MATEMATICKO-FYZIKÁLNY ČASOPIS SAV, VII, 2 — 1957

O PRVOČÍSELNÝCH MŘÍŽOVÝCH BODECH NA KUŽELOSEČKÁCH

MILOŠ LÁNSKÝ, Praha

Nechť P je množina všech prvočísel, C množina všech celých, R množina všech reálných čísel. Každý prvek kartézského součinu $C \times C$ nazýváme mřížovým bodem, každý prvek množiny $P \times C$, resp. $C \times P$ nazýváme zleva, resp. zprava prvočíselným mřížovým bodem. Prvky množiny $P \times P$ nazýváme prostě prvočíselnými mřížovými body.

Z teorie diofantických rovnic je známo (viz na př. [1], str. 130 nebo [2], str. 88), že existují neomezené regulární kuželosečky, na nichž leží nekonečně mnoho mřížových bodů. Takovou kuželosečkou je na př. Pellova hyperbola

$$y^2 - dx^2 = 1,$$

kde $d > 0$ není čtvercem celého čísla.

Snadno bychom dokázali, že tato hyperbola prochází však jen konečným počtem zleva prvočíselných mřížových bodů.[1] Je tedy na místě otázka, zda a které kuželosečky obsahují nekonečně mnoho zleva, resp. zprava prvočíselných mřížových bodů. Částečnou odpovědí na tuto otázku je věta, kterou nyní zformulujeme.

Věta. *Nechť r je racionální číslo; existuje-li regulární kuželosečka, která prochází bodem $(0; r)$ a obsahuje nekonečný počet zleva prvočíselných mřížových bodů, pak je to parabola, jejíž osa je rovnoběžná s osou y.*

Dříve než přistoupíme k elementárnímu důkazu této věty, odvodíme celkem samozřejmou pomocnou větu:

Pomocná věta. *Nechť $\eta \subset C \times C$ je funkce, pro niž platí v $R \times R$ vztah*

$$\lim_{x \to +\infty} \eta(x) = m \in R.$$

Pak

a) je $m \in C$,

b) existuje takové číslo $n \in C$, že pro všechna x větší než n z definičního oboru funkce η platí

$$\eta(x) = m.$$

[1] Důkaz na tomto místě neuvádíme z toho důvodu, že tvrzení je přímým důsledkem věty, kterou v dalším dokážeme. Viz důsledek 3.

Důkaz. Ke každému $\varepsilon > 0$ existuje podle předpokladu přirozené číslo n, takže pro všechna x větší než n a současně z definičního oboru funkce η platí

$$|\eta(x) - m| < \varepsilon, \qquad m \in R. \tag{1}$$

Označme symbolem $\delta(m, C)$ vzdálenost m od C. Je-li m non $\in C$, pak je $\delta(m, C) > 0$; zvolíme-li $\varepsilon \leqq \delta(m, C)$, pak ze vztahu (1) plyne, že platí

$$|\eta(x) - m| < \delta(m, C),$$

kde $\eta(x) \in C$, což je spor. Tím je dokázána prvá část tvrzení.

Položíme-li $\varepsilon \leqq 1$, pak ze vztahu (1) obdržíme

$$|\eta(x) - m| < 1,$$

kde $\eta(x) \in C$, $m \in C$. Odtud plyne $\eta(x) = m$, c. b. d.

Přejdeme nyní k důkazu vlastní věty:

Důkaz. Nechť $\mu \subset P \times C$ je nekonečná množina zleva prvočíselných mřížových bodů; nechť pro všechny uspořádané dvojice $(x, y) \in \mu$ platí vztah

$$a_{11}x^2 + 2a_{12}xy + 2\,a_{13}x + a_{22}y^2 + 2a_{23}y + a_{33} = 0, \tag{2}$$

kde prvky symetrické matice $\| a_{ik} \|$ jsou komplexní čísla a determinant $A = | a_{ik} |$ je různý od nuly.

Protože μ obsahuje alespoň pět různých bodů a platí $\mu \subset C \times C$, dá se na základě úvah z lineární algebry snadno odvodit, že prvky matice $\| a_{ik} \|$ jsou v poměru celočíselných determinantů; můžeme tedy vynásobením vhodným faktorem dosáhnout toho, aby koeficienty v rovnici (2) byly celými čísly. V dalším budeme předpokládat, že tato úprava již byla provedena.

Prochází-li kuželosečka (2) bodem $(0; r)$, pak r je racionálním kořenem polynomu

$$p(y) = a_{22}y^2 + 2a_{23}y + a_{33};$$

označíme-li $A_{11} = a_{22}a_{33} - a_{23}^2$, pak $\sqrt{-A_{11}}$ je celé číslo.

Zřejmě platí pro všechny dvojice $(x, y) \in \mu$ vztah

$$\begin{aligned} &a_{22}\,.\,(a_{11}x + 2a_{12}y + 2a_{13}) + \\ &+ (a_{22}y + a_{23} - \sqrt{-A_{11}})\,.\,(a_{22}y + a_{23} + \sqrt{-A_{11}}) = 0 \end{aligned} \tag{3}$$

a tedy $\quad x \mid (a_{22}y + a_{23} - \sqrt{-A_{11}})\,.\,(a_{22}y + a_{23} + \sqrt{-A_{11}})$.

Protože je $x \in P$, plyne ze známých vlastností dělitelnosti, že platí buď

$$x \mid a_{22}y + a_{23} + \sqrt{-A_{11}}, \tag{4}$$

nebo

$$x \mid a_{22}y + a_{23} - \sqrt{-A_{11}}. \tag{5}$$

Označme symbolem X_μ množinu všech čísel x, která se vyskytují na prvních místech dvojic $(x, y) \in \mu$, symbolem Y_μ množinu všech čísel y, která se vyskytují na druhých místech dvojic $(x, y) \in \mu$. Množina μ je nekonečná. Kdyby

množina X_μ byla konečná, pak Y_μ by byla nekonečná a existovalo by takové číslo $x \in X_\mu$, že pro nekonečně mnoho $y \in Y_\mu$ by platilo $(x, y) \in \mu$; to ovšem odporuje předpokladu $A \neq 0$. Množina X_μ je tedy nekonečná. V dalším nyní dokážeme, že platí $a_{22} = a_{12} = 0$.

I. Nechť je $a_{22} \neq 0$; pak pro všechny dvojice $(x, y) \in \mu$ platí buď

$$y = \frac{-a_{12}x - a_{23} + \sqrt{-A_{33}x^2 + 2A_{13}x - A_{11}}}{a_{22}}, \tag{6}$$

nebo

$$y = \frac{-a_{12}x - a_{23} - \sqrt{-A_{33}\,x^2 + 2A_{13}x - A_{11}}}{a_{22}}. \tag{7}$$

V těchto vzorcích značí A_{ik} doplňky determinantu A.

Definujeme nyní množiny $X_\mu^{\iota\varkappa}$, $\iota, \varkappa = 1, 2$ těmito předpisy:

X_μ^{11} je množina všech x, kde (x, y) vyhovuje vztahům (4) a (6),

X_μ^{12} je množina všech x, kde (x, y) vyhovuje vztahům (4) a (7),

X_μ^{21} je množina všech x, kde (x, y) vyhovuje vztahům (5) a (6),

X_μ^{22} je množina všech x, kde (x, y) vyhovuje vztahům (5) a (7).

Zavedeme-li $\varepsilon^{\iota\varkappa}$, $\delta^{\iota\varkappa}$, $\iota, \varkappa = 1, 2$ takto:

$$\| \varepsilon^{\iota\varkappa} \| = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \qquad \| \delta^{\iota\varkappa} \| = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix},$$

můžeme dále definovat funkce $\eta^{\iota\varkappa} \subset C \times C$, $\iota, \varkappa = 1, 2$ s příslušnými definičními obory $X_\mu^{\iota\varkappa}$ funkčním předpisem

$$\eta^{\iota\varkappa}(x) = \frac{-a_{12}x + \varepsilon^{\iota\varkappa}\sqrt{-A_{11}} + \delta^{\iota\varkappa}\sqrt{-A_{33}x^2 + 2A_{13}x - A_{11}}}{x},$$

$$\iota, \varkappa = 1, 2.$$

Že tyto funkce jsou celočíselné, odvodíme snadno, dosadíme-li ze vzorců (6) nebo (7) do vztahů (4) a (5).

Protože platí $X_\mu = X_\mu^{11} \cup X_\mu^{12} \cup X_\mu^{21} \cup X_\mu^{22}$, je alespoň jedna z množin $X_\mu^{\iota\varkappa}$ nekonečná. Tuto množinu, která je shora, resp. zdola neomezená, označme dvojicí indexů ι_0, $\varkappa_0$.

Pak zřejmě platí vztah

$$\lim_{x \to +\infty} \eta^{\iota_0\varkappa_0}(x) = -a_{12} + \delta^{\iota_0\varkappa_0}\sqrt{-A_{33}};$$

$$\text{resp.} \lim_{x \to -\infty} \eta^{\iota_0\varkappa_0}(x) = -a_{12} - \delta^{\iota_0\varkappa_0}\sqrt{-A_{33}}.$$

Podle pomocné věty existuje číslo $n \in C$, takže pro všechna $x > n$, resp. $x < -n$, $x \in X_\mu^{\iota_0\varkappa_0}$ platí

$$\eta^{\iota_0\varkappa_0}(x) = -a_{12} + \delta^{\iota_0\varkappa_0}\sqrt{-A_{33}},$$

resp.

$$\eta^{t_0x_0}(x) = -a_{12} - \delta^{t_0x_0}\sqrt{-A_{33}}.^{2}$$

Protože tento vztah platí pro více než dvě x, dostaneme po jednoduchých algebraických úpravách

$$A_{11}A_{33} - A_{13}^2 = 0;$$

protože však platí

$$a_{22}A = A_{11}A_{33} - A_{13}^2,$$

plyne odtud $A = 0$, což je spor.

II. Nechť $a_{22} = 0$, $a_{12} \neq 0$; pak pro všechny body $(x, y) \in \mu$ $\left(\text{s eventuální výjimkou těch bodů, pro něž je } x = -\frac{a_{23}}{a_{12}}\right)$, platí

$$y = -\frac{a_{11}x^2 + 2a_{13}x + a_{33}}{2(a_{12}x + a_{23})}. \tag{8}$$

Označme $\overline{X}_\mu = X_\mu - \left\{-\frac{a_{23}}{a_{12}}\right\}$. Ze vztahu (2) plyne, že pro všechna $x \in X_\mu$ platí

$$x \mid 2a_{23}y + a_{33}. \tag{9}$$

Dosadíme-li z (8) do (9), dospějeme k závěru, že je možno funkčním předpisem

$$\eta(x) = \frac{-a_{11}a_{23}x + a_{12}a_{33} - 2a_{13}a_{23}}{a_{12}x + a_{23}}$$

definovat celočíselnou funkci $\eta \subset C \times C$, jejímž definičním oborem je množina $\overline{X}_\mu$.

Protože množina $\overline{X}_\mu$ je nekonečná, je shora, resp. zdola neomezená a platí

$$\lim_{x\to\pm\infty} \eta(x) = -\frac{a_{11}a_{23}}{a_{12}}.$$

Podle pomocné věty existuje $n \in C$, takže pro všechna $x > n$, resp. $x < -n$, $x \in \overline{X}_\mu$, platí

$$\eta(x) = -\frac{a_{11}a_{23}}{a_{12}}.$$

Protože tento vztah platí pro více než jedno x, dostaneme po snadných algebraických úpravách

$$A = a_{12}^2a_{33} - 2a_{12}a_{13}a_{23} + a_{11}a_{23}^2 = 0,$$

což je spor.

III. Je-li $a_{22} = a_{12} = 0$, pak $A = -a_{11}a_{23}^2$; z předpokladu $A \neq 0$ plyne $a_{23} \neq 0$, $a_{11} \neq 0$.

---

[2] Zároveň je odtud patrno, že $\sqrt{-A_{33}}$ je celé (racionální) číslo, a tedy kuželosečka nemůže být eliptického typu.

Pro všechna $(x, y) \in \mu$ platí tedy podle (2)

$$y = -\frac{1}{2a_{23}}(a_{11}x^2 + 2a_{13}x + a_{33}).$$

Jak je známo z analytické geometrie, jde o rovnici paraboly, jejíž osa je rovnoběžná s osou y.

Tento případ může zřejmě nastat na př. tehdy, jsou-li $\frac{a_{11}}{2a_{23}}, \frac{a_{13}}{a_{23}}, \frac{a_{33}}{2a_{23}}$ celá čísla. Tím je důkaz věty proveden.

Důsledek 1. *Nechť r je racionální číslo; existuje-li regulární kuželosečka, která prochází bodem $(r; 0)$ a obsahuje nekonečný počet zprava prvočíselných mřížových bodů, pak je to parabola, jejíž osa je rovnoběžná s osou x.*

Důsledek 2. *Neexistuje regulární kuželosečka, která protíná souřadnicové osy v racionálních bodech a obsahuje nekonečný počet prvočíselných mřížových bodů.*

Důsledek 3. *Neexistuje hyperbola, která protíná aspoň jednu souřadnicovou osu v racionálním bodě a obsahuje nekonečný počet prvočíselných mřížových bodů.*

Důsledek 4. *Pellova hyperbola $y^2 - dx^2 = 1$ obsahuje konečný počet zleva prvočíselných mřížových bodů.*

Důsledek 5. *Nechť (x_0, y_0) je mřížový bod Pellovy hyperboly s nejmenším kladným x_0. Pak v posloupnosti celých čísel $\{x_1, x_2, \dots\}$, určených vztahem*

$$x_r = \frac{1}{\sqrt{d}} \cdot \sum_{k=0}^{k=\left[\frac{r-1}{2}\right]} \binom{r}{2k+1} (x_0\sqrt{d})^{2k+1} y_0^{r-2k-1}$$

je pouze konečný počet prvočísel.

Důkazy důsledků 1—4 jsou očividné. Důkaz důsledku 5 plyne okamžitě z důsledku 4, uvážíme-li, že všechny mřížové body (x, y) Pellovy hyperboly jsou určeny vztahem

$$y + x\sqrt{d} = (y_0 + x_0\sqrt{d})^r$$

(viz [2], str. 88).

Poznámka. Věta je zároveň řešením úlohy, kterou před časem předložil doc. dr. K. Černý. Jde o důkaz tohoto tvrzení:

Nabývá-li kvadratický trojčlen $ax^2 + bx + c$ s celočíselnými koeficienty pro všechna celá x hodnot, které jsou čtverci celých čísel, pak je tento trojčlen dvojmocí lineárního polynomu. My jsme vlastně dokázali více: stačí totiž, aby trojčlen nabýval čtvercových hodnot v bodě 0 a pro nekonečně mnoho prvočísel.

Jak mne upozornil akademik Štefan Schwarz, nelze ovšem větu dokázanou v této práci obrátit v tom smyslu, že by každá parabola procházející bodem $(0; r)$, jejíž osa je rovnoběžná s osou y, obsahovala nutně nekonečně mnoho zleva prvočíselných mřížových bodů. Jako příklad slouží parabola

$y = \frac{1}{3}(-1 + 2x^2)$, která prochází bodem $(0; -\frac{1}{3})$ a neobsahuje žádný mřížový bod.

LITERATURA

1. Schwarz Š., Algebraické čísla, Praha 1950. 2. Vinogradov J. M., Основы теории чисел 1949.

Došlo 6. 9. 1956.

О ПРОСТЫХ ЦЕЛЫХ ТОЧКАХ, ЛЕЖАЩИХ НА КРИВЫХ II-ГО ПОРЯДКА

МИЛОШ ЛАНСКИ

Выводы

Из теории уравнений Диофанта известно, что в действительной евклидовой плоскости существуют регулярные кривые II-го порядка, проходящие через бесконечное множество целых точек.

Примером такой линии служит гипербола Пелля

$$y^2 - dx^2 = 1,$$

где d — целое положительное, не являющееся квадратом целого числа. С другой стороны не трудно показать, что эта гипербола содержит только конечное число таких целых точек, первая координата которых проста. Автор вводит понятие слева (справа) простой целой точки, как целой точки первая (вторая) координата которой проста.

Автор потом формулирует следующую проблему: какого рода кривые II-го порядка вообще могут содержать бесконечное количество точек введеного типа.

Опираясь на лемму о пределе целочисленной функции, доказывается теорема:

Теорема. *Пусть r рациональное число; если существует регулярная кривая II-го порядка, проходящая через точку $(0, r)$ и содержащая бесконечное количество слева простых целых точек, потом это обязательно парабола, ось которой параллельна оси y.*

Эта теорема имеет ряд интересных следствий, напр. такое следствие, что не существует регулярная кривая II-го порядка, пересекающая координатные оси в рациональных точках и содержащая бесконечное количество совместно слева и справа простых целых точек.

ON PRIME LATTICE POINTS LYING ON THE CONICS

MILOŠ LÁNSKÝ

Summary

It is well known from the theory of diophantic equations that there exist in the real euclidean plane regular conics containing an infinite number of lattice points.

Take for an example the so called Pelle's hyperbola

$$y^2 - dx^2 = 1,$$

where $d > 0$ is not the quadrate of a whole number. On the other hand we could easily prove, that such a hyperbola contains only a finite number of lattice points whose first coördinates are prime.

The author introduces the term of the left resp. right prime lattice point like a point whose first resp. second coördinate is prime and formulates the problem of finding all conics which have an infinite number of such points in general.

On the base of a lemma about the limit of a function, the values of which can be only integers, he proves the folowing theorem.

Theorem. *Let r be a rational number; if there exists a regular conic containing the point $(0; r)$ and an infinite number of left prime lattice points, then it is a parabola with the axis paralell to y.*

This theorem implies a series of interesting corrolaries, such as: There exist no regular conics intersecting the coördinate axis in rational points and containing an infinite number of (bilateral) prime lattice points.