Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1936

Kollektion: Mathematica

Werk Id: PPN243919689_0175

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN243919689_0175|LOG_0020

Terms and Conditions

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Über die Irreduzibilität ganzzahliger Polynome nach einem Primzahlmodul.

Von *Erik L. Petterson* in Stockholm.

O. Ore [1]) hat folgenden Satz auf idealtheoretischem Wege bewiesen:

Gegeben sei ein Polynom

$$f(x) \equiv \varphi(x)^t - a \pmod{p}.$$

Es sei $\operatorname{Ind} a = d$ für irgendeine Primitivwurzel für den Primzahlmodul p, und p gehöre mod t zum Exponenten h, so daß also

$$\frac{p^h - 1}{t} = k$$

eine ganze Zahl ist. Weiter sei δ der größte gemeinsame Teiler von $p - 1$ und k, δ_1 der größte gemeinsame Teiler von $\frac{p-1}{\delta}$ und d. Dann kann $f(x) \bmod p$ nur dann durch eine Primfunktion m-ten Grades mit $m \equiv 0 \pmod{h}$ teilbar sein, wenn m von der Form

$$m = s\,\frac{p-1}{\delta\,\delta_1}\,h$$

ist, wo s eine ganze Zahl bedeutet.

Im folgenden werde ich einen analogen und etwas schärferen Satz für das allgemeinere Polynom $F(x) = f(g(x)^m)$ ableiten, wo $f(x) \bmod p$ irreduzibel ist, und auch die Existenz des fraglichen Faktors beweisen. Das Oresche Polynom folgt aus $f(g(x)^m)$ für $f(x) = x - a$. Beim Beweise werde ich nur die Grundgesetze der Theorie der imaginären Kongruenzwurzeln anwenden und im übrigen ganz elementare Beziehungen benutzen, die ich in den ersten Sätzen zusammengefaßt habe. Mittels einer rekurrenten Reihe und der Untersuchungen einer früheren Arbeit [2]) wird schließlich ein Irreduzibilitätskriterium (Satz 9) abgeleitet.

Satz 1. *Es sei $m > 0$ eine ganze Zahl mit der Primzahlzerlegung $m = \prod_{\nu=1}^{N} q_\nu^{n_\nu}$ und $a \neq 1$ eine beliebige ganze Zahl. Ist dann $q_\nu \mid (a-1)$ für $\nu = 1, 2, \ldots, N$ und v ein Teiler von $a - 1$ mit $(m, v) = 1$, ferner $4 \nmid m$, wenn $4 \nmid (a-1)$ ist, so gilt die*

[1]) O. Ore, Über die Reduzibilität von algebraischen Gleichungen, Skrifter Norske Vid. Akad. Oslo 1923, Nr. 1.

[2]) E. L. Petterson, Irreduzibilitätskriterien als Folgerung einiger Beziehungen zwischen den Faktorzerlegungen eines algebraischen Polynoms und seines konstanten Gliedes, Math. Zeitschr. **40** (1935), S. 194—200.

Kongruenz

$$a^m \equiv 1 \left(\mathrm{mod}\ \frac{m(a-1)}{v}\right) \tag{1}$$

mit m als Minimalexponenten.

Ist umgekehrt $a \neq 1$ eine ganze Zahl, die $\mathrm{mod}\ \frac{m(a-1)}{v}$, *wo $v \mid m(a-1)$ ist, zum Exponenten m gehört, so gilt $q_\nu \mid (a-1)$ für $\nu = 1, 2, \ldots, N$; $(m, v) = 1$ und $4 \nmid m$, wenn $4 \nmid (a-1)$ ist.*

Beweis. In der Entwicklung

$$\frac{a^m - 1}{m(a-1)} = \sum_{n=1}^{m} K_n (a-1)^{n-1} \tag{2}$$

ist

$$K_n = \frac{1}{n}\binom{m-1}{n-1} = \frac{1}{m}\binom{m}{n}.$$

Es sind also mK_n und nK_n ganze Zahlen, so daß, wenn $K_n = \frac{r}{s}$ in reduzierter Form geschrieben wird, $s \mid m$ und $s \mid n$ ist. Damit nun $K_n(a-1)^{n-2}$ ganz ist, muß $s \mid (a-1)^{n-2}$ sein. Wegen $s \mid m$ ist $s = \prod_\nu q_\nu^{\beta_\nu}$. Da nach den Voraussetzungen des Satzes jedes $q_\nu \mid (a-1)$ ist, ist sicher $s \mid (a-1)^{n-2}$, wenn jedes $\beta_\nu \leqq n-2$ ist. Dies ist aber, da $s \mid n$ ist, für $n > 3$ erfüllt. Andernfalls wäre nämlich

$$s \geqq q_\nu^{\beta_\nu} \geqq 2^{\beta_\nu} > 2^{n-2} \geqq n \quad \text{für} \quad n > 3.$$

Für $n = 3$ aber ist

$$K_n(a-1)^{n-2} = \frac{(m-1)(m-2)(a-1)}{2 \cdot 3}$$

ebenfalls ganz. Denn es ist $2 \mid (m-1)(m-2)$ und entweder auch $3 \mid (m-1)(m-2)$ oder $3 \mid m$. Dann ist aber nach Voraussetzung auch $3 \mid (a-1)$. Aus (2) folgt also

$$\frac{a^m - 1}{m(a-1)} = 1 + \frac{(m-1)(a-1)}{2} + K(a-1), \tag{3}$$

wo K eine ganze Zahl ist. Da ferner auf Grund der Voraussetzungen m und a nicht beide gerade sein können, gilt jedenfalls die Kongruenz (1) für m.

Es ist noch zu zeigen, daß m Minimalexponent in der Kongruenz (1) ist. Es möge a zum Exponenten m' $\mathrm{mod}\ \frac{m(a-1)}{v}$ gehören; dann ist m' ein Teiler von m. Setzt man $m = m'm''$, so erhält man, da wegen $m' \mid m$ Satz 1 auch auf m' angewandt werden kann, aus (3)

$$\frac{v}{m''}\left(1 + \frac{(m'-1)(a-1)}{2} + K'(a-1)\right) = \frac{v(a^{m'}-1)}{m'm''(a-1)} = \text{ganze Zahl}$$

nach Definition von m'. Hierbei bedeutet K' eine ganze Zahl.

Aus $m = m'm''$ und den Voraussetzungen über m folgt $(m'', v) = 1$. Also gilt

$$m'' \Big| \left(1 + \frac{(m'-1)(a-1)}{2} + K'(a-1)\right).$$

Die Zahl in der Klammer heisse A. Offenbar hat A keinen Primteiler mit $a-1$ gemeinsam außer eventuell den Primteiler 2. Da ferner jeder Primteiler von m'' auch Teiler von m und folglich auch von $a-1$ ist, muß m'' die Form $m''=2^f\,(f\geqq 0)$ haben.

Ist nun $4\,|\,(a-1)$, so ist A ungerade, also $m''=1$.

Ist $2\nmid(a-1)$, so ist m ungerade, also auch m'' ungerade und demnach $m''=1$.

Ist schließlich $4\nmid(a-1)$, aber $2\,|\,(a-1)$, so ist nach Voraussetzung $4\nmid m$ und folglich wenigstens eine der Zahlen m' und m'' ungerade. Ist m'' ungerade, so ist $m''=1$. Ist m' ungerade, so ist A ungerade und also wiederum $m''=1$.

In sämtlichen Fällen ist also $m''=1$, d. h. $m=m'$. Daher ist m in (1) Minimalexponent.

Um die Umkehrung von Satz 1 zu zeigen, nehme ich an $(m,v)=g$, $\dfrac{m}{g}=m'm''$, wo $(m',a-1)=1$ und jeder Primteiler von m'' auch Teiler von $a-1$ ist. Nach Voraussetzung ist $v\,|\,m(a-1)$, mithin

$$\frac{v}{g}\,\Big|\,(a-1),\quad \left(m',\frac{m''(a-1)}{\dfrac{v}{g}}\right)=1,\quad \frac{m}{g}\,\Big|\,(a^m-1).$$

Hieraus folgt $\left(\dfrac{m}{g},a\right)=1$, $(m',a)=1$ und demnach

$$a^{\varphi(m')}\equiv 1\pmod{m'}. \tag{4}$$

Schließlich ergibt sich

$$a^{m''}\equiv 1\left(\mathrm{mod}\,\frac{m''(a-1)}{\dfrac{v}{g}}\right). \tag{5}$$

Aus (4) und (5) folgt wegen der Teilerfremdheit der Moduln

$$a^{\varphi(m')m''}\equiv 1\left(\mathrm{mod}\,\frac{m(a-1)}{v}\right).$$

Da aber m der Minimalexponent ist, folgt

$$\varphi(m')\,m''\geqq m=g\,m'\,m'',\qquad \varphi(m')\geqq gm',$$

also

$$m'=1,\qquad g=1.$$

Dies liefert $(m,v)=1$ und zeigt, daß jeder Primteiler von m auch Teiler von $a-1$ ist.

Ist schließlich, $4\,|\,m$ aber $4\nmid(a-1)$, so gilt nach (3)

$$\frac{\dfrac{a^{\frac{m}{2}}-1}{m(a-1)}}{v}=\frac{v}{2}\left(1+\frac{\left(\dfrac{m}{2}-1\right)(a-1)}{2}+K''(a-1)\right), \tag{6}$$

wo K'' eine ganze Zahl und wegen $4\,|\,m$ auch $2\,|\,(a-1)$ ist.

Weil $\dfrac{m}{2}$ gerade und $4\nmid(a-1)$ ist, muß der Ausdruck in der Klammer gerade

und daher die rechte Seite von (6) eine ganze Zahl sein. Dies bedeutet

$$a^{\frac{m}{2}} \equiv 1 \left(\mathrm{mod}\,\frac{m(a-1)}{v}\right)$$

im Widerspruch zur Voraussetzung, daß m Minimalexponent ist. Also ist $4 \nmid m$, wenn $4 \nmid (a-1)$ ist.

In manchen Fällen ist es besser, Satz 1 in der folgenden Formulierung heranzuziehen:

Satz 2. *Es seien a und P ganze Zahlen, $P > 0$, und $P = \prod_{\nu=1}^{L} q_\nu^{n_\nu}$ die Primzahlzerlegung von P. Es sei ferner $(P, a-1) = g$, $q_\nu \mid (a-1)$ für $\nu = 1, 2, \ldots, L$ und $4 \nmid \frac{P}{g}$, wenn $4 \nmid (a-1)$ ist. Dann gilt die Kongruenz*

$$a^{\frac{P}{g}} \equiv 1 \pmod{P}$$

mit $\frac{P}{g}$ als Minimalexponent. Wenn umgekehrt irgendeine Zahl a mod P zum Exponenten $\frac{P}{g}$ mit $g \mid P$ gehört und $P = \prod_{\nu=1}^{L} q_\nu^{n_\nu}$ die Primzahlzerlegung von P ist, so gilt $q_\nu \mid (a-1)$ für $\nu = 1, 2, \ldots, L$, ferner $(P, a-1) = g$ und $4 \nmid \frac{P}{g}$, wenn $4 \nmid (a-1)$ ist.

Diese Formulierung ergibt sich aus Satz 1 für $m = \frac{P}{g}$, $\frac{a-1}{g} = v$.

Satz 3. *Es seien a, P_1 und P_2 beliebige ganze Zahlen und $(a, P_1) = (a, P_2) = 1$, ferner k und h die Minimalexponenten der Kongruenzen $a^k \equiv 1 \pmod{P_1}$ und $(a^k)^h \equiv 1 \pmod{P_2}$, schließlich $(P_1 P_2, a^{kh} - 1) = d$. Dann ist $kh\frac{P_1 P_2}{d}$ Minimalexponent der Kongruenz $a^{kh\frac{P_1 P_2}{d}} \equiv 1 \pmod{P_1 P_2}$.*

Bemerkung. Aus diesem Satz lassen sich analoge Sätze für eine beliebige Anzahl n von Moduln $P_1, P_2, \ldots, P_n$ ableiten. Die Bedingungen können dabei symmetrisch aufgestellt werden.

Beweis. Es ist zunächst klar, daß der Minimalexponent, zu welchem $a \pmod{P_1 P_2}$ gehört, ein Vielfaches von kh ist Daher genügt es, zu zeigen, daß a^{kh} zum Exponenten $\frac{P_1 P_2}{d} \pmod{P_1 P_2}$ gehört. Ferner ist aber jeder Primfaktor von $P_1 P_2$ auch Teiler von $a^{kh} - 1$, und da aus $\left(P_1, \frac{a^{kh}-1}{P_2}\right) = d'$ folgt $d' = \frac{d}{P_2}$ und demnach $\frac{P_1 P_2}{d} = \frac{P_1}{d'}$ ist, so bleibt nach Satz 2 nur noch zu zeigen, daß $4 \nmid \frac{P_1}{d'}$, wenn $4 \nmid (a^{kh} - 1)$ ist. Aus $4 \nmid (a^{kh} - 1)$ folgt aber unmittelbar $4 \nmid P_1$ und also $4 \nmid \frac{P_1}{d'}$.

Unter einem gemeinsamen Exponenten der Wurzeln ξ_ν eines normierten ganzzahligen Polynoms $f(x)$ vom Grade k in bezug auf eine ganze Zahl E als Modul wird im

folgenden eine Zahl P verstanden, die den Kongruenzrelationen

$$\xi_\nu^P = 1 + EM(\xi_\nu) \qquad (\nu = 1, 2, \ldots, k)$$

genügt, wo $M(x)$ ein ganzzahliges Polynom ist. Die Relationen geben also

$$\xi_\nu^P \equiv 1 \pmod{E}.$$

Wesentlich ist dabei, daß $M(x)$ für alle ξ_ν dasselbe ist, was direkt folgt, wenn $f(x)$ irreduzibel ist. Für ein solches P gilt folgender Satz:

Satz 4. *Ist P nach dem Modul $E > 1$ der kleinste gemeinsame Exponent der Wurzeln eines normierten ganzzahligen Polynoms $f(x)$ und $m > 0$ eine beliebige ganze Zahl, so ist mP der kleinste gemeinsame Exponent der Wurzeln des Polynoms $F(x) = f(x^m)$.*

Beweis. Ohne Beschränkung der Allgemeinheit kann vorausgesetzt werden, daß die Diskriminante von $f(x)$ von 0 verschieden ist. Der Grad von $f(x)$ sei k, und die Wurzeln von $F(x)$ seien mit ξ_ν $(\nu = 1, 2, \ldots, mk)$ bezeichnet.

Unmittelbar klar ist, daß mP ein gemeinsamer Exponent der Wurzeln ξ_ν von $F(x) = f(x^m)$ ist. Der kleinste gemeinsame Exponent muß demnach von der Form $m'P'$ sein, wo $m' \mid m$ und $P' \mid P$ ist. Für diesen ist

$$\xi_\nu^{m'P'} \equiv 1 \pmod{E},$$

folglich erst recht

$$(\xi_\nu^m)^{P'} \equiv 1 \pmod{E}, \qquad \nu = 1, 2, \ldots, mk.$$

Die ξ_ν^m sind nun die Wurzeln von $f(x)$, und da P ein Minimalexponent dieser Wurzeln ist, so folgt

$$P' = P.$$

Der kleinste gemeinsame Exponent mod E für alle ξ_ν $(\nu = 1, 2, \ldots, mk)$ ist also gleich $m'P$.

Ist $\left(\frac{m}{m'}, P\right) = d$, so ist $\frac{m}{m'd}$ ganz, und man erhält

$$1 \equiv \xi_\nu^{\frac{m}{m'd} m'P} = (\xi_\nu^m)^{\frac{P}{d}} \pmod{E}.$$

Da P Minimalexponent ist, muß $d = 1$ sein und demnach

$$\left(\frac{m}{m'}, P\right) = 1.$$

Ich benutze nun die bekannten Beziehungen

$$\sum_{\nu=1}^{mk} \frac{\xi_\nu^l}{F'(\xi_\nu)} = \begin{cases} 0 & \text{für } l = 0, 1, 2, \ldots, mk-2 \\ 1 & \text{für } l = mk-1, \end{cases}$$

und führe eine Zahlenfolge τ_n ein, die durch

$$\tau_n = \sum_{\nu=1}^{mk} \frac{\xi_\nu^{mk-2}}{F'(\xi_\nu)} \xi_\nu^n$$

definiert ist. Für τ_n gilt demnach

$$\tau_{-(mk-2)} = \tau_{-(mk-3)} = \cdots = \tau_0 = 0, \qquad \tau_1 = 1,$$

sowie die Rekursionsformel

$$\tau_n + a_1 \tau_{n-m} + a_2 \tau_{n-2m} + \cdots + a_k \tau_{n-km} = 0,$$

die dem Polynom

$$F(x) = (x^m)^k + a_1(x^m)^{k-1} + \cdots + a_k$$

entspricht. Es folgt

$$\tau_n = 0 \text{ für alle } n \text{ mit } n \not\equiv 1 \pmod m,$$
$$\tau_n \text{ ganz für alle } n \geqq -(mk-2).$$

Für die ξ_ν war nun bereits gezeigt:

$$\xi_\nu^{m'P} = 1 + EN(\xi_\nu), \qquad \nu = 1, 2, \ldots, mk,$$

wo $N(x)$ ein ganzzahliges Polynom

$$N(x) = b_0 x^{mk-1} + b_1 x^{mk-2} + \cdots + b_{mk-1}$$

ist. Es wird dann

$$\tau_n - \tau_{n-m'P} = \sum_{\nu=1}^{mk} \frac{\xi_\nu^{mk-2}}{F'(\xi_\nu)} \xi_\nu^{n-m'P} (\xi_\nu^{m'P} - 1) = E \sum_{\nu=1}^{mk} \frac{\xi_\nu^{mk-2}}{F'(\xi_\nu)} \xi_\nu^{n-m'P} N(\xi_\nu)$$

und folglich

$$\tau_n - \tau_{n-m'P} = E \sum_{\lambda=1}^{mk} b_{mk-\lambda}\, \tau_{n-m'P+\lambda-1}.$$

Hieraus erhält man

$$\tau_n \equiv \tau_{n-m'P} \pmod E$$

für alle $n \geqq m'P - (mk-2)$. Wegen $\left(\frac{m}{m'}, P\right) = 1$ können zwei positive Zahlen U und V so bestimmt werden, daß

$$U\frac{m}{m'} - VP = 1$$

ist. Ist nun m eine Primzahl und $m' \neq m$, so ist $m' = 1$. Dann ist P eine Periode für die τ_n, und man erhält

$$\tau_{Um} \equiv \tau_{Um-VP} \equiv \tau_1 = 1 \pmod E$$

im Widerspruch zu $\tau_{Um} = 0$. Also muß $m' = m$ sein. Ist m eine zusammengesetzte Zahl, $m = \prod_{\nu=1}^{M} q_\nu$ mit gleichen oder verschiedenen Primzahlen q_ν, so ergibt sich $m' = m$ durch sukzessives Ersetzen von x durch x^{q_ν} $(\nu = 1, 2, \ldots, M)$. Damit ist Satz 4 bewiesen.

Es sei nun ξ eine Wurzel des Polynoms $f(x) = x^k + a_1 x^{k-1} + \cdots + a_k$, dann gilt die Relation

$$(7) \qquad \xi^n = -\sum_{\lambda=1}^{k} (a_\lambda \xi^{k-1} + a_{\lambda+1} \xi^{k-2} + \cdots + a_k \xi^{\lambda-1})\, \tau_{n-k-\lambda+2}.$$

Nach der Definition von τ_n ist nämlich diese Beziehung klar für z. B. $n = k$; sie läßt sich dann allgemein durch Schluß von $n-1$ auf n ableiten. Ist

$$\tau_n \equiv \tau_{n-P} \pmod E$$

für alle hinreichend großen $n \geqq k$, so folgt also

$$(8) \qquad \xi^P \equiv 1 \pmod E.$$

Sind nun $f(x)$ und $f_1(x)$ identisch kongruent mod E (und auch $f_1(x)$ normiert), so muß für zugehörige τ_n und τ_n' gelten

$$\tau_n \equiv \tau_n' \pmod{E}$$

für alle $n \geqq -(k-2)$. Damit ist gezeigt, daß $f(x)$ und $f_1(x)$ denselben kleinsten gemeinsamen Exponenten mod E für ihre Wurzeln haben müssen, wenn ihre Diskriminanten von 0 verschieden sind.

Im folgenden soll nun E durch eine Primzahl p ersetzt werden, und es sei $f(x)$ irreduzibel mod p. Ferner sei

$$f(x^q) \equiv \prod_{\lambda=1}^{N} B_\lambda(x) \pmod{p},$$

wo q eine Primzahl $\neq p$ ist und wo alle $B_\lambda(x)$ Primfunktionen mod p sind. Aus $p \neq q$ folgt, daß die Diskriminante von $F(x) = f(x^q)$ durch p nicht teilbar ist. Dieses gilt demnach auch für die Diskriminante von $F_1(x) = \prod_{\lambda=1}^{N} B_\lambda(x)$. Gehört $f(x)$ mod p zum Exponenten P, so müssen ja alle Exponenten P_λ, zu denen die $B_\lambda(x)$ gehören, Vielfache von P sein. Ist nämlich $\xi^{(\lambda)}$ eine Wurzel von $B_\lambda(x)$, so gilt $\xi^{(\lambda)P_\lambda} \equiv 1 \pmod{p}$ und also

$$\left(\xi^{(\lambda)q}\right)^{P_\lambda} \equiv 1 \pmod{p}.$$

Da $\xi^{(\lambda)q}$ aber als eine imaginäre Kongruenzwurzel von $f(x)$ betrachtet werden kann und demnach mod p zu P gehört, so folgt

$$P \mid P_\lambda, \qquad \lambda = 1, 2, \ldots, N.$$

Nach Satz 4 ist qP der kleinste gemeinsame Exponent von $F(x) = f(x^q)$ und folglich auch von $F_1(x) = \prod_{\lambda=1}^{N} B_\lambda(x)$. Mithin muß wenigstens ein Faktor $B_\lambda(x)$ zum Exponenten qP mod p gehören.

Ist nun $p \nmid m$ und $m = \prod_{\nu=1}^{M} q_\nu$ mit gleichen oder verschiedenen Primzahlen q_ν, so folgt durch sukzessives Ersetzen von x durch x^{q_ν}, $\nu = 1, 2, \ldots, M$, daß $F(x) = f(x^m)$ *wenigstens einen Faktor* mod p *enthält, der* mod p *zum Exponenten* mP *gehört.*

Satz 5. *Sind $f(x)$ und $g(x)$ normierte ganzzahlige Polynome und $f(x)$ außerdem irreduzibel* mod p *und vom Grade k, so kann das Polynom $F(x) = f(g(x))$ nur solche Faktoren* mod p *enthalten, deren Gradzahlen Vielfache von k sind.*

Beweis. Es sei

$$F(x) \equiv A_r(x) B(x) \pmod{p},$$

wo $A_r(x)$ ein mod p irreduzibles Polynom vom Grade r ist. Ist dann ξ eine Wurzel von $A_r(x)$, also $A_r(\xi) = 0$, so folgt

$$g(\xi)^{p^r-1} \equiv 1 \pmod{p}.$$

Aus $F(x) = f(g(x))$ ergibt sich ferner, daß $g(\xi)$ eine Kongruenzwurzel (reell oder komplex) des irreduziblen Polynoms $f(x)$ ist. Gehört daher $g(\xi)$ mod p zum Exponenten P,

$$g(\xi)^P \equiv 1 \pmod{p},$$

so folgt

$$p^r \equiv 1 \pmod{P}.$$

Außerdem gehört aber p auch zu der Gradzahl k des Polynoms $f(x) \bmod P$, d. h.

$$p^k \equiv 1 \pmod{P}.$$

Also ist

$$k \mid r.$$

Aus den Sätzen 4 und 5 ergibt sich nun folgender Satz:

Satz 6. *Es seien $f(x)$ und $g(x)$ normierte ganzzahlige Polynome, $f(x)$ irreduzibel* mod p *und vom Grade k. Gehört dann p^k* mod *einer ganzen Zahl m zum Exponenten h,*

$$(p^k)^h \equiv 1 \pmod{m},$$

so muß das Polynom $F(x) = f(g(x)^m)$ wenigstens einen irreduziblen Faktor mod p *von einem Grade, der ein Vielfaches von kh ist, enthalten.*

Beweis. Nach Satz 5 genügt es, den Satz für $f(x^m)$ zu beweisen. Ferner muß die Gradzahl r des fraglichen Faktors sicher von der Form $r = kr_1$ sein. Gehört $f(x) \bmod p$ zum Exponenten P, so muß $f(x^m)$ nach Satz 4 und den danach bewiesenen Beziehungen wenigstens einen irreduziblen Faktor mod p enthalten, der mod p zum Exponenten mP gehört. Man hat also

$$mP \mid (p^{kr_1} - 1)$$

und demnach

$$m \mid ((p^k)^{r_1} - 1).$$

Da $p^k \bmod p$ zu h gehört, folgt

$$h \mid r_1 \quad \text{und} \quad kh \mid r.$$

Satz 7. *Es sei das Polynom $f(x) = x^k + a_1 x^{k-1} + \cdots + a_k$ irreduzibel* mod p, $\frac{p^k - 1}{v_k}$ *der Exponent, zu welchem die Wurzeln von $f(x)$* mod p *gehören, und $g(x)$ ein beliebiges, normiertes, ganzzahliges Polynom. Es sei ferner $m > 0$ eine ganze Zahl mit der einzigen Bedingung $p \nmid m$, h Minimalexponent der Beziehung $m \mid (p^{kh} - 1)$ und d_k der größte gemeinsame Teiler von $\frac{p^k - 1}{v_k}$ und $\frac{p^{kh} - 1}{m}$, d. h. $\left(\frac{p^k - 1}{v_k}, \frac{p^{kh} - 1}{m}\right) = d_k$. Dann muß das Polynom $F(x) = f(g(x)^m)$ wenigstens einen irreduziblen Faktor vom Grade r* (mod p) *enthalten, wo r von der Form $r = i\frac{p^k - 1}{d_k v_k} kh$ ist (i ganze Zahl). Für $g(x) = x$ gibt es einen Faktor* mod p *vom Grade $r = \frac{p^k - 1}{d_k v_k} kh$.*

Beweis. Nach Satz 4 und den danach bewiesenen Beziehungen enthält das Polynom $F_1(x) = f(x^m)$ wenigstens einen irreduziblen Faktor mod p mit Wurzeln, die mod p zum Exponenten $\frac{m(p^k - 1)}{v_k}$ gehören. Die Gradzahl dieses Faktors sei r_1. Es gilt also

$$p^{r_1} \equiv 1 \left(\bmod \frac{m(p^k - 1)}{v_k}\right)$$

mit r_1 als Minimalexponent.

Da $\frac{p^k-1}{v_k}$ der Minimalexponent für die Wurzeln von $f(x) \bmod p$ sein soll, folgt $p^k \equiv 1 \left(\bmod \frac{p^k-1}{v_k}\right)$ mit k als Minimalexponent. Nach Satz 3 für $a=p$, $P_1=\frac{p^k-1}{v_k}$, $P_2=m$ und $d=d_k m$ ist daher $\frac{p^{kh}-1}{d_k v_k} kh$ Minimalexponent der Kongruenz

$$p^{\frac{p^k-1}{d_k v_k} kh} \equiv 1 \left(\bmod \frac{m(p^k-1)}{v_k}\right).$$

Folglich ist

$$r_1 = \frac{p^k-1}{d_k v_k} kh.$$

Wenn in dem irreduziblen Faktor vom Grade r die Variable x durch $g(x)$ ersetzt wird, erhält man ein Polynom, dessen irreduzible Faktoren mod p nach Satz 5 sämtlich Gradzahlen haben, die Vielfache von r_1 sind. Das Polynom $F(x)=f(g(x)^m)$ hat also wenigstens einen irreduziblen Faktor mod p, dessen Gradzahl r die Form

$$r = ir_1 = i\frac{p^k-1}{d_k v_k} kh$$

hat, wo i ganz ist.

Satz 8. *Die Gradzahlen sämtlicher* mod p *irreduziblen Faktoren des Polynoms* $F(x)=f(g(x)^m)$ *von Satz 7, die Vielfache von kh sind, müssen sogar Vielfache von* $\frac{p^k-1}{d_k v_k} kh$ *sein. Für* $g(x)=x$ *sind diese Gradzahlen gleich* $\frac{p^k-1}{d_k v_k} kh$.

Beweis. Es genügt, den Satz für $F_1(x)=f(x^m)$ zu beweisen. Es sei $m=m'm''$, wo m' der größte Teiler von m mit

$$\left(m', \frac{p^k-1}{v_k}\right) = 1$$

ist. Für eine Wurzel ξ irgendeines mod p irreduziblen Faktors von $F_1(x)$ gilt

$$(\xi^m)^{\frac{p^k-1}{v_k}} \equiv 1 \pmod p$$

mit $\frac{p^k-1}{v_k}$ als Minimalexponent. Es folgt dann

$$(\xi^{m'})^{\frac{m''(p^k-1)}{v_k}} \equiv 1 \pmod p \tag{9}$$

mit $\frac{m''(p^k-1)}{v_k}$ als Minimalexponent. Gehört nun $\xi \bmod p$ zum Exponenten Q, ist also

$$\xi^Q \equiv 1 \pmod p \quad \text{und folglich erst recht} \quad (\xi^{m'})^Q \equiv 1 \pmod p,$$

so muß Q ein Vielfaches von $\frac{m''(p^k-1)}{v_k}$ sein, d. h.

$$Q = s\frac{m''(p^k-1)}{v_k}.$$

Wegen (9) muß gelten

$$Q \Big| \frac{m'm''(p^k-1)}{v_k}$$

und also

$$s \mid m' \quad \text{und} \quad \left(s, \frac{m''(p^k-1)}{v_k}\right) = 1 . \tag{10}$$

Wenn nun die Gradzahl r von ξ ein Vielfaches von kh ist, d. h. $r = ikh$, so folgt

$$p^{ikh} \equiv 1 \left(\mathrm{mod}\, s\, \frac{m''(p^k-1)}{v_k}\right)$$

mit ikh als Minimalexponent.

Es sei

$$\left(\frac{sm''(p^k-1)}{v_k}, p^{kh}-1\right) = g . \tag{11}$$

Aus

$$sm'' \Big| (p^{kh}-1) \quad \text{und} \quad \frac{p^k-1}{v_k} \Big| (p^{kh}-1)$$

folgt $4 \nmid \frac{sm''(p^k-1)}{g\, v_k}$, wenn $4 \nmid (p^{kh}-1)$ ist.

Für die Zahl i findet man also nach Satz 2 mit $a = p^{kh}$ und $P = \frac{sm''(p^k-1)}{v_k}$ folgenden Wert

$$i = \frac{sm''(p^k-1)}{g\, v_k} . \tag{12}$$

Nach den Voraussetzungen von Satz 7 ist

$$\left(\frac{(m'm''(p^k-1)}{v_k}, p^{kh}-1)\right) = m'm''\, d_k .$$

Wegen der Relationen (10), (11), ferner

$$\left(m', \frac{m''(p^k-1)}{v_k}\right) = 1 \quad \text{und} \quad m' \mid (p^{kh}-1)$$

muß dann gelten

$$\frac{m'}{s} = \frac{m'm''d_k}{g},$$

also

$$\frac{sm''}{g} = \frac{1}{d_k} .$$

Damit ist nach (12)

$$i = \frac{p^k-1}{d_k\, v_k} \quad \text{und} \quad r = \frac{p^k-1}{d_k\, v_k}\, kh .$$

Bemerkung. Für $f(x) = x - a$ erhält man aus Satz 8 den Satz von Ore. Dabei ist jedoch Ind $a = d$ durch die Zahl v ersetzt, die durch die Kongruenz $a^{\frac{p-1}{v}} \equiv 1 \pmod{p}$ mit $\frac{p-1}{v}$ als Minimalexponent definiert ist.

Für die dem Polynom $(x-a)^k$ entsprechende Reihe τ'_n erhält man

$$\tau'_n = \frac{a^{n-1}}{(k-1)!} \prod_{\lambda=0}^{k-2} (n+\lambda).$$

Die Relation (7) kann auch für $(x-a)^k$ direkt benutzt werden. Es sei nun P eine Periode mod E für τ'_n:

$$\tau'_n \equiv \tau'_{n+P} \pmod{E}.$$

Ferner sei $(E, (k-1)!) = 1$ und $(E, a) = 1$. Wird dann ξ in (7) durch a ersetzt, so folgt wie (8)

$$a^P \equiv 1 \pmod{E}.$$

Da $\prod_{\lambda=0}^{k-2}(n+\lambda)$ ein Polynom in n ist, so muß P ein Vielfaches von E sein [3]). Gehört a mod E zum Exponenten v, so ist also

$$P = \frac{Ev}{(E, v)}$$

die kleinste Periode mod E. Dieses gilt demnach auch für die dem normierten Polynom

$$f(x) = (x-a)^k + EM(x)$$

entsprechende Reihe τ_n, denn hier ist

$$\tau_n \equiv \frac{a^{n-1}}{(k-1)!} \prod_{\lambda=0}^{k-2} (n+\lambda) \pmod{E}.$$

Mithin ist $\frac{Ev}{(E, v)}$ ein gemeinsamer Exponent mod E für die Wurzeln von $f(x)$. Ist die Diskriminante von $f(x)$ von 0 verschieden, so ist umgekehrt ein gemeinsamer Exponent der Wurzeln eine Periode für τ_n. Damit ist gezeigt, daß $\frac{Ev}{(E, v)}$ der kleinste gemeinsame Exponent mod E für die Wurzeln von $f(x)$ ist. Nach Satz 4 muß dann $\frac{mEv}{(E, v)}$ der kleinste gemeinsame Exponent für die Wurzeln des Polynoms

$$F(x) = (x^m - a)^k + EM(x)$$

sein, wenn die Diskriminante von $F(x)$ nicht verschwindet.

Aus früheren Untersuchungen von mir [4]) erhält man nun z. B. folgendes Irreduzibilitätskriterium:

---

[3]) Der Beweis durch Schluß von $k-1$ auf k folgt aus $(k-1)\prod_{\lambda=0}^{k-3}(n+\lambda) = \prod_{\lambda=0}^{k-2}(n+\lambda) - \prod_{\lambda=0}^{k-2}(n-1+\lambda)$.

[4]) a. a. O. [2]).

Satz 9. *Es sei $F(x)$ ein normiertes ganzzahliges Polynom der Form*

$$F(x) = (x^m - a)^k + EM(x),$$

wo $(E, (k-1)!) = 1$ ist und $a \bmod E$ zum Exponenten v gehört. Wenn dann $(-a)^k + EM(0)$ keinen echten Faktor d mit

$$d^{\frac{mEv}{(E,v)}} \equiv 1 \pmod{E}$$

enthält, so kann $F(x)$ nur dann reduzibel sein, wenn unter den Wurzeln von $F(x)$ wenigstens eine algebraische Einheit vorkommt.

Eingegangen 4. Dezember 1935.