Zur Theorie der Potenzreste.

Von **K. Zsigmondy** in Wien.

I.

Die vorliegende Arbeit beschäftigt sich hauptsächlich mit der Lösung des folgenden Problems:

Es sollen alle ganzen Zahlen K angegeben werden, welche zu zwei vorgegebenen ganzen Zahlen a und b relativ prim sind und die Eigenschaft besitzen, dass die Congruenz

$$a^\sigma \equiv b^\sigma \pmod{K}$$

durch den ebenfalls vorgegebenen ganzen positiven Wert

$$\sigma = \gamma$$

und durch keinen kleineren erfüllt wird.

Für $b = 1$ sind dies jene Zahlen, bezüglich welcher a zum Exponenten γ gehört.

In dem allgemeinen, wie in dem erwähnten besonderen Falle kommt wesentlich ein Theorem in Betracht, das nach durchgeführter Specialisierung in folgender Weise ausgesprochen werden kann:

Bezeichnet man mit q den größten Primtheiler der ganzen positiven Zahl γ, mit $q^\varkappa$ die höchste noch in γ enthaltene Potenz von q, und setzt man in dem Producte der primitiven Wurzelfactoren der Gleichung $x^\gamma - 1 = 0$ an die Stelle der Variablen x die ihrem Betrage nach die Einheit übersteigende ganze Zahl a, so stimmen die verschiedenen Primfactoren des so erhaltenen Ausdrucks mit allen Primzahlen, bezüglich welcher a zum Exponenten γ gehört, unter der Voraussetzung vollständig überein, dass a nicht zur Zahl $\frac{\gamma}{q^\varkappa}$ modulo q gehört; tritt dies jedoch ein, so ist aus der Reihe der erwähnten Primfactoren der Divisor q auszuscheiden, welcher dann in der ersten und keiner höheren Potenz in dem angeführten Ausdrucke aufgeht.

Es wird sich zeigen, dass, abgesehen von besonderen Fällen, stets mindestens ein solcher Primfactor existieren muss; eine Thatsache, an die sich von selbst der Nachweis des Satzes knüpft, dass jede arithmetische Progression $\gamma j + 1$ $(j = 1, 2, 3 \ldots)$ unendlich viele Primzahlen enthält, wobei jeweilig eine Grenze, bis zu der spätestens abermals eine Primzahl der genannten Form auftreten muss, angegeben werden kann. Zum Schlusse wird die Irreductibilität der Kreistheilungsgleichung auf Grund des vorhin angeführten Theorems bewiesen werden.

II.

Bevor jedoch zur Behandlung des oben aufgestellten Problems geschritten wird, sollen die Beziehungen zwischen den beiden Reihen der Potenzen von zwei gegebenen ganzen Zahlen nach einem gegebenen Modul etwas näher untersucht werden.

Die beiden ihrem Betrage nach von einander verschiedenen ganzen Zahlen a_1 und a_2 seien relativ prim gegen den Modul K; es muss dann in der Reihe

$$(I) \qquad a_1,\ a_1^2,\ a_1^3 \ldots a_1^{m_1} \ldots$$

eine dem Betrage nach kleinste Zahl $a_1^{\nu_1}$ auftreten, welche modulo K congruent ist Zahlen der Reihe

$$(II) \qquad a_2, a_2^2, a_2^3 \ldots a_2^{m_2} \ldots,$$

unter denen wieder $a_2^{\mu_2}$ den niedrigsten Wert besitze; gehört nämlich a_1 modulo K zum Exponenten δ_1 und a_2 zu δ_2, so lehrt bereits die Congruenz $a_1^{\delta_1} \equiv a_2^{\delta_2}$, dass es in den Reihen (I) und (II) stets mindestens ein Paar congruenter Zahlen gibt.

Der Exponent ν_1 ist insoferne von wesentlicher Bedeutung, als überhaupt eine Potenz von a_1, etwa $a_1^{m_1}$, dann und nur dann mit einer Potenz von a_2, etwa mit $a_2^{m_2}$, modulo K congruent sein kann, wenn der Exponent m_1 ein Multiplum von ν_1 und zugleich der Exponent m_2, abgesehen von einem additiven positiven oder negativen Vielfachen von δ_2, ein Multiplum von μ_2 ist. 1)

Denn die Congruenz $a_1^{m_1} \equiv a_2^{m_2}$ lässt sich auch in der Form $a_1^{n\nu_1 + r_1} \equiv a_2^{n\mu_2 + r_2}$ ansetzen, wobei n die größte noch in dem Quotienten $\frac{m_1}{\nu_1}$ enthaltene ganze Zahl bedeutet und somit $0 \leqq r_1 < \nu_1$ ist. Da aus $a_1^{\nu_1} \equiv a_2^{\mu_2}$ unmittelbar die Beziehung $a_1^{n\nu_1} \equiv a_2^{n\mu_2}$ erschlossen werden kann, ergibt sich die Relation $a_1^{r_1} \equiv a_2^{r_2}$ und nach der Bedeutung von ν_1 als des kleinsten Exponenten, auf den er-

hoben eine Potenz von a_1 einer Potenz von a_2 congruent wird, muss $r_1 = 0$, somit r_2 gleich einem Vielfachen von δ_2 sein. Es folgt also $m_1 = n\nu_1$ und $m_2 = n\mu_2 + \lambda\delta_2$.

Insbesondere sind demnach δ_1 und $\varphi(K)$ Multipla von ν_1. Bezeichnet umgekehrt $a_2^{\nu_2}$ die kleinste Zahl der Reihe (II) die modulo K mit einer Potenz $a_1^{\mu_1}$ der Reihe (I) congruent ist, so ist auch μ_1 ein Multiplum von ν_1 nach dem Satze 1) und nach dem analogen Satze ν_2 Theiler von μ_2, δ_2 und $\varphi(K)$.

Die Zahlen

$$\text{(III)} \qquad a_1^{\nu_1},\ a_1^{2\nu_1},\ \ldots\ a_1^{\nu_1\frac{\delta_1}{\nu_1}}$$

bilden die Gesammtheit derjenigen modulo K incongruenten Individuen der Reihe (I), welche Potenzen von a_2 congruent sind; das Analoge gilt von

$$\text{(IV)} \qquad a_2^{\nu_2},\ a_2^{2\nu_2},\ \ldots\ a_2^{\nu_2\frac{\delta_2}{\nu_2}}.$$

Es müssen somit die Reihen (III) und (IV) modulo K genommen, abgesehen von der Reihenfolge, miteinander vollständig übereinstimmen; und es ist also

$$\frac{\delta_1}{\nu_1} = \frac{\delta_2}{\nu_2}.$$

Bezeichnet t den größten gemeinsamen Divisor von $\delta_1 = \delta_1' t$ und $\delta_2 = \delta_2' t$, so wird hienach $\nu_1 = \lambda\delta_1'$, $\nu_2 = \lambda\delta_2'$. Setzt man $t = 1$, so folgt:

Zwei ganze Zahlen, die modulo K zu gegen einander relativ primen Exponenten gehören, erzeugen bei fortgesetzter Potencierung nur verschiedene Reste nach dem Modul K, den Rest 1 ausgenommen.

III.

Durch Potencieren der Congruenz $a_1^{\nu_1} \equiv a_2^{\mu_2}$ werden auf der linken Seite alle Zahlen der Reihe (III) und damit auch die Reste modulo K der Reihe (IV) erzeugt; es muss sich somit zu jeder ganzen Zahl n stets eine ganze Zahl m angeben lassen derart, dass $m\mu_2 \equiv n\nu_2 \pmod{\delta_2}$ oder $m\frac{\mu_2}{\nu_2} \equiv n \left(\mathrm{mod}\ \frac{\delta_2}{\nu_2}\right)$ wird; dies kommt aber bekanntlich darauf hinaus, dass $\frac{\mu_2}{\nu_2}$ und $\frac{\delta_2}{\nu_2}$ zueinander relativ prim sind; es ist also ν_2 der größte gemeinsame Theiler von μ_2 und δ_2 und danach dann und nur dann gleich μ_2, wenn dieses in δ_2 aufgeht. Analog ist auch ν_1 der größte gemeinsame Divisor von μ_1 und δ_1.

Außer den Zahlen ν_1, μ_1, δ_1 ist noch ein Exponent für das Verhalten modulo K der Reihe (I) zu der Reihe (II) von wesentlicher Bedeutung. Aus der Congruenz $a_1^{\frac{\delta_1 \delta_2}{t}} \equiv a_2^{\frac{\delta_1 \delta_2}{t}}$ folgt nämlich, dass stets eine kleinste ganze positive Zahl γ existieren muss, für welche

$$a_1^\gamma \equiv a_2^\gamma \pmod K$$

wird; es soll dann gesagt werden: a_1 und a_2 haben den Exponenten γ gemeinsam bezüglich des Moduls K.

Es ist dies eine Verallgemeinerung derjenigen Congruenz $a_1^\gamma \equiv 1 \pmod K$, welche die Zahl ermittelt, zu der a_1 bezüglich K gehört. In derselben Weise, wie der Satz 1), kann nun auch hier der analoge bewiesen werden:

Eine Potenz von a_1 ist dann und nur dann congruent derselben Potenz von a_2, wenn der Potenzexponent ein Multiplum von γ ist. 2)

Danach sind insbesondere $\varphi(K)$ und $\frac{\delta_1 \delta_2}{t}$ Vielfache von γ. Ebenso folgt ohne weiteres:

Haben a_1 und a_2 den Exponenten γ gemeinsam, so haben a_1^α und a_2^α den Exponenten $\frac{\gamma}{\varepsilon}$ gemeinsam nach demselben Modul, wenn ε der größte gemeinschaftliche Divisor von α und γ ist.

IV.

Wie zwischen ν_1, δ_1 und δ_2 eine Relation bestand, so stehen auch γ, δ_1 und δ_2 in einer gewissen Beziehung. Aus der Congruenz $a_1^{\gamma\delta_1} \equiv a_2^{\gamma\delta_1} \equiv 1 \pmod K$ folgt nämlich, dass $\gamma \delta_1' t$ ein Multiplum von $\delta_2' t$, also γ ein Vielfaches von δ_2' ist. Da sich analog ergibt, dass auch δ_1' in γ aufgehen muss, kann

$$\gamma = \rho \delta_1' \delta_2'$$

gesetzt werden, wo ρ Divisor von t sein wird, weil γ in $\frac{\delta_1 \delta_2}{t}$ ohne Rest enthalten ist.

Über diesen Theiler ρ von t lässt sich noch etwas Genaueres aussagen. Zunächst erkennt man, dass $\frac{t}{\rho}$ zu δ_1' und zu δ_2' relativ prim sein muss. Bezeichnet nämlich t_1' den größten gemeinschaftlichen Divisor von $\frac{t}{\rho}$ und δ_1', t_2' den von $\frac{t}{\rho}$ und δ_2', so besitzen $\gamma = \rho \delta_1' \delta_2'$ und $\delta_1 = \rho \delta_1' \frac{t}{\rho}$ den größten gemeinsamen Theiler

$\tau_1 = \rho\,\delta_1' t_2'$, ebenso analog γ und δ_2 den größten gemeinsamen Theiler $\tau_2 = \rho\,\delta_2' t_1'$. Die Potenz a_1^γ gehört nun modulo K zum Exponenten $\frac{\delta_1}{\tau_1}$ und a_2^γ zu $\frac{\delta_2}{\tau_2}$. Der Definition von γ zufolge hat man $a_1^\gamma \equiv a_2^\gamma$, also $\frac{\delta_1}{\tau_1} = \frac{\delta_2}{\tau_2}$, woraus sich die Gleichung $t_1' = t_2'$ ergibt. Da δ_1' und δ_2' zu einander relativ prim sind, muss $t_1' = t_2' = 1$, also auch $\frac{t}{\rho}$ zu δ_1' und zu δ_2' prim sein. Daher kann ρ nur ein Multiplum sowohl des größten gemeinschaftlichen Divisors t_1 von t und δ_1', als auch des größten gemeinschaftlichen Divisors t_2 von t und δ_2' sein; das heißt, ρ muss die Form

$$\rho = \tau t_1 t_2$$

haben, wobei der Wert des Theilers τ von $\frac{t}{t_1 t_2}$ wesentlich von der Natur der Zahlen a_1 und a_2 abhängig ist, wie aus dem folgenden Beispiele erschlossen werden kann:

Für $K = 19$; $a_1 = 3$; $a_2 = 4$ hat man $\delta_1 = 18$; $\delta_2 = 9$; $\gamma = 18$, also $\tau = 9$; nimmt man $a_2 = 5$ statt 4, so ist ebenfalls $\delta_2 = 9$, aber $\gamma = 6$, also $\tau = 3$. Besonders einfach gestaltet sich wieder der Fall $t = 1$:

Gehören zwei ganze Zahlen modulo K zu Exponenten, die zu einander prim sind, so haben sie deren Product zum gemeinsamen Exponenten nach demselben Modul.

V.

In den bisher gepflogenen Untersuchungen konnte der Modul auch eine zusammengesetzte Zahl sein; im folgenden möge er als eine Primzahl p vorausgesetzt werden. Dann soll, wie dies analog in dem speciellen Falle $a_2 = 1$ zu geschehen pflegt, auch hier nach der Anzahl derjenigen incongruenten Zahlen gefragt werden, welche mit einer gegebenen Zahl a den Exponenten γ gemeinsam haben. Nach dem Satze 2) erfordert die Existenz solcher Zahlen, dass γ Theiler von $\varphi(p) = p - 1$ sei. Ist diese Bedingung erfüllt, so hat man die verlangten Zahlen unter den Wurzeln der Congruenz $x^\gamma \equiv a^\gamma \pmod p$ zu suchen. Diese werden aber, falls g primitive Wurzel von p, α der Index von a bezüglich g und ξ der von x ist, dargestellt durch

$$\text{(V)} \qquad g^\alpha,\ g^{\alpha+\frac{p-1}{\gamma}},\ g^{\alpha+2\frac{p-1}{\gamma}} \ldots g^{\alpha+(\gamma-1)\frac{p-1}{\gamma}};$$

denn aus $g^{\xi\gamma} \equiv g^{\alpha\gamma} \pmod p$ folgt $\xi \equiv \alpha \left(\mathrm{mod}\ \frac{p-1}{\gamma}\right)$ und umgekehrt.

Man hat mithin aus der Reihe (V) jene Zahlen zu bestimmen, welche mit a den Exponenten γ gemeinsam haben. Bezeichnet θ den größten gemeinschaftlichen Divisor von j und γ, so hat $g^{a+j\frac{p-1}{\gamma}}$ mit a oder g^a den Exponenten $\frac{\gamma}{\theta}$ gemeinsam; es ist nämlich $\left(g^{a+j\frac{p-1}{\gamma}}\right)^{\frac{\gamma}{\theta}} \equiv g^{a\frac{\gamma}{\theta}} \cdot g^{\frac{j}{\theta}(p-1)} \equiv (g^a)^{\frac{\gamma}{\theta}}$, und andererseits muss der gemeinsame Exponent γ' beider Zahlen ein Multiplum von $\frac{\gamma}{\theta}$ sein. γ' wird nun gleich γ dann und nur dann, wenn $\theta = 1$ ist, also γ und j relative Primzahlen sind. Hieraus folgt:

Nur wenn γ in $p-1$ aufgeht, treten Zahlen auf, welche mit a den Exponenten γ modulo p gemeinsam haben, und ihre Anzahl ist $\varphi(\gamma)$.

Es kommen also in einem vollständigen incongruenten Restsysteme überhaupt genau $\frac{(p-1)\,\varphi(\gamma)}{2}$ verschiedene Zahlenpaare vor, welche den Exponenten γ modulo p gemeinsam haben. Setzt man $\gamma = p-1$, so ergibt sich:

Die Anzahl der verschiedenen Zahlenpaare, welche den Exponenten $p-1$ bezüglich p gemeinsam haben, ist gleich der Summe der Zahlen, die relativ prim gegen $p-1$ und kleiner als $p-1$ sind.

VI.

Nach diesen einleitenden Bemerkungen soll nunmehr das Problem behandelt werden, alle Zahlen K zu finden, bezüglich welcher die gegebenen Zahlen a_1 und a_2 den gegebenen Exponenten γ gemeinsam haben.

Zunächst ist klar, dass zufolge der Definition des gemeinsamen Exponenten nur solche Zahlen K in Betracht kommen können, die relativ prim gegen a_1 und a_2 sind. Aber auch a_1 und a_2 kann man von vorneherein ohne einen gemeinsamen Theiler annehmen; denn wäre η_1 ihr größter gemeinschaftlicher Divisor, so ergäbe sich aus $a_1^\gamma \equiv a_2^\gamma \pmod K$ auch $\left(\frac{a_1}{\eta_1}\right)^\gamma \equiv \left(\frac{a_2}{\eta_1}\right)^\gamma \pmod K$; und da auch die Umkehrung bestände, würden die Zahlen K für a_1 und a_2 vollständig mit denen für $\frac{a_1}{\eta_1}$ und $\frac{a_2}{\eta_1}$ übereinstimmen.

Es sei nun γ in seine Primfactoren zerlegt gleich $q_1^{\varkappa_1} q_2^{\varkappa_2} \ldots q_s^{\varkappa_s}$. Wenn dann die Zahlen a_1 und a_2 den Exponenten γ modulo K gemeinsam haben sollen, so muss einerseits die Forderung $a_1^\gamma \equiv a_2^\gamma \pmod K$ erfüllt sein, andererseits dürfen nicht die Congruenzen $a_1^{\frac{\gamma}{q_i}} \equiv a_2^{\frac{\gamma}{q_i}} \pmod K$ $(i = 1, 2 \ldots s)$ bestehen. Umgekehrt

sind diese Bedingungen auch hinreichend; denn hat man irgend eine Zahl K gefunden, bezüglich welcher zwar die Congruenz $a_1^\gamma \equiv a_2^\gamma$ stattfindet, aber $a_1^{\frac{\gamma}{q_i}}$ nicht $a_2^{\frac{\gamma}{q_i}}$ $(i = 1, 2 \ldots s)$ congruent ist, so müssen a_1 und a_2 relativ prim gegen K sein, da sie sonst gegeneinander nicht prim wären, und müssen deshalb einen Exponenten γ' modulo K gemeinsam haben, der nach dem Satze 2) wohl in γ, aber nicht in $\frac{\gamma}{q_i}$ $(i = 1, 2 \ldots s)$ aufgeht, mithin gleich γ ist.

Um der aufgeworfenen Frage näher treten zu können, muss man zunächst alle Primzahlen aufzusuchen trachten, bezüglich welcher a_1 und a_2 den Exponenten γ gemeinsam haben, das heißt, alle Primzahlen, die wohl in $a_1^\gamma - a_2^\gamma$, aber nicht in $a_1^{\frac{\gamma}{q_i}} - a_2^{\frac{\gamma}{q_i}}$ $(i = 1, 2, \ldots s)$ ohne Rest enthalten sind. Hiefür erweist sich die Zerlegung der Differenz $a_1^\gamma - a_2^\gamma$ in die Form

$$a_1^\gamma - a_2^\gamma = \left[\left(a_1^{\frac{\gamma}{q_i}} - a_2^{\frac{\gamma}{q_i}}\right) + a_2^{\frac{\gamma}{q_i}}\right]^{q_i} - a_2^\gamma$$

als zweckmäßig. Durch Einführung zweier Symbole kann man die rechte Seite dieser Gleichung nach ihrer Entwicklung mittelst des binomischen Lehrsatzes in einer übersichtlichen Form schreiben. Setzt man nämlich

$$a_1^{\frac{\gamma}{\omega}} - a_2^{\frac{\gamma}{\omega}} = (\omega),$$

worin ω irgend einen Theiler von γ bezeichnet, und

$$q_i\, a_2^{\frac{\gamma}{q_i}(q_i-1)} + \binom{q_i}{2} a_2^{\frac{\gamma}{q_i}(q_i-2)} \left(a_1^{\frac{\gamma}{q_i}} - a_2^{\frac{\gamma}{q_i}}\right) + \ldots + \left(a_1^{\frac{\gamma}{q_i}} - a_2^{\frac{\gamma}{q_i}}\right)^{q_i-1} = Q_i,$$

so wird

$$a_1^\gamma - a_2^\gamma = (q_i)\, Q_i.$$

VII.

Die verlangten Zahlen müssen Primfactoren von $Q_1, Q_2 \ldots Q_s$ sein, also auch in dem größten gemeinsamen Theiler Δ dieser Größen aufgehen. Umgekehrt wird jeder Primfactor von Δ, sobald er von $q_1, q_2 \ldots q_s$ verschieden ist, nothwendig zu den gesuchten Primzahlen gehören. Denn geht die Primzahl p in Δ, also auch in Q_i auf, so ist sie gewiss nicht Theiler von (q_i) $(i = 1, 2, \ldots s)$, sonst wäre $q_i\, a_2^{\frac{\gamma}{q_i}(q_i-1)}$ und damit, da p von q_i verschieden sein soll,

auch a_2 und danach a_1 ein Multiplum von p, was nicht angeht, weil a_1 und a_2 relativ prim zu einander sind.

Bevor jedoch zur Aufstellung des größten gemeinsamen Theilers Δ geschritten wird, möge gleich an dieser Stelle die Bemerkung eingeschaltet werden, dass Δ unter der Voraussetzung $\gamma > 2$ überhaupt bloß den größten Primtheiler von γ, etwa q_1, und diesen nur in der ersten Potenz als Divisor enthalten kann und zwar dann und nur dann, wenn a_1 und a_2 den Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ modulo q_1 gemeinsam haben.

Geht nämlich q_i in Δ und damit auch in Q_j auf, so wird nach den eben angestellten Schlüssen gewiss nicht (q_j) $(j=1, 2 \ldots i-1, i+1 \ldots s)$ und daher umsoweniger $\left(q_j q_i^{\varkappa_i}\right)$ den Theiler q_i enthalten; wohl aber ist dies mit (q_i) und danach auch mit $\left(q_i^{\varkappa_i}\right)$ der Fall; das heißt, a_1 und a_2 haben den Exponenten $\frac{\gamma}{q_i^{\varkappa_i}}$ modulo q_i gemeinsam; dann ist aber, wie im Satze 2) gezeigt wurde, $q_i = \mu \frac{\gamma}{q_i^{\varkappa_i}} + 1$, wo μ eine ganze Zahl bedeutet. Hieraus erschließt man, dass q_i größer sei, als jeder andere in γ enthaltene Primtheiler, dass also q_i selbst der größte Primtheiler q_1 von γ sein müsse. Umgekehrt erkennt man, dass, wenn a_1 und a_2 den Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ modulo q_1 gemeinsam haben, Δ durch q_1 theilbar sein muss. Es ist ja γ aber nicht $\frac{\gamma}{q_j}$ $(j=2, 3 \ldots s)$ ein Multiplum von $\frac{\gamma}{q_1^{\varkappa_1}}$ und daher (1), aber nicht (q_j) $(j=2, 3 \ldots s)$ durch q_1 theilbar, woraus unmittelbar folgt, dass $Q_2, Q_3 \ldots Q_s$ den Primfactor q_1 besitzen, während dies für Q_1 von selbst einleuchtet.

Was den Grad betrifft, in welchem q_1 in Δ enthalten sein kann, hat man die beiden Fälle $q_1 > 2$ und $q_1 = 2$ zu unterscheiden. Ist $q_1 > 2$, so ergibt sich aus

$$Q_1 = q_1 \left\{ a_2^{\frac{\gamma}{q_1}(q_1-1)} + \binom{q_1}{2} \frac{(q_1)}{q_1} a_2^{\frac{\gamma}{q_1}(q_1-2)} + \ldots \right\},$$

dass, weil der Klammerausdruck nicht durch q_1 theilbar sein kann, sonst wäre es ja auch a_2 und a_1, Q_1 und damit auch Δ den Factor q_1 höchstens in der ersten Potenz enthält. Ist hingegen $q_1 = 2$, also $\gamma = 2^\varkappa$, so hat man $\Delta = a_1^{2^{\varkappa-1}} + a_2^{2^{\varkappa-1}}$, wo a_1 und a_2 ungerade

sein müssen, falls Δ gerade sein soll; und man sieht, dass auch in diesem Falle, sobald $\varkappa > 1$ ist, Δ nur durch 2, aber nicht durch 4 theilbar sein kann. Eine Ausnahme tritt mithin nur dann ein, wenn $\gamma = 2$ ist.

VIII.

Um einen Anhalt für die Form des gesuchten größten gemeinsamen Divisors im allgemeinen Falle zu gewinnen, möge der inductive Weg betreten und zunächst Δ für den speciellen Fall $\gamma = q_1^{\varkappa_1} q_2^{\varkappa_2}$ aufgestellt werden. Das obige Gleichungssystem reduciert sich dann auf 2 Gleichungen

$$(1) = (q_1)\ Q_1 \text{ und } (1) = (q_2)\ Q_2.$$

Die Möglichkeit, einen allgemeinen Ausdruck für den größten gemeinschaftlichen Divisor von Q_1 und Q_2 anzugeben, beruht wesentlich auf dem Umstande, dass Q_i und (q_i) $(i = 1, 2)$ höchstens q_i als gemeinsamen Theiler enthalten können. Sieht man von diesem ab, so hat man, um Δ zu erhalten, bloß aus dem Ausdrucke $Q_1 = \dfrac{a_1^{\gamma} - a_2^{\gamma}}{a_1^{\frac{\gamma}{q_1}} - a_2^{\frac{\gamma}{q_1}}}$, der in seine Primfactoren zerlegt gleich $q_1^{\varepsilon_1} q_2^{\varepsilon_2} r_1^{\varrho_1} r_2^{\varrho_2} \ldots$ sei, jene Divisoren $r_i^{\varrho_i}$ auszuscheiden, welche nicht in Q_2, also gewiss in (q_2) aufgehen. Diese Factoren stimmen mit denjenigen von (q_2) überein, die nicht in (q_1) enthalten sind und werden somit durch den Quotienten von (q_2) durch den größten gemeinsamen Theiler von (q_2) und (q_1) angegeben.

Eine einfache Überlegung ergibt nun, dass $(q_1 q_2)$ der größte gemeinsame Divisor von (q_1) und (q_2) ist.[1]) Es müssen nämlich die beiden Größen

$$\frac{(q_1)}{(q_1 q_2)} = \binom{q_2}{1} a_2^{\frac{\gamma}{q_1 q_2}(q_2-1)} + \binom{q_2}{2} a_2^{\frac{\gamma}{q_1 q_2}(q_2-2)} (q_1 q_2) + \ldots + (q_1 q_2)^{q_2-1} \text{ und}$$

$$\frac{(q_2)}{(q_1 q_2)} = \binom{q_1}{1} a_2^{\frac{\gamma}{q_1 q_2}(q_1-1)} + \binom{q_1}{2} a_2^{\frac{\gamma}{q_1 q_2}(q_1-2)} (q_1 q_2) + \ldots + (q_1 q_2)^{q_1-1}$$

relativ prim zu einander sein; denn hätten sie den Primtheiler p gemeinsam, so wäre dieser sicher Divisor von (q_1), aber gewiss nicht

[1]) Eine analoge Schlussweise lässt erkennen, dass allgemein (ω) der größte gemeinsame Divisor von (ω') und (ω'') ist, wenn mit ω das kleinste gemeinschaftliche Vielfache der beiden Theiler ω' und ω'' von γ bezeichnet wird. Es beweist dies den bekannten Satz, dass $a_1^{f'} - a_2^{f'}$ und $a_1^{f''} - a_2^{f''}$ die Differenz $a_1^{f} - a_2^{f}$ zum größten gemeinsamen Divisor besitzen, falls man unter f den größten gemeinschaftlichen Theiler von f' und f'' versteht.

Theiler von $(q_1 q_2)$. Nach den bereits aufgestellten Sätzen müsste somit der gemeinsame Exponent ρ der Zahlen a_1 und a_2 modulo p die Form

$$\rho = q_1^{\lambda_1} q_2^{\varkappa_2} \quad (\lambda_1 \leqq \varkappa_1 - 1)$$

besitzen. Da aber andererseits p auch Theiler des Ausdruckes (q_2) sein muss, so ergibt sich hieraus für den gemeinsamen Exponenten ρ die Form

$$\rho = q_1^{\varkappa_1} q_2^{\lambda_2} \quad (\lambda_2 \leqq \varkappa_2 - 1).$$

Diese beiden Formen von ρ widersprechen einander und es müssen daher die Größen $\frac{(q_1)}{(q_1 q_2)}$ und $\frac{(q_2)}{(q_1 q_2)}$ relative Primzahlen sein.

Mithin wird das Product jener Factoren $r_i^{\varrho_i}$, welche in (q_2) aber nicht in (q_1), also in Q_1 aber nicht in Q_2 aufgehen, durch $\frac{(q_2)}{(q_1 q_2)}$ dargestellt und man darf schließen, dass

$$\Delta' = \frac{(1)}{(q_1)} : \frac{(q_2)}{(q_1 q_2)} = \frac{\left(a_1^{\gamma} - a_2^{\gamma}\right)\left(a_1^{\frac{\gamma}{q_1 q_2}} - a_2^{\frac{\gamma}{q_1 q_2}}\right)}{\left(a_1^{\frac{\gamma}{q_1}} - a_2^{\frac{\gamma}{q_1}}\right)\left(a_1^{\frac{\gamma}{q_2}} - a_2^{\frac{\gamma}{q_2}}\right)}$$

identisch mit Δ ist, sobald noch der Nachweis geliefert wird, dass Δ' dann und nur dann durch den größeren der beiden Primfactoren von γ, nämlich durch q_1 und durch diesen nur in der ersten Potenz theilbar ist, wenn a_1 und a_2 den Exponenten $q_2^{\varkappa_2}$ modulo q_1 gemeinsam haben.

Dass sich dies in der That so verhält, kann leicht eingesehen werden. Angenommen, es wäre Δ' und somit auch (1) durch q_1 theilbar, so müsste nach einer bereits oben angegebenen Überlegung, da $\gamma > 2$ ist, (q_1) den Primtheiler q_1 in einer um eine Einheit geringeren Potenz als (1) enthalten. (q_2) dagegen enthält entweder den Factor q_1 gar nicht oder in genau derselben Potenz, wie (1). Tritt der erste Fall ein, so kann q_1, da es nicht in (q_2) aufgeht, umsoweniger in $(q_1 q_2)$ aufgehen und es wird daher Δ' den Primtheiler q_1 nur in der ersten Potenz enthalten. Zugleich haben a_1 und a_2 den Exponenten $q_2^{\varkappa_2}$ modulo q_1 gemeinsam. Von diesem Satze gilt auch die Umkehrung. Tritt jedoch der zweite Fall ein, dass (q_2) durch q_1 theilbar ist, so ist $(q_1 q_2)$ durch dieselbe Potenz von q_1 theilbar, wie (q_1), und (1) durch dieselbe Potenz, wie (q_2). Mithin kommt q_1 in dem Ausdrucke Δ' als Factor überhaupt nicht vor. Auf analoge Weise folgt, dass Δ' niemals ein

Multiplum von q_2 sein kann, sobald man $q_2 > 2$ hat. Im Falle als $q_2 = 2$ ist, und a_1 nebst a_2 ungerade sind, geht 2 in derselben Potenz in (1) auf, wie in (q_1), und ebenso in (2), wie in $(2q_1)$; Δ' ist also ungerade und unter allen Umständen hat man mithin $\Delta = \Delta'$.

IX.

Der so für Δ gefundene Ausdruck charakterisiert bereits die Form des größten gemeinsamen Divisors im allgemeinen Falle $\gamma = q_1^{\varkappa_1} q_2^{\varkappa_2} \dots q_s^{\varkappa_s}$. Man darf nunmehr erwarten, dass derselbe dargestellt wird durch

$$\frac{\left(a_1^{\gamma} - a_2^{\gamma}\right) \prod_{qq'} \left(a_1^{\frac{\gamma}{qq'}} - a_2^{\frac{\gamma}{qq'}}\right) \dots}{\prod_{q} \left(a_1^{\frac{\gamma}{q}} - a_2^{\frac{\gamma}{q}}\right) \prod_{qq'q''} \left(a_1^{\frac{\gamma}{qq'q''}} - a_2^{\frac{\gamma}{qq'q''}}\right) \dots} = \Delta',$$

wo die Productzeichen sich auf die entsprechenden Combinationen zu zweien, dreien u. s. f. gebildet aus den Elementen $q_1, q_2 \dots q_s$ zu beziehen haben.

In der That folgt gerade so, wie vorhin, aus der Gleichung

$$(1) = (P)\left\{\binom{P}{1} a_2^{\frac{\gamma}{P}(P-1)} + \binom{P}{2} a_2^{\frac{\gamma}{P}(P-2)} (P) + \dots + (P)^{P-1}\right\},$$

in welcher P irgend eine Combination der Elemente $q_1 \dots q_s$ bedeutet, dass (P) den Primfactor p, wenn er von q_i $(i = 1, 2 \dots s)$ verschieden ist, in derselben Potenz enthält, wie (1). Die Zahlen a_1 und a_2 sind durch p nicht theilbar und müssen daher modulo p einen gemeinsamen Exponenten besitzen, welcher als Divisor von γ entweder gewisse Primfactoren $q_{i_1}, q_{i_2} \dots q_{i_\varrho}$ $(\varrho \geqq 1)$ in niedrigerer Potenz, wie γ, enthält, oder aber gleich γ ist. Im ersten Falle wird $(q'\,q'' \dots q^{(\nu)})$ dann und nur dann durch p^{π} und zwar stets durch dieselbe Potenz theilbar sein, wenn $q'\,q'' \dots q^{(\nu)}$ irgend eine Combination der Elemente $q_{i_1}, q_{i_2} \dots q_{i_\varrho}$ vorstellt, und es wird p in der Potenz $\pi \left\{1 - \binom{\varrho}{1} + \binom{\varrho}{2} - \dots\right\} = 0$ in Δ' aufgehen.

Im zweiten Falle treten dagegen diejenigen Primfactoren von (1) in Δ' auf, die nicht in (q_i) $(i = 1, 2 \dots s)$ enthalten sind und zwar in denselben Potenzen, wie in (1). Damit ist gezeigt, dass jeder Theiler von Δ' auch Theiler von Δ sein muss, wenn man von den Factoren, die eventuell q_i enthalten, absieht; dass auch die Umkehrung gilt, leuchtet unmittelbar ein.

Noch bleibt das Verhalten von Δ' bezüglich der q_i zu untersuchen übrig. Geht q_j in (1) und damit auch in (q_j) auf, so muss der gemeinsame Exponent η von a_1 und a_2 modulo q_j ein Divisor von $\frac{\gamma}{q_j}$ sein. Diejenigen Primfactoren, welche in η in niedrigerer Potenz enthalten sind, als in γ, seien $q_j, q_{i_1}, q_{i_2} \ldots q_{i_\varrho}$; alle Combinationen aus diesen $\varrho + 1$ Elementen sollen in 2 Classen getheilt werden: die eine enthalte nur Combinationen ohne das Element q_j, die andere nur Combinationen mit dem Elemente q_j; ein Repräsentant der ersten Classe sei P, ein solcher der zweiten P_j. Dann geht nach bereits früher angewandten Schlüssen, q_j, sobald es größer als 2 ist, nur in den Factoren (P) und (P_j) auf und zwar in (P) in derselben Potenz, etwa der π_j^{ten}, wie in (1), in (P_j) jedoch in einer um eins niedrigeren. Mithin wird die Zahl, welche angibt, wie oft Δ' den Factor q_j enthält, durch

$$\pi_j \left\{1 - \binom{\varrho}{1} + \binom{\varrho}{2} - \ldots\right\} + (\pi_j - 1)\left\{-1 + \binom{\varrho}{1} - \binom{\varrho}{2} + \ldots\right\}$$

dargestellt. Sie ist also nur im Falle $\varrho = 0$ von Null verschieden und dann gleich 1. Dann hat man aber $\eta = \frac{\gamma}{q_j^{\varkappa_j}}$ und $q_j = \mu \frac{\gamma}{q_j^{\varkappa_j}} + 1$, wo μ eine ganze Zahl bedeutet. Somit kann höchstens der größte Primfactor q_1 von γ in der ersten Potenz in Δ' aufgehen und zwar müssen, wenn dieser Fall eintritt, a_1 und a_2 den Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ modulo q_1 gemeinsam haben. Umgekehrt, haben a_1 und a_2 den gemeinsamen Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ modulo q_1, so ist (1) und (q_1), aber nicht (q_i) $(i = 2, 3 \ldots s)$ durch q_1 theilbar und Δ' enthält den Primfactor q_1 gerade in der ersten Potenz. Endlich erkennt man, dass Δ', falls $s > 1$ angenommen wird, ungerade sein muss; denn besitzt (1) den Factor $2^\varkappa$, so ist 2 auch in $(q_{i_1} \ldots q_{i_\varrho})$, falls $q_{i_1}, \ldots q_{i_\varrho}$ ungerade Primzahlen sind, in derselben Potenz, wie in (1), und in $(2 q_{i_1} \ldots q_{i_\varrho})$ in derselben, etwa der $\varkappa'^{\text{ten}}$, wie in (2), enthalten. 2 kommt mithin auf die Potenz

$$\varkappa\left\{1 - \binom{s-1}{1} + \binom{s-1}{2} \ldots\right\} + \varkappa'\left\{-1 + \binom{s-1}{1} - \ldots\right\} = 0$$

erhoben in Δ' vor. Man hat also wirklich in dem Ausdrucke Δ' den gesuchten größten gemeinsamen Divisor von Q_1, $Q_2 \ldots Q_s$ aufgefunden und ist damit zu dem folgenden Theoreme gelangt:

Sind die beiden gegebenen Zahlen a_1 und a_2 relativ prim zu einander, ist ferner die gegebene positive ganze Zahl γ in ihre Primfactoren zerlegt gleich $q_1^{\varkappa_1} q_2^{\varkappa_2} \ldots q_s^{\varkappa_s}$ und ist endlich q_1 der größte Primtheiler von γ, so stimmen alle Primzahlen, bezüglich welcher a_1 und a_2 den Exponenten γ gemeinsam haben, mit den verschiedenen Primfactoren des Ausdrucks

$$\Delta = \frac{\left(a_1^{\gamma} - a_2^{\gamma}\right) \prod_{qq'} \left(a_1^{\frac{\gamma}{qq'}} - a_2^{\frac{\gamma}{qq'}}\right) \ldots .}{\prod_{q} \left(a_1^{\frac{\gamma}{q}} - a_2^{\frac{\gamma}{q}}\right) \prod_{qq'q''} \left(a_1^{\frac{\gamma}{qq'q''}} - a_2^{\frac{\gamma}{qq'q''}}\right) \ldots .},$$

in welchem die Productzeichen sich auf die entsprechenden Combinationen zu zweien, dreien u. s. f., gebildet aus den Elementen $q_1, q_2, \ldots q_s$ zu beziehen haben, unter der Voraussetzung vollständig überein, dass die Zahlen a_1 und a_2 nicht den Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ modulo q_1 gemeinsam haben; ist dies jedoch der Fall, so ist aus der Reihe der erwähnten Primfactoren die Zahl q_1 auszuscheiden, welche dann in der ersten und keiner höheren Potenz in Δ aufgeht. 3)

Damit sind alle Primzahlen gefunden, bezüglich welcher a_1 und a_2 den Exponenten γ gemeinsam haben: sie ergeben sich als die verschiedenen Primfactoren p von Δ. Man erhält aber noch mehr. Ist nämlich p^{π} die höchste noch in Δ enthaltene Potenz von p, so ist p^{π} auch die höchste Potenz von p, bezüglich welcher noch a_1 und a_2 den Exponenten γ gemeinsam haben. Denn aus den Annahmen

$$a_1^{\gamma} = a_2^{\gamma} + \mu p^{\pi} \text{ und } a_1^{\frac{\gamma}{q_i}} = a_2^{\frac{\gamma}{q_i}} + \mu_i \; (i = 1, 2 \ldots s),$$

wo die ganzen Zahlen μ und μ_i nicht durch p theilbar seien, folgt durch Erheben der Gleichungen auf die p^{te} Potenz

$$a_1^{\gamma p} = a_2^{\gamma p} + \nu p^{\pi+1} \text{ und } a_1^{\frac{\gamma p}{q_i}} = a_2^{\frac{\gamma p}{q_i}} + \nu_i \; (i = 1, 2 \ldots s),$$

wo die ganzen Zahlen ν und ν_i wieder durch p nicht theilbar sind. Die Fortsetzung dieses Verfahrens lehrt, dass a_1 und a_2 bezüglich $p^{\pi+\nu}$ den Exponenten $\gamma . p^{\nu}$ gemeinsam haben.

X.

Nachdem auf diese Art die höchsten Primzahlpotenzen der verlangten Eigenschaft gefunden sind, handelt es sich noch um diejenigen Zahlen, welche verschiedene Primfactoren enthalten. In dieser Hinsicht kommt der folgende Satz wesentlich in Betracht:

Sind die beiden ganzen Zahlen K und K' relativ prim zu einander und haben a_1 und a_2 den Exponenten γ modulo K, den Exponenten γ' modulo K' gemeinsam, so ist das kleinste gemeinschaftliche Vielfache von γ und γ' der gemeinsame Exponent von a_1 und a_2 bezüglich des Productes $K.K'$.

Einerseits muss nämlich der gemeinsame Exponent ρ von a_1 und a_2 modulo $K.K'$ ein Multiplum von γ und γ', somit auch ein solches ihres kleinsten gemeinschaftlichen Vielfachen v sein; denn eine Congruenz, welche bezüglich eines Productes stattfindet, muss auch hinsichtlich jedes einzelnen Factors desselben erfüllt sein. Andererseits muss aber der gemeinsame Exponent ρ auch ein Theiler von v sein. Bezeichnet nämlich r irgend einen gemeinsamen Divisor der Zahlen γ und γ', so findet die Congruenz $a_1^{\frac{\gamma\gamma'}{r}} \equiv a_2^{\frac{\gamma\gamma'}{r}}$ sowohl modulo K, als auch modulo K', somit auch modulo KK' statt. Es ist demnach ρ ein Theiler jedes Ausdruckes $\frac{\gamma\gamma'}{r}$, also auch ein solcher von v. Diese beiden Bedingungen sind nur erfüllt, wenn $\rho = v$ ist.

Ohne weiteres lässt sich dieser Satz auf eine Reihe von Zahlen $K, K', \ldots K^{(\nu)}$, von denen je zwei relativ prim zu einander sind, ausdehnen.

Man erkennt nunmehr leicht, dass das folgende Verfahren die Lösung des Problems, das am Anfange dieser Arbeit aufgestellt wurde, liefert:

Man bilde zu jedem Theiler δ von γ, die Einheit eingeschlossen, das zugehörige Δ, etwa $\Delta(\delta)$; stelle ferner von jedem $\Delta(\delta)$ alle Divisoren auf, abgesehen von den eventuell durch ein q_i theilbaren und, falls $\delta > 1$ ist, von dem Theiler 1; combiniere schließlich alle diejenigen so erhaltenen Divisorensysteme, deren zugehörige Zahlen δ das kleinste gemeinsame Vielfache γ besitzen, multiplicativ ein jedes Element des einen mit einem jeden Elemente des andern.

Die Ausdrücke $\Delta(\delta)$ und $\Delta(\delta')$ müssen ja bis höchstens auf den Primfactor q_i relativ prim zu einander sein, da zwei Zahlen nur einen Exponenten bezüglich eines bestimmten Moduls gemeinsam haben können.

Auf dem angegebenen Wege erhält man also lauter verschiedene Zahlen, bezüglich welcher a_1 und a_2 den Exponenten γ gemeinsam haben. Man gelangt aber in dieser Weise auch zu allen

Zahlen K, welche die eben angeführte Eigenschaft besitzen und zwar aus folgendem Grunde: Bezüglich eines jeden Primfactors von K haben a_1 und a_2 einen Exponenten δ gemeinsam, welcher Theiler von γ ist. Es tritt mithin der betreffende Primfactor in dem Divisorensysteme von $\Delta(\delta)$ in jener Potenz auf, mit welcher er in K eingeht. Wenn mehrere Primzahlpotenzen in demselben Systeme sich vorfinden, so enthält das Divisorensystem von $\Delta(\delta)$ auch das Product derselben. Die Combination dieser Producte gibt K und das kleinste gemeinschaftliche Vielfache der Zahlen δ ist γ.

XI.

Nachdem somit das mehrfach erwähnte Problem gelöst erscheint, mögen hier noch einige Anwendungen der vorstehenden Ausführungen Platz finden.

Zunächst ist unmittelbar ersichtlich, dass das Theorem 3) die Frage nach der Form der Divisoren von dem Ausdrucke Δ beantwortet, eine Frage, welche erst vor wenigen Jahren von den Herren Lefébure[1]) und Bang[2]) ausführlich behandelt wurde. Man gelangt zu dem folgenden Satze:

Ein jeder Primfactor von Δ, welcher nicht zugleich γ theilt, hat die Form $\mu\gamma + 1$ ($\mu = 1, 2 \ldots$). Von den in γ aufgehenden Primzahlen kann höchstens die größte, nämlich q_1, und diese nur in der ersten Potenz in Δ ohne Rest enthalten sein; und zwar tritt dies dann und nur dann ein, wenn die Zahlen a_1 und a_2 den Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ modulo q_1 gemeinsam haben, so dass dann q_1 die Form

$$\mu \frac{\gamma}{q_1^{\varkappa_1}} + 1 \text{ besitzt.} \qquad 4)$$

Ferner gestattet das Theorem 3) auch die Beantwortung der Frage nach der Existenz von Primzahlen, bezüglich welcher die gegebenen Zahlen a_1 und a_2 den gegebenen Exponenten γ gemeinsam haben; es wird sich nämlich zeigen, dass bis auf besondere Fälle stets $\frac{\Delta}{q_1} > 1$ sein muss, so dass mindestens ein von q_1 verschiedener Primfactor von Δ existiert.

Die Anzahl s der verschiedenen Primtheiler von γ sei $\geqq 1$; der Fall $\gamma = 1$ erledigt sich ja von selbst.

Nimmt man vorerst a_1 und a_2 positiv und $a_1 > a_2$ an, welch'

[1]) Mémoire sur la composition de polynomes entiers, qui n'admettent que des diviseurs premiers d'une forme déterminée. Par M. A. Lefébure. Annales scientifiques de l'école normale supérieur; (3) T. I. 1884, p. 389 u. f.; T. II. p. 113 u. f.

[2]) A. S. Bang, talltheoretiske Undersøgelser. Tidsskrift for Mathematik. (Udg. af Gram og Zeuthen), (5) IV. 1886, p. 70 u. f.; p. 130 u. f.

letztere Voraussetzung übrigens keine Beschränkung der Allgemeinheit in sich birgt, so erhält man unter Beachtung der Relation

$$\varphi(\gamma) = \gamma\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_s}\right)$$

mit Hilfe der Ungleichungen

$$a_1^\mu > a_1^\mu - a_2^\mu = a_1^{\mu-1} + \left[(a_1-1)\,a_1^{\mu-1} - a_2^\mu\right] \geqq a_1^{\mu-1} \quad (\mu = 1, 2, 3\ldots)$$

die Beziehung

$$\Delta_\gamma(a_1, a_2) = \frac{\left(a_1^\gamma - a_2^\gamma\right)\prod\limits_{qq'}\left(a_1^{\frac{\gamma}{qq'}} - a_2^{\frac{\gamma}{qq'}}\right)\cdots}{\prod\limits_{q}\left(a_1^{\frac{\gamma}{q}} - a_2^{\frac{\gamma}{q}}\right)\cdots} > a_1^{\varphi(\gamma)-2^{s-1}},$$

welche sich wegen $a_1 \geqq 2$ in die Form

$$\Delta_\gamma(a_1, a_2) > 2^{\varphi(\gamma)-2^{s-1}}$$

setzen lässt.

In dem Falle, dass $s > 2$ ist, besteht die Relation

$$\varphi(\gamma) - 2^{s-1} = q_1 - 1 + \left\{(q_1-1)\left(\frac{\varphi(\gamma)}{q_1-1} - 1\right) - 2^{s-1}\right\} \geqq q_1 - 1,$$

aus welcher die Ungleichung $\Delta > q_1$ erschlossen werden kann. Die angegebene Relation gilt nämlich für die niedrigste Primzahlencombination $s = 3$, nämlich für $q_1 = 5$, $q_2 = 3$, $q_3 = 2$, also umsomehr für irgend eine andere Auswahl von drei Primzahlen. Findet aber diese Beziehung für alle Annahmen von irgend s Primzahlen statt, so besteht sie auch für alle Annahmen von $s+1$ Primzahlen; denn durch Hinzunahme einer Primzahl q zu einer Combination von s Primzahlen verdoppelt sich zwar der Posten 2^{s-1}, es tritt aber auch zu $\frac{\varphi(\gamma)}{q_1-1}$ mindestens der Factor 2, da man ja q stets größer als 2, aber kleiner als q_1, wählen kann.

Es bleiben nur noch die Fälle $s = 2$ und $s = 1$ zu betrachten übrig.

Tritt das erstere ein, so hat man

$$\varphi(\gamma) - 2^{s-1} = q_1^{\varkappa_1-1}\, q_2^{\varkappa_2-1}\,(q_1-1)\,(q_2-1) - 2$$

und, falls wenigstens ein Exponent $\varkappa_i - 1 > 0$ ist,

$$2^{\varphi(\gamma)-2^{s-1}} \geqq 2^{q_1-1+[(q_1-1)(q_2-1)-2]} > q_1.$$

Für $\varkappa_1 = \varkappa_2 = 1$ ergibt sich nach Ausschluss der Annahme $q_1 = 3$, $q_2 = 2$

$$2^{(q_1-1)(q_2-1)-2} \geqq 1 + (q_1-1)(q_2-1) - 2 + \left(\frac{\overline{q_1-1}\;\overline{q_2-1}-2}{2}\right) > q_1,$$

wenn $q_1 - 3 > 2$ ist; der Fall $q_1 = 5$, $q_2 = 2$ bleibt noch unentschieden.

Nun hat man für $\gamma = 6$

$$\Delta = \frac{(a_1^{2.3} - a_2^{2.3})(a_1 - a_2)}{(a_1^3 - a_2^3)(a_1^2 - a_2^2)} = \frac{a_1^3 + a_2^3}{a_1 + a_2} = a_1(a_1 - a_2) + a_2^2 > 3,$$

sobald $a_1 > 2$ vorausgesetzt wird. Nur wenn $a_1 = 2$, $a_2 = 1$, $\gamma = 6$ ist, ergibt sich eine Ausnahme, indem $\Delta = q_1 = 3$ wird. Für $\gamma = 10$ hingegen hat man stets

$$\Delta = \frac{a_1^5 + a_2^5}{a_1 + a_2} = a_1^3(a_1 - a_2) + a_1 a_2^2 (a_1 - a_2) + a_2^4 > 5.$$

Ist endlich $s = 1$, so ersieht man ebenfalls aus der Ungleichung $\Delta > 2^{q_1^{\varkappa_1 - 1}(q_1-1)-1}$ unmittelbar, dass auch hier $\Delta > q_1$ sein muss, es wäre denn $\varkappa_1 = 1$, $q_1 = 3$ oder $= 2$. Im ersten Falle folgt jedoch $\dfrac{a_1^3 - a_2^3}{a_1 - a_2} = a_1^2 + a_1 a_2 + a_2^2 > 3$; nur wenn $\gamma = 2$ und $\Delta = a_1 + a_2 = 2^\mu$ $(\mu = 2, 3 \ldots)$ ist, gibt es neben 2 keinen Primtheiler von Δ.

Die eben durchgeführte Untersuchung erledigt zugleich den Fall, dass beide Zahlen a_1 und a_2 negativ sind. Es folgt nämlich aus der Gleichung $\Delta_\gamma(a_1, a_2) = \pm \Delta_\gamma(-a_1, -a_2)$, dass hier nur die Ausnahmsfälle $a_1 = -2$, $a_2 = -1$, $\gamma = 6$ und $a_1 + a_2 = -2^\mu$ $(\mu = 2, 3 \ldots)$, $\gamma = 2$ auftreten.

Sind schließlich die beiden Zahlen a_1 und a_2, deren Beträge respective α_1 und α_2 genannt werden mögen, entgegengesetzt bezeichnet, so kann man wieder, ohne die Allgemeinheit zu beschränken, $\alpha_1 > \alpha_2$ annehmen.

Den Fall, dass γ durch 4 theilbar, etwa gleich $4\gamma'$ sei, braucht man keiner weiteren Betrachtung zu unterziehen; die Gleichung $\Delta_{4\gamma'}(a_1, a_2) = \Delta_{4\gamma'}(\alpha_1, \alpha_2)$ führt denselben auf bekannte Fälle zurück.

Ist hingegen γ ungerade, so erhält man

$$\Delta_\gamma(a_1, a_2) = \frac{\left(\alpha_1^\gamma + \alpha_2^\gamma\right) \prod_{qq'} \left(\alpha_1^{\frac{\gamma}{qq'}} + \alpha_2^{\frac{\gamma}{qq'}}\right) \cdots}{\prod_{q} \left(\alpha_1^{\frac{\gamma}{q}} + \alpha_2^{\frac{\gamma}{q}}\right) \cdots} > \frac{\alpha_1^{\varphi(\gamma)}}{2^{2^{s-1}}} \text{ oder}$$

$$\Delta > 2^{\varphi(\gamma)-2^{s-1}},$$

also dieselbe Ungleichung, wie früher. Es kann mithin höchstens für $\gamma = 3$, $\Delta = \frac{\alpha_1^3 + \alpha_2^3}{\alpha_1 + \alpha_2}$, also für $\alpha_1 = 2$, $\alpha_2 = 1$ eine Ausnahme eintreten. Dies entspricht aber den Fällen

$$\begin{cases} a_1 = +2 \\ a_2 = -1 \end{cases} \quad \begin{cases} a_1 = -2 \\ a_2 = +1 \end{cases}, \quad \gamma = 3,$$

für welche thatsächlich $\Delta = 3$ ist.

XII.

Es erübrigt demnach nur mehr zu untersuchen, wie sich Δ verhält, sobald $\gamma = 2\gamma'$ und γ' ungerade vorausgesetzt wird. Unter der Annahme $\gamma' > 1$ besteht die Gleichung

$$\Delta_{2\gamma'}(a_1, a_2) = \frac{\Delta_{\gamma'}(\alpha_1^2, \alpha_2^2)}{\Delta_{\gamma'}(a_1, a_2)} = \Delta_{\gamma'}(\alpha_1, \alpha_2),$$

welche, wie nebenbei bemerkt sei, den Satz lehrt, dass die Primzahlen, bezüglich welcher a_1 und a_2 den Exponenten $2\gamma'$ gemeinsam haben, mit denjenigen übereinstimmen, bezüglich welcher die absoluten Beträge α_1 und α_2 den Exponenten γ' gemeinsam haben. Diese Gleichung lässt erkennen, dass auch in diesem Falle stets $\Delta > q_1$ ist.

Hat man $\gamma = 2$, so bildet natürlich $\Delta = a_1 + a_2 = \pm 2^\mu$ ($\mu = 1, 2 \ldots$) die einzige Ausnahme.

Das Resultat der vorstehenden Betrachtungen lässt sich in dem folgenden Theoreme zusammenfassen:

Sind die beiden gegebenen Zahlen a_1 und a_2 relativ prim zu einander und besitzen sie überdies absolute Beträge, welche nicht zugleich den Wert 1 haben, so existiert stets mindestens eine Primzahl, bezüglich welcher a_1 und a_2 den gegebenen Exponenten γ gemeinsam haben. Auszuschließen hievon sind nur für $\gamma = 1$ alle Werte a_1, a_2, welche der Gleichung $a_1 - a_2 = 1$ genügen; für $\gamma = 2$ alle ganzzahligen Lösungen a_1, a_2 der Gleichungen $a_1 + a_2 = \pm 2^\mu$ ($\mu = 1, 2 \ldots$), so weit sie die obigen an a_1 und a_2 gestellten Forderungen erfüllen; ferner für $\gamma = 3$ die Auswahlen $\begin{cases} a_1 = 2 \\ a_2 = -1 \end{cases}, \begin{cases} a_1 = -2 \\ a_2 = 1 \end{cases}$; endlich für $\gamma = 6$ die Auswahlen $\begin{cases} a_1 = 2 \\ a_2 = 1 \end{cases}, \begin{cases} a_1 = -2 \\ a_2 = -1 \end{cases}$. 5)

Wird nunmehr speciell $a_2 = 1$, a_1 gleich einer ganzen Zahl a, deren absoluter Betrag > 1 ist, vorausgesetzt, so geben die verschiedenen Primfactoren von Δ, abgesehen höchstens von q_1, genau die Primzahlen an, bezüglich welcher a zum Exponenten γ gehört, und der Satz 5) lässt sich in folgender Weise aussprechen:

Es gibt stets mindestens eine Primzahl, bezüglich welcher die gegebene, ganze, von ± 1 verschiedene Zahl a zu dem gegebenen Exponenten γ gehört, mit Ausnahme der Fälle

$$\gamma = 1,\ a = 2;\ \gamma = 2,\ \begin{cases} a = 2^{\mu} - 1 & (\mu = 2, 3 \ldots) \\ a = -2^{\mu} - 1 & (\mu = 1, 2 \ldots) \end{cases};$$

$\gamma = 3$, $a = -2$ und $\gamma = 6$, $a = 2$. Hieran schließt sich von selbst der Satz:

Jede arithmetische Progression $\mu\gamma + 1$ $(\mu = 1, 2 \ldots)$ enthält unendlich viele Primzahlen[1]).

Existiert ja doch wenigstens je eine Primzahl, bezüglich welcher z. B. 4 zum Exponenten γ resp. 2γ, $3\gamma, \ldots$ gehört. Jede dieser Primzahlen muss verschieden sein von allen anderen, da der Modul und die Basis den Exponenten eindeutig bestimmen, und jede derselben hat die Form $\mu\gamma + 1$.

Es ist dies ein specieller Fall des bekannten Legendre'schen Satzes, der zuerst von Dirichlet bewiesen wurde: Das Anfangsglied der Progression ist nämlich gleich 1 angenommen worden; doch gibt der Dirichlet'sche Beweis keine Grenzen für das Auftreten solcher Primzahlen. In dem vorliegenden Falle ersieht man unmittelbar, indem man $a = 2$ setzt, dass, $\gamma \gtrless 6$ vorausgesetzt, spätestens bis zu $\Delta_\gamma(2, 1)$ eine Primzahl der Form $\mu\gamma + 1$ auftreten muss. Ist man in der Progression bis $\gamma\mu' + 1$ vorgeschritten, so braucht man nur das Product P aller bis dahin aufgetretenen Primzahlen zu bilden, um versichert zu sein, dass die Reihe $\gamma\mu' + 1$, $\gamma(\mu' + 1) + 1$ u. s. w. nicht über $\Delta_\gamma(P, 1)$ hinaus fortgesetzt, wenigstens eine Primzahl enthält.

XIII.

Nimmt man in $\Delta_\gamma(P, 1)$ P variabel an, so betritt man das Gebiet der Algebra: $\Delta_\gamma(x, 1)$ ist nämlich das Product der primitiven Wurzelfactoren der Gleichung $x^\gamma - 1 = 0$ und man kann nunmehr das Theorem 3) in der zu Anfang dieser Abhandlung angegebenen Form aussprechen.

Ferner ist leicht einzusehen, dass die Congruenz $\Delta_\gamma(x, 1) \equiv 0 \pmod{p}$, wo p eine Primzahl bedeutet, entweder genau so viele Zahlen zu Wurzeln besitzt, als ihr Grad Einheiten enthält, nämlich die $\varphi(\gamma)$ Zahlen, welche bezüglich p zum Exponenten γ gehören, oder überhaupt keine, jenachdem die Primzahl p, die ungleich q_1 vor-

[1]) Vergl. Bang, l. c. und Lefébure, l. c.

ausgesetzt wird, die Form $\mu\gamma+1$, $(\mu=1, 2\ldots)$ hat oder nicht.[1])

Das erstere pflegte Herr Kronecker in seinen Vorlesungen über Zahlentheorie mittelst des Fermat'schen Satzes zu beweisen, indem er denselben auf die Gleichung $x^{p-1}-1=\prod_{\delta}\Delta_\delta(x, 1)$ anwandte, wo δ alle Theiler von $p-1$ durchlauft. Dass diese Gleichung auch in ihrer allgemeinen Form $x^\gamma-1=\prod_{\delta}\Delta_\delta(x, \delta)$, wo das Product sich auf alle Theiler der ganzen Zahl γ zu erstrecken hat, für jede ganze Zahl und damit nach bekannten Principien identisch stattfindet, ergibt sich auf einfache Weise aus den vorstehend angestellten Betrachtungen; a gehört ja bezüglich eines jeden Factors von $a^\gamma-1$ zu einem Exponenten, der Divisor von γ sein muss. Nicht minder einfach lässt sich die Irreductibilität der Kreistheilungsgleichung $f(x)=\frac{x^q-1}{x-1}=0$, wo q eine Primzahl ist, zeigen; und zwar kann gleich allgemeiner bewiesen werden, dass $f(ax+b)$, falls q nicht in der ganzen Zahl a aufgeht und b eine beliebige ganze Zahl bedeutet, irreductibel ist. $ax+b$ durchläuft nämlich ein vollständiges Restsystem, wenn dies x thut. Für alle Elemente $y=ax_i+b$ $(i=1, 2\ldots q-1)$ desselben mit Ausschluss des einzigen Elementes ax_q+b, welches congruent 1 mod. q ist, enthält nach dem Theorem 4) $f(y)$ nur Primfactoren der Form $\mu q+1$, wo μ eine ganze Zahl ist. Zerfiele nun $f(ax+b)$ in 2 ganze ganzzahlige Factoren $g(x)$ und $h(x)$, so enthielte auch $g(x_i)$ $(i=1, 2\ldots q-1)$ nur Primfactoren der Form $\mu q+1$, hätte also selbst diese Form; die Congruenz $g(x)-1\equiv 0 \pmod q$ hätte also $q-1$ Wurzeln. Sie müsste mithin, falls ihr Grad geringer wäre, als $q-1$, identisch erfüllt sein, was nicht eintreten kann, weil ja schon der Coefficient der höchsten Potenz von x nothwendig prim gegen q ist.

---

[1]) Übrigens nur für $p=q_1=\mu\frac{\gamma}{q_1^{\varkappa_1}}+1$ $(\mu=1, 2\ldots)$ erleidet dieser Satz eine Ausnahme; denn nur dann besitzt die Congruenz $\Delta_\gamma(x, 1)\equiv 0 \pmod{q_1}$ Wurzeln; und zwar sind dies genau die $\varphi\left(\frac{\gamma}{q_1^{\varkappa_1}}\right)$ Zahlen, welche mod q_1 zum Exponenten $\frac{\gamma}{q_1^{\varkappa_1}}$ gehören. — Es sei hier bemerkt, dass nach früheren Entwickelungen das Obige allgemein für die Congruenz $\Delta_\gamma(x, a_2)\equiv 0 \pmod p$ gilt, falls a_2 nicht durch p theilbar ist, und dass man hieraus leicht den folgenden Satz ableiten kann, der die Verallgemeinerung eines für $a_2=1$ bekannten Theorems bildet: Das Product aller derjenigen Zahlen, welche mit einer gegebenen Zahl a_2 den von 1 verschiedenen Exponenten γ bezüglich einer Primzahl $p=\mu\gamma+1$ $(\mu=1, 2\ldots)$ gemeinsam haben, ist modulo p mit $(-a_2)^{\varphi(\gamma)}$ congruent; die Summe derselben ist hingegen $\equiv 0$, wenn in γ ein Quadrat einer ganzen Zahl aufgeht, andernfalls $\equiv\pm a_2$, je nachdem γ das Product einer geraden oder ungeraden Anzahl von Primzahlen ist.