Problémy z teorie čísel

Radek Erban

Teorie čísel je jednou z nejstarších částí matematiky. Snad jen geometrie by jí v tomto ohledu mohla konkurovat. Proslulá je především spoustou otevřených problémů, mnohé z nichž matematikům odolávají již přemnoho lidských věků. Krásné na těchto úlohách je, že u mnoha z nich (alespoň u většiny těch nejslavnějších) není jejich formulace vůbec obtížná a dají se jednoduše vysvětlit komukoli, kdo k matematice alespoň trochu přičichl. V následujícím textu se pokusím o některých těch slavnějších (a jejich historii) zmínit a aspoň trochu ukázat, kam během let jejich řešení pokročilo.

Velká Fermatova věta

Začněme trochou historie. Roku 1621 bylo přeloženo do latiny dílo řeckého matematika *Diofanta*. Při jeho studiu si slavný francouzský matematik *Pierre de Fermat* na okraj knihy učinil spoustu poznámek, které později uveřejnil jeho syn. Mezi nimi je též obsažena tzv. velká Fermatova věta (anglicky „Fermat's last theorem"), podle níž rovnice $x^n + y^n = z^n$ nemá řešení v přirozených číslech x, y, z, n pro $n > 2$. Fermat si poznamenal toto tvrzení na okraj vedle Diofantovy věty: „*Dvojmoc rozložit v součet dvou jiných dvojmocí.*" v tomto tvaru: „*Je však nemožné rozložit trojmoc ve dvě trojmoci nebo čtyřmoc ve dvě čtyřmoci a obecně mocninu stupně vyššího než druhého ve dvě mocniny s týmiž exponenty; objevil jsem skutečně podivuhodný důkaz tohoto tvrzení, avšak tento okraj je příliš malý, než aby jej mohl pojmout.*" Během dalších více než 350 let tento problém matematikům odolával. Podařilo se ho sice rozřešit pro nějaká n, ale obecný důkaz nebyl podán. Veliké úsilí tomuto problému věnoval například německý matematik *Ernst Kummer*, jehož tato úloha vedla k vytvoření teorie tzv. ideálních čísel (1847). Na přelomu století dokonce jeden matematik-amatér odkázal značné jmění tomu, kdo tento problém rozlouskne. Definitivní důkaz však podal až anglický matematik *Andrew Wiles*, který v červnu 1993 předvedl před zraky padesáti specialistů na teorii čísel důkaz této věty během tří přednášek na Newton Institute v Cambridgi. Při detailnějším zkoumání odborníky byly v tomto důkazu objeveny nějaké nedostatky, které se však Wilesovi podařilo později dořešit.

Goldbachova hypotéza

Hned dva problémy nesou označení Goldbachova hypotéza. Předně se jedná o domněnku, že každé liché číslo větší než 5 lze napsat jako součet tří prvočísel. Není těžké ověřit, že tomu tak skutečně je pro malá lichá čísla, například: $7 = 2 + 2 + 3$,

$9 = 3 + 3 + 3$, $11 = 3 + 3 + 5$, $13 = 3 + 5 + 5$, $15 = 5 + 5 + 5$, atd. Slavný ruský (vlastně sovětský) matematik *I.M. Vinogradov* v roce 1937 dokázal, že existuje takové přirozené n_0, že pro všechna $n > n_0$ požadovaný rozklad existuje. Doposud však není známo, jak je vlastně číslo n_0 velké.

S tímto problémem souvisí též otázka, zda-li lze každé sudé číslo větší než 2 napsat jako součet dvou prvočísel — taktéž bývá nazývána Goldbachovou hypotézou. Zde opět snadno ověříme, že pro malá sudá čísla požadovaný rozklad najdeme, například $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5 = 3 + 7$, atd. Na počítačích byly samozřejmě uvedené hypotézy prověřeny pro mnohem více přirozených čísel. U této otázky je dobré podotknout její souvislost s předchozím problémem. Pokud bychom dokázali, že každé sudé číslo větší než 2 lze vyjádřit ve tvaru součtu dvou prvočísel, pak libovolné liché číslo můžeme psát ve tvaru $3 + n$, kde n je sudé, a proto každé liché číslo lze vyjádřit ve tvaru součtu tří prvočísel.

Prvočíselná dvojčata

Pokud se člověk podívá na libovolnou tabulku prvočísel, nalezne tam mnoho párů prvočísel p, q, takových, že $q = p+2$. Takovéto dvojice se nazývají prvočíselná dvojčata. Příkladem mohou být dvojice $3, 5$; $17, 19$; $881, 883$; $10^9 + 7, 10^9 + 9$; resp. z těch trochu větších $1691232 \cdot 1001 \cdot 10^{4020} - 1, 1691232 \cdot 1001 \cdot 10^{4020} + 1$. Stále otevřeným problémem zůstává, zda-li je prvočíselných dvojčat konečně, či nekonečně mnoho.[1] Tento problém lze samozřejmě dále rozšiřovat, například, zda-li existuje nekonečně trojic prvočísel p, q, r tak, že $q = p + 2, r = p + 6$, či prvočíselných čtyřčat (definici tohoto pojmu snad čtenář snadno odhadne sám) ....

Fermatova prvočísla

Asi tak kolem roku 1640 vyslovil Pierre Fermat domněnku, že pro každé $n \in \mathbb{N}_0$ je $F_n = 2^{2^n} + 1$ prvočíslo. Skutečně, pro čísla $n = 0, 1, 2, 3, 4$ je tato hypotéza pravdivá. Bohužel však posloupnost F_n se zvětšujícím se n velice rychle roste, což prověřování této hypotézy přímým výpočtem značně znesnadňuje. Proto až téměř o sto let později Leonhard Euler ukázal, že se Fermat spletl (!) a že již číslo F_5 je číslo složené[2],

[1] Dá se ukázat, že když sčítáme převrácené hodnoty všech prvočísel, pak tento součet roste nade všechny meze, tj. formálně zapsáno $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\cdots = \infty$, naproti tomu, sčítáme-li převrácené hodnoty jen prvočíselných dvojčat, blíží se tyto součty ke konečnému číslu. To by nám mohlo napovídat, že prvočíselných dvojčat je „v jistém smyslu“ o dost méně než prvočísel samotných.

[2] Pro zajímavost ukážeme jeden značně trikový postup, jak se dá nahlédnout, že $641 | \mathrm{F}_5$. Zřejmě $641 = 2^4 + 5^4 = 5.2^7 + 1$, proto $2^4 = 641 - 5^4$ a $2^{32} = 2^4 \cdot 2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 =$

konkrétně, že $641|F_5$.

Pro prvočísla tvaru $2^{2^n}+1$ se vžil na paměť slavného Fermatova omylu název Fermatova prvočísla. Dodnes není rozřešeno, zda-li jich je konečně, či nekonečně mnoho. Poznamenám zde jen, že pro $5 \leq n \leq 23$ jsou čísla tohoto tvaru složená a žádné Fermatovo prvočíslo pro $n > 23$ nebylo dosud objeveno.

Zmíním se zde ještě o jedné zajímavé souvislosti Fermatových prvočísel, kterou dokázal slavný německý matematik *Carl Friedrich Gauss* a která se týká od starověku zkoumaného problému konstrukce pravidelných mnohoúhelníků pravítkem a kružítkem. Takže, pravidelný mohoúhelník je takto konstruovatelný, právě když počet jeho vrcholů je roven číslu $v = 2^k p_1 p_2 \dots p_n$, kde $p_1, p_2, \dots, p_n$ jsou navzájem různá Fermatova prvočísla, k, n nezáporná celá čísla a $v \geq 3$. Z této věty například vidíme, že pravidelný sedmiúhelník jen s pomocí pravítka a kružítka nezkonstruujeme, ale pravidelný sedmnáctiúhelník či dvěstěpadesátisedmiúhelník zkonstruovat jdou.

Mersennova prvočísla a dokonalá čísla

Mersennova prvočísla jsou prvočísla tvaru $2^n - 1$. Jméno dostala podle francouzského matematika Martina Mersenna. Doposud není rozhodnuto, zda-li jich je konečně, nebo nekonečně mnoho. Poslední objevené prvočíslo tohoto tvaru je číslo $2^{3021377} - 1$. Důkaz, že je to skutečně prvočíslo, byl ukončen dne 27. ledna 1998. Pro zajímavost, toto číslo má 909526 cifer a jen závěrečný test trval 46 dní na počítači s Pentiem II (200 MHz).

Celkem jednoduše se dá ukázat souvislost mezi Mersennovými prvočísly a tzv. dokonalými čísly. Dokonalá čísla jsou čísla, která se rovnají součtu svých vlastních dělitelů, příkladem mohou být čísla 6, 28, 496, ... , neboť $6 = 1+2+3$, $28 = 1+2+4+7+14$, ... Platí věta, že sudé číslo je dokonalé právě tehdy, je-li tvaru $2^{n-1}(2^n - 1)$, kde $n > 1$ a $2^n - 1$ je (Mersennovo) prvočíslo. Tj. sudých dokonalých čísel známe přesně tolik, kolik známe Mersennových prvočísel. Nadále otevřeným problémem však zůstává otázka existence lichých dokonalých čísel. Doposud nebylo žádné objeveno, ani nebyl nalezen důkaz jejich neexistence.

Čokoládový problém

Existuje samozřejmě mnoho dalších problémů v teorii čísel, které jsou natolik slavné, že by se je slušelo zmínit v tomto výčtu — Riemannova hypotéza, Waringův problém, rozložení prvočísel v intervalech, ... , z nedostatku místa však na ně již nemůže dojít.

$641.2^{28} - (641-1)^4 = 641 \cdot \mathrm{k} - 1$, což dává náš výsledek.

Na závěr jsem se raději rozhodl zařadit problém, který možná není tak slavný, ale celkem mě zajímá a za jehož vyřešení vypisuji cenu **1kg čokolády** dle výběru řešitele.

Každý si snadno ověří, že platí tyto pozoruhodné vztahy: $3^2+4^2=5^2$, $3^3+4^3+5^3=6^3$. První otázka, která člověka tak napadne, je, zda-li je to náhoda, nebo tyto rovnosti vyjadřují nějakou skrytou zákonitost. Nad tím se též můžeš zkusit zamyslet, ale pro samotnou formulaci čokoládového problému nám bude stačit jen rovnice druhá, tj. vztah:

$$3^3+4^3+5^3=6^3$$

Tato rovnost je příkladem toho, že existuje trojice po sobě jdoucích přirozených čísel, jejichž součet třetích mocnin je roven opět třetí mocnině přirozeného čísla. Moje otázka je, zda-li existuje ještě nějaký jiný příklad podobné rovnosti, tj. přesněji mi jde o počet řešení diofantické rovnice

$$(a-1)^3+a^3+(a+1)^3=n^3.$$

Jedním řešením jest $a=4$, $n=6$ dle našeho výchozího vztahu. Existují však i nějaká jiná řešení?

Poznámka. Tento problém mě též zaujal i tím, že snad ten nejpřirozenější postup na jeho řešení (tj. ten, který mě první napadl) vede postupně k diofantickým rovnicím tvaru $x^2=y^3+k$, kde k je celé číslo. To jsou rovnice samy o sobě zajímavé a nazývají se Mordellovy rovnice. Byla pro ně vybudována jistá teorie, na které je celkem pozoruhodné, že dává, co se týče řešitelnosti, jistou výjimečnost Mordellově rovnici pro $k=-432$. Samotná rovnice $x^2=y^3-432$ má i to kouzlo, že se v této teorii „musí brát zvlášť“ a dá se ukázat, že vyřešit ji je problém ekvivalentní důkazu velké Fermatovy věty pro číslo $n=3$.