Časopriestor
Spacetime
26 11/2022
ISSN 2730-0110
Interaktívne vedecko-popularizačné médium významných autorov a vedeckých pracovníkov
Interactive popular science medium of important authors and scientists

OSEMTISÍCOVKY
teórie čísel

prof. RNDr. Miroslav Haviar, CSc.

www.intercedu.com © INTERCEDU, a.s., Moyzesova 4/A, 902 01 Pezinok, Slovakia

Obsah

Časopriestor // Spacetime

Interaktívne vedecko-popularizačné médium významných autorov a vedeckých pracovníkov.

Šéfredaktor: Dr.h.c. mult. prof. PhDr. Ing. Štefan Kassay, DrSc.

Recenzent a editor: Dr.h.c. mult. prof. Ing. Štefan Luby, DrSc.

Grafická úprava: Dušan Ščepka.

Za odborný obsah materiálov zodpovedá autor.

Vydavateľ: INTERCEDU, a.s., Moyzesova 4/A, 902 01 Pezinok, Slovenská republika

ISSN 2730-0110

prof. RNDr. Miroslav Haviar, CSc.

Je matematikom, jeho zahraniční vedeckí spolupracovníci pochádzajú z Austrálie, Južnej Afriky, Portugalska, Švédska a Veľkej Británie. Vedecky pracoval počas dvoch rokov na University of Oxford (včítane štipendijného pobytu v akademickom roku 1993-94) a tri roky v Melbourne (včítane dvojročného postdoktorálneho pobytu 1998-2000). Mal pozvané plenárne prednášky na matematických konferenciách v Lisabone (2003), Nashville (2007), Oxforde (2011), Melbourne (2013) a Bratislave (2018) a opakované pozvané seminárne prednášky v Glasgowe, Lisabone, Melbourne, Olomouci, Oxforde a Viedni. Od roku 1993 prednáša a vedie študentov na Univerzite Mateja Bela v Banskej Bystrici a na Katolíckej univerzite v Ružomberku. Od júna 2020 je aj Visiting Professor na University of Johannesburg (Južná Afrika). Od malička ho priťahovala matematika a rád by jej pozoruhodnými príbehmi pritiahol k nej aj žiakov a mladých ľudí. Popri rodine (5 detí) a matematike sa venoval aktívne futbalu (kariéru zakončil v Oxforde), behom na dlhé trate (7 maratónov) a v súčasnosti sa so synom venuje crossfitu.

Abstrakt

Cieľom tohto článku je informovať čitateľov, ktorí sa zaujímajú o matematiku, o niektorých dôležitých objavoch v oblasti teórie čísel. Niektoré z nich nie sú veľmi známe ani medzi učiteľmi matematiky. Takými sú napríklad Gándhího vzorec pre n-té prvočíslo z roku 1971, algoritmus na testovanie prvočíselnosti z roku 2002 a takmer 400 rokov staré hypotézy o existencii nekonečne veľa Fermatových a Mersennových prvočísel. (Hoci v súčasnosti poznáme len 5 Fermatových prvočísel a 51 Mersennových prvočísel.) Medzi ďalšie tvrdenia, ktoré sú spomenuté, patrí Dirichletova veta z roku 1837, hypotéza o nekonečne veľa primoriálnych prvočíslach, hypotéza prvočíselných dvojčiat, Goldbachova hypotéza a dve Polignacove hypotézy. Fermatove čísla sú spomenuté v súvislosti s dôkazom nekonečného počtu prvočísel. Následne sú uvedené výsledky vlastného skúmania autora s kolegom Maličkým - zavedenie nového pojmu superprvočísla a tri hypotézy týkajúce sa superprvočísel. Ako vrchol vlastného skúmania v teórii čísel je prezentované zavedenie pojmu zovšeobecnenej Dirichletovej postupnosti a formulácia zovšeobecnenej Dirichletovej vety ako hypotézy. Z nej pomerne ľahko vyplývajú aj zmienené staré hypotézy o existencii nekonečne veľa Fermatových a Mersennových prvočísel. Formulácie všetkých uvedených hypotéz sú také jednoduché, že učitelia by mohli (a azda by mali) prezentovať ich žiakom ako dobré príklady otvorených problémov v matematike. Otvorené problémy teórie čísel sú pripodobnené k osemtisícovkam na zemeguli a ich zdolanie k výzvam podobným tým v horolezectve.

Kľúčové slová: teória čísel, prvočíslo, primoriálne číslo, Dirichletova veta, hypotéza prvočíselných dvojčiat, Goldbachova hypotéza, medzera prvočísel, Polignacove hypotézy, Gándhího vzorec, testovanie prvočíselnosti, AKS algoritmus, Fermatove čísla, superprvočísla, zovšeobecnená Dirichletova postupnosť, zovšeobecnená Dirichletova veta, Mersennove prvočísla.

Abstract

The aim of this article is to inform readers interested in Mathematics about some important discoveries in the area of Number Theory. Some of them are not very well-known even among teachers of Mathematics. Such are, for example, Gandhi´s formula for the n th prime from 1971, the prime-verification algorithm from 2002 and almost 400 years old conjectures about the existence of infinitely many Fermat and Mersenne primes. (Though we currently know only 5 Fermat primes and 51 Mersenne primes.) Among other statements which are mentioned are Dirichlet´s Theorem from 1837, conjecture about infinitely many primorial primes, Twin Prime Conjecture, Goldbach´s Conjecture and two Polignac´s Conjectures. Fermat numbers are mentioned in connection with the proof about infinitely many primes. Subsequently, the results of the author's own research with his colleague Maličký are presented - introducing the new concept of superprimes and three conjectures concerning superprimes. As the peak of own research in Number Theory, an introduction of the concept of generalized Dirichlet's sequence and a formulation of Generalized Dirichlet's Theorem as a conjecture are presented. One can derive relatively easily from it the mentioned old conjectures about the existence of infinitely many Fermat and Mersenne primes. The formulations of all the presented conjectures are so simple that teachers could (and perhaps should) present them to pupils as good examples of open problems in Mathematics. Open problems in Number Theory are considered like eight-thousanders on the globe and conquering them like challenges similar to those in mountaineering.

Key Words: Number Theory, prime number, primorial number, Dirichlet´s Theorem, Prime Twin Conjecture, Goldbach´s Conjecture, prime gap, Polignac´s Conjectures, Gandhi´s Formula, primality testing, AKS algorithm, Fermat numbers, superprimes, Generalised Dirichlet´s Sequence, Generalised Dirichlet´s Theorem, Mersenne primes.

Úvod

„Vesmír je ovládaný a riadený číslami." Tento výrok sa prisudzuje Pytagorovi zo Samu, jednej z najinšpiratívnejších postáv histórie matematiky (Singh, 2000). Pytagoras, ktorý žil v 6. storočí pred Kristom na ostrove Samos v Egejskom mori, je považovaný aj za zakladateľa teórie čísel. Staroveké národy Egypta a Babylonu používali matematiku ako prostriedok na riešenie praktických problémov (ako bolo vymeriavanie polí zničených záplavami Nílu, konštruovanie dômyselných stavieb alebo schémy účtovníctva). Avšak Pytagoras sa už zaujímal aj o to, prečo algoritmy či číselné receptúry starovekých národov „fungujú" a aké číselné či geometrické zákony sa za nimi skrývajú. Neskôr v 3. storočí pre Kristom v Ptolemaiovej Alexandrii pokračoval v diele Pytagora prvý vedúci matematického oddelenia slávnej Alexandrijskej knižnice, Euklides. Z jeho 13 kníh Základov, ktoré zahŕňali všetky dovtedy známe matematické poznatky, boli dve venované výlučne dielu „Bratstva" Pytagora. Aj keď Euklidovou hlavnou doménou bola geometria, zaujímala ho aj teória čísel a dokázal okrem iného existenciu iracionálnych čísel, ktoré Pytagoras „neslávne" zavrhol (Singh, 2000). Euklidovo dielo sa stalo na ďalších dvetisíc rokov základom učebných osnov na všetkých školách a univerzitách sveta a jeho Základy možno považovať podnes po Biblii (a aktuálnejšie azda po dielach Pán Prsteňov a Harry Potter) za jedno z najpredávanejších knižných diel sveta.

Teória čísel prešla od Pytagora, Euklida a neskôr Diofanta cez arabských matematikov až k európskym stredovekým a novovekým známym aj menej známym číselným teoretikom, z ktorých musíme spomenúť Fermata a teológa otca Mersenna, neskôr Eulera, Goldbacha, Lagrangeho, Gaussa, Germainovú, Abela, Galoisa, Legendreho, Dirichleta, Lamého, Cauchyho, Kummera, Riemanna, v 20. storočí Hardyho, Ramanujana, Weila, …, v jeho závere predovšetkým Wilesa. K úvodnému zoznámeniu sa so životnými príbehmi i matematickým dielom týchto postáv, predovšetkým však k Wilesovmu strhujúcemu príbehu vyriešenia slávnej Veľkej Fermatovej vety, možno vrelo doporučiť Singhovu vynikajúcu knihu *Fermat's Last Theorem* (Singh, 1998). Táto skvelá kniha vyšla následne aj v českom preklade ako *Velká Fermatova věta* (Singh, 2000). Podľa autora tohto článku by sa táto kniha mala stať „bibliou" pre každého učiteľa matematiky, aby pozitívnou energiou a nadšením z matematiky, ktoré kniha „vyžaruje", dokázal „zapaľovať" svojich žiakov či študentov.

V tomto príspevku sa pokúsime „zapáliť" odbornú i laickú verejnosť pre špeciálnu oblasť matematiky, ktorou je problematika prvočísel. Práve prvočísla sú základnými stavebnými kameňmi v teórii čísel (Pytagoras ich považoval za základné stavebné kamene vesmíru) a viaže sa k nim množstvo zaujímavých hypotéz,

objavov i stále otvorených problémov. Viaceré z nich, z ktorých sú zdá sa niektoré menej známe aj medzi našimi matematikmi, učiteľmi matematiky a laickou verejnosťou, spomenieme v tomto príspevku. Mnoho ďalších dôležitých výsledkov však musíme opomenúť s tým, že pre komplexnejší prehľad autor odkazuje čitateľa napríklad na knižky (Derbyshire, 2003), (Ribenboim, 2000) a (Sautoy, 2003), ktoré sám vlastní a môže ich s pokojným svedomím odporučiť. Cieľom príspevku je podať úvodnú informáciu k vývoju poznania v oblasti prvočísel a poskytnúť niektoré zdroje, z ktorých si učiteľ matematiky môže svoje vedomosti o prvočíslach i prehľad o aktuálnom dianí doplňať. Cieľom príspevku je však aj „apelovať" na matematikov, učiteľov matematiky i ďalšiu odbornú verejnosť, ktorí sú tvorcami učebným osnov a učebníc z matematiky. Ten apel smeruje k tomu, aby boli žiaci a študenti vo väčšej miere oboznamovaní s tým, že matematika ponúka stále množstvo zaujímavých otvorených otázok a nie je teda vednou disciplínou v žiadnom prípade uzavretou ako je rozšírenou domnienkou v značnej časti laickej verejnosti. Práve oblasť teórie čísel a téma prvočísel ponúkajú veľa ťažkých, historicky dôležitých a preslávených otvorených problémov. Väčšina z nich je pritom tak jednoducho formulovateľných, že ich učiteľ môže prezentovať žiakom aj na základnej škole. (Andrew Wiles sa so znením Veľkej Fermatovej vety oboznámil už vo veku 10 rokov.)

Andrew Wiles vo veku 10 rokov (vľavo) a nová budova Matematického ústavu v Oxforde, ktorá nesie jeho meno (vpravo)

Teória čísel zaznamenala svoje prirodzené oživenie ihneď po Wilesovom dôkaze Veľkej Fermatovej vety. Toto oživenie sa ešte vystupňovalo po auguste 2002, kedy trojica Indov Agrawal-Kayal-Saxena (poslední dvaja boli v tom čase mladými informatikmi s čerstvým bakalárskym diplomom!) našla dlho očakávaný polynomiálny algoritmus na testovanie prvočíselnosti. Mnohí považujú tento objav za jeden z najvýznamnejších v matematike za posledné desaťročia (spolu s Wilesovým dôkazom Veľkej Fermatovej vety a Pereľmanovým dôkazom Poincarého hypotézy).

Viac ako 2 300 000 ľudí si stiahlo preprint s algoritmom z web-stránky, na ktorej ho autori uverejnili, už počas prvých 10 dní (Borneman, 2003). O problematiku prvočísel a predovšetkým o (stále rýchlejšie) algoritmy na testovanie prvočíselnosti je momentálne vo svete skutočne obrovský záujem. Autor článku chce veriť, že tento záujem o prvočísla a otvorené problémy teórie čísel i celej matematiky sa časom prenesie práve cez učiteľov matematiky aj na našich študentov, budúcich učiteľov matematiky a ich žiakov.

Tento článok je výrazným doplnením a prepracovaním autorovho pôvodného článku o prvočíslach (Haviar, 2005), ktorý bol inšpirovaný prednáškou kolegu z Melbourne a jeho poznámkami (Cairns, 2003). Je doplnený o výsledky vlastného skúmania ohľadne prvočísel publikované v článku (Haviar, Maličký, 2009). Otvorené problémy teórie čísel sú na rozdiel od pôvodného článku (Haviar, 2005) spájané s osemtisícovkami našej planéty, ktorých je 14. S tým, že ku každému z prezentovaných otvorených problémov teórie čísel je priradená osemtisícovka s uvedením jej názvu, dátumu zdolania a obrázku.

Primoriálne prvočísla

Prvočíslo je prirodzené číslo p≥2, ktorého jedinými kladnými deliteľmi sú p a 1. Symbolom p_k označíme k-te prvočíslo, čiže p_1=2, p_2=3, p_3=5, atď. Je známe od antických čias, Euklida z Alexandrie, ktorý žil asi v období (365-300) pred Kristom, že prvočísel je nekonečne veľa. Klasický prístup, ktorý to ukazuje, sa opiera o pojem *primoriálneho čísla*. Primoriálne číslo P_k je definované ako súčin prvých *k* prvočísel, t.j.

$P_k = p_1 . p_2 . \ldots . p_k$. Dostávame teda:

$P_1 = 2$
$P_2 = 2.3 = 6$
$P_3 = 2.3.5 = 30$
$P_4 = 2.3.5.7 = 210$
$P_5 = 2.3.5.7.11 = 2310$, atď.

Predpokladajme sporom, že by existoval konečný zoznam všetkých prvočísel: $p_1, p_2, \ldots, p_k$. Zoberme *k*-te primoriálne číslo P_k a uvažujme číslo $P_k + 1$. Každé prirodzené číslo väčšie ako 1 je deliteľné prvočíslom, teda aj $P_k + 1$ je deliteľné nejakým prvočíslom p_i. Predpoklad, že P_k je súčinom všetkých prvočísel znamená, že P_k je deliteľné prvočíslom p_i. Preto aj $1 = (P_k + 1) - P_k$ je deliteľné prvočíslom p_i, čo je požadovaný spor. Neexistuje konečný zoznam prvočísel, prvočísel je nekonečne veľa.

Ako väčšina matematiky, aj tento dôkaz môže žiaka inšpirovať alebo odradiť. Existuje niekoľko „intelektuálnych obtiaží" v tomto dôkaze. Azda najväčšou je pre žiaka samotný pojem dôkazu a motivácia pre dôkaz. Autorov kolega a priateľ z Melbourne Grant Cairns spomínal (Cairns, 2003) na vlastnú skúsenosť, keď prezentoval vyššie uvedený dôkaz svojmu 10-ročnému synovi Desmondovi. Spomenul mu, že dôkaz urobil Euklides pred vyše dvetisíc rokmi. Vzápätí začal dôkaz rétorickou otázkou: „Ako vieme, že je nekonečne veľa prvočísel?" Desmond ho ihneď prerušil: „Veď si mi práve povedal, že nejaký chlapík to už ukázal!" Desmond jednoducho nevidel dôvod sa tým ďalej zaoberať. Pre neho v tomto veku, ako pre mnoho mladých ľudí vo všeobecnosti, sú vedomosti spájané s akumulovaním faktov a ich zapamätaním si. Nie je ľahké presvedčiť ich, že *porozumenie* je dôležitejšie ako pamäť. Existuje voči tomu prirodzená rezistencia, pretože dosiahnuť porozumenie je väčšinou ťažšie než sa niečo naučiť naspamäť. V matematike je to však nevyhnutné a už „učňovské roky" si vyžadujú porozumenie takým dôkazom ako je ten Euklidov o nekonečnom počte prvočísel.

Druhou „intelektuálnou obtiažou" uvedeného dôkazu môže byť aplikovanie logického nástroja *reductio ad absurdum* čiže *dôkazu sporom*. Sám Euklides ho použil úspešne už k dôkazu existencie iracionálneho čísla. Anglický matematik G. H. Hardy o tom vo svojom slávnom diele *Obrana matematikova* píše: „Reductio ad absurdum, ktoré Euklides tak miloval, je jednou z matematikových najskvelejších zbraní. Je ďaleko krásnejší ako šachový gambit: šachista pri gambite ponúka pešiaka alebo figúru, matematik však ponúka celú hru." (Singh, 2000).

Tretí obtiažny aspekt dôkazu je uvedomenie si, že v skutočnosti nedokazuje, že $P_k + 1$ je prvočíslo. Čísla $P_k + 1$ sú síce prvočísla pre k = 1, 2, 3, 4, 5, ale už $P_6 + 1 = 30031$ nie je prvočíslo: $30031 = 59 \cdot 509$. Prvočísla tvaru $P_k + 1$ resp. $P_k - 1$ sa nazývajú *primoriálne prvočísla*. Je pravdepodobné, že ich je nekonečne veľa, ale nikto to doposiaľ nedokázal:

Problém č. 1: Je primoriálnych prvočísel nekonečne veľa?

Prvá osemtisícovka – Annapurna, 8091 m (zdolaná 3.6.1950)

Prvočísla majú „častý“ výskyt

V tejto časti uvedieme tri známe tvrdenia v teórii čísel, z toho dve slávne hypotézy, ktoré podporujú rozšírenú intuíciu, že prvočísla sa vyskytujú pomerne „často“ v postupnosti prirodzených čísel (t.j. nezáporných celých čísel). Nielenže je nekonečne veľa prvočísel ako bolo ukázané už vyše 300 rokov pred Kristom Euklidom, ale je aj nekonečne veľa prvočísel rôznych druhov. Medzi najstaršie výsledky tohto typu patrí Dirichletova veta:

Dirichletova veta ([1837]): Ak sú prirodzené čísla a, b nesúdeliteľné, potom v aritmetickej postupnosti

a, a + b, a + 2b, a + 3b, … je nekonečne veľa prvočísel.

K výsledkom poukazujúcim na „častý výskyt“ prvočísel v postupnosti prirodzených čísel radíme aj nasledujúce dve hypotézy, o ktorých pravdivosti sa v teórii čísel príliš nepochybuje. Pripomeňme, že *prvočíselnými dvojčatami* nazývame dvojicu prvočísel v tvare (p, p + 2), ako sú napríklad (3, 5), (5, 7), (11,13), (17, 19) či (29, 31).

Problém č. 2 (Prime Twin Conjecture – Hypotéza prvočíselných dvojčiat [cca 500 rokov pred Kristom]): ***Existuje nekonečne veľa prvočíselných dvojčiat.***

Problém č. 3 (Goldbach's Conjecture – Goldbachova hypotéza [7.6. 1742]): ***Každé párne číslo n≥4 je možné vyjadriť ako súčet dvoch prvočísel.***

V roku 2001 Richstein publikoval v časopise *Math. Comp.* článok s názvom „Overenie Goldbachovej hypotézy po 4.10^{14}“, dnes je overená už aj pre väčšie párne čísla. V súvislosti s vydaním anglickej verzie knihy (Doxiadis, 2000) bola ponúknutá cena 1 milión USD za vyriešenie Goldbachovej hypotézy do dvoch rokov. Jeden z najfascinujúcejších a najstarších otvorených problémov teórie čísel však zostáva aj naďalej nevyriešený. Je obľúbeným problémom autora tohto článku, jeho „srdcovkou“.

Druhá osemtisícovka – Mount Everest, 8848 m (zdolaná 29.5.1953, vľavo)
Tretia osemtisícovka – Nanga Parbat, 8126 m (zdolaná 3.7.1953, vpravo)

Prvočísla majú „zriedkavý“ výskyt

Na druhej strane sú výsledky, ktoré akoby poukazovali na „zriedkavý výskyt” prvočísel v rámci postupnosti prirodzených čísel. Platí napríklad, že medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriálne číslo P_k môže a tiež nemusí číslo $P_k + 1$ byť prvočíslom, ale nasledujúcich $p_{k+1} - 2$ čísel

$$P_k + 2, P_k + 3, P_k + 4, \ldots, P_k + p_{k+1} - 1$$

je určite zložených: v každom z týchto čísel $P_k + i$ sú totiž oba sčítance, P_k aj i, deliteľné tým istým prvočíslom $p \leq p_k$. Preto je napríklad $P_k + 2$ deliteľné dvoma, $P_k + 3$ deliteľné troma, $P_k + 4$ deliteľné opäť dvoma, atď. Pretože (k+1)-vé prvočíslo p_{k+1} môžeme dosiahnuť ľubovoľne veľké vhodným nárastom k, ukazuje to, že existujú ľubovoľne veľké medzery medzi prvočíslami.

Pre prvočíslo p_k sa medzera po nasledujúce prvočíslo nazýva “prime gap” (vhodným prekladom by mohlo byť *medzera prvočísel*) a označuje sa $g(p_k)$; teda definícia je daná rovnosťou $g(p_k) = p_{k+1} - p_k$. Množstvo štúdií pojednáva o tom ako $g(p_k)$ rastie s p_k, ktoré čísla vznikajú ako medzery prvočísel a ako často sa vyskytujú. Pekným projektom na 2. st. základnej školy by bolo zistiť, ktoré medzery prvočísel sa vyskytujú najčastejšie medzi číslami od 1 po 100. Žiaci by zistili, že najčastejšou medzerou je 2 (teda medzera medzi prvočíselnými dvojčatami). Ak sa však hranica 100 posunie o pár desiatok či stoviek, začne prevažovať medzera prvočísel 4 a údajne od hranice 563 (čitateľ to môže preveriť) začne prevažovať medzera prvočísel 6. Vraj okolo hranice 10^{35} bude najčastejšia medzera prvočísel 30, okolo 10^{425} to bude číslo 210 a vznikla „divoká hypotéza“ (čitateľovi sa neodporúča ju preveriť), že s výnimkou čísla 4 budú “jumping champions“ (t.j. najčastejšie sa vyskytujúce medzery prvočísel po istú hranicu) primoriálne čísla 2, 6, 30, 210, 2310,...

Štvrtá osemtisícovka – K2, 8611 m (zdolaná 31.7.1954)

Problém č. 4: Sú s výnimkou čísla 4 "jumping champions" primoriálne čísla 2, 6, 30, 210,...?

A stále sú aj iné otázky ohľadne medzier alebo rozdielov prvočísel nezodpovedané. Nie je známe, či každé párne číslo vzniká ako medzera prvočísel alebo či vôbec každé párne číslo možno napísať ako rozdiel medzi dvoma (nie nevyhnutne po sebe idúcimi) prvočíslami:

Problém č. 5** (Polignac's Conjecture 1 – Polignacova hypotéza 1 [1849]): **Každé párne prirodzené číslo 2n je rozdielom dvoch prvočísel.

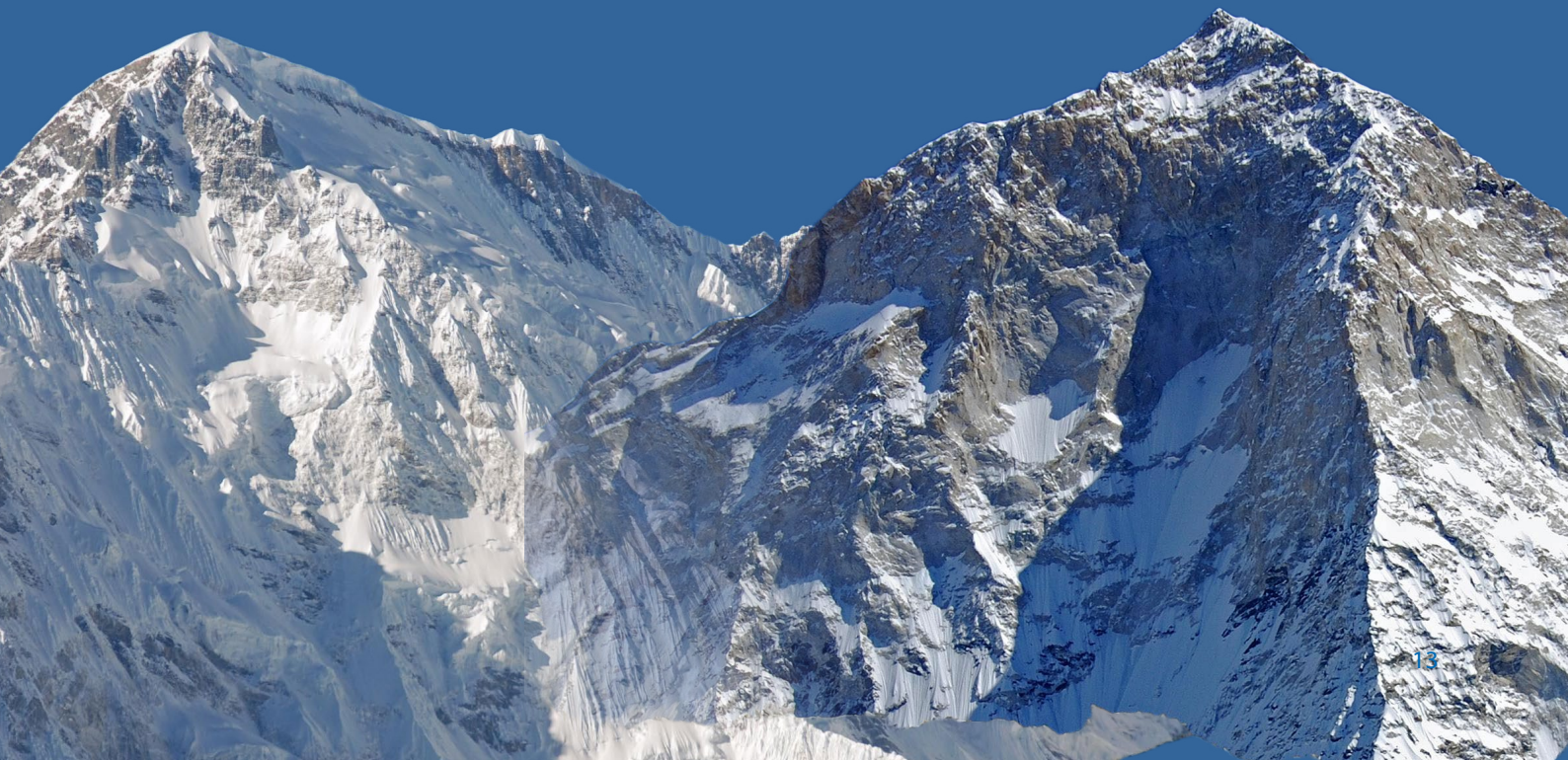
Polignac dokonca tvrdil, každé párne číslo možno napísať ako rozdiel dvoch prvočísel nekonečne veľa spôsobmi:

Problém č. 6** (Polignac's Conjecture 2 – Polignacova hypotéza 2 [1849]): **Dvojíc prvočísel s rozdielom 2n je nekonečne veľa (pre každé párne prirodzené číslo 2n).

Ak by to platilo čo len pre číslo 2, znamenalo by to už platnosť Hypotézy prvočíselných dvojčiat.

Piata osemtisícovka – Cho Oyu, 8201 m (zdolaná 19.10.1954*, vľavo)
Šiesta osemtisícovka – Makalu, 8485 m (zdolaná 15.5.1955, vpravo)

**Ako prvé ženy zdolali Cho Oyu v r. 1984 československé horolezkyne Věra Komárková a Dina Štěrbová (bola aj matematičkou v Olomouci)*



Nevieme „nič“ o prvočíslach

Existuje veľké množstvo otázok ohľadne prvočísel, na ktoré nepoznáme odpoveď. Asi najslávnejšou je *Riemannova* hypotéza ohľadne distribúcie prvočísel, ktorá patrí k tzv. *miléniovým problémom*. Za vyriešenie každého z miléniových problémov je vypísaná odmena 1 milión USD. (V r. 2003 bol vyriešený jeden z nich, *Poincarého hypotéza*, avšak Grigorij Pereľman odmietol za vyriešenie problému prevzatie miliónovej odmeny, čo by bol iste námet na samostatný príbeh.) K Riemannovej hypotéze, ktorú tu nedokážeme v stručnosti prezentovať, by sme doporučili knihy (Derbyshire, 2003) a (Sautoy, 2003).

Poznamenávame, že mnohé hypotézy o prvočíslach už pri malej modifikácii vedú na nové hypotézy, ktoré sa zdajú byť rovnako ťažko overiteľné ako pôvodné. Hypotéza prvočíselných dvojčiat hovorí, že existuje nekonečne veľa dvojíc prvočísel v tvare $(p, p + 2)$. Existujú však aj viaceré príbuzné hypotézy hovoriace, že existuje nekonečne veľa trojíc prvočísel v tvare $(p, p + 2, p + 6)$ a tiež nekonečne veľa trojíc prvočísel v tvare $(p, p + 4, p + 6)$, tzv. prvočíselných trojčiat. Na toto všetko nepoznáme odpoveď. (Vnímavý čitateľ iste príde na to, prečo neexistuje trojica prvočísel v tvare $(p, p + 2, p + 4)$.) Nevieme ani, či existuje nekonečne veľa tzv. prvočíselných štvorčiat v tvare $(p, p + 2, p + 6, p + 8)$, atď. Nevieme naozaj skoro „nič“. (Hypotéza, že pre každé párne prirodzené číslo k existuje nekonečne veľa dvojíc prvočísel v tvare $(p, p + k)$ je vlastne len preformulovaním Polignacovej hypotézy 2.)

Problém č. 7: Existuje nekonečne veľa prvočíselných trojčiat $(p, p + 2, p + 6)$ a nekonečne veľa prvočíselných trojčiat $(p, p + 4, p + 6)$? Existuje nekonečne veľa prvočíselných štvorčiat $(p, p + 2, p + 6, p + 8)$?

Siedma osemtisícovka – Kangchenjunga, 8586 m (zdolaná 25.5.1955)

Tiež existovala slávna a dlho otvorená hypotéza, že pre každé prirodzené n existuje n po sebe idúcich prvočísel v aritmetickej postupnosti. Túto však vyriešil „zázračný“ austrálsky matematik čínskeho pôvodu Terrence Tao spolu s anglickým matematikom Benom Greenom v r. 2004, kedy dokázali tzv. *Green-Taovu vetu*. Tao neskôr už ako 29 ročný získal za tento a ďalšie slávne výsledky tzv. *Fieldsovu medailu*, ktorá je v matematike najvyšším ocenením a udeľuje sa iba na začiatku svetových kongresov v matematike, raz za štyri roky, niekoľkým vybraným matematikom do veku 40 rokov.

Už sme spomenuli, že číslo $P_k + 1$ môže ale nemusí byť prvočíslo. Ak nie je prvočíslo, uvažujme najmenšie prirodzené číslo d_k, že $P_k + d_k$ je prvočíslo. Novozélandský sociálny antropológ Reo Fortune (1903-1979) položil raz otázku, či samotné čísla d_k musia byť prvočíslami (nazývajú sa “fortunate numbers”). Ani na toto nevieme stále odpovedať (t.j. skonštruovať dôkaz), hoci sa predpokladá kladná odpoveď:

Problém č. 8** (Fortune's Conjecture – Fortuneova hypotéza): **Sú čísla d_k (“fortunate numbers”) prvočíslami?

Ôsma osemtisícovka – Manaslu, 8163 m (zdolaná 9.5.1956)

Vieme „všetko“ o prvočíslach

Často sa hovorí, že prvočísla sú zahalené tajomstvom, ktoré človek nikdy nedokáže úplne poodhaliť. Niekedy sa pritom (aj v matematických kruhoch) spomenie, že nepoznáme žiadny explicitný vzorec pre n-té prvočíslo ani žiadnu rekurzívnu formulu, ktorá by určila (n+1)-vé prvočíslo z prvých n prvočísel. Preto iste na mnohých zapôsobí šokujúco, že v roku 1971 indický matematik Gándhí publikoval explicitný vzorec pre n-té prvočíslo! Ide naviac o vzorec relatívne jednoduchý, ktorý teraz uvedieme.

Najprv si všimnime, že primoriálne číslo $P_k = p_1 . p_2 . \ldots . p_k$ má 2^k deliteľov, keďže množina $\{p_1, p_2, \ldots, p_k\}$ má 2^k podmnožín. Napríklad, primoriálne číslo P_3 má 8 deliteľov:

$$\begin{array}{c} 2.3.5 \\ 2.3 \quad 2.5 \quad 3.5 \\ 2 \quad 3 \quad 5 \\ 1 \end{array}$$

Pre každý deliteľ $d \mid P_k$ položíme $\mu(d)=1$, ak d je súčin párneho počtu prvočísel a $\mu(d)=-1$, ak d je súčin nepárneho počtu prvočísel. Funkcia μ sa volá *Möbiusova funkcia*. Uvažujme nasledujúcu sumu počítanú cez všetky delitele d primoriálneho čísla P_k:

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} .$$

Napríklad, pre k = 2 máme $P_k = 2 . 3$ a suma je

$$\frac{1}{2^1-1} + \frac{-1}{2^2-1} + \frac{-1}{2^3-1} + \frac{1}{2^{2.3}-1} = \frac{1}{1} - \frac{1}{3} - \frac{1}{7} + \frac{1}{63} = 1 - \frac{34}{63} .$$

Prvočíslo p_{k+1} sa podľa Gándhího algoritmu z uvedenej sumy vypočíta takto:

(1) Od uvedenej sumy sa odčíta $\frac{1}{2}$.

(2) Z výsledku sa určí logaritmus pri základe 2.
(3) Získaný výsledok sa odčíta od čísla 1.
(4) Z výsledku sa určí celá časť (t.j. číslo sa zaokrúhli nadol na najbližšie celé číslo).
Číslo, ktoré sa týmto dostane je skutočne nasledujúce prvočíslo p_{k+1}.

Veta (Gándhího vzorec). Prvočíslo p_{k+1} možno vyjadriť vzorcom

$$p_{k+1} = [\, 1 - \log_2 (- \frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1} \,],$$

kde [ ] označuje celú časť čísla.

Aplikujme Gándhího vzorec pre k=2 a presvedčme sa, že dá očakávaný výsledok $p_3 = 5$. Pre k=2 sme už vypočítali, že

$$\sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = 1 - \frac{34}{63}.$$

Teda

$$- \frac{1}{2} + \sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = \frac{1}{2} - \frac{34}{63} \approx 0.04,$$

odkiaľ

$$\log_2 (- \frac{1}{2} + \sum_{d|P_2} \frac{\mu(d)}{2^d - 1}) \approx \log_2 (0.04) \approx - 4.6,$$

čiže

$$p_3 = [\, 1 - (- 4.6) \,] = [\, 5.6 \,] = 5.$$

Poznamenávame, že úloha čísla 2 v uvedených sumách a tiež následne ako základu logaritmu je vlastne irelevantná: mohli sme číslo 2 rovnako nahradiť číslom 10 alebo e, a potom použiť logaritmus pri základe 10 resp. prirodzený logaritmus. Gándhího vzorec je kombináciou *Eratostenovho sita* (podľa gréckeho matematika Eratostenosa z Kyrény, ktorý pôsobil v 3. st. pred Kristom) a nekonečného radu

$$\frac{1}{2^d - 1} = \frac{1}{2^d} + \frac{1}{2^{2d}} + \frac{1}{2^{3d}} + \dots$$

Pomocou tohto rozvoja vieme upraviť vyššie uvedenú sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} - (\frac{1}{2^{p_1} - 1} + \frac{1}{2^{p_2} - 1} + \dots + \frac{1}{2^{p_k} - 1}) + \dots$$

na tvar

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \left(\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots\right) - \left(\frac{1}{2^{p_1}} + \frac{1}{2^{2p_1}} + \frac{1}{2^{3p_1}} + \ldots\right.$$
$$+ \frac{1}{2^{p_2}} + \frac{1}{2^{2p_2}} + \frac{1}{2^{3p_2}} + \ldots$$
$$\ldots$$
$$\left. + \frac{1}{2^{p_k}} + \frac{1}{2^{2p_k}} + \frac{1}{2^{3p_k}} + \ldots\right)$$
$$+ \ldots.$$

Vidíme, že od súčtu všetkých zlomkov $\frac{1}{2^n}$ sa postupne odčítajú všetky zlomky, v ktorých exponent *n* je deliteľný prvočíslom p_1, potom p_2, atď. Zlomky $\frac{1}{2^n}$ v ktorých *n* je deliteľné prvočíslom p_1 a súčasne p_2 sa síce odpočítajú dvakrát, ale v nasledujúcej zátvorke sa zase naspäť pripočítajú a tak to funguje aj s ďalšími členmi. Takže po odstránení prvého zlomku $\frac{1}{2}$ zostanú v uvedenej sume len zlomky $\frac{1}{2^n}$, v ktorých *n* nie je deliteľné žiadnym z prvočísel $p_1, p_2, \ldots, p_k$. *Eratostenovo* sito nám potom hovorí, že prvý zo zlomkov, ktoré zostali bude $\frac{1}{2^{p_{k+1}}}$. Preto (záporné) číslo

$$\log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right)$$

je trochu väčšie než $-p_{k+1}$, čiže

$$1 - \log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right)$$

je trochu menšie ako $1+p_{k+1}$, a teda

$$\log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right] = p_{k+1}.$$

Poznámky ku Gándhího vzorcu a jeho ďalšie dôkazy možno nájsť napríklad v knihe (Ribenboim, 2000).

Pseudoprvočísla

Gándhího algoritmus je krásny, ale žiaľ nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d \mid P_k$ rastie s číslom k *exponenciálne* a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Našťastie sú rýchlejšie spôsoby nájdenia (veľkých) prvočísel:

(1) Nájdu sa čísla, ktoré sú s veľkou pravdepodobnosťou prvočísla.
(2) Overí sa, že tieto čísla sú skutočne prvočísla.

Na úlohu (1) sa používa test $n \mid 2^n - 2$. Spĺňajú ho všetky prvočísla (podľa Malej Fermatovej vety) a len veľmi málo zložených čísel (napr. $n = 341 = 11 \times 31$): tieto zložené čísla sa volajú *pseudoprvočísla*. Ak teda číslo n prejde testom $n \mid 2^n - 2$, je s veľmi veľkou pravdepodobnosťou prvočíslo.

K úlohe (2), teda overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov. Otvorenou otázkou zostávalo, či existuje *polynomiálny algoritmus* pre testovanie prvočíselnosti, teda taký, ktorého trvanie je polynomiálna funkcia počtu číslic daného čísla. V roku 2002 Maningra Agrawal, Neeraj Kayal a Nitin Saxena z Indian Institute of Technology v Kanpure šokovali svet nájdením takého algoritmu. *AKS polynomiálny algoritmus* prekvapuje relatívnou jednoduchosťou a jeho štartujúcim bodom je zovšeobecnenie Malej Fermatovej vety: ak $1 < a < p$, tak p je prvočíslo práve vtedy, keď koeficienty polynómu $(x - a)^p - (x^p - a)$ sú všetky deliteľné p. Vynikajúcim zdrojom informácií o AKS algoritme je kniha (Borneman, 2003). Autori, z ktorých poslední dvaja boli v čase objavu len študentami s čerstvými bakalárskymi diplomami, získali v r. 2006 za svoj výsledok prestížne ceny: Gödelovu a Fulkersonovu. Ich úspech môže byť povzbudením pre mnohých mladých matematikov i vedcov.

Fermatove čísla

Sú to čísla, ktorými sa zaoberal Fermat a majú tvar $F_n = 2^{2\wedge n} + 1$ (exponent mocniny je 2^n), kde za n dosadzujeme prirodzené čísla 0,1,2,3,... Dnes sa nazývajú *Fermatove čísla* a pokiaľ sú prvočíslami, tak sa volajú *Fermatove prvočísla*. Fermat bol v 17. storočí schopný vypočítať (samozrejme „ručne“) iba prvých päť z nich:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537.$$

Číslo $F_5 = 2^{32}$ Fermat nevypočítal.

Pretože prvých päť z uvedených čísel boli všetky prvočíslami, Fermat s jemu vlastnou „odvahou“ vyslovil okolo r. 1640 hypotézu, že všetky čísla uvedeného tvaru budú prvočíslami. O necelé storočie neskôr v r. 1732 Euler ukázal, že $F_5 = 2^{32}$ nie je prvočíslom! Euler našiel aj jeho rozklad: $F_5 = 2^{32} = 641 \cdot 6\,700\,417$. Čo je naozaj pozoruhodné, všetky ďalšie doteraz známe Fermatove čísla F_n sú zložené! Poznáme teda stále len tých päť Fermatovych prvočísel, ktoré objavil už Fermat. Čo možno považovať za ešte prekvapujúcejšie, ani s dnešnou silou výpočtovej techniky nedokážeme určiť, či je Fermatovo číslo $F_{33} = 2^{2\wedge 33} + 1$ (exponent mocniny je 2^{33}) prvočíslom alebo nie. (Je to dobrý príklad a lekcia pre tých, ktorí si azda myslia, že dnešné počítače nám dokážu spočítať takmer všetko! Samozrejme, funkčný kvantový počítač budúcnosti nebude mať problém uvedenú otázku, či je Fermatovo číslo F_{33} prvočíslom, zodpovedať.)

Teda vieme, že sa nenachádza žiadne prvočíslo medzi číslami F_5, F_6, ..., F_{32}. Zdá sa, akoby sa Fermat mýlil „maximálne“ ako sa len mohol! Napriek tomu, že poznáme stále iba päť Fermatovych prvočísel, existuje hypotéza z polovice 19. storočia, ktorá hovorí, že v postupnosti Fermatovych čísel sa nachádza nekonečne veľa prvočísel:

Problém č. 9** (Eisenstein's Conjecture – Eisensteinova hypotéza [1844]): **Fermatových prvočísel je nekonečne veľa.

Deviata osemtisícovka – Gasherbrum II, 8035 m (zdolaná 7.7.1956)

Poznamenávame na tomto mieste, že uvedená Eisensteinova hypotéza vyplynie pomerne ľahko z inej hypotézy, nazvanej *zovšeobecnenou Dirichletovou vetou*, ktorú publikoval autor tohto článku v r. 2009 spolu s kolegom Petrom Maličkým a ktorú uvedieme nižšie v rámci autorovho vlastného príspevku k skúmaniu prvočísel.

Pomocou Fermatových čísel možno aj dokázať iným spôsobom, že prvočísel je nekonečne veľa. Je to Godbachova myšlienka z 18. storočia, ktorá hovorí, že nekonečnosť počtu prvočísel vyplýva z existencie (nekonečnej) postupnosti rôznych a po dvoch nesúdeliteľných prirodzených čísel. Podľa Základnej vety aritmetiky možno každé prirodzené číslo väčšie ako 1 jednoznačne rozložiť na súčin prvočísel. V postupnosti po dvoch nesúdeliteľných prirodzených čísel má teda každý člen svojho prvočíselného deliteľa. Tieto prvočíselné delitele musia byť rôzne, keďže dané čísla sú po dvoch nesúdeliteľné a týchto prvočíselných deliteľov je nekonečne veľa, pretože daná postupnosť rôznych a po dvoch nesúdeliteľných prirodzených čísel je nekonečná. Takže z existencie (nekonečnej) postupnosti rôznych a po dvoch nesúdeliteľných prirodzených čísel tiež vyplýva, že prvočísel je nekonečne veľa.

Teraz ukážeme, prečo členy postupnosti (F_n; n = 0, 1, 2, 3, …) Fermatových čísel sú po dvoch nesúdeliteľné: Fermatove čísla sú nepárne, preto číslo 2 nie je ich deliteľom. Predpokladajme, že prvočíslo p > 2 je deliteľom nejakého Fermatovho čísla F_n. Teda $p \mid F_n$, čiže $F_n \equiv 0 \pmod p$ t.j. $2^{2\wedge n} + 1 \equiv 0 \pmod p$, odkiaľ $2^{2\wedge n} \equiv -1 \pmod p$. Po umocnení oboch strán číslom 2^k máme $F_{n+k} = 2^{2\wedge(n+k)} + 1 = (2^{2\wedge n})^{2\wedge k} + 1 \equiv (-1)^{2\wedge k} + 1 = 2 \pmod p$. Teda ak $p \mid F_n$, tak Fermatovo číslo F_{n+k} pri delení prvočíslom p > 2 dáva zvyšok 2, čiže nie je deliteľné prvočíslom p. Keďže uvažovaná dvojica F_n, F_{n+k} členov postupnosti (F_n; n = 0, 1, 2, 3, …) čísel bola ľubovoľná, sú Fermatove čísla po dvoch nesúdeliteľné.

Vlastný výskum k prvočíslam a jeho výsledky. Superprvočísla

Najobľúbenejšie prvočíslo autora je 23. (Má ho ako orientačné číslo domu, ale hlavne je to deň narodenia manželky.) Pri jednej z ciest do Oxfordu ho napadlo, že by mohlo byť zaujímavé skúmať prvočísla ako 23, ktoré majú aj cifry prvočíselné, nazval ich *superprvočísla (superprimes)*. Tak vznikla spolupráca s kolegom doc. RNDr. Petrom Maličkým, CSc. na tejto téme a jej výsledkom bol článok (Haviar, Maličký, 2009). Za hlavné výsledky v ňom možno považovať tri ďalšie otvorené problémy teórie čísel („osemtisícovky"), ktorými sú hypotézy autorov o superprvočíslach. Zrejme najcennejší výsledok článku je ale posledný otvorený problém, ktorým je hypotéza s názvom Zovšeobecná Dirichletova veta. (Pôvodná Dirichletova veta je z roku 1837 a zmienili sme ju vyššie pred Hypotézou prvočíselných dvojčiat.) Z tejto hypotézy totiž pomerne ľahko vyplývajú dve slávne hypotézy. Prvá je Eisensteinova hypotéza z r. 1844, ktorá hovorí, že Fermatových prvočísel je nekonečne veľa (hoci stále poznáme len tých päť, ktoré našiel ešte Fermat). Druhá je rovnako slávna hypotéza, že aj tzv. Mersennových prvočísel je nekonečne veľa. V tejto chvíli je ich známych 51 a za posledné štvrťstoročie takmer všetky novo objavené najväčšie známe prvočísla, včítane posledného objaveného

v r. 2018, sa zaradili práve medzi Mersennove prvočísla. Zavedieme ich zakrátko nižšie.

Superprvočíslom sme teda v článku (Haviar, Maličký, 2009) nazvali každé také prvočíslo, ktorého všetky cifry (v dekadickom zápise) sú tiež prvočíslami (ide teda o cifry 2,3,5 a 7). Superprvočísel do tisíc je evidentne pätnásť: 2, 3, 5, 7, 23, 37, 53, 73, 223, 227, 233, 257, 277, 337, 353, 373, 523, 557, 577, 727, 733, 757, 773. Prvé zaujímavé z nich je zmienené číslo 23, ktoré bolo teda motiváciou pre skúmanie. Následne sme symbolom S_k označili počet k-ciferných superprvočísel a s pomocou matematického softvéru Mathematica sme zistili nasledujúce hodnoty pre čísla S_1 až S_{15}:

k	S_k	**k**	S_k	**k**	S_k
1	4	**6**	389	**11**	214 432
2	4	**7**	1 325	**12**	781 471
3	15	**8**	4 643	**13**	2 885 201
4	38	**9**	16 623	**14**	10 687 480
5	128	**10**	59 241	**15**	39 838 489

Uvedené hodnoty ukazujú, že s rastúcim počtom cifier *k* výrazne rastie aj počet *k*-ciferných superprvočísel. Preto asi nikoho neprekvapí, že sme formulovali nasledovné dva otvorené problémy ako hypotézy (ich platnosť sa nám javí takmer istá, ale podobne ako napr. pri Hypotéze prvočíselných dvojčiat netušíme ako by sa dokazovali):

Problém č. 10 *(Hypotéza o nekonečnom počte superprvočísel):* ***Existuje nekonečne veľa superprvočísel.***

Problém č. 11 *(Hypotéza o existencii k-ciferného superprvočísla pre každé k):* ***Pre každé celé číslo k>0 existuje k-ciferné superprvočíslo.***

Desiata osemtisícovka – Lhotse, 8516 m (zdolaná 18.5.1956, vľavo)
Jedenásta osemtisícovka – Broad Peak, 8051 m (zdolaná 9.6.1957, vpravo)

Ďalej sme zaviedli tzv. *zosilnené superprvočísla* ako tie, kde naviac každá dvojica po sebe idúcich cifier dáva prvočíslo. Opäť s pomocou matematického softvéru Mathematica sme zistili, že vychádzajú iba tri typy zosilnených superprvočísel:

(1) Začínajúce s 23, za ktorým je n kópií 73, prvé také superprvočíslo je 237373 (n=2);
(2) Začínajúce s 53, za ktorým je n kópií 73, prvé také superprvočíslo je 537373 (n=2);
(3) Začínajúce s 5, za ktorým je n kópií 37, prvé také superprvočíslo je 5373737 (n=3).

Vyslovili sme ďalší otvorený problém ako hypotézu:

Problém č. 12 *(Hypotéza o nekonečných počtoch zosilnených superprvočísel):* ***Existuje nekonečne veľa zosilnených superprvočísel každého z typov (1)-(3).***

Zovšeobecnená Dirichletova postupnosť a hypotéza Zovšeobecnenej Dirichletovej vety

Pripomeňme, že *Dirichletovou postupnosťou* nazývame každú aritmetická postupnosť (a, a + b, a + 2b, a+ 3b,...) s diferenciou b, kde a,b sú nesúdeliteľné prirodzené čísla a že Dirichletova veta z r. 1837 hovorí, že v každej takejto postupnosti je nekonečne veľa prvočísel. Najcennejším príspevkom k skúmaniu prvočísel z práce (Haviar, Maličký, 2009) je zavedenie pojmu *zovšeobecnenej Dirichletovej postupnosti* a následne formulovanie zovšeobecnenej *Dirichletovej vety* ako hypotézy, z ktorej vyplývajú aj hypotézy o nekonečnom počte Fermatových a Mersennových prvočísel.

Dvanásta osemtisícovka – Gasherbrum I, 8080 m (zdolaná 5.7.1958)

Zovšeobecnenou Dirichletovou postupnosťou (Generalised Dirichlet's Sequence, GDS) nazývame každú číselnú postupnosť (x_n ; n = 0, 1, 2, 3,...) definovanú rekurzívnym predpisom

$$x_{n+1} = c \,.\, x_n + b,$$

teda číselnú postupnosť (x_0, $c.x_0$+ b, $c.(c.x_0$+ b)+b, $c.[c.(c.x_0$+ b)+ b]+ b,...), kde c, b, x_0 sú celé čísla a čísla b, $c.x_0$ sú nesúdeliteľné. Po zvolení pevnej hodnoty parametra c = 1 a prvého člena x_0 = a z nej dostaneme priamo Dirichletovu postupnosť (a, a + b, a + 2b, a+ 3b,...), preto sme ju nazvali zovšeobecnenou Dirichletovou postupnosťou. Pre hodnoty c ≠ 1 dostaneme pre n-tý člen explicitný vzorec

$$x_n = c^n.x_0 + b.\frac{c^n - 1}{c - 1}.$$

Naviac sme predpokladali v našom článku (Haviar-Maličký, 2009), že parameter *c* nemá hodnoty -1 ani 0 vedúce k triválnym prípadom a taktiež, že b ≠ -(c-1).x_0 , pretože inak by daná postupnosť bola konštantná. Naším cieľom bolo nájsť podmienky za ktorých by v duchu pôvodného Dirichletovho výsledku postupnosť obsahovala nekonečne veľa prvočísel. Našou stratégiou bolo nájsť najprv podmienky, za ktorých naša postupnosť obsahuje konečne veľa prvočísel a následne predpokladom, že tieto podmienky neplatia sa snažiť zabezpečiť uvedený cieľ. Poďme ilustrovať hľadanie daných podmienok.

Ak v zovšeobecnenej Dirichletovej postupnosti zvolíme prvý člen x_0 = 3 a počiatočné parametre c = 5 a b = 1, dostaneme postupnosť (3, 16, 81, 406, 2031, 10156, 50781, ...), kde všetky párne členy (včítane nultého člena x_0) sú násobky čísla 3 a všetky nepárne členy sú násobky čísla 2. Zovšeobecnená Dirichletova postupnosť môže mať teda rozklad na *k* podpostupností s členmi danými pre n = 1, 2, 3, ... predpismi

$$x_{kn} = c^k \,.\, x_{k(n-1)} + (c^{k-1} + ... + c + 1) \,.\, b,$$

$$x_{kn+1} = c^k \,.\, x_{k(n-1)+1} + (c^{k-1} + ... + c + 1) \,.\, b,$$

$$.....$$

$$x_{kn+(k-1)} = c^k \,.\, x_{k(n-1)+(k-1)} + (c^{k-1} + ... + c + 1) \,.\, b,$$

z ktorých každá má vlastného netriviálneho (t.j. väčšieho ako 1) deliteľa. V ilustrujúcej postupnosti (3, 16, 81, 406, 2031, 10156, 50781, ...) sú u dvoch jej podpostupností (k=2) (3, 81, 2031, 50781, ...) a (16, 406, 10156, ...) týmito deliteľmi čísla 3 resp. 2. Označme tieto delitele d_0 = 3 a d_1 = 2. Je vidieť , že ak nejaké číslo d_j > 1 delí vo vyššie uvedených podpostupnostiach zátvorky $A_k = (c^{k-1} + ... + c + 1)$ a delí aj prvý člen podpostupnosti x_j, tak číslo d_j delí aj všetky ďalšie členy danej podpostupnosti (j=0,1,...,k-1). V ilustrujúcom príklade máme k=2, následne zátvorka $A_k = A_2 = 5^1 + 1 = 6$ a najväčšie spoločné delitele zátvorky s prvými členmi podpostupností sú $D(A_2,x_0)=D(6,3)=3$, $D(A_2,x_1)=D(6,16)=2$.

Dostali sme prvú podmienku:

(P1) Zovšeobecnená Dirichletova postupnosť (x_n ; n = 0, 1, 2, 3,...) má konečne veľa prvočísel, ak existuje k ≥ 2, že pre všetky j=0,...,k-1 existuje číslo d_j >1, že $d_j \mid D(A_k,x_j)$.

Uvedieme ďalšie dve naše podmienky z článku (Haviar, Maličký, 2009), ktoré garantujú, že zovšeobecnená Dirichletova postupnosť má konečne veľa prvočísel:

(P2) Zovšeobecnená Dirichletova postupnosť (x_n ; n = 0, 1, 2, 3,...) má konečne veľa prvočísel v prípade hodnôt parametrov $c=e^4$, $b=4d^4.(1-e^4)$ a hodnoty prvého člena $x_0 = a^4 +4d^4$, kde e ≥ 2, d ≥ 1, a ≥ 1 sú celé čísla;

(P3) Zovšeobecnená Dirichletova postupnosť (x_n ; n = 0, 1, 2, 3,...) má konečne veľa prvočísel v prípade hodnôt parametrov $c=e^4$, $b=d^4.(1-e^4)$ a hodnoty prvého člena $x_0 = 4a^4 +d^4$, kde e ≥ 2, d ≥ 1, a ≥ 1 sú celé čísla.

Dôvodom je objavená rovnosť francúzskej matematičky Sophie Germain (1776 – 1831):

$$x^4 + 4y^4 = (x^2 + 2xy + 2y^2) . (x^2 - 2xy + 2y^2) = [(x+y)^2 + y^2)] . [(x-y)^2 + y^2)].$$

S použitím tohto vzorca dostaneme v uvedených podmienkach nasledovné vyjadrenia pre n-tý člen xn zovšeobecnenej Dirichletovej postupnosti, kde n = 0,1,2,3,...:

$$(P2)\ x_n = a^4e^{4n} + 4d^4 = [(ae^n + d)^2 + d^2] . [(ae^n - d)^2 + d^2];$$
$$(P3)\ x_n = 4a^4e^{4n} + d^4 = [(d + ae^n)^2 + e^{2n}] . [(d - ae^n)^2 + a^2e^{2n}].$$

Je vidieť, že faktory v zátvorkách sú väčšie ako 1 okrem prípadu d=1, α=1 a n=0.

S uvedenou rovnosťou Sophie Germain súvisí aj naša podmienka (P4):

(P4) Zovšeobecnená Dirichletova postupnosť (x_n ; n = 0, 1, 2, 3,...) má konečne veľa prvočísel v prípade hodnôt parametrov $a=e^m$, $b=d^m.(e^m - 1)$ a hodnoty prvého člena $x_0 = a^m – d^m$, kde d ≠ 0, a ≠ 0 a e rôzne od -1,0,1 sú celé čísla.

Posledné dve podmienky (P5) a (P6) sa týkajú tzv. zovšeobecnených Mersennových čísel. Najprv si povieme, že Marin Mersenne (1588 – 1648) bol francúzsky matematik, filozof, hudobný teoretik („otec akustiky") a teológ, podľa ktorého sa nazývajú prvočísla v tvare

$$M_p = 2^p – 1,$$

kde exponent p je prvočíslo. (Nie pre všetky prvočísla p je $2^p – 1$ prvočíslom, príkladom je $2^{11} – 1=23 . 89$.) Prvých desať Mersennovych prvočísel je 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, 2305843009213693951, 618970019642690137449562111...

Je známych 51 Mersennových prvočísel. Zatiaľ najväčšie známe Mersennovo prvočíslo je $2^{82\,589\,933}$, bolo objavené v decembri roku 2018 (*Largest Known Prime Number*, 2023) a má takmer 25 miliónov cifier.

Zovšeobecnené Mersennove čísla majú tvar $\frac{e^n-1}{e-1}$, kde číslo *e* rôzne od -1,0,1 je celé číslo a *n* prirodzené číslo. Tieto čísla tiež môžu byť prvočísla iba v prípadoch, keď *n* je prvočíslom, avšak je zaujímavé, že môžu byť prvočíslami iba pre konečne veľa hodnôt *n*. Podmienky (P5) a (P6) majú nasledovné znenia:

(P5) Zovšeobecnená Dirichletova postupnosť (x_n; n = 0, 1, 2, 3,...) má konečne veľa prvočísel v prípade hodnôt parametrov

$c=^{km}$, $b=\pm\frac{e^{km}-1}{e^m-1}$ *a hodnoty prvého člena* $x_0=\pm\frac{e^{jm}-1}{e^m-1}$ pri voľbe rovnakých znamienok v ± , kde e rôzne od -1,0,1 a j ≥ 0, k ≥ 1, m ≥ 2 sú celé čísla;

(P6) zovšeobecnená Dirichletova postupnosť (x_n; n = 0, 1, 2, 3,...) má konečne veľa prvočísel v prípade hodnôt parametrov

$c=(-4e^4)^k$, $b=\pm\frac{(-4)^k e^{4k}-1}{-4e^4-1}$ a hodnoty prvého člena $x_0=\pm\frac{(-4)^j e^{4j}-1}{-4e^4-1}$ pri voľbe rovnakých znamienok v ± , kde e ≥ 1, k ≥ 1, j ≥ 0 sú celé čísla.

Následne sme v článku (Haviar-Maličký, 2009) formulovali ako otvorený problém hypotézu *Zovšeobecnenej Dirichletovej vety*, ktorá je v duchu Dirichletovej vety [1837]:

Problém č. 13 *(Generalised Dirichlet's Theorem - Zovšeobecnená Dirichletova veta [2009]):* ***Predpokladajme, že c, b, x_0 sú celé čísla a D(b, c.x_0) = 1. Predpokladajme, že zovšeobecnená Dirichletova postupnosť (x_n ; n = 0, 1, 2, 3,...) daná rekurzívnym predpisom***

$$x_{n+1} = c \,.\, x_n + b,$$

nespĺňa žiadnu z podmienok (P1)-(P6). Potom táto postupnosť obsahuje nekonečne veľa prvočísel.

Trinásta osemtisícovka – Dhaulagiri, 8167 m (zdolaná 13.5.1960)

Nekonečné počty Fermatových a Mersennových prvočísel

V práci (Haviar, Maličký, 2009) sme následne ukázali ako z hypotézy Zovšeobecnenej Dirichletovej vety vyplývajú zmienené hypotézy o nekonečnom počte Fermatových a Mersennových prvočísel. Najprv naznačíme odvodenie *Eisensteinovej hypotézy:*

Pre hodnoty parametrov c = 2, b = -1 a pre hodnotu prvého člena $x_0 = 2$ je v našej *zovšeobecnenej Dirichletovej postupnosti* s predpisom $x_{n+1} = c \cdot x_n + b$ evidentné, že jej n-tý člen je $x_n = 2^n + 1$. Je známe, že toto je prvočíslom iba keď $n = 2^k$, kedy je x_n potom Fermatovým prvočíslom. Je ľahké vidieť, že podmienka (P1) nie je splnená, pretože čísla $A_k = 2^k - 1$ a $x_0 = 2$ nemajú evidentne spoločného deliteľa $d > 1$. Podobne sa dá ukázať, že ani podmienky (P2) - (P6) nie sú splnené. Preto z našej Zovšeobecnenej Dirichletovej vety ako hypotézy vyplýva ako dôsledok *Eisensteinova hypotéza* z r. 1844, ktorá hovorí, že Fermatových prvočísel je nekonečne veľa. (Hoci poznáme stále len tých päť, ktoré objavil pred takmer štyrmi storočiami Fermat.)

Problém č. 14: Existuje nekonečne veľa Mersennových prvočísel.

Štrnásta osemtisícovka – Shishapangma, 8027 m (zdolaná 2.5.1964)

Záver

Teória čísel je stále považovaná za „kráľovskú disciplínu matematiky" a terajší i budúci učitelia matematiky (aspoň tí s atestáciou) by mali mať aspoň základný prehľad o jej histórii, slávnych problémoch a hypotézach a stále otvorených otázkach. Tiež aj „aké-také poňatie" o aktuálnych objavoch - aspoň o tých najzaujímavejších resp. najväčších ako bolo napríklad nájdenie vzorca pre *n*-té prvočíslo Gándhím v roku 1971 resp. vyriešenie slávnej Fermatovej vety Wilesom v roku 1994 či objavenie polynomiálneho algoritmu testovania prvočíselnosti trojicou Agrawal-Kayal-Saxena v roku 2002. Keďže Wilesov objav sa stal známy aj u nás vďaka českému prekladu knihy (Singh, 1998), z danej trojice významných objavov sa v tomto príspevku venujeme objavom indických matematikov, ktoré sú u nás menej známe. Okrem toho sú spomenuté Dirichletova veta, hypotézy o nekonečnom počte primoriálnych prvočísel a prvočíselných dvojičiek, Goldbachova hypotéza a Polignacove hypotézy. Tieto hypotézy sú tak jednoducho formulovateľné, že učitelia matematiky by ich mohli (a myslíme si, že by aj mali) prezentovať svojím žiakom ako dobré príklady stále otvorených otázok súčasnej matematiky. Autor tohto príspevku vybral do neho 14 otvorených a väščinou aj jednoducho formulovaných problémov o prvočíslach ako „osemtisícovky teórie čísel". Zdroj (Primepuzzles.net, 2023) uvádza 95 takýchto otvorených problémov, väčšinou týkajúcich sa teórie čísel.

Poďakovanie: Autor vyjadruje poďakovanie prof. Grantovi Cairnsovi (La Trobe University, Melbourne) za jeho inšpiratívnu prednášku o prvočíslach v decembri 2003 v Melbourne a poskytnutie jeho poznámok (Cairns, 2003), ktoré sa stali základom aj pre tento príspevok. Taktiež vyjadruje poďakovanie prof. Paulovi Ribenboimovi za jeho začiatky v algebre v oblasti, v ktorej autor tohto článku neskôr napísal dizertáciu a za jeho lásku k prvočíslam a veľkým príbehom matematiky, ako bol príbeh Veľkej Fermatovej vety. Ich šírením inšpiruje k nasledovaniu popularizácie matematiky aj ďalších ľudí. Článok venuje autor práve Paulovi Ribenboimovi, ktorého stretol na algebraickej konferencii v r. 1994, k jeho okrúhlym 95. narodeninám, ktoré mal Paul 13. marca 2023.

Literatúra

BORNEMAN,F., 2003. Spectra PRIMES is in P: a breakthrough for "Everyman". Notices Amer. Math. Soc. 50 (2003), 545-552.

CAIRNS, G., 2003. The prime number family and their relatives. La Trobe University Pre-print, Melbourne, 2003, 11pp.

DERBYSHIRE, J., 2003. Prime Obsesion. Joseph Henry Press, Washington, 2003.

DOXIADIS, A., 2000. Uncle Petros and Goldbach's conjecture. Bloomsbury, New York, 2000.

HAVIAR, M., 2005. Čo by mohli učitelia budúcich učiteľov matematiky vedieť o prvočíslach. Induktívne a deduktívne prístupy v matematike : zborník príspevkov z konferencie s medzinárodnou účasťou, Smolenice 20.4-22.4. 2005. - Trnava : Trnavská univerzita v Trnave, 2005. - ISBN 9788080820305. – s. 99-106.

HAVIAR, M., MALIČKÝ, P., 2009. Superprimes and Generalised Dirichlet Theorem. Acta Universitatis Matthiae Belii, ser. Mathematics 15 (2009), 21–35.

PRIMEPUZZLES.NET. Problems & Puzzles: Conjectures. 2023. Available online [cit. 28.2. 2023]: https://www.primepuzzles.net/conjectures/index.html

RIBENBOIM, P., 2000. My numbers, my friends: popular lectures on number theory. Springer-Verlag, 2000.

SAUTOY, M., 2003. The Music of the Primes. Harper Collins, 2003.

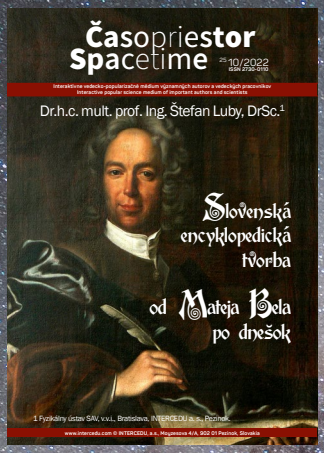
SINGH, S., 1998. Fermat´s Last Theorem. Fourth Estate Limited, 1998.

SINGH, S., 2000. Velká Fermatova věta. Academia, Praha, 2000.

Largest Known Prime Number. 2023. Wikipedia. Available online [cit. 28.2. 2023]: https://en.wikipedia.org/wiki/Largest_known_prime_number

Časopriestor Spacetime

Interaktívne vedecko-popularizačné médium významných autorov a vedeckých pracovníkov
Interactive popular science medium of important authors and scientists



www.kassay.eu • www.intercedu.com