Karel Küpper

Jednoduché důkazy některých vět o kmenných číslech

Časopis pro pěstování mathematiky a fysiky, Vol. 10 (1881), No. 1, 10--20

Persistent URL: http://dml.cz/dmlcz/123969

jeho seznal prostředky k určení *sploštěnosti* naší zeměkoule a který dovedl ze všeobecné gravitace vyložiti *velké nerovnosti planet* Jupitera a Saturna. Jak ohromné bylo však mé sklamání, když jsem jednoho dne uslyšel, kterak paní Laplace-ová, ku svému choti se blížíc, pravila: „Nechtěl bys mi dnes svěřiti klíček od cukru? Ještě živějším spůsobem dojala mne o několik dní později jiná událost. Syn Laplace-ův *Emil* připravoval se ku přijímací zkoušce na polytechniku a docházel někdy ke mně na hvězdárnu. Při jedné takové návštěvě vykládal jsem mu spůsob řešení číselných rovnic pomocí řetězců čili t. zv. *methodu Lagrange-ovu.* O methodě tě vypravoval syn otci se zvláštní zálibou. Nezapomenu nikdy na prudký výbuch hněvu, který po tomto vypravování následoval a slyším dosud ty trpké výčitky, které mi činil, že jsem hájil methodu, která v praxi snad jest dosti zdlouhavá, ale v theorii, co elegance a přesnosti se týče, úplně bezvadná. Žárlivosť a předsudek nejevily se snad nikdy tak okázale a drsně. „Ach pomyslil jsem si, jak pravdivě cítili staří Řekové, připisujíce lidské slabosti i tomu, který pouhým zvraštěním mohl celým Olympem otřásati! —

(Pokračování.)

Jednoduché důkazy některých vět o kmenných číslech.

Sepsal

prof. **Karel Küpper.**

I.

1. Transformace jisté irracionálné hodnoty.

Dán-li irracionálný výraz

$$\frac{\sqrt{A}+J}{D} > 1$$

a platí-li

$$1)\ \sqrt{A} > J,\quad 2)\ A \equiv J^2 \pmod{D},$$

tu jej lze převésti na tvar obdobný

$$\frac{\sqrt{A}+J'}{D'},$$

v němž celistvá čísla J', D' vyhovují podmínkám

$$\sqrt{A} > J' > 0, \quad A \equiv J'^2 \pmod{D'}.$$

Označme literou K největší celistvé číslo obsažené v $\frac{\sqrt{A}+J}{D}$; tedy

$$\frac{\sqrt{A}+J}{D} = K + \frac{\sqrt{A}-(KD-J)}{D}.$$

Položme

$$KD - J = J';$$

pak platí patrně

1) $\sqrt{A} > J' > 0$, a též 2) $KD > J$.

Abychom dokázali druhou nerovnost, různěme případy kdy $D \gtreqless J$. Je-li $D > J$ tu druhá nerovnost patrna. Je-li $D = J$, tu patrně $K > 1$ a tedy $KD > J$. Je-li konečně v případu třetím J obsaženo mezi qD a $(q+1)D$, tu patrně K aspoň $2q$ obnáší a poněvadž $2qD$ nemůže být menší než $(q+1)D$, máme i v tomto případu $KD > J$.

Dále máme

$$\frac{D}{\sqrt{A}-(KD-J)} > 1,$$

aneb odstranivše z jmenovatele irracionálnost

$$\frac{D[\sqrt{A}+KD-J]}{A-(KD-J)^2} > 1 \text{ t. j. } \frac{\sqrt{A}+J'}{\frac{A-J^2}{D}+2KJ-K^2D} > 1.$$

Číslo $A - J'^2$ jest číslem D dělitelno; buď celistvý podíl D', tedy

$$D' = \frac{A-J'^2}{D}. \qquad \text{(I)}$$

Původní výraz tedy takto přetvořen:

$$\frac{\sqrt{A}+J}{D} = K + \frac{\sqrt{A}-J'}{D} = K + \frac{D'}{\sqrt{A}+J'};$$

tak redukován na irracionálnou hodnotu $\frac{\sqrt{A}+J'}{D'}$, kdež D' a J' hoví vytknutým podmínkám.

Platí nyní nerovnosti

$$J' + D > \sqrt{A}, \quad J' + D' > \sqrt{A}.$$

První z nich je patrná, jelikož

$$\frac{\sqrt{A} - J'}{D} < 1 \qquad \text{(II)}$$

vůči definici čísla K. Z rovnice

$$A - J'^2 = DD'$$

plyne

$$\frac{\sqrt{A} - J'}{D} = \frac{D'}{\sqrt{A} + J'} < 1.$$

Dále z $J' = KD - J$ máme

$$\frac{\sqrt{A} + J'}{D} = K + \frac{\sqrt{A} - J}{D} > 1;$$

avšak

$$\frac{\sqrt{A} + J'}{D} = \frac{D'}{\sqrt{A} - J'}, \text{ tedy } \frac{\sqrt{A} - J'}{D'} < 1. \qquad \text{(III)}$$

2. Periodičnost odvozených výrazů.

Podrobíme-li $\frac{\sqrt{A} + J'}{D'}$ opět naznačené transformaci, doděláme se nové irracionálné hodnoty $\frac{\sqrt{A} + J''}{D''}$ atd. Toto operování nemá konce, poněvadž každé dvé čísel J, D vyhovuje původním podmínkám. Současně však nahlížíme, že tato čísla přináleží omezené řadě čísel; neboť značí-li a největší celistvé číslo obsažené v $\sqrt{A}$, tu musí vždy $J \leqq a$, a poněvadž

$$\frac{\sqrt{A} + J}{D} > 1$$

jest $2a$ největší hodnote, jíž D dosáhnouti může. Z toho jde, že v nekonečném počtu družin J, D nemohou se vyskytovati družiny skládající se vždy z nových čísel, nýbrž že se musí nějaká družina nutně opět vyskytnouti.

Budiž J', D' družina, která se při oněch transformacích opět objeví, budiž J, D družina ji předcházející tenkráte, kdy se J', D' poprvé objevila, a buď i, d družina ji předcházející, kdy se podruhé objevila; tu ukážeme, že

$$d = D, \quad i = J.$$

Z rovnice

$$A - J'^2 = DD'; \; A - J'^2 = dD'$$

plyne ihned

$$d = D.$$

Abychom ukázali, že $i = J$, označme literou K' největší celistvé číslo obsažené v $\frac{\sqrt{A} + i}{D}$. Pak máme

$$J' = KD - J \text{ a } J' = K'D - i,$$

tedy

$$(K - K')\, D = J - i.$$

Kdyby se rozdíl $J - i$ nerovnal nulle, tedy by z okolnosti, že je $J - i$ dělitelno D, plynulo, že se větší z čísel J, i alespoň rovná menšímu zvětšenému o jedno D, věc to nemožná, poněvadž J a i jsou $< \sqrt{A}$, kdežto dle (II) a (III), jak $J + D$ tak i $i + D$ jest větší než $\sqrt{A}$.

3. Transformace irracionálného výrazu

$$\frac{\sqrt{A} + a}{A - a^2} \text{ čili } \frac{\sqrt{A} + J_1}{D_1},$$

kdež a značí největší celistvé číslo obsažené v $\sqrt{A}$.

Odvodíme-li z napsaného výrazu po řadě dle návodu udaného výrazy $\frac{\sqrt{A} + J_2}{D_2}$, $\frac{\sqrt{A} + J_3}{D_3}$, atd., tu se objeví $\frac{\sqrt{A} + a}{A - a^2}$ opět a sice dříve než kterýkoli z ostatních výrazů. Pak arci se ostatní v témž pořádku jeviti budou. Máme tu tedy periodu podílů počínající s $\frac{\sqrt{A} + a}{A - a^2}$. Co se tkne posledního podílu $\frac{\sqrt{A} + J_n}{D_n}$ této periody, musí jeho jmenovatel D_n rovnati se 1, neboť souvisí s následujícím podílem rovnicí (I) čl. 1. $A - a^2 = \frac{A - a^2}{D_n}$. Hodnotu J_n ustanovíme, uvážíme-li, že musí

$$J_n < \sqrt{A}, \; J_n + D_n \text{ t. j. } J_n + 1 > \sqrt{A},$$

a tedy

$$J_n = a.$$

Označme $\frac{\sqrt{A}+i_1}{d_1}$ předposlední podíl periody, $\frac{\sqrt{A}+i_2}{d_2}$ předpředposlední atd.; pak odděluje poslední podíl $\frac{\sqrt{A}+a}{1}$ dvě totožné řady. V první řadě jsme právě napsali každý podíl dvojím spůsobem, jednou pomocí liter J, D, podruhé pomocí liter i, d.

Buďtež a_1, a_2, a_3, .. největší celistvá čísla obsažená v podílech $\frac{\sqrt{A}+J_1}{D_1}$, $\frac{\sqrt{A}+J_2}{D_2}$, . . . , a x_1. x_2, x_3, .. největší celistvá čísla obsažená v $\frac{\sqrt{A}+i_1}{d_1}$, $\frac{\sqrt{A}+i_2}{d_2}$, . . . , pak platí

$$x_1 = a_1,\ x_2 = a_2,\ x_3 = a_3,\ x_m = a_m;\ \ldots$$

Vskutku máme

$$1)\ D_1 a_1 - a = J_2;\ d_1 x_1 - i_1 = a;$$

a dle rovnice (I)

$$d_1 = A - a^2 \text{ t. j. } = D_1,$$

čímž

$$D_1 (x_1 - a_1) = i_1 - J_2.$$

Kdyby $x_1 > a_1$, tu by vycházelo, že $i_1 \geqq J_2 + D_1$, t. j. $i_1 > \sqrt{A}$, věc to nemožná. Kdyby $x_1 < a_1$ tu by $J_2 \geqq i_1 + D_1$ t. j. $J_2 > \sqrt{A}$, což opět nemožné. Tudíž

$$x_1 = a_1;\ i_1 = J_2,$$

a tedy

$$\frac{A - i_1^2}{d_1} = \frac{A - J_2^2}{D_1} \text{ t. j. } d_2 = D_2.$$

2) Máme

$$D_2 a_2 - J_2 = J_3;\ d_2 x_2 - i_2 = i_1 = J_2$$

čili

$$D_2 x_2 - i_2 = J_2,$$

z čehož odčítáním

$$D_2 (x_2 - a_2) = i_2 - J_3.$$

Opět nemůže $x_2 > a_2$, neboť by následovalo

$$i_2 \geqq J_3 + D_2 \text{ a tedy } i_2 > \sqrt{A};$$

též nemůže $x_2 < a_2$, neboť by pak plynulo $J_3 > \sqrt{A}$; tudíž

$$x_2 = a_2;\ i_2 = J_3 \text{ z čehož hned } D_3 = d_3.$$

Touto cestou plyne obecně

$$x_m = a_m;\ i_m = J_{m+1};\ D_m = d_m.$$

Shledáváme tedy, že členy řady

$$\frac{\sqrt{A}+J_1}{D_1},\ \frac{\sqrt{A}+J_2}{D_2},\ \ldots\ \frac{\sqrt{A}+i_2}{d_2},\ \frac{\sqrt{A}+i_1}{d_1}$$

od obou konců stejně vzdálené obsahují týž počet jednotek a že mají mimo to stejné jmenovatele. Co do čítatelů, chceme-li tu ku J_m nalézti čitatel i_v stejně velký, musíme počítati v opáčném směru o jeden člen méně, t. j. vzíti $v = m - 1$.

Z předcházejících úvah vychází jasně na jevo povaha řetězce periodického, v nějž se vyvinuje $\sqrt{A}$.

Máme:

$$\sqrt{A} = a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_1 + \cfrac{1}{2a + \cfrac{1}{a_1 + \ddots}}}}}}$$

Perioda končí členem $2a$; členy předcházející se podvojně rovnají, a sice vždy ony dva, jež jsou od konců periody stejným počtem členů odděleny.

Různeme nyní dva případy:

1. Počet členů $a_1, a_2, \ldots$ předcházející člen $2a$ nechť je sudý $2m$;

2. tento počet nechť je lichý $2m + 1$.

Učiňme nyní supposici, že A *je číslem lichým.*

Případ 1. Tu se vyskytnou dva po sobě jdoucí stejné členy a_m, a_m, tedy dva jmenovatele $D_m = d_m$.

Máme:

$$\frac{A - i^2_m}{D_m} = d_m,$$

tedy:

$$A = i^2_m + d_m{}^2.$$

Tím patrno, že případ ten nemůže mít místa, kdykoli je A tvaru $4n+3$.

Předpokládáme-li tedy, že A je tvaru $4n+3$, tu musí nastati

případ 2. Zde se mezi čísly a_1, a_2, vyskytuje střední člen, buďsi α; nechť přísluší k irracionálnému výrazu $\frac{\sqrt{A}+J}{D}$. Výraz ten transformací přejde do*) $\frac{\sqrt{A}+J}{d_m}$ (kdež $d_m = D_m$), tedy máme:

$$J = \alpha D - J \quad \text{t. j.} \quad J = \frac{\alpha D}{2}. \qquad \text{(I)}$$

Uvážíme-li, že se D nemůže $= 1$, neb by pak z nerovnosti $J+1 > \sqrt{A}$ plynulo $J = a$ a tedy $\alpha = 2a$, což teprv v posledním členu se stává, uvážíme-li dále, že se D nemůže rovnati číslu A, poněvadž je rozdíl $A - J^2 > 0$ a zároveň dělitelný číslem D, tu pak nalezneme snadno číslo α pro případ, kdy kmenné číslo $A = 4n+3$ touto úvahou:

Poněvadž je $A - \frac{\alpha^2 D^2}{4}$ dělitelno číslem D, musí α býti číslem lichým a tedy $D^2 = 4$ t. j. $D = 2$. Nyní vychází, že $J = \alpha$ je lichým; a tedy, poněvadž $J+2 > \sqrt{A}$, tedy $J+2 > a$, musí J buď $= a$ aneb $= a-1$; první platí je-li a liché, druhé je-li a sudé.

Je-li $\frac{u}{v}$ sblížený zlomek $a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{m-1}}}}$

*) $\frac{\sqrt{A}+J}{D}$ píšeme k vůli stručnosti místo $\frac{\sqrt{A}+J_{m+1}}{D_{m+1}}$; následující irracionálná hodnota jest patrně $\frac{\sqrt{A}+i_m}{d_m}$ a tedy $i_m = J_m = J$ t. j. ona hodnota je $\frac{\sqrt{A}+J}{d_m}$.

a $\frac{u_0}{v_0}$ sblížený zlomek jemu předcházející, při čemž nechť m jest libovolné, tu máme:

$$\sqrt{A} = \frac{\frac{\sqrt{A} + J_m}{D_m} u + u_0}{\frac{\sqrt{A} + J_m}{D_m} v + v_0},$$

z čehož vůči $uv_0 - vu_0 = \pm 1$ vychází

$$u^2 - Av^2 = \pm D_m.$$

Vyskytne-li se tedy hodnota $D_m = 2$, tu bude:

$$u^2 - Av^2 = \pm 2. \qquad \text{(II)}$$

Aby však měla místa tato rovnice, v níž u a v jsou čísla nesoudělná, musejí u a v býti čísly lichými; pak jest ale i číslo $u^2 + 2$ i $u^2 - 2$ tvaru $4n + 3$, tudíž jest dle (II) i A pak téhož tvaru.

Tím jsme se dodělali těchto výsledků.

Předně. Nabude-li některý z jmenovatelů D hodnoty 2, tu je A nutně tvaru $4n + 3$.

Za druhé. Je-li A *kmenné* číslo $4n + 3$, tu jest střední jmenovatel 2. Kdyby se nevyskytnul žádný střední jmenovatel, tu by se A = součtu dvou čtverců, nemohl by tedy býti A vytknutého tvaru.

Za třetí. Vyskytne-li se při *kmenném* čísle A střední jmenovatel, tu se musí z právě vytknutých důvodů $= 2$.

Za čtvrté. Při *kmenném* čísle $A = 4n + 1$ se tudíž nemůže vyskytnouti střední jmenovatel a tudíž se takové číslo rovná součtu dvou čtverců.

Za páté. Předpokládejme, že se nevyskytuje střední jmenovatel a buďtež $D_m = d_m$ oba stejné jmenovatele uprostřed periody. Máme pak

$$u^2 - Av^2 = \pm D_m,$$
$$u_0^2 - Av_0^2 = \mp D_m,$$
$$uv_0 - u_0 v = \pm 1.$$

Z těchto rovnic vychází, D_m nemůže býti číslem sudým, neboť by pak byla jak čísla u, v, tak u_0, v_0, lichá a tedy poslední rovnice nemožna. Dále musejí A a D_m býti čísla nesoudělná, neboť oběma společný dělitel byl by i dělitelem čtverců u^2 a u_0^2, jež nemohou míti společného dělitele.

Poněvadž zde máme $A - J_m^2 = D_m^2$, tedy nám podává naše transformace rozklad čísla A na dva čtverce a sice tak, *že* J_m *a* D_m *jsou nesoudělná a* J_m *číslem sudým.*

Za šesté. Jestliže střední jmenovatel D, jež se v případu $A = 4n + 3$ nutně vyskytnouti musí, se nerovná 2, tu vůči tomu, že je $A - \frac{\alpha^2 D^2}{4}$ dělitelno A vychází, že A má činitel D aneb $\frac{D}{2}$, dle toho je-li D lichým neb sudým číslem.

Za sedmé. Jestliže se vyskytne, předpokládajíce A tvaru $4n + 1$, střední jmenovatel D, tu musí A býti číslem složeným. Pak se D nemůže rovnati 2; je-li D liché, jest dělitelem čísla A, jinak jest $\frac{D}{2}$ dělitelem jeho.

Za osmé. Při kmenném čísle $A = 4n + 3$ jsme měli

$$u^2 - Av^2 = \pm 2$$

a není rozhodnuto, zda-li při určitém A může míti platnost oboje znamení $\pm$ aneb jen jedno, aneb zda-li snad má oboje znamení obecně místa.

Uvážíme-li, že liché čtverce u^2 a v^2 jsou čísla tvaru $8n + 1$, tu při $A = 8n + 3$ rovnice

$$u^2 = +2 + Av^2$$

nemůže míti místa. K číslům tohoto tvaru tedy patří jedině rovnice

$$u^2 = -2 + Av^2$$

Všem ostatním číslům obsaženým v tvaru $4n + 3$, t. j. tedy číslům $A = 8n + 7$ platí rovnice

$$u^2 = +2 + Av^2.$$

T. j. $+2$ jest kvadratickým zbytkem čísel $8n + 7$, a není kvadratickým zbytkem čísel $8n + 3$; o číslu -2 platí opáčné.

II.

Každé kmenné číslo p, jež dělí $m^2 + kn^2$, kde značí m a n čísla nesoudílná a k číslo nepřesahující 3, možno na týž tvar uvésti.

Důkaz. Mějmež

$$m^2 + kn^2 = \lambda p.$$

Můžeme předpokládati, že i m i n jsou menší než $\frac{p}{2}$ *), že tedy

$$\lambda < p.$$

Kdyby $\lambda > 1$, tu ukážeme, kterak lze stanoviti dvě nesoudělná čísla x, y taková, že

$$x^2 + ky^2 = \lambda' p, \text{ a zároveň } \lambda' < \lambda.$$

Vyviňme zlomek $\frac{m}{n}$ v řetězec a nazveme $\frac{\alpha}{\beta}$ předposlední přibližný zlomek jeho. Pak platí

$$m\beta - n\alpha = \pm 1.$$

Položme nyní

$$x = p\alpha - mt,$$
$$y = p\beta - nt,$$

kdež t značí libovolné celistvé číslo. Pak tedy

$$nx = my = \mp p.$$

Z této rovnice vychází, že jsou x a y buď čísla nesoudělná aneb že jsou násobky čísla p. Máme-li tedy při jistém $t = t'$, jemuž přisluší $x = x'$, $y = y'$ nerovnost

$$x'^2 + ky'^2 < \lambda p$$

tu musí x' a y' býti čísla nesoudělná. Avšak

$$x^2 + ky^2 = p^2(\alpha^2 + k\beta^2) + t^2(m^2 + kn^2) - 2pt(\alpha m + k\beta n)$$
$$= f(t).$$

Aneb po krátké transformaci

$$f(t) = k\frac{p^2}{m^2 + kn^2} + (t - \frac{\alpha m + k\beta n}{m^2 + kn^2} p)^2 (m^2 + kn^2).$$

Hodnota $f(t)$ nepřestává býti dělitelnou p a je zároveň minimem při

$$t_0 = \frac{\alpha m + k\beta n}{m^2 + kn^3} p;$$

neboť

$$f(t_0 \pm \delta) = f(t_0) + \delta^2 (m^2 + kn^2)$$

t. j. $f(t)$ roste s hodnotou δ. Značí-li tedy t' celistvé číslo hodnotě t_0 nejbližší, tedy nemůže $f(t')$ býti větší než $f(t_0 \pm \frac{1}{2})$.

*) Stačí poznamenati, že zbytky, jež vznikají dělením hodnot m a n číslem p, vyhovují obdobné rovnici; jich společné faktory jsouce obsaženy kvadraticky v λp musejí vcházeti svými čtverci do λ a lze je dělením odstraniti t. j. lze pokládati m a n za čísla nesoudělná.

Tudíž

$$x'^2 + ky'^2 \leqq \frac{k}{\lambda} p + \frac{\lambda}{4} p.$$

Avšak při $k = 1$, neb $k = 2$, máme předpokládajíce $\lambda > 1$:

$$\frac{4k + \lambda^2}{4\lambda} < \lambda \text{ tedy } x'^2 + ky'^2 < \lambda p.$$

Je-li $k = 3$, tu máme $\frac{12 + \lambda^2}{4\lambda} < \lambda$ jakmile $\lambda > 2$. Zbývající případ $\lambda = 2$, nemůže se však vyskytnouti; neboť pak by $m^2 + 3n^2$ bylo číslo sudé, tudíž m i n lichá čísla, a tedy by $m^2 + 3n^2$ nanejmíň $= 4p$.

O stanovení orthogonálných trajektorií kružnic v rovině.

Napsal

Eduard Weyr.

K úvahám, jež následují, byl jsem pobídnut prací p. *Catalana* „Sur les trajectoires orthogonales des sections circulaires d'un ellipsoïde“, obsaženou v Liouvilleově žurnalu, tom. XII. Vyvineme-li differencialní rovnici, na níž záleží řešení problému, cestou nejpřímější, tu se vyskytne tvar, jehož integrace by se nám as snadno nepodařila; p. spisovatel překonává tuto obtíž zaváděje vhodné nové proměnné.

Promítneme-li kruhové řezy trojosého ellipsoidu kolmo na rovinu rovnoběžnou s rovinami oněch řezů, tu obdržíme co průměty systém kružnic , které se jisté ellipsy dvakráte dotýkají. Orthogonalné trajektorie těchto kružnic jsou patrně průměty hledaných trajektorií na ellipsoidu. Řešený onen úkol jest tedy jen zvláštním případem stanovení orthogonálných traj ektorií kružnic, jichž středy jsou na přímce.

Tento obecnější problém rozřešíme kvadraturami; totéž ukážeme vzhledem k úkolu obecnějšímu, kdy jde o stanovení orthogonálných trajektorií kružnic, jež protínají pevnou kruž-