

den Begriff der Congruenz für den gegenwärtigen Zweck dahin ausdehnen, daß zwei ganze rationale Functionen der Perioden für den Modul q , welcher eine ganze Zahl sein soll, congruent heißen sollen, wenn in dem Unterschiede derselben, nachdem er auf die Form $c\eta + c_1\eta_1 + \dots + c_{e-1}\eta_{e-1}$ gebracht worden ist, alle Coëfficienten $c, c_1, c_2, \dots, c_{e-1}$ durch q theilbar sind. Nach dieser Erklärung kann man hier, ebenso wie bei den gewöhnlichen Congruenzen, alle Glieder, welche den Modul q als Factor enthalten, weglassen; auch kann man diese Congruenzen ebenso mit einander addiren, subtrahiren, multipliciren und zu Potenzen erheben.

Wir gehen nun von dem bekannten Satze aus, daß, wenn q eine Primzahl ist, die Coëfficienten $b, b_1, b_2, \dots, b_{q-1}$ des entwickelten Products

$$z(z-1)(z-2)\dots(z-q+1) = z^q - b_1z^{q-1} + b_2z^{q-2} - \dots + b_{q-1}z$$
 alle durch q theilbar sind, mit Ausnahme des letzten b_{q-1} , welcher durch q dividirt den Rest -1 läßt. Es ist nemlich für jeden Werth des z dieses Product, als Product von q auf einander folgenden ganzen Zahlen, durch q theilbar, also ist auch

$$z^q - b_1z^{q-1} + b_2z^{q-2} - \dots + b_{q-1}z \equiv 0 \pmod{q},$$

und da nach dem *Hermatschen* Satze $z^q \equiv z$ ist, so ist auch

$$-b_1z^{q-1} + b_2z^{q-2} - \dots + (b_{q-1} + 1)z \equiv 0 \pmod{q}.$$

Diese Congruenz vom Grade $q-1$ kann aber nicht q verschiedene Wurzeln haben: also muß sie identisch erfüllt werden, woraus $b_1 \equiv b_2 \equiv b_3 \equiv \dots \dots \equiv b_{q-2} \equiv b_{q-1} + 1 \pmod{q}$ folgt.

Nimmt man nun in der obigen Gleichung $z = y - \eta_k$ und läßt die durch q theilbaren Glieder weg, so erhält man die Congruenz

$$\begin{aligned} (A.) \quad & (y - \eta_k)(y - 1 - \eta_k)(y - 2 - \eta_k) \dots (y - q + 1 - \eta_k) \\ & \equiv (y - \eta_k)^q - (y - \eta_k) \pmod{q}. \end{aligned}$$

Bekanntlich sind aber in der binomischen Entwicklung einer q ten Potenz, wenn q eine Primzahl ist, alle Glieder, mit Ausnahme des ersten und letzten, durch q theilbar, also ist $(y - \eta_k)^q \equiv y^q - \eta_k^q$. Ferner, ist η_k ein Polynom von f Gliedern, und wenn ein solches zur q ten Potenz erhoben wird, so sind die Coëfficienten aller Glieder durch q theilbar, mit Ausnahme der q ten Potenzen der einzelnen f Glieder, also ist

$$\eta_k^q \equiv x^{qg^k} + x^{qg^{e+k}} + x^{qg^{2e+k}} + \dots + x^{qg^{(f-1)e+k}} \pmod{q},$$

und wenn $q \equiv g^r \pmod{p}$ ist, so hat man hiernach

$$\eta_k^q \equiv \eta_{r+k} \pmod{q},$$

in dem besondern Falle aber, wo $q = p$ ist,

$$\eta_k^p \equiv f \pmod{p}.$$

Die Congruenz $(y - \eta_k)^q \equiv y^q - \eta_k^q \pmod{q}$ geht also allgemein in $(y - \eta_k)^q \equiv y - \eta_{k+r} \pmod{q}$ über, und für den besondern Fall $q = p$ giebt sie $(y - \eta_k)^p \equiv y - f \pmod{p}$.

Giebt man nun hierin dem k nach einander die Werthe $0, 1, 2, \dots, e-1$ und bildet das Product, so erhält man

$$(\varphi(y))^p \equiv (y - f)^e \pmod{p};$$

woraus folgt, daß $\varphi(y)$ für $y \equiv f$ den Factor p hat, aber für keinen andern Werth des y ; oder daß die Congruenz $\varphi(y) \equiv 0 \pmod{p}$ stets eine reelle Wurzel hat, nemlich $y = f = \frac{p-1}{e}$.

Wir kehren nun zur Untersuchung des allgemeinen Primfactors q zurück, für welchen $q \equiv g^r \pmod{p}$ ist. Vermöge der Congruenz $(y - \eta_k)^q \equiv y - \eta_{k+r}$ verwandelt sich die Congruenz (A.) in folgende:

$$(B.) \quad (y - \eta_k)(y - 1 - \eta_k)(y - 2 - \eta_k) \dots (y - q + 1 - \eta_k) \equiv \eta_k - \eta_{k+r} \pmod{q}.$$

Es sind die beiden Fälle besonders zu betrachten: erstens wo r durch e theilbar ist, und zweitens, wo dies nicht der Fall ist. Ist r durch e theilbar, so ist $\eta_k = \eta_{k+r}$, also

$$(y - \eta_k)(y - 1 - \eta_k)(y - 2 - \eta_k) \dots (y - q + 1 - \eta_k) \equiv 0 \pmod{q}.$$

Setzt man nun nach einander $k = 0, 1, 2, \dots, e-1$ und bildet das Product aller dieser Congruenzen, so erhält man

$$\varphi(y)\varphi(y-1)\varphi(y-2)\dots\varphi(y-q+1) \equiv 0 \pmod{q^e}.$$

Es müssen also immer e dieser Factoren durch q theilbar sein, oder auch einige derselben den Factor q mehreremal enthalten, wenn $q \equiv g^r \pmod{p}$, und r durch e theilbar ist, daß heißt, wenn q ein eter Potenzrest der Primzahl p ist. Hieraus erhält man folgenden Lehrsatz:

„Jede Primzahl, welche ein eter Potenzrest von p ist, ist ein Divisor
 „der Form $\varphi(y)$; oder auch so: die Congruenz $\varphi(y) \equiv 0 \pmod{q}$ hat,
 „wenn der Modul q eine Primzahl und zugleich eter Potenzrest von p
 „ist, immer e reelle Wurzeln, welche in besondern Fällen auch zum
 „Theil einander gleich werden können.“

Der besondere Fall, wo die Perioden eingliedrig, also die imaginären Wurzeln der Gleichung $x^p = 1$ selbst sind, giebt das bekannte Resultat, daß die Congruenz $x^{p-1} + x^{p-2} + x^{p-3} + \dots + x + 1 \equiv 0 \pmod{q}$ stets $p-1$ reelle Wur-

zeln hat, wenn die Primzahl q ein $p-1$ ter Potenzrest von p ist, d. h. wenn $q = 2mp + 1$ ist.

Nachdem gezeigt worden, daß alle diejenigen Primzahlen, welche e te Potenzreste von p sind, Divisoren der Form $\varphi(y)$ sind, ist zweitens zu untersuchen, ob diese Form, aufser diesen genannten und dem Divisor p , noch andere Divisoren haben kann, oder nicht. Es sei also wieder $q \equiv g^r \text{ Mod. } p$, aber r nicht durch e theilbar. In diesem Falle giebt die Congruenz (B.), wenn nach einander $k = 0, 1, 2, \dots, e-1$ gesetzt und das Product gebildet wird:

$$\varphi(y)\varphi(y-1)\varphi(y-2)\dots\varphi(y-q+1) \equiv P \text{ Mod. } q,$$

wo $P = (\eta - \eta_r)(\eta_1 - \eta_{r+1})(\eta_2 - \eta_{r+2})\dots(\eta_{e-1} - \eta_{r+e-1})$ ist.

P , als symmetrische Function aller Perioden, ist eine ganze Zahl. Für bestimmte p und e kann diese Zahl, auch wenn man alle verschiedenen Werthe des r zuläßt, nur eine endliche, bestimmte und verhältnißmäfsig sehr geringe Anzahl verschiedener Primfactoren enthalten, und da $\varphi(y)$ keine andern Primfactoren der genannten Art enthalten kann, als diejenigen, welche auch in P vorkommen, so folgt, daß $\varphi(y)$ nur ausnahmsweise eine stets begrenzte Anzahl solcher Primfactoren enthalten kann, welche nicht e te Potenzreste von p sind. Um näher zu untersuchen, in welchen Fällen dergleichen ausnahmsweise Primfactoren des P , und somit auch des $\varphi(y)$, Statt haben können, gebrauchen wir die Congruenz

$$(\eta_k - \eta_{r+k})^q \equiv \eta_{k+r} - \eta_{k+2r} \text{ Mod. } q,$$

deren Richtigkeit nach den oben aufgestellten Principien in die Augen fällt. Werden beide Seiten dieser Congruenz zu wiederholten Malen zur q ten Potenz erhoben, so erhält man die allgemeinere Congruenz

$$(C.) \quad (\eta_k - \eta_{r+k})^{q^h} \equiv \eta_{hr+k} - \eta_{(h+1)r+k} \text{ Mod. } q.$$

Macht man hierin nacheinander $h = 0, 1, 2, \dots, e-1$ und bildet das Product, so erhält man

$$(\eta_k - \eta_{r+k})^{1+q+q^2+\dots+q^{e-1}} \equiv (\eta_k - \eta_{r+k})(\eta_{r+k} - \eta_{2r+k})\dots(\eta_{(e-1)r+k} - \eta_{er+k}) \text{ Mod. } q.$$

Wenn nun r keinen gemeinschaftlichen Factor mit e hat, so sind die Indices der Perioden $k, r+k, 2r+k, \dots, (e-1)r+k$, in anderer Ordnung genommen, den Indices $0, 1, 2, \dots, e-1$ congruent, für den Modul e ; das Product rechterhand ist also kein anderes als das Product P , und da P nach der Voraussetzung durch q theilbar sein soll, so hat man

$$(\eta_k - \eta_{r+k})^{1+q+q^2+\dots+q^{e-1}} \equiv 0 \text{ Mod. } q.$$

Wenn nun zur Potenz $q-1$ erhoben wird, so ist

$$(\eta_k - \eta_{r+k})^{q-1} \equiv 0 \pmod{q},$$

und, wenn mit $\eta_k - \eta_{r+k}$ multiplicirt wird,

$$(\eta_k - \eta_{k+r})^{q^e} \equiv 0 \pmod{q},$$

woraus nach der Congruenz (C.) folgt:

$$\eta_k - \eta_{r+k} \equiv 0 \pmod{q};$$

welches unmöglich ist. Das Product P hat also keinen Primfactor q von der Art, daß $q \equiv g^r \pmod{p}$, wo r keinen gemeinschaftlichen Factor mit e hat. Für den Fall also, wo e Primzahl ist, hat man folgenden Lehrsatz:

„Die Form $\varphi(y)$ hat, wenn der Grad derselben e eine Primzahl ist, außer dem Divisor p nur solche Divisoren, welche e te Potenzreste von p sind.”

Für den Fall aber, wo der Grad der Form $\varphi(y)$ keine Primzahl ist, kann man das gefundene Resultat folgendermaassen aussprechen.

„Die Form $\varphi(y)$ hat außer dem Divisor p im allgemeinen nur solche Primzahlen zu Divisoren, welche e te Potenzreste von p sind; außerdem aber kann sie auch eine endliche bestimmte Anzahl anderer Divisoren haben, welche, wenn e die von Eins verschiedenen Divisoren $\alpha, \beta, \gamma, \dots$ enthält, α te oder β te oder γ te Potenzreste von p sein müssen.”

Man kann die Bedingungen, unter welchen $\varphi(y)$ solche besondere Divisoren enthält, die nicht e te Potenzreste sind, noch etwas genauer angeben. Wenn nemlich r und e den größten gemeinschaftlichen Factor α enthalten, und $r = r'\alpha$, $e = e'\alpha$ ist, so setze man in der Congruenz (C.) nach einander $h = 0, 1, 2, \dots, e'-1$ und bilde das Product der so erhaltenen Congruenzen:

$$\eta_k - \eta_{r+k}^{1+q+q^2+\dots+q^{e'-1}} \equiv (\eta_k - \eta_{r+k})(\eta_{r+k} - \eta_{2r+k}) \dots (\eta_{(e'-1)r+k} - \eta_{e'r+k}).$$

Giebt man hierin wieder dem k die Werthe $0, 1, 2, \dots, \alpha-1$ und bildet das Product, so wird dieses Product auf der rechten Seite gleich P ; wovon man sich sogleich überzeugt, wenn man bemerkt, daß die Zahlen von der Form $hr+k$ für $h = 0, 1, 2, \dots, e'-1$ und $k = 0, 1, 2, \dots, \alpha-1$, wenn $r = r'\alpha$ und $e = e'\alpha$, für den Modul e alle Reste $0, 1, 2, 3, \dots, e-1$ geben. Man hat also, da P durch q theilbar sein soll,

$$\{(\eta - \eta_r)(\eta_1 - \eta_{r+1}) \dots (\eta_{\alpha-1} - \eta_{\alpha+r-1})\}^{1+q+q^2+\dots+q^{e'-1}} \equiv 0 \pmod{q}.$$

Erhebt man wieder zur Potenz $q-1$ und multiplicirt mit $(\eta - \eta_r)(\eta_1 - \eta_{r+1}) \dots (\eta_{\alpha-1} - \eta_{\alpha+r-1})$, so folgt hieraus

$$\{(\eta - \eta_r)(\eta_1 - \eta_{r+1}) \dots (\eta_{\alpha-1} - \eta_{\alpha+r-1})\}^{q^{e'}} \equiv 0 \pmod{q},$$

welches vermöge der Congruenz (C.) folgende einfachere Form annimmt:

$$(\eta - \eta_r)(\eta_1 - \eta_{r+1}) \dots (\eta_{a-1} - \eta_{a+r-1}) \equiv 0 \text{ Mod. } q.$$

Es müssen also schon die ersten α Factoren des Products P den Factor q enthalten, damit P oder $\varphi(y)$ denselben enthalten könne. Man könnte durch diese einschränkende Bedingung auf die Vermuthung kommen, dafs diese ausnahmsweisen Factoren, welche nicht *ete* Potenzreste sind, auch wenn e eine zusammengesetzte Zahl ist, überhaupt gar nicht vorkommen dürften: dafs dieses indefs nicht der Fall ist, vielmehr wirklich dergleichen Factoren Statt haben, kann man an folgendem einfachen Beispiele sehen. Nimmt man $p = 109$, $e = 6$, so erhält man nach bekannten Methoden:

$$\varphi(y) = y^6 + y^5 - 45y^4 - 10y^3 + 135y^2 + 9y - 27,$$

woraus sich leicht für $y = 0, 1, 2, 3, 4, 5$ folgende Werthe des $\varphi(y)$ berechnen lassen: $\varphi(0) = -3^3$; $\varphi(1) = 2^6$; $\varphi(2) = -173$; $\varphi(3) = -2^6 \cdot 3^3$; $\varphi(4) = -4871$; $\varphi(5) = -2^6 \cdot 113$. Die hierin vorkommenden Divisoren 2 und 3 sind keine 6ten Potenzreste von 109; dieselben sind also solche ausnahmsweise Divisoren; und es ist 2 ein cubischer Rest und 3 quadratischer Rest von 109; welches sehr wohl mit dem oben gefundenen Lehrsatz stimmt. Übrigens sind 2 und 3 im gegenwärtigen Falle die einzigen Primfactoren von $\varphi(y)$, welche nicht sechste Potenzreste sind.

Wir zeigen nun noch von zwei wichtigen speciellen Fällen, dafs für sie dergleichen Factoren, welche nicht *ete* Potenzreste von p sind, niemals Statt haben können: nemlich für den Fall, wo die Perioden eingliedrig, und wo sie zweigliedrig sind. Ist $e = p - 1$ und $f = 1$, so ist $\eta = x$, $\eta_1 = x^e$, $\eta_2 = x^{e^2}$ etc.; es ist also

$$P = (x - x^e)(x^e - x^{e^2}) \dots (x^{e^{p-2}} - x^{e^{p-1}}),$$

und wenn man von dem ersten Factor x , vom zweiten x^e , vom dritten x^{e^2} etc., heraushebt, so wird

$$P = (1 - x^{e-1})(1 - x^{e(g-1)}) \dots (1 - x^{e^{p-2}(g-1)}),$$

und da

$$(z - x^m)(z - x^{mg}) \dots (z - x^{m \cdot e^{p-2}}) = z^{p-1} + z^{p-2} + \dots + z + 1$$

ist, so hat man, wenn $z = 1$ und $m = g - 1$ genommen wird,

$$P = p.$$

Da nun P keinen andern Factor enthält als p , so folgt hieraus der bekannte Lehrsatz: dafs die Form $y^{p-1} + y^{p-2} + \dots + y + 1$ aufser dem Divi-

sor p nur solche Divisoren enthalten kann, welche $p-1$ te Potenzreste von p sind, deren lineäre Form also $q = 2mp + 1$ ist.

Wenn ferner die Perioden zweigliedrig sind, also $e = \frac{1}{2}(p-1)$, $f = 2$ ist, so ist $\eta = x + x^{-1}$, $\eta_1 = x^g + x^{-g}$, $\eta_2 = x^{g^2} + x^{-g^2}$ etc., und es wird für diesen Fall bekanntlich

$$\varphi(y) = y^e + y^{e-1} - \frac{e-1}{1} y^{e-2} - \frac{e-2}{1} y^{e-3} + \frac{(e-2)(e-3)}{1 \cdot 2} y^{e-4} + \frac{(e-3)(e-4)}{1 \cdot 2} y^{e-5} - \dots$$

Ferner ist

$$\eta_k - \eta_{r+k} = x^{g^k} + x^{-g^k} - x^{g^{r+k}} - x^{-g^{r+k}},$$

welcher Ausdruck folgendermaassen in Factoren zerfällt:

$$\eta_k - \eta_{r+k} = x^{g^k} (1 - x^{(g^r-1)g^k}) (1 - x^{-(g^r+1)g^k}).$$

Giebt man nun dem k die Werthe 0, 1, 2, ..., $p-2$ und bildet das Product, so erhält man leicht

$$P^2 = p^2, \text{ also } P = \pm p.$$

In diesem Falle hat also P ebenfalls keinen andern Divisor als p , woraus folgt, daß die Form

$$\varphi(y) = y^e + y^{e-1} - \frac{e-1}{1} y^{e-2} - \frac{e-2}{1} y^{e-3} + \dots$$

aufser dem Divisor p nur solche Divisoren hat, welche $\frac{1}{2}(p-1)$ te Potenzreste von p sind, also von der Form $2mp \pm 1$.

Dieselbe Methode, welche in dem Vorhergehenden für die Form $\varphi(y)$ angewendet wurde, giebt fast ganz in derselben Weise die Primfactoren einer weit allgemeineren, sehr merkwürdigen Form vom e ten Grade mit e unbestimmten Zahlen. Wenn man nemlich folgende zusammengehörige lineäre Functionen der Perioden:

$$F(\eta) = z\eta + z_1\eta_1 + z_2\eta_2 + \dots + z_{e-1}\eta_{e-1},$$

$$F(\eta_1) = z\eta_1 + z_1\eta_2 + z_2\eta_3 + \dots + z_{e-1}\eta,$$

$$\dots \dots \dots$$

$$F(\eta_{e-1}) = z\eta_{e-1} + z_1\eta + z_2\eta_1 + \dots + z_{e-1}\eta_{e-2}$$

mit einander multiplicirt, so wird das Product derselben

$$\Psi = F(\eta) F(\eta_1) F(\eta_2) \dots F(\eta_{e-1})$$

eine homogene Form vom e ten Grade der e unbestimmten Zahlen $z, z_1, z_2, \dots, z_{e-1}$, mit ganzzahligen Coëfficienten; welche Form, wie wir sogleich zeigen

werden, in Beziehung auf ihre Divisoren ganz mit der oben untersuchten specielleren Form $\varphi(y)$ übereinstimmt. Wir beweisen zunächst folgenden Lehrsatz:

„Jede Primzahl q , welche ein eter Potenzrest von p ist, so wie auch p selbst, ist ein Divisor der Form Ψ .“

Untersuchen wir zuerst den Divisor p , so haben wir, nach denselben Principien, welche oben angewendet wurden,

$$F(\eta_k)^p \equiv (z + z_1 + z_2 + \dots + z_{e-1})f. \text{ Mod } p,$$

also, wenn die unbestimmten Zahlen $z, z_1, z_2, \dots, z_{e-1}$ so bestimmt werden, daß ihre Summe durch p theilbar ist, so wird $F(\eta_k)^p \equiv 0 \text{ Mod. } p$, und wenn man $k = 0, 1, 2, \dots, e-1$ setzt und diese Congruenzen mit einander multiplicirt, so erhält man $\Psi^p \equiv 0 \text{ Mod. } p$, also auch $\Psi \equiv 0 \text{ Mod. } p$; p ist also ein Divisor der Form Ψ .

Um weiter zu beweisen, daß auch jede Primzahl q , welche ein eter Potenzrest von p ist, immer Divisor von Ψ sei, setze ich die zweite Periode η als ganze rationale Function der ersten Periode η dargestellt; welches bekanntlich immer möglich ist. Es sei also $\eta_1 = \theta(\eta)$, so ist $\eta_2 = \theta\theta(\eta)$, $\eta_3 = \theta\theta\theta(\eta)$ etc. Statt η aber werde eine unbestimmte Gröfse y genommen und folgender Ausdruck gebildet:

$$F(y) \cdot F(\theta y) \cdot F(\theta\theta y) \dots F(\theta^{e-1}y) - \Psi,$$

welcher eine ganze rationale Function von y sein wird. Derselbe verschwindet offenbar, wenn $y = \eta$ oder $y = \eta_1$ oder $y = \eta_2$ etc. genommen wird, und muß deshalb den Factor $(y - \eta)(y - \eta_1)(y - \eta_2) \dots (y - \eta_{e-1})$ enthalten, welchen wir oben durch $\varphi(y)$ bezeichnet haben. Es ist demnach

$$F(y)F(\theta y)(F\theta\theta y) \dots F(\theta^{e-1}y) - \Psi = \varphi(y) \cdot \Phi,$$

wo auch Φ eine ganze rationale Function von y bedeutet. Wird nun für y irgend eine Wurzel der Congruenz $\varphi(y) \equiv 0 \text{ Mod. } q$ genommen (welche, wenn q ein eter Potenzrest von p ist, immer e reale Wurzeln hat, wie wir oben gezeigt haben), so hat man:

$$F(y)F(\theta y)F(\theta\theta y) \dots F(\theta^{e-1}y) \equiv \Psi \text{ Mod. } q.$$

Wenn also irgend ein Factor dieses Productes durch q theilbar wird, so wird allemal auch Ψ durch q theilbar. Es lassen sich daher die unbestimmten Zahlen $z, z_1, z_2, \dots, z_{e-1}$ immer so bestimmen, daß die Form Ψ den Divisor q erhält, und die Bestimmung derselben ist einfach die, daß, wenn man in

$$F(\eta) = z\eta + z_1\eta_1 + z_2\eta_2 + \dots + z_{e-1}\eta_{e-1}$$

für $\eta, \eta_1, \eta_2, \dots, \eta_{e-1}$ nicht mehr die Wurzeln der Gleichung $\varphi(g) = 0$,

sondern die Wurzeln der Congruenz $\varphi(\gamma) \equiv 0 \pmod{q}$, aber in der gehörigen Ordnung genommen, substituirt hat, $F(\eta) \equiv 0 \pmod{q}$ werden mufs.

Die Primfactoren, welche *ete* Potenzreste von p sind, machen auch hier die hauptsächlichsten Divisoren der Form Ψ aus, und aufser diesen haben gewisse andere nur ausnahmsweise Statt, deren Bedingungen wir jetzt näher untersuchen wollen. Es sei q eine Primzahl, von der Art, dafs $q \equiv g^r \pmod{p}$ und r nicht durch e theilbar ist, so ist

$$F(\eta)^q \equiv F(\eta_r) \pmod{q}.$$

Erhebt man dies nun zu wiederholten Malen zur Potenz q , so erhält man

$$F(\eta)^{q^h} \equiv F(\eta_{hr}) \pmod{q}.$$

Setzt man nach einander $h = 0, 1, 2, 3, \dots, e-1$ und multiplicirt die so erhaltenen Congruenzen in einander, so wird

$$F(\eta)^{1+q+q^2+\dots+q^{e-1}} \equiv F(\eta)F(\eta_r)F(\eta_{2r}) \dots F(\eta_{(e-1)r}) \pmod{q}.$$

Wenn nun r und e keinen gemeinschaftlichen Factor haben, so sind die Indices $0, r, 2r, 3r, \dots, (e-1)r$ den Indices $0, 1, 2, \dots, e-1$, in anderer Ordnung genommen, congruent für den Modul e , also ist das Product rechterhand gleich Ψ . Soll nun Ψ den Divisor q enthalten, so folgt, dafs

$$F(\eta)^{1+q+q^2+\dots+q^{e-1}} \equiv 0 \pmod{q}$$

sein mufs, woraus, ebenso wie oben, $F(\eta) \equiv 0 \pmod{q}$ folgt. Damit aber $F(\eta)$ durch q theilbar sei, müssen alle einzelnen Coëfficienten der Perioden, also die Unbestimmten $z, z_1, z_2, \dots, z_{e-1}$, durch q theilbar sein. Hieraus erhalten wir folgenden Lehrsatz:

„Wenn die unbestimmten Zahlen der Form Ψ nicht alle einen gemeinschaftlichen Factor haben, so enthält diese Form aufser dem Divisor p nur solche Primfactoren, welche *ete* Potenzreste von p sind; oder: wenn e die von Eins verschiedenen Divisoren $\alpha, \beta, \gamma, \dots$ enthält, so kann die Form auch solche Primfactoren enthalten, welche *ate* oder β te oder γ te \dots Potenzreste von p sind.“

Daraus geht auch folgender Zusatz hervor:

„Wenn die unbestimmten Zahlen der Form Ψ nicht alle einen gemeinschaftlichen Factor enthalten, und der Grad e dieser Form ist eine Primzahl, so enthält dieselbe aufser dem Divisor p nur solche Divisoren, welche *ete* Potenzreste von p sind.“

Ist e nicht eine Primzahl, sondern α ein Divisor von e , so sei $q \equiv g^r \pmod{p}$ und α der grösste gemeinschaftliche Factor von r und e , so dafs $r \equiv r'\alpha$ und

$e = e'\alpha$. In diesem Falle hat man, vermöge der Congruenz

$$F(\eta_k^{q^h}) \equiv F(\eta_{r_h+k}) \pmod{q},$$

wenn nach einander $h = 0, 1, 2, \dots, e'-1$ gesetzt wird und sodann für jeden einzelnen dieser Werthe des h die Zahl k die Werthe $0, 1, 2, \dots, \alpha-1$ bekommt,

$$\{F(\eta)F(\eta_1)F(\eta_2)\dots F(\eta_{\alpha-1})\}^{1+q+q^2+\dots+q^{e'-1}} \equiv \Psi \pmod{q};$$

denn das Product rechter Hand wird offenbar gleich Ψ , weil $hr+k$ für die angegebenen Werthe des h und k allen den Zahlen $0, 1, 2, \dots, e-1$ congruent wird, für den Modul e . Soll nun Ψ den Factor q haben, so folgt, daß

$$\{F(\eta)F(\eta_1)\dots F(\eta_{\alpha-1})\}^{1+q+q^2+\dots+q^{e'-1}} \equiv 0 \pmod{q}$$

sein muß, woraus man leicht folgert, daß auch

$$F(\eta)F(\eta_1)F(\eta_2)\dots F(\eta_{\alpha-1}) \equiv 0 \pmod{q}$$

sein muß. Damit also Ψ einen Primfactor q habe, welcher nicht e ter Potenzrest, sondern nur α ter Potenzrest von p ist, wo α ein Divisor von e , muß allemal schon das Product der ersten α Factoren des Ψ diesen Factor q enthalten.