Ueber die Irreductibilität ganzzahliger ganzer Functionen.

Von **Eugen Netto.**

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

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

alle Coëfficienten c 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 Journals f. d. r. u. a. 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.

Sind alle Coëfficienten von f(z) durch das Quadrat der Primzahl p theilbar, c_n aber durch keine höhere Potenz von p, dann ist f nur zerlegbar, wenn es in zwei Factoren gleichen Grades zerfällt

$$(z^\mu + \alpha_1 p z^{\mu-1} + \alpha_2 p z^{\mu-2} + \ldots + \alpha_\mu p),$$
$$(z^\mu + \beta_1 p z^{\mu-1} + \beta_2 p z^{\mu-2} + \ldots + \beta_\mu p)$$
$$(\alpha_1 + \beta_1 \equiv 0,\ \alpha_2 + \beta_2 \equiv 0,\ \ldots \pmod{p}),$$

die ihrerseits irreductibel sind.

Hätte man eine Zerlegung

$$f(z) = (z^\mu + a_1 z^{\mu-1} + a_2 z^{\mu-2} + \ldots + a_\mu) \cdot (z^\nu + b_1 z^{\nu-1} + b_2 z^{\nu-2} + \ldots + b_\nu),$$

so würde aus $a_\mu b_\nu = c_n$ folgen, dass entweder einer der beiden Coëfficienten a_μ, b_ν durch p^2, oder dass jeder derselben durch p theilbar wäre. Die erste Möglichkeit wird genau auf demselben Wege beseitigt, auf dem der Eisenstein'sche Satz bewiesen wird. Es bleibt also zur Discussion nur

$$(2) \quad a_\mu = \alpha_\mu p, \; b_\nu = \beta_\nu p$$

übrig, wo α_μ, β_ν zu p theilerfremd sind.

Aus

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

folgt nach Einsetzen von (2)

$$(3) \quad \alpha_\mu b_{\nu-1} + \beta_\nu \alpha_{\mu-1} \equiv 0 \pmod{p},$$

und aus

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

folgt ebenso

$$p(\alpha_\mu b_{\nu-2} + \beta_\nu a_{\mu-2}) + a_{\mu-1} b_{\nu-1} \equiv 0 \pmod{p^2}$$

$$a_{\mu-1} b_{\nu-1} \equiv 0 \pmod{p}$$

$$(4) \quad (\alpha_\mu b_{\nu-1}) \cdot (\beta_\nu a_{\mu-1}) \equiv 0 \pmod{p}.$$

Hier zeigen nun (3), (4), dass jede der beiden Klammern in (4) durch p theilbar, und dass also

$$(5) \quad a_{\mu-1} = \alpha_{\mu-1} p, \; b_{\nu-1} = \beta_{\nu-1} p$$

ist. In derselben Weise kann man fortfahren. Wir wollen annehmen, dass wir schon gezeigt hätten, es wäre

$$(6) \quad \begin{array}{l} a_\mu = \alpha_\mu p, \; a_{\mu-1} = \alpha_{\mu-1} p, \; \ldots \; a_{\mu-\varkappa} = \alpha_{\mu-\varkappa} p \\ b_\nu = \beta_\nu p, \; b_{\nu-1} = \beta_{\nu-1} p, \; \ldots \; b_{\nu-\varkappa} = \beta_{\nu-\varkappa} p \end{array}$$

und wollen nun zeigen, dass auch die beiden folgenden Glieder $a_{\mu-\varkappa-1}$, $b_{\nu-\varkappa-1}$ durch p theilbar sind. Man hat nämlich wegen $c_{\mu+\nu-\varkappa-1} \equiv 0$, $c_{\mu+\nu-2\varkappa-2} \equiv 0 \pmod{p}$ die Congruenzen

$$a_\mu b_{\nu-\varkappa-1} + a_{\mu-1} b_{\nu-\varkappa} + \ldots + a_{\mu-\varkappa-1} b_\nu \equiv 0 \pmod{p^2}$$

$$\left.\begin{array}{l} a_{\mu-\varkappa-1} b_{\nu-\varkappa-1} + a_{\mu-\varkappa} b_{\nu-\varkappa-2} + a_{\mu-\varkappa+1} b_{\nu-\varkappa-3} + \ldots \\ \qquad + a_{\mu-\varkappa-2} b_{\nu-\varkappa} + a_{\mu-\varkappa-3} b_{\nu-\varkappa+1} + \ldots \end{array}\right\} \equiv 0$$

Aus der zweiten dieser Congruenzen folgt unter Verwendung von (6), dass $a_{\mu-\varkappa-1} \cdot b_{\nu-\varkappa-1}$ den Factor p enthält; denn alle anderen Glieder sind durch p theilbar. Aus der ersten der beiden letzten Congruenzen folgt, dass

$$a_\mu b_{\nu-\varkappa-1} + a_{\mu-\varkappa-1} b_\nu \equiv 0 \pmod{p^2}$$

ist; denn alle übrigen Glieder der linken Seite enthalten p^2. Man hat also die beiden Resultate

$$(\alpha_\mu b_{\nu-\varkappa-1}) + (\beta_\nu a_{\mu-\varkappa-1}) \equiv 0,$$
$$(\alpha_\mu b_{\nu-\varkappa-1})\ (\beta_\nu a_{\mu-\varkappa-1}) \equiv 0 \pmod{p}$$

und deshalb sind beide Klammern durch p theilbar, und also

$$a_{\mu-\varkappa-1} = \alpha_{\mu-\varkappa-1}p,\ b_{\nu-\varkappa-1} = \beta_{\nu-\varkappa-1}p,$$

womit unsere Behauptung bewiesen ist.

Diese Schlussfolgerung kann man so lange fortsetzen bis man zu einem Gliede der Reihen

$$a_{\mu-\lambda-1},\ b_{\nu-\lambda-1}\quad (\lambda = 0, 1, 2, \ldots)$$

kommt, dessen Index = 0 ist. Bei ungleichen μ, ν geschieht dies nur für ein a oder ein b und dann tritt ein Widerspruch durch $a_0 = 1$ bezw. $b_0 = 1$ gegen das Resultat der Theilbarkeit durch p heraus. Ist aber $\mu = \nu$, dann versagen unsere Schlüsse bei $\varkappa = \nu + 1$, weil dann die zweite der Gleichungen in $a_0 b_0 = 1$ übergeht. Hier ist also eine Zerlegung denkbar, und diese kann in der That eintreten, wenn die im Theorem angeführten Bedingungen erfüllt sind. Als Beispiel möge für $p = 5$

$$(z^2 + 5z + 10)(z^2 + 20z + 15) = z^4 + 25z^3 + 125z^2 + 275z + 150$$

dienen. —

Nach derselben Richtung hin lassen sich beliebig viele weitere Sätze ableiten. Der nächste dieser Reihe lautet: Sind alle Coëfficienten von f(z) durch die dritte Potenz einer Primzahl p theilbar, c_n aber durch keine höhere Potenz von p, so kann f nur dann zerlegbar sein, wenn die Gradzahl n durch 3 theilbar $= 3\nu$ und

$$f(z) = (z^{2\nu} + \alpha_1 p z^{2\nu-1} + \ldots + \alpha^\nu p z^\nu + \alpha_{\nu+1} p^2 z^{\nu-1} + \ldots + \alpha_{2\nu} p^2) \cdot (z^\nu + \beta_1 p z + \ldots + \beta_\nu p)$$

ist. Die α, β müssen dabei noch einer Reihe von Congruenzbedingungen mod. p und mod. p^2 unterworfen werden.

Zuerst ist es klar, dass $a_\mu \cdot b_\nu = c_n \equiv 0 \pmod{p^3}$ nur so befriedigt werden kann, dass eine der beiden Grössen a_μ, b_ν den Factor p^3 enthält, oder dass die eine, etwa a_μ durch p^2, die andere b_ν durch p theilbar ist. Der erste Fall führt auf dem, beim Eisenstein'schen Satze einzuschlagenden Wege zur Erkenntniss der Existenz eines Widerspruches. Es bleibt also nur

(8) $a_\mu = \alpha_\mu p^2$, $b_\nu = \beta_\nu p$

wobei α_μ, β_ν relativ prim zu p sind, für die Betrachtung zurück. Aus

$$c_{n-1} = a_\mu b_{\nu-1} + a_{\mu-1} b_\nu \equiv 0 \pmod{p^3}$$
$$\alpha_\mu b_{\nu-1} p + a_{\mu-1}\beta_\nu \equiv 0 \pmod{p^2}$$

folgt $a_{\mu-1} = \alpha'_{\mu-1} p$.

Wir wollen nun annehmen, man hätte schon bewiesen

$$a_\mu = \alpha_\mu p^2, \ldots a_{\mu-\varkappa+1} = \alpha_{\mu-\varkappa+1} p^2;$$

(9) $$b_\nu = \beta_\nu p, \ldots b_{\nu-\varkappa+1} = \beta_{\nu-\varkappa+1} p;$$

$$a_{\mu-\varkappa} = \alpha'_{\mu-\varkappa} p, \ldots a_{\mu-2\varkappa+1} = \alpha'_{\mu-2\varkappa+1} p,$$

und wollen daraus folgern

$$a_{\mu-\varkappa} = \alpha_{\mu-\varkappa} p^2; \quad b_{\nu-\varkappa} = \beta_{\nu-\varkappa} p;$$

$$a_{\mu-2\varkappa} = \alpha'_{\mu-2\varkappa} p, \quad a_{\mu-2\varkappa-1} = \alpha_{\mu-2\varkappa-1} p,$$

so dass dadurch das in (9) gegebene Gesetz sich als weiter fortsetzbar ausgewiesen hat. Hierzu brauchen wir die vier aus der Betrachtung von $c_{\mu+\nu-\varkappa}$, $c_{\mu+\nu-2\varkappa}$, $c_{\mu+\nu-2\varkappa-1}$, $c_{\mu+\nu-3\varkappa}$ entspringenden Congruenzen für den Model p^3. Man erhält also die folgenden Beziehungen

(10) $a_{\mu-\varkappa} b_\nu + a_{\mu-\varkappa+1} b_{\nu-1} + \ldots + a_\mu b_{\nu-\varkappa} \equiv 0,$

(11) $$\left.\begin{aligned} &a_{\mu-2\varkappa} b_\nu + a_{\mu-2\varkappa+1} b_{\nu-1} + \ldots + a_{\mu-\varkappa-1} b_{\nu-\varkappa+1} \\ &+ a_{\mu-\varkappa} b_{\nu-\varkappa} + a_{\mu-\varkappa+1} b_{\nu-\varkappa-1} + \ldots \end{aligned}\right\} \equiv 0,$$

(12) $$\left.\begin{aligned} &a_{\mu-2\varkappa-1} b_\nu + a_{\mu-2\varkappa} b_{\nu-1} + \ldots + a_{\mu-\varkappa-1} b_{\nu-\varkappa} \\ &+ a_{\mu-\varkappa} b_{\nu-\varkappa-1} + a_{\mu-\varkappa+1} b_{\nu-\varkappa-2} + \ldots \end{aligned}\right\} \equiv 0,$$

(13) $$\left.\begin{aligned} &a_{\mu-2\varkappa} b_{\nu-\varkappa} + a_{\mu-2\varkappa-1} b_{\nu-\varkappa+1} + \ldots \\ &+ a_{\mu-2\varkappa+1} b_{\nu-\varkappa-2} + \ldots \end{aligned}\right\} \equiv 0.$$

Benutzen wir (9), dann folgt, dass in (11) alle Glieder mit Ausnahme von $a_{\mu-2\varkappa} b_\nu$ und $a_{\mu-\varkappa} b_{\nu-\varkappa}$ durch p^2, und dass in (13) alle Glieder mit Ausnahme von $a_{\mu-2\varkappa} \cdot b_{\mu-\varkappa}$ durch p theilbar sind. Demnach wird

$$\left.\begin{aligned} &(\beta_\nu a_{\mu-2\varkappa}) + (\alpha'_{\mu-\varkappa} b_{\nu-\varkappa}) \equiv 0 \\ &(\beta_\nu a_{\mu-2\varkappa}) \cdot (\alpha'_{\mu-\varkappa} b_{\nu-\varkappa}) \equiv 0 \end{aligned}\right\} \pmod{p}$$

und deshalb sind beide hier eingehenden Klammergrössen durch p theilbar. Aus der ersten folgt $a_{\mu-2\varkappa} \equiv 0$ und damit ein Theil der Behauptung. Aus dem zweiten ergiebt sich

(14) $(\alpha_\mu b_{\nu-\varkappa}) \cdot (\beta_\nu \alpha'_{\mu-\varkappa}) \equiv 0 \pmod{p}$,

und hiermit combiniren wir (10). In (10) sind alle mittleren Glieder durch p^2 theilbar, also auch die Summe der beiden äusseren, d. h. es wird

$$(\beta_\mu \alpha'_{\mu-\varkappa}) + (\alpha_\mu b_{\nu-\varkappa}) \equiv 0 \pmod{p},$$

und hieraus, in Verbindung mit (14) ergeben sich weitere Theile der Behauptung, nämlich

$$a_{\mu-\varkappa} = \alpha'_{\mu-\varkappa} p = \alpha_{\mu-\varkappa} p^2;$$
$$b_{\nu-\varkappa} = \beta_{\nu-\varkappa} p.$$

Der noch fehlende Theil der Behauptung folgt jetzt ohne Weiteres aus (12); denn wenn man die bisherigen Resultate einträgt, sieht man, dass jedes auf das erste folgende Glied durch p^2 theilbar ist. Folglich muss auch das erste durch p^2 oder

$$a_{\mu-2\varkappa-1}\beta_\nu \text{ also auch } a_{\mu-2\varkappa-1}$$

durch p theilbar sein.

Damit ist die Behauptung völlig bewiesen.

Wir haben nun zu untersuchen, wie weit diese Schlussfolgerungen tragen, d. h. wie weit die Reihe (9) fortgesetzt werden kann. Ist zuerst $\mu > 2\nu$, dann nehmen wir $\varkappa = \nu$ und stossen auf den Widerspruch, dass $b_0 = 1$ durch p theilbar sein müsste, ist zweitens $\mu < 2\nu$; $\mu = 2m$, dann nehmen wir $\varkappa = m$, und aus (11) und (13) folgt der Widerspruch, dass $a_0 = 1$ durch p theilbar sein müsste. Bei $\mu < 2\nu$ und $\mu = 2m + 1$, $\varkappa = m$ wird der Widerspruch durch (12) aufgedeckt. In all diesen Fällen ist also keine Zerlegung möglich. Es sei endlich $\mu = 2\nu$; $\varkappa = \nu$

$$a_{2\nu} = \alpha_{2\nu} p^2, \quad \ldots\ldots \quad a_{\nu+1} = \alpha_{\nu+1} p^2;$$
$$(15) \quad b_\nu = \beta_\nu p, \quad \ldots\ldots \quad b_1 = \beta_1 p;$$
$$a_\nu = \alpha'_\nu p, \quad \ldots\ldots \quad a_1 = \alpha'_1 p.$$

Dann fällt beim weiteren Fortschreiten (13) weg; denn dasselbe geht in $a_0 b_0 = 1$ über, und dadurch werden weitere Schlüsse unmöglich gemacht, und ein Widerspruch lässt sich nicht auffinden. In der That ist auch hier wirklich eine Zerlegung in gewissen Fällen möglich; die Factoren haben Coëfficienten von der in (15) abgeleiteten, im Ausspruche des Theorems angegebenen Beschaffenheit. Als Beispiel möge dienen

$$z^3 + p^3 z^2 + p^4 z + p^3(p^2 - 1) = (z^2 + pz + p^2)(z + p^3 - p).$$

Für die Theilbarkeit aller Coëfficienten c durch p^4 lässt sich genau ebenso das entsprechende Theorem ableiten, und der Beweis bietet hier ebenso wenig wie bei höheren Potenzen von

p irgend etwas Neues. Bei p^4 sind zwei Fälle der Zerlegung möglich, $a_\mu = \alpha_\mu p^2$, $b_\nu = \beta_\nu p^2$; dies verläuft buchstäblich wie der obige Satz für p^2 mit gleichen Schlüssen und gleichen Resultaten. Ferner ist $a_\mu = \alpha_\mu p^3$, $b_\nu = \beta_\nu p$ möglich. Hier kann im Ausnahmefalle $\mu = 3\nu$ eine Zerlegung stattfinden, wenn

$$b_\nu = \beta_\nu p, \quad b_{\nu-1} = \beta_{\nu-1} p, \ \ldots \quad b_1 = \beta_1 p;$$

$$a_\nu = \alpha''_\nu p, \quad a_{\nu-1} = \alpha''_{\nu-1} p, \ \ldots \ a_1 = \alpha_1 p;$$

$$a_{2\nu} = \alpha'_{2\nu} p^2, \quad a_{2\nu-1} = \alpha'_{2\nu-1} p^2, \ \ldots \quad a_{\nu+1} = \alpha'_{\nu+1} p^2;$$

$$a_{3\nu} = \alpha_{3\nu} p^3, \quad a_{3\nu-1} = \alpha_{3\nu-1} p^3, \ \ldots \quad a_{2\nu+1} = \alpha_{2\nu+1} p^3$$

ist.

Der allgemeine Satz, zu dem wir so geführt werden, lautet: Sind alle Coëfficienten c von f(z) durch die $\varkappa^{te}$ Potenz einer Primzahl p theilbar, c_n aber durch keine höhere Potenz, dann kann f nur dann, wenn die Gradzahl n von f(z) mit $\varkappa$ einen gemeinsamen Theiler besitzt, in Factoren zerlegbar sein.