TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta přírodovědně-humanitní
a pedagogická

# Prvočísla, jejich vybrané vlastnosti a aplikace

## Bakalářská práce

*Studijní program:* B1101 Matematika
*Studijní obory:* Matematika se zaměřením na vzdělávání
Informatika se zaměřením na vzdělávání

*Autor práce:* **Jana Marhanová**
*Vedoucí práce:* doc. Ing. Martin Plešinger, Ph.D.
Katedra matematiky a didaktiky matematiky

Liberec 2021

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta přírodovědně-humanitní
a pedagogická

**Zadání bakalářské práce**

# Prvočísla, jejich vybrané vlastnosti a aplikace

*Jméno a příjmení:* **Jana Marhanová**
*Osobní číslo:* P18000278
*Studijní program:* B1101 Matematika
*Studijní obory:* Matematika se zaměřením na vzdělávání
Informatika se zaměřením na vzdělávání
*Zadávající katedra:* Katedra matematiky a didaktiky matematiky
*Akademický rok:* **2019/2020**

**Zásady pro vypracování:**

Přirozená čísla mající právě dva různé přirozené dělitele, tedy prvočísla, hrají stěžejní roli v elementární aritmetice, díky čemuž se s nimi lidé potkávají a potýkají již od nepaměti. Do dnešních dní byla objevena celá řada pozoruhodných a často velmi důležitých vlastností těchto čísel. Další řada otázek souvisejících
s prvočísly, např. s jejich rozložením na číselné ose, zůstává stále nezodpovězena. Našli jsme různá jejich zobecnění, např. tzv. Gaußova prvočísla. Našli jsme hluboké souvislosti mezi prvočísly a dalšími disciplínami matematiky, např. tzv. Riemannova hypotéza. Dokázali jsme je i prakticky využít, např. v tzv. RSA šifrování.
Tato bakalářská práce si klade za cíl čtenáře seznámit s vybranými vlastnostmi prvočísel, včetně důkazů v těch případech, kdy to bude vhodné a zejména možné. Práce dále naznačí čtenáři v čem tkví souvislost mezi prvočísly a Riemannovou hypotézou, seznámí jej se základním principem RSA, případně dalšími vhodnými aplikacemi prvočísel v matematice.
Základní znalosti z teorie čísel, obecné algebry, analýzy a diskrétní matematiky. Základní znalost anglického jazyka. Práce by měla být psána tak, aby mohla celá, nebo její části, sloužit jako materiál pro úvod studia dané problematiky. Práce by měla být psaná v LaTeXu, bude-li to v možnostech studenta.

*Rozsah grafických prací:*
*Rozsah pracovní zprávy:*
*Forma zpracování práce:* tištěná/elektronická
*Jazyk práce:* Čeština

**Seznam odborné literatury:**


Tom Mike Apostol: *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer, 1976.
Marcus du Satoy: *The music of the primes: Searching to solve the greatest mystery in mathematics*, Harper Perennial, 2003.
Marcus du Satoy: *Hudba prvočísel: Dvě století Riemannovy hypotézy* (překlad Luboš Pick, Mirko Rokyta), Argo Dokořán, 2019.
Albert Edward Ingham: *The distribution of prime numbers*, Cambridge Mathematical Library, Cambridge University Press, 1964.
Dimitris Koukoulopoulos: *The distribution of prime numbers*, Graduate Studies in Mathematics 203, American Mathematical Society, 2020.
Barry Mazur, William Stein: *Prime numbers and the Riemann hypothesis*, Cambridge University Press, 2016.
Alfred Menezes, Paul van Oorschot, Scott Vanstone: *Handbook of applied cryptography*, CRC Press, 1996.
David Stanovský: *Základy algebry*, Matfyzpress, 2010.
Ramin Takloo-Bighash: *A Pythagorean Introduction to Number Theory: Right Triangles, Sums of Squares, and Arithmetic*, Undergraduate Texts in Mathematics,
Springer, 2018.
Gerald Tenenbaum, Michel Mendes France: *The prime numbers and their distribution*, Student Mathematical Library 6, American Mathematical Society, 2000.


*Vedoucí práce:* doc. Ing. Martin Plešinger, Ph.D.
Katedra matematiky a didaktiky matematiky

*Datum zadání práce:* 1. prosince 2019
*Předpokládaný termín odevzdání:* 1. května 2021

L.S.

prof. RNDr. Jan Picek, CSc.
děkan

doc. RNDr. Jana Příhonská, Ph.D.
vedoucí katedry

V Liberci dne 18. prosince 2019

# Prohlášení

Prohlašuji, že svou bakalářskou práci jsem vypracovala samostatně jako původní dílo s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Jsem si vědoma toho, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu Technické univerzity v Liberci.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti Technickou univerzitu v Liberci; v tomto případě má Technická univerzita v Liberci právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Současně čestně prohlašuji, že text elektronické podoby práce vložený do IS/STAG se shoduje s textem tištěné podoby práce.

Beru na vědomí, že má bakalářská práce bude zveřejněna Technickou univerzitou v Liberci v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

Jsem si vědoma následků, které podle zákona o vysokých školách mohou vyplývat z porušení tohoto prohlášení.

16. dubna 2021 Jana Marhanová

# Prvočísla, jejich vybrané vlastnosti a aplikace

## Abstrakt

Přirozená čísla mající právě dva různé přirozené dělitele, tedy prvočísla, hrají stěžejní roli v elementární aritmetice, díky čemuž se s nimi lidé potkávají a potýkají již od nepaměti. Do dnešních dní byla objevena celá řada pozoruhodných a často velmi důležitých vlastností těchto čísel. Další řada otázek souvisejících s prvočísly, např. s jejich rozložením na číselné ose, zůstává stále nezodpovězena. Zaměřili jsme se na hluboké souvislosti mezi prvočísly a dalšími disciplínami matematiky, např. na tzv. Riemannovu hypotézu. Dokázali jsme je i prakticky využít, např. v tzv. RSA šifrování či při jedenáctkovém samodetekujícím kódu.

Tato bakalářská práce si klade za cíl čtenáře seznámit s vybranými vlastnostmi prvočísel, včetně důkazů v těch případech, kdy to bude vhodné a zejména možné. Práce dále naznačí čtenáři v čem tkví souvislost mezi prvočísly a Riemannovou hypotézou, seznámí jej se základním principem metody RSA, případně dalšími vhodnými aplikacemi prvočísel v matematice.

**Klíčová slova:** prvočísla; testování prvočíselnosti; Mersennova prvočísla; Fermatova prvočísla; Riemannova hypotéza; metoda RSA; Ulamova spirála

# Primes, their selected properties and applications

## Abstract

Natural numbers with two different natural divisors, called prime numbers, are playing a key role in elementary arithmetic, thanks to which people have come across them since the beginning of time. To this day, there have been discovered a number of remarkable and often very important properties of these numbers. There are lots of alternative questions related to prime numbers, which remains unanswered, for example the location of prime numbers on the numerical axis. We focused on deep context between the prime numbers and other mathematical disciplines, namely Riemann hypothesis. We also discribed where they can be used, for instance in RSA algorithm and in eleven self-detecting code.

Main purpose of this bachelor thesis is to familiarize readers with selected properties of prime numbers, including proofs in which it would be appropriate and possible. Thesis also informs about the relationship between the prime numbers and the Riemann hypothesis, introduces the main principle of the RSA algorithm, eventually other applications of prime numbers in mathematics.

**Keywords:** primes; primality testing; Mersenne primes; Fermat primes; Riemann hypothesis; RSA algorithm; Ulam's spiral

# Poděkování

Chtěla bych poděkovat vedoucímu své bakalářské práce Martinu Plešingerovi za jeho vstřícnost, ochotu, cenné rady a připomínky, kterých se mi při zpracování této bakalářské práce dostávalo.

# Obsah

# Seznam obrázků

# Seznam tabulek

# Seznam algoritmů

# Seznam značení

| | |
|---|---|
| $\mathbb{N} = \{1, 2, 3, \ldots\}$ | přirozená čísla |
| $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ | nezáporná celá čísla |
| $\mathbb{Z}$ | celá čísla |
| $\mathbb{Z}^+$ | kladná celá čísla |
| $\mathbb{R}$ | reálná čísla |
| $\mathbb{P} = \{2, 3, 5, \ldots\}$ | prvočísla |
| $!$ | faktoriál |
| $\ln$ | přirozený logaritmus |
| $b \mid a$ | $b$ dělí $a$ |
| $b \nmid a$ | $b$ nedělí $a$ |
| $gcd(a, b)$ | největší společný dělitel $a$ a $b$ |
| $a \equiv b \pmod{m}$ | $a$ je kongruentní s $b$ modulo $m$ |
| $a \not\equiv b \pmod{m}$ | $a$ není kongruentní s $b$ modulo $m$ |
| $\varphi(n)$ | Eulerova funkce |
| $\pi(x)$ | prvočíselná funkce |
| $\zeta(s)$ | Riemannova zeta funkce |
| $\Re(s)$ | reálná část komplexního čísla $s$ |
| $\prod$ | součin |
| $\sum$ | součet |
| $\lim$ | limita |
| $\int$ | integrál |
| $\exists$ | existuje |
| $\forall$ | pro všechna |
| $\in$ | náležet |
| $\notin$ | nenáležet |
| $\iff$ | právě tehdy když |

# Úvod

Prvočísla jsou považována za jednu z nejzáhadnějších oblastí matematiky. Fascinují matematiky po tisíce let a se stále se rozvíjejícími novými technologiemi a matematickými metodami dochází k objevování nových poznatků, informací a s nimi spojených zajímavostí o přirozených číslech mající právě dva různé dělitele. Čím více je určitá oblast zahalena tajemstvím, tím více vyvstává různých otázek s ní spojených. Prvočísla nejsou výjimkou. Na některé otázky, které byly vyřčeny v dávné minulosti, se podařilo nalézt odpovědi téměř okamžitě, na některé jsme si ale museli pár desítek, stovek a někdy až tisíce let počkat. Za jejich vyřešení vděčíme pokroku především v oblasti výpočetní techniky. I přes to dodnes však některé otázky zůstávají nezodpovězeny a není známo, zda se vůbec někdy na ně odpovědi podaří nalézt. Zmiňme například Riemannovu hypotézu, která je považována za jeden z nejtěžších matematických problémů vůbec. Má zásadní vliv na rozložení prvočísel, a proto je ji věnována jedna samostatná kapitola. Dále se sem řadí například Hypotéza prvočíselných dvojic nebo také otázka týkající se počtu Mersennových prvočísel. Nad těmito nevyřešenými otázkami si lámali hlavy jedni z největších matematiků všech dob, a i přesto dodnes důkazy neexistují.

Cílem této bakalářské práce je seznámit čtenáře s vybranými vlastnostmi, souvislostmi a aplikacemi prvočísel, poukázat na jejich jedinečnost a zásadní roli hrající v oblasti matematiky, informatiky nebo také kultury. Taktéž shrnout základní poznatky o prvočíslech z obecné algebry, díky kterým se čtenář může blíže seznámit s testy sloužícími pro ověřování prvočíselnosti a síty určenými k hledání prvočísel, ale také s metodou RSA jako jednou z nejbezpečnějších asynchronních šifer na světě. V neposlední řadě pak co nejdetailněji a nejsrozumitelněji popsat v čem tkví kouzlo Riemannovy hypotézy.

Bakalářská práce v kapitole 1 seznamuje čtenáře s pojmy, větami a důkazy z obecné algebry, jenž přispívají k většímu pochopení souvislostí v celé práci. Mezi ně lze zařadit relaci kongruenci, relaci býti dělitelem a s ní souvisejícími pojmy největší společný dělitel či soudělná a nesoudělná čísla, která využijeme při definici Eulerovy funkce. V kapitole 2 se zaměřujeme na základní poznatky o prvočíslech, známých již ze základních resp. středních škol, jako je samotná definice prvočísla a složeného čísla, důkaz o počtu prvočísel a dvě věty, základní věta aritmetiky a malá Fermatova věta, vyzdvihující jedinečnost prvočísel. V kapitole 3 práce čtenáře seznámí s užitečnými testy sloužícími k ověřování prvočíselnosti čísel a dvěma síty, které lze využít pro hledání prvočísel do určité horní hranice. U těchto sít jsou mimo jiné k dispozici algoritmy vytvořené v programovacím jazyce Matlab. V kapitole 4 představíme vybrané speciální typy prvočísel, především Mersennova čísla a prvočísla a Fer-

matova čísla a prvočísla, u kterých lze zhlédnout tabulku s informacemi o nich, jako je například počet cifer či počet jejich dělitelů. Kapitola 5 je věnována jednomu z nejtěžších a nejzáhadnějších matematických problémů vůbec, nesoucí název po svém představiteli, německému matematikovi Bernhardu Riemannovi, Riemannově hypotéze. Zaměříme se zejména na její blízkou spojitost s rozložením prvočísel. V předposlední kapitole 6 se čtenář seznámí s dalšími využitími prvočísel mimo oblast matematiky, jmenujme například v oblasti šifrování metodu RSA, jež je neodmyslitelnou součástí online bankovnictví či zasílání tajných vojenských zpráv, dále užití jedenáctkového samodetekujícího kódu, který je využíván při ověřování zápisů rodných čísel osob České republiky, ISBN knih, ISSN časopisů či identifikačních čísel osob/organizací. Taktéž zmíníme jedno zajímavé užití prvočísel v přírodě. V poslední kapitole 7 se zaměříme na dvě zajímavosti podtrhující jedinečnost těchto čísel. Konkrétně jsou jimi Ulamova spirála a Prime gaps neboli mezery nacházející se mezi po sobě jdoucími prvočísly.

# 1 Úvod do teorie dělitelnosti

Tato kapitola se zabývá oblastmi obecné algebry, jejichž znalost je pro pochopení souvislostí v této bakalářské práci nezbytná. Připomeneme si relaci býti dělitelem, z čehož plynule přejdeme k pojmu největší společný dělitel, se kterým jsou spjata soudělná a nesoudělná čísla. Ta nám také poslouží jako stavební pilíře pro Eulerovu funkci, o které pojednává samostatná sekce. V této úvodní kapitole nelze nezmínit ani relaci kongruence, kterou využijeme především při testech ověřujících prvočíselnost čísel či metodě RSA v kapitole o využití prvočísel. Abychom předešli občas ne zcela jednotnému značení přirozených čísel, objasníme si značení, které používáme v celé bakalářské práci my – symbolem $\mathbb{N}$ značíme kladná celá čísla, zatímco symbolem $\mathbb{N}_0$ označujeme nezáporná celá čísla.

## 1.1 Relace být dělitelem

Uvažujme, že operaci dělení provádíme na oboru přirozených čísel $\mathbb{N}$. Jestliže dělíme číslo $b$ číslem $a$, pak intuitivně tuto operaci chápeme jako odečítání čísla $b$ od čísla $a$ právě tolikrát, dokud není výsledek tohoto odečítání menší než číslo $b$. *Právě tolikrát, kolikrát číslo $b$ odečteme od čísla $a$* se označuje jako celočíselný podíl, neboli kvocient $q$. Kvocient tudíž v našem případě náleží oboru přirozených čísel $\mathbb{N}$. Jestliže výsledek odečítání je roven nule, pak hovoříme o tom, že číslo $b$ je dělitelem čísla $a$, formálně viz definice 1. Pokud nastane situace, že výsledek je menší než číslo $b$ a číslu nula se nerovná, pak se toto číslo označuje jako zbytek po dělení, neboli reziduum $r$. Dělení čísel se zbytkem můžeme zformulovat následujícím způsobem

**Věta 1.** *Nechť máme $a, b \in \mathbb{N}$. Pak existuje takové $q \in \mathbb{N}$ a $r \in \mathbb{N}_0$, pro které platí, že*

$$a = b \cdot q + r, \qquad 0 \leq r \leq b - 1. \tag{1.1}$$

*Přičemž čísla $q$ a $r$ jsou dána jednoznačně.*

*Důkaz.* Důkaz provedeme důkazem sporem. Předpokládejme, že existují dvě dvojice čísel $q$ a $r$, pro něž platí

$$\begin{aligned} a &= b \cdot q_1 + r_1, \qquad 0 \leq r_1 \leq b - 1; \\ a &= b \cdot q_2 + r_2, \qquad 0 \leq r_2 \leq b - 1. \end{aligned}$$

Oba dva rozklady čísla $a$ se musí tedy rovnat

$$\begin{aligned} b \cdot q_1 + r_1 &= b \cdot q_2 + r_2 \\ b \cdot (q_1 - q_2) &= r_2 - r_1. \end{aligned} \tag{1.2}$$

Z úpravy rovnice (1.2) platí, že číslo $(r_2 - r_1)$ je dělitelné číslem $b$. Dále pokud vezmeme v potaz extrémy čísla $(r_2 - r_1)$, tedy jaké minimální a maximální hodnoty toto číslo může nabývat, dostáváme interval

$$r_2 - r_1 \in \{1 - b, 2 - b, \ldots, -1, 0, 1, \ldots, b - 2, b - 1\}.$$

Pakliže totiž zkoumáme extrém, kde zbytek $r_1$ je roven své maximální hodnotě $(b-1)$ a tudíž zbytek $r_2$ je roven své minimální hodnotě 0, z rovnice (1.2) dostaváme, že číslo $(r_2-r_1)$ je rovno $(1-b)$. A naopak pokud zkoumáme opačný extrém, kde $r_1 = 0$ a $r_2 = b-1$, z totožné rovnice dostáváme, že číslo $(r_2 - r_1)$ je rovno $(b-1)$. Jestliže dbáme současně i na první podmínku, která říká, že rozdíl zbytků je dělitelný číslem $b$, pak jediné číslo, které oběma podmínkám vyhovuje, je číslo 0, tedy

$$\begin{aligned} r_2 - r_1 &= 0 \\ r_2 &= r_1. \end{aligned}$$

Z rovnice (1.2) pak dostáváme rovnost $b \cdot q_1 = b \cdot q_2$, a protože $b$ se jistě nule nerovná, tak zřejmě musí platit, že kvocienty $q_1, q_2$ jsou si rovny. Dokázali jsme tedy, že čísla $r$ a $q$ jsou vždy dána jednoznačně. □

V úvodním odstavci této sekce jsme nastínili možné chápání pojmu dělitel, nyní si ho však zadefinujeme formálně.

**Definice 1.** *Uvažujme čísla $a, b$. Jestliže existuje číslo $q$, pro které platí rovnost $a = b \cdot q$, pak číslo $b$ je dělitelem čísla $a$.*

Symbolicky toto tvrzení lze zapsat následující ekvivalencí

$$b \mid a \iff \exists\, q \;:\; a = b \cdot q. \tag{1.3}$$

Relaci být dělitelem budeme tedy značit jako $b \mid a$. Je zřejmé, že pro každé $a$ platí $a = 1 \cdot a$. Analogicky tak z definice (1.3) platí, že dělitelem čísla $a$ je číslo $a$. Bez pochyb i číslo 1 dělí číslo $a$. Tyto dva dělitelé se označují jako *triviální dělitelé* čísla $a$. *Netriviálními děliteli* čísla $a$ se pak označují všechny dělitelé, které nejsou děliteli triviálními. Vzhledem k zaměření této bakalářské práce je důležité říci, že prvočísla mají pouze triviální dělitele.

**Poznámka 1.** *V úvodu sekce 1.1 jsme zmínili, že operaci dělení provádíme na oboru přirozených čísel $\mathbb{N} = \{1, 2, 3, \ldots\}$. S nulou tedy nepočítáme. Pokud bychom brali v potaz, že operaci dělení provádíme na oboru nezáporných celých čísel $\mathbb{N}_0$, pak platí, že každé číslo $b \in \mathbb{N}_0$ dělí nulu, poněvadž číslem $q$ z definice 1 je nula. Na druhou stranu číslo nula není dělitelem žádného nenulového čísla $a$, neboť v tomto případě číslo $q$ splňující již zmíněnou definici neexistuje.*

**Poznámka 2.** *Všimněme si, že ve větě 1 jsme hovořili o číslech $a, b$ a $q$ z množiny přirozených čísel $\mathbb{N}$ a o čísle $r$ z množiny nezáporných celých čísel $\mathbb{N}_0$. V definici 1 však nezmiňujeme z jaké číselné množiny čísla $a, b$ a $q$ jsou, neboť tato definice platí i pro čísla z jiných číselných množin, než je množina přirozených čísel $\mathbb{N}$. Jmenujme například $\mathbb{Z}$ či $\mathbb{R}$.*

## 1.2 Největší společný dělitel

Nechť máme dvě *různá* nezáporná celá čísla $c, d \in \mathbb{N}_0$ (popř. více *různých* nezáporných celých čísel, popř. můžeme uvažovat i jiné číselné množiny), společnými děliteli čísel $c, d$ jsou čísla z množiny celých čísel, jež dělí obě tato čísla beze zbytku. *Největším společným dělitelem (NSD, the greatest common divisor, gcd)* se pak označuje takové přirozené číslo, které je z množiny společných dělitelů dělitelem největším. Značíme ho $gcd(c, d)$, zkratkou utvořenou z anglického *the greatest common divisor*.

K nalezení NSD máme k dispozici několik algoritmů. Tím pravděpodobně nejznámějším, avšak ne vždy tím nejefektivnějším, je užití rozkladu čísel $c, d$ na součin prvočísel, o kterém pojednává věta 2. Abychom NSD těchto čísel nalezli, v daných rozkladech čísel musíme hledat taková prvočísla umocněna na nejmenší exponent, jež jsou zastoupena v rozkladech všech čísel. Jejich součin je oním NSD čísel $c$ a $d$. Tento způsob hledání je však v mnoha případech prakticky nerealizovatelný, zvláště pokud bychom hledali NSD opravdu velkých čísel. K tomu slouží mnohem efektivnější algoritmus, který je znám jako Euklidův a jenž je detailněji popsán např. ve skriptech [8, str. 40–42] či v knize [6, str. 36–37] i s uvedením konkrétního příkladu a geometrického znázornění Euklidova algoritmu. Znalost pojmu *největší společný dělitel* nám pomůže k zavedení pojmu nesoudělná, resp. soudělná čísla.

**Definice 2.** *Uvažujme dvě různá čísla $c, d \in \mathbb{N}_0$. Jestliže největším společným dělitelem těchto čísel je jedna, symbolicky $gcd(c, d) = 1$, pak čísla $c, d$ nazýváme nesoudělná.*

Opakem jsou čísla *soudělná*, u kterých platí, že jejich největším společným dělitelem je číslo ostře větší než jedna. Vztáhneme-li to s příklady na prvočísla, pak jakákoliv dvě prvočísla jsou spolu vždy nesoudělná. A naopak soudělná čísla s prvočíslem 2 jsou všechna sudá čísla.

**Poznámka 3.** *Nyní se podíváme blíže na anglickou terminologii. V anglickém jazyce se prvočísla označují primes, nesoudělná čísla co-primes. Není tak úplně náhodou, že jsou si oba anglické termíny velmi podobné, poněvadž nesoudělnost představuje v oblasti prvočísel zásadní roli. Můžeme ji nalézt například v prvočíselných rozkladech čísel, ke kterým míříme na následujících stránkách. Jestliže nalezneme alespoň jedno prvočíslo, které se nachází v obou prvočíselných rozkladech, pak s jistotou můžeme říci, že tato dvě čísla jsou čísla soudělná. Naopak, pokud takové prvočíslo neexistuje, pak jsou tato dvě čísla nesoudělná.*

## 1.3 Kongruence

V této sekci se zaměříme na relaci kongruence, která je velmi úzce spjata s relací býti dělitelem, popsanou výše. Rovnici (1.1), kde $b = m$ lze zapsat jako

$$a \bmod m = r,$$

kde mod značí operaci *modulo* a $a, m \in \mathbb{N}$ a $r \in \mathbb{N}_0$. Právě operace modulo bude hrát stěžejní roli v relaci kongruence. Ještě předtím než si tuto relaci zavedeme, přesuňme se na obor celých čísel $\mathbb{Z}$, doposud jsme se totiž pohybovali na oboru přirozených čísel $\mathbb{N}$. Číslo $a$ tak náleží oboru $\mathbb{Z}$, $m \in \mathbb{N}$ a pro zbytek $r$ platí, že $0 \leq r \leq m-1$. Máme-li dvě čísla $a, b \in \mathbb{Z}$, která po dělení číslem $m$ dávají stejný zbytek $r$, symbolicky zapsáno

$$a \bmod m = r, \qquad b \bmod m = r,$$

pak pomocí relace kongruence, kterou zavádí definice 3 lze tento zápis zjednodušit na

$$a \equiv b \pmod{m} \qquad \text{či} \qquad a \equiv_m b.$$

Tento zjednodušený zápis čteme jako „*a je kongruentní s b modulo m*“. V celé práci budeme používat první zmíněný. Definice relace kongruence následuje.

**Definice 3.** *Relaci kongruence zavádíme na množině celých čísel $\mathbb{Z}$ tak, že*

$$\forall\, a, b \in \mathbb{Z} : a \equiv b \pmod{m},$$

*kde $m \in \mathbb{N}$. Často se lze setkat ještě s upřesněním, že $m \geq 2$, což značí, že výsledný zbytek $r$ je vždy větší než nula, neboť v případě $m = 1$ bychom dostali vždy nulový zbytek.*

**Poznámka 4.** *Uvažujme kongruenci $a \equiv 0 \pmod{m}$, kde $a \in \mathbb{Z}$ a $m \in \mathbb{N}$. Pak tato kongruence značí, že číslo $m$ je dělitelem čísla $a$, tedy $m \mid a$. Z rovnice $0 \bmod m = r$ totiž dostáváme, že zbytek $r$ je roven nule. Z toho však vyplývá, že musí platit rovnice $a \bmod m = 0$ a ta platí jen a pouze tehdy, pokud je číslo $m$ dělitelem čísla $a$.*

## 1.4 Eulerova funkce

V sekci 1.2 jsme si zadefinovali soudělná, resp. nesoudělná čísla. Je zřejmé, že když si zvolíme nějaké číslo $n$ z množiny čísel $\{2, 3, 4, \ldots\}$, pak v množině $\{1, 2, \ldots, n-1\}$ můžeme nalézt jak čísla soudělná, tak čísla nesoudělná s číslem $n$. Počet těchto nesoudělných čísel s číslem $n$ označujeme jako Eulerovu funkci $\varphi(n)$. V tabulce 1.1 můžeme zhlédnout příklady této funkce pro přirozená čísla větší než jedna.

**Poznámka 5.** *Všimněme si, že u čísel $2, 3$ a $5$ platí, že Eulerova funkce $\varphi(n)$ je rovna danému číslu mínus jedné. I když jsme si pojem prvočíslo ještě nezavedli, je natolik známý, že lze prohlásit následující. Pro prvočísla $p \in \mathbb{P}$ (tedy i pro uvedená čísla $2, 3, 5$) platí, že $\varphi(p) = p - 1$. Důkaz je patrný na příkladech v tabulce 1.1, kde největší společný dělitel každého čísla z množiny $\{1, 2, \ldots, p-1\}$ a čísla $p$ je roven jedné, tudíž jsou tato všechna čísla s prvočíslem $p$ nesoudělná. Dále si lze všimnout, že u přirozených mocnin prvočísel platí, že $\varphi(p^k) = p^{k-1}(p-1)$ a pro součin různých prvočísel, jež jsou zastoupena v prvočíselném rozkladu právě jednou, $\varphi(p \cdot q) = (p-1)(q-1)$. Důkazy těchto tvrzení lze nalézt ve skriptech [8, str. 75–76].*

Tabulka 1.1: Příklady Eulerovy funkce $\varphi(n)$.

| Přirozené číslo $n > 1$ | Čísla z množiny $\{1, 2, \ldots, n-1\}$ | Eulerova funkce $\varphi(n)$ | Prvočíselný rozklad |
|---|---|---|---|
| 2 | 1 | 1 | 2 |
| 3 | 1, 2 | 2 | 3 |
| 4 | 1, 2, 3 | 2 | $2^2$ |
| 5 | 1, 2, 3, 4 | 4 | 5 |
| 9 | 1, 2, 3, 4, 5, 6, 7, 8 | 6 | $3^2$ |
| 10 | 1, 2, 3, 4, 5, 6, 7, 8, , 9 | 4 | $2 \cdot 5$ |
| 12 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 | 4 | $2^2 \cdot 3$ |
| 15 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 | 8 | $3 \cdot 5$ |

*Dostáváme se tak k obecnému vzorci, který je pro výpočet Eulerovy funkce zásadní. Pakliže chceme určit hodnotu $\varphi(n)$, je třeba číslo $n$ nejprve rozložit na součin prvočísel, viz věta 2, tedy*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ \cdots \ \cdot p_s^{k_s} = \prod_{\ell=1}^{s} p_\ell^{k_\ell}.$$

*Ze zmíněných dvou tvrzení pak snadno odvodíme vzorec pro výpočet Eulerovy funkce $\varphi(n)$ pro jakékoliv přirozené číslo $n > 1$*

$$\varphi(n) = p_1^{k_1-1} \cdot (p_1 - 1) \cdot p_2^{k_2-1} \cdot (p_2 - 1) \cdot \ \cdots \ \cdot p_s^{k_s-1} \cdot (p_s - 1) = \prod_{\ell=1}^{s} p_\ell^{k_\ell-1} \cdot (p_\ell - 1),$$

*neboli*

$$\begin{aligned}
\varphi(n) &= p_1^{k_1} \cdot \left(\frac{p_1 - 1}{p_1}\right) \cdot p_2^{k_2} \cdot \left(\frac{p_2 - 1}{p_2}\right) \cdot \ \cdots \ \cdot p_s^{k_s} \cdot \left(\frac{p_s - 1}{p_s}\right) \\
&= p_1^{k_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot p_2^{k_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ \cdots \ \cdot p_s^{k_s} \cdot \left(1 - \frac{1}{p_s}\right) \\
&= p_1^{k_1} \cdot p_2^{k_2} \cdot \ \cdots \ \cdot p_s^{k_s} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ \cdots \ \cdot \left(1 - \frac{1}{p_s}\right) \\
&= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ \cdots \ \cdot \left(1 - \frac{1}{p_s}\right) \\
&= n \cdot \prod_{\ell=1}^{s} \left(1 - \frac{1}{p_l}\right).
\end{aligned}$$

# 2 Základní informace o prvočíslech

V této kapitole se blíže zaměříme na základní informace o prvočíslech, se kterými jsme se seznámili již na základních, resp. středních školách. Mezi ně patří definice prvočísel a složených čísel, z nichž bude patrný rozdíl mezi nimi. Uvedeme kolik prvočísel existuje a jako důkaz nám poslouží ten, jehož autorem je řecký matematik Euklides, a který je patrně tím nejznámějším důkazem co se počtu prvočísel týče. Mimo to si také představíme základní větu arimetiky poukazující na unikátnost prvočísel a malou Fermatovu větu, na které jsou založeny některé testy prvočíselnosti, o nichž pojednává následující kapitola.

## 2.1 Prvočísla a čísla složená

Abychom se mohli prvočísly a dalšími záležitostmi s nimi spojenými v této práci zabývat, je nutné si tento pojem v úvodu zavést. K tomu nám poslouží následující definice 4, resp. později zmíněná alternativní definice 1, která říká, že

**Definice 4.** *Prvočíslo je přirozené číslo, které má právě dva dělitele. Totiž jedničku a samo sebe.*

Vznikají diskuze, zda je číslo jedna prvočíslem či nikoli, poněvadž číslo jedna má dělitele jedničku a samo sebe, což je ale také jednička. Proto se zde veřejnost rozchází, jak je ostatně patrné i v přehledu [12], který sumarizuje názory na toto téma od cca 100 let př. n. l. až do roku 2011. Mimo jiné v něm lze najít názory jedněch z nejlepších světových matematiků vůbec, jako je Euklides, Marin Mersenne, Christian Goldbach, či Leonhard Euler, ale i dalších odborníků, kteří svými komentáři a poznámkami dokazují či vyvracejí, že číslo jedna je prvočíslem. Z přibližně 125 vzorků cca 40 lidí, což činí 32 %, uvedlo, že číslo jedna prvočíslem skutečně je. Ztotožňují se tak s definicí 4. Většina matematiků a odborníků však tvrdila opak a z jejich komentářů je patrné, že číslo jedna prvočíslem není. Je tedy namístě zavést následující definici, která je uváděna v mnoha publikacích a skriptech a většina odborníků ji v nynější době považuje za jedinou správnou. I my z této definice budeme v celé práci vycházet.

**Alternativní definice 1.** *Prvočíslo je přirozené číslo $p > 1$, které má právě dva různé dělitele. Totiž jedničku a samo sebe.*

Množina prvočísel začíná $\{2, 3, 5, 7, 11, 13, \ldots\}$ a lze o ni říci, že kromě jediného sudého prvočísla 2 v ní nalezneme pouze lichá čísla, poněvadž všechna sudá čísla, kromě čísla 2, jsou složenými čísly, která lze definovat takto:

**Definice 5.** *Číslo $n > 1, n \in \mathbb{N}$, které má minimálně tři různé dělitele, je číslo složené.*

Již víme, že nejmenším prvočíslem je číslo dva, naopak tím největším, které bylo doposud objeveno, je prvočíslo $(2^{82\,589\,933} - 1)$. Stalo se tak díky Patrickovi Larochemu z Floridy z projektu GIMPS, o kterém se lze více dozvědět v sekci 4.1.1, v prosinci roku 2018. Má 24 862 048 číslic a o více než jeden a půl milionu číslic překonalo předchozí rekordní prvočíslo z prosince roku 2017. Je zároveň i 51. *známým* Mersennovým prvočíslem, viz [30]. Zda je opravdu 51. Mersennovým prvočíslem nelze se stoprocentní jistotou říci, neboť na témže odkazu se uvádí, že poslední čtyři představená Mersennova prvočísla nemusí odpovídat svým prozatimním pořadovým číslům. Mersennovým prvočíslům se více věnujeme v sekci 4.1.

## 2.2 Počet prvočísel

Zaměříme-li se na počet prvočísel, zjistíme, že v první stech přirozených číslech najdeme přesně 25 prvočísel. Tedy každé čtvrté číslo je prvočíslem. Mezi 1000 a 1100 nalezneme 16 prvočísel, mezi 10 000 a 10 100 jich je 11 a mezi $10^{20}$ a $10^{20} + 100$ je dokonce jediné, viz [7, str. 15]. I když se zdá, že se stále se zvětšujícími čísly prvočísla řídnou, a tím pádem se musíme dostat do bodu, kdy již žádné prvočíslo nenalezneme, existuje několik důkazů, že tomu tak není. Pravděpodobně tím nejznámějším důkazem, který je zároveň i jedním z nejstarších, se kterými jsme do dnešního dne obeznámeni, je důkaz pocházející od řeckého matematika Euklida, který žil přibližně před 300 lety př. n. l., z jeho knihy Základy. Odpověď na otázku, zda je prvočísel konečně či nekonečně mnoho, byla tak známa již před více než 2000 lety.

*Důkaz.* Důkaz přiřazován Euklidovi je založen na důkazu sporem. Předpokládejme, že prvočísel je konečně mnoho. Označme tedy *konečnou* množinu prvočísel $\mathbb{P}_\kappa = \{p_1, p_2, \ldots, p_\ell\}$. Dále uvažujme číslo $q$ jako součin těchto prvočísel plus jedna

$$q = p_1 \cdot p_2 \cdot \cdots \cdot p_\ell + 1 = \prod_{j=1}^{\ell} p_j + 1. \tag{2.1}$$

Jak lze vypozorovat, žádné prvočíslo z množiny $\mathbb{P}_\kappa$ nedělí číslo $q$, jelikož zbytek po dělení bude vždy jedna. To znamená, že $q$ je buď prvočíslem nebo je dělitelné prvočíslem, které se v množině $\mathbb{P}_\kappa$ nenachází. Což je spor s předpokladem. Prvočísel existuje tudíž nekonečně mnoho. □

**Poznámka 6.** *Stává se, že je tento důkaz někdy mylně interpretován tak, že číslo $q$ je nové prvočíslo nenacházející se v množině $\mathbb{P}_\kappa$, a tím jsme došli ke sporu. Není tomu tak, číslo $q$ nemusí být prvočíslo, jak se můžeme ostatně přesvědčit na následujícím příkladu. Pro hypoteticky konečnou množinu prvočísel*

$$\mathbb{P}_\kappa = \{7, 11, 13\},$$

*zřejmě platí*

$$q = 7 \cdot 11 \cdot 13 + 1 = 1002.$$

*Číslo* 1002 *je sudé, tudíž určitě prvočíslem není. Obdobný výsledek zřejmě dostaneme pro součin libovolně mnoha lichých prvočísel.*

*Pokud bychom analogicky vzali všechna prvočísla menší nebo rovna např. třinácti,*

$$\mathbb{P}_\kappa = \{2, 3, 5, 7, 11, 13\},$$

*pak dostaneme*

$$q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509.$$

*Výsledné číslo tak opět není prvočíslem.*

Tento důkaz 2.1 je takto prezentován v mnoha učebnicích, na mnoha školách, ale originální důkaz, který Euklides ve své knize popsal, byl mírně odlišný. Staří Řekové totiž chápali čísla jako délky úseček, úsečka délky dva byla dvakrát delší než úsečka délky jedna apod. Což poněkud znesnadňovalo jakýkoliv zápis, v tomto případě konkrétně zápis množiny prvočísel. A právě díky tomu, že Euklid nebyl vybaven vhodnými prostředky pro její zapsání, vybral si tři prvočísla A, B, C, která znázornil jako úsečky o různých velikostech a pomocí nich a jejich měření dokázal, že vždy je schopen nalézt další prvočíslo. Před 2000 lety byla představa o nekonečnu odlišná, než jakou máme dnes my, a proto Euklides ve své knize Základy nenapsal, že existuje nekonečně mnoho prvočísel, nýbrž že *„prvočísel je více než přiřazené množství prvočísel“*, viz [2, str. 271]. Originální Euklidův důkaz lze zhlédnout na obrázku 2.1.

Mezi další důkazy patří např. Goldbachův důkaz z roku 1730, jenž k důkazu používá Fermatova čísla, o kterých se lze více dočíst v sekci 4.2, Fürstenbergův důkaz z roku 1955, důkaz Filipa Saidaka z roku 2005 či Kummerovo přepracování Euklidova důkazu. O těchto důkazech je možno nalézt více informací na webové stránce [11].

**Otevřený problém 1.** *Otázkou zůstává, kolik existuje prvočíselných dvojic (někdy také označovaných jako prvočíselných dvojčat), dvou po sobě jdoucích prvočísel, mezi nimiž rozdíl činí dvě. Lze je tedy zapsat ve tvaru* $(p, p+2)$*, kde* $p \in \mathbb{P}$*. S touto otázkou souvisí tzv. Hypotéza prvočíselných dvojic a dodnes zůstává nezodpovězena.*

**Komentář 1.** *Stejně tak bychom se mohli ptát na otázku, kolik existuje prvočíselných trojic (též označovaných jako prvočíselných trojčat), tří po sobě jdoucích prvočísel, u kterých rozdíl mezi prvním a druhým prvočíslem, resp. mezi druhým a třetím prvočíslem je roven dvěma. Prvočíselné trojice mají tvar* $(p, p+2, p+4)$*, kde* $p \in \mathbb{P}$*. Odpověď je ale v tomto případě snadná, prvočíselná trojice existuje pouze jediná* $(3,\ 5,\ 7)$*. Důkaz zní následovně, uvědomme si, že se jedná o tři za sebou jdoucí lichá čísla, jedno z nich tak musí být vždy dělitelné třemi. Jediné prvočíslo, které je dělitelné třemi je číslo* 3*. Jiná než zmíněná prvočíselná trojice tedy neexistuje.*

*Dnes jsou známy další speciální typy dvojic, resp. trojic, resp. čtveřic prvočísel. Např. cousin primes, což je dvojice prvočísel, jejichž rozdíl činí čtyři a lze je zapsat ve tvaru* $(p, p+4)$*, kde* $p \in \mathbb{P}$ *či sexy primes, tedy dvojice prvočísel, která se liší o šest a jež jsou ve tvaru* $(p, p+6)$*, kde* $p \in \mathbb{P}$*. Další trojice prvočísel jsou například ve tvaru* $(p, p+2, p+6)$ *či* $(p, p+4, p+6)$*, kde* $p \in \mathbb{P}$*, nebo také čtveřice prvočísel ve tvaru* $(p, p+2, p+6, p+8)$*, kde* $p \in \mathbb{P}$*. Více informací o těchto a dalších typech prvočísel se lze dočíst na webové stránce [34]. Vybrané typy jsou pak popsány v kapitole 4.*

κ′.

Οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.

Ἔστωσαν οἱ προτεθέντες πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ· λέγω, ὅτι τῶν Α, Β, Γ πλείους εἰσὶ πρῶτοι ἀριθμοί.

Εἰλήφθω γὰρ ὁ ὑπὸ τῶν Α, Β, Γ ἐλάχιστος μετρούμενος καὶ ἔστω ΔΕ, καὶ προσκείσθω τῷ ΔΕ μονὰς ἡ ΔΖ. ὁ δὴ ΕΖ ἤτοι πρῶτός ἐστιν ἢ οὔ. ἔστω πρότερον πρῶτος· εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ οἱ Α, Β, Γ, ΕΖ πλείους τῶν Α, Β, Γ.

Ἀλλὰ δὴ μὴ ἔστω ὁ ΕΖ πρῶτος· ὑπὸ πρώτου ἄρα τινὸς ἀριθμοῦ μετρεῖται. μετρείσθω ὑπὸ πρώτου τοῦ Η· λέγω, ὅτι ὁ Η οὐδενὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. εἰ γὰρ δυνατόν, ἔστω. οἱ δὲ Α, Β, Γ τὸν ΔΕ μετροῦσιν· καὶ ὁ Η ἄρα τὸν ΔΕ μετρήσει. μετρεῖ δὲ καὶ τὸν ΕΖ· καὶ λοιπὴν τὴν ΔΖ μονάδα μετρήσει ὁ Η ἀριθμὸς ὤν· ὅπερ ἄτοπον. οὐκ ἄρα ὁ Η ἑνὶ τῶν Α, Β, Γ ἐστιν ὁ αὐτός. καὶ ὑπόκειται πρῶτος. εὑρημένοι ἄρα εἰσὶ πρῶτοι ἀριθμοὶ πλείους τοῦ προτεθέντος πλήθους τῶν Α, Β, Γ οἱ Α, Β, Γ, Η· ὅπερ ἔδει δεῖξαι.

Obrázek 2.1: Originální znění Euklidova důkazu o nekonečně mnoha prvočíslech. Obrázek převzat z knihy Základy, viz [2, Book IX, Proposition 20].

## 2.3 Základní věta aritmetiky

V mnoha případech se můžeme dočíst toho, že prvočísla tvoří jakési *základy* celého oboru matematiky. A nejen jeho, o čemž svědčí kapitola 6, pojednávající o využití prvočísel. Je to dáno především jejich unikátními a nenahraditelnými vlastnostmi, na což poukazuje také základní věta aritmetiky, která říká, že

**Věta 2** (Základní věta aritmetiky)**.** *Každé přirozené číslo $a > 1$ lze rozložit na součin prvočísel. Tento rozklad je jednoznačný až na pořadí prvočísel.*

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ \cdots \ \cdot p_\ell^{k_\ell} = \prod_{j=1}^{\ell} p_j^{k_j},$$

*kde $p_1, p_2, \ldots, p_\ell$ jsou různá prvočísla a $k_1, k_2, \ldots, k_\ell$ jsou kladná přirozená čísla.*

Znění této věty a její důkaz pochází od Euklida z knihy Základy, viz [2, Book VII, Propositions 30, 31, 32]. Stejně jako u důkazu o nekonečně mnoha prvočíslech pocházející z totožné knihy i v tomto případě pracoval Euklides s prvočísly jako s velikostmi úseček.

*Důkaz.* Důkaz základní věty aritmetiky rozdělíme na dvě části. Tou první je *důkaz existence* prvočíselného rozkladu, druhou pak *důkaz* jeho *jednoznačnosti*.

*Důkaz existence.* Tento důkaz provedeme matematickou indukcí. Předpokládejme, že existují prvočíselné rozklady malých čísel až do čísla $n$, např.

$$\begin{aligned} 2 &= 2, \\ 3 &= 3, \\ 4 &= 2^2, \\ 5 &= 5, \\ 6 &= 2 \cdot 3, \\ 7 &= 7, \\ 8 &= 2^3, \\ &\vdots \end{aligned}$$

Následující číslo $(n+1)$ je pak buď prvočíslo (výraz $n+1$ je tedy rovnou hledaný rozklad čísla), nebo se jedná o číslo složené. Pokud by platil druhý případ, pak ale musí existovat čísla $a, b$ taková, že jejich součin je hledaný rozklad čísla $(n+1)$, symbolicky $n+1 = a \cdot b$, kde $1 < a, b < n+1$, resp. $a, b \leq n$. Jak plyne z indukčního předpokladu, prvočíselné rozklady čísel $a$ i $b$ určitě existují a vypadají následovně

$$a = \prod_{j=1}^{\ell} p_j^{k_j}, \quad b = \prod_{t=1}^{r} q_t^{s_t},$$

kde $p_j, q_t \in \mathbb{P}$ a $k_j, s_t \in \mathbb{N}$. Součin těchto dvou čísel

$$n+1 = a \cdot b = \prod_{j=1}^{\ell} p_j^{k_j} \cdot \prod_{t=1}^{r} q_t^{s_t},$$

je právě hledaným prvočíselným rozkladem čísla $(n+1)$. Dokázali jsme, že prvočíselný rozklad vždy existuje. □

*Důkaz jednoznačnosti.* I tento důkaz provedeme matematickou indukcí. Předpokládejme, že rozklad čísel je jednoznačný až do čísla $n$ a číslo $(n+1)$ nechť má dva prvočíselné rozklady

$$n+1 = \prod_{j=1}^{\ell} p_j^{k_j} = \prod_{t=1}^{r} q_t^{s_t},$$

kde $p_j, q_t \in \mathbb{P}$ a $k_j, s_t \in \mathbb{N}$. Vidíme, že $p_1 \mid (n+1)$ a z toho plyne, že $\exists\, r^* \in \{1, \ldots, r\}$ takové, že $p_1 \mid q_{r^*}^{s_{r^*}}$. Obě tato čísla se musí rovnat, neboť jsou prvočísly, $p_1 = q_{r^*}^{s_{r^*}}$. Nyní po označení čísla $c$ jako podíl $(n+1)/p_1$ dostáváme, že

$$c = \frac{n+1}{p_1} = p_1^{k_1 - 1} \cdot \prod_{j=2}^{\ell} p_j^{k_j} = q_{r^*}^{s_{r^*} - 1} \cdot \prod_{t=1, t \neq r^*}^{r} q_t^{s_t}.$$

Z uvedeného podílu také vyplývá nerovnost $n+1 > c$ a tím pádem z indukčního předpokladu plyne, že rozklad čísla $c$ je jednoznačný. Oba rozklady tohoto čísla tak musí být totožné. Z podílu

$$c = \frac{n+1}{p_1}$$

dostáváme, že i číslo $(n+1)$ musí být jednoznačné, což má za důsledek totožnost obou rozkladů tohoto čísla $\prod_{j=1}^{\ell} p_j^{k_j} = \prod_{t=1}^{r} q_t^{s_t}$. Tím jsme dokázali, že prvočíselný rozklad je vždy jednoznačný. □

Dokázali jsme jak *existenci* prvočíselného rozkladu, tak jeho *jednoznačnost* a tím i celou *základní větu aritmetiky*, viz [8, str. 51–52]. □

## 2.4 Malá Fermatova věta

Ještě než si uvedeme znění malé Fermatovy věty (MFV), představíme si Eulerovu větu. Tu v roce 1736 publikoval Leonhard Euler a říká, že pokud jsou čísla $a \in \mathbb{N}$ a $m \in \mathbb{N}, m > 1$ nesoudělná, pak platí

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

kde $\varphi(m)$ značí Eulerovu funkci, o které jsme psali v sekci 1.4. Speciálním případem Eulerovy věty je právě malá Fermatova věta, která bývá připisována francouzskému matematikovi Pierru de Fermatovi, po němž nese svůj název.

**Věta 3** (Malá Fermatova věta)**.** *Nechť $p \in \mathbb{P}$ a nechť $a \in \mathbb{N}$ leží v intervalu $0 < a < p$. Pak*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Důkaz.* Tím, že MFV je speciálním případem Eulerovy věty, v úvodu se zaměříme na to, zda jsou předpoklady této věty splněny. Prvočíslo $p$ je přirozeným číslem, kde $p > 1$ a číslo $a$ je taktéž přirozeným číslem, zároveň je nenulovým a s číslem $p$ je nesoudělné, což jsou všechny předpoklady Eulerovy věty a jenž jsme právě ukázali, že jsou splněny. Nyní po provedení $m = p$, kde $p \in \mathbb{P}$, dostáváme z Eulerovy věty kongruenci $a^{\varphi(p)} \equiv_p 1$. Počet nesoudělných čísel s číslem $p$, tedy hodnota Eulerovy funkce $\varphi(p)$, je roven $(p-1)$, neboť všechna čísla z množiny $\{1, 2, \ldots, p-1\}$ jsou nesoudělná s prvočíslem $p$ (viz tabulka 1.1). Tzn., že zmíněnou kongruenci lze zapsat ve tvaru $a^{p-1} \equiv 1 \pmod{p}$, což byl poslední krok k dokázání malé Fermatovy věty, viz [8, str. 79]. □

# 3 Testování prvočíselnosti a hledání prvočísel

V některých situacích potřebujeme rozhodnout, zda je číslo $n \in \mathbb{N}$ prvočíslo či číslo složené. K tomu nám dopomohou testy, které si v této kapitole představíme. Testy lze rozřadit do dvou skupin, přičemž s užitím tzv. *deterministických testů prvočíselnosti* získáváme stoprocentní jistotu, že námi testované číslo je prvočíslo či číslo složené. Druhou skupinou jsou pak tzv. *pravděpodobnostní testy prvočíselnosti*, které dokážou odhalit, že testované číslo není prvočíslem, anebo v opačném případě, že se jedná o *pravděpodobné* prvočíslo, u kterého je pořád přítomna jistá šance, že prvočíslem není. U každého testu se zaměříme zejména na princip jeho fungování a taktéž si představíme dvě nejznámější síta, která se využívají pro hledání prvočísel do určitého čísla $n \in \mathbb{N}$. U nich kromě principů poukážeme také na algoritmy sestavené v programovacím jazyce Matlab. Bližší informace o zmíněných testech, ale i o těch, jenž v této práci zastoupeny nejsou, se lze dozvědět např. z knih [3] a [9] a či z webové stránky [11].

## 3.1 Eratosthenovo síto

Na úvod je vhodné říci, že Eratosthenovo síto se neřadí k typickým testům pro ověřování prvočíselnosti čísla $n \in \mathbb{N}$, byť jistým způsobem tento účel plní také. Jeho hlavní smysl je však v tom, že díky němu lze získat prvočísla, která jsou menší nebo rovno tohoto námi zadaného čísla $n$. Algoritmus jako první představil matematik, astronom a slavný knihovník Eratosthenes z knihovny v Alexandrii žijící mezi roky 276–194 př. n. l. Eratosthenes nebyl znám *pouze* jako matematik a knihovník, ale také jako vědec, který se zajímal o rozměry Země a přispíval svými postřehy k dalšímu bádání. Jeho síto je dodnes považováno za jeden z nejefektivnějších způsobů nalezení prvočísel a to až do hodnoty 10 000 000, viz [11]. Pro větší čísla je vhodné využít některý z dalších popsaných testů v této kapitole. Výhodou je, že při jeho užití prakticky nepoužíváme žádné dělení, jako tomu je např. u základního testu, který si představíme na dalších stránkách. Označení za síto je velmi výstižné, poněvadž v principu *prosíváme* ze seznamu složená čísla až do doby, kdy nám v něm zbudou pouze prvočísla. Dnes je známa modernější verze Eratosthenova síta z roku 2003 tzv. *Atkinovo síto*, jehož autory jsou Arthur Oliver Lonsdale Atkin a Daniel Julius Bernstein. Zatímco Eratosthenovo síto vyškrtává vždy násobky prvočísel, Atkinovo síto vyškrtává násobky čtverců prvočísel. Stále však zůstává daleko za popularitou jeho předchůdce a pravděpodobně tam navždy zůstane. Jeho princip lze nalézt např. na webové stránce [36].

### 3.1.1 Princip

Princip Eratosthenova síta spočívá ve vyškrtání všech složených čísel z našeho seznamu. Toho dosáhneme tak, že si zapíšeme čísla od 2 do $n \in \mathbb{N}$, kde $n$ určuje horní hranici čísel. Po správném vyškrtání složených čísel nám v seznamu zbudou pouze prvočísla menší nebo rovno $n$. Algoritmus začíná označením prvního čísla v seznamu za prvočíslo a jeho násobky ze seznamu vyškrtneme. Analogicky postupujeme se zbylými neoznačenými čísly až do doby, kdy odstraníme ze seznamu poslední číslo či překročíme hranici $\sqrt{n}$, která je klíčová pro nalezení prvočísel, viz sekce 3.3.

Uveďme si názorný příklad pro hledání prvočísel, jež jsou menší než číslo 100. Čísla se ve většině případů zapisují do seznamu do řádků po deseti číslech, což vede k větší přehlednosti a k usnadnění práce, jak se můžeme ostatně přesvědčit vzápětí na popsaném konkrétním příkladu, resp. na obrázku 3.1. Pokud bychom se rozhodli pro jiné seskupení čísel, na výsledek to nemá žádný vliv. Algoritmus začíná označením prvního čísla ze seznamu za prvočíslo, tím je číslo 2, označme si jej. Následně všechny jeho násobky ze seznamu odstraňme. Nyní první neoznačené číslo v seznamu je číslo 3, které si označme za prvočíslo a stejně jako tomu bylo v případě čísla 2, odstraňme všechny jeho násobky, pakliže doposud odstraněny nebyly. Dále prvním neoznačeným číslem v seznamu je číslo 5, které označme za prvočíslo a vyškrtněme všechny jeho násobky. Takto stejně postupujme i s číslem 7. To je totiž poslední číslo, které nám v seznamu po odstranění všech násobků zbylo a je menší než $\sqrt{100} = 10$, což je důležitá hranice, za kterou se již žádné složené číslo nenachází. V seznamu nám tak zbylo celkem 25 prvočísel, ze sekce 2.1 víme, že je to počet správný.

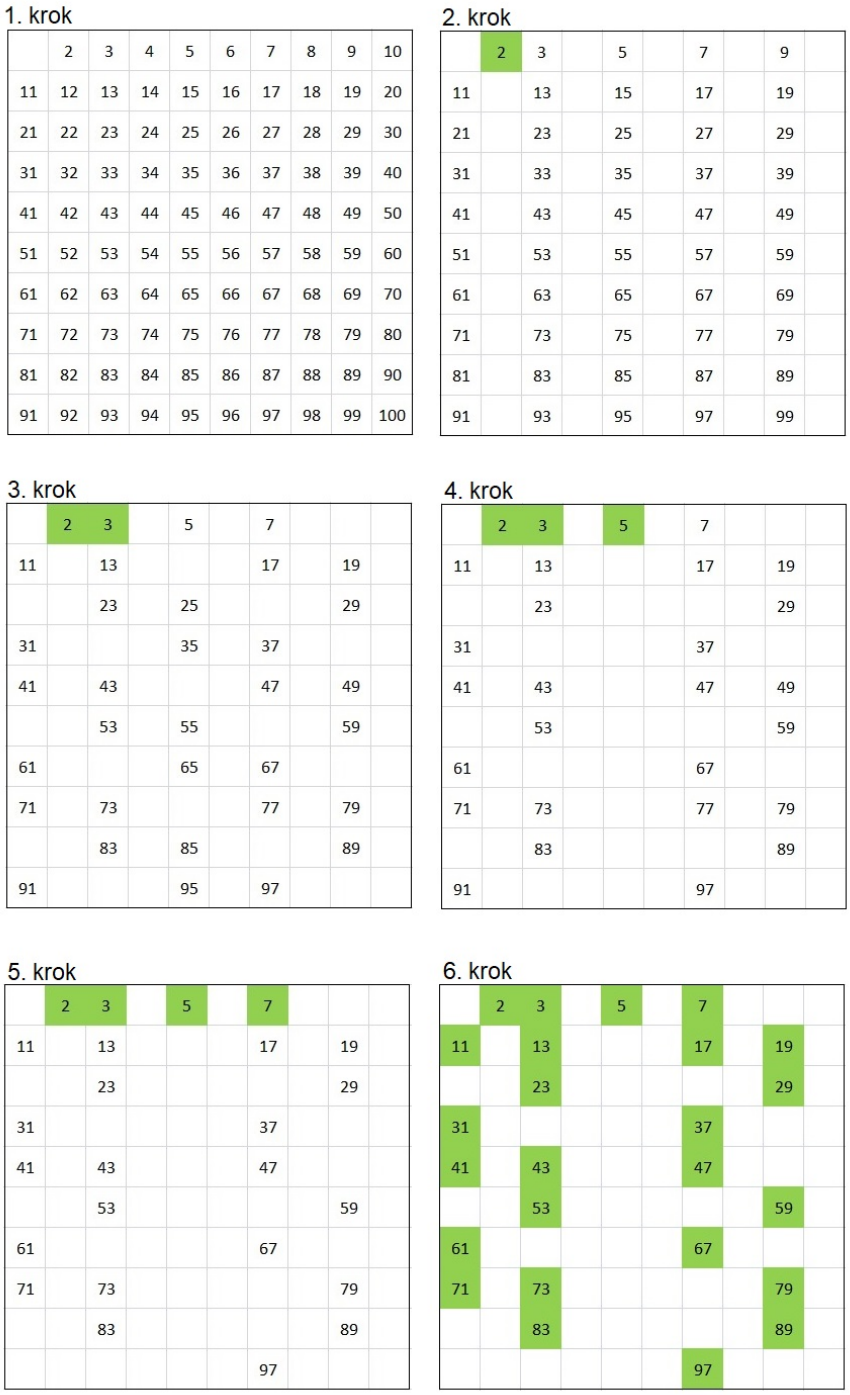
Obrázek 3.1 názorně ilustruje postupné „prosívání“ prvních stovky přirozených čísel (větších než jedna) Eratosthenovovým sítem. V následující sekci představíme obecný algoritmus.

### 3.1.2 Algoritmus

Algoritmus 3.1 (str. 30) ukazuje možnou implementaci Eratosthenova síta v programovacím jazyce Matlab.

## 3.2 Sundaramovo síto

Druhé síto, které si v této práci blíže popíšeme, je Sundaramovo síto. Jedná se o mnohem novější algoritmus, který však slouží ke stejnému účelu jako síto Eratosthenovo, tedy k nalezení všech prvočísel až do čísla $n \in \mathbb{N}$ včetně. Autorem je indický matematik S. P. Sundaram a představil jej v roce 1934. Zatímco Eratosthenovo síto vyškrtává všechny násobky prvočísel, Sundaramovo síto je založeno na principu vyškrtat taková čísla $x$, pro která platí, že $2x + 1$ je rovno lichému složenému číslu. Tato zmíněná operace se totiž provádí na samotném konci algoritmu s čísly zůstávajícími v seznamu. Sudá čísla po provedení operace mezi výslednými čísly nejsou, proto se stačí zaměřit pouze na lichá složená čísla.




Obrázek 3.1: Eratosthenovo síto.

### 3.2.1 Princip

Princip Sundaramova síta začíná obdobně jako princip Eratosthenova síta, zapsáním čísel do seznamu. Dolní hranicí je tentokrát jednička a horní hranicí $\frac{n-1}{2}$, pakliže hledáme prvočísla menší nebo rovno číslu $n$. V závěru tohoto algoritmu se totiž

**Algoritmus 3.1:** Algoritmus Eratosthenova síta v programovacím jazyce Matlab. V algoritmu jsou některé části zjednodušeny.

```
vstup  : cisla = [2, 3, 4, ..., N] ∈ ℕ
vystup: prvocisla = [p_1, p_2, ..., p_k] ∈ ℙ menší nebo rovno N
v = zeros();
for c = 2 : N do
    p(c) = true;
end
for c = 2 : √N do
    n = c + c;
    while n <= N do
        p(n) = false;
        n = n + c;
    end
end
for c = 2 : N do
    if p(c) == true then
        v(c) = c;
    end
end
prvocisla = choosenonzerosof(v)
```

provádí operace $2x + 1$, kde $x$ jsou nevyškrtaná čísla v seznamu, a tím pádem dostáváme, že

$$2x + 1 = 2 \cdot \frac{n-1}{2} + 1 = n - 1 + 1 = n$$

je maximální číslo, které díky tomuto sítu můžeme dostat. Algoritmus začíná tak, že ze seznamu postupně odstraňujeme čísla, která jsou ve tvaru

$$i + j + 2ij, \tag{3.1}$$

kde

$$i + j + 2ij \leq \frac{n-1}{2} \qquad \wedge \qquad i, j \in \mathbb{N}, 1 \leq i \leq j.$$

Abychom dokázali rozšifrovat, proč právě čísla tvaru (3.1) máme ze seznamu odstranit, označme si tento výraz jako $y$. Jako $z$ označme výsledná čísla, se kterými provádíme operaci $2y + 1$. Po dosazení dostáváme, že

$$z = 2y{+}1 = 2{\cdot}(i{+}j{+}2ij){+}1 = 2i{+}2j{+}4ij{+}1 = 2i{\cdot}(1{+}2j){+}2j{+}1 = (2i{+}1){\cdot}(2j{+}1).$$

Z toho vyplývá, že číslo $z$, které se ve výsledném seznamu prvočísel neobjeví, je ve tvaru $(2i + 1) \cdot (2j + 1)$, což je opravdu tvar všech lichých složených čísel.

Stejně jako u Eratosthenova síta, i zde si představíme konkrétní příklad. Hledejme prvočísla, která jsou menší nebo rovno $n = 201$. Odstraňme všechna čísla splňující podmínku (3.1) a kde $i = 1$. Číslo $j$ tak nabývá hodnot $j = \{1, 2, \ldots, 33\}$. Dále

odstraňme čísla, pokud ještě odstraněna nebyla, která opět splňují podmínku (3.1) a kde $i = 2$, $j = \{2, 3, \ldots, 19\}$. Takto postupně pokračujme, když $i = 3$, tak $j = \{3, 4, \ldots, 13\}$, pro $i = 4$, $j = \{4, 5, \ldots, 10\}$, pro $i = 5$, $j = \{5, 6, \ldots, 8\}$ a konečně pro $i = 6$, $j = \{6, 7\}$. Nyní jsme tak všechna čísla, která se vyškrtat dala, vyškrtali. Zbývající čísla v seznamu zdvojnásobme a přičtěme k nim jedničku. Důvod jsme si vysvětlili výše. Dostáváme tedy všechna prvočísla, která jsou menší nebo rovno číslu 201 kromě prvočísla 2, poněvadž zřejmě platí, že nejmenší možné prvočíslo, které díky Sundaramovu sítu lze nalézt, je prvočíslo 3.

Celý popsaný proces lze opět vidět na obrázku 3.2, který je sestaven tak, aby co nejvíce korespondoval s obrázkem 3.1 (na kterém je popsán princip Eratosthenova síta) a čtenář si tak mohl tyto principy porovnat. V následující sekci představíme obecný algoritmus.

**Poznámka 7.** *Zatímco Eratosthenovo síto zkoumá postupně všechna přirozená čísla, Sundaramovo síto zajímají jen lichá čísla díky provedení operace* $2x + 1$ *se zbylými čísly zůstávajícími v seznamu.*

### 3.2.2 Algoritmus

Algoritmus 3.2 ukazuje možnou implementaci Sundaramova síta v programovacím jazyce Matlab.

**Algoritmus 3.2:** Algoritmus Sundaramova síta v programovacím jazyce Matlab. V algoritmu jsou některé části zjednodušeny.

```
vstup  : cisla = [1, 2, 3, ..., (N − 1)/2] ∈ ℕ
vystup: prvocisla = [p_1, p_2, ..., p_k] ∈ ℙ menší nebo rovno N
v = zeros();
for c = 1 : (N − 1)/2 do
    p(c) = true;
end
for i = 1 : (N − 3)/6 do
    for j = 1 : (N − 3)/6 do
        k = i + j + 2 * i * j;
        if k <= (N − 1)/2 && (1 <= i) && (i <= j) then
            p(k) = false;
        end
    end
end
for c = 1 : (N − 1)/2 do
    if p(c) == true then
        v(c) = c;
    end
end
l = choosenonzerosof(v);
prvocisla = 2 * l + 1
```

1. krok

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

2. krok

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | | 5 | 6 | | 8 | 9 | |
| 11 | 12 | | 14 | 15 | | 17 | 18 | | 20 |
| 21 | | 23 | 24 | | 26 | 27 | | 29 | 30 |
| | 32 | 33 | | 35 | 36 | | 38 | 39 | |
| 41 | 42 | | 44 | 45 | | 47 | 48 | | 50 |
| 51 | | 53 | 54 | | 56 | 57 | | 59 | 60 |
| | 62 | 63 | | 65 | 66 | | 68 | 69 | |
| 71 | 72 | | 74 | 75 | | 77 | 78 | | 80 |
| 81 | | 83 | 84 | | 86 | 87 | | 89 | 90 |
| | 92 | 93 | | 95 | 96 | | 98 | 99 | |

3. krok

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | | 5 | 6 | | 8 | 9 | |
| 11 | | | 14 | 15 | | | 18 | | 20 |
| 21 | | 23 | 24 | | 26 | | | 29 | 30 |
| | | 33 | | 35 | 36 | | 38 | 39 | |
| 41 | | | 44 | 45 | | | 48 | | 50 |
| 51 | | 53 | 54 | | 56 | | | 59 | 60 |
| | | 63 | | 65 | 66 | | 68 | 69 | |
| 71 | | | 74 | 75 | | | 78 | | 80 |
| 81 | | 83 | 84 | | 86 | | | 89 | 90 |
| | | 93 | | 95 | 96 | | 98 | 99 | |

4. – 6. krok

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | | 5 | 6 | | 8 | 9 | |
| 11 | | | 14 | 15 | | | 18 | | 20 |
| 21 | | 23 | | | 26 | | | 29 | 30 |
| | | 33 | | 35 | 36 | | | 39 | |
| 41 | | | 44 | | | | 48 | | 50 |
| 51 | | 53 | 54 | | 56 | | | | |
| | | 63 | | 65 | | | 68 | 69 | |
| | | | 74 | 75 | | | 78 | | |
| 81 | | 83 | | | 86 | | | 89 | 90 |
| | | | | 95 | 96 | | 98 | 99 | |

7. krok

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | | 5 | 6 | | 8 | 9 | |
| 11 | | | 14 | 15 | | | 18 | | 20 |
| 21 | | 23 | | | 26 | | | 29 | 30 |
| | | 33 | | 35 | 36 | | | 39 | |
| 41 | | | 44 | | | | 48 | | 50 |
| 51 | | 53 | 54 | | 56 | | | | 60 |
| | | 63 | | 65 | | | 68 | 69 | |
| | | | 74 | 75 | | | 78 | | |
| 81 | | 83 | | | 86 | | | 89 | 90 |
| | | | | 95 | 96 | | 98 | 99 | |

Seznam prvočísel $\leq 201$

| | | | | |
|---|---|---|---|---|
| 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 |

Obrázek 3.2: Sundaramovo síto.

## 3.3 Základní test

Prvním typickým testem pro ověření prvočíselnosti je základní test. Funguje na principu, kde námi zadané číslo dělíme všemi čísly, které by mohly být jeho potenciálním dělitelem. Pokud žádný z možných dělitelů dělitelem čísla není, zadané číslo je prvočíslem. Tento způsob ověřování není příliš efektivní pro velká čísla, neboť se jedná o velmi časově náročný způsob testování prvočíselnosti. Využijeme-li ho však pro malá čísla, pak je považován za jeden z nejrychlejších testů, poněvadž pro hledání možných dělitelů čísla $n \in \mathbb{N}$ stačí projít množinu $\{2, 3, \ldots, \sqrt{n}\}$.

### 3.3.1 Princip

Prinicip základního testu spočívá v odhalení alespoň jednoho netriviálního dělitele čísla $n$. Pokud se nám tak podaří, nalezli jsme složené číslo. Pokud nikoli a číslo $n$ má pouze dělitele triviální, jedná se o prvočíslo. Alespoň jednoho případného netriviálního dělitele daného čísla musíme hledat v množině $\{2, 3, \ldots, \sqrt{n}\}$. Dolní hranicí je číslo dva, nikoli jedna, neboť ta je dělitelem triviálním. Horní hranicí je $\sqrt{n}$, nikoli $n$. Není nutné abychom při užívání základního testu prvočíselnosti testovali možné dělitele až do čísla $n$, neboť právě hranice $\sqrt{n}$ *láme* dělitele na menší a větší z dvojice. Tím, že k označení čísla za složené nám stačí odhalit pouze jednoho netriviálního dělitele, stačí nám, když nalezneme právě menšího dělitele z dané dvojice, který je vždy menší než $\sqrt{n}$, a proto možné dělitele hledáme pouze do této hodnoty. Navíc nemusíme procházet všech $(\sqrt{n} - 1)$ čísel, protože nám k usnadnění práce pomohou určitá pravidla. Víme například, že pokud je námi testované číslo sudé, pak nám k tomuto zjištění dopomůže sudé číslo 2, ostatními sudými čísly z množiny $\{2, 3, \ldots, \sqrt{n}\}$ dál zkoušet dělit nemusíme. Pokud je námi testované číslo dělitelné třemi, odhalí nám to číslo 3 a násobky tohoto čísla ze zmíněné množiny tak opět již zkoušet dělit dál nemusíme. To samé platí i pro čísla $5, 7, 11, 13$ atd. Postupně zjišťujeme, že možní netriviální dělitelé námi testovaného čísla $n$ jsou jen a pouze mezi prvočísly nacházející se v množině $\{2, 3, \ldots, \sqrt{n}\}$. K ověření prvočíselnosti daného čísla $n$ tak stačí dělit pouze prvočísly až do čísla $\sqrt{n}$. V následující sekci představíme obecný algoritmus.

**Poznámka 8.** *Z výše popsaného principu je zřejmé, že základní test funguje na velmi podobném principu jako Eratosthenovo síto. Představme si, že u základního testu máme taktéž pomyslný seznam čísel. Ta zkoušíme dělit postupně všemi prvočísly* $2, 3, 5, 7, \ldots$ *a ta, která jsou dělitelná těmito čísly (kromě sebe samých) ze seznamu odstraňujeme, protože se jedná o složená čísla. U Eratosthenova síta je tomu přesně naopak. Zde bereme postupně čísla* $2, 3, 5, 7, \ldots$ *a jejich násobky ze seznamu odstraňujeme. V obou dvou seznamech nám zůstanou pouze prvočísla. U Eratosthenova síta jsme dosáhli cíle, nalezli jsme všechna prvočísla menší nebo rovno než je číslo* $n$*. U základního testu musíme těmito prvočísly (až do čísla* $\sqrt{n}$*) zkoušet dělit číslo* $n$*, abychom ověřili jeho prvočíselnost.*

### 3.3.2 Algoritmus

Algoritmus 3.3 ukazuje možnou implementaci základního testu prvočíselnosti v programovacím jazyce Matlab.

**Algoritmus 3.3:** Algoritmus základního testu prvočíselnoti v programovacím jazyce Matlab. V algoritmu jsou některé části zjednodušeny.

```
vstup  : c ∈ ℕ
vystup: true × false
v(c) = true;
if c == 1 then
|  v(c) = false;
end
for P = 2, 3, 5, ..., √c do
|  if mod(c, P) == 0 then
|  |  v(c) = false;
|  end
end
v(c)
```

## 3.4 Moderní testy

V této sekci, kterou jsme nazvali Moderní testy, představíme podstatu sedmi, resp. osmi testů moderní doby, které jsou využívány pro testování prvočíselnosti převážně velkých čísel, pro která jsou tyto testy mnohem efektivnější než například základní test popsaný výše. Důkazy platnosti těchto testů a bližší informace o nich lze dohledat v uvedených zdrojích u každého jednotlivého testu.

### 3.4.1 Lucasův–Lehmerův test

Lucasův–Lehmerův test je testem deterministickým, tzn. dokáže odhalit se stoprocentní jistotou, že testované číslo je prvočíslem či číslem složeným. Vychází z malé Fermatovy věty (MFV), o které jsme psali více v sekci 2.4. Malá Fermatova věta nám také sama o sobě může pomoci při testování prvočíselnosti, pakliže totiž nalezneme číslo $a \in \mathbb{N}$ nesoudělné s číslem $p$, pro které MFV neplatí, pak $p$ prvočíslem určitě není. Číslo $p$ je tudíž složeným číslem a zmíněné číslo $a$ je označováno jako jeho *svědek*. Právě popsaný test, nazývaný jako Fermatův, však odhalit prvočísla nedokáže, poněvadž malou Fermatovu větu splňují i některá složená čísla, byť jich je velmi málo, viz [9, str. 179]. Tato složená čísla se označují jako Lucasova pseudoprvočísla a díky nim tak lze Fermatův test označit *pouze* za pravděpodobnostní test prvočíselnosti. Z tohoto důvodu se číslům $p$, která splňují malou Fermatovu větu, říká *pravděpodobná prvočísla*.

Na Fermatův test navázal později právě Édouard Lucas, příznivec oblasti teorie čísel a její historie, jehož cílem bylo zkonstruovat takový test, který bude

testem deterministickým. V roce 1876 tak přidal ještě jednu podmínku, kterou spolu s malou Fermatovou větou splňují pouze prvočísla. Celý Lucasův–Lehmerův test zní následovně. Požadujeme ověřit prvočíselnost daného čísla $p$. Jestliže nalezneme alespoň jedno číslo $a$, které splňuje obě dvě podmínky

$$a^{p-1} \equiv 1 \pmod{p} \quad \wedge \quad a^{\ell} \not\equiv 1 \pmod{p} \quad \text{pro} \quad \ell = 1 \text{ až } (p-2),$$

kde $a, p, \ell \in \mathbb{N}$, pak $p$ je prvočíslem. Tento test však byl posléze ještě upravován. O 15 let později sám Lucas tento test zkrátil a následně jej vylepšili matematici Derrick Henry Lehmer a Maurice Kraitchik a zní takto. Předpokládejme, že požadujeme ověřit prvočíselnost čísla $p > 1, p \in \mathbb{N}$. Pokud pro každý prvočíselný dělitel $q \in \mathbb{N}$ čísla $(p-1)$ nalezneme alespoň jedno číslo $a \in \mathbb{Z}$, pro které platí, že

$$a^{p-1} \equiv 1 \pmod{p} \quad \wedge \quad a^{(n-1)/q} \not\equiv 1 \pmod{p},$$

pak $p$ je prvočíslem, viz [9, str. 146].

Dnes často ale pod tímto názvem nalezneme test, který je určen speciálně pro Mersennova čísla, kterým se více věnujeme v sekci 4.1. V této práci jej budeme označovat pro odlišení jako *Lucasův–Lehmerův test pro Mersennova čísla*. Za jeho autory se považují dva matematici, prvním z nich je autor předchozího testu Édouard Lucas, díky němuž počátky tohoto testu sahají do roku 1856, tedy o dvacet let dříve než přišel s výše zmíněným testem. Druhým autorem je pak D. H. Lehmer, který navázal na výsledky svého kolegy ve 30. letech 20. století a jenž tento test zdokonalil. Je založen na testování prvočíselnosti Mersennových čísel a tím dochází k případnému odhalení Mersennových prvočísel. Spočívá v tom, že máme posloupnost čísel, pro kterou platí, že

$$S(1) = 4,$$
$$S(n+1) = S(n)^2 - 2, \text{kde } n \in \mathbb{N}.$$

Pokud je Mersennovo číslo $M_{2n+1}$ prvočíslem, pak musí splňovat podmínku, že je dělitelem členu posloupnosti $S(2n)$. Lucasův–Lehmerův test pro Mersennova čísla dokáže odhalit Mersennova prvočísla v řádech několika milionů cifer, viz [7, str. 14], a pro tato čísla se jedná o velmi praktický a účinný test. Názorný příklad pro číslo $M_{13} = 8191$ lze nalézt v knize [9, str. 158-159].

### 3.4.2 Pocklingtonův test

Prvním autorem Pocklingtonova testu je matematik, fyzik a člen královské společnosti Henry Cabourn Pocklington, druhým pak Derrick Henry Lehmer, který na Pocklingtona navázal v roce 1927. Je velmi podobný Lucasovu–Lehmerovu testu s tím rozdílem, že u něj není třeba znát kompletní prvočíselný rozklad čísla $(p-1)$, ale stačí znát pouze jeho část. Předpokládejme, že číslo $(p-1)$, kde $p > 1, p \in \mathbb{N}$ můžeme rozložit na součin dvou nesoudělných čísel $m, n$, kde $m > n$. Jestliže pro každý prvočíselný dělitel $q \in \mathbb{N}$ čísla $m$ existuje číslo $a > 1, a \in \mathbb{N}$, které splňuje kongruenci

$$a^{p-1} \equiv 1 \pmod{p}$$

a čísla $a^{(n-1)/q} - 1$ a $n$ jsou nesoudělná, pak $p$ je prvočíslem, viz [9, str. 175]. Pocklingtonův test je testem deterministickým.

### 3.4.3 Pepinův test

Pepinův test slouží ke stejnému účelu jako Lucasův–Lehmerův test pro Mersennova čísla, s tím rozdílem, že tento test je založený na testování Fermatových čísel a tím dochází k odhalování Fermatových prvočísel, o kterých pojednává více sekce 4.2. Test pochází z roku 1877 a za autora bývá označován jezuitský kněz Jean Pépin. Díky němu dostáváme, že Fermatovo číslo $F_n$ je prvočíslem, resp. Fermatovým prvočíslem jen a pouze tehdy, pokud

$$F(n) \mid (3^{(F(n)-1)/2} + 1).$$

Ve starších verzích lze tuto podmínku vidět s číslem 5 namísto 3, viz např. [9, str. 169]. Fermatův test byl mimo jiné dvakrát užitečný k odhalení složených Fermatových čísel. Prvně v roce 1905, kdy s pomocí něho James Caddall Morehead [17] a Alfred E. Western [29] nezávisle na sobě odhalili, že Fermatovo číslo $F_7$ je složeným číslem. A následně o čtyři roky později, v roce 1909, kdy ke stejnému závěru došli Morehead a Western, tentokrát již společně pro Fermatovo číslo $F_8$ [18].

### 3.4.4 Solovayův–Strassenův test

Autory pravděpodobnostního Solovayova–Strassenova testu z roku 1977 jsou Robert Solovay a Volker Strassen. V dnešní době je označován jako předchůdce tzv. Baillieho–PSW (Pomeranceho–Selfridgova–Wagstaffova) testu a Millerova–Rabinova testu, na který se zaměříme vzápětí. Solovayův–Strassenův test vychází z Eulerova důkazu o platnosti následující kongruence

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}, \tag{3.2}$$

kde $a$ je kladné celé číslo, $p$ je liché prvočíslo a obě tato čísla musí být nesoudělná. V Solovayově–Strassenově testu je $p$ námi testované číslo, které musí být z množiny lichých přirozených čísel a číslo $a$ musí splňovat stejné podmínky jako platily v Eulerově důkazu, viz [38].

Abychom mohli označit $p$ za *pravděpodobné prvočíslo*, kongruenci (3.2) musí splňovat všechna $a$ z intervalu, který z podmínek vyplývá, tedy z intervalu $0 < a < p$. Z tohoto tvrzení logicky plyne, že pokud se nám podaří najít alespoň jedno číslo $a$ ležící v daném intervalu $0 < a < p$, které kongruenci (3.2) nesplňuje, pak testované číslo $p$ je složeným číslem. Stejně jako u Lucasova–Lehmerova testu, i zde je číslo $a$, které kongruenci nesplňuje, označováno jako *svědek* složeného čísla $p$. Jak jsme již zmínili, Solovayův–Strassenův test je pravděpodobnostním testem, kongruenci (3.2) totiž splňují i některá složená čísla, jimiž jsou tzv. Euler-Jakobiho pseudoprvočísla. Konkrétní příklad s číslem 221 lze zhlédnout na webové stránce [38].

### 3.4.5 Millerův–Rabinův test

O tento test prvočíselnosti z roku 1980 se zasloužili matematici Gary Miller a Michael Rabin. Jeho vývoj začal v roce 1976, kdy se objevila první verze tohoto testu od Millera, která byla deterministická. Mohlo by se zdát, že tato verze byla

konečná a nebylo třeba dalších úprav. Problém však byl a je v tom, že tato verze stojí na pravdivosti Riemannovy hypotézy, o které pojednává celá kapitola 5, viz [35]. V této kapitole 5 se lze dozvědět mimo jiné i to, že Riemannova hypotéza dodnes zůstává nedokázána, a proto tato verze testu nemohla být a není nikterak využívána, ač by jistě patřila k jedné z nejpoužívanějších metod pro ověřování prvočíselnosti. Kolega Millera Rabin se rozhodl tuto verzi upravit a roku 1980 byla představena druhá verze tohoto testu, která je však verzí pravděpodobnostní a její podoba je následující. Nechť pro každé celé číslo $a$ z intervalu $0 < a < p$ a pro testované liché celé číslo $p > 2$ platí jedna z kongruencí

$$a^d \equiv 1 \pmod{p} \quad \vee \quad a^{2^r \cdot d} \equiv -1 \pmod{p} \quad \text{pro nějaké } 0 \leq r \leq s-1, \tag{3.3}$$

kde $2^s d + 1 = p$, $s$ je kladné celé číslo a $d$ je kladné liché celé číslo, pak $p$ je *pravděpodobné prvočíslo*.

Stejně jako u Fermatova a Solovayova–Strassenova testu i zde platí, že pokud se nám podaří nalézt číslo $a$ z intervalu $0 < a < p$, pro které platí

$$a^d \not\equiv 1 \pmod{p} \quad \wedge \quad a^{2^r \cdot d} \not\equiv -1 \pmod{p} \qquad \text{pro všechna } 0 \leq r \leq s-1,$$

pak $p$ není prvočíslem a číslo $a$ je jeho *svědkem*. Složená čísla, která vyhovují podmínce (3.3) i přesto, že nejsou prvočísly, se nazývají tzv. silná pseudoprvočísla. Detailnější informace o tomto testu i s konkrétním příkladem nebo také s popsanou deterministickou verzí tohoto testu z roku 1976 lze nalézt na stránce [35].

### 3.4.6 Agrawalův–Kayalův–Saxenův test

Agrawalův–Kayalův–Saxenův test je deterministickým testem prvočíselnosti z roku 2002, jehož autory jsou Indové Manindra Agrawal a jeho studenti Neeraj Kayal a Nitin Saxena. Častěji uváděný název tohoto testu je AKS test, jenž je zkratkou počátečních písmen příjmení autorů. Veřejnost byla při prvním zveřejnění tohoto testu v článku [1] překvapena jeho jednoduchostí a stručností, viz [9, str. 8]. Agrawalův–Kayalův–Saxenův test vychází z malé Fermatovy věty a jeho princip lze nalézt na webové stránce [11] či v knize [3, str. 239–241].

**Komentář 2.** *Číslu, které tyto uvedené moderní pravděpodobnostní testy označí za prvočíslo, se říká pravděpodobné prvočíslo. Nelze o něm tak se stoprocentní jistotou říci, že je opravdu prvočíslem, poněvadž tyto testy prvočíselnosti odhalí kromě prvočísel i v některých případech čísla složená, která jsou obecně nazývána pseudoprvočísly. Abychom si byli skutečně jisti, že se jedná o prvočíslo, museli bychom užít test základní, o kterém jsme psali v sekci 3.3 či testy deterministické, ke kterým patří například Lucasův–Lehmerův test, Pocklingtonův test či AKS test.*

V dnešní době existuje mnoho dalších testů prvočíselnosti, jmenujme například pravděpodobnostní Baillieho–PSW test, test pomocí eliptických křivek či Frobeniův test.

# 4 Speciální typy prvočísel

Některá prvočísla vykazují stejné vlastnosti, ať už tím, že byla objevena podle určitého vzorce, nebo tím, že se jejich stejné vlastnosti objevily až posléze. Nic to nemění na tom, že prvočísla se stejnými vlastnostmi lze zařadit do skupin, jež jsou často nazývány podle svých objevitelů, jmenujme např. Mersennova prvočísla či Fermatova prvočísla, která jsou mimo jiné popsána právě v této kapitole. Některé speciální typy prvočísel jsou pojmenovány podle ustálených slov a slovních spojení, příklad takových jsou palindromická prvočísla, bezpečná prvočísla či šťastná prvočísla. Speciálních typů prvočísel existuje veliké množství, jejichž menší přehled lze najít v této kapitole a v závěrečné sekci této kapitoly, rozsáhlejší seznam pak můžeme vidět např. na webové stránce [34], kde na mnoho z nich existuje odkaz směřující na databázi celočíselných posloupností OEIS, obsahující bližší informace o těchto typech prvočísel.

## 4.1 Mersennova čísla a prvočísla

Mersennova čísla, resp. Mersennova prvočísla jsou pojmenována po francouzském matematikovi a mnichovi Marinu Mersennovi. Jako Mersennovo číslo se označuje číslo tvaru $M_n = 2^n - 1$, kde $n \in \mathbb{N}$. Pokud je výraz $2^n - 1$ sám o sobě prvočíslem, pak je $M_n$ označováno jako Mersennovo prvočíslo. Příklady Mersennových prvočísel, resp. Mersennových čísel, jsou např. $3, 7, 31, \ldots$ a příklady Mersennových čísel, která nejsou Mersennovými prvočísly, jsou např. $15, 63, 255, \ldots$ Další příklady lze vidět v tabulce 4.1. Platí, že všechna doposud známá největší prvočísla jsou zároveň i Mersennovými prvočísly. Důvod je prostý, pro testování Mersennových čísel a tím odhalování Mersennových prvočísel využíváme Lucasův–Lehmerův test pro Mersennova čísla, popsaný v sekci 3.4.1. Ten dokáže odhalit velmi velká Mersennova prvočísla, jež jsou tím pádem zároveň i prvočísly samy o sobě. K Mersennovým prvočíslům se váže následující věta.

**Věta 4.** *Pokud je číslo $2^n - 1$ prvočíslem, pak je $n$ prvočíslem.*

*Důkaz.* Tuto větu dokážeme nepřímým důkazem, tedy využijeme obměněné implikace. Označíme číslo $n$ jako číslo složené $n = a \cdot b$, kde $n > a \geq b > 1$ a $a, b, n \in \mathbb{N}$. Výraz $2^n - 1$ přepíšeme na výraz $2^{(a \cdot b)} - 1$ a následně tento dvojčlen rozložíme na součin následujícím způsobem

$$2^{(a \cdot b)} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{(b-1)} + (2^a)^{(b-2)} + (2^a)^{(b-3)} + \cdots + (2^a) + 1).$$

Vidíme, že číslo $(2^n - 1)$, kde $n \notin \mathbb{P}$, lze tedy rozložit na součin dvou čísel, která jsou různá od jedničky a od čísla sebe samého, tedy $(2^n - 1)$. Z toho vyplývá, že toto číslo je určitě číslem složeným. Dokázali jsme obměněnou implikaci, ze které plyne pravdivost věty 4. Pakliže bychom zkoumaly, zda platí tato věta i v opačném smyslu, tedy když je $n$ prvočíslem, pak je číslo $(2^n - 1)$ prvočíslem, dostaneme negativní odpověď. Pro vybrané prvočíslo $n = 11$ totiž platí, že číslo $M_{11}$ je složené, $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ a tím pádem obráceně věta 4 v obecném případě neplatí. □

Tabulka 4.1: Seznam vybraných známých Mersennových čísel.

| Pořadí $M_p, p \in \mathbb{P}$ | $2^p - 1$ | Počet cifer | Mersennovo prvočíslo |
|---|---|---|---|
| $M_2$ | 3 | 1 | ano |
| $M_3$ | 7 | 1 | ano |
| $M_5$ | 31 | 2 | ano |
| $M_7$ | 127 | 3 | ano |
| $M_{11}$ | 2047 | 4 | ne |
| $M_{13}$ | 8191 | 4 | ano |
| $M_{17}$ | 131 071 | 6 | ano |
| $M_{19}$ | 524 287 | 6 | ano |
| ... | ... | ... | ... |
| $M_{67}$ | $2^{67} - 1$ | 21 | ne |
| ... | ... | ... | ... |
| $M_{89}$ | $2^{89} - 1$ | 27 | ano |
| ... | ... | ... | ... |
| $M_{199}$ | $2^{199} - 1$ | 60 | ne |
| ... | ... | ... | ... |
| $M_{2281}$ | $2^{2281} - 1$ | 687 | ano |
| ... | ... | ... | ... |
| $M_{11\,213}$ | $2^{11\,213} - 1$ | 3376 | ano |
| ... | ... | ... | ... |
| $M_{756\,839}$ | $2^{756\,839} - 1$ | 227 832 | ano |
| ... | ... | ... | ... |
| $M_{3\,021\,377}$ | $2^{3\,021\,377} - 1$ | 909 526 | ano |
| ... | ... | ... | ... |
| $M_{43\,112\,609}$ | $2^{43\,112\,609} - 1$ | 12 978 189 | ano |
| $M_{57\,885\,161}$ | $2^{57\,885\,161} - 1$ | 17 425 170 | ano |
| $M_{74\,207\,281}$ | $2^{74\,207\,281} - 1$ | 22 338 618 | ano |
| $M_{77\,232\,917}$ | $2^{77\,232\,917} - 1$ | 23 249 425 | ano |
| $M_{82\,589\,933}$ | $2^{82\,589\,933} - 1$ | 24 862 048 | ano |

### 4.1.1 GIMPS

George Woltman v roce 1995 shromáždil všechna, do té doby známá, Mersennova prvočísla a o rok později tento seznam umístil na webovou stránku. Kromě seznamu se zde nacházel i program, který odhaloval, zda jsou testovaná čísla Mersennovými prvočísly či nikoli. Web přilákal nejednoho odborníka a nadšence do matematiky a díky Woltmanovi tak vznikl projekt nazývaný GIMPS, neboli *The Great Internet Mersenne Prime Search*. Jak z anglického názvu vyplývá, cílem GIMPS je hledat a objevovat nová Mersennova prvočísla. Abychom se mohli stát součástí tohoto projektu, je zapotřebí splnění dvou podmínek, tou první je stáhnutí vhodného software z webové stránky GIMPS, tou druhou pak stvrzení podmínky o rozdělení případné výhry při nalezení Mersennova prvočísla s daným minimálním počtem cifer. Tuto cenu vyplácí *Electronic Frontier Foundation*, jež byla založena Johnem Gilmorem, a která odměnila již například Nayana Hajratwala v roce 2006 za objevení prvního Mersennova prvočísla, které má více než milion cifer. Dalším odměněným byl Hans-Michael Elvenich, který jako první objevil Mersennovo prvočíslo, jež má více jak 10 000 000 cifer. Další odměny čekají na ty, kteří objeví Mersennovo prvočíslo s více jak 100 000 000, resp. 1 000 000 000 ciframi, viz [9].

Projekt je velmi úspěšný, od jeho založení až do dnešního dne se mu podařilo objevit 17 největších *známých* Mersennových prvočísel. To poslední největší *známé* 51. Mersennovo prvočíslo bylo objeveno projektem GIMPS, resp. jedním z jeho přispěvatelů Patrickem Larochem, v prosinci roku 2018, viz [30]. Má 24 862 048 číslic a jedná se o doposud největší známé prvočíslo.

### 4.1.2 Mersennova prvočísla a dokonalá čísla

S Mersennovými prvočísly mají velmi úzkou spojitost dokonalá čísla. To jsou čísla, u kterých součet jejich dělitelů (kromě sebe samých) je roven právě oněm číslům. Mezi ně se řadí např. $6, 28, 496, 8128, \ldots$ Euklides zjistil, že číslo ve tvaru

$$2^{n-1}(2^n - 1)$$

je dokonalé, jestliže $(2^n - 1)$ je prvočíslem. Euler Euklidovo zjištění později zpřesnil tím, že dokázal, že toto tvrzení platí pouze pro sudá dokonalá čísla, viz [4, str. 71]. Jeden z nejznámějších nevyřešených problémů v teorii čísel je existence lichých dokonalých čísel. Dodnes se žádné takové číslo nenalezlo. Ve stejném zdroji se pak lze dočíst podmínek, která by případná lichá dokonalá čísla musela splňovat. Tím, že do dnešního dne známe pouze sudá dokonalá čísla, jejichž existence je závislá na Mersennových prvočíslech, můžeme prohlásit, že *známých* dokonalých čísel existuje 51, stejný počet jako *známých* Mersennových prvočísel.

**Otevřený problém 2.** *Otázkou taktéž zůstává, zda je Mersennových prvočísel konečně či nekonečně mnoho. Většina matematiků a odborníků se přiklání k verzi, že jich je nekonečně mnoho, důkaz však dodnes neexistuje.*

## 4.2 Fermatova čísla a prvočísla

Fermatova čísla, nesoucí název po francouzském matematikovi Pierru de Fermatovi, jsou čísla ve tvaru $F_n = 2^{2^n} + 1$, kde $n \in \mathbb{N}_0$. Pokud je navíc výraz $2^{2^n} + 1$ prvočíslem, pak se $F_n$ označuje jako Fermatovo prvočíslo. Dodnes je známo pouze pět Fermatových prvočísel a těmi jsou čísla $3, 5, 17, 257$ a $65537$. Fermat se domníval, že všechna Fermatova čísla jsou zároveň i Fermatovými prvočísly. To bylo však roku 1732 Eulerem vyvráceno, protože dokázal, že všichni dělitelé Fermatových čísel $F_n$ pro $n \geq 2$ jsou ve tvaru $k \cdot 2^{n+2} + 1$, kde $k \in \mathbb{N}_0$, viz [7, str. 41]. Dělitelé šestého Fermatova čísla $F_5$ jsou tudíž ve tvaru $128 \cdot k + 1$, kde $k \in \mathbb{N}_{\not\vdash}$. Pakliže za $k$ dosadíme 5, dostáváme číslo 641, jež je dělitelem Fermatova čísla $F_5$ a toto číslo tak jistě Fermatovým prvočíslem není.

Eulerův důkaz posloužil k závěru, že Fermatova čísla $F_5$ až $F_{32}$ jsou čísla složená. U Fermatova čísla $F_{33}$ dodnes nemáme prostředky k jeho označení za Fermatovo prvočíslo či číslo složené, viz [7, str. 41]. To stejné platí například u čísel $F_{34}$, $F_{35}$, $F_{40}$, $F_{41}$, $F_{44}$ atd., viz [15]. Z téže stránky se dozvídáme, že do dnešního dne víme o 314 Fermatových číslech, která jsou složená, byť u většiny z nich neznáme jejich prvočíselný rozklad. Ten známe pouze u prvních dvanácti čísel, tedy do čísla $F_{11}$ včetně. Přehled Fermatových čísel do čísla $F_{33}$ lze vidět v tabulce 4.2 a podrobnější přehled o nich a o dalších Fermatových číslech, o roku jejich objevení a samotných objevitelech, o doposud známých dělitelech čísel, o jejich rozkladu atd. lze nalézt na webové stránce [15], vedené členem projektu Fermat Prime Search. K určení prvočíselnosti Fermatových čísel se nejčastěji užívá Pepinův test, který je znám od roku 1877 a jenž je popsán v sekci 3.4.3.

**Otevřený problém 3.** *Otázkou zůstává, zda existují ještě nějaká další Fermatova prvočísla nebo také to, zda jsou všechna Fermatova čísla squarefree, tedy že jejich prvočíselný rozklad neobsahuje žádné násobky prvočísel.*

### 4.2.1 Fermat Prime Search

Fermat Prime Search je projekt principem velice podobný projektu GIMPS, o kterém jsme psali v sekci 4.1.1. Sdružuje zájemce a dobrovolníky, jejichž hlavním cílem je hledat dělitele Fermatových čísel. Jedině tak dojde k vyvrácení případných Fermatových prvočísel. Díky tomuto projektu, jehož hlavním organizátorem je Phil Carmody, bylo za tři století nalezeno více než 350 dělitelů. Velmi podrobné informace o dělitelích, o jejich roku objevení, objevitelích, počtu cifer atd. vede Wilfrid Keller na webové stránce [15].

**Poznámka 9.** *Informace na stránce [15] jsou velmi aktuální, například poslední je ze* 3. *března roku 2021, kdy byl* Garym Gostinem *nalezen dělitel Fermatova čísla* $F_{25\,599}$*, které je tak číslem složeným.*

Tabulka 4.2: Orientační seznam Fermatových čísel do čísla $F_{33}$. Hvězdička (*) značí, že počet vlastních dělitelů není konečný. Žádní dělitelé čísel $F_{20}$ a $F_{24}$ doposud nejsou známy, nicméně je dokázáno, že se jedná o složená čísla, viz [31], resp. [14]. Poslední cifra každého Fermatova čísla, kromě prvních dvou, je 7, viz [7, str. 41]. U neoznačených Fermatových čísel pocházejí všechny údaje ze stránky [15]. Údaje s otazníky (?) se nám dohledat nepodařily.

| Pořadí $F_n, n \in \mathbb{N}_0$ | $2^{2^n}+1$ | Počet cifer | Počet vl. dělitelů |
|---|---|---|---|
| $F_0$ | 3 | 1 | 0 |
| $F_1$ | 5 | 1 | 0 |
| $F_2$ | 17 | 2 | 0 |
| $F_3$ | 257 | 3 | 0 |
| $F_4$ | 65 537 | 5 | 0 |
| $F_5$ | 4 294 967 297 | 10 | 2 |
| $F_6$ | 18 446 744 073 709 551 617 | 20 | 2 |
| $F_7$ | | 39 | 2 |
| $F_8$ | | 78 | 2 |
| $F_9$ | | 155 | 3 |
| $F_{10}$ | | 309 | 4 |
| $F_{11}$ | | 617 | 5 |
| $F_{12}$ | | 1133 | 6* |
| $F_{13}$ | | 2391 | 4* |
| $F_{14}$ | | 4880 | 1* |
| $F_{15}$ | | 9808 | 3* |
| $F_{16}$ | | 19 694 | 2* |
| $F_{17}$ | | 39 395 | 2* |
| $F_{18}$ | | 78 884 | 2* |
| $F_{19}$ | | 157 770 | 3* |
| $F_{20}$ | | 315 653 | 0* |
| $F_{21}$ | | 631 294 | 1* |
| $F_{22}$ | | 1 262 577 | 1* |
| $F_{23}$ | | 2 525 215 | 1* |
| $F_{24}$ | | 5 050 446 | 0* |
| $F_{25}$ [16] | | 10 100 891 | 3* |
| $F_{26}$ [16] | | 20 201 782 | 1* |
| $F_{27}$ [16] | | 40 403 563 | 2* |
| $F_{28}$ [16] | | 80 807 125 | 1* |
| $F_{29}$ [16] | | 161 614 249 | 1* |
| $F_{30}$ | | ? | 2* |
| $F_{31}$ | | ? | 1* |
| $F_{32}$ | | ? | 1* |
| $F_{33}$ [14] | | 2 585 827 973 | ? |

### 4.2.2 Fermatova prvočísla a konstruovatelné mnohoúhelníky

S Fermatovými čísly souvisí konstrukce pravidelných mnohoúhelníků. Těmi se zabýval mimo jiné také slavný matematik Johann Carl Friedrich Gauss, který ve své knize Disquisitiones Arithmeticae (str. 472) uvedl přehled 38 euklidovsky zkonstruovatelných mnohoúhelníků do hodnoty 300. Euklidovsky zkonstruovatelné $n$-úhelníky jsou takové mnohoúhelníky, které lze sestrojit pomocí kružítka a pravítka. Tomuto závěru však předcházelo Gaussovo zjištění před pěti lety od vydání této publikace, kdy ukázal, že jestliže chceme euklidovsky zkonstruovat $n$-úhelníky, pak číslo $n$ musí být součin mocniny čísla dvě a nejméně jednoho (popř. více, ale různých) Fermatova prvočísla, viz [9, str. 110]. Takto zkonstruovatelných $n$-úhelníků je nekonečně mnoho, do dnešní doby je však známo pouze 31 mnohoúhelníků s lichými počty stran. Ty jsou na obrázku 4.1 znázorněny červeně.

## 4.3 Prvočísla ve tvaru $an + b$

V úvodu této sekce zmíníme větu, která je dnes známa jako Dirichletova věta a jež se váže k prvočíslům, které mají tvar $an + b$.

**Věta 5** (Dirichletova věta)**.** *Budeme-li předpokládat, že čísla $a, b \in \mathbb{N}$ jsou čísla nesoudělná a platí tedy, že $gcd(a, b) = 1$, pak lze dokázat, že existuje nekonečně mnoho prvočísel ve tvaru $an + b$.*

Důkaz této věty nebudeme zde uvádět z důvodu obtížnosti, ale ke zhlédnutí je v knize [3, str. 112–131]. Speciálními příklady těchto prvočísel jsou tzv. *pythagorejská prvočísla* (*Pythagorean primes*), jež jsou ve tvaru $4n + 1$ či *Gaussova prvočísla* (*Gaussian primes*) ve tvaru $4n + 3$, u kterých jistě platí, že čísla $\{4, 1\}$, resp. $\{4, 3\}$ jsou čísla nesoudělná, viz definice 2. Pakliže vezmeme v potaz prvočísla ve tvaru $10n + 1, 10n + 3, 10n + 7$ a $10n + 9$, které podmínku Dirichletovy věty jistě taktéž splňují, pak z toho vyplývá, že existuje nekonečně mnoho prvočísel končících cifry $1, 3, 7$, resp. 9. Příklady prvočísel, jež jsou ve zmíněných tvarech $an + b$, kde $gcd(a, b) = 1$ lze vidět v tabulce 4.3, kde je vždy uvedeno prvních sedm takových prvočísel daného tvaru.

Tabulka 4.3: Prvočísla ve tvaru $an + b$, kde $gcd(a, b) = 1$.

| Tvar $an + b$ | Příklady prvočísel |
|---|---|
| $4n + 1$ | $5, 13, 17, 29, 37, 41, 53$ |
| $4n + 3$ | $3, 7, 11, 19, 23, 31, 43$ |
| $10n + 1$ | $11, 31, 41, 61, 71, 101, 131$ |
| $10n + 3$ | $3, 13, 23, 43, 53, 73, 83$ |
| $10n + 7$ | $7, 17, 37, 47, 67, 97, 107$ |
| $10n + 9$ | $19, 29, 59, 79, 89, 109, 139$ |

| Fermatova prvočísla | | | | | | | | | Mocniny čísla 2 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_0$ | | $F_1$ | | $F_2$ | | $F_3$ | | $F_4$ | | $\times 2^0$ | $\times 2^1$ | $\times 2^2$ | $\times 2^3$ | $\times 2^4$ | $\times 2^5$ | $\times 2^6$ | $\times 2^7$ | $\times 2^8$ | $\times 2^9$ |
| | | | | | | | | | = | [1] | [2] | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 |
| 3 | | | | | | | | | = | 3 | 6 | 12 | 24 | 48 | 96 | 192 | 384 | 768 | 1 536 |
| | | 5 | | | | | | | = | 5 | 10 | 20 | 40 | 80 | 160 | 320 | 640 | 1 280 | 2 560 |
| 3 | × | 5 | | | | | | | = | 15 | 30 | 60 | 120 | 240 | 480 | 960 | 1 920 | 3 840 | 7 680 |
| | | | | 17 | | | | | = | 17 | 34 | 68 | 136 | 272 | 544 | 1 088 | 2 176 | 4 352 | 8 704 |
| 3 | | | × | 17 | | | | | = | 51 | 102 | 204 | 408 | 816 | 1 632 | 3 264 | 6 528 | 13 056 | 26 112 |
| | | 5 | × | 17 | | | | | = | 85 | 170 | 340 | 680 | 1 360 | 2 720 | 5 440 | 10 880 | 21 760 | 43 520 |
| 3 | × | 5 | × | 17 | | | | | = | 255 | 510 | 1 020 | 2 040 | 4 080 | 8 160 | 16 320 | 32 640 | 65 280 | 130 560 |
| | | | | | | 257 | | | = | 257 | 514 | 1 028 | 2 056 | 4 112 | 8 224 | 16 448 | 32 896 | 65 792 | 131 584 |
| 3 | | | × | | | 257 | | | = | 771 | 1 542 | 3 084 | 6 168 | 12 336 | 24 672 | 49 344 | 98 688 | 197 376 | 394 752 |
| | | 5 | | | × | 257 | | | = | 1 285 | 2 570 | 5 140 | 10 280 | 20 560 | 41 120 | 82 240 | 164 480 | 328 960 | 657 920 |
| 3 | × | 5 | | | × | 257 | | | = | 3 855 | 7 710 | 15 420 | 30 840 | 61 680 | 123 360 | 246 720 | 493 440 | 986 880 | 1 973 760 |
| | | | | 17 | × | 257 | | | = | 4 369 | 8 738 | 17 476 | 34 952 | 69 904 | 139 808 | 279 616 | 559 232 | 1 118 464 | 2 236 928 |
| 3 | | | × | 17 | × | 257 | | | = | 13 107 | 26 214 | 52 428 | 104 856 | 209 712 | 419 424 | 838 848 | 1 677 696 | 3 355 392 | 6 710 784 |
| | | 5 | × | 17 | × | 257 | | | = | 21 845 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | × | 5 | × | 17 | × | 257 | | | = | 65 535 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | | | | | | | 65 537 | = | 65 537 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | | | | | | | × | 65 537 | = | 196 611 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | 5 | × | | | | × | 65 537 | = | 327 685 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | × | 5 | | | | | × | 65 537 | = | 983 055 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | | | 17 | | | × | 65 537 | = | 1 114 129 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | | | × | 17 | | | × | 65 537 | = | 3 342 387 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | 5 | × | 17 | | | × | 65 537 | = | 5 570 645 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | × | 5 | × | 17 | | | × | 65 537 | = | 16 711 935 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | | | | | 257 | × | 65 537 | = | 16 843 009 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | | | | | × | 257 | × | 65 537 | = | 50 529 027 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | 5 | | | × | 257 | × | 65 537 | = | 84 215 045 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | × | 5 | | | × | 257 | × | 65 537 | = | 252 645 135 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | | | 17 | × | 257 | × | 65 537 | = | 286 331 153 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | | | × | 17 | × | 257 | × | 65 537 | = | 858 993 459 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| | | 5 | × | 17 | × | 257 | × | 65 537 | = | 1 431 655 765 | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 3 | × | 5 | × | 17 | × | 257 | × | 65 537 | = | 4 294 967 295 | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Obrázek 4.1: Zkonstruovatelné mnohoúhelníky. Upravená grafika obrázku [13].

## 4.4 Příznivá čísla a prvočísla

Posledním typem, který si v této kapitole blíže představíme, jsou příznivá čísla, resp. příznivá prvočísla. Od zbylých třech výše zmíněných speciálních typů prvočísel se liší tím, že nemají předem určený tvar. Získáváme je pomocí síta, které připomíná Eratosthenovo síto. Jeho princip si nyní představíme. Začneme tím, že si napíšeme posloupnost lichých přirozených čísel, my uvedeme příklad pro čísla do hodnoty 60. Postup celého algoritmu pak vidíme na obrázku 4.2.


Obrázek 4.2: Princip hledání příznivých čísel. V seznamu postupně přibývají červeně označená čísla, která značí příznivá čísla. Mezi nimi pak lze najít příznivá prvočísla, která jsou zároveň příznivými čísly i prvočísly.

Po jeho úspěšném vyhotovení dostaneme tzv. příznivá čísla, v angličtině označována jako *Lucky numbers*. Z nich pak příznivá prvočísla jsou ta, která jsou příznivými čísly a zároveň jsou prvočísly (pozn. pokud není uvedeno přídavné jméno *příznivá*, nemáme na mysli příznivá prvočísla). Největší doposud známé příznivé číslo je 9 999 999 997, objevené Walterem Schneiderem v roce 2002, viz [24], [9, str. 147].

Stanislav Ulam a jeho kolegové s použitím výpočetního stroje došli k poměrně zajímavým výsledkům, které jsou shrnuty v knize [9, str. 147–148]. Zjistili například, že do čísla 48 000 se nachází 4523 příznivých čísel, ve stejném intervalu je potom 4947 prvočísel. Ačkoli příznivých čísel i prvočísel je nekonečně mnoho, příznivých čísel je na konečných intervalech přeci jenom o něco méně. Svědčí to o tom, že prvočísla jsou hustější, tedy v jakémkoliv konečném intervalu se vyskytují s větší frekvencí. Mimo to si také všimli různých podobností mezi příznivými čísly a prvočísly. Příkladem může být, že počet příznivých čísel ve tvaru $4n+1$ a $4n+3$ je přibližně stejně velký jako počet prvočísel ve stejném tvaru (jedná se o *pythagorejská prvočísla* a *Gaussova prvočísla*, viz sekce 4.3), nebo také, že mezery mezi po sobě jdoucími příznivými čísly se zhruba shodují s mezerami mezi po sobě jdoucími prvočísly, o kterých pojednává samostatná sekce 7.2. Taktéž zjistili, že počet příznivých dvojčat, tedy dvou příznivých čísel lišících se o dvě, je přibližně stejný jako počet prvočíselných dvojčat, ke kterým se váže tzv. Hypotéza prvočíselných dvojic, viz otevřený problém 1. Rozdíly v počtech příznivých čísel, resp. prvočísel a příznivých dvojčat, resp. prvočíselných dvojčat až do čísla $10^6$ lze zhlédnout v tabulce 4.4. Mezi další zajímavé výsledky jejich bádání patří zjištění, že každé sudé číslo až do čísla 100 000 je součtem dvou příznivých čísel a také to, že v intervalu 1 až 48 600 existuje 715 čísel, které jsou příznivými čísly a zároveň prvočísly, viz [9, str. 148].

Tabulka 4.4: Srovnání počtu příznivých a prvočíselných dvojčat. V obou případech se jedná o dvouprvkovou množinu po sobě jdoucích lichých čísel ve tvaru $(n, n+2)$. Rozdíl je však v tom, že pro příznivá dvojčata platí, že $(n, n+2)$ jsou lichá čísla nacházející se v seznamu příznivých čísel a prvočíselná dvojčata jsou dvě po sobě jdoucí prvočísla, tudíž $(n, n+2)$ jsou z množiny prvočísel $\mathbb{P}$.

| Horní mez | Počet příznivých čísel | Počet prvočísel | Počet příznivých dvojčat | Počet prvočíselných dvojčat |
|---|---|---|---|---|
| $10^1$ | 4 | 4 | 2 | 2 |
| $10^2$ | 23 | 25 | 7 | 8 |
| $10^3$ | 153 | 168 | 33 | 35 |
| $10^4$ | 1118 | 1229 | 178 | 205 |
| $10^5$ | 8772 | 9592 | 1162 | 1224 |
| $10^6$ | 71 918 | 78 498 | 7669 | 8169 |

**Otevřený problém 4.** *Víme, že příznivých čísel je nekonečně mnoho, otázkou však zůstává, zda je tomu tak i u příznivých prvočísel.*

## 4.5 Další typy prvočísel

Na začátku kapitoly 4 jsme uvedli, že typů prvočísel existuje veliké množství. Zde přikládáme list 4.5 náhodně vybraných typů s jejich názvy, stručným popisem, příklady a také odkazem na databázi celočíselných posloupností OEIS (*The On-Line Encyclopedia of Integer Sequences*) [25], kde je možno se o jednotlivých typech dozvědět více informací. Po kliknutí na příslušné identifikační číslo typu prvočísel se lze dostat na odpovídající webové stránky.

Tabulka 4.5: Příklady dalších typů prvočísel. Názvy těchto typů prvočísel jsme ponechali v anglickém jazyce, poněvadž překlady do českého jazyka u některých typů neexistují. Poznamenejme, že $p \in \mathbb{P}$.

| Název | Tvar prvočísel (popis) | Příklady prvočísel | Odkaz na OEIS |
|---|---|---|---|
| Carol primes | $4^n - 2^{(n+1)} - 1$, kde $n \geq 2, n \in \mathbb{N}$. | $7, 47, 223$ | A091516 |
| Emirps | Pr., u kterých po zapsání číslic v obráceném pořadí dostaneme opět prvočíslo. | $17, 31, 37$ | A006567 |
| Factorial primes | $n! - 1$, kde $n \geq 3, n \in \mathbb{N}$ nebo $n! + 1$, kde $n \in \mathbb{N}$. | $5, 7, 23$ | A088054 |
| Kynea primes | $(2^n + 1)^2 - 2$, kde $n \in \mathbb{N}_0$. | $7, 23, 79$ | A091514 |
| Palindromic primes | Pr., která zůstávají neměnná při čtení zleva doprava a zprava doleva. | $7, 11, 101$ | A002385 |
| Permutable primes | Pr., u kterých jakákoliv změna pozic číslic dává stále prvočíslo. | $11, 13, 17$ | A003459 |
| Pythagorean primes | $4n + 1$, kde $n \in \mathbb{N}$. | $37, 41, 53$ | A002144 |
| Safe primes | Pr., u kterých platí, že $p$ a $(p-1)/2$ jsou prvočísly. | $59, 83, 107$ | A005385 |
| Sophie Germain primes | Pr., u kterých platí, že $p$ a $2p + 1$ jsou prvočísly. | $41, 53, 83$ | A005384 |
| Woodall primes | $n \cdot 2^n - 1$, kde $n \geq 2, n \in \mathbb{N}$. | $7, 23, 383$ | A050918 |

# 5 Riemannova hypotéza

Riemannova hypotéza, jeden z nejzáhadnějších a nejtěžších problémů v oblasti teorie čísel, resp. v celé oblasti matematiky, byla veřejnosti představena roku 1859 na Berlínské akademii. Autorem, po němž nese tato hypotéza název, je německý matematik Bernhard Riemann, který ji zformuloval ve svém devítistránkovém článku *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* [21] (česky *O počtu prvočísel menších než daná hodnota*). Jeho podnětem se stala prvočíselná věta, kterou ve svých patnácti letech v roce 1792 zformuloval slavný německý matematik Johann Carl Friedrich Gauss. Ta pojednává o rozmístění prvočísel mezi ostatními přirozenými čísly, což fascinovalo právě i zmíněného Riemanna. Hypotézu však Riemann nikdy nedokázal a nepodařilo se to ani jeho následovníkům, mezi kterými byla například dvojice Godfrey Harold Hardy a John Littlewood, kteří spolu pracovali více než třicet let či David Hilbert. Ten je znám mimo jiné díky seznamu 23 tzv. *Hilbertových problémů*, které představil v roce 1900 na Druhém mezinárodním kongresu matematiků v Paříži, a jenž označují matematické problémy, které by po předložení důkazu o jejich pravdivosti či nepravdivosti, přispěly velkou měrou k rozvoji celé oblasti tehdejší matematiky. Dodnes nebyly dokázány pouze čtyři z nich. Za stejným účelem bylo o sto let později opět v Paříži představeno 7 tzv. *Problémů milénia*, které byly odlišné od Hilbertových problémů kromě jediného, kterým byla Riemannova hypotéza. Není tedy pochyb, že k nalezení důkazu vede velmi trnitá cesta a je velmi těžké odhadovat, zda se důkazu, který by přinesl obrovský pokrok v různých oblastech našich životů, počínaje kvantovou mechanikou a končící v byznyse, někdy v budoucnu dočkáme. Na druhou stranu, tak jak to většinou bývá, není známo, zda by případný důkaz neposkytl v některých oblastech opačné důsledky. Jako jednou z nejvíce probíraných oblastí je bezpečnost šifrovací metody RSA, která je nedílnou součástí internetového bankovnictví, viz [22]. O ni se lze dočíst v sekci 6.1. Díky velikému zájmu mnoha lidí o zkoumání této hypotézy, máme možnost se obohatit novými informacemi z různých zdrojů, jmenujme např. knihy [3] a [7], velmi populární přednášku Mirko Rokyty [22] či doplňující video [27].

## 5.1 Souvislost Riemannovy hypotézy s prvočísly

Pokud bychom se zaměřili na rozložení prvočísel mezi přirozenými čísly, došli bychom k závěru, že chování prvočísel je velmi zvláštní. Je totiž velmi obtížné odhalit, jaké prvočíslo bude v předložené řadě prvočísel následovat. Riemann se při tomto

zkoumání opřel o tzv. Riemannovu zeta funkci $\zeta$, jejíž kořeny nám pomáhají pochopit, jak se prvočísla mezi přirozenými čísly chovají. S tím má mimo jiné velmi blízkou souvislost také prvočíselná funkce $\pi(x)$, jejíž nejpřesnější aproximací je funkce, která sčítá přes všechny netriviální kořeny zeta funkce. Nyní si všechny zmíněné pojmy a funkce představíme, začneme s definicí Riemannovy zeta funkce $\zeta$.

**Definice 6.** *Riemannova zeta funkce $\zeta$ je součet nekonečné řady převrácených hodnot všech přirozených čísel umocněných na mocninu $s$*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{5.1}$$

Tuto funkci, ač nese název po Riemannovi, jako první definoval Leonhard Euler a to pro body $s > 1, s \in \mathbb{R}$, když dokazoval, že prvočísel existuje nekonečně mnoho. Tím, že hledáme kořeny zeta funkce, které mají co dočinění s prvočíselnou funkcí, zajímá nás ve kterých reálných bodech $s$ tato funkce, resp. řada konverguje.

**Věta 6.** *Riemannova zeta funkce $\zeta$ pro $s \in \mathbb{R}$ konverguje v bodech $s > 1$.*

*Důkaz.* Důkaz si rozložíme na čtyři části. Nejprve ověříme, jak se funkce chová v bodech $s < 0$. Zde nám k důkazu poslouží nutná podmínka konvergence, která říká, že pokud řada $\sum_{n=1}^{\infty} 1/n^s$ konverguje, pak limita členů posloupnosti $1/n^s$ je rovna nule. Jinak řečeno, pokud se limita rovnat nule nebude, pak řada $\sum_{n=1}^{\infty} 1/n^s$ diverguje. Pro

$$s < 0 \quad \text{platí} \qquad \lim_{n\to\infty} \frac{1}{n^s} = \infty$$

a tedy limita se nule nerovná. Lze tudíž říci, že řada $\sum_{n=1}^{\infty} 1/n^s$ v bodech $s < 0$ diverguje.

U druhé části důkazu budeme zkoumat chování funkce v bodě $s = 0$. Nyní na první pohled vidíme, že v tomto bodě řada opět diverguje, neboť sčítáme nekonečnou řadu jedniček.

V třetí části důkazu, tedy pro body $0 < s \leq 1$ nutná podmínka konvergence nejde limitně k nule a tím pádem nám v tomto případě nikterak k rozhodnutí nepomůže. Nejprve se podíváme na konvergenci či divergenci řady, kde $s = 1$, tedy

$$\sum_{n=1}^{\infty} \frac{1}{n^1} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots$$

Tato řada se nazývá *harmonická* a k důkazu využijeme integrální kritérium, které říká, že pakliže máme řadu $\sum_{n=1}^{\infty} 1/n$, která je definovaná na intervalu $[1, \infty)$ a pro niž platí, že $\forall\, n \in \mathbb{N}\ f(n) = a_n$ a tato funkce je nezáporná a nerostoucí, pak řada $\sum_{n=1}^{\infty} 1/n$ diverguje, resp. konverguje právě tehdy, když diverguje, resp. konverguje integrál $\int_1^{\infty} 1/x\, dx$. A tedy

$$\lim_{n\to\infty} \int_1^n \frac{1}{x}\, dx = \lim_{n\to\infty} \left[\ln(x)\right]_1^n = \lim_{n\to\infty} \left(\ln(n) - \ln(1)\right) = \infty.$$

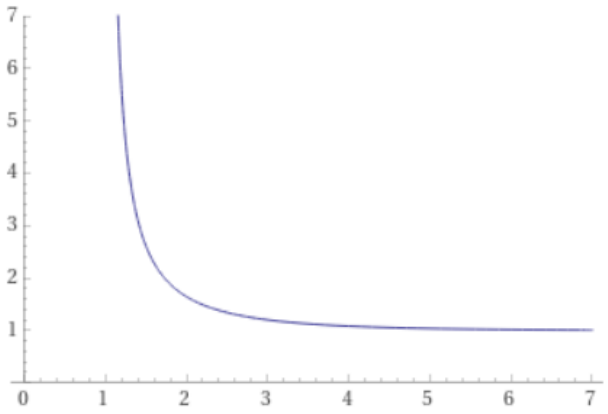
Integrál diverguje a ze znění integrálního kritéria tudíž diverguje i harmonická řada $\sum_{n=1}^{\infty} 1/n$. Zbývá nám již tedy rozhodnout o konvergenci či divergenci řady pro interval $0 < s < 1$. I zde využijeme harmonickou řadu, tentokrát pro porovnávací kritérium, které říká, že jestliže pro dvě řady s kladnými členy, v našem případě $\sum_{n=1}^{\infty} 1/n$ a $\sum_{n=1}^{\infty} 1/n^s$, kde $0 < s < 1$, platí pro každé $n \geq 1$, že $1/n \leq 1/n^s$, kde $0 < s < 1$, pak z divergence řady $\sum_{n=1}^{\infty} 1/n$ plyne divergence řady $\sum_{n=1}^{\infty} 1/n^s$, kde $0 < s < 1$. Záměrně jsme zvolili harmonickou řadu, neboť u ní víme, že diverguje. Podíváme-li se na členy těchto řad, zjistíme, že v případě harmonické řady dostáváme vždy menší hodnoty, neboť ve jmenovateli se nacházejí vždy větší čísla, než u řady, kde $0 < s < 1$. Podmínka je tak splněna a řada $\sum_{n=1}^{\infty} 1/n^s$, kde $0 < s < 1$ diverguje.

Poslední částí tohoto důkazu je pak rozhodnout o konvergenci či divergenci řady v bodech $s > 1$. I zde využijeme integrálního kritéria, kdy dostáváme, že

$$\lim_{n\to\infty} \int_1^n \frac{1}{x^s}\,dx = \lim_{n\to\infty} \left[\frac{x^{-s+1}}{-s+1}\right]_1^n = \lim_{n\to\infty} \left(\frac{n^{-s+1}}{-s+1} - \frac{1}{-s+1}\right) = \frac{1}{s-1}.$$

Po uvědomění si, že se pohybujeme na intervalu, kde $s > 1$, dostáváme, že výsledná limita bude vždy konečná. Integrál $\int_1^{\infty} 1/x^s\,dx$ tudíž vždy konverguje a z integrálního kritéria vyplývá, že vždy konverguje i řada v bodech $s > 1$. □

Záměrně jsme si důkaz rozložili na tyto čtyři části, protože zásadní hodnotou zeta funkce se ukázala $\zeta(1)$, viz [23]. A my nyní již víme proč. Riemannova zeta funkce $\zeta$ totiž diverguje v bodech $s \leq 1, s \in \mathbb{R}$ a konverguje v bodech $s > 1, s \in \mathbb{R}$, o čemž svědčí i graf funkce zeta na obrázku 5.1. V těchto bodech by se tudíž mohly nacházet hledané kořeny Riemannovy zeta funkce $\zeta$. Zaměříme-li se však na fakt, že tato funkce je definována jako součet nekonečné řady a navíc bereme-li v potaz i podmínku, že $s > 1, s \in \mathbb{R}$, pak členy této řady jsou vždy kladná čísla. Součet kladných čísel nikdy není roven nule a takto definovaná Riemannova zeta funkce $\zeta$ nemá v žádných bodech $s$ kořeny.




Obrázek 5.1: Graf zeta funkce, kde $s \in \mathbb{R}$. Graf je vytvořen v prostředí WolframAlpha.

My však dnes již víme, že kořeny zeta funkce existují a jsou dokonce dvojího druhu – triviální a netriviální kořeny. Abychom je byli schopni nalézt, musíme nejprve rozšířit definiční obor Riemannovy zeta funkce do komplexní roviny, kdy dostáváme, že

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in \mathbb{C},$$

konverguje v bodech $s \in \mathbb{C}, \Re(s) > 1$, kde $\Re(s)$ značí reálnou část komplexního čísla $s$, viz [22]. Riemann tak navázal na Eulera a jeho funkci, kdy ji posléze úspěšně *analyticky prodloužil* do komplexní roviny. O analytickém prodloužení se více lze dozvědět z přednášky Mirko Rokyty [22], který ho vysvětluje na obrázcích a posléze i na konkrétním příkladu funkce, resp. řady $1+x+x^2+x^3+\ldots$ Analytické prodloužení Riemannovy zeta funkce, které Riemann představil veřejnosti ve svém článku, vypadá následujícím způsobem

$$\zeta(s) = \begin{cases} \dfrac{1}{s-1} + \displaystyle\sum_{n=1}^{\infty} \int_n^{n+1} \left( \frac{1}{n^s} - \frac{1}{x^s} \right) \mathrm{d}x, & \text{kde} \quad 0 < \Re(s) \leq 1, \ s \neq 1, \\ \\ 2^s \pi^{s-1} \cdot |s|! \cdot \sin\left( \dfrac{\pi s}{2} \right) \cdot \zeta(1-s), & \text{kde} \quad \Re(s) \leq 0, \end{cases} \tag{5.2}$$

viz [22]. Nyní tedy položme analytické prodloužení Riemannovy zeta funkce rovno nule, poněvadž je naším cílem nalézt kořeny této funkce. Zaměříme se nejprve na druhou zmíněnou funkci (5.2) a využijeme toho, že je definovaná jako součin. Čísla $2^s\pi^{s-1}$ a $|s|!$ se nikdy nerovnají nule, to stejné platí i pro hodnoty zeta funkce v bodech $(1-s)$, neboť když si uvědomíme, že jsme na oboru, kde $\Re(s) \leq 0$, pak zmíněná hodnota zeta funkce $\zeta(1-s)$ je rovna zeta funkci $\zeta$ v kladných hodnotách, kde je definována předpisem (5.1). Již víme, že takto definovaná Riemannova zeta funkce $\zeta$ nemá v žádných bodech $s$ kořeny a tedy ani zde se zeta funkce v bodech $(1-s)$ nikdy nebude rovnat nule. Zbývá nám zjistit, zda a popřípadě ve kterých bodech $s$ má funkce $\sin\left(\frac{\pi s}{2}\right)$ nulové body, řešme tedy rovnici

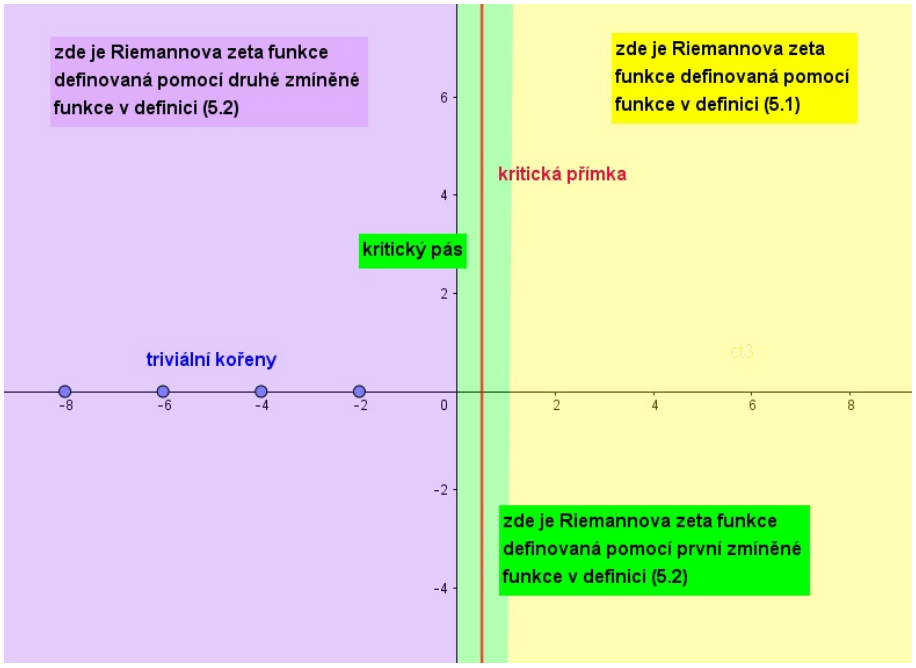
$$\begin{aligned} \sin\left(\frac{\pi s}{2}\right) &= 0, \\ \frac{\pi s}{2} &= n\pi, \\ \frac{s}{2} &= n, \\ s &= 2n, \quad n \in \mathbb{Z}. \end{aligned}$$

Z podmínky $\Re(s) \leq 0$ plyne, že výsledek lze ještě upravit a to pouze na záporná sudá čísla

$$s = -2n, \quad n \in \mathbb{N}.$$

Tyto kořeny se nazývají *triviální kořeny*. Netriviální kořeny, u kterých Riemann ukázal, že jejich umístění souvisí s rozložením prvočísel mezi přirozenými čísly, jsou spojeny s první zmíněnou funkcí (5.2), kde $0 < \Re(s) \leq 1$. Tento interval se nazývá kritický pás a osa tohoto pásu je pak známa jako kritická přímka. Body, které tuto

přímku tvoří mají tedy reálnou složku komplexního čísla $s$ rovno $1/2$. A slavná Riemannova hypotéza říká, že všechny *netriviální kořeny* leží na této přímce. Důkaz, že se Riemann nemýlil, však nepodal ani on sám, ani doposud nikdo jiný. Otázky vyvstávaly mimo jiné i v počtu netriviálních kořenů. Roku 1914 anglický matematik Godfrey Harold Hardy přišel s důkazem, že těchto netriviálních kořenů se na přímce nachází nekonečně mnoho, viz [3, str. 185]. Do roku 2005 existovala internetová stránka nesoucí název ZetaGrid, která se specializovala na hledání netriviálních kořenů Riemannovy zeta funkce, v knize [9, str. 28] se uvádí, že byla schopna každý den přicházet s více jak jedním bilionem nových netriviálních kořenů. Hlavní pojmy Riemannovy hypotézy lze vidět graficky zpracované na obrázku 5.2.



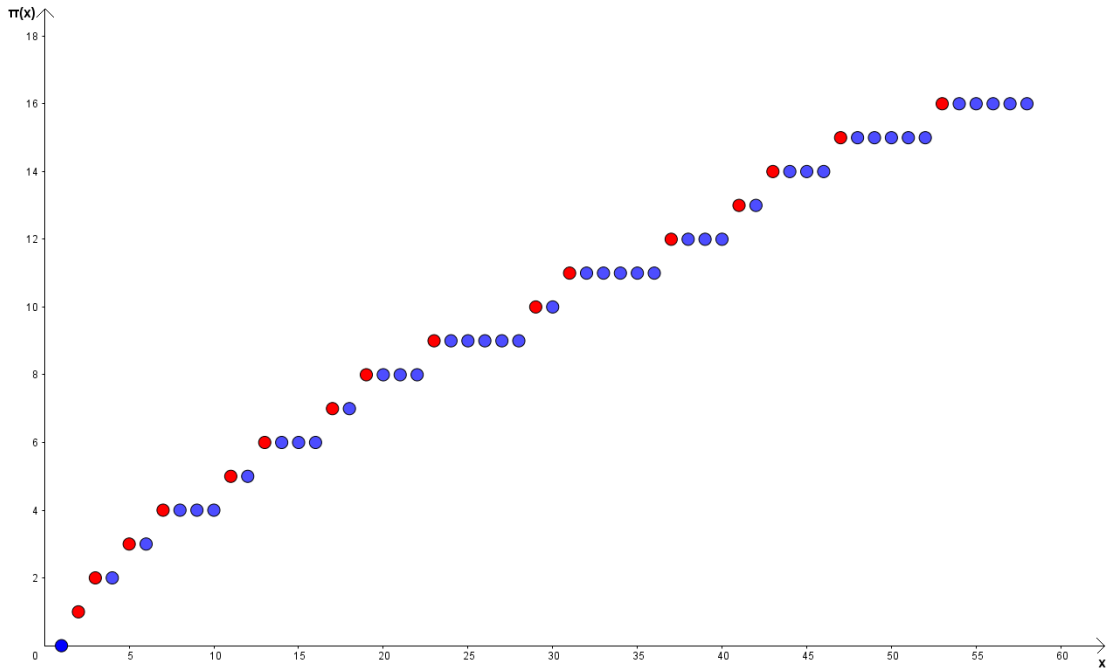

Obrázek 5.2: Mapa Riemannovy zeta funkce. Upravená grafika obrázku ze stránky [23].

## 5.2 Prvočíselná věta

Prvočíselná věta, zformulovaná Gaussem, byla hlavním impulsem Riemannova zájmu o detailnější zkoumání této oblasti. Ještě před jejím vyřčením si však musíme zadefinovat prvočíselnou funkci, která je základním kamenem této věty.

**Definice 7.** *Prvočíselná funkce $\pi(x)$ je funkce, která udává, kolik prvočísel je menších nebo rovných než číslo $x \in \mathbb{R}$.*

Na obrázku 5.3 lze vidět hodnoty prvočíselné funkce v bodech $x \in \mathbb{Z}^+$. Červeně jsou označeny hodnoty této funkce v bodech $x \in \mathbb{P}$ a lze tak vidět, že díky každému prvočíslu se hodnota prvočíselné funkce zvýší o jedna, což plyne i z definice 7.




Obrázek 5.3: Prvočíselná funkce $\pi(x)$, kde $x \in \mathbb{Z}^+$.

Původní myšlenkou Gausse bylo nalézt takovou funkci, jejíž hodnoty se co nejblíže blíží hodnotám prvočíselné funkce $\pi(x)$ v týchž bodech. Výsledek jeho zkoumání je dnes znám jako prvočíselná věta, která následuje.

**Věta 7** (Prvočíselná věta)**.** *Prvočíselná věta říká, že prvočíselnou funkci* $\pi(x)$ *lze aproximovat funkcí* $x/\ln(x)$*, neboli*

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

*kde* $\ln(x)$ *je přirozený logaritmus z čísla* $x$*.*

K tomuto odhadu Gauss dospěl, když si za $x$ označil mocniny deseti a spočítal poměr $x/\pi(x)$. Tento poměr lze volně přeložit tak, že „přibližně každé $x/\pi(x)$. číslo je v tomto intervalu prvočíslem“. Jestliže vezmeme například interval nula až sto a spočítáme tento poměr vyjde nám hodnota čtyři. V tomto intervalu je tak přibližně každé čtvrté číslo prvočíslem. Když tyto poměry od sebe odečítal, vycházel mu rozdíl přibližně roven $\ln(x) \approx 2,303$. Po následné úpravě získal zmíněnou aproximaci prvočíselné funkce. V tabulce 5.1 lze tento popis zhlédnout v prvních čtyřech sloupcích. Poměr $x/\pi(x)$ je klíčový při zkoumání mezer mezi po sobě jdoucími prvočísly, o kterých píšeme v sekci 7.2.

Bernhard Riemann již na začátku svého bádání vycházel z nedokázané prvočíselné věty. Gaussovi se nalézt důkaz nikdy nepodařilo a nebyl jediný. Roku 1848, tedy jedenáct let před vyřčením Riemannovy hypotézy, přišel ruský matematik Chebyshev

Tabulka 5.1: Příklady hodnot nejoptimálnějších aproximací prvočíselné funkce.

| $x$ | $\pi(x)$ | $x/\pi(x)$ | Rozdíl | $x/(\ln(x)-1,08366)$ | $x/\ln(x)$ | $\mathrm{Li}(x)$ |
|---|---|---|---|---|---|---|
| $10^1$ | 4 | 2,5 | — | 8 | 4 | 6 |
| $10^2$ | 25 | 4 | 1,5 | 28 | 22 | 30 |
| $10^3$ | 168 | 5,952 | 1,952 | 172 | 145 | 178 |
| $10^4$ | 1229 | 8,137 | 2,185 | 1231 | 1086 | 1246 |
| $10^5$ | 9592 | 10,425 | 2,288 | 9588 | 8686 | 9630 |
| $10^6$ | 78 498 | 12,739 | 2,314 | 78 534 | 72 382 | 78 628 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

s prvním pokusem o důkaz této věty. Tvrdil, že pokud má funkce

$$\frac{\pi(x)}{x/\ln(x)},$$

což je pouze jiná interpretace prvočíselné věty, limitu, pak musí být rovna jedné, viz [3, str. 144]. Za důkaz to však bráno nebylo. Dalším možným řešitelem mohl být Riemann, který však ani s užitím Riemannovy zeta funkce pro komplexní čísla $s$ důkaz nikdy nepředložil. Důkaz o platnosti prvočíselné věty však přeci jen máme. O něj se zasloužili nezávisle na sobě dva matematici Jacques Hadamard a Charles de la Vallée Poussin v roce 1896. Oba vycházeli z pokusů o důkaz prvočíselné věty Riemannem, jejichž hlavní myšlenkou bylo, že pokud Riemannova zeta funkce nemá žádné kořeny na přímce, kde $\Re(s) = 1$, pak platí prvočíselná věta, viz [3, str. 183]. Někteří matematici a odborníci se ale i nadále snažili přijít s jednodušším důkazem, který by se neopíral o znalost komplexní analýzy. To se povedlo Atle Selbergovi a posléze i Pálu Erdősovi, kteří předložili důkaz, jenž opravdu na komplexní analýze založen není, nicméně i přesto se považuje za mnohem těžší, než který podali Hadamard s Poussinem, viz [3, str. 145].

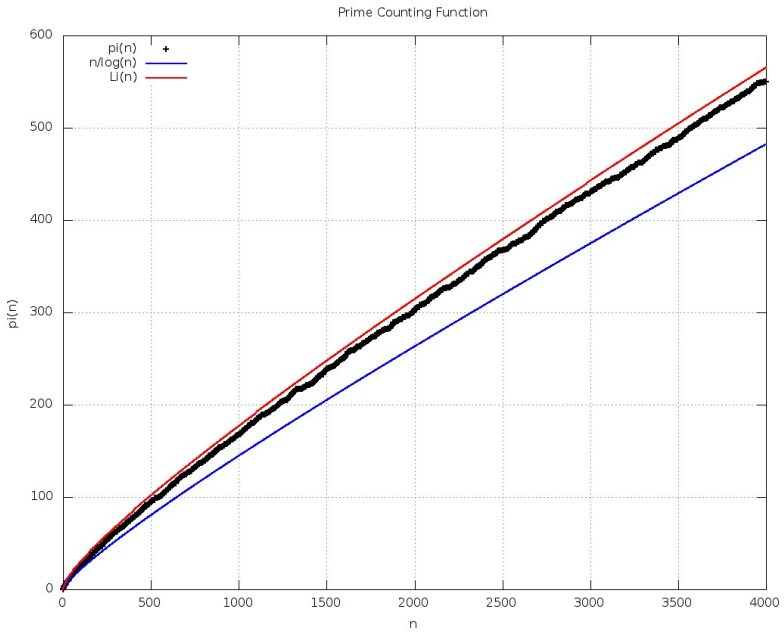
Gauss nebyl první, který se o aproximaci prvočíselné funkce $\pi(x)$ zajímal. Jako jeden z prvních se ji pokusil nalézt francouzský matematik Adrien-Marie Legendre, který tvrdil, že prvočíselnou funkci lze aproximovat funkcí

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

což se nápadně podobá té, se kterou přišel později Gauss. Ten však na své závěry přišel jinou cestou, jak jsme si ukázali a popsali výše. Co však mají s jistotou společné je, že ani Legendre své tvrzení důkazem nikdy nepodložil. Hodnoty Legendreovy funkce lze vidět v tabulce 5.1 v pátém sloupci. Můžeme tedy snadno porovnat, jak se liší od té, co později Gauss v roce 1792 označil za svou optimální aproximaci prvočíselné funkce. Gauss však ve svých pozdějších letech v roce 1849 přišel se zpřesňujícím odhadem, kdy tvrdil, že prvočíselnou funkci $\pi(x)$ lze vhodněji aproximovat funkcí $\mathrm{Li}(x)$,

$$\pi(x) \approx \mathrm{Li}(x) = \int_2^x \frac{1}{\ln(t)}\,dt,$$

viz [22] a [7, str. 79]. Hodnoty této funkce jsou taktéž ke zhlédnutí v tabulce 5.1. Tato tabulka porovnává hodnoty prvočíselné funkce v bodech $x$ s lišícími se hodnotami jejích optimálních aproximací v týchž bodech. Na první pohled se zdá, že hodnoty funkce $\mathrm{Li}(x)$ jsou vždy větší než hodnoty prvočíselné funkce $\pi(x)$, stejně tak hodnoty funkce $x/\ln(x)$ jsou vždy menší než hodnoty prvočíselné funkce $\pi(x)$. Ke stejnému závěru dospíváme i pomocí vyobrazení grafů těchto funkcí na obrázku 5.4.




Obrázek 5.4: Grafy funkcí $\mathrm{Li}(x)$, $\pi(x)$ a $\frac{x}{\ln(x)}$. Obrázek převzat z [33].

V roce 1933 Stanley Skewes však dokázal, že existuje alespoň jeden bod $x$, ve kterém hodnota funkce $\mathrm{Li}(x)$ je menší než hodnota prvočíselné funkce $\pi(x)$. První takový bod je menší než $((10^{10})^{10})^{34}$, později se tato horní hranice upravila na hodnotu $e^{72\,795\,133}$, viz [7, str. 79]. V roce 1986 matematik Hermanus Johannes Joseph te Riele dokázal, že pro více jak $10^{180}$ složených čísel z rozmezí $6,62 \cdot 10^{370} < x < 6,69 \cdot 10^{370}$ platí, že hodnota prvočíselné funkce v těchto bodech je větší než hodnota funkce $\mathrm{Li}(x)$ v týchž bodech, viz [3, str. 146].

V této kapitole jsme nejednou zmínili, že Riemann poukázal na spojitost netriviálních kořenů s rozložením prvočísel mezi přirozenými čísly. Taktéž jsme upozornili na to, že Riemann své bádání započal díky Gaussově prvočíselné větě. Z těchto dvou poznámek budeme dále vycházet. Ani Riemann nebyl výjimkou a i on se snažil najít vhodnou aproximaci prvočíselné funkce, tak jak se o to před ním pokusil již Legendre či Gauss. Vycházel z Gaussovy funkce $\mathrm{Li}(x)$, pomocí níž definoval novou funkci, která je dnes známa jako Riemannova funkce $\mathrm{R}(x)$ a má následující podobu

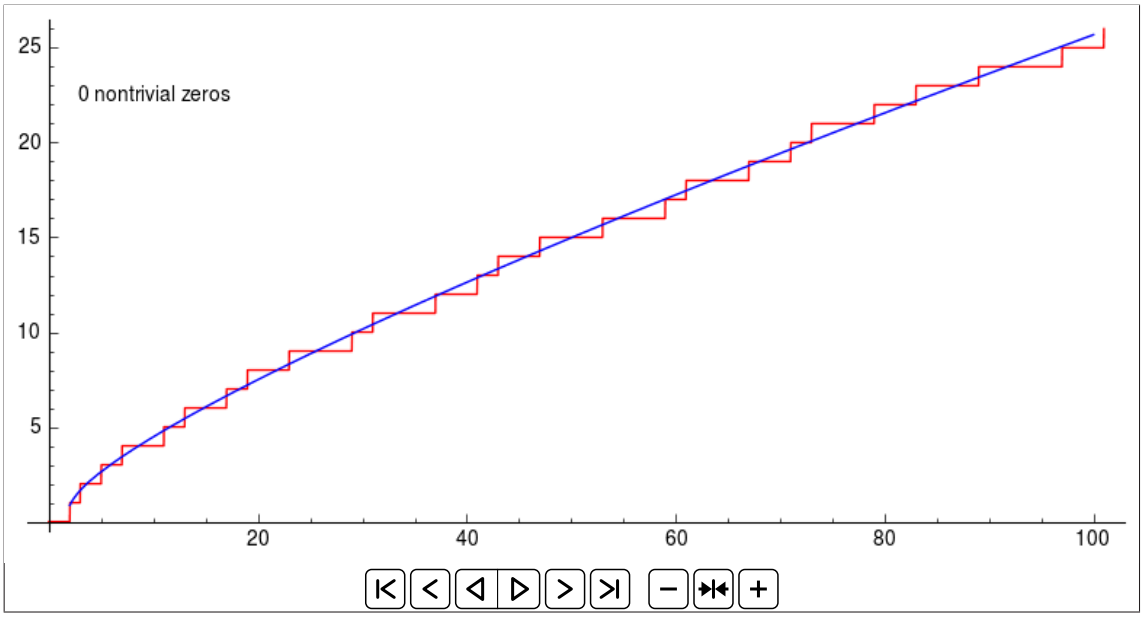
$$\mathrm{R}(x) = \mathrm{Li}(x) - \frac{1}{2}\mathrm{Li}(x^{\frac{1}{2}}) - \frac{1}{3}\mathrm{Li}(x^{\frac{1}{3}}) - \frac{1}{5}\mathrm{Li}(x^{\frac{1}{5}}) + \cdots,$$

viz [22]. Pokud k této funkci ještě navíc přičteme součet nekonečné řady $\sum_{\alpha} \mathrm{R}(x^{\alpha})$,

jejíž členy jsou hodnoty Riemannovy funkce $\mathrm{R}(x)$ v bodech, jimiž jsou netriviální kořeny Riemannovy zeta funkce $\zeta$, pak dostáváme další aproximaci prvočíselné funkce. Tato je však oproti zmíněným odlišná tím, že hodnoty této funkce jsou naprosto identické s hodnotami prvočíselné funkce v týchž bodech. Tedy

$$\pi(x) = \mathrm{R}(x) + \sum_{\alpha} \mathrm{R}(x^{\alpha}).$$

Tato Riemannem objevená rovnost však platí jen a pouze tehdy, platí-li Riemannova hypotéza, viz [22]. Na obrázku, resp. animaci 5.5 lze zhlédnout jak se tato funkce formuje, pakliže sčítáme přes čím dál tím větší množství netriviálních kořenů. Vidíme, že sčítáme-li přes čím dál tím více netriviálních kořenů, tím lepší aproximaci prvočíselné funkce získáváme.




Obrázek 5.5: Funkce $\mathrm{R}(x) + \sum_{\alpha} \mathrm{R}(x^{\alpha})$. Animace ve formátu gif převzata z [32], autora se nám nepodařilo dohledat.

**Otevřený problém 5.** *Riemannova hypotéza nebyla do dnešního dne dokázána, ač se o její důkaz pokoušelo mnoho matematiků, fyziků i odborníků z různých oblastí. Bohužel neúspěšně. Čím dál tím více lidí se však přiklání k tomu, že je Riemannova hypotéza pravdivá a někteří odborníci na této nedokázané hypotéze dokonce postavili svá tvrzení a domněnky. Stejně tak se však čím dál tím více objevují otázky, zda je současná matematika a její prostředky vůbec postačující k jejímu dokázání... A také zda vůbec důkaz existuje...*

**Poznámka 10.** *Pro doplnění souvislostí mezi částmi této kapitoly o Riemannově hypotéze doporučujeme podívat se na přednášku Mirko Rokyty [22], kde jsou mimo jiné uvedeny i počty spočtených kořenů v kritickém pásu či jaké je jejich rozložení na kritické přímce.*

## 5.3 Důkaz Riemannovy hypotézy

Není pochyb, že Riemannova hypotéza je opravdu jeden z nejzajímavějších a zároveň nejtěžších matematických problémů, jaký v současnosti máme k dispozici. Poutá nejednoho zájemce a odborníka, kteří se ji pokoušejí úspěšně dokázat. Již víme, že ač se Riemann díky zformulování Riemannovy hypotézy stal nepochybně jedním z největších matematiků nejen 19. století, nikdy svou hypotézu důkazem nestvrdil. Na stránce [28] lze najít přehled některých pokusů o důkaz i s uvedením jejich autorů. Mezi nimi je zmíněn i britský matematik sir Michael Atiyah, jehož důkaz je považován za jeden z nejnovějších důkazů. Ten byl jím představen veřejnosti v září roku 2018 na konferenci Heidelberg Laureate Forum. V té době devětaosmdesátiletý Atiyah upoutal širokou veřejnost takovým způsobem, že bylo obtížné se na tuto konferenci dostat osobně, a tak byla přenášena i online. Videopřenos byl ale často díky přítomnosti mnoha lidí provázen výpadky. Na téže stránce lze nalézt odkaz, díky kterému můžeme celou jeho přednášku zhlédnout i s prezentací, kterou promítal veřejnosti a jež prý obsahuje důkaz Riemannovy hypotézy. Do dnešního dne nemáme potvrzeno, že tento Atiyahem představený důkaz je opravdu platným důkazem Riemannovy hypotézy, nicméně mnoho lidí je rozporuplných z jeho jednoduchosti a stručnosti, a tak tomuto důkazu příliš nevěří. Oficiální verdikt však od vědecké obce zatím k dispozici není, a tak je pořád možné, že Atiyah se po své smrti možná stane tím slavným člověkem, který kdy Riemannovu hypotézu dokázal.

# 6 Využití prvočísel

Prvočísla nacházejí svá využití v různých oblastech, a to nejen matematiky. Pravděpodobně tou nejznámější a zároveň jednou z nejdůležitějších oblastí, co se týče využití prvočísel, je online bankovnictví, kde je zapotřebí chránit velice citlivá data. K tomu nám slouží tzv. metoda RSA, jejíž bezpečnost spočívá v doposud neobjevených prostředcích pro rozložení velkého čísla na součin dvou prvočísel (o více jak dvěstě cifrách, viz [9, str. 214]), z nichž je číslo utvořeno, viz [7, str. 245]. Svůj podíl na bezpečnosti této metody má i asynchronnost šifry, neboli to, že je postavena na odlišných klíčích sloužících pro zašifrování, resp. dešifrování zprávy. Pokud by na odlišných klíčích nezáleželo a odesílatel i příjemce by při posílání zpráv vlastnili stejný klíč, pak by ho bylo snadné zachytit a zneužít jej. V této kapitole metodu RSA blíže představíme, uvedeme základní informace o ni, na jakém principu funguje a uvedeme také konkrétní příklad s konkrétními čísly pro snazší pochopení. Prvočísla jsou využívána i pro ověřování správných zápisů různých identifikačních čísel, jmenujme např. rodná čísla osob České republiky, identifikační čísla osob či organizací (IČO), ISBN knih či ISSN časopisů, o kterých se lze rovněž v této kapitole dočíst.

## 6.1 Metoda RSA

Metoda RSA pochází z roku 1978 a je připisována třem počítačovým expertům, z jejichž prvních písmen příjmení je utvořen název této metody. Jimi jsou dva Američané Ronald Lorin Rivest a Leonard Adleman a Izraelec Adi Shamir. Původní myšlenka o různých klíčích potřebných k šifrování a dešifrování zprávy však pochází od Whitfielda Diffieho a Martina Hellmana z roku 1976, viz [9, str. 193]. Jejich vize byla taková, že klíč sloužící k zašifrování zprávy by mohl být veřejný, tedy přístup k němu by mohl mít kdokoliv, ale dešifrovat zprávu by již lidé s tímto klíčem nemohli. Ti by museli vlastnit tajný klíč, který, jak přívlastek napovídá, by široká veřejnost k dispozici neměla. Mezi těmito dvěma klíči by pochopitelně musel panovat určitý vztah, aby metoda RSA byla efektivní.

O dva roky později se všechny tyto postřehy promítly do metody RSA, která je díky odlišným klíčím označována jako asynchronní šifra a mluví se o ni jako o nejznámější asynchronní šifře na světě. Využívá se všude tam, kde je třeba chránit velice citlivá data, tedy v již zmíněném online bankovnictví, ale také třeba ve vojenství při šifrování tajných zpráv.

### 6.1.1 Bezpečnost metody RSA

V knize [7, str. 245] se uvádí, že *„S počítačovým hardwarem, který máme v dnešních dnech k dispozici, můžeme vyloučit možnost prolomení klíčů, protože požadovaný výpočetní čas by se rovnal celému věku vesmíru“*. Oním prolomením klíčů se rozumí rozložení velkého čísla na dvě velká prvočísla, z nichž je toto číslo utvořeno, a na kterém je bepečnost metody RSA založena. Nikdo však nedokáže říci, jak rychle bude vývoj v oblasti počítačů pokračovat a zda například kvantové počítače nebudou schopny tuto bezpečnost prolomit. Dalším otazníkem se stává dokázání Riemannovy hypotézy, o které jsme psali v kapitole 5. Co však s jistotou lze říci je to, že prolomení bezpečnosti metody RSA by znamenalo obrovský problém v celém online bankovnictví.

### 6.1.2 Popis metody

Metoda RSA začíná tím, že se obě dvě strany, tedy odesílatel i příjemce zprávy, domluví na komunikaci. Poté si příjemce zprávy určí dvě prvočísla $p$ a $q$, která musí být různá a dostatečně velká a jejichž součin $n$ je částí veřejného klíče, který může příjemce zprávy zveřejnit (resp. musí ho zveřejnit odesílateli zprávy), neboť rozložit ho zpět na tato prvočísla je při současných metodách prakticky nereálné, viz sekce 6.1.1. Dále si zvolí libovolné číslo $e$ takové, které splňuje dvě podmínky. Tou první je, že číslo $e$ a hodnota Eulerovy funkce $\varphi(n)$ musí být čísla nesoudělná, tou druhou pak je, že $e < \varphi(n)$. Ze vztahu

$$de \equiv 1 \pmod{\varphi(n)}$$

vypočítá číslo $d$. Jako veřejný klíč metody RSA se označuje dvojice čísel $n$ a $e$, který příjemce zprávy odešle odesílateli zprávy. Soukromým klíčem metody RSA je pak dvojice $n$ a $d$, který si příjemce ponechá pro sebe. Odesílatel zprávu, kterou budeme značit $Z$, zašifruje jako číslo $x$

$$x = Z^e \bmod n$$

a pošle příjemci. *Problém RSA*, který je obtížností velmi podobný prolomení bezpečnosti této metody, tedy v dnešní době je ho prakticky nereálné vyřešit, spočívá v získání čísla $Z^e$ jen s pomocí čísel $n$ a $e$, viz [9, str. 214]. Příjemci po vyřešení rovnice

$$Z = x^d \bmod n$$

už nic nebrání v tom si původní zprávu $Z$ přečíst.

### 6.1.3 Konkrétní příklad

Nyní si představíme zmíněný popis metody RSA s konkrétními čísly. Čísla (resp. prvočísla) jsou volena velmi malá, aby byl příklad názornější a snazší na výpočet bez dalších programů, nicméně pro bezpečnost této metody se doporučuje volit prvočísla

o více jak dvěstě cifrách, viz úvod kapitoly 6. Odesílatele zprávy značíme písmenem O a příjemce zprávy písmenem P.

O: Chtěl bych ti poslat tajnou zprávu metodou RSA (pozn. zpráva $Z$ nechť je zašifrovaná pod číslem 4).

P: Dobře, zvolím si tedy dvě prvočísla $p = 3, q = 11$ a vypočtu jejich součin $n$, který je roven 33 a Eulerovu funkci $\varphi(n)$, jež je rovna 20, viz sekce 1.4. Dále zvolím číslo $e$ takové, které je s číslem 33 nesoudělné a zároveň je menší než 33. Nechť je to číslo 7. Nyní spočítám číslo $d$ z kongruence

$$d \cdot 7 \equiv 1 \pmod{20}. \tag{6.1}$$

Ze sekce 1.3 víme, že zbytek $r$ u rovnice (6.1) je roven jedné. Ihned se nabízí, že číslo $d$ je rovno 3. Odesílateli zprávy odešlu veřejný klíč $(33, 7)$, soukromý klíč $(33, 3)$ si ponechám.

O: Zprávu $Z = 4$ zašifruju jako číslo $x$

$$x = 4^7 \bmod 33,$$

z čehož vyplývá, že číslo $x$ je rovno 16 a tuto informaci $x = 16$ odešlu příjemci.

P: Abych si původní zašifrovanou zprávu mohl přečíst, zbývá mi vyřešit rovnici

$$Z = 16^3 \bmod 33.$$

Po vyřešení dostávám, že mi odesílatel poslal zašifrovanou zprávu $Z = 4$.

## 6.2 Jedenáctkový samodetekující kód

Tzv. jedenáctkový samodetekující kód, jehož hlavním prvkem je prvočíslo 11, pomáhá při ověřování zápisu různých identifikačních čísel osob, organizací, knih či časopisů v počítačových databázích. Taktéž je využíván při zápisu rodných čísel.

### 6.2.1 Rodná čísla

První oblast, kde se tento kód využívá, je zápis rodných čísel. Rodná čísla slouží k jasné identifikaci obyvatelů České republiky. Osobám narozeným do roku 1954 byla přidělována devíticiferná čísla mající tvar

$$\boxed{r_1 r_2 m_1 m_2 d_1 d_2 / x_1 x_2 x_3},$$

kde $r_1 r_2$ jsou dvě poslední cifry roku narození dané osoby, $m_1 m_2$ je měsíc narození osoby, přičemž pokud se jedná o ženu, pak se k tomuto dvoucifernému číslu přičítá 50 a $d_1 d_2$ určuje den, kdy se daná osoba narodila. Tři čísla za lomítkem $x_1 x_2 x_3$ pak jednoznačně identifikují člověka, poněvadž prvních šest cifer rodného čísla mohou mít dvě osoby tytéž. Od roku 1954 jsou rodná čísla deseticiferná, za lomítkem jsou namísto tří číslic číslice čtyři

$$\boxed{r_1 r_2 m_1 m_2 d_1 d_2 / x_1 x_2 x_3 x_4}.$$

Do roku 1986 se jednalo o číslici, jež je rovna zbytku dělení devíticiferného čísla číslem jedenáct. Takové deseticiferné číslo je tedy již dělitelné jedenácti. Pokud se jednalo o zbytek deset po dělení, poslední číslicí v rodném čísle byla 0, viz [6, str. 166]. To však způsobovalo poněkud obtíže, poněvadž takové číslo nesplňovalo dělitelnost jedenácti.

Od roku 1986 jsou všechna rodná čísla, resp. čtyřčíslí za lomítkem, tvořena tak, aby celé deseticiferné číslo představující rodné číslo osoby České republiky bylo vždy dělitelné jedenácti. Důvod je prostý, pro identifikaci osob či k získání informací o nich samotných jsou často rodná čísla zadávána do databází v počítačích – u lékařů, ve školách či například v pojišťovnách. Aby počítačový software ověřil, že zadané rodné číslo může vůbec existovat, je zde, kromě *na první pohled viditelných věcí* jako je například počet číslic, právě nutná podmínka dělitelnosti jedenácti.

Nyní si představíme důvody, proč je právě oním dělitelem prvočíslo 11. Prvním takovým je, že deseticiferných čísel dělitelných tímto prvočíslem je poměrně dost, určitě více než jiných minimálně dvouciferných prvočísel, viz [6, str. 166]. Druhým pak je, že chybně zadané rodné číslo se liší od správně zadaného rodného čísla hodnotou $a \cdot 10^n$, kde $a = \{1, 2, \ldots, 9\}$ a $n \in \mathbb{N}_0$. Jak lze ze součinu vidět, takové číslo není nikdy dělitelné jedenácti, což je nezbytné k odhalení chyby v zápisu rodného čísla. Pokud by totiž zmíněný součin byl v některém případě dělitelný jedenácti, pak při záměně číslic rodného čísla by software chybu neodhalil, obě dvě rodná čísla by totiž splňovala podmínku dělitelnosti jedenácti. Pakliže by došlo k omylu ve více cifrách, v knize [6, str. 166] se uvádí, že by software odhalil chybu s pravděpodobností cca $10/11 \doteq 0,91$.

Složená čísla a jednociferná prvočísla nejsou pro odhalení chyb v zápisu rodných čísel vhodná, neboť výše zmíněná hodnota rozdílu $a \cdot 10^n$, kde $a = \{1, 2, \ldots, 9\}$ a $n \in \mathbb{N}_0$, může být těmito složenými čísly či jednocifernými prvočísly dělitelná i přesto, že se v zápisu rodného čísla nachází chyba. Názorným příkladem takového správně a chybně zapsaného rodného čísla je pokud rozdíl mezi oněmi rodnými čísly činí např. $3 \cdot 10^2$. Pak je totiž správně i chybně zapsané číslo dělitelné třemi a počítačový software by chybu v zápisu rodného čísla neodhalil.

### 6.2.2 ISBN knih

Další oblastí, kde je pro ověřování správného zápisu využívána dělitelnost jedenácti, jsou ISBN knih a ISSN časopisů. Kódy ISBN a ISSN jsou určeny pro jednoznačnou identifikaci knih a časopisů. ISBN deseticiferné kódy mají následující podobu

$$\boxed{z\text{-}n\text{-}k\text{-}c},$$

kde $z$ je označení země, popř. jazyku knihy (například číslo 80 označuje knihy pocházející z České či Slovenské republiky). Číslo $n$ určuje nakladatelství, u kterého byla kniha vydána, $k$ určuje identifikační číslo samotné knihy u daného nakladatelství a $c$ značí kontrolní číslici, díky níž je celé číslo

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10},$$

kde $\{x_1, x_2, \ldots, x_{10}\}$ jsou jednotlivé cifry deseticiferného čísla ISBN v daném pořadí, dělitelné jedenácti. Obdobně jako u rodných čísel, i zde nastává poněkud potíž, pakliže by měla být kontrolní číslicí hodnota 10, protože kontrolní číslicí v ISBN je vždy pouze jednociferné číslo. Řešení této situace je však snadné, neboť namísto čísla 10 se jako kontrolní číslice uvádí X — římsky deset, viz [6, str. 167].

Takto probíhá ověřovací proces zápisu ISBN knih vydaných do roku 2007, odkdy jsou ISBN knih třinácticiferné. Před celé deseticiferné ISBN knih se totiž ještě uvádí trojciferné číslo 978, oddělené spojovníkem od ostatních cifer, které značí, že se jedná o knihu, nikoli o hudebninu. Podoba ISBN pak vypadá takto:

$$\boxed{978\text{-}z\text{-}n\text{-}k\text{-}c},$$

kde významy písmen $z, n, k, c$ jsou neměnné, avšak kontrolní číslice $c$ je tentokrát volena tak, aby číslo

$$9 + 3 \cdot 7 + 8 + 3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10}$$

kde $\{x_1, x_2, \ldots, x_{10}\}$ jsou jednotlivé cifry třinácticiferného čísla ISBN v daném pořadí počítané bez prvního trojčíslí 978, bylo dělitelné deseti.

### 6.2.3 ISSN časopisů

Již jsme uvedli, že dělitelnost jedenácti je využívána i pro ISSN časopisů. Ty mají tvar

$$\boxed{x_1x_2x_3x_4\text{-}x_5x_6x_7x_8},$$

kde $\{x_1, x_2, \ldots, x_8\}$ jsou jednociferná čísla. V tomto případě kontrolní číslicí je osmá cifra $x_8$, díky níž je číslo

$$8x_1 + 7x_2 + 6x_3 + 5x_4 + 4x_5 + 3x_6 + 2x_7 + x_8$$

dělitelné jedenácti. Stejně jako u ISBN knih, pokud by kontrolní číslice měla být 10, pak je nahrazena římskou desítkou X, viz [6, str. 168]. Aby byla zachována systematičnost v identifikačních číslech ISBN, ISSN apod., u kódů ISSN se pro odlišení uvádí před zmíněným osmiciferným číslem trojčíslí 977 oddělené spojovníkem stejně jako u ISBN knih. Na ověřování správného zápisu toto trojčíslí však nemá žádný vliv.

### 6.2.4 Identifikační čísla osob/organizací

Čtvrtou oblastí, kde jsou využívány jedenáctkové samodetekující kódy, jsou IČA, neboli identifikační čísla osob, popř. organizací. Dnes jsou složena z osmiciferných čísel

$$\boxed{x_1x_2x_3x_4x_5x_6x_7x_8},$$

v minulosti tomu tak ale nebylo. Proto jsou tato IČA doplňována nulami na prvních pozicích tak, aby celé IČO splňovalo podmínku osmi cifer, viz [6, str. 168]. Je zřejmé,

že i zde bude figurovat kontrolní číslice, která je volena tak, aby nějakým způsobem přispívala k dělitelnosti jedenácti, resp. k ověřování zápisu daného čísla v různých databázích. A to tak, že poslední cifra osmiciferného IČA je rovna zbytku odečteného od čísla 11. Zbytek je číslo, které dostaneme po dělení čísla

$$8x_1 + 7x_2 + 6x_3 + 5x_4 + 4x_5 + 3x_6 + 2x_7,$$

kde $\{x_1, x_2, \ldots, x_8\}$ jsou jednotlivé cifry IČA v daném pořadí, jedenácti. Mohou však nastat dva problémy, kdy bychom jako kontrolní cifru $x_8$ dostali dvouciferné číslo. Takové číslo kontrolní číslicí být nemůže, neboť kontrolní čislicí je vždy pouze jedna cifra. Namísto kontrolní číslice 10, tedy v případě, že zbytek po dělení je roven jedné, se volí číslice 0. Druhý problém nastává při zbytku, který je roven nule, tudíž kontrolní číslicí by byla 11. Ten je však vyřešen velmi podobně jako při prvním problému, a to tak, že kontrolní číslicí je v tomto případě volena 1, viz [6, str. 168].

Jedenáctkové samodetekující kódy jsou využívány pro ověřování zápisů a odhalování chyb i v řadě dalších oblastí, jmenujme například čísla bankovních účtů, kódy ISMN či kódy na platebních kartách.

## 6.3 Prvočísla v přírodě

Velmi zajímavým úkazem ve využití prvočísel se staly cikády. Tento hmyz, pro něhož jsou typické hlasité zvuky, má mezi sebou dva druhy, které jsou velmi unikátní svým vztahem k prvočíslům. Tyto dva druhy Magicicada tredecim a Magicicada septendecim žijí pod zemí, až jako dospělí jedinci se objevují nad zemí, a to každých 13, resp. 17 let. Což samo o sobě je poněkud zvláštní, protože oba životní cykly jsou prvočíselné a to znamená, že se potkají spolu až každých 221 let. Neméně zajímavý je fakt, že díky těmto prvočíselným životním cyklům cikády předchází častému kontaktu se svým parazitem, jehož životní cyklus je dvouletý či tříletý, viz [6, str. 210]. Z toho vyplývá, že se cikády a jejich parazit potkávají každých 26, resp. 34 let. Jedná se tak o relativně dlouhou dobu, poněvadž pokud by byly délky jejich cyklů (berme v potaz přibližně stejně velké jako jsou ty nynější) soudělné s cyklem parazita, jednalo by se o mnohem dřívější setkání a jejich ochrana před ním by tak byla velmi nízká.

**Poznámka 11.** *Nejmenší společný násobek nesoudělných čísel je roven jejich součinu, proto se druhy cikád Magicicada tredecim a Magicicada septendecim potkají poprvé až po* 221 *letech* $(13 \cdot 17 = 221)$. *Pokud by byly délky životních cyklů čísla soudělná, např.* 9 *a* 15, *pak by se cikády těchto druhů setkávaly nad zemí častěji, konkrétně každých* 45 *let.*

# 7 Další souvislosti

Tato poslední kapitola pojednává o dosud nevyřčených zajímavostech a souvislostech týkajících se celé oblasti prvočísel. Troufáme si říci, že již nikdo nepochybuje o tom, že prvočísla jsou oblastí, kde se každým dnem objevují nové poznatky, které vedou mnohdy až k objevování často velmi složitých problémů. V dnešní době tak oplýváme širokým rozpětím různě zaměřených zajímavostí o prvočíslech, které bychom mohli rozdělit do dvou větších skupin. Do první oblasti bychom mohli zařadit zajímavosti, jež patří jednotlivým prvočíslům. Na základě toho pak lze přicházet například s novými speciálními typy prvočísel, které vykazují stejné vlastnosti, viz kapitola 4, nebo mohou být hybateli ke zkoumání nových složitějších problémů. Při této příležitosti bychom rádi zmínili knihu *Prime Curios!*, která pojednává o zajímavostech týkajících se některých vybraných prvočísel (i například těch, jejichž počet cifer převyšuje 100; pozn. do hodnoty 1000 lze nalézt v této knize zajímavosti o 159 prvočíslech z celkových 168). Druhou skupinu bychom poté mohli označit jako zajímavosti a souvislosti patřící celé oblasti prvočísel. Zde bychom tak mohli zařadit například překvapivé vlastnosti, které vykazují všechna prvočísla, ale také zajímavosti, jež jsou zaměřeny na komplexní pojetí prvočísel. A právě kromě Riemannovy hypotézy, o které jsme psali v kapitole 5, se v této kapitole podíváme na dva další takové příklady – Ulamovu spirálu a mezery mezi po sobě jdoucími prvočísly.

## 7.1 Ulamova spirála

Velmi zajímavým grafickým úkazem spojeným s prvočísly se stala Ulamova spirála z roku 1963, nesoucí název po svém objeviteli, polskému matematikovi Stanislavu Ulamovi. Její zkonstruování autorem bylo náhodné, o to zajímavější jsou pak postřehy, které díky této spirále dostáváme. Počáteční číslicí volil jedničku a každé další přirozené číslo zapisoval tak, že výsledný tvar připomínal spirálu, proto je dnes tento grafický jev znám jako Ulamova spirála, viz obrázek 7.1 nahoře vlevo. Sama o sobě nepřinášela žádné zvláštní důsledky co se matematické oblasti týče, až do doby, kdy si Ulam začal označovat ve spirále prvočísla. Všiml si totiž, že se začínají seskupovat na určitých diagonálních přímkách, což je důsledek toho, že všechna sudá čísla leží na odlišných diagonálních přímkách než lichá čísla a ze sekce 2.1 víme, že všechna prvočísla jsou lichá kromě sudého čísla 2. Na obrázku 7.2, kde je zobrazeno prvních 16 000 prvočísel, lze tyto přímky vidět zřetelněji, ba dokonce některé lze vidět zřetelněji než jiné. S tím mají jistou spojitost tzv. polynomy gene-

rující prvočísla, neboť čím více prvočísel daný polynom generuje, tím je přímka, na které leží tato prvočísla, *zřetelnější*. Pravděpodobně tím nejznámějším polynomem generující prvočísla je

$$x^2 + x + 41, \tag{7.1}$$

díky kterému po dosazení $x = 0, 1, \ldots, 39$ dostáváme posloupnost čtyřiceti prvočísel:

$$41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251,$$
$$281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853,$$
$$911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.$$

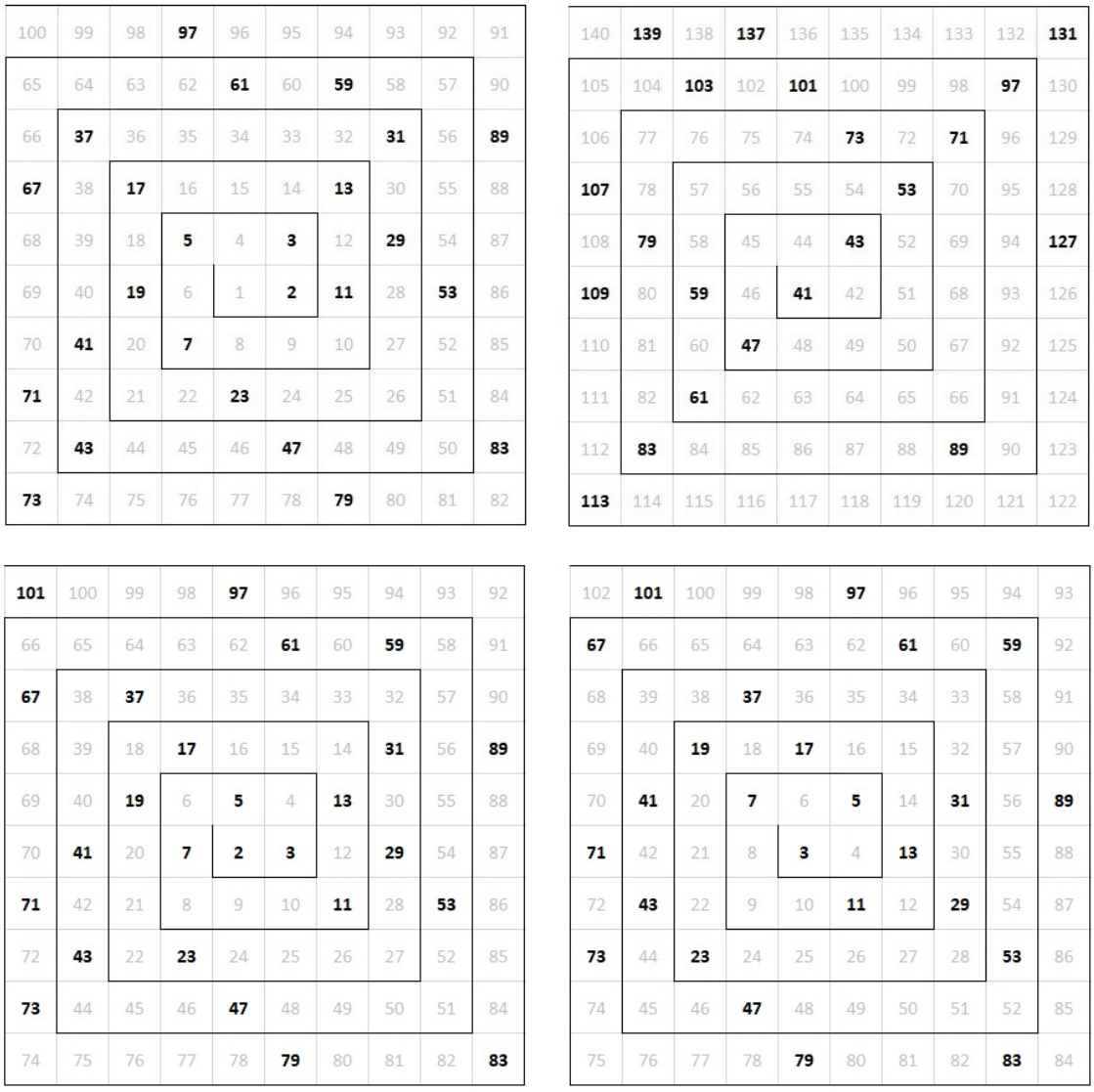
Tato prvočísla leží na přímce, kterou v Ulamově spirále začínající číslem jedna, nenalezneme, neboť tvar kvadratického polynomu je odlišný od těch, které lze v této spirále nalézt, jak si vzápětí ukážeme. Pakliže však Ulamovu spirálu začneme psát od čísla 41, jež je prvním číslem, resp. prvočíslem, které tento polynom generuje, dostáváme onu hledanou přímku, na které leží všech čtyřicet prvočísel, viz [6, str. 101] a [9, str. 233]. Náznak této přímky lze vidět na obrázku 7.1 nahoře vpravo.

Ulamova spirála je nejčastěji uváděna s počáteční číslicí rovno jedné. Jak lze vidět na obrázku 7.1, pokud ji však začneme psát od jiného čísla, můžeme sledovat, jak se pozice prvočísel mění a tím pádem vznikají často delší úsečky, které přispívají k větší zřetelnosti přímek, o které jsme psali výše. Podívejme se na Ulamovy spirály začínající čísly 1, resp. 2, resp. 3, u nichž bude měnící se pozice prvočísel patrnější. Lze si povšimnout, že části úseček tvořený konkrétními prvočísly zůstávají ve všech třech Ulamových spirálách neměnné, pouze se liší svou pozicí. Jako příklad uveďme posloupnosti prvočísel $\{5, 17, 37\}, \{19, 41, 71\}$ či $\{23, 47, 79\}$. Tím, že se pozice prvočísel ve spirálách liší, ale části úseček (resp. posloupnost stejných prvočísel) zůstávají beze změn, dochází v některých případech k tvoření delších úseček. Jednou takovou je například posloupnost šesti prvočísel $\{37, 17, 5, 13, 29, 53\}$, kterou lze vidět, pakliže začneme Ulamovu spirálu tvořit od čísla tři. Dalším takovým příkladem je posloupnost pěti prvočísel $\{71, 43, 23, 47, 79\}$, které získáváme díky změně pozic posloupností prvočísel $\{71, 43\}$ a $\{23, 47, 79\}$, které jsou opět součástí všech tří Ulamových spirál.

Nyní se však budeme zabývat *původní* Ulamovou spirálou začínající číslem jedna a podíváme se blíže na tvar polynomu, který generuje prvočísla ležící na diagonálních přímkách (přesněji spíše polopřímkách, jak uvidíme dále). Všechna prvočísla a tím pádem i přímky, na kterých leží tato prvočísla, jsou generována kvadratickými polynomy, viz [9, str. 232]. V knize [6, str. 101] je uvedeno, že mají tvar

$$4x^2 + bx + c,$$

kde $b, c \in \mathbb{Z}$. My však tento tvar polynomu ještě zpřesníme a to tak, že se zaměříme pouze na polynomy generující lichá čísla, mezi nimiž lze nalézt prvočísla. Jak můžeme na obrázku 7.1 vidět, diagonální přímky mají směrnici rovno $+1$ či $-1$. V této práci se zaměříme na přímky se směrnicí $-1$, v článku [10] potom lze vidět obdobný postup pro přímky se směrnicí $+1$. Zásadní roli v našem případě hraje úhlopříčka se směrnicí $+1$ procházející bodem jedna, viz obrázek 7.3.




Obrázek 7.1: Ulamovy spirály.

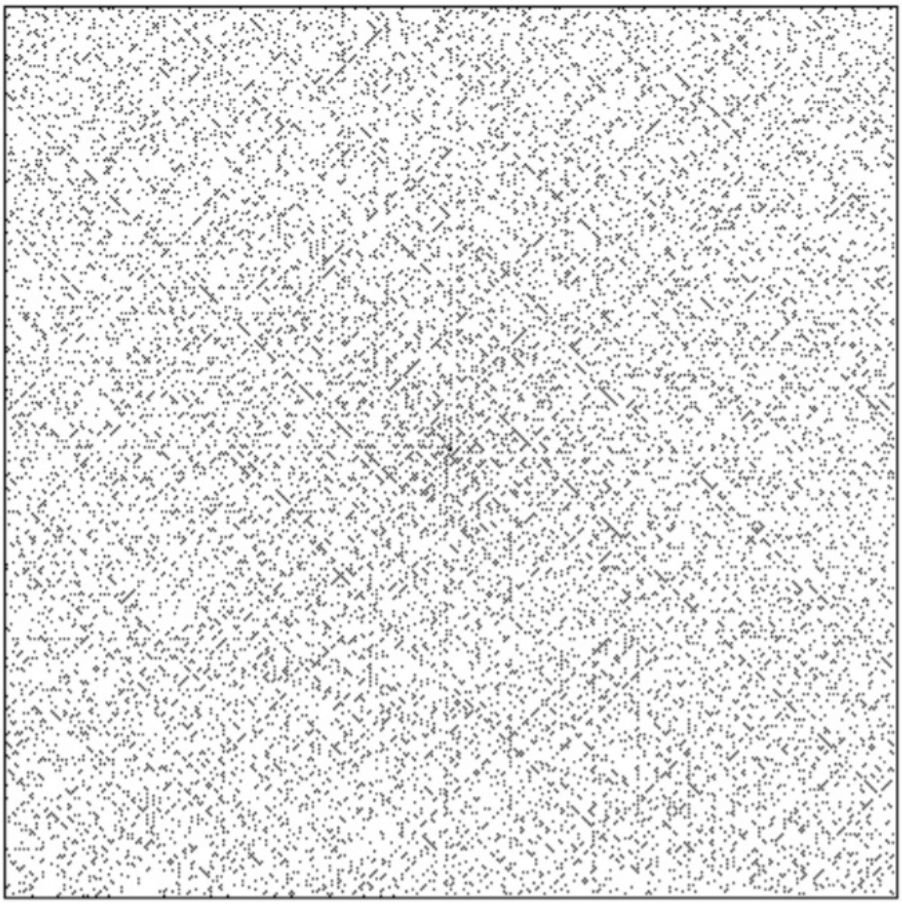
Uvažujme dva polynomy $a_\alpha(x)$ a $b_\alpha(x)$, kde $\alpha \in \mathbb{Z}$ označuje $\alpha$-tou diagonální polopřímku, jež má počáteční bod na oné úhlopříčce, o které jsme psali v předchozím odstavci a $x \in \mathbb{N}$, které označuje pozice čísel na těchto polopřímkách, pak platí

$$a_\alpha(x) = \begin{cases} 4x^2 + (8\alpha - 8)x + (4\alpha^2 - 10\alpha + 5), & \text{kde} \quad \alpha > 0, \\ 4x^2 - (8\alpha + 8)x + (4\alpha^2 + 6\alpha + 5), & \text{kde} \quad \alpha \leq 0, \end{cases} \tag{7.2}$$

a

$$b_\alpha(x) = \begin{cases} 4x^2 + (8\alpha - 12)x + (4\alpha^2 - 10\alpha + 9), & \text{kde} \quad \alpha > 0, \\ 4x^2 - (8\alpha + 4)x + (4\alpha^2 + 6\alpha + 1), & \text{kde} \quad \alpha \leq 0, \end{cases}$$

viz [10, str. 8]. Důkaz provedeme pro polynom $a_\alpha(x)$, kde $\alpha > 0$, odpovídající (zeleně



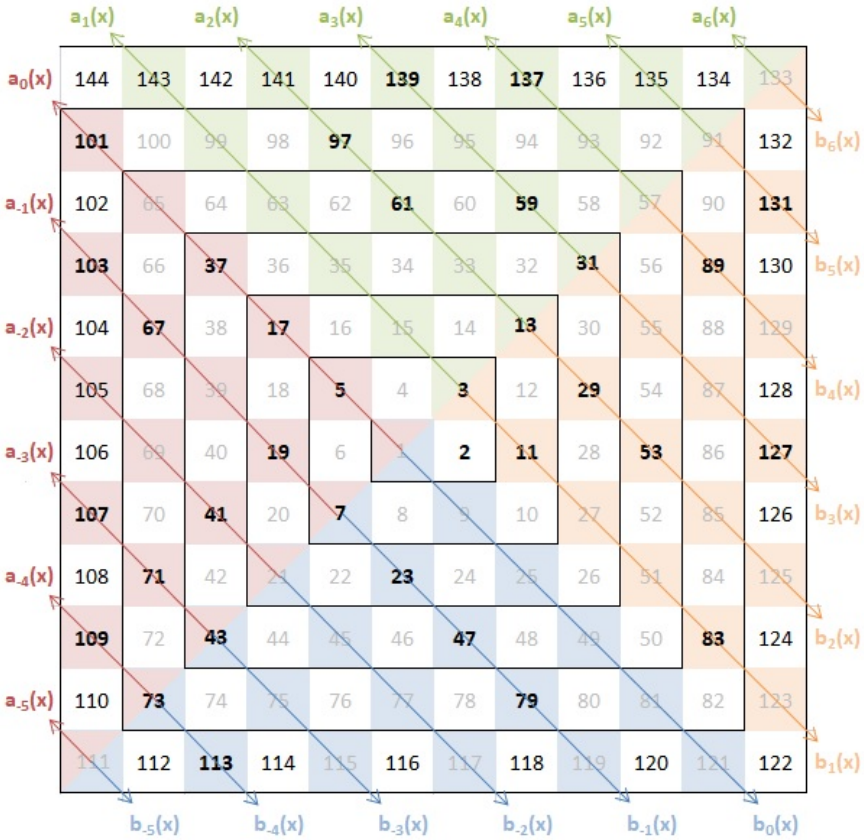
Obrázek 7.2: Diagonální přímky v Ulamově spirále. Obrázek převzat z knihy [6, str. 101].

označeným) polopřímkám, které se nacházejí v „horní čtvrtvýseči“ na obrázku 7.3.

*Důkaz.* Nejprve si spočítáme počáteční body všech těchto polopřímek, tedy platí, že $x = 1$ a $\alpha = \{1, 2, 3, \ldots\}$,

$$\begin{aligned} a_1(1) &= 3 \\ a_2(1) &= 13 \\ a_3(1) &= 31 \\ a_4(1) &= 57 \\ a_5(1) &= 91 \quad \text{atd.} \end{aligned}$$

Nyní lze odvodit rekurzivní vztah pro všechna čísla nacházející se na pozicích $x = 1$.




Obrázek 7.3: Kvadratické polynomy generující přímky se směrnicí $-1$.

Stejným způsobem popsaným v článku [10, str. 25] získáváme, že

$$\begin{aligned} a_1(1) &= 3 \\ a_2(1) &= a_1(1) + 2 \cdot 2 + 2 \cdot 3 \\ a_3(1) &= a_2(1) + 2 \cdot 4 + 2 \cdot 5 \\ a_4(1) &= a_3(1) + 2 \cdot 6 + 2 \cdot 7 \\ a_5(1) &= a_4(1) + 2 \cdot 8 + 2 \cdot 9, \end{aligned}$$

a tedy

$$\begin{aligned} a_1(1) &= 3 \\ a_\alpha(1) &= a_{\alpha-1}(1) + 2 \cdot 2 \cdot (\alpha - 1) + 2 \cdot (2\alpha - 1) \quad \text{kde} \quad \alpha > 1. \end{aligned}$$

Vyjdeme-li z tvrzení (7.2), dostáváme, že polynom $a_\alpha(1)$ lze vyjádřit i následujícím způsobem

$$a_\alpha(1) = 4\alpha^2 - 2\alpha + 1,$$

což využijeme při dalších výpočtech. Již máme tedy odvozený rekurzivní vztah pro čísla ležící na hlavní úhlopříčce a mající pozici rovno jedné ($x = 1$). Nyní se zaměříme na polynomy, kde $\alpha \in \{1, 2, 3, 4\}$ a $x \in \{1, 2, 3, 4\}$, určujeme tudíž první čtyři

po sobě jdoucí čísla ležící na odpovídajících si diagonálních (zeleně označených) polopřímkách, nacházející se v „horní čtvrtvýseči“ na obrázku 7.3.

Pro $a_1(x)$,
$$\begin{aligned} a_1(1) &= 3, \\ a_1(2) &= a_1(1) + 2 + 2 \cdot 2 + 4 + 2, \\ a_1(3) &= a_1(2) + 2 + 2 \cdot 4 + 6 + 4, \\ a_1(4) &= a_1(3) + 2 + 2 \cdot 6 + 8 + 6. \end{aligned}$$

Pro $a_2(x)$,
$$\begin{aligned} a_2(1) &= 13, \\ a_2(2) &= a_2(1) + 4 + 2 \cdot 4 + 6 + 2, \\ a_2(3) &= a_2(2) + 4 + 2 \cdot 6 + 8 + 4, \\ a_2(4) &= a_2(3) + 4 + 2 \cdot 8 + 10 + 6. \end{aligned}$$

Pro $a_3(x)$,
$$\begin{aligned} a_3(1) &= 31, \\ a_3(2) &= a_3(1) + 6 + 2 \cdot 6 + 8 + 2, \\ a_3(3) &= a_3(2) + 6 + 2 \cdot 8 + 10 + 4, \\ a_3(4) &= a_3(3) + 6 + 2 \cdot 10 + 12 + 6. \end{aligned}$$

Pro $a_4(x)$,
$$\begin{aligned} a_4(1) &= 57, \\ a_4(2) &= a_0(1) + 8 + 2 \cdot 8 + 10 + 2, \\ a_4(3) &= a_0(2) + 8 + 2 \cdot 10 + 12 + 4, \\ a_4(4) &= a_0(3) + 8 + 2 \cdot 12 + 14 + 6. \end{aligned}$$

Stejně jako v předchozím případě díky uvedeným šestnácti příkladům lze odvodit rekurzivní vztah, tentokrát pro všechna čísla nacházející se na (zeleně označených) polopřímkách v „horní čtvrtvýseči“ na obrázku 7.3. Pro polynom $a_\alpha(x)$ tudíž platí

$$\begin{aligned} a_\alpha(x) &= a_\alpha(x-1) + 2\alpha + 2 \cdot 2 \cdot (x - 2 + \alpha) + 2 \cdot (x - 1 + \alpha) + 2 \cdot (x - 1) \\ &= a_\alpha(x-1) + 8\alpha + 8x - 12, \quad \text{kde} \quad \alpha > 0 \quad a \quad x > 1. \end{aligned}$$

V tomto případě rekurzivní vyjádření nachází své využití pouze tehdy, když bychom znali číslo nacházející se na předchozí pozici. My však chceme dokázat tvrzení (7.2), které je nezávislé na hodnotě předchozího čísla. K tomu využijeme hodnoty na odpovídajících si pozicích, které rozepíšeme následovně:

$$\begin{aligned} a_1(3) &= 3 + 2 + 2 \cdot 2 + 4 + 2 + 2 + 2 \cdot 4 + 6 + 4, \\ a_2(3) &= 13 + 4 + 2 \cdot 4 + 6 + 2 + 4 + 2 \cdot 6 + 8 + 4, \\ a_3(3) &= 31 + 6 + 2 \cdot 6 + 8 + 2 + 6 + 2 \cdot 8 + 10 + 4, \end{aligned}$$

$$\begin{aligned} a_1(4) &= 3 + 2 + 2 \cdot 2 + 4 + 2 + 2 + 2 \cdot 4 + 6 + 4 + 2 + 2 \cdot 6 + 8 + 6, \\ a_2(4) &= 13 + 4 + 2 \cdot 4 + 6 + 2 + 4 + 2 \cdot 6 + 8 + 4 + 4 + 2 \cdot 8 + 10 + 6, \\ a_3(4) &= 31 + 6 + 2 \cdot 6 + 8 + 2 + 6 + 2 \cdot 8 + 10 + 4 + 6 + 2 \cdot 10 + 12 + 6, \end{aligned}$$

z čehož dostáváme, že

$$\begin{aligned} a_\alpha(x) &= a_\alpha(1) + (x-1) \cdot (2\alpha + 4\alpha + 2x - 4 + 2\alpha + x + x) \\ &= a_\alpha(1) + (x-1) \cdot (8\alpha + 4x - 4) \\ &= a_\alpha(1) + 4x^2 - 8x + 8\alpha x - 8\alpha + 4, \quad \text{kde} \quad \alpha > 0 \quad a \quad x > 0. \end{aligned}$$

Využijeme-li nyní výpočet z úvodní části důkazu $a_\alpha(1) = 4\alpha^2 - 2\alpha + 1$, obdržíme

$$\begin{aligned} a_\alpha(x) &= 4\alpha^2 - 2\alpha + 1 + 4x^2 - 8x + 8\alpha x - 8\alpha + 4 \\ &= 4\alpha^2 - 10\alpha + 5 + 4x^2 - 8x + 8\alpha x \\ &= 4\alpha^2 + (8\alpha - 8)x + (4\alpha^2 - 10\alpha + 5), \quad \text{kde} \quad \alpha > 0 \quad a \quad x > 0, \end{aligned}$$

což jsme chtěli dokázat. □

Pro polynomy $a_\alpha(x)$, kde $\alpha \leq 0$ a $b_\alpha(x)$, kde $\alpha > 0$ i $\alpha \leq 0$ bychom tvrzení (7.2) dokazovali obdobně jako jsme si ukázali pro polynom $a_\alpha(x)$, kde $\alpha > 0$.

## 7.2 Mezery mezi prvočísly

Další zajímavostí, kterou jsme v kapitole 5 již trochu nastínili, je rozložení prvočísel a s ním související velikosti mezer mezi po sobě jdoucími prvočísly. Posloupnost čísel

$$1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, \ldots \tag{7.3}$$

označuje právě tyto velikosti počínaje prvním prvočíslem 2 a v našem případě končící prvočíslem 79. Ačkoliv všechny členy posloupnosti nelze napsat, neboť víme, že prvočísel je nekonečně mnoho, což jsme dokázali v sekci 2.2, s jistotou lze říci, že číslo 1 se vyskytuje v této posloupnosti právě jednou a to jako první člen posloupnosti. Důkaz vychází z faktu, že všechna prvočísla jsou lichá, kromě čísla 2, tudíž velikost mezery mezi nimi je minimálně rovna dvěma. Dokonce se v posloupnosti kromě čísla 1 nenachází žádné jiné liché číslo, poněvadž pokud by tomu tak bylo, pak by muselo být jedno prvočíslo sudé a po něm jdoucí prvočíslo liché (nebo naopak), aby jejich rozdíl činil liché číslo. A to jak víme z předchozí věty či ze sekce 2.1 nikdy nenastane, kromě již zmíněného sudého prvočísla 2 a po něm jdoucím lichém prvočíslu 3.

Jestliže čísla v posloupnosti značí rozdíly po sobě jdoucích prvočísel, resp. velikost mezery $k$ mezi nimi, pak zřejmě platí, že mezi těmito prvočísly lze nalézt $(k-1)$ po sobě jdoucích složených čísel. Jako příklad se zaměřme na první mezeru o velikosti 4, značící mezeru mezi prvočísly 7 a 11. V tomto intervalu nalezneme právě tři po sobě jdoucí složená čísla – $8, 9$ a $10$. Nebo pro první mezeru o velikosti 6, jež znázorňuje rozdíl prvočísel 23 a 29, platí, že mezi těmito dvěma prvočísly nalezneme právě pět po sobě jdoucích složených čísel – $24, 25, 26, 27$ a $28$. Tímto se dostáváme ke známému tvrzení, které říká, že

**Věta 8.** *Mezi po sobě jdoucími prvočísly lze najít libovolně velké mezery.*

*Důkaz.* Nechť požadujeme najít mezeru mezi prvočísly o velikosti alespoň $n > 1, n \in \mathbb{N}$, tedy alespoň $(n-1)$ po sobě jdoucích složených čísel. Pak existují čísla

$$\begin{aligned}
n! + 2 &= (1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot n) + 2 \\
n! + 3 &= (1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot n) + 3 \\
n! + 4 &= (1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot n) + 4 \\
&\vdots \\
n! + n &= (1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot n) + n,
\end{aligned}$$

jež jsou právě oněmi hledanými po sobě jdoucími složenými čísly. Platí totiž, že číslo $n! + 2$ je dělitelné dvěma, poněvadž první i druhý sčítanec je dělitelný dvěma (viz barevné značení), číslo $n! + 3$ je dělitelné třemi, číslo $n! + 4$ je dělitelné čtyřmi atd. až do čísla $n! + n$, které je dělitelné $n$. Tato čísla mají tedy více než dva dělitele a o prvočísla se tak s jistotou nejedná, viz definice 1, resp. 5. Dokázali jsme tudíž, že mezi po sobě jdoucími prvočísly můžeme nalézt libovolně velké mezery. □

V úvodu této sekce jsme zmínili, že mezery mezi po sobě jdoucími prvočísly souvisí s rozložením prvočísel, tedy konkrétně s prvočíselnou větou 7, která sděluje, že hodnota prvočíselné funkce $\pi(x)$, počet prvočísel menších nebo rovných než číslo $x$, v bodě $x$ je přibližně rovna hodnotě funkce $x/\ln(x)$ v témže bodě

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

Když provedeme následující úpravu

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

dostáváme, že průměrná velikost mezery mezi po sobě jdoucími prvočísly poblíž čísla $x$ je přibližně rovna hodnotě $\ln(x)$. V tabulce 7.1 jsou pro srovnání uvedeny hodnoty těchto funkcí pro vybraná čísla $x$. Lze tak volně říci, že každé $x/\pi(x)$. číslo je v intervalu nula až $x$ prvočíslem.

Tabulka 7.1: Příklady průměrných velikostí mezer mezi prvočísly.

| $x$ | $x/\pi(x)$ | $\ln(x)$ |
|---:|:---:|:---:|
| 10 | 2,5 | 2,303 |
| 100 | 4 | 4,605 |
| 1000 | 5,952 | 6,908 |
| 10 000 | 8,137 | 9,210 |
| 100 000 | 10,425 | 11,513 |
| 1 000 000 | 12,739 | 13,816 |
| 10 000 000 | 15,047 | 16,118 |
| ⋮ | ⋮ | ⋮ |

Ze sekce 2.1 víme, že se stále se zvětšujícími čísly prvočísla řídnou. Je tak evidentní, že v posloupnosti (7.3) se postupně začínají objevovat větší a větší čísla resp. větší mezery mezi po sobě jdoucími prvočísly jsou stále pravděpodobnější (na odkazu *A001223*, v databázi celočíselných posloupností OEIS, lze vidět některé další členy posloupnosti). Tohoto poznatku si také můžeme povšimnout ve druhém sloupci v tabulce 7.1, označující výše zmíněné průměrné velikosti mezer mezi po sobě jdoucími prvočísly poblíž čísla $x$.

Na stránce [19] lze najít všechny doposud známé mezery mezi po sobě jdoucími prvočísly až do čísla 999 999 998, kde u každé z nich je mimo jiné uveden rok jejího objevení, objevitel či po jakém prvočísle se tato mezera nachází (nemusí se však jednat o první výskyt této mezery). Z hlediska největší mezery mezi po sobě jdoucími prvočísly je mezera o velikosti 6 582 144 právě tou doposud největší, jež byla objevena roku 2017 Martinem Raabem. Z hlediska největší maximální mezery mezi po sobě jdoucími prvočísly je to pak mezera o velikosti 1550, kterou objevil v roce 2014 Bertil Nyman. Maximální mezery jsou totiž takové mezery, které jsou maximální vzhledem k velikosti mezer před nimi.

**Poznámka 12.** *Na zmíněné stránce [19] jsou maximální mezery vyznačeny hvězdičkou. U ostatních mezer, které hvězdičkou označeny nejsou a jsou větší než* 1550*, tak platí, že se mezi po sobě následujícími prvočísly minimálně jednou vyskytují, není však známo, zda se jedná o mezery maximální.*

# Závěr

V této bakalářské práci jsme čtenáře seznámili se základními poznatky a různými zajímavostmi týkající se prvočísel. Ta totiž hrají klíčovou roli v mnoha oblastech matematiky, ale své využití nacházejí i v oblastech na první pohled s nimi nesouvisejícími. Jmenujme například oblast informatiky a šifrování, kde jsme představili metodu RSA, využívanou především v online bankovnictví a jejíž bezpečnost spočívá v doposud neobjevených prostředcích rozložení velkého čísla na prvočísla či oblast kultury, kde je využíváno prvočíslo 11 sloužící k ověřování správnosti zadávaných identifikačních čísel. Jejich nezastupitelnost spočívá v unikátních vlastnostech, které jsme čtenáři přiblížili především v prvních dvou kapitolách.

Čtenáři byly taktéž představeny nejpoužívanější testy prvočíselnosti, které se v dnešní době díky vývoji výpočetní techniky stávají čím dál tím efektivnější pro odhalování prvočísel v řádech až několika milionů cifer. Díky těmto testům čtenář získal povědomí o Mersennových prvočíslech, která jsou zároveň doposud největšími známými prvočísly či o Fermatových prvočíslech, která zase mají velmi úzkou souvislost s konstruovatelnými mnohoúhelníky. Ačkoliv spoustu zajímavostí o prvočíslech již dnes známo je a my se tak s některými z nich mohli blíže seznámit, mnoho takových na své objevení stále čeká. Často tyto zajímavosti a souvislosti s jinými obory vedou k velmi rozsáhlým a obtížným problémům, které i přes současné prostředky matematiky, stávající znalosti z ostatních oborů a rozvíjející se technologie, zůstávají nedokázány. Typickým příkladem je Riemannova hypotéza, u které byl čtenář seznámen nejen s jejím zněním, ale zejména s její souvislostí s rozložením prvočísel.

Cílem práce bylo čtenáře seznámit s jedinečnými vlastnostmi prvočísel, díky nimž jsou prvočísla označována za stavební bloky celé oblasti matematiky, a přiblížit různé zajímavosti a souvislosti týkající se nejen jednotlivých prvočísel, ale především celé této oblasti. V neposlední řadě poukázat na to, jak na první pohled *elementárně a neškodně* vypadající čísla mohou vést až k velmi složitým problémům, které se i přes všechny do dnešního dne dostupné prostředky, nepodařilo dokázat.

Při psaní bakalářské práce jsem se utvrdila v tom, že i ta nejprobádanější oblast může pořád přicházet s novými poznatky, díky kterým tak máme možnost objevovat stále hlubší souvislosti mezi různými oblastmi našich životů. Rozšířila jsem si povědomí o spoustu nových informací, co se prvočísel týče a taktéž neméně opomíjeným přínosem mi byla, do té doby neznámá, práce s programem TEX, resp. jeho balíkem LATEX, ve kterém je celá tato bakalářská práce vysázena.

# Literatura


[1] Manindra Agrawal, Neeraj Kayal, Nitin Saxena: *PRIMES is in P*, Annals of Mathematics, Volume 160 (2004), pp. 781–793.
https://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf

[2] Euklides, Johan Ludvig Heiberg, Richard Fitzpatrick: *Euclid's Elements of Geometry*, first edition, 2007, revised and corrected, 2008. Řecký text z Euklidovy knihy Základy pochází od J. L. Heiberga (1883–1885), moderní anglický překlad editoval R. Fitzpatrick. ISBN 978-0-6151-7984-1.
http://farside.ph.utexas.edu/Books/Euclid/Elements.pdf

[3] Benjamin Fine, Gerhard Rosenberger: *Number Theory — An Introduction via the Density of Primes*, second edition, Birkhäuser, Switzerland, 2016. ISBN 978-3-319-43875-7.

[4] Richard K. Guy: *Unsolved Problems in Number Theory*, Third Edition, Springer-Verlag New York, 2004. ISBN 978-1-4419-1928-1.

[5] Michal Křížek, Florian Luca, Lawrence Somer, Alena Šolcová: *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, Springer, 2002. ISBN 978-0387953328.
https://www.springer.com/gp/book/9780387953328

[6] Michal Křížek, Lawrence Somer, Alena Šolcová: *Kouzlo čísel — Od velkých objevů k aplikacím*, Academia, 2018. ISBN 978-80-200-2840-2.
https://www.academia.cz/uploads/media/preview/0001/05/56daa8a00d306afd25f6771969fe65918e93b479.pdf

[7] Karl-Heinz Kuhl: *Prime Numbers — Things Long-Known and Things New-Found*, third edition, Eckhard Bodner publishing house, Pressath, 2019. ISBN 978-3-939247-93-7.
https://yapps-arrgh.de/data/primes_Online.pdf

[8] Martin Plešinger: *Úvod do obecné algebry — Poznámky k přednáškám*, rukopis, Liberec, 2020.

[9] David Wells: *Prime Numbers — The Most Mysterious Figures in Math*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2005. ISBN 978-0-471-46234-7.

[10] Steven Bode, David Roberts: *Quadratic Polynomials With High Asymptotic Prime Density in The Ulam Spiral*, University of Minnesota, Morris, 2018.
https://www.researchgate.net/publication/341540065_Quadratic_Polynomials_With_High_Asymptotic_Prime_Density_in_The_Ulam_Spiral

[11] Chris K. Caldwell: *Prime Pages — Finding primes and proving primality* (webová stránka), PrimePages, 2020.
https://primes.utm.edu/prove/merged.html

[12] Chris K. Caldwell, Angela Reddick, Yeng Xiong: *The History of the Primality of One: A Selection of Sources*, Journal of Integer Sequences, Volume 15 (2012), Article 12.9.8.
https://cs.uwaterloo.ca/journals/JIS/VOL15/Caldwell2/cald6.pdf

[13] Cmglee: *Number of sides of known constructible polygons* (obrázek), 2018.
https://en.wikipedia.org/wiki/Fermat_number#/media/File:Constructible_polygoon_set.svg

[14] Richard E. Crandall, Ernst W. Mayer, Jason S. Papadopoulos: *The twenty-fourth Fermat number is composite*, Mathematics of Computation, Volume 72, Number 243 (2002), pp. 1555–1572.
https://www.ams.org/journals/mcom/2003-72-243/S0025-5718-02-01479-5/S0025-5718-02-01479-5.pdf

[15] Wilfrid Keller: *List of Fermat numbers* (webová stránka), akt. 2021.
http://www.prothsearch.com/fermat.html

[16] Mike Mol: *Fermat numbers* (webová stránka), 2007, akt. 2021.
https://rosettacode.org/wiki/Fermat_numbers

[17] J. C. Morehead: *Note on the factors of Fermat's numbers*, Bulletin of the American Mathematical Society, Volume 12, Number 9 (1906), pp. 449–451.
https://www.ams.org/journals/bull/1906-12-09/S0002-9904-1906-01371-4/S0002-9904-1906-01371-4.pdf

[18] J. C. Morehead, A. E. Western: *Note on Fermat's numbers*, Bulletin of the American Mathematical Society, Volum 16, Number 1 (1909), pp. 1–6.
https://www.ams.org/journals/bull/1909-16-01/S0002-9904-1909-01841-5/S0002-9904-1909-01841-5.pdf

[19] Thomas R. Nicely: *Some Results of Research in Computational Number Theory* (webová stránka), 2019.
https://faculty.lynchburg.edu/~nicely/index.html#TPG

[20] Bertil Nyman, Thomas R. Nicely: *New prime gaps between 1e15 and 5e16* (webová stránka), 2017.
https://faculty.lynchburg.edu/~nicely/gaps/gaps3.html

[21] Bernhard Riemann: *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsberichte der Berliner Akademie, November 1859.
https://diglib.tugraz.at/download.php?id=4f673027cef68&location=browse

[22] Mirko Rokyta: *Riemannova hypotéza — jeden z nejtěžších matematických problémů*, YouTube (video), 2019.
https://www.youtube.com/watch?v=tHm7MnPkBiI

[23] Jan Řeháček: *Matykání: chcete vyhrát milión dolarů?*, iDnes.cz Blog, 2017.
https://janrehacek.blog.idnes.cz/blog.aspx?c=624121

[24] Walter Schneider: *Lucky numbers* (webová stránka), 2001.
http://web.archive.org/web/20041220184405/http://www.wschnei.de/number-theory/lucky-numbers.html

[25] Neil J. A. Sloane: *The On-Line Encyclopedia of Integer Sequences* (webová stránka), 1964.
https://oeis.org

[26] Bohumil Tesařík: *Michael Atiyah*, Třípól, 2019.
https://www.3pol.cz/cz/rubriky/biografie/2339-michael-atiyah

[27] Marek Valášek: *O matematice s Mirko Rokytou 4 — Problém za milion dolarů — Riemannova hypotéza*, YouTube (video), 2016.
https://www.youtube.com/watch?v=9iA5B2BwYtc

[28] Matthew R. Watkins: *Proposed (dis)proofs of the Riemann Hypothesis* (webová stránka).
http://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/RHproofs.htm

[29] A. E. Western: *Notes and corrections*, Proceedings of the London Mathematical Socicety, Serie 2, Volume 3 (1905), pp. xxi–xxii.
https://academic.oup.com/plms/article-abstract/s2-3/1/1/1455796

[30] George Woltman, Scott Kurowski: *Great Internet Mersenne Prime Search — GIMPS* (webová stránka), Mersenne Research, 2020.
https://www.mersenne.org

[31] Jeff Young, Duncan A. Buell: *The Twentieth Fermat Number is Composite*, Mathematics of Computation, Volume 50, Number 181 (1988), pp. 261–263.
https://www.ams.org/journals/mcom/1988-50-181/S0025-5718-1988-0917833-8/S0025-5718-1988-0917833-8.pdf

## Další webové zdroje (s kolektivním nebo neznámým autorstvím)


[32] *Riemann's Explicit Formula for the number of primes less than x using the zeros of the zeta function* (GIF), Imgur, 2017.
https://imgur.com/a41LdwK

[33] *ThatsMaths — The Prime Number Theorem* (webová stránka), 2014.
https://thatsmaths.com/2014/02/27/the-prime-number-theorem

[34] *Wikipedia: List of prime numbers* (webová stránka), 2020.
https://en.wikipedia.org/wiki/List_of_prime_numbers

[35] *Wikipedia: Miller–Rabin primality test* (webová stránka), 2021.
https://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test

[36] *Wikipedia: Sieve of Atkin* (webová stránka), 2020.
https://en.wikipedia.org/wiki/Sieve_of_Atkin

[37] *Wikipedia: Sieve of Sundaram* (webová stránka), 2020.
https://en.wikipedia.org/wiki/Sieve_of_Sundaram

[38] *Wikipedia: Solovay–Strassen primality test* (webová stránka), 2021.
https://en.wikipedia.org/wiki/Solovay%E2%80%93Strassen_primality_test