# 1.

# Abrifs einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus.

(Von Herrn *Dedekind* in Göttingen.)

Es ist meine Absicht, dem in der Ueberschrift bezeichneten Gegenstande, welcher, von *Gaufs* zuerst angeregt, später mit Erfolg von *Galois, Serret, Schönemann* wieder aufgenommen ist, eine einfache zusammenhängende Darstellung zu widmen, welche sich streng an die Analogie mit den Elementen der Zahlentheorie binden soll. Diese ist in der That so durchgreifend, dafs es mit Ausnahme einiger unserm Gegenstande eigenthümlicher Untersuchungen nur einer Wortänderung in den Beweisen der Zahlentheorie bedarf. Ich folge genau dem Gange, welchen *Dirichlet* in seinen Vorlesungen über die Zahlentheorie (oder in seiner kurzen Darstellung der Theorie der complexen Zahlen im 24sten Bande dieses Journals) eingeschlagen hat. In Rücksicht hierauf wird man es nicht tadeln, dafs ich meist nur die Hauptmomente der Beweise hervorhebe, da gröfsere Ausführlichkeit für den Kenner der Zahlentheorie, welche hier vorausgesetzt wird, ermüdend sein müfste.

Die hier dargestellte Theorie, deren Erweiterungen auf der Hand liegen, ist vielfacher Anwendungen fähig, namentlich auf die Algebra, wie ich in einer spätern Abhandlung zeigen werde; zunächst schien es mir zweckmäfsig, dieselbe ohne alle Einmischung algebraischer Principien abzuhandeln.

## Gebiet der Untersuchung; Definitionen und Fundamentalsätze.

### 1.

Unter einer *Function* einer Variabeln $x$ wird hier immer eine ganze rationale Function von $x$ verstanden, deren Coefficienten reelle ganze Zahlen sind. Es werden die Eigenschaften solcher Functionen untersucht in Bezug auf einen *Modulus,* der eine reelle *Primzahl* $p$ ist. Zwei Functionen $A$, $B$ heifsen *congruent* in Bezug auf den Modul $p$, in Zeichen

$$A \equiv B \pmod{p},$$

wenn sämmtliche Coefficienten der nach Potenzen von $x$ geordneten Differenz $A-B$ durch $p$ theilbar sind, oder, was dasselbe sagt, wenn die Coefficienten gleich hoher Potenzen von $x$ in den beiden Functionen paarweise einander congruent sind in Bezug auf den Modulus $p$. Es ist daher diese Congruenz nur ein Ausdruck für die *Identität*

$$A = B + p.C,$$

in welcher $C$ eine beliebige Function bedeutet. Hieraus gehen sogleich die beiden folgenden Sätze hervor:

Man darf in jeder Congruenz zwischen zwei Functionen die Variabeln $x$ durch eine beliebige Function von $x$ ersetzen.

Man darf jede Congruenz beliebig oft nach der Variabeln $x$ differentiiren.

Ebenso leuchten folgende Sätze ein, in welchen der Modulus $p$ unveränderlich beibehalten wird:

Ist $A \equiv A'$, $B \equiv B'$; so ist auch $A \pm B \equiv A' \pm B'$, ferner $AB \equiv A'B'$, ferner $A^n \equiv A'^n$, wo $n$ eine positive ganze Zahl bedeutet; und allgemein: Sind die beiden Seiten einer Congruenz ganze rationale Functionen (mit ganzen Zahlcoefficienten) von einer Reihe von Functionen $A$, $B$, $C$ etc. der Variabeln $x$, so darf man dieselben (an beliebigen Stellen) durch ihnen resp. congruente Functionen $A'$, $B'$, $C'$ etc. ersetzen.

## 2.

Der Exponent der höchsten Potenz von $x$ in einer Function, deren Coefficient nicht durch den Modul theilbar ist, heifse der *Grad* der Function. Aus dieser Definition, welche für alle Functionen gilt, die nicht $\equiv 0 \pmod{p}$ sind, ergiebt sich, dafs alle die unendlich vielen einander congruenten Functionen einen und denselben Grad haben. Ist ferner $\alpha$ der Grad von $A$, $\beta$ der Grad von $B$, so ist $\alpha + \beta$ der Grad von $AB$; denn das Product zweier durch eine Primzahl $p$ nicht theilbaren Zahlen-Coefficienten ist ebenfalls nicht theilbar durch $p$. Hieraus folgt weiter: Ist $AB \equiv 0 \pmod{p}$, so ist mindestens eine der beiden Functionen $A$, $B \equiv 0 \pmod{p}$; und ferner: Ist $AB \equiv A'B'$, und $A \equiv A'$ *nicht* $\equiv 0 \pmod{p}$, so ist $B \equiv B' \pmod{p}$; denn es ist $AB \equiv AB'$, oder $A(B-B') \equiv 0 \pmod{p}$. Dieser Satz giebt daher die Bedingung für die Berechtigung zur Division einer Congruenz durch eine andere. Ferner ist leicht zu sehen, dafs die Anzahl der einander nicht congruenten (*incongruenten*) Functionen vom Grade $\alpha$ gleich $(p-1)p^\alpha$ ist; denn der Coefficient von $x^\alpha$ kann $p-1$, der jeder niedrigern Potenz kann $p$

nach dem Modul $p$ incongruente Werthe haben, und der Coefficient jeder höhern Potenz ist $\equiv 0 \pmod{p}$. Dies Resultat gilt auch für den Fall $\alpha = 0$, insofern bei den Functionen, welche $\equiv 0$ sind, überhaupt von einem Grade keine Rede ist.

## 3.

Sind $A, B, C$ drei solche Functionen von $x$, dafs $A \equiv BC \pmod{p}$, so heifsen $B, C$ (oder alle diesen congruente Functionen) ***Divisoren*** oder ***Factoren*** von $A$ (oder jeder mit $A$ congruenten Function) in Bezug auf den Modul $p$. Gleichbedeutend sind die Ausdrücke: $A$ ist ein ***Multiplum*** von $B, C$; oder: $A$ ist ***theilbar*** durch $B, C$. Diese Theilbarkeit nach einem Modulus ist natürlich nicht mit der algebraischen Theilbarkeit zu verwechseln, obwohl aus der letztern stets die erstere folgt. Offenbar kann der Grad eines Divisors $B$ von $A$ nicht höher sein als der Grad von $A$. Jede Function ist theilbar durch jede der $p-1$ incongruenten Functionen vom Grade Null; denn jede der letztern ist einer durch $p$ nicht theilbaren Zahl $a$ congruent; bestimmt man nun $a'$ so, dafs $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a.a'A$, wo $A$ jede beliebige Function bedeutet. Aufser diesen $p-1$ Functionen vom Grade Null hat keine andere die Eigenschaft, Divisor von jeder beliebigen Function zu sein; denn eine Function, deren Grad höher als Null ist, kann nicht mehr Divisor der Functionen vom Grade Null sein. Man kann deshalb (zufolge der Analogie mit ähnlichen Untersuchungen) diese $p-1$ incongruenten Functionenclassen vom Grade Null ***Einheiten*** nennen.

Man kann jede Function vom Grade $\alpha$ congruent setzen dem Producte aus einer bestimmten Function vom Grade Null und einer Function vom Grade $\alpha$, in welcher der Coefficient von $x^\alpha \equiv 1 \pmod{p}$ ist (solche Functionen sollen ***primäre*** heifsen); denn ist $a$ der durch $p$ nicht theilbare Coefficient von $x^\alpha$ in $A$, und $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a.a'A$, worin $a'A$ eine primäre Function ist. — Die Anzahl der incongruenten primären Functionen vom Grade $\alpha$ ist gleich $p^\alpha$.

Aus der Definition der Multipla ergeben sich unmittelbar die beiden folgenden Sätze: Ist eine Function ein Multiplum von einer zweiten, diese ein Multiplum von einer dritten, diese von einer vierten u. s. w., so ist jede frühere in der Reihe dieser Functionen ein Multiplum von jeder spätern. — Die Summe und die Differenz zweier Multipla von einer Function sind selbst wieder Multipla derselben Function.

## 4.

Von grofser Bedeutung für die spätern Untersuchungen ist folgende *Aufgabe:* Zu untersuchen, ob zwei gegebene Functionen $A$, $A'$ nach dem Modul $p$ gemeinschaftliche Divisoren haben.

Zunächst läfst sich zeigen, dafs man stets eine Congruenz von der Form

$$A \equiv QA' + A'' \pmod{p}$$

aufstellen kann, in welcher $Q$, $A''$ zwei neue Functionen sind, deren letztere $A''$ einen niedrigern Grad als $A'$ hat, oder gar $\equiv 0 \pmod{p}$ ist. Denn es sei $\alpha$ der Grad von $A$, $\alpha'$ der von $A'$; im Fall nun $\alpha < \alpha'$ ist, braucht man nur $Q \equiv 0$, $A'' \equiv A \pmod{p}$ zu setzen; ist aber $\alpha \geqq \alpha'$, so kann man die Zahl $q$ so bestimmen, dafs $A - qx^{\alpha-\alpha'}.A'$ von niedrigerm Grade $\alpha_1$ als $\alpha$ ist; ist dann $\alpha_1$ auch $< \alpha'$, so ist das Ziel schon erreicht, wenn man $Q \equiv qx^{\alpha-\alpha'}$ setzt; ist aber $\alpha_1 \geqq \alpha'$, so verfährt man mit der Function $A - qx^{\alpha-\alpha'}.A'$ ebenso, wie bei dem ersten Schritte mit $A$, man bestimmt $q_1$ so, dafs $A - qx^{\alpha-\alpha'}.A' - q_1 x^{\alpha_1-\alpha'}.A'$ von niedrigerm Grade ist als $\alpha_1$ u. s. f. bis man zu einer Function von niedrigerm Grade als $\alpha'$ gelangt, was nach einer endlichen Anzahl von Operationen geschehen mufs. Man setzt dann

$$Q \equiv qx^{\alpha-\alpha'} + q_1 x^{\alpha_1-\alpha'} + \text{etc.} \pmod{p}$$

und dann ist $A'' \equiv A - QA'$ von niedrigerm Grade als $\alpha'$. W. Z. B. W.

Aus der so gebildeten Congruenz folgt nun unmittelbar, dafs jeder gemeinschaftliche Divisor von $A$, $A'$ auch Divisor von $A''$, und umgekehrt dafs jeder gemeinschaftliche Divisor von $A'$, $A''$ auch Divisor von $A$ sein mufs. Man braucht daher die Operation nur fortzusetzen und ein System von Congruenzen zu bilden:

$$\left.\begin{aligned} A &\equiv QA' + A'' \\ A' &\equiv Q'A'' + A''' \\ &\cdots\cdots\cdots \\ A^{(\nu-2)} &\equiv Q^{(\nu-2)}A^{(\nu-1)} + A^{(\nu)} \\ A^{(\nu-1)} &\equiv Q^{(\nu-1)}A^{(\nu)} \end{aligned}\right\} \pmod{p}$$

in welchem die Grade $\alpha'$, $\alpha''$ etc. eine abnehmende Reihe bilden, woraus von selbst folgt, dafs nach einer endlichen Anzahl von Operationen es geschehen mufs, dafs eine Function $A^{(\nu-1)}$ durch die nächstfolgende $A^{(\nu)}$ theilbar ist. Schreitet man von der ersten bis zur letzten Congruenz fort, so ergiebt sich, dafs jeder gemeinschaftliche Divisor von $A$, $A'$ auch Divisor von $A^{(\nu)}$ sein mufs; verfolgt man den umgekehrten Weg, so ergiebt sich, dafs $A^{(\nu)}$ Divisor

aller vorhergehenden Functionen und folglich auch gemeinschaftlicher Divisor der beiden Functionen $A$, $A'$ ist. Es heifse daher $A^{(\nu)}$ ein *gröfster* gemeinschaftlicher Divisor von $A$, $A'$. Multiplicirt man $A^{(\nu)}$ mit einer beliebigen Function vom Grade Null (mit einer Einheit), so hat das Product offenbar dieselbe Eigenschaft wie $A^{(\nu)}$; es giebt daher $p-1$ incongruente gröfste gemeinschaftliche Divisoren desselben Grades, und ein einziger unter diesen ist primär.

Drückt man vermöge der vorletzten Congruenz $A^{(\nu)}$ durch $A^{(\nu-1)}$ und $A^{(\nu-2)}$, diese vermöge der vorhergehenden Congruenzen durch die vorhergehenden Functionen aus, so kommt man zuletzt auf eine Congruenz von der Form

$$G.A+G'.A' \equiv A^{(\nu)} \pmod{p},$$

welche also stets möglich ist, wenn $A^{(\nu)}$ gröfster gemeinschaftlicher Divisor von $A$, $A'$ ist.

## 5.

Ist der gröfste gemeinschaftliche Divisor $A^{(\nu)}$ der Functionen $A$, $A'$ vom Grade Null (also $\equiv 1 \pmod{p}$, wenn er primär ist), so heifsen $A$, $A'$ *relativ prim* gegen einander.

Aus dieser Definition folgt der *Hauptsatz:* Sind $A$, $A'$ zwei relative Primfunctionen, und ist $M$ eine beliebige Function, so ist jeder gemeinschaftliche Divisor der beiden Functionen $AM$, $A'$ zugleich gemeinschaftlicher Divisor von $M$, $A'$. Denn multiplicirt man die Reihe der Congruenzen, durch welche die Functionen $A$, $A'$, $A''$ ... $A^{(\nu)}$ zusammenhängen, mit $M$, so ergiebt sich unmittelbar, dafs jeder gemeinschaftliche Divisor von $AM$, $A'$ auch Divisor von $A''M$, $A'''M$ ... $A^{(\nu)}M$ und folglich auch (da der Annahme nach $A^{(\nu)}$ vom Grade Null ist) von $M$, also gemeinschaftlicher Divisor von $M$, $A'$ ist. (Dies folgt auch unmittelbar aus der Congruenz $GAM+G'MA' \equiv A^{(\nu)}M$.)

Die wichtigsten Specialfälle dieses Satzes sind die folgenden: Ist auch $M$ relativ prim gegen $A'$, so ist der gröfste gemeinschaftliche Divisor von $M$ und $A'$, und folglich auch der von $AM$ und $A'$ eine Function vom Grade Null, d. h. $AM$ und $A'$ sind relativ prim gegen einander; und hieraus ergiebt sich der Satz: Wenn zwei Reihen von Functionen so beschaffen sind, dafs jede Function der einen Reihe relativ prim gegen jede Function der andern Reihe ist, so ist das Product aus sämmtlichen Functionen der einen Reihe relativ prim gegen das Product aus sämmtlichen Functionen der andern Reihe.

Eine zweite Specialisirung ist die folgende. Ist wieder $A$ relativ prim gegen $A'$, und ist $AM$ durch $A'$ theilbar, so ist $A'$ als gemeinschaftlicher

Divisor von $AM$, $A'$ auch gemeinschaftlicher Divisor von $M$, $A'$, also Divisor von $M$.

Hieraus folgt weiter: Ist jede der Functionen $A$, $B$, $C$ etc. relativ prim gegen jede der andern, und ist ferner eine Function $M$ durch jede der Functionen $A$, $B$, $C$ etc. theilbar, so ist $M$ auch durch das Product $ABC\ldots$ theilbar. Denn der Annahme nach ist $M \equiv GA$ durch $B$ theilbar, folglich ist, da $A$ relativ prim gegen $B$, $G \equiv HB$, also $M \equiv HAB$ u. s. w.

## 6.

Eine Function, welche nach dem Modul $p$ nur solche Divisoren hat, die entweder ihr selbst, oder Functionen vom Grade Null (d. h. Einheiten), oder Producten aus beiden congruent sind (denn jede Function hat alle diese Divisoren), heifst (*irreductibel* oder) eine *Primfunction* nach dem Modul $p$; jede andere heifst (*reductibel* oder) *zusammengesetzt*. Es leuchtet ein, dafs eine beliebige Function entweder durch eine bestimmte Primfunction theilbar, oder relativ prim gegen dieselbe ist. Ist daher ein Product $AB$ durch eine Primfunction $P$ theilbar, so ist mindestens einer der Factoren $A$, $B$ für sich allein durch $P$ theilbar; denn ist $A$ nicht durch $P$ theilbar, so ist $A$ relativ prim gegen $P$, und folglich $B$ durch $P$ theilbar. Derselbe Satz gilt für ein Product aus beliebig vielen Functionen.

Es leuchtet ein, dafs jede beliebige Function $M$ sich darstellen läfst als Product aus Potenzen von Primfunctionen, welche unter einander incongruent sind, und deren Anzahl eine endliche ist (wenn der Grad von $M$ endlich ist); und zwar ist *wesentlich* nur eine einzige solche Darstellung möglich; d. h. wenn in der einen Zerfällung $a$ Factoren vorkommen, welche einer und derselben Primfunction $A$ congruent sind, so werden auch in jeder andern Zerfällung $a$ Factoren vorkommen, welche derselben Primfunction $A$ oder einem Product aus $A$ in eine Einheit congruent sind. Man kann die Primfunctionen sämmtlich primär annehmen; ist dann

$$M \equiv \varepsilon A^a B^b C^c \ldots \pmod{p}$$

wo $\varepsilon$ eine Einheit, $A$, $B$, $C$ etc. incongruente primäre Primfunctionen, $a$, $b$, $c$ etc. positive ganze Zahlen bedeuten, so ist jeder primäre Divisor $D$ von $M$ von der Form

$$D \equiv A^{a'} B^{b'} C^{c'} \ldots \pmod{p}$$

wo $a'$, $b'$, $c'$ etc. die Null oder positive ganze Zahlen bedeuten, welche resp.

nicht gröfser als $a$, $b$, $c$ etc. sind. Die Anzahl der incongruenten primären Divisoren von $M$ ist demnach $= (a+1)(b+1)(c+1)$.

Wenn eine Function $M$ einen Divisor $D$ $m$mal enthält, d. h. wenn $M \equiv GD^m \pmod{p}$, so folgt durch Differentiation

$$\frac{dM}{dx} \equiv \left(G.m\frac{dD}{dx} + D.\frac{dG}{dx}\right)D^{m-1} \pmod{p};$$

also enthält die Derivirte von $M$ denselben Divisor $D$ mindestens $(m-1)$mal (sie kann ihn auch öfter enthalten). Ist daher eine Function relativ prim gegen ihre erste Derivirte, so ist sie einem Product aus lauter incongruenten Primfunctionen congruent.

---

## Allgemeine Sätze über die Congruenzen, welche sich auf einen doppelten Modulus beziehen.

### 7.

Die vorhergehenden Sätze entsprechen vollständig denen über die Theilbarkeit der Zahlen in der Weise, dafs das ganze System der unendlich vielen einander nach dem Modulus $p$ congruenten Functionen einer Variabeln sich hier verhält, wie eine einzige bestimmte Zahl in der Zahlentheorie, indem jede einzelne Function eines solchen Systems jede beliebige andere desselben Systems in jeder Beziehung vollständig ersetzt; eine solche Function ist der Repräsentant der ganzen Classe; jede Classe hat ihren bestimmten Grad, ihre bestimmten Divisoren u. s. w., und alle diese Merkmale kommen jedem einzelnen Gliede einer Classe in derselben Weise zu. Das System der unendlich vielen incongruenten Classen — unendlich vielen, da der Grad unbegrenzt wachsen kann — entspricht der Reihe der ganzen Zahlen in der Zahlentheorie. Der Congruenz der Zahlen entspricht hier Congruenz von Functionenclassen nach einem doppelten Modulus in der folgenden Weise.

Zwei Functionenclassen oder deren Repräsentanten $A$, $B$ heifsen *congruent* in Bezug auf die Functionenclasse, deren Repräsentant $M$, in Zeichen

$$A \equiv B \pmod{p, M} \text{ oder } A \equiv B \pmod{M},$$

wenn die Differenz $A-B$ nach dem Modul $p$ durch $M$ theilbar ist.

Eine solche Congruenz zweier Functionen $A$, $B$ in Bezug auf eine dritte $M$ ist also nur ein anderer Ausdruck für die Congruenz

$$A \equiv B + CM \pmod{p},$$

und hieraus ergiebt sich, dafs man $A$, $B$, $M$ durch beliebige Functionen $A'$, $B'$, $M'$ ersetzen kann, welche resp. jenen nach dem Modul $p$ congruent sind. Ferner leuchtet ein, dafs man in einer solchen Congruenz die Variabele $x$ in den drei Functionen $A$, $B$, $M$ durch eine beliebige Function von $x$ ersetzen kann.

Aus der Definition dieser Congruenzen ergeben sich folgende Sätze: Ist $A \equiv A'$ (mod. $M$), $B \equiv B'$ (mod. $M$); so ist $A \pm B \equiv A' \pm B'$ (mod. $M$), ferner $AB \equiv A'B'$ (mod. $M$), ferner $A^n \equiv A'^n$ (mod. $M$), wo $n$ eine positive ganze Zahl bedeutet. Und allgemein: Sind die beiden Seiten einer Congruenz nach dem Modulus $M$ ganze rationale Functionen (mit ganzen Zahlcoefficienten) von Functionen, so darf man jede der letztern (an beliebigen Stellen) durch eine andere ersetzen, welche ihr nach dem Modulus $M$ congruent ist.

Ist ferner $AB \equiv 0$ (mod. $M$), und $A$ relativ prim gegen $M$, so ist auch $B \equiv 0$ (mod. $M$); allgemeiner: ist $AB \equiv A'B'$ (mod. $M$) und $A \equiv A'$ (mod. $M$) und $A$ relativ prim gegen $M$, so ist auch $B \equiv B'$ (mod. $M$).

Sind endlich $A$, $A'$ congruent nach dem Modul $M$, und beide von niedrigerm Grade als $M$, so müssen $A$, $A'$ auch nach dem einfachen Modul $p$ einander congruent sein.

## 8.

Man kann nun ein System von Functionen aufstellen, so dafs irgend eine beliebige Function einer von diesen Functionen, aber auch nur einer einzigen nach dem Modulus $M$ congruent ist. Es sei $A$ eine beliebige Function, so kann man, wie früher gezeigt ist, stets eine Congruenz von der Form

$$A \equiv QM + A' \pmod{p}$$

aufstellen, in welcher $A'$ von niedrigerm Grade ist als $M$. Stellt man daher sämmtliche nach dem Modul $p$ incongruente Functionen von niedrigerm Grade als $M$ auf, so ist jede beliebige Function einer von diesen nach dem Modulus $M$ congruent, aber auch nur einer einzigen von ihnen, weil zwei nach dem Modul $p$ incongruente Functionen von niedrigerm Grade als $M$ auch in Bezug auf $M$ incongruent sind. Ist $\mu$ der Grad von $M$, so ist $p^\mu$ die Anzahl dieser Functionen, welche also ein System der verlangten Art bilden. Jedes solche System heifse ein ***vollständiges System incongruenter Functionen*** in Bezug auf den Modul $M$. Multiplicirt man jedes Glied eines solchen Systems mit einer und derselben Function, welche gegen den Modulus $M$ relativ prim ist, so bilden die Producte wieder ein solches System, wie sich leicht beweisen läfst.

## 9.

Seien $N$, $N'$ etc. beliebige Functionen, deren erste durch den Modulus $M$ nicht theilbar ist, ferner $n$ eine positive ganze Zahl, so heifst die Bedingung

$$Ny^n + N'y^{n-1} + \text{etc.} + N^{(n)} \equiv 0 \pmod{M}$$

eine *Congruenz vom Grade n mit einer Unbekannten y;* und jede Function, welche für $y$ substituirt diese Bedingung befriedigt, heifst eine *Wurzel* derselben. Ist eine solche Wurzel gefunden, so ist jede mit ihr nach dem Modul $M$ congruente Function ebenfalls eine Wurzel; die Hauptaufgabe ist daher, sämmtliche nach dem Modul $M$ incongruente Wurzeln zu finden.

Wir betrachten zunächst die Congruenz *ersten* Grades, welche auf die Form

$$Ay \equiv B \pmod{M}$$

gebracht werden kann. Nehmen wir zuerst an, $A$ sei relativ prim gegen den Modul $M$, so giebt es (zufolge der Schlufsbemerkung des vorigen Artikels) in jedem vollständigen Systeme incongruenter Functionen eine, aber auch nur eine Function $y$, für welche $Ay \equiv B$ wird; die Congruenz hat daher in diesem Falle nur eine einzige Wurzel (d. h. alle Wurzeln sind dieser einen nach $M$ congruent). Hat aber $A$ mit $M$ den gröfsten gemeinschaftlichen Divisor $D$, so mufs, wenn die Congruenz lösbar sein soll, auch $B$ durch $D$ theilbar sein; in diesem Falle sei $A \equiv A'D$, $B \equiv B'D$, $M \equiv M'D \pmod{p}$, so folgt aus der obigen Congruenz

$$A'y \equiv B' \pmod{M'}$$

und umgekehrt jene aus dieser. Da nun hierin $A'$ relativ prim gegen den Modulus $M'$, so hat die letztere Congruenz eine aber auch nur eine einzige Wurzel $W$ nach dem Modulus $M'$. Alle Wurzeln der ersten Congruenz sind daher in der Form

$$y \equiv W + HM' \pmod{p}$$

enthalten, und alle in dieser Form enthaltenen Functionen $y$ sind auch Wurzeln der ersten Congruenz; und zwei in dieser Form enthaltene Functionen $W + HM'$, $W + GM'$ sind stets, aber auch nur dann nach dem Modulus $M$ incongruent, wenn $H$ und $G$ nach dem Modulus $D$ incongruent sind. Mithin hat in diesem Falle die erste Congruenz ebensoviel nach $M$ incongruente Wurzeln, als es nach dem Modul $D$ incongruente Functionen giebt, also $p^\delta$, wenn $\delta$ der Grad von $D$ ist.

Für die spätern Untersuchungen ist auch noch die Lösung der folgenden *Aufgabe* wichtig: Seien $M$, $N$ relativ prim gegen einander; es soll die

allgemeine Form der Functionen $y$ gefunden werden, welche die *beiden* Congruenzen $y \equiv A \pmod{M}$, $y \equiv B \pmod{N}$ befriedigen. Aus der ersten Form folgt $y \equiv A + zM \pmod{p}$, wo $z$ eine beliebige Function ist, welche aber der Bedingung $A + zM \equiv B \pmod{N}$ genügen mufs; diese Congruenz hat nach dem Vorhergehenden eine einzige Wurzel nach dem Modul $N$, und es folgt daraus die allgemeine Lösung $y \equiv W \pmod{MN}$.

## 10.

Hat man ein vollständiges System incongruenter Functionen in Bezug auf den Modul $M$ aufgestellt, so drängen sich die beiden folgenden Fragen auf: Wieviele dieser Functionen haben mit $M$ einen bestimmten Divisor $D$ gemeinschaftlich? und: Wieviele unter diesen haben $D$ zum gröfsten gemeinschaftlichen Divisor mit $M$? — Die Beantwortung dieser Fragen ist unabhängig von der besondern Wahl des vollständigen Systems incongruenter Functionen, da jede von zwei einander nach $M$ congruenten Functionen denselben gröfsten Divisor mit $M$ gemeinschaftlich hat, wie die andere.

Die erste Frage ist im vorigen Artikel schon mit beantwortet; zwei Functionen $GD$, $HD$ sind stets, aber auch nur dann nach dem Modul $M \equiv ND$ incongruent, wenn $G$, $H$ nach dem Modul $N$ incongruent sind; ist daher $\nu$ der Grad von $N$, so giebt es $p^{\nu} = p^{\mu-\delta}$ nach $M$ incongruente Functionen, welche mit $M$ den Divisor $D$ gemeinsam haben.

Irgend eine dieser Functionen $GD$ hat ferner stets, aber auch nur dann $D$ zum gröfsten gemeinschaftlichen Divisor mit $M$, wenn $G$ relativ prim gegen $N$ ist. Bezeichnen wir daher allgemein mit $\varphi(A)$ die Anzahl der in Bezug auf $A$ incongruenten Functionen, welche gegen $A$ relativ prim sind, so ist die zweite von uns gesuchte Anzahl $= \varphi(N)$.

Schreiben wir nun sämmtliche Divisoren von $M$ auf, mit der Beschränkung, dafs keiner von ihnen dem Producte aus einem andern in eine Einheit congruent ist, also z. B. sämmtliche incongruente *primäre* Divisoren von $M$; so hat irgend eine Function einen dieser Divisoren, aber auch nur einen einzigen zum gröfsten gemeinschaftlichen Divisor mit $M$, woraus in Verbindung mit dem Vorhergehenden der Satz

$$\Sigma\varphi(N) = p^{\mu}$$

folgt, wo das Summenzeichen sich auf ein so definirtes System von Divisoren $N$ der Function $M$ bezieht.

Aus diesem Satze ergiebt sich sogleich der Ausdruck für $\varphi(M)$ in dem Fall, wenn $M$ einer Potenz $A^\alpha$ einer einzigen Primfunction congruent ist. Ist $\alpha$ der Grad von $A$, so hat man zufolge des Satzes

$$\varphi(1)+\varphi(A)+\varphi(A^2)+\cdots+\varphi(A^{\alpha-1})+\varphi(A^\alpha) = p^{\alpha\alpha}$$

und ebenso

$$\varphi(1)+\varphi(A)+\varphi(A^2)+\cdots+\varphi(A^{\alpha-1}) = p^{\alpha(\alpha-1)};$$

folglich

$$\varphi(A^\alpha) = p^{\alpha\alpha}-p^{\alpha(\alpha-1)} = p^{\alpha\alpha}\left(1-\frac{1}{p^\alpha}\right).$$

Auf diesen Fall wird aber jeder andere durch folgenden Satz zurückgeführt: Sind $M$, $N$ relativ prim gegen einander, so ist $\varphi(MN)=\varphi(M)\varphi(N)$; welcher sich so beweisen läfst. Man bilde das vollständige System der gegen $M$ relativ primen und nach $M$ incongruenten Functionen $G$, deren Anzahl $\varphi(M)$; ebenso bilde man in Bezug auf den Modulus $N$ ein entsprechendes System von $\varphi(N)$ Functionen $H$, und in Bezug auf $MN$ ein solches System von $\varphi(MN)$ Functionen $F$. Es ergiebt sich dann mit Hülfe der Schlufsbemerkung des vorigen Artikels, dafs allen $\varphi(M)\varphi(N)$ Combinationen von Congruenzen $y\equiv G \pmod{M}$ und $y\equiv H \pmod{N}$ eine, aber auch nur eine Lösung von der Form $y\equiv F \pmod{MN}$, und umgekehrt jeder der $\varphi(MN)$ Congruenzen der letztern Form eine, aber auch nur eine Combination der erstern Form entspricht; woraus unmittelbar $\varphi(MN)=\varphi(M)\varphi(N)$ folgt.

Seien nun $A$, $B$, $C$ etc. sämmtliche einander incongruente Primfunctionen resp. von den Graden $\alpha$, $\beta$, $\gamma$ etc., welche in einer Function $M$ vom Grade $\mu$ als Factoren enthalten sind, und zwar so, dafs keine dieser Primfunctionen etwa einem Producte aus einer andern von ihnen in eine Einheit congruent ist, was man z. B. dadurch erreicht, dafs man sie alle als primär annimmt; dann ist

$$\varphi(M) = p^\mu\left(1-\frac{1}{p^\alpha}\right)\left(1-\frac{1}{p^\beta}\right)\left(1-\frac{1}{p^\gamma}\right)\cdots,$$

wie sich aus den vorhergehenden Sätzen leicht ergiebt.

## 11.

Man schreibe das vollständige System der gegen $M$ relativ primen und in Bezug auf $M$ incongruenten Functionen auf, deren Anzahl wir mit $\varphi(M)$ bezeichnet haben. Multiplicirt man sie sämmtlich mit einer und derselben $F$, welche sich in ihrem Complexe findet, so bilden die $\varphi(M)$ Producte wieder ein solches System, so dafs jedes Glied des einen Systems einem,

aber auch nur einem einzigen Gliede des andern Systems nach dem Modul $M$ congruent ist. Multiplicirt man daher alle diese $\varphi(M)$ Congruenzen mit einander, und berücksichtigt, dafs das Product der $\varphi(M)$ gegen $M$ relativ primen Functionen ebenfalls gegen $M$ relativ prim ist, so erhält man den Satz

$$F^{\varphi(M)} \equiv 1 \pmod{M},$$

welcher dem verallgemeinerten Satz von *Fermat* in der Zahlentheorie entspricht.

Ist $M$ eine Primfunction $P$ vom Grade $\pi$, so ist $\varphi(P) = p^\pi - 1$, und folglich

$$F^{p^\pi - 1} \equiv 1 \pmod{P}$$

wenn $F$ eine durch $P$ nicht theilbare Function bedeutet, und allgemein ist ohne alle Beschränkung für $F$

$$F^{p^\pi} \equiv F \pmod{P},$$

wie unmittelbar einleuchtet.

Hieraus folgt, dafs die Auflösung der Congruenz ersten Grades

$$Ay \equiv B \pmod{M}$$

in dem Falle, wo $A$ gegen $M$ relativ prim ist, durch die Formel

$$y \equiv BA^{\varphi(M)-1} \pmod{M}$$

gegeben wird.

## 12.

Von nun an wenden wir uns zu dem besondern Fall, in welchem der Modulus der Congruenzen eine *Primfunction* $P$ vom Grade $\pi$ ist. Dann besteht folgender *Satz:* Eine Congruenz $F(y) = Ny^n + N'y^{n-1} + \text{etc.} \equiv 0 \pmod{P}$ kann nicht mehr als $n$ nach dem Modul $P$ incongruente Wurzeln haben. — *Beweis:* Wir nehmen an, der Satz sei für Congruenzen vom Grade $n-1$ bewiesen, und zeigen, dafs er dann auch für Congruenzen vom Grade $n$ gilt. Gesetzt dann, unsere Congruenz $n^{\text{ten}}$ Grades hätte mehr als $n$ incongruente Wurzeln, also mindestens $n+1$. Sei $W$ eine derselben, so ist für jede andere von dieser verschiedene $y$

$$F(y) - F(W) = (y - W)F_1(y) \equiv 0 \pmod{P},$$

wo $F_1(y)$ ein Polynom vom Grade $n-1$ ist, und folglich hätte, da $y - W$ nicht $\equiv 0 \pmod{P}$ sein kann, die Congruenz $F_1(y) \equiv 0 \pmod{P}$ vom Grade $n-1$ gegen unsere Annahme mindestens $n$ Wurzeln. — Nun ist der

Satz für die Congruenzen ersten Grades schon früher bewiesen, folglich gilt er für jeden Grad.

Hat aber unsere Congruenz $n^{ten}$ Grades wirklich $n$ incongruente Wurzeln $W$, $W'$, $W''$ etc., so müssen die Coefficienten gleich hoher Potenzen von $y$ in den beiden Polynomen

$$F(y) = Ny^n + N'y^{n-1} + \text{etc.}$$
$$G(y) = N(y-W)(y-W')(y-W'') \ldots$$

einander paarweise nach dem Modul $P$ congruent sein; denn sonst hätte die Congruenz

$$F(y) - G(y) \equiv 0 \pmod{P},$$

deren Grad jedenfalls niedriger als $n$ ist, $n$ incongruente Wurzeln; sie darf daher gar keinen Grad haben, d. h. alle Coefficienten derselben müssen durch $P$ theilbar sein.

Nun haben wir im vorigen Artikel gesehen, dafs die Congruenz

$$y^{p^\pi - 1} \equiv 1 \pmod{P}$$

durch jede der $p^\pi - 1$ incongruenten gegen $P$ relativ primen Functionen $F$ befriedigt wird; mithin ist *identisch*

$$y^{p^\pi - 1} - 1 \equiv \Pi(y - F) \pmod{P},$$

wo $\Pi(y-F)$ das Product aus allen Factoren $(y-F)$ bezeichnet. Daraus folgt als Analogon zu dem Satze von *Wilson* in der Zahlentheorie das Theorem

$$\Pi(F) + 1 \equiv 0 \pmod{P},$$

wo $\Pi(F)$ das Product aus allen $p^\pi - 1$ nach $P$ incongruenten und durch $P$ nicht theilbaren Functionen bedeutet. Und umgekehrt mufs $P$ eine Primfunction sein, wenn dieser Satz gilt; denn hätte $P$ einen von einer Einheit verschiedenen Divisor $D$ von niedrigerm Grade als $\pi$, so fände sich unter den $p^\pi - 1$ Functionen $F$ eine (im Art. 10 bestimmte) Anzahl solcher, welche mit $P$ den Divisor $D$ gemeinsam hätten; daraus würde aber folgen, dafs auch die Einheit diesen Divisor hätte, was unmöglich ist.

---

## Potenzreste.

### 13.

Sei $M$ wieder ein beliebiger Modulus, $A$ relativ prim gegen denselben, so sind auch alle Glieder der Reihe 1, $A$, $A^2$ ... in inf. relativ prim gegen

$M$; es mufs daher geschehen, dafs $A^{m+n} \equiv A^m \pmod{M}$ und folglich $A^n \equiv 1 \pmod{M}$ wird. Sei $a$ der kleinste Werth von $n$, für welchen dies eintritt, so sagt man: *A gehört* zum Exponenten $a$; und es sind die $a$ Functionen

$$1, \quad A, \quad A^2 \quad \ldots \quad A^{a-1}$$

incongruent nach dem Modul $M$, woraus folgt, dafs jede Zahl $n$, für welche $A^n \equiv 1 \pmod{M}$ wird, durch $a$ theilbar ist. Zufolge des Art. 11 ist aber $A^{\varphi(M)} \equiv 1 \pmod{M}$, also ist $a$ ein Divisor von $\varphi(M)$. Doch kann dies leicht direct bewiesen werden, und daraus ergiebt sich dann ein neuer Beweis des Satzes $A^{\varphi(M)} \equiv 1 \pmod{M}$. Man braucht zu dem Zweck sich nur der bekannten Exhaustionsmethode zu bedienen, durch welche man die $\varphi(M)$ gegen $M$ relativ primen Functionen in $\frac{\varphi(M)}{a}$ Gruppen, jede von $a$ Gliedern zerfällt, deren allgemeine Form

$$F, \quad FA, \quad FA^2, \quad \ldots \quad FA^{a-1}$$

ist, wo $F$ irgend eine gegen $M$ relativ prime Function bedeutet; denn es ist leicht zu zeigen, dafs zwei solche Gruppen entweder ganz identisch, oder ganz verschieden in Bezug auf den Modulus $M$ sind.

Wir verlassen den allgemeinen Fall und nehmen nun an, dafs der Modulus eine *Primfunction* $P$ vom Grade $\pi$ ist. Ist dann $A$ irgend eine durch $P$ nicht theilbare Function, welche in Bezug auf $P$ zum Exponenten $a$ gehört, so ist $a$ ein Divisor von $p^\pi - 1$; es fragt sich: gehören zu jedem Divisor $a$ von $p^\pi - 1$ wirklich Functionen $A$? und wie viele? —

Nehmen wir zuerst an, es gebe mindestens eine Function $A$, welche zu $a$ gehört, so sind die $a$ incongruenten Functionen $1, A, A^2, \ldots A^{a-1}$ sämmtliche Wurzeln der Congruenz $y^a \equiv 1 \pmod{P}$; alle zum Exponenten $a$ gehörenden Functionen müssen daher Gliedern dieser Gruppe congruent sein, und es ergiebt sich leicht, dafs eine Function $A^{a'}$ stets, aber auch nur dann zum Exponenten $a$ gehört, wenn $a'$ relativ prim gegen $a$ ist. Wenden wir daher die Charakteristik $\varphi$ in der Bedeutung an, wie sie in der Zahlentheorie gebräuchlich ist, so ist die Anzahl der zu einem Divisor $a$ von $p^\pi - 1$ gehörenden Functionen entweder $= 0$, oder $= \varphi a$. Da aber jede der $p^\pi - 1$ durch $P$ nicht theilbaren Functionen zu einem, aber auch nur zu einem einzigen der Divisoren $a, a', a'' \ldots$ von $p^\pi - 1$ gehören mufs, und aufserdem bekanntlich $\varphi a + \varphi a' + \varphi a'' + \text{etc.} = p^\pi - 1$ ist, so ergiebt sich leicht, dafs zu jedem Divisor $a$ von $p^\pi - 1$ wirklich $\varphi a$ Functionen gehören.

Es giebt daher auch $\varphi(p^\pi - 1)$ incongruente durch den Modul $P$ nicht theilbare Functionen, welche zum Exponenten $p^\pi - 1$ gehören. Sei $G$ irgend eine derselben, so sind die $p^\pi - 1$ Functionen

$$1,\ G,\ G^2,\ G^3,\ \ldots\ G^{p^\pi - 2}$$

sämmtlich incongruent, und sie bilden daher das vollständige System der incongruenten durch $P$ nicht theilbaren Functionen, so dafs also jede durch $P$ nicht theilbare Function einer von ihnen, aber auch nur einer einzigen congruent ist. Diese $\varphi(p^\pi - 1)$ Functionen $G$ heifsen ***primitive Wurzeln*** der Primfunction $P$. Nimmt man eine derselben $G$ als ***Basis*** an, und ist $F$ eine beliebige durch $P$ nicht theilbare Function, so kann man stets

$$F \equiv G^n \pmod{P}$$

setzen, wo $n = 0$ oder eine positive ganze Zahl $< p^\pi - 1$ ist. Diese Zahl $n$ heifst dann der ***Index*** der Function $F$ bezüglich der Basis $G$, in Zeichen

$$F \equiv G^{\mathrm{Ind}.F} \pmod{P}.$$

Dann leuchten folgende Sätze ein, in welchen $A$, $B$ Functionen bedeuten, welche durch $P$ nicht theilbar sind, und in denen die Basis der Indices unverändert bleibt: $\mathrm{Ind}.(AB) \equiv \mathrm{Ind}.A + \mathrm{Ind}.B \pmod{p^\pi - 1}$, $\mathrm{Ind}.(A^n) \equiv n\,\mathrm{Ind}.A \pmod{p^\pi - 1}$; ferner folgt aus $A \equiv B \pmod{P}$ nothwendig $\mathrm{Ind}.A = \mathrm{Ind}.B$ und umgekehrt.

Ein anderer Satz welcher seiner Natur nach von der Wahl der Basis, unabhängig ist, lautet folgendermafsen: Gehört eine Function $A$ zum Exponenten $a$, so ist $\frac{p^\pi - 1}{a}$ der gröfste gemeinschaftliche Divisor von $p^\pi - 1$ und $\mathrm{Ind}.A$; und umgekehrt.

---

## Binomische Congruenzen.

### 14.

Soll die binomische Congruenz $y^n \equiv A \pmod{P}$, in welcher $A$ eine durch $P$ nicht theilbare Function bedeutet, lösbar sein, so mufs $n\,\mathrm{Ind}.y \equiv \mathrm{Ind}.A \pmod{p^\pi - 1}$ sein; ist nun $\delta$ der gröfste gemeinschaftliche Divisor von $n$ und $p^\pi - 1$, so mufs auch $\mathrm{Ind}.A$ durch $\delta$ theilbar sein, wenn diese Congruenz möglich sein soll, und dann hat sie in der That $\delta$ nach dem Modul $p^\pi - 1$ incongruente Wurzeln $\mathrm{Ind}.y$, denen ebenso viele nach dem Modul $P$ incongruente Wurzeln $y$ der binomischen Congruenz entsprechen.

Die erforderliche und hinreichende Bedingung für die Möglichkeit dieser Congruenz, dafs nämlich Ind. $A$ durch den gröfsten gemeinschaftlichen Divisor $\delta$ von $n$ und $p^\pi - 1$ theilbar sein mufs, ist unabhängig von der Wahl der Basis und offenbar identisch mit der Bedingung, dafs $A$ eine Wurzel der Congruenz $y^{\frac{p^\pi-1}{\delta}} \equiv 1 \pmod{P}$ ist; und man hätte dieses Kriterium auch leicht ohne Hülfe der Theorie der Indices ableiten können. Zugleich leuchtet nun ein, dafs die vorgelegte binomische Congruenz für $\frac{p^\pi-1}{\delta}$ incongruente Functionen $A$ möglich ist, und nur für diese.

---

## Quadratische Reste.

### 15.

Wenden wir die letzten Resultate auf den Fall an, in welchem $n = 2$ und $p$ ungerade ist (der Fall $p = 2$ ist leicht zu absolviren), so ergiebt sich, dafs die Congruenz

$$y^2 \equiv A \pmod{P}$$

stets, aber auch nur dann möglich ist, wenn $A$ eine der $\frac{1}{2}(p^\pi-1)$ Wurzeln der Congruenz

$$y^{\frac{1}{2}(p^\pi-1)} \equiv 1 \pmod{P}$$

ist, die wir *quadratische Reste* der Primfunction $P$ nennen, während die übrigen $\frac{1}{2}(p^\pi - 1)$ incongruenten durch $P$ nicht theilbaren Functionen quadratische *Nichtreste* von $P$ heifsen; und jedes Mal, wenn $A$ quadratischer Rest von $P$ ist, hat die vorgelegte Congruenz zwei incongruente Wurzeln. Die $\frac{1}{2}(p^\pi - 1)$ Nichtreste sind offenbar die Wurzeln der Congruenz

$$y^{\frac{1}{2}(p^\pi-1)} \equiv -1 \pmod{P}.$$

Doch lassen sich alle diese Sätze auch unmittelbar aus den ersten Elementen ableiten, und zugleich ergeben sich dann neue Beweise für die beiden Sätze, welche denen von *Fermat* und *Wilson* in der Zahlentheorie analog sind. Ist $A$ eine bestimmte der $p^\pi - 1$ durch $P$ nicht theilbaren Functionen, so gehört zu jeder beliebigen $F$ derselben eine, aber auch nur eine $F'$, so dafs $FF' \equiv A \pmod{P}$; wenn nun *erstens* $A$ quadratischer Nichtrest von $P$ ist (d. h. wenn die Congruenz $y^2 \equiv A \pmod{P}$ unmöglich), so sind $F$ und $F'$ stets incongruent, und es zerfällt das System sämmtlicher $p^\pi - 1$

Functionen $F$ in $\frac{1}{2}(p^n-1)$ Paare $F, F'$; woraus leicht folgt, dafs

$$\Pi(F) \equiv A^{\frac{1}{2}(p^n-1)} \pmod{P}$$

ist, wo das Zeichen $\Pi$ dieselbe Bedeutung hat, wie im Art. 12. Ist aber *zweitens* $A$ quadratischer Rest, d. h. ist die Congruenz $y^2 \equiv A \pmod{P}$ möglich, so ist einleuchtend, dafs diese zwei Wurzeln von der Form $W$ und $-W$ hat, und das Product dieser beiden Functionen ist $\equiv -A \pmod{P}$; die übrigen $p^n-3$ Functionen $F$ zerfallen aber, wie im ersten Falle, in $\frac{1}{2}(p^n-3)$ Paare incongruenter Functionen $F, F'$; woraus folgt, dafs in diesem Falle

$$\Pi(F) \equiv -A^{\frac{1}{2}(p^n-1)} \pmod{P}$$

ist. Da nun 1 quadratischer Rest von $P$ ist, so folgt aus dem zweiten Fall zunächst der Satz

$$\Pi(F)+1 \equiv 0 \pmod{P},$$

sodann, dafs

$$A^{\frac{1}{2}(p^n-1)} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{P}$$

je nachdem $A$ quadratischer Rest oder Nichtrest von $P$ ist, und endlich, dafs in beiden Fällen

$$A^{p^n-1} \equiv 1 \pmod{P}$$

ist. Die Anzahl der quadratischen Reste bestimmt sich endlich folgendermafsen. Man kann die $p^n-1$ Functionen $F$ in $\frac{1}{2}(p^n-1)$ Paare von der Form $F$, $-F$ zerlegen, woraus folgt, dafs es höchstens $\frac{1}{2}(p^n-1)$ incongruente Quadrate, also auch höchstens ebenso viel incongruente quadratische Reste giebt; da aber aufserdem je zwei verschiedenen Paaren, wie leicht zu beweisen ist, wirklich incongruente Quadrate entsprechen, so giebt es in der That $\frac{1}{2}(p^n-1)$ quadratische Reste und ebenso viele Nichtreste.

## 16.

Das Zeichen $\left(\frac{A}{P}\right)$ möge $+1$ oder $-1$ bedeuten, je nachdem (die durch die Primfunction $P$ nicht theilbare Function) $A$ quadratischer Rest oder Nichtrest von $P$ ist. Dann leuchten folgende Sätze ein:

1) Ist $A \equiv B \pmod{P}$, so ist $\left(\frac{A}{P}\right) = \left(\frac{B}{P}\right)$.

2) $\left(\frac{AB}{P}\right) = \left(\frac{A}{P}\right)\left(\frac{B}{P}\right)$ oder allgemeiner: das Product aus einer beliebigen Anzahl von Functionen (die durch $P$ nicht theilbar sind) ist quadra-

tischer Rest oder Nichtrest, je nachdem die Anzahl der Factoren, welche Nichtreste sind, gerade oder ungerade ist.

Man kann auch noch ein anderes Kriterium aufstellen, um zu entscheiden, ob eine Function $A$ quadratischer Rest oder Nichtrest von $P$ ist. Theilt man nämlich sämmtliche $p^\pi-1$ Functionen $F$ in $\frac{1}{2}(p^\pi-1)$ Paare von der Form $F$, $-F$, und nimmt aus jedem Paare willkürlich eine Function, so erhält man eine Gruppe von $\frac{1}{2}(p^\pi-1)$ Functionen $F$, deren Quadrate sämmtlich incongruent sind, und ebenso bilden die übrigen $\frac{1}{2}(p^\pi-1)$ Functionen $-F$ eine solche Gruppe. Nun bilde man die Producte aus jeder Function der einen Gruppe in die Function $A$ und bezeichne mit $\mu$ die Anzahl derjenigen unter diesen Producten, welche Functionen der andern Gruppe congruent sind; so ist leicht zu zeigen, dafs

$$A^{\frac{1}{2}(p^\pi-1)} \equiv (-1)^\mu \pmod{P}$$

oder $\left(\frac{A}{P}\right) = (-1)^\mu$ ist. Je nachdem also $\mu$ gerade oder ungerade, ist $A$ quadratischer Rest oder Nichtrest von $P$.

## 17.

Die Frage: „Von welchen Primfunctionen $P$ ist eine gegebene Function $A$ quadratischer Rest?", welche für die Theorie der *quadratischen Formen* (mit Functionen einer Variablen $x$) von Wichtigkeit ist, wird vermöge des vorigen Artikels auf den Fall reducirt, in welchem $A$ eine Primfunction $R$ (vom Grade $\varrho$) ist. Die analoge Frage in der Zahlentheorie wird bekanntlich durch den (zuerst von *Gauſs* bewiesenen) sogenannten Reciprocitäts-Satz von *Legendre* beantwortet. Diese Analogie, welche sich bisher in allen Principien und Beweisen bewährt hat, läfst keinen Zweifel an der Existenz eines entsprechenden Satzes in unserer Theorie übrig. Dieses Theorem lautet in der That

$$\left(\frac{P}{R}\right)\left(\frac{R}{P}\right) = \left(\frac{-1}{p}\right)^{\pi\cdot\varrho},$$

worin $P$, $R$ *primäre* Primfunctionen resp. von den Graden $\pi$, $\varrho$ bedeuten, und $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$ das Zeichen von *Legendre* ist. Der Fall, in welchem $P$, $R$ nicht primär sind, läfst sich unmittelbar auf diesen zurückführen. Denn bedeutet $E$ irgend eine der $p-1$ Einheiten, so ist stets $\left(\frac{A}{EP}\right)=\left(\frac{A}{P}\right)$, wo $A$ irgend eine durch $P$ nicht theilbare Function ist; und aufserdem ist $\left(\frac{E}{P}\right)=\left(\frac{e}{p}\right)^\pi$,

wo $e$ eine Zahl $\equiv E \pmod{p}$ und $\left(\frac{e}{p}\right)$ das Zeichen von *Legendre* ist. Beide Sätze sind leicht zu beweisen.

Der Beweis unseres Theorems kann ganz analog dem fünften *Gaufs*schen für den Satz von *Legendre* geführt werden und stützt sich dann auf das am Schlusse des vorigen Artikels bewiesene Lemma. Man betrachtet die vollständigen Systeme incongruenter Functionen (mit Ausnahme derer, welche $\equiv 0$ sind) in Bezug auf die drei Moduli $P$, $R$, $PR$, und wählt dazu immer die incongruenten Functionen, deren Grade kleiner sind als der des entsprechenden Modul. Jedes dieser drei Systeme theilt man in zwei Gruppen von gleich viel Gliedern ein, deren erstere sämmtliche Functionen $F$ enthält, deren höchster Coefficient einer der Zahlen $1, 2, \ldots \frac{1}{2}(p-1)$ congruent ist, während die andere Gruppe die übrigen Functionen $-F$ enthält, deren höchster Coefficient einer der Zahlen $-1, -2, \ldots -\frac{1}{2}(p-1)$ congruent ist. Die weitere Eintheilung der beiden Gruppen des dritten Systems, welches sich auf den Modulus $PR$ bezieht, in jedesmal acht Classen mit Bezug auf die Moduli $P$, $R$ und die Schlufsfolgerungen daraus bis zu dem letzten Resultat hin, in welchem der Beweis des Theorems enthalten ist, sind denen der citirten Abhandlung von *Gaufs* so ähnlich, dafs die vollständige Durchführung Niemandem entgehen kann. Und hiermit wollen wir diesen Theil unserer Theorie verlassen, da seine weitere Entwicklung sich von selbst ergiebt.

---

## Bestimmung der Primfunctionen.

### 18.

Sei $P$ eine Primfunction vom Grade $\pi$, $A$ eine beliebige Function; bildet man die unendliche Reihe $A, A^p, A^{p^2}, A^{p^3} \ldots$, so mufs es natürlich geschehen, dafs ein Glied $A^{p^{m+n}}$ einem frühern Gliede $A^{p^m}$ nach dem Modul $P$ congruent ist (im Fall $A$ der Null oder einer Einheit congruent ist, wird schon $A^p \equiv A \pmod{P}$); da ferner allgemein $A^{p^\pi} \equiv A \pmod{P}$ ist, so kann man annehmen, dafs $m < \pi$ ist; erhebt man daher die Congruenz $A^{p^{m+n}} \equiv A^{p^m}$ zur Potenz $p^{\pi-m}$, so ergiebt sich leicht $A^{p^n} \equiv A \pmod{P}$. Sei nun $\varrho > 0$ der niedrigste Werth von $n$, für welchen dies eintritt, so wollen wir sagen: die Function $A$ *pafst* zur Zahl $\varrho$. Dann sind die $\varrho$ Functionen

$$(\mathfrak{A}.) \qquad A, \; A^p, \; A^{p^2}, \; \ldots \; A^{p^{\varrho-1}}$$

sämmtlich incongruent, denn aus $A^{p^{m+n}} \equiv A^{p^m}$ würde wieder $A^{p^n} \equiv A$ folgen. Daraus ergiebt sich dann leicht, dafs, wenn $A^{p^n} \equiv A$ ist, $n$ nothwendig durch $\varrho$ theilbar sein mufs. Also ist jedenfalls $\varrho$ ein Divisor von $\pi$.

Es fragt sich nun: Passen zu jedem Divisor $\varrho$ von $\pi$ wirklich Functionen? und wieviele? — Zunächst leuchtet ein, dafs die Anzahl der (incongruenten) Functionen, welche zu $\varrho$ passen, ein Multiplum $\varrho.\psi(\varrho)$ von $\varrho$ sein mufs (die Null vorläufig nicht ausgeschlossen). Denn wenn $A$ zu $\varrho$ pafst, so passen auch die $\varrho$ in dem Complex ($\mathfrak{A}$.) enthaltenen Functionen zu $\varrho$; ebenso die $\varrho$ Functionen

$$(\mathfrak{B}.) \qquad B,\ B^p,\ B^{p^2},\ \ldots\ B^{p^{\varrho-1}},$$

wenn $B$ zu $\varrho$ pafst; und endlich sind zwei solche Complexe ($\mathfrak{A}$.) und ($\mathfrak{B}$.) entweder ganz identisch, oder ganz verschieden in Bezug auf den Modulus $P$.

Ferner ist klar, dafs alle zu $\varrho$ passenden Functionen unter den Wurzeln der Congruenz

$$y^{p^\varrho} \equiv y \pmod{P}$$

zu suchen sind, und jede Wurzel dieser Congruenz pafst zu einem bestimmten Divisor von $\varrho$. Endlich hat diese Congruenz in der That $p^\varrho$ incongruente Wurzeln, was sich unmittelbar daraus ergiebt, dafs $y^{p^\pi} - y$ algebraisch durch $y^{p^\varrho} - y$ theilbar ist. Und da unter diesen $p^\varrho$ Wurzeln auch sämmtliche Functionen enthalten sind, die zu einem beliebigen Divisor $\delta$ von $\varrho$ passen, so ergiebt sich die Gleichung:

$$\Sigma\delta.\psi(\delta) = p^\varrho,$$

wo sich das Summenzeichen auf sämmtliche Divisoren $\delta$ von $\varrho$ bezieht. Stellt man nun diese Gleichung für jeden Divisor $\varrho$ von $\pi$ auf, so erhält man offenbar ebensoviel Gleichungen, als unbekannte Zahlen $\psi(\delta)$ zu bestimmen sind. Für den Fall, dafs $\pi$ eine Potenz $a^\alpha$ einer Primzahl $a$ ist, ergiebt sich die Auflösung unmittelbar; denn dann ist, wenn $\alpha'$ eine der Zahlen 1, 2, 3 ... $\alpha$ bedeutet,

$$1.\psi(1) + a.\psi(a) + \cdots + a^{\alpha'}.\psi(a^{\alpha'}) = p^{a^{\alpha'}}$$
$$1.\psi(1) + a.\psi(a) + \cdots + a^{\alpha'-1}\psi(a^{\alpha'-1}) = p^{a^{\alpha'-1}}$$

folglich $a^{\alpha'}.\psi(a^{\alpha'}) = p^{a^{\alpha'}} - p^{a^{\alpha'-1}}$ die Anzahl der incongruenten Functionen, welche zu dem Divisor $a^{\alpha'}$ von $\pi = a^\alpha$ passen.

Doch läfst sich auch die allgemeine Auflösung des Problems vermöge

des folgenden *allgemeinen Theorems* leicht hinschreiben: Seien $f(m)$ und $F(m)$ zwei von der ganzen Zahl $m$ in der Weise abhängige Functionen, dafs die letztere gleich ist der Summe der Werthe der erstern für alle Divisoren von $m$; so läfst sich umgekehrt $f(m)$ als algebraische Summe einer Reihe von Werthen der Function $F(m)$ darstellen. Seien $a, b, c \ldots$ sämmtliche von einander verschiedenen Primzahlen, welche in $m$ aufgehen, so ist

$$f(m) = F(m) - \Sigma F\left(\frac{m}{a}\right) + \Sigma F\left(\frac{m}{ab}\right) - \Sigma F\left(\frac{m}{abc}\right) + \cdots,$$

wo die Summenzeichen auf der rechten Seite sich der Reihe nach auf alle Combinationen zu 1, 2, 3 u. s. w. aus den Primzahlen $a, b, c \ldots$ beziehen. Und es ist leicht zu sehen, dafs dasselbe Theorem auch gilt, wenn die Functionen $f$, $F$ sich auf irgend welche Elemente $m$ beziehen, denen jedesmal bestimmte andere Elemente nach denselben Principien entsprechen, wie die Divisoren einer ganzen Zahl dieser Zahl selbst entsprechen.

So folgt aus diesem Satze unmittelbar die Bestimmung der in der Zahlentheorie gebräuchlichen Function

$$\begin{aligned}\varphi(m) &= m - \Sigma\frac{m}{a} + \Sigma\frac{m}{ab} - \Sigma\frac{m}{abc} + \cdots \\ &= m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots\end{aligned}$$

aus dem Satze $\Sigma\varphi(\delta) = m$, wo $\delta$ alle Divisoren von $m$ zu durchlaufen hat.

Ebenso ergiebt sich aus dem in Art. 10 bewiesenen Satze $\Sigma\varphi(N) = p^\mu$ die Umkehrung

$$\begin{aligned}\varphi(M) &= p^\mu - \Sigma p^{\mu-\alpha} + \Sigma p^{\mu-(\alpha+\beta)} - \Sigma p^{\mu-(\alpha+\beta+\gamma)} + \cdots \\ &= p^\mu\left(1-\frac{1}{p^\alpha}\right)\left(1-\frac{1}{p^\beta}\right)\left(1-\frac{1}{p^\gamma}\right)\cdots;\end{aligned}$$

denn in diesem Falle war $F(M) = p^\mu$.

In unserm Falle haben wir $f(m) = m.\psi(m)$ und $F(m) = p^m$, und es ergiebt sich also

$$m.\psi(m) = p^m - \Sigma p^{\frac{m}{a}} + \Sigma p^{\frac{m}{ab}} - \Sigma p^{\frac{m}{abc}} + \cdots$$

als die Anzahl der nach dem Modul $P$ incongruenten Functionen, welche zu dem Divisor $m$ des Grades $\pi$ von $P$ passen; und hier bezeichnen wieder $a, b, c \ldots$ sämmtliche von einander verschiedene Primzahlen, welche in $m$ aufgehen.

Die Unabhängigkeit dieses Ausdrucks von dem Multiplum $\pi$ der Zahl $m$ und der besondern Natur der Primfunction $P$ läfst vermuthen, dafs derselbe eine allgemeinere Bedeutung hat, was sich auch bald herausstellen wird.

## 19.

*Satz:* Die Function $x^{p^\pi} - x$ ist nach dem Modul $p$ congruent dem Producte aus allen primären incongruenten Primfunctionen, deren Grade Divisoren von $\pi$ sind. —

*Beweis:* 1) Die vorgelegte Function kann keine einander congruenten Factoren enthalten, da ihre Derivirte einer Einheit congruent ist.

2) Sie ist durch jede Primfunction $R$ theilbar, deren Grad $\varrho$ ein Divisor von $\pi$ ist. Denn es ist $x^{p^\varrho} \equiv x \pmod{R}$, und wenn man beide Seiten immer wieder zur Potenz $p^\varrho$ erhebt

$$x \equiv x^{p^\varrho} \equiv x^{p^{2\varrho}} \equiv \cdots \equiv x^{p^\pi} \pmod{R}.$$

3) Sie kann keinen Primfactor von höherm Grade als $\pi$ enthalten. Denn bezeichnet $f(x)$ eine beliebige Function, so ist, wie leicht zu zeigen, für jede positive ganze Zahl $h$:

$$f(x)^{p^h} \equiv f(x^{p^h}) \pmod{p}.$$

Ist nun $Q$ irgend ein Primfactor von $x^{p^\pi} - x$, so ist also

$$f(x)^{p^\pi} \equiv f(x^{p^\pi}) \equiv f(x) \pmod{Q};$$

mithin sind alle in Bezug auf $Q$ incongruenten Functionen $f(x)$ Wurzeln der Congruenz $y^{p^\pi} \equiv y \pmod{Q}$, und folglich kann die Anzahl dieser in Bezug auf $Q$ incongruenten Functionen nicht grösser als $p^\pi$, folglich der Grad von $Q$ nicht gröfser als $\pi$ sein.

4) Der Grad jedes Primfactors von $x^{p^\pi} - x$ ist ein Divisor von $\pi$. Denn es folgt aus 3), dafs die Function $x$ in Bezug auf eine Primfunction $Q$ vom Grade $\mu$ zur Zahl $\mu$ selbst pafst (so dafs die $\mu$ Functionen $x$, $x^p$, $x^{p^2}$, $\ldots$ $x^{p^{\mu-1}}$ in Bezug auf $Q$ incongruent sind); ist daher $x^{p^\pi} \equiv x \pmod{Q}$, so mufs $\mu$ ein Divisor von $\pi$ sein.

5) Die Function $x^{p^\pi} - x$ enthält daher alle Primfunctionen, deren Grade Divisoren von $\pi$ sind, und nur solche, ferner jede nur ein Mal, und da ihr höchster Coefficient $\equiv 1 \pmod{p}$ ist, so ist sie dem Producte aus allen primären Primfunctionen congruent, deren Grade Divisoren von $\pi$ sind. W. Z. B. W.

## 20.

Bezeichnet man daher die Anzahl der primären Primfunctionen von irgend einem Grade $\varrho$ mit $\psi(\varrho)$, so ist

$$\Sigma\varrho.\psi(\varrho) = p^{\pi},$$

worin sich das Summenzeichen auf alle Divisoren $\varrho$ der Zahl $\pi$ bezieht. Vergleicht man diese Formel mit der im Art. 18, wo die allgemeine Auflösung solcher Gleichungen gelehrt ist, so ergiebt sich, dafs die Function $\psi$ hier wie dort für gleiche Argumente stets denselben Werth hat; und es ist nun auch nicht schwer, die Identität der Bedeutung derselben in beiden Untersuchungen nachzuweisen.

Zunächst ziehen wir aus der im Art. 18 entwickelten Form für $m.\psi(m)$ den Schlufs, dafs es in der That Primfunctionen von jedem Grade $m$ giebt; denn wäre die rechte Seite $=0$, so könnte man sie durch ihr letztes Glied $p^{\frac{m}{abc\cdots}}$ dividiren, woraus folgen würde, dafs die Zahl 1 als algebraische Summe einer Reihe von Potenzen einer Primzahl $p(>1)$ darstellbar wäre, was unmöglich ist, da 1 nicht durch $p$ theilbar ist; und negativ kann $m.\psi(m)$ seiner Bedeutung nach nicht sein.

Sei nun $\boldsymbol{P}$ eine Primfunction vom Grade $\pi$, und $\boldsymbol{A}$ eine Function, welche in Bezug auf den Modulus $\boldsymbol{P}$ zu dem Divisor $\varrho$ von $\pi$ pafst. Dann sind die Coefficienten sämmtlicher Potenzen von $y$ in dem Producte

$$(y-\boldsymbol{A})(y-\boldsymbol{A}^{p})(y-\boldsymbol{A}^{p^2})\ \ldots\ (y-\boldsymbol{A}^{p^{\varrho-1}})$$

nach dem Modulus $\boldsymbol{P}$ ***Zahlen*** congruent. Denn jeder Coefficient ist eine symmetrische Function der $\varrho$ Functionen $\boldsymbol{A}$, $\boldsymbol{A}^{p}$, $\ldots$ $\boldsymbol{A}^{p^{\varrho-1}}$ und bleibt daher sich selbst congruent, wenn man $x$ durch $x^{p}$ ersetzt, d. h. er ist eine Wurzel der Congruenz $y^{p} \equiv y \pmod{\boldsymbol{P}}$. Mit andern Worten, diese Gruppe von $\varrho$ Functionen, welche zu dem Divisor $\varrho$ passen, bildet das vollständige Wurzelsystem einer Congruenz

$$\boldsymbol{R}(y) \equiv 0 \pmod{\boldsymbol{P}}$$

vom Grade $\varrho$, deren Coefficienten von $x$ unabhängig sind. Umgekehrt läfst sich aber auch leicht zeigen, dafs, wenn eine Congruenz, deren Coefficienten von $x$ unabhängig sind, eine Wurzel $\boldsymbol{A}$ besitzt, welche zu dem Divisor $\varrho$ von $\pi$ pafst, sie auch die übrigen $\varrho-1$ Functionen $\boldsymbol{A}^{p}$, $\boldsymbol{A}^{p^2}$, $\ldots$ $\boldsymbol{A}^{p^{\varrho-1}}$ zu Wurzeln haben mufs (ein Satz, der sich leicht verallgemeinern läfst). Daraus folgt, dafs $\boldsymbol{R}(y)$ nach dem Modul $p$ nicht in Factoren niedrigern Grades zerlegt

werden kann, oder mit andern Worten, dafs $R(x)$ eine Primfunction vom Grade $\varrho$ ist. Die identische Congruenz

$$y^{p^\pi} - y \equiv \Pi(y - F) \pmod{P}$$

führt daher, wenn man die Factoren, welche eine Gruppe zusammengehöriger zu einer und derselben Zahl passender Functionen $F$ bilden, jedesmal in einen Factor zusammenzieht, zur Zerlegung der Function $y^{p^\pi} - y$ in ihre irreductibeln Factoren in Bezug auf den Modulus $p$. Auf diese Weise ist der Zusammenhang der Betrachtungen des Art. 18 mit der Bestimmung der Anzahl der Primfunctionen vollständig dargelegt.

## 21.

Sei nun $M$ eine beliebige Function vom Grade $\mu$ und zwar

$$M \equiv E A^a B^b C^c \ldots \pmod{p},$$

worin $E$ eine Einheit, $A$, $B$, $C$ etc. incongruente primäre Primfunctionen resp. von den Graden $\alpha$, $\beta$, $\gamma$ etc. sind. Sei ferner $\pi$ irgend eine durch sämmtliche Zahlen $\alpha$, $\beta$, $\gamma$ etc. theilbare Zahl und $P$ eine Primfunction vom Grade $\pi$. Dann hat nach dem Vorhergehenden jede der Congruenzen

$$A(y) \equiv 0 \pmod{P}, \qquad B(y) \equiv 0 \pmod{P}, \quad \text{etc.}$$

ebensoviel incongruente Wurzeln, als ihr Grad beträgt, und zwar ist der Grad die Zahl, zu welcher die Wurzeln passen. Daraus folgt, dafs man stets eine *identische* Congruenz von der Form

$$M(y) \equiv E\{\Pi(y - A')\}^a\{\Pi(y - B')\}^b \ldots \pmod{P}$$

aufstellen kann, in welcher

$$\Pi(y - A') = (y - A')(y - A'^p)\ldots(y - A'^{p^{\alpha-1}})$$

und $A'$ eine Function ist, welche zum Divisor $\alpha$ von $\pi$ pafst.

## 22.

Man kann endlich auch das Product aller primären Primfunctionen eines bestimmten Grades $m$ isolirt darstellen, mit Hülfe eines Satzes, welcher dem im Art. 18 ohne Beweis angeführten analog ist und durch einen logarithmischen Uebergang leicht aus diesem abgeleitet werden kann. Dazu führt folgender Gedankengang. Sind $a$, $b$ zwei ganze positive Zahlen, und ist $c < b$ der bei der Division von $a$ durch $b$ bleibende (nicht negative) Rest, so ist $x^c - 1$ der Rest, welcher bei der algebraischen Division von $x^a - 1$ durch $x^b - 1$

bleibt; und dies bleibt auch noch richtig, wenn man für $x$ eine beliebige positive ganze Zahl $p$ einsetzt. Ist daher $h$ der gröfste gemeinschaftliche Theiler von $a$, $b$, so ist algebraisch $x^h - 1$ der gröfste gemeinschaftliche Theiler von $x^a - 1$, $x^b - 1$; und ebenso ist im gewöhnlichen Sinne $p^h - 1$ der gröfste gemeinschaftliche Theiler von $p^a - 1$, $p^b - 1$. Daraus folgt durch abermalige Anwendung desselben Satzes, dafs algebraisch $x^{p^h-1} - 1$ der gröfste gemeinschaftliche Theiler von $x^{p^a-1} - 1$, $x^{p^b-1} - 1$, und also auch $x^{p^h} - x$ der gröfste gemeinschaftliche Theiler von $x^{p^a} - x$, $x^{p^b} - x$ ist.

Sei nun $m$ irgend eine positive ganze Zahl, welche durch keine andern Primzahlen als $a$, $b$, $c$ ... theilbar ist, so folgt aus den vorhergehenden Principien, dafs

$$(x^{p^m} - x) : \Pi(x^{p^{\frac{m}{a}}} - x) \times \Pi(x^{p^{\frac{m}{ab}}} - x) : \Pi(x^{p^{\frac{m}{abc}}} - x) \times \cdots$$

eine ganze Function ist; hierin bezieht sich das Product-Zeichen $\Pi$ der Reihe nach auf die verschiedenen Combinationen zu 1, 2, 3 u. s. w.; und die mit einander abwechselnden Divisions- und Multiplicationszeichen beziehen sich jedesmal nur auf das zunächst folgende Product.

Nehmen wir nun hierin $p$ als Primzahl an, so ergiebt sich aus den vorhergehenden Artikeln, dafs die nach dem so eben bezeichneten Gesetze gebildete ganze Function in Bezug auf den Modul $p$ congruent ist dem Producte aus allen incongruenten primären Primfunctionen vom Grade $m$. Der Grad dieser Function ist, übereinstimmend mit Art. 18, gleich

$$p^m - \Sigma p^{\frac{m}{a}} + \Sigma p^{\frac{m}{ab}} - \Sigma p^{\frac{m}{abc}} + \cdots$$

Die gemeinschaftliche Quelle des im Art. 18 angeführten und des analogen so eben benutzten Satzes ist folgende. Sei $m$ irgend eine ganze Zahl; ferner $a$, $b$, $c$, ... $k$ sämmtliche von einander verschiedene in $m$ aufgehende Primzahlen; man bilde zwei getrennte Complexe $D$, $D'$ von Divisoren der Zahl $m$ nach folgendem Princip. In den Complex $D$ nehme man zunächst alle Divisoren der Zahl $m$ auf; in den Complex $D'$ alle Divisoren von $\frac{m}{a}$, alle Divisoren von $\frac{m}{b}$ u. s. w.; dann wieder in den Complex $D$ alle Divisoren von $\frac{m}{ab}$, von $\frac{m}{ac}$, von $\frac{m}{bc}$ u. s. w.; dann wieder in den Complex $D'$ alle Divisoren von $\frac{m}{abc}$ u. s. w., bis man endlich auch alle Divisoren von $\frac{m}{abc...k}$ entweder in den Complex $D$ oder in den Complex $D'$ aufgenommen hat, je

nachdem die Anzahl der Primzahlen $a, b, c, \ldots k$ eine gerade oder ungerade ist. Dann ist leicht zu zeigen, dafs jeder Divisor der Zahl $m$ eben so oft in dem einen wie in dem andern Complex vorkommt, mit Ausnahme des Divisors $m$ selbst, der lediglich und nur ein einziges Mal in dem Complex $D$ vorkommt. Es bedarf nur eines Blickes, um hieraus die Umkehrungen der Gleichungen

$$\Sigma f(\delta) = F(m) \quad \text{oder} \quad \Pi f(\delta) = F(m)$$

abzuleiten, in welchen das Summen- oder Product-Zeichen $\Sigma$ oder $\Pi$ sich auf sämmtliche Divisoren $\delta$ einer *beliebigen* Zahl $m$ bezieht; diese Auflösungen sind in den Formeln

$$f(m) = F(m) - \Sigma F\left(\frac{m}{a}\right) + \Sigma F\left(\frac{m}{ab}\right) - \text{etc.}$$

oder

$$f(m) = F(m) : \Pi F\left(\frac{m}{a}\right) \times \Pi F\left(\frac{m}{ab}\right) : \ldots$$

enthalten.

Göttingen, im October 1856.