Ueber die Irreductibilität ganzzahliger ganzer Functionen.

Von

Eugen Netto in Giessen.

Eisenstein hat den Beweis der Irreductibilität der Kreistheilungsgleichung für Primzahlen und Primzahlpotenzen auf den Satz gestützt: *Wenn in einer ganzzahligen ganzen Function*

(1) $$f(z) = z^n + c_1 z^{n-1} + c_2 z^{n-2} + \cdots + c_n$$

alle Coefficienten c_λ *durch eine Primzahl* p *theilbar sind,* c_n *aber durch keine höhere Potenz von* p, *dann ist* f *unzerlegbar.*

Herr Königsberger hat im 115. Bande des Journ. f. Math. Erweiterungen dieses Satzes gegeben. Nach anderer Richtung und mit anderen Hülfsmitteln als dies dort geschehen ist, wollen wir hier den Eisenstein'schen Satz als Anfangsglied einer ganzen Reihe ähnlicher Theoreme nachweisen.

I. *Ein Polynom von der Gestalt*

(2) $$z^n + \gamma_1 p z^{n-1} + \cdots + \gamma_{n-\varkappa-1} p z^{\varkappa+1} + \gamma_{n-\varkappa} p^2 z^\varkappa + \gamma_{n-\varkappa+1} p^2 z^{\varkappa-1} + \cdots + \gamma_n^0 p^2,$$

in welchem γ_n^0 *eine gegen* p *theilerfremde ganze Zahl bedeutet, und* $n > 2\varkappa$ *ist, besitzt keinen Theiler von geringerem als dem* $(\varkappa+1)^{ten}$ *Grade.* Auch im Folgenden soll der obere Index 0 an einer Constanten andeuten, dass diese Constante zu p theilerfremd ist.

Gilt für (2) die Zerlegung

(3) $$(z^\mu + a_1 z^{\mu-1} + \cdots + a_\mu)(z^\nu + b_1 z^{\nu-1} + \cdots + b_\nu) \qquad (\mu + \nu = n),$$

dann folgt aus $a_\mu b_\nu = \gamma_n^0 p^2$ entweder, dass einer der beiden Coefficienten a_μ, b_ν durch p^2, oder dass jeder durch p theilbar ist. Der erste Fall

$$a_\mu = \alpha_\mu^0 p^2, \qquad b_\nu = \beta_\nu^0$$

leitet auf dem durch Eisenstein gegebenen Wege durch

$$c_{n-1} = \gamma_{n-1} p^2 = \alpha_\mu^0 p^2 b_{\nu-1} + a_{\mu-1} \beta_\nu^0 \equiv 0 \pmod{p}$$

u. s. w. zu der Einsicht, dass $a_{\mu-1}$ und dann ebenso $a_{\mu-2}, \ldots$ durch p theilbar sein müssen. Bei $a_0 = 1$ tritt dann ein Widerspruch heraus.

Man darf deshalb nur

$$a_\mu = \alpha_\mu^0 p, \quad b_\nu = \beta_\nu^0 p \tag{4}$$

setzen, und nun wollen wir annehmen, es wäre schon bewiesen, dass

$$\begin{aligned} a_{\mu-1} &= \alpha_{\mu-1} p, \ldots a_{\mu-\lambda} = \alpha_{\mu-\lambda} p, \\ b_{\nu-1} &= \beta_{\nu-1} p, \ldots b_{\nu-\lambda} = \beta_{\nu-\lambda} p \end{aligned} \tag{5}$$

ist, was ja nach (4) für $\lambda = 0$ wirklich feststeht. Daraus leiten wir dann her, dass, wenn λ eine gewisse Grenze nicht überschreitet, auch

$$a_{\mu-\lambda-1} = \alpha_{\mu-\lambda-1} p, \quad b_{\nu-\lambda-1} = \beta_{\nu-\lambda-1} p \tag{5a}$$

sein muss. Dazu betrachten wir

$$c_{n-\lambda-1} \equiv 0 \pmod{p^2} \quad \text{und} \quad c_{n-2\lambda-2} \equiv 0 \pmod{p};$$

das ergiebt

$$\begin{aligned} a_\mu b_{\nu-\lambda-1} + \cdots + a_{\mu-\lambda-1} b_\nu &\equiv 0 \pmod{p^2}, \\ a_{\mu-\lambda-1} b_{\nu-\lambda-1} + \cdots\cdots\cdots &\equiv 0 \pmod{p}. \end{aligned} \tag{6}$$

Wir haben in diese Congruenzen die Werthe aus (4) und (5) einzusetzen. Dann werden in der ersten alle nicht hingeschriebenen Mittelglieder durch p^2, die hingeschriebenen äusseren Glieder durch p theilbar. Dividirt man durch p, dann entsteht

$$\alpha_\mu^0 b_{\nu-\lambda-1} + a_{\mu-\lambda-1} \beta_\nu^0 \equiv 0 \pmod{p}. \tag{7}$$

In der zweiten Congruenz aus (6) werden alle nicht hingeschriebenen Glieder durch p theilbar; das erste muss daher auch durch p theilbar sein, und somit ist auch

$$(\alpha_\mu^0 b_{\nu-\lambda-1}) \cdot (a_{\mu-\lambda-1} \beta_\nu^0) \equiv 0 \pmod{p}, \tag{8}$$

woraus dann in Verbindung mit (7) sofort die Behauptung (5a) folgt.

Da bei uns in der Form (2) der Coefficient $\gamma_{n-\varkappa} p^2$ noch durch p^2 und $\gamma_1 p$ noch durch p theilbar ist, so können wir in (5) bis $\lambda = \varkappa$ gehen, und erst dann bricht die Folgerungsmöglichkeit ab. Dabei muss aber gleichzeitig noch $\gamma_{n-2\varkappa} p$ zu den Coefficienten von (2) gehören, und daher erklärt sich die Nothwendigkeit der Annahme von $n > 2\varkappa$.

In die Reihe (5) für $\lambda = \varkappa$ darf nun weder $a_0 = 1$ noch $b_0 = 1$ eingehen, d. h. es ist $\mu > \varkappa$, $\nu > \varkappa$, so dass also keiner der beiden Factoren von geringerem als dem $(\varkappa+1)^{\text{ten}}$ Grade sein kann. Damit ist I. bewiesen.

Ist $n = 2\varkappa + 1$, dann folgt die Irreductibilität von (2), da ja kein Factor von geringerem als dem $(\varkappa+1)^{\text{ten}}$ Grade existiren kann. Ist $n = 2\varkappa + 2$, dann kann (2) nach I. nur in zwei irreductible Factoren $(\varkappa+1)^{\text{ten}}$ Grades zerfallen, deren Coefficienten sämmtlich als durch p theilbar nachgewiesen sind. So erhalten wir den Satz:

II. *Das Polynom*

$$z^{2\varkappa+1} + \gamma_1 p z^{2\varkappa} + \cdots + \gamma_\varkappa p z^{\varkappa+1} + \gamma_{\varkappa+1} p^2 z^\varkappa + \cdots + \gamma_{2\varkappa+1}^0 p^2$$

ist irreductibel (vgl. Königsberger). *Das Polynom*

$$z^{2\varkappa+2}+\gamma_1 p z^{2\varkappa+1}+\cdots+\gamma_{\varkappa+1} p z^{\varkappa+1}+\gamma_{\varkappa+2} p^2 z^{\varkappa}+\cdots+\gamma_{2\varkappa+2}^{0} p^2$$

kann nur in der Form

$$(z^{\varkappa+1}+\alpha_1 p z^{\varkappa}+\cdots+\alpha_{\varkappa+1}^{0} p)(z^{\varkappa+1}+\beta_1 p z^{\varkappa}+\cdots+\beta_{\varkappa+1}^{0} p)$$

zerfallen; die beiden dabei auftretenden Factoren sind irreductibel.

Wir knüpfen weiter an das Theorem I. an.

III. *Ein Polynom von der Gestalt*

$$(9)\qquad \begin{aligned} &z^n+\gamma_1 p z^{n-1} &&+\cdots+\gamma_{n-2\varkappa-2} p z^{2\varkappa+2}\\ &+\gamma_{n-2\varkappa-1} p^2 z^{2\varkappa+1} &&+\cdots+\gamma_{n-\varkappa-1} p^2 z^{\varkappa+1}\\ &+\gamma_{n-\varkappa} p^3 z^{\varkappa} &&+\cdots+\gamma_{n-1} p^3 z+\gamma_n^{(0)} p^3 \end{aligned}\qquad (n>3\varkappa)$$

kann nur so in zwei Factoren zerfallen, dass der Grad des einen nicht geringer als $(\varkappa+1)$, *der der andern nicht geringer als* $(2\varkappa+2)$ *ist.*

Gilt wieder für (9) die Zerlegung (3) und setzt man

$$a_\mu=\alpha_\mu^0 p^3,\quad b_\nu=\beta_\nu^0,$$

so zeigt sich auf dem bereits oben angedeuteten Wege der Widerspruch gegen die Zerlegbarkeit. Es muss demnach

$$(10)\qquad a_\mu=\alpha_\mu^0 p^2,\quad b_\nu=\beta_\nu^0 p$$

gesetzt werden. Aus

$$c_{n-1}=a_\mu b_{\nu-1}+a_{\mu-1} b_\nu=\gamma_{n-1} p^3$$

ergiebt sich sofort wegen (10)

$$(11)\qquad a_{\mu-1}=\alpha'_{\mu-1} p.$$

Wir setzen voraus, es gälte, was für $\lambda=1$ eben bewiesen ist,

$$(12)\qquad \begin{aligned} a_{\mu-1}&=\alpha_{\mu-1} p^2, \ldots\ a_{\mu-\lambda+1}=\alpha_{\mu-\lambda+1} p^2,\\ a_{\mu-\lambda}&=\alpha'_{\mu-\lambda} p, \ldots\ a_{\mu-2\lambda+1}=\alpha'_{\mu-2\lambda+1} p,\\ b_{\nu-1}&=\beta_{\nu-1} p, \ldots\ b_{\nu-\lambda+1}=\beta_{\nu-\lambda+1} p; \end{aligned}$$

dann wollen wir zeigen, dass, wenn λ eine gewisse Grenze nicht überschreitet, auch noch

$$(13)\qquad a_{\mu-\lambda}=\alpha_{\mu-\lambda} p^2;\quad a_{\mu-2\lambda}=\alpha'_{\mu-2\lambda} p,\quad a_{\mu-2\lambda-1}=\alpha'_{\mu-2\lambda-1} p;\quad b_{\nu-\lambda}=\beta_{\nu-\lambda} p$$

sein muss. Dazu brauchen wir die vier Congruenzen

$$(14)\qquad \begin{aligned} c_{n-\lambda}&\equiv 0\ (\text{mod. } p^3),\quad c_{n-2\lambda}\equiv 0\ (\text{mod. } p^2),\\ c_{n-2\lambda-1}&\equiv 0\ (\text{mod. } p^2),\quad c_{n-3\lambda}\equiv 0\ (\text{mod. } p). \end{aligned}$$

Setzen wir die Werthe (10), (11), (12) in diese Congruenzen ein, dann liefert $c_{n-2\lambda}\equiv 0$ nach Division durch p, und $c_{n-3\lambda}\equiv 0$ nach Multiplication mit $\beta_\nu^0 \cdot \alpha'_{\mu-\lambda}$ die beiden Congruenzen

$$\left.\begin{array}{l}(\beta_\nu^0 a_{\mu-2\lambda}) + (\alpha'_{\mu-\lambda} b_{\nu-\lambda}) \equiv 0 \\ (\beta_\nu^0 a_{\mu-2\lambda}) \quad (\alpha'_{\mu-\lambda} b_{\nu-\lambda}) \equiv 0\end{array}\right\} \pmod{p},$$

und deshalb ergiebt sich, wie unmittelbar ersichtlich ist,

$$\text{(13a)} \qquad a_{\mu-2\lambda} = \alpha'_{\mu-2\lambda} p,$$

$$\text{(15)} \qquad \alpha'_{\mu-\lambda} \,.\, b_{\nu-\lambda} \equiv 0 \qquad \pmod{p}.$$

Hier ist durch (13a) schon ein Theil der Behauptungen (13) bewiesen. Mit (15) combiniren wir die erste Congruenz aus (14), tragen wieder (10), (11), (12) in sie ein, heben durch p^2 und erhalten

$$\alpha'_{\mu-\lambda} \beta_\nu^0 + \alpha_\mu^0 b_{\nu-\lambda} \equiv 0 \pmod{p}.$$

Das liefert mit (15) zusammen weitere Theile von (13), nämlich

$$\text{(13b)} \qquad \begin{array}{l} b_{\nu-\lambda} = \beta_{\nu-\lambda} p, \\ a_{\mu-\lambda} = \alpha'_{\mu-\lambda} p = \alpha_{\mu-\lambda} p^2. \end{array}$$

Der noch fehlende Theil der Behauptung geht ohne Weiteres aus $c_{n-2\lambda-1} \equiv 0 \pmod{p^2}$ hervor. Denn hierin bleibt, wenn man alle bisherigen Resultate einträgt, nur $a_{\mu-2\lambda-1} \beta_\nu^0 p \equiv 0 \pmod{p^2}$ zurück, und damit ist auch

$$\text{(13c)} \qquad a_{\mu-2\lambda-1} = \alpha'_{\mu-2\lambda-1} p$$

nachgewiesen.

Bei der Form (9) des Polynoms sieht man, dass (12) bis zu $\lambda = (\varkappa + 1)$ fortgesetzt werden kann. Nur darf $a_0 = 1$ und $b_0 = 1$ nicht unter den in (12) enthaltenen Coefficienten auftreten; daher muss $\mu \geqq 2\varkappa + 2$, $\nu \geqq \varkappa + 1$ sein. Damit ist III. bewiesen.

Es war $n > 3\varkappa$ zu nehmen. Ist $n = 3\varkappa + 1$ oder $n = 3\varkappa + 2$, so wird $\mu + \nu \geqq 3\varkappa + 3 > n$; in diesen Fällen ist demnach eine Zerlegung nicht möglich. Ist dagegen $n = 3\varkappa + 3$, dann kann $\mu = 2\varkappa + 2$, $\nu = \varkappa + 1$ sein, und daher ist ein Zerfallen des Polynoms nicht ausgeschlossen.

In beiden Factoren müssen die Coefficienten den Gleichungen (12) gemäss gebildet sein. So liefert

$$(z^2 + \alpha_1' p z + \alpha_2^0 p^2)(z + \beta^0 p) = z^3 + (\alpha_1' + \beta^0) p z^2 + (\alpha_2^0 + \alpha_1' \beta^0) p^2 z + \alpha_2^0 \beta^0 p^3$$

ein Beispiel für eine solche Zerlegung. Wir haben also:

IV. *Die Polynome von der Form*

$$\begin{array}{lll} z^n + \gamma_1 p z^{n-1} & + \cdots + \gamma_{n-2\varkappa-2} p z^{2\varkappa+2} & \\ \quad + \gamma_{n-2\varkappa-1} p^2 z^{2\varkappa+1} & + \cdots + \gamma_{n-\varkappa-1} p^2 z^{\varkappa+1} & (n = 3\varkappa+1, 3\varkappa+2) \\ \quad + \gamma_{n-\varkappa} p^3 z^\varkappa & + \cdots + \gamma_{n-1} p^3 z + \gamma_n^0 p^3 & \end{array}$$

sind irreductibel, diejenigen von der Form

$$\begin{aligned} z^{3\varkappa+3} &+ \gamma_1 p z^{3\varkappa+2} + \cdots + \gamma_{\varkappa+1} p z^{2\varkappa+2} \\ &+ \gamma_{\varkappa+2} p^2 z^{2\varkappa+1} + \cdots + \gamma_{2\varkappa+2} p^2 z^{\varkappa+1} \\ &+ \gamma_{2\varkappa+3} p^3 z^{\varkappa} + \cdots + \gamma_{3\varkappa+2} p^3 z + \gamma^0_{3\varkappa+3} p^3 \end{aligned}$$

können, wenn sie überhaupt reductibel sind, nur in zwei Factoren

$$z^{2\varkappa+2} + \alpha_1 p z^{2\varkappa+1} + \cdots + \alpha_{\varkappa+1} p z^{\varkappa+1} + \alpha_{\varkappa+2} p^2 z^{\varkappa} + \cdots + \alpha^0_{2\varkappa+2} p^2,$$

$$z^{\varkappa+1} + \beta_1 p z^{\varkappa} + \cdots + \beta_{\varkappa} p z + \beta^0_{\varkappa+1} p$$

zerfallen, deren zweiter irreductibel ist, und deren erster auch nur eine Zerfällung in zwei irreductible Factoren des Grades $(\varkappa+1)$ *zulassen kann.*

Die hier abgeleiteten Theoreme II. und IV. schlagen in die Richtung hinein, welche von Herrn Königsberger angegeben ist. — Der Eisenstein'sche Satz kann aber auch als das Anfangsglied einer Kette anderer Theoreme angesehen werden, deren nächstes das folgende ist:

V. *Wenn im Polynome*

$$z^n + c_1 z^{n-1} + c_2 z^{n-2} + \cdots + c_{n-1} z + c_n \tag{16}$$

alle Coefficienten c_λ *durch* p *theilbar sind,* c_{n-1} *aber durch keine höhere Potenz von* p *als die erste, dann ist es entweder irreductibel oder es zerfällt in der Weise, dass es einen Factor des Grades* 1 *und einen anderen irreductiblen Factor des Grades* $(n-1)$ *besitzt.*

Es sei den Voraussetzungen entsprechend

$$c_n = \gamma^0_n p^\tau, \quad c_{n-1} = \gamma^0_{n-1} p \qquad (\tau \geqq 1);$$

wenn dann $a_\mu = \alpha^0_\mu p^\tau$, $b_\nu = \beta^0_\nu$ gesetzt wird, dann stossen wir in der schon mehrfach dagewesenen Art auf den Widerspruch, dass $a_0 = 1$ durch p theilbar sein müsste. Es ist also allein möglich

$$a_\mu = \alpha^0_\mu p^{\tau-\varrho}, \quad b_\nu = \beta^0_\nu p^\varrho \qquad (\tau-\varrho,\ \varrho \geqq 1) \tag{17}$$

zu setzen. Aus der Gleichung

$$c_{n-1} = \gamma^0_{n-1} p = \alpha^0_\mu b_{\nu-1} p^{\tau-\varrho} + a_{\mu-1} \beta^0_\nu p^\varrho$$

folgt dann, dass nicht beide Exponenten $(\tau-\varrho)$ und ϱ grösser als 1 sein können. Wir dürfen demnach etwa $\varrho = 1$, d. h. statt (17)

$$a_\mu = \alpha^0_\mu p^{\tau-1}, \qquad b_\nu = \beta^0_\nu p \tag{18}$$

annehmen, und dann zeigt die vorangehende Gleichung, dass für $\tau > 2$ nicht $a_{\mu-1}$, und für $\tau = 2$ nicht gleichzeitig $a_{\mu-1}$ und $b_{\nu-1}$ durch p theilbar sein kann. Weiter ergiebt sich aus

$$c_{n-2} = \alpha^0_\mu b_{\nu-2} p^{\tau-1} + a_{\mu-1} b_{\nu-1} + a_{\mu-2} \beta^0_\nu p \equiv 0 \pmod{p},$$

dass eine der beiden Grössen $a_{\mu-1}$ und $b_{\nu-1}$ durch p theilbar ist. Den so gefundenen Forderungen wird, abgesehen von einer Aenderung der Bezeichnung nur durch

$$(19) \qquad a_{\mu-1} = \alpha^0_{\mu-1}, \quad b_{\nu-1} = \beta_{\nu-1} p$$

genüge geleistet. Geht man mit (18), (19) in die Congruenz

$$c_{n-3} \equiv 0 \pmod{p},$$

dann folgt, dass $b_{\nu-2} = \beta_{\nu-2} p$ werden muss, und nun gelangt man genau wie früher zu

$$b_{\nu-2} = \beta_{\nu-2} p, \quad b_{\nu-3} = \beta_{\nu-3} p, \ldots$$

und kommt daher im Allgemeinen zu dem Widerspruch, dass $b_0 = 1$ durch p theilbar sein müsste. Der Widerspruch wird aber dann und nur dann vermieden, wenn b_0 nicht durch eine Congruenz (mod. p) sondern durch die Gleichung

$$c_0 = \alpha^0_{\mu-1} b_{\nu-\nu} = 1$$

eingeführt wird. Dann ist also $n = (\nu + 1)$ d. h. $\mu = 1$, und die Factorenzerlegung wird, da $\alpha^0_{\mu-1} = b_0 = 1$ sein muss,

$$(z + \alpha^0_\mu p^{\tau-1})(z^{n-1} + \beta_1 p z^{n-2} + \cdots + \beta_{\nu-1} p z + \beta^0_\nu p)$$

werden, wobei der zweite Factor nach dem Eisenstein'schen Satze irreductibel ist.

VI. *Wenn im Polynome* (16) *alle Coefficienten c_λ durch p theilbar sind, c_{n-2} aber durch keine höhere Potenz von p als die erste, dann ist* (16) *entweder irreductibel, oder es besitzt einen irreductiblen Factor vom Grade* $(n-1)$ *oder* $(n-2)$.

Es sei, der Voraussetzung entsprechend,

$$c_n = \gamma^0_n p^\tau, \quad c_{n-1} = \gamma^0_{n-1} p^\sigma, \quad c_{n-2} = \gamma^0_{n-2} p,$$

wobei $\tau, \sigma > 1$ angenommen werden können und sollen, da man ja sonst auf den Fall des Eisenstein'schen Satzes oder auf V. zurückkommt. Wenn dann

$$a_\mu = \alpha^0_\mu p^\tau, \quad b_\nu = \beta^0_\nu$$

gesetzt wird, dann stossen wir in der schon mehrfach dagewesenen Weise auf den Widerspruch, dass $a_0 = 1$ durch p theilbar sein müsste. Es ist also allein möglich

$$(20) \qquad a_\mu = \alpha^0_\mu p^{\tau-\varrho}, \quad b_\nu = \beta^0_\nu p^\varrho \qquad (\tau - \varrho,\ \varrho \geqq 1)$$

zu setzen. Aus der Gleichung

$$(21) \qquad c_{n-2} = \gamma^0_{n-2} p = \alpha^0_\mu b_{\nu-2} p^{\tau-\varrho} + a_{\mu-1} b_{\nu-1} + a_{\mu-2} \beta^0_\nu p^\varrho$$

geht dann hervor, dass mindestens eine der beiden Grössen $a_{\mu-1}$, $b_{\nu-1}$ durch p theilbar ist.

Ist nur eine von beiden, etwa $b_{\nu-1}$ durch p theilbar, dann wird

$$(22) \qquad a_{\mu-1} = \alpha^0_{\mu-1}, \quad b_{\nu-1} = \beta_{\nu-1}p.$$

Jetzt aber stehen wir genau auf dem Boden der an (19) geknüpften Schlüsse, und wir ersehen daher, dass wenn (16) reductibel ist, die Annahme (22) auf einen irreductiblen Theiler vom Grade $(n-1)$ führen wird. In diesem Falle zeigt

$$c_{n-1} = \gamma^0_{n-1}p^\sigma = \alpha^0_\mu \beta_{\nu-1} p^{\tau-\varrho+1} + \alpha^0_{\mu-1}\beta^0_\nu p^\varrho,$$

dass nicht beide Zahlen ϱ und $(\tau-\varrho+1)$ grösser als σ sein können.

Gilt aber (22) nicht, und sind beide Zahlen $a_{\mu-1}$, $b_{\nu-1}$ durch p theilbar

$$(22\text{a}) \qquad a_{\mu-1} = \alpha_{\mu-1}p, \quad b_{\nu-1} = \beta_{\nu-1}p,$$

so folgt aus (21), dass eine der beiden Zahlen ϱ und $(\tau-\varrho)$ gleich 1 sein muss. Da in (20) beide mit einander vertauscht werden können, so dürfen wir, ohne eine Beschränkung einzuführen,

$$(20\text{a}) \qquad a_\mu = \alpha^0_\mu p^{\tau-1}, \quad b_\nu = \beta^0_\nu p \qquad (\tau-1 \geqq 1)$$

setzen. Ist $(\tau-1) > 1$, dann kann wegen

$$(21\text{a}) \qquad \gamma^0_{n-2}p = \alpha^0_\mu b_{\nu-2}p^{\tau-1} + \alpha_{\mu-1}\beta_{\nu-1}p^2 + a_{\mu-2}\beta^0_\nu p$$

$a_{\mu-2}$ nicht durch p theilbar sein. Ist $(\tau-1) = 1$, dann kann, auch wegen (21a), nicht gleichzeitig $a_{\mu-2}$ und $b_{\nu-2}$ durch p theilbar werden. Auch hier können wir aber $a_{\mu-2}$ als prim zu p ansehen, da bei $(\tau-1) = 1$ wieder die a und b in (20a), (22a) vertauscht werden könnten. Es ist also jedenfalls

$$(23) \qquad a_{\mu-2} = \alpha^0_{\mu-2}.$$

Aus den weiteren Congruenzen mod. p

$$c_{n-4} \equiv 0, \; c_{n-5} \equiv 0, \ldots$$

entnimmt man dann der Reihe nach

$$b_{\nu-2} \equiv 0, \; b_{\nu-3} \equiv 0, \ldots \pmod{p};$$

und so sind wir durch (23) auf unseren alten Weg gelangt.

Will man den hier auftretenden Widerspruch beseitigen, so muss an Stelle der Congruenz, durch welche b_0 eingeführt werden würde, die Gleichung

$$c_0 = \alpha^0_{\mu-2}b_{\nu-\nu} = 1$$

treten. Dann ist also $n = (\nu + 2)$ d. h. $\mu = 2$, und die Factorenzerlegung wird, da $\alpha^0_{\mu-2} = b_{\nu-\nu} = 1$ entsteht,

$$(z^2 + \alpha_{\mu-1} pz + \alpha^0_\mu p^{\tau-1})\,(z^{n-2} + \beta_1\, p z^{n-3} + \cdots + \beta_{\nu-1} pz + \beta^0_\nu p)$$

werden, wobei der zweite Factor nach dem Eisenstein'schen Satze irreductibel ist.

Es ist klar, dass wir in gleicher Weise fortgehen können. Die Resultate der Untersuchung werden sich dabei ganz ähnlich den zuletzt gewonnenen beiden Sätzen ausdrücken lassen.