Werk

Titel: Ueber eine zahlentheoretische Funktion.

Autor: Stern, M.

Jahr: 1858

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0055|log15

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

12.

Ueber eine zahlentheoretische Funktion.

(Von Herrn *Stern* zu Göttingen.)

In den „Monatsberichten der Akademie der Wissenschaften zu Berlin, aus dem Jahre 1850" findet man S. 36 einen Aufsatz von *Eisenstein* über eine zahlentheoretische Funktion, auf welche er bei seinen Untersuchungen über die höheren Reciprocitätsgesetze geführt wurde, worüber in einer anderen Arbeit *Eisenstein*'s (dieses Journal Bd. 39 S. 356) weitere Erörterungen vorkommen. In dem erwähnten Aufsatze giebt *Eisenstein* den Werth der Funktion an, und zeigt, dafs dieser Werth der einzige ist, der den Bedingungen entspricht, welchen die Funktion genügen soll. Die Analyse aber, die zu diesem Werthe geführt hat, und die der Verfasser als eine schwierige bezeichnet, hat er nicht mitgetheilt. Weiter bemerkt er, dafs ihn die Betrachtung dieser Funktion auf eine merkwürdige Zahlenreihe geführt habe. Er giebt eine Anzahl von Sätzen, die eben so viel Eigenschaften dieser Reihe ausdrücken; der Beweis derselben, sagt er am Schlusse, sei in derselben Analyse mit enthalten, welche zur Bestimmung der erwähnten Funktion geführt hätte.

Dieser Aufsatz wurde der Akademie den 18. Februar mitgetheilt. Schon etwas früher, in einem vom 14. Januar datirten Briefe, theilte mir *Eisenstein* die Auffindung dieser Reihe und die so eben erwähnten Eigenschaften mit, ohne jedoch der zahlentheoretischen Funktion zu gedenken, und schrieb mir noch Folgendes dabei. „Meine Beweise dieser Sätze sind ziemlich complicirt, vielleicht finden Sie einfachere, es wäre mir lieb solche zu besitzen, die sich unmittelbar aus der gegebenen Bildungsweise auf elementare Weise ergeben." Ich war damals verhindert, diesem Gegenstande meine Aufmerksamkeit zu widmen. Gegenwärtig aber hoffe ich, leider zu spät, dem Wunsche meines unvergefslichen Freundes vollständig zu entsprechen, indem ich die Eigenschaften der Reihe, wie der damit eng verbundenen Funktion aus den elementarsten Betrachtungen ableiten werde.

1.

Es seien zwei positive Zahlen m und n gegeben, man addire sie und setze die Summe $m+n$ zwischen dieselben, so erhält man die Folge

$$(1.) \quad m,\ m+n,\ n.$$

Man addire in dieser Folge wieder je zwei aufeinanderfolgende Zahlen, und setze ihre Summe zwischen dieselben, so erhält man die Folge

$$(2.) \quad m,\ 2m+n,\ m+n,\ m+2n,\ n.$$

Behandelt man diese Folge weiter auf dieselbe Weise, so erhält man

$$(3.) \quad m,\ 3m+n,\ 2m+n,\ 3m+2n,\ m+n,\ 2m+3n,\ m+2n,\ m+3n,\ n$$

und man sieht, dafs sich das Verfahren ins Unendliche fortsetzen läfst.

Die Folge (1.) nenne ich die *erste* Reihe, die Folge (2.) die *zweite* Reihe u. s. w. Alle diese ins Unbestimmte fortgesetzten Reihen sollen die ***Entwickelung*** (m, n) heifsen und m das *erste*, n das *zweite* ***Argument*** dieser Reihen. Wo es die Deutlichkeit fordert, werde ich die p^{te} Reihe auch als die p^{te} ***Entwickelungsreihe*** (m, n) bezeichnen, und die Folge m, n die ***nullte*** Entwickelungsreihe nennen. Jede in einer Reihe enthaltene Zahl heifse ein ***Glied*** dieser Reihe, eine Anzahl unmittelbar aufeinanderfolgender Glieder eine ***Gruppe.*** Jede Zahl, welche die Summe der sie einschliefsenden Zahlen ist, nenne ich ein ***Summenglied,*** jede andere Zahl ein ***Stammglied;*** ein und dieselbe Zahl kann also an gewissen Stellen ein Summenglied und an anderen ein Stammglied sein.

Aus der Bildung der Reihen ergeben sich nun unmittelbar folgende Eigenschaften derselben.

Die Zahl m kommt nur und immer nur am ***Anfange,*** die Zahl n nur und immer nur am ***Ende*** jeder Reihe vor, die Zahl $m+n$ nur und immer nur in der ***Mitte,*** weswegen sie auch das ***Mittelglied*** heifsen soll. Die Reihe der Glieder von dem ersten an bis zu dem Mittelgliede, dieses eingeschlossen, soll die ***erste Hälfte*** der Reihe heifsen, die Reihe der Glieder von dem Mittelgliede an, dieses eingeschlossen, bis zum Ende der Reihe, heifse die *zweite* Hälfte. In den Reihen, welche auf die erste folgen, sind die zwischen dem Anfangsgliede m und dem Mittelgliede enthaltenen Glieder ebenso aus diesen gebildet, wie die zwischen dem Mittelgliede und dem Endgliede n liegenden Glieder aus diesen. Zwei gleichweit von dem Mittelgliede entfernte Glieder müssen also in einander übergehen, wenn man m und n vertauscht (da das Mittelglied durch diese Vertauschung nicht geändert wird).

Ist das eine dieser Glieder $km+ln$, so mufs das andere $lm+kn$ sein; zwei solche Glieder nenne ich *symmetrische*. Die Coefficienten des ersten und zweiten Arguments in irgend einem Gliede sollen bezüglich der *erste* und *zweite* Coefficient dieses Gliedes heifsen.

Zwischen je zwei Stammgliedern steht ein Summenglied, zwischen je zwei Summengliedern ein Stammglied. Die Stammglieder nehmen die *ungeraden* Stellen in der Reihe ein, die Summenglieder die *geraden;* die Zahlen in den geraden Stellen sind daher gröfser als die unmittelbar folgenden und vorhergehenden. Daraus folgt, dafs in jeder Reihe, von den zwei Stammgliedern, welche ein Summenglied bilden, abwechselnd das vorhergehende oder das folgende das kleinere ist. Beginnt z. B. irgend eine Reihe mit den Gliedern

$$m,\ s,\ m_1,\ s_1,\ m_2,\ s_2,\ \ldots$$

so beginnt die folgende mit

$$m,\ m+s,\ s,\ m_1+s,\ m_1,\ m_1+s_1,\ s_1,\ \ldots$$

und man hat $m<s;\ s>m_1;\ m_1<s_1,\ \ldots$

Es ist also allgemein ein Glied in der Stelle $4k+3$, gröfser als die Glieder in der Stelle $4k+1$ und $4k+5$.

2.

Ist die Anzahl der Glieder in irgend einer Reihe $=k$, so ist die Anzahl der Glieder der folgenden Reihe $2(k-1)+1$. Nun ist die Anzahl der Glieder der ersten Reihe $=2+1$, also allgemein die Anzahl der Glieder in der p^{ten} Reihe $=2^p+1$.

Stellt man sich die einzelnen Glieder einer Reihe zusammen addirt vor, und nennt dies die *Summe* der Reihe, so ist leicht zu sehen, dafs die Summe einer folgenden Reihe gefunden wird, wenn man das *dreifache* der Summe der unmittelbar vorhergehenden nimmt und die Summe der Argumente $m+n$ abzieht. Denn in der folgenden Reihe kommen nicht blofs die Glieder der vorhergehenden wieder unmittelbar vor, sondern jedes derselben wird noch aufserdem doppelt wiederholt, indem es zum vorhergehenden und folgenden addirt wird; mit Ausnahme des ersten Gliedes, welches nur zum folgenden, und des letzten, welches nur zum vorhergehenden addirt wird. Bezeichnet also $S_p(m,n)$ die Summe der p^{ten} Reihe mit den Argumenten m, n, so findet sich

$$S_p(m,n) = \frac{3^p+1}{2}(m+n).$$

Im Folgenden sollen die Argumente immer *ganze* Zahlen sein, doch darf eines derselben auch Null werden.

Man hat

$$S_p(m, n) = S_p(n, m)$$
$$\frac{S_p(m', n')}{S_p(m, n)} = \frac{m'+n'}{m+n}$$
$$S_p(m+m', n+n') = S_p(m, n)+S_p(m', n')$$

Aus der letzten Gleichung folgen die speciellen Gleichungen

$$S_p(1, 1) = S_p(1, 0)+S_p(0, 1)$$
$$S_p(1, 2) = S_p(0, 1)+S_p(1, 1)$$
$$S_p(2, 3) = S_p(1, 1)+S_p(1, 2)$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

also auch

$$\frac{S_p(1, 1)}{S_p(1, 0)} = 1+\frac{S_p(0, 1)}{S_p(1, 0)} = 1+\frac{1}{1}$$
$$\frac{S_p(1, 2)}{S_p(1, 1)} = 1+\cfrac{1}{1+\frac{1}{1}}$$
$$\frac{S_p(2, 3)}{S_p(1, 2)} = 1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}}$$

u. s. w.

3.

Ich betrachte nun den besonderen Fall, wenn die beiden Argumente *der Einheit gleich sind,* also die Entwickelung (1, 1), auf welche sich, wie später gezeigt werden soll, alle übrigen Fälle zurückführen lassen. Aus den obigen allgemeinen Erörterungen ergiebt sich unmittelbar, dafs hier die Einheit *immer* und *nur* am *Anfang* und *Ende* jeder Reihe vorkommt, dafs das *Mittelglied* $= 2$ ist und dafs die *symmetrischen* Glieder *gleich* sind; so dafs die der Zahl 2 vorausgehenden Glieder sich hinter derselben in umgekehrter Ordnung wiederholen.

Es können nie zwei *gerade* Zahlen in einer Reihe unmittelbar auf einander folgen. Bezeichnen g, g', g'' irgend welche *gerade* Stammglieder, u, u', u'' irgend welche *ungerade*, G, G', G'' irgend welche *gerade* Summenglieder, U, U', U'' irgend welche *ungerade,* so müfste eine Gruppe von *zwei* geraden Gliedern, die in der p^{ten} Reihe vorkäme, entweder G, g oder g, G

sein; in beiden Fällen hätte man also eine Gruppe von *drei* geraden Gliedern, entweder g', G, g oder g, G, g' und mithin in der $p-1^{\text{ten}}$ Reihe eine Gruppe von *zwei* geraden Gliedern, g', g oder g, g', d. h. wenn in der p^{ten} Reihe eine Gruppe von zwei geraden Gliedern vorkommt, mufs auch in der $p-1^{\text{ten}}$, und mithin in jeder vorhergehenden Reihe, eine solche Gruppe vorkommen, während doch die erste, aus den Gliedern 1, 2, 1 bestehende Reihe keine solche Gruppe enthält, also überhaupt keine solche vorkommen kann.

In keiner Reihe kann eine Gruppe von *drei* Zahlen vorkommen, so beschaffen, dafs *jede* dieser Zahlen, oder *nur* die *mittlere*, *ungerade* ist. Gäbe es in der p^{ten} Reihe eine Gruppe u, u', u'', so könnte sie, wie sich versteht, nicht u, U, u' sein, sondern U, u', U'. Diese letztere Gruppe würde also die Gruppe g, U, u', U', g' bedingen und mithin müfste die $p-1^{\text{te}}$ Reihe die Gruppe g, u', g' enthalten; diese müfste G, u', G' sein, (da sie nicht g, U, g' sein kann) und würde daher die Gruppe u, G, u', G', u'' bedingen; in der $p-2^{\text{ten}}$ Reihe müfste mithin wieder eine aus drei ungeraden Gliedern bestehende Gruppe u, u', u'' vorkommen. Setzt man diesen Schlufs fort, so folgt, dafs überhaupt in den Reihen vom Range $p, p-2, p-4, \ldots$ eine Gruppe von der Form u, U', u', und in den Reihen vom Range $p-1, p-3, p-5, \ldots$ eine Gruppe von der Form G, u, G' vorkommen müfste. Da aber die zwei ersten Reihen 1, 2, 1 und 1, 3, 2, 3, 1 weder die eine noch die andere dieser Gruppen enthalten, so folgt, dafs sie überhaupt nicht vorkommen können.

Aus dem Vorhergehenden folgt, dafs von den *acht* Zusammenstellungen zu *drei* Elementen, die sich aus irgend welchen geraden Elementen g und irgend welchen ungeraden u bilden lassen, nur die drei folgenden in irgend einer Reihe als Gruppe vorkommen können, nemlich

$$guu$$
$$ugu$$
$$uug.$$

Man sieht aber zugleich, dafs nur eine dieser Gruppen sich fortwährend in der Reihe wiederholen kann und mufs. Geht man z. B. von der Gruppe guu aus, so kann die nächstfolgende weder uug noch ugu sein, weil in beiden Fällen drei ungerade Zahlen auf einander folgen würden.

Beginnt irgend eine Reihe mit ugu, so ist klar, dafs die nächste mit uug, die darauf folgende wieder mit ugu beginnen mufs u. s. w. Nun beginnt die erste Reihe wirklich mit ugu, folglich wird sich in jeder Reihe

vom Range $2p+1$ diese Gruppe von Anfang an wiederholen; und da die Zahl aller Glieder $=2^{2p+1}+1$, also durch 3 theilbar ist, so wiederholt sich diese Gruppe bis ans Ende der Reihe. Ist dagegen die Reihe vom Range $2p$, also die Anzahl der Glieder $2^{2p}+1$, so wird sich die Gruppe uug vom Anfang der Reihe an wiederholen, die Reihe wird aber mit uu schliefsen.

4.

In jeder Reihe ist die Summe der zwei äufseren von je drei aufeinander folgenden Gliedern durch das mittlere Glied theilbar. Ist das mittlere Glied ein Summenglied, so versteht sich der Satz von selbst. Ist dagegen das mittlere Glied, welches m heifsen soll, ein Stammglied, sind also die äufseren, s und s', Summenglieder, so wird m jedenfalls aus einer früheren Reihe herstammen, in welcher es Summenglied war. War es in der $p-1^{\text{ten}}$ Reihe Summenglied und dort von den Gliedern a und b eingeschlossen, $a+b=m$, so hat man in der p^{ten} Reihe die Gruppe a, s, m, s', b, also $s=a+m, s'=m+b$ und $s+s'=3m$. War m in der $p-2^{\text{ten}}$ Reihe Summenglied, so hat man, mit Beibehaltung der vorhergehenden Bezeichnung, in der $p-1^{\text{ten}}$ Reihe die Folge $s-m, m, s'-m$, und nach dem eben Bewiesenen, $s-m+s'-m=3m$, also $s+s'=5m$. Setzt man diese Betrachtung fort, so findet man allgemein Folgendes:

Wenn in der p^{ten} Reihe die Gruppe a, b, c vorkommt, und b ist in der $p-k^{\text{ten}}$ Reihe als Summenglied entstanden, so ist

$$(4.) \qquad a+c=(2k+1)b.$$

Man sieht dafs diese Formel zugleich den Fall umfafst, wenn $k=0$, also m in der p^{ten} Reihe selbst als Summenglied entstanden ist.

Umgekehrt kann man also auch aus einer gegebenen Gruppe a, b, c, in der p^{ten} Reihe finden, in welcher Reihe das Mittelglied b als Summenglied entstanden ist. Denn bezeichnet man diese Reihe durch $p-k$, so ist

$$k=\frac{a+c-b}{2b}.$$

Man findet z. B. dafs die sechste Reihe mit den Zahlen

$$1, 7, 6, 11, 5, 14, 9, 13, 4, 15, 11, \ldots$$

beginnt. Nimmt man die Gruppe 13, 4, 15, so folgt aus $\frac{13+15-4}{8}=3$, dafs die Zahl 4 in der 3^{ten} Reihe als Summenzahl entstanden ist. In der That entspringt die Gruppe 13, 4, 15 aus der Gruppe 1, 4, 3, mit welcher die dritte Reihe beginnt.

Da die geradstelligen Glieder in jeder Reihe Summenglieder sind, und das Glied, welches in der $p-1^{\text{ten}}$ Reihe die Stelle $2l$ einnimmt, in der folgenden Reihe in der $4l-1^{\text{ten}}$ Stelle erscheint, so kann man auch behaupten, dafs das $4l-1^{\text{te}}$ Glied der p^{ten} Reihe in der $p-1^{\text{ten}}$ Reihe als Summenglied entstanden ist; ebenso findet sich, dafs das $8l-3^{\text{te}}$ Glied der p^{ten} Reihe in der $p-2^{\text{ten}}$ Reihe als Summenglied entstanden ist; und allgemein, dafs das Glied, welches in der p^{ten} Reihe die Stelle $2^{t-1}2l-(2^{t-1}-1)=2^{t-1}(2l-1)+1$ einnimmt, in der Reihe $p-(t-1)$ als Summenglied entsteht. Ist also b das Glied, welches die Stelle $2^{t-1}(2l-1)+1$ einnimmt, a das vorhergehende und c das folgende, so hat man nach der Formel (4.):

$$(2t-1)b = a+c.$$

Es ist klar, dafs durch die Form $2^{t-1}(2l-1)+1$ *jede* ganze Zahl, und zwar nur auf eine einzige Weise dargestellt werden kann. Sobald mithin die Reihe p und die Stelle $2^k(2l-1)+1$ in dieser Reihe, in welcher eine Zahl vorkommt, gegeben ist, weifs man, dafs diese Zahl in der Reihe $p-k$ als Summenzahl entstanden ist. Auf den Werth von l kommt es hierbei nicht an.

Ist in einer Reihe die Gruppe $a, b, c,$ in einer andern die Gruppe α, β, γ enthalten, und steht α in derselben Stelle wie $a,$ so hat man auch $\frac{\alpha+\gamma}{\beta}=\frac{a+c}{b}$.

5.

Es können nie zwei aufeinander folgende Glieder einer Reihe einen gemeinschaftlichen Faktor haben. Es seien a, b, c drei unmittelbar auf einander folgende Glieder. Hätten b und c einen gemeinschaftlichen Faktor, so müfsten, nach der Form (4.), auch a und b diesen Faktor gemeinschaftlich haben, und aus der Fortsetzung dieser Schlufsweise würde folgen, dafs *alle* Glieder der Reihe diesen Faktor enthalten müfsten; was nicht sein kann, da das erste Glied der Reihe $=1$ ist. Der früher bewiesene Satz (§. 3), dafs nicht zwei *gerade* Zahlen in der Reihe unmittelbar auf einander folgen können, ist also ein spezieller Fall dieses allgemeineren.

Ein Summenglied b kann also nur dadurch entstehen, dafs zwei Zahlen, welche relative Primzahlen zu b sind, zusammen addirt werden. Mit anderen Worten: ***wenn in der Gruppe a, b, c die Zahl $b=a+c$ ist, so müssen a und c relative Primzahlen sein.***

6.

Eine und dieselbe Gruppe a, b kann nicht zugleich in zwei verschiedenen Reihen vorkommen. Man nehme zuerst an, es sei $a > b$, also a eine Summenzahl. Geht das Glied β dem a voraus, so ist $\beta < a$ und in der vorhergehenden Reihe findet sich die Gruppe β, b. Hier ist wieder entweder $\beta > b$ und es geht daher ein Glied $\beta' < \beta$ dem Gliede β voraus, oder es ist $\beta < b$, und es folgt dann auf b ein Glied $b' < b$. In der nächstvorhergehenden Reihe hat man also entweder die Gruppe β', β, oder die Gruppe b, b'. Man wird also jedenfalls, von einer zweigliedrigen Gruppe der vorhergehenden Reihe geführt, in welcher wenigstens das erste, oder das zweite Glied kleiner ist als das entsprechende Glied der Gruppe, von welcher man ausging. Setzt man dieses Verfahren fort, so mufs man zuletzt, nach einer bestimmten Zahl von Operationen, zu einer zweigliedrigen Gruppe kommen, in welcher entweder das erste, oder das zweite Glied der ***Einheit*** gleich ist. Man nehme nun an, die Gruppe a, b komme in der p^{ten} Reihe vor und man werde nach k Operationen zur Gruppe 1, β oder zur Gruppe β, 1 geführt, welche also zur $p-k^{\text{ten}}$ Reihe gehört. Die Gruppe 1, β kann nur am Anfang, die Gruppe β, 1 nur am Ende der Reihe stehen (und beide Gruppen müssen zugleich in der Reihe vorkommen). Fände sich nun die Gruppe a, b noch aufserdem in der q^{ten} Reihe, so müfste sich auch in der $q-k^{\text{ten}}$ Reihe die Gruppe 1, β am Anfang finden; was nicht sein kann. Dasselbe Resultat erhält man, wenn man $a < b$ voraussetzt.

Eine und dieselbe Gruppe a, b kann nicht zweimal in derselben Reihe vorkommen. Indem man sich der vorhergehenden Beweisführung bedient, läfst sich nämlich zeigen, dafs wenn in irgend einer Reihe eine zweigliedrige Gruppe doppelt vorkäme, dies auch in jeder vorhergehenden Reihe der Fall sein müfste, während doch in der ersten Reihe 1, 2, 1 keine solche Doppelgruppe existirt.

Eine bestimmte Gruppe a, b, kann also überhaupt ***nicht mehr als einmal in der Entwickelung*** (1, 1) ***vorkommen.***

Es folgt zugleich hieraus, dafs in derselben Hälfte einer Reihe nicht irgend eine Gruppe a, b, und die umgekehrte b, a vorkommen kann, weil sonst in der zweiten Hälfte dieselben Gruppen vorkommen müfsten (§. 3.); sowie dafs nicht in einer Reihe die Gruppe a, b, und in einer anderen die Gruppe b, a, vorkommen kann.

7.

Aus dem Vorhergehenden ergeben sich unmittelbar folgende Sätze:

In keiner Reihe kann eine Summenzahl mehr als einmal auf dieselbe Weise gebildet werden. Ist z. B. b die Summe von a und c, so kann die Gruppe a, b, c nicht zweimal in derselben Reihe vorkommen. Ebenso folgt, dafs nicht in derselben Hälfte einer Reihe eine Summenzahl auf dieselbe und auf umgekehrte Weise gebildet werden kann, d. h. es können nicht in derselben Hälfte einer Reihe zugleich die zwei Gruppen a, b, c und c, b, a vorkommen. Auch kann nicht in zwei verschiedenen Reihen eine Summenzahl auf dieselbe oder auf umgekehrte Weise gebildet vorkommen.

Nun sind a und c relative Primzahlen (§. 5), man hat also den Satz:

Eine Zahl (die gröfser als die Einheit ist) kann *höchstens* so oft als Summenzahl vorkommen, als es kleinere Zahlen giebt, die zu ihr *Primzahlen* sind.

8.

In der Entwickelung (1, 1) *kommt jede ganze Zahl vor.* Denn die erste Reihe beginnt mit 1, 2; die zweite mit 1, 3'; allgemein die $n-1^{\text{te}}$ mit 1, n.

In der Entwickelung (1, 1) *kommt jede Gruppe a, c vor, bei welcher a und c relative Primzahlen sind.* Da mit der Gruppe a, c jedenfalls die Gruppe c, a zugleich vorkommt, oder fehlt, so kann man immer $a > c$ setzen; im entgegengesetzten Falle hätte man nur die umgekehrte Gruppe zu betrachten. Man setze $a = kc + r$, wo $r < c$; kommt nun die Gruppe r, c in irgend einer Reihe vor, so mufs auch die Gruppe a, c vorkommen. Denn wenn in irgend einer Reihe die Gruppe r, c steht, so steht in der *ersten* folgenden die Gruppe $r + c, c$, in der *zweiten* folgenden die Gruppe $r + 2c, c$, in der k^{ten} folgenden die Gruppe $r + kc, c$. Setzt man ferner $c = k'r + r'$, wo $r' < r$, so wird ebenso bewiesen, dafs wenn die Gruppe r', r vorkommt, auch die Gruppe c, r, mithin auch die Gruppe r, c und die Gruppe a, c vorkommen mufs. Geht man so fort, so kommt man zuletzt, da die Zahlen $r, r' \ldots$ immerfort abnehmen, an eine Zahl $r_n = 1$. Eine Gruppe, in welcher ein Glied der *Einheit* gleich ist, kommt aber nach dem Vorhergehenden immer vor, welches auch die ganze Zahl sei, die das andere Glied bildet, folglich mufs auch jede Gruppe a, c vorkommen, wenn a und c *relative Primzahlen* sind; käme sie nicht vor, so könnte auch eine

bestimmte zweigliedrige Gruppe nicht vorkommen, in welcher ein Glied der Einheit gleich wäre.

Verbindet man dieses mit §. 6, so hat man also den Satz:

In der Entwickelung (1, 1) *kommt jede Zahl so oft als Summenzahl vor, als es kleinere Zahlen giebt, die zu ihr relative Primzahlen sind.* Eine Primzahl p kommt mithin $p-1$ mal als Summenzahl vor.

9.

Die letzte Reihe, in welcher die Zahl n als Summenzahl vorkommt, ist die $n-1^{te}$, *in keiner späteren kann sie als solche vorkommen.*

Dafs sie in der $n-1^{ten}$ Reihe als Summenzahl vorkommt, ist klar, denn diese Reihe beginnt mit der Gruppe 1, n, $n-1$. Sie kann aber in keiner spätern Reihe als solche vorkommen. Fände sich in einer solchen die Gruppe a, n, b und $a+b=n$, so hätte man in der vorhergehenden Reihe entweder die Gruppe a, b, $b-a$ oder $a-b$, a, b; jedenfalls wäre in der Gruppe a, b, oder $a-b$, a *eine* Zahl kleiner als die entsprechende in der Gruppe a, n, und indem man auf diese Weise immer von Reihe zu Reihe zurückgeht, mufs man zuletzt auf die Gruppe 1, 1 kommen, von der man ausging. Das *langsamste* Verfahren zu dieser letzteren Gruppe zurückzukehren ist offenbar das, wenn man von 1, n zu 1, $n-1$, dann zu 1, $n-2$ u. s. w. zurückgeht. Und da man in diesem Falle doch nur durch $n-1$ Reihen zurückzugehen braucht, so mufs man, mit der Gruppe a, n anfangend, schon früher zu 1, 1 zurückkommen.

Bezeichnet $\varphi(n)$ die Anzahl der Zahlen, die kleiner als n und zu dieser *relative Primzahlen* sind, so folgt, dafs die $n-1^{te}$ Reihe die erste ist, in welcher die Zahl n $\varphi(n)$ mal vorkommt, und dafs sie in jeder folgenden Reihe ebenso oft vorkommt.

Die Zahl n kommt also nur dann und immer $n-1$ *mal in der* $n-1^{ten}$ *Reihe vor, wenn n eine Primzahl ist.* Hierin hätte man also ein neues, freilich in der Art, wie der *Wilson*'sche Satz, praktisch unbrauchbares Mittel, die *Primzahlen* von den *zusammengesetzten* zu unterscheiden.

10.

Da eine bestimmte Gruppe a, c nur in einer einzigen Reihe vorkommt so mufs es auch möglich sein, aus der Gruppe selbst zu finden, welcher Reihe sie angehört. Den Weg hierzu zeigt die Beweisführung in §. 8. Setzt man nemlich

$$\begin{aligned} a &= kc+r \\ c &= k'r+r' \\ r &= k''r'+r'' \\ &\cdots\cdots\cdots \\ r_{m-2} &= k_m.r_{m-1}+1 \end{aligned}$$

so folgt, dafs die Gruppe a, c in der $(k+k'+k''\cdots+k_m)^{\text{ten}}$ Reihe nach derjenigen folgt, in welcher die Gruppe 1, r_{m-1} vorkommt, d. h. die Gruppe a, c kommt in der $(k+k'+k''\cdots+k_m+r_{m-1}-1)^{\text{ten}}$ Reihe vor. Nun ist

$$\frac{a}{c} = k+\cfrac{1}{k'+\cfrac{1}{k''+\cdots+\cfrac{1}{k_m+\cfrac{1}{r_{m-1}}}}}.$$

Man hat also folgende Regel:

Um zu erfahren in welcher Reihe die Gruppe a, c vorkommt, verwandele man den Quotienten $\frac{a}{c}$ in einen Kettenbruch, die Summe der Theilnenner um eine Einheit vermindert giebt die Zahl der Reihe. Die Glieder der $p-1^{\text{ten}}$ Reihe sind also so beschaffen, dafs der Quotient je zweier aufeinanderfolgenden einen Kettenbruch giebt, bei welchem die Summe der Theilnenner $=p$ ist. Die fünfte Reihe z. B. beginnt mit

$$1,\ 6,\ 5,\ 9,\ 4,\ 11,\ 7\ \ldots;$$

hier ist

$$\frac{6}{1}=6,\ \frac{6}{5}=1+\frac{1}{5},\ \frac{9}{5}=1+\frac{1}{1+\frac{1}{4}},\ \frac{9}{4}=2+\frac{1}{4},\ \frac{11}{4}=2+\frac{1}{1+\frac{1}{3}}$$

u. s. w.

Um zu erfahren, wie oft eine Zahl N in der Reihe p vorkommt, zerlege man daher N, so oft es geht, in zwei Theile a und c, die relative Primzahlen sind, und bilde aus $\frac{a}{c}$ einen Kettenbruch. Soviel solcher Kettenbrüche es giebt, bei welchen die Summe der Theilnenner nicht gröfser als p ist, so oft kommt N in der p^{ten} Reihe vor. Denn die Gruppe a, c kann spätestens in der $p-1^{\text{ten}}$ vorkommen, soviel solcher Gruppen aber in den vorhergehenden Reihen gebildet sind, so oft kommt N in einer folgenden vor.

Auch kann es keinen Kettenbruch geben, bei welchem die Summe der Theilnenner $=p$ ist, dessen reducirter Werth $\frac{a}{c}$ nicht als Gruppe a, c in

der $p-1^{\text{ten}}$ Reihe vorkäme. Ferner folgt, dafs zwei Gruppen a, c und α, γ, die zu verschiedenen Reihen gehören, niemals Kettenbrüchen entsprechen können, bei welchen die Summe der Theilnenner dieselbe ist.

11.

Bezeichnet $(m, n)_p$ die p^{te} Entwickelungsreihe (m, n) und das Symbol $(m, n)_p \pm (m', n')_p$ die Reihe, welche man erhält, wenn man die einzelnen in $(m', n')_p$ enthaltenen Glieder zu den gleichstelligen Gliedern von $(m, n)_p$ addirt oder davon abzieht, je nachdem das obere oder das untere Zeichen gilt, so hat man offenbar:

$$(m, n)_p \pm (m', n')_p = (m \pm m', n \pm n')_p ,$$

und als speciellen Fall:

$$(5.) \qquad (1, 2)_p - (1, 1)_p = (0, 1)_p .$$

Die Entwickelung $(0, 1)$ hat aber die Eigenthümlichkeit, dafs die erste Hälfte jeder Reihe $(0, 1)_{p+1}$ nichts Anderes ist, als die vorhergehende Reihe $(0, 1)_p$. So ist z. B. $(0, 1)_2 = 0, 1, 1, 2, 1$ und $(0, 1)_3 = 0, 1, 1, 2, 1, 3, 2, 3, 1,$ und es ist leicht zu sehen, dafs dies allgemein so sein mufs. Das k^{te} Glied in $(0, 1)_p$ ist also identisch mit dem k^{ten} Gliede in $(0, 1)_{p+1}$ und überhaupt mit dem k^{ten} Gliede aller Entwickelungsreihen $(0, 1)$, die nicht weniger als k Glieder haben. Ferner ist $(1, 2)_p$ nichts Anderes als die erste Hälfte der Reihe $(1, 1)_{p+1}$. Die Gleichung (5.) sagt also, dafs das k^{te} Glied in $(0, 1)_p$ die Differenz der k^{ten} Glieder in $(1, 1)_{p+1}$ und $(1, 1)_p$ ist. Setzt man aber in dieser Gleichung $p+1$ statt p, so folgt aus dem eben Gesagten, dafs auch die Differenz der k^{ten} Glieder in $(1, 1)_{p+2}$ und $(1, 1)_{p+1}$ dem k^{ten} Gliede in $(0, 1)_p$ gleich ist. Hieraus ergiebt sich also folgender Satz:

In den Entwickelungsreihen $(1, 1)$ *bilden die gleichstelligen Glieder eine arithmetische Progression, deren Differenz das gleichstellige Glied in der Entwickelung* $(0, 1)$ *ist.* Die Glieder z. B., welche in den Entwickelungsreihen $(1, 1)$ die *vierte* Stelle einnehmen, bilden die Progression 3, 5, 7, 9 ... Die Differenz ist $= 2$, wie die *vierte* Zahl in der Reihe 0, 1, 1, 2, 1 ...

Es ist klar, dafs ein Glied in $(1, 1)_p$ gröfser sein mufs, als das gleichstellige Glied in $(0, 1)_p$, das letzte Glied ausgenommen, welches in beiden Fällen $= 1$ ist. Bezeichnet man durch α, a und d beziehlich das k^{te} Glied in $(1, 1)_p$, $(1, 1)_{p+1}$ und $(0, 1)_p$, so hat man, wenn nicht $\alpha = d = 1$ ist,

$$a > d.$$

Nun ist, nach (Gleich. 5), $a - \alpha = d$, mithin $\alpha > \frac{1}{2}a$, d. h. ein Glied in der

Reihe $(1,1)_p$ ist immer gröfser als die Hälfte des gleichstelligen Gliedes der Reihe $(1,1)_{p+1}$, ausgenommen das letzte Glied in $(1,1)_p$, welches $=1$ und also gerade die Hälfte des entsprechenden Gliedes 2 in $(1,1)_{p+1}$ ist.

Sind β, γ die unmittelbar auf α folgenden Glieder, b, c die unmittelbar auf a, und e, f die unmittelbar auf d folgenden, so ist (§. 4):

$$\frac{\alpha+\gamma}{\beta} = \frac{a+c}{b} = \frac{\alpha+\gamma+d+f}{\beta+e},$$

also auch:

$$\frac{\alpha+\gamma}{\beta} = \frac{d+f}{e}.$$

12.

Mit Beibehaltung der vorhergehenden Bezeichnung kann man nun den Satz aussprechen: Es ist

$$(6.) \qquad \alpha b - a\beta = 1.$$

Es ist leicht zu zeigen, dafs diese Gleichung allgemein richtig ist, wenn sie bis zu irgend einer Reihe gilt. Ist sie nemlich unter der Voraussetzung, dafs α zur p^{ten} Reihe gehört, richtig, so entsteht aus der Gruppe α, β, in dieser Reihe, die Gruppe α, σ, β, in der Reihe $p+1$, so dafs $\sigma = \alpha+\beta$, und aus der Gruppe a, b entsteht in der $p+2^{\text{ten}}$ Reihe die Gruppe a, s, b, wo $s=a+b$. Nach der Voraussetzung müssen also die Glieder a, s, b beziehlich dieselben Stellen einnehmen, wie die Glieder α, σ, β, und man hat offenbar $\alpha s - a\sigma = 1$ und $\sigma b - s\beta = 1$, sobald $\alpha b - a\beta = 1$ ist. Man überzeugt sich aber leicht, dafs der Satz bei den ersten Entwickelungsreihen $(1,1)$ wirklich Statt hat.

Hieraus folgt ferner, dafs auch

$$(7.) \qquad \alpha e - \beta d = 1$$

ist, da $a = \alpha + d$; $b = \beta + e$. Es sind aber zugleich d und e die ***kleinsten*** zusammengehörenden Werthe, welche der Gleichung

$$\alpha x - \beta y = 1$$

Genüge leisten. Gäbe es noch kleinere x' und y', so hätte man $x' = e - k\beta$; $y' = d - k\alpha$, wo k irgend eine ganze positive Zahl wäre, mithin wäre $\alpha < d$; was nach §. 11 nicht sein kann.

13.

Ich gehe nun zur Entwickelung $(1,n)$ über, wo $n>1$ sein soll. Die k^{te} Entwickelungsreihe $(1,n)$ ist offenbar identisch mit dem Theile der $(n+k-1)^{\text{ten}}$ Entwickelungsreihe $(1,1)$, welcher die Glieder, von dem ersten

an bis zu dem ersten in dieser Reihe vorkommenden n, dieses eingeschlossen, umfafst, da dieser Theil aus den Elementen 1, n gebildet ist, mit welchen die $n-1^{te}$ Entwickelungsreihe $(1,1)$ beginnt. Alle Eigenschaften der letzteren Entwickelungsreihen, welche einem solchen Theile zukommen, gelten also auch für die Entwickelung $(1,n)$, und umgekehrt. Namentlich ist also auch im gegenwärtigen Falle in jeder dreigliedrigen Gruppe die Summe der äufseren Glieder durch das mittlere theilbar; es können nicht zwei aufeinander folgende Glieder einen gemeinschaftlichen Faktor haben, und es kann eine bestimmte zweigliedrige Gruppe nicht mehr als einmal vorkommen. Da n *mindestens* $=2$ ist, also die Entwickelung $(1,n)$ *höchstens* die erste Hälfte der Entwickelung $(1,1)$ umfafst, so kann auch bei der ersteren Entwickelung nicht zugleich eine Gruppe und die umgekehrte in derselben Reihe vorkommen; auch nicht eine Gruppe in einer, und die umgekehrte in einer anderen Reihe (§. 6).

Hier hat jede Reihe das Anfangsglied 1, das Mittelglied $1+n$, das Endglied n. Die übrigen Glieder sind sämmtlich in der Form $k+ln$ enthalten; die symmetrischen Glieder (§. 1) haben hier die Form $k+ln$ und $l+kn$. Es kann aber kein Glied von der Form $k+kn$ vorkommen, wenn es nicht das Mittelglied, also $k=1$ ist; denn nur bei der Bildung des Mittelgliedes concurriren die Elemente 1 und n auf gleiche Weise. Bei den Gliedern aber, welche zwischen 1 und $1+n$ gebildet werden, überwiegt das erste Argument $=1$ ebenso, wie bei den Gliedern welche zwischen $1+n$ und n gebildet werden, das zweite. Hieraus folgt, dafs die symmetrischen Glieder nicht gleich sein können, denn wäre $k+ln=l+kn$, so müfste $k=l$ sein. In der ersten Hälfte der Reihe ist immer $k>l$, in der zweiten $l>k$, das Mittelglied ausgenommen.

Das Anfangsglied ausgenommen, enthalten die Glieder keine Zahl, welche kleiner als n ist, dagegen kommen alle Zahlen vor, welche gröfser als n sind, da die auf das Anfangsglied folgenden Glieder in der 1^{ten}, 2^{ten} Reihe u. s. w. $1+n$, $2+n$ u. s. w. sind.

14.

Die *ersten* Coefficienten (§. 1) der Glieder der Reihe $(1,n)_p$, bis zum Mittelgliede, bilden eine Reihe, die mit $(1,1)_{p-1}$ identisch ist, die *zweiten* Coefficienten dieser Glieder bilden eine Reihe, die mit $(0,1)_{p-1}$ identisch ist. Entwickelt man die ersten Reihen

$$1,\ 1+n,\ n$$
$$1,\ 2+n,\ 1+n,\ 1+2n,\ n$$
$$1,\ 3+n,\ 2+n,\ 3+2n,\ 1+n,\ 2+3n,\ 1+2n,\ 1+3n,\ n,$$

so zeigt sich, dafs die ersten Coefficienten, bis zum Mittelgliede genommen, die Reihen

$$1,\ 1 = (1,1)_0$$
$$1,\ 2,\ 1 = (1,1)_1$$
$$1,\ 3,\ 2,\ 3,\ 1 = (1,1)_2$$

geben, die zweiten Coefficienten dagegen die Reihen

$$0,\ 1 = (0,1)_0$$
$$0,\ 1,\ 1 = (0,1)_1$$
$$0,\ 1,\ 1,\ 2,\ 1 = (0,1)_2,$$

und man sieht leicht, dafs das allgemein gelten mufs. Da nemlich die Glieder bis zum Mittelgliede aus den Elementen $1,\ 1+n$ gebildet werden, so heifst das, ihre ersten Coefficienten werden aus $1,\ 1$, und ihre zweiten aus $0,\ 1$ gebildet. Während aber die Gruppen $1,\ 1$ und $0,\ 1$ beziehlich die *nullte* Reihe der Entwickelung $(1,1)$ und $(0,1)$ bilden, so erscheinen sie hier als erste und zweite Coefficienten in der *ersten* Reihe; und so geht es weiter.

Dieselbe Erwägung zeigt, dafs vom Mittelgliede an bis zum Endgliede, die *ersten* Coefficienten eine mit $(1,0)_{p-1}$ identische Reihe, d. h. eine Reihe, welche die Glieder der Reihe $(0,1)_{p-1}$ in umgekehrter Ordnung enthält, bilden, die *zweiten* Coefficienten dagegen eine mit $(1,1)_{p-1}$ identische Reihe.

Hieraus folgt nun unmittelbar, dafs wenn eine Gruppe aus den zwei Gliedern $k+ln$ und $k'+l'n$ besteht, die Gleichung

$$(8.)\qquad kl'-k'l = 1$$

Statt findet, da hier $k,\ k',\ l,\ l'$ beziehlich an die Stelle von $\alpha,\ \beta,\ d,\ e,$ in der Gleichung (7.) treten. Es sind also l und l' die kleinsten Werthe, welche dieser Gleichung genügen, und mithin gegeben, sobald k und k' gegeben sind. Da $k,\ k',\ l$ und l' keinen gemeinschaftlichen Faktor haben können, so kann in der Entwickelung $(1,n)$ kein Glied von der Form $hk+h'kn$ vorkommen.

15.

Da $k,\ k'$ irgend eine Gruppe aus der Entwickelung $(1,1)$ bedeutet, so folgt aus §. 8, dafs diese Gruppe alle möglichen Zusammenstellungen zweier

relativen Primzahlen ausdrückt, und aus §. 6, dafs jede solche Zusammenstellung *nur einmal* vorkommt. Hieraus folgt weiter, dafs in der Entwickelung $(1, n)$ alle Zahlen von der Form $K+Ln$ vorkommen müssen, wenn K und L relative Primzahlen sind, und zwar, insofern K und L *bestimmte* Zahlen sind, jede nur einmal als Summenglied. Da die Glieder $K+Ln$ und $L+Kn$ jedenfalls zugleich vorkommen, oder nicht vorkommen, so kann man immer denjenigen dieser zwei Ausdrücke betrachten, bei welchem der erste Coefficient gröfser ist als der zweite. Ich setze daher $K>L$. Man suche nun die kleinsten Werthe, welche der Gleichung $Kx-Ly=1$ genügen; sie seien $x=L_0$, $y=K_0$, also sind auch L_0 und L die kleinsten Werthe, welche der Gleichung $Kx-K_0y=1$ genügen. Da K und K_0 relative Primzahlen sind, so mufs es jedenfalls eine Gruppe in der Entwickelung (m, n) geben, bei welcher die ersten Coefficienten K und K_0 sind; dann müssen aber nach der Gleichung (8.) die zweiten Coefficienten L und L_0 sein, d. h. es giebt ein Glied $K+Ln$.

Es kann aber ein solches Glied nur einmal als Summenglied gebildet werden. Man nehme an, die beiden Stammglieder seien $k+ln$ und $k'+l'n$, so dafs also in irgend einer Reihe die Glieder $k+ln$, $K+Ln$, $k'+l'n$ auf einander folgen. Mithin ist

$$K = k+k'; \qquad L = l+l'$$

und

$$(k+k')l'-(l+l')k' = 1$$

so dafs l' und k' die kleinsten Werthe sind, welche der Gleichung

$$(9.) \quad (k+k')x-(l+l')y = 1$$

Genüge leisten. Gäbe es nun noch eine andere Gruppe $\varkappa+\lambda n$, $K+Ln$, $\varkappa'+\lambda'n$, so dafs $K=\varkappa+\varkappa'$, $L=\lambda+\lambda'$ wäre, so hätte man auch

$$(\varkappa+\varkappa')\lambda'-(\lambda+\lambda')\varkappa' = (k+k')\lambda'-(l+l')\varkappa' = 1$$

und es wären λ' und $\varkappa'$ die kleinsten Werthe, die der Gleichung (9.) genügen. Mithin $l'=\lambda'$ $k=\varkappa'$, $k=\varkappa$, $l=\lambda$, d. h. die Gruppe $k+ln$, $k'+l'n$ käme *doppelt* vor, was nicht sein kann (§. 13).

16.

Nun wurde schon früher nachgewiesen, dafs jede Zahl N, die gröfser als n ist, in der Entwickelung $(1, n)$ vorkommen mufs. Nach dem Vorhergehenden können wir also sagen, dafs eine jede solche Zahl $N>n$ so oft

vorkommt, als es möglich ist, der Gleichung

$$(10.) \quad K+Ln = N$$

so zu genügen, dafs K und L ***relative Primzahlen*** sind. Dies kann man auch auf eine andere Weise ausdrücken.

Es seien zuerst N und n relative Primzahlen; hat man dann einen Ausdruck $K+Ln$ gefunden, welcher $=N$ ist, und ist zugleich L Primzahl zu N, so mufs auch K Primzahl zu N sein. Soviel Zahlen L es also giebt, welche kleiner als $\frac{N}{n}$ und zu N relative Primzahlen sind, so oft kann die Gleichung (10.) erfüllt werden; d. h. die Zahl N kommt in der Entwickelung $(1,n)$ so oft vor, als es Zahlen zwischen 0 und $\frac{N}{n}$ giebt, die ***relative Primzahlen*** zu N sind.

Haben N und n den gröfsten gemeinschaftlichen Faktor f, so mufs, wenn $K+Ln=N$ sein soll, auch K diesen Faktor enthalten. Man setze daher $K=fK'$, $n=fn'$, $N=fN'$, so ist $K'+Ln'=N'$. Ist L eine relative Primzahl zu N', so mufs auch K' relative Primzahl zu N' und mithin auch K' relative Primzahl zu L sein. Die letzte Gleichung wird also so oft mit der Bedingung, dafs K' und L' relative Primzahlen sind, erfüllt, als es Zahlen $L<\frac{N'}{n'}$ d. h. $L<\frac{N}{n}$ giebt, welche relative Primzahlen zu N' sind. Soll aber zugleich der Gleichung (10.) genügt werden, so mufs L auch relative Primzahl zu N sein. Man hat mithin auch in diesem Falle die Regel, dafs N so oft vorkommt, als es Zahlen zwischen 0 und $\frac{N}{n}$ giebt, welche relative Primzahlen zu N sind.

Nach einer früheren Bemerkung (§. 13) kann man auch sagen, dafs die Zahl N in der Entwickelung $(1,1)$ so oft zwischen dem Anfangsgliede und dem ersten Gliede, welches den Werth n hat, vorkommt, als es Zahlen zwischen 0 und $\frac{N}{n}$ giebt, die relative Primzahlen zu N sind.

17.

Nach dem Vorhergehenden erledigt sich nun von selbst die Entwickelung $(n,1)$, indem die Reihen dieselben Glieder enthalten, wie die entsprechenden Reihen der Entwickelung $(1,n)$; nur in umgekehrter Ordnung. Ich gehe daher sogleich zu dem allgemeinsten Falle über, nemlich zur Entwickelung (m,n). Ich setze aber hierbei voraus, dafs m und n keinen gemeinschaftlichen Faktor haben; wäre nemlich ihr gröfster gemeinschaftlicher

Faktor $= p$, und zwar $m = pm'$, $n = pn'$, wären also m' und n' relative Primzahlen, so brauchte man nur die Entwickelung (m', n') zu betrachten; multiplicirte man dann jedes Glied dieser Entwickelung mit p, so hätte man die gesuchte Entwickelung (m, n).

In der Entwickelung $(1, 1)$ kommt irgendwo, wie früher bewiesen, die Gruppe m, n vor; mithin kann man auch die Entwickelung (m, n) als Bruchstück der Entwickelung $(1, 1)$ ansehen. Alle diesem Bruchstücke zukommenden Eigenschaften gelten also auch für die Entwickelung (m, n), und umgekehrt.

Zu den schon in §. 1 entwickelten Eigenschaften der Reihe (m, n) setze ich zunächst noch Folgendes hinzu. Die symmetrischen Glieder können *nicht gleich* sein, da kein Glied von der Form $km + kn$ vorkommen kann, sobald $k > 1$ ist, was ebenso bewiesen wird, wie es bei der Entwickelung $(1, n)$ geschah (§. 13). Ferner läfst sich ebenso wie dort (§. 14) zeigen, dafs die ersten Coefficienten der Entwickelung $(m, n)_p$ bis zu dem Mittelgliede, eine mit $(1, 1)_{p-1}$, die zweiten Coefficienten eine mit $(0, 1)_{p-1}$ identische Reihe bilden. Hier kommen aber nicht, wie in der Entwickelung $(1, n)$ *alle* Zahlen vor die über einer gewissen Grenze liegen, sondern nur solche, die in der Form $km + ln$ enthalten sind. Es kommen aber alle in dieser Form enthaltenen Zahlen, bei welchen k und l relative Primzahlen sind, und zwar jede nur *einmal*, als Summenzahl vor, während solche Zahlen, wo k und l einen gemeinschaftlichen Faktor haben, nicht vorkommen können; was ebenso wie bei der Entwickelung $(1, n)$ bewiesen wird. Mithin kommt jede Zahl N so oft in der Entwickelung (m, n) vor, als es möglich ist, sie in der Form $km + ln$ darzustellen, so dafs k und l relative Primzahlen sind, und es läfst sich daher die Anzahl der Darstellungen der Zahl N auf eine einfache Weise ausdrücken.

Ich mufs, um dies nachzuweisen, einige Worte über die Auflösung der Gleichung

$$(11.) \qquad mx + ny = c$$

einschalten, wo sowohl m, n, als x, y, *ganze positive* Zahlen sein sollen. Hier sind m und n, der Voraussetzung gemäfs, *relative Primzahlen.* Man löse nun zuerst die Gleichung

$$nx - my = 1$$

auf. Es seien $x = m_0$ und $y = n_0$ die kleinsten zusammengehörenden Werthe, welche dieser Gleichung genügen. Man bilde alsdann die zwei Brüche $\frac{m_0}{m} c$

und $\frac{n_0}{n}c$, von welchen der erste der gröfsere ist und bezeichne beziehlich durch $E\left(\frac{m_0}{m}c\right)$ und $E\left(\frac{n_0}{n}c\right)$ die gröfste in denselben enthaltene ganze Zahl. Die sämmtlichen Auflösungen der Gleichung (11.) erhält man dann durch die Formel

$$x = nc_0 - n_0 c; \quad y = m_0 c - mc_0$$

wo c_0 jede ganze Zahl bezeichnet, welche gröfser als $\frac{n_0}{n}c$ und kleiner als $\frac{m_0}{m}c$ ist, so dafs man allmälig

$$c_0 = E\left(\frac{n_0}{n}c\right)+1, \quad E\left(\frac{n_0}{n}c\right)+2, \quad \ldots$$

zu setzen hat; wo als letzter Werth von c_0 entweder $E\left(\frac{m_0}{m}c\right)$ oder $E\left(\frac{m_0}{m}c\right)-1$ zu nehmen ist, je nachdem $\frac{m_0}{m}c$ ein Bruch oder eine ganze Zahl ist. Je nachdem $\frac{m_0}{m}c$ ein Bruch oder eine ganze Zahl ist, ist also die Anzahl der Auflösungen der Gleichung (11.) entweder

$$E\left(\frac{m_0}{m}c\right)-E\left(\frac{n_0}{n}c\right) \quad \text{oder} \quad E\left(\frac{m_0}{m}c\right)-E\left(\frac{n_0}{n}c\right)-1.$$

Dafs nemlich diese Werthe von x und y der Gleichung (11.) genügen, zeigt die unmittelbare Substitution; sollen sie aber zugleich positiv sein, so ist es nothwendig und hinreichend, dafs $c_0 > \frac{n_0}{n}c$ und $c_0 < \frac{m_0}{m}c$.

Ist nun noch aufserdem die Bedingung gestellt, dafs x und y relative Primzahlen sein sollen, so darf man nur solche Werthe für x und y setzen, bei welchen c und c_0 relative Primzahlen werden. Sind umgekehrt c und c_0 relative Primzahlen, so müssen auch x und y relative Primzahlen sein. Aus den Werthen von x und y folgt nemlich

$$m_0 x + n_0 y = c_0.$$

Hätten nun x und y den gemeinschaftlichen Factor f, so müfste dieser auch in c_0 und mithin auch in c enthalten sein. Sobald also x und y relative Primzahlen sein sollen, hat die Gleichung (11.) so viel Auflösungen, als es ganze Zahlen zwischen $\frac{n_0}{n}c$ und $\frac{m_0}{m}c$ giebt, welche relative Primzahlen zu c sind.

18.

Da die Zahl N so oft als Summenzahl in der Entwickelung (m, n) vorkommt, als es möglich ist, der Gleichung

$$mk + nl = N$$

durch Werthe von k und l zu genügen, welche relative Primzahlen sind, so folgt aus dem Vorhergehenden unmittelbar, dafs diese Zahl so oft vorkommt, als es relative Primzahlen zu N zwischen $\frac{n_0}{n}N$ und $\frac{m_0}{m}N$ giebt; insofern, wie früher, m_0 und n_0 die kleinsten Lösungen der Gleichung $nm_0 - mn_0 = 1$ bedeuten. Dies ist einer der *Eisenstein*schen Sätze.

Ist $m = 1$, so ist auch $m_0 = 1$ und $n_0 = n-1$; die Zahl N kommt demnach in der Entwickelung $(1, n)$ so oft als Summenzahl vor, als es relative Primzahlen zu N zwischen $\frac{n-1}{n}N$ und N giebt. Da aber jeder relativen Primzahl α eine andere $N-\alpha$ entspricht, so dafs $N-\alpha$ zwischen Null und $\frac{N}{n}$ liegt, wenn α zwischen $\frac{n-1}{n}N$ und N liegt, so kann man auch sagen, dafs die Zahl N so oft vorkommt, als es relative Primzahlen zu ihr zwischen Null und $\frac{N}{n}$ giebt; wie es früher in §. 16 angegeben wurde. Die allgemeine Regel umfafst zugleich den Fall, wenn $m = n = 1$; denn alsdann ist $m_0 = 2$, $n_0 = 1$. Die Zahl N kommt also in der Entwickelung $(1, 1)$ so oft als Summenzahl vor, als es relative Primzahlen zu ihr zwischen N und $2N$, d. h. also, zwischen 0 und N, giebt, was mit der früheren Regel (§. 8) übereinstimmt.

19.

Setzt man noch immer

$$mk + ln = N$$

und bezeichnet irgend welche der Zahlen die zwischen $\frac{n_0}{n}N$ und $\frac{m_0}{m}N$ liegen und zu N Primzahlen sind, durch N_0, so ist (§. 17):

$$k = nN_0 - n_0N; \qquad l = m_0N - mN_0.$$

Ist $k'm + l'n$, $k''m + l''n$ die Gruppe durch deren Summation N entstanden ist, so hat man

$$m(k' + k'') + n(l' + l'') = N.$$

Multiplicirt man diese Gleichung mit k'' und berücksichtigt die Gleichung

$$k'l'' - k''l' = 1,$$

so findet sich:

$$(k' + k'')k''m + (k' + k'')l''n - n = k''N,$$

d. h.

$$(k' + k'')(k''m + l''n) \equiv n \pmod{N}$$

oder

$$\frac{k'+k''}{n}(k''m+l''n) \equiv 1 \pmod{N}.$$

Aus

$$k = nN_0 - n_0 N$$

folgt aber

$$N_0 \equiv \frac{k'+k''}{n} \pmod{N}$$

also auch

$$N_0(k''m+l''n) \equiv 1 \pmod{N}.$$

Nun wurde vorausgesetzt, dafs man die dreigliedrige Gruppe

$$k'm+l'n, \quad N, \quad k''m+l''n$$

hat, mithin ist die unmittelbar auf N folgende Zahl der Werth von $\frac{1}{N_0} \pmod{N}$.

Dies ist ein zweiter Satz von *Eisenstein*, zunächst für den Fall bewiesen, wenn N eine Summenzahl ist; woraus sich aber dann von selbst ergiebt, dafs er allgemein gültig ist. Denn aus der dreigliedrigen Gruppe, in welcher das Mittelglied N Summenzahl ist, entsteht in jeder folgenden Reihe eine Gruppe $\alpha, N, \beta,$ wo $\alpha = k'm+l'n+sN$ und $\beta = k''m+l''n+tN$ sein mufs, also $\beta \equiv k''m+l''n \pmod{N}$.

Da $k'm+l'n \equiv -(k''m+l''n) \pmod{N}$ ist, so läfst sich auch sagen, dafs die Zahl, welche dem N unmittelbar vorausgeht, der Werth von $-\frac{1}{N_0} \pmod{N}$ ist, also $(k'm+l'n)(N-N_0) \equiv 1 \pmod{N}$. Mithin ist, nach dem bekannten Kunstausdrucke (Disq. ar. 77), N_0 der numerus socius von $k''m+l''n$ und $N-N_0$ der numerus socius von $k'm+l'n$.

20.

Nach §. 16 kommt in der Entwickelung (1, 2) jede Zahl N so oft als Summenzahl vor, als es relative Primzahlen zu ihr zwischen 0 und $\frac{N}{2}$ giebt. Die der Zahl unmittelbar vorausgehenden und folgenden Zahlen bilden also das vollständige Restsystem der relativen Primzahlen zum Modulus N. Nun ist hier $m=1$, $n=2$, also $m_0=1$, $n_0=1$, und es bedeutet daher N_0 jede relative Primzahl zu N zwischen $\frac{N}{2}$ und N. Mithin $N_0 > \frac{N}{2}$, $N-N_0 < \frac{N}{2}$, es folgen daher auf N die Zahlen, deren numerus socius gröfser als $\frac{N}{2}$ ist, während die Zahlen, deren numerus socius kleiner als $\frac{N}{2}$ ist, der Zahl N vorausgehen. Dies ist der letzte *Eisenstein*sche Satz.

Nach dem Vorhergehenden ist es leicht ihn zu verallgemeinern. Die Entwickelung (1, 1) stimmt in der ersten Hälfte jeder Reihe mit der Entwickelung (1, 2) zusammen; in der zweiten Hälfte kommen alle Glieder in umgekehrter Ordnung vor. Demnach bilden in der Entwickelung (1, 1) sowohl die N unmittelbar vorausgehenden, wie die unmittelbar folgenden Zahlen, das ganze Restsystem der relativen Primzahl zum Modulus N, und zwar in der Weise, dafs eine vorausgehende Zahl in der ersten oder zweiten Hälfte der Reihe vorkommt, je nachdem ihr numerus socius kleiner oder gröfser als $\frac{N}{2}$ ist, während bei den nachfolgenden Zahlen das umgekehrte Verhältnifs Statt findet.

Dies führt zugleich zur Beantwortung einer in diesem Gebiete nicht uninteressanten Frage. Da nemlich früher bewiesen wurde, dafs in der Entwickelung (1, 1) jede Gruppe a, b zugleich mit der umgekehrten b, a in irgend einer Reihe vorkommt, sobald a und b relative Primzahlen sind, und zwar nur einmal, so kann man fragen, wie sich entscheiden lasse, ob die Gruppe a, b in der ersten, oder in der zweiten Hälfte der Reihe vorkommt? Die Antwort lautet: das erstere oder das letztere wird Statt finden, je nachdem der numerus socius von a nach dem Modulus $a+b$ kleiner oder gröfser als $\frac{a+b}{2}$ ist. Dies in Verbindung mit §. 10 zeigt also, dafs sich für jede gegebene Gruppe a, b bestimmen läfst, nicht blofs in welcher Reihe, sondern zugleich in welcher Hälfte der Reihe sie vorkommt.

Bei der Entwickelung $(1, n)$ ist, wie schon bemerkt (§. 18), $m_0 = 1$, $n_0 = n-1$; also liegt N_0 zwischen $\frac{n-1}{n}N$ und N; die zu N relativen Primzahlen stehen also unmittelbar vor oder nach N, je nachdem ihr numerus socius kleiner oder gröfser als $\frac{N}{n}$ ist, im letzteren Falle sind sie zugleich gröfser als $\frac{n-1}{n}N$. Umgekehrt verhält es sich natürlich bei der Entwickelung $(n, 1)$.

Bei der allgemeinen Entwickelung (m, n) liegt N_0 zwischen den Grenzen $\frac{n_0}{n}N$ und $\frac{m_0}{m}N$. Man hat also folgende allgemeine, die früheren speciellen Fälle zugleich umfassende Regel: die zu N relativen Pimzahlen, deren numerus socius zwischen $\frac{n_0}{n}N$ und $\frac{m_0}{m}N$ liegt, folgen unmittelbar auf N, dagegen

gehen diejenigen unmittelbar voraus, deren numerus socius zwischen $\left(\frac{m-m_0}{m}\right)N$ und $\left(\frac{n-n_0}{n}\right)N$ liegt.

21.

Zum Abschlufs dieses Theils der Untersuchung soll noch gezeigt werden, wie sich finden läfst, in welcher Entwickelungsreihe (m, n) das Glied $km+ln$ als Summenglied gebildet wird; was, wie in (§. 15) bewiesen wurde, nur in einer bestimmten Reihe Statt hat. Je nachdem $k>l$ oder $k<l$ kommt dieses Glied in der ersten oder zweiten Hälfte der Reihe vor (§. 13). Man setze zuerst $k>l$ und nehme an, dafs $km+ln$ die Summe des vorhergehenden Gliedes $k'm+l'n$ und des folgenden $k''m+l''n$ ist. Es ist also

$$k'l-kl' = 1,$$
$$k''l-kl'' = -1,$$

und zwar sind in der ersten Gleichung k' und l' in der zweiten k'' und l'' die kleinsten zusammengehörenden Werthe, welche diesen Gleichungen genügen. Es sei $\frac{k}{l}$ der Werth des Kettenbruchs $a+\frac{1}{a_1+\cdots+\frac{1}{a_{m-1}+\frac{1}{a_m}}}$ und $\frac{k_0}{l_0}$ der unmittelbar vorhergehende Näherungswerth, mithin

$$k_0l-kl_0 = -1$$

und k_0, l_0 die kleinsten dieser Gleichung genügenden Werthe. Gilt daher das obere Zeichen, so setze man $k'=k_0$ und $l'=l_0$, folglich $k''=k-k_0$, $l''=l-l_0$, gilt dagegen das untere, so ist $k''=k_0$, $l''=l_0$ und $k'=k-k_0$, $l'=l-l_0$. Da hiernach k' und k'' bekannt sind, so hat man nur zu fragen, in welcher Reihe diese Gröfsen als erste Coefficienten zweier auf einander folgender Glieder vorkommen; ist diese Reihe gefunden, so weifs man, dafs in der nächstfolgenden $km+ln$ als Summenglied vorkommt. Nun bilden die ersten Coefficienten der Reihe $(m, n)_p$ bis zum Mittelgliede dieselbe Reihe wie $(1, 1)_{p-1}$ (§. 17); man hat also nur zu fragen, in welcher Entwickelungsreihe $(1, 1)$ die Gruppe k', k'' vorkommt. Dies findet sich aber, indem man den Quotienten $\frac{k'}{k''}$ in einen Kettenbruch verwandelt und die um eine Einheit verminderte Summe der Theilnenner nimmt (§. 10). Ist also diese Summe p, so kommen k', k'' als erste Coefficienten zweier auf einander folgender Glieder in der Reihe $(m, n)_p$ vor, und mithin das Glied $km+ln$ in der Reihe $(m, n)_{p+1}$.

Da $\frac{k'}{k''}$ entweder $\frac{k_0}{k-k_0}$ oder $\frac{k-k_0}{k_0}$ ist, und die Summe der Theilnenner des entsprechenden Kettenbruchs dieselbe bleibt, welchen dieser zwei Brüche man in einen Kettenbruch entwickeln mag, so kann man sich immer an den letzteren Bruch halten. Da aber

$$\frac{k-k_0}{k_0} = a_m - 1 + \frac{1}{a_{m-1} + \cdots + \frac{1}{a_1 + \frac{1}{a}}}$$

ist, so mufs

$$a + a_1 + \cdots + a_{m-1} + a_m - 1 = p$$

oder

$$a + a_1 + \cdots + a_{m-1} + a_m = p + 1$$

sein. Man hat also folgende einfache Regel:

Um zu erfahren in welcher Entwickelungsreihe (m, n) das Glied $km + ln$ vorkommt, verwandle man $\frac{k}{l}$ in einen Kettenbruch, und berechne die Summe der Theilnenner, dies ist die gesuchte Zahl.

Im Vorhergehenden wurde $k > l$ angenommen, wäre $k < l$, so käme das Glied $km + ln$ in der zweiten Hälfte der Reihe vor, dann müfste in der ersten Hälfte das Glied $lm + kn$ vorkommen, und um die Reihe zu finden, in welcher das letztere Glied sich befindet, hätte man $\frac{l}{k}$ in einen Kettenbruch zu verwandeln; da es aber in Beziehung auf die Summe der Theilnenner vollkommen gleichgültig ist, wenn man statt dessen $\frac{k}{l}$ in einen Kettenbruch verwandelt, so bleibt die Regel dieselbe wie im vorhergehenden Falle.

Es folgt hieraus der Satz, dafs das Glied $km + ln$ in der Reihe (m, n) als Summenglied erscheint, wenn die Gruppe k, l in der Reihe $(1, 1)_{p-1}$ steht, was sich auch schon daraus ergiebt, dafs diese Summe $= k + l$ wird, wenn $m = n = 1$ ist.

Da die *geraden* Glieder in jeder Reihe Summenglieder sind, so hat man auch noch den Satz:

Wenn man die Quotienten des ersten und zweiten Coefficienten jedes geraden Gliedes in der Entwickelung $(m, n)_p$ in einen Kettenbruch verwandelt, so giebt die Summe der Theilnenner in allen diesen Kettenbrüchen denselben Werth p.

22.

Es läfst sich nun ohne Schwierigkeit die Funktion finden, welche folgenden drei Bedingungsgleichungen genügen soll, nemlich

$$\text{(a.)} \quad f(m, n) = f(m, m+n) + f(m+n, n)$$
$$\text{wenn} \quad m+n < \lambda,$$
$$\text{(b.)} \quad f(m, n) = n$$
$$\text{wenn} \quad m+n = \lambda,$$
$$\text{(c.)} \quad f(m, n) = 0$$
$$\text{wenn} \quad m+n > \lambda,$$

wo m und n *ganze positive* Zahlen sind und λ eine ***ungerade Primzahl*** ist. Es wird hierbei zunächst vorausgesetzt, dafs m und n ***relative Primzahlen*** sind.

Entwickelt man $f(m, n)$ nach der Gleichung (a.), so findet sich

$$\begin{aligned} f(m, n) &= f(m, m+n) + f(m+n, n) \\ &= f(m, 2m+n) + f(2m+n, m+n) + f(m+n, m+2n) + f(m+2n, n) \end{aligned}$$

u. s. w.

Schreibt man hier die in jeder Reihe unter dem Funktionszeichen vorkommenden Ausdrücke in der Ordnung, wie sie auf einander folgen, nebeneinander, indem man jedoch zwei unmittelbar auf einander folgende Glieder, welche dieselbe Form haben, nur einmal setzt, so erhält man

$$m,\ n$$
$$m,\ m+n,\ n$$
$$m,\ 2m+n,\ m+n,\ m+2n,\ n$$

u. s. w.

d. h. man erhält die Entwicklungsreihen (m, n). Umgekehrt kann man also aus diesen Entwickelungsreihen die Entwickelung von $f(m, n)$ ableiten, indem man sich alle Glieder, das erste und letzte abgerechnet, doppelt geschrieben vorstellt, dann je zwei auf einander folgende Glieder unter das Funktionszeichen setzt, und endlich alle hieraus entstehenden Ausdrücke addirt.

Dies gilt aber nur so lange, als es überhaupt noch erlaubt ist, die Funktion $f(m, n)$ nach der Gleichung (a.) zu entwickeln. Sobald man an eine Entwickelung gekommen ist, in welcher ein Ausdruck $f(km+ln, k'm+l'n)$ sich zeigt, so dafs $(k+k')m+(l+l')n = \lambda$ ist, darf derselbe natürlich nicht mehr weiter nach (a.) entwickelt werden, da er vielmehr $= (l+l')n$ ist. Ist

aber $(k+k')m+(l+l')n > \lambda$, so mufs der correspondirende Ausdruck $f(km+ln, k'm+l'n) = 0$ gesetzt werden, damit den Bedingungsgleichungen (b.) und (c.) entsprochen werde.

Man kann aber jedenfalls, vermöge der Bedingungsgleichung (a.), die Entwickelung von $f(m, n)$ so weit treiben, bis man entweder an einen Ausdruck $f(km+ln, k'm+l'n)$ kommt, der den Werth $(l+l')n$ hat, weil $(k+k')m+(l+l')n = \lambda$, oder an einen Ausdruck von dieser Form, der $= 0$, also ganz unbeachtet zu lassen ist, weil $(k+k')m+(l+l')n > \lambda$. Der Werth von $f(m, n)$ ist also ein vollkommen bestimmter.

Es sollen auch hier die Gröfsen m, n die *Argumente* der Funktion $f(m, n)$ heifsen. Man betrachte nun zunächst den einfachsten Fall, wenn $m = 1$, $n = 2$. Da λ eine Primzahl ist, so wird solche in der Entwickelung $(1, 2)$ so oft gebildet, als es ganze Zahlen zwischen Null und $\frac{1}{2}\lambda$ giebt (§. 16). Jedesmal also, wenn man in der Entwickelung $(1, 2)$ an eine Gruppe α, $\lambda - \alpha$ kommt, hat man, dieser entsprechend, in der Entwickelung von $f(1, 2)$ statt $f(\alpha, \lambda - \alpha)$ den Werth $\lambda - \alpha$ zu setzen. Eine jede solche Gruppe kommt aber nur *einmal* vor (§. 13). Bezeichnet man daher die übrigen Gruppen in der Entwickelung $(1, 2)$, bei welchen die Summe der zwei Glieder der Gruppe $= \lambda$ ist, durch α', $\lambda - \alpha'$; α'', $\lambda - \alpha''$; u. s. w., so mufs

$$f(1, 2) = \lambda - \alpha + \lambda - \alpha' + \lambda - \alpha'' + \cdots$$

sein, da die übrigen Funktionen, welche noch in der Entwickelung $f(1, 2)$ vorkommen können, so beschaffen sein müssen, dafs die Summe ihrer Argumente gröfser als λ ist, mithin diese Funktionen $= 0$ sind.

Also z. B. wenn man den Werth von $f(1, 2)$ für den Modulus $\lambda = 5$ sucht, so hat man, der Reihe 1, 3, $2 = (1, 2)$ entsprechend:

$$f(1, 2) = f(1, 3) + f(3, 2) = f(1, 3) + 2.$$

Jetzt kann man in der Reihe 1, 3, 2 die Zahl 2 ganz weglassen; aus 1, 3 folgt die weitere Entwickelung 1, 4, 3, also $f(1, 3) = f(1, 4) + f(4, 3) = 4$, mithin $f(1, 2) = 6$ oder, wenn man nur den Rest nach dem Modulus 5 berücksichtigt, $f(1, 2) = 1$. Sowie nun hier nur die Zusammenstellungen $3+2 = 5$, $1+4 = 5$ zu machen waren, um daraus $f(1, 2) = f(3, 2) + f(1, 4)$ zu finden, so sind überhaupt, wenn der Werth von $f(1, 2)$ nach irgend einem Modulus zu bestimmen ist, nur aus den Zahlen, welche kleiner als dieser Modulus λ sind, alle Zusammenstellungen zu zweien zu machen, so dafs die Summe der zwei Zahlen $= \lambda$ ist. Die einzige Schwierigkeit besteht darin,

dafs entschieden werden mufs, welche von den beiden Zahlen in die erste Stelle zu setzen ist, da, wenn $\alpha+\beta=\lambda$ ist, es darauf ankommt, ob $f(\alpha,\beta)=\beta$ oder $f(\beta,\alpha)=\alpha$ ist. Hierauf ist aber schon früher die Antwort gegeben. Denn es wurde nachgewiesen, dafs in der Entwickelung (1, 2) immer diejenige der zwei Zahlen α und β in zweiter Stelle steht, deren numerus socius gröfser als $\frac{\lambda}{2}$ ist (§. 20); mit anderen Worten: in zweiter Stelle stehen die Zahlen, welche der Congruenz $x\equiv\frac{1}{r}$ (mod. λ) entsprechen, wo r alle ganzen Zahlen von $r=\frac{\lambda+1}{2}$ bis $r=\lambda-1$ bedeutet, und man hat mithin

$$f(1,2)\equiv\Sigma\frac{1}{r}\pmod{\lambda},$$

wo sich die Summation auf die oben genannten Werthe von r bezieht.

Es ist nun leicht auch das allgemeine Resultat anzugeben, wenn man das, was früher über die Entwickelung (m, n) gesagt wurde, berücksichtigt. Soll nemlich $f(m, n)$ bestimmt werden, so hat man nur zu suchen, wie oft λ als Summe zweier Ausdrücke von der Form $km+ln$ und $k'm+l'n$ dargestellt werden kann, so dafs $kl'-k'l=1$ ist; jede solche Gruppe giebt, wenn in der Entwickelung (m, n) das Glied $km+ln$ zuerst steht, den Theil $k'm+l'n$ des Werthes von $f(m, n)$. Solcher Gruppen, welche λ zur Summe haben, giebt es aber so viele, als es ganze Zahlen r zwischen den Grenzen $\frac{n_0}{n}\lambda$ und $\frac{m_0}{m}\lambda$ giebt, die Buchstaben m_0 und n_0 in ihrer früheren Bedeutung genommen (§. 18). Um noch zu entscheiden, ob $km+ln$ oder $k'm+l'n$ zuerst stehe, hat man nur zu bemerken, dafs diejenige Zahl in zweiter Stelle steht, deren numerus socius $>\frac{n_0}{n}\lambda$ und $<\frac{m_0}{m}\lambda$. Setzt man also wieder $x\equiv\frac{1}{r}$ (mod. λ), so ist

$$f(m, n)\equiv\Sigma\frac{1}{r}\pmod{\lambda};$$

wo r zwischen den angegebenen Grenzen zu nehmen ist. Dies ist der ***Eisenstein*sche** Satz.

Ist λ keine ***Primzahl***, so sind von den zwischen den angegebenen Grenzen enthaltenen Zahlen nur diejenigen zu nehmen, die ***relative Primzahlen*** zu λ sind.

Bleiben die Bedingungsgleichungen (a.) und (c.) dieselben, und man hat dagegen statt der Bedingungsgleichung (b.) die andere $f(m, n)=F(n)$

für den Fall $m+n=\lambda$, so bringt dies in der früheren Betrachtung nur die Aenderung hervor, dafs jetzt eine jede Gruppe α, β nicht mehr den Beitrag β, sondern $F(\beta)$ zum Werthe von $f(m,n)$ liefert. Man hat also

$$f(m,n) \equiv \Sigma F\frac{1}{r} \pmod{\lambda},$$

wo wieder r durch die Congruenz $x \equiv \frac{1}{r} \pmod{\lambda}$ und die Bedingung $r > \frac{n_0}{n}\lambda$, $r < \frac{m_0}{m}\lambda$ bestimmt wird. Auch dies hat ***Eisenstein*** angegeben.

Es wurde bis jetzt vorausgesetzt, dafs m und n ***relative Primzahlen*** sind; hätten sie einen gemeinschaftlichen Faktor, so müfste $f(m,n)$ für die Primzahl λ als Modulus immer Null sein, da kein in der Entwickelung (m,n) vorkommendes Glied $km+ln$ dem Werthe λ gleich sein könnte.

Göttingen, im Juli 1855.