Prvočísla

Pavel Hrubý

Pruh Soft 2025

Úvod

Je mi naprosto jasné, že 90 % uživatelů tento článek ani neotevře. A ostatní se maximálně pousmějí. No, není to účelem tohoto psaní. Pravý účel je čistě osobní, udělat si malý přehled v této oblasti. Zopakujeme si definici, základní věty, domněnky a najdeme si odkazy na literaturu. Na první pohled se jedná o jednoduchý přehled. Začíná základními pojmy. V dalším textu jsou stěžejní odkazy na další publikace a na internet, zejména na Wikipedii a to anglickou verzi. I když se článek týká prvočísel, nevyhnu se některým zmínkám do jiných oblastí matematiky, tím vlastně ukazuji, jak je tato problematika stěžejní pro její rozvoj. Lze celkem snadno vystopovat, že hodně matematických metod a postupů v jiných oblastech je přímo inspirováno nevyřešenými problémy teorie prvočísel. Od součtů řad po komplexní analýzu, p-adická čísla, teorii grup, eliptické křivky a moduly, všude narazíte na prvočísla. Tak do toho.

Litoměřice 2025

Obsah

Úvod 2

Kapitola 1 – Co je to prvočíslo? 3

Kapitola 2 – Kolik je prvočísel? 5

Kapitola 3 – Jak jsou prvočísla od sebe daleko? 9

Kapitola 4 – Koho je víc? 11

Kapitola 5 – Řady s prvočísly 14

Kapitola 6 – Riemannova zeta funkce 15

Kapitola 7 – Druhy prvočísel 17

- Mersennova prvočísla 17
- Fermatova prvočísla 17
- Prvočísla Sophie Germainové 18
- Prothova prvočísla 18
- Cullenova čísla 18
- Woodallova čísla 19
- Fibonacciho čísla 19

Kapitola 8 – Problémy a domněnky 20

- Silný Goldbachův problém 20
- Rieselův problém 20
- Artinova domněnka 20
- Legendreova hypotéza 21

Oppermannova hypotéza 21
Andricova hypotéza 21
Brocardova hypotéza 22
Firuzbekhtova hypotéza 22
Cramerova domněnka 23
Polignacova hypotéza 23
Ago-Jugi hypotéza 24
Konvergence řady R 24
Gilbraithova domněnka 25
Bunyakovskyho domněnka 25
Kapitola 8 – Skeptický závěr 26
Bibliografie 27

Kapitola 1 – Co je to prvočíslo?

Definice prvočísla. Již staří Řekové...

Takže nejdříve „ústřední mozek lidstva“ – Wikipedie.

Prvočíslo je přirozené číslo větší než 1, které je beze zbytku dělitelné jen dvěma děliteli: jedničkou a samo sebou. Jednička není prvočíslo, neboť nemá dva různé dělitele. Přirozená čísla větší než jedna, která nejsou prvočísly, se nazývají složená čísla. Prvním prvočíslem je číslo 2, které je jediným sudým prvočíslem.

To je snad jasné i pro laiky. Zkusme formální definici (tamtéž)

Číslo $n \in N$ je prvočíslem právě když platí:

$$n > 1 \ \wedge \ \forall k \in N: (k/n \Longrightarrow (k = 1 \ \vee k = n)$$

Jaká jsou tedy prvočísla? Zkusme si je vypsat (alespoň několik ...)

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997,...

To jsou všechna prvočísla menší než 1000.

Z toho automaticky plyne závěr, že pokud nějaké přirozené číslo není prvočíslem, tak je určitě dělitelné alespoň dvěma prvočísly (nemusí být různá). Třeba číslo 45 je dělitelné 3 a 5. Takovým číslům budeme říkat **čísla složená**. Takže je možné zavést prvočíselný rozklad složených čísel např. $45 = 3^2 \cdot 5$ je prvočíselný rozklad čísla 45. Tomuto postupu se říká **faktorizace**.

Jak můžeme vyčíslit prvočísla? Můžeme vzít jedno číslo po druhém a zkoušet dělitelnost menšími prvočísly. Vezměme nějaké číslo. Stačí najít jedno prvočíslo, které dané číslo dělí a hned víme, že zadané číslo není prvočíslo. Z toho hned plyne, že stačí testovat lichá čísla, neboť každé sudé číslo je dělitelné 2. Dokonce stačí testovat dělitelnost daného čísla prvočísly, která jsou menší než druhá odmocnina tohoto čísla. (Proč?)

Tedy vyzkoušejme, zda číslo 259 je, či není prvočíslo. Druhá odmocnina z 259 je přibližně 16,09... a tak stačí testovat, zda číslo 259 není dělitelné 2,3,5,7,11,13. Základy příznaků dělitelnosti 2,3,5 známe, někteří snad znáte i příznak dělitelnosti 7 a11. No zkoušejte, zkoušejte. Zjistíte, že číslo 7 dělí 259. Pak 259 = 7*37. Tedy 259 není prvočíslo.

Pro určení všech prvočísel až do nějakého zadaného čísla starořecký matematik Eratosthenes použil metodu, která se nazývá **Eratosthenovo síto**. Metoda používá vyškrtávání násobků známých prvočísel. Vezmou všechna přirozená čísla menší než zadané číslo, z těchto čísel se vyškrtají násobky 2, nejmenší číslo, které zbude, je určitě prvočíslo. Tedy 3. Vyškrtají se všechny násobky 3, nejmenší číslo, které zbude je 5. Vyškrtají se všechny násobky 5. A tak dále. Po dokončení pak tabulka obsahuje pouze prvočísla.

Ukázka výsledku pro čísla do 30.

	2	3		5
	7			
11		13		
	17		19	
		23		
			29	

Tak základní školu bychom snad měli hotovou.

- Spočítali jste si počet prvočísel menších než 1000?
- A kolik je prvočísel menších než 10000?

A kolik je vůbec prvočísel? Je jich opravdu hodně, tak hodně, že si t ani nedovedete představit. Vlastně jej jich nekonečně mnoho. Nekonečno se představit nedá, ale dá se normálně říct, že pokud máte nějaké prvočíslo vždy existuje prvočíslo, které je větší.

Že toto tvrzení je pravdivé, dokázal již velký starořecký matematik **Euklidés**. Provedl takzvaný důkaz sporem:

Nechť existuje jen konečně mnoho prvočísel. Označme je p1,p2,p3,...,pn. Potom číslo x=p1.p2.p3....pn+1 není dělitelné žádným z těchto prvočísel, jelikož při dělení dostaneme vždy zbytek 1. Tím pádem číslo x musí být buď prvočíslo, nebo musí být dělitelné nějakým jiným prvočíslem. To ale znamená, že množina prvočísel z počátku důkazu nebyla úplná, což je spor s předpokladem.

Opakování, cvičení, vyhledávání, programování

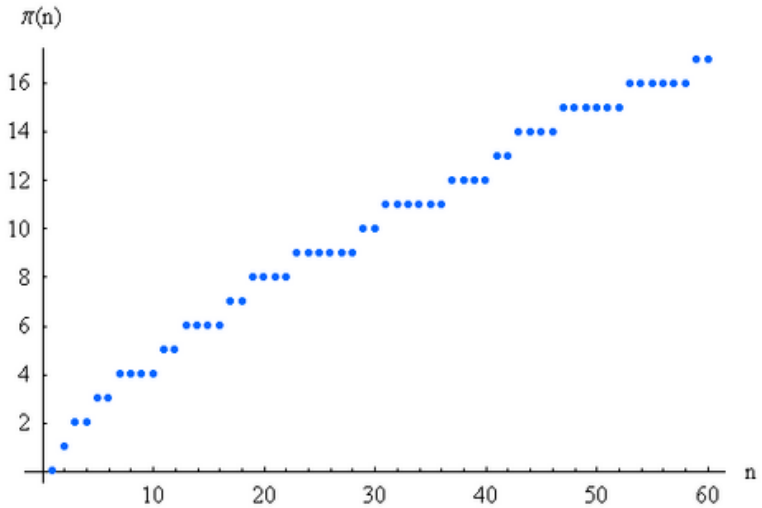
- Ukaž, že číslo 1001 není prvočíslo.
- Napiš si v Pythonu (pomůže AI) program pro výpis Eratosthenova síta do zadaného čísla (třeba 1000).
- Kolik je prvočísel do 100000?

Kapitola 2 – Kolik je prvočísel?

Není pí jako pí. Co na to pánové Gauss a Legandre?

Již ve starověku si matematici kladli otázku, kolik je vlastně prvočísel menších než nějaké zvolené číslo. Pro malá čísla to lze jistě získat tak, že použjeme Eratosthenova síta a počet prvočísel prostě spočítáme. To určitě pro obrovská čísla není nejlepší postup. Zkuste si to pro 1000, a to není moc velké číslo. Matematici proto zavedli pojem prvočíselná funkce a začali ji zkoumat.

Prvočíselná funkce je funkce udávající počet prvočísel menších nebo rovných zadanému reálnému číslu x. Bývá značena pomocí řeckého písmenem π jako π(x) (ovšem nesouvisí nijak přímo se známějším Ludolfovým číslem) a je předmětem studia v matematice, v teorii čísel.



Tedy např. $\pi(20) = 8$ (tj. počet prvočísel do 20 – 2,3,5,7,11,13,17,19)

Rozložení prvočísel mezi přirozenými čísly je předmětem zájmu číselných teoretiků již dlouho. Na konci 18. století vyslovili Carl Friedrich Gauss a Adrien-Marie Legendre domněnku, že prvočíselná funkce přibližně odpovídá funkci

$$\pi(x) \approx \frac{x}{\ln x}$$

Kde ln x je přirozený logaritmus čísla x. Což vlastně znamená, že

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Tento výsledek, známý jako **prvočíselná věta**, se podařilo dokázat až v roce 1896, kdy jeho důkaz podali nezávisle na sobě Jacques Hadamard a Charles de la Vallée Poussin za použití Riemannovy funkce.

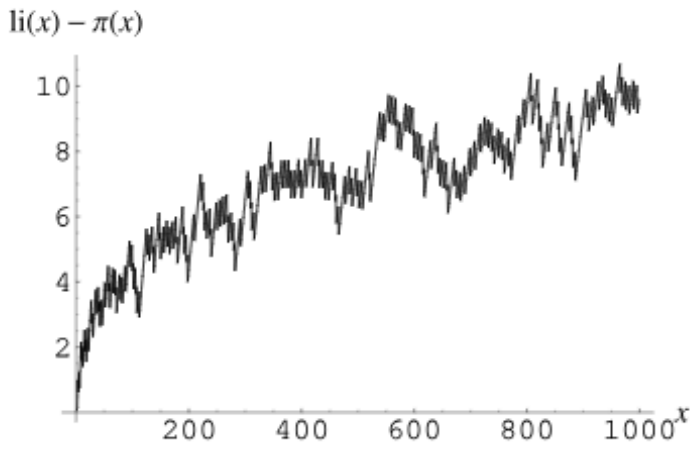
O mnoho jednodušší důkaz podal německý matematik Edmund Landau v roce 1909 a roku 1949 objevil elementární důkaz nejprve norský matematik Atle Selberg a poté Paul Erdös, který lehce upravil některé Selbergovy myšlenky ke konstrukci vlastního důkazu.

Zjednodušený názor je, že pro velká čísla platí $\pi(x) = \frac{x}{\ln x}$, a to není pravda, neboť „mezera“ $\pi(x) - \frac{x}{\ln x}$ se neustále rozšiřuje a $\lim_{x\to\infty} \left(\pi(x) - \frac{x}{\ln x}\right) = \infty$.

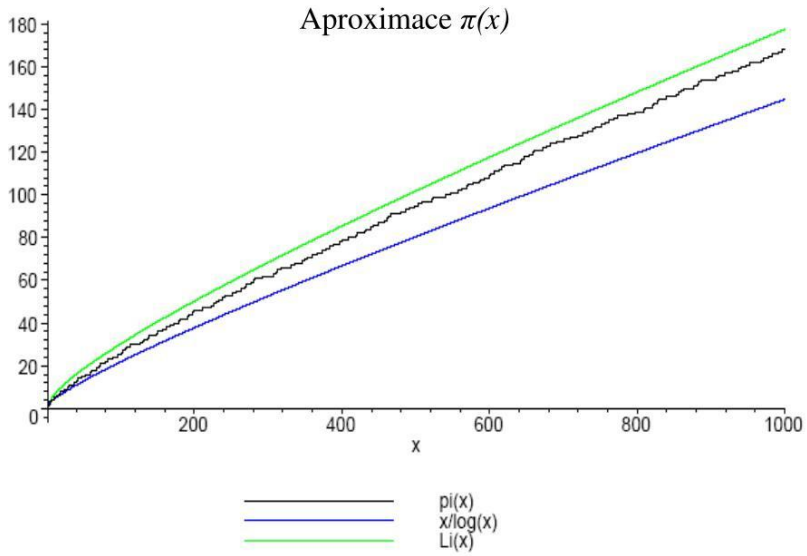
Další, možná přesnější vyjádření pro prvočíselnou funkci je

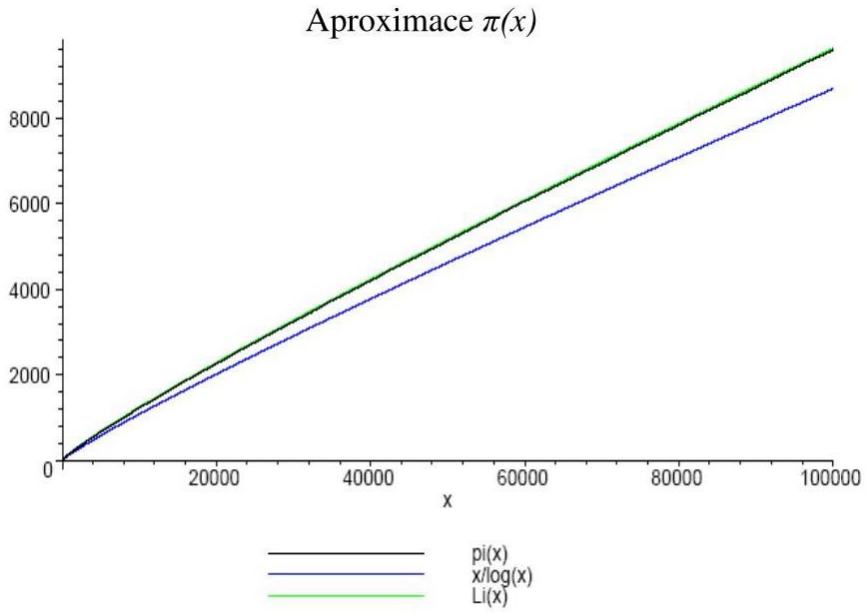
$$\pi(n) \approx Li(n) = \int_2^n \frac{dx}{\ln x} = li(n) - li(2)$$

Kde je *Li(n)* polylogaritmus a *li(n)* je logaritmusintegrál. To jsou funkce, které nelze jinak vyjádřit pomocí elementárních funkcí. Odchylky ukazuje následující graf. Ty se zmenšují s rostoucím x.



Možná pro lepší představu náhled aproximací ukazují následující grafy.





Zajímavé je také se seznámit s Čebyševovými nerovnostmi, kde získáte méně přehledný, ale přesnější odhad prvočíselné funkce:

$$(\ln 2)\frac{x}{\ln x} - \frac{\ln 4}{\ln x} - 1 < \pi(x) < 2(\ln 4)\frac{x}{\ln x} - \sqrt{x}$$

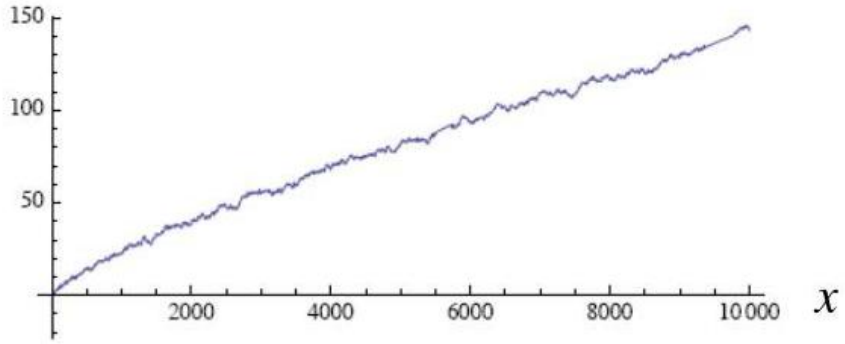
Další odhady jsou čistě empirické.

Legendre, pro malá x

$$\pi(x) \approx \frac{x}{\ln x \ - \ 1{,}08366}$$

Zajímavé je i hledání chyby odhadu prvočíselné funkce tj.

$$chyba(x) = \pi(x) - \frac{x}{\ln x}$$



Již Riemann vyslovil domněnku, že existuje konstanta C taková, že

$$chyba(x) \leq C \cdot \sqrt{x}$$

Zkusme si to porovnat (pomocí sekvencí OEIS)

x	$\pi(x)$	$\pi(x) - x/\log x$	$\pi(x)/x$ / $\log x$	$\mathrm{li}(x) - \pi(x)$	$x/\pi(x)$
10	4	−0,3	0,921	2.2	2,5
10^2	25	3.3	1,151	5.1	4
10^3	168	23,0	1,161	100	5,952
10^4	1 229	143,0	1,132	17,0	8,137
10^5	9 592	906,0	1.104	38,0	10,425
10^6	78 498	6 116,0	1,084	130,0	12,740
10^7	664 579	44 158	1,071	339,0	15,047
10^8	5 761 455	332 774	1,061	754,0	17,357
10^9	50 847 534	2 592 592	1,054	1 701,0	19,667
10^{10}	455 052 511	20 758 029	1,048	3 104,0	21,975
10^{11}	4 118 054 813	169 923 159	1,043	11 588	24,283
10^{12}	37 607 912 018	1 416 705 193	1,039	38 263	26,590

10^{13}	346 065 536 839	11 992 858 452	1,034	108 971,0	28,896
10^{14}	3 204 941 750 802	102 838 308 636	1,033	314 890	31,202
10^{15}	29 844 570 422 669	891 604 962 452	1,031	1 052 619	33,507
10^{16}	279 238 341 033 925	7 804 289 844 393	1,029	3 214 632	35,812
10^{17}	2 623 557 157 654 233	68 883 734 693 281	1,027	7 956 589	38,116
10^{18}	24 739 954 287 740 860	612 483 070 893 536	1,025	21 949 555	40,420
10^{19}	234 057 667 276 344 607	5 481 624 169 369 960	1,024	99 877 775	42,725
10^{20}	2 220 819 602 560 918 840	49 347 193 044 659 701	1,023	222 744 644	45,028
10^{21}	21 127 269 486 018 731 928	446 579 871 578 168 707	1,022	597 394 254	47,332
10^{22}	201 467 286 689 315 906 290	4 060 704 006 019 620 994	1,021	1 932 355 208	49,636
10^{23}	1 925 320 391 606 803 968 923	37 083 513 766 578 631 309	1,020	7 250 186 216	51,939
10^{24}	18 435 599 767 349 200 867 866	339 996 354 713 708 049 069	1,019	17 146 907 278	54,243
10^{25}	176 846 309 399 143 769 411 680	3 128 516 637 843 038 351 228	1,018	55 160 980 939	56,546
OEIS	A006880	A057835		A057752	

Tady vidíte, že prvočísel do 100000 je 9592.

Jistě existují i další empirické odhady, které jsou potvrzené pomocí počítačových výpočtů až do velkých čísel, ale ty též nejsou explicitně dokázány.

Kapitola 3 – Jak jsou prvočísla od sebe daleko?

A co mezery? Nápady, hypotézy, teorie.

Mezery mezi po sobě následujícími prvočísly lze u malých lichých prvočísel docela dobře vysledovat. Mezi 3 a 5 je mezera 2, mezi 23 a 29 je mezera 6. A co tedy obecně mezera $g_n = p_{n+1} - p_n$?

Opět neexistuje přesný vztah. A navíc je možné ukázat, že existuje libovolně velká mezera mezi dvěma po sobě jdoucími prvočísly.

Vezměme n-tici $(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+n+1$ ve které evidentně není ani jedno prvočíslo. Pak je mezera mezi prvočísly minimálně právě n (nebo větší). Tedy pokud vezmu za n =4, 5!=120, pak jsou čísla 122, 123, 124, 125 jistě složená.

Záhadou jsou i takzvaná prvočíselná dvojčata (dvojice), to jsou dvojice prvočísel, mezi nimiž je právě jedno sudé číslo, tedy mezera g_n=2. Máme tedy množinu dvojčat $\{[3,5], [5,7], [11,13], \ldots\}$

A je tato množina konečná nebo nekonečná? Tak to se také neví. Domněnka o prvočíselných dvojicích tvrdí, že je jejich množina nekonečná, ale zatím se to nepodařilo dokázat.

Co víme je, že všechny prvočíselné dvojice musí být ve tvaru 6n-1 a 6n+1, pro n>0. Dokonce lze ukázat, že každá prvočíselná dvojice kromě (3, 5) a (5, 7) je ve tvaru (30*k* – 1, 30*k* + 1) nebo (30*k* + 11, 30*k* + 13) nebo (30*k* + 17, 30*k* + 19).

Pokud tedy budeme zkoumat velikost intervalů mezi po sobě následujícími prvočísly pak si nejprve zkusíme vypsat prvních 30 primárních intervalů: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4, 2, 4, 14, … (sekvence A001223 v OEIS).

Podívejme se na tento problém ještě pomocí **primorialu**.

Pro libovolné prvočíslo p budeme pomocí p# označovat primorial p, tedy součin všech prvočísel nepřesahujících p.

Jestliže q je prvočíslo následující po p, pak posloupnost

$$p\#+2, p\#+3, \ldots, p\#+(q-1)$$

je posloupnost po sobě jdoucích složených čísel, takže mezi prvočísly jsou intervaly o délce ne menší než q-2 (p#+1 může, ale nemusí být prvočíslo).

Vezměme si například 7#=2.3.5.7 =210. Následující prvočíslo po 7 je 11. Číslo 211 je prvočíslo. Pak 212,213,214,215,216,217,218,219,220 jsou čísla složená. Dalším prvočíslem po 211 je pak 223.

Mezi prvočísly jsou tedy libovolně velké intervaly a pro každé prvočíslo p_n jistě existuje mezera g_n taková, že $g_n \geq p_{n+1} - 2$.

Ve skutečnosti může interval mezi prvočísly p_n a p_{n+1} nastat mezi prvočísly mnohem menšími než p#. Například úplně první sekvence 71 po sobě jdoucích složených čísel je mezi 31398 a 31468, zatímco 71# je 27místné číslo.

Průměrná hodnota intervalů mezi prvočísly roste jako přirozený logaritmus n.

$$\lim_{n\to\infty} \frac{g_{nprum.}}{\ln n} = 1$$

Na druhé straně, jednoduchá (ale nedokázaná) domněnka prvočíselných dvojčat říká, že pro nekonečně mnoho n existuje interval 2.

$$\lim_{n\to\infty} \inf g_n = 2$$

Prvotřídní intervaly lze také odhadnout shora a zdola pomocí Jacobsthalovy funkce, což ovšem již není žádná procházka růžovým sadem. (viz sekvence A048670 v OEIS a podpůrné články).

Kapitola 4 – Koho je víc?

Koho je víc? Přirozených čísel nebo prvočísel?

Pokud použijeme teorii množin a jejich kardinální čísla, tak je počet prvočísel stejný, jako počet přirozených čísel. Proč? Protože prvočísla můžeme „očíslovat“ p1, p2, … Takže jejich kardinální čísla jsou stejná a rovnají se $\aleph_0$ (Alef nula) .

$$card\ \mathcal{N} = card\ \mathcal{P} = \aleph_0$$

Tudy nám cesta nevede. Kardinální číslo – Wikipedie

Na počátku 20. století se ustálil v moderní matematice pojem asymptotická hustota, systematicky jej používal Edmund Landau a zpopularizovali je matematici Hardy a Wright. Dále existují pojmy logaritmická hustota a Schnirelmannova hustota. (Jahoda, 2010)

Pro základní představu je asymptotická hustota rovna pravděpodobnosti, že v nějakém podmnožině (nebo celé množině) přirozených čísle nalezneme prvky z nějaké jiné podmnožiny. Takže třeba asymptotická hustota sudých čísel (mezi všemi přirozenými čísly) je rovna ½.

Tak trochu vážněji. *N* označíme množinu všech přirozených čísel.

Definice:

Definice (Asymptotická hustota). Pro $A \subset N$ definujme horní a dolní asymptotickou hustotu následovně (svislé závorky označují počet prvků množiny – kardinalitu, hranaté závorky interval přirozených čísel):

$$d^*(A) = \lim_{n\to\infty} \sup \frac{|A \cap [1,n]|}{n}$$

$$d_*(A) = \lim_{n\to\infty} \inf \frac{|A \cap [1,n]|}{n}$$

Dále označme

$$D \equiv \{A: A \subseteq N, d_*(A) = d^*(A)\}$$

Na množině D definujme novou funkci d, které budeme říkat **asymptotická hustota**,

$$d(A) \equiv d^*(A)$$

Je okamžitě zřejmě, že konečné množiny mají asymptotickou hustotu 0 a pro množinu všech přirozených čísel platí *d(N) = 1*.

Příkladem nekonečné množiny, která má nulovou asymptotickou hustotu je množina všech prvočísel. Tedy:

Tvrzení 0: Buď $\mathbb{P} = \{p_1, p_2, \dots\}$ *množina všech prvočísel. Pak* $d(\mathbb{P}) = 0$.

Opravdu? Důkaz je docela dlouhý a náročný, viz (Grebík, 2014), nebo trochu kratší a jednodušší za využití Čebyševovy nerovnosti.

$$d(P) \leq d^*(P) = \lim_{n\to\infty} \sup \frac{\pi(n)}{n} \leq \lim_{n\to\infty} sup \frac{\mathrm{c}\frac{n}{\ln n}}{n} = \lim_{n\to\infty} sup \frac{c}{\ln n} = 0$$

A podobně pro dolní asymptotickou hustotu. Věta 3.4. (Jahoda, 2010).

Odvození Čebyševových nerovností je srozumitelně uvedeno v publikaci (Halaš, 1997).

V bakalářské práci nalezneme důležitá tvrzení (Grebík, 2014)

Tvrzení 1: Buď $\{a_i\}_{i\in N}$ *posloupnost navzájem nesoudělných přirozených čísel. Definujme*

$A \equiv \{n: \forall i \in N\ a_i \nmid n\}$ *(*a_i *nedělí n)*

Potom $A \in D$ *(tj. A má asymptotickou hustotu) a*

$$d(A) = \prod_{i\in N} \left(1 - \frac{1}{a_i}\right)$$

speciálně d(A) = 0, když řada $\sum_{i=1}^{\infty} \frac{1}{a_i}$ *diverguje.*

Taková posloupnost A je evidentně tvořena čísly nesoudělnými s čísly posloupnosti a_i. Ta čísla v posloupnosti musí být podle předpokladu nesoudělná. Takže to mohou být prvočísla nebo nějaký výběr z prvočísel nebo mocniny prvočísel atd. Množina A je tedy nekonečná a neobsahuje čísla nedělitelná a_i. Pokud tedy $\{a_i\}_{i\in N}$ je posloupnost všech prvočísel, je množina A rovna {1} a asymptotická hustota A je 0.

Definice 2 (Bezkvadrátová čísla, Bezčtvercová čísla). Přirozené číslo větší 1 nazveme bezkvadrátovým, pokud ho nedělí žádná druhá mocnina přirozeného čísla většího než 1. Množinu bezkvadrátových čísel označíme P_2.

Množina všech bezkvadrátových čísel začíná

$$P_2 = \{1,2,3,5,7,10,11,13,14,15,17, \dots\}$$

Pak můžeme tvrdit, že platí

Důsledek 1. Volbou posloupnosti $\{p_n^2\}_{n\in N}$ *dostáváme dle Tvrzení 1.*

$$d(P_2) = \prod_{i\in N} \left(1 - \frac{1}{p_i^2}\right)$$

Důsledek 2. Asymptotická hustota bezkvadrátových čísel je

$$d(P_2) = \frac{6}{\pi^2}$$

To by nebylo nic proti ničemu, kdyby pan Euler roku 1735 neukázal řešení tkzv. Basilejského problému, tedy že platí

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Což je hodnota Riemannovy funkce v bodě 2.

Navíc tu máme souvislost s Möbiovou funkcí $\mu(n)$:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$$

, kde suma vlevo se nazývá Dirichletova řada. Odtud pak vede nalezení souvislosti s Riemannovou hypotézou přes tkzv. Mertenzenovu hypotézu a Mellinovu transformaci. Viz kapitola 6. Mertensova domněnka – Wikipedie

Takže máme

$$d(P_2) = \frac{1}{\zeta(2)}$$

Riemannova zeta-funkce s Eulerovou součinovou formulí je pro $r \in \mathbb{C}, \Re e(r) > 1$, n je přirozené číslo, p_n je prvočíslo

$$\zeta(r) = \sum_{n=1}^{\infty} \frac{1}{n^r} = \prod_{n=1}^{\infty} \left(1 - \frac{1}{p_n^r}\right)^{-1}$$

Eulerův důkaz nalezneme v každé publikaci, která se zabývá teorií čísel. Např. (Jahoda, 2010)

Zajímavá je i **Schnirelmannova hustota**, definovaná pomocí infima vybraných podmnožin přirozených čísel.

$$\sigma(A) = \inf_{n \in N} \frac{A(n)}{n}$$

, kde číslo $\frac{A(n)}{n}$ udává poměr počtu prvků množiny A mezi těmito čísly ku počtu všech těchto čísel.

Např. pro množinu $A = \{1,3,4,5, \dots\}$ je $\sigma(A) = \frac{1}{2}$.

A tedy, jaká je Schnirelmannova hustota prvočísel?

$$\sigma(P) = 0$$

Proč? Protože 1 není prvočíslo.

Pomocí aplikace této hustoty lze dojít k důkazu Waringova problému. Ale to se již vzdalujeme od tématu tohoto článku.

Kapitola 5 – Řady s prvočísly

To se nám to tak pěkně sčítá anebo nesčítá.

Sčítat prvočísla asi nedává smysl, součet se nám bude stále zvětšovat a zvětšovat... A co takhle zkusit sčítat převrácené hodnoty prvočísel?

Asi si nejdříve vzpomeneme na harmonickou řadu, která diverguje, tedy její součet je nekonečný.

$$\sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

Ale co tedy

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = ?$$

Asi spoustu nematematiků zklamu, součet taky diverguje. Viz věta 2.42 (Halaš, 1997)

A co třeba prvočíselné dvojice?

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots = ?$$

Tak tady matematik Bruno dokázal, že řada konverguje, tedy má konečný součet Na jeho počet tento součet se nazývá Brunova konstanta a tedy B=1,90216054...Věta 2.43 (Halaš, 1997).

Další zajímavé součty se týkají tzv. poloprvočísel. Poloprvočíslo je číslo, které vznikne vynásobením dvou prvočísel, ta nemusí být různá.

Můžeme využít tabelovanou prvočíselnou zeta-funkce . Prime zeta function - Wikipedia

$$P_k(s) = \sum_{n:\Omega(n)=k} \frac{1}{n^s}$$

Kde sčítáme s-mocniny čísel. To velké omega je Liuvillova funkce, která určuje součet exponentů u prvočísel, ze kterých je složeno číslo n. Takže když k=2 tak to mohou být dvě prvočísla s exponentem 1 nebo jedno prvočíslo s exponentem 2.

Tabulka z Wiki

k	s	approximate value $P_k(s)$	OEIS
2	2	0.14076043434...	OEIS: A117543
2	3	0.02380603347...	
3	2	0.03851619298...	OEIS: A131653
3	3	0.00304936208...	

Pak pro součet převrácených hodnot poloprvočísel platí

$$\sum_{p_i \in P} \frac{1}{p_n p_m} = 0{,}14076043434\cdots$$

Výpočet byl proveden numericky v roce 2018.

Kapitola 6 – Riemannova zeta funkce

Souvislosti, Riemann a jeho funkce.

Tak jsme se dostali nenápadně k řadám. Řadou myslíme konečný nebo nekonečný součet, $a_1 + a_2 + \cdots a_n = \sum_{i=1}^{n} a_i$, $a_1 + a_2 + \cdots = \sum_{i=1}^{\infty} a_i$.

Součet konečné řady vždy existuje. U nekonečné řady součet buď existuje, pak říkáme, že řada konverguje, nebo součet je nekonečno, říkáme, že řada diverguje. Někdy ani nelze o součtu rozhodnout. Taková řada součet nemá.

Za prvky a_i si můžete dosadit čísla, funkce nebo cokoliv z matematických objektů, které lze sčítat, tedy a_i jsou prvky nějaké vhodné matematické struktury (třeba aditivní grupy).

U číselných nekonečných řad se (mimo geometrické řady) okamžitě setkáme s řadou

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

Která se nazývá **harmonická** řada a lze snadno dokázat, že diverguje. Takže celkem logicky matematici zkoumali i řady podobné

$$\sum_{n=1}^{\infty} \frac{1}{n^k}$$

Pro různá přirozená k. Jeden z prvních problémů, který vyřešil důvtipnou metodou Leonhard Euler byl tkzv. Basilejský problém, tedy určení součtu řady

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = ?$$

Problém formuloval Pietro Mengoli roku 1650; a protože evropské matematiky na tuto otázku upozornil basilejský profesor matematiky Jacob Bernoulli, říká se mu Basilejský problém. Basilejský problém – Wikipedie Vyřešil ho 28letý Leonard Euler v roce 1735 a ukázalo se, že výsledek je

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Tento matematik též odvodil formuli pro libovolné r>1.

$$\zeta(r) = \sum_{n=1}^{\infty} \frac{1}{n^r} = \prod_{n=1}^{\infty} \left(1 - \frac{1}{p_n^r}\right)^{-1}$$

a tedy ukázal souvislost mezi prvočísly a přirozenými čísly. Matematik Riemann šel ještě dál a podařilo se mu propojit diskrétní algebru s komplexní analytickou matematikou rozšířením oboru funkce zeta $\zeta(s)$ na komplexní čísla formulí

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx$$

kde s je komplexní číslo a $\Gamma(s)$ je gama-funkce, zobecněný faktoriál. Tedy máme i propojení prvočísel a komplexních čísel a není to první ani jediná souvislost. Mimochodem, tento vztah použil Riemann roku 1859 ve své přednášce "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse", kde propojil tento vztah s prvočíselnou větou.

Takže pro s=2 máme

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \int_0^{\infty} \frac{x}{e^x - 1} dx = \prod_{n=1}^{\infty} \left(1 - \frac{1}{p_n^2}\right)^{-1} = \frac{\pi^2}{6}$$

Matematici se důkladně věnovali výzkumu Riemannovy funkce a také řešení rovnice

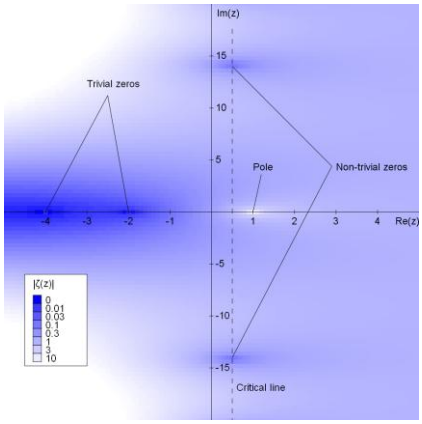
$$\zeta(s) = 0$$

Kde s je komplexní číslo. Lze dokázat, že tzv. Triviální nuly jsou sudá záporná čísla, tedy $\zeta(-2) = \zeta(-4) = \cdots = 0$. Riemann vyslovil domněnku, že netriviální nuly jsou čísla, která leží na tzv. kritické přímce (myšlena přímka v Gaussově rovině komplexních čísel)

$$\zeta\left(\frac{1}{2} + ki\right) = 0$$

pro nekonečně mnoho reálných k. Tato domněnka také není do dnešní doby dokázána i když matematik Michael Atiyah tvrdil, že ji dokázal, ověření postupu jinými matematiky tento důkaz nepodpořilo.

Navíc tato domněnka přímo souvisí s rozložením prvočísel, a navíc má určitý vztah ke kvantování veličin v kvantové teorii.



Kapitola 7 – Druhy prvočísel

Jaké druhy prvočísel vlastně známe?

Prvočíslům se věnovala v průběhu let spousta matematiků a některé druhy prvočísel si byly pojmenovány podle matematiků, které je zkoumali. Zde je uveden pouze reprezentativní výběr, další druhy prvočísel se objeví v následující kapitole.

Mersennova prvočísla

Jsou to prvočísla, které lze zapsat ve tvaru $M_n = 2^p - 1$, kde p je prvočíslo. Dnes největší známá prvočísla jsou právě tato prvočísla. To souvisí s tím, že lze velice rychle testovat, zda číslo M_n je či není prvočíslo. Testem je např. Lucasův-Lehmerův test, který spočívá na vlastnosti rekurentní posloupnosti $s_k = s_{k-1}^2 - 2$ pro $s_0 = 4$ a Mersennovo číslo M_m je prvočíslo tehdy a jen tehdy, pokud dělí číslo s_{n-2}.

Přehled všech známých Mersennových prvočísel je v sekvenci A000668 v OEIS.

Je dobré též vědět, že tato čísla mají těsnou souvislost s tkzv. dokonalými čísly.

Fermatova prvočísla

Těch prvočísel je jenom několik. Snad. Jsou to prvočísla, která lze zapsat ve tvaru $F_n = 2^{2^n} + 1$ pro nějaké nezáporné celé číslo n. Svoje jméno tato čísla získala podle matematika Pierra de Fermata, který je zkoumal jako jeden z prvních.

F_0 = 2^1 +1 = 3

F_1 = 2^2+1 = 5

F_2 = 2^4+1 = 17

F_3 = 2^8+1 = 257

F_4 = 2^{16}+1 = 65 537

F_5 = 2^{32}+1 = 4 294 967 297 a to není prvočíslo =641 × 6 700 417

V rozporu s Fermatovým očekáváním se dodnes (2008) nepodařilo objevit žádná další Fermatova prvočísla kromě F_0, F_1, F_2, F_3 a F_4, která znal už Fermat. Vzhledem k tomu, jak rychle Fermatova čísla rostou, se o Fermatových číslech pro velká n mnoho neví a pojí se k nim následující otevřené problémy:

- jsou všechna Fermatova čísla F_n pro n>4 složená?
- existuje nekonečně mnoho Fermatových složených čísel?
- existuje nekonečně mnoho Fermatových prvočísel?

A zásadní věta o možnosti konstrukce pravidelných n-úhelníků, která vyřešila problém, který se táhnul již od antiky či ještě dříve.

Věta 2.34. Pravidelný n-úhelník lze sestrojit pouze pomocí pravítka a kružítka právě když n > 3 pro $n = 2^m p_1 \cdots p_j$, kde $m \in N_0$ a pro každé i = 0... j, jsou čísla p_1... p_j Fermatova prvočísla.

Takže 7-úhelník a 13-úhelník kružítkem a pravítkem nesestrojíme.

Prvočísla Sophie Germainové

Jako prvočíslo Sophie Germainové je označováno každé prvočíslo p, kde $p' = 2p + 1$, kde také prvočíslem. Tato prvočísla byla pojmenována po francouzské matematičce Sophii Germainové. Příslušnému prvočíslu p' se říká bezpečné prvočíslo, vzhledem k možnému využití v kryptografii.

Několik prvních prvočísel Sophie Germainové jsou 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173 atd.

Předpokládá se, že prvočísel Sophie Germainové existuje nekonečně mnoho, ale zatím se to nepodařilo dokázat. Je však známo, že prvočíslem Sophie Germainové nemůže být žádné prvočíslo končící na číslo 7, jelikož po jeho vynásobení dvěma vyjde číslo končící na 4, a po přičtení 1 vyjde číslo končící na 5, a tato čísla jsou vždy dělitelná alespoň číslem 5.

Prothova prvočísla

Pro *n* je přirozená číslo a *k* liché přirozené číslo, je definováno Prothovo číslo jako

$$P(k,n) = k \cdot 2^n + 1$$

a některá z těchto čísel jsou prvočísla.

Posloupnost Prothových prvočísel začíná: 3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929, 1153,...

Existují distribuované projekty k vyhledávání P. čísel – Proth Prime Search.

Mezi speciální případy Prothových čísel patří Cullenova čísla a Fermatova čísla (k=1, $n = 2^m$.

Cullenova čísla

V matematice jsou Cullenova čísla přirozená čísla tvaru

$$C_n = n \cdot 2^n + 1$$

Cullenova čísla byla poprvé studována irským matematikem Jamesem Cullenem v roce 1905. Cullenova čísla jsou zvláštním druhem Prothových čísel.

Všechna známá Cullenova prvočísla odpovídají n rovno: 1, 161, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275, 481899, 13542825, 13542825, 63548167 (v sekvenci OEIS A005849)

Existuje předpoklad, že Cullenových prvočísel je nekonečně mnoho.

Woodallova čísla

V teorii čísel je Woodallovo (také Rieselovo) číslo (W_n) libovolné přirozené číslo tvaru

$W_n = n \cdot 2^n - 1$,

pro nějaké přirozené n.

Několik prvních Woodallových čísel: 1, 7, 23, 63, 159, 383, 895, ... (OEIS sekvence A003261.

Woodallova čísla poprvé studoval Allan J. Cunningham a G. J. Woodall v roce 1917, inspirovaný dřívějším výzkumem Jamese Cullena na podobně definovaných Cullenových číslech.

Woodallova čísla se v Goodsteinově větě objevila zvláštním způsobem. Mimochodem, Goodsteinova věta je také jeden z filosofických problémů matematiky, totiž je nezávislá na Peanových axiomech. Z filosofického hlediska je fakt, že je nějaké tvrzení o přirozených číslech možné dokázat pouze s použitím aktuální formy nekonečna - tj. ordinálních čísel, jistě zarážející.

Woodallova čísla, která jsou prvočísla , se nazývají Woodallova prvočísla .

Prvních několik exponentů n , pro které jsou odpovídající Woodallova čísla W_n prvočísla: 2, 3, 6, 30, 75, 81, 115, 123, 249, 362, 384, ... OEIS sekvence A002234 .

Samotná Woodallova prvočísla tvoří posloupnost: 7, 23, 383, 32212254719, ... OEIS sekvence A050918 .

V roce 1976 Christopher Hooley ukázal , že téměř všechna Cullenova čísla jsou složená . Důkaz Christophera Hooleyho přepracoval matematik Hirmi Suyama , aby ukázal, že platí pro jakoukoli posloupnost čísel , kde a a b jsou celá čísla, a částečně také pro Woodallova čísla.

Předpokládá se, že existuje nekonečně mnoho Woodallových prvočísel. Od října 2018 je největším známým Woodallovým prvočíslem číslo, které má 5122515 číslic a bylo nalezen Diego Bertolotti v roce 2018 v projektu distribuovaných počítačů PrimeGrid .

Fibonacciho čísla

Jako Fibonacciho posloupnost je v matematice označována nekonečná posloupnost přirozených čísel, začínající 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ... (čísla nacházející se ve Fibonacciho posloupnosti jsou někdy nazývána Fibonacciho čísla), kde každé číslo je součtem dvou předchozích. Fibonacciho prvočísla jsou prvočísla, která se zároveň nacházejí ve Fibonacciho posloupnosti. Jsou to čísla jako 2, 3, 5, 13, 89, 233 a možná jich je nekonečně mnoho.

Kapitola 8 – Problémy a domněnky

A budeme řešit problémy a hádat, zda domněnky platí nebo neplatí. A bude nás bolet hlava.

Silný Goldbachův problém

Také binární Goldbachův problém nebo Eulerova domněnka.

Každé sudé číslo větší než 2 lze vyjádřit jako součet dvou prvočísel.

V roce 1966 Chen Jingrun dokázal , že každé dostatečně velké sudé číslo může být reprezentováno buď jako součet dvou prvočísel, nebo jako součet prvočísel a poloprvočísel (součin dvou prvočísel). Například $100 = 23 + 7 \cdot 11$.

Rieselův problém

V matematice je Rieselovo číslo liché přirozené číslo k, pro které jsou celá čísla ve tvaru $k \cdot 2^n - 1$ složená pro všechna přirozená čísla n. Jinými slovy, když k je Rieselovo číslo, všechny prvky množiny $\{k \cdot 2^n - 1; n \in N\}$ jsou složené. V roce 1956 Hans Riesel dokázal, že existuje nekonečný počet celých čísel k, takže $k\,2^n - 1$ je složené pro jakékoli celé číslo n. Ukázal, že tuto vlastnost má číslo 509203, stejně jako 509203 plus libovolné přirozené číslo vynásobené 11184810.

Problém je existence čísla menšího než 509203, které by bylo Riesselovo číslo. Existuje nebo neexistuje?

Mimochodem čísla $x = 509203.2^n-1$ mají krycí sadu prvočísel 3, 5, 7, 13, 17, 241 tzn., že každé toto číslo (pro libovolné n) je dělitelné alespoň jedním prvočíslem z krycí sady.

Artinova domněnka

V teorii čísel Artinova domněnka o primitivních kořenech uvádí, že existuje celé číslo a, které není dokonalým čtvercem a není rovno −1, které je primitivním kořenem modulo nekonečně mnoho prvočísel p.

Toto tvrzení už vyžaduje jisté základní znalosti z teorie čísel. Primitivní kořen v přirozených číslech modulo p je definován jako číslo, které generuje grupu modulo p. Takže např. 3 je primitivní kořen modulo 5 poněvadž (multiplikativní grupa)

$3^1 \bmod 5 = 3$

$3^2 \bmod 5 = 4$

$3^3 \bmod 5 = 2$

$3^4 \bmod 5 = 1$

Generuje multiplikativní grupu o p-1 tj. 4 prvcích. Co je grupa tady nebudu popisovat.

Víme, že např. 3 je generátorem mnoha grup, ale zda je jich nekonečně mnoho, to není dokázáno. Muselo by pro nekonečně prvočísel platit, že $3^{x-1} \equiv 1\ mod\ p$ a x nesmí být menší než p.

Jinak. Číslo 2 je primitivní kořen, konkrétně modulo 3 a modulo 5, ale ne modulo 7. Posloupnost prvočísel, jejichž modulo 2 je primitivní kořen, začíná takto: 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, ... (sekvence A001122 v OEIS)

V tuto chvíli zůstává otevřená otázka nekonečnosti této sekvence. Artinova hypotéza naznačuje kladnou odpověď na tuto otázku.

Pokud by byla posloupnost prvočísel konečná (např. pro a=3), pak existuje maximální prvočíslo p v této posloupnosti a pro libovolné další prvočíslo q>p musí existovat k>1 tak, že

$$3^{\frac{q-1}{k}} \equiv 1\ mod\ q$$

Dohad také popisuje asymptotickou hustotu těchto prvočísel (jedná se o poměr počtu čísel v této sekvenci ku počtu všech prvočísel menších a rovno než maximální číslo sekvence) Tato domnělá hustota se rovná Artinově konstantě nebo jejímu racionálnímu násobku.

$C_{Artin} = \prod_{prime}\left(1 - \frac{1}{p(p-1)}\right) = 0.3739558$ ... (viz A005596 in the OEIS)

Artin's conjecture on primitive roots - Wikipedia

Dohad formuloval Emil Artin v dopise Helmutu Hasseovi 27. září 1927 (podle jeho deníku).

Legendreova hypotéza

Pro jakékoli přirozené číslo *n* mezi n^2 a $(n+1)^2$ existuje alespoň jedno prvočíslo.

Oppermannova hypotéza

Pro jakékoli přirozené číslo *x* mezi $x(x-1)$ a x^2 existuje alespoň jedno prvočíslo a mezi x^2 a $x(x+1)$ existuje alespoň jedno (jiné) prvočíslo.

Tedy lze alternativně napsat

$$\pi(x^2 - x) < \pi(x^2) < \pi(x^2 + x)$$

Pokud je hypotéza správná, pak platí pro nějaké p a p_n>p

$$g_n < \sqrt{p_n}$$

Andricova hypotéza

(Dorin Andrica, Rumunsko, 1986)

Pro každé prvočíslo p_n větší než 6 platí $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$.

Z tohoto vztahu pak jednoduchou úpravou dostaneme, že

$$p_{n+1} - p_n < 2\sqrt{p_n} + 1$$

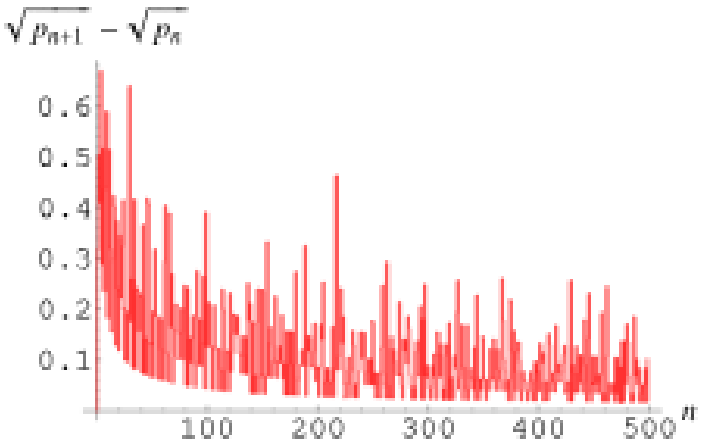
Tedy pokud hypotéza platí, pak pro mezeru g_n mezi prvočísly za prvočíslem p_n máme

$$g_n < 2\sqrt{p_n} + 1$$

Empiricky je zjištěno, že

$$g_n < p_n^{0,525}$$

Ve MathWorld Wolfram je graf



Lze předpokládat, že platí i vtah $g_n < \sqrt{2p_n}$.

Ilustrace

$p_9 = 23, g_9 = 6, \sqrt{23} \approx 4{,}8, \sqrt{2 \cdot 23} \approx 6{,}8, 23^{0,525} \approx 5{,}2$

$p = 31398, g = 72, \sqrt{31398} \approx 177, 31398^{0,525} \approx 230$

Mimochodem, testování velikosti mezery mezi prvočísly, resp. infima těchto mezer je věnováno nemalé úsilí viz Polignacova hypotéza.

Brocardova hypotéza

Mezi čtverci po sobě jdoucích prvočísel, s výjimkou prvních dvou, jsou vždy alespoň 4 prvočísla. Tedy pro n>2 platí

$$\pi(p_{n+1}^2) - \pi(p_n^2) \geq 4$$

Ilustrace

$$\pi(5^2) - \pi(3^2) = \|\{11,13,17,19,23\}\| = 5$$

Firuzbekhtova hypotéza

Posloupnost $(p_n)^{\frac{1}{n}}$ je ostře klesající (zde p_n je n-té prvočíslo).

Firuzbekhtova domněnka je další domněnka o rozdělení prvočísel. Tato domněnka je pojmenována po íránské matematičce Faridě Firuzbakhtové (1962-2019) z univerzity v Isfahánu, která ji navrhla v roce 1982.

Jiný zápis

$$\sqrt[n+1]{p_{n+1}} < \sqrt[n]{p_n}$$

Nebo jinak

$$p_{n+1} < p_n^{1+\frac{1}{n}}$$

Takže pro $p_{30} = 113$ máme $127 = p_{31} < 113^{1+\frac{1}{30}} \cong 132$

Pokud je hypotéza pravdivá, pak pro mezeru mezi prvočísly lze odhadnout

$g_n < (\ln p_n)^2 - \ln p_n$, pro všechna n>4 a dokonce

$g_n < (\ln p_n)^2 - \ln p_n - 1$, pro všechna n>9

Viz také sekvence A111943 .

A ilustrace

$6 < (\ln 23)^2 - \ln 23 \cong 6{,}7$

$14 < (\ln 113)^2 - \ln 113 - 1 \cong 16{,}6$

Cramerova domněnka

Cramerova domněnka je teoretická hypotéza čísel formulovaná švédským matematikem Haraldem Cramerem v roce 1936

$$p_{n+1} - p_n = O((\ln p_n)^2)$$

kde označuje n-té prvočíslo a O je velké (tedy pro velká n se rozdíl po sobě jdoucích prvočísel chová jako funkce v závorce).

V podstatě to znamená, že intervaly mezi po sobě jdoucími prvočísly jsou vždy malé. Cramerova domněnka je také označována jako o něco silnější tvrzení:

$$\lim_{n\to\infty} \sup \frac{p_{n+1} - p_n}{(\ln p_n)^2} = 1$$

Na druhou stranu E. Westzynthius v roce 1931 dokázal, že rozdíly mezi prvočísly jsou více než logaritmické. To znamená

$$\lim_{n\to\infty} \sup \frac{p_{n+1} - p_n}{\ln p_n} = \infty$$

Polignacova hypotéza

Polignacova hypotéza je dosud nevyřešený problém z oblasti teorie čísel. Hypotézu zformuloval fracouzský matematik Alphonse de Polignac v roce 1849 a zní následovně:

Pro každé kladné sudé číslo n existuje nekonečně mnoho párů po sobě jdoucích prvočísel, jejichž rozdíl je roven n. Pro n = 2 se konkrétně jedná o hypotézu prvočíselných dvojčat.

Tato domněnka nebyla dosud (červenec 2025) dokázána, ani vyvrácena pro žádné n.

Ačkoliv dosud nebyla Polignacova hypotéza potvrzena ani vyvrácena pro žádnou konkrétní hodnotu n, v roce 2013 dosáhl zásadního průlomu matematik Yitang Zhang. Dokázal, že existuje nekonečně mnoho párů po sobě jdoucích prvočísel, jejichž rozdíl odpovídá nějakému číslu n<70000000.

Následně téhož roku James Maynard oznámil další průlom, dokázal, že existuje nekonečně mnoho párů prvočísel, jejichž rozdíl je nejvýše n≤600.

V roce 2014 Terence Tao a James Maynard v rámci Polymath8 projektu dokázali snížit hranici na n<246. Existuje tedy nekonečně mnoho dvojic prvočísel s rozdílem nejvýše 246, avšak přesná hodnota n, pro kterou to platí, zatím není známa.

Za předpokladu platnosti Elliottovy–Halberstamovy hypotézy a její zobecněné formy se tato hranice ještě povedla snížit na n≤12 a n≤6. Zároveň bylo ukázáno, že metodami používanými v těchto důkazech již nelze tuto mez zlepšit pod hodnotu 6.

Ago-Jugi hypotéza

Historicky formuloval tuto hypotézu v roce 1950 italský matematik Guiseppe Gluge.

Je pravda, že pokud,

$$\sum_{i=1}^{p-1} i^{p-1} \equiv -1 \; mod \; p$$

pak p je prvočíslo?

Vyzkoušíme pro 7 (zkusili hledat p, kdy vztah neplatí, až do 10^{36067})

$$\sum_{i=1}^{7-1} i^{7-1} \equiv -1 \; mod \; 7$$

$$\sum_{i=1}^{6} i^6 = 1^6 + 2^6 + 3^6 + 4^6 + 5^6 + 6^6 = 67171 \equiv -1 \; mod \; 7$$

Konvergence řady R

Konverguje řada R?

$$R = \sum_{k=1}^{\infty} (-1)^k \frac{k}{p_k}$$

Další odkazy na [Prime Sums -- from Wolfram MathWorld]

Pokud však konverguje, pak je jistě existuje nekonečně mnoho prvočíselných dvojčat . Vyplývá to z věty o rozdělení prvočísel a Leibnizova testu (což je konvergentní kritérium pro alternující řady).

Gilbraithova domněnka

Gilbreath's Conjecture -- from Wolfram MathWorld

Pro jakékoli přirozené číslo začíná posloupnost absolutních rozdílů 3. řádu pro posloupnost prvočísel na 1.

Absolutní rozdíly 1. řádu jsou absolutní velikosti rozdílů mezi sousedními prvočísly: Rozdíly 2. řádu jsou absolutní velikosti rozdílu mezi sousedními prvky v posloupnosti absolutních rozdílů 1. řádu: atd.

Hypotéza je ověřena empiricky pro všechna n < $3{,}4\times10^{11}$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, …
1, 2, 2, 4, 2, 4, 2, 4, 6, …
1, 0, 2, 2, 2, 2, 2, 2, …
1, 2, 0, 0, 0, 0, 0, …
1, 2, 0, 0, 0, 0, …
1, 2, 0, 0, 0, …
1, 2, 0, 0, …
1, 2, 0, …
1, 2, …
1, …

Bunyakovskyho domněnka

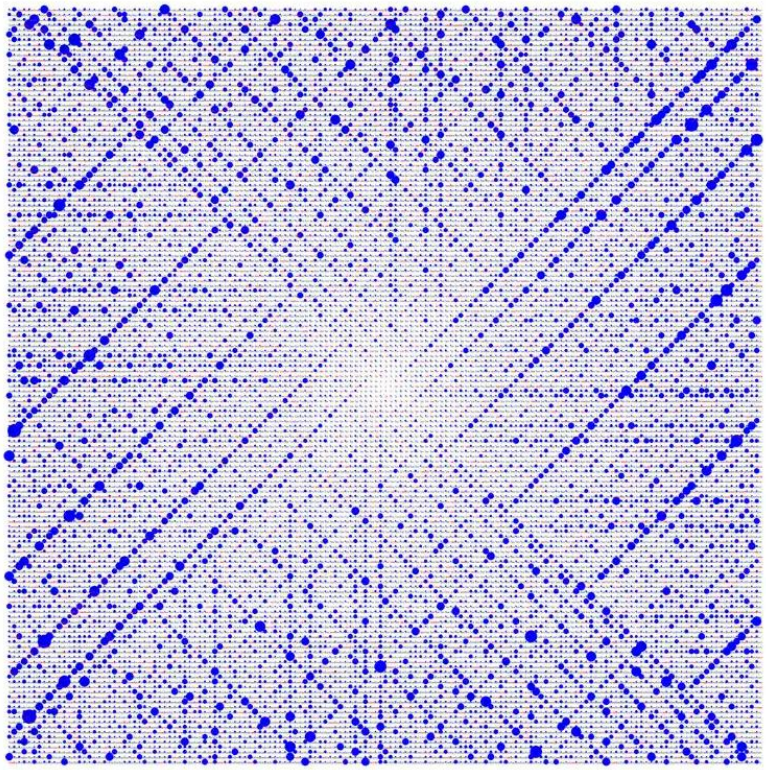
Bunyakovsky conjecture - Wikipedia

Jestliže $f(x)$ je integrální ireducibilní polynom a d=1 je největší společný dělitel všech jeho hodnot, pak integrální polynom nabývá nekonečně mnoho prvočísel. Landauův 4. problém je konkrétním případem této domněnky pro $f(x) = x^2 + 1$.

Další nepříliš jednoduché problémy:

- Jsou všechna Mersennova čísla s prvočísly bez čtverců ?
- Existuje třetí Wieferichovo prvočíslo?
    - To je prvočíslo p, pro něž platí, $2^{p-1} \equiv 1 \; mod \; p^2$. Jediná dosud známá Wieferichova prvočísla jsou 1093 a 3511. Dále je známo, že až do $6{,}7\times10^{15}$ další Wieferichovo prvočíslo neexistuje.
- Existují nějaká Wolstenholmova prvočísla jiná než 16843 a 2124679 ?
    - V teorii čísel je Wolstenholmeovo číslo prvočíslo p, pokud splňuje následující podmínku: $\binom{2p-1}{p-1} \equiv 1 \; mod \; p$

- Existuje polynom jiný než lineární, mezi jehož hodnotami je nekonečně mnoho prvočísel?
- Proč jsou prvočísla uspořádána v řetězcích podél úhlopříček Ulamovy spirály ?



- Je pravda, že pouze tři prvočísla, konkrétně 5, 13 a 97, mohou být reprezentována ve tvaru $2^k + 3^k$ pro nějaké přirozené číslo k?

Nevyřešených problémů a zobecnění těchto problémů je celá řada. Jimi se zabývá celá řada publikací, které lze na internetu nalézt.

Kapitola 8 – Skeptický závěr

Závěr aneb nikdo nic neví.

Asi to bude chtít nějaký zásadní objev. Spousta matematiků tuší, že řada vztahů mezi prvočísly je důsledkem vztahů mezi čísly v nějakém vyšším řádu, nového číselného uspořádání, metamatematiky,...

Něco podobného, jako je základní věta algebry jednoduše dokázána v komplexní analytice.

Možná, že se bude jednat o teorii nekonečných svazů s pseudonáhodnými prvky anebo spíše o úplně něco jiného. Třeba ta teorie již vznikla, ale nedočkala se zatím náležitého ocenění, jako kdysi teorie množin. Tak uvidíme.

Bibliografie

Grebík, J. (2014). *Od asymptotické hustoty k Riemannově zeta-funkci.* Praha: MFF UK KTIaML.

Halaš, R. (1997). *Úvod do teorie čísel.* Olomouc: Universita Palackého v Olomouci.

Jahoda, P. (2010). *Základy teorie čísel a jejích aplikací pro nematematiky.* Ostrava, Plzeň: VŠB Ostrava, ZČU Plzeň.

MathWorld, W. (2025). *Number Theory.* Načteno z Wolfram MathWorld: https://mathworld.wolfram.com/topics/NumberTheory.html

OEIS. (2025). *The On-Line Encyclopedia of Integer Sequences (OEIS).* Načteno z The On-Line Encyclopedia of Integer Sequences (OEIS): https://oeis.org/

wiki7, W. (2024). *Otevřené problémy v teorii čísel* . Načteno z wiki7.org: https://cs.wiki7.org/wiki

WolframAlpfa. (2025). *WolframAlpfa.* Načteno z WolframAlpfa: https://www.wolframalpha.com/