Časopis pro pěstování matematiky a fysiky

Vojtěch Jarník

Nový důkaz věty o rozdělení prvočísel

Časopis pro pěstování matematiky a fysiky, Vol. 74 (1949), No. 1, D51--D54

Persistent URL: http://dml.cz/dmlcz/109141

$$\lim_{x\to x_0}\left(\frac{f(x)-f(x_0)}{(x-x_0)^2}-\frac{f'(x_0)}{x-x_0}\right)\neq 0.$$

Il faut encore préciser la notion de la „tangente" à la „courbe" $y = f(x)$ au point P_i. Si $f'(x_i)$ existe et est finie, on a la définition habituelle; mais, si $f'(x_i)$ existe et est égale à $+\infty$ ou à $-\infty$, on appelle la droite $x = x_i$ „tangente" à la „courbe" au point P_i seulement dans le cas où f est *continue* au point x_i. Si l'on supprime cette condition de continuité (tout en conservant la condition de continuité au point x_0), on peut construire des exemples bizarres (voir § 4), où le cercle K^4 existe mais n'a rien de commun avec l'idée intuitive du „cercle de courbure".

NOVÝ DŮKAZ VĚTY O ROZDĚLENÍ PRVOČÍSEL.

Vojtěch JARNÍK, Praha.

Označme znakem $\pi(x)$ počet prvočísel, která nejsou větší než x. Otázka, jak se chová funkce $\pi(x)$ pro $x \to +\infty$, patří k nejproslulejším problémům analytické theorie čísel. Abychom zkrátili vyjadřování, budeme říkati, že dvě kladné funkce $f(x)$, $g(x)$ jsou „téhož řádu", jestliže

$$\liminf_{x\to+\infty}\frac{f(x)}{g(x)} > 0,\quad \limsup_{x\to+\infty}\frac{f(x)}{g(x)} < +\infty;$$

budeme dále říkati, že funkce $f(x)$, $g(x)$ jsou si asymptoticky rovny (znak $f(x) \sim g(x)$), jestliže dokonce

$$\lim_{x\to+\infty}\frac{f(x)}{g(x)} = 1.$$

Již ČEBYŠEV dokázal elementárně r. 1850, že funkce $\pi(x)$, $\frac{x}{\log x}$ jsou téhož řádu. Ale teprve v r. 1896 dokázali HADAMARD a de la VALLÉE-POUSSIN, že

$$\pi(x) \sim \frac{x}{\log x} \tag{1}$$

(jde ovšem o přirozený logaritmus). Ale tento důkaz nebyl již vůbec elementární: spočíval na theorii analytické funkce $\zeta(s)$; tato funkce komplexní proměnné s je definována, pokud reálná část s je větší než 1, rovnicí

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}.^{1)} \tag{2}$$

[1]) Že tato funkce souvisí s prvočísly, poznal již EULER, který pro $s > 1$ odvodil rovnici (součin se vztahuje na všechna prvočísla p)

$$\sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p (1 + p^{-s} + p^{-2s} + p^{-3s} + \ldots) = \prod_p \frac{1}{1 - p^{-s}}.$$

Tuto funkci lze analyticky pokračovati v celé komplexní rovině, při čemž jedinou singularitou je jednoduchý pól v bodě $s = 1$. HADAMARDOVI též náleží zásluha, že vybudoval theorii celistvých transcendentních funkcí, na jejímž základě byl dokázán vzorec (1). Ukázalo se však, že ještě lépe, než funkce $\frac{x}{\log x}$, aproximuje funkci $\pi(x)$ funkce

$$\int_2^x \frac{dt}{\log t} = li(x).$$

Řádová velikost rozdílu $\pi(x) - li(x)$ byla potom předmětem četných a významných prací (LANDAU, HARDY, LITTLEWOOD, INGHAM, ČUDAKOV a jiní). Současně byl postupně zjednodušován důkaz rovnice (1) (i důkazy ostřejších odhadů pro rozdíl $\pi(x) - li(x)$); v tomto směru se zvláště zasloužil LANDAU. Ale všechny tyto důkazy spočívaly na analytickém pokračování funkce $\zeta(s)$ přes přímku $\Re s = 1$ doleva ($\Re s$ = reálná část čísla s).[2]) Teprve okolo r. 1930 podal WIENER důkaz vzorce (1), v němž se neužívá vůbec theorie funkce $\zeta(s)$ pro $\Re s < 1$, takže pomůcky z theorie analytických funkcí byly vlastně eliminovány, a důkaz spočívá v podstatě na integrálním počtu.[3]) Podotýkám, že obdobné výsledky jako pro funkci $\pi(x)$ byly odvozeny také pro rozdělení prvočísel, patřících k libovolně předepsané aritmetické posloupnosti $l, l + q, l + 2q, l + 3q, \ldots$ (q, l nesoudělná kladná čísla).

Ale vzorec tak elementární, jako je vzorec (1), si zasluhoval také elementárního důkazu. Takový důkaz podali teprve v r. 1948 ATLE SELBERG a PAVEL ERDÖS. SELBERG je norský matematik (nezaměňovati s jinými matematiky téhož jména!), který za války napsal překrásné práce o nulových bodech funkce $\zeta(s)$; ERDÖS je maďarský matematik, který má za sebou již mnoho významných prací z theorie čísel i z mnoha jiných oborů. Jejich důkaz, který znám dosud pouze ze skript amsterodamského matematického centra, se skládá ze dvou částí.

Zaveďme napřed dvě označení. Je-li n celé kladné, definujeme $\mu(n)$ (t. zv. MÖBIOVU funkci) takto: $\mu(1) = 1$; $\mu(n) = (-1)^k$, je-li n součinem *k různých* prvočísel; $\mu(n) = 0$, je-li n dělitelno aspoň druhou mocninou nějakého prvočísla. Tato funkce má mnoho jednoduchých vlastností, takže se s ní dobře pracuje. Za druhé položme $\vartheta(x) = \sum_{p \leqq x} \log p$ (t. j. sčítá se přes všechna prvočísla $p \leqq x$). S touto funkcí se lépe pracuje než s funkcí $\pi(x)$. Je dávno známo a lze dokázati na několika řádcích, že

---

[2]) Velmi pohodlně je možno se poučiti o těchto věcech z krásné knížky INGHAMOVY: The distribution of prime numbers, Cambridge, 1932.

[3]) Další zjednodušení tohoto důkazu podal LANDAU. Lze je nalézti na př. v knize VALIRONOVĚ: Théorie des fonctions (Cours d'Analyse mathématique), 2. vyd., Paříž 1948, str. 509—513.

vzorec (1) je ekvivalentní vzorci

$$\vartheta(x) \sim x. \tag{3}$$

První částí důkazu je nyní důkaz SELBERGOVA vzorce

$$\frac{\vartheta(x)}{x} + \frac{2}{x \log x} \sum_{p \leqq \sqrt{x}} \vartheta\left(\frac{x}{p}\right) \log p \sim 2 \tag{4}$$

(t. j. limita levé strany pro $x \to +\infty$ je 2). Napřed se dokáže, že levá strana v (4) je asymptoticky rovna výrazu

$$\frac{1}{x \log x} \sum_{1 \leqq m \leqq x} \sum_{d} \mu(d) \log^2 \frac{x}{d}, \tag{5}$$

kde ve vnitřním součtu se sčítá přes všechny kladné dělitele d čísla m. Tento výraz již neobsahuje explicite prvočísla (implicite ovšem ano, v definici funkce μ) a proto se s ním dobře pracuje.[4]) Dokáže se pak, že výraz (5) je asymptoticky roven dvěma, čímž (4) je dokázáno.

V druhé části se pak z (4) odvozuje (3). Základní myšlenka je asi tato: Položme

$$\limsup_{x \to +\infty} \frac{\vartheta(x)}{x} = A, \quad \liminf_{x \to +\infty} \frac{\vartheta(x)}{x} = a.$$

Z citované věty ČEBYŠEVOVY plyne, že čísla a, A jsou konečná a kladná. Užijeme-li snadno dokazatelného vzorce

$$\sum_{p \leqq \sqrt{x}} \frac{\log p}{p} \sim \log \sqrt{x},$$

dostaneme z (4) téměř okamžitě, že $A + a = 2$. Všimněme si nyní, že člen $\vartheta(x) : x$ se musí vykompensovati s druhým členem levé strany v (4) tak, aby součet dal přibližně 2 (pro velká x). Tedy: Jestliže $\vartheta(x) : x$ je „velké", t. j. blízko číslu A, je „většina" čísel $\vartheta\left(\frac{x}{p}\right) : \frac{x}{p}$ „malá", t. j. blízká číslu a.[5]) Přesnou formulací této zde jenom naznačené úvahy a jejím opakováním (viz pozn. [5])) a obratným využitím se obdrží $A = a = 1$, čímž vzorec (3) a tedy i (1) dokázán.

Důkaz, který jsem zde naznačil, není příliš složitý, a je naprosto elementární. Není zde řeči o funkci $\zeta(s)$, z analysy se pak užívá jedině funkce logaritmické;[6]) a také u této funkce potřebujeme vedle elementár-

[4]) Také v řadě (2) prvočísla nijak zjevně nevystupují.

[5]) Načež, použiji-li vzorce (4) s hodnotou $x : p$ místo x, vidím, že „většina" čísel $\vartheta\left(\frac{x}{pp'}\right) : \frac{x}{pp'}$ (p, p' prvočísla) je zase „velká".

[6]) A ovšem základních pojmů limitních. Funkce logaritmická vystupuje ostatně ve výsledku (1), a tedy by snad bylo přemrštěné se jí vyhýbat. Bylo by ovšem jistě možno, nahraditi $\log n$ výrazem (asymptoticky jemu rovným pro $n \to +\infty$) $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$, ale to by asi velmi zkomplikovalo důkaz.

ních vlastností (jako je logaritmus součinu, podílu, mocniny) pouze nerovnosti (n celé kladné)

$$\frac{1}{n} > \log\left(1 + \frac{1}{n}\right) > \frac{1}{n+1} = \frac{1}{n} - \frac{1}{n(n+1)} > \frac{1}{n} - \frac{1}{n^2},$$

t. j.

$$n \log\left(1 + \frac{1}{n}\right) < 1 < (n+1) \log\left(1 + \frac{1}{n}\right),$$

jež plynou ihned logaritmováním z nerovností

$$\left(1 + \frac{1}{n}\right)^n < e < \left(1 + \frac{1}{n}\right)^{n+1},$$

používaných k definici čísla e.

Nový důkaz SELBERGŮV a ERDÖSŮV znamená velký methodický pokrok a splnění starého desiderata. Podotýkám ovšem, že autoři dokazují touto methodou pouze vzorec (1) a nikoliv jemnější známé věty o rozdílu $\pi(x) - x : \log x$ nebo $\pi(x) - li(x)$.

*

Une démonstration nouvelle de la loi de la distribution des nombres premiers. Une bréve information sur la démonstration élémentaire donnée par MM. Erdös et Selberg.

PŘÍSPĚVEK K NUMERICKÉMU ŘEŠENÍ ROVNIC 3. STUPNĚ.

Ing. dr FRANTIŠEK BRANDLER, Praha.

Článek tento má za účel, ukázati v souvislosti se zajímavou studií p. dr B. KÖNIGA „Řešení rovnic algebraických vyšších stupňů“ (uveřejněnou na str. 118—124, roč. *24* (1944/45) „Rozhledů matematicko-přírodovědeckých“), že k řešení těchto rovnic lze namnoze s výhodou užíti též methody nejmenších čtverců, kterážto methoda — pokud je mi známo — na tento obor způsobem v dalším uváděným dosud aplikována nebyla. Jde v podstatě o to, že křivku $y = f(x)$, která jest grafickým obrazem dotyčné funkce (rovnice), nahradíme v určitém intervalu ξ — v okolí kořene rovnice — jinou vhodnou křivkou $y = \varphi(x)$, jež ve smyslu uvedené methody k dané křivce co nejtěsněji přiléhá, t. j. tuto křivku v intervalu ξ „vyrovnává“ tak, aby součet čtverců odchylek $\Delta y = \varphi(x) - f(x)$ byl minimem.

Omezíme se zde na řešení rovnic kubických. Za náhradní funkci $\varphi(x)$ volíme jednak parabolu 2. stupně („vyrovnávací parabolu“), jednak přímku („vyrovnávací přímku“), jakožto útvary s praktického hlediska nejúčelnější.