Karel Rychlík

O poslední větě Fermatově pro $n = 5$. [I.]

Časopis pro pěstování mathematiky a fysiky, Vol. 39 (1910), No. 2, 185--195

Persistent URL: http://dml.cz/dmlcz/121877

O poslední větě Fermatově pro $n = 5$.*)

Napsal Dr. K. Rychlík.

§ 1.

V následujícím podáme důkaz poslední věty Fermatovy pro $n = 5$ na základě theorie tělesa pátých kořenů z jednotky.

Abychom toto těleso mohli definovati, uvažujme rovnici

$$x^5 - 1 = 0. \qquad (1)$$

Rovnice tato rozpadá se v oboru čísel racionálných, neboť

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1).$$

Kořeny od 1 různé rovnice (1) vyhovují tedy této rovnici:

$$x^4 + x^3 + x^2 + x + 1 = 0. \qquad (2)$$

Řešení rovnice (2) provádí se postupným řešením dvou rovnic kvadratických.

Položíme-li

$$x + \frac{1}{x} = y, \qquad (3)$$

obdržíme pro y kvadratickou rovnici

$$y^2 + y - 1 = 0. \qquad (4)$$

O kořenech rovnice (2) lze dokázati:

Označíme-li ζ jeden z kořenů rovnice (2), budou ostatní $\zeta^2, \zeta^3, \zeta^4$.

Kořeny rovnice té nejsou ani racionálné, ani nevyhovují rovnici stupně druhého neb třetího s racionálnými koefficienty: rovnice (2) jest irreducibilní.

*) Článek tento jest pokračováním článku: »O poslední větě Fermatově pro $n = 4$ a pro $n = 3$« minulého čísla »Přílohy« a předpokládá znalost § 1., částečně i § 2. a 4.

Absolutní hodnota (modul) kořenů rovnice (2) jest rovna 1. Kořeny ζ a ζ^4 resp. ζ^2 a ζ^3 jsou čísla komplexní sdružená. Z rovnic (1) a (2) plynou ihned vztahy:

$$\zeta^5 = 1, \tag{5}$$

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0 \tag{6}$$

a rovněž

$$x^5 - 1 = (x - 1)(x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4) \tag{7}$$

$$x^4 + x^3 + x^2 + x + 1 = (x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4). \tag{8}$$

Čísla tvaru

$$\alpha = a + b\zeta + c\zeta^2 + d\zeta^3, \tag{9}$$

kdež a, b, c, d jsou čísla racionálná, tvoří těleso $R(\zeta)$, zvané tělesem pátých kořenů z jednotky.

Že součet a rozdíl dvou čísel tvaru (9) jest téhož tvaru, jest přímo patrno; o součinu to plyne z té okolnosti, že každý polynom v ζ s racionálnými koefficienty lze na základě vztahu (6) převésti na polynom stupně třetího.

Abychom to dokázali i o podílu, vysvětlíme nejprve pojem čísel sdružených a pojem normy.

Klademe-li v čísle

$$\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$$

místo ζ ostatní kořeny rovnice (2), totiž ζ^2, ζ^3, ζ^4, obdržíme čísla

$$\begin{aligned} \alpha' &= a + b\zeta^2 + c\zeta^4 + d\zeta, \\ \alpha'' &= a + b\zeta^3 + c\zeta + d\zeta^4, \\ \alpha''' &= a + b\zeta^4 + c\zeta^3 + d\zeta^2, \end{aligned}$$

která jsou s číslem α sdružená (konjugovaná). Součin těchto čtyř sdružených spolu čísel bude jisté číslo racionálné a to nazývá se normou čísla α

$$n(\alpha) = \alpha\alpha'\alpha''\alpha'''.$$

Poněvadž ζ a ζ^4 resp. ζ^2 a ζ^3 jsou čísla komplexní sdružená, budou i α a α''' resp. α' a α'' čísla komplexní sdružená.

Násobme spolu nejprve $\alpha\alpha'''$. Dostaneme

$$\begin{aligned} \alpha\alpha''' = a^2 + b^2 + c^2 + d^2 &+ (\zeta + \zeta^4)(ab + bc + cd) \\ &+ (\zeta^2 + \zeta^3)(ac + bd + da). \end{aligned}$$

Užijme relace

$$1 = -(\zeta + \zeta^4) - (\zeta^2 + \zeta^3),$$

plynoucí z (6).

Pak bude

$$\alpha\alpha''' = -(\zeta + \zeta^4)(a^2 + b^2 + c^2 + d^2 - ab - bc - cd) \\ -(\zeta^2 + \zeta^3)(a^2 + b^2 + c^2 + d^2 - ac - bd - da)$$

neboli

$$\alpha\alpha''' = -(\zeta + \zeta^4)p - (\zeta^2 + \zeta^3)q$$

označíme-li výrazy v závorkách resp. p a q.

Pro výrazy ty lze psáti

$$2p = (a - b)^2 + (b - c)^2 + (c - d)^2 + a^2 + d^2$$
$$2q = (a - c)^2 + (b - d)^2 + (d - a)^2 + b^2 + c^2,$$

tedy

$$2(p + q) = 5(a^2 + b^2 + c^2 + d^2) - (a + b + c + d)^2. \quad (10)$$

Podobně nalezneme pro součin

$$\alpha'\alpha'' = -(\zeta + \zeta^4)q - (\zeta^2 + \zeta^3)q$$

a konečně

$$n(\alpha) = 3pq - p^2 - q^2 = 5pq - (p + q)^2$$
$$= \left(\frac{p+q}{2}\right)^2 - 5\left(\frac{p-q}{2}\right)^2. \quad (11)$$

$\alpha\alpha'''$ a $\alpha'\alpha''$ jako součiny komplexně sdružených čísel jsou čísla kladná. Bude tedy i $n(\alpha)$ racionálné, kladné číslo.

Z posledního výrazu v (11) pro $n(\alpha)$ plyne

$$n(\alpha) \leqq \left(\frac{p+q}{2}\right)^2$$

a ježto dle (10)

$$2(p + q) \leqq 5(a^2 + b^2 + c^2 + d^2),$$

bude

$$n(\alpha) \leqq \frac{25}{16}(a^2 + b^2 + c^2 + d^2)^2. \quad (12)$$

O normě platí vzorce snadno dokázatelné

$$n(\alpha\beta) = n(\alpha)\, n(\beta) \quad (13)$$

$$n\left(\frac{\alpha}{\beta}\right) = \frac{n(\alpha)}{n(\beta)}. \quad (14)$$

Abychom podíl dvou čísel z tělesa $R(\zeta)$ uvedli na tvar (9), násobme ve zlomku

$$\frac{\beta}{\alpha}$$

čitatele i jmenovatele čísly sdruženými s α, totiž α', α'', α'''.

Tak dostaneme

$$\frac{\beta}{\alpha} = \frac{\beta\alpha'\alpha''\alpha'''}{n(\alpha)}$$

a toto číslo lze snadno převésti na tvar (9), uvážíme-li že $n(\alpha)$ jest číslo racionální.

Číslo z tělesa $R(\zeta)$, psané ve tvaru (9), může býti rovno nulle jen když $a = b = c = d = 0$. To plyne z irreducibility rovnice (2).

Jsou-li při čísle

$$\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$$

a, b, c, d racionálná čísla celistvá, nazývá se α celým číslem tělesa $R(\zeta)$. Tato celá čísla reprodukují se sčítáním, odčítáním a násobením.

Na základě vztahu (6) lze psáti čísla z tělesa $R(\zeta)$ též ve tvaru

$$\alpha = A\zeta + B\zeta^2 + C\zeta^3 + D\zeta^4, \tag{15}$$

kdež A, B, C, D jsou čísla racionálná. Číslo psané v tomto tvaru může býti $= 0$, jen když $A = B = C = D = 0$ a bude celé, budou-li A, B, C, D racionálná čísla celá.

Kořeny rovnice kvadratické (4) budou

$$\zeta + \frac{1}{\zeta} = \zeta + \zeta^4$$

$$\text{a} \quad \zeta^2 + \frac{1}{\zeta^2} = \zeta^2 + \zeta^3 = -1 - \zeta - \zeta^4.$$

Čísla tvaru $A + B(\zeta + \zeta^4)$ tvoří těleso kvadratické, které označíme $R(\zeta + \zeta^4)$. Poněvadž číslo $\zeta + \zeta^4$ jakožto součet dvou komplexních čísel sdružených jest číslo reálné, budou všechna čísla tělesa $R(\zeta + \zeta^4)$ reálná.

Naopak lze tvrditi:

Každé realné číslo z tělesa $R(\zeta)$ náleží tělesu $R(\zeta + \zeta^4)$.

Pišme $\alpha = A\zeta + B\zeta^2 + C\zeta^3 + D\zeta^4$. Je-li α číslo reálné, bude rovno číslu komplexně sdruženému

$$\bar{\alpha} = A\zeta^4 + B\zeta^3 + C\zeta^2 + D\zeta,$$

z čehož plyne

$$A = D, \quad B = C,$$

tak že

$$\alpha = A(\zeta + \zeta^4) + B(\zeta^2 + \zeta^3) = - B + (A - B)(\zeta + \zeta^4),$$

z čehož jest patrno, což bylo tvrzeno.

ζ jest kořenem rovnice kvadratické

$$x + \frac{1}{x} = \zeta + \zeta^4,$$

neboli

$$x^2 - (\zeta + \zeta^4)x + 1 = 0,$$

jejíž koefficienty jsou čísla z tělesa $R(\zeta + \zeta^4)$.

Těleso $R(\zeta)$ jest relativně kvadratické vzhledem k tělesu $R(\zeta + \zeta^4)$.

Zaveďme pojem dělitelnosti pro celá čísla z tělesa $R(\zeta)$. To provedeme jako při číslech racionálných.

Celé číslo α jest dělitelno celým číslem δ, je-li $\frac{\alpha}{\delta}$ opět číslo celé.

Je-li číslo α celé, jsou i čísla s ním sdružená celá. Z toho plyne, že norma $n(\alpha)$ jest číslem α dělitelná.

Ze vzorce (13) plyne ihned:

Je-li celé číslo α dělitelno celým číslem β, jest $n(\alpha)$ dělitelno $n(\beta)$.

Jednotkami budeme nazývati čísla celá ε, která jsou děliteli čísla 1. Budou tedy jednotky obsaženy ve všech číslech celých. Poněvadž jednotka ε jest obsažena v 1, bude $n(\varepsilon)$ obsaženo v $n(1) = 1$, z čehož plyne, uvážíme-li, že norma jest celým číslem kladným, že $n(\varepsilon) = 1$.

Ale i opak platí: je-li pro celé číslo ε $n(\varepsilon) = 1$, jest ε jednotkou. Převratná hodnota jednotky jest opět jednotkou. Je-li číslo ε i jeho převratná hodnota $\frac{1}{\varepsilon}$ číslem celým, jest číslo to jednotkou.

Jest přímo patrno, že v tělese našem jsou především jednotkami ± 1, $\pm \zeta^k$, $k = 1, 2, 3, 4$. Oproti tělesům dříve uvažovaným shledáme však ten rozdíl, že v nich byl počet jednotek konečný, kdežto, jak později uvidíme, v tělese pátých kořenů z jednotky jest jednotek nekonečně mnoho.

Čísla, jichž podíl jest jednotkou, nazývají se associovanými. Poněvadž jest nekonečně mnoho jednotek, bude také nekonečně mnoho spolu associovaných čísel.

Celé číslo π z tělesa pátých kořenů z jednotky nazývá se prvočíslem, má-li pouze dělitele 1, π a čísla s těmito čísly associovaná.

Také v tělese pátých kořenů z jednotky platí věta o jednoznačné rozložitelnosti v prvočinitele. Důkaz provedeme opět pomocí Euklidova algorithmu. Dokážeme si nejprve větu:

Jsou-li α, β dvě libovolná čísla z tělesa pátých kořenů z jednotky, lze nalézti v tělese tom celé číslo $\varkappa$ té vlastnosti, že

$$n(\alpha - \beta\varkappa) < n(\beta). \tag{16}$$

Aby tomu tak bylo, bude musiti býti

$$\frac{n(\alpha - \beta\varkappa)}{n(\beta)} < 1,$$

neboli

$$n\left(\frac{\alpha}{\beta} - \varkappa\right) < 1.$$

Proto dokážeme:

Je-li μ libovolné číslo z tělesa pátých kořenů z jednotky, lze nalézti v tělese tom celé číslo $\varkappa$ té vlastnosti, že

$$n(\mu - \varkappa) < 1. \tag{17}$$

Znázorněme čísla tělesa $R(\zeta)$ ve tvaru

$$\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4, \tag{18}$$

kdež a_0, a_1, a_2, a_3, a_4 jsou čísla racionálná. Znázornění toto ovšem není jednoznačné. Vzhledem k relaci (6) lze k číslům a přičísti ke všem totéž číslo racionálné. Zvolme si tedy čísla a tak, aby

$$a_0 + a_1 + a_2 + a_3 + a_4 = 0. \tag{19}$$

Není-li tomu již tak při čísle α, docílíme toho tím, že přičteme ke všem číslům a výraz

$$-\frac{a_0 + a_1 + a_2 + a_3 + a_4}{5}.$$

Ptejme se, jaké musí býti číslo a, aby číslo α ve tvaru (18) bylo číslem celým tělesa $R(\zeta)$. Pišme

$$\alpha = (a_0 - a_4) + (a_1 - a_4)\zeta + (a_2 - a_4)\zeta^2 + (a_3 - a_1)\zeta^3.$$

I vidíme, že musí býti

$$a_0 - a_4,\ a_1 - a_4,\ a_2 - a_4,\ a_3 - a_4$$

čísla celá.

Utvoříme-li součet těchto čísel, shledáme vzhledem k relaci (19), že musí býti $5a_4$ celé číslo A_4. Pak budou nutně také $5a_0 = A_0$, $5a_1 = A_1$, $5a_2 = A_2$, $5a_3 = A_3$ čísla celá a dále bude nutno, aby

$$A_0 \equiv A_1 \equiv A_2 \equiv A_3 \equiv A_4 \quad (mod\ 5).$$

Jest tedy číslo

$$\frac{A_0 + A_1\zeta + A_2\zeta^2 + A_3\zeta^3 + A_4\zeta^4}{5}, \tag{20}$$

kdež

$$A_0 + A_1 + A_2 + A_3 + A_4 = 0 \tag{21}$$

číslem celým, platí-li

$$A_0 \equiv A_1 \equiv A_2 \equiv A_3 \equiv A_4\ (mod\ 5).$$

Položme

$$\mu = \frac{m_0 + m_1\zeta + m_2\zeta^2 + m_3\zeta^3 + m_4\zeta^4}{5}, \tag{22}$$

kdež m jsou racionálná čísla. Kladme

$$m_k = A_k + r_k,\quad k = 0, 1, 2, 3, 4, \tag{23}$$

kdež A_k jsou celá čísla a r_k pravé zlomky kladné, pro něž tedy

$$0 \leqq r_k < 1. \tag{24}$$

Poněvadž jest

$$m_0 + m_1 + m_2 + m_3 + m_4 = 0 \tag{25}$$

a A_k jsou celá čísla, bude

$$s = r_0 + r_1 + r_2 + r_3 + r_4 \tag{26}$$

celé číslo a vzhledem k nerovnostem (24) rovno buď 0, neb 1, 2, 3, 4. Předpokládejme nejprve, že

$$s = 0.$$

I musí býti vzhledem k (24)

$$r_0 = r_1 = r_2 = r_3 = r_4 = 0.$$

Bude tedy

$$\mu = \frac{A_0 + A_1\zeta + A_2\zeta^2 + A_3\zeta^3 + A_4\zeta^4}{5},$$

$$\mu = \frac{A_0 - A_4 + (A_1 - A_4)\zeta + (A_2 - A_4)\zeta^2 + (A_3 - A_4)\zeta^3}{5}.$$

Kladme

$$\frac{A_0 - A_4}{5} = \bar{a} + a, \quad \frac{A_1 - A_4}{5} = \bar{b} + b, \quad \frac{A_2 - A_4}{5} = \bar{c} + c,$$

$$\frac{A_3 - A_4}{5} = \bar{d} + d,$$

kdež $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$ jsou celá čísla a a, b, c, d zlomky o absolutní hodnotě $\leqq \frac{1}{2}$, tedy rovné 0, $\pm \frac{1}{5}$, $\pm \frac{2}{5}$. Bude tudíž

$$|a|, |b|, |c|, |d| \leqq \frac{2}{5}. \tag{27}$$

Položme

$$\varkappa = \bar{a} + \bar{b}\zeta + \bar{c}\zeta^2 + \bar{d}\zeta^3.$$

I bude

$$n(\mu - \varkappa) = n(a + b\zeta + c\zeta^2 + d\zeta^3)$$

a dle vzorce (12)

$$n(\mu - \varkappa) \leqq \frac{25}{16}(a^2 + b^2 + c^2 + d^2)^2,$$

tedy na základě (27)

$$n(\mu - \varkappa) \leqq \frac{25}{16}\left(\left(\frac{2}{5}\right)^2 + \left(\frac{2}{5}\right)^2 + \left(\frac{2}{5}\right)^2 + \left(\frac{2}{5}\right)^2\right)^2 \leqq \frac{16}{25}$$

a tedy skutečně

$$n(\mu - \varkappa) < 1.$$

Obraťme se nyní k případu

$$s = 1, 2, 3, 4.$$

Poněvadž

$$m_0 + m_1 + m_2 + m_3 + m_4 = 0,$$

bude

$$A_0 + A_1 + A_2 + A_3 + A_4 + s = 0 \tag{28}$$

a tedy

$$(A_0 - A_4) + (A_1 - A_4) + (A_2 - A_4) + (A_3 - A_4) + s \equiv 0 \pmod 5. \tag{29}$$

Označme

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3$$

čísla o nejmenší absolutní hodnotě, s nimiž jsou resp.

$$A_0 - A_4, A_1 - A_4, A_2 - A_4, A_3 - A_4$$

kongruentní dle modulu 5. I bude

$$|\lambda_k| \leqq 2, \qquad k = 0, 1, 2, 3. \tag{30}$$

Tu mohou nastati dva případy: Buď jest jedno z čísel $\lambda_k = 0$, neb jsou dvě z nich sobě rovna. (Kdyby byla vesměs různá, musilo by býti

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3 = -1, 1, -2, 2;$$

pak by bylo

$$\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 0,$$

tedy na základě (29)

$$s \equiv 0 \qquad (mod\ 5),$$

což jest proti předpokladu.)

Předpokládejme tedy nejprve, že jest jedno z čísel

$$\lambda_0, \lambda_1, \lambda_2, \lambda_3 = 0,$$

na př.

$$\lambda_2 = 0.$$

Kladme

$$\frac{m_1 - m_4}{5} = \bar{a} + a, \quad \frac{m_1 - m_4}{5} = \bar{b} + b, \quad \frac{m_2 - m_4}{5} = \bar{c} + c,$$

$$\frac{m_3 - m_4}{5} = \bar{d} + d,$$

kdež $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ jsou celá čísla a a, b, c, d zlomky absolutní hodnotou $\leqq \frac{1}{2}$.

Položíme-li

$$\varkappa = \bar{a} + \bar{b}\zeta + \bar{c}\zeta^2 + \bar{d}\zeta^3,$$

bude

$$\mu - \varkappa = a + b\zeta + c\zeta^2 + d\zeta^3,$$

při čemž

$$|a| \leqq \frac{1}{2}, \quad |b| \leqq \frac{1}{2}, \quad |c| \leqq \frac{1}{2}. \tag{31}$$

Avšak
$$\bar{c}+c=\frac{m_2-m_4}{5}=\frac{A_2-A_4}{5}+\frac{r_2-r_4}{5}$$
a poněvadž na základě $\lambda_2=0$ jest $\frac{A_2-A_4}{5}$ celé číslo, a na základě nerovností, plynoucích z (24)
$$0\leqq r_2<1,\quad 0\leqq r_4<1,$$
platí
$$\left|\frac{r_2-r_4}{5}\right|<\frac{1}{5},$$
bude
$$\bar{c}=\frac{A_2-A_4}{5}$$
$$c=\frac{r_2-r_4}{5}$$
a tedy
$$|c|<\frac{1}{5}. \tag{32}$$
Bude tudíž
$$n(\mu-\varkappa)=n(a+b\zeta+c\zeta^2+d\zeta^3)$$
a dle vzorce (12)
$$n(\mu-\varkappa)\leqq\frac{25}{16}(a^2+b^2+c^2+d^2)^2$$
a na základě nerovností (31) a (32)
$$n(\mu-\varkappa)\leqq\frac{25}{16}\left(\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{5}\right)^2+\left(\frac{1}{2}\right)^2\right)^2\leqq\left(\frac{79}{80}\right)^2$$
a tedy skutečně
$$n(\mu-\varkappa)<1.$$
Případ, kdy dvě z čísel $\lambda_0, \lambda_1, \lambda_2, \lambda_3$ jsou si rovna, na př.
$$\lambda_2=\lambda_3,$$
převedeme na předešlý tím, že násobíme μ jistou mocností ζ, zde přímo ζ.

Bude totiž
$$\mu\zeta=\frac{m_4+m_0\zeta+m_1\zeta^2+m_2\zeta^3+m_3\zeta^4}{5}$$
$$\mu\zeta=\frac{(m_4-m_3)+(m_0-m_3)\zeta+(m_1-m_3)\zeta^2+(m_2-m_3)\zeta^3}{5}$$
$$\frac{m_2-m_3}{5}=\frac{A_2+r_2-A_3-r_3}{5},$$

při čemž

$$A_2 - A_3 = (A_2 - A_4) - (A_3 - A_4),$$

tedy

$$A_2 - A_3 \equiv \lambda_2 - \lambda_3 \equiv 0 \quad (mod\ 5).$$

Lze tedy nalézti celé číslo $\varkappa'$ takové, že

$$n(\zeta\mu - \varkappa') < 1$$

a ježto

$$n(\zeta) = 1,$$

bude, klademe-li

$$\varkappa = \varkappa'\zeta^4,$$

$$n(\mu - \varkappa) < 1.$$

Z platnosti Euklidova algorithmu plyne věta:

Každé celé číslo z tělesa pátých kořenů z jednotky lze rozložiti „podstatně“ jediným způsobem v součin prvočinitelů. Slovo podstatně značí, že nepokládáme za různé rozklady, při nichž prvočinitelé jsou zaměněni prvočiniteli associovanými.

(Dokončení.)

Algebraická analyse dvojstředového čtyřúhelníku.

Napsal **Ant. Jeřábek.**

Úloha I. *Sestrojiti dvojstředový čtyřúhelník, jsou-li dány opsaná kružnice K a bod P, jímž probíhají úhlopříčky.*

Rozbor. Budiž O střed opsané kružnice K, jejíž poloměr $= r$, a $OP = l$. (obr. 1.)

Protože dvojstředový čtyřúhelník teprv třemi podmínkami dostatečně jest určen, jest naše úloha neurčitá; i lze očekávati nekonečně mnoho takových čtyřúhelníků, mezi nimiž se vyskytnou i *deltoid s pravými úhly* i *rovnoramenný lichoběžník.*

Snadno nahlédneme, že v obou těch případech *střed O' vepsané kružnice K'* leží na OP. Jest otázkou, zdali bude tak ve všech případech. —

Označme písmenem P zatím průsečík *jedné* úhlopříčky ku př. úhlopříčky BD s přímkou OO' a kladme $OO' = d$ a *poloměr kružnice $K' = \varrho$.* Vrchol A hledaného čtyřúhelníku bude na přímce AO', jež jsouc prodloužena, rozpoluje oblouk BD v bodě