

Zdeněk Chládek

Nová metoda rozkladu reducibilních mnohočlenů jedné proměnné

Časopis pro pěstování matematiky a fysiky, Vol. 51 (1922), No. 2, 97--101

Persistent URL: <http://dml.cz/dmlcz/121915>

## Terms of use:

© Union of Czech Mathematicians and Physicists, 1922

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>

$$(37) \quad S \begin{pmatrix} x_i = \sum_{\varrho=1}^2 \sum_{t\varrho=0}^2 x_i^{\varrho, t\varrho} \bar{x}_{\varrho, t\varrho} \\ y_k = \sum_{\sigma=1}^2 \sum_{t\sigma=0}^2 x_k^{\sigma, t\sigma} \bar{y}_{\sigma, t\sigma} \end{pmatrix}$$

Dostaneme tak ze svazku  $A - \lambda E$  svazek

$$\bar{A} - \lambda \bar{E} = \sum_{\varrho, \sigma=1}^2 \sum_{t\varrho, t\sigma=0}^2 (a_{\varrho, t\varrho; \sigma, t\sigma} - \lambda \bar{\varepsilon}_{\varrho, t\varrho; \sigma, t\sigma}) \bar{x}_{\varrho, t\varrho} \bar{y}_{\sigma, t\sigma} =$$

$$= S' (A - \lambda E) S \text{ v němž jest}$$

$$(38) \quad \begin{cases} \bar{a}_{\varrho, t\varrho; \sigma, t\sigma} = \sum_{i, k=1}^6 a_{i, k} x_i^{\varrho, t\varrho} x_k^{\sigma, t\sigma} \\ \bar{\varepsilon}_{\varrho, t\varrho; \sigma, t\sigma} = \sum_{i, k=1}^6 \varepsilon_{i, k} x_i^{\varrho, t\varrho} x_k^{\sigma, t\sigma} = x_1^{\varrho, t\varrho} x_1^{\sigma, t\sigma} - x_4^{\varrho, t\varrho} x_1^{\sigma, t\sigma} \\ + x_2^{\varrho, t\varrho} x_5^{\sigma, t\sigma} - x_6^{\varrho, t\varrho} x_2^{\sigma, t\sigma} + x_3^{\varrho, t\varrho} x_6^{\sigma, t\sigma} - x_6^{\varrho, t\varrho} x_3^{\sigma, t\sigma} \end{cases}$$

(Pokračování.)

## Nová metoda rozkladu reducibilních mnohočlenů jedné proměnné.

Napsal Prof. Zdeněk Čhtádek v Hodonině.

Jsou známy dvě metody, jak stanovit dělitele mnohočlenu reducibilního: metoda starší, Kroneckerova<sup>1)</sup> posléze zjednodušená Rungem,<sup>2)</sup> opírající se o interpolační vzorce, a druhá, Mandlova,<sup>3)</sup> která vypočítává součinitele dělitelů hledaných přímo pomocí diofantických rovnic, jež vzniknou ze vztahů platících mezi součiniteli danými a hledanými. Obě vyžadují mnoho počítání a jsou proto pro praxi nevýhodné.

V následujícím vyložím metodu novou, vzniklou zjednodušením a sloučením obou uvedených, která už proto, že obecně po krátkých úvahách umožňuje zjistiti, zda předložený mnohočlen jest vůbec reducibilní nebo ne, uspoří mnoho počítání pokusného, s použitím tabulek multiplikačních pak omezuje počet nutných operací na minimum.

Mnohočlen daný s celistvými součiniteli buďž

$$F(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n, \text{ kde } c_n > 0.$$

Jest patrnó, že  $F(x) \equiv c_0 \pmod{x}$  a každý dělitel  $F(x)$  musí dle celistvého čísla  $co$  modulu, jež za  $x$  dosadíme, být shodný se svým absolutním členem.

<sup>1)</sup> Crelles Journ. sv. 92.

<sup>2)</sup> Crelles Journ. sv. 94.

<sup>3)</sup> Crelles Journ. sv. 113.

Dejme tomu, že by předložený mnohočlen dal se rozložití ve dva nebo více dělitelů stupňů nižších s celistvými součiniteli, tudíž: byl reducibilní, tak že ku př. by platilo

$$F(x) = \varphi_1(x) \cdot \varphi_2(x) \cdot \varphi_3(x).$$

Je-li  $r$  číslo celistvé, musí pak existovati rozklady celistvého čísla  $F(r) = \varphi_1(r) \cdot \varphi_2(r) \cdot \varphi_3(r)$  a členu absolutního  $c_0 = \gamma_1 \cdot \gamma_2 \cdot \gamma_3$ , kde  $\varphi_1(r) \equiv \gamma_1, \varphi_2(r) \equiv \gamma_2, \varphi_3(r) \equiv \gamma_3 \pmod{r}$ . Máme tu dvě skupiny čísel; každému z čísel skupiny jedné jest kongruenci přiřazeno jisté číslo skupiny druhé; čísla jedné skupiny dají spolu násobena  $F(r)$ , čísla skupiny druhé pak  $c_0$ . Jest to jeden způsob rozkladu absolutního členu a to pro modul  $r$ .

Všimněme si nyní rozkladů, které jsou možny vždy, i když  $F(r)$  a  $c_0$  jsou prvočíslly. Jsou to rozklady  $F(r) = 1 \cdot F(r)$ ,  $c_0 = 1 \cdot c_0$ , které si též vždy odpovídají. Nasvědčovaly by děliteli  $\varphi_1(x)$  pro který  $\varphi_1(r) = 1$ . Možnost, že by jeden z hledaných dělitelů pro  $x = r$  stal se rovným jedné, vyloučíme tím, že zvolíme  $r > \varrho$ , kde  $\varrho$  značí horní mez absolutních hodnot kořenů rovnice  $F(x) = 0$ , již určíme dle známého vzorce  $\varrho = M + 1$ , při čemž  $M = \frac{|c_m|}{c_n}$

a  $c_m$  značí součinitele největší absolutní hodnoty z řady součinitelů mnohočlenu  $F(x)$ . V mnohých případech bude však lze udati číslo mnohem menší co horní mez kořenů. Volíme-li modul  $r$  se zřením k uvedeně nerovnině, můžeme rozklad  $F(r)$  z našich úvah vyloučiti.

Můžeme pak říci, že předložený mnohočlen  $F(x)$  jest irreducibilní, jestliže pro  $r > \varrho$  celistvé číslo  $F(r)$  nemá dělitelů skutečných shodných s děliteli svého členu absolutního  $c_0$ , jednotku a  $c_0$  v to počítaje. Jest to podmínka postačující, nutná nikoliv.

Obecně nebude rozklad absolutního členu  $c_0$  uvedenými podmínkami stanoven jednoznačně. Proto zvolíme si další modul  $s > r$ . Vyhledáme-li nyní přípustné rozklady absolutního členu, máme druhý způsob jeho rozkladu. Oba způsoby musí souhlasit v jistém rozkladu, jinak jest  $F(x)$  irreducibilní.

Obecně rozkladů souhlasných bude víc. Tu uvažujeme následovně. V intervalu  $(\varrho, \infty)$   $F(x)$  s rostoucím  $x$  stále roste, totéž platí o všech dělitelích. Máme-li dle modulu  $r$  rozklad  $F(r) = R = R_1 \cdot R_2 \cdot R_3$  a  $c_0 = \gamma_1 \cdot \gamma_2 \cdot \gamma_3$ , kde  $R_1 \equiv \gamma_1, R_2 \equiv \gamma_2, R_3 \equiv \gamma_3 \pmod{r}$  a dle mod.  $s$  rozklad  $F(s) = S = S_1 \cdot S_2 \cdot S_3$ , kde  $S_1 \equiv \gamma_1, S_2 \equiv \gamma_2, S_3 \equiv \gamma_3 \pmod{s}$ , musí též býti  $F(r) < F(s)$ ,  $R_1 < S_1, R_2 < S_2, R_3 < S_3$ . To nám dovoluje dále omeziti počet přípustných rozkladů. Ve většině případů bude nyní rozklad členu absolutního jednoznačně stanoven, jinak jest nutno uvažovati další rozklady pro modul  $t > s$ .

Budíž jednoznačný rozklad členu  $c_0 = \gamma_1 \cdot \gamma_2 \cdot \gamma_3$ , pak shrneme tyto tři dělitele ve dva pišice  $\gamma_1 = a_0, \gamma_2 \cdot \gamma_3 = b_0$ . Pro další

postup víme, že platí vztahy:  $c_0 = a_0 b_0$ ,  $c_1 = a_0 b_1 + b_0 a_1$ ,  $c_2 = a_0 b_2 + b_0 a_2 + b_1 a_1$  a obecně  $C_r = c_r = \sum_{i=1}^{r-1} a_i b_{r-i} + a_0 b_r + b_0 a_r$  ( $r = 1, 2, 3, \dots, n$ ), kde  $c_0, a_0$  a  $b_0$  jsou čísla známá a  $a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_{n-m}$  součinitelé příslušných dělitelů  $\varphi(x) = \varphi_1(x)$  a  $\psi(x) = \varphi_2(x) \cdot \varphi_3(x)$ .

Pro součinitele  $a_1, b_1$  stanovíme zbytky dle modulu  $s: z_{a,1}$  a  $z_{b,1}$ . Jest totiž  $a_1 = \frac{\varphi(s) - a_0}{s} \equiv \alpha_1 s + z_{a,1}$  a  $b_1 = \frac{\psi(s) - b_0}{s} \equiv \beta_1 s + z_{b,1}$ . První rovnice diofantická o neznámých  $\alpha_1, \beta_1$  bude  $a_0(\alpha_1 s + z_{a,1}) + b_0(\beta_1 s + z_{b,1}) = c_1$  nebo

$$a_0 \beta_1 + b_0 \alpha_1 = \frac{c_1 - (a_0 z_{b,1} + b_0 z_{a,1})}{s}$$

zvolíme jisté řešení  $\alpha_1, \beta_1$  a vypočteme  $a_1, b_1$ , nato stanovíme zbytky  $z_{a,2}, z_{b,2}$  z kongruenci  $a_2 \equiv \frac{\varphi(s) - a_1 s - a_0}{s^2} \equiv \alpha_2 s + z_{a,2}$  a  $b_2 \equiv \frac{\psi(s) - b_1 s - b_0}{s^2} \equiv \beta_2 s + z_{b,2}$ . Pro  $\alpha_2, \beta_2$  máme pak rovnici

$$a_0 \beta_2 + b_0 \alpha_2 = \frac{C_2 - (a_0 z_{b,2} + b_0 z_{a,2})}{s}$$

kde  $C_2$  má svrchu uvedený význam. Nyní z jistého řešení  $\alpha_2, \beta_2$  vypočteme  $a_2, b_2$ , na to pak zbytky  $z_{a,3}, z_{b,3}$  dle vzorce  $a_3 \equiv \frac{\varphi(s) - a_2 s^2 - a_1 s - a_0}{s^3} \equiv \alpha_3 s + z_{a,3}$ . Tak pokračujeme až

do konce; další průběh počtů z uvedeného jest jasný. Theoreticky rovnice diofantické sice připouštějí řešení nekonečně mnoho avšak čísla  $\alpha_r, \beta_r$  ( $r = 1, 2, \dots, n$ ) budou malá, tím menší, čím větší byl zvolen modul  $s$  a bude tudíž možno nalézt je na první pohled bez soustavného řešení příslušných rovnic diofantických. Kdyby další počet ukázal, že jsme nepřipadli na hodnoty správné, jest pak hledati hodnoty jiné, což zajisté nevyžaduje mnoho času, neboť se jedná o počty prajednoduché. Může se ovšem ještě státi, že žádná soustava čísel  $\alpha_r, \beta_r$  s dotýcnými zbytky nevede ku řešení naší úlohy;  $F(x)$  jest pak irreducibilní, což bychom též seznali z rozkladu absolutního členu  $c_0$  pro další modul  $t > s$ .

Když jsme byli stanovili  $\varphi(x)$  a  $\psi(x)$ , jest nám ještě stejnou cestou nalézt  $\varphi_2(x)$  a  $\varphi_3(x)$ .

Celý postup objasníme na příkladu, jež Runge i Mandl řeší cestou mnohem obtížnější.

Budíž dán mnohočlen

$$F(x) = 3x^7 + 7x^6 - 10x^5 - 19x^4 + 172x^3 + 71x^2 + 17x - 66.$$

Jakožto horní mez absolutních hodnot kořenů rovnice  $F(x) = 0$  postačí vzít  $\varrho = 5$ , zvolíme tedy za moduly  $r = 7$ ,  $s = 10$ . Jest pak

$$F(7) = 3143011 = 17 \cdot 293 \cdot 631, \\ F(10) = 35989204 = 2^2 \cdot 17 \cdot 23 \cdot 23011.$$

Ježto první rozklad dává tři prvočísla, nebude mít náš mnohočlen jistě více než tři dělitele ireducibilní, neboť jednotku co dělitele lze vyloučiti. Rozložíme-li však  $F(10)$  všemi možnými způsoby ve tři činitele, shledáme, že není možno naléztí rozklad takový, aby současně každému z činitelů odpovídalo mezi děliteli  $F(7)$  číslo menší; nebude tedy  $F(x)$  mítí tři, nýbrž toliko dva dělitele ireducibilní.

Rozložíme  $F(7)$ ,  $F(10)$ , a  $-66$  všemi možnými způsoby ve dva činitele. To dá, když v závorce připojíme vždy zbytek čísla předcházejícího dle dotyčného modulu (7 resp. 10), tuto soustavu:

$$\begin{aligned} F(7) &= 17(3) \cdot 184883(6) \quad (\alpha) & -66 &= -1(6) \cdot +66(3) \quad (a) \\ &= 293(6) \cdot 10727(3) \quad (\beta) & &= -2(5) \cdot +33(5) \quad (b) \\ &= 631(1) \cdot 4981(4) \quad (\gamma) & &= -3(4) \cdot +22(1) \quad (c) \\ & & &= -6(1) \cdot +11(4) \quad (d) \\ & & &= +1(1) \cdot -66(4) \quad (e) \\ & & &= +2(2) \cdot -33(2) \quad (f) \\ & & &= +3(3) \cdot -22(6) \quad (g) \\ & & &= +6(6) \cdot -11(3) \quad (h) \\ \\ F(10) &= 2 \cdot 17994602 \quad (\delta) & -66 &= -1(9) \cdot +66(6) \quad (a) \\ &= 4 \cdot 8997301 \quad (\epsilon) & &= -2(8) \cdot +33(3) \quad (b) \\ &= 17 \cdot 2157052 \quad (\eta) & &= -3(7) \cdot +22(2) \quad (c) \\ &= 23 \cdot 1564748 \quad (\theta) & &= -6(4) \cdot +11(1) \quad (d) \\ &= 34 \cdot 1078526 \quad (\iota) & &= +1(1) \cdot -66(4) \quad (e) \\ &= 46 \cdot 782374 \quad (\kappa) & &= +2(2) \cdot -33(7) \quad (f) \\ &= 68 \cdot 529263 \quad (\lambda) & &= +3(3) \cdot -22(8) \quad (g) \\ &= 92 \cdot 391187 \quad (\mu) & &= +6(6) \cdot -11(9) \quad (h) \\ &= 391 \cdot 92044 \quad (\nu) \\ &= 782 \cdot 46022 \quad (\omega) \\ &= 1564 \cdot 23011 \quad (\varrho) \end{aligned}$$

Předně můžeme vyloučiti rozklady  $\delta$ ,  $\epsilon$ ,  $\eta$ , neboť nevyhovují podmínce, že dělitelé v  $(\varrho, \sim)$  musí být funkce stále rostoucí. Taktéž vyloučíme rozklady  $a$ ,  $b$ ,  $f$ ,  $h$ , neboť  $a$ ,  $h$  nemá dle modulu 10 analogie v rozkladu  $F(10)$  a  $b$ ,  $f$  dle modulu 7 v rozkladu  $F(7)$ . Zato je vzítí v úvahu rozklady  $\alpha$ ,  $\beta$  jež rozkladem  $g$  jsou sobě přiřazeny. Vedly by ku děliteli  $\varphi(x)$  pro něž  $\varphi(7) = 17$ ,  $\varphi(10) = 23$ , tudíž  $\varphi(x) = 2x + 3$ . Ten však nevyhovuje, neboť 2 není dělitelem

