^{\beta_n} \equiv n \pmod{2^\lambda}$$

durch einen und nur durch einen Exponenten oder Index β_n genügen, wenn dieser $< 2^{\lambda-2}$ sein soll. Hat n die Form $4\mu+3$, so ist diese Congruenz unmöglich. Da aber unter dieser Voraussetzung $-n$ die Form $4\mu+1$ hat, so wollen wir allgemein unter dem Index einer ungeraden Zahl n den völlig bestimmten Exponenten β_n verstehen, welcher $< 2^{\lambda-2}$ ist und der Congruenz

$$5^{\beta_n} \equiv \pm n \pmod{2^\lambda}$$

genügt, in welcher das obere und das untere Zeichen zu nehmen ist, je nachdem n die Form $4\mu+1$ oder $4\mu+3$ hat. Wegen dieses doppelten Zei-

chens ist also der Rest von n nach dem Modul 2^λ durch den Index β_n nicht mehr völlig bestimmt, indem demselben Index zwei Reste entsprechen, die sich zu 2^λ ergänzen. Für die so definirten Indices gelten offenbar die Sätze, dafs der Index eines Productes der Summe der Indices der Factoren, um das darin enthaltene gröfste Vielfache von $2^{\lambda-2}$ vermindert, gleich ist, so wie dafs β_n gerade oder ungerade sein wird, je nachdem n die Form $8\mu \pm 1$ oder die Form $8\mu \pm 5$ haben wird. Um die vorher erwähnte Zweideutigkeit zu heben, wird es genügen, neben dem Index β_n, welcher sich auf den Modul 2^λ und die Basis 5 bezieht, noch den Index α_n, welcher dem Modul 4 und der Basis -1 entspricht, zu betrachten, indem dann, je nachdem $\alpha_n = 0$ oder 1 ist, das obere oder untere Zeichen in

$$5^{\beta_n} \equiv \pm n \pmod{2^\lambda}$$

zu nehmen sein wird. Man kann auch, wenn man will, beide Indices in einer Formel vereinigen, und

$$(-1)^{\alpha_n} 5^{\beta_n} \equiv n \pmod{2^\lambda}$$

schreiben, durch welche Congruenz der Rest von n nach dem Modul 2^λ vollständig bestimmt ist.

III. Es sei nun $k = 2^\lambda p^\pi p'^{\pi'} \ldots$, wo, wie in II. 2, $\lambda \gtrless 3$, und $p, p', \ldots$ von einander verschiedene ungerade Primzahlen bezeichnen. Hat man irgend eine durch keine der Primzahlen $2, p, p', \ldots$ theilbare Zahl n, und kennt man die den Moduln

$$4,\ 2^\lambda,\ p^\pi,\ p'^{\pi'},\ \ldots$$

und ihren primitiven Wurzeln

$$-1,\ 5,\ c,\ c',\ \ldots$$

entsprechenden Indices

$$\alpha_n, \beta_n, \gamma_n, \gamma'_n, \ldots$$

so hat man die Congruenzen

$$(-1)^{\alpha_n} \equiv n \pmod 4, \quad 5^{\beta_n} \equiv \pm n \pmod{2^\lambda},$$
$$c^{\gamma_n} \equiv n \pmod{p^\pi}, \quad c'^{\gamma'_n} \equiv n \pmod{p'^{\pi'}}, \ \ldots$$

durch deren Inbegriff der Rest von n, nach dem Divisor k genommen, vollständig bestimmt ist, wie aus bekannten Sätzen sogleich folgt, wenn man

berücksichtigt, dafs das doppelte Zeichen in der zweiten dieser Congruenzen durch die erste festgestellt wird. Wir werden die Indices α_n, β_n, γ_n, γ'_n, ... oder α, β, γ, γ', ..., das System der Indices für die Zahl n nennen. Da die Indices α, β, γ, γ', ... resp. 2, $2^{\lambda-2}$, $(p-1)p^{\pi-1}$, $(p'-1)p'^{\pi'-1}$, ... verschiedene Werthe erhalten können, so ist

$$2 \cdot 2^{\lambda-2}(p-1)p^{\pi-1} \cdot (p'-1)p'^{\pi'-1} \ldots = k\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{p'}\right)\ldots = K \quad (8)$$

die Anzahl aller möglichen Systeme dieser Art, was mit dem bekannten Satze übereinstimmt, nach welchem K die Anzahl derjenigen Zahlen ausdrückt, welche kleiner als k und zu k relative Primzahlen sind.

§. 8.

Indem wir nun dazu übergehen, das Theorem über die arithmetische Progression in seiner ganzen Allgemeinheit zu beweisen, bemerken wir, dafs man, ohne dieser Allgemeinheit zu schaden, die Differenz k der Progression als durch 8 theilbar und also in der Form des vorigen §. n. III. enthalten, annehmen kann. Ist der Satz unter dieser Voraussetzung bewiesen, so wird er offenbar um so mehr gelten, wenn die Differenz ungerade oder nur durch 2 oder 4 theilbar ist. Es seien θ, ϕ, ω, ω', ... irgend welche Wurzeln der Gleichungen

$$\theta^2-1=0,\ \phi^{2^{\lambda-2}}-1=0,\ \omega^{(p-1)p^{\pi-1}}-1=0,\ \omega'^{(p'-1)p'^{\pi'-1}}-1=0,\ \ldots \quad (9)$$

und q eine beliebige von 2, p, p', ... verschiedene Primzahl. Bildet man nun die Gleichung

$$\frac{1}{1-\theta^\alpha\phi^\beta\omega^\gamma\omega'^{\gamma'}\ldots\frac{1}{q^s}} = 1+\theta^\alpha\phi^\beta\omega^\gamma\omega'^{\gamma'}\ldots\frac{1}{q^s}+\theta^{2\alpha}\phi^{2\beta}\omega^{2\gamma}\omega'^{2\gamma'}\ldots\frac{1}{q^{2s}}+\ldots,$$

in welcher $s>1$, und das System der Indices α, β, γ, γ', ... sich auf q bezieht und multiplicirt alle Gleichungen dieser Form, welche man erhält, wenn man für q alle von 2, p, p', ... verschiedenen Primzahlen setzt, in einander, so kommt, mit Berücksichtigung der oben erwähnten Eigenschaften der Indices und der Gleichungen (9),

$$\Pi\frac{1}{1-\theta^\alpha\phi^\beta\omega^\gamma\omega'^{\gamma'}\ldots\frac{1}{q^s}} = \Sigma\theta^\alpha\phi^\beta\omega^\gamma\omega'^{\gamma'}\ldots\frac{1}{n^s} = L, \quad (10)$$

wo sich das Multiplicationszeichen auf die ganze Reihe der Primzahlen, mit Ausschluſs von $2, p, p', \ldots$, und das Summenzeichen auf alle positiven ganzen Zahlen, welche durch keine der Primzahlen $2, p, p', \ldots$ theilbar sind, erstreckt. Das System der Indices $\alpha, \beta, \gamma, \gamma', \ldots$ entspricht auf der ersten Seite der Zahl q, auf der zweiten der Zahl n. Die allgemeine Gleichung (10), in welcher die verschiedenen Wurzeln $\theta, \phi, \omega, \omega', \ldots$ auf irgend eine Weise mit einander combinirt werden können, enthält offenbar eine Anzahl K besonderer Gleichungen. Um die jeder dieser Verbindungen entsprechende Reihe L bequem zu bezeichnen, kann man sich die Wurzeln von jeder der Gleichungen (9) als Potenzen von einer derselben dargestellt denken. Sind $\Theta = -1$; $\Phi, \Omega, \Omega', \ldots$ hierzu geeignete Wurzeln, so kann man setzen

$$\theta = \Theta^{\mathfrak{a}}, \quad \phi = \Phi^{\mathfrak{b}}, \quad \omega = \Omega^{\mathfrak{c}}, \quad \omega' = \Omega'^{\mathfrak{c}'}, \quad \ldots$$

wo $$\mathfrak{a} < 2, \quad \mathfrak{b} < 2^{\lambda-2}, \quad \mathfrak{c} < (p-1)p^{\pi-1}, \quad \mathfrak{c}' < (p'-1)p'^{\pi'-1}, \quad \ldots$$

und dieser Darstellung entsprechend, die Reihe L mit

$$L_{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots} \tag{11}$$

bezeichnen. Die Nothwendigkeit der Voraussetzung $s > 1$ in der Gleichung (10) beruht auf den schon in §. 1. entwickelten Gründen.

§. 9.

Die im vorigen §. mit L bezeichneten Reihen, deren Anzahl $= K$ ist, lassen sich, nach den verschiedenen Wurzelcombinationen $\theta, \phi, \omega, \omega', \ldots$, denen sie entsprechen, in folgende drei Klassen theilen. Die erste Klasse enthält nur eine Reihe, nämlich $L_{0, 0, 0, 0, \ldots}$, d. h. diejenige, in welcher

$$\theta = 1, \quad \phi = 1, \quad \omega = 1, \quad \omega' = 1, \quad \ldots$$

Die zweite Klasse soll alle übrigen Reihen umfassen, in welchen nur reelle Wurzeln der Gleichungen (9) vorkommen, so daſs also zur Darstellung dieser Reihen die Zeichen in

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

auf jede mögliche Weise combinirt werden müssen, wobei nur die eine der ersten Klasse entsprechende Zeichenverbindung auszuschlieſsen ist. Die dritte Klasse endlich wird alle Reihen L in sich begreifen, in denen wenig-

stens eine der Wurzeln ϕ, ω, ω', ... imaginär ist, und es leuchtet ein, daſs die Reihen dieser Klasse einander paarweise zugeordnet sind, da die beiden Wurzelcombinationen

$$\theta,\ \phi,\ \omega,\ \omega',\ \ldots\ ;\ \frac{1}{\theta}=\theta,\ \frac{1}{\phi},\ \frac{1}{\omega},\ \frac{1}{\omega'},\ \ldots$$

unter der eben ausgesprochenen Voraussetzung offenbar von einander verschieden sind. Wir haben jetzt das Verhalten dieser Reihen zu untersuchen, wenn man darin $s=1+\varrho$ setzt, und das positive ϱ unendlich klein werden läſst. Betrachten wir zunächst diejenige Reihe, welche die erste Klasse constituirt, so ist klar, daſs diese als die Summe von K Partialreihen angesehen werden kann, deren jede die Form hat

$$\frac{1}{m^{1+\varrho}}+\frac{1}{(k+m)^{1+\varrho}}+\frac{1}{(2k+m)^{1+\varrho}}+\ldots,$$

wo $m<k$ und zu k relative Primzahl ist. Mithin ist die Reihe dieser Klasse nach §. 2. dem Ausdrucke

$$\frac{K}{k}\frac{1}{\varrho}+\phi(\varrho), \qquad (12)$$

gleich, wo $\phi(\varrho)$ für ein unendlich kleines ϱ endlich bleibt.

Was die Reihen der zweiten und dritten Klasse betrifft, so findet man, wenn man sich darin die Glieder so geordnet denkt, daſs die Werthe von n wachsend fortschreiten und $s>0$ setzt, für diese die Gleichung

$$\Sigma\,\theta^{\alpha}\phi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots\frac{1}{n^{s}}=\frac{1}{\Gamma(s)}\int_{0}^{1}\frac{\Sigma\,\theta^{\alpha}\phi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots x^{n-1}}{1-x^{k}}\log^{s-1}\left(\frac{1}{x}\right)\partial x, \qquad (13)$$

wo sich das Zeichen Σ auf der zweiten Seite auf alle positiven ganzen Zahlen n erstreckt, welche $<k$ und zu k relative Primzahlen sind, und α, β, γ, γ', ... das System der Indices für n bedeutet, und man beweist leicht, daſs die zweite Seite einen endlichen Werth hat. Man darf hierzu nur bemerken, daſs das Polynom $\Sigma\,\theta^{\alpha}\phi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots x^{n-1}$ den Factor $1-x$ involvirt, was sogleich erhellt, wenn man $x=1$ setzt, wodurch dieses Polynom in das Product

$$(1+\theta)\left(1+\phi+\ldots+\phi^{2^{\lambda-2}-1}\right)\left(1+\omega+\ldots+\omega^{(p-1)p^{\pi-1}-1}\right)$$
$$\left(1+\omega'+\ldots+\omega'^{(p'-1)p'^{\pi'-1}-1}\right)\ldots$$

übergeht, von dessen Factoren wenigstens einer verschwindet, da die Wurzelcombination

$$\theta = 1,\ \phi = 1,\ \omega = 1,\ \omega' = 1,\ \ldots,$$

als der ersten Klasse entsprechend, ausgeschlossen ist. Eben so leicht überzeugt man sich, dafs die zweite Seite der Gleichung (13), so wie ihr nach s genommener Differentialquotient stetige Functionen von s sind. Es folgt hieraus sogleich, dafs jede Reihe der zweiten und dritten Klasse sich für ein unendlich klein werdendes ϱ einer endlichen, durch

$$\Sigma\, \theta^{\alpha} \phi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots \frac{1}{n} = \int_0^1 \frac{\Sigma\, \theta^{\alpha} \phi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots x^{n-1}}{1-x^k}\, \partial x \qquad (14)$$

ausgedrückten Grenze nähert. Es bleibt nun zu beweisen, dafs diese Grenze immer von Null verschieden ist.

§. 10.

Die Grenze für ein L der zweiten oder dritten Klasse läfst sich nun zwar leicht, wie in §. 4., durch Logarithmen und Kreisfunctionen ausdrücken, allein diese Darstellung derselben gewährt gar keinen Nutzen für die geforderte Nachweisung, selbst dann nicht, wenn L zur zweiten Klasse gehört, obgleich dieser Fall sonst eine grofse Analogie mit dem in der letzten Hälfte des §. 4. betrachteten darbietet. Wir wollen für jetzt annehmen, die erwähnte Eigenschaft sei für jedes L der zweiten Klasse bewiesen, und nun zeigen, wie derselben Forderung für ein L der dritten Klasse genügt werden kann. Zu diesem Zwecke nehme man die Logarithmen von beiden Seiten der Gleichung (10) und entwickle; man erhält so

$$\Sigma\, \theta^{\alpha} \phi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots \frac{1}{q^{i+\varrho}} + \tfrac{1}{2} \Sigma\, \theta^{2\alpha} \phi^{2\beta} \omega^{2\gamma} \omega'^{2\gamma'} \ldots \frac{1}{q^{2i+2\varrho}} + \ldots = \log L,$$

wo die Indices $\alpha, \beta, \gamma, \gamma', \ldots$ zu q gehören, und auch das Zeichen Σ sich auf q bezieht. Stellt man die Wurzeln $\theta, \phi, \omega, \omega', \ldots$ auf die in §. 8. angegebene Weise dar, und setzt $\theta = \Theta^{a}$, $\phi = \Phi^{b}$, $\omega = \Omega^{c}$, $\omega' = \Omega'^{c'}$, ..., so wird das allgemeine Glied der ersten Seite

$$\frac{1}{h} \Sigma\, \Theta^{h\alpha a} \Phi^{h\beta b} \Omega^{h\gamma c} \Omega'^{h\gamma' c'} \ldots \frac{1}{q^{h+h\varrho}},$$

während nach (11) für die zweite Seite

$$\log L_{a, b, c, c', \ldots}$$

zu schreiben ist.

Es sei nun m irgend eine ganze Zahl $<k$, welche keinen gemeinschaftlichen Factor mit k hat. Multiplicirt man auf beiden Seiten mit

$$\Theta^{-\alpha_m \mathfrak{a}}\, \Phi^{-\beta_m \mathfrak{b}}\, \Omega^{-\gamma_m \mathfrak{c}}\, \Omega'^{-\gamma'_m \mathfrak{c}'} \ldots,$$

und schreibt zur Abkürzung auf der ersten Seite nur das allgemeine Glied, so kommt

$$\ldots + \frac{1}{h} \Sigma\, \Theta^{(h\alpha-\alpha_m)\mathfrak{a}}\, \Phi^{(h\beta-\beta_m)\mathfrak{b}}\, \Omega^{(h\gamma-\gamma_m)\mathfrak{c}}\, \Omega'^{(h\gamma'-\gamma'_m)\mathfrak{c}'} \ldots \frac{1}{q^{h+h\varrho}} + \ldots$$
$$= \Theta^{-\alpha_m \mathfrak{a}}\, \Phi^{-\beta_m \mathfrak{b}}\, \Omega^{-\gamma_m \mathfrak{c}}\, \Omega'^{-\gamma'_m \mathfrak{c}'} \ldots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$$

Summirt man jetzt, um alle Wurzelcombinationen zu umfassen, von $\mathfrak{a}=0$, $\mathfrak{b}=0$, $\mathfrak{c}=0$, $\mathfrak{c}'=0$, ..., bis $\mathfrak{a}=1$, $\mathfrak{b}=2^{\lambda-2}-1$, $\mathfrak{c}=(p-1)p^{\pi-1}-1$, $\mathfrak{c}'=(p'-1)p'^{\pi'-1}-1$, ..., so kommt auf der ersten Seite als allgemeines Glied

$$\frac{1}{h} \Sigma\, W \frac{1}{q^{h+h\varrho}},$$

wo sich das Zeichen Σ auf q erstreckt, und W das Product der nach $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{c}'$, ... resp. zwischen den angegebenen Grenzen zu nehmenden Summen bedeutet,

$$\Sigma\, \Theta^{(h\alpha-\alpha_m)\mathfrak{a}},\ \Sigma\, \Phi^{(h\beta-\beta_m)\mathfrak{b}},\ \Sigma\, \Omega^{(h\gamma-\gamma_m)\mathfrak{c}},\ \Sigma\, \Omega'^{(h\gamma'-\gamma'_m)\mathfrak{c}'},\ \ldots$$

Nun ist, mit Berücksichtigung von §. 7., leicht zu sehen, dafs die erste dieser Summen 2 oder 0 ist, je nachdem die Congruenz $h\alpha-\alpha_m \equiv 0 \pmod 2$, oder was dasselbe ist, die Congruenz $q^h \equiv m \pmod 4$ Statt findet oder nicht Statt findet, dafs die zweite $2^{\lambda-2}$ oder 0 ist, je nachdem die Congruenz $h\beta-\beta_m \equiv 0 \pmod{2^{\lambda-2}}$, oder was dasselbe ist, die Congruenz $q^h \equiv \pm m \pmod{2^\lambda}$ Statt findet oder nicht Statt findet, dafs die dritte $(p-1)p^{\pi-1}$ oder 0 ist, je nachdem die Congruenz $h\gamma-\gamma_m \equiv 0 \pmod{(p-1)p^{\pi-1}}$, oder was dasselbe ist, die Congruenz $q^h \equiv m \pmod{p^\pi}$ Statt findet oder nicht Statt findet, u. s. w. Es folgt hieraus, dafs W immer verschwindet, aufser wenn man gleichzeitig $q^h \equiv m$, nach den Moduln 2^λ, p^π, $p'^{\pi'}$, ... hat, oder was dasselbe ist, aufer wenn $q^h \equiv m \pmod k$, ist, in welchem Falle $W=K$ wird. Unsere Gleichung wird daher

$$\Sigma \frac{1}{q^{1+\varrho}} + \frac{1}{2} \Sigma \frac{1}{q^{2+2\varrho}} + \frac{1}{3} \Sigma \frac{1}{q^{3+3\varrho}} + \ldots$$
$$= \frac{1}{K} \Sigma\, \Theta^{-\alpha_m \mathfrak{a}}\, \Phi^{-\beta_m \mathfrak{b}}\, \Omega^{-\gamma_m \mathfrak{c}}\, \Omega'^{-\gamma'_m \mathfrak{c}'} \ldots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}, \quad (15)$$

wo sich die Summationen auf der ersten Seite resp. auf alle Primzahlen q beziehen, deren erste, zweite, dritte Potenzen in der Form $\mu k + m$ enthalten sind, während die Summation auf der zweiten Seite über $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{c}'$, ..., zwischen den schon angegebenen Grenzen zu erstrecken ist. Setzt man speciell $m = 1$, so wird $\alpha_m = 0$, $\beta_m = 0$, $\gamma_m = 0$, $\gamma'_m = 0$, ..., und die zweite Seite reducirt sich auf

$$\frac{1}{K} \Sigma \log L_{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots}$$

Unter den Gliedern dieser Summe wird dasjenige, welches dem L der ersten Klasse, oder nach (11), $L_{0, 0, 0, 0, 0, \ldots}$ entspricht, vermöge (12), $\log(\frac{1}{\varrho})$ enthalten. Diejenigen Glieder, welche den verschiedenen L der zweiten Klasse entsprechen, werden, unter Voraussetzung der oben geforderten Nachweisung, für ein unendlich kleines ϱ endlich bleiben. Wäre nun der Grenzwerth für irgend ein L der dritten Klasse der Null gleich, so würde, wie in §. 5., die Betrachtung der Continuität des Ausdrucks (13) für den Logarithmus dieses L, mit dem des ihm zugeordneten L verbunden, das Glied $-2\log(\frac{1}{\varrho})$ ergeben, aus dessen Vereinigung mit $\log(\frac{1}{\varrho})$ in $\log L_{0, 0, 0, 0, 0, \ldots}$ noch $-\log(\frac{1}{\varrho})$ bliebe, welches Glied für ein unendlich klein werdendes ϱ den Werth $-\infty$ annimmt, während die erste Seite aus lauter positiven Gliedern besteht. Es kann daher kein L der dritten Klasse die Null zum Grenzwerth haben, und wir haben das Resultat (unter Vorbehalt des noch zu gebenden Beweises für die Reihen der zweiten Klasse), dafs

$$\log L_{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots}$$

sich für ein unendlich klein werdendes ϱ immer einer endlichen Grenze nähert, ausgenommen, wenn gleichzeitig $\mathfrak{a} = 0$, $\mathfrak{b} = 0$, $\mathfrak{c} = 0$, $\mathfrak{c}' = 0$, ... ist, in welchem Falle dieser Logarithmus einen unendlich grofsen Werth erhält.

Wendet man dieses Resultat auf die allgemeine Gleichung (15) an, so sieht man sogleich, dafs die zweite Seite derselben für ein unendlich kleines ϱ unendlich wird, und zwar durch das Glied $\frac{1}{K} \log L_{0, 0, 0, 0, 0, \ldots}$, welches über jede Grenze hinaus wächst, während alle übrigen endlich bleiben. Es mufs also auch die erste Seite jede endliche Grenze überschreiten, woraus, wie in §. 6. folgt, dafs die Reihe $\Sigma \frac{1}{q^{1+\varrho}}$ unendlich viele Glieder enthält, oder mit anderen Worten, dafs die Anzahl derjenigen Primzahlen q, welche die Form $k\mu + m$ haben, in welcher μ eine unbestimmte ganze Zahl und

m eine gegebene Zahl bezeichnet, die keinen gemeinschaftlichen Factor mit k hat, unendlich ist, w. z. b. w.

§. 11.

Was nun die zur Vervollständigung des eben entwickelten Beweises noch erforderliche Nachweisung betrifft, so reducirt sich diese nach dem unter (14) gegebenen Ausdruck für den Grenzwerth eines L der zweiten oder dritten Klasse darauf, daſs man zeige, daſs für irgend eine Wurzelcombination der Form $\pm 1, \pm 1, \pm 1, \pm 1, \ldots$, mit alleiniger Ausnahme der folgenden $+1, +1, +1, +1, \ldots$, die Summe

$$\Sigma (\pm 1)^{\alpha} (\pm 1)^{\beta} (\pm 1)^{\gamma} (\pm 1)^{\gamma'} \ldots \frac{1}{n}, \qquad (16)$$

worin $\alpha, \beta, \gamma, \gamma', \ldots$ das System der Indices für n bedeutet, und für n alle positiven ganzen Zahlen, welche durch keine der Primzahlen $2, p, p', p'', \ldots$ theilbar sind, und so wie sie ihrer Gröſse nach auf einander folgen, zu setzen sind, einen von der Null verschiedenen Werth hat. In der Abhandlung, so wie sie der Akademie ursprünglich vorgelegt wurde, hatte ich diese Eigenschaft durch indirecte und ziemlich complicirte Betrachtungen beweisen. Ich habe mich aber später überzeugt, daſs man denselben Zweck auf einem andern Wege weit kürzer erreicht. Die Principien, von welchen wir hier ausgegangen sind, lassen sich auf mehrere andere Probleme anwenden, zwischen denen und dem hier behandelten Gegenstande man zunächst keinen Zusammenhang vermuthen sollte. Namentlich kann man mit Hülfe dieser Principien die sehr interressante Aufgabe lösen, die Anzahl der verschiedenen quadratischen Formen zu bestimmen, welche einer beliebigen positiven oder negativen Determinante entsprechen, und man findet, daſs diese Anzahl (was jedoch nicht die Endform des Resultates dieser Untersuchung ist) als Product von zwei Factoren dargestellt werden kann, wovon der erste eine sehr einfache Function der Determinante ist, welche für jede Determinante einen endlichen Werth hat, während der andere Factor durch eine Reihe ausgedrückt ist, die mit der obigen (16) zusammenfällt. Aus diesem Resultat folgt dann unmittelbar, daſs die Summe (16) nie Null sein kann, da sonst für die entsprechende Determinante die Anzahl der quadratischen Formen sich auf Null reduciren würde, während diese Anzahl wirklich immer $\geqq 1$ ist.

Aus diesem Grunde werde ich meinen früheren Beweis für die genannte Eigenschaft der Reihe (16) hier weglassen, und wegen dieses Punktes auf die erwähnten Untersuchungen über die Anzahl der quadratischen Formen verweisen (1), welche nächstens erscheinen werden, und aus welchen der zur Vervollständigung der gegenwärtigen Abhandlung erforderliche Satz, wie schon bemerkt worden, als ein bloſses Corollar hervorgeht.

---

(1) Eine vorläufige Notiz über diesen Gegenstand findet man im Crelleschen Journal Band XVIII. unter dem Titel: *Sur l'usage des séries infinies dans la théorie des nombres.*