Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti

Martin Klazar*

1 Úvod

Tak praví název preprintu [21] uveřejněného 8. dubna 2004 na preprintovém servru arXiv [55] a popisuje přesně hlavní výsledek:

Věta 1.1[1] **(Greenova-Taova věta).** *Prvočísla obsahují aritmetickou posloupnost délky k pro každé přirozené číslo k.*

Jinak řečeno, pro každé přirozené číslo k existuje k-tice prvočísel $p_1 < p_2 < \ldots < p_k$ taková, že $p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1}$. (Např. aritmetické posloupnosti 5, 11, 17, 23, 29 nebo 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 jsou tvořeny prvočísly.) Autoři, B. Green a T. Tao [2], dosáhli velkého průlomu v teorii prvočísel a v teorii čísel vůbec. Jejich výsledek vzbudil okamžitě velkou pozornost a zájem. Bezpochyby se zařadili do číselně-teoretické „síně slávy" po bok Dirichleta, Riemanna, Vinogradova, Erdőse a dalších (viz oddíl 3). Cílem tohoto článku je začlenit jejich výsledek do historického kontextu (oddíl 3) a zejména čtenáři přiblížit metody, které Green a Tao pro důkaz své věty o prvočíslech použili (oddíl 2). Protože [21]

*Doc. RNDr. Martin Klazar, Dr. (1966), Katedra aplikované matematiky a Institut teoretické informatiky, Matematicko-fyzikální fakulta UK, Malostranské náměstí 25, 118 00 Praha 1, e-mail: klazar@kam.mff.cuni.cz

[1] Číslování definic, vět, tvrzení a lemmat přebíráme z [21].

[2] Ben Green (1977) získal titul Ph.D. v r. 2002 na Univerzitě v Cambridge pod vedením T. Gowerse. Od r. 2005 je profesorem na Univerzitě v Bristolu. Terence Tao (1975) získal titul Ph.D. v r. 1996 na Princetonské Univerzitě pod vedením E. Steina. Od r. 2000 je („full") profesorem na UCLA v Kalifornii. Z jeho mnoha ocenění zmiňme alespoň medaile na Mezinárodní matematické olympiádě: bronzová v r. 1986, stříbrná v r. 1987 a zlatá v r. 1988.

má téměř 50 stran, v tomto článku jde pochopitelně jen o přehled, nicméně podáváme přesné formulace použitých výsledků (v originálním číslování práce [21]).

Důkaz věty 1.1 je efektivní, dává konkrétní funkci $f : \mathbf{N} \to \mathbf{N}$ takovou, že množina $\{1, 2, \ldots, f(k)\}$ pro každé k obsahuje aritmetickou posloupnost délky k složenou z prvočísel. Tao v [50] uvádí, že lze vzít

$$f(k) = 2^{2^{2^{2^{2^{2^{2^{100k}}}}}}}.$$

Green a Tao modifikací důkazu věty 1.1 dokázali její zesílení, větu 1.2: Je-li P množina všech prvočísel a podmnožina $Q \subset P$ splňuje $\limsup_{n\to\infty} \frac{Q(n)}{P(n)} = c > 0$ ($Q(n)$ je počet prvků q v Q, $q \leq n$, podobně $P(n)$), musí Q obsahovat libovolně dlouhé aritmetické posloupnosti. Je známo, že pro $Q_1 = \{p \in P : p = 4n+1\}$ máme $c = 1/2$ a každé $p \in Q_1$ je součet dvou čtverců ($p = a^2 + b^2$ pro dvě přirozená čísla a, b, viz část 3). Věta 1.2 tedy dává (například) dosud neznámý fakt, že existují libovolně dlouhé aritmetické posloupnosti tvořené součty dvou čtverců. (Např. $37 = 1^2 + 6^2$, $61 = 5^2 + 6^2$, $85 = 9^2 + 2^2$, $109 = 10^2 + 3^2$ je taková posloupnost délky 4.)

2 Důkaz Greenovy a Taovy věty o prvočíslech

Přirozená čísla $\{1, 2, \ldots\}$ označíme $\mathbf{N}$ a množinu $\{1, 2, \ldots, N\}$, pro $N \in \mathbf{N}$, jako $[N]$. Symboly $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ a $\mathbf{C}$ označují množiny celých, racionálních, reálných a komplexních čísel. Je-li A konečná množina, symbol $|A|$ označuje počet jejích prvků (jinak znamená absolutní hodnotu). Aritmetickou posloupností délky k v $\mathbf{N}$ se rozumí k-tice čísel $x + ir$, kde $x, r \in \mathbf{N}$ a $i = 0, 1, \ldots, k-1$. Okruh $\mathbf{Z}/N\mathbf{Z}$ (sčítání a násobení modulo N) označíme $\mathbf{Z}_N$ a jeho prvky reprezentujeme čísly $0, 1, \ldots, N-1$. Pro reálnou funkci $f : A \to \mathbf{R}$ na *konečné* množině A nechť symbol $\mathbf{E}(f)$ označuje *střední hodnotu* $\mathbf{E}(f) = \mathbf{E}(f(x) \mid x \in A) = \frac{1}{|A|}\sum_{x\in A} f(x)$. Nezáporná funkce $\nu : \mathbf{Z}_N \to \mathbf{R}^+$ se nazývá *mírou*, pokud $\mathbf{E}(\nu) = 1 + o(1)$. Symbol $o(1)$, resp. $O(1)$, zde a dále vždy označuje reálnou funkci $e(N)$ hlavního parametru N (velikosti základní množiny $\mathbf{Z}_N$) takovou, že pro $N \to \infty$ máme $e(N) \to 0$, resp. funkce $|e(N)|$ je omezená. Závisí-li tato funkce na dalších parametrech, jsou většinou uvedeny v indexu, např. $o_k(1)$. Symbol $O(F)$, kde F je funkce N, je zkratka pro $O(1)F$, podobně $o(F)$. Parametr $k \geq 3$ je během důkazu pevný a znamená (až na případ k-pseudonáhodnosti) délku aritmetické posloupnosti. Aby se prvky $1, 2, \ldots, k$ daly v $\mathbf{Z}_N$ multiplikativně invertovat, předpokládá se, že N je velké prvočíslo.

Klíčovým nástrojem důkazu věty 1.1 je Szemerédiho [3] věta [46]: *Pro každé reálné $\delta > 0$ a přirozené $k \geq 3$ existuje $N_0 = N_0(\delta, k)$ tak, že pro $N \geq N_0$ a $X \subset [N]$ splňující $|X| \geq \delta N$ množina X nutně obsahuje aritmetickou posloupnost délky k.* Szemerédiho větu lze ekvivalentně přeformulovat následujícím způsobem.

Věta 2.3 (Szemerédiho věta). *Nechť $0 < \delta < 1$, $k \geq 3$ jsou dané konstanty, funkce $f : \mathbf{Z}_N \to \mathbf{R}$ splňuje $0 \leq f(x) \leq 1$ pro každé $x \in \mathbf{Z}_N$ a $\mathbf{E}(f) \geq \delta$. Potom pro každé N platí*

$$\mathbf{E}\Big(\prod_{i=0}^{k-1} f(x+ir) \mid x, r \in \mathbf{Z}_N\Big) \geq c - o_{\delta,k}(1),$$

kde $c = c(k, \delta) > 0$ je kladná konstanta závisející jen na δ a k.

Green a Tao svou větu dokázali ve dvou krocích.

1. Relativní Szemerédiho věta. Z věty 2.3 odvodili Relativní Szemerédiho větu, která říká toto (přesnou formulaci podáme za chvíli): *Pro každé $\delta > 0$ a $k \geq 3$ existuje $N_1 = N_1(\delta, k)$ tak, že jakmile $N \geq N_1$ a $\widetilde{X} \subset \mathbf{Z}_N$ je k-pseudonáhodná množina, každá její podmnožina $X \subset \widetilde{X}$ splňující $|X| \geq \delta|\widetilde{X}|$ obsahuje aritmetickou posloupnost délky k.*

2. Obalení prvočísel pseudonáhodnou množinou. Označme $P = P_N \subset \mathbf{Z}_N$ množinu všech prvočísel menších než N. Green a Tao nalezli způsob, jak krok 1 použít pro prvočísla. Dokázali, že pro každé $k \geq 3$ a dostatečně velké N existuje k-pseudonáhodná množina $\widetilde{P} \subset \mathbf{Z}_N$ a konstanta $\delta = \delta(k) > 0$ tak, že $\widetilde{P} \supset P$ a $|P| \geq \delta|\widetilde{P}|$.

Oba kroky dohromady dávají, že množina prvočísel obsahuje libovolně dlouhé aritmetické posloupnosti. Podívejme se na ně detailněji.

2.1 Relativní Szemerédiho věta

Zformulujme nyní zobecnění Szemerédiho věty, které je jádrem celého důkazu. Od věty 2.3 se liší „pouze“ přidáním k-pseudonáhodné míry ν (definice k-pseudonáhodnosti následuje za větou), která koncentruje funkci f.

[3]Endre Szemerédi (1941) je maďarský matematik, člen Maďarské akademie věd.

Věta 3.5 (Relativní Szemerédiho věta). *Nechť $0 < \delta < 1$, $k \geq 3$ jsou dané konstanty, $\nu : \mathbf{Z}_N \to \mathbf{R}^+$ je k-pseudonáhodná míra a funkce $f : \mathbf{Z}_N \to \mathbf{R}$ splňuje $0 \leq f(x) \leq \nu(x)$ pro každé $x \in \mathbf{Z}_N$ a $\mathbf{E}(f) \geq \delta$. Potom pro každé N platí*

$$\mathbf{E}\Big(\prod_{i=0}^{k-1} f(x+ir) \mid x, r \in \mathbf{Z}_N\Big) \geq c - o_{\delta,k}(1),$$

kde $c = c(k,\delta) > 0$ je kladná konstanta závisející jen na δ a k.

Konstanta c je tatáž v obou větách. Co se rozumí k-pseudonáhodností?

Definice k-pseudonáhodnosti. Míra $\nu : \mathbf{Z}_N \to \mathbf{R}^+$ je *k-pseudonáhodná*, splňuje-li následující dvě podmínky:

Podmínka lineárních funkcí. Nechť $\psi_i(x) = \sum_{j=1}^{t} L_{ij}x_j + b_i$, $i \in [m]$, je m lineárních funkcí o t proměnných, kde $b_i \in \mathbf{Z}_N$, $m \leq k2^{k-1}$, $t \leq 3k-4$ a L_{ij} jsou racionální čísla, jejichž čitatele a jmenovatele v absolutní hodnotě nepřesahují k; L_{ij} chápeme přirozeným způsobem jako prvky $\mathbf{Z}_N$. Předpokládá se, že matice (L_{ij}) nemá nulové řádky a žádný řádek není násobek jiného řádku. Potom (pro každou volbu takových funkcí ψ_i) platí

$$\mathbf{E}\Big(\prod_{i=1}^{m} \nu(\psi_i(x)) \mid x \in \mathbf{Z}_N^t\Big) = 1 + o_k(1).$$

Korelační podmínka. Pro každé přirozené číslo m, $m \leq 2^{k-1}$, existuje váhová funkce $\tau = \tau_m : \mathbf{Z}_N \to \mathbf{R}^+$, jejíž všechny momenty jsou omezené (tj. $\mathbf{E}(\tau^q) = O_{k,q}(1)$ pro každé $q \in \mathbf{N}$) a pro každou m-tici (ne nutně různých) čísel $h_1, \ldots, h_m \in \mathbf{Z}_N$ platí

$$\mathbf{E}\Big(\prod_{i=1}^{m} \nu(x+h_i) \mid x \in \mathbf{Z}_N\Big) \leq \sum_{1 \leq i < j \leq m} \tau(h_i - h_j).$$

Povšimněme si, že definice míry je speciálním případem podmínky lineárních funkcí a že v korelační podmínce máme m lineárních funkcí $x + h_i$, v odpovídající matici se tedy opakuje jediný řádek $L_{11} = L_{21} = \cdots = L_{m1} = 1$.

Struktura důkazu Relativní Szemerédiho věty. Důkaz používá tři výsledky: větu 2.3 a níže uvedená tvrzení 5.3 a 7.1. Větu 2.3 (Szemerédiho větu) Green a Tao nedokazují; pro její důkazy viz [46], [12], [13], [18], [48] a

[49] [4]. Podívejme se na zbylé dva výsledky.

Pro $\omega \in Q_d = \{0,1\}^d$ a $h \in \mathbf{Z}_N^d$ označíme $\omega \cdot h = \omega_1 h_1 + \cdots + \omega_d h_d$. Pro $d \in \mathbf{N}$ a funkci $f : \mathbf{Z}_N \to \mathbf{R}$ definujeme tzv. *Gowersovu normu uniformity* U^d (název zavedený Greenem a Taem)

$$\|f\|_{U^d} = \mathbf{E}\Big(\prod_{\omega \in Q_d} f(x + \omega \cdot h) \mid x \in \mathbf{Z}_N, h \in \mathbf{Z}_N^d \Big)^{1/2^d}.$$

Není těžké vidět, že tato střední hodnota je vždy nezáporná, lze ji tedy umocnit na $1/2^d$ a definice je korektní. Například $\|f\|_{U^1} = (\mathbf{E}(f)^2)^{1/2} = |\mathbf{E}(f)|$; $\|\cdot\|_{U^1}$ je jen seminorma (může být 0 i pro nenulovou funkci f). Lze ukázat, že $\|\cdot\|_{U^d}$ je pro $d \geq 2$ norma.

Tvrzení 5.3 (zobecněná von Neumannova věta). *Nechť jsou dány k-pseudonáhodná míra $\nu : \mathbf{Z}_N \to \mathbf{R}^+$ a k-tice funkcí $f_0, f_1, \ldots, f_{k-1} : \mathbf{Z}_N \to \mathbf{R}$ splňujících $|f_i(x)| \leq 1 + \nu(x)$ pro každé $x \in \mathbf{Z}_N$ a $i = 0, \ldots, k-1$. Potom*

$$\mathbf{E}\Big(\prod_{i=0}^{k-1} f_i(x + ir) \mid x, r \in \mathbf{Z}_N \Big) \leq O\big(\min_{0 \leq i \leq k-1} \|f_i\|_{U^{k-1}}\big) + o(1).$$

Systém $\mathcal{B}$ podmnožin množiny $\mathbf{Z}_N$ se nazývá *σ-algebrou* (na $\mathbf{Z}_N$), jestliže obsahuje množiny $\emptyset$ a $\mathbf{Z}_N$ a je uzavřený vzhledem k operacím průniku, sjednocení a doplňku. *Atomem* $\mathcal{B}$ rozumíme minimální neprázdnou množinu v $\mathcal{B}$. Atomy tvoří rozklad množiny $\mathbf{Z}_N$. *Podmíněná střední hodnota* f vzhledem k $\mathcal{B}$ je, pro danou funkci $f : \mathbf{Z}_N \to \mathbf{R}$ a σ-algebru $\mathcal{B}$, funkce $\mathbf{E}(f \mid \mathcal{B}) : \mathbf{Z}_N \to \mathbf{R}$ definovaná vztahem $\mathbf{E}(f \mid \mathcal{B})(x) = \frac{1}{|A(x)|} \sum_{y \in A(x)} f(y)$, kde $A(x)$ je atom obsahující x (tato funkce je konstantní na každém atomu).

Tvrzení 7.1 (zobecněná Koopman-von Neumannova věta). *Buďte dány $0 < \varepsilon < 1$, k-pseudonáhodná míra $\nu : \mathbf{Z}_N \to \mathbf{R}^+$ a funkce $f : \mathbf{Z}_N \to \mathbf{R}$ splňující $0 \leq f(x) \leq \nu(x)$ pro každé $x \in \mathbf{Z}_N$. Potom pro dostatečně velké N existuje σ-algebra $\mathcal{B}$ na $\mathbf{Z}_N$ a její množina $\Omega \in \mathcal{B}$ tak, že*

1. $\sum_{x \in \Omega} \nu(x) = o_\varepsilon(N)$;

[4] Nový kombinatorický důkaz Szemerédiho věty a jejích zobecnění nalezli nedávno nezávisle V. Rödl a jeho studenti (B. Nagle, M. Schacht, J. Skokan) a T. Gowers. Vojtěch Rödl (1949) je český matematik působící trvale na Emory University v Atlantě v USA. Timothy Gowers (1963) je profesor na Univerzitě v Cambridge ve Velké Británii; v r. 1998 mu byla udělena Fieldsova medaile.

2. $\mathbf{E}(\nu - 1 \mid \mathcal{B})(x) = o_\varepsilon(1)$ *stejnoměrně pro x probíhající $\mathbf{Z}_N\backslash\Omega$;*

3. $\|g - \mathbf{E}(g \mid \mathcal{B})\|_{U^{k-1}} \le \varepsilon^{1/2^k}$, *kde g se rovná f na $\mathbf{Z}_N\backslash\Omega$ a je 0 na Ω.*

Důkaz tvrzení 5.3 má asi 4 strany, využívá Cauchy–Schwarzovu nerovnost a k-pseudonáhodnost ν. Důkaz tvrzení 7.1 zabírá asi 12 stran a objevuje se v něm například klasická Weierstrassova věta o aproximaci spojité funkce polynomy.

Důkaz věty 3.5. Za pomoci tří výše uvedených výsledků je už důkaz snadný (půl strany) a stručně ho naznačíme. Mějme δ, k, ν a f jako ve větě 3.5 a $\varepsilon > 0$ buď libovolné pevné. Tvrzení 7.1 nám (pro daná ε, k, ν, f) poskytne σ-algebru $\mathcal{B}$ a množinu $\Omega \in \mathcal{B}$. Položíme $f = g + h$, kde $g = f - \mathbf{E}(f \mid \mathcal{B})$ a $h = \mathbf{E}(f \mid \mathcal{B})$. Střední hodnotu

$$S = \mathbf{E}\Big(\prod_{i=0}^{k-1} f(x+ir) \mid x, r \in \mathbf{Z}_N\Big)$$

z dokazované věty 3.5 díky linearitě $\mathbf{E}$ vyjádříme jako

$$\begin{aligned} S &= \mathbf{E}\Big(\prod_{i=0}^{k-1} h(x+ir) \mid x, r \in \mathbf{Z}_N\Big) + \sum \mathbf{E}\Big(\prod_{i=0}^{k-1} (g \text{ či } h)(x+ir) \mid x, r \in \mathbf{Z}_N\Big) \\ &= M + E, \end{aligned}$$

kde suma E obsahuje všech $2^k - 1$ sčítanců, v nichž se v součinu alespoň v jednom faktoru objevuje funkce g. Výjimečnou množinu Ω můžeme podle tvrzení 7.1.1 zanedbat. Mimo ni se podle tvrzení 7.1.2 podmíněná střední hodnota $\mathbf{E}(\nu \mid \mathcal{B})$ chová zhruba jako konstantní 1, a M tak můžeme odhadnout obyčejnou Szemerédiho větou 2.3: $M \ge c(k,\delta) - o_{k,\delta,\varepsilon}(1)$. Každý z $2^k - 1$ sčítanců sumy E je malý díky tvrzení 7.1.3 a tvrzení 5.3, a tak $E = O(\varepsilon^{1/2^k}) + o(1)$. Dohromady dostaneme $S \ge c(k,\delta) - O_k(\varepsilon^{1/2^k}) - o_{k,\delta,\varepsilon}(1)$. Protože $\varepsilon > 0$ lze volit libovolné, dolní odhad $\mathbf{E}(\cdot)$ z věty 3.5 je dokázán.

2.2 Obalení prvočísel pseudonáhodnou množinou

Von Mangoldtova funkce $\Lambda : \mathbf{N} \to \mathbf{R}$ a *Möbiova funkce* $\mu : \mathbf{N} \to \{-1, 0, 1\}$ se definují vztahy $\Lambda(n) = \log p$, je-li n mocninou prvočísla p, a $\Lambda(n) = 0$ jinak a $\mu(n) = (-1)^r$, je-li n součinem r různých prvočísel, a $\mu(n) = 0$ jinak (ale $\mu(1) = 1$). Platí identita

$$\Lambda(n) = \sum_{d \mid n} \mu(d) \log(n/d),$$

což je Möbiova inverze identity $\log n = \sum_{d|n} \Lambda(d)$, která plyne hned z definice. *Eulerova funkce* $\varphi :\ \mathbf{N} \to \mathbf{N}$ daná formulí $\varphi(n) = n(1-1/p_1)\dots(1-1/p_r)$, kde p_i jsou prvočísla dělící n, udává počet čísel $m \in \mathbf{N}, m \leq n$, nesoudělných s n. Symbol p bude vždy označovat prvočíslo.

Z Prvočíselné věty (počet prvočísel menších než x je asymptoticky $x/\log x$) plyne, že $\mathbf{E}(\Lambda(n) \mid n \in \mathbf{Z}_N) = 1 + o(1)$. Kdyby existovala k-pseudonáhodná míra ν a konstanta $c = c(k) > 0$ tak, že $\nu(n) \geq c\Lambda(n)$ pro každé $n \in \mathbf{Z}_N$, věta 3.5 by okamžitě implikovala Greenovu-Taovu větu (protože $\mathbf{E}(c\Lambda) = c + o(1) \geq \delta > 0$ pro velká N a čísla tvaru $n = p^r$ s $r \geq 2$ lze zanedbat). Taková míra ν však neexistuje. Pro $q \in \mathbf{N}$ totiž ν musí být rozdělena zhruba rovnoměrně mezi q zbytkových tříd modulo q, kdežto Λ je koncentrována na $\varphi(q)$ třídách nesoudělných s q. Protože $\liminf \varphi(q)/q = 0$, pro velká N kýžená majorizace nemůže platit. Jednoduchá strategie „nalezni k-pseudonáhodnou míru ν majorizující až na konstantní faktor funkci Λ“ tedy nefunguje.

Tuto potíž Green a Tao obešli tzv. W-trikem. Nechť $w = w(N)$ je pomalu rostoucí funkce (stačí např. $w = \log\log\log N$) a nechť

$$W = W(N) = \prod_{p \leq w} p.$$

Modifikovaná funkce Λ je definována vztahem

$$\widetilde{\Lambda}(n) = \begin{cases} \frac{\varphi(W)}{W}\log(Wn+1) & \text{je-li } Wn+1 \text{ prvočíslo,} \\ 0 & \text{jinak.} \end{cases}$$

Všimněme si, že pokud n probíhá aritmetickou posloupnost, probíhá ji i $Wn+1$. Takto pozměněná Λ už má k-pseudonáhodnou majorantu.

Tvrzení 8.1. *Nechť* $\varepsilon_k = \frac{1}{2^k(k+4)!}$ *a* N *je dostatečně velké prvočíslo. Potom existuje* k*-pseudonáhodná míra* $\nu :\ \mathbf{Z}_N \to \mathbf{R}^+$ *tak, že*

$$\nu(n) \geq \frac{1}{k2^{k+5}}\widetilde{\Lambda}(n)$$

platí pro každé n *z intervalu* $\varepsilon_k N \leq n \leq 2\varepsilon_k N$.

Z věty 3.5 a tvrzení 8.1 už Greenova-Taova věta plyne jednoduše. (Čtenáře možná napadnou dva technické problémy. 1. Chceme aritmetickou posloupnost v $\mathbf{N}$ a ne pouze v $\mathbf{Z}_N$. To je právě „ošetřeno“ omezením n na interval $[\varepsilon_k N, 2\varepsilon_k N]$. 2. Nechceme „degenerované“ aritmetické posloupnosti typu $x + ir$, $0 \leq i \leq k-1$, $r = 0$. Ty však do $\mathbf{E}(\cdot)$ ve větě 3.5 přispívají pouze $O(\log^k N/N) = o(1)$ a nemají žádný vliv.)

Jak je míra ν z tvrzení 8.1 definována?

Definice majoranty. *Zkrácená von Mangoldtova funkce* $\Lambda_R(n)$, kde $R > 0$ je parametr, je definována vztahem

$$\Lambda_R(n) = \sum_{d|n, d\le R} \mu(d)\log(R/d) = \sum_{d|n}\mu(d)\log_+(R/d),$$

kde $\log_+ x = \max(0, \log x)$. Funkci Λ_R zkoumali Goldston a Yildirim ([15], [16], [17]) v souvislosti s odhady mezer mezi prvočísly.

Definice 8.3. *Nechť* $R = N^{k^{-1}2^{-k-4}}$ *a* ε_k *je jako výše. Funkci* $\nu : \mathbf{Z}_N \to \mathbf{R}^+$ *definujeme formulí*

$$\nu(n) = \begin{cases} \frac{\varphi(W)}{W}\cdot\frac{1}{\log R}\cdot\Lambda_R(Wn+1)^2 & \textit{pro } n\in[\varepsilon_k N, 2\varepsilon_k N], \\ 1 & \textit{jinak.}\end{cases}$$

O takto definované funkci Green a Tao ukázali, že má vlastnost majoranty z tvrzení 8.1 (lemma 8.4), že je mírou (lemma 8.7) a že je k-pseudonáhodná (tvrzení 8.8 a 8.10). Tím jsme dokončili přehled důkazu věty 1.1. Nyní popíšeme, jak Green a Tao dokázali k-pseudonáhodnost ν.

Jak sami uvádějí, obvyklé postupy z teorie sít (sieve theory), které se snažili aplikovat, se ukazovaly jako nedostatečně mocné. Pak jim A. Granville poradil, aby zkusili použít novou metodu pro odhady funkce Λ_R pomocí komplexní integrace, kterou vyvinuli D. Goldston a C. Yildirim [5] při výzkumu velikosti mezer mezi prvočísly. Green a Tao zjistili, že Goldstonova-Yildirimova metoda se přesně hodí pro získání asymptotik součinů čtverců funkce Λ_R, které jsou zapotřebí k důkazu k-pseudonáhodnosti majoranty.

Důkaz k-pseudonáhodnosti majoranty ν metodou Goldstona a Yildirima.

Tvrzení 8.5 (Goldston a Yildirim). *Uvažme* m *lineárních funkcí* $\psi_i(x) = \sum_{j=1}^t L_{ij}x_j + b_i$, $i \in [m]$, *o* t *proměnných, kde* L_{ij} *a* b_i *jsou celá čísla, přičemž* $|L_{ij}| \le \frac{1}{2}w(N)^{1/2}$ *a matice* (L_{ij}) *nemá nulové řádky a žádný řádek není násobek jiného. Nechť* $B = I_1\times\ldots\times I_t$, *kde* $I_i \subset \mathbf{R}$ *je* t *intervalů, každý o délce alespoň* R^{10m}. *Potom pro dostatečně pomalu rostoucí funkci* $w(N)$ *platí*

$$\mathbf{E}\Big(\prod_{i=1}^m \Lambda_R(W\psi_i(x)+1)^2 \mid x\in B\cap\mathbf{Z}^t\Big) = (1+o_{m,t}(1))\Big(\frac{W\log R}{\varphi(W)}\Big)^m.$$

[5]Daniel Goldston (1954) je profesorem na San José State University v Kalifornii v USA. Cem Yalçın Yıldırım (1961) působí na Bogaziçi University v Istanbulu v Turecku.

Podmínka lineárních funkcí pro ν (jakož i vlastnost $\mathbf{E}(\nu) = 1 + o(1)$) se dostane aplikací tvrzení 8.5. Podobné tvrzení 8.6, které v tomto přehledu neuvádíme, se použije pro důkaz korelační podmínky.

V důkazu tvrzení 8.5 se výše uvedená střední hodnota vyjádří (až na malou chybu) pomocí integrálů (nadále $i = \sqrt{-1}$) jako

$$\begin{aligned} &\frac{1}{(2\pi i)^m}\int_{\Gamma_1}\cdots\int_{\Gamma_1} F(z,u)\prod_{j=1}^{m}\frac{R^{z_j+u_j}}{z_j^2u_j^2}\,dz_j\,du_j \\ = \;&\frac{1}{(2\pi i)^m}\int_{\Gamma_1}\cdots\int_{\Gamma_1}\left(\sum_{d,e\in\mathbf{N}^m}\prod_{j=1}^{m}\frac{\mu(d_j)\mu(e_j)}{d_j^{z_j}e_j^{u_j}}\prod_p M_{d,e}(p)\right)\prod_{j=1}^{m}\frac{R^{z_j+u_j}}{z_j^2u_j^2}\,dz_j\,du_j, \end{aligned}$$

kde $2m$-krát komplexně integrujeme po dráze $\Gamma_1 = \{\frac{1}{\log R} + i\tau:\ \tau\in\mathbf{R}\}$, $z = z_1,\dots,z_m$ a $u = u_1,\dots,u_m$ je $2m$ komplexních proměnných, $d = d_1,\dots,d_m$ a $e = e_1,\dots,e_m$ jsou m-tice přirozených čísel, a

$$M_{d,e}(p) = \frac{1}{p^t}\cdot|\{x\in\mathbf{Z}_p^t:\ \forall j\in[m]\ p|d_je_j \Rightarrow W\psi_j(x)+1=0\}|.$$

(Pro pevné d,e je $M_{d,e}(p)\neq 1$ jen pro konečně mnoho prvočísel p.) Při této transformaci se využije definice funkce Λ_R, záměna pořadí sumace a integrální reprezentace funkce $\log_+$ (vystupující v definici Λ_R):

$$\log_+ x = \frac{1}{2\pi i}\int_\Gamma \frac{x^z}{z^2}\,dz$$

pro každé reálné $x > 0$ a přímku $\Gamma = \{\alpha + i\tau:\ \tau\in\mathbf{R}\}$, $\alpha > 0$. (Tento integrál se snadno spočte pomocí reziduí a integrace přes dostatečně velký obdélník s jednou stranou na Γ.)

Pro reálné $\sigma > 0$ označme $D_\sigma^m = \{(z,u)\in\mathbf{C}^{2m}:\ -\sigma < \mathrm{Re}(z_j), \mathrm{Re}(u_j) < 100, j\in[m]\}$. Pro funkci $G = G(z,u)$ $2m$ proměnných, holomorfní v oblasti D, nechť $V_l(G,D)$ označuje největší supremum $\sup_{z,u\in D}|\partial G(z,u)|$, kde ∂G probíhá parciální derivace G řádu nejvýše l. Funkce $F(z,u)$, vystupující ve výše uvedeném $2m$-násobném integrálu, se pomocí eulerovských součinů přes prvočísla faktorizuje jako $F = G_1G_2G_3$, kde

$$G_3(z,u) = \prod_{j=1}^{m}\prod_p\frac{(1-p^{-1-z_j})(1-p^{-1-u_j})}{1-p^{-1-z_j-u_j}} = \prod_{j=1}^{m}\frac{\zeta(1+z_j+u_j)}{\zeta(1+z_j)\zeta(1+u_j)}$$

($\zeta(s) = \prod_p (1-p^{-s})^{-1} = \sum_{n\geq 1} n^{-s}$ je klasická Eulerova–Riemannova dzeta funkce). Takže G_3 je holomorfní pro $\mathrm{Re}(z_j), \mathrm{Re}(u_j) > 0$. Funkce G_1 a G_2 jsou dány složitějšími eulerovskými součiny, ale zato jsou holomorfní i trochu nalevo od 0, totiž v $D = D^m_{1/6m}$, a splňují $G_1(0,0) = 1 + o_m(1)$, $G_2(0,0) = (W/\varphi(W))^m$, $V_m(G_1, D) \leq O_m(1)$ a $V_m(G_2, D) \leq w(N)^{O_m(w(N))}$ (lemma 9.3). Výše uvedený $2m$-násobný integrál, počítající $\mathbf{E}(\cdot)$ z tvrzení 8.5, Green a Tao nakonec spočítali pomocí následujícího lemmatu, které také připsali Goldstonovi a Yildirimovi v [17].

Lemma 9.4. *Nechť $G(z,u)$ je funkce $2m$ komplexních proměnných závisející i na reálném parametru $N > 0$, která je holomorfní v $D = D^m_\sigma$ pro nějaké $\sigma > 0$ a splňuje odhad $V_m(G,D) = \exp(O_{m,\sigma}(\log^{1/3} R))$ [6] . Potom*

$$\begin{aligned} &\frac{1}{(2\pi i)^m} \int_{\Gamma_1} \cdots \int_{\Gamma_1} G(z,u) \prod_{j=1}^{m} \frac{\zeta(1+z_j+u_j)}{\zeta(1+z_j)\zeta(1+u_j)} \frac{R^{z_j+u_j}}{z_j^2 u_j^2}\, dz_j\, du_j \\ = \quad & G(0,0)\log^m R + \sum_{j=1}^{m} O_{m,\sigma}(V_j(G,D)\log^{m-j} R) + O_{m,\sigma}(\mathrm{e}^{-\delta\sqrt{\log R}}) \end{aligned}$$

pro nějaké $\delta = \delta(m) > 0$.

Hledaná asymptotika pak plyne aplikací lemmatu 9.4 na $G = G_1 G_2$ a $\sigma = 1/6m$. (Protože $R = N^{k^{-1}2^{-k-4}}$ a $w(N)$ roste pomalu, předpoklad lemmatu 9.4 o $V_m(G,D)$ je splněn a $G(0,0)\log^m R$ je řádově větší než další členy.) Důkaz lemmatu 9.4 probíhá indukcí podle m a zabírá v Appendixu preprintu [21] asi 4 strany. Používá reziduí, deformací integrační dráhy a standardního výsledku o oblasti v $\mathbf{C}$ bez nulových bodů funkce $\zeta(s)$ (ten je zapotřebí kvůli ζ ve jmenovateli integrandu). [7]

3 Stručná historie výzkumu prvočísel

Prvočísly se lidé zabývají již od antiky a objevování jejich vlastností je jedním z nejkrásnějších a nejvýznamnějších odvětví matematiky. Praktická důležitost prvočísel pro kryptografii a přenos informace však byla objevena až nedávno, v 70-tých letech 20. století. Uveďme některé nejvýznamnější milníky historie jejich výzkumu. Greenova-Taova věta je jistě jedním z nich.

[6] $R = R(N)$ je funkce N. Lemma se použije s R definovaným v definici 8.3.

[7] V září 2004 Tao v [51] přišel se zjednodušeným důkazem tvrzení 8.5, který už vůbec nepotřebuje tyto vlastnosti $\zeta(s)$.

• Euklides ve 4. století před Kristem uvedl ve svých „Základech" důkaz nekonečnosti počtu prvočísel ([2]).

• P. de Fermat (1601–1665) v r. 1640 vyslovil větu: Je-li p prvočíslo, pak p dělí $n^p - n$ pro všechna $n \in \mathbf{N}$. Tuto tzv. Malou Fermatovu větu v r. 1736 dokázal Euler ([8], [36]).

• L. Euler (1707–1783) též dokázal další Fermatovo tvrzení, že každé prvočíslo tvaru $4n+1$ je součet dvou čtverců ([8]). Dále odvodil identitu $\prod_p (1-p^{-s})^{-1} = \sum_{n\geq 1} n^{-s}$ (platí pro $s > 1$, dokonce pro $\mathrm{Re}(s) > 1$) a ukázal, že řada $\sum_p p^{-1}$ diverguje.

• C. F. Gauss (1777–1855) v r. 1794 ukázal, že pro každé prvočíslo p tvaru $2^{2^n} + 1$ lze sestrojit pravidelný p-úhelník pravítkem a kružítkem ([25], [26], [45]). V r. 1796 nalezl důkaz zákona kvadratické reciprocity a snad ještě dříve empiricky odvodil Prvočíselnou větu: $\pi(x) \sim x/\log x$ či přesněji $\pi(x) \sim \mathrm{li}(x) = \int_2^x (dt/\log t)$ ([14]). (Symbol $\pi(x)$ tradičně označuje počet prvočísel nepřesahujících x.)

• P. Dirichlet (1805–1859) v r. 1837 dokázal, že pro každá dvě nesoudělná čísla $a, m \in \mathbf{N}$ (nekonečná) aritmetická posloupnost $\{a+im : i = 0, 1, 2, \ldots\}$ obsahuje nekonečně mnoho prvočísel ([6], [33], [42], [52]).

• P. L. Čebyšev (1824–1894) v r. 1852 dokázal slabou formu Prvočíselné věty: Pro $x \geq 2$ a dvě kladné konstanty c_1, c_2 platí $c_1 x/\log x < \pi(x) < c_2 x/\log x$ ([14], [33], [52]).

• B. Riemann (1826–1866) v r. 1859 publikoval přelomovou práci [39], v níž načrtl komplexně-analytickou metodu důkazu Prvočíselné věty a k níž se váže slavná *Riemannova hypotéza*, jeden z nejznámějších otevřených matematických problémů současnosti: pokud $\zeta(s) = 0$ a $\mathrm{Re}(s) > 0$, pak $\mathrm{Re}(s) = 1/2$ ([39], [7]).

• J. Hadamard (1865–1963) a Ch. de la Vallée Poussin (1866–1962) v r. 1896 nezávisle na sobě podali pomocí metod komplexní analýzy první důkaz Prvočíselné věty ([7], [14], [52], [54]).

• V. Brun (1882–1978) v období po 1. světové válce průkopnickými pracemi vytvořil novou číselně-teoretickou disciplínu, metody síta. Podařilo se mu např. dokázat, že existuje nekonečně mnoho dvojic čísel $n, n+2$ takových, že obě mají nejvýše 9 prvočinitelů (počítaných s násobností) ([3], [20]).

• L. G. Šnirelman (1905–1938) r. 1930 publikoval větu, podle níž je každé přirozené číslo n, $n \geq 2$, součtem omezeně mnoha prvočísel ([47], [44], [32]).

• I. M. Vinogradov (1891–1983) v r. 1937 dokázal, že každé dostatečně velké liché číslo je součtem tří prvočísel ([53], [19], [32]).

• P. Erdős (1913–1996) a A. Selberg (1917) v r. 1949 nalezli elementární důkaz Prvočíselné věty nepoužívající komplexní analýzu ([9], [41], [28], [33], [34]).

• Jin-run Chen (1933–1996) v r. 1966 dokázal, že existuje nekonečně mnoho prvočísel p tak, že $p+2$ je také prvočíslo nebo součin dvou prvočísel ([23], [24], [32]).

• Ju. V. Matijasevič (1947) v r. 1970 vyřešil Desátý Hilbertův problém (ukázal, že řešitelnost celočíselné polynomiální rovnice celými čísly je algoritmicky nerozhodnutelná úloha). Z jeho řešení plyne, že existuje celočíselný polynom $P(x_1, \ldots, x_r)$ tak, že množina $\mathbf{N} \cap P(\mathbf{N}^r)$ je právě množina prvočísel ([29], [30], [5], [31]).

• V. R. Pratt (1944) v r. 1975 ukázal, že vlastnost „být prvočíslo" patří v teorii složitosti do třídy tzv. NP problémů ([37], [4], [35]).

• M. Rabin (1931) v r. 1976 navrhl polynomiální pravděpodobnostní algoritmus pro testování prvočíselnosti ([38], [4], [27], [35]).

• R. Rivest (1947), A. Shamir (1952) a L. Adleman (1945) v r. 1978 publikovali kryptografický systém s veřejným klíčem, později podle jejich iniciál nazvaný RSA systémem, založený na obtížnosti faktorizace čísel na prvočísla ([4], [35], [40]).

• P. Shor (1959) v r. 1994 předložil kvantový polynomiální algoritmus pro faktorizaci přirozených čísel na prvočísla ([43], [4]).

• J. Friedlander (?) a H. Iwaniec (1947) v r. 1998 ukázali, že existuje nekonečně mnoho prvočísel tvaru $x^2 + y^4$, $x, y \in \mathbf{N}$ ([10] a [11]).

• D. R. Heath-Brown (1952) v r. 2001 ukázal, že existuje nekonečně mnoho prvočísel tvaru $x^3 + 2y^3$, $x, y \in \mathbf{N}$ ([22]).

• M. Agrawal (1966), N. Kayal (?) a N. Saxena (1981) v r. 2002 společně nalezli první deterministický polynomiální algoritmus pro testování prvočíselnosti ([1]).

Poděkování. Tato práce vznikla díky podpoře grantu LN00A056 Ministerstva školství, mládeže a tělovýchovy ČR.

Reference

[1] Agrawal, M., Kayal, N., Saxena, N.: *PRIMES is in P*, `http://www.cse.iitk.ac.in/news/primality.html`

[2] Bečvářová, M.: *Eukleidovy Základy. Jejich vydání a překlady.* Prometheus, Praha 2002.

[3] Brun, V.: *Le crible d'Eratosthène et le théorème de Goldbach.* C. R. Acad. Sci. Paris *168* (1919), 544–546.

[4] Crandall, R., Pomerance, C.: *Prime Numbers. A Computational Perspective.* Springer-Verlag, New York 2001.

[5] Davis, M.: *Hilbert's tenth problem is unsolvable.* Amer. Math. Monthly *80* (1973), 233–269.

[6] Dirichlet, P. G. L.: *Beweis des Satzes, daß jede unbegrenzte aritmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.* Abh. Akad. Berlin (1837), 45–71.

[7] Edwards, H. M.: *Riemann's zeta function.* Academic Press, New York-London 1974.

[8] Edwards, H. M.: *Fermat's last theorem. A genetic introduction to algebraic number theory.* Springer-Verlag, New York 1977.

[9] Erdős, P.: *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem.* Proc. Nat. Acad. Sci. U. S. A. *35* (1949), 374–384.

[10] Friedlander, J., Iwaniec, H.: *Asymptotic sieve for primes.* Ann. of Math. (2) *148* (1998), 1041–1065.

[11] Friedlander, J., Iwaniec, H.: *The polynomial* $X^2 + Y^4$ *captures its primes.* Ann. of Math. (2) *148* (1998), 945–1040.

[12] Furstenberg, H.: *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions.* J. Analyse Math. *31* (1977), 204–256.

[13] Furstenberg, H., Katznelson, Y., Ornstein, D.: *The ergodic theoretical proof of Szemerédi's theorem.* Bull. Amer. Math. Soc. (N.S.) *7* (1982), 527–552.

[14] Goldstein L. J.: *A history of the prime number theorem.* Amer. Math. Monthly *80* (1973), 599–615.

[15] Goldston, D., Yildirim, C. Y.: *Higher correlations of divisor sums related to primes, I: Triple correlations.* Integers *3* (2003), 66 s.

[16] Goldston, D., Yildirim, C. Y.:*Higher correlations of divisor sums related to primes, III: k-correlations.* arXiv:math.NT/0209102, 32 s.

[17] Goldston, D., Yildirim, C. Y.: *Small gaps between primes.* preprint.

[18] Gowers, W. T.: *A new proof of Szemerédi's theorem.* Geom. Funct. Anal. *11* (2001), 465–588.

[19] Gowers, T., *Vinogradov's Three-Primes Theorem,* 17 s.
`http://www.dpmms.cam.ac.uk/~wtg10/`

[20] Greaves, G.: *Sieves in number theory.* Springer-Verlag, Berlin 2001.

[21] Green, B., Tao, T.: *The primes contain arbitrarily long arithmetic progressions.* arXiv:math.NT/0404188 (verze 1 z 8. dubna 2004), 49 s.

[22] Heath-Brown, D. R.: *Primes represented by* x^3+2y^3. Acta Math. *186* (2001), 1–84.

[23] Chen, J.: *On the representation of a large even integer as the sum of a prime and the product of at most two primes.* Kexue Tongbao *17* (1966), 385–386.

[24] Chen, J.: *On the representation of a large even integer as the sum of a prime and the product of at most two primes.* Sci. Sinica *16* (1973), 157–176.

[25] Křížek, M., *Od Fermatových prvočísel ke geometrii.* In: Šolcová, A., Křížek, M., Mink, G., editoři, *Matematik Pierre de Fermat. Cahiers du CEFRES č. 28,* 131–161. CEFRES, Praha 2002.

[26] Křížek, M., Luca, F., Somer, L.: *17 lectures on Fermat numbers. From number theory to geometry.* Springer-Verlag, New York 2001.

[27] Kučera, L.: *Kombinatorické algoritmy.* SNTL, Praha 1983.

[28] Levinson, N.: *A motivated account of an elementary proof of the prime number theorem.* Amer. Math. Monthly *76* (1969), 225–245.

[29] Matijasevič, Ju. V.: *Diofantovosť perečislimych množestv.* Dokl. Akad. Nauk SSSR *191* (1970), 279–282.

[30] Matijasevič, Ju. V.: *Diofantovo predstavlenie množestva prostych čisel.* Dokl. Akad. Nauk SSSR *196* (1971), 770–773.

[31] Matijasevič, Ju. V.: *Hilbert's tenth problem.* MIT Press, Cambridge, MA 1993.

[32] Nathanson, M. B.: *Additive Number Theory. The Classical Bases.* Springer-Verlag, New York 1996.

[33] Nathanson, M. B.: *Elementary Methods in Number Theory.* Springer-Verlag, New York 2000.

[34] Novák, B.: *O elementárním důkazu prvočíselné věty.* Časopis pro pěstování matematiky *100* (1975), 71–84.

[35] Papadimitriou, Ch. H.: *Computational Complexity.* Addison-Wesley, Reading, MA 1994.

[36] Porubský, Š., *Fermat a teorie čísel.* In: Šolcová, A., Křížek, M., Mink, G., editoři, *Matematik Pierre de Fermat. Cahiers du CEFRES č. 28,* 49–86. CEFRES, Praha 2002.

[37] Pratt, V. R.: *Every prime has a succinct certificate.* SIAM J. Comput. *4* (1975), 214–220.

[38] Rabin, M. O.: *Probabilistic Algorithms.* In: J. F. Traub, editor, *Algorithms and Complexity,* 21–39. Academic Press, New York 1976.

[39] Riemann, B.: *Über die Anzahl der Primzahlen unter einer gegebenen Grösse.* Monatsberichte der Berliner Akademie (1859), 671–680.

[40] Rivest, R., Shamir, A., Adleman, L.: *A method for obtaining digital signatures and public-key cryptosystems.* Comm. ACM *21* (1978), 120–126.

[41] Selberg, A.: *An elementary proof of the prime-number theorem.* Ann. of Math. (2) *50* (1949), 305–313.

[42] Serre, J.-P.: *A Course in Arithmetics.* Springer-Verlag, New York 1973.

[43] Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994),* 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA 1994.

[44] Schnirelmann, L.: *Über additive Eigenschaften von Zahlen.* Mat. Annalen *107* (1933), 649–690.

[45] Stillwell, J.: *Elements of algebra. Geometry, numbers, equations.* Springer-Verlag, New York 1994.

[46] Szemerédi, E.: *On sets of integers containing no k elements in arithmetic progression.* Acta Arith. *27* (1975), 199–245.

[47] Šnirel'man, L. G.: *Ob additivnych svojstvach čisel.* Izvestija donskogo politechničeskogo instituta v Novočerkasske *14* (1930), 3–28.

[48] Tao, T.: *A quantitative ergodic theory proof of Szemerédi's theorem.* arXiv:math.CO/0405251, 51 s.

[49] Tao, T.: *A quantitative ergodic theory proof of Szemerédi's theorem (abridged),* 20 s. `http://www.math.ucla.edu/~tao/preprints/`

[50] Tao, T.: *A bound for progressions of length k in the primes,* 4 s. `http://www.math.ucla.edu/~tao/preprints/`

[51] TAO, T.: *A remark on Goldston-Yildirim correlation estimates,* 8 s. http://www.math.ucla.edu/~tao/preprints/

[52] TENENBAUM, G.: *Introduction to analytic and probabilistic number theory.* Cambridge University Press, Cambridge, U.K. 1995.

[53] VINOGRADOV, I. M.: *Predstavlenie nečotnogo čisla summoj trjoch prostych čisel.* Dokl. Akad. Nauk SSSR *15* (1937), 291–294.

[54] ZAGIER, D.: *Newman's short proof of the prime number theorem.* Amer. Math. Monthly *104* (1997), 705–708.

[55] http://www.arxiv.org/