MATEMATIKA

Diofantovské n-tice

IVAN CHAJDA

Přírodovědecká fakulta UP, Olomouc

Řecký matematik Diofantos z Alexandrie (asi 250 n. l.) byl již ve starověku nazýván otcem algebry. Jsou po něm nazvány rovnice, které řešíme v oboru celých či přirozených čísel, jako diofantovské. Věnoval se řešením těchto rovnic a základům teorie čísel. Do této oblasti spadá i problém nalezení čtveřice čísel takových, že součin každých dvou *různých* (z nich) zvětšený o 1 je roven druhé mocnině některého čísla. Příkladem takové čtveřice je $[1, 3, 8, 120]$, neboť

$$\begin{aligned} 1 \cdot 3 + 1 &= 2^2, & 3 \cdot 8 + 1 &= 5^2, \\ 1 \cdot 8 + 1 &= 3^2, & 3 \cdot 120 + 1 &= 19^2, \\ 1 \cdot 120 + 1 &= 11^2, & 8 \cdot 120 + 1 &= 31^2. \end{aligned}$$

Diofantos se ovšem neomezoval na čísla přirozená, ale hledal takové čtveřice mezi čísly racionálními, které musí být i v základu druhých mocnin. Příkladem čtveřice, kterou našel, je

$$\left[\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right].$$

První uvedenou celočíselnou čtveřici našel až *P. Fermat* v 17. století. *L. Euler* nalezl nekonečně mnoho takových celočíselných čtveřic ve tvaru

$$[a, b, a + b + 2r, 4r(r + a)(r + b)],$$

kde $ab + 1 = r^2$. Nalezl ovšem také pětice kladných racionálních čísel s uvedenou vlastností. Toto zkoumání nás vede k následující definici.

Definice 1

Konečná posloupnost m přirozených čísel $a_1, a_2, \ldots, a_m$ se nazývá *diofantovská m-tice*, je-li $a_i a_j + 1$ druhou mocninou přirozeného čísla pro všechna $1 \leq i < j \leq m$. Konečná posloupnost $a_1, a_2, \ldots, a_m$ nenulových racionálních čísel se nazývá *racionální diofantovská m-tice*, je-li $a_i a_j + 1$ druhou mocninou racionálního čísla pro všechna $1 \leq i < j \leq m$.

Je přirozenou otázkou, pro která m existují tyto diofantovské m-tice, a v jakém počtu. Byla vyslovena základní hypotéza o možných délkách m takových celočíselných m-tic:

Hypotéza 1

Neexistují diofantovské pětice.

Podstatný krok k vyřešení této hypotézy podnikli *A. Baker* a *H. Davenport*, viz [2] v r. 1969, když dokázali, že jediné přirozené číslo d takové, že $[1, 3, 8, d]$ je diofantovská čtveřice, je $d = 120$. Odtud plyne, že Fermatem nalezená čtveřice $[1, 3, 8, 120]$ nemůže být rozšířena na diofantovskou pětici. Avšak pro racionální čísla překvapivě existuje i racionální diofantovská šestice, jejíž příklad nalezl *P. Gibbs*, viz [7]:

$$\left[\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right].$$

Nabízí se myšlenka, zda existuje obecnější teorie, která by umožnila odpovědi na otázky o diofantovských m-ticích. Pokusíme se zde shrnout některé takové výsledky. V článku [1] dokázali *J. Arkin*, *V. E. Hoggart* a *E. G. Strauss*, že každou diofantovskou trojici lze rozšířit na diofantovskou čtveřici. Přesněji, je-li $[a, b, c]$ diofantovská trojice, a platí-li

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2,$$

kde r, s, t jsou přirozená čísla, pak $[a, b, c, d]$ jsou diofantovské čtveřice pro

$$d = a + b + c + 2abc + 2rst. \tag{1}$$

Čtenář snadno může ověřit, že platí

$$ad + 1 = (at + rs)^2, \quad bd + 1 = (bs + rt)^2, \quad cd + 1 = (cr + st)^2.$$

Otázkou zůstává, zda pro každou diofantovskou čtveřici $[a, b, c, d]$ takovou, že $d > \max\{a, b, c\}$, platí, že d splňuje (1). Jak již bylo zmíněno, Baker a Davenport to dokázali pro trojici $[1, 3, 8]$. *M. Veluppillai* [9] to dokázal pro $[2, 4, 12]$ a *K. S. Kedlaya* [8] pro trojice $[1, 3, 120]$, $[1, 8, 120]$, $[1, 8, 15]$, $[1, 15, 35]$, $[1, 24, 35]$ a $[2, 12, 24]$. Dokonce *A. Dujella* to dokázal pro všechny trojice tvaru $[k - 1, k + 1, 4k]$. Takové čtveřice $[a, b, c, d]$ se nazývají *regulární*. Ekvivalentní podmínkou k tomu, aby diofantovská čtveřice $[a, b, c, d]$ byla regulární, je splnění rovnosti

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

To je samozřejmě kvadratická rovnice pro d, jejíž jeden kořen je určen vztahem (1) a druhý je číslo

$$d = a + b + c + 2abc - 2rst.$$

Je dokázáno, že pro čísla a, b, c, d menší než 10^6 existuje právě 207 diofantovských čtveřic $[a, b, c, d]$, které jsou všechny regulární. Jelikož pro daná a, b, c je počet celočíselných bodů $[x, y]$ na křivce

$$y^2 = (ax + 1)(bx + 1)(cx + 1),$$

jak známo, konečný, plyne odtud, že nemůže existovat nekonečná posloupnost

$$a, b, c, \dots, x, \dots,$$

splňující Diofantovu podmínku (na pravé straně poslední rovnosti je součet tří druhých mocnin). Je tedy otázkou, jaké je největší číslo m, pro které existuje diofantovská m-tice. A. Dujella [5] dokázal v roce 2001, že $m \leq 8$. Avšak v roce 2004 tento výsledek sám podstatně zesílil dvěmá tvrzeními:

Věta 1

Neexistují diofantovské šestice.

Věta 2

Existuje nejvýše konečný počet diofantovských pětic.

Zda vůbec a kolik diofantovských pětic existuje, bylo zkoumáno řadou matematiků. Původní odhad byl, že pro jejich počet platí $Q < 10^{1930}$. Během několika let se tento odhad zpřesňoval, a nynější údaj je mnohem vylepšený, totiž $Q < 1,18{\cdot}10^{27}$. *Y. Fujita* [6] dokázal, že každá diofantovská pětice obsahuje regulární diofantovskou čtveřici a dále, je-li $[a, b, c, d, e]$ diofantovská pětice splňující $a < b < c < d < e$, pak musí platit jedna z podmínek:

(i) $4a < b$; $4ab + a + b < c < b^{3/2}$,
(ii) $4a < b$; $c = a + b + 2\sqrt{ab+1}$,
(iii) $4a < b$; $c > b^{3/2}$,
(iiii) $b < 4a$; $c = a + b + 2\sqrt{ab+1}$.

Pro racionální diofantovské pětice je situace zcela odlišná. Nechť $[a, b, c, d]$ je racionální diofantovská čtveřice, tj. pro vhodná racionální r_i platí

$$\begin{aligned} ab + 1 &= r_1^2, & bc + 1 &= r_4^2,\\ ac + 1 &= r_2^2, & bd + 1 &= r_5^2,\\ ad + 1 &= r_3^2, & cd + 1 &= r_6^2. \end{aligned}$$

Nechť $abcd \neq 1$. Položme

$$e = \frac{((a+b+c+d)(abcd+1) + 2abc + 2abd + 2acd + 2bcd \pm 2r_1r_2r_3r_4r_5r_6)}{(abcd-1)^2}.$$

Pak lze dokázat, že $[a, b, c, d, e]$ je racionální diofantovská pětice. S ohledem na symetrii stačí např. ukázat, že $ae+1 = (ar_4r_5r_6 \pm r_1r_2r_3)^2/(abcd-1)^2$.

Příkladem takové pětice je

$$\left[\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}, e\right],$$

kde výpočtem, jak výše uvedeno, zjistíme dvě možné hodnoty

$$e = \frac{549120}{10201} \quad \text{nebo} \quad e = -\frac{26880}{177241}.$$

Již Eulerovi bylo známo, že existuje nekonečně mnoho racionálních diofantovských pětic, ale teprve nedávno bylo zkoumáno, zda existuje nekonečně mnoho takových šestic. Nejmenší z nich je

$$\left[\frac{19}{12}, \frac{33}{4}, \frac{52}{3}, \frac{60}{2209}, -\frac{495}{24964}, \frac{595}{12}\right].$$

Kromě toho bylo dokázáno, že existuje nekonečně mnoho racionálních diofantovských šestic, které obsahují trojici $\left[\frac{15}{14}, -\frac{16}{21}, \frac{7}{6}\right]$. Stejný výsledek byl odvozen i pro trojice

$$\left[\frac{48}{17}, -\frac{35}{102}, \frac{17}{6}\right] \quad \text{a} \quad \left[\frac{56}{69}, -\frac{165}{184}, \frac{23}{24}\right].$$

Otevřenou otázkou zůstává existence racionální diofantovské sedmice. *P. Gibbs* nalezl 45 racionálních diofantovských šestic.

Při zkoumání celočíselných diofantovských m-tic jsme požadovali, aby $a_i a_j + 1$ bylo rovno r^2 pro některé přirozené číslo r, kdykoli $i \neq j$, Je totiž evidentní, že $a_i^2 + 1$ nemůže být druhou mocninou přirozeného čísla. Pro racionální diofantovské m-tice však takové omezení $i \neq j$ není nutné. Proto lze uvažovat i racionální diofantovské m-tice $[a_1, a_2, \ldots, a_m]$, kde $a_i^2 + 1$ je rovněž čtverec racionálního čísla. Takové m-tice se nazývají *silné*. Příkladem silné diofantovské trojice je

$$\left[\frac{1976}{5607}, \frac{3780}{1691}, \frac{14596}{1197}\right].$$

Není však znám žádný příklad silné diofantovské čtveřice.

Náš přehled některých výsledků o diofantovských m-ticích, které poutají pozornost matematiků pracujících v teorii čísel již po několik desetiletí, zakončíme vysvětlením, v které oblasti současného matematického výzkumu vznikají výše uvedené teorie a výsledky jako zajímavý „vedlejší produkt“. Je to v teorii eliptických křivek, což jsou právě křivky tvaru

$$y^2 = (ax + 1)(bx + 1)(cx + 1),$$

na kterých hledáme body s celočíselnými či racionálními souřadnicemi x, y. Že se jedná o poměrně složitý matematický aparát, který přesahuje elementární rámec našeho výkladu, si pravděpodobně čtenář umí představit.

Za pozornost stojí, že úloha s podobnou tematikou byla předložena reprezentantům na 27. mezinárodní matematické olympiádě, která se konala v roce 1986 ve Varšavě. viz např. [10]. Jako první byla zadána soutěžícím následující úloha:

Nechť a je přirozené číslo, různé od $2, 5, 13$. *Dokažte, že v množině* $\{2, 5, 13, d\}$ *lze nalézt dva prvky a, b takové, že* $\sqrt{ab - 1}$ *není celé číslo.*

Zájemcům doporučujeme pokusit se o vlastní řešení této úlohy.

Literatura

[1] *Arkin, J. – Hoggart, V. E. - Strauss E. G.*: On Euler's solution of a problem of Diophantus. Fibonacci Quart. **17** (1979).

[2] *Baker, A. – Davenport, H.*: The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. Quart. J. Mathem. Oxford Ser. (2) **20** (1969).

[3] *Dujella, A.*: The problem of the extension of a parametric family of Diophantine triples, Publ. Math. Debrecen **51** (1997).

[4] *Dujella, A.*: What is a Diophantine m-tuple? Notices of the Amer. Math. Soc., **63** (7), (2016).

[5] *Dujella, A.*: An absolute bound for the size of Diophantine m-tuples. Journal of Number Theory **89** (2001).

[6] *Fujita, Y.*: Any Diophantine quintuple contains a regular Diophantine quadruple. Journal of Number Theory **129** (2009).

[7] *Gibbs, P.*: Some rational Diophantine sextuples. Glas. Mat. Ser. III, Soft Computing **41** (2006).

[8] *Kedlaya, K. S.*: Solving constrained Pell equations. Math. Comp **67** (1998).

[9] *Veluppillai, M.*: The equations $z^2 - 3y^2 = -2$ and $z^2 - 6x^2 = -5$. A Collection of Manuscripts Related to the Fibonacci sequence, The Fibonacci Association, Santa Clara, 1980.

[10] 35. ročník MO na středních školách, SPN, Praha, 1988.

Polibky kružnic: Jakob Steiner, 1. část

PAVEL LEISCHNER

Pedagogická fakulta JU, České Budějovice

Již ve starověkém Řecku bylo známo: Pokud sečna z vnějšího bodu X protíná kružnici $k(O;r)$ v bodech A, B a tečna z téhož bodu má s kružnicí dotyk v bodě T, pak

$$|AX| \cdot |BX| = |AT|^2. \tag{1}$$

Eukleidovy *Základy* uvádí i analogickou větu pro vnitřní bod kružnice. Rovněž byla známa analogická věta pro vnitřní bod X kružnice k. Jakob Steiner (1796–1863) ve své první knižně vydané práci [2] tyto poznatky rozšířil. Zavedl veličinu zvanou *mocnost bodu ke kružnici* nebo též *mocnost kružnice k bodu*, kterou v dané rovině chápal jako charakteristiku vzájemné polohy libovolného bodu X a pevně zvolené kružnice k, resp.