Antonín Čejchan

O částečných součtech prvočíselné řady

Rozhledy matematicko-fyzikální, Vol. 92 (2017), No. 1, 14–22

Persistent URL: http://dml.cz/dmlcz/146733

O částečných součtech prvočíselné řady

Antonín Čejchan, FÚ AV ČR, Praha

Abstract. The article deals with interesting properties of partial sums of a prime numbers sequence and their relations to the values of integer powers of integer numbers. The exploration of these relations probably has never been published. The article presents two hypotheses and summarizes previous achievements in their numerical verification. Finally, the readers are encouraged to find proofs or counterexamples to the proposed hypotheses

Úvod

Jednou jsem v rámci pracovní úlohy (pracuji jako matematik-programátor na fyzikálním pracovišti, kde většinou pro vědce z nejrůznějších disciplín tohoto oboru zápasím se symbolickými i numerickými integrály, diferenciálními rovnicemi, průběhy nejrůznějších funkcí a jejich maximy a minimy, ale i se soustavami lineárních rovnic s řadou symbolických parametrů a samozřejmě následně i s numerikou v požadované přesnosti a nakonec obvykle s 2D či 3D grafikou, nejčastěji za pomoci integrovaného matematického systému *Maple* [1]) velmi volně narazil na pro mě zajímavý poznatek z teorie čísel, z něhož se vyklubaly následující otázky. Tyto otázky jsou podložené nemalým výpočetním úsilím, nikoliv však důkazy. Dovolte, abych vás s nimi během následujících kapitol seznámil.

Stručný přehled terminologie

Všichni si asi ze školy pamatujeme, co jsou prvočísla. Prvočíslo je přirozené číslo, tedy celé číslo větší než nula, které je dělitelné právě dvěma různými přirozenými čísly, jedničkou a sebou samým. Protože mají být tito dělitelé různí, není jednička prvočíslo. Počátek posloupnosti prvočísel je tedy

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ \ldots$$

Označme si členy této posloupnosti $p(n)$, kde $n \geq 1$, takže např. $p(3) = 5$. Prvočísla jsou velmi důležitá v teorii i v praxi. Víme, že každé přirozené číslo větší než 1 lze jednoznačně rozložit na součin prvočísel [2].

V praxi je v dnešní době záplavy počítači využívána pro bezpečný přenos zpráv *metoda RSA*, při níž se pracuje s tzv. *tajným a veřejným klíčem*, které jsou vytvořeny na základě velkých prvočísel [3].

Již řečtí matematici v antice věděli, že prvočísel je nekonečně mnoho [2]. Tudíž v našem označení bude $n = 1, 2, \ldots$ Vezměme nyní *řadu příslušnou posloupnosti se členy* $p(n)$, což je součet

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

Tento výraz je samozřejmě roven $+\infty$.

Součet prvních i členů

$$s(i) = p(1) + p(2) + \cdots + p(i)$$

se potom nazývá *i-tým částečným součtem řady příslušné posloupnosti se členy* $p(n)$, např. $s(5) = 28$. A těchto částečných součtů se budou týkat následující úvahy.

Popis problému a první otázky

Při tehdejší úloze jsem sčítal několik prvých prvočísel, konkrétně jich bylo devět, a dospěl jsem k součtu 100, čímž jsem vlastně vyhodnotil částečný součet $s(9)$. Toto číslo je druhou mocninou desítky, což je samozřejmě přirozené číslo. Nebylo na tom nic zvláštního. Proč by se nemohly „stýkat“ v určitých vztazích, zde v rovnosti, prvky jedné posloupnosti (zde posloupnosti druhých mocnin 1, 4, 9, ...) například s částečnými součty řady posloupnosti zcela jiné, která nemá s první posloupností co do činění (snad jen to, že jsou v našem případě obě tvořeny přirozenými čísly)? Rozhodl jsem se podívat, jak často k tomuto případu dochází. Napsal jsem program v jazyku *Maple* a dal se do počítání. A postupně přicházela první překvapení. V první miliardě a půl částečných součtů prvočíselné řady program nalezl pouze 5 shod se čtverci některých přirozených čísel. Výsledky jsou uvedeny v tab. 1. V jejím prvním sloupci je index částečného součtu, ve druhém jeho hodnota, ve třetím je potom částečný součet zobrazen v podobě druhé mocniny a ve čtvrtém je uveden s faktorizací základu.

Prověřené půldruhé miliardy částečných součtů, i když to není vůči obdrženému výsledku tak zcela „malé“ číslo, jistě neodpovídá na dotaz, kolik takových rovností může existovat. Je však docela zajímavé, že všech pět jich bylo nalezeno již v prvním milionu indexů částečných součtů. Pro představu je

$$s(1\,500\,000\,000) = 25\,540\,154\,953\,182\,951\,389,$$

přičemž bylo prověřeno 5,05 mld. druhých mocnin.

Vznikají zde tak první otázky:

Je částečných součtů prvočíselné řady rovných čtverci nějakého přirozeného čísla konečně nebo nekonečně mnoho?

Nebo je jich dokonce pouze právě těch pět výše citovaných a uvedených v tab. 1?

i	$s(i)$	$s(i)$ ve tvaru čtverce	faktorizace $s(i)$
9	100	10^2	$(2 \cdot 5)^2$
2 474	25 633 969	$5\,063^2$	$(61 \cdot 83)^2$
6 694	212 372 329	$14\,573^2$	$(13 \cdot 19 \cdot 59)^2$
7 785	292 341 604	$17\,098^2$	$(2 \cdot 83 \cdot 103)^2$
709 838	3 672 424 151 449	$1\,916\,357^2$	$(463 \cdot 4\,139)^2$

Tab. 1

Třetí mocnina

„Jak to asi pokračuje dále?“, řekl jsem si. Tím „dále“ jsem měl na mysli třetí mocninu. Tedy: Kolik je částečných součtů prvočíselné řady, které by byly třetí mocninou nějakého přirozeného čísla? Lehce jsem upravil vstupní data a začal výpočty realizovat. Samozřejmě, že jsem nějaké pozitivní výsledky očekával. Jak však testy programem pokračovaly, postupně jsem ztrácel naději, ale až příliš brzy jsem se také vzdát nechtěl. Dostal jsem se výpočetně k jedné miliardě, tentokrát však *program nenalezl jediný částečný součet prvočíselné řady, který by se rovnal třetí mocnině nějakého přirozeného čísla*! I zde uveďme základní hodnoty

$$s(1\,000\,000\,000) = 11\,138\,479\,445\,180\,240\,497,$$

přičemž počet prověřených třetích mocnin je 2,23 mil. Otázka, která se zde vynořila, tedy zní:

Existuje vůbec nějaký částečný součet prvočíselné řady rovnající se třetí mocnině nějakého přirozeného čísla?

Úvahy o vyšších mocninách

Nyní by nás mohlo zajímat, jak je to u těchto částečných součtů vůči vyšším mocninám, tedy páté, sedmé, jedenácté atd. V úvahu na testy zde stačily jen mocniny prvočíselné, protože složená čísla jsou mocninami i (menších) prvočísel, obdržených z jejich rozkladů, např. číslo, které je třicátou pátou mocninou nějakého přirozeného čísla, je i pátou a sedmou mocninou dvou jiných přirozených čísel.

Další postup byl nasnadě. Zkusit ještě některé vyšší mocniny v předchozím smyslu. Provedl jsem tento test (velmi omezeně) ještě pro páté, sedmé, jedenácté, třinácté, sedmnácté a devatenácté mocniny, tentokráte do hodnoty $s(100\,000\,000)$, a výsledek byl stejný! Program nenalezl *ani jediný částečný součet prvočíselné řady, který by se rovnal páté, sedmé, … až devatenácté mocnině nějakého přirozeného čísla*! Shrnutí těchto výsledků se nachází v tab. 2.

$s(i)$ hledány jako k-té mocniny	$s(i)$ prověřeny do počtu	počet k-tých mocnin v prověřeném intervalu pro $s(i)$	počet nalezených $s(i)$ v podobě k-tých mocnin přirozených čísel
2	1,5 mld.	5,05 mld.	5
3	1 mld.	2,23 mil.	0
5	100 mil.	2 508	0
7	100 mil.	267	0
11	100 mil.	35	0
13	100 mil.	20	0
17	100 mil.	9	0
19	100 mil.	7	0

Tab. 2

Zvláště u druhé a třetí mocniny jsme se propracovali k vysokým hodnotám částečných součtů. Ale to vlastně až tak „nic zvláštního neznamená“, protože jak částečných součtů, tak jakýchkoli mocnin je nekonečně mnoho.

Vyvstává zde tudíž další otázka:

Existuje vůbec nějaký částečný součet rovnající se páté, sedmé, … až devatenácté mocnině přirozeného čísla?

Pokud předchozí otázky shrneme a zobecníme, dospějeme k následujícímu:

Zjistili jsme, že existuje 5 částečných součtů prvočíselné řady, které se rovnají druhé mocnině přirozeného čísla. Existují další? A pokud ano, je jich konečně nebo nekonečně mnoho?

Existuje nějaký částečný součet prvočíselné řady $s(i)$ takový, aby se rovnal nějaké k-té mocnině přirozeného čísla, kde k je větší než 2?

Předchozí výpočty nás zatím spíše svádějí k tomu, abychom na tyto otázky odpověděli:

Existuje pouze těchto 5 částečných součtů prvočíselné řady (a tedy jich je konečně mnoho), které se rovnají druhé mocnině přirozeného čísla.

Neexistuje žádný částečný součet prvočíselné řady, který by se rovnal k-té mocnině přirozeného čísla pro $k > 2$.

Číslice c na pozici jednotek u $s(i)$	Výskyt číslic c u $s(i)$ (v procentech), $i = 1, \dots, 10\,000\,000$
0	10,000 85
1	10,002 86
2	10,010 46
3	9,991 89
4	9,994 46
5	10,012 86
6	10,002 79
7	9,990 86
8	9,991 44
9	10,001 53

Tab. 3

Některé úvahy o případných nerovnostech částečných součtů a mocnin přirozených čísel

„Proč tomu tak asi je? Nejsou částečné součty prvočíselné řady nějak (matematicky) znevýhodňovány vůči mocninám přirozených čísel (nebo naopak)?“ Napadlo mě podívat se alespoň na statistiky posledních číslic (číslic na pozici jednotek) čísel z obou množin.

Začal jsem posledními číslicemi částečných součtů a vyhodnotil jejich procentuální četnost na vzorku o počtu deseti milionů. Výsledky jsou zachyceny v tab. 3.

A jak je to s posledními číslicemi u celočíselných mocnin přirozených čísel? Podívejme se, jakou číslicí končí jednotlivé mocniny (výsledky jsou podle sloupců, mocnina je označena symbolem $\hat{}\,n$, tedy v prvním sloupci je vlastně vyjmenováno všech deset koncových číslic přirozených čísel; symbol ˆ1 zde představuje první mocninu) (tab. 4).

ˆ1	ˆ2	ˆ3	ˆ4	ˆ5	ˆ6	ˆ7	ˆ8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	8	6	2	4	8	6
3	9	7	1	3	9	7	1
4	6	4	6	4	6	4	6
5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6
7	9	3	1	7	9	3	1
8	4	2	6	8	4	2	6
9	1	9	1	9	1	9	1

Tab. 4

V řádcích jsou postupně uvedeny poslední číslice mocnin čísel (až do osmé) končících na číslici v prvním sloupci. Takže např. druhá, třetí, čtvrtá a pátá mocnina čísla končícího trojkou budou mít postupně na pozici jednotek devítku, sedmičku, jedničku a trojku. Všimněme si, že se sloupce v tab. 4 po každých čtyřech opakují, tedy že pátý sloupec je totožný s prvním, druhý se šestým atd. Stejně tak je tomu i nadále, tedy devátý bude opět shodný s prvním, desátý s druhým atd.[1)]

Výskyt jednotlivých číslic na pozici jednotek u k-tých mocnin získáme pomocí počtu výskytů jednotlivých číslic v tab. 4, přičemž díky opakování, jak již bylo poznamenáno výše, se lze omezit pouze na první čtyři sloupce. Vezmeme tedy výřez o rozměrech 10 (řádek) krát 4 (sloupce). Číslo 40 tedy představuje všechny možnosti, které mohou pro poslední číslici c nastat, jestliže vezmeme libovolné přirozené číslo končící nějakou číslicí d a umocníme je na $k + 4j$, kde $k = 1, 2, 3, 4$ a j je rovno nule nebo libovolnému přirozenému číslu. Jak již víme, hodnota j výsledek neovlivní.

c	Příznivé možnosti, že číslo n^{k+4j} končí číslicí c přičemž n končí číslicí d
0	(0, 1), (0, 2), (0, 3), (0, 4)
1	(1, 1), (1, 2), (1, 3), (1, 4), (3, 4), (7, 4), (9, 2), (9, 4)
2	(2, 1), (8, 3)
3	(3, 1), (7, 3)
4	(2, 2), (4, 1), (4, 3), (8, 2)
5	(5, 1), (5, 2), (5, 3), (5, 4)
6	(2, 4), (4, 2), (4, 4), (6, 1), (6, 2), (6, 3), (6, 4), (8, 4)
7	(3, 3), (7, 1)
8	(2, 3), (8, 1)
9	(3, 2), (7, 2), (9, 1), (9, 3)

Tab. 5

[1)] Pozn. redakce: V tomto odstavci je popsána triviální vlastnost mod 10 – zbytky mohou být 0, ±1, ±2, ±3, ±4, 5. Páté mocniny 0, 1 a 5 jsou zřejmé. Dále $(\pm2)^5 = \pm32$, $(\pm3)^5 = \pm243$ a $(\pm4)^5 = \pm1\,024$, takže končí stejnou číslicí.

Na základě uvedených úvah sestavíme tab. 5. V jejím druhém sloupci uvedeme dvojice (d, k) příznivé pro obdržení číslice c. Např. v řádku pro $c = 3$ si ve druhém sloupci přečteme, že číslici 3 můžeme na místě jednotek obdržet jako první (a také jako pátou, devátou atd.) mocninu čísla končícího trojkou, pro což použijeme zápis $(3, 1)$, nebo také jako třetí (a také jako sedmou, jedenáctou atd.) mocninu čísla končícího sedmičkou (zápis $(7, 3)$). Toto jsou tedy dvě jediné příznivé možnosti pro získání číslice 3 na místě jednotek u libovolné mocniny libovolného přirozeného čísla (viz druhý sloupec tab. 5).

My jsme se však v našich výpočtech nejvíce soustředili na druhou a třetí mocninu. Zredukujme tedy pro naše účely tab. 5 na tab. 6, v níž budou zachyceny pouze tyto dva případy.

c	^2	^3
0	(0, 2)	(0, 3)
1	(1, 2), (9, 2)	(1, 3)
2	–	(8, 3)
3	–	(7, 3)
4	(2, 2), (8, 2)	(4, 3)
5	(5, 2)	(5, 3)
6	(4, 2), (6, 2)	(6, 3)
7	–	(3, 3)
8	–	(2, 3)
9	(3, 2), (7, 2)	(9, 3)

Tab. 6

Jak vidíme z tab. 6, neexistují přirozená čísla, jejichž druhá mocnina končí číslicemi 2, 3, 7 nebo 8. A jaké číslice se tedy uplatnily v nalezených pěti případech (viz tab. 1)? Dvakrát to byla dvojice $(3, 2)$, jedenkrát $(7, 2)$, tedy třikrát dvojice pro koncovou devítku, dále jedenkrát $(0, 2)$ (pro koncovou nulu) a jedenkrát $(8, 2)$ (pro koncovou čtyřku). Žádný z miliardy testovaných částečných součtů prvočíselné řady není roven třetí mocnině nějakého přirozeného čísla.

Otázky, hypotézy a (chybějící) důkazy

Otázky z probíraného tématu byly vysloveny na konci několika kapitol. Také byly vysloveny nesmělé hypotézy. Nesmělé proto, že jsou podloženy pouze vykonanou výpočetní prací. To nejdůležitější – důkazy, případně protipříklady – chybějí. Důkazy neumím prozatím (a pravděpodobně nikdy umět nebudu) provést. Pokusy o nalezení protipříkladů, které by vyslovené hypotézy vyvrátily, by vyžadovaly další výpočty s nějakými „chytrými“ algoritmy.

Literatura

[1] Bernardin, L. a kol.: *Maple Programmning Guide*. Maplesoft, a division of Waterloo Maple Inc., Waterloo, ON, 2012.

[2] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel*. Academia, Praha, 2011.

[3] Křížek, M.: Má ryze teoretická matematika uplatnění v technické praxi? *Pokroky matematiky, fyziky a astronomie*, roč. 44 (1999), č. 1, s. 14–24.

* * * * *

ARISTOTELES ZE STAGEIRY

(asi 284–322 př. n. l.)

Je to docent
na sto procent
úplně všech věd.
Nepromarnil svoje léta,
učenost celého světa
přežvýkal a sněd.
V jeho knihách nejsou chyby.
Jenom moudrost mu v nich chybí!

Emil Calda*)

*) Úvod do obecné teorie prostoru, Karolinum, Praha, 2003