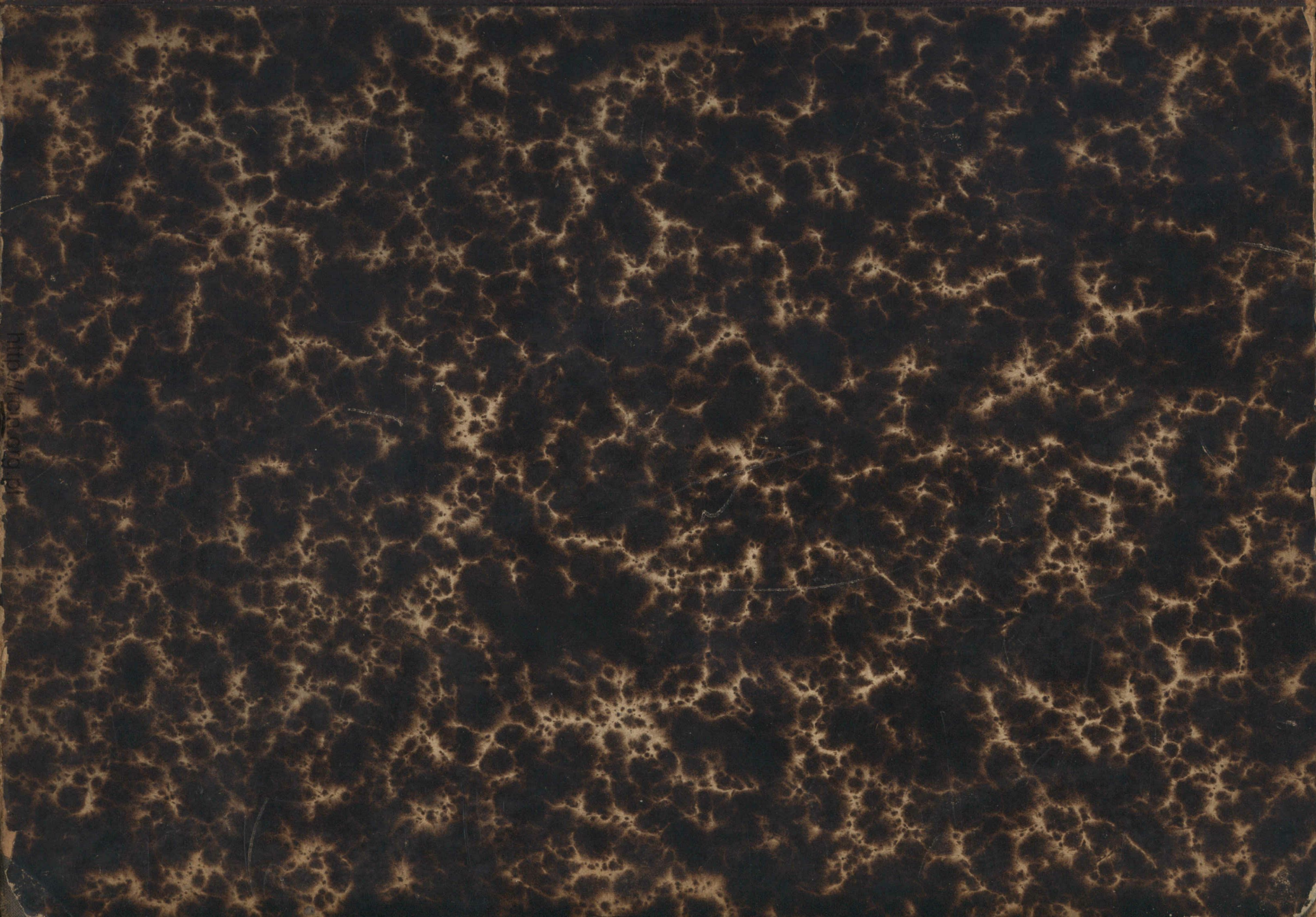

http://rcin.org.pl

49

http://rcin.org.pl

http://rcin.org.pl

839

Theorie der idealen Primfaktoren der complexen Zahlen,

welche

aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind,
wenn n eine zusammengesetzte Zahl ist.

Von

E. E. KUMMER.

N 49.
Dział: I22b.

Aus den Abhandlungen der Königl. Akademie der Wissenschaften zu Berlin 1856.

GABINET MATEMATYCZNY
Towarzystwa Naukowego Warszawskiego

Berlin.
Gedruckt in der Buchdruckerei der Königl. Akademie
der Wissenschaften.
1857.

In Commission bei F. Dümmler's Verlags-Buchhandlung.

GABINET MATEMATYCZNY
TOWARZYSTWA NAUKOWEGO WARSZAWSKIEGO

http://rcin.org.pl

Gelesen in der Akademie der Wissenschaften am 18. December 1856. Die Seitenzahl bezeichnet die laufende Pagina des Jahrgangs 1856 in den Abhandlungen der mathematischen Klasse der Königl. Akademie der Wissenschaften.

http://rcin.org.pl

In mehreren früheren Abhandlungen habe ich die Theorie der aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen für den Fall, dafs λ eine Primzahl ist, vollständig behandelt und deren Anwendung auf die allgemeinen Reciprocitätsgesetze, auf den letzten Fermat'schen Satz und auf die Theorie der Kreistheilung gezeigt. Seitdem hat die Grundidee dieser Theorie, nämlich die Zerlegung der complexen Zahlen in ihre wahren idealen Primfaktoren auch in der Algebra ihre Anwendung gefunden, da z. B. das von Herrn Kronecker gefundene, der Akademie unter dem 14. April d. J. mitgetheilte Resultat: dafs die Wurzeln jeder Abel'schen Gleichung mit ganzzahligen Coefficienten nur rationale Funktionen von Wurzeln der Einheit sind, von demselben nur mit Hülfe der idealen Primfaktoren gefunden und bewiesen worden ist. Damit nun die Anwendungen dieser Theorie nicht nur auf die Fälle beschränkt bleiben, wo es sich um Einheitswurzeln handelt, deren Exponent eine Primzahl ist, habe ich dieselbe in dem Folgenden auf die Einheitswurzeln mit beliebig zusammengesetzten Wurzelexponenten ausgedehnt. Die hauptsächlich in den Unterscheidungen vieler einzelnen Fälle bestehenden Weitläufigkeiten, welche die Betrachtung zusammengesetzter Zahlen in der Zahlentheorie gewöhnlich mit sich führt, habe ich durch zweckmäfsige Wahl der Methoden überall vermeiden können, und da in dieser allgemeinen Untersuchung die Beweise der Sätze der Natur der Sache nach nur auf die in allen Fällen bleibenden und daher wesentlichen Eigenschaften gegründet werden konnten, so ist es mir gelungen, dieselbe sogar einfacher darzustellen als die früher behandelte speciellere Theorie.

http://rcin.org.pl

§. 1.

Die sämmtlichen primitiven Wurzeln der Gleichung

$$\omega^n = 1,$$

in welcher n eine beliebig zusammengesetzte Zahl bedeutet, deren Anzahl bekanntlich gleich der Anzahl aller Zahlen ist, welche kleiner als n und relative Primzahlen zu n sind, also nach der von Gauſs eingeführten Bezeichnung gleich $\phi(n)$, sind die Wurzeln einer bekannten Gleichung des Grades $\phi(n)$ mit ganzzahligen Coefficienten, in welcher der Coefficient der höchsten Potenz gleich Eins ist. Hieraus folgt, daſs jede ganze complexe Zahl, als ganze und ganzzahlige rationale Funktion einer primitiven Wurzel ω, in die Form gesetzt werden kann

$$F(\omega) = a + a_1\omega + a_2\omega^2 + \ldots + a_{\phi(n)-1}\omega^{\phi(n)-1};$$

alle höheren Potenzen des ω können nämlich mit Hülfe der Gleichung des Grades $\phi(n)$ eliminirt werden. Aus der Irreduktibilität dieser Gleichung, deren Wurzeln die sämmtlichen primitiven Wurzeln der Gleichung $\omega^n = 1$ sind, welche zuerst von Kronecker in Liouville's Journal, Jahrgang 1854 pag. 177 sqq. bewiesen worden ist, folgt ferner unmittelbar, daſs eine bestimmte complexe Zahl $F(\omega)$ sich nur auf eine einzige Weise in die obige Form setzen läſst. Eben so folgt daraus weiter, daſs wenn $F(\omega)$ durch eine nichtcomplexe ganze Zahl c theilbar sein soll, alle $\phi(n)$ Coefficienten derselben, a, a_1, a_2, etc. einzeln durch c theilbar sein müssen. Die Congruenz $F(\omega) \equiv 0$, mod. c, enthält daher $\phi(n)$ Congruenzen unter nichtcomplexen, ganzen Zahlen in sich und ist mit diesen vollkommen gleichbedeutend.

Setzt man in eine complexe Zahl $F(\omega)$ für ω nacheinander alle primitiven Wurzeln der Gleichung $\omega^n = 1$, so erhält man $\phi(n)$ zusammengehörige complexe Zahlen, welche conjugirte heiſsen sollen. Diese conjugirten complexen Zahlen sind also alle von der Form $F(\omega^k)$, wo k relative Primzahl zu n ist; wenn aber k mit n einen gemeinschaftlichen Faktor hat, ω^k also nicht primitive Wurzel ist, so soll $F(\omega^k)$ nicht als conjugirte Zahl zu $F(\omega)$ angesehen werden, in diesem Falle ist auch die obige allgemeine Form für $F(\omega)$ oder $F(\omega^k)$ keine bestimmte mehr.

Das Produkt aller $\phi(n)$ mit $F(\omega)$ conjugirten complexen Zahlen, welches als symmetrische Funktion aller primitiven Wurzeln der Gleichung

http://rcin.org.pl

$\omega^n = 1$ nothwendig eine nichtcomplexe ganze Zahl ist, soll die Norm von $F(\omega)$ heifsen und durch $NF(\omega)$ bezeichnet werden.

Da jede complexe Zahl $F(\omega)$ ein Faktor ihrer Norm, also Faktor einer nichtcomplexen ganzen Zahl ist, so folgt, dafs auch alle complexen Faktoren des $F(\omega)$ als Faktoren nichtcomplexer ganzer Zahlen angesehen werden können. Aus diesem Grunde werden wir auch die zu untersuchenden idealen Primfaktoren der complexen Zahlen überall als Primfaktoren nichtcomplexer ganzer Zahlen, und weil diese selbst nur aus nichtcomplexen Primzahlen zusammengesetzt sind, als ideale Primfaktoren der nichtcomplexen Primzahlen betrachten. Diese gewöhnlichen Primzahlen sind nun entweder solche, welche nicht in n enthalten sind, oder sie sind Faktoren des n. Demgemäfs werden auch zwei verschiedene Arten idealer Primfaktoren gesondert zu betrachten sein, nämlich erstens die idealen Primfaktoren der nicht in n enthaltenen gewöhnlichen Primzahlen und zweitens die idealen Primfaktoren der in n enthaltenen gewöhnlichen Primzahlen. Die idealen Primfaktoren der zweiten Art, welche stets nur einer endlichen beschränkten Anzahl gewöhnlicher Primzahlen angehören, werden hierbei gegen die der ersten Art nur als Ausnahmen anzusehen sein, deren besondere Eigenthümlichkeiten nach der allgemeinen Untersuchung der idealen Primfaktoren der ersten Art und mit Hülfe derselben behandelt werden sollen.

§. 2.

Es sei q eine Primzahl, welche nicht in n enthalten ist, und t der Exponent, zu welchem q gehört, für den Modul n, so dafs

$$q^t \equiv 1, \text{ mod. } n,$$

dafs aber kein kleinerer Exponent als t existire, für welchen diese Congruenz Statt habe. Es sind dann die Potenzen

$$1, q, q^2, q^3 \ldots\ldots q^{t-1}$$

in Beziehung auf den Modul n alle verschieden von einander. Ferner ist nach bekannten Principien

$$F(\omega)^q \equiv F(\omega^q), \text{ mod. } q,$$

und allgemein für jeden ganzzahligen Werth von h

$$F(\omega)^{q^h} \equiv F(\omega^{q^h}), \text{ mod. } q,$$

also wenn h gleich einem Vielfachen von t, $h = kt$ genommen wird, weil

http://rcin.org.pl

$q^{kt} \equiv 1$, mod. n, ist

$$F(\omega)^{q^{kt}} \equiv F(\omega), \text{ mod. } q.$$

Hieraus folgt: Wenn $F(\omega)$ nicht durch q theilbar ist, so ist auch keine Potenz von $F(\omega)$ durch q theilbar. Wäre nämlich $F(\omega)^m$ durch q theilbar, so müfste jede höhere Potenz ebenfalls durch q theilbar sein, darum, wenn k so grofs genommen wird, dafs $q^{kt} > m$ ist, so müfste $F(\omega)^{q^{kt}}$ durch q theilbar sein, also vermöge der obigen Congruenz auch $F(\omega)$ theilbar durch q.

Nimmt man nacheinander $h = 0, 1, 2, \ldots . t-1$ und multiplicirt alle diese Congruenzen mit einander, so erhält man auch

$$F(\omega)^{1+q+q^2+\ldots+q^{t-1}} \equiv F(\omega)F(\omega^q)F(\omega^{q^2}) \ldots F(\omega^{q^{t-1}}), \text{ mod } q.$$

Der aus den Wurzeln der Gleichung $\omega^n = 1$ gebildete Ausdruck

$$\varpi = \omega + \omega^q + \omega^{q^2} + \ldots . + \omega^{q^{t-1}}$$

oder allgemeiner

$$\varpi_k = \omega^k + \omega^{kq} + \omega^{kq^2} + \ldots . + \omega^{kq^{t-1}}$$

in welchem ω eine primitive Wurzel dieser Gleichung bezeichnet und der Index k alle möglichen ganzzahligen Werthe haben kann, welcher für den allgemeineren Fall, wo n eine zusammengesetzte Zahl ist, genau dieselbe Rolle spielt, als die Gaufsischen Perioden für den besonderen Fall, wo in der Gleichung $\omega^n = 1$ n eine Primzahl ist, soll nun ebenfalls mit dem Namen Periode bezeichnet werden.

Aus der Definition dieser Perioden ergiebt sich zunächst unmittelbar:

$$\varpi_{k+hn} = \varpi_k,$$

so dafs man nur die Perioden

$$\varpi_1, \varpi_2, \varpi_3, \ldots . \varpi_n,$$

zu betrachten hat. Diese zerfallen nun ihrer Natur nach in eben so viele Gruppen, als n Divisoren hat. Ist nämlich d irgend ein Divisor von n, und bezeichnen $s, s_1, s_2, \ldots .$ alle Zahlen kleiner als n, deren gröfster gemeinschaftlicher Faktor mit n gleich d ist, so bilden die Perioden

$$\varpi_s, \varpi_{s_1}, \varpi_{s_2}, \varpi_{s_3}, \ldots . .$$

eine besondere Gruppe, welche als die zum Divisor d gehörende bezeichnet werden soll. Die Perioden einer solchen Gruppe, deren Anzahl, wenn die

http://rcin.org.pl

Gruppe zum Divisor d gehört, gleich $\phi(\frac{n}{d})$ ist, sind nicht alle verschieden von einander, denn man hat offenbar

$$\varpi_s = \varpi_{sq} = \varpi_{sq^2} = \ldots .$$

Ist nun sq^τ der erste Index dieser Reihe, welcher congruent s ist, für den Modul n, so ist, weil s mit n den gröfsten gemeinschaftlichen Faktor d hat, $q^\tau \equiv 1$, mod. $\frac{n}{d}$, und τ der kleinste Exponent, welcher dieser Congruenz genügt; also wenn q zum Exponenten τ gehört, für den Modul $\frac{n}{d}$, so sind je τ Perioden der zum Divisor d gehörenden Gruppe einander gleich, die Anzahl der verschiedenen daher nicht gröfser als $\frac{\phi(\frac{n}{d})}{\tau}$. Es läfst sich auch beweisen, dafs diese wirklich immer von einander verschieden sind, aufser wenn sie alle gleich Null sind. Dieser Fall, dafs alle Perioden einer Gruppe gleich Null werden, tritt allemal dann, aber auch nur dann ein, wenn n eine nicht aus lauter verschiedenen Primfaktoren zusammengesetzte, sondern irgend welche quadratische Faktoren enthaltende Zahl ist. Wir haben aber für unseren gegenwärtigen Zweck nicht nöthig zu beweisen, dafs die oben angegebene reducirte Anzahl der Perioden einer Gruppe, wenn diese nicht alle gleich Null sind, wirklich aus lauter verschiedenen besteht, noch auch zu untersuchen, in welchen Gruppen alle Perioden gleich Null sind; denn die Methode, welche wir gebrauchen werden, so wie auch die durch dieselbe zu erlangenden Resultate setzen nicht voraus, dafs die Perioden wirklich verschieden sind und gelten eben so, wenn gewisse Perioden gleich Null werden.

Die sämmtlichen Perioden einer Gruppe sind immer die Wurzeln einer Gleichung des so vielten Grades, als die Gruppe Perioden enthält, mit ganzzahligen Coefficienten, in welcher der Coefficient der höchsten Potenz der Unbekannten gleich Eins ist.

Bildet man nämlich das Produkt

$$(z - \varpi_s)(z - \varpi_{s_1})(z - \varpi_{s_2}) \ldots = \mathrm{P}(z)$$

für alle Perioden der zum Divisor d gehörenden Gruppe, wobei man sich auch nur auf diejenigen $\frac{\phi(\frac{n}{d})}{\tau}$ Perioden beschränken kann, die sich schon beim Anblick wenigstens als formal verschieden zeigen, so sind die symme-

http://rcin.org.pl

trischen Funktionen der Perioden ϖ_s, ϖ_{s_1}, ϖ_{s_2} .... zugleich symmetrische Funktionen aller primitiven Wurzeln der Gleichung $\omega^n = 1$, also nur ganze Zahlen. In den Fällen, wo alle Perioden der Gruppe gleich Null sind, wird $P(z)$ zu einer blofsen Potenz von z.

Das Produkt zweier Perioden, sei es dafs sie einer und derselben, oder auch verschiedenen Gruppen angehören, läfst sich immer als lineäre Funktion der Perioden darstellen.

Multiplicirt man nämlich die beiden Perioden

$$\varpi_h = \omega^h + \omega^{hq} + \omega^{hq^2} + \ldots + \omega^{hq^{t-1}}$$

$$\varpi_k = \omega^k + \omega^{kq} + \omega^{kq^2} + \ldots + \omega^{kq^{t-1}}$$

mit einander in der Art, dafs jedes Glied des Multiplicators zuerst mit dem in derselben Stelle stehenden des Multiplicandus, sodann mit dem darauf folgenden Gliede, sodann mit dem um zwei Stellen folgenden u. s. w. verbunden wird, so erhält man

$$\varpi_k \varpi_h = \varpi_{k+h} + \varpi_{k+hq} + \varpi_{k+hq^2} + \ldots + \varpi_{k+hq^{t-1}}$$

Diese Gleichung, in welcher k und h alle Zahlen 1, 2, 3, ... n bezeichnen können, repräsentirt ein System von n^2 Gleichungen, auf welchem die Rechnung mit diesen Perioden und mit den dieselben enthaltenden complexen Zahlen beruht. Vermittelst dieses Systems von Gleichungen kann jede beliebige ganze rationale Funktion der Perioden als eine lineäre Funktion derselben dargestellt werden, auch können mit Hülfe desselben die Gleichungen gebildet werden, welche alle Perioden einer Gruppe zu Wurzeln haben.

Eine complexe Zahl, welche nur die Perioden ϖ_1, ϖ_2, ϖ_3 ... ϖ_n enthält, nicht aber aufserdem noch Wurzeln der Gleichung $\omega^n = 1$, welche also immer als lineäre Funktion dieser Perioden dargestellt werden kann, bezeichne ich im allgemeinen kurz durch $F(\varpi_1)$ anstatt $F(\varpi_1, \varpi_2, \ldots \varpi_n)$, so dafs

$$F(\varpi_1) = a + a_1\varpi_1 + a_2\varpi_2 \ldots + a_n\varpi_n,$$

wo die erste Periode ϖ_1 als Repräsentant aller Perioden anzusehen ist. Die conjugirte complexe Zahl, welche aus $F(\varpi_1)$ entsteht, wenn die primitive Wurzel ω in ω^r verwandelt wird, soll demgemäfs durch $F(\varpi_r)$ bezeichnet werden, so dafs allgemein

http://rcin.org.pl

$$F(\varpi_r) = a + a_1 \varpi_r + a_2 \varpi_{2r} + \ldots + a_n \varpi_{nr}$$

ist. Die Anzahl der verschiedenen zu $F(\varpi_1)$ conjugirten complexen Zahlen ist hier nicht gleich $\phi(n)$, sondern nur gleich $\frac{\phi(n)}{t}$, weil von den $\phi(n)$ complexen Zahlen, welche man aus $F(\varpi_1)$ erhält, wenn man für ω nach einander alle primitiven Wurzeln der Gleichung $\omega^n = 1$ setzt, offenbar je t einander gleich sind. Ich setze nun

$$\frac{\phi(n)}{t} = \nu,$$

welche abgekürzte Bezeichnung auch in dem Folgenden überall angewendet werden soll; ferner bezeichne ich durch

$$r_1, r_2, r_3, \ldots r_\nu$$

diejenigen ν ganzen Zahlen, welche kleiner als n sind und relative Primzahlen zu n, und von denen der Quotient zweier niemals einer Potenz von q congruent ist, für den Modul n: so sind:

$$\omega^{r_1}, \omega^{r_2}, \omega^{r_3}, \ldots \omega^{r_\nu}$$

alle primitiven Wurzeln, welche in der complexen Zahl $F(\varpi)$ anstatt ω substituirt, alle verschiedenen, mit $F(\varpi_1)$ conjugirten complexen Zahlen geben, nämlich:

$$F(\varpi_{r_1}), F(\varpi_{r_2}), F(\varpi_{r_3}) \ldots F(\varpi_{r_\nu}).$$

§. 3.

Es soll nun gezeigt werden, wie den in dem vorigen Paragraphen aufgestellten Perioden immer gewisse ganzzahlige Congruenzwurzeln für den Modul q entsprechen, in der Art, dafs jede rationale Gleichung unter den Perioden, als Congruenz für den Modul q aufgefafst, befriedigt wird, wenn anstatt der Perioden diese entsprechenden Congruenzwurzeln gesetzt werden. Zu diesem Zwecke wird zunächst bewiesen, dafs die Gleichungen höherer Grade, deren Wurzeln die verschiedenen Perioden einer und derselben Gruppe sind, wenn sie als Congruenzen für den Modul q aufgefafst werden, stets reale Congruenzwurzeln haben.

Macht man nämlich Gebrauch von der Congruenz

$$y(y-1)(y-2) \ldots (y-q+1) \equiv y^q - y, \text{ mod. } q,$$

welche identisch für jeden beliebigen Werth des y Statt hat, in der Art,

http://rcin.org.pl

dafs wenn das Produkt linker Hand nach Potenzen von y entwickelt wird, die Coefficienten der gleichen Potenzen von y auf beiden Seiten einzeln congruent sind, und setzt in derselben $y = \varpi_i$, wo i ein ganz beliebiger Index ist, also ϖ_i eine beliebige Periode bezeichnet, so hat man bekanntlich

$$\varpi_i^{\,q} \equiv \varpi_i, \text{ mod. } q,$$

und daher

$$\varpi_i (\varpi_i - 1) (\varpi_i - 2) \ldots\ldots (\varpi_i - q + 1) \equiv 0, \text{ mod. } q.$$

Setzt man nun für i nach einander alle Indices einer und derselben Gruppe der Perioden, welche s, s_1, s_2 .... sein mögen, so erhält man, wenn wie im vorigen Paragraphen

$$(z - \varpi_s) (z - \varpi_{s_1}) (z - \varpi_{s_2}) \ldots\ldots = \mathrm{P}(z)$$

gesetzt wird, durch Multiplication aller dieser Congruenzen:

$$\mathrm{P}(0)\,\mathrm{P}(1)\,\mathrm{P}(2) \ldots\ldots \mathrm{P}(q-1) \equiv 0, \text{ mod. } q^{\mu},$$

wo μ die Anzahl der Perioden dieser Gruppe bezeichnet. Es müssen also von den ganzen Zahlen $\mathrm{P}(0)$, $\mathrm{P}(1)$, $\mathrm{P}(2)$.... immer einige, mindestens eine, durch q theilbar sein, d. h. die Congruenz

$$\mathrm{P}(z) \equiv 0, \text{ mod. } q,$$

hat immer mindestens eine reale Congruenzwurzel.

Es seien jetzt a^i, a^i_1, a^i_2, ... a^i_{h-1} alle von einander verschiedenen Wurzeln der Congruenz $\mathrm{P}(z) \equiv 0$, mod. q, und ϖ_i eine Wurzel der Gleichung $\mathrm{P}(z) = 0$, dagegen seien b^i, b^i_1, b^i_2 ... b^i_{q-h-1} alle Nichtwurzeln derselben Congruenz, so dafs die Zahlen a^i, a^i_1 ... a^i_{h-1}, b^i, b^i_1 .... b^i_{q-h-1} mit den Zahlen 0, 1, 2, ... $q-1$, wenn auch in anderer Ordnung, vollständig übereinstimmen: so kann die Congruenz

$$\varpi_i (\varpi_i - 1) (\varpi_i - 2) \ldots\ldots (\varpi_i - q + 1) \equiv 0, \text{ mod } q$$

folgendermaafsen dargestellt werden:

$$(a^i - \varpi_i)(a^i_1 - \varpi_i) \ldots (a^i_{h-1} - \varpi_i) \cdot (b^i - \varpi_i)(b^i_1 - \varpi_i) \ldots (b^i_{q-h-1} - \varpi_i) \equiv 0, \text{mod. } q,$$

Da nun $b^i - \varpi_i$, $b^i_1 - \varpi_i$ u. s. w. Faktoren von $\mathrm{P}(b^i)$, $\mathrm{P}(b^i_1)$ u. s. w. sind, so folgt hieraus

$$(a^i - \varpi_i)(a^i_1 - \varpi_i) \ldots (a^i_{h-1} - \varpi_i) \cdot \mathrm{P}(b^i)\,\mathrm{P}(b^i_1) \ldots \mathrm{P}(b^i_{q-h-1}) \equiv 0, \text{ mod. } q,$$

und weil b^i, b^i_1 .... b^i_{q-h-1} Nichtwurzeln der Congruenz $\mathrm{P}(z) \equiv 0$, mod. q, sind, so sind $\mathrm{P}(b^i)$, $\mathrm{P}(b^i_1)$ .... $\mathrm{P}(b^i_{q-h-1})$ durch q nicht theilbare ganze Zahlen, durch welche diese Congruenz dividirt werden kann. Man hat demnach

$$(a^i - \varpi_i)(a^i_1 - \varpi_i) \ldots (a^i_{h-1} - \varpi_i) \equiv 0, \text{ mod. } q.$$

http://rcin.org.pl

Ich bilde jetzt aus einer gewissen Anzahl von allen verschiedenen unter den $h \cdot n$ Faktoren, welche entstehen wenn man in

$$a^i - \varpi_i,\ a_1^i - \varpi_i,\ \ldots\ (a_{h-1}^i - \varpi_i)$$

dem i die Werthe $1, 2, 3, \ldots n$ beilegt, ein Produkt, so beschaffen, dafs es möglichst viele verschiedene dieser Faktoren enthalte, ohne jedoch durch q theilbar zu sein; dafs es also durch q theilbar wird, sobald irgend einer dieser Faktoren, der nicht schon darin enthalten ist, hinzugefügt wird. Bei der Bildung dieses Produkts hat man von den angegebenen $h \cdot n$ Faktoren zunächst alle diejenigen zu verwerfen, welche etwa für sich selbst congruent Null sein sollten nach dem Modul q, welches offenbar immer der Fall ist, wenn die Periode ϖ_i der Null gleich ist; ferner hat man von allen denen unter diesen Faktoren, welche wegen der Gleichheit der Perioden ϖ_i und der Congruenzwurzeln a^i für verschiedene Werthe des i einander gleich sind, nur je einen beizubehalten; von den übrig bleibenden Faktoren nimmt man einen beliebigen, multiplicirt diesen mit einem zweiten und wenn das Produkt nicht durch q theilbar ist, so fügt man einen dritten hinzu u. s. w. Wird durch Hinzufügung eines neuen Faktors das Produkt durch q theilbar, so wird derselbe verworfen und ein anderer der noch vorhandenen genommen. Sind auf diese Weise alle verschiedene Faktoren an die Reihe gekommen, also entweder dem Produkte zugefügt oder verworfen, so ist das Produkt gefunden, welches die verlangte Eigenschaft hat, dafs es nicht durch q theilbar ist, dafs es aber durch Multiplikation mit einem jeden noch nicht darin enthaltenen der obigen Faktoren ein durch q theilbares Produkt giebt. Sollte der besondere Fall eintreten, dafs alle Faktoren, aus welchen dieses Produkt zu bilden ist, für sich durch q theilbar wären (welcher Fall wirklich eintritt, wenn n eine Primzahl ist und $t = n - 1$), so würde dieses Produkt, welches keinen dieser Faktoren enthalten dürfte, einfach gleich Eins zu nehmen sein. Das nach den angegebenen Regeln gebildete Produkt, welches in der ganzen gegenwärtigen Theorie die wichtigste Rolle spielt, bezeichne ich durch $\Psi(\varpi_1)$.

Ist nun ϖ_i eine beliebige Periode irgend einer Gruppe, und $P(z) = 0$ die Gleichung, deren Wurzeln alle Perioden dieser Gruppe sind, welcher ϖ_i angehört, und sind $a^i, a_1^i \ldots a_{h-1}^i$ alle verschiedenen Wurzeln der Congruenz $P(z) \equiv 0$, mod. q, so können die Faktoren

$$a^i - \varpi_i,\ a_1^i - \varpi_i,\ \ldots\ a_{h-1}^i - \varpi_i$$

http://rcin.org.pl

nicht alle zugleich in dem Produkte $\Psi(\varpi_1)$ enthalten sein, weil sonst vermöge der Congruenz

$$(a^i - \varpi_i)\,(a^i_1 - \varpi_i) \ldots . (a^i_{h-1} - \varpi_i) \equiv 0, \text{ mod. } q,$$

$\Psi(\varpi_1)$ durch q theilbar sein würde. Es mufs also wenigstens einen dieser Faktoren geben, der in $\Psi(\varpi_1)$ nicht enthalten ist, welchen ich durch $u_i - \varpi_i$ bezeichne, wo u_i eine der Zahlen a^i, $a^i_1 \ldots a^i_{h-1}$, d. h. eine der verschiedenen Wurzeln der Congruenz $P(z) \equiv 0$, mod. q, vorstellt. Durch Multiplikation mit diesem Faktor $u_i - \varpi_i$ mufs nun $\Psi(\varpi_1)$ durch q theilbar werden; man hat also

$$\Psi(\varpi_1)\,(u_i - \varpi_i) \equiv 0, \text{ mod. } q,$$

oder

$$\Psi(\varpi_1)\varpi_i \equiv \Psi(\varpi_1) \cdot u_i, \text{ mod. } q.$$

welche Congruenz für jeden beliebigen Werth des Index $i = 1, 2, 3 \ldots n$ Statt hat, und darum wesentlich ein System von n Congruenzen repräsentirt. Aus diesem Systeme von Congruenzen, welches die hauptsächlichste Grundlage der folgenden Untersuchungen bildet, folgt nun zunächst der wichtige Satz:

Jede rationale Gleichung unter den Perioden ϖ_i, welche aufser diesen nur ganze Zahlen enthält, wird, wenn anstatt der Perioden ϖ_i die entsprechenden Congruenzwurzeln u_i gesetzt werden, als Congruenz für den Modul q befriedigt.

Denkt man sich nämlich die gegebene Gleichung unter den Perioden von den etwa darin vorkommenden Brüchen befreit und alle Glieder auf eine Seite gebracht, so dafs sie die Form $F(\varpi_1) = 0$ annimmt, und multiplicirt mit $\Psi(\varpi_1)$, so kann man anstatt $\Psi(\varpi_1)\,\varpi_i$ überall die für den Modul q congruenten Ausdrücke $\Psi(\varpi_1)\,u_i$ setzen, und erhält so

$$\Psi(\varpi_1)\,F(\varpi_1) \equiv \Psi(\varpi_1)\,F(u_1), \text{ mod. } q,$$

wo $F(u_1)$ den ganzzahligen Ausdruck bezeichnet, welchen man aus $F(\varpi_1)$ durch die Substitution der ganzen Zahlen u_i anstatt der entsprechenden Congruenzwurzeln ϖ_i erhält. Da nun $F(\varpi_1) = 0$ ist und $\Psi(\varpi_1)$ nicht $\equiv 0$, mod, q, so mufs nothwendig der ganzzahlige Ausdruck $F(u_1) \equiv 0$, mod. q, sein, was zu beweisen war.

Nach diesem Satze erhält man zum Beispiel aus dem Systeme der n^2 Fundamentalgleichungen für die Perioden, nämlich

$$\varpi_k \varpi_h = \varpi_{k+h} + \varpi_{k+hq} + \varpi_{k+hq^2} + \ldots + \varpi_{k+hq^{i-1}}$$

http://rcin.org.pl

für $k = 1, 2, 3, \ldots n$, $h = 1, 2, 3, \ldots n$, augenblicklich das entsprechende System von n^2 Congruenzen, welchen die Zahlen $u_1, u_2, u_3, \ldots u_n$ genügen müssen:

$$u_k u_h \equiv u_{k+h} + u_{k+hq} + u_{k+hq^2} + \ldots + u_{k+hq^{t-1}}, \text{ mod. } q,$$

für $k = 1, 2, 3, \ldots n$, $h = 1, 2, 3, \ldots n$, welches System mit Erfolg zur direkten Berechnung der Congruenzwurzeln $u_1, u_2, u_3, \ldots u_n$ benutzt werden kann.

Die Congruenzwurzeln u_i können immer auf mehrere verschiedene Weisen den Perioden ϖ_i entsprechend zugeordnet werden. Verwandelt man nämlich in dem Systeme der Congruenzen:

$$\Psi(\varpi_1)\,\varpi_i \equiv \Psi(\varpi_1)\,u_i \text{ mod. } q,$$

die den Perioden zu Grunde gelegte primitive Wurzel ω der Gleichung $\omega^n = 1$ in eine andere, z. B. in ω^r, wo r relative Primzahl zu n ist, so geht dasselbe über in

$$\Psi(\varpi_r)\,\varpi_{r\,i} \equiv \Psi(\varpi_r)\,u_i \text{ mod. } q.$$

Es giebt nun $\phi(n)$ verschiedene primitive Wurzeln ω^r, oder was dasselbe ist, $\phi(n)$ verschiedene Werthe des r, für welche ω^r eine primitive Wurzel ist, von diesen geben aber, wie oben (§ 2) gezeigt worden, je t nur genau dieselben Perioden. Die Anzahl der verschiedenen Congruenzen dieser Art ist also nicht gröfser als $\nu = \frac{\phi(n)}{t}$, und diesen entsprechen eben so viele, nämlich ν verschiedene Arten und Weisen, wie die Congruenzwurzeln u_i den Perioden $\varpi_{r\,i}$ zugeordnet und anstatt derselben substituirt werden können, wenn Gleichungen unter den Perioden in Congruenzen unter den Zahlen u_i verwandelt werden sollen. Die Substitution, nach welcher die Perioden $\varpi_r, \varpi_{2r}, \varpi_{3r}, \ldots \varpi_{nr}$ beziehungsweise durch die Zahlen $u_1, u_2, u_3, \ldots u_n$ ersetzt werden, bezeichne ich einfach als die Substitution $\varpi_{r\,i} = u_i$, indem i jede der Zahlen $1, 2, 3, \ldots n$ repräsentirt. Genau dieselbe Substitution kann demgemäfs auch als Substitution $\varpi_i = u_{\varrho i}$ bezeichnet werden, wenn ϱ durch die Congruenz $r\varrho \equiv 1$ mod. n, bestimmt ist; die Identität dieser Substitution mit der anderen fällt sogleich in die Augen, wenn man in dieser ir statt i setzt. Bringt man in einer complexen Zahl $F(\varpi_1)$ die Substitution $\varpi_{r\,i} = u_i$ an, oder was dasselbe ist, die Substitution $\varpi_i = u_{\varrho i}$, so soll die daraus entstehende nicht complexe ganze Zahl künftig durch $F(u_\varrho)$ bezeichnet werden; dieselbe Substitution in $F(\varpi_r)$ angebracht wird demnach $F(u_{\varrho r})$ ergeben.

http://rcin.org.pl

§. 4.

Es sollen nun die für den vorliegenden Zweck wesentlichen Eigenschaften der complexen Zahl $\Psi(\varpi_1)$ aufgezeigt werden, und zwar zunächst die folgende:

Die zu $\Psi(\varpi_1)$ conjugirten complexen Zahlen, deren Anzahl gleich ν ist, sind alle wirklich verschieden von einander.

Wären irgend zwei dieser conjugirten Zahlen einander gleich, z. B.

$$\Psi(\varpi_k) = \Psi(\varpi_h)$$

wo k und h irgend zwei verschiedene der oben (§. 2) genau bestimmten Zahlen $r_1, r_2, r_3, \ldots r_\nu$ bedeuten, so würde man durch eine passende Veränderung der primitiven Wurzel ω hieraus eine Gleichung

$$\Psi(\varpi_1) = \Psi(\varpi_r)$$

erhalten, in welcher r relative Primzahl zu n und keiner Potenz von q congruent wäre, nach dem Modul n. Da nun aber nach dem Hauptresultate des vorigen Paragraphen

$$\left.\begin{aligned} \Psi(\varpi_1)\,\varpi_i &\equiv \Psi(\varpi_1)\,u_i \\ \Psi(\varpi_r)\,\varpi_{ri} &\equiv \Psi(\varpi_r)\,u_i \end{aligned}\right\} \text{ mod. } q,$$

so würde auch

$$\Psi(\varpi_1)\,\varpi_i \equiv \Psi(\varpi_1)\,\varpi_{ri}, \quad \text{mod. } q,$$

sein, für alle Werthe des $i = 1, 2, 3, \ldots . n$. Multiplicirt man diese Congruenz auf beiden Seiten mit ω^{-i} und nimmt die Summe für $i = 1, 2, 3, \ldots . n$, so erhält man hieraus

$$\Psi(\varpi_1) \sum_1^n{}_i\, \omega^{-i}\,\varpi_i \equiv \Psi(\varpi_1) \sum_1^n{}_i\, \omega^{-i}\,\varpi_{ri}, \text{ mod. } q.$$

Setzt man nun anstatt der Perioden ihre Ausdrücke durch die Wurzel ω, so hat man

$$\omega^{-i}\,\varpi_i = 1 + \omega^{i(q-1)} + \omega^{i(q^2-1)} + \ldots\ldots\ldots + \omega^{i(q^{t-1}-1)}$$

$$\omega^{-i}\,\varpi_{ri} = \omega^{i(r-1)} + \omega^{i(rq-1)} + \omega^{i(rq^2-1)} + \ldots . + \omega^{i(rq^{t-1}-1)}$$

Nimmt man jetzt die Summen in Beziehung auf $i = 1, 2, 3, \ldots . n$ und bemerkt, dafs $\sum_1^n{}_i\, \omega^{mi}$ immer gleich Null ist, mit Ausnahme des einen Falles, wo m durch n theilbar, dafs aber $q-1, q^2-1, \ldots q^{t-1}-1$ und $r-1, rq-1, rq^2-1, \ldots . rq^{t-1}-1$ nicht durch n theilbar sind, so hat man

http://rcin.org.pl

$$\sum_1^n{}_i\, \omega^{-i}\, \varpi_i = n,$$

$$\sum_1^n{}_i\, \omega^{-i}\, \varpi_{r_i} = 0.$$

die obige Congruenz giebt daher

$$\Psi(\varpi_1) \cdot n \equiv 0, \text{ mod. } q,$$

welches unmöglich ist, weil weder die ganze Zahl n noch die complexe Zahl $\Psi(\varpi_1)$ durch q theilbar ist. Die Annahme, dafs zwei der ν mit $\Psi(\varpi_1)$ conjugirten complexen Zahlen einander gleich sein könnten, ist also eine falsche.

Das Produkt je zweier verschiedener zu $\Psi(\varpi_1)$ conjugirter complexer Zahlen ist stets durch q theilbar.

Dieser Satz folgt unmittelbar aus der Bildungsweise dieser complexen Zahlen, welche, wie wir oben gezeigt haben, aus Faktoren von der Form $a_s^i - \varpi_i$ so zusammengesetzt sind, dafs keiner derselben mehrmals darin enthalten ist und dafs durch das Hinzutreten eines jeden nicht schon in $\Psi(\varpi_1)$ enthaltenen dieser Faktoren das Produkt durch q theilbar wird. Sind nun zwei solche complexe Zahlen verschieden von einander, so enthalten sie nicht genau dieselben Faktoren von dieser Form, sondern eine mufs gewisse enthalten, welche in der andern nicht vorkommen, darum mufs ihr Produkt nothwendig durch q theilbar sein.

Nach dem Bildungsgesetze, welches wir oben für die durch Ψ bezeichneten Produkte aufgestellt haben, scheint es, als ob einer und derselben Primzahl q mehrere wesentlich verschiedene solche Produkte angehören könnten; dafs diefs aber in der That nicht der Fall ist, wird folgendermaafsen gegeigt.

Sei $\Psi(\varpi_1)$ irgend eines der nach dem im vorigen Paragraphen angegebenen Bildungsgesetze aus den Faktoren von der Form $a_s^i - \varpi_i$ zu bildenden Produkte, so werden auch die zu $\Psi(\varpi_1)$ conjugirten complexen Zahlen offenbar solche Produkte sein, welche sich ebenfalls aus diesen Faktoren bilden lassen und den gegebenen Bedingungen genügen. Es sei nun die Summe dieser mit $\Psi(\varpi_1)$ conjugirten complexen Zahlen gleich M, also

$$M = \Psi(\varpi_{r_1}) + \Psi(\varpi_{r_2}) + \Psi(\varpi_{r_3}) + \ldots + \Psi(\varpi_{r_\nu})$$

so ist M, als symmetrische Funktion dieser Perioden, oder auch als symmetrische Funktion aller primitiven Wurzeln der Gleichung $\omega^n = 1$, eine nichtcomplexe ganze Zahl. Die Zahl M ist auch nicht durch q theilbar, denn

http://rcin.org.pl

multiplicirt man dieselbe mit $\Psi(\varpi_{r_1})$ und beachtet, dafs das Produkt je zweier verschiedener conjugirter Ψ durch q theilbar ist, so hat man

$$\Psi(\varpi_{r_1})\, M \equiv \Psi(\varpi_{r_1})^2, \text{ mod. } q,$$

und weil $\Psi(\varpi_{r_1})$ nicht durch q theilbar ist, so ist auch das Quadrat dieser complexen Zahl nicht durch q theilbar, also auch M nicht durch q theilbar. Wäre nun $\Psi'(\varpi_1)$ irgend eine von $\Psi(\varpi_1)$ und von allen conjugirten derselben verschiedene complexe Zahl, welche ebenfalls nach dem angegebenen Bildungsgesetze aus den Faktoren von der Form $a_s^i - \varpi_i$ zusammengesetzt wäre, so würde $\Psi'(\varpi_1)\,\Psi(\varpi_r)$ nothwendig durch q theilbar sein für alle Werthe des $r = r_1, r_2, \ldots\ldots r_\nu$. Die Verschiedenheit des $\Psi'(\varpi_1)$ von $\Psi(\varpi_r)$ kann nämlich nicht darin liegen, dafs eines dieser beiden Produkte irgend einen der Faktoren von der Form $a_s^i - \varpi_i$ mehrmals enthält als das andere, weil nach der Voraussetzung keiner dieser Faktoren mehr als einmal in einem solchen Produkte vorkommen kann, diese Verschiedenheit müfste daher nur daher kommen, dafs eine der beiden complexen Zahlen $\Psi'(\varpi_1)$ und $\Psi(\varpi_r)$ irgend einen der Faktoren von der Form $a_s^i - \varpi_i$ enthält, welcher in der andern nicht vorkommt, woraus folgen würde, dafs das Produkt derselben durch q theilbar sein müfste. Da also alle einzelnen Theile, aus welchen M besteht, nach Multiplication mit $\Psi'(\varpi_1)$ durch q theilbar wären, so würde auch $\Psi'(\varpi_1)\, M$ durch q theilbar sein, welches unmöglich ist, weil weder die nichtcomplexe Zahl M, noch die complexe Zahl $\Psi'(\varpi_1)$ durch q theilbar ist. Das gefundene Resultat läfst sich nun folgendermaafsen aussprechen:

Die Anzahl aller verschiedenen Produkte, welche nach dem festgesetzten Bildungsgesetze aus den Faktoren von der Form $a_s^i - \varpi_i$ gebildet werden können ist gleich $\nu = \frac{\phi(n)}{t}$ und dieselben sind conjugirte complexe Zahlen. Die complexe Zahl $\Psi(\varpi_1)$ ist also, abgesehen von der zu Grunde liegenden primitiven Wurzel ω, eine vollständig bestimmte für jede Primzahl q.

Eine andere wichtige Eigenschaft der complexen Zahl $\Psi(\varpi_1)$ erhält man aus der Congruenz

$$\Psi(\varpi_1)\,\Psi(\varpi_r) \equiv \Psi(\varpi_1)\,\Psi(u_r), \text{ mod. } q,$$

welche aus dem Systeme der Congruenzen

$$\Psi(\varpi_1)\,\varpi_i \equiv \Psi(\varpi_1)\, u_i, \text{ mod. } q,$$

http://rcin.org.pl

unmittelbar folgt, da nämlich $\Psi(\varpi_1)\,\Psi(\varpi_r) \equiv 0$, mod. q, sobald r weder der Eins noch einer Potenz von q congruent ist, für den Modul n, so giebt obige Congruenz

$$\Psi(\varpi_1)\,\Psi(u_r) \equiv 0, \text{ mod. } q,$$

woraus folgt:

$$\Psi(u_r) \equiv 0, \text{ mod. } q,$$

für den Fall $r = 1$ aber, wo $\Psi(\varpi_1) \cdot \Psi(\varpi_1)$ nicht durch q theilbar ist, folgt eben so:

$$\Psi(u_1) \text{ nicht} \equiv 0, \text{ mod. } q.$$

Diese Resultate geben folgenden Satz:

Die complexe Zahl $\Psi(\varpi_1)$ wird durch die Substitution $\varpi_{r\,i} = u_i$, wenn r für den Modul n weder der Eins noch einer Potenz von q congruent ist, immer eine durch q theilbare, durch die Substitution $\varpi_i = u_i$ aber eine durch q nicht theilbare ganze Zahl.

Aus diesem Satze folgt fast unmittelbar auch der folgende:

Wenn für eine nur die Perioden enthaltende complexe Zahl $F(\varpi_1)$ die Congruenz

$$\Psi(\varpi_r)\,F(\varpi_1) \equiv 0, \text{ mod. } q,$$

Statt hat, so ist

$$F(u_\varrho) \equiv 0, \text{ mod. } q,$$

wo ϱ durch die Congruenz $r\varrho \equiv 1$, mod. n, bestimmt ist, und auch umgekehrt: wenn $F(u_\varrho) \equiv 0$, mod. q, so ist $\Psi(\varpi_r)\,F(\varpi_1) \equiv 0$ mod. q.

Durch Anwendung der Substitution $\varpi_{r\,i} = u_i$, oder was dasselbe ist, $\varpi_i = u_{\varrho\,i}$, hat man nämlich aus der Congruenz, welche die Voraussetzung des Satzes bildet, sogleich $\Psi(u_1)\,F(u_\varrho) \equiv 0$, mod. q, und weil $\Psi(u_1)$ nicht durch q theilbar ist, mufs $F(u_\varrho) \equiv 0$, mod. q, sein. Multiplicirt man aber $F(u_\varrho)$ mit $\Psi(\varpi_r)$ und ersetzt umgekehrt die Congruenzwurzeln durch die Perioden, nach der Substitution $\varpi_i = u_{\varrho\,i}$, so erhält man aus $F(u_\varrho) \equiv 0$, mod. q, sogleich $\Psi(\varpi_r)\,F(\varpi_1) \equiv 0$ mod. q.

Die Congruenzwurzeln $u_1, u_2, u_3 \ldots u_n$, welche den Perioden $\varpi_1, \varpi_2, \varpi_3 \ldots \varpi_n$ auf ν verschiedene Weisen entsprechen, können, wenn denselben passende Vielfache von q zugefügt werden, immer so gewählt werden, dafs sie, in einer rationalen Gleichung unter den Perioden substituirt,

http://rcin.org.pl

eine Congruenz geben, welche nicht nur für den einfachen Modul q, sondern sogar für eine beliebig hohe Potenz von q richtig ist. Setzt man nämlich die Congruenz

$$\Psi(\varpi_1)\,(u_i - \varpi_i) \equiv 0, \mod. q,$$

in die Form einer Gleichung

$$\Psi(\varpi_1)\,(u_i - \varpi_i) = q \,.\, Q(\varpi_1)$$

und addirt auf beiden Seiten $\Psi(\varpi_1) \,.\, q \,.\, h$, wo h eine ganze Zahl bezeichnet, und multiplicirt sodann nochmals mit $\Psi(\varpi_1)$, so erhält man

$$\Psi(\varpi_1)^2\,(u_i + hq - \varpi_i) = q\,\Psi(\varpi_1)\,(Q(\varpi_1) + h\Psi(\varpi_1))$$

und weil

$$\begin{aligned} \Psi(\varpi_1)\,Q(\varpi_1) &\equiv \Psi(\varpi_1)\,Q(u_1) \\ \Psi(\varpi_1)\,\Psi(\varpi_1) &\equiv \Psi(\varpi_1)\,\Psi(u_1) \end{aligned} \mod. q,$$

so hat man

$$\Psi(\varpi_1)^2\,(u_i + hq - \varpi_i) \equiv q\Psi(\varpi_1)\,(Q(u_1) + h\Psi(u_1)) \mod. q^2.$$

Da nun $\Psi(u_1)$ nicht durch q theilbar ist, so giebt es stets einen Werth des h für welchen die Congruenz

$$Q(u_1) + h\Psi(u_1) \equiv 0, \mod. q,$$

erfüllt ist, für welchen also

$$\Psi(\varpi_1)^2\,(u_i + hq - \varpi_i) \equiv 0, \mod. q^2,$$

ist, also wenn $u_i + hq$ durch $\overset{2}{u}_i$ bezeichnet wird:

$$\Psi(\varpi_1)^2\,(\overset{2}{u}_i - \varpi_i) \equiv 0, \mod. q^2.$$

Ganz auf dieselbe Weise kann man hieraus weiter die Congruenz

$$\Psi(\varpi_1)^3\,(\overset{3}{u}_i - \varpi_i) \equiv 0, \mod. q^3,$$

ableiten, und so fortfahrend findet man allgemein für jeden ganzzahligen Werth des m

$$\Psi(\varpi_1)^m\,(\overset{m}{u}_i - \varpi_i) \equiv 0, \mod q^m,$$

welche auch so dargestellt werden kann:

$$\Psi(\varpi_1)^m\,\varpi_i \equiv \Psi(\varpi_1)^m\,\overset{m}{u}_i, \mod. q^m,$$

oder wenn die primitive Wurzel ω in ω^r verändert wird

$$\Psi(\varpi_r)^m\,\varpi_{r\,i} \equiv \Psi(\varpi_r)^m \,.\, \overset{m}{u}_i, \mod q^m.$$

Aus dieser Congruenz, welche, weil sie für alle Werthe des $i = 1, 2, 3, \ldots . n$ gültig ist, ein System von n Congruenzen repräsentirt, folgt nun ganz auf dieselbe Weise, wie oben (§. 3) für den Fall $m = 1$ gezeigt worden, der allgemeine Satz:

http://rcin.org.pl

Jede rationale Gleichung unter den Perioden ϖ_i, welche aufser diesen nur ganze Zahlen enthält, wird, wenn anstatt der Perioden $\varpi_r, \varpi_{2r}, \varpi_{3r} \ldots \varpi_{nr}$ beziehungsweise die ganzen Zahlen $\overset{m}{u}_1, \overset{m}{u}_2, \overset{m}{u}_3 \ldots \overset{m}{u}_n$ gesetzt werden, also durch die Substitution $\varpi_{r\,i} = \overset{m}{u}_i$, als Congruenz für den Modul q^m befriedigt.

Ferner hat man für die Zahlen $\overset{m}{u}_i$ und den Modul q^m genau ebenso den Satz:

Die Bedingung $\Psi(\varpi_r)\,{}^mF(\varpi^i) \equiv 0$, mod. q^m, ist gleichbedeutend mit $F(\overset{m}{u}_i) \equiv 0$, mod. q^m, wo $r\varrho \equiv 1$, mod. n.

In Betreff derjenigen Perioden ϖ_i, in welchen i mit n einen gemeinschaftlichen Faktor hat, welche also eigentlich nicht die n^{ten}, sondern niedere Wurzeln der Einheit enthalten, ist hier noch zu bemerken, dafs es in einzelnen Fällen nöthig ist dieselben besonders zu betrachten, wenn gleich sie, wie in dem Vorhergehenden gezeigt worden ist, genau denselben allgemeinen Regeln unterworfen sind, als die nur die primitiven Wurzeln der Gleichung $\omega^n = 1$ enthaltenden. Wenn in dem Ausdrucke der Periode

$$\varpi_i = \omega^i + \omega^{iq} + \omega^{iq^2} + \ldots + \omega^{iq^{t-1}}$$

i mit n den gröfsten gemeinschaftlichen Faktor ν hat und $i = \nu i'$, $n = \nu n'$ gesetzt wird, wo i' und n' relative Primzahlen sind und wenn q zum Exponenten τ gehört in Beziehung auf den Modul n', so ist τ nothwendig ein Divisor von t. Setzt man daher $t = d\tau$, so werden nur die ersten τ Glieder dieser Periode verschieden von einander und dieselben wiederholen sich $d$mal, es wird also

$$\varpi_i = d\,(\omega^i + \omega^{iq} + \omega^{iq^2} + \ldots + \omega^{iq^{\tau-1}})$$

Diesen ganzzahligen Faktor d kann man nun in den niederen Perioden, sowohl bei der Ermittelung der den Perioden entsprechenden Congruenzwurzeln, als bei der Bildung der mit Ψ bezeichneten complexen Zahlen überall beibehalten, oder auch weglassen, wodurch in den entwickelten Methoden und Sätzen nichts geändert wird. In dem besonderen Falle aber, wo d durch die Primzahl q theilbar ist, ist es unbedingt nöthig, dafs dieser ganzzahlige Faktor weggelassen und die Periode nicht als aus t Gliedern von denen je d einander gleich sind, sondern nur als aus den τ verschiedenen Gliedern bestehend angenommen wird. In diesem Falle, welcher übrigens nur für ge-

GABINET MATEMATYCZNY Towarzystwa Naukowego Warszawskiego
http://rcin.org.pl

wisse besondere und zwar kleine Werthe des q eintreten kann, würde nämlich die Beibehaltung des ganzzahligen Faktors d eine Unbestimmtheit herbeiführen, welche wie leicht zu sehen ist daher kommen würde, dafs die Congruenzen nach dem Modul q für die Perioden und die entsprechenden Congruenzwurzeln den Faktor q selbst enthalten und indem sie so nur $0 \equiv 0$, mod. q, ergeben, nichtssagend sein würden. Man kann aber, um einer jeden besonderen Betrachtung dieser speciellen Werthe des q überhoben zu sein, allgemein die Periode ϖ_i auch definiren als die Summe

$$\omega^i + \omega^{iq} + \omega^{iq^2} + \omega^{iq^3} + \ldots\ldots$$

fortgesetzt bis zu demjenigen Gliede ausschliefslich, welches dem ersten Gliede gleich wird. Da der Unterschied dieser Definition von der oben gegebenen lediglich darin besteht, dafs der die niederen Perioden behaftende ganzzahlige Faktor überall ausgeschlossen wird, so ist klar, dafs wenn man dieselbe an die Stelle der im §. 2. gegebenen Definition setzt, die Methoden so wie die entwickelten Resultate überall dieselben bleiben.

§. 5.

Die leitende Grundidee bei der Einführung der idealen Primfaktoren der aus den Wurzeln der Gleichung $\omega^n = 1$ gebildeten complexen Zahlen ist dieselbe, welche ich in meinen früheren Abhandlungen über die speciellere Art complexer Zahlen umständlich auseinandergesetzt habe. Sie liegt im wesentlichen darin, dafs, weil die einfachsten wirklichen Faktoren der complexen Zahlen nicht immer die wahre Natur von Primfaktoren haben, nach welcher jede gegebene Zahl eine endliche Anzahl derselben in unveränderlich bestimmter Weise enthalten mufs, die Primfaktoren durch gewisse Congruenzbedingungen ersetzt werden, welche alle wesentlichen Eigenschaften wahrhafter Primfaktoren darstellen, und welche in allen den Fällen, wo wirkliche Primfaktoren vorhanden sind, mit diesen vollständig übereinstimmen, so dafs diese Congruenzbedingungen als die permanenten Eigenschaften der complexen Zahlen zu betrachten sind, die wirkliche Darstellbarkeit derselben aber, in Form von selbständigen ganzen complexen Faktoren, nur als eine accidentelle Eigenschaft aufzufassen ist. Einer weiteren Ausführung dieser Grundidee glaube ich mich hier enthalten zu dürfen und stelle sogleich die Definition der idealen Primfaktoren der aus den Wurzeln der Gleichung $\omega^n = 1$ gebildeten complexen Zahlen auf.

http://rcin.org.pl

Wenn eine complexe Zahl $F(\omega)$ die Eigenschaft hat, dafs

$$\Psi(\varpi_r)\, F(\omega) \equiv 0, \text{ mod. } q,$$

so soll von dieser Zahl $F(\omega)$ ausgesagt werden: sie enthält einen idealen Primfaktor des q, und zwar denjenigen, welcher zur Substitution $\varpi_{r,i} = u_i$ gehört. Hat die complexe Zahl $F(\omega)$ ausserdem die Eigenschaft, dafs

$$\Psi(\varpi_r)^m F(\omega) \equiv 0, \text{ mod. } q^m,$$

aber

$$\Psi(\varpi_r)^{m+1} F(\omega) \text{ nicht} \equiv 0, \text{ mod. } q^{m+1},$$

so soll von ihr ausgesagt werden, dafs sie den idealen Primfaktor des q, welcher zur Substitution $\varpi_{r,i} = u_i$ gehört, genau m mal enthält.

Da die Anzahl der verschiedenen complexen Zahlen $\Psi(\varpi_r)$, für die verschiedenen Werthe des r, und darum auch die Anzahl der verschiedenen Substitutionen $\varpi_{r,i} = u_i$, wie oben gezeigt worden, gleich ν ist, so folgt:

Die Anzahl der verschiedenen idealen Primfaktoren der nichtcomplexen Primzahl q, welche zum Exponenten t gehört für den Modul n, ist gleich $\frac{\phi(n)}{t} = \nu$.

Von den hier definirten idealen Primfaktoren des q ist nun nachzuweisen, dafs sie alle wesentlichen Eigenschaften wahrhafter Primfaktoren besitzen, zu welchem Zwecke zunächst folgender Satz bewiesen werden soll:

Wenn zwei oder mehrere complexe Zahlen einen idealen Primfaktor des q nicht enthalten, so enthält das entwickelte Produkt derselben diesen idealen Primfaktor ebenfalls nicht.

Es seien $f(\omega)$ und $f_1(\omega)$ zwei complexe Zahlen, deren keine den zur Substitution $\varpi_{r,i} = u_i$ gehörenden idealen Primfaktor des q enthalte, so ist nach der Definition

$$\left.\begin{array}{l} \Psi(\varpi_r)\, f(\omega) \text{ nicht} \equiv 0, \\ \Psi(\varpi_r)\, f_1(\omega) \text{ nicht} \equiv 0, \end{array}\right\} \text{ mod. } q.$$

Weil nun diese beiden complexen Ausdrücke nicht durch q theilbar sind, so ist auch keine Potenz derselben durch q theilbar; erhebt man dieselben daher zur Potenz des Exponenten $1 + q + q^2 + \ldots + q^{l-1}$ und bemerkt, dafs allgemein

$$F(\omega)^{1+q+q+\ldots+q^{l-1}} \equiv F(\omega)\, F(\omega^q)\, F(\omega^{q^2}) \ldots F(\omega^{q^{l-1}}), \text{ mod. } q.$$

http://rcin.org.pl

ist, so hat man, wenn der Kürze wegen $1 + q + q^2 \ldots + q^{t-1} = Q$ gesetzt wird:

$$\Psi(\varpi_r) \overset{Q}{.} f(\omega) f(\omega^q) f(\omega^{q^2}) \ldots f(\omega^{q^{t-1}}) \text{ nicht} \equiv 0.$$

$$\Psi(\varpi_r) \overset{Q}{.} f_1(\omega) f_1(\omega^q) f_1(\omega^{q^2}) \ldots f_1(\omega^{q^{t-1}}) \text{ nicht} \equiv 0. \quad \text{mod. } q.$$

Setzt man nun:

$$f(\omega)\, f(\omega^q) f(\omega^{q^2}) \ldots f(\omega^{q^{t-1}}) = F(\varpi_1)$$

$$f_1(\omega)\, f_1(\omega^q) f_1(\omega^{q^2}) \ldots f_1(\omega^{q^{t-1}}) = F_1(\varpi_1),$$

welche Bezeichnungen als nur die Perioden enthaltende complexe Zahlen ihnen wirklich zukommen, weil sie als symmetrische Funktionen aller in einer Periode vorkommenden Wurzeln $\omega, \omega^q, \ldots . \omega^{q^{t-1}}$ nur die Perioden, nicht aber ausfer diesen die Wurzel ω enthalten können, wo die Perioden in dem Sinne aufzufassen sind, welcher denselben am Schlusse des vorigen Paragraphen gegeben worden ist, nämlich befreit von den sie etwa behaftenden ganzzahligen Faktoren: so hat man

$$\Psi(\varpi_r) \overset{Q}{F}(\varpi_1) \text{ nicht} \equiv 0,$$

$$\Psi(\varpi_r) \overset{Q}{F_1}(\varpi_1) \text{ nicht} \equiv 0, \quad \text{mod. } q.$$

Hieraus folgt weiter, dafs auch die durch die Substitution $\varpi_{r\,i} = u_i$ aus $F(\varpi_1)$ und $F_1(\varpi_1)$ entstehenden nichtcomplexen ganzen Zahlen $F(u_\varrho)$ und $F_1(u_\varrho)$ nicht durch q theilbar sind, also auch nicht das Produkt derselben $F(u_\varrho) . F_1(u_\varrho)$. Multiplicirt man dieses Produkt noch mit $\Psi(\varpi_r)$ und substituirt rückwärts die Perioden für die Congruenzwurzeln, nach der Substitution $\varpi_{r\,i} = u_i$, so hat man

$$\Psi(\varpi_r)\, F(\varpi_1)\, F_1(\varpi_1) \text{ nicht} \equiv 0, \text{ mod. } q.$$

und daher auch

$$\Psi(\varpi_r) \,.\, f(\omega) \,.\, f_1(\omega) \text{ nicht} \equiv 0, \text{ mod. } q.$$

weil dieser Ausdruck nur ein Theiler des vorigen ist. Das Produkt der beiden complexen Zahlen $f(\omega)$ und $f_1(\omega)$ enthält also den zur Substitution $\varpi_{r\,i} = u_i$ gehörenden idealen Primfaktor des q nicht. Da nun der Satz für ein Produkt von zwei Faktoren bewiesen ist, so folgt unmittelbar, dafs er auch für ein Produkt beliebig vieler Faktoren ebenso gelten mufs.

Dieser Satz dient nun zum Beweise des folgenden allgemeineren:

Das entwickelte Produkt zweier oder mehrerer complexer

http://rcin.org.pl

Zahlen enthält genau dieselben idealen Primfaktoren des q, und jeden genau eben so oft, als die Faktoren zusammengenommen.

Es enthalte $f(\omega)$ den zur Substitution $\varpi_{r,i} = u_i$ gehörenden idealen Primfaktor des q genau m mal, $f_1(\omega)$ enthalte denselben genau m' mal, so ist nach der Definition

$$\Psi(\varpi_r)^m f(\omega) \equiv 0, \text{ mod. } q^m$$

$$\Psi(\varpi_r)^{m'} f_1(\omega) \equiv 0, \text{ mod. } q^{m'};$$

setzt man demnach

$$\Psi(\varpi_r)^m f(\omega) = q^m P(\omega),$$

$$\Psi(\varpi_r)^{m'} f_1(\omega) = q^{m'} P_1(\omega),$$

so ist

$$\Psi(\varpi_r)^{m+m'} f(\omega) f_1(\omega) = q^{m+m'} P(\omega) P_1(\omega);$$

weil ferner $f(\omega)$ den zur Substitution $\varpi_{r,i} = u_i$ gehörenden idealen Primfaktor des q nicht mehr als m mal, $f_1(\omega)$ denselben nicht mehr als m' mal enthält, so folgt, dafs $P(\omega)$ und $P_1(\omega)$ diesen idealen Primfaktor nicht enthalten, also vermöge des vorhergehenden Satzes, dafs das Produkt $P(\omega) P_1(\omega)$ denselben auch nicht enthält, also $\Psi(\varpi_r) P(\omega) P_1(\omega)$ nicht $\equiv 0$ ist mod. q. Darum ist

$$\Psi(\varpi_r)^{m+m'} f(\omega) f_1(\omega) \equiv 0, \text{ mod. } q^{m+m'},$$

aber

$$\Psi(\varpi_r)^{m+m'+1} f(\omega) f_1(\omega) \text{ nicht} \equiv 0, \text{ mod. } q^{m+m'+1},$$

d. h. das Produkt $f(\omega) f_1(\omega)$ enthält diesen idealen Primfaktor genau $m+m'$ mal. Was nun für diesen einen idealen Primfaktor bewiesen ist, gilt offenbar ebenso für alle idealen Primfaktoren der nicht in der Zahl n enthaltenen Primzahlen, ebenso versteht sich von selbst, dafs der Satz auch für ein Produkt beliebig vieler Faktoren giltig bleibt.

Wenn eine complexe Zahl alle verschiedenen idealen Primfaktoren des q enthält, und zwar jeden mindestens m mal, so ist sie durch q^m theilbar. Enthält sie jeden der verschiedenen idealen Primfaktoren des q genau m mal, so erschöpft q^m alle in ihr enthaltenen idealen Primfaktoren des q.

Die Bedingung, dafs $F(\omega)$ alle idealen Primfaktoren des q enthält, und zwar jeden mindestens m mal, wird durch folgende Gleichungen ausgedrückt:

http://rcin.org.pl

$$\Psi(\varpi_{r_1})^m F(\omega) = q^m P_1(\omega)$$
$$\Psi(\varpi_{r_2})^m F(\omega) = q^m P_2(\omega)$$
$$\vdots$$
$$\Psi(\varpi_{r_\nu})^m F(\omega) = q^m P_\nu(\omega).$$

Durch Addition aller dieser Gleichungen hat man, wenn der Kürze wegen

$$\Psi(\varpi_{r_1})^m + \Psi(\varpi_{r_2})^m + \ldots + \Psi(\varpi_{r_\nu})^m = M$$

gesetzt wird

$$MF(\omega) = q^m (P_1(\omega) + P_2(\omega) + \ldots + P_\nu(\omega))$$

Nun ist aber M, als symmetrische Funktion aller primitiven Wurzeln der Gleichung $\omega^n = 1$, eine nichtcomplexe ganze Zahl, von der eben so, wie im vorigen §. für den besonderen Fall $m = 1$ geschehen ist, bewiesen werden kann, dafs sie nicht durch q theilbar ist. Es mufs daher $F(\omega)$ durch q^m theilbar sein. Setzt man also $F(\omega) = q^m f(\omega)$, so ist:

$$\Psi(\varpi_{r_1})^m f(\omega) = P_1(\omega)$$
$$\Psi(\varpi_{r_2})^m f(\omega) = P_2(\omega)$$
$$\vdots$$
$$\Psi(\varpi_{r_\nu})^m f(\omega) = P_\nu(\omega)$$

Wenn nun, wie in dem zweiten Theile des zu beweisenden Satzes vorausgesetzt wird, $F(\omega)$ jeden der idealen Primfaktoren des q genau m mal enthält, so ist keine der Zahlen $P_1(\omega)$, $P_2(\omega) \ldots P_\nu(\omega)$ durch q theilbar, also $f(\omega)$ enthält keinen idealen Primfaktor des q. Somit ist auch dieser zweite Theil des Satzes bewiesen.

Wenn eine complexe Zahl genau m ideale Primfaktoren des q enthält, dieselben mögen verschieden oder auch zum Theil oder alle einander gleich sein, so enthält die Norm derselben den Faktor q genau mt mal.

Es möge $F(\omega)$ genau m ideale Primfaktoren des q enthalten, so enthält die Norm $NF(\omega)$, welche aus den $\phi(n)$ conjugirten complexen Zahlen zusammengesetzt ist, deren genau $m\phi(n)$, und es ist leicht zu übersehen, dafs jeder der ν verschiedenen idealen Primfaktoren des q in der Norm gleich viel mal enthalten sein mufs, also jeder derselben $\frac{m\phi(n)}{\nu}$ mal, oder weil

http://rcin.org.pl

$\nu = \frac{\phi(n)}{t}$, jeder mt mal. Die Norm ist daher, vermöge des vorhergehenden Satzes, theilbar durch q^{mt}, aber durch keine höhere Potenz von q.

§. 6.

Es ist nun auch die besondere Art der idealen Primfaktoren, welche den in der zusammengesetzten Zahl n enthaltenen Primzahlen angehören, in ähnlicher Weise zu behandeln. Sei p eine Primzahl, Faktor von n, und zwar a mal in n enthalten, so dafs $n = p^a \acute{n}$ und $\acute{n}$ nicht weiter durch p theilbar ist, sei ferner $\omega = z\omega'$, wo z eine primitive Wurzel der Gleichung $z^{p^a} = 1$, ω' eine primitive Wurzel der Gleichung $\omega'^{\acute{n}} = 1$ bezeichnet. Die Primzahl p gehöre zum Exponenten Θ, für den Modul $\acute{n}$, so dafs $p^\Theta \equiv 1$, mod. $\acute{n}$, dafs aber keine niedere Potenz als die des Exponenten Θ dieser Congruenz genüge. Sei auch

$$\varpi'_r = \omega'^r + \omega'^{rp}\ \omega'^{rp^2} + \ldots + \omega'^{rp^{\Theta-1}}$$

ebenso bezeichne $\Psi(\varpi'_1)$ dieselbe complexe Zahl für die Wurzel ω' und die Primzahl p, als oben $\Psi(\varpi_1)$ für die Wurzel ω und die Primzahl q, alsdann entsprechen hier ebenfalls den Perioden ϖ'_i bestimmte Congruenzwurzeln u'_i, in der Art, dafs die Congruenz

$$\Psi(\varpi'_1)\,(\varpi'_i - u'_i) \equiv 0, \text{ mod. } p.$$

für alle Werthe des $i = 1, 2, 3, \ldots . \acute{n}$ Statt hat.

Nimmt man in einer complexen Zahl $F(\omega)$ oder $F(z\acute{\omega})$ für z alle verschiedenen primitiven Wurzeln der Gleichung $z^{p^a} = 1$ und bildet das Produkt dieser verschiedenen complexen Zahlen, so soll dasselbe die in Beziehung auf die Wurzel z genommene partielle Norm der complexen Zahl $F(z\acute{\omega})$ genannt und durch $N_z F(z\acute{\omega})$ bezeichnet werden. Diese partielle Norm, als symmetrische Funktion aller primitiven Wurzeln der Gleichung $z^{p^a} = 1$, enthält die Wurzel z selbst nicht weiter in sich, und ist daher eine nur die Wurzel ω' enthaltende complexe Zahl. In gleicher Weise wird die in Beziehung auf die Wurzel ω' genommene partielle Norm, welche durch $N_{\omega'} F(z\acute{\omega})$ bezeichnet werden soll, das Produkt aller derjenigen complexen Zahlen vorstellen, welche man erhält, indem man für ω' alle verschiedenen primitiven Wurzeln der Gleichung $\omega'^{\acute{n}} = 1$ setzt, und wird eine nur die Wurzel z enthaltende complexe Zahl sein. Die vollständige Norm von

http://rcin.org.pl

$F(z\omega')$ erhält man offenbar, indem man von der in Beziehung auf die Wurzel z genommenen Norm noch in Beziehung auf die Wurzel ω' die Norm nimmt, oder auch umgekehrt, indem man zuerst die partielle Norm in Beziehung auf die Wurzel ω' und von dieser die Norm in Beziehung auf z nimmt, welches folgendermaafsen dargestellt werden kann:

$$NF(z\omega') = N_{\omega'} N_z F(z\omega') = N_z N_{\omega'} F(z\omega').$$

Die Primzahl p läfst sich immer in wirkliche complexe Faktoren von der Form $f(z)$ zerlegen, denn man hat bekanntermaafsen:

$$p = \Pi_h (1 - z^h),$$

wo das Produkt Π_h über alle ganzzahligen Werthe des h zu erstrecken ist, welche kleiner als p^a und relative Primzahlen zu p sind, so dafs dieses Produkt aus $p^{a-1}(p-1)$ Faktoren besteht.

Weil ferner

$$1 - z^h = (1 - z)(1 + z + z^2 + \ldots + z^{h-1})$$

und $1 + z + z^2 + \ldots + z^{h-1}$, wenn h nicht durch p theilbar ist, nur eine complexe Einheit darstellt, so hat man ebenfalls

$$p = (1 - z)^{p^{a-1}(p-1)} E(z),$$

wo $E(z)$ eine complexe Einheit bezeichnet.

Eine complexe Zahl $F(\omega')$, welche nur die Wurzel ω', nicht aber die Wurzel z enthält, kann nicht durch $1 - z$ theilbar sein, ohne dafs sie auch durch p theilbar ist.

Ist nämlich $F(\omega')$ durch $1 - z$ theilbar, so ist nothwendig die $p^{a-1}(p-1)$ te Potenz derselben durch $(1 - z)^{p^{a-1}(p-1)}$, also auch durch p theilbar. Da aber oben §. 2. bewiesen worden, dafs eine Potenz einer complexen Zahl der Wurzel ω der Gleichung $\omega^n = 1$ durch eine nicht in n enthaltene Primzahl q nicht theilbar sein kann, ohne dafs diese complexe Zahl selbst durch q theilbar ist, so folgt für den gegenwärtigen Fall, dafs eine Potenz der complexen Zahl $F(\omega')$ der Wurzel ω' der Gleichung $\omega'^{n'} = 1$ durch die nicht in n' enthaltene Primzahl p nicht theilbar sein kann, ohne dafs $F(\omega')$ selbst durch p theilbar ist. Aus $F(\omega') \equiv 0$, mod. $(1 - z)$, folgt daher nothwendigerweise $F(\omega') \equiv 0$, mod. p.

Wenn die complexe Zahl $F(z\omega')$ durch $1 - z$ theilbar ist, so ist offenbar die in Beziehung auf z genommene partielle Norm derselben durch p theilbar, weil $N_z(1 - z) = p$ ist. Die Umkehrung dieses Satzes, nämlich

http://rcin.org.pl

Wenn die in Beziehung auf z genommene partielle Norm einer complexen Zahl $F(z\omega')$ durch p theilbar ist, so ist $F(z\omega')$ selbst durch $1 - z$ theilbar,

wird folgendermaafsen bewiesen. Jede complexe Zahl $F(z\omega')$ genügt, weil $z = 1 - (1 - z)$ ist, der Congruenz

$$F(z\omega') \equiv F(\omega'), \text{ mod. } (1 - z),$$

und hieraus, wenn auf beiden Seiten die Norm in Beziehung auf z genommen wird, folgt:

$$N_z F(z\omega') \equiv F(\omega')^{p^{a-1}(p-1)}, \text{ mod. } (1 - z),$$

also, weil nach der Voraussetzung des Satzes $N_z F(z\omega')$ durch p, und darum auch durch $1 - z$ theilbar ist:

$$F(\omega')^{p^{a-1}(p-1)} \equiv 0, \text{ mod. } (1 - z),$$

woraus nach der Ausführung im vorigen Satze folgt, dafs $F(\omega') \equiv 0$, mod. p, also auch mod. $(1 - z)$, und darum endlich $F(z\omega') \equiv 0$, mod. $(1 - z)$.

Da die Primzahl p, abgesehen von einer Einheit, einer Potenz von $1 - z$ gleich ist, so werden sämmtliche ideale Primfaktoren des p zugleich als ideale Primfaktoren des $1 - z$ angesehen werden können. Dieselben sollen nun folgendermaafsen definirt werden:

Wenn p eine in n enthaltene Primzahl ist und a, n', z, ω', ϖ'_r, u'_i, $\Psi(\varpi'_1)$ die angegebenen Bedeutungen haben, so soll von einer complexen Zahl $F(z\omega')$, welche die Eigenschaft hat, dafs

$$\Psi(\varpi'_r) F(z\omega') \equiv 0, \text{ mod. } (1 - z),$$

ausgesagt werden: sie enthält einen idealen Primfaktor des p, und zwar denjenigen, welcher zur Substitution $\varpi'_{r,i} = u'_i$ gehört. Hat die complexe Zahl $F(z\omega')$ aufserdem die Eigenschaft, dafs

$$\Psi(\varpi'_r)^k F(z\omega') \equiv 0, \text{ mod. } (1 - z)^\mu,$$

aber

$$\Psi(\varpi'_r)^k F(z\omega') \text{ nicht} \equiv 0, \text{ mod. } (1 - z)^{\mu+1},$$

wo

$$kp^{a-1}(p - 1) > \mu,$$

so soll von dieser complexen Zahl ausgesagt werden, dafs sie den zur Substitution $\varpi'_{r,i} = u'_i$ gehörenden idealen Primfaktor des p genau μ mal enthält.

http://rcin.org.pl

Die Anzahl aller verschiedenen idealen Primfaktoren des p, für complexe Zahlen der Wurzel $\omega = z\omega'$ ist hiernach gleich der Anzahl aller verschiedenen Substitutionen von der Form $\varpi'_{r,i} = u_i$, oder was dasselbe ist gleich der Anzahl aller verschiedenen complexen Zahlen $\Psi(\varpi')$; sie ist also nach dem was oben (§. 4.) für die Anzahl der verschiedenen complexen Zahlen $\Psi(\varpi_r)$ gezeigt worden ist, hier, wo p zum Exponenten Θ gehört für den Modul n', gleich $\frac{\Phi(n')}{\Theta}$.

Die Bedingung, dafs die complexe Zahl $F(z\omega')$ den zur Substitution $\varpi'_{r,i} = u'$ gehörenden idealen Primfaktor des p genau μ mal enthalte, kann offenbaar auch folgendermaafsen in Form einer Gleichung dargestellt werden:

$$\Psi(\varpi'_r)^k F(z\omega') = (1 - z)^\mu \chi(z\omega'),$$

wo $\chi(z\omega')$ nicht weiter durch $1 - z$ theilbar ist und $kp^{a-1}(p-1) > \mu$, Nimmt man nun auf beiden Seiten die Norm in Beziehung auf z, so erhält man

$$\Psi(\varpi'_r)^{kp^{a-1}(p-1)} N_z F(z\omega') = p^\mu N_z \chi(z\omega'),$$

und weil $\chi(z\omega')$ nicht durch $1 - z$ theilbar ist, so ist auch $N_z \chi(z\omega')$ nicht durch p theilbar. Hieraus folgt der Satz:

Die complexe Zahl $F(z\omega')$ enthält den zur Substitution $\varpi'_{r,i} = u'_i$ gehörenden idealen Primfaktor des p, für complexe Zahlen der Wurzel $\omega = z\omega'$ genau eben so oft, als $N_z F(z\omega')$ den zur Substitution $\varpi'_{r,i} = u'_i$ gehörenden idealen Primfaktor des p für complexe Zahlen der Wurzel ω' enthält.

Weil $N_z F(z^h\omega') = N_z F(z\omega')$, wenn h nicht durch p theilbar ist, so folgt hieraus unmittelbar der Satz:

Die in der complexen Zahl $F(z\omega')$ enthaltenen idealen Primfaktoren des p bleiben für alle verschiedenen primitiven Wurzeln der Gleichung $z^{p^a} = 1$, welche man für z nehmen mag, stets dieselben.

Ferner gilt auch für die idealen Primfaktoren des p der Satz:

Das Produkt zweier oder mehrerer complexer Zahlen der Wurzel $\omega = z\omega'$ enthält genau dieselben idealen Primfaktoren des p als alle Faktoren zusammengenommen;
hat man nämlich

$$F(z\omega') = f(z\omega') \cdot f_1(z\omega') \cdot f_2(z\omega') \ldots$$

http://rcin.org.pl

so ist auch

$$N_z F(z\omega') = N_z f(z\omega') \cdot N_z f_1(z\omega') \cdot N_z f_2(z\omega') \ldots .$$

Für die in dieser Gleichung enthaltenen Normen in Beziehung auf z, welche nur ω' enthaltende complexe Zahlen sind, gilt aber in Betreff der idealen Primfaktoren der in dem Wurzelexponenten n nicht enthaltenen Primzahl p der in dem vorigen Paragraphen bewiesene Satz: dafs die idealen Primfaktoren des Produktes dieselben sind, als die der einzelnen Faktoren zusammengenommen, woraus vermöge des Satzes, welcher zeigt wie die idealen Primfaktoren des p, welche in $F(z\omega')$ enthalten sind, mit den in $N_z F(z\omega')$ enthaltenen übereinstimmen, die Richtigkeit des aufgestellten Satzes erhellt.

Wenn eine complexe Zahl $F(z\omega')$ alle verschiedenen idealen Primfaktoren des p enthält, und zwar jeden mindestens μ mal, so ist sie durch $(1-z)^\mu$ theilbar.

Nach der Voraussetzung dieses Satzes findet die Congruenz

$$\Psi(\varpi'_r)^k F(z\omega') \equiv 0, \text{ mod. } (1-z)^\mu,$$

statt, für alle Werthe des r, welche verschiedene conjugirte complexe Zahlen $\Psi(\varpi'_r)$ ergeben. Bezeichnet man nun die Summe der $k$ten Potenzen dieser verschiedenen conjugirten complexen Zahlen durch M', so hat man durch Addition dieser Congruenzen

$$M' F(z\omega') \equiv 0, \text{ mod. } (1-z)^\mu$$

und weil M' eine nichtcomplexe ganze Zahl ist, welche nicht durch p und folglich auch nicht durch $1-z$ theilbar ist, so ist:

$$F(z\omega') \equiv 0, \text{ mod. } (1-z)^\mu,$$

wie im Satze behauptet worden. Ich bemerke noch, dafs in dem besonderem Falle, wo μ ein Vielfaches von $p^{c-1}(p-1)$ also $\mu = cp^{c-1}(p-1)$, $F(\omega')$ durch p^c theilbar ist.

Wenn eine complexe Zahl $F(\omega)$ genau μ ideale Primfaktoren des p enthält, welche verschieden oder auch zum Theil oder alle einander gleich sein können, so enthält die vollständige Norm derselben den Faktor p genau $\mu\Theta$ mal.

Es ist nämlich

$$NF(\omega) = N_{\omega'} N_z F(z\omega')$$

und wenn $F(z\omega')$ μ ideale Primfaktoren des p enthält für complexe Zahlen der Wurzel $\omega = z\omega'$, so enthält $N_z F(z\omega')$ genau eben so viele ideale Primfaktoren des p für complexe Zahlen der Wurzel ω'; darum enthält nach dem ent-

http://rcin.org.pl

sprechenden Satze des vorhergehenden Paragraphen $N_{\omega'} N_z F(z\omega')$ den Faktor p genau $\mu\Theta$ mal.

§. 7.

Nachdem nun in den vorhergehenden beiden Paragraphen die Eigenschaften der beiden verschiedenen Arten idealer Primfaktoren, nämlich der allgemeineren, welche den in dem Wurzelexponenten n nicht enthaltenen mit q bezeichneten Primzahlen, und der besonderen, welche den in n enthaltenen, mit p bezeichneten Primzahlen angehören, für sich behandelt worden sind, sollen jetzt die gefundenen Resultate zusammengefafst werden.

Wenn die Norm einer complexen Zahl $F(\omega)$ durch irgend eine der Primzahlen q oder p, d. h. durch eine in dem Wurzelexponenten n nicht enthaltene oder durch eine darin enthaltene, theilbar ist, so enthält $F(\omega)$ nothwendig irgend einen idealen Primfaktor dieser Primzahl; denn die entwickelte ganzzahlige Norm, wenn sie ein Vielfaches von q oder p ist, enthält alle idealen Primfaktoren des q oder p, also die conjugirten complexen Zahlen zu $F(\omega)$, welche die Norm bilden, müssen ebenfalls irgend welche ideale Primfaktoren des q oder p enthalten, nach dem für beide Arten der idealen Primfaktoren geltenden Satze: dafs das entwickelte Produkt genau dieselben idealen Primfaktoren enthält als die Faktoren zusammengenommen. Andererseits ist in den vorhergehenden beiden Paragraphen bewiesen worden, dafs wenn eine complexe Zahl m ideale Primfaktoren des q enthält ihre Norm den Faktor q^{mt} enthalten mufs und ebenso, wenn sie μ ideale Primfaktoren des p enthält, dafs ihre Norm den Faktor $p^{\mu\Theta}$ enthalten mufs. Fafst man diese Resultate zusammen und bezeichnet irgend welche andere Primzahlen derselben Art als q oder p durch $q', q'' \ldots p', p'' \ldots$ und die Exponenten zu welchen erstere für den Modul n, letztere für den Modul n' gehören, beziehungsweise durch $t', t'' \ldots \Theta', \Theta'' \ldots$ so hat man den Satz:

Die Norm einer jeden complexen Zahl $F(\omega)$ ist eine Zahl von der Form

$$NF(\omega) = p^{\mu\Theta} \cdot p'^{\mu'\Theta'} \ldots q^{mt} \cdot q'^{m't'} \cdot q''^{m''t''} \ldots$$

Da die Summe der Zahlen $\mu + \mu' + \ldots + m + m' + m'' + \ldots$, welche für jede bestimmte Zahl $F(\omega)$ nur eine endliche ist, der Anzahl aller in $F(\omega)$ enthaltenen idealen Primfaktoren gleich ist, und da durch die gegebenen Definitionen selbst unzweideutig bestimmt ist: ob und wie viel mal

http://rcin.org.pl

eine gegebene complexe Zahl einen bestimmten idealen Primfaktor enthält, so hat man den Hauptsatz:

Jede gegebene complexe Zahl enthält nur eine endliche Anzahl unveränderlich bestimmter idealer Primfaktoren.

Wenn umgekehrt nicht die complexe Zahl selbst gegeben ist, sondern nur alle idealen Primfaktoren, welche sie enthält, so ist sie dadurch noch nicht vollständig bestimmt, weil die complexen Einheiten, mit welchen sie multiplicirt sein kann, dabei unbestimmt bleiben. Es seien $F(\omega)$ und $F_1(\omega)$ zwei complexe Zahlen, welche beide genau dieselben idealen Primfaktoren enthalten sollen, so ist für dieselben

$$NF(\omega) = NF_1(\omega).$$

Setzt man nun

$$\frac{NF(\omega)}{F(\omega)} = \Phi(\omega),$$

so ist

$$\frac{F_1(\omega)}{F(\omega)} = \frac{F_1(\omega)\,\Phi(\omega)}{NF(\omega)}.$$

Wenn nun $F(\omega)$ so wie $F_1(\omega)$ μ ideale Primfaktoren des p, μ' ideale Primfaktoren des p', m ideale Primfaktoren des q, m' des q', u. s. w. enthält, so ist

$$NF(\omega) = NF_1(\omega) = p^{\mu\Theta} \cdot p'^{\mu'\Theta'} \ldots q^{mt} \cdot q'^{m't'} q''^{m''t''} \ldots .$$

also

$$\frac{F_1(\omega)}{F(\omega)} = \frac{F_1(\omega)\,\Phi(\omega)}{p^{\mu\Theta} \cdot p'^{\mu'\Theta'} \ldots q^{mt} \cdot q'^{m't'} \ldots .}$$

Da nun $F_1(\omega)$ genau dieselben idealen Primfaktoren enthält als $F(\omega)$, so enthält auch $F_1(\omega)\ \Phi(\omega)$ genau dieselben als $F(\omega)\ \Phi(\omega) = NF(\omega)$. Dieses Produkt enthält daher alle idealen Primfaktoren des p, jeden $\mu p^{\alpha-1}\ (p-1)$ mal und ist darum durch $p^{\mu\Theta}$ theilbar; es enthält alle idealen Primfaktoren des p', jeden $\mu' p'^{\alpha'-1}\ (p'-1)$ mal und ist darum durch $p'^{\mu'\Theta'}$ theilbar; es enthält alle idealen Primfaktoren des q, jeden mt mal, und ist darum durch q^{mt} theilbar; es enthält alle idealen Primfaktoren des q', jeden $m't'$ mal, und ist darum durch $q'^{m't'}$ theilbar u. s. w. Das Produkt $F_1(\omega)\ \Phi(\omega)$ ist darum durch $NF(\omega)$ theilbar, folglich

$$\frac{F_1(\omega)}{F(\omega)} = E(\omega)$$

wo $E(\omega)$ eine ganze complexe Zahl ist, oder

$$F_1(\omega) = E(\omega)\,F(\omega)$$

http://rcin.org.pl

Nimmt man endlich auf beiden Seiten die Norm, so erhält man vermöge $NF_1(\omega) = NF(\omega)$

$$NE(\omega) = 1.$$

$E(\omega)$ ist also nur eine complexe Einheit. Diefs giebt den Satz:

Zwei complexe Zahlen, welche genau dieselben idealen Primfaktoren enthalten, unterscheiden sich nur durch complexe Einheiten, mit welchen sie multiplicirt sein können.

Wenn die complexe Zahl $F_1(\omega)$ alle idealen Primfaktoren des $F(\omega)$ enthält, aber aufser diesen vielleicht noch andere, so gelten alle Schlüsse für den Beweis des vorhergehenden Satzes bis dahin, dafs $\frac{F_1(\omega)}{F(\omega)}$ einer ganzen complexen Zahl gleich sein mufs; da aber in diesem Falle $NF_1(\omega)$ nicht gleich $NF(\omega)$ ist, so ist dieser Quotient nicht eine complexe Einheit, sondern er enthält genau alle idealen Primfaktoren, welche $F_1(\omega)$ mehr enthält als $F(\omega)$. Man hat also den Satz:

Eine complexe Zahl ist durch eine andere theilbar, wenn alle idealen Primfaktoren des Divisors auch im Dividendus enthalten sind. Der Quotient enthält alsdann genau den Überschuss der idealen Primfaktoren des Dividendus über die des Divisors.

Wenn es eine wirkliche complexe Zahl $f(\omega)$ giebt, von der Art, dafs sie nur einen einzigen idealen Primfaktor und zwar nur einmal enthält, wenn ferner $F(\omega)$ irgend eine complexe Zahl ist, welche denselben idealen Primfaktor enthält: so ist nach dem soeben bewiesenen Satze $F(\omega)$ theilbar durch $f(\omega)$, und wenn der Quotient durch $Q(\omega)$ bezeichnet wird, so ist

$$F(\omega) = f(\omega) \cdot Q(\omega) .$$

$f(\omega)$ ist aber in diesem Falle nicht mehr ein idealer, sondern ein wirklicher complexer Primfaktor. Hieraus folgt:

Die durch die gegebenen Definitionen bestimmten idealen Primfaktoren der nichtcomplexen Primzahlen stimmen überall wo es wirkliche complexe Primzahlen giebt mit diesen vollkommen überein.

Die idealen Primfaktoren, für welche, wie in dem Vorhergehenden gezeigt worden ist, die Rechnungsregeln genau dieselben sind als für gewöhnliche Primzahlen, da das Produkt mehrerer Faktoren genau dieselben enthält

http://rcin.org.pl

als die Faktoren zusammengenommen, und da jede gegebene complexe Zahl eine endliche unveränderlich bestimmte Anzahl solcher idealer Primfaktoren enthält, welche auch in allen Fällen, wo es wirkliche complexe Primfaktoren giebt, mit diesen vollkommen übereinstimmen, besitzen somit alle wesentlichen Eigenschaften wahrhafter Primfaktoren.

§. 8.

Für die Klassifikation der idealen complexen Zahlen, welche in dem Folgenden gegeben werden soll, ist es von Wichtigkeit die Congruenzbedingungen, durch welche die idealen Primfaktoren bestimmt werden, etwas genauer zu untersuchen. Eine Congruenz unter complexen Zahlen der Wurzel ω, deren Modul eine nichtcomplexe ganze Zahl ist, ist wie oben (§. 1.) gezeigt worden mit $\phi(n)$ Congruenzen unter nichtcomplexen ganzen Zahlen für denselben Modul gleichbedeutend, welche in besonderen Fällen sich auch auf eine geringere Anzahl reduciren können.

Einen solchen besonderen Fall gewährt die Congruenz

$$\Psi(\varpi_r)^m F(\omega) \equiv 0, \text{ mod. } q^m,$$

welche ausdrückt, dafs die complexe Zahl $F(\omega)$ den zur Substitution $\varpi_{r,i} = u_i$ gehörenden idealen Primfaktor des q m mal enthält; die Anzahl der nothwendigen Congruenzbedingungen unter den Coefficienten von $F(\omega)$, welche mit dieser einen für complexe Zahlen gleichbedeutend sind, reducirt sich nämlich immer auf t. Um dieſs zu zeigen, betrachte ich die Gleichung, des Grades t, deren Wurzeln die in der Periode ϖ_1 enthaltenen Wurzeln ω, ω^q, ω^{q^2}, ... $\omega^{q^{t-1}}$ sind, welche ich folgendermaafsen darstelle,

$$\omega^t + P_1\omega^{t-1} + P_2\omega^{t-2} + ... + P_t = 0.$$

Die Coefficienten dieser Gleichung, P_1, P_2, ... P_t, als symmetrische Funktionen aller in einer Periode enthaltenen Wurzeln können offenbaar nur Funktionen der Perioden ϖ_1, ϖ_2 .... ϖ_n sein. Ist nun $F(\omega)$ irgend eine complexe Zahl, so hat man

$$F(\omega) = a + a_1\omega + a_2\omega^2 + ... + a_{\phi(n)-1}\omega^{\phi(n)-1}$$

und man kann nun vermittelst der Gleichung des Grades t alle Potenzen von ω, welche höher sind als die $(t-1)$ te eliminiren und dadurch jede complexe Zahl $F(\omega)$ in die Form setzen:

$$F(\omega) = \Phi(\varpi_1) + \Phi_1(\varpi_1)\omega + \Phi_2(\varpi_1)\omega^2 + ... + \Phi_{t-1}(\varpi_1)\omega^{t-1},$$

http://rcin.org.pl

in welcher $\Phi(\varpi_1)$, $\Phi_1(\varpi_1)$ .... $\Phi_{t-1}(\varpi_1)$ nur die Perioden enthalten und in Beziehung auf die Coefficienten a, a_1, a_2 .... der complexen Zahl $F(\omega)$ lineäre Funktionen sind. Hieraus folgt zunächst, dafs wenn

$$\Psi(\varpi_r)^m \Phi_k(\varpi_1) \equiv 0, \text{ mod. } q^m,$$

für alle Werthe $k = 0, 1, 2, \ldots t-1$, auch

$$\Psi(\varpi_r)^m F(\omega) \equiv 0, \text{ mod. } q^m$$

ist. Um nun zu beweisen, dafs auch umgekehrt aus dieser einen Congruenzbedingung nothwendig jene t Congruenzen folgen, verwandle ich in dem Ausdrucke des $F(\omega)$ nach einander ω in ω^q, ω^{q^2} .... $\omega^{q^{t-1}}$, wobei die Perioden ϖ_1, ϖ_2 .... ϖ_n alle ungeändert bleiben. Es entsteht so folgendes System von t Gleichungen:

$$\begin{aligned}
F(\omega) &= \Phi(\varpi_1) + \omega\,\Phi_1(\varpi_1) + \omega^2\,\Phi_2(\varpi_1) + \ldots + \omega^{t-1}\,\Phi_{t-1}(\varpi_1)\\
F(\omega^q) &= \Phi(\varpi_1) + \omega^q\,\Phi_1(\varpi_1) + \omega^{2q}\,\Phi_2(\varpi_1) + \ldots + \omega^{(t-1)q}\,\Phi_{t-1}(\varpi_1)\\
&\vdots \qquad\qquad \vdots\\
F(\omega^{q^{t-1}}) &= \Phi(\varpi_1) + \omega^{q^{t-1}}\,\Phi_1(\varpi_1) + \omega^{2q^{t-1}}\,\Phi_2(\varpi_1) + \ldots +\\
&\qquad \omega^{(t-1)q^{t-1}}\,\Phi_{t-1}(\varpi_1).
\end{aligned}$$

Betrachtet man $\Phi(\varpi_1)$, $\Phi_1(\varpi_1)$ .... $\Phi_{t-1}(\varpi_1)$ als die Unbekannten dieses Systems und löst dasselbe auf, so erhält man allgemein:

$$D(\omega)\,\Phi_k(\varpi_1) = \overset{k}{A} F(\omega) + \overset{k}{A}_1 F(\omega^q) + \overset{k}{A}_2 F(\omega^{q^2}) + \ldots + \overset{k}{A}_{t-1} F(\omega^{q^{t-1}}),$$

wo die Determinante $D(\omega)$ nach bekannten Regeln der Algebra gleich dem Produkte aller Faktoren von der Form $\omega^{q^r} - \omega^{q^s}$ ist, für $r = 0, 1, 2, \ldots$ $t-1$, $s = 0, 1, 2, \ldots t-1$, mit Ausschlufs der Werthe $r = s$, und wo $\overset{k}{A}$, $\overset{k}{A}_1$ .... $\overset{k}{A}_{t-1}$ complexe ganze Zahlen der Wurzel ω sind. Wenn nun

$$\Psi(\varpi_r)^m F(\omega) \equiv 0, \text{ mod. } q^m,$$

so ist auch allgemein

$$\Psi(\varpi_r)^m F(\omega^{q^h}) \equiv 0, \text{ mod. } q^m,$$

für alle Werthe $h = 0, 1, 2, \ldots t-1$, und darum vermöge der gefundenen Gleichung:

$$D(\omega) \cdot \Psi(\varpi_r)^m \cdot \Phi_k(\varpi_1) \equiv 0, \text{ mod. } q^m,$$

für alle Werthe des $k = 0, 1, 2, \ldots t-1$. Multiplicirt man diese Congruenz noch mit allen zu $D(\omega)$ conjugirten complexen Zahlen so hat man

http://rcin.org.pl

$$\mathfrak{N}D(\omega) \cdot \Psi(\varpi_r)^m \Phi_k(\varpi_1) \equiv 0, \text{ mod. } q^m.$$

Die Norm $\mathfrak{N}D(\omega)$, welche eine nichtcomplexe ganze Zahl ist, enthält, wie leicht zu zeigen ist, niemals den Faktor q; da nämlich $D(\omega)$ nur aus Faktoren von der Form $\omega^{q^r} - \omega^{q^s}$ zusammengesetzt ist, so kann $\mathfrak{N}D(\omega)$ keine anderen Primfaktoren enthalten als solche, welche in n vorkommen, also niemals den Primfaktor q. Es kann daher $\mathfrak{N}D(\omega)$ aus dieser Congruenz hinweggehoben werden, welche alsdann zeigt, dafs wenn

$$\Psi(\varpi_r)^m F(\omega) \equiv 0, \text{ mod. } q^m,$$

nothwendig auch

$$\Psi(\varpi_r)^m \Phi_k(\varpi_1) \equiv 0, \text{ mod. } q^m,$$

ist, für jeden der Werthe $k = 0, 1, 2, \ldots t-1$. Da ferner, wie oben (§. 4.) gezeigt worden, bei Anwendung der Substitution $\varpi_{r,i} = \overset{m}{u}_i$ diese Congruenzen gleichbedeutend sind mit

$$\Phi_k(\overset{m}{u}_\varrho) \equiv 0, \text{ mod. } q^m,$$

für $k = 0, 1, 2, \ldots t-1$, wo $r\varrho \equiv 1$, mod. n, so hat man folgenden Satz:

Die Bedingung, dafs die complexe Zahl $F(\omega)$ den zur Substitution $\varpi_{r,i} = u_i$ gehörenden idealen Primfaktor des q m mal enthalte, oder was dasselbe ist die Congruenz

$$\Psi(\varpi_r)^m F(\omega) \equiv 0, \text{ mod. } q^m,$$

ist gleichbedeutend mit den t Congruenzen

$$\Phi(\overset{m}{u}_\varrho) \equiv 0, \Phi_1(\overset{m}{u}_\varrho) \equiv 0, \ldots \Phi_{t-1}(\overset{m}{u}_\varrho) \equiv 0, \text{ mod. } q^m,$$

welche man erhält wenn man $F(\omega)$ in die Form

$$F(\omega) = \Phi(\varpi_1) + \omega \Phi_1(\varpi_1) + \omega^2 \Phi_2(\varpi_1) + \ldots + \omega^{t-1} \Phi_{t-1}(\varpi_1)$$

setzt, und in diesen Coefficienten der einzelnen Potenzen von ω die Perioden durch die Congruenzwurzeln $\overset{m}{u}_i$ ersetzt, welche ihnen für den Modul q^m entsprechen.

Es sind also t Congruenzen, welche in Beziehung auf die Coefficienten einer complexen Zahl $F(\omega)$ nur lineär sind, für den Modul q^m, nothwendig und hinreichend, damit $F(\omega)$ einen idealen Primfaktor des q m mal enthalte.

In ähnlicher Weise sollen nun auch für die besondere Art der idealen Primfaktoren, welche den in n enthaltenen Primzahlen angehören die Congruenzbedingungen entwickelt werden.

http://rcin.org.pl

Ordnet man die complexe Zahl $F(z\omega')$ nach Potenzen von z allein, so kann man sie in folgende Form setzen:

$$F(z\omega') = A(\omega') + A_1(\omega')\, z + A_2(\omega')\, z^2 + \ldots + A_{\phi-1}(\omega')\, z^{\phi-1},$$

wo der Kürze wegen $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ einfach durch ϕ bezeichnet ist, alle höheren Potenzen von z können nämlich vermittelst der Gleichung

$$z^{p^{\alpha-1}(p-1)} + z^{p^{\alpha-1}(p-2)} + z^{p^{\alpha-1}(p-3)} + \ldots + 1 = 0$$

eliminirt werden. Setzt man ferner $1-(1-z)$ statt z und ordnet nach Potenzen von $1-z$, so erhält man

$$F(z\omega') = B(\omega') + B_1(\omega')\,(1-z) + B_2(\omega')\,(1-z)^2 + \ldots + B_{\phi-1}(\omega')\,(1-z)^{\phi-1}$$

Die Bedingung, dafs $F(z\omega')$ den zur Substitution $\varpi'_r = u'_i$ gehörenden idealen Primfaktor des p μ mal enthalte, nämlich

$$\Psi(\varpi'_r)^k\, F(z\omega') \equiv 0, \text{ mod. } (1-z)^\mu,$$

wo $k\phi > \mu$, giebt daher, wenn der Kürze wegen

$$\Psi(\varpi'_r)^k\, B_h(\omega') = C_h$$

gesetzt wird:

$$C + C_1(1-z) + C_2(1-z)^2 + \ldots + C_{\phi-1}(1-z)^{\phi-1}, \text{ mod. } (1-z)^\mu.$$

Hieraus folgt zunächst, dafs C durch $1-z$ theilbar sein mufs, welches, weil C nur die Wurzel ω', nicht aber z enthält, nicht anders geschehen kann, als dafs C durch p theilbar ist, also den Faktor $1-z$ ϕ mal enthält. Hebt man nun aus dieser Congruenz und dem Modul den Faktor $1-z$ einmal hinweg, so sieht man ferner, dafs auch C_1 durch $1-z$ und also durch p theilbar sein mufs u. s. w. Ist nun $\mu \leqq \phi$, so müssen, wie auf diese Weise gezeigt wird, die ersten μ Coefficienten C, C_1, C_2, $\ldots$ $C_{\mu-1}$ durch p theilbar sein, und wenn dieselben durch p theilbar sind so ist auch dieser Congruenz genügt. Ist aber $\mu > \phi$, so müssen zunächst alle Coefficienten C, C_1, $\ldots$ $C_{\phi-1}$ durch p theilbar sein, man kann daher diesen gemeinschaftlichen Faktor p, oder was dasselbe ist $(1-z)^\phi$, aus der Congruenz und dem Modul hinwegheben und erhält so eine Gleichung derselben Form, für den Modul $(1-z)^{\mu-\phi}$, auf welche man dieselben Schlüsse von Neuem anwenden kann. Ist in dieser $\mu \leqq 2\phi$ so müssen die ersten $\mu - \phi$ Coefficienten nochmals durch p theilbar sein, also C, C_1, $\ldots$ $C_{\mu-\phi-1}$ theilbar durch p^2, und $C_{\mu-\phi}$, $C_{\mu-\phi+1}$, $\ldots$ $C_{\phi-1}$ theilbar durch p. Fährt man, wenn $\mu > 2\phi$ ist, in derselben Weise fort zu schliefsen, so sieht man leicht, dafs allgemein wenn μ in den Grenzen $c\phi$ und $(c+1)\phi$

http://rcin.org.pl

liegt, also $\mu = c\phi + \mu_1$ ist, wo $\mu_1 < \phi$, die ersten μ_1 Coefficienten C, C', $\ldots C_{\mu_1 - 1}$, durch p^{c+1}, die übrigen aber C_{μ_1}, $C_{\mu_1 + 1} \ldots C_{\phi - 1}$ durch p^c theilbar sein müssen, damit dieser Congruenz genügt werde. Dafs aber umgekehrt, wenn diese Bedingungen erfüllt sind dieser Congruenz wirklich genügt wird, ist von selbst klar, da p den Faktor $1 - z^{\phi}$ mal enthält. Betrachtet man noch, dafs die Bedingung $C_k \equiv 0$, mod. p^k nichts anderes ausdrückt, als dafs $B_k(\omega')$ den zur Substitution $\varpi'_{r,i} = u'_i$ gehörenden idealen Primfaktor des p, für complexe Zahlen der Wurzel ω', k mal enthält, so hat man folgendes Resultat.

Die Bedingung, dafs die complexe Zahl $F(z\omega')$ den zur Substitution $\varpi'_{r,i} = u'_i$ gehörenden idealen Primfaktor des p, für complexe Zahlen der Wurzel $\omega = z\omega'$, μ mal enthalte, wo $\mu = c\phi + \mu_1$, $\mu_1 < \phi$, $\phi = p^{a-1}(p-1)$, ist gleichbedeutend damit, dafs von den complexen Zahlen

$$B(\omega'), B_1(\omega'), B_2(\omega') \ldots\ldots B_{\phi-1}(\omega'),$$

welche man erhält indem man $F(z\omega')$ in die Form

$$F(z\omega') = B(\omega') + B_1(\omega')(1-z) + B_2(\omega')(1-z)^2 + \ldots + B_{\phi-1}(\omega')(1-z)^{\phi-1}$$

setzt, die ersten μ_1 den zur Substitution $\varpi'_{r,i} = u'_i$ gehörenden idealen Primfaktor des p für complexe Zahlen der Wurzel ω', $c+1$ mal, die übrigen $\phi - \mu_1$ aber denselben idealen Primfaktor c mal enthalten.

Die Bedingung, dafs $B_k(\omega')$ einen bestimmten idealen Primfaktor des p $c+1$ mal oder c mal enthalte kann aber, wie oben gezeigt worden, da die Primzahl p in dem Wurzelexponenten n' der Wurzel ω' nicht enthalten ist, und p zum Exponenten Θ gehört, mod. n', durch Θ Congruenzen für den Modul p^{c+1} oder p^c ausgedrückt werden, welche in Beziehung auf die ganzzahligen Coefficienten der complexen Zahl $B_k(\omega')$ nur lineär sind. Da nun $B_k(\omega')$ die Coefficienten der ursprünglich gegebenen complexen Zahl $F(z\omega')$ nur in lineärer Weise enthält, so schliefst man:

Die Bedingung, dafs die complexe Zahl $F(z\omega')$ einen bestimmten idealen Primfaktor des p μ mal enthält, wird, wenn $\mu = c\phi + \mu_1$ ist und $\mu_1 < \phi$, $\phi = p^{a-1}(p-1)$, durch μ_1 Θ lineäre Congruenzen für den Modul p^{c+1}, und durch $(\phi - \mu_1)$ Θ lineäre Congruenzen für den Modul p^c, unter den Coefficienten der complexen Zahl $F(z\omega')$, ausgedrückt.

http://rcin.org.pl

§. 9.

Es sollen nun die idealen Primfaktoren und die aus denselben zusammengesetzten oder zusammenzusetzenden idealen complexen Zahlen auf dieselbe Weise bezeichnet werden als die wirklichen, so dafs $f(\omega)$ oder $F(\omega)$ in dem Folgenden complexe Zahlen bezeichnen sollen, welche gewisse gegebene ideale Primfaktoren enthalten, abgesehen davon, ob solche complexe Zahlen wirklich existiren oder nicht. Die Aufgabe, eine wirkliche complexe Zahl zu finden, welche gewisse gegebene ideale Primfaktoren enthält, aber nur diese allein, ist nämlich im Allgemeinen nicht lösbar, wenn man aber zuläfst, dafs dieselbe aufser diesen gegebenen auch andere ideale Primfaktoren enthalten darf, so hat sie stets unendlich viele Lösungen. Diefs kann auch so ausgesprochen werden: es giebt für jede ideale complexe Zahl $F(\omega)$ eine unendliche Anzahl verschiedener idealer Multiplikatoren $F_1(\omega)$ von der Art, dafs das Produkt $F(\omega)\,F_1(\omega)$ eine wirkliche complexe Zahl wird. Wählt man diese idealen Multiplikatoren so aus, dafs die Normen derselben, welche stets wirkliche nichtcomplexe Zahlen sind, möglichst klein werden, so findet man, dafs eine endliche bestimmte Anzahl idealer Multiplikatoren hinreichend ist um alle idealen complexen Zahlen zu wirklichen zu machen.

Um diesen Hauptpunkt der Theorie der hier behandelten complexen Zahlen zu beweisen, stelle ich die ideale complexe Zahl $F(\omega)$ als Produkt der in ihr enthaltenen idealen Primfaktoren dar, nämlich

$$F(\omega) = \phi(\omega)^{\mu} \cdot \phi'(\omega)^{\mu'} \cdots f(\omega)^{m} \cdot f'(\omega)^{m'} \cdot f''(\omega)^{m''} \cdots\cdots$$

wo $\phi(\omega)$ ein bestimmter idealer Primfaktor der in n enthaltenen Primzahl p ist, welche für den Modul n' zum Exponenten Θ gehört, $\phi'(\omega)$ ein idealer Primfaktor, der ebenfalls in n enthaltenen Primzahl p', welche zum Exponenten Θ' gehört u. s. w., ferner $f(\omega)$ ein idealer Primfaktor, der nicht in n enthaltenen, zum Exponenten t gehörenden Primzahl q, $f'(\omega)$ Primfaktor von q', welche zum Exponenten t' gehört, u. s. w. Ferner sei

$$\Phi(\omega) = x + x_1\omega + x_2\omega^2 + \cdots\cdots + x_{\phi(n)-1}\,\omega^{\phi(n)-1}$$

eine wirkliche complexe Zahl, welche alle idealen Primfaktoren des $F(\omega)$ und somit diese ideale complexe Zahl selbst als Faktor enthält, so dafs

$$\Phi(\omega) = F(\omega)\,F_1(\omega),$$

http://rcin.org.pl

wo $F_1(\omega)$ ebenfalls eine ideale complexe Zahl ist. Die Coefficienten der zu suchenden wirklichen complexen Zahl $\Phi(\omega)$, sind hier als die zu bestimmenden Unbekannten durch x, x_1, x_2 . . . . . bezeichnet worden. Die Bedingung, dafs $\Phi(\omega)$ den idealen Primfaktor $\phi(\omega)$ des p μ mal enthalte, wenn $\mu = cp^{a-1}(p-1) + \mu_1$, $\mu_1 < p^{a-1}(p-1)$ wird nun, wie im vorhergehenden §. gezeigt worden, durch $\mu_1 \Theta$ Congruenzen mod. p^{c+1} und durch $(p^{a-1}(p-1) - \mu_1)\Theta$ Congruenzen, mod. p^c, ausgedrückt, welche in Beziehung auf die Coefficienten x, x_1, x_2 . . . . der complexen Zahl $\Phi(\omega)$ nur lineär sind. Von derselben Art sind die Bedingungen dafür, dafs der ideale Primfaktor $\phi'(\omega)$ μ' mal in $\Phi(\omega)$ enthalten sei, u. s. w. Ferner die Bedingung dafür, dafs $\Phi(\omega)$ den idealen Primfaktor $f(\omega)$ der nicht in n enthaltenen Primzahl q m mal enthält wird, wie ebenfalls im vorhergehenden §. gezeigt worden, durch t Congruenzen für den Modul q^m ausgedrückt, ebenso die Bedingung dafs $\Phi(\omega)$ den idealen Primfaktor $f'(\omega)$ des q' m' mal enthält, durch t' Congruenzen für den Modul $q'^{m'}$ u. s. w. Also $\Phi(\omega)$ wird den ganzen idealen Faktor $F(\omega)$ enthalten, wenn gewisse

$\mu_1 \Theta$ Congruenzen mod. p^{c+1} und $(p^{a-1}(p-1) - \mu_1)\Theta$ Congruenzen mod. p^c

$\mu'_1 \Theta'$ - mod. $p^{c'+1}$ - $(p'^{a'-1}(p'-1) - \mu'_1)\Theta'$ - - $p^{c'}$

u. s. w. und

t Congruenzen mod. q^m

t' - - $q'^{m'}$

t'' - - $q''^{m''}$

u. s. w. erfüllt sind, welche Congruenzen in Beziehung auf die Coefficienten x, x_1, x_2, ... der complexen Zahl $\Phi(\omega)$ alle nur lineäre sind. Denkt man sich alle diese Congruenzen auf die Form $X \equiv 0$ gebracht, wo X eine lineäre Funktion von x, x_1, x_2, . . . bezeichnet, so werden, wenn man diesen Coefficienten beliebige ganzzahlige Werthe giebt, diese X im Allgemeinen nicht congruent Null werden, in Beziehung auf die ihnen zugehörenden Moduln, sondern irgend welche Reste geben, welche kleiner als diese Moduln genommen werden können. Die gröfstmögliche Anzahl verschiedener Reste, welche eine solche Congruenz geben kann, ist daher nur gleich dem Modul selbst. Das System aller der Congruenzen, welche die Bedingung ausdrücken, dafs $\Phi(\omega)$ den idealen Faktor $F(\omega)$ enthält, wird demnach höchstens so viele verschiedene Restensysteme geben können, als das Produkt

http://rcin.org.pl

sämmtlicher Moduln Einheiten enthält, also wie aus der Anzahl und den Muduln dieser Congruenzen leicht zu erkennen, nur

$$p^{\mu\Theta} \cdot p'^{\mu'\Theta'} \ldots q^{mt} \cdot q'^{m't'} q''^{m''t''} \ldots$$

welche Anzahl der Norm der idealen complexen Zahl $F(\omega)$ gleich ist. Es giebt also nicht mehr verschiedene Restensysteme der Gröfsen X als $NF(\omega)$. Giebt man nun jedem der $\phi(n)$ Coefficienten $x, x_1, x_2, \ldots$ alle Werthe $0, 1, 2, \ldots k-1$, so hat man $k^{\Phi(n)}$ verschiedene Werthcombinationen dieser Coefficienten und jeder derselben gehört ein bestimmtes Restensystem der Gröfsen X zu. Nimmt man nun k so grofs, dafs

$$k^{\Phi(n)} > NF(\omega),$$

so hat man mehr Werthsysteme dieser Coefficienten als Restensysteme der Gröfsen X, es können also diese Restensysteme, welche jenen Werthsystemen zugehören, nicht alle verschieden von einander sein, sondern für irgend welche zwei verschiedene Werthsysteme der Coefficienten $x, x_1, x_2, \ldots$ müssen alle Gröfsen X für ihre Moduln dieselben Reste geben. Seien nun

$$x = a,\ x_1 = a_1,\ x_1 = a_2, \ldots .$$

und

$$x = b,\ x_1 = b_1,\ x_2 = b_2, \ldots .$$

zwei Werthsysteme der Coefficienten, welche genau dasselbe Restensystem für die Gröfsen X geben, so ist, weil diese Gröfsen X nur lineäre Funktionen von $x, x_1, x_2, \ldots$ sind, das Werthsystem

$$x = a - b,\ x_1 = a_1 - b_1,\ x_2 = a_2 - b_2 \ldots .$$

offenbaar ein solches, für welches alle Reste der X gleich Null, also alle obigen Congruenzen erfüllt werden. Da die Gröfsen $a, a_1, a_2 \ldots$ sowohl als $b, b_1, b_2, \ldots$ alle kleiner als k und nicht negativ sind, so folgt, dafs die Differenzen $a - b, a_1 - b_1, a_2 - b_2, \ldots .$ abgesehen von ihren Vorzeichen alle kleiner als k sein müssen. Also wenn k so grofs angenommen wird, dafs $k^{\Phi(n)} > NF(\omega)$, so wird der Bedingung, dafs eine wirkliche complexe Zahl $\Phi(\omega)$ den idealen Faktor $F(\omega)$ enthält, stets durch solche Werthe der Coefficienten von $\Phi(\omega)$ genügt, welche abgesehen von den Vorzeichen alle kleiner als k sind.

Multiplicirt man nun die complexe Zahl

$$\Phi(\omega) = x + x_1\omega + x_2\omega^2 + \ldots . + x_{\Phi(n)-1}\,\omega^{\Phi(n)-1}$$

mit ihrer reciproken $\Phi(\omega^{-1})$ und nimmt die Summe dieser Produkte in Be-

http://rcin.org.pl

ziehung auf alle Wurzeln der Gleichung $\omega^n = 1$, (nicht in Beziehung auf die primitiven allein,) so erhält man ohne Schwierigkeit

$$\sum_1^n{}_h \Phi(\omega^h)\,\Phi(\omega^{-h}) = n\,(x^2 + x_1^2 + x_2^2 + \ldots + x_{\phi(n)-1}^2).$$

Da nun alle Glieder von der Form $\Phi(\omega^h)\,\Phi(\omega^{-h})$ nur positiv sein können, so ist klar, dafs wenn man die Summe nur auf alle primitiven Wurzeln ω erstreckt, diese kleiner sein mufs als diejenige, welche sich auf alle Wurzeln der Gleichung $\omega^n = 1$ erstreckt, man hat daher

$$\Sigma\,\Phi(\omega)\,\Phi(\omega^{-1}) < n\,(x^2 + x_1^2 + x_2^2 + \ldots + x_{\phi(n)-1}^2),$$

wo die Summe Σ nur auf alle primitiven Wurzeln ω zu beziehen ist. Wendet man nun den bekannten Satz an, dafs das Produkt von m positiven Gröfsen immer kleiner ist als die $m$te Potenz des arithmetischen Mittels derselben, und bemerkt, dafs das Produkt der $\phi(n)$ Gröfsen von der Form $\Phi(\omega)\,\Phi(\omega^{-1})$ gleich dem Quadrate der Norm $N\Phi(\omega)$ ist, so hat man

$$(N\Phi(\omega))^2 < n^{\phi(n)}\,\left(\frac{x^2 + x_1^2 + x_2^2 + \ldots + x_{\phi(n)-1}^2}{\phi(n)}\right).$$

Nimmt man nun für alle Coefficienten x, x_1, x_2, ... die gröfsten Werthe, welche sie überhaupt haben können, nämlich $k-1$, und zieht auf beiden Seiten die Quadratwurzel aus, so hat man

$$N\Phi(\omega) < n^{\frac{1}{2}\phi(n)} \cdot (k-1)^{\phi(n)}.$$

Die Zahl k ist nach der Voraussetzung so grofs zu wählen, dafs

$$k^{\phi(n)} > NF(\omega),$$

wodurch ihre untere Gränze bestimmt wird; bestimmt man aufserdem die obere Gränze dadurch, dafs

$$(k-1)^{\phi(n)} < NF(\omega)$$

sein soll, so ist

$$N\Phi(\omega) < n^{\frac{1}{2}\phi(n)} \cdot NF(\omega)$$

und weil $\Phi(\omega) = F(\omega)\,F_1(\omega)$, also $N\Phi(\omega) = NF(\omega)\,NF_1(\omega)$, so ist endlich

$$NF_1(\omega) < n^{\frac{1}{2}\phi(n)};$$

d. h. die idealen Multiplikatoren, welche mit einer gegebenen idealen complexen Zahl zusammengesetzt, wirkliche complexe Zahlen als Produkte geben, können immer so gewählt werden, dafs die Normen derselben kleiner sind als $n^{\frac{1}{2}\phi(n)}$. Dieser Bedingung aber kann offenbaar nur eine endliche Anzahl idealer Multiplikatoren genügen; man hat daher den Satz:

Alle idealen complexen Zahlen, deren Anzahl unendlich ist, können durch Zusammensetzung mit einer endlichen

http://rcin.org.pl

Anzahl idealer Multiplikatoren zu wirklichen complexen Zahlen gemacht werden.

§. 10.

Auf die Multiplikatoren, welche in endlicher Anzahl ausreichen, um alle idealen complexen Zahlen zu wirklichen zu machen, wird nun die Eintheilung der idealen Zahlen in verschiedene Klassen gegründet, nämlich:

Alle diejenigen idealen Zahlen, welche mit einem und demselben idealen Multiplikator zusammengesezt wirkliche complexe Zahlen als Produkte ergeben, sollen *äquivalente* ideale Zahlen genannt und einer und derselben *Klasse* der ideale Zahlen zugerechnet werden.

Die wirklichen complexen Zahlen werden in diese Klassifikation mit einbegriffen, in welcher sie eine Klasse für sich ausmachen, welche die Hauptklasse genannt wird.

Jeder Multiplikator, welcher eine ideale Zahl zu einer wirklichen macht, macht auch alle dieser äquivalenten idealen Zahlen zu wirklichen. Die Klassifikation der idealen Zahlen ist von der zufälligen Wahl der Multiplikatoren unabhängig.

Sind nämlich $F(\omega)$ und $G(\omega)$ zwei äquivalente ideale Zahlen, so mufs es einen Multiplikator $M(\omega)$ geben, welcher beide zu wirklichen macht. Es sei nun $M_1(\omega)$ ein anderer Multiplikator, welcher $F(\omega)$ zu einer wirklichen complexen Zahl macht, so sind die Produkte $F(\omega)M(\omega)$, $G(\omega)M(\omega)$ und $F(\omega)M(\omega)$ wirkliche complexe Zahlen. Multiplicirt man nun das zweite und dritte dieser Produkte mit einander und dividirt durch das erste, so erhält man als Quotienten $G(\omega)M_1(\omega)$ welches also ebenfalls eine wirkliche complexe Zahl ist. Jeder Multiplikator, welcher eine von zwei äquivalenten idealen Zahlen zu einer wirklichen macht, macht also ebenfalls auch die andere zu einer wirklichen.

Zwei ideale Zahlen, welche einer und derselben dritten äquivalent sind, sind auch unter sich äquivalent.

Denn ein bestimmter idealer Multiplikator, welcher die erste und dritte dieser idealen Zahlen zu wirklichen macht, mufs auch die zweite zu einer wirklichen machen, da auch die zweite der dritten äquivalent ist.

http://rcin.org.pl

Äquivalente ideale Zahlen mit äquivalenten zusammengesetzt, geben äquivalente Produkte.

Sind nämlich $F(\omega)$ und $G(\omega)$ zwei äquivalente ideale Zahlen, $M(\omega)$ ihr gemeinschaftlicher Multiplikator, und auch $F_1(\omega)$ und $G_1(\omega)$ äquivalent und $M_1(\omega)$ ihr gemeinschaftlicher Multiplikator, so ist offenbaar $M(\omega)\,M_1(\omega)$ ein Multiplikator, welcher sowohl $F(\omega)\,F_1(\omega)$ als auch $G(\omega)\,G_1(\omega)$ zu wirklichen complexen Zahlen macht, weshalb diese Produkte äquivalent sind.

Fasst man diese Resultate mit dem zusammen, dafs eine endliche Anzahl von Multiplikatoren hinreicht, um alle idealen Zahlen zu wirklichen zu machen, so schliefst man:

Die Klassen, in welche alle idealen Zahlen sich vertheilen, sind der Zahl nach endlich und vollkommen bestimmt, so dafs jede ideale Zahl nur einer bestimmten Klasse angehört.

Ist $F(\omega)$ irgend eine ideale Zahl, so können die idealen Zahlen der Reihe

$$F(\omega),\ F(\omega)^2,\ F(\omega)^3,\ F(\omega)^4\ \ldots\ldots$$

welche man in's Unendliche fortsetzen kann, nicht alle verschiedenen Klassen angehören, weil die Anzahl der Klassen nur eine endliche ist; es müssen also irgend welche verschiedene Glieder dieser Reihe äquivalent sein, d. h. $F(\omega)^r$ äquivalent $F(\omega)^s$, für gewisse verschiedene Werthe des r und s. Ist nun $M(\omega)$ ein Multiplikator dieser beiden äquivalenten Zahlen, so sind $F(\omega)^r\,M(\omega)$ und $F(\omega)^s\,M(\omega)$ beide wirklich, und darum ist auch der Quotient derselben, nämlich $F(\omega)^{r-s}$ eine wirkliche complexe Zahl. Man hat also den wichtigen Satz:

Jede ideale Zahl wird durch Erhebung zu einer bestimmten Potenz zu einer wirklichen.

Hieraus folgt ferner:

Jede ideale Zahl läfst sich als eine Wurzel aus einer wirklichen darstellen.

Wenn h der niedrigste Exponent ist, für welchen die Potenz $F(\omega)^h$ zu einer wirklichen complexen Zahl wird, so gehören die h Zahlen

$$1,\ F(\omega),\ F(\omega)^2,\ F(\omega)^3,\ \ldots\ldots\ F(\omega)^{h-1}$$

wie leicht zu übersehen ist alle verschiedenen Klassen an. Diese h Klassen können nun entweder alle vorhandenen Klassen idealer Zahlen erschöp-

http://rcin.org.pl

fen, oder auch nicht. Ist das letztere der Fall, so sei $G(\omega)$ eine ideale Zahl, welche keiner dieser h Klassen äquivalent ist, alsdann sind wie leicht zu zeigen auch folgende h ideale Zahlen

$$G(\omega),\ G(\omega)\,F(\omega),\ G(\omega)\,F(\omega)^2,\ \ldots\ .\ G(\omega)\,F(\omega)^{h-1}$$

weder unter sich noch den vorigen äquivalent. Wenn diese $2h$ Klassen nun noch nicht alle vorhandenen erschöpfen und $H(\omega)$ eine ideale Zahl ist, welche keiner derselben äquivalent ist, so wird ebenso leicht gezeigt, dafs folgende h ideale Zahlen

$$H(\omega),\ H(\omega)\,F(\omega),\ H(\omega)\,F(\omega)^2\ .\ .\ .\ .\ .\ H(\omega)F(\omega)^{h-1}$$

weder unter sich noch mit irgend einer der vorhergehenden äquivalent sein können. Fährt man so fort bis alle Klassen der idealen Zahlen erschöpft sind, so erkennt man, dafs dieselben in Gruppen von je h Klassen sich ordnen lassen und man hat den Satz:

Der Exponent der niedrigsten Potenz einer jeder idealen Zahl, welche zu einer wirklichen wird, ist immer ein genauer Theil der Anzahl aller Klassen der idealen Zahlen.

§. 11.

Die in dem Vorhergehenden gegebene Theorie der Zerlegung der complexen Zahlen in ihre idealen Primfaktoren will ich nun noch auf die complexen Zahlen der Kreistheilung anwenden, weil sie allgemeinere Resultate liefert als meine früheren Arbeiten in diesem Gebiete, welche sich auf den Fall beschränkten, dafs der Wurzelexponent der zu Grunde gelegten Wurzel der Einheit eine Primzahl war.

Ist x eine imaginäre Wurzel der Gleichung $x^p = 1$, p eine Primzahl, g eine primitive Wurzel derselben, ω eine primitive Wurzel der Gleichung $\omega^n = 1$, n irgend ein Divisor von $p - 1$ und setzt man

$$(\omega,\ x) = x + \omega x^g + \omega^2 x^{g^2} + \ldots + \omega^{p-2}\, x^{g^{p-2}}$$

so hat man bekanntlich

$$(\omega,\ x)\,(\omega^{-1},\ x) = \omega^{\frac{p-1}{2}}\,p$$

$$\frac{(\omega,\ x)\,(\omega^s,\ x)}{(\omega^{s+1},\ x)} = \psi_s\,(\omega)$$

wo $\psi_s\,(\omega)$ eine nur die Wurzel ω, nicht aber x enthaltende ganze complexe Zahl ist, welche folgendermaafsen dargestellt werden kann:

http://rcin.org.pl

$$\psi_s(\omega) = \Sigma\, \omega^{h + s \text{ Ind. } (g^h + 1)}$$

wo das Summenzeichen auf alle Werthe des $h = 0, 1, 2, \ldots p - 2$ zu beziehen ist, mit Ausschluss des Werthes $h = \frac{p-1}{2}$, und das Zeichen Ind. den Index andeutet für die primitive Wurzel g und den Modul p. Ferner ist:

$$\psi_s(\omega)\, \psi_s(\omega^{-1}) = p$$

und

$$(\omega, x)^n = \omega^{\frac{p-1}{2}} p\, \psi_1(\omega)\, \psi_2(\omega)\, \psi_3(\omega) \ldots \psi_{n-2}(\omega).$$

Ich untersuche nun zunächst die idealen Primfaktoren der complexen Zahl $\psi_s(\omega)$. Diese können, weil $\psi_s(\omega)$ ein Faktor von p ist, nur ideale Primfaktoren des p sein, welches eine nicht in dem Wurzelexponenten n der Wurzel ω enthaltene Primzahl ist. Diese Primzahl p gehört, weil n ein Divisor von $p - 1$ ist, zum Exponenten Eins, für den Modul n, so dafs in dem vorliegenden Falle $t = 1$ ist. Die Perioden ϖ_i werden also nur eingliedrig und sind den Wurzeln ω^i selbst gleich, die ihnen entsprechenden Congruenzwurzeln u_i sind nur die Wurzeln der Congruenz $u^n \equiv 1$, mod. p. Wird der Kürze wegen gesetzt $\frac{p-1}{n} = m$, so ist $u \equiv g^m$ eine primitive Wurzel dieser Congruenz, und wenn man festsetzt, dafs diese der Periode ϖ_1 oder was dasselbe ist der Wurzel ω entspreche, so ist klar, dafs allgemein die Congruenzwurzel g^{mi} die der Wurzel ω^i entsprechende sein wird. Es sei nun $f(\omega)$ ein idealer Primfaktor des p, und zwar der zur Substitution $\omega^i = g^{mi}$, gehörende, so wird der zur Substitution $\omega^{ri} = g^{mi}$ gehörende, wo r eine relative Primzahl zu n sein soll, durch $f(\omega^r)$ zu bezeichnen sein. Bedeutet ϱ diejenige Zahl, welche der Congruenz $r\varrho \equiv 1$, mod. n, genügt, so ist die Substitution $\omega^{ri} = g^{mi}$ gleichbedeutend mit $\omega^i = g^{m\varrho i}$, und weil $\omega^i = g^{m\varrho i}$ offenbaar den idealen Primfaktor $f(\omega^r)$ enthält, so hat man die Congruenz

$$\omega^i \equiv g^{m\varrho i}, \text{ mod. } f(\omega^r),$$

für alle Werthe $i = 1, 2, 3, \ldots n$. Substituirt man nun diese Congruenzwurzeln anstatt der Wurzeln ω^i in dem oben gegebenen Ausdrucke des $\psi_s(\omega)$ so hat man:

$$\psi_s(\omega) \equiv \Sigma_h\, g^{m\varrho(h + s \text{ Ind. } (g^h + 1))}, \text{ mod. } f(\omega^r),$$

und weil

$$g^{\text{Ind. } (g^h + 1)} \equiv g^h + 1$$

für den Modul p, folglich auch für den Modul $f(\omega^r)$, so ist

http://rcin.org.pl

$$\psi_s(\omega) \equiv \Sigma_h\, g^{m\varrho h}\,(g^h+1)^{m\varrho s},\ \text{mod. } f(\omega^r),$$

für $h = 0, 1, 2, \ldots p-2$, wo man nicht weiter nöthig hat den Werth $h = \frac{p-1}{2}$ auszuschliefsen, da das demselben zugehörende Glied dieser Summe congruent Null ist. Anstatt des Potenzexponenten $m\varrho s$ kann nun sein kleinster positiver Rest für den Modul $p-1$ gesetzt werden, welcher wenn σ den kleinsten positiven Rest von ϱs, für den Modul n, bezeichnet, gleich $m\sigma$ ist, so dafs man hat

$$\psi_s(\omega) \equiv \sum_0^{p-2}{}_h\, g^{m\varrho h}\,(g^h+1)^{m\sigma},\ \text{mod. } f(\omega^r).$$

Wird nun die Potenz von g^h+1 nach dem binomischen Lehrsatze entwickelt, so ist

$$(g^h+1)^{m\sigma} = \sum_0^{m\sigma}{}_k\, \frac{\Pi(m\sigma)}{\Pi(k)\,\Pi(m\sigma-k)}\, g^{hk},$$

wo $\Pi(k)$ das Produkt $1.\ 2.\ 3.\ \ldots\ k$ bezeichnet. Man hat daher

$$\psi_s(\omega) \equiv \sum_0^{m\sigma}{}_k \sum_0^{p-2}{}_h\, \frac{\Pi(m\sigma)}{\Pi(k)\,\Pi(m\sigma-k)}\, g^{(m\varrho+k)h},\ \text{mod. } f(\omega^r).$$

Summirt man nun in Beziehung auf alle Werthe des h, so wird diese Summe stets congruent Null, für den Modul p, also auch für den Modul $f(\omega^r)$, mit Ausnahme des einzigen Falles, wo $m\varrho + k$ ein Vielfaches von $p-1$ ist. Da aber der höchste Werth des k, nämlich $m\sigma$, kleiner als $p-1$ ist, und auch $m\varrho < p-1$, so kann dieser Fall nur Statt haben, wenn $m\varrho + k = p-1$ ist. Diese Bedingung kann, da $k \equiv m\sigma$ und $p-1 = mn$ ist, auch als $\varrho + \sigma \equiv n$ dargestellt werden. Ist diese Bedindung $\varrho + \sigma \equiv n$ nicht erfüllt, so hat man

$$\psi_s(\omega) \equiv 0,\ \text{mod. } f(\omega^r)$$

ist sie aber erfüllt, so wird für den Werth $k = p-1-m\varrho$

$$\sum_0^{p-2}{}_h\, g^{(m\varrho+k)h} \equiv -1,\ \text{mod. } p,$$

also

$$\psi_s(\omega) \equiv \frac{-\Pi(m\sigma)}{\Pi m(n-\rho)\,\Pi m(\rho+\sigma-n)},\ \text{mod. } f(\omega^r),$$

welcher Binomialcoefficient nicht durch p, also auch nicht durch $f(\omega^r)$ theilbar ist. In dem Falle, dafs $\varrho + \sigma \geqq n$, ist also

$$\psi_s(\omega) \text{ nicht} \equiv 0,\ \text{mod. } f(\omega^r).$$

Ich bezeichne nun allgemein durch $\left|\frac{b}{a}\right|$ den kleinsten positiven Werth des z, welcher der Congruenz $az \equiv b$, mod. n, genügt; wodurch die Zahlen ϱ und

http://rcin.org.pl

σ als $\varrho = \left|\frac{1}{r}\right|$, $\sigma = \left|\frac{s}{r}\right|$ dargestellt werden, und die Bedingung $\varrho + \sigma < n$ als $\left|\frac{1}{r}\right| + \left|\frac{s}{r}\right| < n$, und bemerke, dafs vermöge der Gleichung $\psi_s(\omega)\,\psi_s(\omega^{-1}) = p$, $\psi_s(\omega)$ keinen idealen Primfaktor des p mehrfach enthalten kann. Demnach kann das gefundene Resultat folgendermaafsen ausgesprochen werden:

Die complexe Zahl $\psi_s(\omega)$ enthält alle diejenigen idealen Primfaktoren des p von der Form $f(\omega^r)$, für welche r, als relative Primzahl zu n und $< n$, der Bedingung

$$\left|\frac{1}{r}\right| + \left|\frac{s}{r}\right| < n$$

genügt, und zwar jeden derselben nur einmal, ausser diesen aber keinen anderen.

Demgemäfs kann man die Zerlegung des $\psi_s(\omega)$ in seine Primfaktoren auch so darstellen:

$$\psi_s(\omega) = E(\omega)\,\Pi f(\omega^r),$$

wo das durch Π angedeutete Produkt auf alle Werthe des r zu erstrecken ist, welche der Bedingung

$$\left|\frac{1}{r}\right| + \left|\frac{s}{r}\right| < n$$

genügen, und wo $E(\omega)$ eine complexe Einheit darstellt.

Aus der gefundenen Zerlegung der complexen Zahl $\psi_s(\omega)$ wird nun auch die Zerlegung von $(\omega, x)^n$ leicht zusammengesetzt, vermittelst der Formel

$$(\omega, x)^n = \omega^{\frac{p-1}{2}}\, p \,.\, \psi_1(\omega)\,\psi_2(\omega)\,\psi_3(\omega) \,.\,.\,.\,.\, \psi_{n-2}(\omega)$$

Die Anzahl, wie viel mal der ideale Primfaktor $f(\omega^r)$ in diesem Produkte enthalten ist, ist nach dem Obigen gleich der Anzahl der Werthe des s aus der Reihe $s = 1, 2, 3, \ldots\ldots n-2$, für welche $\left|\frac{1}{r}\right| + \left|\frac{s}{r}\right| < n$ ist, vermehrt um eine Einheit, welche daher kommt, dafs der Faktor p dieses Ausdrucks den idealen Primfaktor $f(\omega^r)$ einmal enthält. Es ist nun $\left|\frac{1}{r}\right| + \left|\frac{n-1}{r}\right| = n$, woraus folgt, dafs alle Werthe des $\left|\frac{s}{r}\right|$, welche kleiner sind als $\left|\frac{n-1}{r}\right|$ der Bedingung $\left|\frac{1}{r}\right| + \left|\frac{s}{r}\right| < n$ genügen müssen, aufser diesen aber keine. Die Anzahl dieser Werthe des $\left|\frac{s}{r}\right|$ und folglich auch die des s ist aber gleich $\left|\frac{n-1}{r}\right| - 1$, und wenn diese um eine Einheit vermehrt wird, so hat man $\left|\frac{n-1}{r}\right|$

http://rcin.org.pl

gleich der Anzahl wie viel mal der ideale Primfaktor $f(\omega^r)$ in $(\omega,x)^n$ enthalten ist. Das gefundene Resultat kann nun in folgender Form dargestellt werden:

$$(\omega, x)^n = E(\omega) \Pi f(\omega^r)^{\left|\frac{n-1}{r}\right|}$$

wo das Produkt auf alle ganzzahligen Werthe des r zu erstrecken ist, welche kleiner als n und relative Primzahlen zu n sind und $E(\omega)$ eine complexe Einheit bedeutet.

Verwandelt man ω in ω^{-1} und setzt $n - r$ statt r, so kann man dieselbe Formel auch so darstellen:

$$(\omega^{-1}, x)^n = E(\omega^{-1}) \Pi f(\omega^r)^{\left|\frac{1}{r}\right|}.$$

Es kann hier auch die Aufgabe gestellt werden den Lagrangeschen Ausdruck (ω, x) selbst, und nicht nur dessen $n$te Potenz, welche von x unabhängig ist, in die idealen Primfaktoren zu zerlegen. Dieser Ausdruck ist nämlich eine complexe Zahl der Wurzel $x\omega$ der Gleichung $(x\omega)^{p^n} = 1$ und gehört somit den in der gegenwärtigen Theorie behandelten complexen Zahlen an. Derselbe kann nur ideale Primfaktoren des p enthalten, weil $(\omega, x)\,(\omega^{-1}, x) = \omega^{\frac{p-1}{2}}\, p$ ist, p ist hier aber eine in dem Wurzelexponenten pn enthaltene Primzahl, so dafs es sich also in diesem nur um die idealen Primfaktoren der besonderen Art handelt, deren Eigenschaften im §. 6. entwickelt worden sind. Die in Beziehung auf x allein genommene Norm von (ω, x) ist, wie aus der Eigenschaft dieses Ausdruks

$$(\omega, x^{g^h}) = \omega^{-h}\ (\omega, x)$$

folgt, gleich der $(p-1)$ten Potenz desselben, d. h.

$$N_x(\omega, x) = (\omega, x)^{p-1};$$

die oben gefundene Zerlegung des $(\omega, x)^n$ in seine idealen Primfaktoren giebt daher folgende Zerlegung der Norm

$$N_x(\omega, x) = E(\omega)^m \Pi f(\omega^r)^{m\left|\frac{n-1}{r}\right|},$$

wo $m = \left|\frac{p-1}{n}\right|$. Wendet man nun auf die complexe Zahl (ω, x) den Satz an, dafs eine solche complexe Zahl die idealen Primfaktoren des p für complexe Zahlen der Wurzel $x\omega$ genau eben so oft enthält, als ihre in Beziehung auf x allein genommene Norm die entsprechenden, derselben Substitution angehörenden idealen Primfaktoren des p für complexe Zahlen der Wurzel

http://rcin.org.pl

ω enthält, und bezeichnet durch $f(x\omega^r)$ den idealen Primfaktor des p, welcher der Substitution $\omega^{r\,i} = g^{m\,i}$ angehört, welcher also dem idealen Primfaktor $f(\omega^r)$, für complexe Zahlen der Wurzel ω entspricht, so erkennt man aus der Zerlegung von $N_x(\omega, x)$ unmittelbar, dafs (ω, x) den idealen Primfaktor $f(x\omega^r)$ genau $m\left|\frac{n-1}{p}\right|$ mal enthalten mufs, und man hat folgende Zerlegung

$$(\omega, x) = E(x\omega)\,\Pi\, f(x\omega^r)^{m\left|\frac{n-1}{r}\right|}$$

wo das Produktzeichen ebenfalls auf alle Werthe des r zu beziehen ist, welche kleiner als n sind und relative Primzahlen zu n, und $E(x\omega)$ eine complexe Einheit bezeichnet.

GABINET MATEMATYCZNY
Towarzystwa Mańkowego Warszawskie

INSTYTUT MAT. BIBLIOTEKA

http://rcin.org.pl

http://rcin.org.pl