

Karel Petr

Über die Reduzibilität eines Polynoms mit ganzzahligen Koeffizienten nach einem Primzahlmodul

Časopis pro pěstování matematiky a fysiky, Vol. 66 (1937), No. 2, 85--94

Persistent URL: <http://dml.cz/dmlcz/121487>

Terms of use:

© Union of Czech Mathematicians and Physicists, 1937

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

ČÁST MATEMATICKÁ

Über die Reduzibilität eines Polynoms mit
ganzzahligen Koeffizienten nach einem
Primzahlmodul.*)

Karel Petr, Praha.

(Eingegangen am 12. Oktober 1936.)

In dieser Arbeit werden Polynome $c_0x^n + c_1x^{n-1} + \dots + c_n$ mit ganzen rationalen Koeffizienten c_0, c_1, \dots, c_n betrachtet. Man nennt ein solches Polynom reduzibel nach dem Primzahlmodul p , wenn es ein Polynomprodukt

$(d_0x^r + d_1x^{r-1} + \dots + d_r)(e_0x^s + e_1x^{s-1} + \dots + e_s)$, $r > 0, s > 0$ mit ganzen rationalen Koeffizienten gibt, dessen Koeffizienten den Koeffizienten gleichen Grades des ursprünglichen Polynoms kongruent (mod p) sind; d. h. wenn

$$\begin{aligned} & c_0x^n + c_1x^{n-1} + \dots + c_n \equiv \\ \equiv & (d_0x^r + d_1x^{r-1} + \dots + d_r)(e_0x^s + e_1x^{s-1} + \dots + e_s) \pmod{p}. \end{aligned}$$

Um die Darstellung möglichst einfach zu gestalten, setzen wir voraus, daß die Koeffizienten c_0, d_0, e_0 durch p nicht teilbar sind. Dann ist das gegebene Polynom ein Polynom n -ten Grades und die Polynome der Zerlegung sind vom r -ten bzw. s -ten Grade, wobei $r + s = n$; r, s sind selbstverständlich ganze positive Zahlen.

Die Definition der Reduzibilität eines Polynoms (mod p) läßt sich einfacher aussprechen, wenn man Polynome einführt, deren Koeffizienten Elemente des zur Primzahl p gehörigen Primkörpers K_p (des Körpers der Restklassen (mod p)) sind. Hier können die Koeffizienten c_0, c_1, \dots, c_n als Repräsentanten der zugehörigen Restklassen mod p betrachtet werden und das gleiche gilt auch von den d_k, e_j . Dann heißt das Polynom $c_0x^n + c_1x^{n-1} + \dots + c_n$ reduzibel, im Körper K_p , wenn es sich schreiben läßt als Produkt zweier Polynome der Gerade r bzw. s ,

*) Die folgenden Entwicklungen wurden im wesentlichen vor einigen Jahren in „Jednota Českoslov. Mat. a Fysiků“ (Sitzung vom 9. V. 1934) vorgetragen.

$r > 0, s > 0$ mit den Koeffizienten aus K_p (kurz: zweier Polynome in K_p).

Wenn ein Polynom eine solche Darstellung als Produkt nicht zuläßt, so heißt es irreduzibel in K_p .

In dieser Arbeit bezeichnen x, y, z, u, t Unbestimmte; a, b, c, d, e Restklassen (mod p) (Elemente aus K_p); 0 bezeichnet die Nullklasse (die Menge aller ganzen durch p teilbaren Zahlen); $i, j, k, l, m, n, p, q, r, s$ sollen ganze rationale Zahlen bedeuten, mit p wird immer eine Primzahl gemeint.

I.

Die vorliegende Arbeit hat das Ziel Kriterien für die Reduzibilität eines Polynoms in K_p aufzustellen und Aufschluß über die irreduziblen Bestandteile zu geben. Es genügt, sich auf Polynome mit dem höchsten Koeffizienten 1 (Einsklasse (mod p)) zu beschränken. Sei also

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$$

ein solches Polynom in K_p . $f(x)$ hat in einer passenden Erweiterung von K_p , die durch Adjunktion der sogenannten Galoisschen Imaginären zu K_p entsteht, n Wurzeln. Diese Wurzeln sind alle voneinander verschieden, wenn die Diskriminante von $f(x)$ ungleich Null ist (d. h. wenn die Diskriminante nicht durch die Nullklasse (mod p) gegeben ist). Wäre die Diskriminante von $f(x)$ gleich Null, so hätte $f(x)$ mehrfache Wurzeln und dann ließe sich $f(x)$ auf bekannte Weise in ein Produkt von Polynomen in K_p zerlegen, deren Diskriminanten alle von Null verschieden sind.

Wir werden also voraussetzen, daß $f(x)$ eine von Null verschiedene Diskriminante besitzt. Die Wurzeln von $f(x)$ genügen der Gleichung

$$x^n = -a_1x^{n-1} - a_2x^{n-2} - \dots - a_n.$$

Wenn wir diese Gleichung mit x multiplizieren und dann das Glied $-a_1x^n$ mittels der vorigen Gleichung durch $a_1^2x^{n-1} + a_1a_2x^{n-2} + a_1a_3x^{n-3} + \dots + a_1a_n$ ersetzen, so bekommen wir die folgende Gleichung

$$x^{n+1} = a'_1x^{n-1} + a'_2x^{n-2} + \dots + a'_n$$

mit

$$a'_1 = a_1^2 - a_2, \quad a'_2 = a_1a_2 - a_3, \dots,$$

der wieder alle Wurzeln von $f(x)$ genügen. Auf diese Weise fortschreitend sehen wir, daß sich die Potenzen $x^n, x^{n+1}, x^{n+2}, \dots$ in K_p linear durch $x^0, x^1, x^2, \dots, x^{n-1}$ ausdrücken lassen, falls x eine Wurzel von $f(x)$ ist. Für das folgende sind besonders wichtig die linearen Ausdrücke für folgende Potenzen:

$$x^{0 \cdot p}, x^{1 \cdot p}, x^{2 \cdot p}, \dots, x^{(n-1)p}.$$

Nach Durchführung der betreffenden Rechnungen bekommen wir folgende n Gleichungen:

$$x^{kp} = c_{k,0} + c_{k,1}x + c_{k,2}x^2 + \dots + c_{k,n-1}x^{n-1} \quad (A)$$

$$k = 0, 1, 2, \dots, n-1,$$

die für jede Wurzel von $f(x)$ gültig sind. Hier ist $c_{00} = 1$, $c_{0j} = 0$ für $j = 1, 2, \dots, n-1$; ähnlich ist, falls $p < n$, $c_{1p} = 1$, alle übrigen $c_{1j} = 0$. Die Gleichungen (A) drücken die Elemente $1, x^p, x^{2p}, \dots, x^{(n-1)p}$ linear durch die Elemente $1, x, x^2, \dots, x^{n-1}$ aus. Die lineare Substitution von n Unbestimmten mit den Koeffizienten c_{kj} hat folgende Gestalt:

$$X_k = c_{k0}x_0 + c_{k1}x_1 + \dots + c_{k,n-1}x_{n-1} \quad (A')$$

$$k = 0, 1, 2, \dots, n-1.$$

Die Eigenschaften dieser Substitution werden uns Auskunft über die Reduzibilität des Polynomes $f(x)$ geben.

Um die erwähnten Eigenschaften zu ermitteln, werden wir die Substitution (A') auf eine einfache Gestalt bringen. Zu diesem Zwecke suchen wir, wie sich durch die Substitution (A) gewisse passend gewählte lineare Ausdrücke in $1, x, x^2, \dots, x^{n-1}$ transformieren. Um unnötige Länge der Formeln zu vermeiden, setzen wir voraus, daß sich $f(x)$ in drei *irreduzible* Polynome $f_1(x), f_2(x), f_3(x)$ der Grade q, r, s zerlegen läßt:

$$f(x) = f_1(x) f_2(x) f_3(x), \quad q > 0, r > 0, s > 0$$

$$q + r + s = n.$$

α soll nun eine festgewählte Wurzel von $f_1(x)$, β von $f_2(x)$, γ von $f_3(x)$ bezeichnen. Wenn wir den Körper K_p durch α zu $K_p(\alpha)$ erweitern, so liegen bekanntlich alle Wurzeln von $f_1(x)$ in $K_p(\alpha)$ und sind durch die Folge

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{q-1}}, \alpha^{p^q} = \alpha$$

gegeben. Ähnlich lassen sich alle Wurzeln von $f_2(x)$ bzw. $f_3(x)$ durch die Potenzen von β bzw. γ in $K_p(\beta)$ bzw. $K_p(\gamma)$ ausdrücken. Wir führen noch die Bezeichnung

$$\alpha_k = \alpha^{p^k}, \beta_k = \beta^{p^k}, \gamma_k = \gamma^{p^k}$$

ein. Wir bilden nun folgende Ausdrücke

$$\frac{f(x)}{x - \alpha} = y_0, \quad \frac{f(x)}{x - \alpha_1} = y_1, \dots, \frac{f(x)}{x - \alpha_{q-1}} = y_{q-1}, \quad (+)$$

die *linear* in $1, x, x^2, \dots, x^{n-1}$ mit Koeffizienten aus $K_p(\alpha)$ sind. Formal ganz gleiche Ausdrücke, die nur linear in $1, x^p, x^{2p}, \dots, x^{(n-1)p}$ sind, erhalten wir, wenn wir in (+) x durch x^p ersetzen:

$$\frac{f(x^p)}{x^p - \alpha} = Y_0, \quad \frac{f(x^p)}{x^p - \alpha_1} = Y_1, \dots, \frac{f(x^p)}{x^p - \alpha_{q-1}} = Y_{q-1}.$$

Es läßt sich auf folgende Weise leicht finden, wie sich die Ausdrücke y_0, y_1, \dots, y_{q-1} in Y_0, Y_1, \dots, Y_{q-1} transformieren, und zwar mittels der Gleichungen (A), die für alle Wurzeln von $f(x)$ gelten. Der Ausdruck Y_0 wird Null für alle Wurzeln des Polynoms $f(x)$ mit einer Ausnahme. Diese wird gebildet von der Wurzel der Gleichung $x^p - \alpha = 0$ oder, was dasselbe ist, der Gleichung $x^p - \alpha^{p^2}$ d. h. von der Wurzel α_{q-1} . Dasselbe gilt aber von dem Ausdruck y_{q-1} .

Es ist also, falls x eine Wurzel des Polynoms $f(x)$ und folglich infolge der Gl. (A) Y_0 linear in $1, x, x^2, \dots, x^{n-1}$ ist:

$$Y_0 = \delta_0 y_{q-1} \text{ und ähnlich}$$

$$Y_1 = \delta_1 y_0, \quad Y_2 = \delta_2 y_1, \quad \dots, \quad Y_{q-1} = \delta_{q-1} y_{q-2}.$$

$\delta_1, \delta_2, \dots, \delta_{q-1}$ sind Elemente des Körpers $K_p(\alpha)$ und es ist

$$\delta_0 = \frac{f'(\alpha)}{f'(\alpha_{q-1})}, \quad \delta_1 = \frac{f'(\alpha_1)}{f'(\alpha)}, \quad \delta_2 = \frac{f'(\alpha_2)}{f'(\alpha_1)}, \quad \dots, \quad \delta_{q-1} = \frac{f'(\alpha_{q-1})}{f'(\alpha_{q-2})}.$$

Es gilt also für die $\delta_0, \delta_1, \dots$ die Beziehung

$$\delta_0 \delta_1 \delta_2 \dots \delta_{q-1} = 1. \quad (—)$$

Außer den y_0, y_1, \dots, y_{q-1} können wir noch folgende lineare Ausdrücke in $1, x, x^2, \dots, x^{n-1}$ bilden:

$$z_i = \frac{f(x)}{x - \beta_i}, \quad u_j = \frac{f(x)}{x - \gamma_j} \quad \begin{matrix} i = 0, 1, \dots, r-1 \\ j = 0, 1, \dots, s-1 \end{matrix}. \quad (+')$$

Wenn wir hier wieder x durch x^p ersetzen, so erhalten wir Ausdrücke, die den Y_i ähnlich gebaut sind und die wir durch Z_i, U_j bezeichnen werden. Zwischen den Z_i und z_i , bzw. U_j und u_j gelten analoge lineare Beziehungen wie zwischen den Y_k und y_k . Die in $1, x, x^2, \dots, x^{n-1}$ linearen Ausdrücke y_k, z_i, u_j sind untereinander linear unabhängig und ihre Anzahl ist gleich $n = q + r + s$. Führen wir in (A') anstatt der x_0, x_1, \dots, x_{n-1} die Unbestimmten y_k, z_i, u_j , die durch (+) und (+') als lineare Formen der x_0, x_1, \dots, x_{n-1} gegeben sind (es genügt in (+), (+') x_k statt x^k zu setzen), ein und führen wir weiter anstatt der X_0, X_1, \dots, X_{n-1} die ähnlich gebauten Y_k, Z_i, U_j ein, so geht das System der n Gleichungen (A') in das folgende einfache System von n Gleichungen

$$Y_k = \delta_k y_{k-1}, \quad Z_i = \varepsilon_i z_{i-1}, \quad U_j = \eta_j u_{j-1} \quad (B)$$

$$k = 0, 1, \dots, q-1, \quad i = 0, 1, \dots, r-1, \quad j = 0, 1, \dots, s-1$$

über. Es läßt sich also die lineare Substitution (A') auf die einfache Gestalt (B) transformieren.

Die lineare Substitution (B) ist aus drei linearen Substitutionen zusammengestellt. Jede von diesen drei Substitutionen bezieht sich nur auf eine Gruppe von Unbestimmten: die erste auf die Unbestimmten (y_k, Y_k) , die zweite auf (z_i, Z_i) , die dritte auf (u_j, U_j) . Die linke Seite der annullierten charakteristischen Gleichung von (B) und damit auch diejenige von (A') läßt sich also in ein Produkt von drei Faktoren zerlegen. Diese Faktoren sind die linken Seiten der charakteristischen Gleichungen der drei Substitutionen, in welche die Substitution (B) zerlegt ist. Diese linken Seiten lassen sich leicht ausrechnen. Für die lineare Substitution zwischen den y_k und Y_k bekommen wir so, wenn wir $q = 5$ setzen, als linke Seite der charakteristischen Gleichung:

$$\begin{vmatrix} -\lambda & 0 & 0 & 0 & \delta_0 \\ \delta_1 & -\lambda & 0 & 0 & 0 \\ 0 & \delta_2 & -\lambda & 0 & 0 \\ 0 & 0 & \delta_3 & -\lambda & 0 \\ 0 & 0 & 0 & \delta_4 & -\lambda \end{vmatrix} = -\lambda^5 + \delta_0 \delta_1 \delta_2 \delta_3 \delta_4 = -\lambda^5 + 1.$$

Die charakteristische Gleichung der Substitution (B) hat also die Gestalt

$$(\lambda^q - 1)(\lambda^r - 1)(\lambda^s - 1) = 0.$$

Wenn sich allgemein $f(x)$ im Körper K_p in l irreduzible Faktoren von Graden q_1, q_2, \dots, q_l zerlegen läßt, so hat die charakteristische Gleichung der Substitution (A') die Gestalt:

$$(\lambda^{q_1} - 1)(\lambda^{q_2} - 1)(\lambda^{q_3} - 1) \dots (\lambda^{q_l} - 1) = 0,$$

$$q_1 + q_2 + \dots + q_l = n.$$

Die linke Seite dieser Gleichung charakterisiert umgekehrt für unsere Zwecke genügend die Substitution (A'), folgende zwei Fälle ausgenommen:

a) falls eine oder mehrere unter den Zahlen q_1, q_2, \dots durch p teilbar sind,

b) falls wenigstens p von den Zahlen q_1, q_2, \dots, q_l einander gleich sind.

In diesen Fällen ist nämlich die Gestalt, die man der charakteristischen Gleichung geben kann, vieldeutig. Wenn zum Beispiel q_1 durch p teilbar ist $q_1 = pq'_1$, gilt in K_p folgende Gleichheit

$$(\lambda^{q_1} - 1) = (\lambda^{q'_1} - 1)^p \text{ in } K_p.$$

Diese Ausnahmen können nicht zutreffen, wenn p genug groß ist, zum Beispiel wenn $p > n$. Wenn $p = n$, so findet Zweideutigkeit bei den charakteristischen Gleichungen

$$(\lambda - 1)^n = 0, (\lambda^n - 1) = 0$$

statt, die zusammenfallen. Für $p = n - 1$ gibt es gleichfalls eine

Zweideutigkeit:

$$(\lambda - 1)^n = (\lambda^{n-1} - 1)(\lambda - 1)$$

und s. w.

Die Ergebnisse, die wir so gewonnen haben, kann man in dem folgenden Satze zusammenfassen: *Eine notwendige Bedingung dafür, daß das Polynom n -ten Grades $f(x)$ mit ganzen rationalen Koeffizienten im Restklassenkörper $(\text{mod } p)$ in ein Produkt von in K_p irreduziblen Polynomen der Grade q_1, q_2, \dots, q_l zerlegbar sei, ist, daß sich die linke Seite der annullierten charakteristischen Gleichung der linearen Substitution (A') in K_p in der Gestalt*

$$(\lambda^{q_1} - 1)(\lambda^{q_2} - 1) \dots (\lambda^{q_l} - 1)$$

schreiben lasse.

Diese Bedingung ist auch hinreichend, falls keine identische Gleichheit

$$(\lambda^{q_1} - 1)(\lambda^{q_2} - 1) \dots (\lambda^{q_l} - 1) = (\lambda^{q'_1} - 1)(\lambda^{q'_2} - 1) \dots (\lambda^{q'_l} - 1)$$

in K_p besteht, in der die Menge der ganzen Zahlen (q_1, q_2, \dots, q_l) nicht mit der Menge $(q'_1, q'_2, \dots, q'_l)$ identisch ist. Insbesondere trifft dies ein, wenn $p > n$. Da ist die angegebene Bedingung notwendig und hinreichend.

II.

Einige Beispiele. 1. Man soll feststellen, ob $x^2 - a$ in K_p reduzibel sei; p sei > 2 . Für $x^2 - a = 0$ gilt auch

$$x^p = a^{\frac{p-1}{2}} x$$

und die Gleichungen (A) lauten:

$$x^{0 \cdot p} = 1$$

$$x^{1 \cdot p} = 0 + a^{\frac{p-1}{2}} x.$$

Die charakteristische Gleichung ist dann:

$$\begin{vmatrix} 1 - \lambda & 0 \\ 0 & a^{\frac{p-1}{2}} - \lambda \end{vmatrix} = 0, \text{ d. h.}$$

$$(\lambda - 1)(\lambda - a^{\frac{p-1}{2}}) = 0.$$

Die Gleichung kann in K_p für $a \neq 0$ nur eine von diesen zwei Formen $(\lambda - 1)^2 = 0$, $\lambda^2 - 1 = 0$ haben. Es ist also entweder $a^{\frac{p-1}{2}} = +1$ oder $a^{\frac{p-1}{2}} = -1$. Im ersten Fall ist die Gleichung in zwei lineare Faktoren zerlegbar, im zweiten Fall ist sie irreduzibel. Dieses Ergebnis ist aus den Anfängen der Zahlentheorie

bekannt und wird durch den Satz ausgesprochen: a ist quadratischer Rest oder Nichtrest (mod p), je nachdem

$$a^{\frac{p-1}{2}} \equiv +1 \text{ oder } \equiv -1 \pmod{p} \text{ ist.}$$

2. Untersuchen wir die Gleichung

$$x^p - ax - b = 0$$

in K_p . Hier ist

$$\begin{aligned} x^p &= b + ax \\ x^{2p} &= b^2 + 2abx + a^2x^2 \\ x^{3p} &= b^3 + 3ab^2x + 3a^2bx^2 + a^3x^3 \\ &\dots\dots\dots \end{aligned} \quad (\times)$$

Die linke Seite der charakteristischen Gleichung hat hier die Form:

$$(\lambda - 1)(\lambda - a)(\lambda - a^2) \dots (\lambda - a^{p-1}).$$

Wir müssen $a \neq 0$ in K_p voraussetzen, sonst hätte die gegebene Gleichung n gleiche Wurzeln. (Auch die linke Seite der charakteristischen Gleichung hätte dann eine ganz andere, von der oben angeführten abweichende Gestalt.)

Wenden wir uns zuerst dem Fall $a = 1$ zu. Die linke Seite der charakteristischen Gleichung hat die Gestalt

$$(\lambda - 1)^p$$

und das ist in K_p dem Ausdruck $(\lambda^p - 1)$ gleich.

Daraus folgt, daß die gegebene Gleichung in K_p entweder in p lineare Faktoren zerlegbar oder irreduzibel ist. Der erste Fall tritt aber dann und nur dann ein, falls die Gleichungen (\times) folgende Gestalt haben:

$$x^p = x, \quad x^{2p} = x^2, \quad x^{3p} = x^3, \dots,$$

d. h. falls die Substitution (A') die identische Substitution ist. Das trifft nur für $b = 0$ zu. Wenn also $a = 1, b \neq 0$ ist, so ist die untersuchte Gleichung in K_p irreduzibel.

Es soll nun a zum Exponenten r gehören, (d. h. $a^r = 1, a^{r'} \neq 1$ für $0 < r' < r$). Man kann dann die linke Seite der charakteristischen Gleichung in der Form

$$(\lambda - 1)(\lambda^r - 1)^{\frac{p-1}{r}}$$

schreiben. Offensichtlich ist hier das Polynom $x^p - ax - b$ in $\frac{p-1}{r}$ irreduzible Faktoren r -ten Grades und in einen linearen Faktor in K_p zerlegbar.

3. Nehmen wir weiter das Polynom

$$f(x) = x^4 - 2x^3 + 3x^2 - 7x + 4$$

in K_5 . Es gilt in jedem K_p für $f(x) = 0$

$$\begin{aligned}x^4 &= 2x^3 - 3x^2 + 7x - 4 \\x^5 &= x^3 + x^2 + 10x - 8 \\x^6 &= 3x^3 + 7x^2 - x - 4.\end{aligned}$$

In K_5 gilt nun

$$x^5 = x^3 + x^2 + 2,$$

und daraus durch Potenzieren bekommt man

$$\begin{aligned}x^{10} &= x^3 + x \\x^{15} &= -x^3 + 3x - 1.\end{aligned}$$

Die linke Seite der charakteristischen Gleichung ist also

$$\begin{vmatrix} 1 - \lambda & 0 & 0 & 0 \\ 2 & -\lambda & 1 & 1 \\ 0 & 1 & -\lambda & 1 \\ -1 & 3 & 0 & -1 - \lambda \end{vmatrix} = \lambda^4 - 1.$$

Folglich ist $x^4 - 2x^3 + 3x^2 - 7x + 4$ in K_5 irreduzibel.

4. Als letztes Beispiel nehme ich das Polynom $f(x) = x^5 + 7x^4 - 2x^3 + 6x^2 - 11x + 24$. Ich werde zuerst seine Reduzibilität in K_3 untersuchen. In K_3 zerfällt $f(x)$ augenscheinlich in das Produkt von x und dem Polynom 4. Grades $x^4 + 7x^3 - 2x^2 + 6x - 11 = g(x)$. Für $g(x) = 0$ gilt in K_3

$$\begin{aligned}x^4 &= -x^3 - x^2 - 1 \\x^5 &= x^2 - x + 1 \\x^6 &= x^3 - x^2 + x \\x^9 &= -x + 1\end{aligned}$$

Die Gleichungen (A) haben also für $g(x) = 0$ die Gestalt:

$$x^0 = 1, x^3 = x^3, x^6 = x - x^2 + x^3, x^9 = 1 - x$$

und die linke Seite der charakteristischen Gleichung ist

$$(1 - \lambda) \begin{vmatrix} -\lambda & 0 & 1 \\ 1 & -1 - \lambda & 1 \\ -1 & 0 & -\lambda \end{vmatrix} = \lambda^4 - 1$$

Folglich ist $g(x)$ in K_3 irreduzibel und $f(x)$ zerfällt in das Produkt eines linearen Polynoms und eines irreduziblen Polynoms 4. Grades.

Untersuchen wir weiter die Reduzibilität von $f(x)$ in K_5 , wo man

$$\begin{aligned}x^5 &= -2x^4 + 2x^3 - x^2 + x + 1 \\x^{10} &= 2x^4 + 2x^3 + x^2 + 1 \\x^{15} &= x^4 - 2x^3 - x^2 + 2x + 1 \\x^{20} &= -2x^3 - x - 1\end{aligned}$$

schreiben kann. Die linke Seite der charakteristischen Gleichung ist

$$(1 - \lambda) \begin{vmatrix} 1 - \lambda, & -1, & 2, & -2 \\ 0, & 1 - \lambda, & 2, & 2 \\ 2, & -1, & -2 - \lambda, & 1 \\ -1, & 0, & -2, & -\lambda \end{vmatrix} = -(\lambda - 1)(\lambda^4 - 1)$$

Folglich zerfällt $f(x)$ in K_5 ebenfalls in das Produkt eines irreduziblen Polynoms 4. Grades und eines linearen Polynoms.

III.

Wenn wir die Gleichung (A) zur p -ten Potenz erheben, so erhalten wir (in K_p) die Beziehung

$$x^{kp^2} = c_{k,0} + c_{k,1}x^p + c_{k,2}x^{2p} + \dots + c_{k,n-1}x^{(n-1)p}.$$

Wenn wir auf der rechten Seite dieser Gleichung für die Potenzen x^{kp} , $k = 0, 1, \dots, n-1$ die Ausdrücke auf der rechten Seite von (A) einführen, so bekommen wir

$$x^{kp^2} = c_{k0}^{(1)} + c_{k1}^{(1)}x + c_{k2}^{(1)}x^2 + \dots + c_{k,n-1}^{(1)}x^{n-1} \quad (A_1)$$

$$k = 0, 1, 2, \dots, n-1.$$

Wir wollen jetzt die Substitution (A') symbolisch

$$X = S(x) \quad (A')$$

schreiben. Durch das Wiederholen der Substitution (A') bekommen wir ihr Quadrat und die zugehörigen Beziehungen wollen wir in der Form

$$X^{(1)} = S^2(x) \quad (A_1^1)$$

schreiben. Wenn wir hier auf der rechten Seite x_k durch x^k ersetzen, so ist, falls x eine Wurzel von $f(x)$ ist, nach dem vorhergesagten $X_k^{(1)}$ gleich x^{kp^2} . Auf ähnliche Weise erhalten wir Ausdrücke für x^{kp^3} , x^{kp^4} , ..., wenn wir die Substitutionen S^3, S^4, \dots benutzen. Wir wollen die Koeffizienten dieser Substitutionen durch $c_{kl}^{(2)}$, $c_{kl}^{(3)}$, ... bezeichnen.

Betrachten wir nun zum Beispiel die Gleichung

$$x^{p^2} = c_{10}^{(2)} + c_{11}^{(2)}x + c_{12}^{(2)}x^2 + \dots + c_{1,n-1}^{(2)}x^{n-1}$$

welche für alle Wurzeln des Polynoms $f(x)$ gilt. Wenn $f(x)$ einen irreduziblen Teiler dritten Grades besitzt, so gilt für die Wurzeln dieses Teilers gleichzeitig die Beziehung $x^{p^2} = x$. Daraus folgt, daß für diejenigen Wurzeln von $f(x)$, die gleichzeitig Wurzeln des irreduziblen Polynoms dritten Grades sind, die Beziehung

$$c_{10}^{(2)} + (c_{11}^{(2)} - 1)x + c_{12}^{(2)}x^2 + \dots + c_{1,n-1}^{(2)}x^{n-1} = 0 \quad (.)$$

gilt. Der größte gemeinschaftliche Teiler der linken Seite der letzten Gleichung und des Polynoms $f(x)$ ist das Produkt aller

irreduziblen Bestandteile dritten und ersten Grades von $f(x)$ (das letzte, weil die Wurzeln der linearen Bestandteile von $f(x)$ ebenfalls der Gleichung $x^p = x$ genügen).

Auf solche Weise bekommen wir durch sukzessives Dividieren, zuerst das Produkt aller linearen Teiler von $f(x)$, dann das Produkt aller irreduziblen Teiler zweiten, dritten und s. w. Grades. Falls die Gleichung (.) eine identische Gleichung ist (d. h. für jedes x erfüllt ist: $c_{10}^{(2)} = 0, c_{11}^{(2)} = 1, c_{12}^{(2)} = 0, \dots$), so besteht $f(x)$ nur aus irreduziblen Faktoren dritten und ersten Grades. Die Substitution $X^{(2)} = S^3(x)$ ist die identische Substitution.

*

0 rozložitelnosti mnohočlenů s celistvými součiniteli dle modulu p ,
kde p jest prvočíslo.

(Obsah předešlého článku.)

V článku jest vyložena metoda, kterou lze nalézt pro daný polynom $f(x)$ n -tého stupně s celými racionálními součiniteli, v kolik ireducibilních faktorů se tento polynom rozpadá mod p , a jaké mají tyto faktory stupně. Autor sestruje pomocí součinitelů polynomu $f(x)$ jistou lineární substituci o n proměnných. Charakteristická rovnice této substituce má v tělese \bar{K}_p vždy tvar:

$$(\lambda^{q_1} - 1) (\lambda^{q_2} - 1) \dots (\lambda^{q_n} - 1) = 0.$$

Každý faktor $(\lambda^{q_i} - 1)$ odpovídá jednoznačně určitému ireducibilnímu faktoru mod p stupně q_i -tého polynomu $f(x)$ mimo tyto případy:

- 1) když jedno neb více z čísel q_i jest dělitelno p ,
- 2) když nejméně p z čísel q_i jest si navzájem rovno.