10.

Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen.

(Von Herrn *E. E. Kummer,* Professor an der Universität zu Breslau.)

Das Reciprocitätsgesetz für die quadratischen Reste erstreckt sich bekanntlich nicht auf die Primzahl 2, für welche ein besonderer Satz lehrt, ob sie quadratischer Rest einer gegebenen Primzahl sei, oder Nichtrest. Eben so ist von dem Reciprocitätsgesetze für die cubischen Reste die Primzahl 3 ausgenommen; nebst den beiden complexen Primfactoren derselben $1-\alpha$, $1-\alpha^2$, wo α eine dritte Wurzel der Einheit bezeichnet. Für die höheren Potenzreste, welche hier nur für den Fall in Betracht kommen sollen, wo der Potenz-Exponent λ eine ***Primzahl*** ist, sind ebenfalls, aufser dem allgemeinen Reciprocitätsgesetze, Ergänzungssätze nöthig, welche entscheiden, ob der Potenz-Exponent λ und die aus λten Wurzeln der Einheit gebildeten Primfactoren desselben, $1-\alpha$, $1-\alpha^2$, ... $1-\alpha^{\lambda-1}$, für eine gegebene complexe Primzahl λte Potenzreste sind, oder zu welcher Classe der Nichtreste sie gehören. Auch kommen für diese höheren Potenzreste noch die complexen Einheiten hinzu, für welche die Untersuchung noch besonders anzustellen ist. Die Aufgabe, deren vollständige Lösung ich in dem Folgenden geben werde, besteht also darin, die Werthe der auf λte Potenzreste sich beziehenden Symbole

$$\left(\frac{\lambda}{f(\alpha)}\right), \quad \left(\frac{1-\alpha^k}{f(\alpha)}\right) \quad \text{und} \quad \left(\frac{\varepsilon(\alpha)}{f(\alpha)}\right)$$

zu finden, wo α eine λte Wurzel der Einheit, $\varepsilon(\alpha)$ eine beliebige complexe Einheit und $f(\alpha)$ eine complexe Primzahl bedeutet; welche eine wirkliche oder eine ideale sein kann. Die Bedeutung des Symbols $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ ist durch die Congruenz

$$\left(\frac{\varphi(\alpha)}{f(\alpha)}\right) \equiv \varphi(\alpha)^{\frac{Nf(\alpha)-1}{\lambda}} \equiv \alpha^i, \qquad \text{Mod. } f(\alpha),$$

definirt, in welcher $Nf(\alpha)$ die ***Norm*** von $f(\alpha)$ bedeutet. Für den Fall, dafs $\varphi(\alpha)$ ***ideal*** ist, welcher jedoch vorläufig, da $\varphi(\alpha)$ nur einen der drei Werthe λ, $1-\alpha^k$ oder $\varepsilon(\alpha)$ haben soll, nicht in Betracht kommt, wird diese Definition

dahin erweitert, dafs man statt $\varphi(\alpha)$ diejenige Potenz von $\varphi(\alpha)$ nimmt, welche zu einer wirklichen complexen Zahl wird, wenn die Hte Potenz es ist. So hat das Symbol $\left(\frac{\varphi(\alpha)^H}{f(\alpha)}\right)$ nach der obigen Definition einen ganz bestimmten Sinn, und es ist sodann $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ nach der Gleichung

$$\left(\frac{\varphi(\alpha)^H}{f(\alpha)}\right) = \left(\frac{\varphi(\alpha)}{f(\alpha)}\right)^H$$

zu definiren; welche immer einen bestimmten Werth dafür giebt, wenn H nicht durch λ theilbar ist. Für diesen Fall aber, welcher, wie ich anderweit gezeigt habe, nur dann vorkommen kann, wenn λ eine von den Ausnahmszahlen ist, für welche eine der ersten $\frac{1}{2}(\lambda-3)$ *Bernoulli*schen Zahlen in ihrem Zähler λ selbst als Factor enthält, ist die gegebene Definition unzureichend. Der Exponent derjenigen Potenz von α, welcher $\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ gleich ist, heifst der *Index* von $\varphi(\alpha)$ für den Mod. $f(\alpha)$ und soll in dem Folgenden durch Ind. $\varphi(\alpha)$ bezeichnet werden, so dafs die vorliegende Aufgabe auch so ausgedrückt werden kann: Die Werthe von

$$\text{Ind. } \lambda, \quad \text{Ind. } (1-\alpha^\lambda) \quad \text{und} \quad \text{Ind. } \varepsilon(\alpha)$$

zu finden, für den Mod. $f(\alpha)$.

Es werden hierbei zwei Fälle zu unterscheiden und besonders zu behandeln sein; nämlich *erstens* der Fall, wo $f(\alpha)$ eine complexe Primzahl ist, deren Norm $Nf(\alpha) = p$ eine Primzahl von der Form $\nu\lambda + 1 = p$ ist, in welchem Falle ich $f(\alpha)$ eine zum Exponenten *Eins* gehörende *complexe* Primzahl nenne; und *zweitens* der Fall, wo $f(\alpha)$ eine zu einem beliebigen andern Exponenten gehörende complexe Primzahl ist, d. h., wo $Nf(\alpha) = q^t$ und q eine für den Modul λ zum Exponenten t gehörende *nichtcomplexe* Primzahl ist. In dem ersten Falle, für welchen ich eine einfache Methode und die Hauptresultate im vorigen Jahre der Königlichen Akademie der Wissenschaften zu Berlin mitgetheilt habe (M. s. die Monatsberichte vom Mai 1850), ist die Lehre von der *Kreistheilung* allein ausreichend, um die vorliegende Aufgabe zu lösen; in dem zweiten Falle aber ist noch eine, auch in anderer Beziehung nicht unwichtige Erweiterung oder Verallgemeinerung der Theorie der Kreistheilung nöthig; welche in dem Folgenden ebenfalls entwickelt werden soll. Endlich gedenke ich hier auch noch eine Anwendung der gefundenen Resultate anf das *allgemeine* Reciprocitätsgesetz zu geben, bestehend in der Lösung der Aufgabe: Wenn das Reciprocitätsgesetz zwischen zwei complexen

Primzahlen gegeben ist, für besondere Bedingungen, welche die Einheiten bestimmen, die als Factoren dieser complexen Zahlen vorhanden sein können: daraus das Reciprocitätsgesetz für dieselben complexen Primfactoren zu finden, welche jenen Bedingungen nicht weiter unterliegen.

§. 1.

Entwickelung der Indices von λ, $1-\alpha^k$ und $\varepsilon(\alpha)$ für den Fall, dafs der Modul, auf welchen sich die Indices beziehen, ein zum Exponenten *Eins* gehörender complexer Primfactor ist.

Es sei $f(\alpha)$ ein complexer, idealer oder wirklicher Primfactor der realen Primzahl p, von der Form $\nu\lambda+1$; λ sei eine *ungerade* Primzahl; g eine primitive Wurzel der Congruenz $g^{p-1}\equiv 1$, Mod. p; γ eine primitive Wurzel der Congruenz $\gamma^{\lambda-1}\equiv 1$, Mod. λ; x eine imaginäre Wurzel der Gleichung $x^p=1$, und α eine imaginäre Wurzel der Gleichung $\alpha^\lambda=1$. Ferner seien $\eta, \eta_1, \eta_2, \ldots \eta_{\lambda-1}$ die λ Perioden, welche aus je $\nu=\frac{p-1}{\lambda}$ Wurzeln der Gleichung $x^p=1$ gebildet werden können, so dafs

$$\eta = x + x^{g^\lambda} + x^{g^{2\lambda}} + \cdots + x^{g^{(\nu-1)\lambda}},$$
$$\eta_1 = x^g + x^{g^{\lambda+1}} + x^{g^{2\lambda+1}} + \cdots + x^{g^{(\nu-1)\lambda+1}} \text{ ist,}$$

u. s. w.

Die Producte je zweier Perioden lassen sich bekanntlich immer als lineäre Functionen aller ähnlichen Perioden darstellen. Diese Ausdrücke nehmen in dem gegenwärtigen Falle, wo λ *ungrade* ist, folgende Gestalt an:

$$\begin{aligned}
\eta^2 &= \nu + m\eta + m_1\eta_1 + m_2\eta_2 + \cdots + m_{\lambda-1}\eta_{\lambda-1},\\
\eta\eta_1 &= \overset{1}{m}\eta + \overset{1}{m}_1\eta_1 + \overset{1}{m}_2\eta_2 + \cdots + \overset{1}{m}_{\lambda-1}\eta_{\lambda-1},\\
\eta\eta_2 &= \overset{2}{m}\eta + \overset{2}{m}_1\eta_1 + \overset{2}{m}_2\eta_2 + \cdots + \overset{2}{m}_{\lambda-1}\eta_{\lambda-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\eta\eta_{\lambda-1} &= \overset{\lambda-1}{m}\eta + \overset{\lambda-1}{m}_1\eta_1 + \overset{\lambda-1}{m}_2\eta_2 + \cdots + \overset{\lambda-1}{m}_{\lambda-1}\eta_{\lambda-1},
\end{aligned}$$

in welchen allgemein der Coëfficient $\overset{k}{m}_h$ gleich ist der Anzahl der Werth-Verbindungen des r und s, aus den Zahlen $r=0, 1, 2, \ldots r-1$ und $s=0, 1, 2, \ldots s-1$, welche der Congruenz

$$g^{k+r\lambda}+1 \equiv g^{h+s\lambda}, \text{ Mod. } p,$$

genügen, oder, was Dasselbe ist, gleich der Anzahl der Werthe des r aus

der Reihe $r = 0, 1, 2, \ldots r-1$, welche der Congruenz

$$\text{Ind.}(g^{k+r\lambda}+1) \equiv h, \quad \text{Mod. } \lambda,$$

genügen, wenn das Zeichen des Index (Ind.) sich auf die Primzahl p und deren primitive Wurzel g bezieht. Ich stelle hier, wegen des in dem Folgenden davon zu machenden Gebrauchs, die Haupt-Eigenschaften dieser Zahlen $\overset{k}{m}_h$, welche ich in der Abhandlung über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren (Bd. 35, S. 327 dieses Journals) hergeleitet habe, für den vorliegenden Fall, wo λ die Anzahl der Perioden, ***ungerade*** ist, noch einmal zusammen, nämlich:

$$\overset{k+r\lambda}{m}_h = \overset{k}{m}_h, \qquad \overset{k}{m}_{h+s\lambda} = \overset{k}{m}_h,$$

$$\overset{k}{m}_h = \overset{h}{m}_k, \qquad \overset{k}{m}_h = \overset{\lambda-k}{m}_{h-k},$$

$$\overset{k}{m} + \overset{k}{m}_1 + \overset{k}{m}_2 + \cdots + \overset{k}{m}_{\lambda-1} = \nu;$$

aber für $k = 0$,

$$m + m_1 + m_2 + \cdots + m_{\lambda-1} = \nu - 1.$$

Betrachtet man nun die Summe

$$\Sigma \text{Ind.}(g^{k+r\lambda}+1)$$

für alle Werthe $0, 1, 2, \ldots r-1$ des r, so finden sich in derselben $\overset{k}{m}_0$ Glieder, welche congruent Null werden für den Modul λ; ferner giebt es $\overset{k}{m}_1$ Glieder, welche congruent 1 werden, $\overset{k}{m}_2$ Glieder, welche congruent 2 werden u. s. w.; woraus

$$\Sigma \text{Ind.}(g^{k+r\lambda}+1) \equiv 1\overset{k}{m}_1 + 2\overset{k}{m}_2 + 3\overset{k}{m}_3 + \cdots + (\lambda-1)\overset{k}{m}_{\lambda-1}, \quad \text{Mod. } \lambda,$$

folgt. Nun wird aber, wie leicht zu zeigen, für $\nu = \frac{p-1}{\lambda}$ die Congruenz

$$z^\nu - 1 \equiv (z-1)(z-g^\lambda)(z-g^{2\lambda}) \ldots (z-g^{(\nu-1)\lambda}), \quad \text{Mod. } p,$$

für alle beliebigen Werthe des z identisch erfüllt. Setzt man daher in derselben $z \equiv -g^{p-1-k}$, Mod. p, und multiplicirt auf beiden Seiten mit $g^{\nu k}$, so wird

$$1 - g^{\nu k} \equiv (g^k+1)(g^{k+\lambda}+1)(g^{k+2\lambda}+1) \ldots (g^{k+(\nu-1)\lambda}+1), \quad \text{Mod. } p,$$

also, wenn auf beiden Seiten die Indices genommen werden:

$$\text{Ind.}(1-g^{\nu k}) \equiv \Sigma \text{Ind.}(g^{k+r\lambda}+1), \quad \text{Mod. } \lambda,$$

und diese Congruenz, mit der obigen Congruenz verglichen, giebt:

$$\text{Ind.}(1-g^{\nu k}) \equiv 1\overset{k}{m}_1 + 2\overset{k}{m}_2 + 3\overset{k}{m}_3 + \cdots + (\lambda-1)\overset{k}{m}_{\lambda-1}, \quad \text{Mod. } \lambda.$$

Ist nun $f(\alpha)$ ein complexer Primfactor des p, und zwar der zu $\alpha = g^\nu$ gehörige, so ist $g^\nu \equiv \alpha$, Mod. $f(\alpha)$. Ferner ist nach der oben gegebenen

Definition des Zeichens Ind., welches sich auf den Mod. $f(\alpha)$ bezieht,

$$\varphi(\alpha)^{\frac{Nf(\alpha)-1}{\lambda}} \equiv \alpha^{\text{Ind. }\varphi(\alpha)}, \text{ Mod. } f(\alpha),$$

oder weil $Nf(\alpha) = p$, $\frac{p-1}{\lambda} = \nu$ und $\alpha \equiv g^\nu$, Mod. $f(\alpha)$, ist:

$$\varphi(g^\nu)^\nu \equiv g^{\nu \text{ Ind. } \varphi(\alpha)},$$

für den Modul $f(\alpha)$ und, da diese Congruenz nur nichtcomplexe Zahlen enthält, auch für den Mod. p. Hieraus folgt, wenn $\varphi(\alpha) = 1-\alpha^k$ gesetzt wird:

$$\nu \text{ Ind.}(1-g^{\nu k}) \equiv \nu \text{ Ind.}(1-\alpha^k), \text{ Mod. } p-1,$$

also, wenn man durch ν dividirt,

$$\text{Ind.}(1-g^{\nu k}) \equiv \text{Ind.}(1-\alpha^k), \text{ Mod. } \lambda.$$

Demnach hat man auch

$$\text{Ind.}(1-\alpha^k) \equiv 1\overset{k}{m}_1 + 2\overset{k}{m}_2 + 3\overset{k}{m}_3 + \cdots + (\lambda-1)\overset{k}{m}_{\lambda-1}, \text{ Mod. } \lambda;$$

welche Congruenz eine sehr einfache Lösung einer der obigen Aufgaben darstellt. Aus diesem Ausdrucke läfst sich sehr leicht der entsprechende Ausdruck des Ind. (λ) ableiten, indem man nach einander $k = 1, 2, 3, \ldots \lambda-1$ setzt; wobei zu beachten ist, dafs

$$(1-\alpha)(1-\alpha^2)(1-\alpha^3)\ldots(1-\alpha^{\lambda-1}) = \lambda$$

und

$$m_h + \overset{1}{m}_h + \overset{2}{m}_h + \cdots\cdots + \overset{\lambda-1}{m}_h = \nu.$$

So erhält man

$$\text{Ind.}(\lambda) \equiv -(m_1 + 2m_2 + 3m_3 + \cdots + (\lambda-1)m_{\lambda-1}), \text{ Mod. } \lambda.$$

Endlich ergeben sich aus derselben Quelle auch die Indices der complexen Einheiten. Nimmt man nämlich die Einheit

$$e(\alpha) = \sqrt[2]{\left(\frac{(1-\alpha^\gamma)(1-\alpha^{-\gamma})}{(1-\alpha)(1-\alpha^{-1})}\right)} = \pm\frac{\alpha^{\frac{1}{2}(1-\gamma)}(1-\alpha^\gamma)}{1-\alpha},$$

welche ich ***Kreistheilungs-Einheit*** nenne, so hat man

$$\text{Ind. } e(\alpha^k) \equiv \tfrac{1}{2}k(1-\gamma)\,\text{Ind. }\alpha + \text{Ind.}(1-\alpha^{k\gamma}) - \text{Ind.}(1-\alpha^k), \text{ Mod. } \lambda,$$

also

$$\text{Ind. } e(\alpha^k) \equiv \tfrac{1}{2}k(1-\gamma)\nu + 1\overset{k\gamma}{m}_1 + 2\overset{k\gamma}{m}_2 + 3\overset{k\gamma}{m}_3 + \cdots + (\lambda-1)\overset{k\gamma}{m}_{\lambda-1} - 1\overset{k}{m}_1 - 2\overset{k}{m}_2 - 3\overset{k}{m}_3 - \cdots - (\lambda-)\overset{k}{m}_{\lambda-1}, \text{ Mod. } \lambda.$$

Ein System conjugirter Kreistheilungs-Einheiten ist ein unabhängiges System von Einheiten, welches die Eigenschaft hat, dafs überhaupt jede Einheit ohne Ausnahme sich als ein Product von Potenzen der conjugirten Kreistheilungs-Einheiten darstellen läfst, und zwar so, dafs die Potenz-Exponenten

nur rationale Brüche sind; d. h., wenn $\varepsilon(\alpha)$ eine beliebige complexe Einheit ist, so hat man immer

$$\varepsilon(\alpha) = \pm\alpha^k e(\alpha)^n . e(\alpha^\gamma)^{n_1} . e(\alpha^{\gamma^2})^{n_2} \ldots e(\alpha^{\gamma^{\mu-1}})^{n_{\mu-1}},$$

wo zur Abkürzung $\frac{1}{2}(\lambda-1)=\mu$ gesetzt ist, und wo $n, n_1, n_2, \ldots n_{\mu-1}$ rationale Brüche sind. Man erhält daher auch den Index jeder beliebigen Einheit $\varepsilon(\alpha)$ durch die Indices der Kreistheilungs-Einheiten ausgedrückt, nämlich:

$$\text{Ind. } \varepsilon(\alpha) \equiv k\nu + n \text{ Ind. } e(\alpha) + n_1 \text{ Ind. } e(\alpha^\gamma) + \cdots + n_{\mu-1} \text{ Ind. } e(\alpha^{\gamma^{\mu-1}}), \text{ Mod. } \lambda.$$

In den Nennern der rationalen Brüche $n, n_1, \ldots n_{\mu-1}$ kann, wie ich in der Abhandlung (Bd. 40. S. 117 dieses Journals) gezeigt habe, der Factor λ nur dann vorkommen, wenn die Classen-Anzahl aller idealen complexen Zahlen durch λ theilbar ist, also nur dann, wenn λ in einer der ersten $\frac{1}{2}(\lambda-3)$ *Bernoulli*schen Zahlen als Factor des Zählers auftritt. Schliefst man diese Ausnahmszahlen λ auch hier aus, so sind mit den Indices der Kreistheilungs-Einheiten $e(\alpha^k)$ zugleich auch die Indices aller möglichen Einheiten gegeben; denn man kann alle in dem Ausdrucke des Ind. $\varepsilon(\alpha)$ vorkommenden Brüche $n, n_1, \ldots n_{\mu-1}$ durch die ganzen Zahlen ersetzen, denen sie congruent sind für den Modul λ.

Hiermit ist also die erste Lösung der Aufgabe, die Indices der Zahlen $1-\alpha^k$ und λ, und der complexen Einheiten zu finden, in sehr einfacher Weise gegeben; für den Fall, dafs die complexe Primzahl, auf welche die Indices sich beziehen, eine solche ist, die für den Modul λ zum Exponenten *Eins* gehört. Die Zahlen $\overset{k}{m}_h$, mittels welcher die Lösung dieser Aufgabe gegeben ist, lassen sich auf mannichfache Weise auf andere in der Lehre von der Kreistheilung vorkommende Zahlen reduciren, namentlich auf die Coëfficienten der complexen Zahlen $\psi_r(\alpha)$, welche, wenn man

$$F(\alpha, x) = x + \alpha x^g + \alpha^2 x^{g^2} + \cdots + \alpha^{p-2} x^{g^{p-2}}$$

setzt, durch die Gleichung

$$\frac{F(\alpha, x)F(\alpha^r, x)}{F(\alpha^{r+1}, x)} = \psi_r(\alpha) = \overset{r}{a} + \overset{r}{a}_1\alpha + \overset{r}{a}_2\alpha^2 + \cdots + \overset{r}{a}_{\lambda-1}\alpha^{\lambda-1}$$

bestimmt werden. Durch dieselben können die Zahlen $\overset{k}{m}_h$ in folgender Art ausgedrückt werden:

$$\lambda \overset{k}{m}_h = \overset{\lambda-2}{\Sigma}_r \overset{r}{a}_{h+kr} - (\lambda-3)\nu + 1;$$

wo in den besondern Fällen $h=k$, $h=0$ oder $k=0$ die *Eins* auf der rechten Seite wegfallen mufs. Da ferner, wie ich in früheren Abhandlungen

gezeigt habe, alle in der Kreistheilung vorkommenden Zahlen durch die Coëfficienten eines complexen Primfactors von p sich ausdrücken lassen, so wird man auch die Indices von λ, $1-\alpha^k$ und $\varepsilon(\alpha)$ durch die Coëfficienten von $f(\alpha)$ selbst ausdrücken können. Ich will jedoch nicht alle diese Umformungen der gefundenen Formeln hier wirklich ausführen. Für Ind. λ und Ind. $(1-\alpha^k)$ sind auch die gefundenen Ausdrücke so einfach uud elegant, dafs sie vollständig genügen können; für die Indices der Einheiten dagegen giebt es noch einige merkwürdige und einfache Ausdrücke, welche ich entwickeln will, weil sie auch für andere Untersuchungen wichtig sind. Sie gestalten sich am einfachsten für die zusammengesetzte Kreistheilungs-Einheit

$$\boldsymbol{E}_n(\alpha) = e(\alpha)e(\alpha^\gamma)^{\gamma^{-2n}}.e(\alpha^{\gamma^2})^{\gamma^{-4n}} \ldots e\left(\alpha^{\gamma^{\mu-1}}\right)^{\gamma^{-2(\mu-1)n}},$$

welche überhaupt in mehrfacher Beziehung vor den übrigen Einheiten bevorzugt ist. Für diese Einheit hat man

$$\text{Ind.}\,\boldsymbol{E}_n(\alpha) \equiv \text{Ind.}\,e(\alpha) + \gamma^{-2n}\,\text{Ind.}\,e(\alpha^\gamma) + \cdots + \gamma^{-2(\mu-1)n}\,\text{Ind.}\,e(\alpha^{\gamma^{\mu-1}}),\ \text{Mod.}\,\lambda,$$

und man kann umgekehrt Ind. $e\left(\alpha^{\gamma^h}\right)$ mittels der aus jener leicht abzuleitenden Formel

$$\text{Ind.}\,e(\alpha^{\gamma^h}) \equiv -2\,(\gamma^{2h}\,\text{Ind.}\,\boldsymbol{E}_1(\alpha) + \gamma^{4h}\,\text{Ind.}\,\boldsymbol{E}_2(\alpha) + \cdots + \gamma^{2(\mu-1)h}\,\text{Ind.}\,\boldsymbol{E}_{\mu-1}(\alpha)),\ \text{Mod.}\,\lambda,$$

durch die Indices von $\boldsymbol{E}_1(\alpha)$, $\boldsymbol{E}_2(\alpha)$, $\ldots$ $\boldsymbol{E}_{\mu-1}(\alpha)$ ausdrücken.

Substituirt man in diesem Ausdrucke des Ind. $\boldsymbol{E}_n(\alpha)$ für $e(\alpha)$, für $e(\alpha^\gamma)$ u. s. w. ihre Werthe nach dem oben gegebenen Ausdrucke dieser Kreistheilungs-Einheiten, so erhält man nach einigen leichten Reductionen:

$$2\,\text{Ind.}\,\boldsymbol{E}_n(\alpha) \equiv (\gamma^{2n})(\text{Ind.}\,(1-\alpha) + \gamma^{-2n}\,\text{Ind.}\,(1-\alpha^\gamma) + \cdots + \gamma^{-(\lambda-2)2n}\,\text{Ind.}\,(1-\alpha^{\gamma^{\lambda-2}})),$$

und wenn $\gamma^h \equiv k$, Mod. λ, gesetzt wird, was $\gamma^{-2hn} \equiv k^{\lambda-1-2n}$ giebt, so erhält man, mit Anwendung des Summenzeichens:

$$2\,\text{Ind.}\,\boldsymbol{E}_n(\alpha) \equiv (\gamma^{2n}-1)\Sigma k^{\lambda-2n-1}\,\text{Ind.}\,(1-\alpha^k),$$

für $k = 1, 2, 3, \ldots \lambda-1$; wozu, wenn $\lambda - 2n - 1$, wie hier angenommen werden soll, *positiv* ist, auch der Werth $k = 0$ hinzugethan werden kann. Da nun oben

$$\text{Ind.}\,(1-\alpha^k) \equiv 1\overset{k}{m}_1 + 2\overset{k}{m}_2 + \cdots + (\lambda-1)\overset{k}{m}_{\lambda-1} \equiv \sum_0^{\lambda-1} h\overset{k}{m}_h$$

gefunden wurde, so hat man

$$2\,\text{Ind.}\,\boldsymbol{E}_n(\alpha) \equiv (\gamma^{2n}-1)\sum_0^{\lambda-1}\sum_0^{\lambda-1} hk^{\lambda-2n-1}\overset{k}{m}_h.$$

In diesen Ausdruck sollen nun statt der Zahlen $\overset{k}{m}_h$ die **Perioden** η, η_1, η_2, ... $\eta_{\lambda-1}$ eingeführt werden. Dies geschieht mit Hülfe der Gleichung

$$\eta\eta_k = \overset{k}{m}\eta + \overset{k}{m}_1\eta_1 + \overset{k}{m}_2\eta_2 + \cdots + \overset{k}{m}_{\lambda-1}\eta_{\lambda-1} = \sum_0^{\lambda-1} \overset{k}{m}_h\eta_h,$$

aus welcher

$$\eta_i\eta_{i+k} = \sum_h^{\lambda-1} \overset{k}{m}_h\eta_{i+h}$$

folgt. Multiplicirt man mit i und nimmt die Summe für $i = 0, 1, 2, 3, \ldots \lambda-1$, so ergiebt sich

$$\sum_0^{\lambda-1} i\eta_i\eta_{i+k} = \sum_0^{\lambda-1}\sum_0^{\lambda-1} \overset{k}{im}_h\eta_{i+h},$$

oder, was Dasselbe ist,

$$\sum_0^{\lambda-1} i\eta_i\eta_{i+k} = \sum_0^{\lambda-1}\sum_0^{\lambda-1} (i+h)\overset{k}{m}_h\eta_{i+h} - \sum_0^{\lambda-1}\sum_0^{\lambda-1} h\overset{k}{m}_h\eta_{i+h}$$

und, da $\Sigma\eta_{i+h} = -1$, $\sum_0^{\lambda-1}(i+h)\eta_{i+h} \equiv \sum_0^{\lambda-1} i\eta_i$, Mod. λ, und $\sum_0^{\lambda-1} \overset{k}{m}_h = \nu$ ist, so erhält man

$$\sum_0^{\lambda-1} i\eta_i\eta_{i+k} \equiv \nu\sum_0^{\lambda-1} i\eta_i + \sum_0^{\lambda-1} h\overset{k}{m}_h, \text{ Mod. } \lambda.$$

Multiplicirt man jetzt mit $k^{\lambda-2n-1}$, nimmt die Summe für $k = 0, 1, 2, \ldots \lambda-1$, und beachtet, dafs $\Sigma k^{\lambda-2n-1} \equiv 0$, Mod. λ ist, für $k = 0, 1, 2, \ldots \lambda-1$, so erhält man

$$\sum_0^{\lambda-1}\sum_0^{\lambda-1} ik^{\lambda-2n-1}.\eta_i\eta_{i+k} \equiv \sum_0^{\lambda-1}\sum_0^{\lambda-1} hk^{\lambda-2n-1}.\overset{k}{m}_h, \text{ Mod. } \lambda.$$

Der Ausdruck des zweiten Ind. $E_n(\alpha)$ verwandelt sich demnach in den folgenden:

$$2\,\text{Ind.}\,E_n(\alpha) \equiv (\gamma^{2n}-1)\sum_0^{\lambda-1}\sum_0^{\lambda-1} ik^{\lambda-2n-1}\eta_i\eta_{i+k}, \text{ Mod. } \lambda.$$

Anstatt dem k in dieser Doppelsumme die Werthe $0, 1, 2, \ldots \lambda-1$ zu geben, kann man ihm auch die Werthe $-i$, $-i+1$, $-i+2$, ... $-i+\lambda-1$ zutheilen, ohne dafs in Beziehung auf den Modul λ diese Summe ihren Werth ändert. Setzt man also $k-i$ statt i, so erhält man

$$2\,\text{Ind.}\,E_n(\alpha) \equiv (\gamma^{2n}-1)\sum_0^{\lambda-1}\sum_0^{\lambda-1} i(k-i)^{\lambda-2n-1}.\eta_i\eta_k.$$

Wird jetzt $(k-i)^{\lambda-2n-1} = (i-k)^{\lambda-2n-1}$ nach dem binomischen Lehrsatze entwickelt, so trennen sich in den einzelnen Gliedern die in Beziehung auf i zu nehmenden Summen von den in Beziehung auf k zu nehmenden, und wenn

der Kürze wegen

$$\sum_{0}^{\lambda-1} k^r \eta_k = \sum_{0}^{\lambda-2} i^r \eta_i = D_r$$

gesetzt und für einen Augenblick $\lambda - 2n - 1$ einfach durch m bezeichnet wird, so erhält man

$$2\,\text{Ind.}\, E_n(\alpha) \equiv (\gamma^{2n}-1)\Big(D_{m+1}D_0 - \frac{m}{1}D_m D_1 + \frac{m(m-1)}{1.2}D_{m-1}D_2 - \cdots\Big).$$

Um die durch D_0, D_1, D_2, ... bezeichneten Gröfsen noch auf andere Weise zu bestimmen, gebe ich dem Ausdruck der Kreistheilung

$$F(\alpha, x) = x + \alpha x^g + \alpha^2 x^{g^2} + \cdots + \alpha^{p-2} x^{g^{p-2}}$$

die Form

$$F(\alpha, x) = \eta + \alpha\eta_1 + \alpha^2\eta_2 + \cdots + \alpha^{\lambda-1}\eta_{\lambda-1}$$

und verwandle α in ε^v, wo v eine ***continuirliche Variable*** bedeutet. Hiernach wird

$$\frac{d_0^r F(e^v, x)}{dv^r} \equiv 1^r\eta_2 + 2^r\eta_2 + 3^r\eta_3 + \cdots + (\lambda-1)^r\eta_{\lambda-1} \equiv D_r;$$

wo die dem Zeichen des Differentials d zugefügte Null bedeutet, dafs nach der Differentiation $v = 0$ zu setzen ist. Verwandelt man v in $-v$, so erhält man eben so:

$$\frac{d_0^r F(e^{-v}, x)}{dv^r} \equiv (-1)^r D^r.$$

Aus diesen Werthen der Gröfsen D_r, als Differentialquotienten, folgt nach einem bekannten Satze der Differentialrechnung über die Differentiation eines Products zweier Factoren:

$$D_{m+1}D_0 - \frac{m}{1}D_m D_1 + \frac{m(m-1)}{1.2}D_{m-1}D_2 - \cdots = \frac{d_0^m\Big(\frac{dF(e^v, x)}{dv}\cdot F(e^{-v}, x)\Big)}{dv^m}.$$

Aus der bekannten Gleichung der Kreistheilung

$$F(\alpha, x)F(\alpha^{-1}, x) = p$$

erhält man aber nach bekannten Principien die für jeden Werth der Variabeln v geltende Gleichung

$$F(e^v, x)F(e^{-v}, x) = p + V.W,$$

in welcher $V = 1 + e^v + e^{2v} + \cdots + e^{(\lambda-1)v}$ und W irgend eine ganze rationale Function von e^v ist, deren Coëfficienten ganze, die Wurzel x enthaltende complexe Zahlen sind; folglich ist auch

$$F(e^{-v}, x) = \frac{p}{F(e^v, x)} + \frac{VW}{F(e^v, x)}$$

und

$$\frac{dF(e^v, x)}{dv} F(e^{-v}, x) = \frac{dlF(e^v, x)}{dx}(p + VW).$$

Differentiirt man diesen Ausdruck $m$mal nach einander und setzt $v = 0$, indem man bemerkt, dafs für $v = 0$, V und alle Differentialquotienten davon, bis zum $\lambda - 2$ten einschliefslich, durch λ theilbar sind, da $1^r + 2^r + 3^r + \cdots + (\lambda-1)^r \equiv 0$, Mod. λ, für $r = 1, 2, 3, \ldots \lambda - 2$ ist, und indem man ferner bemerkt, dafs $p \equiv 1$, Mod. λ ist, so erhält man:

$$\frac{d_0^m\left(\frac{dF(e^v, x)}{dx} F(e^{-v}, x)\right)}{dv^m} \equiv \frac{d_0^{m+1} lF(e^v, x)}{dv^{m+1}}, \text{ Mod. } \lambda,$$

also

$$D_{m+1}D_0 - \frac{m}{1} D_m D_1 + \frac{m(m-1)}{1.2} D_{m-1}D_2 - \cdots \equiv \frac{d_0^{m+1} lF(e^v, x)}{dv^{m+1}}, \text{ Mod. } \lambda.$$

Macht man von diesem einfachen Ausdrucke Gebrauch, und setzt zugleich für m wieder seinen Werth $\lambda - 2n - 1$, so erhält man folgenden merkwürdigen Ausdruck des Index von $E_n(\alpha)$:

$$\text{Ind. } E_n(\alpha) \equiv \tfrac{1}{2}(\gamma^{2n} - 1)\frac{d_0^{\lambda-2n} lF(e^v, x)}{dv^{\lambda-2n}}, \text{ Mod. } \lambda.$$

Die in diesem Ausdrucke vorkommende Wurzel x ist in demselben nur scheinbar enthalten, weil sie, wenn nach Ausführung der Differentiation $v = 0$ gesetzt wird, und alle Glieder, die den Factor λ haben, weggelassen werden, von selbst mit herausfällt.

Aus dieser Darstellung des Ind. $E_n(\alpha)$ läfst sich sehr leicht eine andere, ebenfalls sehr bemerkenswerthe Darstellung desselben erlangen, in welcher der von α und x abhängige Ausdruck $F(\alpha, x)$ durch die nur von α allein abhängige, oben definirte complexe Zahl $\psi_r(\alpha)$ ersetzt wird. Aus der Gleichung

$$F(\alpha, x)F(\alpha^r, x) = \psi_r(\alpha)F(\alpha^{r+1}, x)$$

folgt nämlich, wenn α in e^v verwandelt wird, nach denselben Principien wie oben, die für jeden beliebigen Werth der Variabel v geltende Gleichung

$$F(e^v, x)F(e^{rv}, x) = \psi_r(e^v)F(e^{(r+1)v}, x) + V.W.$$

Und vermöge der Eigenschaft des $V = 1 + e^v + e^{2v} + \cdots + e^{(\lambda-1)v}$, dafs V selbst, so wie seine Differentialquotienten, bis zum $(\lambda-2)$ten einschliefslich, für den Werth $v = 0$ congruent Null sind, nach dem Modul λ, erhält man aus dieser Gleichung

$$\frac{d_0^{\lambda-2n} lF(e^v, x)}{dv^{\lambda-2n}} + \frac{d_0^{\lambda-2n} lF(e^{rv}, x)}{dv^{\lambda-2n}} \equiv \frac{d_0^{\lambda-2n} lF(e^{(r+1)v}, x)}{dv^{\lambda-2n}} + \frac{d_0^{\lambda-2n} l\psi_r(e^v)}{dv^{\lambda-2n}},$$

oder, vereinfacht:

$$(1+r^{\lambda-2n}-(r+1)^{\lambda-2n})\frac{d_0^{\lambda-2n}lF(e^v,\,x)}{dv^{\lambda-2n}} \equiv \frac{d_0^{\lambda-2n}l\psi_r(e^v)}{dv^{\lambda-2n}},\ \text{Mod. } \lambda.$$

Durch diese Congruenz verwandelt sich der obige Ausdruck des Ind. $E_n(\alpha)$ in folgenden:

$$\text{Ind. } E_n(\alpha) \equiv \frac{\gamma^{2n}-1}{2(1+r^{\lambda-2n}-(r+1)^{\lambda-2n})}\cdot\frac{d_0^{\lambda-2n}l\psi_r(\alpha)}{dv^{\lambda-2n}},\ \text{Mod. } \lambda.$$

Endlich leite ich hieraus noch einen andern Ausdruck des Ind. $E_n(\alpha)$ ab, welcher deshalb der wichtigste von allen zu sein scheint, weil er diesen Index der Einheit $E_n(\alpha)$ durch die complexe Primzahl $f(\alpha)$ selbst ausdrückt, in Beziehung auf welche das Zeichen Ind. zu nehmen ist. Hierzu wird die Zerfällung der complexen Zahl $\psi_r(\alpha)$ in ihre complexen idealen oder wirklichen Primfactoren gebraucht, welche ich im (35ten Bande dieses Journals, S. 362) gegeben habe und welche sich in folgender Art darstellen läfst:

$$\psi_r(\alpha) = \pm\alpha^k \Pi f(\alpha\gamma^h);$$

wo das Productenzeichen Π sich auf alle diejenigen Werthe des h erstreckt, welche nicht negativ, aber kleiner als $\lambda-1$ sind, und dabei der Bedingung genügen, dafs

$$\gamma_{\mu-h}+\gamma_{\mu-h+\text{Ind.}r} > \lambda$$

ist; wo das Zeichen γ_k den kleinsten positiven Werth von γ^k für den Modul λ, Ind. r den Index des r für die primitive Wurzel γ und den Modul λ bezeichnet und $\mu=\frac{1}{2}(\lambda-1)$ ist. Um die in diesem Producte enthaltenen Primfactoren, welche im Allgemeinen ideal sein werden, zu wirklichen complexen Zahlen zu machen, erhebe ich beide Seiten dieser Gleichung zur Hten Potenz und nehme H so an, dafs $f(\alpha)^H$ eine wirkliche complexe Zahl ist. Diese complexe Zahl soll auch durch Multiplication mit einer passenden einfachen Einheit α^m so zubereitet angenommen werden, dafs sie für den Modul $(1-\alpha)^2$ einer nicht complexen ganzen Zahl congruent ist. Alsdann fällt in dem obigen Ausdrucke des $\psi_r(\alpha)$ die einfache Einheit α^k weg, und man hat

$$\psi_r(\alpha)^H = \pm\Pi f(\alpha\gamma^h)^H.$$

Diese Gleichung wird wieder, wie oben, in folgende, für alle beliebigen Werthe der Variabel v geltende Gleichung verwandelt:

$$\psi_r(e^v)^H = \Pi f(e^{v\gamma^h})^H + V.W,$$

und giebt alsdann in derselben Weise:

$$H.\frac{d_0^{\lambda-2n}l\psi_r(e^v)}{dv^{\lambda-2n}} = \Sigma_h\frac{d_0^{\lambda-2n}l\left(f(e^{v\gamma^h})^H\right)}{dv^{\lambda-2n}},$$

oder vereinfacht:,

$$H.\frac{d_0^{\lambda-2n} l\psi_r(e^v)}{dv^{\lambda-2n}} = \frac{d_0^{\lambda-2n} l(f(e^v)^H)}{dv^{\lambda-2n}} \Sigma_h \gamma^{(\lambda-2n)h}.$$

Es ist nun die Summe $\Sigma_h \gamma^{(\lambda-2n)h}$ zu suchen, in welcher dem h alle diejenigen Werthe von $h=0$ bis $h=\lambda-2$ zu geben sind, welche der Bedingung genügen, dafs $\gamma_{\mu-h}+\gamma_{\mu-h+\text{Ind. }r} > \lambda$ ist. Zu diesem Zwecke bemerke ich, dafs, wie leicht zu beweisen, der Ausdruck

$$\frac{1}{\lambda}(\gamma_{\mu-i}+\gamma_{\mu-i+\text{Ind. }r}-\gamma_{\mu-i+\text{Ind. }(r+1)})$$

in allen den Fällen, wo i einen der mit h bezeichneten Werthe hat, für welche $\gamma_{\mu-1}+\gamma_{\mu-1+\text{Ind. }r} > \lambda$ ist, gleich *Eins* ist; während derselbe für alle andern Werthe des i gleich Null ist. Hieraus folgt

$$\Sigma_h \gamma^{(\lambda-2n)h} = \Sigma_i \frac{1}{\lambda}(\gamma_{\mu-i}+\gamma_{\mu-i+\text{Ind. }r}-\gamma_{\mu-i+\text{Ind. }(r+1)})\gamma^{(\lambda-2n)i};$$

wo dem h nur die oben angegebenen Werthe, aber dem i alle Werthe $0, 1, 2, \ldots \lambda-2$ zu geben sind. Um bequeme Congruenzen für den Modul λ^2 anwenden zu können, welches wegen des als Divisor hier vorkommenden λ nöthig ist, setze ich $\gamma^{\lambda(\lambda-2n)i}$ statt $\gamma^{(\lambda-2n)i}$; was in Beziehung auf den Modul λ keinen Unterschied macht. Ich bezeichne ferner die zu suchende Summe $\Sigma_h \gamma^{(\lambda-2n)h}$ mit dem Buchstaben T, multiplicire mit λ, und erhalte so folgende Congruenz für den Modul λ^2:

$$\lambda T \equiv \Sigma(\gamma_{\mu-i}+\gamma_{\mu-i+\text{Ind. }r}-\gamma_{\mu-i+\text{Ind. }(r+1)})\gamma^{\lambda(\lambda-2n)i}, \text{ Mod. } \lambda^2,$$

oder

$$\lambda T \equiv \Sigma\gamma_{\mu-i}\gamma^{\lambda(\lambda-2n)i}+\Sigma\gamma_{\mu+i+\text{Ind. }r}\gamma^{\lambda(\lambda-2n)i}-\Sigma\gamma_{\mu-i+\text{Ind. }(r+1)}\gamma^{\lambda(\lambda-2n)i}.$$

Ich betrachte nun zuerst nur die zweite dieser drei Summen, nämlich die Summe

$$\sum_0^{\lambda-2} {}_i\gamma_{\mu-i+\text{Ind. }r}\gamma^{\lambda(\lambda-2n)i},$$

aus welcher die erste hervorgeht, wenn $r=1$ gesetzt, und die dritte, wenn r in $r+1$ verwandelt wird. Ich verwandle i in $i+\mu+\text{Ind. }r$ und bemerke, dafs nach dieser Verwandlung dem i in der Summe immer noch dieselben Werthe $0, 1, 2, \ldots \lambda-2$ zukommen; was daraus folgt, dafs in Beziehung auf den Modul λ^2 die Glieder dieser Summe einen Cyclus bilden. Diese Summe ist daher für den Modul λ^2 der folgenden congruent:

$$\sum_0^{\lambda-2} {}_i\gamma_{-i}\gamma^{\lambda(k-2n)(i+\mu+\text{Ind. }r)},$$

und da $\gamma^{\lambda(\lambda-2n)\mu} \equiv -1$, $\gamma^{\lambda(\lambda-2n)\text{Ind. }r} \equiv r^{\lambda(\lambda-2n)}$ für den Modul λ^2 ist, so wird

dieselbe in folgende Form gebracht:

$$-r^{\lambda(\lambda-2n)}\sum_0^{\lambda-2} {}_i\gamma_{-i}\gamma^{\lambda(\lambda-2n)i}.$$

Macht man von diesem Werthe Gebrauch, und von den entsprechenden, welche man erhält, wenn $r=1$ und $r+1$ statt r gesetzt wird, so erhält man folgenden Ausdruck der Summe T:

$$\lambda T \equiv -(1+r^{\lambda(\lambda-2n)}-(r+1)^{\lambda(\lambda-2n)})\sum_0^{\lambda-2} {}_i\gamma_{-i}\gamma^{\lambda(\lambda-2n)i}, \text{ Mod. } \lambda^2.$$

Man setze jetzt $\gamma_{-i}=k$, so wird $\gamma^{-i}\equiv k$ und $\gamma^i\equiv k^{\lambda-2}$, für den Modul λ; woraus $\gamma^{i\lambda}\equiv k^{\lambda(\lambda-2)}$, Mod. λ^2, also

$$\sum_0^{\lambda-2} {}_i\gamma_{-i}\gamma^{\lambda(\lambda-2n)i} \equiv \sum_0^{\lambda-1} {}_k k^{\lambda(\lambda-2n)(\lambda-2)+1}, \text{ Mod. } \lambda^2$$

folgt, oder, vereinfacht, mit Hülfe der Congruenz $k^{\lambda(\lambda-1)}\equiv 1$, Mod. λ^2:

$$\sum_0^{\lambda-2} {}_i\gamma_{-i}\gamma^{\lambda(\lambda-2n)i} \equiv \sum_0^{\lambda-1} {}_k k^{\lambda(2n-1)+1}, \text{ Mod. } \lambda^2.$$

Nun folgt aber aus den bekannten Summen-Ausdrücken der Potenzen der natürlichen Zahlen, dafs

$$\sum_0^{\lambda-1} {}_k k^{\lambda(2n-1)+1} \equiv (-1)^{m-1}B_m\lambda, \text{ Mod. } \lambda^2$$

ist; wo B_m die $m$te *Bernoulli*sche Zahl bezeichnet und wo der Kürze wegen auf einen Augenblick für $\frac{1}{2}(\lambda(2n-1)+1)$ das einfache Zeichen m gesetzt ist. Demnach ist

$$\lambda T = (-1)^m(1+r^{\lambda(\lambda-2n)}-(r+1)^{\lambda(\lambda-2n)})B_m\lambda, \text{ Mod. } \lambda^2.$$

Und wenn durch λ dividirt wird und für $r^{\lambda(\lambda-2n)}$ und $(r+1)^{\lambda(\lambda-2n)}$ die nach dem Modul λ congruenten einfacheren Potenzen $r^{\lambda-2n}$ und $(r+1)^{\lambda-2n}$ gesetzt werden, so ist

$$T \equiv (-1)^m(1+r^{\lambda-2n}-(r+1)^{\lambda-2n})B_m, \text{ Mod. } \lambda.$$

Die hierin vorkommende *Bernoulli*sche Zahl B_m kann noch durch Reduction auf eine möglichst niedrige *Bernoulli*sche Zahl vereinfacht werden; mittels der von mir in einer kleinen Abhandlung (Bd. 41, S. 371 dieses Journals) bewiesenen Eigenschaft der *Bernoulli*schen Zahlen, dafs

$$\frac{B_n}{n} \equiv \frac{(-1)^\mu B_{n+\mu}}{n+\mu}, \text{ Mod. } \lambda$$

ist, für $\mu=\frac{1}{2}(\lambda-1)$ und für alle Werthe des n, welche nicht Vielfache von μ sind. Diese Congruenz giebt unmittelbar die allgemeinere:

$$\frac{B_n}{n} \equiv \frac{(-1)^{s\mu}B_{n+s\mu}}{n+s\mu}, \text{ Mod. } \lambda,$$

welche für alle ganzzahligen Werthe von s gültig ist. Setzt man in dieser $s = 2n-1$, so erhält man für $m = \frac{1}{2}(\lambda(2n-1)+1)$:

$$B_m \equiv (-1)^{\mu}\frac{B_n}{2n}, \text{ Mod. } \lambda.$$

Wird dieser einfachere Werth des B_m angewendet und erwogen, dafs $(-1)^{m+\mu} = (-1)^n$ ist, so erhält man

$$T \equiv (-1)^n(1+r^{\lambda-2n}-(r+1)^{\lambda-2n})\frac{B_n}{2n}, \text{ Mod. } \lambda,$$

und demnach

$$H\frac{d_0^{\lambda-2n} l\psi_r(e^v)}{dv^{\lambda-2n}} \equiv (-1)^n(1+r^{\lambda-2n}-(r+1)^{\lambda-2n})\frac{B_n}{2n}\frac{d_0^{\lambda-2n} l(f(e^v)^H)}{dv^{\lambda-2n}}, \text{ Mod. } \lambda.$$

Vermöge dieser Congruenz verwandelt sich der zuletzt gegebene Ausdruck des Ind. $E_n(\alpha)$ in folgenden:

$$\text{Ind. } E_n(\alpha) \equiv (-1)^n(\gamma^{2n}-1)\frac{B_n}{4nH}\frac{d_0^{\lambda-2n} l(f(e^v)^H)}{dv^{\lambda-2n}}, \text{ Mod. } \lambda.$$

Dieser Ausdruck, in welchem die Zahlen der Kreistheilung nicht weiter vorkommen, welcher vielmehr den Index der Einheit $E_n(\alpha)$ durch die complexe Primzahl $f(\alpha)$ selbst darstellt, in Beziehung auf welche das Zeichen Index zu nehmen ist, wird in dem Falle, wo H ein Vielfaches von λ ist, nichtssagend. Es sind also auch bei der Anwendung dieser Formel diejenigen Ausnahmewerthe des λ auszuschliefsen, für welche λ ein Factor des Zählers einer der ersten $\frac{1}{2}(\lambda-3)$ *Bernoulli*schen Zahlen ist. Für den Fall, dafs $f(\alpha)$ eine wirkliche complexe Primzahl ist, hat man einfach $H = 1$ zu setzen. Man kann aber auch für den Fall, dafs $f(\alpha)$ eine ideale complexe Primzahl ist, den Ausdruck des Ind. $E_n(\alpha)$ einfach durch

$$\text{Ind. } E_n(\alpha) \equiv (-1)^n(\gamma^{2n}-1)\frac{B_n}{4n}\frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}}, \text{ Mod. } \lambda$$

darstellen, wenn man ein für allemal festsetzt, dafs für $f(\alpha)$, falls es ideal ist, sein Ausdruck als Hte Wurzel aus der wirklichen complexen Zahl $f(\alpha)^H$ genommen werden soll.

§. 2.

Eine Erweiterung der Theorie der Kreistheilung.

Nachdem in dem vorhergehenden Paragraphen die Indices von λ, $1-\alpha^k$ und $e(\alpha)$ oder $E_n(\alpha)$ gefunden worden sind, für welche der Modul $f(\alpha)$ ein Primfactor einer nichtcomplexen ganzen Primzahl p von der Form $\nu\lambda+1$ ist, mufs noch dieselbe Aufgabe für den allgemeinern Fall gelöset werden, dafs

der Modul $f(\alpha)$ eine zu irgend einem Exponenten t (Divisor von $\lambda-1$) gehörende complexe Primzahl ist. Die Lösung dieser Aufgabe erfordert als Vorarbeit eine Erweiterung der Theorie der *Kreistheilung*, welche ich hier kurz entwickeln will.

Es sei also $f(\alpha)$ ein idealer complexer Primfactor der nichtcomplexen Primzahl q, welche zum Exponenten t (einem Divisor von $\lambda-1$) gehört, für den Modul λ, so dafs $q^t \equiv 1$, Mod. λ, dafs aber keine niedrigere Potenz von q der Einheit congruent ist, für den Modul λ. Wird eine solche complexe Primzahl $f(\alpha)$ zum Modul genommen, so ist ein vollständiges Resten-System dieses Moduls in der Form

$$a + a_1\alpha + a_2\alpha^2 + \cdots + a_{t-1}\alpha^{t-1}$$

enthalten, in welcher alle die Zahlen a, a_1, a_2, $\ldots$ a_{t-1} alle ganzzahligen Werthe von 0 bis $q-1$ einschliefslich erhalten können. Die Anzahl aller verschiedenen Reste ist also gleich q^t; nämlich gleich der Anzahl aller Verbindungen der q Zahlen a mit den q Zahlen a_1, mit den q Zahlen a_2, u. s. w. Die Richtigkeit dieser Behauptung ergiebt sich daraus, dafs, *erstens*, jeder wirklichen complexen Zahl $F(\alpha)$ die Form

$$F(\alpha) = \varphi(\eta) + \alpha\varphi_1(\eta) + \alpha^2\varphi_2(\eta) + \cdots + \alpha^{t-1}\varphi_{t-1}(\eta)$$

gegeben werden kann, wo $\varphi(\eta)$, $\varphi_1(\eta)$, u. s. w. complexe Zahlen sind, welche nur die aus je t Gliedern bestehenden Perioden der Wurzeln α, α^2, $\ldots$ $\alpha^{\lambda-1}$ enthalten (M. s. meine Abhandlung Bd. 35. S. 337 dieses Journals); *zweitens* daraus, dafs in Beziehung auf einen solchen Modul $f(\alpha)$ diese Perioden, und also auch die complexen Zahlen $\varphi(\eta)$, $\varphi_1(\eta)$, u. s. w., stets nichtcomplexen ganzen Zahlen congruent sind; und endlich, *drittens*, daraus, dafs eine complexe Zahl von der Form

$$(a-b) + (a_1-b_1)\alpha + (a_2-b_2)\alpha^2 + \cdots + (a_{t-1}-b_{t-1})\alpha^{t-1}$$

nicht durch $f(\alpha)$ theilbar sein kann, ohne dafs zugleich $a \equiv b$, $a_1 \equiv b_1$, $a_2 \equiv b_2$, $\ldots$ $a_{t-1} \equiv b_{t-1}$ ist, für den Modul q.

Es giebt ferner für den Modul $f(\alpha)$ stets primitive Wurzeln $g(\alpha)$, in der Art, dafs die verschiedenen Potenzen einer solchen primitiven Wurzel

$$(1.) \qquad g(\alpha),\ g(\alpha)^2,\ g(\alpha)^3,\ \ldots\ g(\alpha)^{q^t-2},$$

alle verschiedenen Reste für den Modul $f(\alpha)$, mit alleiniger Ausnahme des Restes 0, vollständig erschöpfen. Der Beweis dieser Behauptung kann eben so leicht und nach derselben Methode gegeben werden, nach welcher man in den Elementen der Zahlentheorie die Existenz der primitiven Wurzeln für die gewöhnlichen Primzahlen beweiset; weshalb ich denselben übergehe.

Wenn $F(\alpha)$ eine beliebige, jedoch nicht durch den Modul $f(\alpha)$ theilbare complexe Zahl bezeichnet, so ist

$$F(\alpha)^{q^t-1} \equiv 1, \quad \text{Mod.} f(\alpha).$$

Wenn ferner $g(\alpha)$ eine primitive Wurzel ist, so hat man

$$g(\alpha)^{\frac{1}{2}(q^t-1)} \equiv -1, \quad g(\alpha)^{\frac{q^t-1}{\lambda}} \equiv \alpha^k, \text{ Mod.} f(\alpha);$$

wo k niemals congruent Null ist, für den Modul λ. Es kann auch die primitive Wurzel $g(\alpha)$, welche in dem Folgenden einfach durch g bezeichnet werden soll, immer so angenommen werden, dafs $k = 1$ ist und dafs man also

$$g^{\frac{q^t-1}{\lambda}} \equiv \alpha, \text{ Mod.} f(\alpha)$$

hat. Wir wollen ein für allemal festsetzen, dafs die primitive Wurzel g *immer* dieser Bedingung gemäfs angenommen werden soll. Die Beweise der in diesen Congruenzen enthaltenen Sätze, welche nach den in der Theorie der complexen Zahlen gebräuchlichen Methoden leicht sind, glaube ich ebenfalls hier übergehen zu können. Zu bemerken ist noch, dafs die primitive Wurzel g niemals eine nichtcomplexe Zahl sein kann, aufser in dem Falle $t = 1$, für welchen die primitiven Wurzeln des Modul $f(\alpha)$ genau dieselben sind, wie die primitiven Wurzeln der gewöhnlichen Primzahl $p = Nf(\alpha)$.

Ist $g^i \equiv \varphi(\alpha)$, Mod. $f(\alpha)$, so soll i hier ebenfalls der Index von $\varphi(\alpha)$ für den Mod. $f(\alpha)$ heifsen und durch Ind. $\varphi(\alpha)$ bezeichnet werden. Es gelten dann für die Indices ebenfalls die Gleichungen

$$\text{Ind.}\varphi(\alpha) + \text{Ind.}F(\alpha) \equiv \text{Ind.}(\varphi(\alpha)F(\alpha)), \quad \text{Mod.} q^t - 1 \quad \text{und}$$
$$n\,\text{Ind.}\varphi(\alpha) \equiv \text{Ind.}(\varphi(\alpha)^n), \quad \text{Mod.} q^t - 1.$$

Nachdem Dieses vorbereitet ist, gehe ich zu dem Hauptgegenstande dieses Paragraphen über, nämlich zu der Erweiterung der Theorie der *Kreistheilung;* und zwar knüpfe ich dieselbe an die complexe Zahl $\psi_r(\alpha)$ der Kreistheilung an, welche schon oben definirt wurde und für welche die Lehre von der Kreistheilung folgende sechs Ausdrücke giebt:

$$\psi_r(\alpha) = \Sigma\alpha^{h-(r+1)\,\text{Ind.}(g^h+1)},$$
$$\psi_r(\alpha) = \Sigma\alpha^{h+r\,\text{Ind.}(g^h+1)},$$
$$\psi_r(\alpha) = \Sigma\alpha^{rh-(r+1)\,\text{Ind.}(g^h+1)},$$
$$\psi_r(\alpha) = \Sigma\alpha^{-(r+1)h+r\,\text{Ind.}(g^h+1)},$$
$$\psi_r(\alpha) = \Sigma\alpha^{rh+\text{Ind.}(g^h+1)},$$
$$\psi_r(\alpha) = \Sigma\alpha^{-(r+1)h+\text{Ind.}(g^h+1)};$$

wo die Summenzeichen sich auf die Werthe $h = 0, 1, 2, \ldots p-2$ erstrecken, mit Ausschlufs des Werths $h = \frac{1}{2}(p-1)$, für welchen $g^h + 1 \equiv 0$, Mod. p, sein würde.

Die hier auszuführende Erweiterung der Theorie der Kreistheilung soll nun darin bestehen, dafs in diesen Ausdrücken des $\psi_r(\alpha)$ die primitive Wurzel g der Primzahl p als primitive Wurzel für den complexen Modul $f(\alpha)$ aufgefafst und demgemäfs auch das Zeichen Ind. auf denselben Modul $f(\alpha)$ bezogen werden soll. Die Summen werden dann in Beziehung auf die Werthe $h = 0, 1, 2, 3, \ldots q^t - 2$ zu nehmen sein, mit Ausschlufs des Werths $h = \frac{1}{2}(q^t-1)$, für welchen $g^h + 1 \equiv 0$, Mod. $f(\alpha)$ sein und folglich Ind. (g^h+1) keinen Sinn haben würde. Die complexen Zahlen $\psi_r(\alpha)$, in diesem neuen Sinne genommen, sollen zur Unterscheidung von denen der Kreistheilung durch $\Psi_r(\alpha)$ bezeichnet werden. Die obigen sechs verschiedenen Ausdrücke von $\psi_r(\alpha)$ stimmen auch bei dieser neuen Auffassung der Zeichen g und Ind. ganz miteinander überein; in der Art, dafs sie alle nur verschiedene Ausdrücke einer und derselben complexen Zahl sind. Es wird also hinreichen, nur einen dieser Ausdrücke zu untersuchen, zu welchem ich den letzten wähle. Ich setze also

$$\Psi_r(\alpha) = \Sigma \alpha^{-(r+1)h + \text{Ind.}(g^h+1)};$$

wo das Summenzeichen sich auf die Werthe $h = 0, 1, 2, 3, \ldots q^t - 2$ erstreckt; mit Ausschlufs von $h = \frac{1}{2}(q^t-1)$, und wo g eine primitive Wurzel für den Modul $f(\alpha)$ bedeutet, auch das Zeichen Ind. sich auf denselben Modul und dieselbe primitive Wurzel bezieht. Der Modul $f(\alpha)$ selbst ist ein complexer idealer Primfactor der zum Exponenten t gehörenden gewöhnlichen Primzahl q.

Aus dieser Definition der complexen Zahl $\Psi_r(\alpha)$ folgt zunächst unmittelbar

$$\Psi_{r+\lambda}(\alpha) = \Psi_r(\alpha), \quad \Psi_v(\alpha) = -1, \quad \Psi_{\lambda-1}(\alpha) = -1.$$

Setzt man ferner α^q statt α, so erhält man

$$\Psi_r(\alpha^q) = \Sigma \alpha^{-(r+1)qh + q\,\text{Ind.}(g^h+1)}.$$

Es ist aber $(g^h+1)^q \equiv g^{hq} + 1$, für den Modul q, und also auch für den Modul $f(\alpha)$, welcher ein Factor von q ist; demnach ist auch $q\,\text{Ind.}(g^h+1) \equiv \text{Ind.}(g^{qh}+1)$, Mod. (q^t-1). Setzt man Dieses in den obigen Ausdruck des $\Psi_r(\alpha^q)$ und $k \equiv qh$, Mod. (q^t-1), so entsprechen den Werthen $h = 0, 1, 2, \ldots \ldots q^t-2$, mit Ausschlufs von $h = \frac{1}{2}(q^t-1)$, genau die Werthe $k = 0, 1, 2, 3, \ldots q^t-2$, mit Ausschlufs von $k = \frac{1}{2}(q^t-1)$, wenn auch in anderer Ordnung genommen,

und darum ist

$$\Psi_r(\alpha^q) = \Sigma\alpha^{-(r+1)k+\mathrm{Ind.}(g^k+1)},$$

also

$$\Psi_r(\alpha^q) = \Psi_r(\alpha);$$

aus welcher Gleichung auch sogleich die allgemeinere

$$\Psi_r(\alpha^{q^h}) = \Psi_r(\alpha)$$

für jeden beliebigen Werth des h folgt. Man sieht hieraus, dafs die complexe Zahl $\Psi_r(\alpha)$ nicht die einzelnen Wurzeln α, α^2, α^3, ... $\alpha^{\lambda-1}$ in sich enthält, sondern nur die ***Perioden*** derselben, welche je t Glieder umfassen. Dies ist die ***erste wesentliche Grund-Eigenschaft*** der complexen Zahl $\Psi_r(\alpha)$.

Multiplicirt man die beiden reciproken complexen Zahlen $\Psi_r(\alpha)$ und $\Psi_r(\alpha^{-1})$ miteinander, so wird das Product derselben durch die Doppelsumme

$$\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = \Sigma\Sigma\alpha^{-(r+1)(h-k)+\mathrm{Ind.}(g^h+1)-\mathrm{Ind.}(g^k+1)}$$

ausgedrückt, für $h = 0, 1, 2, 3, \ldots q^t-2$, $k = 0, 1, 2, \ldots q^t-2$; mit Ausschlufs von $h = \frac{1}{2}(q^t-1)$ und $k = \frac{1}{2}(q^t-1)$. Ich scheide aus dieser Doppelsumme zunächst alle die Werth-Verbindungen von h und k aus, für welche $h = k$ ist. Ihrer finden offenbar q^t-2 Statt, und es wird für dieselben die Potenz des α unter dem doppelten Summenzeichen nur gleich ***Eins***. Man hat also

$$\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^t-2+\Sigma\Sigma\alpha^{-(r+1)(h-k)+\mathrm{Ind.}(g^h+1)-\mathrm{Ind.}(g^k+1)}$$

für alle ganzzahligen Werthe des h und k von 0 bis q^t-2 einschliefslich; mit Ausschlufs der Werthe $\frac{1}{2}(q^t-1)$ und der Werth-Verbindungen, für welche $h = k$ ist. Man transformire nun diese Doppelsumme, indem man

$$g^{k-h} \equiv g^{k'}, \quad \frac{g^k+1}{g^h+1} \equiv g^{h'}, \quad \mathrm{Mod.}\, f(\alpha),$$

setzt, so erhält man

$$\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^l-2+\Sigma\Sigma\alpha^{(r+1)k'-h'}.$$

Die Summenzeichen beziehen sich hier auf die verschiedenen Werthe des k' und h', und es sind denselben alle Werthe von 1 bis q^t-2 einschliefslich zu geben; mit Ausschlufs derjenigen Werth-Verbindungen, für welche $h' = k'$ ist. Vermöge der Congruenzen, welche die neuen Unbestimmten k' und h' durch die alten k und h ausdrücken, entspricht nämlich jeder einzelnen Verbindung der Werthe von h und k eine, und nur eine Werth-Verbindung der angegebenen Werthe von h' und k'; und eben so, umgekehrt: jeder beliebigen Werth-Verbindung des h' und k' entspricht unter den angegebenen Bedingungen eine, und nicht mehr als eine der Werth-Verbindungen des h und k. Ich

nehme jetzt mit dieser Doppelsumme noch die kleine Änderung vor, dafs ich sie mit auf diejenigen Werth-Verbindungen erstrecke, welche $h' = k'$ geben. Dies wird ohne Beeinträchtigung der Richtigkeit der obigen Gleichung geschehen können, wenn die Summe aller, der Werth-Verbindung $h' = k'$ entsprechenden Glieder, nämlich $\Sigma\alpha^{rk'}$, in Abzug gebracht wird. Es ist demnach

$$\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^t - 2 - \Sigma\alpha^{rk'} + \Sigma\Sigma\alpha^{(r+1)k'-h'},$$

für $h' = 1, 2, 3, \ldots q^t - 2$, $k' = 1, 2, 3, \ldots q^t - 2$. Die Werthe des h' und k' sind nun gänzlich unabhängig von einander, und man kann die Summation in Beziehung auf beide einzeln ausführen.

Summirt man zuerst in Beziehung auf h', so erhält man

$$\Sigma\alpha^{-h'} = \alpha^{-1} + \alpha^{-2} + \alpha^{-3} + \cdots + \alpha^{-(q^t-2)} = -1,$$

also

$$\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^t - 2 - \Sigma\alpha^{rk'} - \Sigma\alpha^{(r+1)k'}.$$

Schliefst man die beiden besonderen Fälle aus, wo $r \equiv 0$, oder $r+1 \equiv 0$, Mod. λ, so ist wieder jede dieser beiden Summen gleich -1, und man hat als Endresultat:

$$\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^t;$$

welches die *zweite Grund-Eigenschaft* der complexen Zahl $\Psi_r(\alpha)$ ist, deren Analogie mit der entsprechenden Eigenschaft der complexen Zahlen der Kreistheilung $\psi_r(\alpha)$ auf der Hand liegt.

In den beiden besondern Fällen, $r \equiv 0$ oder $r+1 \equiv 0$, Mod. λ wird allemal eine der beiden Summen $\Sigma\alpha^{k'r}$ oder $\Sigma\alpha^{(r+1)k'}$, weil sie alsdann aus lauter *Einsen* besteht, gleich $q^t - 2$, die andere aber gleich -1. Man erhält demnach

$$\Psi_0(\alpha)\Psi_0(\alpha^{-1}) = 1, \qquad \Psi_{-1}(\alpha)\Psi_{-1}(\alpha^{-1}) = 1;$$

welches mit den oben angegebenen, aus der Definition unmittelbar folgenden Werthen von $\Psi_0(\alpha) = -1$ und $\Psi_{-1}(\alpha) = -1$ übereinstimmt, aber nichts Neues lehrt.

Nach der *ersten* Grund-Eigenschaft der hier behandelten complexen Zahlen ist:

$$\Psi_r(\alpha^{q^h}) = \Psi_r(\alpha).$$

Wenn nun t eine *gerade* Zahl ist, so ist, weil q zum Exponenten t gehört, $q^t \equiv 1$ und $q^{\frac{1}{2}t} \equiv -1$, Mod. λ. Es ergiebt sich daher, wenn $h = \frac{1}{2}t$ gesetzt wird:

$$\Psi_r(\alpha^{-1}) = \Psi_r(\alpha);$$

woraus, vermöge der *zweiten* Grund-Eigenschaft dieser complexen Zahlen,

$$\Psi_r(\alpha) = q^{\frac{1}{2}t}$$

folgt. Für den Fall, dafs t eine *gerade* Zahl ist, ist also die Zahl $\Psi_r(\alpha)$ in Wahrheit nicht eine complexe Zahl, sondern einer Potenz der gewöhnlichen Primzahl q gleich. Das Haupt-Interesse der gegenwärtigen Untersuchung liegt demnach nur in dem Falle, wo t *ungerade* ist, in welchem $\Psi_r(\alpha)$ nicht nur scheinbar, sondern auch *wirklich* eine complexe Zahl ist.

Zur vollständigen Erkenntnifs der complexen Zahlen $\Psi_r(\alpha)$, namentlich für den Fall wo t *ungerade* ist, gehört noch die Zerlegung derselben in ihre complexen, idealen oder wirklichen Primfactoren, welche, weil nach der *zweiten* Grund-Eigenschaft derselben das Product zweier reciproker Zahlen einer Potenz von q gleich ist, nur die idealen Primfactoren des q sein können; also nur die Primfactoren $f(\alpha)$, $f(\alpha^\gamma)$, $f(\alpha^{\gamma^2})$, ... u. s. w. Von diesen sind bekanntlich, da q zum Exponenten t gehört, je t einander gleich, so dafs nur $\frac{\lambda-t}{t}$ wesentlich verschiedene Primfactoren vorhanden sind; als welche, wenn $\frac{\lambda-1}{t} = \tau$ gesetzt wird (welche Bedeutung der Buchstabe τ in dem Folgenden überall beibehalten soll), die Primfactoren

$$f(\alpha),\ f(\alpha^\gamma),\ f(\alpha^{\gamma^2}),\ \ldots f(\alpha^{\gamma^{\tau-1}})$$

genommen werden können. Man hat daher

$$\Psi_r(\alpha) = E(\alpha) f(\alpha)^m . f(\alpha^\gamma)^{m_1} \ldots f(\alpha^{\gamma^{\tau-1}})^{m_{\tau-1}},$$

wo $E(\alpha)$ eine *Einheit* ist und $m, m_1, \ldots m_{\tau-1}$ die noch zu bestimmenden Exponenten sind, welche angeben, wievielmal jeder der verschiedenen Primfactoren des q in $\Psi_r(\alpha)$ enthalten ist.

Mittels der zweiten Grund-Eigenschaft der complexen Zahl $\Psi_r(\alpha)$ kann nun sogleich die eine Hälfte dieser Exponenten durch die andere Hälfte ausgedrückt werden. Wenn nämlich, wie hier vorausgesetzt wird, t eine *ungerade* Zahl ist, so ist τ eine *gerade* Zahl, weil $\lambda - 1 = t\tau$ ist. Verwandelt man α in α^{-1} und erwägt, dafs $f(\alpha^{\gamma^h}) = f(\alpha^{\gamma^{h+\tau}}) = f(\alpha^{\gamma^{h+2\tau}})$ u. s. w. ist, so erhält man

$$\Psi_r(\alpha^{-1}) = E(\alpha^{-1}) . f(\alpha)^{m_{\frac{1}{2}\tau}} . f(\alpha^\gamma)^{m_{\frac{1}{2}\tau+1}} \ldots f(\alpha^{\gamma^{\tau-1}})^{m_{\frac{1}{2}\tau-1}}.$$

Multiplicirt man diesen Ausdruck mit dem vorigen, so erhält man, vermöge der Gleichung $\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^t$, für die Exponenten $m, m_1, m_2, \ldots m_{\tau-1}$ folgende Gleichungen:

$$m + m_{\frac{1}{2}\tau} = t,\quad m_1 + m_{\frac{1}{2}\tau+1} = t,\quad \ldots\quad m_{\frac{1}{2}\tau-1} + m_{\tau-1} = t.$$

Also ist die Summe je zweier dieser Exponenten, deren Stellenzeiger um $\frac{1}{2}\tau$ unterschieden sind, immer gleich t.

Die vollständige Bestimmung dieser Exponenten ist etwas mühsam, führt aber, wie sich zeigen wird, zu einem ziemlich einfachen und sehr eleganten Resultate. Es müssen dazu Congruenzen angewendet werden, deren Modul eine Potenz der complexen Primzahl $f(\alpha)$ ist, und es kommt dabei hauptsächlich darauf an, die Wurzel α durch eine Potenz der primitiven Wurzel g zu ersetzen, welcher sie in Beziehung auf den Modul $f(\alpha)^n$ congruent ist. Dies geschieht auf folgende Weise. Wenn der Kürze wegen $\nu = \frac{q^t-1}{\lambda}$ gesetzt wird (welche Bedeutung der Buchstabe ν hier überall beibehalten soll), so ist, wie oben gezeigt worden:

$$g^\nu \equiv \alpha, \text{ Mod.} f(\alpha),$$

oder, wenn man diese Congruenz als Gleichung schreibt:

$$g^\nu = \alpha + wf(\alpha).$$

Erhebt man dies zur Potenz q, so ist

$$g^{\nu q} = \alpha^q + q\alpha^{q-1}wf(\alpha) + \frac{q(q-1)}{1.2}\alpha^{q-2}w^2f(\alpha)^2 + \cdots$$

und, da q den Primfactor $f(\alpha)$ einmal enthält:

$$g^{\nu q} \equiv \alpha^q, \text{ Mod.} f(\alpha)^2.$$

Auf dieselbe Weise weiter schliefsend, findet man, dafs allgemein für jeden Werth des k die Congruenz

$$g^{\nu q^k} \equiv \alpha^{q^k}, \text{ Mod.} f(\alpha)^{k+1},$$

Statt hat; und wenn für k ein Vielfaches von t genommen wird, da $q^{nt} \equiv 1$, Mod. λ ist, so ergiebt sich

$$g^{\nu q^{nt}} \equiv \alpha, \text{ Mod.} f(\alpha)^{nt+1};$$

wo n eine beliebige positive ganze Zahl ist.

Nachdem Dieses vorbereitet worden, verwandle ich in dem ursprünglichen Ausdrucke, durch welchen $\Psi_r(\alpha)$ definirt wurde, α in $\alpha^{\gamma^{-i}}$. Dann ist

$$\Psi_r(\alpha^{\gamma^{-i}}) = \Sigma\alpha^{-(r+1)\gamma^{-i}h+\gamma^{-i}\,\text{Ind.}(g^h+1)}.$$

Man setze ferner $r+1 \equiv \gamma^\varrho$, Mod. λ, so wird $(r+1)\gamma^{-i} \equiv \gamma^{\varrho-i}$, und wenn wieder γ_k den kleinsten positiven Rest von γ^k für den Modul λ bezeichnet, so ist $(r+1)\gamma^{-i} \equiv \gamma_{\varrho-i}$, $\gamma^{-i} \equiv \gamma_{-i}$, Mod. λ. Endlich setze man noch Ind. $(g^{hq^{nt}}+1)$ statt Ind. (g^h+1); welches demselben vollkommen gleichbedeutend ist, indem $g^{q^{nt}} \equiv g$ ist, für den Modul $f(\alpha)$. Dann erhält man

$$\Psi_r(\alpha^{\gamma^{-i}}) = \Sigma\alpha^{-\gamma_{\varrho-i}h+\gamma_{-i}\,\text{Ind.}(g^{hq^{nt}}+1)}.$$

Wird nun die Congruenz $g^{\nu q^{nt}} \equiv \alpha$, Mod. $f(\alpha)^{nt+1}$ angewendet, so verwandelt sich diese Gleichung in folgende Congruenz:

$$\Psi_r(\alpha^{\gamma^{-i}}) \equiv \Sigma g^{-\gamma_{\varrho-i}\nu q^{nt}h} . g^{\gamma_{-i}\nu q^{nt}\,\mathrm{Ind.}(g^{hq^{nt}}+1)}, \text{ Mod. } f(\alpha)^{nt+1}.$$

Es ist aber

$$g^{\mathrm{Ind.}(g^{hq^{nt}}+1)} \equiv g^{hq^{nt}}+1, \text{ Mod. } f(\alpha),$$

woraus

$$g^{q^{nt}\,\mathrm{Ind.}(g^{hq^{nt}}+1)} \equiv (g^{hq^{nt}}+1)^{q^{nt}}, \text{ Mod. } f(\alpha)^{nt+1}.$$

folgt, also

$$\Psi_r(\alpha^{\gamma^{-i}}) \equiv \Sigma g^{-\gamma_{\varrho-i}\nu q^{nt}h}(g^{hq^{nt}}+1)^{\gamma_{-i}\nu q^{nt}}, \text{ Mod. } f(\alpha)^{nt+1}.$$

Das Summenzeichen erstreckt sich auf die Werthe $0, 1, 2, \ldots q^t-2$ von h und es ist hier nicht weiter nöthig, den Werth $h = \frac{1}{2}(q^t-1)$ auszuschliefsen, weil für denselben der Ausdruck unter dem Summenzeichen congruent Null ist, für den Mod. $f(\alpha)^{nt+1}$.

Nun ist die unter dem Summenzeichen stehende Potenz des Binoms $g^{hq^{nt}}+1$ nach dem binomischen Lehrsatze zu entwickeln. Wird dabei durch $\Pi(m)$ das Product der Zahlen $1.2.3.4 \ldots m$ bezeichnet, so erhält man die daraus hervorgehende Doppelsumme in folgender Form:

$$\Psi_1(\alpha^{\gamma^{-i}}) \equiv \Sigma\Sigma \frac{\Pi(\gamma_{-i}\nu q^{nt})}{\Pi(k)\,\Pi(\gamma_{-i}\nu q^{nt}-k)} g^{(-\gamma_{\varrho-i}\nu+k)hq^{nt}}, \text{ Mod. } f(\alpha)^{nt+1},$$

für $h = 0, 1, 2, 3, \ldots q^t-2$ und $k = 0, 1, 2, 3, \ldots \gamma_{-i}\nu q^{nt}$. Setzt man für einen Augenblick $-\gamma_{\varrho-i}\nu q^{nt}+k = l$ und führt die Summation in Beziehung auf h aus, so ist allgemein

$$\Sigma g^{lhq^{nt}} = \frac{1-g^{l(q^t-1)q^{nt}}}{1-g^{lq^{nt}}},$$

also immer congruent Null für den Modul $f(\alpha)^{nt+1}$; mit Ausnahme der Fälle, wo l ein Vielfaches von q^t-1 ist. Es sei also

$$l = -\gamma_{\varrho-i}\nu q^{nt}+k = s(q^t-1) = s\lambda\nu,$$

so ist

$$\Psi_r(\alpha^{\gamma^{-i}}) \equiv \Sigma \frac{(q^t-1)\,\Pi(\gamma_{-i}\nu q^{nt})}{\Pi(\gamma_{\varrho-i}\nu+s\lambda\nu)\,\Pi(\gamma_{-i}\nu q^{nt}-\gamma_{\varrho-i}\nu-s\lambda\nu)}, \text{ Mod. } f(\alpha)^{\lambda n+1};$$

wo sich das Summenzeichen auf alle ganzzahligen Werthe von s bezieht, für welche weder $\gamma_{\varrho-i}\nu+s\lambda\nu$, noch $\gamma_{-i}\nu q^{nt}-\gamma_{\varrho-i}\nu-s\lambda\nu$ negativ wird. Wird endlich noch $s = \frac{\gamma_{\varrho-i}(q^{nt}-1)}{\lambda} - z$ gesetzt und aufserdem α in α^{γ^i} verwandelt, so ergiebt sich

$$\Psi_r(\alpha) \equiv \Sigma \frac{(q^t-1)\,\Pi(\gamma_{-i}\nu q^{nt})}{\Pi(\gamma_{\varrho-i}\nu q^{nt}-\lambda\nu z)\,\Pi((\gamma_{-i}-\gamma_{\varrho-i})\nu q^{nt}+\lambda\nu z)}$$

für den Modul $f(\alpha^{\gamma_i})^{n\lambda+1}$; wo das Summenzeichen auf alle ganzzahligen Werthe des z sich bezieht, für welche weder $\gamma_{\varrho-i}q^{nt}-\lambda z$, noch $(\gamma_{-i}-\gamma_{\varrho-i})q^{nt}+\lambda z$ negativ wird.

Durch diese Congruenz, in welcher n beliebig grofs angenommen werden kann, wird die Untersuchung, wievielmal $\Psi_r(\alpha)$ den complexen Primfactor $f(\alpha^{\gamma_i})$ enthält, darauf zurückgeführt, zu untersuchen, wievielmal diese Summe, welcher $\Psi_r(\alpha)$ congruent und welche eine nichtcomplexe Zahl ist, den Factor q enthält; denn es ist klar, dafs, wenn n hinreichend grofs angenommen wird, die Summe den Factor q genau ebensovielmal enthalten mufs, als $\Psi_r(\alpha)$ den Factor $f(\alpha^{\gamma_i})$ enthält, welcher ein Primfactor von q und dessen $(n\lambda+1)$te Potenz der Modul dieser Congruenz ist.

Zu diesem Zwecke werde ich zunächst beweisen, dafs, unter der Voraussetzung, $\gamma_{-i}-\gamma_{\varrho-i}$ sei positiv, dasjenige Glied dieser Summe, welches dem Werthe $z=0$ entspricht, von allen die niedrigste Potenz von q als Factor enthält; in der Art, dafs jedes beliebige andere Glied als dieses, eine höhere Potenz von q als Factor enthalten mufs. Demgemäfs wird die Untersuchung, wievielmal die ganze Summe den Factor q enthält, darauf reducirt sein, zu untersuchen, wievielmal das eine dem Werthe $z=0$ entsprechende Glied der Summe den Factor q enthält.

Ich bediene mich hier des folgenden, wenn nicht bekannten, so doch leicht zu beweisenden Satzes:

Lehrsatz: Wenn q eine Primzahl ist und die Zahl A auf die Form

$$A = a+a_1q+a_2q_2+\cdots+a_{k-1}q^{k-1}$$

gebracht wird, in der Art, dafs die Zahlen a, a_1, a_2, ... a_{k-1} nicht negativ und alle kleiner als q sind (welches nichts anderes ist, als die Zahl A nach $q$theiligem Zahlensysteme geschrieben), so ist die Anzahl der in dem Producte

$$1.2.3.4\ldots A = \Pi(A)$$

enthaltenen Factoren q gleich

$$\frac{A-(a+a_1+a_2+\cdots+a_{k-1})}{q-1}.$$

Mittels dieses Satzes läfst sich nun folgendermaafsen untersuchen, wievielmal der Factor q in dem Binomialcoëfficienten $\frac{\Pi(A+B)}{\Pi(A)\Pi(B)}$ enthalten ist. Man giebt beiden Zahlen A und B diese Form, nämlich

$$A = a + a_1 q + a_2 q^2 + \cdots + a_{k-1} q^{k-1} \quad \text{und}$$
$$B = b + b_1 q + b_2 q^2 + \cdots + b_{k-1} q^{k-1},$$

so dafs die Zahlen a, α_1, a_2, ... a_{k-1}, b, b_1, b_2, ... b_{k-1} alle kleiner als q und nicht negativ sind, und bildet folgende Reihe von Gleichungen:

$$\begin{aligned} a + b &= \varepsilon q + c, \\ \varepsilon + a_1 + b_1 &= \varepsilon_1 q + c_1, \\ \varepsilon_1 + a_2 + b_2 &= \varepsilon_2 q + c_2, \\ &\cdots \\ \varepsilon_{k-2} + a_{k-1} + b_{k-1} &= \varepsilon_{k-1} q + c_{k-1}, \end{aligned}$$

in welchen die Zahlen c, c_1, c_2, ... c_{k-1} derselben Bedingung unterworfen sein sollen, dafs sie nicht negativ und kleiner als q sind, und in welchen demgemäfs die Zahlen ε, ε_1, ε_2, ... ε_{k-1} nur die Werthe ***Null*** oder ***Eins*** erhalten können. Addirt man alle diese Gleichungen, nachdem die erste mit 1, die zweite mit q, die dritte mit q^2, u. s. w. multiplicirt worden, so erhält man

$$A + B = c + c_1 q + c_2 q^2 + \cdots + c_{k-1} q^{k-1} + \varepsilon_{k-1} q^k.$$

Nennt man N die Anzahl, wievielmal der Factor q in dem Binomialcoëfficienten $\frac{\Pi(A+B)}{\Pi(A)\Pi(B)}$ enthalten ist, so ergiebt sich nach dem obigen Satze:

$$N = \frac{A+B-(c+c_1+\cdots+c_{k-1}+\varepsilon_{k-1})}{q-1} - \frac{(A-(a+a_1+\cdots+a_{k-1}))}{q-1} - \frac{(B-(b+b_1+\cdots+b_{k-1}))}{q-1},$$

oder, vereinfacht,

$$N = \frac{a+a_1+\cdots+a_{k-1}+b+b_1+\cdots+b_{k-1}-c-c_1-\cdots-c_{k-1}}{q-1},$$

und da durch Addition des aufgestellten Systems von Gleichungen

$$\begin{aligned} a + a_1 + \cdots + a_{k-1} + b + b_1 + \cdots + b_{k-1} - c - c_1 - \cdots - c_{k-1} \\ = (q-1)(\varepsilon + \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{k-1}) \end{aligned}$$

ist, so erhält man

$$N = \varepsilon + \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{k-1}.$$

Um die Anwendung auf die vorliegende Summe zu machen, welche dem $\Psi_r(\alpha)$ congruent ist und deren einzelne Glieder Binomialcoëfficienten sind, setze man

$$A = \gamma_{\varrho-i} \nu q^{nt} - \lambda \nu z, \quad B = (\gamma_{-i} - \gamma_{\varrho-i}) \nu q^{nt} + \lambda \nu z,$$
$$A + B = \gamma_{-i} \nu q^{nt},$$

so wird

$$\gamma_{-i} \nu q^{nt} = c + c_1 q + c_2 q^2 + \cdots + c_{k-1} q^{k-1} + \varepsilon_{k-1} q^k,$$

woraus zu sehen, dafs die Zahlen $c, c_1, c_2, \ldots$, bis c_{nt-1} einschliefslich, gleich ***Null*** sein müssen. Ist nun aufserdem auch $a = a_1 = a_2 = \ldots = a_{nt-1} = 0$ und $b = b_1 = b_2 = \ldots = b_{nt-1} = 0$, so folgt aus dem die Zahlen a, b, c und ε verbindenden Systeme von Gleichungen, dafs auch die Zahlen $\varepsilon, \varepsilon_1, \varepsilon_2, \ldots \varepsilon_{nt-1}$ gleich ***Null*** sind. Auch werden durch diese Bestimmungen die Werthe der übrigen Zahlen $\varepsilon_{nt}, \varepsilon_{nt+1}, \ldots \varepsilon_{k-1}$ im Allgemeinen gar nicht verändert, und nur in dem ganz besondern Falle, wo in der Gleichung

$$\varepsilon_{nt-1} + a_{nt} + b_{nt} = \varepsilon_{nt} q + c_{nt}$$

$a_{nt} + b_{nt} = q - 1$ wäre, würde ε_{nt} von ε_{nt-1} abhängig sein, indem, wenn ε_{nt-1} nicht gleich ***Null***, sondern gleich ***Eins*** wäre, auch ε_{nt} den Werth ***Eins*** statt ***Null*** erhalten würde. Durch andere als die angenommenen Bestimmungen der Werthe $\varepsilon, \varepsilon_1, \varepsilon_2, \ldots \varepsilon_{nt-1}$ können also die Werthe der folgenden Zahlen in einem besondern Falle zwar ***erhöht***, niemals aber ***erniedrigt*** werden. Für diejenigen Glieder der zu untersuchenden Summe von Binomialcoëfficienten, für welche die Bedingungen $a = a_1 = a_2 = \cdots = a_{nt-1} = 0$ und $b = b_1 = b_2 = \cdots = b_{nt-1} = 0$ erfüllt werden, mufs demnach nothwendig die Totalsumme aller ε, nämlich $\varepsilon + \varepsilon_1 + \cdots + \varepsilon_{k-1}$, kleiner sein als für alle andern; d. h. die Anzahl der in solchen Gliedern enthaltenen Factoren q mufs nothwendig kleiner sein, als die Anzahl der in einem der andern Glieder dieser Summe enthaltenen Factoren q.

Vermöge der Bedingungen $a = a_1 = \cdots = a_{nt-1} = 0$ und $b = b_1 = \cdots = b_{nt-1} = 0$ ist

$$\gamma_{\varrho-i}\nu q^{nt} - \lambda\nu z = q^{nt}(a_{nt} + a_{nt+1}q + \cdots + a_{k-1}q^{k-nt-1}) \text{ und}$$
$$(\gamma - \gamma_{\varrho-i})\nu q^{nt} + \lambda\nu z = q^{nt}(b_{nt} + b_{nt+1}q + \cdots + b_{k-1}q^{k-nt-1});$$

woraus folgt, dafs z durch q^{nt} theilbar sein mufs. Setzt man daher $z = q^{nt}z'$, und beachtet, dafs $\gamma_{\varrho-i} < \lambda$ und nach der obigen Voraussetzung auch $\gamma_{-i} - \gamma_{\varrho-1}$ positiv und $< \lambda$ ist, so zeigt sich aus den Bedingungen, dafs $\gamma_{\varrho-i}q^{nt} - \lambda z$ und $(\gamma_{-i} - \gamma_{\varrho-i})q^{nt} + \lambda z$ nicht negativ werden dürfen, dafs $z' = 0$, also auch $z = 0$ der einzige Werth von z ist, welcher diesen Bedingungen genügt. Da ferner jeder andere Theil der zu untersuchenden Summe den Factor q öfter enthält, als der dem Werthe $z = 0$ angehörende, so folgt, dafs die ganze Summe den Factor q genau eben so oft enthalten mufs, als dieser eine Theil derselben, und dafs also endlich die complexe Zahl $\Psi_r(\alpha)$ den complexen Factor $f(\alpha^{\gamma^i})$ genau eben so vielemal enthält, als der Binomial-

coëfficient

$$\frac{\Pi(\gamma_{-i}\nu q^{nt})}{\Pi(\gamma_{\varrho-i}\nu q^{nt})\,\Pi(\gamma_{-i}-\gamma_{\varrho-i})\nu q^{nt}}$$

den Factor q.

Um diese Anzahl mittels des obigen Satzes zu finden, bringe ich die Zahl $\gamma_h\nu$, in welcher $\nu=\frac{q^t-1}{\lambda}$ ist, auf die Form

$$\gamma_h\nu = d+d_1q+d_2q^2+\cdots+d_{t-1}q^{t-1};$$

wo d, d_1, $\ldots$ d_{t-1} alle kleiner als q und nicht negativ sind. Alsdann ist die Anzahl der in dem Producte $\Pi(\gamma_h\nu q^{nt})$ enthaltenen Factoren q gleich

$$\frac{\gamma_h\nu q^{nt}-(d+d_1+d_2+\cdots+d_{t-1})}{q-1}.$$

Multiplicirt man den Ausdruck des $\gamma_h\nu$ mit λ, so erhält man

$$\gamma_h q^t = \gamma_h+\lambda d+\lambda d_1q+\lambda d_2q^2+\cdots+\lambda d_{t-1}q^{t-1}.$$

Hieraus folgt zunächst, dafs $\gamma_h+\lambda d$ durch q theilbar ist. Setzt man also $\gamma_h+\lambda d=\delta q$, so folgt weiter, dafs auch $\delta+\lambda d_1$ durch q theilbar sein mufs u. s. w. Man erhält also folgende Reihe von Gleichungen:

$$\begin{aligned}
\gamma_h + \lambda d &= \delta q,\\
\delta + \lambda d_1 &= \delta_1 q,\\
\delta_1 + \lambda d_2 &= \delta_2 q,\\
&\cdots\\
\delta_{t-2}+\lambda d_{t-1} &= \delta_{t-1}q;
\end{aligned}$$

in welchen die Zahlen δ, δ_1, δ_2, $\ldots$ δ_{t-1} alle kleiner als λ und positiv sein müssen. Macht man aus diesen Gleichungen Congruenzen für den Modul λ, und ersetzt q durch eine Potenz der primitiven Wurzel γ (welche, weil q zum Exponenten t gehört und $\tau=\frac{\lambda-1}{t}$ ist, nothwendig $q\equiv\gamma^{m\tau}$ sein mufs, wo m eine relative Primzahl zu t ist): so erhält man

$$\gamma^h\equiv\delta\gamma^{m\tau},\quad \delta\equiv\delta_1\gamma^{m\tau},\quad \ldots\quad \delta_{t-2}\equiv\delta_{t-1}\gamma^{m\tau},$$

also

$$\delta\equiv\gamma^{h+m\tau},\ \delta_1\equiv\gamma^{h-2m\tau},\ \ldots\ \delta_{t-1}\equiv\gamma^h,$$

und da alle diese Zahlen positiv und kleiner als λ sind:

$$\delta=\gamma_{h-m\tau},\ \delta_1=\gamma_{h-2m\tau},\ \ldots\ \delta_{t-1}=\gamma_h.$$

Addirt man alle die Gleichungen, durch welche die Zahlen d, d_1, $\ldots$ d_{t-1} mittels der Zahlen δ, δ_1, $\ldots$ δ_{t-1} bestimmt werden, und setzt für die letzteren ihre gefundenen Werthe, so erhält man

$$\lambda(d+d_1+\cdots+d_{t-1}) = (q-1)(\gamma_{h-m\tau}+\gamma_{h-2m\tau}+\cdots+\gamma_h).$$

Die Reihe der eine Periode bildenden Reste

$$\gamma_{h-m\tau}+\gamma_{h-2m\tau}+\gamma_{h-3m\tau}+\cdots+\gamma_{h-t\tau}$$

ist, weil m relative Primzahl zu t ist, wenn man von der bestimmten Ordnung der Glieder absieht, dieselbe wie

$$\gamma_h+\gamma_{h+\tau}+\gamma_{h+2\tau}+\cdots+\gamma_{h+(t-1)\tau}.$$

Diese ist, wie man weifs, immer durch λ theilbar, aufser für $t=1$, weshalb sie durch λS_h bezeichnet werden soll, so dafs

$$\lambda S_h = \gamma_h+\gamma_{h+\tau}+\gamma_{h+2\tau}+\cdots+\gamma_{h+(t-1)\tau}$$

ist. Demzufolge giebt die vorige Gleichung:

$$d+d_1+d_2+\cdots+d_{t-1} = (q-1)S_h$$

und man erhält die Anzahl der in dem Producte $\Pi(\gamma_h\nu q^{nt})$ enthaltenen Factoren q durch die Zahl

$$\frac{\gamma_h\nu q^{nt}}{q-1}-S_h$$

ausgedrückt. Setzt man nun $\gamma_{-i}-\gamma_{\varrho-i}$, welches nach der Voraussetzung positiv und nothwendig kleiner als λ ist, gleich γ_σ, und nimmt sodann nach einander $h=-i$, $h=\varrho-i$ und $h=\sigma$, so erhält man für die Anzahl der in dem Binomialcoëfficienten

$$\frac{\Pi(\gamma_{-i}\nu q^{nt})}{\Pi(\gamma_{\varrho-i}\nu q^{nt}\,\Pi(\gamma_{-i}-\gamma_{\varrho-i})\nu q^{nt}}$$

enthaltenen Factoren q:

$$S_{\varrho-i}+S_\sigma-S_{-i}.$$

Genau eben so vielemal enthält also, nach Dem was oben bewiesen wurde, die complexe Zahl $\Psi_r(\alpha)$ den complexen Primfactor $f(\alpha\gamma^i)$; das heifst: in dem Ausdrucke

$$\Psi_r(\alpha) = E(\alpha)f(\alpha)^m f(\alpha\gamma)^{m_1}\ldots f(\alpha\gamma^{\tau-1})^{m_{\tau-1}}$$

werden diejenigen Exponenten m_i, für welche $\gamma_{-i}-\gamma_{\varrho-i}$ eine positive Zahl ist, durch die Gleichung

$$m_i = S_{\varrho-i}+S_\sigma-S_{-i}$$

bestimmt.

Aus der Gleichung $\gamma_{-i}-\gamma_{\varrho-i}=\gamma_\sigma$ folgt die Congruenz $\gamma^{-i}-\gamma^{\varrho-i}\equiv\gamma^\sigma$ oder $1-\gamma^\varrho\equiv\gamma^{\sigma+i}$, Mod. λ, und da $\gamma^\varrho\equiv r+1$ ist, so folgt weiter $-r\equiv\gamma^{\sigma+i}$ oder $r\equiv\gamma^{\sigma+i-\mu}$. Es ist also $\sigma+i-\mu\equiv\text{Ind.}\,r$ oder $\sigma\equiv\mu-i+\text{Ind.}\,r$, Mod. $\lambda-1$, wenn das Zeichen Ind., wie oben, sich auf den Mod. λ und dessen primitive Wurzel γ bezieht; und da eben so $\varrho\equiv\text{Ind.}\,(r+1)$ ist, so ist

$$m_i = S_{-i+\text{Ind.}(r+1)}+S_{-i+\mu+\text{Ind.}\,r}-S_{-i}.$$

Die mit S_h bezeichneten Zahlen haben aber, wie bekannt, die Eigenschaft, dafs $S_{h+\mu} = t - S_h$ ist. Also kann dem Ausdruck des m_i auch eine der folgenden beiden Formen gegeben werden:

$$m_i = t - S_{-i} - S_{-i+\text{Ind.}r} + S_{-i+\text{Ind.}(r+1)},$$

oder

$$m_i = S_{\mu-i} + S_{\mu-i+\text{Ind.}r} - S_{\mu-i+\text{Ind.}(r+1)}.$$

Es ist jetzt auch nicht schwer zu zeigen, dafs die Bestimmung der Exponenten m_i, welche bis jetzt nur für diejenigen Werthe des i bewiesen wurde, für welche $\gamma_{-i} - \gamma_{\varrho-i}$ positiv ist, ebensowohl für alle andern Werthe von i gültig bleibt.

Aus der Gleichung $\gamma_{\mu+h} = \lambda - \gamma_h$ folgt, dafs

$$\gamma_{-i} - \gamma_{\varrho-i} = -(\gamma_{-i-\mu} - \gamma_{\varrho-i-\mu}).$$

Wenn also i einen Werth hat, welcher der Bedingung, dafs $\gamma_{-i} - \gamma_{\varrho-i}$ positiv sein soll, nicht genügt, so genügt dagegen allemal der Werth $i+\mu$ dieser Bedingung. Ferner kann das oben gefundene Resultat, nach welchem $m_i + m_{i\frac{1}{2}\tau} = t$, weil $m_i = m_{i+\tau} = m_{i+2\tau}$ u. s. w. und $t.\frac{1}{2}\tau = \mu = \frac{1}{2}(\lambda-1)$ ist, auch so dargestellt werden, dafs $m_i + m_{i+\mu} = t$ ist. Es sei nun i eine Zahl, welche der obigen Bedingung nicht genügt, so ist dagegen $\mu+i$ eine solche Zahl, für welche der gefundene Ausdruck für $m_{i+\mu}$ richtig ist. Setzt man diesen aber in die Gleichung $m_i = t - m_{i+\mu}$, so findet man, vermöge der Gleichung $S_{h+\mu} = t - S_h$, für m_i wieder denselben Ausdruck; welcher also für alle Werthe des i richtig ist

Die Zerlegung der complexen Zahl $\Psi_r(\alpha)$ in ihre complexen Primfactoren, welche nur die complexen Primfactoren des q sind, wird demnach durch folgende Formel ausgedrückt:

$$\Psi_r(\alpha) = E(\alpha) f(\alpha)^m f(\alpha^\gamma)^{m_1} f(\alpha^{\gamma^2})^{m_2} \dots f(\alpha^{\gamma^{\tau-1}})^{m_{\tau-1}},$$

in welcher $E(\alpha)$ eine complexe Einheit, $f(\alpha)$ ein complexer idealer Primfactor der für den Modul λ zum Exponenten t gehörenden Primzahl q ist; ferner $\tau = \frac{\lambda-1}{t}$ und

$$m_i = S_{\mu-i} + S_{\mu-i+\text{Ind.}r} - S_{\mu-i+\text{Ind.}(r+1)} \quad \text{und}$$
$$\lambda S_h = \gamma_h + \gamma_{h+\tau} + \gamma_{h+2\tau} + \dots + \gamma_{h+(t-1)\tau}.$$

Die complexe Einheit $E(\alpha)$, welche in diesem Ausdrucke als Factor vorkommt, ist nothwendig unbestimmt, so lange über den complexen Primfactor $f(\alpha)$, welcher im Allgemeinen ideal sein wird, keine nähere Bestimmung gemacht ist. Stellt man sich aber diesen Ausdruck zur Hten Potenz erhoben

vor, wo H der Exponent derjenigen Potenz sein soll, für welche $f(\alpha)^H$ zu einer wirklichen complexen Zahl wird, so kann man dieselbe immer so darstellen, dafs sie nicht die einzelnen Wurzeln $\alpha, \alpha^2, \ldots \alpha^{\lambda-1}$, sondern nur die Perioden derselben enthält; nämlich die τ Perioden von je t Gliedern. Es mufs alsdann, weil, wie oben bewiesen wurde, $\Psi_r(\alpha)$ auch nur diese Perioden enthält, die Einheit $E(\alpha)$ ebenfalls nur aus diesen Perioden zusammengesetzt sein. Aus der Gleichung $\Psi_r(\alpha)\Psi_r(\alpha^{-1}) = q^t$ folgt ferner, dafs $E\alpha)E(\alpha^{-1}) = 1$ sein mufs; woraus nach einer bekannten Eigenschaft aller Einheiten folgt, dafs $E(\alpha)$ nur gleich $\pm\alpha^k$ sein kann; und da $E(\alpha)$ eine solche einzelne Wurzel α^k nicht enthalten kann, so folgt endlich, dafs $E(\alpha) = \pm 1$ ist; nämlich, wenn $f(\alpha)^H$ als eine, nur die Perioden enthaltende wirkliche complexe Zahl dargestellt angenommen wird. Diese Zerlegung der complexen Zahl $\Psi_r(\alpha)$ soll als die ***dritte Grund-Eigenschaft*** derselben bezeichnet werden.

Schliefslich bemerke ich noch, dafs dieser Ausdruck der complexen Zahl $\Psi_r(\alpha)$ durch ihre Primfactoren für den Fall $t = 1$ den entsprechenden Ausdruck der Kreistheilungszahl $\psi_r(\alpha)$ giebt, welchen ich in dem vorhergehenden Paragraphen dieser Abhandlung angewendet und zuerst in dem Programm der Universität ***Breslau*** zur Jubelfeier der Universität ***Königsberg*** im Jahre 1844 und später in diesem Journale (Band. 35, S. 362) gegeben habe. An demselben Orte (S. 364) wird man auch schon eine Anwendung der complexen Zahl $\Psi_r(\alpha)$ finden, von welcher ich damals nur die Zerlegung in die Primfactoren kannte, und wufste, dafs sie eine wirkliche complexe Zahl sei, für welche aber der in der gegenwärtigen Untersuchung zum Grunde gelegte, der complexen Kreistheilungszahl $\psi_r(\alpha)$ vollständig entsprechende Ausdruck

$$\Psi_r(\alpha) = \Sigma\alpha^{-(r+1)h+\mathrm{Ind.}(g^h+1)}$$

mir damals noch unbekannt war.

§. 3.

Entwickelung der Indices der complexen Einheiten und der Zahlen λ und $1-\alpha^k$, für welche der Modul eine zu einem beliebigen Exponenten gehörende complexe Primzahl ist.

Mittels der in dem vorigen Paragraphen entwickelten Eigenschaften der complexen Zahl $\Psi_r(\alpha)$ können nun die Indices der complexen Einheiten, so wie der Zahlen λ und $1-\alpha^k$, auch für den Fall gefunden werden, wo der Modul $f(\alpha)$, auf welchen sich die Indices beziehen, ein ***complexer***

idealer Primfactor einer zum Exponenten t gehörenden *nichtcomplexen* Primzahl q ist. Die Ausdrücke derselben sind den in dem ersten Paragraphen für den speciellen Fall $t=1$ gefundenen, namentlich den beiden letzten derselben, vollständig entsprechend. Ich untersuche also sogleich den $(\lambda-2n)$ten Differentialquotienten des Logarithmen der complexen Zahl $\Psi_r(\alpha)$, in welcher die Wurzel α durch die variable Exponentialgröfse e^v zu ersetzen ist, für den Werth $v=0$.

Es sei demnach

$$\Psi_r(e^v) = \Sigma e^{v(-(r+1)h+\mathrm{Ind.}(g^h+1))}$$

für $h=0, 1, 2, \ldots q^t=2$, mit Ausschlufs von $h=\frac{1}{2}(q^t-1)$. Dann ist zunächst

$$\frac{d^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} = \frac{d^{\lambda-2n-1}\left(\frac{d\Psi_r(e^v)}{dv}\right)\cdot\frac{1}{\Psi_r(e^v)}\right)}{dv^{\lambda-2n-1}},$$

und wenn man zur Abkürzung für einen Augenblick $\lambda-2n-1=m$ und $\frac{1}{\Psi_r(e^v)}=U$ setzt, so folgt hieraus nach den Regeln der Differentiation eines Products zweier Factoren:

$$\frac{d^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} = \frac{d^{m+1}\Psi_r(e^v)}{dv^{m+1}}U + \frac{m}{1}\frac{d^m\Psi_r(e^v)}{dv^m}\frac{dU}{dv} + \cdots$$

Macht man jetzt Gebrauch von der *zweiten* Grund-Eigenschaft der complexen Zahl $\Psi_r(\alpha)$, nach welcher $\Psi_r(\alpha)\Psi_r(\alpha^{-1})=q^t$ ist, so erhält man folgende, für jeden beliebigen Werth der Variabel v geltende Gleichung:

$$\Psi_r(e^v)\Psi_r(e^{-v}) = q^t + V.W;$$

wo $V=1+e^v+e^{2v}+\cdots e^{(\lambda-1)v}$ und W eine ganze rationale Function von e^v ist. Hieraus folgt

$$\Psi_r(e^{-v}) = \frac{q^t+VW}{\Psi_r(e^v)} = (q^t+VW)U,$$

und wenn man den $i$ten Differentialquotienten nimmt,

$$\frac{d^i\Psi_r(e^{-v})}{dv^i} = \frac{d^iU}{dv^i}(q^t+VW) + \frac{i}{1}\frac{d^{i-1}U}{dv^{i-1}}\frac{d(VW)}{dv} + \cdots$$

Setzt man nun $v=0$ und macht aus dieser Gleichung eine Congruenz für den Modul λ, so verschwinden V und alle Differentialquotienten des V, bis zum $(\lambda-2)$ten einschliefslich, weil sie durch λ theilbar sind; und wenn man noch beachtet, dafs $q^t\equiv 1$, Mod. λ ist, so erhält man

$$\frac{d_0^i\Psi_r(e^{-v})}{dv^i} \equiv \frac{d_0^iU}{dv^i}, \text{ Mod. } \lambda,$$

für alle Werthe 0, 1, 2, ... $\lambda-2$ von i, oder, was Dasselbe ist:

$$\frac{d_0^i U}{dv^i} \equiv (-1)^i \frac{d_0^i \Psi_r(e^v)}{dv^i} \equiv (-1)^i \mathrm{D}_i, \text{ Mod. } \lambda;$$

wenn der Kürze wegen der $i$te Differentialquotient von $\Psi_r(e^v)$ für $v=0$ durch Di bezeichnet wird. Der obige Ausdruck des $(\lambda-2n)$ten Differentialquotienten von $l\Psi_r(e^v)$ nimmt daher für $v=0$ folgende Gestalt an:

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv \mathrm{D}_{m+1}\mathrm{D}_0 - \frac{m}{1}\mathrm{D}_m\mathrm{D}_1 + \frac{m(m-1)}{1.2}\mathrm{D}_{m-1}\mathrm{D}_2 - \cdots, \text{ Mod. } \lambda.$$

Durch Differentiation des oben gegebenen Ausdrucks für $\Psi_r(e^v)$ erhält man nun für $v=0$:

$$\mathrm{D}^i = \Sigma(-(r+1)h + \mathrm{Ind.}\,(g^h+1))^i$$

für $h=0, 1, 2, \ldots q^t-2$, mit Ausschlufs von $h=\frac{1}{2}(q^t-1)$. Setzt man, um abzukürzen, für einen Augenblick

$$-(r+1)h + \mathrm{Ind.}\,(g^h+1) = C_h \quad \text{und} \quad -(r+1)k + \mathrm{Ind.}\,(g^k+1) = C_k,$$

so ergiebt sich

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv \Sigma\Sigma\Big(C_h^{m+1}C_k^0 - \frac{m}{1}C_h^m C_k + \frac{m(m-1)}{1.2}C_h^{m-1}C_k^2 - \cdots\Big);$$

wo die Doppelsumme auf alle ganzzahligen Werthe des h und k, von 0 bis q^t-2, sich erstreckt; mit Ausschlufs des Werths $h=\frac{1}{2}(q^t-1)$ und $k=\frac{1}{2}(q^t-1)$. Summirt man nun die Binomialreihe unter den beiden Summenzeichen, so erhält man

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv \Sigma\Sigma C_h(C_h - C_k)^m,$$

und wenn für C_h und C_k und für m wieder ihre Werthe gesetzt werden:

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv \Sigma\Sigma(-(r+1)h + \mathrm{Ind.}\,(g^h+1)) \times(-(r+1)(h-k) + \mathrm{Ind.}\,(g^h+1) + \mathrm{Ind.}\,(g^k+1))^{\lambda-2n-1},$$

für $h=0, 1, 2, \ldots q^t-2$ und $k=0, 1, 2, \ldots q^t-2$, mit Ausschlufs von $h=\frac{1}{2}(q^t-1)$, $k=\frac{1}{2}(q^t-1)$.

Man transformire nun diese Doppelsumme, in welcher alle Glieder, die gleichen Werthen von h und k angehören, als congruent Null, von selbst wegfallen, durch dieselbe Substitution, welche oben im zweiten Paragraphen zur Transformation einer ähnlichen Doppelsumme angewendet worden ist, nämlich:

$$g^{k-h} \equiv g^{k'}, \quad \frac{g^k+1}{g^h+1} \equiv g^{h'}, \text{ Mod. } f(\alpha),$$

so erhält man diesen $(\lambda-2n)$ten Differentialquotienten durch die Doppelsumme

$$\Sigma\Sigma(-(r+1)\,\mathrm{Ind.}\,(g^{h'}-1) + \mathrm{Ind.}\,(g^{k'}-1) + r\,\mathrm{Ind.}\,(g^{k'}-g^{h'}))\,((r+1)k'-h)^{\lambda-2n-1}$$

ausgedrückt, wo h' und k' alle Werthe $1, 2, 3, \ldots q^t-2$ bekommen müssen, die Werthverbindung $h'=k'$ aber ausgeschlossen ist. Man zerlege diese Doppelsumme in folgende drei Theile:

$$-(r+1)\Sigma\Sigma \text{Ind.}(g^{h'}-1)\ ((r+1)k'-h')^{\lambda-2n-1},$$
$$\Sigma\Sigma \text{Ind.}(g^{k'}-1)\ ((r+1)k'-h')^{\lambda-2n-1},$$
$$r\Sigma\Sigma \text{Ind.}(g^{k'}-g^{h'})((r+1)k'-h')^{\lambda-2n-1},$$

und suche die Werthe dieser drei Theile einzeln; mit dem ersten Theile anfangend. Um in demselben die Werthverbindung $k'=h'$ nicht ferner ausschliefsen zu müssen, füge man den dieser Werthverbindung entsprechenden Theil mit entgegengesetztem Vorzeichen hinzu. Der erste Theil ist

$+r^{\lambda-2n-1}(r+1)\Sigma h'^{\lambda-2n-1}\text{Ind.}(g^{h'}-1)-(r+1)\Sigma\Sigma\text{Ind.}(g^{h'}-1)((r+1)k'-h')^{\lambda-2n-1}$;

wo jetzt den k' und h' alle Werthe von 1 bis q^t-2 einschliefslich, ohne Ausnahme, zu geben sind. Ich führe nun die Summation in Beziehung auf k' aus, indem zu bemerken ist, dafs $q^t-1\equiv 0$, Mod. λ und dafs die Summe $\Sigma k'^i$ ebenfalls congruent Null ist, für jeden der Werthe $1, 2, 3, \ldots \lambda-2$ von i. Dies giebt zunächst

$$\Sigma((r+1)k'-h')^{\lambda-2n-1}\equiv(q^t-2)h'^{\lambda-2n-1}\equiv -h'^{\lambda-2n-1}.$$

Der erste Theil ist vermöge Dessen dem folgenden Ausdrucke congruent:

$$(r+1)(1+r^{\lambda-2n-1})\Sigma h'^{\lambda-2n-1}\text{Ind.}(g^{h'}-1).$$

Genau auf dieselbe Weise findet man den zweiten Theil congruent

$$-(r^{\lambda-2n-1}+(r+1)^{\lambda-2n-1})\Sigma h'^{\lambda-2n-1}\text{Ind.}(g^{h'}-1).$$

Um auch den dritten Theil auf eine ähnliche einfache Summe zu reduciren, dehne man die Werthe von h' und k' auch auf den Werth $h'=0$ und $k'=0$ aus; welches ohne Weiteres geschehen kann, wenn man die diesen Werthen entsprechenden Glieder

$$r\Sigma k'^{\lambda-2n-1}\text{Ind.}(g^{k'}-1) \quad \text{und} \quad r(r+1)^{\lambda-2n-1}\Sigma h'^{\lambda-2n-1}\text{Ind.}(g^{h'}-1)$$

subtrahirt.

Ich verwandle nun diese Doppelsumme, in welcher jetzt h' und k' alle Werthe von 0 bis q^t-2 einschliefslich haben (jedoch mit Ausschlufs der Werthverbindung $h'=k'$), indem ich $h'+k'$ statt h' setze; wodurch sie folgende Form annimmt:

$$r\Sigma\Sigma(\text{Ind.}(g^{h'}-1)+k')(rk'-h')^{\lambda-2n-1},$$

für $k'=0, 1, 2, 3, \ldots q^t-2$ und $h'=1, 2, 3, \ldots q^t-2$. Die Summation in Beziehung auf k' läfst sich wieder ohne Schwierigkeit ausführen und giebt das Resultat, dafs die Doppelsumme einfach congruent Null ist, für den Modul λ. Der dritte Theil ist den beiden einfachen Summen, welche zu subtrahiren

waren, deshalb congruent, damit die Werthe von h' und k' auch auf $h'=0$ und $k'=0$ ausgedehnt werden konnten. Diese zusammengefafst, geben den dritten Theil congruent

$$-r(1+(r+1)^{\lambda-2n-1})\Sigma h'^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{h'}-1).$$

Fafst man alle drei Theile wieder in einen zusammen, so erhält man nach einigen leichten Reductionen:

$$\frac{d_0^{\lambda-2n}l\Psi_r(e^v)}{dv^{\lambda-2n}} = (1+r^{\lambda-2n}-(r+1)^{\lambda-2n})\Sigma h'^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{h'}-1),$$

für $h'=1, 2, 3, \ldots q^t-2$.

Die hierin enthaltene einfache Summe kann nun auf folgende Weise leicht als Index der complexen Einheit $E_n(\alpha)$ dargestellt werden. Zuerst werden alle Glieder, für welche h' durch λ theilbar ist, als congruent Null, weggelassen, und dann wird $h'=i+\lambda k$ gesetzt und es werden dem i die Werthe $1, 2, 3, \ldots \lambda-1$, dem k die Werthe $0, 1, 2, \ldots \nu-1$ gegeben (wo $\nu=\frac{q^t-1}{\lambda}$ ist). Dann ist

$$\Sigma h'^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{h'}-1) \equiv \Sigma\Sigma i^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{i+k\lambda}-1),$$

für $i=1, 2, 3, \ldots \lambda-1$, $k=0, 1, 2, \ldots \nu-1$. Nun ist aber, wie leicht zu beweisen,

$$(g^i-1)(g^{i+\lambda}-1)(g^{i+2\lambda}-1)\ldots(g^{i+(\nu-1)\lambda}-1) \equiv 1-g^{\nu i},\ \mathrm{Mod.}\,f(\alpha),$$

also auch

$$\Sigma\,\mathrm{Ind.}\,(g^{i+k\lambda}-1) \equiv \mathrm{Ind.}\,(1-g^{\nu i}) \equiv \mathrm{Ind.}\,(1-\alpha^i),\ \mathrm{Mod.}\,\lambda,$$

indem $g^\nu \equiv \alpha$, Mod. $f(\alpha)$, ist. Die Ausführung der Summation in Beziehung auf k giebt daher

$$\Sigma h'^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{h'}-1) = \Sigma i^{\lambda-2n-1}\,\mathrm{Ind.}\,(1-\alpha^i),$$

für $i=1, 2, 3, \ldots \lambda-1$. Setzt man $i\gamma$ statt i, multiplicirt mit γ^{2n} und subtrahirt von der so erhaltenen Congruenz die unveränderte, so erhält man

$$(\gamma^{2n}-1)\Sigma h'^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{h'}-1) \equiv \Sigma i^{\lambda-2n-1}\,\mathrm{Ind.}\left(\frac{1-\alpha^{\nu i}}{1-\alpha^i}\right),\ \mathrm{Mod.}\,\lambda.$$

Verwandelt man endlich i in γ^h, so zeigt sich sogleich, dafs die Summe rechts in dieser Congruenz dem doppelten Index der Einheit

$$E_n(\alpha) = e(\alpha).e(\alpha^\gamma)^{\gamma^{-2n}}.e(\alpha^{\gamma^2})^{\gamma^{-4n}}\ldots e(\alpha^{\gamma^{\mu-1}})^{\gamma^{-2(\mu-1)n}}$$

congruent, also

$$(\gamma^{-2n}-1)\Sigma h'^{\lambda-2n-1}\,\mathrm{Ind.}\,(g^{h'}-1) \equiv 2\,\mathrm{Ind.}\,E_n(\alpha)$$

ist. Dadurch hat man nun folgenden Ausdruck für den Index dieser Einheit:

$$\mathrm{Ind.}\,E_n(\alpha) \equiv \frac{(\gamma^{2n}-1)}{2(1+r^{\lambda-2n}-(r+1)^{\lambda-2n})}\cdot\frac{d_0^{\lambda-2n}l\Psi_r(e^v)}{dv^{\lambda-2n}},\ \mathrm{Mod.}\,\lambda.$$

Diese Formel, welche der entsprechenden, im ersten Paragraphen für den besondern Fall $t = 1$ bewiesenen ganz gleich ist, giebt die Indices der Einheiten $E_1(\alpha)$, $E_2(\alpha)$, u. s. w.; also auch die Indices aller Einheiten, welche durch diese sich darstellen lassen. Es ist aber hier nicht nöthig, die Indices aller dieser Einheiten $E_1(\alpha)$, $E_2(\alpha)$, ... $E_{\mu-1}(\alpha)$ nach der Formel besonders zu berechnen, denn es läfst sich leicht ein- für allemal zeigen, dafs für alle Werthe von n, für welche $\lambda - 2n$ nicht durch t theilbar ist, der Index Ind. $E_n(\alpha)$ nur congruent Null ist. Es kann Dies auf folgende Weise aus dem gefundenen Ausdrucke des Ind. $E_n(\alpha)$ selbst abgeleitet werden. Da, vermöge der ersten Grund-Eigenschaft der complexen Zahl $\Psi_r(\alpha)$, dieselbe nur die τ Perioden von je t Gliedern, nicht aber die Wurzeln α, α^2, ... $\alpha^{\lambda-1}$ einzeln enthält, so ist

$$\Psi_r(\alpha) = \Psi_r(\alpha^{\gamma^\tau}),$$

woraus nach den schon mehrmals angewendeten Principien

$$\Psi_r(e^v) = \Psi_r(e^{v\gamma^\tau}) + V.W$$

und weiter

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv \frac{d_0^{\lambda-2n} l\Psi_r(e^{v\gamma^\tau})}{dv^{\lambda-2n}},$$

oder

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv \gamma^{(\lambda-2n)\tau} \frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}}$$

folgt. Es mufs also nothwendig, entweder

$$\gamma^{(\lambda-2n)\tau} - 1 \equiv 0, \quad \text{oder} \quad \frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv 0$$

sein, für den Mod. λ. In dem letztern Falle ist aber Ind. $E_n(\alpha) \equiv 0$, Mod. λ, und nur wenn $\gamma^{(\lambda-2n)\tau} \equiv 1$, Mod. λ, ist, kann Ind. $E_n(\alpha)$ einen von Null verschiedenen Werth haben; also nur dann, wenn $(\lambda - 2n)\tau$ ein Vielfaches von $\lambda - 1 = t\tau$ oder, was Dasselbe ist, wenn $\lambda - 2n$ ein Vielfaches von t ist; wie behauptet wurde. Dasselbe läfst sich übrigens auch ohne Hülfe der allgemeinen Formel für Ind. $E_n(\alpha)$ auf elementare Art leicht beweisen.

Aus dem gefundenen Ausdruck des Ind. $E_n(\alpha)$ wird nun ein anderer, welcher nicht die complexe Zahl $\Psi_r(\alpha)$, sondern den Primfactor $f(\alpha)$ selbst enthält, mittels der dritten Grund-Eigenschaft der $\Psi_r(\alpha)$, welche ihre Zerlegung in die Primfactoren giebt, auf folgende Weise hergeleitet. Wenn der im Allgemeinen ideale Primfactor $f(\alpha)$ als Hte Wurzel aus der Potenz $f(\alpha)^H$ dargestellt und H so angenommen wird, dafs $f(\alpha)^H$ eine wirkliche complexe Zahl ist, so kann, wie schon oben bemerkt, diese wirkliche complexe Zahl $f(\alpha)^H$

immer so angenommen werden, dafs sie nur die τ Perioden von je t Gliedern enthält. Bei dieser Annahme hat man

$$\Psi_r(\alpha) = \pm f(\alpha)^m f(\alpha^\gamma)^{m_1} f(\alpha^{\gamma^2})^{m_2} \dots f(\alpha^{\gamma^{\tau-1}})^{m_{\tau-1}} \text{ und}$$
$$m_i = S_{\mu-i} + S_{\mu-i+\text{Ind. } r} - S_{\mu-i+\text{Ind. } (r+1)}.$$

Daraus folgt sogleich

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv m \frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}} + m_1 \frac{d_0^{\lambda-2n} lf(e^{\gamma v})}{dv^{\lambda-2n}} + \dots + m_{\tau-1} \frac{d_0^{\lambda-2n} lf(e^{\gamma^{\tau-1} v})}{dv^{\lambda-2n}},$$

oder, vereinfacht:

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv (m + \gamma^{\lambda-2n} m_1 + \gamma^{2(\lambda-2n)} m_2 + \dots + \gamma^{(\tau-1)(\lambda-2n)} m_{\tau-1}) \frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}}.$$

Es ist nun die rechts in dieser Congruenz vorkommende Summe zu suchen, welche durch den Buchstaben R bezeichnet werden soll, so dafs

$$R = m + \gamma^{\lambda-2n} m_1 + \gamma^{2(\lambda-2n)} m_2 + \dots + \gamma^{(\tau-1)(\lambda-2n)} m_{\tau-1}$$

ist. Es wird auch hinreichen, diesen Werth von R nur für diejenigen Werthe von n zu suchen, für welche $\lambda - 2n$ ein Vielfaches von t ist; denn wenn dies nicht der Fall ist, so giebt die Congruenz, nach Dem was oben gezeigt, nur identisch $0 \equiv 0$, Mod. λ. Wird mehrerer Einfachheit wegen das Summenzeichen angewendet und für m_i sein Werth gesetzt, so ist

$$R = \Sigma \gamma^{i(\lambda-2n)} (S_{\mu-i} + S_{\mu-i+\text{ind. } r} - S_{\mu-i+\text{ind. } (r+1)})$$

für $i = 0, 1, 2, \dots \tau-1$. Nun sollen hierin für die drei Gröfsen $S_{\mu-i}$, $S_{\mu-i+\text{ind. } r}$ und $S_{\mu-i+\text{Ind. } (r+1)}$ ihre Werthe nach der Formel

$$S_h = \frac{1}{\lambda}(\gamma_h + \gamma_{h+\tau} + \gamma_{h+2\tau} + \dots + \gamma_{h+(t-1)\tau}) = \frac{1}{\lambda} \Sigma \gamma_{h+k\tau}$$

gesetzt werden. Alsdann sind, wegen des als Nenner vorkommenden λ, wieder Congruenzen für den Modul λ^2 zur Bestimmung von R nöthig, und deshalb soll $\gamma^{i\lambda(\lambda-2n)}$ statt $\gamma^{i(\lambda-2n)}$ genommen werden, welches demselben für den Mod. λ congruent ist. Wird sodann mit λ multiplicirt, so erhält man folgende Congruenz:

$$\lambda R \equiv \Sigma\Sigma \gamma^{i\lambda(\lambda-2n)} (\gamma_{\mu-i+k\tau} + \gamma_{\mu-i+k\tau+\text{ind. } r} - \gamma_{\mu-i+k\tau+\text{ind. } (r+1)}),$$

für den Mod. λ^2, wo die beiden Summenzeichen auf die Werthe $i = 0, 1, 2, \dots \tau-1$ und $k = 0, 1, 2, \dots t-1$ zu beziehen sind. Setzt man $i + k\tau$ statt i und beachtet, dafs bei dieser Veränderung $\gamma^{i\lambda(\lambda-2n)}$ in Beziehung auf den Mod. λ^2 unverändert bleibt, weil $\lambda - 2n$ nach der Voraussetzung durch t theilbar und $t\tau = \lambda - 1$ ist, so verwandelt sich die Doppelsumme in die einfache:

$$\lambda R \equiv \Sigma \gamma^{i\lambda(\lambda-2n)} (\gamma_{\mu-i} + \gamma_{\mu-i+\text{ind. } r} - \gamma_{\mu-i+\text{ind. } (r+1)}), \text{ Mod. } \lambda^2,$$

für $i = 0, 1, 2, \dots \lambda-2$.

Vergleicht man nun dieses Resultat mit dem in der ähnlichen Untersuchung im ersten Paragraphen dieser Abhandlung gefundenen Ausdrucke der dort mit T bezeichneten Summe, so findet sich $\lambda R \equiv \lambda T$, Mod. λ^2, also $R \equiv T$, Mod. λ. Macht man demnach von dem oben gefundenen Werthe von T Gebrauch, so erhält man

$$R \equiv (-1)^n (1 + r^{\lambda-2n} - (r+1)^{\lambda-2n}) \frac{B_n}{2n}, \text{ Mod. } \lambda,$$

also

$$\frac{d_0^{\lambda-2n} l\Psi_r(e^v)}{dv^{\lambda-2n}} \equiv (-1)^n (1 + r^{\lambda-2n} - (r+1)^{\lambda-2n}) \frac{B_n}{2n} \cdot \frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}}.$$

Der gefundene Ausdruck des Ind. $E_n(\alpha)$ giebt demnach folgenden neuen Ausdruck des Index dieser Einheit:

$$\text{Ind. } E_n(\alpha) \equiv \frac{(-1)^n (\gamma^{2n}-1) B^n}{4n} \cdot \frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}}, \text{ Mod. } \lambda.$$

Die Vergleichung dieses Ausdrucks mit dem entsprechenden, für den besondern Fall $t = 1$ im ersten Paragraphen gefundenen, zeigt, dafs er genau derselbe ist, wie jener, dafs also in allen Fällen, ohne Unterschied, d. h. für alle complexen idealen Primfactoren $f(\alpha)$ als Moduln, derselbe Ausdruck gilt.

Es bleibt noch übrig, auch für die zu einem beliebigen Exponenten t gehörigen Primfactoren $f(\alpha)$, als Moduln, den Index von λ und die Indices der Primfactoren des λ von der Form $1-\alpha^k$ zu suchen. Zunächst läfst sich leicht zeigen, dafs Ind. (λ) allemal congruent Null ist, wenn t nicht gleich Eins ist; also für alle Moduln, mit Ausnahme der in dem ersten Paragraphen behandelten. Für diese Moduln ist nämlich nicht blofs Ind. (λ), sondern überhaupt der Index jeder nichtcomplexen ganzen Zahl congruent Null. Denn aus der Congruenz

$$c^{\frac{q^t-1}{\lambda}} \equiv \alpha^{\text{Ind. } c}, \text{ Mod. } f(\alpha),$$

in welcher c eine beliebige (jedoch nicht durch $f(\alpha)$ theilbare) nichtcomplexe Zahl bedeutet, folgt, wenn α in α^{γ^τ} verwandelt wird, weil $f(\alpha) = f(\alpha^{\gamma^\tau})$ ist:

$$c^{\frac{q^t-1}{\lambda}} \equiv \alpha^{\gamma^\tau \text{Ind. } c}, \text{ Mod. } f(\alpha),$$

also $\alpha^{\text{Ind. } c} \equiv \alpha^{\gamma^\tau \text{Ind. } c}$, Mod. $f(\alpha)$, mithin auch Ind. $c \equiv \gamma^\tau$ Ind. c, Mod. λ, und Ind. $(c) \equiv 0$, Mod. λ; mit Ausnahme des einzigen Falles, wo $\gamma^\tau \equiv 1$, also $\tau = \lambda - 1$ und $t = 1$ ist.

Um auch Ind. $(1-\alpha^k)$ für die in diesem Paragraphen behandelte Moduln

zu finden, nehme man

$$\lambda = (1-\alpha)(1-\alpha^\gamma)(1-\alpha^{\gamma^2}) \ldots (1-\alpha^{\gamma^{\lambda-2}})$$

an, und gebe dieser Gleichung die Form

$$\lambda = (1-\alpha)^{\lambda-1}\left(\frac{1-\alpha\gamma}{1-\alpha}\right)\left(\frac{1-\alpha\gamma^2}{1-\alpha}\right) \ldots \left(\frac{1-\alpha\gamma^{\lambda-2}}{1-\alpha}\right).$$

Man drücke die Einheiten, welche hierin vorkommen, alle durch die Kreistheilungs-Einheiten $e(\alpha)$, $e(\alpha^\gamma)$, u. s. w, aus, so erhält man

$$\lambda = (1-\alpha)^{\lambda-1}\alpha^{-\mu}.e(\alpha)^{\lambda-1}.e(\alpha^\gamma)^{\lambda-2}.e(\alpha^{\gamma^2})^{\lambda-3} \ldots e(\alpha^{\gamma^{\lambda-2}})^1,$$

und wenn α in α^k verwandelt wird:

$$\lambda = (1-\alpha^k)^{\lambda-1}\alpha^{-\mu k}.e(\alpha^k)^{\lambda-1}.e(\alpha^{k\gamma})^{\lambda-2}.e(\alpha^{k\gamma^2})^{\lambda-3} \ldots e(\alpha^{k\gamma^{\lambda-2}})^1.$$

Man nehme nun auf beiden Seiten die Indices für den Modul $f(\alpha)$, so ergiebt sich, weil $\text{Ind.}(\lambda) \equiv 0$ ist:

$$0 \equiv -\text{Ind.}(1-\alpha^k) - \mu k\nu - \text{Ind.}\,e(\alpha^k) - 2\,\text{Ind.}\,e(\alpha^{k\gamma}) - \cdots - (\lambda-1)\,\text{Ind.}\,e(\alpha^{k\gamma^{\lambda-2}}),$$

wo $\lambda\nu = q^t - 1$, oder, mit Anwendung des Summenzeichens,

$$\text{Ind.}(1-\alpha^k) \equiv -\mu k\nu - \Sigma h\,\text{Ind.}\,e(\alpha^{k\gamma^{h-1}})$$

für $h = 1, 2, 3, \ldots \lambda-1$ ist. Man drücke ferner $\text{Ind.}\,e(\alpha^{k\gamma^{h-1}})$ durch die Indices der Einheiten $E_1(\alpha)$, $E_2(\alpha)$, $\ldots$ $E_{\mu-1}(\alpha)$ mittels der Formel

$$\text{Ind.}\,e(\alpha^{\gamma^{h-1}}) \equiv -2\Sigma\gamma^{2n(h-1)}\,\text{Ind.}\,E_n(\alpha)$$

aus, für $n = 1, 2, 3, \ldots \mu-1$, so wird

$$\text{Ind.}(1-\alpha^k) \equiv -\mu k\nu + 2\Sigma\Sigma h\gamma^{2n(h-1)}\,\text{Ind.}\,E_n(\alpha^k),$$

für $h = 1, 2, 3, \ldots \lambda-1$ und $n = 1, 2, 3, \ldots \mu-1$. Die Summation in Beziehung auf h wird nach der leicht zu beweisenden Formel

$$\Sigma h\gamma^{2n(h-1)} \equiv \frac{1}{1-\gamma^{2n}}$$

ausgeführt und giebt

$$\text{Ind.}(1-\alpha^k) \equiv -\mu k\nu + 2\Sigma\frac{\text{Ind.}\,E_n(\alpha^k)}{1-\gamma^{2n}},$$

für $n = 1, 2, 3, \ldots \mu-1$. Endlich kann man noch von der Eigenschaft der Einheit $E_n(\alpha)$ Gebrauch machen, nach welcher

$$\text{Ind.}\,E_n(\alpha^k) \equiv k^{2n}\,\text{Ind.}\,E_n(\alpha), \quad \text{Mod.}\,\lambda$$

ist. Vermöge derselben erhält man

$$\text{Ind.}(1-\alpha^k) \equiv -\mu k\nu + 2\Sigma\frac{k^{2n}\,\text{Ind.}\,E_n(\alpha)}{1-\gamma^{2n}}, \quad \text{Mod.}\,\lambda,$$

für $n = 1, 2, 3, \ldots \mu-1$. Dieser Ausdruck, welcher darauf sich stützt, dafs $\text{Ind.}(\lambda) \equiv 0$ ist, gilt aber nicht für den Fall $t = 1$, für welchen die in dem

ersten Paragraphen gegebenen Ausdrücke von Ind. (λ) und Ind. $(1-\alpha^k)$ zu nehmen sind. Es könnten auch für Ind. $E_n(\alpha)$ die gefundenen Ausdrücke hier eingesetzt werden; da aber dadurch keine besonders eleganten Formeln entstehen, so mag es hinreichen, den Ind. $(1-\alpha^k)$ durch die oben gefundenen Indices der Einheiten $E_1(\alpha)$, $E_2(\alpha)$, ... $E_{\mu-1}(\alpha)$ ausgedrückt zu haben.

§. 4.

Über die Anwendung logarithmischer Ausdrücke der complexen Zahlen auf Congruenzen, deren Modul λ oder eine Potenz von λ ist.

Die Anwendung der in dem vorhergehenden Paragraphen gefundenen Resultate auf die allgemeinen Reciprocitätsgesetze, welche ich in dem Folgenden zu geben gedenke, erfordert, dafs ich zunächst eine allgemeine Methode mittheile, nach welcher Congruenzen für den Modul λ, oder eine Potenz von λ, namentlich wenn sie Producte mehrerer complexen Zahlen und Potenzen derselben enthalten, auf die einfachste Weise eben so behandelt werden können, wie in der Analysis dergleichen Ausdrücke mit Hülfe der Logarithmen. Eine Andeutung einer solchen Methode, welche ich in der Form, wie ich sie hier entwickeln werde, schon seit mehreren Jahren vielfach angewendet, aber bisher noch nicht veröffentlicht habe, findet sich in einer Abhandlung des Herrn *Eisenstein* (im 39ten Bande dieses Journals S. 351), auf welche Abhandlung ich in dem Folgenden noch einmal zurückkommen werde.

Ich stelle für den *Logarithmen* einer complexen Zahl, in Beziehung auf den Modul λ^{n+1} genommen, folgende Definition auf:

Wenn $\varphi(\alpha)$ eine complexe Zahl ist, welche den Factor $1-\alpha$ nicht enthält, so dafs auch $\varphi(1)$ nicht $\equiv 0$, Mod. λ ist, so soll unter dem Ausdrucke

$$l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \text{ für den Modul } \lambda^{n+1}$$

die endliche Anzahl von Gliedern der Reihe

$$\frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)} - \tfrac{1}{2}\left(\frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)}\right)^2 + \tfrac{1}{3}\left(\frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)}\right)^3 - \ldots$$

verstanden werden, welche nicht congruent Null sind für den Modul λ^{n+1}.

Dafs die Glieder dieser Reihe, von einem bestimmten an, wirklich alle congruent Null werden, für den Modul λ^{n+1}, erhellet daraus, dafs $\varphi(\alpha)-\varphi(1)$ den Factor $1-\alpha$ enthält, und dafs $(1-\alpha)^{\lambda-1}$ durch λ theilbar ist. Wenn nämlich in dem allgemeinen Gliede der Reihe

$$\pm\frac{1}{k}\left(\frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)}\right)^k$$

k nicht durch λ theilbar ist, so ist Dasselbe allemal congruent Null für den Modul λ^{n+1}, sobald $k > (\lambda-1)(n+1)$ ist. Wenn aber k den Factor λ enthält, und man setzt $k = c\lambda^a$, wo c nicht weiter durch λ theilbar sein soll, so müssen noch die a Factoren λ des Nenners durch $(\lambda-1)a$ Factoren $1-\alpha$ des Zählers compensirt werden. Wenn daher $k > (\lambda-1)(n+a+1)$ angenommen wird, so sind alle Glieder congruent Null für den Modul λ^{n+1}. In Beziehung auf diesen Modul bricht also diese Reihe nothwendig ab. Die Logarithmen der complexen Zahlen für den Modul λ^{n+1} sind demnach nur endliche Ausdrücke, d. h. sie sind selbst nur gewöhnliche complexe Zahlen. Auch geht aus der Definition hervor, dafs $l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right)$ für den Modul λ^{n+1} nur einen einzigen bestimmten Werth hat, wenn nämlich aufser $\varphi(\alpha)$ auch $\varphi(1)$ nur einen bestimmten Werth hat. Aus den bekannten Eigenschaften der Reihe, durch welche $l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right)$ dargestellt wird, erhält man ferner sogleich für die Grund-Eigenschaften dieser Ausdrücke:

$$l\left(\frac{f(\alpha)}{f(1)}\right)+l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \equiv l\left(\frac{f(\alpha)\varphi(\alpha)}{f(1)\varphi(1)}\right)$$
$$ml\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \equiv l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right)^m \quad \ldots \text{Mod. } \lambda^{n+1}.$$

Es kommt nun darauf an, für $l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right)$, Mod. λ^{n+1}, den einfachsten Ausdruck zu finden. Zu diesem Ende werde die complexe Zahl $\varphi(\alpha)-\varphi(1)$, welche durch $1-\alpha$ theilbar ist, auf folgende Form gebracht:

$$\varphi(\alpha)-\varphi(1) = A_1(1-\alpha)+A_2(1-\alpha)^2+\cdots+A_{\lambda-1}\alpha^{\lambda-1}.$$

Stellt man sich diesen Werth in die obige Reihe gesetzt vor, welche nur so weit fortgeführt anzunehmen ist, als die Glieder nicht von selbst wegfallen, weil sie congruent Null werden, und dann die einzelnen Glieder alle entwickelt, nach Potenzen von $1-\alpha$, so erhält man eine Reihe von folgender Form:

$$l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \equiv \frac{C_1(1-\alpha)}{1.\varphi(1)}+\frac{C_2(1-\alpha)^2}{2.\varphi(1)^2}+\frac{C_3(1-\alpha)^3}{3.\varphi(1)^3}+\cdots, \text{ Mod. } \lambda^{n+1},$$

welche man ebenfalls nur so weit fortzusetzen braucht, als noch Glieder sich finden, welche nicht congruent Null sind. Wendet man das Summenzeichen an und verwandelt α in α^{γ^h}, so erhält man

$$l\left(\frac{\varphi(\alpha\gamma^h)}{\varphi(1)}\right) \equiv \Sigma\frac{C_i(1-\alpha\gamma^h)^i}{i\varphi(1)^i}, \text{ Mod. } \lambda^{n+1},$$

und wenn man mit $\gamma^{-hk\lambda^n}$ multiplicirt und die Summe für $h = 0, 1, 2, \ldots \lambda-2$

nimmt, so ergiebt sich

$$\sum_{0}^{\lambda-2}{}_h \gamma^{-hk\lambda^n} l\left(\frac{\varphi(\alpha\gamma^h)}{\varphi(1)}\right) \equiv \sum_{0}^{\lambda-2}{}_h \sum_i \frac{C_i \gamma^{-hk\lambda^n}(1-\alpha\gamma^h)^i}{i\,\varphi(1)^i}.$$

Wird nun die $i$te Potenz von $1-\alpha^{\gamma^h}$ nach dem binomischen Lehrsatze entwickelt, so erhält man

$$(1-\alpha^{\gamma^h})^i = \sum_{0}^{i}{}_s \frac{(-1)_s \Pi(i)\,\alpha^{s\gamma^h}}{\Pi(s)\Pi(i-s)},$$

folglich

$$\sum_{0}^{\lambda-2}{}_h \frac{\gamma^{-hk\lambda^n}(1-\alpha\gamma^h)^i}{i} = \sum_{0}^{\lambda-2}{}_h \sum_{0}^{i}{}_s \frac{(-1)_s \Pi(i)\gamma^{-hk\lambda^n}\alpha^{s\gamma^h}}{i\Pi(s)\Pi(i-s)}.$$

Nun führe ich folgende für die hier zu behandelnden logarithmischen Ausdrücke besonders wichtige complexe Zahl ein:

$$X_k(\alpha) = \alpha + \gamma^{-k\lambda^n}\alpha^{\gamma} + \gamma^{-2k\lambda^n}\alpha^{\gamma^2} + \cdots + \gamma^{-(\lambda-2)k\lambda^n}\alpha^{\gamma^{\lambda-2}}.$$

Diese durch $X_k(\alpha)$ bezeichneten complexen Zahlen haben mehrere besondere Eigenschaften, welche denen des entsprechenden Ausdrucks der Kreistheilung

$$F(\beta, \alpha) = \alpha + \beta\alpha^{\gamma} + \beta^2\alpha^{\gamma^2} + \cdots + \beta^{\lambda-2}\alpha^{\gamma^{\lambda-2}},$$

wo α eine Wurzel der Gleichung $\alpha^{\lambda}=1$ und β eine Wurzel der Gleichung $\beta^{\lambda-1}=1$ ist, ganz analog sind. Für den gegenwärtigen Zweck aber soll nur von der einen Eigenschaft derselben Gebrauch gemacht werden, nämlich von

$$X_k(\alpha^m) \equiv m^{k\lambda^n} X_k(\alpha), \text{ Mod. } \lambda^{n+1};$$

welche Eigenschaft aus der Definition selbst leicht zu beweisen ist, und als deren specieller Fall, für $m=1$, noch der Congruenz

$$X_k(\alpha^{-1}) \equiv (-1)^k X_k(\alpha), \text{ Mod. } \lambda^{n+1},$$

besonders erwähnt werden mag.

Durch Einführung des Zeichens $X_k(\alpha)$ wird die obige Gleichung folgendermafsen dargestellt:

$$\sum_{0}^{\lambda-2}{}_h \frac{\gamma^{-hk\lambda^n}(1-\alpha\gamma^h)^i}{i} = \sum_{0}^{i}{}_s \frac{(-1)^s \Pi(i)}{i\Pi(s)\Pi(i-s)} X_k(\alpha^s).$$

Man zerlege nun die Summe rechter Hand in λ Partialsummen, indem man die Fälle sondert, wo $s\equiv 0$, $s\equiv 1$, $s\equiv 2$, $\ldots$ $s\equiv\lambda-1$ ist, für den Modul λ. Dabei bezeichne man durch P_t folgende Summe von Binomialcoëfficienten:

$$P_t = (-1)^t\left(\frac{\Pi(i)}{\Pi(t)\Pi(i-t)} - \frac{\Pi(i)}{\Pi(t+\lambda)\Pi(i-t-\lambda)} + \frac{\Pi(i)}{\Pi(t+2\lambda)\Pi(i-t-2\lambda)} - \cdots\right).$$

Alsdann ist

$$\sum_{0}^{\lambda-2}{}_h \frac{\gamma^{-hk\lambda^n}(1-\alpha\gamma^h)^i}{i} = \frac{1}{i}\left(P_0 X_k(1) + P_1 X_k(\alpha) + P_2 X_k(\alpha^2) + \cdots + P_{\lambda-1} X_k(\alpha^{\lambda-1})\right).$$

Um aus dieser Gleichung eine Congruenz für den Modul λ^{n+1} machen zu können, werde ich zunächst beweisen, dafs, auch wenn i den Factor λ enthält, dennoch $\frac{P_t}{i}$ denselben niemals im Nenner enthalten kann; oder, dafs P_t diesen Factor λ immer eben so oft enthält als i. Es sei wieder $i = c\lambda^\alpha$, so sind in allen den Fällen, wo t nicht $= 0$ ist, alle einzelnen in P_t enthaltenen Binomialcoëfficienten durch λ^α theilbar; welches mit Hülfe des in (§. 2) angewendeten Satzes über die Anzahl der in dem Producte $\Pi(A)$ enthaltenen Primfactoren von einer bestimmten Art, leicht bewiesen werden kann. Um aber für den Fall $t = 0$ zu zeigen, dafs P_0 durch λ^α theilbar ist, bemerke ich, dafs $P_0 + P_1 + P_2 + \cdots + P_{\lambda-1}$ gleich der Summe aller Binomialcoëfficienten von der $i$ten Potenz mit abwechselnden Vorzeichen, also gleich $(1-1)^i = 0$ ist. Wenn daher, wie gezeigt worden, $P_1, P_2, \ldots P_{\lambda-1}$ alle den Factor λ^α enthalten, so folgt, dafs P_0 ebenfalls durch diesen Factor theilbar sein mufs. Also $\frac{P_t}{i}$, aus dessen Nenner jeder Factor λ sich gegen die Zähler hinweghebt, kann in Beziehung auf den Mod. λ^{n+1} als ganze Zahl betrachtet werden. Wendet man nun die Congruenz

$$X_k(\alpha) \equiv m^{k\lambda^n} X_k(\alpha), \text{ Mod. } \lambda^{n+1}$$

auf die obige Gleichung an, und beachtet, dafs $X_k(1) \equiv 0$, Mod. λ^{n+1} ist, so erhält man

$$\sum_0^{\lambda-2}{}_h \frac{\gamma^{-hk\lambda^n}(1-\alpha\gamma^h)^i}{i} \equiv \frac{1}{i}(1^{k\lambda^n} P_1 + 2^{k\lambda^n} P_2 + \cdots + (\lambda-1)^{k\lambda^n} P_{\lambda-1}) X_k(\alpha),$$

für den Mod. λ^{n+1}; welche Congruenz auch in dem Falle richtig bleibt, wenn i durch λ theilbar ist.

Man entwickle jetzt die Potenz $(1-e^v)^i$ nach dem binomischen Lehrsatze und nehme den $k\lambda^n$ten Differentialquotienten für $v = 0$, so ist

$$\frac{d_0^{k\lambda^n}(1-e^v)^i}{i dv^{k\lambda^n}} = \frac{1}{i} \sum_0^i{}_s \frac{(-1)^s \Pi(i)\, s^{k\lambda^n}}{\Pi(s)\,\Pi(i-s)}.$$

Man zerlege ferner diese Summe genau eben so in Partialsummen, wie die obige, indem man von der Congruenz

$$(s + m\lambda)^{k\lambda^n} \equiv s^{k\lambda^n}, \text{ Mod. } \lambda^{n+1}$$

Gebrauch macht, so wird

$$\frac{d_0^{k\lambda^n}(1-e^v)^i}{dv^{k\lambda^n}} \equiv \frac{1}{i}(1^{k\lambda^n} P_1 + 2^{k\lambda^n} P_2 + \cdots + (\lambda-1^{k\lambda^n} P_{\lambda-1}), \text{ Mod. } \lambda^{n+1},$$

also

$$\sum_{0}^{\lambda-2}{}_h \frac{\gamma^{-hk\lambda^n}(1-\alpha\gamma^h)^i}{i} \equiv \frac{d_0^{k\lambda^n}(1-e^v)^i}{dv^{k\lambda^n}} \cdot X_k(\alpha), \text{ Mod. } \lambda^{n+1},$$

und demzufolge auch

$$\sum_{0}^{\lambda-2}{}_h \gamma^{-hk\lambda^n} l\left(\frac{\varphi(\alpha\gamma^h)}{\varphi(1)}\right) \equiv \Sigma_i \frac{C_i d_0^{k\lambda^n}(1-e^v)^i}{i\varphi(1)^i dv^{k\lambda^n}} \cdot X_k(\alpha).$$

Nun ist aber die Summe

$$\Sigma \frac{C_i(1-e^v)^i}{i\varphi(1)^i}$$

nichts anderes, als die nach Potenzen von $1-e^v$ geordnete Entwickelung des Logarithmus von $\frac{\varphi(e^v)}{\varphi(1)}$, also

$$\Sigma \frac{C_i(1-e^v)^i}{i\varphi(1)^i} = l\left(\frac{\varphi(e^v)}{\varphi(1)}\right) = l\varphi(e^v) - l\varphi(1);$$

folglich ist, wenn hiervon der $k\lambda^n$te Differentialquotient genommen und $v=0$ gesetzt wird:

$$\Sigma \frac{C_i d_0^{k\lambda^n}(1-e^v)^i}{i\varphi(1)^i dv^{k\lambda^n}} = \frac{d_0^{k\lambda^n} l\varphi(e^v)}{dv^{k\lambda^n}},$$

also

$$\sum_{0}^{\lambda-2}{}_k \gamma^{-hk\lambda^n} l\left(\frac{\varphi(\alpha\gamma^h)}{\varphi(1)}\right) \equiv \frac{d_0^{k\lambda^n} l\varphi(e^v)}{dv^{k\lambda^n}} \cdot X_k(\alpha), \text{ Mod. } \lambda^{n+1}.$$

Setzt man endlich $k=1, 2, 3, \ldots \lambda-2$ und bildet die Summe, wobei der Werth $h=0$ von den übrigen zu trennen ist, so erhält man folgenden Ausdruck des Logarithmen einer complexen Zahl in Beziehung auf den Mod. λ^{n+1}:

$$(\lambda-1)l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \equiv l\left(\frac{N\varphi(\alpha)}{\varphi(1)^{\lambda-1}}\right) + \frac{d_0^{\lambda^n} l\varphi(e^v)}{dv^{\lambda^n}} X_1(\alpha) + \frac{d_0^{2\lambda^n} l\varphi(e^v)}{dv^{2\lambda^n}} X_2(\alpha) + \cdots$$

$$\cdots + \frac{d_0^{(\lambda-2)\lambda^n} l\varphi(e^v)}{dv^{(\lambda-2)\lambda^n}} X_{\lambda-2}(\alpha), \text{ Mod. } \lambda^{n+1}.$$

Der Fall $n=0$, als der in den Anwendungen am häufigsten vorkommende, verdient noch eine besondere Berücksichtigung. Für denselben hat man, weil $N\varphi(\alpha) \equiv 1$ und $\varphi(1)^{\lambda-1} \equiv 1$, Mod. λ ist,

$$\sum_{0}^{\lambda-2}{}_h \gamma^{-hk} l\left(\frac{\varphi(\alpha\gamma^h)}{\varphi(1)}\right) \equiv \frac{d_0^k l\varphi(e^v)}{dv^k} \cdot X_k(\alpha),$$

und

$$-l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \equiv \frac{d_0 l\varphi(e^v)}{dv} X_1(\alpha) + \frac{d_0^2 l\varphi(e^v)}{dv^2} X_2(\alpha) + \cdots + \frac{d_0^{\lambda-2} l\varphi(e^v)}{dv^{\lambda-2}} X_{\lambda-2}(\alpha), \text{ Mod. } \lambda,$$

und es ist in diesem Falle

$$X_k(\alpha) = \alpha + \gamma^{-k}\alpha^{\gamma} + \gamma^{-2k}\alpha^{\gamma^2} + \cdots + \gamma^{-(\lambda-2)k}\alpha^{\gamma^{\lambda-2}};$$

wofür man auch den congruenten Ausdruck

$$X_k(\alpha) \equiv \alpha + 2^{\lambda-1-k}\alpha^2 + 3^{\lambda-1-k}\alpha^3 + \cdots + (\lambda-1)^{\lambda-1-k}\alpha^{\lambda-1}$$

setzen kann.

Um nun diese Logarithmen der complexen Zahlen und die für dieselben gefundenen Entwickelungen, in der Rechnung, da wo es sich um Congruenzen für den Mod. λ^{n+1} oder λ handelt, überall mit Sicherheit anwenden zu können, sind noch zwei Sätze nöthig, welche hier aufgestellt und bewiesen werden sollen. Nemlich:

Lehrsatz. Wenn zwei complexe Zahlen congruent sind, für den Modul λ^{n+1}, und wenn auch die beiden ganzen Zahlen, welche man erhält, wenn man in denselben $\alpha = 1$ setzt, congruent sind, für denselben Modul: so sind auch die Logarithmen dieser complexen Zahlen für diesen Modul congruent.

Die beiden complexen Zahlen seien $f(\alpha)$ und $\varphi(\alpha)$, so ist nach der Voraussetzung $f(\alpha) \equiv \varphi(\alpha)$ und $f(1) \equiv \varphi(1)$, Mod. λ^{n+1}. Setzt man der Kürze wegen

$$\frac{f(\alpha)-f(1)}{f(1)} = x, \qquad \frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)} = y,$$

so erhält man

$$l\left(\frac{f(\alpha)}{f(1)}\right) \equiv x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \tfrac{1}{4}x^4 + \cdots,$$

$$l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) \equiv y - \tfrac{1}{2}y^2 + \tfrac{1}{3}y^3 - \tfrac{1}{4}y^4 + \cdots$$

für den Mod. λ^{n+1}; welche Reihen von selbst abbrechen, weil, von einem bestimmten Gliede an, alle folgenden congruent Null werden; die man aber auch über diese Grenze hinaus noch fortgesetzt annehmen kann, so weit man will. Aus den beiden Voraussetzungen des Satzes folgt $x \equiv y$, Mod. λ^{n+1}; woraus sogleich erhellet, dafs auch $\frac{1}{k}x^k \equiv \frac{1}{k}y^k$, Mod. λ^{n+1} ist, für alle diejenigen Werthe von k, welche nicht Vielfache von λ sind. Um zu zeigen, dafs eben Das auch für alle durch λ theilbaren Werthe von k Statt findet, also allgemein für $k = c\lambda^a$, wo c nicht weiter durch λ theilbar ist, setze ich $y = x + \lambda^{n+1}z$. Dann giebt die binomische Entwickelung:

$$y^{c\lambda^a} \equiv x^{c\lambda^a} + c\lambda^{n+a+1}x^{c\lambda^a-1}z + \cdots,$$

also

$$y^{c\lambda^a} \equiv x^{c\lambda^a}, \text{ Mod. } \lambda^{n+a+1},$$

und hieraus folgt

$$\frac{y^{c\lambda^a}}{c\lambda^a} \equiv \frac{x^{c\lambda^a}}{c\lambda^a}, \text{ Mod. } \lambda^{n+1}.$$

Da nun alle einzelnen Glieder der einen Entwicklung den entsprechenden der andern Entwicklung congruent sind, so ist nothwendig

$$l\left(\frac{f(\alpha)}{f(1)}\right) \equiv l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right), \text{ Mod. } \lambda^{n+1};$$

was zu beweisen war.

Der zweite, jetzt zu beweisende Satz (die Umkehrung des ersten) ist nur unter Hinzufügung einer neuen Bedingung richtig und lautet so:

Lehrsatz. Wenn die Logarithmen zweier complexen Zahlen, nemlich $l\left(\frac{f(\alpha)}{f(1)}\right)$ und $l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right)$ congruent sind für den Modul λ^{n+1}, und auch $f(1) \equiv \varphi(1)$, Mod. λ^{n+1} ist, und wenn überdies die complexen Zahlen $f(\alpha)$ und $(\varphi\alpha)$ so beschaffen sind, dafs $f(\alpha) - f(1)$ und $\varphi(\alpha) - \varphi(1)$ beide durch $(1-\alpha)^2$ theilbar sind: so sind die complexen Zahlen $f(\alpha)$ und $\varphi(\alpha)$ selbst congruent für den Mod. λ^{n+1}.

Es sei wieder

$$\frac{f(\alpha)-f(1)}{f(1)} = x, \qquad \frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)} = y,$$

und

$$l\left(\frac{f(\alpha)}{f(1)}\right) = u, \qquad l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right) = v,$$

so ist

$$u \equiv x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \tfrac{1}{4}x^4 + \cdots, \text{ Mod. } \lambda^{n+1}.$$

Es läfst sich nun diese Reihe nach den gewöhnlichen Methoden umkehren, so dafs x in eine nach Potenzen von u geordnete Reihe entwickelt wird. Aus den ersten N Gliedern der gegebenen Reihe werden so die ersten N Glieder der umgekehrten Reihe bestimmt, und wenn man N grofs genug annimmt, so dafs in beiden Reihen, der gegebenen sowohl, als der umgekehrten, über das Nte Glied hinaus nur noch solche Glieder liegen, welche für den Mod. λ^{n+1} congruent Null sind, so hat man den vollständigen Ausdruck des x durch u in Beziehung auf den Mod. λ^{n+1}. Das Resultat der Umkehrung dieser Reihe ist aus der Analysis bekannt. Es ist

$$x \equiv \frac{u}{1} + \frac{u^2}{1.2} + \frac{u^3}{1.2.3} + \frac{u^4}{1.2.3.4} + \cdots$$

Nun ist zu beweisen, dafs auch in dieser Reihe die Anzahl der ersten

Glieder N immer so grofs angenommen werden kann, dafs alle folgenden Glieder congruent Null werden. Zu diesem Zwecke untersuche ich das allgemeine Glied der Reihe, nämlich

$$\frac{u^k}{\Pi(k)}.$$

Aus dem im zweiten Paragraphen mitgetheilten Satze über die Anzahl, wievielmal ein bestimmter Primfactor in dem Producte $\Pi(A)$ enthalten ist, folgt zunächst, dafs die Anzahl der in dem Producte $\Pi(k)$ enthaltenen Factoren λ stets kleiner ist als $\frac{k}{\lambda-1}$. Ferner enthält, nach der Voraussetzung, $f(\alpha)-f(1)$, also auch x, den Factor $(1-\alpha)^2$; woraus sogleich folgt, dafs auch u den Factor $(1-\alpha)^2$ enthalten mufs. Der Zähler u^k enthält demnach den Factor $1-\alpha$ genau $2k$ mal, und wenn man erwägt, dafs ein Factor λ genau $\lambda-1$ Factoren $1-\alpha$ giebt, so weifs man, dafs der Nenner $\Pi(k)$ stets weniger als k Factoren $1-\alpha$ enthält. Nach Aufhebung der Factoren λ im Nenner, gegen die im Zähler, bleiben folglich im Zähler mehr als k Factoren $1-\alpha$ stehen, und wenn daher $k>(n+1)(\lambda-1)$ angenommen wird, so enthält $\frac{u^k}{\Pi(k)}$ den Factor $(1-\alpha)^{(\lambda-1)(n+1)}$, d. h. den Factor λ^{n+1}. Von einem solchen Gliede an sind demnach alle folgenden $\equiv 0$. Ohne die Bedingung: $f(\alpha)-f(1)$ theilbar durch $(1-\alpha)^2$, würde aber, wie sich hieraus zeigt, die Reihe nach dem Mod. λ^{n+1} keinen endlichen Ausdruck geben.

Ganz auf dieselbe Weise ist nun auch

$$y \equiv \frac{v}{1}+\frac{v^2}{1.2}+\frac{v^3}{1.2.3}+\frac{v^4}{1.2.3.4}+\cdots, \text{ Mod. } \lambda^{n+1}.$$

Nach der Voraussetzung des zu beweisenden Satzes ist aber $u \equiv v$, Mod. λ^{n+1}. Schreibt man diese Congruenz, als Gleichung, in die Form $u = v+\lambda^{n+1}w$, so findet sich durch Entwicklung der Potenz des Binoms:

$$\frac{u^k}{\Pi(k)} = \frac{(v+\lambda^{n+1}w)^k}{\Pi(k)} = \frac{v^k}{\Pi(k)}+\frac{\lambda^{n+1}v^{k-1}w}{\Pi(1)\Pi(k-1)}+\frac{\lambda^{2n+2}v^{k-2}w^2}{\Pi(2)\Pi(k-2)}+\cdots$$

Nun heben sich, nach Dem was so eben gezeigt, alle in $\Pi(k-1)$ enthaltenen Factoren λ gegen die in v^{k-1} enthaltenen vollständig hinweg; eben so die in $\Pi(k-2)$ enthaltenen gegen die in v^{k-2} enthaltenen u. s. w. Für den Modul λ^{n+1} bleibt also von dieser binomischen Entwicklung nur das erste Glied stehen; alle übrigen verschwinden, als Vielfache von λ^{n+1}. Folglich ist

$$\frac{u^k}{\Pi(k)} \equiv \frac{v^k}{\Pi(k)}, \quad \text{Mod. } \lambda^{n+1}.$$

Da also alle Glieder der Entwicklung von x einzeln denen der Entwicklung

von y congruent sind, so ist nothwendig $x \equiv y$, Mod. λ^{n+1}, d. h.

$$\frac{f(\alpha)-f(1)}{f(1)} \equiv \frac{\varphi(\alpha)-\varphi(1)}{\varphi(1)}, \quad \text{Mod. } \lambda^{n+1};$$

und da ferner nach der Voraussetzung auch $f(1) \equiv \varphi(1)$ ist, so ist

$$f(\alpha) \equiv \varphi(\alpha), \quad \text{Mod. } \lambda^{n+1};$$

was zu beweisen war.

Um den Gebrauch der hier entwickelten Methode an einem Beispiele zu zeigen, wende ich sie zur Lösung folgender in der Theorie der complexen Zahlen sehr wichtigen Aufgabe an.

Aufgabe. Eine gegebene *complexe* Zahl durch Multiplication mit Einheiten in eine solche Form zu bringen, dafs sie, mit ihrer reciproken multiplicirt, ein Product giebt, welches einer *nichtcomplexen* ganzen Zahl congruent ist, für den Mod. λ.

Die Aufgabe ist, wie sich ergeben wird, immer lösbar, aufser wenn λ eine von den Ausnahmezahlen ist, d. h. wenn λ in einer der ersten $\frac{1}{2}(\lambda-3)$ *Bernoulli*schen Zahlen als Factor des Zählers vorkommt. Ich wende zur Lösung der Aufgabe wieder die Einheiten von der Form

$$E_n(\alpha) = e(\alpha).e(\alpha^\gamma)^{\gamma^{-2n}}.e(\alpha^{\gamma^2})^{\gamma^{-4n}} \ldots e(\alpha^{\gamma^{\mu-1}})^{\gamma^{-2(\mu-1)n}}$$

an; nemlich diejenigen, für welche die Indices sich am einfachsten darstellten.

Durch Anwendung der Logarithmen erhält man

$$l\left(\frac{E_n(\alpha)}{E(1)}\right) \equiv l\left(\frac{e(\alpha)}{e(1)}\right)+\gamma^{-2n}l\left(\frac{e(\alpha^\gamma)}{e(1)}\right)+ \cdots \gamma^{-2(\mu-1)n}l\left(\frac{e(\alpha^{\gamma^{\mu-1}})}{e(1)}\right),$$

oder, durch Anwendung des Summenzeichens:

$$l\left(\frac{E_n(\alpha)}{E_n(1)}\right) \equiv \sum_0^{\mu-1}{}_h \gamma^{-2hn} l\left(\frac{e(\alpha^{\gamma^h})}{e(1)}\right), \quad \text{Mod. } \lambda.$$

Giebt man dem h weiter die Werthe $h = \mu, \mu+1, \mu+2, .. \lambda-2$, so kehren dieselben Glieder wieder, für den Mod. λ. Wenn daher die Summe für alle Werthe $h = 0, 1, 2, \ldots \lambda-2$ genommen wird, so verdoppelt sie sich und man erhält

$$2l\left(\frac{E_n(\alpha)}{E_n(1)}\right) \equiv \Sigma\gamma^{-2hn} l\left(\frac{e(\alpha^{\gamma^h})}{e(1)}\right), \quad \text{Mod. } \lambda.$$

Setzt man nun in der einen der für den Mod. λ in diesem Paragraphen gegebenen allgemeinen Formeln $\varphi(\alpha) = e(\alpha)$, so ergiebt sich

$$2l\left(\frac{E_n(\alpha)}{E_n(1)}\right) \equiv \frac{d_0^{2n} le(e^v)}{dv^{2n}} X_{2n}(\alpha), \quad \text{Mod. } \lambda.$$

Nun ist

$$e(\alpha) = \pm\frac{\alpha^{\frac{1}{2}(1-\gamma)}(1-\alpha^{\gamma})}{1-\alpha},$$

also

$$e(e^{v}) = \pm\frac{e^{\frac{1}{2}v(1-\gamma)}1-e^{\gamma v})}{1-e^{v}} = \pm\frac{e^{\frac{1}{2}\gamma v}-e^{-\frac{1}{2}\gamma v}}{e^{\frac{1}{2}v}-e^{-\frac{1}{2}v}}.$$

Die nach Potenzen von v geordnete Reihen-Entwicklung des Logarithmen dieser Gröfse ist bekanntlich

$$le(e^{v}) = l\gamma + \frac{(\gamma^{2}-1)B_{1}v^{2}}{1.2.2} - \frac{(\gamma^{4}-1)B_{2}v^{4}}{1.2.3.4.4} + \cdots,$$

wo B_1, B_2, u. s. w. die *Bernoulli*schen Zahlen sind. Hieraus erhält man unmittelbar den $2n$ten Differentialquotienten für den Werth $v=0$, nämlich

$$\frac{d_0^{2n}le(e^{v})}{dv^{2n}} = (-1)^{n+1}\frac{(\gamma^{2n}-1)B_n}{2n},$$

also

$$l\left(\frac{E_n(\alpha)}{E_n(1)}\right) \equiv (-1)^{n+1}\frac{(\gamma^{2n}-1)B_n}{4n}X_{2n}(\alpha), \quad \text{Mod } \lambda.$$

Es sei nun $F(\alpha)$ eine beliebige, nicht durch $1-\alpha$ theilbare complexe Zahl, welche auch so angenommen werden soll, dafs $F(\alpha)-F(1)$ durch $(1-\alpha)^2$ theilbar ist, in welche Form sich jede solche complexe Zahl durch Multiplication mit einer passenden einfachen Einheit α^k bringen läfst: so hat man für den Logarithmen derselben folgende Entwicklung:

$$-l\left(\frac{F(\alpha)}{F(1)}\right) \equiv \frac{d_0lF(e^{v})}{dv}X_1(\alpha) + \frac{d_0^2lF(e^{v})}{dv^2}X_2(\alpha) \cdots \frac{d_0^{\lambda-2}lF(e^{v})}{dv^{\lambda-2}}X_{\lambda-2}(\alpha), \text{ Mod. } \lambda.$$

Nun möge die Zahl M_n durch folgende Congruenz bestimmt werden:

$$\frac{(-1)^{n+1}(\gamma^{2n}-1)B_n}{4n}M_n \equiv \frac{d_0^{2n}lF(e^{v})}{dv^{2n}}, \quad \text{Mod. } \lambda.$$

Der Werth von M_n wird durch diese Congruenz immer vollständig bestimmt sein, wenn nicht etwa der Coëfficient des M_n in derselben durch λ theilbar ist. Hat n nur einen der Werthe 1, 2, 3, ... $\mu-1$, so ist $\gamma^{2n}-1$ niemals durch λ theilbar. Es kommt also nur darauf an, dafs die *Bernoulli*sche Zahl B_n für einen der Werthe $n=1, 2, 3, \ldots \mu-1$ nicht durch λ theilbar sei. Ich setze deshalb voraus, dafs λ nicht eine von diesen Ausnahmezahlen sei, welche auch schon bei mehreren der vorhergehenden Untersuchungen ausgeschlossen werden mufsten, und für welche im Allgemeinen die vorliegende Aufgabe immer unlösbar ist. Verbindet man die für M_n aufgestellte Congruenz mit dem gefundenen Ausdrucke des Logarithmus der Einheit $E_n(\alpha)$, so er-

hält man

$$M_n l\left(\frac{E_n(\alpha)}{E_n(1)}\right) \equiv \frac{d_0^{2n} lF(e^v)}{dv^{2n}} \cdot X_{2n}(\alpha), \quad \text{Mod. } \lambda,$$

und wenn man in der Entwicklung des $-l\left(\frac{F(\alpha)}{F(1)}\right)$ alle Glieder mit geradem Stellenzeiger durch die für $n = 1, 2, 3, \ldots \mu - 1$ in dieser Congruenz gegebenen Ausdrücke ersetzt, so ergiebt sich:

$$-l\left(\frac{F(\alpha)}{F(1)}\right) \equiv M_1 l\left(\frac{E_1(\alpha)}{E_1(1)}\right) + M_2 l\left(\frac{E_2(\alpha)}{E_2(1)}\right) + \cdots + M_{\mu-1} l\left(\frac{E_{\mu-1}(\alpha)}{E_{\mu-1}(1)}\right)$$
$$+ \frac{d_0 lF(e^v)}{dv} X_1(\alpha) + \frac{d_0^3 lF(e^v)}{dv^3} X_3(\alpha) + \cdots + \frac{d_0^{\lambda-2} lF(e^v)}{dv^{\lambda-2}} X_{\lambda-2}(\alpha).$$

Es sei nun

$$F(\alpha) . E_1(\alpha)^{M_1} . E_2(\alpha)^{M_2} \ldots E_{\mu-1}(\alpha)^{M_{\mu-1}} = F_1(\alpha),$$

so ist vermöge dieser Congruenz:

$$-l\left(\frac{F_1(\alpha)}{F_1(1)}\right) \equiv \frac{d_0 lF(e^v)}{dv} X_1(\alpha) + \frac{d_0^3 lF(e^v)}{dv^3} X_3(\alpha) \cdots + \frac{d_0^{\lambda-2} lF(e^v)}{dv^{\lambda-3}} X_{\lambda-2}(\alpha),$$

für den Mod. λ. Verwandelt man α in α^{-1}, so wird für alle ungeraden Werthe von k:

$$X_k(\alpha^{-1}) \equiv -X_k(\alpha).$$

Durch diese Änderung wird also lediglich das Vorzeichen von $l\left(\frac{F_1(\alpha)}{F_1(1)}\right)$ umgekehrt, und man erhält

$$l\left(\frac{F_1(\alpha)}{F_1(1)}\right) \equiv -l\left(\frac{F_1(\alpha^{-1})}{F_1(1)}\right) \quad \text{oder} \quad l\left(\frac{F_1(\alpha) F_1(\alpha^{-1})}{F_1(1) F_1(1)}\right) \equiv 0,$$

und hieraus folgt endlich

$$F_1(\alpha) F_1(\alpha^{-1}) \equiv F(1)^2, \quad \text{Mod. } \lambda.$$

Die complexe Zahl

$$F_1(\alpha) = F(\alpha) . E_1(\alpha)^{M_1} . E_2(\alpha)^{M_2} \ldots E_{\mu-1}(\alpha)^{M_{\mu-1}},$$

in welcher die Exponenten der Einheiten durch die Congruenz

$$\frac{(-1)^{n+1}(\gamma^{2n}-1) B_n}{4n} M_n \equiv \frac{d_0^{2n} lF(e^v)}{dv^{2n}}, \quad \text{Mod. } \lambda$$

bestimmt sind, ist also eine solche, welche der vorgelegten Aufgabe genügt.

Ich füge noch die Bemerkung hinzu, dafs in der logarithmischen Entwicklung einer beliebigen complexen Zahl

$$-l\left(\frac{F(\alpha)}{F(1)}\right) \equiv \frac{d_0 lF(e^v)}{dv} X_1(\alpha) + \frac{d_0^2 lF(e^v)}{dv^2} X_2(\alpha) + \cdots + \frac{d_0^{\lambda-2} lF(e^v)}{dv^{\lambda-2}} X_{\lambda-2}(\alpha), \quad \text{Mod. } \lambda$$

die Glieder von ungeraden Stellenzeigern von den complexen Einheiten in der

complexen Zahl $F(\alpha)$ ganz unabhängig sind, d. h., dafs sie ungeändert bleiben, wenn man $F(\alpha)$ in $F(\alpha).\varepsilon(\alpha)$ verwandelt, wo $\varepsilon(\alpha)$ eine beliebige Einheit bezeichnet. Nur das erste Glied ist von der einfachen Einheit α^k abhängig, mit welcher $F(\alpha)$ multiplicirt sein kann; es ist congruent Null, wenn $F(\alpha)$ der Bedingung genügt, dafs $F(\alpha)-F(1)$ durch $(1-\alpha)^2$ theilbar ist:

§. 5.

Lösung einer Aufgabe, betreffend die allgemeinen Reciprocitätsgesetze.

In den Monatsberichten der Königlichen Akademie der Wissenschaften zu Berlin vom Mai 1851 habe ich zuerst das allgemeine Reciprocitätsgesetz für complexe Primzahlen veröffentlicht, welches ich bereits einige Jahre früher gefunden und in einem Schreiben vom 20ten Januar 1848 Herrn ***Lejeune-Dirichlet*** und durch diesen ***Jacobi*** mitgetheilt hatte. Dieses Gesetz, welches ich durch gewisse, so zu sagen metaphysische Schlüsse fand und nachher durch ziemlich umfangreich berechnete Tabellen verificirte, stützt sich auf die am Schlusse des vorhergehenden Paragraphen gelösete Aufgabe: eine ***complexe*** Zahl durch Multiplication mit passenden Einheiten auf eine solche Form zu bringen, dafs sie, mit ihrer reciproken multiplicirt, ein Product giebt, welches, für den Mod. λ, einer ***nichtcomplexen*** ganzen Zahl congruent ist. Wenn eine complexe Zahl durch Multiplication mit Einheiten in dieser Art zubereitet ist, und sie aufserdem auch der Bedingung genügt, dafs sie für den Mod. $(1-\alpha)^\lambda$ einer nichtcomplexen ganzen Zahl congruent ist, so nenne ich die complexe Zahl eine ***primäre,*** oder eine complexe Zahl in der ***primären Form.*** Die primäre Form der complexen Zahl $\varphi(\alpha)$ wird also durch folgende zwei Congruenzen definirt:

$$\varphi(\alpha)\varphi(\alpha^{-1}) \equiv \varphi(1)^2, \text{ Mod. } \lambda,$$
$$\varphi(\alpha) \equiv \varphi(1), \text{ Mod. } (1-\alpha)^2,$$

und es kann jede gegebene (nicht durch $1-\alpha$ theilbare) complexe Zahl durch Multiplication mit passenden Einheiten auf diese primäre Form gebracht werden, wenn λ nicht eine von den Ausnahmezahlen ist, welche in einer der ersten $\frac{1}{2}(\lambda-3)$ ***Bernoulli***schen Zahlen als Factoren enthalten sind. Das von mir gefundene allgemeine Reciprocitätsgesetz, auf diese Definition der primären Form der complexen Zahlen sich stützend, lautet nun einfach folgendermaafsen:

Wenn die beiden complexen Primzahlen $f_1(\alpha)$ und $\varphi_1(\alpha)$ in der primären Form genommen werden, oder, falls sie ideal sind, wenn die zu ***wirklichen*** complexen Zahlen werdenden Potenzen derselben in der pri-

mären Form genommen werden: so ist

$$\left(\frac{f_1(\alpha)}{\varphi_1(\alpha)}\right) = \left(\frac{\varphi_1(\alpha)}{f_1(\alpha)}\right).$$

Sowohl wegen der am Anfange dieser Abhandlung gegebenen Definition des Symbols $\left(\frac{f_1(\alpha)}{\varphi_1(\alpha)}\right)$, als auch wegen der Forderung, dafs $f_1(\alpha)$ und $\varphi_1(\alpha)$ complexe Zahlen von der primären Form sein sollen, erstreckt sich dieses Gesetz nicht auf die Ausnahmefälle, wo λ ein Factor einer der ersten $\frac{1}{2}(\lambda-3)$ *Bernoulli*schen Zahlen ist.

Einen strengen und allgemeinen Beweis des Gesetzes habe ich bisher noch nicht gefunden, da die neuen Hülfsmittel, welche ich zu diesem Zwecke aufgesucht habe und welche ich ein anderesmal zu veröffentlichen gedenke, nur für den Beweis einiger besondern, bisher noch nirgend bewiesenen Fälle ausgereicht haben, (z. B. für den Fall, dafs $f_1(\alpha)$ und $\varphi_1(\alpha)$ conjugirte complexe Zahlen sind, oder $\varphi_1(\alpha) = f_1(\alpha^k)$ ist). Wenn gleich daher die allgemeine Gültigkeit dieses einfachen Reciprocitätsgesetzes noch problematisch ist, bis ein strenger Beweis davon gefunden sein wird, so ist doch so viel klar, dafs die von mir definirte *primäre* Form der complexen Zahlen, für welche wenigstens in vielen Fällen die Reciprocitätsgesetze sich am einfachsten darstellen, für dieselben eine besondere Bedeutung hat. Es wird deshalb nicht uninteressant sein, eine Vergleichung des Reciprocitätsgesetzes für die *primären complexen* Primzahlen mit dem Reciprocitätsgesetze für diejenigen *complexen* Primzahlen aufzustellen, welche den Bedingungen primärer Zahlen nicht unterworfen sind. Um sogleich vollkommen präcis auszusprechen, um was es sich hier handeln soll, fasse ich es in die folgende

Aufgabe. Wenn das Reciprocitätsgesetz für zwei complexe Primzahlen, für die primäre Form derselben als gegeben angenommen wird: daraus das Reciprocitätsgesetz für die complexen Primzahlen abzuleiten, welche der Bedingung, primär zu sein, nicht unterliegen.

Es seien $f(\alpha)$ und $\varphi(\alpha)$ zwei beliebige complexe Primzahlen, von welchen ich der Einfachheit wegen nur das Eine voraussetze, dafs sie durch Multiplication mit einer passenden Potenz der einfachen Einheit α so zubereitet sind, dafs sie den Bedingungen

$$f(\alpha) \equiv f(1) \quad \text{und} \quad \varphi(\alpha) \equiv \varphi(1), \quad \text{Mod.}(1-\alpha)^2$$

genügen. Es seien ferner $f_1(\alpha)$ und $\varphi_1(\alpha)$ dieselben complexen Primzahlen in der *primären* Form, also gereinigt von den in den Zahlen $f(\alpha)$ und $\varphi(\alpha)$

beliebig vorkommenden complexen Einheiten, so hat man, wie im vorigen Paragraphen gezeigt worden:

$$f(\alpha)\,E_1(\alpha)^{M_1}\,.\,E_2(\alpha)^{M_2}\,\ldots\,E_{\mu-1}(\alpha)^{M_{\mu-1}} \equiv f_1(\alpha),$$

wo die Exponenten M_1, M_2, $\ldots$ $M_{\mu-1}$ durch die Congruenz

$$\frac{(-1)^{n+1}(\gamma^{2n}-1)\,B_n}{4n}\,M_n \equiv \frac{d_0^{2n}\,lf(e^v)}{dv^{2n}}, \quad \text{Mod. } \lambda$$

bestimmt sind. Eben so hat man auch

$$\varphi(\alpha)\,E_1(\alpha)^{N_1}\,.\,E_2(\alpha)^{N_2}\,\ldots\,E_{\mu-1}(\alpha)^{N_{\mu-1}} \equiv \varphi_1(\alpha),$$

wo die Exponenten N_1, N_2, $\ldots$ $N_{\mu-1}$ durch die Congruenz

$$\frac{(-1)^{n+1}(\gamma^{2n}-1)\,B_n}{4n}\,N_n \equiv \frac{d_0^{2n}\,l\varphi(e^v)}{dv^{2n}}, \quad \text{Mod. } \lambda$$

bestimmt werden. Es soll nun das Zeichen des Index Ind. auf den Mod. $f(\alpha)$, oder, was Dasselbe ist $f_1(\alpha)$, und das Zeichen ind. auf den Mod. $\varphi(\alpha)$ oder $\varphi_1(\alpha)$ sich beziehen, so dafs, wenn $F(\alpha)$ eine beliebige complexe Zahl bezeichnet:

$$F(\alpha)^{\frac{Nf(\alpha)-1}{\lambda}} \equiv \alpha^{\text{Ind.}F(\alpha)}, \quad \text{Mod. } f(\alpha),$$

$$F(\alpha)^{\frac{N\varphi(\alpha)-1}{\lambda}} \equiv \alpha^{\text{ind.}F(\alpha)}, \quad \text{Mod. } \varphi(\alpha) \text{ ist.}$$

Nimmt man nun auf beiden Seiten der Gleichung, welche $f_1(\alpha)$ durch $f(\alpha)$ ausdrückt, die Indices in Beziehung auf den Modul $\varphi(\alpha)$, so erhält man

$$\text{ind.}f(\alpha)+M_1\,\text{ind.}E_1(\alpha)+M_2\,\text{ind.}E_2(\alpha)+\cdots+M_{\mu-1}\,\text{ind.}E_{\mu-1}(\alpha)\equiv\text{ind.}f_1(\alpha)$$

für den Mod. λ. Eben so, wenn man auf beiden Seiten der Gleichung, welche $\varphi_1(\alpha)$ durch $\varphi(\alpha)$ ausdrückt, die Indices in Beziehung auf den Mod. $f(\alpha)$ nimmt:

$$\text{Ind.}\varphi(\alpha)+N_1\,\text{Ind.}E_1(\alpha)+N_2\,\text{Ind.}E_2(\alpha)+\cdots+N_{\mu-1}\,\text{Ind.}E_{\mu-1}(\alpha)\equiv\text{Ind.}\varphi_1(\alpha).$$

Ich wende jetzt die in dem ersten und dritten Paragraphen der gegenwärtigen Abhandlung gefundenen Ausdrücke der Indices der Einheiten $E_n(\alpha)$ an; und zwar diejenigen, welche nur die complexe Primzahl selbst enthalten, auf die der Index sich bezieht, welche auch in allen Fällen, es mag der Modul eine zum Exponenten Eins oder zu einem andern Exponenten gehörende complexe Primzahl sein, dieselben sind, nämlich:

$$\left.\begin{aligned}\text{Ind.}E_n(\alpha) &\equiv \frac{(-1)^n(\gamma^{2n}-1)\,B_n}{4n}\cdot\frac{d_0^{\lambda-2n}\,lf(e^v)}{dv^{\lambda-2n}},\\ \text{ind.}E_n(\alpha) &\equiv \frac{(-1)^n(\gamma^{2n}-1)\,B_n}{4n}\cdot\frac{d_0^{\lambda-2n}\,l\varphi(e^v)}{dv^{\lambda-2n}},\end{aligned}\right\} \quad \ldots \text{ Mod. } \lambda.$$

Diese Ausdrücke, verbunden mit den Congruenzen, welche M_n und N_n be-

stimmen, geben

$$\begin{aligned} M_n \operatorname{ind}. E_n(\alpha) &\equiv -\frac{d_0^{2n} lf(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} l\varphi(e^v)}{dv^{\lambda-2n}}, \\ N_n \operatorname{Ind}. E_n(\alpha) &\equiv -\frac{d_0^{2n} l\varphi(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}}, \end{aligned} \quad \ldots \text{ Mod. } \lambda.$$

Vermöge dieser Ausdrücke verwandeln sich die obigen Congruenzen in folgende:

$$\begin{aligned} \operatorname{ind}. f(\alpha) &\equiv \operatorname{ind}. f_1(\alpha) + \sum_1^{\mu-1}{}_n \frac{d_0^{2n} lf(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} l\varphi(e^v)}{dv^{\lambda-2n}}, \\ \operatorname{Ind}. \varphi(\alpha) &\equiv \operatorname{Ind}. \varphi_1(\alpha) + \sum_1^{\mu-1}{}_n \frac{d_0^{2n} l\varphi(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} lf(e^v)}{dv^{\lambda-2n}}, \end{aligned} \quad \ldots \text{ Mod. } \lambda.$$

Nimmt man die Glieder der in der zweiten dieser Congruenzen vorkommenden Summe in umgekehrter Ordnung, so läfst sich dieselbe auch folgendermaafsen darstellen:

$$\operatorname{Ind}. \varphi(\alpha) \equiv \operatorname{Ind}. \varphi_1(\alpha) + \sum_1^{\mu-1}{}_n \frac{d_0^{2n+1} lf(e^v)}{dv^{2n+1}} \cdot \frac{d_0^{\lambda-2n-1} l\varphi(e^v)}{dv^{\lambda-2n-1}}.$$

Subtrahirt man dieselbe von der ersten, so erhält man

$$\operatorname{ind}. f(\alpha) - \operatorname{Ind}. \varphi(\alpha) \equiv \operatorname{ind}. f_1(\alpha) - \operatorname{Ind}. \varphi_1(\alpha) + \Sigma,$$

wo der einfache Buchstabe Σ als abgekürztes Zeichen für die Reihe

$$\Sigma = \sum_2^{\lambda-2}{}_h (-1)^h \frac{d_0^h lf(e^v)}{dv^h} \cdot \frac{d_0^{\lambda-h} l\varphi(e^v)}{dv^{\lambda-1}}$$

gesetzt ist.

Diese Congruenz enthält die vollständige Lösung der gestellten Aufgabe. Wendet man die dem *Legendre*schen Zeichen für die quadratischen Reste analogen Zeichen für die höheren Potenzreste an, welche mit den Zeichen ind. und Ind. so zusammenhangen, dafs

$$\left(\frac{F(\alpha)}{\varphi(\alpha)}\right) = \alpha^{\operatorname{ind}. F(\alpha)}, \quad \left(\frac{F(\alpha)}{f(\alpha)}\right) = \alpha^{\operatorname{Ind}. F(\alpha)},$$

so nimmt das gefundene Resultat folgende Form an:

$$\frac{\left(\frac{f(\alpha)}{\varphi(\alpha)}\right)}{\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)} = \frac{\left(\frac{f_1(\alpha)}{\varphi_1(\alpha)}\right)}{\left(\frac{\varphi_1(\alpha)}{f_1(\alpha)}\right)} \cdot \alpha^{\Sigma}.$$

Der Ausdruck des Σ, welcher entwickelt folgendermaafsen geschrieben wird:

$$\begin{aligned} \Sigma = \frac{d_0^2 lf(e^v)}{dv^2} \cdot \frac{d_0^{\lambda-2} l\varphi(e^v)}{dv^{\lambda-2}} - \frac{d_0^3 lf(e^v)}{dv^3} \cdot \frac{d_0^{\lambda-3} l\varphi(e^v)}{dv^{\lambda-3}} + \ldots \\ \ldots - \frac{d_0^{\lambda-2} lf(e^v)}{dv^{\lambda-2}} \cdot \frac{d_0^2 l\varphi(e^v)}{dv^2}, \end{aligned}$$

enthält, da die complexen Zahlen $f(\alpha)$ und $\varphi(\alpha)$ als gegeben betrachtet werden, nur gegebene Gröfsen, und wenn nun auch das Reciprocitätsgesetz für die primären complexen Zahlen $f_1(\alpha)$ und $\varphi_1(\alpha)$ als gegeben angenommen wird, d. h., wenn das Verhältnifs $\left(\frac{f_1(\alpha)}{\varphi_1(\alpha)}\right):\left(\frac{\varphi_1(\alpha)}{f_1(\alpha)}\right)$ bekannt ist: so ist vermöge dieser Gleichung auch das Reciprocitäts-Verhältnifs $\left(\frac{f(\alpha)}{\varphi(\alpha)}\right):\left(\frac{\varphi(\alpha)}{f(\alpha)}\right)$ der complexen Primzahlen $f(\alpha)$ und $\varphi(\alpha)$ gegeben.

Angenommen, dafs das von mir gefundene, oben aufgestellte Reciprocitätsgesetz, nach welchem

$$\left(\frac{f_1(\alpha)}{\varphi_1(\alpha)}\right) = \left(\frac{\varphi_1(\alpha)}{f_1(\alpha)}\right)$$

sein soll, richtig sei, so hat man für die nichtprimären complexen Primzahlen $f(\alpha)$ und $\varphi(\alpha)$, welche nur der einen Bedingung genügen müssen, dafs $f(\alpha)-f(1)\equiv 0$ und $\varphi(\alpha)-\varphi(1)\equiv 0$ ist, nach dem Mod. $(1-\alpha)^2$, das Reciprocitätsgesetz:

$$\left(\frac{f(\alpha)}{\varphi(\alpha)}\right) = \left(\frac{\varphi(\alpha)}{f(\alpha)}\right)\cdot\alpha^{\Sigma}.$$

Mit dem Reciprocitätsgesetze für die ***primären complexen*** Primzahlen ist also zugleich auch das Reciprocitätsgesetz für beliebige ***nichtprimäre complexe*** Primzahlen gegeben.

In der schon oben erwähnten Abhandlung (im 39ten Bande S. 351 dieses Journals) hat Herr ***Eisenstein*** eine, zwar auf einer unbewiesenen Voraussetzung beruhende, jedoch sehr sinnreiche Methode entwickelt, um diejenige Potenz von α zu finden, welche dem Verhältnisse $\left(\frac{A}{B}\right):\left(\frac{B}{A}\right)$ gleich ist, wenn A und B complexe Zahlen sind. Der Ausdruck dieser mit dem Namen ***Umkehrungsfactor*** bezeichneten Potenz von α, welchen er daselbst giebt, würde, wie es mir scheint, gehörig entwickelt und vereinfacht, sich auf dieselbe Form bringen lassen, wie der in der hier gegebenen Reciprocitätsgleichung enthaltene Ausdruck des Umkehrungsfactors α^{Σ}, in welchem Σ durch die Differentialquotienten der Logarithmen der complexen Zahlen $f(\alpha)$ und $\varphi(\alpha)$, für $\alpha = e^{\nu}$, gegeben ist. Wenn wirklich, wie ich vermuthe, dieses Resultat der erwähnten Abhandlung mit dem hier aufgestellten übereinstimmt, so hätte Herr ***Eisenstein*** aus denselben auch das von mir gefundene einfache Reciprocitätsgesetz für die primären complexen Primzahlen finden können; denn dieses

ist eben so eine Folge von jenem, als jenes eine Folge von diesem ist. Dies ist ihm aber nicht gelungen, obgleich er wirklich (S. 361) den Versuch macht, nach seiner Methode ein Reciprocitätsgesetz von der einfachsten Form $\left(\frac{A}{B}\right) = \left(\frac{B}{A}\right)$ durch passende Bestimmung der Einheiten in complexen Zahlen A und B zu erlangen; denn die Bedingungen, welche er dafür aufstellt, lassen sich, wie leicht zu zeigen, im Allgemeinen nicht erfüllen.

Breslau. den 30ten November 1851.

Berichtigungen.

S. 103 Z. 17 v. u. bis S. 104 Z. 1 v. u. und S. 119 Z. 4 v. u. bis S. 120 Z. 6 v. u. l. ind. st. Ind.

S. 123 Z. 9 v. o. l. D_i st. D^i