Časopis pro pěstování mathematiky a fysiky

Karel Rychlík

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

Časopis pro pěstování mathematiky a fysiky, Vol. 39 (1910), No. 3, 305--317

Persistent URL: http://dml.cz/dmlcz/122987

O poslední větě Fermatově pro $n = 5$.

Napsal Dr. **K. Rychlík.**

(Dokončení.)

V následujícím budeme potřebovati rozklad přirozeného prvočísla 5 v tělese pátých kořenů z jednotky.

Ze vzorce (8) plyne

$$5 = (1 - \zeta)(1 - \zeta^2)(1 - \zeta^3)(1 - \zeta^4). \tag{33}$$

Poněvadž činitelé na pravé straně jsou spolu sdružení, jest

$$5 = n(1 - \zeta) = n(1 - \zeta^2) = n(1 - \zeta^3) = n(1 - \zeta^4). \tag{34}$$

Činitelé ti jsou však také associovaní: podíl libovolných dvou z nich jest jednotkou. To dokážeme tím, že podíl takový i jeho převratná hodnota jest celé číslo.

Uvažujme na př.

$$\frac{1 - \zeta^3}{1 - \zeta^4} = \frac{1 - \zeta^8}{1 - \zeta^4} = 1 + \zeta^4,$$

$$\frac{1 - \zeta^4}{1 - \zeta^3} = \frac{1 - \zeta^9}{1 - \zeta^3} = 1 + \zeta^3 + \zeta^6 = 1 + \zeta + \zeta^3.$$

Jest tedy na př.

$$5 = \varepsilon(1 - \zeta)^4, \tag{35}$$

kdež ε jest jednotka.

Dokážeme snadno, že $1 - \zeta$ a tedy i

$$1 - \zeta^2, \quad 1 - \zeta^3, \quad 1 - \zeta^4$$

jsou prvočísla.

Předpokládejme, že by bylo

$$1 - \zeta = \alpha\beta,$$

kdež α, β jsou celá čísla.

I musilo by býti

$$n(1-\xi) = n(\alpha)\ n(\beta)$$

a tedy dle (34)

$$5 = n(\alpha)\ n(\beta).$$

Bylo by tedy buď $n(\alpha)$ neb $n(\beta) = 1$ a pak by bylo β, resp. α associováno s $1-\xi$.

Kongruenci definujeme pro celá čísla z tělesa pátých kořenů z jednotky tak jako při číslech racionálných. Modul lze zaměniti kterýmkoliv z čísel s ním associovaných.

Obraťme se nyní k určení jednotek v tělese pátých kořenů z jednotky.

Dokažme si nejprve věty:

Podíl dvou komplexně sdružených jednotek z tělesa pátých kořenů z jednotky rovná se jisté mocnině ξ.

Každá jednotka ε z tělesa $R(\zeta)$ dá se vyjádřiti ve tvaru

$$\varepsilon = \zeta^h \eta,$$

kdež h jest racionálné celé číslo a η reálná jednotka tělesa.

Značme $\bar{\alpha}$ číslo komplexně sdružené s α.

Podíl jednotek $\frac{\bar{\varepsilon}}{\varepsilon}$ jest opět jednotka a lze psáti

$$\frac{\bar{\varepsilon}}{\varepsilon} = \eta = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4, \qquad (36)$$

kdež a jsou racionálná čísla celá. Čísla ta nejsou vzhledem k relaci (6) určena jednoznačně, nýbrž lze přičísti ke všem totéž číslo celé.

Pak bude

$$\eta\bar{\eta} = \frac{\varepsilon}{\bar{\varepsilon}} \cdot \frac{\bar{\varepsilon}}{\varepsilon} = 1.$$

Provedeme-li násobení

$$\eta\bar{\eta} = (a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4)$$
$$(a_0 + a_1\zeta^4 + a_2\zeta^3 + a_3\zeta^2 + a_4\zeta),$$

dostaneme

$$\eta\bar{\eta} = A_0 + A_1\zeta + A_2\zeta^2 + A_3\zeta^3 + A_4\zeta^4, \qquad (37)$$

kdež

$$A_0 = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2,$$
$$A_1 = a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_0,$$
$$A_2 = a_0a_2 + a_1a_3 + a_2a_4 + a_3a_0 + a_4a_1,$$
$$A_3 = a_0a_3 + a_1a_4 + a_2a_0 + a_3a_1 + a_4a_2,$$
$$A_4 = a_0a_4 + a_1a_0 + a_2a_1 + a_3a_2 + a_4a_3.$$

Sečtením obdržíme

$$A_0 + A_1 + A_2 + A_3 + A_4 = (a_0 + a_1 + a_2 + a_3 + a_4)^2. \tag{38}$$

Z rovnice

$$\eta\bar{\eta} = A_0 + A_1\xi + A_2\xi^2 + A_3\xi^3 + A_4\xi^4 = 1$$

plyne

$$A_0 - A_4 - 1 + (A_1 - A_4)\,\xi + (A_2 - A_4)\,\xi^2 + (A_3 - A_1)\,\xi^3 = 0,$$

tedy

$$A_0 - A_4 - 1 = A_1 - A_4 = A_2 - A_4 = A_3 - A_4 = 0,$$

a z toho

$$A_0 - 1 = A_1 = A_2 = A_3 = A_4. \tag{39}$$

Dosadíme-li do (38), dostaneme

$$1 + 5A_1 = (a_0 + a_1 + a_2 + a_3 + a_4)^2, \tag{40}$$

kteroužto rovnici lze psáti ve tvaru kongruence

$$(a_0 + a_1 + a_2 + a_3 + a_4)^2 \equiv 1 \pmod 5.$$

Z ní plyne, že musí býti

$$a_0 + a_1 + a_2 + a_3 + a_4 \equiv \pm 1 \pmod 5,$$

neboli

$$a_0 + a_1 + a_2 + a_3 + a_4 = \pm 1 + 5k,$$

kdež k jest celé číslo.

Čísla a, jak bylo řečeno, nejsou jednoznačně určena, nýbrž lze k nim ke všem přičísti totéž číslo celé. Přičtěme k nim ke všem $-k$, čímž docílíme toho, že bude

$$a_0 + a_1 + a_2 + a_3 + a_4 = \pm 1,$$

a obdržíme tedy z rovnice (40)

$$A_1 = 0,$$

a z rovnic (39)

$$A_2 = A_3 = A_4 = 0, \quad A_0 = 1,$$

tudíž

$$A_0 = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1.$$

Avšak této rovnici nelze jinak vyhověti racionálnými celými čísly než když položíme jedno z čísel $a = \pm 1$, ostatní $= 0$. Pak bude

$$\eta = \pm \xi^k,$$

a tedy

$$\frac{\varepsilon}{\bar{\varepsilon}} = \pm \xi^k. \tag{41}$$

Ukážeme, že může platiti jen znamení $+$.

Je-li v (41) k číslo sudé, klaďme $k = 2h$, je-li pak k číslo liché, bude $k + 5$ číslo sudé; i klaďme $k + 5 = 2h$. Při tom bude

$$\zeta^k = \xi^{k+5} = \xi^{2h}.$$

Klaďme dále

$$\varepsilon = \zeta^h \eta, \tag{42}$$

tudíž

$$\bar{\varepsilon} = \zeta^{-h} \bar{\eta}.$$

Z rovnice (41) obdržíme pak

$$\frac{\eta}{\bar{\eta}} = \pm 1.$$

Pišme

$$\eta = A\xi + B\xi^2 + C\xi^3 + D\xi^4,$$

tedy

$$\bar{\eta} = A\xi^4 + B\xi^3 + C\xi^2 + D\xi.$$

Kdyby bylo

$$\frac{\eta}{\bar{\eta}} = -1,$$

tedy

$$\eta + \bar{\eta} = 0,$$

neboli

$$(A + D)\xi + (B + C)\xi^2 + (B + C)\xi^3 + (A + D)\xi^4 = 0,$$

musilo by býti

$$A + D = 0, \quad B + C = 0.$$

Pak by bylo

$$\eta = A\xi(1 - \xi^3) + B\xi^2(1 - \xi).$$

Z toho by plynulo, že η jest dělitelno prvočíslem $1 - \xi$, což jest nemožno vzhledem k předpokladu, že η jest jednotkou. Jest tedy nutně

$$\frac{\eta}{\bar{\eta}} = 1,$$

tudíž η rovno hodnotě komplexní sdružené $\bar{\eta}$, z čehož plyne, že η jest číslo reálné.

Máme tudíž na základě (42)

$$\varepsilon = \xi^h \eta,$$

a tedy

$$\frac{\varepsilon}{\bar{\varepsilon}} = \xi^{2h}, \tag{43}$$

čímž obě věty uvedené svrchu dokázány.

Hledejme reálné jednotky z tělesa $R(\xi)$. Pišme je ve tvaru

$$\eta = A + B(\xi + \xi^4). \tag{44}$$

Pak bude pro hodnoty sdružené

$$\eta = \eta''', \qquad \eta' = \eta'',$$

tedy

$$n(\eta) = (\eta\eta')^2 = 1,$$

z čehož

$$\eta\eta' = \pm 1.$$

$\eta\eta'$ jest součin sdružených spolu hodnot v tělese $R(\xi + \xi^4)$, jest to tedy norma v tomto kvadratickém tělese. Označme ji $N(\eta)$. I bude

$$N(\eta) = \eta\eta' = \pm 1, \tag{45}$$

η bude jednotkou v tělese $R(\xi + \xi^4)$.

Rovnici (45) lze psáti, užijeme-li znázornění daného v (44)

$$A^2 - AB - B^2 = \pm 1. \tag{46}$$

Násobíme-li rovnici (46) čtyřmi, shledáme, že ji můžeme psáti ve tvaru

$$(2A - B)^2 - 5B^2 = \pm 4 \tag{47}$$

a klademe-li

$$x = 2A - B, \qquad y = B, \tag{48}$$

$$x^2 - 5y^2 = \pm 4, \tag{49}$$

což jest tak zvaná rovnice Pellova.

Ať jsou x, y jakákoliv celá čísla vyhovující rovnici (49), budou také A, B čísla celá. O $B = y$ jest to přímo patrné; z rovnice (49) pak plyne, že, je-li x sudé, tedy jest též y sudé a je-li x liché, jest y také liché; proto $A = \frac{x+y}{2}$ jest číslo celé. Z toho plyne, že každému řešení rovnice (49) v celých číslech odpovídá jistá jednotka tělesa $R(\zeta + \zeta^4)$.

Rovnice (49) má samozřejmé řešení $x = \pm 2$, $y = 0$. Tomu odpovídají jednotky ± 1.

Je-li η libovolná jednotka z $R(\zeta + \zeta^4)$, jest $\pm \frac{1}{\eta}$ jednotka sdružená s η v tělese $R(\zeta + \zeta^4)$. Z jednotek různých od ± 1 náležejí vždy 4 dohromady.

$$\pm \eta, \pm \frac{1}{\eta}.$$

Z těchto jednotek jest jedna positivní a > 1. Tu dostaneme pro x a y kladné; druhá jednotka jest positivní a < 1, ostatní dvě jsou záporné. Je-li x_0, y_0 nejmenší positivní řešení rovnice Pellovy (49) jest

$$\eta_0 = \frac{x_0 + y_0\sqrt{5}}{5}$$

nejmenší z kladných jednotek > 1. Můžeme dokázati, že ve tvaru $\pm \eta_0^n$, kdež n jest celé číslo, obsaženy jsou všechny jednotky. Stačí ukázati, že výraz η_0^n pro n positivní poskytuje všechny positivní jednotky > 1. To lze však snadno provésti, je-li η_1 jedna z takových jednotek, bude ležeti mezi dvěma po sobě jdoucími mocninami η_0, ježto η_0^n roste s mocnitelem n do nekonečna; bude pak

$$\eta_0^n \leqq \eta_1 < \eta^{n+1},$$

tedy

$$1 \leqq \eta_1 \eta_0^{-n} < \eta.$$

Ježto $\eta_1 \eta_0^{-n}$ jest rovněž jednotkou, jest, neplatí-li znamení rovnosti, $\eta_1 \eta_0^{-n} > 1$ a $< \eta$, což jest proti předpokladu, že η jest nejmenší kladná jednotka > 1. Musí tedy býti $\eta_1 = \eta_0^n$, jak bylo dokázati.

Zkoušením nalezneme, že nejmenší positivní řešení rovnice Pellovy (49) jest

$$x_0 = 1, \qquad y_0 = 1.$$

Tomu bude odpovídati

$$A = 1, \qquad B = 1,$$

tak že

$$\eta_0 = 1 + \xi + \xi^4 = -(\xi^2 + \xi^3).$$

Všechny jednotky tělesa $R(\xi + \xi^4)$ *budou zahrnuty ve vzorci*

$$\pm (\xi^2 + \xi^3)^n,$$

kdež n jest racionálné celé číslo, a všechny jednotky tělesa $R(\xi)$ *ve vzorci*

$$\pm \xi^k (\xi^2 + \xi^3)^n,$$

kdež k, n jsou racionálná celá čísla.

Dokážeme si ještě tuto důležitou větu o jednotkách.

Je-li v tělese pátých kořenů z jednotky jednotka ε *kongruentní s celým číslem racionálným dle modulu 5, jest* ε *pátou mocninou jiné jednotky tohoto tělesa.*

Vyjádřeme jednotku ε ve tvaru

$$\varepsilon = \pm \xi^k (\xi^2 + \xi^3)^n, \tag{50}$$

kdež k a n jsou racionálná, celá čísla. Je-li

$$\varepsilon \equiv c \pmod 5, \tag{51}$$

kdež c jest racionálné celé číslo (musí býti $c \equiv \pm 1$ neb ± 2 $(mod\ 5)$), bude též pro hodnotu $\bar{\varepsilon}$ komplexně sdruženou s ε platiti kongruence

$$\bar{\varepsilon} = \pm \xi^{-k} (\xi^2 + \xi^3)^n \equiv c \pmod 5. \tag{52}$$

Dělením kongruencí (51) a (52) obdržíme

$$\frac{\varepsilon}{\bar{\varepsilon}} = \xi^{2k} \equiv 1 \pmod 5$$

neboli

$$\xi^{2k} - 1 \equiv 0 \pmod 5.$$

Není-li $k \equiv 0$ $(mod\ 5)$, jest $\xi^{2k} - 1$ associováno s prvočíslem $\lambda = 1 - \xi$, kdežto 5 jest associováno s λ^4. Musí tedy býti $k \equiv 0$ $(mod\ 5)$, $\xi^k = 1$. Pak bude

$$\varepsilon = \pm (\xi^2 + \xi^3)^n. \tag{53}$$

Předpokládejme nejprve n kladné. Pak lze psáti

$$\varepsilon = \pm (2 + (\xi - \xi^4)^2)^n, \tag{54}$$

tak že bude, rozvineme-li dle binomické poučky a neuvažujeme již členy dělitelné λ^4 a vyššími mocninami λ:

$$\varepsilon \equiv c \equiv \pm (2^n + n\,2^{n-1}(\zeta - \zeta^4)^2) \pmod{\lambda^4}. \qquad (55)$$

I bude také

$$c \equiv \pm 2^n, \mod \lambda^2,$$

a ježto je c číslo racionálné, musí platiti tato kongruence též $mod\ 5$, tedy i $mod\ \lambda^4$, t. j.

$$c \equiv \pm 2^n, \mod \lambda^4.$$

I dostaneme z (55)

$$\pm n\,2^{n-1}(\zeta - \zeta^4)^2 \equiv 0 \mod \lambda^4$$

a ježto 2^{n-1} není λ dělitelno a $\zeta - \zeta^4$ jest associováno s λ, bude

$$n \equiv 0 \mod \lambda^2.$$

Poněvadž pak jest n racionálné číslo, musí býti též

$$n \equiv 0 \mod 5.$$

Položíme-li $n = 5m$, bude

$$\varepsilon = \pm (\zeta^2 + \zeta^3)^{5m},$$

tedy ε skutečně pátou mocninou jednotky

$$\pm (\zeta^2 + \zeta^3)^m.$$

Kdyby bylo n záporné, $n = -n'$, položili bychom

$$\zeta^2 + \zeta^3 = -\frac{1}{\zeta + \zeta^4}$$

$$\varepsilon = \mp (\zeta + \zeta^4)^{n'} = \mp (2 + (\zeta^2 - \zeta^3)^2)^{n'}$$

a dokázati úvahou zcela analogickou, že n' musí býti dělitelno 5ti.

§ 2.

Značí-li α, β, γ celá čísla z tělesa pátých kořenů z jednotky, z nichž žádné není rovno nulle, není splněna nikdy rovnice

$$\alpha^5 + \beta^5 + \gamma^5 = 0. \qquad (1)$$

V rovnici (1) můžeme patrně pokládati α, β, γ za čísla nesoudělná.

Při důkaze budeme rozeznávati dva případy: Předně, kdy žádné z čísel α, β, γ není dělitelno číslem $\lambda = 1 - \zeta$ a za druhé, je-li jedno z nich λ dělitelné.

Obraťme se nejprve k případu prvnímu.

Pišme

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

ve tvaru

$$\alpha = a + b + c + d - b(1 - \zeta) - c(1 - \zeta^2) - d(1 - \zeta^3).$$

Aby α nebylo dělitelno $1 - \zeta$, nesmí býti

$$a + b + c + d$$

dělitelno 5, musí tedy býti

$$a + b + c + d \equiv \pm 1 \text{ neb } \pm 2 \quad mod\ 5.$$

Pak bude

a) $\qquad \alpha \equiv \pm 1 \text{ neb } \pm 2 \quad mod\ \lambda$

a z toho odvodíme *)

b) $\qquad \alpha^5 \equiv \pm 1 \text{ neb } \pm 32 \quad mod\ \lambda^5.$

Nejsou-li β a γ dělitelna λ, jest podobně

$$\beta^5 \equiv \pm 1 \text{ neb } \pm 32 \quad mod\ \lambda^5$$

$$\gamma^5 \equiv \pm 1 \text{ neb } \pm 32 \quad mod\ \lambda^5.$$

I shledáme, že $\alpha^5 + \beta^5 + \gamma^5$ bude $mod\ \lambda^5$ kongruentní s jedním z čísel

$$\pm 1, \pm 3, \pm 30, \pm 32, \pm 34, \pm 63, + 65, \pm 96.$$

Z těchto není ani jedno $\equiv 0\ (mod\ \lambda^5)$; vyjímaje ± 30, ± 65 nejsou čísla ta vůbec 5ti dělitelná, ± 30, ± 65 jsou dělitelná pouze 5, t. j. λ^4, nikoliv však vyšší mocností λ. Vidíme tedy, že v prvém z obou uvedených případů vede rovnice (1) ke sporu, čímž nemožnost její pro tento případ dokázána.

---

*) Na př. kongruenci $\alpha^5 \equiv -1 \quad mod\ \lambda^5$ odvodíme z $\alpha \equiv -1 \quad mod\ \lambda$ tím, že tuto kongruenci napíšeme jako rovnici $\alpha \equiv -1 + \varkappa\lambda$, kdež $\varkappa$ jest celé číslo, umocníme pěti, čímž dostaneme $\alpha^5 = -1 + 5\varkappa\lambda + 10\varkappa^2\lambda^2 + 10\varkappa^3\lambda^3 + 5\varkappa^4\lambda^4 + \varkappa^5\lambda^5$. Vzhledem k tomu, že 5 jest associováno s λ^4, bude možno psáti $\alpha^5 \equiv -1\ (mod\ \lambda^5)$.

Obraťme se nyní k případu druhému, kdy jedno z čísel α, β, γ jest dělitelno λ. Předpokládejme, že jest to γ, položme

$$\gamma = \lambda^n \gamma_1 \text{ a uvažujme rovnici obecnější}$$

$$\alpha^5 + \beta^5 = \varepsilon \lambda^{5n} \gamma_1, \tag{2}$$

kdež ε značí libovolnou jednotku z tělesa $R(\zeta)$.

Rovnici (2) můžeme psáti, rozložíme-li levou stranu v činitele, ve tvaru

$$(\alpha + \beta)(\alpha + \beta\zeta)(\alpha + \beta\zeta^2)(\alpha + \beta\zeta^3)(\alpha + \beta\zeta^4) = \varepsilon \lambda^{5n} \gamma_1{}^5. \tag{3}$$

Pravá strana v této rovnici jest dělitelna prvočíslem λ; musí tedy býti i na levé straně aspoň jeden činitel λ dělitelný; poněvadž jsou však činitelé ti spolu kongruentní $(mod\ \lambda)$, budou všichni dělitelní λ a tedy

$$\alpha + \beta \equiv \alpha + \beta\zeta \equiv \alpha + \beta\zeta^2 \equiv \alpha + \beta\zeta^3 \equiv \alpha + \beta\zeta^4 \equiv 0 \ (mod\ \lambda). \tag{4}$$

Ježto α, β jsou čísla nedělitelná λ, jsou $\equiv \pm 1, \pm 2$ $(mod\ \lambda)$ a sice může býti jen na základě kongruencí (4)

$$\begin{array}{ll} \alpha) & \alpha \equiv 1, \ \beta \equiv -1 \\ \beta) & \alpha \equiv 2, \ \beta \equiv -2 \end{array} \ (mod\ \lambda)$$

$$\begin{array}{ll} \alpha') & \alpha \equiv -1, \ \beta \equiv 1 \\ \beta') & \alpha \equiv -2, \ \beta \equiv 2 \end{array} \ (mod\ \lambda)$$

V dalším můžeme se omeziti na uvažování jen prvních dvou případů (ke druhým dvěma bychom přišli, kdybychom spolu zaměnili α a β, což můžeme učiniti, poněvadž se tím rovnice (2) nezmění).

Pišme $\alpha)$ $\alpha = 1 + \lambda\mu, \quad \beta = -1 + \lambda\nu$

neb $\beta)$ $\alpha = 2 + \lambda\mu, \quad \beta = -2 + \lambda\nu,$

kdež μ, ν značí čísla celá.

Poněvadž jest

$$\zeta^k = (1 - (1 - \zeta))^k = (1 - \lambda)^k,$$

tedy

$$\zeta^k \equiv 1 - k\lambda \quad (mod\ \lambda^2),$$

bude buď

$$\alpha) \quad \alpha + \beta\zeta^k \equiv \lambda(\mu + \nu + k)$$

neb $$\beta)\quad \alpha + \beta\zeta^k \equiv \lambda\,(\mu + \nu + 2k)$$
$$(k = 0,\ 1,\ 2,\ 3,\ 4).$$

Z čísel $\alpha)\quad \mu + \nu + k \quad (k = 0,\ 1,\ 2,\ 3,\ 4)$

bude jistě jedno dělitelno λ; podobně tomu bude též u čísel

$$\beta)\quad \mu + \nu + 2k_1 \quad (k_1 = 0,\ 1,\ 2,\ 3,\ 4).$$

Bude tedy z čísel

$$\alpha + \beta\zeta^k \qquad (k = 0,\ 1,\ 2,\ 3,\ 4)$$

jistě jedno dělitelno λ^2.

I vidíme, že v rovnici (3) jest levá strana dělitelna aspoň λ^6, z čehož plyne nemožnost rovnice (3) pro $n = 1$.

Předpokládejme tedy $n > 1$.

Poněvadž se rovnice (2) nemění, píšeme-li v ní $\beta\zeta^k$ $(k + 1,\ 2,\ 3,\ 4)$ místo β, lze změnou označení převésti $\alpha + \beta\zeta^k$ $(k = 1,\ 2,\ 3,\ 4)$ v $\alpha + \beta$.

Stačí tedy v dalším uvažovati jen případ, kdy $\alpha + \beta$ jest dělitelno λ^2.

Kterékoliv dva faktory na levé straně rovnice (3) mohou míti za společnou míru jen λ. Společný dělitel čísel $\alpha + \beta\zeta^k$ a $\alpha + \beta\zeta^{k'}$ $(k \neq k')$ musí totiž býti též společným dělitelem čísel

$$(\alpha + \beta\zeta^{k'})\,\zeta^k - (\alpha + \beta\zeta^k)\,\zeta^{k'} = (\zeta^k - \zeta^{k'})\,\alpha$$
$$(\alpha + \beta\zeta^k) \quad - (\alpha + \beta\zeta^{k'}) \quad = (\zeta^k - \zeta^{k'})\,\beta$$

a čísla ta mají za společného dělitele pouze λ.

Z toho plyne dále, že jen $\alpha + \beta$ jest dělitelno λ^2, $\alpha + \beta\zeta$ $(k = 1,\ 2,\ 3,\ 4)$ jsou dělitelna pouze λ.

Aby pak bylo možno vyhověti rovnici (3), bude nutno položiti

$$\alpha + \beta = \eta\lambda^{5n-4}\gamma'^5$$
$$\alpha + \beta\zeta^k = \eta^k\lambda\delta_k^5 \quad (k = 1,\ 2,\ 3,\ 4),$$

kdež η, η_k jsou jednotky a δ, δ_k celá čísla z tělesa $K(\zeta)$, nedělitelná λ. Z rovnic těchto budeme potřebovati pouze 3, na př.

$$\alpha + \beta = \eta\lambda^{5n-4}\gamma'^5$$
$$\alpha + \beta\zeta = \eta_1\lambda\delta_1^5$$
$$\alpha + \beta\zeta^2 = \eta_2\lambda\delta_2^5.$$

Vylučme z nich nejprve α. Dostaneme

$$(1-\xi)\,\beta = \eta\lambda^{5n-4}\gamma'^5 - \eta_1\lambda\delta_1^5$$
$$(1-\xi^2)\,\beta = \eta\lambda^{5n-4}\gamma'^5 - \eta_2\lambda\delta_2^5.$$

Z těchto rovnic vylučme nyní β. Dostaneme

$$\delta_1^5 + \vartheta\delta_2^5 = \varepsilon'\lambda^{5(n-1)}\gamma'^5, \tag{5}$$

klademe-li

$$\vartheta = -\frac{1-\xi}{1-\xi^2}\frac{\eta^2}{\eta^1}, \quad \varepsilon' = \frac{\xi-\xi^2}{1-\xi^2},$$

což jsou opět jednotky.

Poněvadž jest $n > 1$, bude

$$\delta_1^5 + \vartheta\delta_2^5 \equiv 0 \pmod{\lambda^5}. \tag{6}$$

Avšak pro čísla nedělitelná λ platí dle rovnic (b)

$$\delta_1^5 \equiv c_1 \pmod{\lambda^5}$$
$$\delta_2^5 \equiv c_2 \pmod{\lambda^5},$$

kdež c_1 a c_2 jsou racionálná celá čísla nedělitelná 5ti.

Bude tedy

$$c_1 + \vartheta c_2 \equiv 0 \pmod{\lambda^5}$$

a také

$$c_1 + \vartheta c_2 \equiv 0 \pmod{5}.$$

Stanovme racionálná celá čísla c, d z rovnice

$$c_1 + cc_2 = 5d,$$

což jest možno, vzhledem k tomu, že c_1 a c_2 nejsou dělitelná pěti.

Pak bude plynouti z kongruencí

$$c_1 + \vartheta c_2 \equiv 0 \pmod{5}$$
$$c_1 + cc_2 \equiv 0 \pmod{5},$$

že

$$c_2(\vartheta - c) \equiv 0 \pmod{5}$$

a ježto c_2 není dělitelno pěti, též

$$\vartheta \equiv c \pmod{5}.$$

Bude tedy dle věty uvedené na str. 311. ϑ rovno páté mocnině jednotky z tělesa $R(\xi)$

$$\vartheta = \eta^5.$$

Položíme-li pak v rovnici (5)

$$\delta_1 = \alpha', \quad \eta\delta_2 = \beta',$$

dostaneme

$$\alpha'^5 + \beta'^5 = \varepsilon'\lambda^{5(n-1)}\gamma'^5. \tag{6}$$

Rovnice tato jest téhož typu jako (2), jen že jest v ní $n - 1$ místo n. Podobným způsobem, jako jsme přešli od rovnice (2) k rovnici (6), mohli bychom přejíti od (6) k rovnici téhož typu jako (2), kde by však bylo u 2 místo n a tak podobně až k rovnici s $n = 1$, která, jakož již vytčeno, jest nemožná. Tím dokázána věta Fermatova i pro druhý z obou vytčených případů.

O immaginárných bodech.

Píše dr. **B. Bydžovský.**

§ 1. Základní úvahy.

1. V algebře nazýváme *úlohou n-ho stupně* takovou úlohu, jež vede k rovnici (nebo soustavě rovnic) n-ho stupně. Omezíme-li se na úlohy o jedné neznámé, je patrno, že úloha n-ho stupně má n řešení; tedy úloha stupně prvého (lineárná) jediné řešení, úloha stupně druhého (kvadratická) dvě řešení atd.

Podobným způsobem lze tříditi konstruktivní úlohy v geometrii. Konstruktivní úloha žádá, aby byl sestrojen útvar vyhovující daným podmínkám.

Vyhovuje-li daným podmínkám jediný útvar, pravíme, že úloha má jediné řešení a nazýváme ji *lineárnou*; vyhovují-li útvary dva, *kvadratickou*: všeobecně je úloha stupně n-ho, vyhovuje-li podmínkám daným n útvarů. Pomýšlejme na úlohy, jež žádají nalezení bodů, vyhovujících daným podmínkám (na takové úlohy lze za jistých předpokladů převésti všechny konstruktivní úlohy). Budiž na příklad dána úloha, určiti na dané přímce p bod mající od dvou daných bodů A a B tutéž vzdálenost. Takový bod je jen jeden, ježto je dán jako průsečík dvou přímek, přímky p a osy úsečky $\overline{AB}$. Tuto úlohu nazveme v našem smyslu lineárnou. Naproti tomu úloha: určiti bod mající od dvou daných bodů S, S' dané vzdálenosti