Učitel matematiky

Tomáš Kepka; A. Jančařík; Jakub Michal

Aritmetika III – změny číslic vedoucí k prvočíslům aneb variace na Bertrandův postulát

Učitel matematiky, Vol. 30 (2022), No. 2, 77–91

Persistent URL: http://dml.cz/dmlcz/150455

ARITMETIKA III – ZMĚNY ČÍSLIC VEDOUCÍ K PRVOČÍSLŮM ANEB VARIACE NA BERTRANDŮV POSTULÁT

Tomáš Kepka, Antonín Jančařík, Jakub Michal

Úvod

Dělitelnost patří mezi základní témata, se kterými se žáci seznamují již od základní školy. Přitom některé otázky spojené s dělitelností a prvočísly představují jedny z nejtěžších problémů matematiky a mnohé z nich zůstávají stále otevřené. Důkaz, že prvočísel je nekonečně mnoho, je jednoduchý, a tak je možné s ním žáky seznámit. Na druhou stranu otázku počtu prvočíselných dvojčat lze stejně snadno zformulovat, zůstává však stále otevřená. V tomto článku je naším cílem představit čtenářům poznatky, které jsou spojeny s otázkou, jak častá jsou v posloupnosti prvočísla, přesněji jak blízko ke zvolenému číslu již můžeme nalézt nějaké prvočíslo.

Základní značení a úvodní pozorování

V celém článku pracujeme s nezápornými celými čísly, jejichž množinu označíme symbolem $\mathbb{N}_0$. Kladná čísla pak symbolem $\mathbb{N}$. Je tedy $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Čísla budou zapsána v desítkové číselné soustavě. To připomínáme proto, že předkládané úlohy jsou závislé na zvoleném základu číselné soustavy.

Připomeňme tedy, co rozumíme zápisem a rozvojem čísla v soustavě o základu deset. Buď $n \in \mathbb{N}_0$. Pak existují jednoznačně určená k, $a_0, \ldots, a_k \in \mathbb{N}_0$ taková, že $0 \leq a_0, \ldots, a_k \leq 9$ (čili tato čísla odpovídají číslicím v desítkové soustavy), $a_k \geq 1$ pro $k \geq 1$, a $n = \sum_{i=0}^{k} a_i \cdot 10^i$, tento součet nazýváme rozvojem čísla

v desítkové soustavě. Píšeme $n = a_k \dots a_0$ a tento zápis nazýváme zápisem čísla v desítkové soustavě. Označíme $\lambda(n) = k + 1$ (o čísle n říkáme, že je $\lambda(n)$-ciferné; jednociferná jsou všechna čísla $0, 1, \dots, 9$, dvojciferná jsou čísla $10, 11, \dots, 99$, atd.).

O čísle $m = b_k \dots b_0$, $\lambda(m) = k + 1$ řekneme, že je blizoučké k číslu n, jestliže $a_i \neq b_i$ nejvýše pro jeden index $i, 0 \leq i \leq k$. Tedy buďto $m = n$, nebo číslo m vznikne z čísla n změnou právě jedné číslice (jelikož je $\lambda(m) = \lambda(n)$, tak pro $k \geq 1$ lze první číslici zleva, tj. a_k, změnit pouze na jinou nenulovou číslici).

Blizoučká čísla mají (v desítkovém zápise) stejný počet číslic. Tak například k jednocifernému číslu je blizoučké opět jen jednociferné číslo. K číslu 100 jsou blizoučká čísla 100, 101, ..., 109, 110, 120, ..., 190, 200, 300, ..., 900, tedy celkem $27 (= 3^3)$ různých čísel. Je-li číslo n l-ciferné, $l \geq 1$, pak počet čísel m blizoučkých číslu n je 10 pro $l = 1$ a $9l$ pro $l \geq 2$.

A teď již k naší hlavní úloze. Označme A množinu všech (nezáporných) čísel, která jsou blizoučká k alespoň jednomu prvočíslu. Ihned z definice vyplývá, že v množině A se ocitnou všechna prvočísla a také všechna čísla $0, 1 \dots, 9$. Jednociferná čísla jsou přece blizoučká k prvočíslu 2 (nebo $3, 5, 7$). Pokračujme v úvaze započaté v předchozím odstavci a sepišme si všechna dvojciferná prvočísla. Jsou to: 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 (je vhodné umět tento seznam nazpaměť). Buď $n = 10a + b, 1 \leq a \leq 9, 0 \leq b \leq 9$ dvojciferné číslo. Z předchozích výčtů dvojciferných prvočísel je patrné, že s výjimkou $n = 97$, lze z n vytvořit prvočíslo změnou číslice b (a to i v případě, že již n samo bylo prvočíslo). Ovšem, 97 je již prvočíslo. Nicméně 67 je prvočíslo též a je blizoučké k 97.

Zjistili jsme, že v množině A se ocitají všechna (nejvýše) dvojciferná čísla. Postupme k trojciferným číslům $n = 100 + 10a + b, 0 \leq a, b \leq 9$.

Máme $100 \leq n \leq 199$ a v tomto intervalu nacházíme tato prvočísla: 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199. Tudíž, pro $n \neq 113, 127, 149, 181$, lze změnou číslice b získat prvočíslo. Vyjmenovaná čísla jsou vesměs prvočísla. (Nicméně, i v jejich případě

je možné změnou číslice a dostat nové prvočíslo; $113 \to 103$, $127 \to 137$, $149 \to 139$, $181 \to 101$.) Je $n \in A$.

Buď $n = 200 + 10a + b, 0 \leq a, b \leq 9$. V intervalu $200, \ldots, 299$ jsou tato prvočísla: 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293. Takže je-li $a \geq 1$ a $n \neq 211, 241, 293$ (což jsou prvočísla), pak vhodnou změnou číslice b dostaneme prvočíslo. (Pro prvočísla 241, 293 lze změnit číslici a; $241 \to 251$, $293 \to 223$.) Zbyla nám čísla 200, ..., 209. Rozložme si tato čísla na součin prvočísel. Dostaneme $200 = 2^3 \cdot 5^2$, $201 = 3 \cdot 67$, $202 = 2 \cdot 101$, $203 = 7 \cdot 29$, $204 = 2^2 \cdot 3 \cdot 17$, $205 = 5 \cdot 41$, $206 = 2 \cdot 103$, $207 = 3^2 \cdot 23$, $208 = 2^4 \cdot 13$, $209 = 11 \cdot 19$ ($210 = 2 \cdot 3 \cdot 5 \cdot 7$ a čísla 199, 211 jsou prvočísla). To znamená, že je-li $200 \leq n \leq 209$, pak žádnou změnou číslice b nelze získat prvočíslo. U čísel 201, 203, 207, 209 lze však změnit číslici a: $201 \to 211$, $203 \to 223$, $207 \to 227$, $209 \to 229$ (a nebo číslici 2, $201 \to 101$, $203 \to 103$, $207 \to 107$, $209 \to 109$). A nakonec zbývají $n = 200, 202, 204, 205, 206, 208$. U sudých n, ať už změnou číslice a, či (první) číslice 2 vždy dostaneme sudé číslo. A u $n = 205$ vždy vyjde násobek prvočísla 5. Tedy $200, 202, 204, 205, 206, 208 \notin A$.

Poučení: $0, 1, 2, \ldots, 199, 201, 203, 207, 209, 210, \ldots, 299 \in A$; $200, 202, 204, 205, 206, 208 \notin A$. Jako cvičení si můžete zkusit spočítat, že $209, \ldots, 319, 321, 323, 327, 329 \in A$ a $320, 322, 324, 325, 326, 328 \notin A$. Postup je obdobný předchozímu.

Množina A je nekonečná, neboť obsahuje všechna prvočísla. Množina A však také obsahuje nekonečně mnoho nezáporných celých čísel, která nejsou prvočísla.

Nechť je p prvočíslo, $p \geq 11$. Desítkový zápis prvočísla p budiž $p = a_l \ldots a_0$, kde $l \geq 1$, $1 \leq a_l \leq 9$, $0 \leq a_0 \leq 9$. Jelikož p je číslo liché, tak $a_0 \neq 0, 2, 4, 6, 8$. Jelikož 5 nedělí p, tak $a_0 \neq 5$. Tudíž $a_0 = 1, 3, 7, 9$. Je-li $n = p - 1$, pak $n = a_l \ldots a_1 b_0$, $b_0 = a_0 - 1$, $b_0 = 0, 2, 6, 8$; n není prvočíslo a $n \in a$. Je-li $a_0 \neq 9$, pak také $n + 1 \in A$, přičemž $p + 1$ není prvočíslo.

Buď $B = \mathbb{N}_0 \setminus A$ (tj. $B = \{n | n \in \mathbb{N}_0, n \notin A\}$. Již jsme si všimli, že 200, 202, 204, 205, 206, $208 \in B$, čili množina B je neprázdná. Číslo 200 je nejmenší číslo z množiny B. O něco později se dozvíme, že množina B je také nekonečná!

Bertrandův postulát

V článku (Bertrand, 1845) uveřejněném více než před 175 lety francouzský matematik J. Bertrand napsal: „Abych tuto větu dokázal, připustím jako fakt, že pro každé číslo n větší než 6 existuje vždy alespoň jedno prvočíslo mezi $n-2$ a $\frac{n}{2}$. Tato věta platí pro všechna čísla menší než 6 milionů a vše nasvědčuje tomu, že platí obecně."

Betrandův postulát (přesněji řečeno domněnka) je ekvivalentní následujícímu tvrzení: Pro každé $n \geq 4$ existuje alespoň jedno prvočíslo p takové, že $n < p < 2n-2$. Toto tvrzení (a další) dokázal roku 1852 ruský matematik P. L. Čebyšev (Tchebichef, 1852). Krátký důkaz využívající vlastností Γ-funkce publikoval indický matematik S. Ramanujan (1919) a důkaz využívající pouze elementární postupy předložil roku 1932 maďarský matematik P. Erdös (Erdös, 1932). Čistě aritmetický velmi elementární důkaz je nám znám, avšak není zde uveden z důvodu délky.

Z *Bertrandova postulátu* okamžitě plyne tvrzení, že pro každé $n \geq 2$ existuje alespoň jedno prvočíslo p takové, že $n < p < 2n$. I toto slabší tvrzení se někdy zve *Bertrandův postulát.*

V roce 1952 japonský matematik J. Nagura publikoval důkaz tvrzení (viz Nagura, 1952), podle kterého pro každé $n \geq 25$ existuje alespoň jedno prvočíslo p takové, že $n < p < \frac{6n}{5}$. Například pro $n = 25$ získáváme jediné prvočíslo p, a sice $p = 29$, $25 < 29 < 30$. Totéž pro $n = 26$. Pro $n = 27$ již získáváme dvě prvočísla, a to $p = 29$ a $p = 31$. Všimněme si, že Nagurovo tvrzení platí také pro $n = 10, 12, 15, 16, 17, 18, 20, 21, 22$ a neplatí pro ostatní n, $0 \leq n \leq 24$. Ve slabší podobě $n \leq p \leq \frac{6n}{5}$, ovšem tvrzení platí pro $n = 2, 3, 5, 6, 7, 11, 13, 19, 23$ (a stále neplatí pro $n = 0, 1, 4, 8, 9, 14, 24$).

Z Nagurova tvrzení snadno plyne, že pro každé $n \geq 2$ existuje alespoň jedno prvočíslo p takové, že $2n < p < 3n$ ($2 \cdot 1 = 2 < 3 = 3 \cdot 1$). Toto další tvrzení je též dokázáno v (Bachraouni, 2006) s použitím mírně jednodušších prostředků.

Z Nagurova výsledku plyne ještě další tvrzení, které říká, že pro každé $n \geq 2$ existuje alespoň jedno prvočíslo p takové, že

$3n < p < 4n$. I pro toto tvrzení (snad) existují jednodušší důkazy, viz (Hanson, 1973), (Loo, 2011).

Je $\frac{24n}{5} < 5n$, takže ještě máme tvrzení, že pro každé $n \geq 3$ existuje alespoň jedno prvočíslo p takové, že $4n < p < 5n$ ($4 \cdot 1 = 4 < 5 = 5 \cdot 1$, $4 \cdot 2 = 8 < 10 = 5 \cdot 2$, 9 není prvočíslo). Viz též (Schur, 1929).

Nakonec je $\frac{30n}{5} = 6n$. Takže pro každé $n \geq 2$ existuje alespoň jedno prvočíslo p takové, že $5n < p < 6n$ ($5 \cdot 1 = 5 < 6 = 6 \cdot 1$).

Je ovšem $7 < \frac{36}{5}$, takže nelze dále pokračovati předchozím způsobem.

V (Breusch, 1932) se dokazuje, že pro každé $n \geq 48$ existuje alespoň jedno prvočíslo p takové, že $n < p < \frac{9n}{8}$. Odtud snadno plyne, že pro každé $n \geq 2$, $n \neq 3, 4$, existuje alespoň jedno prvočíslo p takové, že $8n < p < 9n$.

Je $\frac{54}{8} < 7$, takže pro každé $n \geq 2$, $n \neq 4$, existuje alespoň jedno prvočíslo p takové, že $6n < p < 7n$.

Je $\frac{63}{8} < 8$, takže pro každé $n \geq 3$ existuje alespoň jedno prvočíslo p takové, že $7n < p < 8n$.

Je $10 < \frac{81}{8}$.

V (Gatteschi, 1947) se dokazuje, že pro každé $n \geq 24$ existuje alespoň jedno prvočíslo p tak, že $n < p < \frac{11n}{9}$. To nám nestačí, avšak v (Rohrbach & Weis, 1964b, s. 433) se dokazuje, že pro každé $n \geq 118$ existuje alespoň jedno prvočíslo p takové, že $n < p < \frac{14n}{13}$. Odtud už snadno plynou následující tvrzení:

Pro každé $n \geq 3$, $n \neq 9$ existuje alespoň jedno prvočíslo p takové, že $13n < p < 14n$.

Pro každé $n \geq 3$, $n \neq 4$ existuje alespoň jedno prvočíslo p takové, že $12n < p < 13n$.

Pro každé $n \geq 2$, $n \neq 3$ existuje alespoň jedno prvočíslo p takové, že $11n < p < 12n$.

Pro každé $n \geq 3$ existuje alespoň jedno prvočíslo p takové, že $10n < p < 11n$.

Pro každé $n \geq 2$ existuje alespoň jedno prvočíslo p takové, že $9n < p < 10n$.

Dle (Schoenfeld, 1976), pro každé $n \geq 2\,010\,760$ existuje alespoň jedno prvočíslo p takové, že $n < p < \frac{16\,598n}{16\,597}$ (povšimněme

si, že $16\,597 = 7 \cdot 2\,371$, $16\,598 = 2 \cdot 43 \cdot 193$, $2\,010\,760 = 2^3 \cdot 5 \cdot$ $\cdot 17 \cdot 2\,957$). Buď nyní $n \geq 122$, $1 \leq k \leq 16\,597$ a $\frac{2\,010\,760}{k} \leq n$. Potom je $kn \geq 2\,010\,760$ a tedy máme prvočíslo p takové, že $kn < p < \frac{16\,598kn}{16\,597} = kn + \frac{kn}{1\,659} \leq kn + n = (k+1)n$. Takže $kn < p < (k+1)n$ pro výše uvedená n a k. Například je-li $k = 60$, pak se dozvídáme, že $14n < p < 15n$ pro všechna $n \geq 143\,612$. Snadno ověříme, že p existuje i pro $2 \leq n \leq 100$. Pomocí vyspělé výpočetní techniky lze zjistit, že p existuje pro všechna $n \geq 2$.

Volme $k = 16\,597$. Tedy $16\,597n < p < 16\,598n$ pro všechna $n \geq 122$. Můžeme postupovat jako výše. Je $16\,597 \cdot 2 = 33\,194$, $16\,598 \cdot 2 = 33\,196$ a (mezi)číslo $16\,595$ rovněž není prvočíslo. Je $16\,597 \cdot 3 = 49\,791$, $16\,598 \cdot 3 = 49\,794$ a (mezi)čísla $49\,792$ a $49\,793$ $(= 17 \cdot 2\,929)$. Je $16\,597 \cdot 4 = 66\,388$, $16\,598 \cdot 4 = 66\,392$, $66\,389 =$ $= 197 \cdot 337$. A dále použijeme technické prostředky pro $5 \leq n \leq$ ≤ 121. A závěr je ten, že pro každé $n \geq 9, n \neq 10, 11, 12, 15, 29$, existuje alespoň jedno prvočíslo p takové, že $16\,597n < p <$ $< 16\,598n$ (a neexistuje pro $n = 1, 2, 3, \ldots 8, 10, 11, 12, 15, 29$).

Pro každé $k \in \mathbb{N}_0$ označme γ_k množinu těch čísel $n \in \mathbb{N}_0$, že $kn < p < (k+1)n$ pro alespoň jedno prvočíslo p. Ihned pozorujeme, že $\gamma_0 = \{n | n \geq 2\}$, $0, 1 \notin \gamma_k$ a $2 \in \gamma_k$ právě když (liché) číslo $2k+1$ je prvočíslo $(k = 1, 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, \ldots)$. Z Bertrandova postulátu nám plyne rovnost $\gamma_1 = \{n | n \geq 2\}$.

Z poznatků sepsaných v předchozích odstavcích dostáváme rovnosti:

$$\begin{aligned}
\gamma_1 = \gamma_2 = \gamma_3 = \gamma_5 = \gamma_9 = \gamma_{14} &= \{n | n \geq 2\},\\
\gamma_0 = \gamma_4 = \gamma_7 = \gamma_{10} &= \{n | n \geq 3\},\\
\gamma_6 &= \{n | n \geq 2, n \neq 4\},\\
\gamma_8 &= \{n | n \geq 2, n \neq 3, 4\},\\
\gamma_{11} &= \{n | n \geq 2, n \neq 3\},\\
\gamma_{12} &= \{n | n \geq 3, n \neq 4\},\\
\gamma_{13} &= \{n | n \geq 3, n \neq 9\},\\
\gamma_{16\,597} &= \{n | n \geq 9, n \neq 10, 11, 12, 15, 29\}.
\end{aligned}$$

V této souvislosti poznamenejme, že na rozdíl od dnes již klasického Bertrandova postulátu se nám důkazy dalších citovaných

výsledků nezdařilo plně prostudovat, a tudíž nemůžeme poskytnout návrhy na jejich modifikace.

A. M. Legendre vyslovil domněnku, že pro každé $n \geq 1$ existuje alespoň jedno prvočíslo p takové, že $n^2 < p < (n+1)^2$. Zdá se, že tato domněnka nebyla dosud ani dokázána ani vyvrácena (i když různé více či méně pochybné důkazy se tu a tam objevují). *Legendrova domněnka* byla potvrzena pro $n \leq 2 \cdot 10^9$ (Oliveira e Silva et al., 2014) a navíc plyne z následující (formálně silnější) domněnky: $n \in \gamma_n$ pro každé $n \geq 2$. Tato nová domněnka představuje jednu polovinu tzv. *Oppermannovy domněnky*, kterou roku 1877 vyslovil dánský matematik L. Oppermann. A sice: $n \in \gamma_{n-1} \cap \gamma_n$ pro každé $n \geq 2$. Nabízí se ještě silnější domněnka: $n \in \gamma_k$ pro $n \geq 2$, $1 \leq k \leq n$. A jistě lze pokračovat dále.

Z *Dirichletovy prvočíselné věty* (se kterou se seznámíme za chviličku) plyne, že pro každé $n \geq 2$ existuje nekonečně mnoho $k \in \mathbb{N}$ takových, že $kn + 1$ je prvočíslo. Jelikož je $kn < kn + 1 < (k+1)n$, tak je $n \in \gamma_k$.

Buď $k \geq 2$. Pro každé prvočíslo p takové, že $p \geq k^2 - 1 (\geq 3)$ existují $n \in \mathbb{N}_0$ a $l \in \mathbb{N}_0$ tak, že $0 \leq l < k$ a $p = kn + l$. Vyjde-li $l = 0$, pak $p = kn$, $n = 1$, neboť p je prvočíslo, $k = p \geq k^2 - 1 \geq 2k - 1$, $1 \geq k$, spor. Tudíž je $1 \leq l \leq k - 1$ a $kn + k - 1 \geq kn + l = p \geq k^2 - 1$, $n \geq k - 1 \geq 1$. Je-li $n = 1$, pak $k = 2$, $p = 3$. Je-li $n = l$, pak $n = l = k-1$, $p = kn+l = (k+1)(k-1) = k^2-1$, $k = 2$, $p = 3$. Takže je-li $(k, p) \neq (2, 3)$, potom $kn < p = kn+l < (k+1)n$ a $n \in \gamma_k$. Jelikož je $n \geq \frac{p-k}{k}$, množina γ_k je nekonečná.

Buď $m \geq 2$. Pro každé k, $2 \leq k \leq m$, máme $\frac{k}{m!} + k$, $m! + k \geq 2 + k > k \geq 2$. Ihned pozorujeme, že číslo $m! + k$ není prvočíslem. A tudíž označme $p(m)$ a $p'(m)$ největší a nejmenší prvočíslo takové, že $p(m) < m! + 2$ a $m! + m < p'(m)$. Je $p'(m) - p(m) \geq m$ a žádné z čísel $p(m)+1, \ldots, p'(m)-1$ není prvočíslo. Pro ověření si spočítáme malou tabulku 1.

Znovu zdůrazňujeme, že prvočísla $p(m)$ a $p'(m)$ jsou bezprostředně po sobě jdoucí, a také to, že $p'(m) - p(m) \geq m$.

A teď buď $n \geq 2$. Pro každé $l \geq 2$ máme $p(ln) < (ln)! + 2 < (ln)! + ln < p'(ln)$, $p'(ln) - p(ln) > ln \geq 2n \geq 4$. Buď $t \geq 0$ největší číslo takové, že $tn \leq p(ln)$. Je tedy $p(ln) < (t+1)n <$

Tab. 1: Po sobě jdoucí prvočísla $p(m)$ a $p'(m)$ a velikosti mezer mezi nimi

m	2	3	4	5	6	7	8
$p'(m)$	5	11	29	127	727	5 051	40 427
$p(m)$	3	7	23	113	719	5 039	40 253
$p'(m)-p(m)$	2	4	6	14	8	12	174
$p'(m)-p(m)-m$	0	1	2	9	2	5	166

m	9	10	11	12
$p'(m)$	362 969	3 628 811	39 916 817	479 001 629
$p(m)$	362 851	3 628 789	39 916 801	479 001 599
$p'(m)-p(m)$	118	22	16	30
$p'(m)-p(m)-m$	109	12	5	18

$< (t+2)n \leq p(ln)+2n < p'(ln)$. Také žádné z čísel $(t+1)n+$ $+1, \ldots, (t+2)n-1$ není prvočíslo. Čili $n \notin \gamma_{t+1}$.

Z *Bertrandova postulátu* vyplývá, že $p'(m) < 2p(m)$. Tedy máme nerovnost $p(m) > \frac{m!}{2} + \frac{m}{2}$. V našem případě $m = ln$ dostáváme nerovnosti $t+1 > \frac{p(ln)}{n} > \frac{(ln)!}{2n} + l > l$.

Zjistili jsme, že $n \notin \gamma_k$ pro nekonečně mnoho čísel $k \in \mathbb{N}_0$.

Seřaďme si prvočísla tak, jak jdou za sebou: $\gamma_1(=2) < \gamma_2(=$ $=3) < \gamma_3(=5) < \ldots$ a položme $\tau(i) = i + \gamma_i - \gamma_{i+1}$ pro každé $i \geq 1$. Sestrojme tabulku (tab. 2).

Tab. 2: Hodnoty $\tau(i)$ pro $i \in \langle 1; 38 \rangle$

i	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(i)$	0	0	1	0	3	2	5	4	3	8	5	8
i	13	14	15	16	17	18	19	20	21	22	23	24
$\tau(i)$	11	10	9	10	15	12	15	18	15	18	17	16
i	25	26	27	28	29	30	31	32	33	34	35	36
$\tau(i)$	21	24	23	26	25	16	27	26	31	24	33	30

Stále není známo, zda $\tau(i) = i-2$ pro nekonečně mnoho i. Je však známo, že $\tau(i) \geq i - 246$ pro nekonečně mnoho čísel i.

Dirichletova prvočíselná věta

Znamenitou větu o výskytu prvočísel v aritmetické posloupnosti uveřejnil P. G. Z. Dirichlet (1837). Věta říká, že pro všechna nesoudělná celá čísla $a \geq 1$, $b \geq 0$ existuje nekonečně mnoho kladných celých čísel a takových, že $ca + b$ je prvočíslo.

Pro všechna i, $0 \leq i \leq 9$, položme $K(i) = \{k | k \in \mathbb{N}_0, 10k + i \in \mathbb{P}\}$ (zde symbolem $\mathbb{P}$ označujeme množinu všech prvočísel).

Snadno si uvědomíme, že $K(0) = K(4) = K(6) = K(8) = \emptyset$ a $K(2) = K(5) = \{0\}$. Oproti tomu, podle *Dirichletovy prvočíselné věty* jsou množiny $K(1), K(3), K(7)$ a $K(9)$ nekonečné. Z každé z těchto množin si sepišme prvních 33 čísel.

$K(1)$: 1, 3, 4, 6, 7, 10, 13, 15, 18, 19, 21, 24, 25, 27, 28, 31, 33, 40, 42, 43, 46, 49, 54, 57, 60, 63, 64, 66, 69, 70, 75, 76, 81;

$K(3)$: 0, 1, 2, 4, 5, 7, 8, 10, 11, 16, 17, 19, 22, 23, 26, 28, 29, 31, 35, 37, 38, 43, 44, 46, 50, 52, 56, 59, 61, 64, 65, 67, 68;

$K(7)$: 0, 1, 3, 4, 6, 9, 10, 12, 13, 15, 16, 19, 22, 25, 27, 30, 31, 33, 34, 36, 39, 45, 46, 48, 54, 55, 57, 58, 60, 61, 63, 64;

$K(9)$: 1, 2, 5, 7, 8, 10, 13, 14, 17, 19, 22, 23, 26, 34, 35, 37, 38, 40, 41, 43, 44, 47, 49, 50, 56, 59, 61, 65, 70, 71, 73, 76.

Všimněme si, že průnik $K(1) \cap K(3) \cap K(7) \cap K(9)$ začíná takto: 1, 10, 19, 82, 148, 187, 208, 325, 500.

Položme $K = K(1) \cup K(3) \cup K(7) \cup K(9)$. Předně ihned vidíme z předchozích zjištění, že $K = \bigcup_{i=0}^{9} K_i$. Dále vidíme, že množina K začíná takto: 0, 1, 2, 3, . . . , 19, 21, . . . , 31, 33, 34, . . . , 50, 52, 54, . . . , 61, 63.

Množina K je ovšem nekonečná a my položíme $L = \mathbb{N}_0 \setminus K$ $(= \{l | l \in \mathbb{N}_0, l \notin K\}$. Množina L začíná takto: 20, 32, 51, 53, 62, 84, 89, 107, 113, 114, 126, 133, 134, 135, 141, 146, 150. Již v následujícím odstavci si dokážeme, že množina L je také nekonečná.

Je $21(11j - 1) \in L$ pro každé $j \geq 1$.

Toto tvrzení je velmi snadné. Je totiž $10 \cdot 21(11j - 1) + 1 = 2310j - 209 = 11(210j - 19)$, $10 \cdot 21(11j - j) + 3 = 2310j - 207 =$

$= 3(770j - 69)$, $10 \cdot 21(11j - 1) + 7 = 2310j - 203 = 7(330j - 67)$, $10 \cdot 21(11j - 1) + 9 = 2310j - 201 = 3(770j - 67)$. Žádné z těchto čísel není prvočíslo.

Tedy vskutku, množina L je nekonečná. Poznamenejme, že nevíme, zda množina L obsahuje nekonečně mnoho prvočísel.

Nechť $k \geq 1$, $k = a_m \dots a_0$, $m \geq 0$, $0 \leq a_i \leq 9$, $a_m \neq 0$ (zápis v desítkové soustavě). Je $10k = a_m \dots a_0 0$ (opět desítkový zápis). Zajisté $\lambda(k) = m + 1$ a $\lambda(10k) = m + 2 \geq 2$. Je-li $k \in K$, pak alespoň jedno z čísel $10k + j$, $j = 1, 3, 7, 9$ je prvočíslo a je tedy jasné, že $10k \in A \setminus \mathbb{P}$. Úvahu obraťme a předpokládejme, že $10k \in A$. Existuje tedy $p \in \mathbb{P}$ takové prvočíslo, že p je blizoučké k číslu $10k$. Máme $\lambda(p) = \lambda(10k) = m + 2$, $p = b_m + 1 \dots b_0$, $0 \leq b_i \leq 9$, $b_{m+1} \neq 0$ (desítkový zápis). Zajisté $p > 10^{m+1} \geq 10$, p je liché prvočíslo, $b_0 = 1, 3, 7, 9$. Jelikož p je blizoučké k $10k$, tak $b_{m+1} = a_m, \dots, b_1 = a_0$, $p = 10k + b_0$. Odtud plyne $k \in K$.

Dokázali jsme tvrzení, že pokud je $k \in \mathbb{N}_0$, pak $k \in K$ tehdy a jen tehdy, jestliže $10k \in A$. (Případ $k = 0$ je zřejmý.)

Z předchozího plyne tento důsledek: $210(11j - 1) \in B$ pro každé $j \geq 1$. Množina B je tedy nekonečná. Tato množina obsahuje prvky: $200, 202, 204, 205, 206,\ 208, 320, 322, 324, 325, 326, 328 \dots$

Poznamenejme, že nám není známo, zda $n \in A$ platí pro každé liché n takové, že $5 \nmid n$. Není těžké prověřit, že je tomu tak pro malá n.

Množina $B = \mathbb{N}_0 \setminus A$ je nekonečná. Zdá se však býti otevřeným problémem, zdali z každého $n \in B$ lze „vytvořit“ prvočíslo dvěma změnami jeho číslic. Pokud by odpověď na domněnku z (Hanson, 1973) byla kladná, tak by každé číslo $n \in B$ bylo buďto sudé, nebo liché avšak dělitelné prvočíslem 5. Stačilo by tedy změnit poslední číslici vpravo $(= 0, 2, 4, 5, 6, 8)$, např. na číslici 1 a toto nové číslo by patřilo do množiny A. K získaní prvočísla by pak stačila jediná změna. Celkově dvě změny.

Čínská věta o zbytcích

Pro každé $q \geq 0$ si definujme nezáporné celé číslo $\alpha(q)$. Nuže, $\alpha(q)$ je nejmenší nezáporné celé číslo s těmito vlastnostmi:

1. $q \mid \alpha(q)$,

2. Součet $\alpha(q) + i$ není prvočíslo pro žádné i, $0 \leq i \leq q - 1$.

Ihned je zřejmé, že $\alpha(0) = \alpha(1) = \alpha(2) = 0$. Sepíšeme-li si tabulku všech malých prvočísel, pak pozornou prohlídkou tohoto soupisu získáme malou příruční tabulku čísel $\alpha(q)$ (a jejich prvočíselných rozkladů) pro $0 \leq q \leq 23$.

Tab. 3: Čísla $\alpha(q)$ a jejich prvočíselné rozklady pro $q \in \langle 0; 23 \rangle$

q	0	1	2	3
$\alpha(q)$	0	0	0	24
πp	-	-	-	$2^3 \cdot 3$
q	4	5	6	7
$\alpha(q)$	24	90	90	119
πp		$2^3 \cdot 3$ $2 \cdot 3^2 \cdot 5$	$2 \cdot 3^2 \cdot 5$	$7 \cdot 17$
q	8	9	10	11
$\alpha(q)$	200	117	200	319
πp		$2^3 \cdot 5^2$	$3^2 \cdot 13$ $2^3 \cdot 5^2$	$11 \cdot 29$
q	12	13	14	15
$\alpha(q)$	324	1 131	1 134	1 260
πp	$2^2 \cdot 3^4$	$3 \cdot 13 \cdot 29$	$2 \cdot 3^4 \cdot 7$	$2^2 \cdot 3^2 \cdot 5 \cdot 7$
q	16	17	18	19
$\alpha(q)$	1 136	1 343	1 638	1 330
πp	$2^4 \cdot 71$	$17 \cdot 79$	$2 \cdot 3^2 \cdot 7 \cdot 13$	$2 \cdot 5 \cdot 7 \cdot 19$
q	20	21	22	23
$\alpha(q)$	1 340	9 555	15 686	1 334
πp	$2^2 \cdot 5 \cdot 67$	$3 \cdot 5 \cdot 7^2 \cdot 13$	$2 \cdot 11 \cdot 23 \cdot 31$	$2 \cdot 23 \cdot 29$

Čísla $\alpha(0), \ldots, \alpha(23)$ jsme nalezli, avšak zůstává tu otázka, zda existují čísla $\alpha(q)$ pro všechna q. A odpověď zní ano. K důkazu použijeme starodávnou *Čínskou větu o zbytcích*.

Roku 1247 sepsal čínský matematik Čin Čin-šao spis nazvaný *Šušu Činčang*. V něm pak, mimo jiné, dokázal i jednu velmi uži-

tečnou větu – *Čínskou větu o zbytcích*. V tomto spisu je tato věta poprvé vyslovena v obecné podobě a dokázána. Samotný algoritmus byl znám dříve. Poprvé je problém vedoucí k této větě zmíněn již ve spisu čínského matematika Sun-C' ze 3. století. Bez důkazu ji nalézáme použitou i ve spisech Brahmagupty či Fibonacciho.

Pro $q \geq 0$ označme W_q množinu těch nezáporných čísel w, že $q|w$ a žádné z čísel $w+i$, $0 \leq i \leq$
$\leq q-1$ není prvočíslo. Snadno se nahlédne, že $W_0 = \{0\}$, $W_1 = \mathbb{N}_0 \setminus \mathbb{P}$ a $W_2 = \{w | \, 2 \mid w, w+1 \notin \mathbb{P}\}$. Množina W_2 začíná takto: 0, 8, 14, 20, 24, 26, 32, 38, 44, 48, 50. Množina W_2 je nekonečná, neboť $10k+4 \in W_2$ pro každé $k \geq 1$.

Z definice čísla $\alpha(q)$ je zřejmé, že $\alpha(q)$ je právě nejmenší číslo z množiny W_q. Stačí tedy dokázat, že tato množina je neprázdná.

Nuže, nechť $q \geq 2$ a $s \geq 2q-1 (\geq 3)$. Označme $p_1, \ldots, p_s$ prvních s prvočísel ($p_1 = 2$, $p_2 = 3$, $p_3 = 5 \ldots$). Položme $u_j = \prod_{i=1, i \neq j}^{s} p_i$ pro každé j, $1 \leq j \leq s$. Čísla p_j a u_j jsou nesoudělná, a tudíž existují celá čísla q_j, h_j (třeba i záporná) taková, že $1 = q_j p_j + h_j u_j$. Zvolme $t \geq 1$ tak, aby $v = tp_1 \ldots p_s + \sum_{i=1}^{s} i h_i u_i \geq p_s + s + 1$. Není příliš obtížné se přesvědčit o tom, že $p_i | v - i$ pro každé $i = 1, 2, \ldots, s$. Čísla $v - i$ jsou vesměs kladná a žádné z nich není prvočíslo.

Předpokládejme na malou chvíli, že $q \nmid v - l$ pro všechna $q \leq$
$\leq l \leq s$. Čísla $v - l$ skýtají po dělení číslem q zbytky v_l, $1 \leq$
$\leq v_l \leq q-1$. Zbytků v_l je nejvýše $q-1$ různých a čísel $v-l$ je právě $s-q+1$ různých. Protože $s-q+1 \geq q$, musí existovat indexy l_1, l_2 takové, že $1 \leq l_1 < l_2 \leq q$, přičemž $v_{l_1} = v_{l_2}$. Odtud $q \mid (v-l_1) - v_{l_1}$, $q \mid (v-l_2) - v_{l_1}$, $q \mid l_2 - l_1$, spor s tím, že $1 \leq l_2 - l_1 < q$.

Dozvěděli jsme se, že existuje k takové, že $q \leq k \leq s$ a $q \mid v-k$. Položme $w = v - k$. Je $w \geq p_s + 1$ a žádné z čísel $w (= v-k)$, $w+1 (= w-k+1), \ldots, w+q-1$ $(= v-k-1+q)$ není prvočíslo. Je totiž $q \leq k \leq s$. Dokázali jsme, že $w \in W_q$.

Jelikož $q \mid \alpha(q)$, z rozkladů $\alpha(q)$ v předchozí tabulce vidíme, že $\alpha(q) \geq 24$ pro každé $q \geq 3$. Ovšem $\alpha(q) \geq 2q$ pro každé $q \geq 3$. Kdyby totiž bylo $\alpha(q) < 2q$, pak by bylo $\alpha(q) = q$ a žádné z čísel $q, q+1, \ldots, 2q-1$ by nebylo prvočíslo. Toto je však ve sporu s nám

již důvěrně známým *Bertrandovým postulátem*. Odhad $\alpha(q) \geq 2q$ je zajisté velmi hrubý. Nakonec uvedeme tabulku 4.

Tab. 4: Podíly $\alpha(q)$ a q pro $q \in \langle 0; 23 \rangle$

q	0	1	2	3	4	5	6	7
$\alpha(q)/q$	-	0	0	8	6	18	15	17
q	8	9	10	11	12	13	14	15
$\alpha(q)/q$	25	13	20	29	27	87	81	84
q	16	17	18	19	20	21	22	23
$\alpha(q)/q$	71	79	91	70	67	455	713	58

Závěr

Na začátku článku jsme si položili otázku, jak blízko ke zvolenému číslu již lze nalézt prvočíslo. Pomocí dílčích výsledků, které v článku s pomocí základních aritmetických výpočtů navzájem kombinujeme, jsme nakonec došli k závěru, že za předpokladu platnosti domněnky z (Hanson, 1973) lze změnou nejvýše dvou číslic libovolné číslo upravit na prvočíslo. To představuje nejen zajímavý teoretický výsledek, ale také podklad pro řadu zábavných aktivit do hodin matematiky, zaměřených na vyhledávání blízkých prvočísel ke zvolenému číslu.

Literatura

[1] Bachraoui, M. E. (2006). Primes in the interval [2n,3n]. *The International Journal of Contemporary Mathematical Sciences*, *1*, 617–621.

[2] Bertrand, J. (1845). Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. *Journal de l'École Royale Polytechnique*, *30*(18), 123–140.

[3] Breusch, R. (1932). Zur Verallgemeinerung des Bertrandschen Postulates, daß zwischen x und 2x stets Primzahlen liegen. *Mathematische Zeitschrift*, *18*, 505–526.

[4] Dirichlet, P. G. L. (1837). Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhandlungen der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, *48*, 45–91.

[5] Erdös, P. (1932). Beweis eines Satzes von Tschebyschef. *Acta Litt*, *5*, 194–198.

[6] Gatteschi, L. (1947). Un perfezionamento di un teorema di I. Schur sulla frequenza dei numeri primi. *Bollettino dell'Unione Matematica Italiana*, *3*(2), 123–125.

[7] Hanson, D. (1973). On a Theorem of Sylvester and Schur. *Canadian Mathematical Bulletin. 16*, 195–199.

[8] Loo, A. (2011). On the Primes in the Interval [3n, 4n]. *International Journal of Contemporary Mathematical Sciences*, *6*(38), 1871–1872.

[9] Nagura, J. (1952). On the interval containing at least one prime number. Proceedings of the Japan Academy, Series A, *Mathematical Sciences*, *28*(4), 177–181.

[10] Oliveira e Silva, T., Herzog, S., & Pardi, S. (2014). Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$, *Mathematics of Computation*, *83*(288), 2033–2060.

[11] Ramanujan, S. (1919). A proof of Bertrand's postulate. *Journal of the Indian Mathematical Society*, *11*, 181–182.

[12] Rohrbach, H., & Weis, J. (1964a). Berichtigung zu der Arbeit 'Zum finiten Fall des Bertrandschen Postulats'. *Journal für die reine und angewandte Mathematik*, *216*, 220–220 .

[13] Rohrbach, H., & Weis, J. (1964b). Zum finiten Fall des Bertrandschen Postulats. *Journal für die reine und angewandte Mathematik*, *0214_0215*, 432–440.

[14] Schoenfeld, L. (1976). Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$. II. *Mathematics of Computation*, *30*(134), 337–360.

[15] Schur, I. (1929). Einige Sätze über Primzahlen : mit Anwendungen auf Irreduzibilitätsfragen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften (Physikalisch-Mathematische Klasse)*, 126–136.

[16] Tchebichef, P. L. (1852). Mémoire sur les nombres premiers. *Journal de Mathématiques Pures et Appliquées*, *17*, 366–390.

Abstract

Prime numbers and the questions associated with them are some of the most difficult problems in mathematics, and many of them remain open. In this article, we address the question of how close to a chosen number we can already find a prime. On the basis of well-known statements, it can be conjectured that a prime number can be obtained from any natural number by changing at most two digits. The reasoning by which we develop the known results is of a purely arithmetical nature. The hypothesis stated, which is dependent on the hypothesis from (Hanson, 1973), is not only an interesting theoretical observation, but can also serve to enliven mathematics lessons by activities in which the pupils themselves search for close prime numbers to the chosen number.

Tomáš Kepka
Matematicko-fyzikální fakulta, Univerzita Karlova
Sokolovská 49/83
186 75 Praha 8
e-mail: tomas.kepka@mff.cuni.cz

Antonín Jančařík
Pedagogická fakulta, Univerzita Karlova
Magdalény Rettigové 4
116 39 Praha 1
e-mail: antonin.jancarik@pedf.cuni.cz

Jakub Michal
Pedagogická fakulta, Univerzita Karlova
Magdalény Rettigové 4
116 39 Praha 1
e-mail: cjakub@email.cz