V.

Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus.

[Journal für reine und angewandte Mathematik, Bd. 54, S. 1—26 (1857)].

Es ist meine Absicht, dem in der Überschrift bezeichneten Gegenstand, welcher, von Gauß[*)] 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 Tat so durchgreifend, daß es mit Ausnahme einiger unserem Gegenstand eigentümlicher 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 komplexen Zahlen im 24. Bande dieses Journals) eingeschlagen hat. In Rücksicht hierauf wird man es nicht tadeln, daß ich meist nur die Hauptmomente der Beweise hervorhebe, da größere Ausführlichkeit für den Kenner der Zahlentheorie, welche hier vorausgesetzt wird, ermüdend sein müßte.

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

Gebiet der Untersuchung; Definitionen und Fundamentalsätze.

1.

Unter einer Funktion einer Variabeln x wird hier immer eine ganze rationale Funktion von x verstanden, deren Koeffizienten reelle ganze Zahlen sind. Es werden die Eigenschaften solcher Funktionen

[*) Man vgl. C. F. Gauß' Werke, Bd. 2, S. 212—240.]

[**) E. Galois: Oeuvres mathématiques, S. 15—23. I. A. Serret: Cours d'algèbre, 2. Ausg., S. 343—370. Th. Schönemann, Journ. f. Math., Bd. 31, S. 269—325 und Bd. 32, S. 93—105, 1846.]

untersucht in bezug auf einen Modulus, der eine reelle Primzahl p ist. Zwei Funktionen A, B heißen kongruent in bezug auf den Modul p, in Zeichen

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

wenn sämtliche Koeffizienten der nach Potenzen von x geordneten Differenz $A - B$ durch p teilbar sind, oder, was dasselbe sagt, wenn die Koeffizienten gleich hoher Potenzen von x in den beiden Funktionen paarweise einander kongruent sind in bezug auf den Modulus p. Es ist daher diese Kongruenz nur ein Ausdruck für die Identität

$$A = B + p \cdot C,$$

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

Man darf in jeder Kongruenz zwischen zwei Funktionen die Variabeln x durch eine beliebige Funktion von x ersetzen.

Man darf jede Kongruenz beliebig oft nach der Variabeln x differentiieren.

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 Kongruenz ganze rationale Funktionen (mit ganzen Zahlkoeffizienten) von einer Reihe von Funktionen A, B, C etc. der Variabeln x, so darf man dieselben (an beliebigen Stellen) durch ihnen resp. kongruente Funktionen A' B', C' etc. ersetzen.

2.

Der Exponent der höchsten Potenz von x in einer Funktion, deren Koeffizient nicht durch den Modul teilbar ist, heiße der Grad der Funktion. Aus dieser Definition, welche für alle Funktionen gilt, die nicht $\equiv 0 \pmod{p}$ sind, ergibt sich, daß alle die unendlich vielen einander kongruenten Funktionen einen und denselben Grad haben. Ist ferner α der Grad von A, β der Grad von B, so ist $\alpha + \beta$ der Grad von AB; denn das Produkt zweier durch eine Primzahl p nicht teilbaren Zahlen-Koeffizienten ist ebenfalls nicht teilbar

durch p. Hieraus folgt weiter: Ist $AB \equiv 0 \pmod{p}$, so ist mindestens eine der beiden Funktionen 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 gibt daher die Bedingung für die Berechtigung zur Division einer Kongruenz durch eine andere. Ferner ist leicht zu sehen, daß die Anzahl der einander nicht kongruenten (inkongruenten) Funktionen vom Grade α gleich $(p-1)p^{\alpha}$ ist; denn der Koeffizient von x^{α} kann $p-1$, der jeder niedrigeren Potenz kann p nach dem Modul p inkongruente Werte haben, und der Koeffizient jeder höheren Potenz ist $\equiv 0 \pmod{p}$. Dies Resultat gilt auch für den Fall $\alpha = 0$, insofern bei den Funktionen, welche $\equiv 0$ sind, überhaupt von einem Grade keine Rede ist.

3.

Sind A, B, C drei solche Funktionen von x, daß $A \equiv BC \pmod{p}$, so heißen B, C (oder alle diesen kongruente Funktionen) Divisoren oder Faktoren von A (oder jeder mit A kongruenten Funktion) in bezug auf den Modul p. Gleichbedeutend sind die Ausdrücke: A ist ein Multiplum von B, C; oder: A ist teilbar durch B, C. Diese Teilbarkeit nach einem Modulus ist natürlich nicht mit der algebraischen Teilbarkeit zu verwechseln, obwohl aus der letzteren stets die erstere folgt. Offenbar kann der Grad eines Divisors B von A nicht höher sein als der Grad von A. Jede Funktion ist teilbar durch jede der $p-1$ inkongruenten Funktionen vom Grade Null; denn jede der letzteren ist einer durch p nicht teilbaren Zahl a kongruent; bestimmt man nun a' so, daß $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a \cdot a'A$, wo A jede beliebige Funktion bedeutet. Außer diesen $p-1$ Funktionen vom Grade Null hat keine andere die Eigenschaft, Divisor von jeder beliebigen Funktion zu sein; denn eine Funktion, deren Grad höher als Null ist, kann nicht mehr Divisor der Funktionen vom Grade Null sein. Man kann deshalb (zufolge der Analogie mit ähnlichen Untersuchungen) diese $p-1$ inkongruenten Funktionenklassen vom Grade Null Einheiten nennen.

Man kann jede Funktion vom Grade α kongruent setzen dem Produkte aus einer bestimmten Funktion vom Grade Null und einer Funktion vom Grade α, in welcher der Koeffizient von $x^{\alpha} \equiv 1 \pmod{p}$ ist (solche Funktionen sollen primäre heißen); denn ist a der durch

p nicht teilbare Koeffizient von x^α in A, und $aa' \equiv 1 \pmod{p}$, so ist $A \equiv a \cdot a'A$, worin $a'A$ eine primäre Funktion ist. — Die Anzahl der inkongruenten primären Funktionen vom Grade α ist gleich p^α.

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

4.

Von großer Bedeutung für die späteren Untersuchungen ist folgende Aufgabe: Zu untersuchen, ob zwei gegebene Funktionen A, A' nach dem Modul p gemeinschaftliche Divisoren haben.

Zunächst läßt sich zeigen, daß man stets eine Kongruenz von der Form

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

aufstellen kann, in welcher Q, A'' zwei neue Funktionen sind, deren letztere A'' einen niedrigeren Grad als A' hat, oder gar $\equiv 0 \pmod{p}$ ist. Denn es sei α der Grad von A, α' der von A'; im Falle 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, daß $A - qx^{\alpha-\alpha'} \cdot A'$ von niedrigerem Grade α_1 als α ist; ist dann α_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 Funktion $A - qx^{\alpha-\alpha'} \cdot A'$ ebenso, wie bei dem ersten Schritte mit A; man bestimmt q_1 so, daß $A - qx^{\alpha-\alpha'} \cdot A' - q_1 x^{\alpha_1-\alpha'} \cdot A'$ von niedrigerem Grade ist als α_1 u. s. f., bis man zu einer Funktion von niedrigerem Grade als α' gelangt, was nach einer endlichen Anzahl von Operationen geschehen muß. 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 niedrigerem Grade als α'. W. Z. B. W.

Aus der so gebildeten Kongruenz folgt nun unmittelbar, daß jeder gemeinschaftliche Divisor von A, A' auch Divisor von A'', und umgekehrt, daß jeder gemeinschaftliche Divisor von A', A'' auch

Divisor von A sein muß. Man braucht daher die Operation nur fortzusetzen und ein System von Kongruenzen zu bilden:

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

in welchem die Grade α', α'' etc. eine abnehmende Reihe bilden, woraus von selbst folgt, daß nach einer endlichen Anzahl von Operationen es geschehen muß, daß eine Funktion $A^{(\nu-1)}$ durch die nächstfolgende $A^{(\nu)}$ teilbar ist. Schreitet man von der ersten bis zur letzten Kongruenz fort, so ergibt sich, daß jeder gemeinschaftliche Divisor von A, A' auch Divisor von $A^{(\nu)}$ sein muß; verfolgt man den umgekehrten Weg, so ergibt sich, daß $A^{(\nu)}$ Divisor aller vorhergehenden Funktionen und folglich auch gemeinschaftlicher Divisor der beiden Funktionen A, A' ist. Es heiße daher $A^{(\nu)}$ ein größter gemeinschaftlicher Divisor von A, A'. Multipliziert man $A^{(\nu)}$ mit einer beliebigen Funktion vom Grade Null (mit einer Einheit), so hat das Produkt offenbar dieselbe Eigenschaft wie $A^{(\nu)}$; es gibt daher $p - 1$ inkongruente größte gemeinschaftliche Divisoren desselben Grades, und ein einziger unter diesen ist primär.

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

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

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

5.

Ist der größte gemeinschaftliche Divisor $A^{(\nu)}$ der Funktionen A, A' vom Grade Null (also $\equiv 1$ (mod. p), wenn er primär ist), so heißen A, A' relativ prim gegeneinander.

Aus dieser Definition folgt der Hauptsatz: Sind A, A' zwei relative Primfunktionen, und ist M eine beliebige Funktion, so ist jeder gemeinschaftliche Divisor der beiden Funktionen AM, A' zugleich gemeinschaftlicher Divisor von M, A'. Denn multipliziert man

die Reihe der Kongruenzen, durch welche die Funktionen A, A', $A'', \cdots, A^{(\nu)}$ zusammenhängen, mit M, so ergibt sich unmittelbar, daß jeder gemeinschaftliche Divisor von AM, A' auch Divisor von $A''M$, $A'''M, \cdots, A^{(\nu)}M$ 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 Kongruenz $GAM + G'MA' \equiv A^{(\nu)}M$.)

Die wichtigsten Spezialfälle dieses Satzes sind die folgenden: Ist auch M relativ prim gegen A', so ist der größte gemeinschaftliche Divisor von M und A', und folglich auch der von AM und A' eine Funktion vom Grade Null, d. h. AM und A' sind relativ prim gegeneinander; und hieraus ergibt sich der Satz: Wenn zwei Reihen von Funktionen so beschaffen sind, daß jede Funktion der einen Reihe relativ prim gegen jede Funktion der anderen Reihe ist, so ist das Produkt aus sämtlichen Funktionen der einen Reihe relativ prim gegen das Produkt aus sämtlichen Funktionen der anderen Reihe.

Eine zweite Spezialisierung ist die folgende. Ist wieder A relativ prim gegen A', und ist AM durch A' teilbar, 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 Funktionen A, B, C etc. relativ prim gegen jede der anderen, und ist ferner eine Funktion M durch jede der Funktionen A, B, C etc. teilbar, so ist M auch durch das Produkt $ABC\cdots$ teilbar. Denn der Annahme nach ist $M \equiv GA$ durch B teilbar, folglich ist, da A relativ prim gegen B ist, $G \equiv HB$, also $M \equiv HAB$ usw.

6.

Eine Funktion, welche nach dem Modul p nur solche Divisoren hat, die entweder ihr selbst oder Funktionen vom Grade Null (d. h. Einheiten) oder Produkten aus beiden kongruent sind (denn jede Funktion hat alle diese Divisoren), heißt (irreduktibel oder) eine Primfunktion nach dem Modul p; jede andere heißt (reduktibel oder) zusammengesetzt. Es leuchtet ein, daß eine beliebige Funktion entweder durch eine bestimmte Primfunktion teilbar, oder relativ prim gegen dieselbe ist. Ist daher ein Produkt AB durch eine Primfunktion P teilbar, so ist mindestens einer der Faktoren A, B für sich allein durch P teilbar; denn ist A nicht durch P

teilbar, so ist A relativ prim gegen P, und folglich B durch P teilbar. Derselbe Satz gilt für ein Produkt aus beliebig vielen Funktionen.

Es leuchtet ein, daß jede beliebige Funktion M sich darstellen läßt als Produkt aus Potenzen von Primfunktionen, welche untereinander inkongruent 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 Faktoren vorkommen, welche einer und derselben Primfunktion A kongruent sind, so werden auch in jeder anderen Zerfällung a Faktoren vorkommen, welche derselben Primfunktion A oder einem Produkt aus A in eine Einheit kongruent sind. Man kann die Primfunktionen sämtlich primär annehmen; ist dann

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

wo z eine Einheit, A, B, C etc. inkongruente primäre Primfunktionen, a, b, c etc. positive ganze Zahlen bedeuten, so ist jeder primäre Divisor D von M von der Form

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

wo a', b', c' etc. die Null oder positive ganze Zahlen bedeuten, welche resp. nicht größer als a, b, c etc. sind. Die Anzahl der inkongruenten primären Divisoren von M ist demnach $= (a+1)(b+1)(c+1)\cdots$.

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

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

also enthält die Derivierte von M denselben Divisor D mindestens $(m-1)$mal (sie kann ihn auch öfter enthalten). Ist daher eine Funktion relativ prim gegen ihre erste Derivierte, so ist sie einem Produkt aus lauter inkongruenten Primfunktionen kongruent.

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

7.

Die vorhergehenden Sätze entsprechen vollständig denen über die Teilbarkeit der Zahlen in der Weise, daß das ganze System der unendlich vielen einander nach dem Modulus p kongruenten Funktionen

einer Variabeln sich hier verhält, wie eine einzige bestimmte Zahl in der Zahlentheorie, indem jede einzelne Funktion eines solchen Systems jede beliebige andere desselben Systems in jeder Beziehung vollständig ersetzt; eine solche Funktion ist der Repräsentant der ganzen Klasse; jede Klasse hat ihren bestimmten Grad, ihre bestimmten Divisoren usw., und alle diese Merkmale kommen jedem einzelnen Gliede einer Klasse in derselben Weise zu. Das System der unendlich vielen inkongruenten Klassen — unendlich vielen, da der Grad unbegrenzt wachsen kann — entspricht der Reihe der ganzen Zahlen in der Zahlentheorie. Der Kongruenz der Zahlen entspricht hier Kongruenz von Funktionenklassen nach einem doppelten Modulus in der folgenden Weise.

Zwei Funktionenklassen oder deren Repräsentanten A, B heißen kongruent in bezug auf die Funktionenklasse, deren Repräsentant M, in Zeichen

$$A \equiv B \text{ (modd. } p, M) \quad \text{oder} \quad A \equiv B \text{ (mod. } M),$$

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

Eine solche Kongruenz zweier Funktionen A, B in bezug auf eine dritte M ist also nur ein anderer Ausdruck für die Kongruenz

$$A \equiv B + CM \text{ (mod. } p),$$

und hieraus ergibt sich, daß man A, B, M durch beliebige Funktionen A', B', M' ersetzen kann, welche resp. jenen nach dem Modul p kongruent sind. Ferner leuchtet ein, daß man in einer solchen Kongruenz die Variable x in den drei Funktionen A, B, M durch eine beliebige Funktion von x ersetzen kann.

Aus der Definition dieser Kongruenzen 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 Kongruenz nach dem Modulus M ganze rationale Funktionen (mit ganzen Zahlenkoeffizienten) von Funktionen, so darf man jede der letzteren (an beliebigen Stellen) durch eine andere ersetzen, welche ihr nach dem Modul M kongruent 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' kongruent nach dem Modul M, und beide von niedrigerem Grade als M, so müssen A, A' auch nach dem einfachen Modul p einander kongruent sein.

8.

Man kann nun ein System von Funktionen aufstellen, so daß irgend eine beliebige Funktion einer von diesen Funktionen, aber auch nur einer einzigen nach dem Modulus M kongruent ist. Es sei A eine beliebige Funktion, so kann man, wie früher gezeigt ist, stets eine Kongruenz von der Form

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

aufstellen, in welcher A' von niedrigerem Grade ist als M. Stellt man daher sämtliche nach dem Modul p inkongruente Funktionen von niedrigerem Grade als M auf, so ist jede beliebige Funktion einer von diesen nach dem Modulus M kongruent, aber auch nur einer einzigen von ihnen, weil zwei nach dem Modul p inkongruente Funktionen von niedrigerem Grade als M auch in bezug auf M inkongruent sind. Ist μ der Grad von M, so ist p^μ die Anzahl dieser Funktionen, welche also ein System der verlangten Art bilden. Jedes solche System heiße ein vollständiges System inkongruenter Funktionen in bezug auf den Modul M. Multipliziert man jedes Glied eines solchen Systems mit einer und derselben Funktion, welche gegen den Modulus M relativ prim ist, so bilden die Produkte wieder ein solches System, wie sich leicht beweisen läßt.

9.

Seien N, N' etc. beliebige Funktionen, deren erste durch den Modulus M nicht teilbar ist, ferner n eine positive ganze Zahl, so heißt die Bedingung

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

eine Kongruenz vom Grade n mit einer Unbekannten y; und jede Funktion, welche für y substituiert diese Bedingung befriedigt, heißt eine Wurzel derselben. Ist eine solche Wurzel gefunden, so ist jede mit ihr nach dem Modul M kongruente Funktion ebenfalls eine Wurzel; die Hauptaufgabe ist daher, sämtliche nach dem Modul M inkongruente Wurzeln zu finden.

Wir betrachten zunächst die Kongruenz 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 gibt es (zufolge der Schlußbemerkung des vorigen Artikels) in jedem vollständigen System inkongruenter Funktionen eine, aber auch nur eine Funktion y, für welche $Ay \equiv B$ wird; die Kongruenz hat daher in diesem Falle nur eine einzige Wurzel (d. h. alle Wurzeln sind dieser einen nach M kongruent). Hat aber A mit M den größten gemeinschaftlichen Divisor D, so muß, wenn die Kongruenz lösbar sein soll, auch B durch D teilbar sein; in diesem Falle sei $A \equiv A'D$, $B \equiv B'D$, $M \equiv M'D \pmod{p}$, so folgt aus der obigen Kongruenz

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

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

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

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

Für die späteren Untersuchungen ist auch noch die Lösung der folgenden Aufgabe wichtig: Seien M, N relativ prim gegeneinander; es soll die allgemeine Form der Funktionen y gefunden werden, welche die beiden Kongruenzen $y \equiv A \pmod{M}$, $y \equiv B \pmod{N}$ befriedigen. Aus der ersten Form folgt $y \equiv A + zM \pmod{p}$, wo z eine beliebige Funktion ist, welche aber der Bedingung $A + zM \equiv B \pmod{N}$ genügen muß; diese Kongruenz 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 inkongruenter Funktionen in bezug auf den Modul M aufgestellt, so drängen sich die beiden folgenden Fragen auf: Wieviele dieser Funktionen haben mit M einen bestimmten Divisor D gemeinschaftlich? und: Wieviele unter diesen haben D zum größten gemeinschaftlichen Divisor mit M? — Die Beantwortung dieser Fragen ist unabhängig von der besonderen Wahl des vollständigen Systems inkongruenter Funktionen, da jede von zwei einander nach M kongruenten Funktionen denselben größten Divisor mit M gemeinschaftlich hat, wie die andere.

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

Irgend eine dieser Funktionen GD hat ferner stets, aber auch nur dann D zum größten 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 inkongruenten Funktionen, welche gegen A relativ prim sind, so ist die zweite von uns gesuchte Anzahl $= \varphi(N)$.

Schreiben wir nun sämtliche Divisoren von M auf, mit der Beschränkung, daß keiner von ihnen dem Produkt aus einem anderen in eine Einheit kongruent ist, also z. B. sämtliche inkongruente primäre Divisoren von M; so hat irgend eine Funktion einen dieser Divisoren, aber auch nur einen einzigen zum größten 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 definiertes System von Divisoren N der Funktion M bezieht.

Aus diesem Satze ergibt sich sogleich der Ausdruck für $\varphi(M)$ in dem Falle, wenn M einer Potenz A^α einer einzigen Primfunktion kongruent ist. Ist α 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

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

folglich

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

Auf diesen Fall wird aber jeder andere durch folgenden Satz zurückgeführt: Sind M, N relativ prim gegeneinander, so ist $\varphi(MN) = \varphi(M)\varphi(N)$; welcher sich so beweisen läßt. Man bilde das vollständige System der gegen M relativ primen und nach M inkongruenten Funktionen G, deren Anzahl $\varphi(M)$; ebenso bilde man in bezug auf den Modulus N ein entsprechendes System von $\varphi(N)$ Funktionen H, und in bezug auf MN ein solches System von $\varphi(MN)$ Funktionen F. Es ergibt sich dann mit Hilfe der Schlußbemerkung des vorigen Artikels, daß allen $\varphi(M)\varphi(N)$ Kombinationen von Kongruenzen $y \equiv G \pmod{M}$ und $y \equiv H \pmod{N}$ eine, aber auch nur eine Lösung von der Form $y \equiv F \pmod{MN}$, und umgekehrt jeder der $\varphi(MN)$ Kongruenzen der letzteren Form eine, aber auch nur eine Kombination der ersteren Form entspricht; woraus unmittelbar $\varphi(MN) = \varphi(M)\varphi(N)$ folgt.

Seien nun A, B, C etc. sämtliche einander inkongruente Primfunktionen resp. von den Graden α, β, γ etc., welche in einer Funktion M vom Grade μ als Faktoren enthalten sind, und zwar so, daß keine dieser Primfunktionen etwa einem Produkt aus einer anderen von ihnen in eine Einheit kongruent ist, was man z. B. dadurch erreicht, daß 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 ergibt.

11.

Man schreibe das vollständige System der gegen M relativ primen und in bezug auf M inkongruenten Funktionen auf, deren Anzahl wir mit $\varphi(M)$ bezeichnet haben. Multipliziert man sie sämtlich mit einer und derselben F, welche sich in ihrem Komplex findet, so bilden die $\varphi(M)$ Produkte wieder ein solches System, so daß jedes Glied des einen Systems einem, aber auch nur einem einzigen Gliede des anderen Systems nach dem Modul M kongruent

ist. Multipliziert man daher alle diese $\varphi(M)$ Kongruenzen miteinander, und berücksichtigt, daß das Produkt der $\varphi(M)$ gegen M relativ primen Funktionen ebenfalls gegen M relativ prim ist, so erhält man den Satz

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

welcher dem verallgemeinerten Satze von Fermat in der Zahlentheorie entspricht.

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

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

wenn F eine durch P nicht teilbare Funktion bedeutet, und allgemein ist ohne alle Beschränkung für F

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

wie unmittelbar einleuchtet.

Hieraus folgt, daß die Auflösung der Kongruenz 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 besonderen Falle, in welchem der Modulus der Kongruenzen eine Primfunktion P vom Grade π ist. Dann besteht folgender Satz: Eine Kongruenz $F(y) = Ny^n + N'y^{n-1} + \text{etc.} \equiv 0 \pmod{P}$ kann nicht mehr als n nach dem Modul P inkongruente Wurzeln haben. — Beweis: Wir nehmen an, der Satz sei für Kongruenzen vom Grade $n-1$ bewiesen, und zeigen, daß er dann auch für Kongruenzen vom Grade n gilt. Gesetzt dann, unsere Kongruenz $n$ten Grades hätte mehr als n inkongruente 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 Kongruenz $F_1(y) \equiv 0 \pmod{P}$ vom Grade $n-1$ gegen unsere Annahme mindestens n Wurzeln. — Nun ist der Satz für die Kongruenz ersten Grades schon früher bewiesen, folglich gilt er für jeden Grad.

Hat aber unsere Kongruenz $n$ten Grades wirklich n inkongruente Wurzeln W, W', W'' etc., so müssen die Koeffizienten gleich hoher Potenzen von y in den beiden Polynomen

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

einander paarweise nach dem Modul P kongruent sein; denn sonst hätte die Kongruenz

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

deren Grad jedenfalls niedriger als n ist, n inkongruente Wurzeln sie darf daher gar keinen Grad haben, d. h. alle Koeffizienten derselben müssen durch P teilbar sein.

Nun haben wir im vorigen Artikel gesehen, daß die Kongruenz

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

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

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

wo $\Pi(y - F)$ das Produkt aus allen Faktoren $(y - F)$ 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 Produkt aus allen $p^\pi - 1$ nach P inkongruenten und durch P nicht teilbaren Funktionen bedeutet. Und umgekehrt muß P eine Primfunktion sein, wenn dieser Satz gilt; denn hätte P einen von einer Einheit verschiedenen Divisor D von niedrigerem Grade als π, so fände sich unter den $p^\pi - 1$ Funktionen F eine (im Art. 10 bestimmte) Anzahl solcher, welche mit P den Divisor D gemeinsam hätten; daraus würde aber folgen, daß 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 $1, A, A^2 \ldots$ in inf. relativ prim gegen M; es muß daher geschehen, daß $A^{m+n} \equiv A^m \pmod{M}$ und folglich $A^n \equiv 1 \pmod{M}$ wird. Sei a der kleinste

Wert von n, für welchen dies eintritt, so sagt man: A gehört zum Exponenten a; und es sind die a Funktionen

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

inkongruent nach dem Modul M, woraus folgt, daß jede Zahl n, für welche $A^n \equiv 1 \pmod{M}$ wird, durch a teilbar 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 direkt bewiesen werden, und daraus ergibt sich dann ein neuer Beweis des Satzes $A^{\varphi(M)} \equiv 1 \pmod{M}$. Man braucht zu dem Zwecke sich nur der bekannten Exhaustionsmethode zu bedienen, durch welche man die $\varphi(M)$ gegen M relativ primen Funktionen in $\frac{\varphi(M)}{a}$ Gruppen, jede von a Glieder zerfällt, deren allgemeine Form

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

ist, wo F irgend eine gegen M relativ prime Funktion bedeutet; denn es ist leicht zu zeigen, daß 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, daß der Modulus eine Primfunktion P vom Grade π ist. Ist dann A irgend eine durch P nicht teilbare Funktion, 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 Funktionen A? und wieviele? —

Nehmen wir zuerst an, es gebe mindestens eine Funktion A, welche zu a gehört, so sind die a inkongruenten Funktionen $1, A, A^2, \cdots, A^{a-1}$ sämtliche Wurzeln der Kongruenz $y^a \equiv 1 \pmod{P}$; alle zum Exponenten a gehörenden Funktionen müssen daher Gliedern dieser Gruppe kongruent sein, und es ergibt sich leicht, daß eine Funktion $A^{a'}$ stets, aber auch nur dann zum Exponenten a gehört, wenn a' relativ prim gegen a ist. Wenden wir daher die Charakteristik φ 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 Funktionen entweder $= 0$, oder $= \varphi a$. Da aber jede der $p^\pi - 1$ durch P nicht teilbaren Funktionen zu einem, aber auch nur zu einem einzigen der Divisoren $a, a', a'', \cdots$ von $p^\pi - 1$ gehören muß, und außerdem bekanntlich $\varphi a + \varphi a' + \varphi a'' + \cdots = p^\pi - 1$ ist, so ergibt sich leicht, daß zu jedem Divisor a von $p^\pi - 1$ wirklich φa Funktionen gehören.

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

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

sämtlich inkongruent, und sie bilden daher das vollständige System der inkongruenten durch P nicht teilbaren Funktionen, so daß also jede durch P nicht teilbare Funktion einer von ihnen, aber auch nur einer einzigen kongruent ist. Diese $\varphi(p^\pi - 1)$ Funktionen G heißen primitive Wurzeln der Primfunktion P. Nimmt man eine derselben G als Basis an, und ist F eine beliebige durch P nicht teilbare Funktion, 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 heißt dann der Index der Funktion F bezüglich der Basis G, in Zeichen

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

Dann leuchten folgende Sätze ein, in welchen A, B Funktionen bedeuten, welche durch P nicht teilbar sind, und in denen die Basis der Indizes unverändert bleibt: Ind. $(AB) \equiv$ Ind. $A +$ Ind. B (mod. $p^\pi - 1$), Ind. $(A^n) \equiv n$ Ind. A (mod. $p^\pi - 1$); ferner folgt aus $A \equiv B$ (mod. P) notwendig Ind. $A =$ Ind. B und umgekehrt.

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

Binomische Kongruenzen.

14.

Soll die binomische Kongruenz $y^n \equiv A$ (mod. P), in welcher A eine durch P nicht teilbare Funktion bedeutet, lösbar sein, so muß n Ind. $y \equiv$ Ind. A (mod. $p^\pi - 1$) sein; ist nun δ der größte gemeinschaftliche Divisor von n und $p^\pi - 1$, so muß auch Ind. A durch δ teilbar sein, wenn diese Kongruenz möglich sein soll, und dann hat sie in der Tat δ nach dem Modul $p^\pi - 1$ inkongruente Wurzeln Ind. y, denen ebenso viele nach dem Modul P inkongruente Wurzeln y der binomischen Kongruenz entsprechen.

Die erforderliche und hinreichende Bedingung für die Möglichkeit dieser Kongruenz, daß nämlich Ind. A durch den größten gemeinschaftlichen Divisor δ von n und $p^\pi - 1$ teilbar sein muß, ist unabhängig von der Wahl der Basis und offenbar identisch mit der Bedingung, daß A eine Wurzel der Kongruenz $y^{\frac{p^\pi - 1}{\delta}} \equiv 1 \pmod{P}$ ist; und man hätte dieses Kriterium auch leicht ohne Hilfe der Theorie der Indizes ableiten können. Zugleich leuchtet nun ein, daß die vorgelegte binomische Kongruenz für $\frac{p^\pi - 1}{\delta}$ inkongruente Funktionen 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 absolvieren), so ergibt sich, daß die Kongruenz

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

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

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

ist, die wir quadratische Reste der Primfunktion P nennen während die übrigen $\frac{1}{2}(p^\pi - 1)$ inkongruenten durch P nicht teilbaren Funktionen quadratische Nichtreste von P heißen; und jedesmal, wenn A quadratischer Rest von P ist, hat die vorgelegte Kongruenz zwei inkongruente Wurzeln. Die $\frac{1}{2}(p^\pi - 1)$ Nichtreste sind offenbar die Wurzeln der Kongruenz

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

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 teilbaren Funktionen, so gehört zu jeder beliebigen F derselben eine, aber auch nur eine F', so daß $FF' \equiv A \pmod{P}$; wenn nun erstens A quadratischer Nichtrest von P ist (d. h. wenn die Kongruenz $y^2 \equiv A \pmod{P}$ unmöglich), so sind F und F' stets

inkongruent, und es zerfällt das System sämtlicher $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare F, F'; woraus leicht folgt, daß

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

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

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

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

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

sodann, daß

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

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

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

ist. Die Anzahl der quadratischen Reste bestimmt sich endlich folgendermaßen. Man kann die $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare von der Form $F, -F$ zerlegen, woraus folgt, daß es höchstens $\frac{1}{2}(p^\pi - 1)$ inkongruente Quadrate, also auch höchstens ebenso viel inkongruente quadratische Reste gibt; da aber außerdem je zwei verschiedenen Paaren, wie leicht zu beweisen ist, wirklich inkongruente Quadrate entsprechen, so gibt es in der Tat $\frac{1}{2}(p^\pi - 1)$ quadratische Reste und ebenso viele Nichtreste.

16.

Das Zeichen $\left(\frac{A}{P}\right)$ möge $+1$ oder -1 bedeuten, je nachdem (die durch die Primfunktion P nicht teilbare Funktion) 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 Produkt aus einer beliebigen Anzahl von Funktionen (die durch P nicht teilbar sind) ist quadratischer Rest oder Nichtrest, je nachdem die Anzahl der Faktoren, welche Nichtreste sind, gerade oder ungerade ist.

Man kann auch noch ein anderes Kriterium aufstellen, um zu entscheiden, ob eine Funktion A quadratischer Rest oder Nichtrest von P ist. Teilt man nämlich sämtliche $p^\pi - 1$ Funktionen F in $\frac{1}{2}(p^\pi - 1)$ Paare von der Form F, $-F$, und nimmt aus jedem Paare willkürlich eine Funktion, so erhält man eine Gruppe von $\frac{1}{2}(p^\pi - 1)$ Funktionen F, deren Quadrate sämtlich inkongruent sind, und ebenso bilden die übrigen $\frac{1}{2}(p^\pi - 1)$ Funktionen $-F$ eine solche Gruppe. Nun bilde man die Produkte aus jeder Funktion der einen Gruppe in die Funktion A und bezeichne mit μ die Anzahl derjenigen unter diesen Produkten, welche Funktionen der anderen Gruppe kongruent sind; so ist leicht zu zeigen, daß

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

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

17.

Die Frage: „Von welchen Primfunktionen P ist eine gegebene Funktion A quadratischer Rest?“, welche für die Theorie der quadratischen Formen (mit Funktionen einer Variablen x) von Wichtigkeit ist, wird vermöge des vorigen Artikels auf den Fall reduziert, in welchem A eine Primfunktion R (vom Grade ϱ) ist. Die analoge Frage in der Zahlentheorie wird bekanntlich durch den (zuerst von Gauß bewiesenen) sogenannten Reziprozitäts-Satz von Legendre beantwortet. Diese Analogie, welche sich bisher in allen Prinzipien und Beweisen bewährt hat, läßt keinen Zweifel an der Existenz eines entsprechenden Satzes in unserer Theorie übrig. Dieses Theorem lautet in der Tat

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

worin P, R primäre Primfunktionen resp. von den Graden π, ϱ 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, läßt 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 teilbare Funktion ist; und außerdem 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 Gaußschen 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 inkongruenter Funktionen (mit Ausnahme derer, welche $\equiv 0$ sind) in bezug auf die drei Moduli P, R, PR, und wählt dazu immer die inkongruenten Funktionen, deren Grade kleiner sind als der des entsprechenden Moduls. Jedes dieser drei Systeme teilt man in zwei Gruppen von gleich viel Gliedern ein, deren erstere sämtliche Funktionen F enthält, deren höchster Koeffizient einer der Zahlen $1, 2, \cdots, \frac{1}{2}(p-1)$ kongruent ist, während die andere Gruppe die übrigen Funktionen $-F$ enthält, deren höchster Koeffizient einer der Zahlen $-1, -2, \cdots, -\frac{1}{2}(p-1)$ kongruent ist. Die weitere Einteilung der beiden Gruppen des dritten Systems, welches sich auf den Modulus PR bezieht, in jedesmal acht Klassen mit Bezug auf die Moduli P, R und die Schlußfolgerungen daraus bis zu dem letzten Resultat hin, in welchem der Beweis des Theorems enthalten ist, sind denen der zitierten Abhandlung von Gauß so ähnlich, daß die vollständige Durchführung Niemandem entgehen kann. Und hiermit wollen wir diesen Teil unserer Theorie verlassen, da seine weitere Entwicklung sich von selbst ergibt.

Bestimmung der Primfunktionen.

18.

Sei P eine Primfunktion vom Grade π, A eine beliebige Funktion; bildet man die unendliche Reihe $A, A^p, A^{p^2}, A^{p^3}, \cdots$, so muß es natürlich geschehen, daß ein Glied $A^{p^{m+n}}$ einem früheren Gliede A^{p^m}

nach dem Modul P kongruent ist (im Falle A der Null oder einer Einheit kongruent ist, wird schon $A^p \equiv A \pmod{P}$); da ferner allgemein $A^{p^\pi} \equiv A \pmod{P}$ ist, so kann man annehmen, daß $m < \pi$ ist; erhebt man daher die Kongruenz $A^{p^{m+n}} \equiv A^{p^m}$ zur Potenz $p^{\pi-m}$, so ergibt sich leicht $A^{p^n} \equiv A \pmod{P}$. Sei nun $\varrho > 0$ der niedrigste Wert von n, für welchen dies eintritt, so wollen wir sagen: Die Funktion A paßt zur Zahl ϱ. Dann sind die ϱ Funktionen

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

sämtlich inkongruent, denn aus $A^{p^{m+n}} \equiv A^{p^m}$ würde wieder $A^{p^n} \equiv A$ folgen. Daraus ergibt sich dann leicht, daß, wenn $A^{p^n} \equiv A$ ist, n notwendig durch ϱ teilbar sein muß. Also ist jedenfalls ϱ ein Divisor von π.

Es fragt sich nun: Passen zu jedem Divisor ϱ von π wirklich Funktionen? und wieviele? — Zunächst leuchtet ein, daß die Anzahl der (inkongruenten) Funktionen, welche zu ϱ passen, ein Multiplum $\varrho \cdot \psi(\varrho)$ von ϱ sein muß (die Null vorläufig nicht ausgeschlossen). Denn wenn A zu ϱ paßt, so passen auch die ϱ in dem Komplex ($\mathfrak{A}.$) enthaltenen Funktionen zu ϱ; ebenso die ϱ Funktionen

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

wenn B zu ϱ paßt; und endlich sind zwei solche Komplexe ($\mathfrak{A}.$) und ($\mathfrak{B}.$) entweder ganz identisch, oder ganz verschieden in bezug auf den Modulus P.

Ferner ist klar, daß alle zu ϱ passenden Funktionen unter den Wurzeln der Kongruenz

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

zu suchen sind, und jede Wurzel dieser Kongruenz paßt zu einem bestimmten Divisor von ϱ. Endlich hat diese Kongruenz in der Tat p^ϱ inkongruente Wurzeln, was sich unmittelbar daraus ergibt, daß $y^{p^\pi} - y$ algebraisch durch $y^{p^\varrho} - y$ teilbar ist. Und da unter diesen p^ϱ Wurzeln auch sämtliche Funktionen enthalten sind, die zu einem beliebigen Divisor δ von ϱ passen, so ergibt sich die Gleichung

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

wo sich das Summenzeichen auf sämtliche Divisoren δ von ϱ bezieht. Stellt man nun diese Gleichung für jeden Divisor ϱ von π auf, so erhält man offenbar ebensoviel Gleichungen, als unbekannte Zahlen $\psi(\delta)$ zu bestimmen sind. Für den Fall, daß π eine Potenz a^α

einer Primzahl a ist, ergibt sich die Auflösung unmittelbar; denn dann ist, wenn α' eine der Zahlen 1, 2, 3, $\cdots$, α bedeutet,

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

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

Doch läßt 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 Funktionen, daß die letztere gleich ist der Summe der Werte der ersteren für alle Divisoren von m; so läßt sich umgekehrt $f(m)$ als algebraische Summe einer Reihe von Werten der Funktion $F(m)$ darstellen. Seien a, b, c, $\cdots$ sämtliche voneinander 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 Kombinationen zu 1, 2, 3 usw. aus den Primzahlen $a, b, c, \cdots$ beziehen. Und es ist leicht zu sehen, daß dasselbe Theorem auch gilt, wenn die Funktionen f, F sich auf irgendwelche Elemente m beziehen, denen jedesmal bestimmte andere Elemente nach denselben Prinzipien entsprechen, wie die Divisoren einer ganzen Zahl dieser Zahl selbst entsprechen.

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

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

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

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

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

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

In unserem Falle haben wir $f(m) = m \cdot \psi(m)$ und $F(m) = p^m$, und es ergibt sich also

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

als die Anzahl der nach dem Modul P inkongruenten Funktionen, welche zu dem Divisor m des Grades π von P passen; und hier bezeichnen wieder a, b, $c \cdots$ sämtliche voneinander verschiedene Primzahlen, welche in m aufgehen.

Die Unabhängigkeit dieses Ausdrucks von dem Multiplum π der Zahl m und der besonderen Natur der Primfunktion P läßt vermuten, daß derselbe eine allgemeinere Bedeutung hat, was sich auch bald herausstellen wird.

19.

Satz: Die Funktion $x^{p^\pi} - x$ ist nach dem Modul p kongruent dem Produkt aus allen primären inkongruenten Primfunktionen, deren Grade Divisoren von π sind. —

Beweis: 1. Die vorgelegte Funktion kann keine einander kongruenten Faktoren enthalten, da ihre Derivierte einer Einheit kongruent ist.

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

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

3. Sie kann keinen Primfaktor von höherem Grade als π enthalten. Denn bezeichnet $f(x)$ eine beliebige Funktion, 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 Primfaktor 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 inkongruenten Funktionen $f(x)$ Wurzeln der Kongruenz $y^{p^\pi} \equiv y \pmod{Q}$, und folglich kann die Anzahl dieser in bezug auf Q inkongruenten Funktionen nicht größer als p^π, folglich der Grad von Q nicht größer als π sein.

4. Der Grad jedes Primfaktors von $x^{p^\pi} - x$ ist ein Divisor von π. Denn es folgt aus 3., daß die Funktion x in bezug auf eine Primfunktion Q vom Grade μ zur Zahl μ selbst paßt (so daß die μ

Funktionen x, x^p, x^{p^2}, $\cdots$, $x^{p^{\mu-1}}$ in bezug auf Q inkongruent sind); ist daher $x^{p^\pi} \equiv x \pmod{Q}$, so muß μ ein Divisor von π sein.

5. Die Funktion $x^{p^\pi} - x$ enthält daher alle Primfunktionen, deren Grade Divisoren von π sind, und nur solche, ferner jede nur einmal, und da ihr höchster Koeffizient $\equiv 1 \pmod{p}$ ist, so ist sie dem Produkt aus allen primären Primfunktionen kongruent, deren Grade Divisoren von π sind. W. z. b. w.

20.

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

$$\Sigma \varrho \cdot \psi(\varrho) = p^\pi,$$

worin sich das Summenzeichen auf alle Divisoren ϱ der Zahl π bezieht. Vergleicht man diese Formel mit der im Art. 18, wo die allgemeine Auflösung solcher Gleichungen gelehrt ist, so ergibt sich, daß die Funktion ψ hier wie dort für gleiche Argumente stets denselben Wert 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 $m \cdot \psi(m)$ den Schluß, daß es in der Tat Primfunktionen von jedem Grade m gibt; denn wäre die rechte Seite $= 0$, so könnte man sie durch ihr letztes Glied $p^{\frac{m}{abc\cdots}}$ dividieren, woraus folgen würde, daß die Zahl 1 als algebraische Summe einer Reihe von Potenzen einer Primzahl $p(>1)$ darstellbar wäre, was unmöglich ist, da 1 nicht durch p teilbar ist; und negativ kann $m \cdot \psi(m)$ seiner Bedeutung nach nicht sein.

Sei nun P eine Primfunktion vom Grade π, und A eine Funktion, welche in bezug auf den Modulus P zu dem Divisor ϱ von π paßt. Dann sind die Koeffizienten sämtlicher Potenzen von y in dem Produkte

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

nach dem Modulus P Zahlen kongruent. Denn jeder Koeffizient ist eine symmetrische Funktion der ϱ Funktionen A, A^p, $\cdots$, $A^{p^{\varrho-1}}$ und bleibt daher sich selbst kongruent, wenn man x durch x^p ersetzt, d. h. er ist eine Wurzel der Kongruenz $y^p \equiv y \pmod{P}$. Mit anderen Worten, diese Gruppe von ϱ Funktionen, welche zu dem

Divisor ϱ passen, bildet das vollständige Wurzelsystem einer Kongruenz

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

vom Grade ϱ, deren Koeffizienten von x unabhängig sind. Umgekehrt läßt sich aber auch leicht zeigen, daß, wenn eine Kongruenz, deren Koeffizienten von x unabhängig sind, eine Wurzel A besitzt, welche zu dem Divisor ϱ von π paßt, sie auch die übrigen $\varrho - 1$ Funktionen $A^p, A^{p^2}, \ldots, A^{p^{\varrho-1}}$ zu Wurzeln haben muß (ein Satz, der sich leicht verallgemeinern läßt). Daraus folgt, daß $R(y)$ nach dem Modul p nicht in Faktoren niedrigen Grades zerlegt werden kann, oder, mit anderen Worten, daß $R(x)$ eine Primfunktion vom Grade ϱ ist. Die identische Kongruenz

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

führt daher, wenn man die Faktoren, welche eine Gruppe zusammengehöriger zu einer und derselben Zahl passender Funktionen F bilden, jedesmal in einen Faktor zusammenzieht, zur Zerlegung der Funktion $y^{p^\pi} - y$ in ihre irreduzibeln Faktoren in bezug auf den Modulus p. Auf diese Weise ist der Zusammenhang der Betrachtungen des Art. 18 mit der Bestimmung der Anzahl der Primfunktionen vollständig dargelegt.

21.

Sei nun M eine beliebige Funktion vom Grade μ, und zwar

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

worin E eine Einheit, A, B, C etc. inkongruente primäre Primfunktionen resp. von den Graden α, β, γ etc. sind. Sei ferner π irgend eine durch sämtliche Zahlen α, β, γ etc. teilbare Zahl und P eine Primfunktion vom Grade π. Dann hat nach dem Vorhergehenden jede der Kongruenzen

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

ebensoviel inkongruente Wurzeln, als ihr Grad beträgt, und zwar ist der Grad die Zahl, zu welcher die Wurzeln passen. Daraus folgt, daß man stets eine identische Kongruenz von der Form

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

aufstellen kann, in welcher

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

und A' eine Funktion ist, welche zum Divisor α von π paßt.

22.

Man kann endlich auch das Produkt aller primären Primfunktionen eines bestimmten Grades m isoliert darstellen, mit Hilfe eines Satzes, welcher dem im Art. 18 ohne Beweis angeführten analog ist und durch einen logarithmischen Übergang 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 größte gemeinschaftliche Teiler von a, b, so ist algebraisch $x^h - 1$ der größte gemeinschaftliche Teiler von $x^a - 1$, $x^b - 1$; und ebenso ist im gewöhnlichen Sinne $p^h - 1$ der größte gemeinschaftliche Teiler von $p^a - 1$, $p^b - 1$. Daraus folgt durch abermalige Anwendung desselben Satzes, daß algebraisch $x^{p^h-1} - 1$ der größte gemeinschaftliche Teiler von $x^{p^a-1} - 1$, $x^{p^b-1} - 1$, und also auch $x^{p^h} - x$ der größte gemeinschaftliche Teiler von $x^{p^a} - x$, $x^{p^b} - x$ ist.

Sei nun m irgend eine positive ganze Zahl, welche durch keine anderen Primzahlen als a, b, c, $\cdots$ teilbar ist, so folgt aus den vorhergehenden Prinzipien, daß

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

eine ganze Funktion ist; hierin bezieht sich das Produkt-Zeichen Π der Reihe nach auf die verschiedenen Kombinationen zu 1, 2, 3 usw.; und die mit einander abwechselnden Divisions- und Multiplikationszeichen beziehen sich jedesmal nur auf das zunächst folgende Produkt.

Nehmen wir nun hierin p als Primzahl an, so ergibt sich aus den vorhergehenden Artikeln, daß die nach dem soeben bezeichneten Gesetz gebildete ganze Funktion in bezug auf den Modul p kongruent ist dem Produkte aus allen inkongruenten primären Primfunktionen vom Grade m. Der Grad dieser Funktion 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 soeben benutzten Satzes ist folgende. Sei m irgend

eine ganze Zahl, ferner a, b, c, ..., k sämtliche voneinander verschiedene in m aufgehende Primzahlen; man bilde zwei getrennte Komplexe D, D' von Divisoren der Zahl m nach folgendem Prinzip. In den Komplex D nehme man zunächst alle Divisoren der Zahl m auf; in den Komplex D' alle Divisoren von $\frac{m}{a}$, alle Divisoren von $\frac{m}{b}$ usw.; dann wieder in den Komplex D alle Divisoren von $\frac{m}{ab}$, von $\frac{m}{ac}$, von $\frac{m}{bc}$ usw.; dann wieder in den Komplex D' alle Divisoren von $\frac{m}{abc}$ usw., bis man endlich auch alle Divisoren von $\frac{m}{abc \ldots k}$ entweder in den Komplex D oder in den Komplex D' aufgenommen hat, je nachdem die Anzahl der Primzahlen a, b, c, ..., k eine gerade oder ungerade ist. Dann ist leicht zu zeigen, daß jeder Divisor der Zahl m ebenso oft in dem einen wie in dem anderen Komplex vorkommt, mit Ausnahme des Divisors m selbst, der lediglich und nur ein einziges Mal in dem Komplex 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 Produkt-Zeichen Σ oder Π sich auf sämtliche Divisoren δ einer beliebigen Zahl m bezieht; diese Auflösungen sind in den Formeln

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

oder

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

enthalten.

Göttingen, im Oktober 1856.

Erläuterungen zur vorstehenden Abhandlung.

Die Resultate dieser Abhandlung befinden sich schon zum größten Teil in den in der Einleitung erwähnten Abhandlungen von Galois, Serret und Schönemann; bei Galois und Serret werden aber die Resultate unter Anwendung der Galoisschen Imaginären, bei Schönemann durch eine algebraische Betrachtungsweise unter Anwendung des Fundamentalsatzes der Algebra abgeleitet. Dedekind

reduziert hier die Theorie auf ihre einfachste, rein zahlentheoretische Form, wodurch auch die ganze Theorie der Galoisschen Imaginären überflüssig gemacht wird.

Der Restbereich für den Doppelmodul (modd. p, $P(x)$) [$P(x)$ Primfunktion (mod. p) vom Grade π] bilden offenbar einen endlichen Körper (Galoissches Feld) von der Charakteristik p mit p^π Elementen. Nach einem bekannten Satz von E. H. Moore (Papers read at the international mathematical congress, Chicago 1893 (1896), S. 208—226) ist jeder endliche Körper mit einem solchen Restbereich (modd. p, $P(x)$) isomorph und die vorstehende Dedekindsche Abhandlung gibt daher sogleich die arithmetische und zum Teil die algebraische Theorie der endlichen Körper. Für die algebraischen Eigenschaften der endlichen Körper und ihre Erweiterungen muß auf die Arbeit von E. Steinitz, Algebraische Theorie der Körper, Journ. f. Math., Bd. 137 (1910) hingewiesen werden.

Zuletzt sei noch erwähnt, daß diese Abhandlung eine wichtige Grundlage für die spätere Arbeit: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, bildet.

Ore.
