Pokroky matematiky, fyziky a astronomie

Břetislav Novák

Opět o Riemannově dzeta funkci

Pokroky matematiky, fyziky a astronomie, Vol. 38 (1993), No. 1, 7--13

Persistent URL: http://dml.cz/dmlcz/138710

Opět o Riemannově dzeta funkci

Břetislav Novák, Praha

Krása a přitažlivost matematiky je i v tom, že existuje celá řada problémů poměrně jednoduše formulovatelných, které odolávají úsilí celých generací. V teorii čísel zde byly klasické problémy rektifikace kružnice a kvadratury kruhu, které vyřešil až Lindemannův výsledek o transcendentnosti čísla π. Nejznámější však jsou tzv. Velká věta Fermatova a Riemannova hypotéza. Zatím co Fermatova věta láká svou formulací a historií i laiky, je Riemannova hypotéza výsadou těch, kteří mají větší matematické vzdělání.

Před více než rokem byly naše matematická veřejnost informována (Informace MVS JČMF, 34, 1990) o vystoupení J. S. Hwanga (Academia Sinica, Taipei, Taiwan) na mezinárodní konferenci o teorii potenciálu (ICPT-90, Nagoya), o níž byli informováni i účastníci světového kongresu matematiků (ICM-90, Kyoto). Název přednášky „On the falsity of Riemann's hypotesis" vzbudil všeobecný zájem. Protože i v časopise PMFA byla tato problematika připomenuta bizarním hororem [10], vraťme se k Riemannově funkci ještě jednou, tentokrát na matematické úrovni.

Sláva Riemannovy funkce $\zeta(s)$, která je pro komplexní s, $\operatorname{Re} s > 1$ definována vztahem

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

vznikla díky Riemannově krátké práci [9], kde jsou dokázány a částečně předpověděny její vlastnosti, zejména se zřetelem na problematiku rozložení prvočísel. Připomeňme její základní vlastnosti (podrobněji viz [8] a literaturu tam uvedenou, dále nedávné přehledné články [5] a [6]).

Funkce $\zeta(s)$ má analytické pokračování v celé komplexní rovině: získáme tak funkci, která je meromorfní s jediným jednoduchým pólem v bodě $s = 1$ a splňuje následující funkcionální rovnici: položíme-li

$$\xi(s) = \Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s),$$

platí

$$\xi(s) = \xi(1-s).$$

(Γ je Eulerova funkce gamma.) Funkce $\zeta(s)$ má reálné nulové body v sudých záporných číslech (tzv. triviální nulové body); všechny ostatní nulové body jsou imaginární a leží v tzv. kritickém pásu $0 \leqq \operatorname{Re} s \leqq 1$. Pro jejich počet v obdélníku $0 \leqq \operatorname{Re} s \leqq 1$, $0 < \operatorname{Im} s \leqq T$ platí vztah

$$N(T) = \frac{T}{2\pi}\ln\frac{T}{2\pi} - \frac{T}{2\pi} + O(\ln T) \tag{1}$$

Prof. RNDr. Břetislav Novák, DrSc. (1938), MFF UK, Sokolovská 83, 186 00 Praha 8.

(stejný vztah platí pro dolní polorovinu, neboť $\zeta(\bar{s}) = \overline{\zeta(s)}$). Jediná vlastnost funkce $\zeta(s)$, Riemannem jen předpověděná v práci [9], je jeho fascinující hypotéza:

Všechny netriviální nulové body $\zeta(s)$ leží na tzv. kritické přímce $\operatorname{Re} s = \frac{1}{2}$.

Souvislost $\zeta(s)$ s prvočísly byla známa již Eulerovi:

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}, \quad \operatorname{Re} s > 1,$$

kde p v nekonečném součinu probíhá všechna prvočísla. Pro $s > 1$ odtud ihned dostaneme

$$\ln \zeta(s) = \sum_p \frac{1}{p^s} + O(1), \quad s \to 1_+$$

a z divergence harmonické řady (pól $\zeta(s)$ v bodě 1) máme Eulerův důkaz nekonečnosti prvočísel.

Souvislost je však ještě těsnější: informace o poloze netriviálních nulových bodů se přímo přenáší na chování funkce $\pi(x)$, vyjadřující počet prvočísel, nepřesahujících x. Víme-li jen, že $\zeta(s) \neq 0$ na přímce $\operatorname{Re} s = 1$, dostaneme vztah

$$\pi(x) \sim \frac{x}{\ln x}, \quad \text{tj.} \lim_{x \to +\infty} \frac{\pi(x) \ln x}{x} = 1$$

nebo přesněji

$$\pi(x) \sim \operatorname{Li} x = \int_2^x \frac{\mathrm{d}t}{\ln t},$$

jak ukázali (a ještě v silnějším tvaru) Hadamard a nezávisle de la Vallée Poussin v r. 1896. Víme-li že $\zeta(s) \neq 0$ „více vlevo“ od přímky $\operatorname{Re} s = 1$, dostaneme pro rozdíl $\pi(x) - \operatorname{Li} x$ odhady jeho velikosti. Nejlepší současný výsledek pochází již z roku 1958 (Vinogradov a nezávisle Korobov): je-li $s = \sigma + it$, kde

$$\sigma > 1 - \frac{c}{\ln^{2/3}|t| \ln\ln^{-1/3}|t|}, \quad |t| \geqq 2,$$

pak $\zeta(s) \neq 0$. Odtud

$$\pi(x) = \operatorname{Li} x + O\left(x \mathrm{e}^{-c \frac{\ln^{3/5} x}{\ln\ln^{1/5} x}}\right)$$

(písmenem c označujeme různé „absolutní“ kladné konstanty).

Z platnosti Riemannovy hypotézy však plyne

$$\pi(x) = \operatorname{Li} x + O(\sqrt{x} \ln x).$$

Tento vztah je dokonce s Riemannovou hypotézou ekvivalentní.

Riemannova hypotéza, ev. její zobecnění pro další podobně definované funkce (Dedekindovy funkce dzeta atp.) mají zásadní význam pro celou řadu problémů teorie čísel. Uveďme tři příklady, které mají vztah i k dalším oblastem matematiky (a navíc dva z nich jsou významné i vzhledem k přínosu českých a slovenských matematiků).

Je-li t přirozené číslo, uvažujme Fareyovy zlomky, příslušné k číslu t v intervalu $(0, 1\rangle$, tj. zlomky ve tvaru p/q s celými nesoudělnými p, q, $0 < p \leqq q \leqq t$. Tyto zlomky se užívají v teorii funkcí, teorii aproximací a i v numerické matematice. Označme $\Phi(t)$ jejich počet; zřejmě je $\Phi(t) = \varphi(1) + \varphi(2) + \ldots + \varphi(t)$, kde $\varphi(n)$ je známá Eulerova funkce, označující počet přirozených čísel, nepřesahujících n a s n nesoudělných. Zkoumejme, jak jsou tyto zlomky rozloženy v intervalu $(0, 1\rangle$. Uspořádejme je podle velikosti: $0 < r_1 < r_2 < \ldots < r_u \leqq 1$, kde $u = \Phi(t)$ a porovnejme je s pravidelně rozdělenými body i/u, $i = 1, 2, \ldots, u$. Buď

$$\delta_i = r_i - i/u.$$

V r. 1924 ukázal Franel, že Riemannova hypotéza je ekvivalentní s platností vztahu

$$\sum_{i=1}^{u} \delta_i^2 = O(t^{-1+\varepsilon})$$

($t \to +\infty$, $\varepsilon > 0$ libovolné). Landau ve stejném roce nalezl další ekvivalentní vztah

$$\sum_{i=1}^{u} |\delta_i| = O\left(t^{1/2+\varepsilon}\right).$$

V práci [3] ukázal Kopřiva, že i platnost podobného vztahu

$$\sum_{i=1}^{u} \left(r_i^{n-1} - \frac{1}{n}\right) = O\left(t^{1/2+\varepsilon}\right)$$

($n > 1$ je pevně zvolené přirozené číslo) je ekvivalentní Riemannově hypotéze. V práci [4] pak zjemňuje tento výsledek, dokázaný v r. 1949 Mikolásem: Uvažujme rozdíl

$$R(t) = \int_0^1 f(x)dx - \frac{1}{\Phi(t)} \sum_{i=1}^{\Phi(t)} f(r_i).$$

Lze ukázat, že pro každou Riemannovsky integrovatelnou funkci f je $R(t) = o(1)$, $t \to +\infty$. Má-li f omezenou derivaci v intervalu $\langle 0, 1)$, lze $R(t)\Phi(t)$ odhadnout stejně, jako zbytek v prvočíselné větě; z platnosti Riemannovy hypotézy pak plyne $R(t)\Phi(t) = O\left(t^{1/2+\varepsilon}\right)$ pro každé $\varepsilon > 0$. Pro představu účinnosti těchto vztahů uveďme, že lze snadno ukázat, že $\Phi(t) = \frac{3}{\pi^2}t^2 + O(t \ln t)$. Z obecné teorie dostaneme jen odhad $R(t) = O(t^{-1})$. Zajímavé je, že platí-li vztah $R(t)\Phi(t) = O\left(t^{1/2+\varepsilon}\right)$ pro každé $\varepsilon > 0$ a pro každý polynom druhého stupně $f(x) = a_0x^2 + a_1x + a_2$ (a lze ukázat i jiné volby f), platí Riemannova hypotéza.

Druhý příklad spadá do teorie kódování. Popišme nejprve formu tzv. RSA algoritmu (Rivest, Shamir, Adleman 1978 — pro podrobnější výklad odkazujeme na krásnou monografii [7]). Zvolme dvě velká prvočísla p a q a buď $n = pq$. Zřejmě $\varphi(n) = (p-1)(q-1)$. Zvolme dále přirozené číslo s, nesoudělné s $\varphi(n)$. Máme-li nyní zakódovat posloupnost čísel

$$N_1,\ N_2,\ \ldots,\ N_k,\ \ldots$$

(představujme si je třeba jako pořadová čísla písmen nebo znaků na psacím stroji) utvořme posloupnost

$$C_1 \equiv N_1^s \pmod n, \ C_2 \equiv N_2^s \pmod n, \ \ldots, \ C_k \equiv N_k^s \pmod n, \ \ldots$$

(budeme předpokládat, že $N_i < \min(p, q)$; C_i znamená zde nejmenší kladné číslo, pro než rozdíl $N_i^s - C_i$ je dělitelný číslem n). Jak provést dekódování? Určíme přirozené t tak, aby rozdíl $st - 1$ byl dělitelný číslem $\varphi(n)$ (protože s a $\varphi(n)$ jsou nesoudělná, takové t vždy existuje; zvolíme třeba nejmenší číslo této vlastnosti).

Připomeňme nyní malou Fermatovu větu; je-li číslo C nesoudělné s n, pak

$$C^{\varphi(n)} \equiv 1 \pmod n.$$

protože podle naší volby je $s \cdot t = 1 + u\varphi(n)$ s vhodným přirozeným u, dostáváme postupně

$$C_i^t \equiv (N_i^s)^t = N_i^{s \cdot t} = N_i^{1+u\varphi(n)} = N_i \big(N_i^{\varphi(n)}\big)^u \equiv N_i \pmod n$$

(opět hledáme nejmenší nezáporný zbytek C_i^t při dělení n). Nalezli jsme tedy zpět původní posloupnost. Uvědomme si, že pro kódování potřebujeme jen dvojici s a n, pro dekódování dvojici t a n. Role s a t je symetrická: pomocí t můžeme kódovat a pomocí s dekódovat. Celý postup je snadno proveditelný na počítači; existují i účelová kódovací zařízení. Zdánlivě prostý algoritmus má však vysoký stupeň „utajení". Získá-li někdo dvojici s a n, potřebuje pro nalezení hodnoty t nutně hodnotu $\varphi(n)$, a tedy rozklad čísla n. Zvolíme-li však p a q dosti velká, je „prakticky" nemožné ze znalosti součinu $n = pq$ nalézti p a q. Odtud plyne důležitost „rychlých algoritmů" pro nalezení dělitele daného velkého čísla pro určení, je-li číslo prvočíslo atp. Zde se opět objevuje Riemannova hypotéza, tentokrát zobecněná pro Dirichletovy L-řady mod k tj. řady

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

kde χ je charakter mod k, tj. platí $\chi(n) = 0$ pro k/n a $\chi(n_1 \cdot n_2) = \chi(n_1) \cdot \chi(n_2)$ pro $(n_1, n_2) = 1$ $\chi \not\equiv 0$. Platí-li zobecněná Riemannova hypotéza, tj. leží-li všechna s, pro něž je $L(s, \chi) = 0$ a $\operatorname{Im} s \neq 0$ na přímce $\operatorname{Re} s = \frac{1}{2}$, lze ukázat, že velmi efektivní Millerův-Rabinův test prvočíselnosti vyžaduje pro dané n nejvýše $2(\ln n)^2$ zkoušek. Pro podrobný výklad odkazujeme na [7] a další literaturu tam uvedenou.

Jako třetí uveďme výsledky bratislavského matematika J. Mosera, jednoho z nejvýznamnějších světových odborníků v oblasti Riemannovy dzeta funkce. Celá řada jeho výsledků by si zasloužila samostatný článek, který by těžko mohl být přístupný nespecialistům. Zájemce odkazujeme na přehledné články [5] a [6], eventuálně na originální Moserovy ráce v Acta Arithmetika, Czech. Math. Journal a Acta Math. Univ. Comen. Právě v posledním časopise publikoval J. Moser v posledních pěti letech několik prací, ukazujících na souvislost Riemannovy funkce s teorií informace, radiotechnikou a teoretickou fyzikou. Jen jeden příklad z poslední oblasti: platí-li

Riemannova hypotéza, existuje v libovolném okolí Einsteinova rovnovážného stavu nekonečně mnoho asymptoticky rovnovážných stavů.

Snad je z uvedeného výčtu patrné, proč Riemannova hypotéza je již 133 let středem zájmu matematiků. Nikdo asi nespočítá kolik chybných důkazů bylo podáno. Uveďme pro zajímavost několik příkladů. Mezi nejzatvrzelejší patřil oděsský matematik (známý pracemi z oblasti diferenciálních rovnic) N. I. Gavrilov. Svou práci z r. 1961 vydal i knižně. Protože nalezené chyby stále opravoval, museli jeho oponenti použít drastického protipříkladu: sestrojili funkci, která má všechny vlastnosti Riemannovy funkce, které Gavrilov používal a pro niž Riemannova hypotéza neplatila. V roce 1966 na ICM v Moskvě, ohlásil důkaz německý matematik Haneke. V r. 1990 ohlásil důkaz známý matematik Luis de Branges (autor důkazu slavné Bieberbachovy domněnky). Svou přednášku odvolal. Konečně podle ústního sdělení podali nyní důkaz — nezávisle na sobě — dva významní matematici, žijící na území bývalého SSSR.

Vraťme se však k J. S. Hwangovi. Svou práci [1] zaslal do polského časopisu Acta Arithmetica a podle ústního sdělení A. Schinzela, našel její recenzent přibližně v polovině rozsáhlého sedmdesátistránkového rukopisu chybu skoro numerického charakteru, podstatnou pro výsledek. J. S. Hwang však svůj postup modifikoval a v letošním roce se objevily dva nové rukopisy. První [1] nese stejný název jako práce z r. 1990, ale liší se postupem (i délkou — 34 stran) a neobsahuje o svém předchůdci žádnou zmínku.

Základní myšlenka původní Hwangovy práce je jednoduchá. Z Hadamardovy teorie celých funkcí vyplývá, že

$$\zeta(s) = \frac{e^{as}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{\varrho} \left(1 - \frac{s}{\varrho}\right) e^{\frac{s}{\varrho}},$$

kde ϱ probíhá netriviální nulové body funkce $\xi(s)$, $a = \ln 2\pi - 1 - \frac{1}{2}\gamma$, γ je Eulerova konstanta. Srovnáme-li netriviální kořeny v polorovině $\operatorname{Im} z > 0$ podle imaginárních částí, dostaneme posloupnost $\varrho_n = \sigma_n + i\gamma_n$, $0 \leqq \gamma_1 \leqq \gamma_2 \leqq \ldots$, $0 < \sigma_n < 1$. Ze vztahu (1) pak ihned plyne

$$\gamma_n \sim |\varrho_n| \sim \frac{2\pi n}{\ln n}. \tag{2}$$

Protože všechny netriviální kořeny $\zeta(s)$ jsou ϱ_n a $\overline{\varrho_n}$ a řada

$$b = \sum_{\varrho} \frac{1}{\varrho} = \sum_{n=1}^{\infty} \left(\frac{1}{\varrho_n} + \frac{1}{\overline{\varrho_n}}\right) = \sum_{n=1}^{\infty} \frac{\varrho_n + \overline{\varrho_n}}{|\varrho_n|^2}$$

$(0 < \varrho_n + \overline{\varrho_n} = 2\delta_n < 2)$ podle (2) konverguje, získáme vyjádření

$$\zeta(s) = \frac{e^{as+bs}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{n=1}^{\infty} \left(1 - \frac{s}{|\varrho_n|^2}(2\sigma_n - s)\right).$$

Předpokládejme, že Riemannova hypotéza platí, tj. $\sigma_n \equiv \frac{1}{2}$ a omezme se na $s = \frac{1}{2} + it$, $t > 0$. Máme

$$\zeta(s) = \frac{e^{(a+b)s}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{n=1}^{\infty} \left(1 - \frac{s(1-s)}{|\varrho_n|^2}\right). \tag{3}$$

Pro naše s na polopřímce $\frac{1}{2} + it$, $t > 0$ je $s(1-s) = |s|^2 \geqq \frac{1}{4}$ a nekonečný součin má reálné faktory. Ze Stirlingovy formule pro funkci Γ dostaneme ihned pro $s = \frac{1}{2} + it$, $t \to +\infty$

$$\frac{1}{\left|\Gamma\left(\frac{s}{2}+1\right)\right|} = \frac{1}{\sqrt{2\pi}} e^{\frac{\pi t}{4}} t^{-\frac{3}{4}} (1 + O(t)).$$

Výraz před nekonečným součinem v (3) roste tedy na naší polopřímce exponenciálně. Je však známo, že

$$\zeta(s) = O(|t|) \tag{4}$$

(tento vztah platí dokonce v celé polorovině $\operatorname{Re} s \geqq \frac{1}{2}$). Exponenciální růst první části v (3) musí být tedy potlačen nekonečným součinem. Hwang se nyní snaží ukázat, že na naší polopřímce existuje posloupnost bodů $s_j = \frac{1}{2} + it_j$, pro něž je nekonečný součin dosti velký, aby celkově — ve sporu s (4) — platilo

$$|\zeta(s_j)| > e^{\sqrt{|s_j|}}.$$

Jak volí s_j? Je přirozené, volit s_j „mezi" nulovými body. Hwang ukazuje, že pro nekonečně mnoho n je $|\varrho_n|^2 - |\varrho_{n-1}|^2 \geqq 2$ a čísla s_j postupně volí jako „průměr" těchto dvojic, tj. jako čísla

$$\frac{1}{2} + i\left[\frac{1}{2}\left(|\varrho_n|^2 + |\varrho_{n-1}|^2\right) - \frac{1}{4}\right]^{\frac{1}{2}}.$$

Pro dolní odhad nekonečného součinu v bodech s_j je potřeba bedlivě vážit vzájemnou polohu s_j a ϱ_n. Hwang nejprve na deseti stranách výpočtu odvozuje místo (2) mnohem přesnější vyjádření — asymptotiku s chybou $O(n \ln^{-7} n)$. Vlastní odhad součinu provádí na skoro čtyřiceti stranách — a zde byla nalezena chyba.

Obraťme se nyní na závěr k novým pracím J. S. Hwanga, jejichž recenze v době dokončování rukopisu tohoto článku ještě probíhá. Jejich základní myšlenka je stejně zajímavá jako u původní verze práce [1]. Vytvořme novou funkci $\zeta^*(s)$ („zeta like function") tak, že v původním vyjádření

$$\zeta(s) = \frac{e^{as}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{\varrho} \left(1 - \frac{s}{\varrho}\right) e^{\frac{s}{\varrho}}$$

zaměňme netriviální kořeny ϱ hodnotami $\varrho^* = \frac{1}{2} + \mathrm{i}\,\mathrm{Im}\varrho$, tedy

$$\zeta^*(s) = \frac{\mathrm{e}^{as}}{2(s-1)\Gamma\left(\frac{s}{2}+1\right)} \prod_{\varrho^*} \left(1 - \frac{s}{\varrho^*}\right) \mathrm{e}^{\frac{s}{\varrho^*}}.$$

Je-li Riemannova hypotéza pravdivá, je $\zeta(s) = \zeta^*(s)$. Hwang nyní chce ukázat, že pro kladná s je $\zeta(s) \neq \zeta^*(s)$, dokonce

$$\ln \zeta^*(s) > \ln \zeta(s) + \frac{3}{4s} > \ln \zeta(s).$$

K tomuto účelu místo přibližného vztahu (1) užívá (složitého) přesného vyjádření funkce $N(T)$, pocházející od Backlunda.

V práci [2] je dokazována Lindelöfova hypotéza

$$\zeta\left(\frac{1}{2} + \mathrm{i}t\right) = O\left(|t|^\varepsilon\right), \quad \varepsilon > 0$$

(která je důsledkem hypotézy Riemannovy). Navíc jsou zde uvedena některá tvrzení a hypotézy, které — zjednodušeně řečeno — řeší vše, co zůstalo v této oblasti teorie čísel dosud otevřené.

Označíme-li p_n n-té prvočíslo, platí známá nerovnost

$$p_{n+1} - p_n \leqq p_n^{3/4+\varepsilon}$$

pro každé $\varepsilon > 0$. Hwang dokazuje zesílení této nerovnosti ve tvaru

$$p_{n+1} - p_n \leqq p_n^{1/2+\varepsilon}.$$

Dále dokazuje analogii Bombieriho „hypotézy o hustotě" a tvrdí, že zobecnění Riemannovy hypotézy pro Dirichletovy řady neplatí. V závěru své práce vyslovuje hypotézu, že známá Goldbachova hypotéza (každé sudé číslo větší než dvě je součtem dvou prvočísel) rovněž neplatí. I kdyby se v těchto pracích (jak autor těchto řádků pevně věří) nalezla chyba, jsou práce J. S. Hwanga zajímavou součástí historie teorie čísel.

Literatura

[1] HWANG J. S.: *On the falsity of Riemann's hypotesis.* Preprint 1992, 34 stran.
[2] HWANG, J. S.: *On the zeta-like function and Lindelöf hypotesis.* Preprint 1992, 22 stran.
[3] KOPŘIVA J.: *Contribution to the relation of the Farey series to the Riemann hypothesis.* Čas. pěst. mat. *79* (1954), 77–82.
[4] KOPŘIVA J.: *Remark on the significance of the Farey series in number theory.* Publ. Fac. Sci. Univ. Masaryk 1955, 267–279.
[5] KARACUBA A. A.: *Dzeta-funkcija Rimana i ějo nuli.* Uspěchi mat. nauk *40* (1988), 19–70.
[6] KARACUBA A. A.: *Rasprědelěnije prostych čisěl.* Uspěchi mat. nauk *45* (1990), 51–140.
[7] KOBLITZ N.: *A course in number theory and cryptography.* Springer Verlag 1987.
[8] NOVÁK B.: *O osmém Hilberově problému.* PMFA *XVIII* (1973), 9–17.
[9] RIEMANN B.: *Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse.* Monatsber. Akad. Berlin (1859), 671–680.
[10] STANLEY R. P.: *Profesor Eubanks v říši Dzéta.* PMFA *35* (1990), 90–93.