Vilém Jung

Příspěvek k nauce o číslech

Časopis pro pěstování mathematiky a fysiky, Vol. 14 (1885), No. 1, 30--35

Persistent URL: http://dml.cz/dmlcz/122095

$$z^n - a_1 z^{n-1} + \ldots \mp z_0(z_0{}^{n-1} - a_1 z_0^{n-2} + \ldots)$$
$$= (z^n - z_0^n) - a_1(z^{n-1} - z_0^{n-1}) + \ldots = (z - z_0)\,P_{n-1},$$

značí-li P_{n-1} polynom stupně $n-1$-ho. Poněvadž však

$$P_{n-1} = (z - z'_1)\ldots(z - z'_{n-1}),$$

máme

$$P_n = (z - z_0)(z - z'_1)\ldots(z - z'_{n-1}). \qquad \text{Q. E. D.}$$

Příspěvek k nauce o číslech.

Píše

Vilém Jung,

assistent na české vysoké škole technické v Praze.

1. Soustavu n jednoduchých shod formy $x_k \equiv \alpha_k \pmod{a_k}$ řešil Euler jednoduše vzorcem

$$x \equiv \sum_{k=1}^{n} \alpha_k A_k u_k \pmod{\prod_{k=1}^{n} a_k},$$

kde $A_k = \dfrac{\prod_{k=1}^{n} a_k}{a_k}$, a veličiny u_k se určí ze soustavy shod formy $A_k u_k \equiv 1 \pmod{a_k}$.*)

Má-li se však řešiti soustava shod jednoduchých:

$$\begin{aligned} \beta_1 x &\equiv \alpha_1 \pmod{a_1} \\ \beta_2 x &\equiv \alpha_2 \pmod{a_2} \\ &\cdots\cdots\cdots \\ \beta_k x &\equiv \alpha_k \pmod{a_k} \\ &\cdots\cdots\cdots \\ \beta_n x &\equiv \alpha_n \pmod{a_n}, \end{aligned} \qquad (1)$$

kde jsou k sobě příslušné veličiny β_k, a_k nesoudělnými, nutno uvésti soustavu (1) na jednodušší, kde obecně $\beta_k = 1$, což se provede, řeší-li se jednotlivé shody dle x. Na základě soustavy jednodušších shod dospěje se pak způsobem Eulerovým nebo Gaussovým **) ku shodě výsledné.

Řešení shod soustavy (1) obejdeme na základě následující jednoduché úvahy.

---

*) Viz dr. Studničky: „Nauka o číslech“ pg. 137. §. 23.

**) ibid. pag. 139.

Budiž N jedno z čísel, vyhovujících veškerým podmínkám, vyjádřeným soustavou (1). Obecně musí tedy

$$Z\left(\frac{\beta_k N - \alpha_k}{a_k}\right) = 0. \qquad (2)$$

Pišme N formou:

$$N = C_1 \alpha_1 + C_2 \alpha_2 + \ldots + C_k \alpha_k + \ldots + C_n \alpha_n, \qquad (3)$$

kde čísla C_1, C_2, ... C_k, ... C_n jest nám určiti. Z (3) plyne jednoduchou cestou:

$$\frac{\beta_k N - \alpha_k}{a_k} = \frac{\beta_k C_1 \alpha_1 + \ldots + \alpha_k(\beta_k C_k - 1) + \ldots + \beta_k C_n \alpha_n}{a_k} \qquad (4)$$

Má-li se rovnice (2) vyplniti, musí čitatel pravé strany rovnice (4) býti dělitelný veličinou a_k, čemuž se vyhoví, je-li každý člen zmíněného součtu touto dělitelný.

Poněvadž jsou β_k, a_k nesoudělnými a veličiny α_1, α_2, ... α_k, ... α_n obecně veličinou a_k dělitelny býti nemusí, nutno především, aby C_1, C_2, C_3, ..., C_{k-1}, C_{k+1}, ..., C_n obsahovaly veličinu a_k, a dále aby se vyhovělo podmínce

$$\beta_k C_k \equiv 1 \pmod{a_k}. \qquad (5)$$

Ježto jest β_k s a_k nesoudělné, musí býti dle (5) i C_k s tímto nesoudělné.

Provedeme-li tuto úvahu vzhledem k ostatním ukazovatelům, poznáme, že C_k musí obsahovati veškeré moduly mimo a_k, s kterým jest nesoudělné, a musí vyhověti shodě

$$\beta_k C_k \equiv 1 \pmod{a_k}.$$

Z té příčiny nutno psáti $C_k = \frac{\prod_{k=1}^{n} a_k}{a_k} u_k = A_k u_k$, kde u_k určíme ze shody $\beta_k A_k u_k \equiv 1 \pmod{a_k}$. Z toho konečně plyne

$$N = \sum_{k=1}^{n} \alpha_k A_k u_k.$$

Úloze pak obecně vyhoví $x = N + \lambda \prod_{k=1}^{n} a_k$, t. j.

$$x \equiv \sum_{k=1}^{n} \alpha_k A_k u_k \pmod{\prod_{k=1}^{n} a_k}.$$

Tento vzorec se úplně shoduje se vzorcem, jejž stanovil Euler pro soustavu shod formy $x \equiv \alpha_k \pmod{a_k}$, jen že se v případě tuto rozebraném stanoví veličiny u_k ze soustavy shod formy $\beta_k A_k u_k \equiv 1 \pmod{a_k}$ od $k = 1$ až $k = n$.

Tím tedy pouze ukázáno k tomu, kterak lze význam tohoto Eulerova vzorce rozšířiti.

K objasnění stojž zde příklad následující. Má se řešiti soustava shod:

$$5x \equiv 9 \pmod{7},$$
$$6x \equiv 5 \pmod{11},$$
$$4x \equiv 7 \pmod{3}.$$

Ježto $\prod_{k=1}^{n} a_k = 7 . 11 . 3 = 231,$

$$A_1 = 3 . 11 = 33, \quad A_2 = 7 . 3 = 21, \quad A_3 = 7 . 11 = 77,$$
$$\alpha_1 = 9 \qquad \alpha_2 = 5 \qquad \alpha_3 = 7$$
$$\beta_1 = 5, \qquad \beta_2 = 6, \qquad \beta_3 = 4,$$

plyne soustava shod, úlohu řešících

$$5 . 3 . 11\, u_1 \equiv 1 \pmod{7},$$
$$6 . 7 . 3\, u_2 \equiv 1 \pmod{11},$$
$$4 . 7 . 11\, u_3 \equiv 1 \pmod{3},$$

z kteréž cestou známou se podává:

$$u_1 \equiv 2 \pmod{7},$$
$$u_2 \equiv -2 \pmod{11},$$
$$u_3 \equiv -1 \pmod{3}.$$

Pomocí hodnot pro u_1, u_2, u_3 číselně nejmenších dospějeme co nejkratčeji ku

$$N = 9 . 3 . 11 . 2 + 5 . 7 . 3 . -2 + 7 . 7 . 11 . -1 = -155.$$

Z toho plyne výsledná shoda

$$x \equiv -155 \pmod{231},$$

aneb nejkratčeji

$$x \equiv 76 \pmod{231}.$$

V příkladě voleny moduly nesoudělné, ježto se každá soustava shod na tu formu dle známých zásad převésti dá.

2. Eulerova vzorce, řešícího soustavu jednoduchých shod, možno užiti jen tenkráte, jsou-li moduly $a_1, a_2, \ldots, a_k, \ldots, a_n$ čísly nesoudělnými.

Má-li se totiž vyhověti shodě $\beta_k A_k u_k \equiv 1 \pmod{a_k}$ celistvým u_k, musí býti veličiny A_k, a_k nesoudělné, a ježto $A_k = \frac{\prod_{k=1}^{n} a_k}{a_k}$,

musí veškeré ostatní moduly býti s modulem a_k nesoudělnými. Úhrnný výsledek podobné úvahy vzhledem ku všem ukazovatelům od $k = 1$ až $k = n$ zřejmě dokazuje, že musí a_1, a_2, a_k, ..., a_n býti vespolek nesoudělnými. Z Eulerova vzorce pak vysvítá, že možno soustavě jednoduchých shod, jichž moduly jsou nesoudělné, vyhověti řadou čísel celistvých. Ze všeho tedy patrno, že nutno soustavu daných shod převésti na soustavu shod o modulech nesoudělných. Každou shodu rozložíme dle známé zásady *) přiměřeně v jistý počet parcialních shod. V této odvozené soustavě vyskytnou se skupiny shod, majících *stejné* moduly. A tu nutno rozeznávati dvé případů:

a) Jsou-li shody každé skupiny tohoto rázu od sebe podstatně různé, nelze shodám odvozené soustavy vyhověti současně jistou řadou celistvých čísel pro x. Původní soustava pak není řešitelnou.

b) Veškeré shody každé z oněch skupin neliší se podstatně od sebe a dají se pokaždé jedinou shodou nahraditi. Odvozené soustavě shod vyhovuje jistá řada celistvých čísel pro x, tak že původní soustava jest řešitelnou. V tomto případě se vynechají přebytečné shody, a odvozená soustava obsahuje shody, jichž moduly jsou vespolek nesoudělnými, a proto ji možno známým způsobem řešiti.

Nutno tedy v podobných případech tyto okolnosti vyšetřiti, nemá-li se bezúčelně počítati.

3. V následujícím ještě ukáži, kterak možno řešitelné soustavě n jednoduchých shod přímo zjednati shodu výslednou.

Budiž dáno:

$$\begin{aligned} \beta_1 x &\equiv \alpha_1 \pmod{a_1} \\ \beta_2 x &\equiv \alpha_2 \pmod{a_2} \\ &\cdots\cdots\cdots \\ \beta_k x &\equiv \alpha_k \pmod{a_k} \\ &\cdots\cdots\cdots \\ \beta_n x &\equiv \alpha_n \pmod{a_n}, \end{aligned} \qquad (1)$$

kde jsou k sobě příslušné veličiny β_k a a_k nesoudělné, a dle předeslaného možno také předpokládati, že jsou a_1, a_2, ..., a_k, ..., a_n nesoudělnými.

*) ibid, pag. 103.

Znamená-li jako prvé $A_k = \frac{\prod_{k=1}^{n} a_k}{a_k}$, a platí-li

$$\beta_k x \equiv \alpha_k \pmod{a_k},$$

platí i zajisté

$$\beta_k A_k x \equiv \alpha_k A_k \left(\text{mod. } \prod_{k=1}^{n} a_k\right),$$

aneb obecněji

$$\lambda_k \beta_k A_k x \equiv \lambda_k \alpha_k A_k \left(\text{mod. } \prod_{k=1}^{n} a_k\right).$$

Z (1) pak plyne:

$$\begin{aligned}
\lambda_1 \beta_1 A_1 x &\equiv \lambda_1 \alpha_1 A_1 \left(\text{mod. } \prod_{k=1}^{n} a_k\right) \\
&\cdots\cdots\cdots\cdots \\
\lambda_k \beta_k A_k x &\equiv \lambda_k \alpha_k A_k \left(\text{mod. } \prod_{k=1}^{n} a_k\right) \\
&\cdots\cdots\cdots\cdots \\
\lambda_n \beta_n A_n x &\equiv \lambda_n \alpha_n A_n \left(\text{mod. } \prod_{k=1}^{n} a_k\right).
\end{aligned} \tag{2}$$

Z toho se snadno sestaví dle známých vět výsledná shoda:

$$x \sum_{k=1}^{n} \lambda_k \beta_k A_k \equiv \sum_{k=1}^{n} \lambda_k \alpha_k A_k \left(\text{mod. } \prod_{k=1}^{n} a_k\right), \tag{3}$$

kterou nutno někdy na základě rozkladu modulu $\prod_{k=1}^{n} a_k$ řešiti, aby se vyhnulo nesnázi, do níž přivádí počtáře ta okolnosť, že mu nelze krátiti shodu číslem soudělným s modulem. *)

Co se týče neurčitých součinitelů λ_k, nutno je voliti dle libosti tak, aby ve výsledné shodě objevila se čísla co nejmenší; ovšem nesmí býti λ_k nullou. Při tomto řešení působí nepohodlí složitosť modulu výsledné shody. Eulerův způsob přivádí na pomocné shody s moduly jednoduššími, za to jest nám ale dle tohoto řešiti n shod!

Způsob právě vyložený vede často velmi rychle k cíli, čehož důkazem budiž řešení úlohy, která jest v Dr. Studničky: „Nauce o číslech“, pag. 138. řešena Eulerovským způsobem.

---

*) ibid. pag. 135.

Tam jest řešiti

$$x \equiv 8 \pmod{28},$$
$$x \equiv 14 \pmod{19},$$
$$x \equiv 3 \pmod{15}.$$

Z toho plyne dle (3) pro $\lambda_1 = -1$, $\lambda_2 = +2$, $\lambda_3 = -1$ po krátké úpravě:

$$x\{15(28-19)+28(15-19)\} \equiv 15(14 \,.\, 28 - 19 \,.\, 8) + 28\,(14 \,.\, 15 - 3 \,.\, 19) \pmod{7980},$$

čili

$$23x \equiv -96 \pmod{7980},$$

z čehož

$$347 \,.\, 23x - 7980x \equiv 347 \,.\, -96 + 50 \,.\, 7980 \pmod{7980},$$

tak že konečně $x \equiv 6588 \pmod{7980}$.

Rozřešme dále tímto způsobem příklad, řešený v odst. 1.

Pro tento platí dle (3) pro

$$-\lambda_1 = -\lambda_2 = +\lambda_3 = +1$$

výsledná shoda:

$$17x \equiv 137 \pmod{231},$$

čili

$$13 \,.\, 17x \equiv 13 \,.\, 137,$$

avšak

$$231x \equiv 8 \,.\, 231,$$

odečtením

$$10x \equiv 67 \pmod{231},$$

čili

$$23 \,.\, 10x \equiv 23 \,.\, 67,$$

avšak

$$231x \equiv 7 \,.\, 231,$$

odečtením

$$x \equiv 76 \pmod{231},$$

jako předešle.

O chvějní době.

Napsal

Vavřinec Jelínek,

professor v Novém Městě u Vídně.

Odstředivé kývadlo. Proběhne-li hmota m vodorovnou kružnici o poloměru $r = bc$ jednou za dobu T, dá její odstředivost

$$p = \frac{4\pi^2 mr}{T^2}$$

s její váhou

$$P = mg$$