

27.

Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze.

(Von Herrn Dr. G. Eisenstein, Docent an der Universität zu Berlin.)

§. 1.

Obwohl bei den höheren Reciprocitätssätzen das wahre wissenschaftliche Interesse ohne Zweifel in den *Beweisen* liegt, so möchte es doch nicht überflüssig sein, hier zu zeigen, wie die *Sätze selbst* durch eine eigenthümliche Art von Induction ohne alle ermüdende Rechnung leicht herausgebracht werden können; auf dem eingeschlagenen Wege wird man außerdem unwillkürlich zur Anknüpfung mehrerer anderer interessanter Betrachtungen veranlaßt.

Um nicht den allgemeinsten, jedoch einen Fall von großer Allgemeinheit zu behandeln, aus dem die unbeschränkte Anwendbarkeit des Verfahrens erhellen wird, sei λ eine positive ungerade Primzahl, ζ eine primitive λ te Wurzel der Einheit. Die lateinischen Buchstaben sollen im Allgemeinen ganze complexe Zahlen aus solchen Wurzeln der Einheit bezeichnen, also ganze ganzzahlige Functionen von ζ ; und zwar wird noch vorausgesetzt, daß dieselben den Factor $1 - \zeta = \eta$ nicht enthalten; endlich sollen die Symbole $\left(\frac{A}{B}\right)$ u. s. w. *) sich auf die Theorie der λ ten Potenzreste beziehen. Alles kommt darauf an, das Verhältniß $\left(\frac{A}{B}\right) : \left(\frac{B}{A}\right)$ zu ermitteln, welches ich durch (A, B) bezeichne. Da beide Symbole gewisse Potenzen von ζ vorstellen, so ist auch ihr Verhältniß eine Potenz von ζ , und man kann daher $(A, B) = \left(\frac{A}{B}\right) : \left(\frac{B}{A}\right) = \zeta^{\varphi(A, B)}$ setzen, wo man den Exponenten $\varphi(A, B)$ zwar nicht gradezu als Function von A und B , aber doch als Function der in beiden complexen Zahlen vorkommenden ganzzahligen Elemente ansehen kann; es versteht sich, daß A und B ohne gemeinschaftlichen Theiler angenommen werden.

Der eigentliche Nerv der hier anzustellenden Betrachtungen besteht in der Zurückführung des Verhältnisses $\left(\frac{A}{B}\right) : \left(\frac{B}{A}\right) = (A, B)$ auf das analoge

*) Über die Definition dieser Symbole sehe man weiter unten.

Verhältniß $\left(\frac{A'}{B'}\right): \left(\frac{B'}{A'}\right) = (A', B')$ für zwei möglichst einfache complexe Zahlen A', B' , von der Art, daß $(A, B) = (A', B')$ wird. Diese Relation wird Statt finden, wenn man A', B' so bestimmen kann, daß $\varphi(A, B) \equiv \varphi(A', B') \pmod{\lambda}$ wird. Wie complicirt die Function $\varphi(A, B)$, der Exponent des Umkehrungsfactors, auch sein mag, so ist es doch naturgemäß, sie als eine ganze Function der in A und B vorkommenden Elemente (Factoren der Potenzen von ζ) mit rationalen Zahlen-Coëfficienten anzunehmen *). Wenn nun die numerischen Coëfficienten in $\varphi(A, B)$ entweder ganze Zahlen sind, oder doch nicht den Nenner λ enthalten, so reicht es hin, $A \equiv A', B \equiv B' \pmod{\lambda}$ zu setzen, um daraus $\varphi(A, B) \equiv \varphi(A', B') \pmod{\lambda}$ schliessen zu können; wenn aber jene numerischen Coëfficienten, wie es doch sein könnte, den Nenner λ enthalten, und es bedeutet λ^μ die höchste in ihrem Generalnenner aufgehende Potenz von λ , so wird es nothwendig sein, die Congruenzen $A \equiv A', B \equiv B'$ in Bezug auf $\text{mod. } \lambda^{\mu+1}$, oder auf eine noch höhere Potenz von λ gelten zu lassen, um aus denselben $\varphi(A, B) \equiv \varphi(A', B') \pmod{\lambda}$ zu folgern. Da jede Potenz von λ , wenn sie als Modul auftritt, auch durch eine $\lambda-1$ mal so hohe Potenz von $\eta = 1 - \zeta$ ersetzt werden kann, so wird $\varphi(A, B) \equiv \varphi(A', B') \pmod{\lambda}$, also $(A, B) = (A', B')$ sein, wenn in den Congruenzen $A \equiv A' \pmod{\eta^\sigma}, B \equiv B' \pmod{\eta^\sigma}$ der Exponent σ eine gewisse Grenze überschreitet. Eine obere Grenze für diesen Exponenten von η existirt nicht, weil die Folgerung *a fortiori* richtig sein wird, wenn man den Exponenten vergrößert.

Um die untere Grenze für den Exponenten σ möglichst zu reduciren, was jetzt geschehen soll, dient die leicht zu beweisende Bemerkung, daß für jede complexe Zahl A in Bezug auf $\text{mod. } \eta^{\lambda+1}$ immer eine Congruenz von folgender Form angenommen werden kann:

$$A \equiv P = g^\alpha (1 - k_1 \eta)^{\alpha_1} (1 - k_2 \eta^2)^{\alpha_2} \dots (1 - k_\lambda \eta^\lambda)^{\alpha_\lambda} \pmod{\eta^{\lambda+1}},$$

wo g eine reelle primitive Congruenzwurzel $\text{mod. } \lambda$, α eine Zahl aus der Reihe $0, 1, 2, 3, \dots, \lambda-2$, und $\alpha_1, \alpha_2, \dots, \alpha_\lambda$ Zahlen aus der Reihe $0, 1, 2, \dots, \lambda-1$ sind, während $k_1, k_2, \dots, k_\lambda$ beliebige, nicht durch η

*) Für das gewöhnliche quadratische Reciprocitätsgesetz, durch welches das Verhältniß $\left(\frac{p}{q}\right): \left(\frac{q}{p}\right)$ bestimmt wird, ist diese Function $\frac{1}{4}(p-1)(q-1)$.

theilbare ganze complexe Zahlen bedeuten; dafs ferner, wenn man

$$A \equiv g^\alpha (1 - k_1 \eta)^{\alpha_1'} (1 - k_2 \eta^2)^{\alpha_2'} \dots (1 - k_\lambda \eta^\lambda)^{\alpha_\lambda'} \pmod{\eta^\sigma}$$

setzt, wo σ eine beliebige Zahl $> \lambda + 1$ ist, die Exponenten $\alpha_1', \alpha_2', \dots, \alpha_\lambda'$ sich resp. von $\alpha_1, \alpha_2, \dots, \alpha_\lambda$ nur um Vielfache von λ unterscheiden, so dafs dieselbe Zahl A , welche $\equiv P \pmod{\eta^{\lambda+1}}$ ist, in Bezug auf eine beliebige hohe Potenz von η als Modul $\equiv L^\lambda P$ gesetzt werden kann. Ist Q ein ähnliches Product, wie P , von der Art, dafs $B \equiv Q \pmod{\eta^{\lambda+1}}$, so wird in derselben Weise $B \equiv M^\lambda Q \pmod{\eta^\sigma}$. Sind ferner a und b irgend zwei complexe Zahlen, welche den Congruenzen $A \equiv a \pmod{\eta^{\lambda+1}}$, $B \equiv b \pmod{\eta^{\lambda+1}}$ Genüge leisten, so wird auch $a \equiv P \pmod{\eta^{\lambda+1}}$, $b \equiv Q \pmod{\eta^{\lambda+1}}$ und hieraus wieder $a \equiv l^\lambda P$, $b \equiv m^\lambda Q \pmod{\eta^\sigma}$ sein. Nimmt man hier σ hinreichend grofs an, damit die obige Folgerung, nach welcher $(A, B) = (A', B')$ aus $A \equiv A'$, $B \equiv B' \pmod{\eta^\sigma}$ gezogen werden kann, zuläfslich sei, so hat man aus $A \equiv L^\lambda P$ und $B \equiv M^\lambda Q \pmod{\eta^\sigma}$ die Gleichung $(A, B) = (L^\lambda P, M^\lambda Q)$, und eben so aus $a \equiv l^\lambda P$, $b \equiv m^\lambda Q \pmod{\eta^\sigma}$ die Gleichung $(a, b) = (l^\lambda P, m^\lambda Q)$; da nun nach der Natur der Symbole für die λ ten Potenzreste die λ ten Potenzen, so oft sie als Factoren vorkommen, also hier L^λ , M^λ , l^λ und m^λ , weggelassen werden können, so wird endlich $(A, B) = (P, Q) = (a, b)$, wenn $A \equiv a \equiv P \pmod{\eta^{\lambda+1}}$ und $B \equiv b \equiv Q \pmod{\eta^{\lambda+1}}$. Hieraus folgt, dafs es vollkommen hinreicht, oben λ selbst als untere Grenze für σ anzunehmen, und dafs man allgemein folgenden Satz hat:

I. „Das Verhältnifs $\left(\frac{A}{B}\right) : \left(\frac{B}{A}\right)$ ändert sich nicht, wenn man A und B durch ihre Reste $\pmod{\eta^{\lambda+1}}$ oder $\pmod{\lambda \eta^2}$ ersetzt;“ wobei man nur darauf zu achten hat, dafs diese Reste ebenfalls relative Primzahlen zu einander werden.

Da, wie dies bereits bemerkt und bei der Ableitung des eben aufgestellten Satzes benutzt worden ist, jede ganze complexe Zahl einem Producte von der Form $P \pmod{\eta^{\lambda+1}}$ congruent gesetzt werden kann, so wird nach eben jenem Satze die Vergleichung irgend zweier complexen Zahlen auf die Vergleichung der Factoren des Productes P unter einander und mit ähnlichen, etwa für andere Werthe der Gröfsen k , zurückgeführt. Um das Product P noch etwas zu vereinfachen, schreibe man g^λ , welches ebenfalls eine primitive Wurzel ist, statt g , dann kann man den ersten Factor von P als eine λ te Potenz in den Symbolen ganz weglassen. Die allgemeine Bestimmung von (A, B) ist dann allein auf die Untersuchung aller Gröfsen von der Form $(1 - k_\mu \eta^\mu, 1 - k_\nu' \eta^\nu)$ für die Werthe 1, 2, 3, \dots, λ von μ und ν zurückge-

führt. Von diesen Größen ist zu bemerken, daß sie sich nicht ändern, wenn k_μ um ein Vielfaches von $\eta^{\lambda+1-\mu}$, oder k'_ν um ein Vielfaches von $\eta^{\lambda+1-\nu}$ geändert werden, wie dies ebenfalls aus obigem Satze hervorgeht, indem hierdurch die Zahlen $1-k_\mu\eta^\mu$ und $1-k'_\nu\eta^\nu$ nur eine Änderung um Vielfache von $\eta^{\lambda+1}$ erleiden. Die Willkürlichkeit von k_μ und k'_ν wird man dazu benutzen, um, wie dies bei der Bedeutung des Zeichens $(1-k_\mu\eta^\mu, 1-k'_\nu\eta^\nu)$ nöthig ist, gemeinschaftliche Theiler der beiden in demselben vorkommenden Zahlen zu vermeiden. Zur Vereinfachung der Resultate nehme ich $k_\mu \equiv 1 \pmod{\eta^{\lambda+1-\mu}}$, $k'_\nu \equiv 1 \pmod{\eta^{\lambda+1-\nu}}$ an; dann wird $1-k_\mu\eta^\mu \equiv 1-\eta^\mu \pmod{\eta^{\lambda+1}}$, $1-k'_\nu\eta^\nu \equiv 1-\eta^\nu \pmod{\eta^{\lambda+1}}$ und $(1-k_\mu\eta^\mu, 1-k'_\nu\eta^\nu)$ wird eine bloß von μ und ν abhängige Größe $= \varepsilon_{\mu,\nu}$, welche geradezu $= (1-\eta^\mu, 1-\eta^\nu) = \varepsilon_{\mu,\nu}$ gesetzt werden kann, wenn $1-\eta^\mu$ zu $1-\eta^\nu$ relative Primzahl ist. Dies letztere findet übrigens Statt, wie leicht zu zeigen, wenn μ zu ν relative Primzahl ist. Setzt man nun, den eben gemachten Annahmen entsprechend,

$$(1.) \quad A \equiv \alpha^1(1-\eta)^{\alpha_1}(1-\eta^2)^{\alpha_2}(1-\eta^3)^{\alpha_3} \dots (1-\eta^\lambda)^{\alpha_\lambda} \pmod{\eta^{\lambda+1}},$$

$$(2.) \quad B \equiv \beta^1(1-\eta)^{\beta_1}(1-\eta^2)^{\beta_2}(1-\eta^3)^{\beta_3} \dots (1-\eta^\lambda)^{\beta_\lambda} \pmod{\eta^{\lambda+1}},$$

wo beiläufig die reellen ganzen Zahlen α , β der Summe der Elemente in A respective B congruent werden $\pmod{\lambda}$ und die Exponenten von $1-\eta$, $1-\eta^2$, u. s. w. der Reihe $0, 1, 2, \dots, \lambda-1$ entnommen sind, so wird allgemein

$$(3.) \quad \left(\frac{A}{B}\right) : \left(\frac{B}{A}\right) = (A, B) = \prod \varepsilon_{\mu,\nu}^{\alpha_\mu\beta_\nu} = \varepsilon_{1,1}^{\alpha_1\beta_1} \cdot \varepsilon_{1,2}^{\alpha_1\beta_2} \cdot \varepsilon_{2,1}^{\alpha_2\beta_1} \dots \varepsilon_{\lambda,\lambda}^{\alpha_\lambda\beta_\lambda}.$$

Durch ganz analoge Betrachtungen findet man den Ergänzungssatz:

II. „Daß $\left(\frac{\eta}{A}\right)$ unverändert bleibt, wenn A um Vielfache von $\eta^{\lambda+1}$ geändert wird,“ und daß unter Voraussetzung der Congruenz (1.) die Formel

$$(4.) \quad \left(\frac{\eta}{A}\right) = \left(\frac{\eta}{1-\eta}\right)^{\alpha_1} \left(\frac{\eta}{1-\eta^2}\right)^{\alpha_2} \dots \left(\frac{\eta}{1-\eta^\lambda}\right)^{\alpha_\lambda}$$

gilt. Diese letzteren Behauptungen können auch leicht als Folgerungen aus dem ersten Satze vollkommen streng abgeleitet werden, indem man, wie ich wegen Mangel an Raum nur kurz andeuten kann, aus einer Gleichung von der Form $A-a = \eta^{\lambda+1} \cdot c$, oder von der Form $(A+a\eta^{\lambda+1})-a = \eta^{\lambda+1} \cdot (c+a)$, wenn c durch η theilbar sein sollte, drei Congruenzen und aus diesen wiederum Gleichungen zwischen Symbolen hervorgehen läßt, durch welche $\left(\frac{\eta}{A}\right)$ in $\left(\frac{\eta}{a}\right)$ ausgedrückt werden kann.

§. 2.

Die Größen ε haben merkwürdige und leicht abzuleitende Eigenschaften, durch welche ihre Berechnung ungemein vereinfacht wird. Es ist zunächst allgemein

$$(5.) \quad \varepsilon_{\mu, \nu} = \varepsilon_{\mu, \mu+\nu} \cdot \varepsilon_{\mu+\nu, \nu} \cdot \left(\frac{\eta}{1-\eta^{\mu+\nu}} \right)^\nu.$$

Denn setzt man $1-\eta^\mu = h_\mu$, $1-\eta^\nu = h_\nu$, $1-\eta^{\mu+\nu} = h_{\mu+\nu}$, so ergibt sich die identische Gleichung $h_{\mu+\nu} - h_\nu = \eta^\nu h_\mu$. Die aus ihr hervorgehenden Congruenzen $h_{\mu+\nu} \equiv h_\nu \pmod{h_\mu}$, $h_{\mu+\nu} \equiv \eta^\nu h_\mu \pmod{h_\nu}$ und $(-1)^\lambda h_\nu \equiv \eta^\nu h_\mu \pmod{h_{\mu+\nu}}$ liefern die Gleichungen zwischen Symbolen resp. $\left(\frac{h_{\mu+\nu}}{h_\mu} \right) = \left(\frac{h_\nu}{h_\mu} \right)$, $\left(\frac{h_{\mu+\nu}}{h_\nu} \right) = \left(\frac{\eta^\nu}{h_\nu} \right) \left(\frac{h_\mu}{h_\nu} \right) = \left(\frac{h_\mu}{h_\nu} \right)$, $\left(\frac{h_\nu}{h_{\mu+\nu}} \right) = \left(\frac{\eta}{h_{\mu+\nu}} \right)^\nu \left(\frac{h_\mu}{h_{\mu+\nu}} \right)$, durch deren geeignete Verbindung sich unmittelbar die Formel (5.) ergibt, wenn man erwägt, daß $\varepsilon_{\mu, \nu} = (h_\mu, h_\nu) = \left(\frac{h_\mu}{h_\nu} \right) : \left(\frac{h_\nu}{h_\mu} \right)$, u. s. w. ist. Gegen diesen Beweis ist nichts einzuwenden, so lange μ zu ν , also auch zu $1-\eta^\mu$ zu $1-\eta^\nu$ relative Primzahl ist *); im entgegengesetzten Falle sind, um der vollkommenen Strenge zu genügen, h_μ , h_ν und $h_{\mu+\nu}$ durch andere Zahlen zu ersetzen, welche ihnen $\equiv \pmod{\eta^{\lambda+1}}$ sind. Setzt man $h_\mu = 1-\eta^\mu - l\eta^{\lambda+1}$, $h_\nu = 1-\eta^\nu$, so wird wieder $h_{\mu+\nu} - h_\nu = \eta^\nu h_\mu$, wenn $h_{\mu+\nu} = 1-\eta^{\mu+\nu} - l\eta^\nu \cdot \eta^{\lambda+1}$ angenommen wird, und man erreicht es hier sicher, daß h_μ mit h_ν keinen gemeinschaftlichen Theiler hat, wenn man $l\eta^{\lambda+1}$ als Potenz von η annimmt, deren Exponent $> \lambda$ und durch ν theilbar ist; denn es wird dann $1-l\eta^{\lambda+1}$ durch $1-\eta^\nu$ theilbar und also $1-l\eta^{\lambda+1} - \eta^\mu = h_\mu$ zu $1-\eta^\nu$ relative Primzahl. Die ferneren Schlüsse erleiden nur leichte Modificationen, bei denen auch Satz II. zu Hülfe zu nehmen ist. Uebrigens ist stets $\varepsilon_{\mu, \nu} = 1$, wenn μ mit ν einen gemeinschaftlichen Theiler hat; auch wenn $\mu = \nu$ ist.

Eine zweite Eigenschaft besteht darin, daß immer

$$(6.) \quad \varepsilon_{\mu, \nu} = 1 \text{ ist,}$$

wenn einer der beiden Indices μ oder ν die Primzahl λ an Gröfse übertrifft. Denn setzt man $h_\mu = 1-\eta^\mu - l\eta^{\lambda+1}$, $h_\nu = 1-\eta^\nu - l'\eta^{\lambda+1}$, so wird $\varepsilon_{\mu, \nu} = (h_\mu, h_\nu)$. Ist nun $\mu > \lambda$, so wird $h_\mu \equiv 1 \pmod{\eta^{\lambda+1}}$, also nach Satz I., $\varepsilon_{\mu, \nu} = (1, h_\nu) = 1$, und ist $\nu > \lambda$, so wird $h_\nu \equiv 1 \pmod{\eta^{\lambda+1}}$, also nach Satz I., $\varepsilon_{\mu, \nu} = (h_\mu, 1) = 1$.

Die Formel (5.) vereinfacht sich, wenn man die Symbole von der Form $\left(\frac{\eta}{1-\eta^\mu} \right)$ einer genauern Betrachtung unterwirft. Ein solches Symbol

*) Der gemeinschaftliche Factor $1-\eta$ zählt nicht mit, weil er der Einheit ζ gleich ist, da aus $\eta = 1-\zeta$, $\zeta = 1-\eta$ folgt.

wird stets = 1; mit Ausnahme des einzigen speciellen Falles $\mu = \lambda$. Denn für $\mu > \lambda$ hat man, wenn wieder $1 - \eta^\mu = h_\mu$ gesetzt wird, $h_\mu \equiv 1 \pmod{\eta^{\lambda+1}}$, also nach Satz II. $\left(\frac{\eta}{h_\mu}\right) = \left(\frac{\eta}{1}\right) = 1$. Ferner ist im Allgemeinen $\eta^\mu \equiv 1 \pmod{h_\mu}$, also $\left(\frac{\eta^\mu}{h_\mu}\right) = \left(\frac{\eta}{h_\mu}\right)^\mu = 1$; woraus leicht folgt, dafs auch $\left(\frac{\eta}{h_\mu}\right) = 1$, aufser wenn $\mu \equiv 0 \pmod{\lambda}$. Setzt man das noch unbekannte Symbol $\left(\frac{\eta}{1-\eta^\lambda}\right) = \delta$, so wird aus (5.) $\varepsilon_{\mu,\nu} = \varepsilon_{\mu,\mu+\nu} \cdot \varepsilon_{\mu+\nu,\nu}$, wenn $\mu + \nu \leq \lambda$, und $\varepsilon_{\mu,\nu} = \varepsilon_{\mu,\mu+\nu} \cdot \varepsilon_{\mu+\nu,\nu} \cdot \delta^\nu$, wenn $\mu + \nu = \lambda$ ist. Setzt man ferner allgemein $\varepsilon_{\mu,\nu} = \delta^{x_{\mu,\nu}}$, so ergeben sich folgende Formeln zur Bildung der Exponenten x :

$$(7.) \quad \begin{cases} 1^\circ. & x_{\mu,\nu} \equiv x_{\mu,\mu+\nu} + x_{\mu+\nu,\nu} \pmod{\lambda}, \text{ wenn } \mu + \nu < \lambda, \\ 2^\circ. & x_{\mu,\nu} \equiv 0, \text{ wenn } \mu + \nu > \lambda, \\ 3^\circ. & x_{\mu,\nu} \equiv \nu, \text{ wenn } \mu + \nu = \lambda. \end{cases}$$

Nach diesen Formeln können die Werthe der Zahlen $x_{\mu,\nu}$ sehr leicht und zwar auf doppelte Weise berechnet werden, indem man entweder jedes zu berechnende *individuelle* x nach 1°. durch neue x mit wachsenden Indices so lange ersetzt, bis man zu lauter solchen gelangt, welche durch 2°. resp. 3°. bestimmt sind; oder auch indem man, was für *tabellarische* Zusammenstellung vorzuziehen ist, auf dem umgekehrten Wege, von denjenigen Combinationen μ, ν anfangend, für welche $\mu + \nu$ am grössten ist, zu solchen zurückgeht, denen nach und nach immer kleinere Werthe der Summe $\mu + \nu$ entsprechen. In Betreff ausführlicher Untersuchung dieser merkwürdigen Zahlen mufs ich wegen Mangel an Raum auf eine der Akademie neuerdings vorgelegte Mittheilung verweisen; auch mufs ich mich jedes Beispiels enthalten.

Die noch nöthige Bestimmung des Symbols $\delta = \left(\frac{\eta}{1-\eta^\lambda}\right)$ ergibt sich durch Betrachtung einer speciellen Combination μ, ν , für welche $\varepsilon_{\mu,\nu}$ *a priori* und unabhängig von den hier angestellten Untersuchungen ermittelt und auch das zugehörige $x_{\mu,\nu}$ leicht angegeben werden kann, in ähnlicher Weise, wie man in der Theorie der Functionen die willkürlichen Constanten zu bestimmen pflegt. Am Besten eignet sich hierzu die Combination $\mu = 1, \nu = \lambda - 1$; denn da für diese $\mu + \nu = \lambda$ ist, so wird nach 3°. in (7.) $x_{1,\lambda-1} \equiv \lambda - 1 \equiv -1 \pmod{\lambda}$, also $\varepsilon_{1,\lambda-1} = \delta^{-1}$, $\delta = \varepsilon_{1,\lambda-1}^{-1}$; ferner wird $\varepsilon_{1,\lambda-1} = (1 - \eta, 1 - \eta^{\lambda-1}) = (\zeta, 1 - \eta^{\lambda-1}) = \left(\frac{\zeta}{1 - \eta^{\lambda-1}}\right) : \left(\frac{1 - \eta^{\lambda-1}}{\zeta}\right) = \left(\frac{\zeta}{1 - \eta^{\lambda-1}}\right)$. Bezeichnet man allgemein das Product der $\lambda - 1$ Werthe der complexen Zahl A durch $\mathfrak{N}(A)$

$= 1 + \lambda \mathcal{A}(\mathcal{A})$, so wird $\left(\frac{\zeta}{\mathcal{A}}\right) = \zeta^{\mathcal{A}(\mathcal{A})}$, also speciell $\varepsilon_{1,\lambda-1} = \zeta^{\mathcal{A}(1-\eta^{\lambda-1})}$. Um den Exponenten dieser Potenz von ζ zu finden, hat man nur $\mathfrak{N}(1-\eta^{\lambda-1}) = (1-(1-\zeta)^{\lambda-1})(1-(1-\zeta^2)^{\lambda-1}) \dots (1-(1-\zeta^{\lambda-1})^{\lambda-1})$ in Bezug auf mod. λ^2 zu bestimmen. Da in diesem Producte $\prod_{\mu=1}^{\mu=\lambda-1} \{1-(1-\zeta^\mu)^{\lambda-1}\}$ das zweite Glied $(1-\zeta^\mu)^{\lambda-1}$ jedes Factors durch λ theilbar ist, so wird das Product $\equiv 1 - \sum_{\mu=1}^{\mu=\lambda-1} (1-\zeta^\mu)^{\lambda-1} \pmod{\lambda^2}$. Entwickelt man $(1-\zeta^\mu)^{\lambda-1}$ nach dem binomischen Satze und überträgt die Summation nach μ auf die einzelnen Glieder dieser Entwicklung, so erhält man $\mathfrak{N}(1-\eta^{\lambda-1}) \equiv 1 - (\lambda-1) + (\lambda-1)\sum \zeta^\mu - \frac{1}{2}(\lambda-1)(\lambda-2)\sum \zeta^{2\mu} + \dots - \sum \zeta^{(\lambda-1)\mu} \pmod{\lambda^2}$. Die sämtlichen hier vorkommenden Summen nehmen den Werth -1 an, daher wird $\mathfrak{N}(1-\eta^{\lambda-1}) \equiv 1 - \lambda + \{1 - (\lambda-1) + \frac{1}{2}(\lambda-1)(\lambda-2) - \dots + 1\} \pmod{\lambda^2} = 1 - \lambda + (1-1)^{\lambda-1} = 1 - \lambda$, mithin endlich $\mathcal{A}(1-\eta^{\lambda-1}) \equiv -1 \pmod{\lambda}$, $\varepsilon_{1,\lambda-1} = \zeta^{-1}$, und $\delta = \varepsilon_{1,\lambda-1}^{-1} = \zeta$. Vereinigen wir dieses Resultat mit der frühern Bemerkung über die Symbole $\left(\frac{\eta}{1-\eta^\mu}\right)$ in der Formel

$$(8.) \quad \left(\frac{\eta}{1-\eta^\mu}\right) = 1 \text{ oder } = \zeta,$$

je nachdem $\mu \leq \lambda$ oder $\mu = \lambda$.

§. 3.

Nach Einsetzung des sehr einfachen Werthes $\delta = \zeta$ und mit Benutzung der Zahlen \varkappa wird $\varepsilon_{\mu,\nu} = \zeta^{\varkappa_{\mu,\nu}}$; daher läßt sich die Formel (3.) folgendermaßen darstellen:

$$(9.) \quad \varphi(\mathbf{A}, \mathbf{B}) = \sum \varkappa_{\mu,\nu} \alpha_\mu \beta_\nu = \varkappa_{1,1} \alpha_1 \beta_1 + \varkappa_{1,2} \alpha_1 \beta_2 + \varkappa_{2,1} \alpha_2 \beta_1 + \dots,$$

und die Formel (4.) wird wegen (8.) ganz einfach

$$(10.) \quad \left(\frac{\eta}{\mathbf{A}}\right) = \zeta^{\alpha_\lambda}.$$

Wegen der verschwindenden \varkappa nach (7.) 2°. fallen aus der Summe rechts in (9.) alle diejenigen Glieder weg, für welche $\mu + \nu > \lambda$ ist; namentlich fehlen alle Glieder, welche α_λ oder β_λ enthalten. Man kann deshalb die Congruenzen (1.) und (2.), welche zu Bestimmung der α und β dienen, durch folgende aus ihnen hervorgehenden einfacheren

$$(11.) \quad \begin{cases} \mathbf{A} \equiv a^\lambda (1-\eta)^{\alpha_1} (1-\eta^2)^{\alpha_2} (1-\eta^3)^{\alpha_3} \dots (1-\eta^{\lambda-1})^{\alpha_{\lambda-1}} \\ \mathbf{B} \equiv b^\lambda (1-\eta)^{\beta_1} (1-\eta^2)^{\beta_2} (1-\eta^3)^{\beta_3} \dots (1-\eta^{\lambda-1})^{\beta_{\lambda-1}} \end{cases} \pmod{\eta^\lambda}$$

ersetzen, und die Kenntnifs von α_λ ist nur zur Aufstellung des Werthes von

$\left(\frac{\eta}{A}\right)$ nach (10.) erforderlich. Eine noch gröfsere Vereinfachung dieser Congruenzen ist gestattet, wenn man A und B einer Beschränkung unterwirft, die sich immer durch Multiplication mit einer Potenz von ζ erreichen läfst, derjenigen nämlich, dafs die Exponenten von $1 - \eta = \zeta$, d. h. α_1 und β_1 verschwinden (durch λ theilbar sind). Unter dieser Voraussetzung fallen auch noch die Glieder mit $\alpha_{\lambda-1}$ und $\beta_{\lambda-1}$ aus (9.) weg; und da diese beiden Exponenten sich als überflüssig erweisen, so genügt es, die Congruenzen blofs in Bezug auf mod. $\eta^{\lambda-1}$, oder, was auf Dasselbe hinauskommt, auf mod. λ aufzufassen, und da noch aufserdem $a^\lambda \equiv a$, $b^\lambda \equiv b \pmod{\lambda}$ ist, blofs

$$(12.) \quad \begin{cases} A \equiv a(1-\eta^2)^{\alpha_2}(1-\eta^3)^{\alpha_3} \dots (1-\eta^{\lambda-2})^{\alpha_{\lambda-2}} \\ B \equiv b(1-\eta^2)^{\beta_2}(1-\eta^3)^{\beta_3} \dots (1-\eta^{\lambda-2})^{\beta_{\lambda-2}} \end{cases} \pmod{\lambda}$$

zu schreiben. In diesem Falle sind A und B reellen Zahlen congruent (mod. η^2) und sollen als *primär* bezeichnet werden.

Ich will jetzt zeigen, wie die Exponenten α , β , welche in (9.) vorkommen, auch durch eine eigenthümliche Art logarithmischer Entwicklungen gefunden, und dadurch jene Congruenzen ganz vermieden werden können; doch beschränke ich mich, um unnöthige Complicationen zu vermeiden, auf primäre Werthe der Zahlen A, B . Da in der irreductibeln Gleichung, welcher η genügt, nämlich $\frac{1-\zeta^\lambda}{1-\zeta} = \frac{1-(1-\eta)^\lambda}{\eta} = \lambda - \frac{1}{2}\lambda(\lambda-1)\eta + \dots - \lambda\eta^{\lambda-2} + \eta^{\lambda-1} = 0$, mit Ausnahme des höchsten Gliedes $\eta^{\lambda-1}$ alle Coëfficienten mit λ aufgehen, so werden, wenn man beide Seiten der Congruenzen (12.) nach steigenden Potenzen von η entwickelt und diese Entwicklungen vor den Gliedern mit $\eta^{\lambda-1}$ abbricht, die entsprechenden Coëfficienten sich nur um Vielfache von λ unterscheiden. Dasselbe wird gelten, wenn man vor der Entwicklung auf beiden Seiten die Logarithmen nimmt. Schreibt man daher A und B zunächst als Functionen von η in der Form

$$A = A(\zeta) = A(1-\eta) = A(1) - A'(1)\eta + \frac{1}{2}A''(1)\eta^2 - \text{etc.}$$

$$B = B(\zeta) = B(1-\eta) = B(1) - B'(1)\eta + \frac{1}{2}B''(1)\eta^2 - \text{etc.},$$

wo das primäre Verhalten durch die Bedingungen $A'(1) = B'(1) = 0$ oder wenigstens $A'(1) \equiv B'(1) \equiv 0 \pmod{\lambda}$ ausgesprochen wird, und entwickelt dann, indem man η für einen Augenblick als unbestimmte Variable ansieht, $\log A(1-\eta)$ und $\log B(1-\eta)$ in folgender Weise:

$$(13.) \quad \begin{cases} \log A = \log A(1) + \alpha_1 \log(1-\eta) + \alpha_2 \log(1-\eta^2) + \alpha_3 \log(1-\eta^3) + \dots, \\ \log B = \log B(1) + \beta_1 \log(1-\eta) + \beta_2 \log(1-\eta^2) + \beta_3 \log(1-\eta^3) + \dots, \end{cases}$$

was immer nur auf eine Art möglich ist und wo α_1, β_1 mit $A'(1)$ resp. $B'(1)$ zugleich verschwinden: so werden die Coëfficienten, wenn man nur bis $\alpha_{\lambda-2}$ resp. $\beta_{\lambda-2}$ fortgeht, genau die oben durch dieselben Buchstaben bezeichneten Zahlen, oder sie werden ihnen wenigstens congruent, wenn man etwa vorkommende Nenner mit Hülfe des mod. λ beseitigt, und es wird daher

$$(14.) \quad \varphi(A, B) = \varkappa_{2,2} \alpha_2 \beta_2 + \varkappa_{2,3} \alpha_2 \beta_3 + \varkappa_{3,2} \alpha_3 \beta_2 + \text{etc.},$$

wo die Reihe wegen der verschwindenden \varkappa von selbst abbricht und die Gröfsen α, β aus (13.) zu ziehen sind.

Die Coëfficienten der logarithmischen Entwicklungen in (13.), welche nur bis zu dem Gliede mit $\log(1-\eta^{\lambda-1})$ excl. fortgesetzt werden dürfen, sind lineare Verbindungen der in den gewöhnlichen Entwicklungen von $\log A(1-\eta)$ resp. $\log B(1-\eta)$ nach steigenden Potenzen von η vorkommenden Coëfficienten. Denn setzt man, immer noch η als unbestimmte Variable betrachtend,

$$\log A(1-\eta) = \log A(1) + a_1 \eta + a_2 \eta^2 + a_3 \eta^3 + \dots$$

$$\log B(1-\eta) = \log B(1) + b_1 \eta + b_2 \eta^2 + b_3 \eta^3 + \dots,$$

so darf man nur noch aus den Formeln

$$\log(1-\eta) = -\eta - \frac{1}{2}\eta^2 - \frac{1}{3}\eta^3 - \text{etc.}, \quad \log(1-\eta^2) = -\eta^2 - \frac{1}{2}\eta^4 - \frac{1}{3}\eta^6 - \text{etc.},$$

allgemein

$$\log(1-\eta^\mu) = -\eta^\mu - \frac{1}{2}\eta^{2\mu} - \frac{1}{3}\eta^{3\mu} - \text{etc.},$$

umgekehrt die Potenzen von η durch die Gröfsen $\log(1-\eta), \log(1-\eta^2)$ u. s. w. linear ausdrücken, um die Entwicklungen von der Form (13.) zu erhalten. Eine derartige Reihen-Umkehrung ist ein bekanntes, wenn ich nicht irre zuerst von *Moebius* im 9ten Bande dieses Journals S. 105 ff. behandeltes Problem. Es findet sich allgemein

$$z = -\log(1-z) + \frac{1}{2}\log(1-z^2) + \frac{1}{3}\log(1-z^3) + \frac{1}{4}\log(1-z^4) - \frac{1}{5}\log(1-z^5) + \text{etc.},$$

wo rechts nur diejenigen Potenzen von z vorkommen, deren Exponent keinen quadratischen Theiler enthält, und das Vorzeichen $+$ oder $-$ gilt, je nachdem die Anzahl der in diesem Exponenten aufgehenden verschiedenen Primfactoren ungerade oder gerade ist. Hiernach wird $\alpha_1 = -a_1$, $\alpha_2 = -a_2 + \frac{1}{2}a_1$, $\alpha_3 = -a_3 + \frac{1}{3}a_1$, u. s. w., $\alpha_6 = -a_6 + \frac{1}{2}a_3 + \frac{1}{3}a_2$, u. s. w. Für den allgemeinen Ausdruck von α_μ durch die Coëfficienten a ergeben sich die Vorzeichen und Zahlenfactoren aus dem Anblick des entwickelten Products $-(1-\frac{1}{p})(1-\frac{1}{q})\dots$, wenn p, q, \dots die verschiedenen Primfactoren von μ sind; auf dieselbe Weise werden die β durch die b ausgedrückt.

Der Exponent $\varphi(A, B)$ des Umkehrungsfactors $(A, B) = \left(\frac{A}{B}\right) : \left(\frac{B}{A}\right)$ wird also ein Ausdruck, der sowohl aus den Coëfficienten der Entwicklung von $\log A = \log A(1-\eta)$ nach steigenden Potenzen von η , als auch aus denen der ähnlichen Entwicklung von $\log B$ linear und aus beiden Arten von Coëfficienten quadratisch zusammengesetzt ist; wobei man übrigens die Entwicklungen nur bis $\eta^{\lambda-1}$ excl. fortzusetzen hat. Die Zahlenfactoren jenes Ausdrucks können entweder aus dem Vorhergehenden zusammengesetzt, oder auch nach irgend einer Interpolations-Methode direct ermittelt werden. Setzt man $\varphi(A, B) = \sum k_{\mu, \nu} a_{\mu} b_{\nu}$, so darf man, um $k_{\sigma, \tau}$ zu finden, nur zwei solche complexe Zahlen als specielle Werthe von A und B aufsuchen, für welche a_{μ} und b_{ν} , mit Ausnahme der stehenden Combination $\mu = \sigma, \nu = \tau$, stets verschwinden. Solche Zahlen sind

$$1 + \eta^{\sigma} + \frac{1}{2}\eta^{2\sigma} + \frac{\eta^{3\sigma}}{2 \cdot 3} + \dots + l\eta^{\lambda-1} = u_{\sigma},$$

$$1 + \eta^{\tau} + \frac{1}{2}\eta^{2\tau} + \frac{\eta^{3\tau}}{2 \cdot 3} + \dots + l'\eta^{\lambda-1} = u_{\tau},$$

wo die Reihen abzubrechen sind, sobald die Exponenten die Zahl $\lambda - 2$ übersteigen, und wo die beliebigen complexen Zahlen l und l' nur dazu dienen, um gemeinschaftliche Factoren zwischen u_{σ} und u_{τ} zu vermeiden. Mittels dieser Zahlen u wird $k_{\mu, \nu}$ aus der Gleichung

$$\left(\frac{u_{\mu}}{u_{\nu}}\right) = \zeta^{k_{\mu, \nu}} \left(\frac{u_{\nu}}{u_{\mu}}\right) \text{ oder } k_{\mu, \nu} = \varphi(u_{\mu}, u_{\nu})$$

bestimmt.

Es wird nicht überflüssig sein, nochmals zu erinnern, dafs die letzten Resultate in dieser Einfachheit nur unter der Voraussetzung primärer Werthe von A, B gelten. Eine genauere Betrachtung zeigt, dafs ohne diese Voraussetzung die logarithmischen Entwicklungen um ein Glied weiter fortgesetzt werden müssen und dafs dann zu dem Ausdrücke für $\varphi(A, B)$ in (14.) aufser den Gliedern

$$\alpha_{1,1}\alpha_1\beta_1 + \alpha_{1,2}\alpha_1\beta_2 + \alpha_{2,1}\alpha_2\beta_1 + \alpha_{1,3}\alpha_1\beta_3 + \alpha_{3,1}\alpha_3\beta_1 + \text{etc.},$$

noch die folgenden beiden

$$\alpha_1 A B(1) - \beta_1 A A(1) = \frac{1}{\lambda} \{ \alpha_1 (B(1)^{\lambda-1} - 1) - \beta_1 (A(1)^{\lambda-1} - 1) \}$$

hinzutreten.

Für den speciellen Fall, wenn B einer reellen ganzen Zahl $= q = B(1)$ gleich ist, reducirt sich die ganze Entwicklung von $\log B$ auf das erste Glied

und es wird geradezu

$$\left(\frac{A}{q}\right) = \left(\frac{q}{A}\right),$$

wenn A primär, nämlich $A'(1) = 0$ angenommen wird; ohne diese Voraussetzung wird

$$\left(\frac{A}{q}\right) = \zeta^{\alpha_1 \mathcal{A}(q)} \left(\frac{q}{A}\right),$$

wo $\alpha_1 = A'(1)$ und $\mathcal{A}(q)$ die durch die Congruenz $q^{\lambda-1} \equiv 1 + \lambda \mathcal{A}(q) \pmod{\lambda^2}$ definirte Function ist. Diesen speciellen Fall habe ich schon vor langer Zeit mittels einer gewissen Erweiterung der Principien der Kreistheilung streng erwiesen.

Die unmittelbare Reciprocität $\left(\frac{A}{B}\right) = \left(\frac{B}{A}\right)$ findet allgemein dann Statt, wenn $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{\frac{1}{2}(\lambda-1)}$ und ebenso $\beta_1, \beta_2, \beta_3, \dots, \beta_{\frac{1}{2}(\lambda-1)}$ verschwinden; denn da die Factoren α ihrerseits verschwinden, wenn μ und ν beide $> \frac{1}{2}(\lambda-1)$ sind, so reducirt sich in diesem Falle der ganze Werth von $\varphi(A, B)$ auf Null. Es geschieht dies, wenn in den Entwicklungen von $\log A$ und $\log B$ alle Potenzen von η bis incl. $\eta^{\frac{1}{2}(\lambda-1)}$ fehlen; wozu es wiederum hinreicht, daß $A'(1), A''(1), \dots, A^{\frac{1}{2}(\lambda-1)}(1)$, so wie $B'(1), B''(1), \dots, B^{\frac{1}{2}(\lambda-1)}(1)$ verschwinden. Ob es aber immer möglich sein wird, diesen Bedingungen durch Multiplication der Zahlen mit complexen Einheiten zu entsprechen, muß ferneren Untersuchungen vorbehalten bleiben. Bezeichnet man durch e_1, e_2, e_3, \dots ein System von Fundamental-Einheiten, deren Anzahl nach *Dirichlet* $\frac{1}{2}(\lambda-3)$ beträgt, so wäre zu zeigen, daß die aus den Coëfficienten von $\eta, \eta^2, \dots, \eta^{\frac{1}{2}(\lambda-1)}$ in den Entwicklungen von $\log \zeta = \log(1-\eta), \log e_1, \log e_2, \dots, \log e_{\frac{1}{2}(\lambda-3)}$ gebildete Determinante niemals $\equiv 0 \pmod{\lambda}$ werden kann. Wie dem auch sein mag, so wird zur Bestimmung der als Factor hinzutretenden Einheit immer auf die hier gegebene Theorie zurückzugehen sein; auch ist zu erwägen, daß bei einer solchen Specialisirung der zu vergleichenden Zahlen neue Ergänzungssätze, betreffend den Character der complexen Einheiten selbst, hinzutreten müssen.

Man bemerke noch den ebenfalls aus diesen Principien hervorgehenden merkwürdigen Satz, daß man $\mathcal{A}(A)$ in $\mathfrak{N}(A) \equiv 1 + \lambda \mathcal{A}(A) \pmod{\lambda^2}$ erhält, wenn man $\log A$ nach steigenden Potenzen von η entwickelt, in dieser Entwicklung die Glieder, deren Exponent $\geq \lambda$ ist, wegläßt, sodann $\eta = 1$ setzt und das erste Glied $\log A(1)$ durch $\mathcal{A}(1)$ ersetzt.

§. 4.

Zum Schlusse füge ich noch einige Worte über die Definition der Symbole $\left(\frac{A}{B}\right)$ hinzu. Die Schwierigkeiten, welchen eine solche Definition auf den ersten Blick zu unterliegen scheint, können sowohl auf anderen Wegen, als auch durch Benutzung der von *Kummer* eingeführten idealen Primfactoren beseitigt werden. Ist p eine von λ verschiedene gewöhnliche ungerade Primzahl, μ der kleinste Exponent, der $p^\mu \equiv 1 \pmod{\lambda}$ macht, und setzt man $p^\mu - 1 = \lambda q$, bezeichnet ferner durch $\psi(\zeta)$ irgend eine ganze ganzzahlige Function einer primitiven λ ten Wurzel der Einheit ζ , so ist $\psi(\zeta)^{p^\mu} = \psi(\zeta)^{\lambda q + 1} \equiv \psi(\zeta) \pmod{p}$; wovon man sich leicht durch die polynomische Entwicklung der Potenz $\psi(\zeta)^{p^\mu}$ überzeugt. Die durch p theilbare Differenz $\psi(\zeta)^{\lambda q + 1} - \psi(\zeta)$ läßt sich in das Product aus $\psi(\zeta)$ und λ andern Factoren von der Form $\psi(\zeta)^q - \zeta^r$ zerlegen, in denen r die Zahlen $0, 1, 2, \dots, \lambda - 1$ bedeutet. Im Allgemeinen wird sich p nicht auf diese $\lambda + 1$ Factoren vertheilen lassen: führt man aber ideale Primfactoren von p ein, deren Anzahl nach *Kummer* $\frac{\lambda - 1}{\mu}$ beträgt, so wird jeder dieser Primtheiler in einem und nur in einem der obigen $\lambda + 1$ Factoren aufgehen. Ist $\bar{\omega}$ ein idealer Primfactor von p , welcher nicht in $\psi(\zeta)$ enthalten ist, so bezeichne ich diejenige ganze bestimmte Potenz von ζ , für welche die Congruenz $\psi(\zeta)^q \equiv \zeta^r \pmod{\bar{\omega}}$ erfüllt wird, durch $\left(\frac{\psi(\zeta)}{\bar{\omega}}\right) = \zeta^r$. Sind $\bar{\omega}, \bar{\omega}', \bar{\omega}'', \dots$ die sämtlichen idealen Primfactoren der beliebigen complexen Zahl $\chi(\zeta)$, welche mit $\psi(\zeta)$ keinen (auch keinen idealen) Factor gemein hat, so bezeichne ich ferner durch $\left(\frac{\psi(\zeta)}{\chi(\zeta)}\right)$ das Product $\left(\frac{\psi(\zeta)}{\bar{\omega}}\right)\left(\frac{\psi(\zeta)}{\bar{\omega}'}\right)\left(\frac{\psi(\zeta)}{\bar{\omega}''}\right) \dots = \left(\frac{\psi(\zeta)}{\chi(\zeta)}\right)$. Das Symbol $\left(\frac{A}{B}\right)$ hat dann eine ganz bestimmte Bedeutung, B mag eine wirkliche oder eine ideale complexe Zahl sein; der Zähler A muß aber eine wirkliche complexe Zahl sein. Übrigens muß noch B zu λ relative Primzahl sein, darf also nicht durch $1 - \zeta = \eta$ theilbar sein. Bei der Aufstellung des Reciprocitätsgesetzes zur Vergleichung von $\left(\frac{A}{B}\right)$ mit $\left(\frac{B}{A}\right)$ werden A und B beide als *wirkliche* complexe Zahlen angenommen und die Betrachtung der idealen Primfactoren von B resp. A ist nur bei der *Definition* dieser Zeichen erforderlich; wenigstens vortheilhaft. Bei einer andern Gelegenheit werde ich zeigen, wie diese Symbole auch ohne Einführung idealer Primfactoren sehr einfach defnirt werden können.

Die Betrachtungen dieser Abhandlung, die sich leicht auf beliebige zusammengesetzte Werthe von λ ausdehnen lassen, gründen sich auf eine unbewiesene Voraussetzung, deren Wahrscheinlichkeit aber der Gewissheit deshalb sehr nahe steht, weil man immer zu demselben Resultate kommt, man mag den Werth des Exponenten σ oben in η^σ (§. 1.) bei dieser Voraussetzung *so groß* annehmen, als man will. Da jedoch mein Streben stets auf Erforschung strenger Beweise gerichtet war, so legte ich weniger Werth auf diese Untersuchungen, bis ich neuerdings erfuhr, dafs auch andere Mathematiker sich mit der Auffindung der höhern Reciprocitätsgesetze auf dem Wege der Induction beschäftigen. Dies besonders veranlafste mich zur Publication vorliegender Arbeit, um auch meinerseits Gelegenheit zu einigen Bemerkungen über einen Gegenstand zu finden, dem ich seit langer Zeit fast ausschliesslich alle meine Kräfte widme. Übrigens ist nicht zu verkennen, wie sehr der hier eingeschlagene, fast ganz theoretische Weg sich von einer gewöhnlichen Induction unterscheidet, bei welcher man für specielle Werthe von λ etwa die einfachsten complexen Zahlen bis zu einer gewissen Grenze mit einander vergleicht, um durch numerische Prüfung einer Anzahl von Fällen die Reciprocitätssätze herauszubringen.

Schliesslich in einigen Worten zusammengefasst, was durch die Betrachtungen dieser Abhandlungen geleistet ist, enthält dieselbe eine sichere Methode, nach welcher, unter der Voraussetzung, dafs überhaupt irgend eine, wenn auch noch so hohe Potenz von η existirt, um deren Vielfache A und B in dem Verhältnisse $\left(\frac{A}{B}\right) : \left(\frac{B}{A}\right)$ geändert werden dürfen, der niedrigste dieser Bedingung genügende Exponent von η aufgefunden und mit Hülfe einer solchen Reduction sodann das Reciprocitätsgesetz für alle Fälle vollständig aufgestellt werden kann.

Da nach bereits vollendeter Abfassung dieser Arbeit wider Erwarten noch einiger Raum bleibt, so benutze ich denselben, um ein Paar Bemerkungen zu dem Vorhergehenden hinzuzufügen.

1) Es wurde oben im Vorbeigehen angedeutet, dafs $1 - \eta^\mu$ mit $1 - \eta^\nu$ keinen gemeinschaftlichen Theiler haben kann, wenn μ zu ν relative Primzahl ist. Ich will hier beweisen, dafs jene beiden complexen Zahlen den *größten* gemeinschaftlichen Theiler $1 - \eta^\theta$ haben, wenn θ den größten gemeinschaft-

lichen Theiler von μ und ν bezeichnet. Setzt man allgemein $1 - \eta^n = f(n)$, so folgt aus der oben bereits zum Grunde gelegten identischen Gleichung $f(\mu + \nu) = \eta^\nu f(\mu) + f(\nu)$, daß jeder gemeinschaftliche Theiler von $f(\mu + \nu)$ und $f(\mu)$ auch in $f(\nu)$ aufgeht. Setzt man $\mu + \nu = \sigma$, so wird $\nu = \sigma - \mu$: es geht also jeder gemeinschaftliche Theiler von $f(\sigma)$ und $f(\mu)$ auch in $f(\sigma - \mu)$ auf, wenn $\sigma > \mu$ ist. Aus demselben Grunde geht ein solcher gemeinschaftlicher Theiler, da er in $f(\sigma - \mu)$ und $f(\mu)$ enthalten ist, auch in $f(\sigma - 2\mu)$ auf, und allgemein in jedem Gliede der Reihe

$$f(\sigma - \mu), f(\sigma - 2\mu), f(\sigma - 3\mu), \dots,$$

welche man so weit fortsetzen kann, als die Zahlen unter dem Functionszeichen f positiv bleiben. Es geht also namentlich, wenn man erst beim letzten Gliede einer solchen Zahlenreihe stehen bleibt, der größte gemeinschaftliche Theiler von $f(a)$ und $f(b)$, wo $a > b$ ist, in $f(c)$ auf, wo c den kleinsten positiven Rest von $a \pmod{b}$ bedeutet. Bildet man die bei der Operation der Aufsuchung des größten gemeinschaftlichen Theilers zwischen a und b sich ergebenden Reste c, d, e u. s. w. und nennt den vorletzten Rest, welcher zugleich der letzte Divisor ist, h , so folgt aus dem eben Bewiesenen, daß jeder gemeinschaftliche Theiler von $f(a)$ und $f(b)$ in $f(c)$, also auch in $f(d)$, also auch in $f(e)$ u. s. w., endlich in $f(h)$ aufgeht, während h der größte gemeinschaftliche Theiler von a und b ist. Andererseits geht $f(h)$ wirklich in $f(a)$ und $f(b)$ auf, da h in den Exponenten a und b aufgeht: also ist $f(h)$ der *größte* gemeinschaftliche Theiler von $f(a)$ und $f(b)$. Dieser Beweis bleibt gültig, welche Art von complexer Zahl auch η sein mag.

2) Das in einer Notiz im Monatsberichte der Berliner Akademie (Märzheft 1850) bewiesene independente Gesetz der Zahlen $x_{\mu,\nu}$ (§. 2.), die mit den dortigen $f(\mu, \nu) \pmod{\lambda}$ übereinstimmen, ist folgendes. Bezeichnet man durch μ^0, ν^0 die kleinsten positiven Lösungen der unbestimmten Gleichung

$$\nu\mu^0 - \mu\nu^0 = 1$$

und durch r den Inbegriff aller zwischen den Grenzen $\frac{\nu^0}{\nu}\lambda$ und $\frac{\mu^0}{\mu}\lambda$ liegenden ganzen Zahlen, so wird $x_{\mu,\nu} \equiv \sum \frac{1}{r} \pmod{\lambda}$, wo die Nenner mittelst $\pmod{\lambda}$ wegzuschaffen sind, und die Summation sich auf die eben definirten Werthe von r bezieht; z. B. $x_{1,2} \equiv \sum_{r=\frac{1}{2}(\lambda+1)}^{r=\lambda-1} \frac{1}{r} \pmod{\lambda}$.