Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra matematiky

Bakalářská práce

Zajímavá prvočísla a jejich vlastnosti

Vypracoval: Daniel Kratochvíl
Vedoucí práce: prof. RNDr. Pavel Tlustý, CSc.

České Budějovice 2020

Prohlášení

Prohlašuji, že svoji bakalářskou práci na téma „Zajímavá prvočísla a jejich vlastnosti“ jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 14. 5. 2020 ……..

Kratochvíl Daniel

Poděkování

Tímto bych rád poděkoval svému vedoucímu bakalářské práce panu prof. RNDr. Pavlu Tlustému, CSc. za jeho pozitivní přístup, vedení a odborné rady při psaní této bakalářské práce. Velké díky patří také mým blízkým, kteří pro mě byli hnacím motorem a motivací.

Anotace

Cílem této bakalářské práce je seznámit čtenáře se speciálními typy prvočísel. Celá práce je rozdělena na čtyři části. V úvodní části je čtenáři představena definice prvočísel a představeny jsou také základní poznatky o nich a jedna z metod pro jejich vyhledání. Následující dvě části jsou zaměřeny na speciální typy prvočísel, přičemž první z nich se soustředí na typy prvočísel, které nesou názvy slavných matematiků, zatímco následující část se zabývá typy prvočísel, které jsou speciální pro svou určitou specifickou vlastnost. Závěrečná část obsahuje několik příkladů s řešením a několik bez něho.

Klíčová slova

prvočísla, speciální typy prvočísel, dělitelnost, přirozená čísla, faktorizace, kongruence, zbytek po dělení

Annotation

The aim of this bachelor thesis is to introduce special kinds of prime numbers to the reader. The thesis is divided into four parts. The first, introductory, one deals with the definition of prime numbers, provides some basic information about them, and offers one of the methods for finding the prime numbers. The following two parts focus on special kinds of prime numbers, the former of them contains those kinds of prime numbers which are named after famous mathematicians. The latter part is concern with prime numbers which are special for their unique attribute. In the closing part there are some exercises either with or without their solution.

Key words

prime numbers, special kinds of prime numbers, divisibility, natural numbers, congruence, remainder after division

Obsah

Úvod

Prvočísla, která jsou neopomenutelnou součástí teorie čísel, mají svou unikátní historii a lidé se jimi zabývají již od starověku. Eukleidés z Alexandrie ve svém díle *Základy* podal důkaz o tom, že existuje nekonečně mnoho prvočísel. Napříč historií jsme jako lidstvo dokázali přinést spoustu objevů o prvočíslech, přičemž s některými zajímavými se seznámíme v této bakalářské práci.

Do oblasti prvočísel žáci pronikají již na základních školách, kde se řeší úlohy na nejmenší společný násobek, největší společný dělitel či rozklad složených čísel na prvočinitele. Je to důležitá oblast pro další rozvoj matematických dovedností, proto by se prvočíslům měla věnovat patřičná pozornost. Úlohy spjaté s prvočísly jsou tradičními úlohami ve všech matematických soutěžích, jako je například Matematická olympiáda, Matematický klokan, Pythagoriáda atd.

Prvočísla nacházejí široké uplatnění i v reálném životě. Jedním z příkladů využití prvočísel jsou samodetekující kódy, které slouží k ověřování správnosti zadávaných dat. Od roku 1954 se občanům České republiky přidělují desetimístná rodná čísla, která jsou beze zbytku dělitelná prvočíslem 11. Tento systém slouží k jednoduchému objevování případných překlepů. Dalšími příklady využití jsou šifrované zprávy, čárové kódy či tranzistorové počítače, které zpracovávají nesmírně velké množství dat.

Úvod, který obsahuje základní informace o prvočíslech, je doplněn o jednu z jednodušších metod hledání prvočísel. Speciální typy prvočísel jsou rozděleny do dvou kategorií. První kategorie se zaměřuje na typy prvočísel, které jsou pojmenovány po slavných matematicích, druhá pak pojednává o typech prvočísel, které jsou speciální pro svou určitou specifickou vlastnost. Jednotlivé kapitoly jsou doplněny o definice, tvrzení či zajímavosti z různých odvětví matematiky. Práce je zakončena sekcí řešených i neřešených příkladů, aby si čtenář mohl nabyté poznatky procvičit.

1 Základní poznatky o prvočíslech

1.1 Definice prvočísel

Prvočíslo je přirozené číslo, které je beze zbytku dělitelné pouze jedničkou a sebou samým, přičemž číslo jedna prvočíslem není.

Pokud číslo není prvočíslem nebo jednička, pak se jedná o *číslo složené* a lze ho rozložit na součin prvočísel. To nám v podstatě říká i *základní věta aritmetiky*.

Základní věta aritmetiky

Každé přirozené číslo lze rozložit na součin přirozených mocnin prvočísel, a to až na pořadí jednoznačně. Operace, při které rozkládáme přirozené číslo na součin prvočísel, se nazývá *faktorizace*. (Michal Křížek, 2018)

Věta 1.1

„Číslo n je složené, jestliže je dělitelné některým prvočíslem $p \leq \sqrt{n}$.

Důkaz. Je-li n složené, pak má alespoň dva netriviální dělitele u, v, tj. $n = u \cdot v$.

Je-li například $u \leq v$, *pak* $n = u \cdot v \geq u^2$, *tedy* $u \leq \sqrt{n}$.“

□

Pokud tedy zkoumáme, zda je dané číslo prvočíslem, stačí vyšetřit dělitelnost pouze těmi prvočísly, která jsou menší nebo rovna $\sqrt{n}$. (Halaš, 2014)

Uvedeme si tabulku čísel od 1 do 100 a vyznačíme si v tomto intervalu všechna prvočísla zeleně, všechna čísla složená červeně, číslo 1 bude modré.

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

1.2 Hustota prvočísel

Nechť funkce $\pi(n)$ značí počet prvočísel menších nebo rovno n.

Dolní odhad této funkce je $\pi(n) \approx \frac{n}{\ln(n)}$.

Ukážeme si chování této funkce pro n z intervalu 2 až 19.

n	$\frac{n}{ln(n)}$	$\pi(n)$
2	2.9	1
3	2.7	2
4	2.9	2
5	3.1	3
6	3.4	3
7	3.6	4
8	3.9	4
9	4.1	4
10	4.3	4
11	4.6	5
12	4.8	5
13	5.1	6
14	5.3	6
15	5.5	6
16	5.8	6
17	6.0	7
18	6.2	7
19	6.5	8

Pro malá n je tento odhad poměrně přesný.

Čím dále jdeme množinou přirozených čísel do nekonečna, tím se četnost prvočísel na jednotlivých intervalech snižuje. Přibývají i série po sobě jdoucích složených čísel. Je to zapříčiněno tím, že čím dále v množině přirozených čísel jsme, tím více máme k dispozici prvočísel, a z nich pak máme prostor pro vytvoření více čísel složených. (Fuchs, 1993)

1.3 Eratosthenovo síto

Eratosthenés z Kyrény (asi 273 př. n. l. – 194 př. n. l.) byl matematik, astronom a geograf, který pocházel z antického Řecka.

Eratosthenovo síto je jednoduchá metoda pro hledání prvočísel. Jeho princip spočívá v postupném vyškrtávání složených čísel, jakožto násobků prvočísel.

Tuto snadnou metodu si ukážeme na příkladu, kdy budeme chtít najít všechna prvočísla, která jsou menší nebo rovna 100.

Vypíšeme si do tabulky všechna čísla od 2 do 100. Jak již víme, číslo 1 nepatří do prvočísel, je to samostatná skupina. Vezmeme tedy nejmenší známé prvočíslo, kterým je 2, a vyřadíme všechny jeho násobky. Prvočísla budeme zvýrazňovat zelenou barvou, jejich přirozené násobky (větší než jedna) budeme zvýrazňovat červenou barvou.

	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

Tím jsme vyřadili všechna ostatní sudá čísla. Nyní se vrátíme na začátek tabulky a nejmenší „neobarvené číslo“ musí být prvočíslo, tj. 3 je další prvočíslo. Podobně jako

v případě čísla 2, vyřadíme všechny přirozené násobky čísla 3. Je zřejmé, že některé násobky prvočísla 3 se shodují s násobky prvočísla 2. Tyto násobky se nazývají společné násobky. V matematických úlohách, které jsou spjaty s teorií čísel, se pak často hledá *nejmenší společný násobek*.

	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

Dalším prvočíslem v pořadí je 5. I zde vyškrtneme všechny násobky, které nejsou společné s násobky prvočísel 2 a 3.

	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

Následuje prvočíslo 7. Také zde vyškrtneme všechny jeho násobky, které ještě vyškrtnuty nebyly.

	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

Tím jsme s vyškrtáváním u konce, protože podle věty 1.1 stačí brát v potaz pouze prvočísla, která jsou menší nebo rovna $\sqrt{100}$. Vyznačíme tedy zbývající prvočísla v tabulce a máme síto zkompletované.

	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

Nutno podotknout, že metoda síta Eratosthena je metoda účinná, pouze pokud se pohybujeme v relativně malých číslech. Pomocí dnešní počítačové techniky jsme schopni najít prvočísla velmi vysokých řádů. S využitím Eratoshenova síta k nalezení takových prvočísel by nebylo v lidských silách, abychom taková velká prvočísla našli.

2 Speciální typy prvočísel

2.1 Mersennova prvočísla

Marin Mersenne (1588 – 1648), po němž jsou nazvána *Mersennova prvočísla*, byl francouzský matematik a fyzik.

Nechť je dán předpis $M_p = 2^p - 1$. Všechna čísla tohoto tvaru se nazývají Mersennova čísla. Pokud je číslo $2^p - 1$ navíc prvočíslo, pak ho nazveme Mersennovým prvočíslem.
Pojďme nyní ověřit validitu předpisu $M_p = 2^p - 1$, kde p je prvočíslo.

p	***Mp***	***Je Mp prvočíslo?***
2	*3*	*Ano*
3	*7*	*Ano*
5	*31*	*Ano*
7	*127*	*Ano*
11	*2 047*	*Ne*
13	*8 191*	*Ano*

Z tabulky je patrné, že M_p nemusí být nutně prvočíslo, i když p je prvočíslo. Pro $p = 11$ je $M_p = 2\,047 = 23 \cdot 89$, což je číslo složené. Z toho vyplývá nutná, nikoli postačující podmínka pro M_p z hlediska prvočíselnosti.

Věta 2.1

Je-li p prvočíslo, pak $2^p - 1$ může být prvočíslo.

„Povšimněme si, že číslo $2^{ij} - 1$ pro celá čísla $i > 1$ a $j > 1$ lze napsat jako součin dvou netriviálních činitelů

$$2^{ij} - 1 = (2^i - 1)(2^{i(j-1)} + 2^{i(j-2)} + \cdots + 2^i + 1). \qquad (2.1)$$

Proto požadujeme, aby exponent p Mersennova čísla $2^p - 1$ byl prvočíslem. Sporem snadno z rozkladu (2.1) odvodíme následující větu, kterou znal již Pierre de Fermat.“
(Michal Křížek, 2018)

Věta 2.2

„Je-li $2^p - 1$ prvočíslo, pak p je také prvočíslo.

Důkaz. Nechť $2^p - 1$ je prvočíslo a předpokládejme naopak, že p je složené, tj. existují přirozená čísla i > 1 a j > 1 tak, že p = ij. Pak oba činitelé na pravé straně rovnice (2.1) jsou větší než jedna, a tedy číslo 2^p -1 je složené, což je ve sporu s předpokladem.“ (Michal Křížek, 2018)

□

Ve vzájemném vztahu s Mersennovými prvočísly jsou tzv. *dokonalá čísla*, se kterými se vzápětí seznámíme.

Dokonalá čísla

Přirozené číslo *n* se nazývá dokonalé, jestliže je rovno součtu všech svých kladných dělitelů, které jsou menší než *n*.

Uvedeme několik prvních dokonalých čísel, které byly známé již ve starověku. Staří Řekové znali první čtyři dokonalá čísla, kterými jsou 6, 28, 496, 8 128. Přesvědčíme se o jejich platnosti alespoň u prvních dvou. (Fuchs, 1993)

Označme *σ(n)* jako součet všech kladných dělitelů čísla *n*, tj.

$$\sigma(n) = \sum_{d|n} d.$$

S využitím funkce *σ* můžeme vyslovit alternativní definici dokonalých čísel.

Číslo *n* je dokonalé, jestliže platí σ(*n*) = 2*n*.

Pro funkci σ navíc platí, že je multiplikativní, tzn. *σ(mn) = σ(m) · σ(n)*, jsou-li *m* a *n* nesoudělná přirozená čísla. (Křížek, 2018)

σ(6) = 6 + 3 + 2 + 1 = **12** = 2·**6**

σ(28) = 28 + 14 + 7 + 4 + 2 + 1 = 2·**28**

Jak tedy souvisí dokonalá čísla s Mersennovými prvočísly?

Věta 2.3

„Je-li $2^p - 1$ prvočíslo, pak je číslo $n = 2^{p-1}(2^p - 1)$ dokonalé.

Důkaz. Protože jsou čísla 2^{p-1} a $2^p - 1$ nesoudělná, platí

$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p-1}{2-1}(1 + 2^p - 1) = (2^p - 1)2^p$, a tedy n je dokonalé.“ (Michal Křížek, 2018)

□

Je zřejmé, že všechna dokonalá čísla, vycházející z věty 2.3 jsou sudá, protože násobíme sudým číslem 2^{p-1} Mersennovo prvočíslo ($2^p - 1$), které je vždy liché. Součin sudého a lichého čísla nám pak dá pokaždé číslo sudé.

Jak sám pojem dokonalé číslo napovídá, mají tyto čísla ve své podstatě skutečnou dokonalost. Co už tak dokonalé není, jsou nevyřešené problémy v oblasti dokonalých čísel či Mersennových prvočísel, jako jsou například otázky, zda existuje liché dokonalé číslo, nebo zda existuje nekonečně mnoho dokonalých čísel či Mersennových prvočísel. Tyto otázky jsme dodnes nebyli schopni vyřešit. Víme ovšem, že k roku 2020 bylo nalezeno 51 Mersennových prvočísel a na hledání dalších se podílejí nadšenci i experti z celého světa. K hledání dalších Mersennových prvočísel cílí projekt GIMPS (Great Internet Mersenne Prime Search - https://www.mersenne.org/).

V následující tabulce uvedeme seznam všech dosud známých Mersennových prvočísel. Poslední nalezené Mersennovo prvočíslo $2^{82\,589\,933} - 1$ má 24 862 048 cifer, bylo nalezeno Patrickem Larochem a jeho nalezení se datuje k 7. prosinci 2018.

#	M_p	*Počet číslic*	*Datum nalezení*	*Nálezce*
1	2^2-1	*1*	*500 př. n. l.*	*Starověcí řečtí matematici*
2	2^3-1	*1*	*500 př. n. l.*	*Starověcí řečtí matematici*
3	2^5-1	*2*	*275 př. n. l.*	*Starověcí řečtí matematici*
4	2^7-1	*3*	*275 př. n. l.*	*Starověcí řečtí matematici*
5	$2^{13}-1$	*4*	*1456*	*Anonymní*
6	$2^{17}-1$	*6*	*1588*	*Pietro Cataldi*
7	$2^{19}-1$	*6*	*1588*	*Pietro Cataldi*
8	$2^{31}-1$	*10*	*1772*	*Leonhard Euler*
9	$2^{61}-1$	*19*	*1883*	*Ivan Mikheevich Pervushin*

10	$2^{89}-1$	*27*	*červen 1911*	*R. E. Powers*
11	$2^{107}-1$	*33*	*11. června 1914*	*R. E. Powers*
12	$2^{127}-1$	*39*	*10. ledna 1876*	*Édouard Lucas*
13	$2^{521}-1$	*157*	*30. ledna 1952*	*Raphael M. Robinson*
14	$2^{607}-1$	*183*	*30. ledna 1952*	*Raphael M. Robinson*
15	$2^{1\,279}-1$	*386*	*25. června 1952*	*Raphael M. Robinson*
16	$2^{2\,203}-1$	*664*	*7. října 1952*	*Raphael M. Robinson*
17	$2^{2\,281}-1$	*687*	*9. října 1952*	*Raphael M. Robinson*
18	$2^{3\,217}-1$	*969*	*8. září 1957*	*Hans Riesel*
19	$2^{4\,253}-1$	*1 281*	*3. listopadu 1961*	*Alexander Hurwitz*
20	$2^{4\,423}-1$	*1 332*	*3. listopadu 1961*	*Alexander Hurwitz*
21	$2^{9\,689}-1$	*2 917*	*11. května 1963*	*Donald B. Gillies*
22	$2^{9\,941}-1$	*2 993*	*16. května 1963*	*Donald B. Gillies*
23	$2^{11\,213}-1$	*3 376*	*2. června 1963*	*Donald B. Gillies*
24	$2^{19\,937}-1$	*6 002*	*4. března 1971*	*Bryant Tuckerman*
25	$2^{21\,701}-1$	*6 553*	*30. října 1978*	*L. C. Noll & Laura Nickel*
26	$2^{23\,209}-1$	*6 987*	*9. února 1979*	*Landon Curt Noll*
27	$2^{44\,497}-1$	*13 395*	*8. dubna 1979*	*H. L. Nelson & D. Slowinski*
28	$2^{86\,243}-1$	*25 962*	*25. září 1982*	*David Slowinski*
29	$2^{110\,503}-1$	*33 265*	*28. ledna 1988*	*W. Colquitt & L. Welsh*
30	$2^{132\,049}-1$	*39 751*	*19. září 1983*	*David Slowinski*
31	$2^{216\,091}-1$	*65 050*	*1. září 1985*	*David Slowinski*
32	$2^{756\,839}-1$	*227 832*	*19. února 1992*	*David Slowinski & P. Gage*
33	$2^{859\,433}-1$	*258 716*	*4. ledna 1994*	*David Slowinski & P. Gage*
34	$2^{1\,257\,787}-1$	*378 632*	*3. září 1996*	*David Slowinski & P. Gage*
35	$2^{1\,398\,269}-1$	*420 921*	*13. listopadu 1996*	*GIMPS / Joel Armengaud*
36	$2^{2\,976\,221}-1$	*895 932*	*24. srpna 1997*	*GIMPS / Gordon Spence*
37	$2^{3\,021\,377}-1$	*909 526*	*27. ledna 1998*	*GIMPS / Roland Clarkson*
38	$2^{6\,972\,593}-1$	*2 098 960*	*1. června 1999*	*GIMPS / Nayan Hajratwala*
39	$2^{13\,466\,917}-1$	*4 053 946*	*14. listopadu 2001*	*GIMPS / Michael Cameron*
40	$2^{20\,996\,011}-1$	*6 320 430*	*17. listopadu 2003*	*GIMPS / Michael Shafer*
41	$2^{24\,036\,583}-1$	*7 235 733*	*15. května 2004*	*GIMPS / Josh Findley*
42	$2^{25\,964\,951}-1$	*7 816 230*	*18. února 2005*	*GIMPS / Martin Nowak*
43	$2^{30\,402\,457}-1$	*9 152 052*	*15. prosince 2005*	*GIMPS / Cooper & Boone*
44	$2^{32\,582\,657}-1$	*9 828 358*	*4. září 2006*	*GIMPS / Cooper & Boone*
45	$2^{37\,156\,667}-1$	*11 185 272*	*6. září 2008*	*GIMPS / H.-M. Elvenich*
46	$2^{42\,643\,801}-1$	*12 837 064*	*4. června 2009*	*GIMPS / Odd M. Strindmo*
47	$2^{43\,112\,609}-1$	*12 978 189*	*23. srpna 2008*	*GIMPS / Edson Smith*
48	$2^{57\,885\,161}-1$	*17 425 170*	*25. ledna 2013*	*GIMPS / Curtis Cooper*
49	$2^{74\,207\,281}-1$	*22 338 618*	*7. ledna 2016*	*GIMPS / Curtis Cooper*
50	$2^{77\,232\,917}-1$	*23 249 425*	*26. prosince 2017*	*GIMPS / Jon Pace*
51	$2^{82\,589\,933}-1$	*24 862 048*	*7. prosince 2018*	*GIMPS / Patrick Laroche*

Tabulka Mersennových prvočísel (https://www.mersenne.org/primes/)

2.2 Fermatova prvočísla

Pierre de Fermat (1601 – 1665), po němž jsou nazvána *Fermatova prvočísla*, byl francouzský matematik.

Nechť je dán předpis $F_m = 2^{2^m} + 1$, pro $m = 0, 1, 2, \ldots$.

Všechna čísla tohoto tvaru se nazývají Fermatova čísla. Pokud je číslo $2^{2^m} + 1$ navíc prvočíslo, pak ho nazveme Fermatovým prvočíslem.

Nyní se zaměříme opět na ověření prvočíselnosti Fermatových čísel.

m	F_m	*Je* F_m **prvočíslo?**
0	*3*	*Ano*
1	*5*	*Ano*
2	*17*	*Ano*
3	*257*	*Ano*
4	*65 537*	*Ano*
5	*4 294 967 297*	*Ne*

Z tabulky je patrné, že ne každé Fermatovo číslo je prvočíslem.

Pro $m = 5$ je $F_m = 641 \cdot 6\,700\,417$, což je číslo složené. Francouzský matematik Pierre de Fermat, po kterém jsou pojmenována Fermatova prvočísla, vyslovil nepravdivou domněnku, že všechna čísla tvaru $2^{2^m} + 1$ jsou prvočísla. Tuto domněnku však vyvrátil Leonhard Euler a v roce 1732 ukázal, že platí $641 | F_5$. (Halaš, 2014)

I přesto, že Fermatova čísla v oblasti prvočísel patří k nejznámějším, jejich prvočíselnost „se zdá být spíše výjimečnou vlastností, neboť $F_4 = 65\,537$ je dosud největší známé Fermatovo prvočíslo.“ (Halaš, 2014)

Při zkoumání Fermatových prvočísel je vhodné uvést nutnou podmínku k tomu, aby pro $n \in \mathbb{N}$ bylo číslo $2^n + 1$ prvočíslem. Z ní je patrné, proč Fermat volil exponenciální tvar exponentu n. (Křížek, 2018)

Věta 2.4

„Nechť n je přirozené číslo. Je-li $2^n + 1$ prvočíslo, pak $n = 2^m$ pro nějaké $m \in \{0, 1, 2, \ldots\}$.

Důkaz. Jestliže k je přirozené číslo a $l \geq 3$ liché, pak

$$2^{kl} + 1 = (2^k + 1)(2^{k(l-1)} - 2^{k(l-2)} + \cdots - 2^k + 1).$$

Odtud plyne, že číslo $2^n + 1$ je složené, je-li exponent n dělitelný lichým přirozeným číslem $l \geq 3$. Proto n musí být mocninou dvojky.“ (Michal Křížek, 2018)

□

Věta 2.5

Každé Fermatovo číslo F_m pro $m \geq 2$ končí cifrou 7.

Důkaz. Exponent 2^m nabývá tvaru $4k$ pro $m \geq 2$. ($k = 1, 2, 3, \ldots$)

Pak $F_m = 2^{4k} + 1 = (2^4)^k + 1 = 16^k + 1 \equiv 7 \bmod 10$.

□

Díky nynější pokročilé výpočetní technice a moderním matematickým metodám dnes již víme, že F_m je číslo složené pro $5 \leq m \leq 32$. Nevyřešeným problémem však dodnes zůstává, zda je množina Fermatových prvočísel konečná nebo nekonečná. Kvůli vysoké náročnosti faktorizace obrovských čísel, kterých posloupnost Fermatových čísel skutečně velmi rychle nabývá, je velmi obtížné rozhodovat o prvočíselnosti Fermatových čísel. (Křížek, 2018)

Německý matematik Carl Friedrich Gauss (1777 – 1855) dokázal větu, která objevuje senzační souvislost mezi geometrií a teorií čísel.

Gaussova věta

„*Pravidelný mnohoúhelník je eukleidovsky konstruovatelný (tj. pomocí kružítka a pravítka) tehdy a jen tehdy, když počet jeho vrcholů je roven číslu $k = 2^i p_1 p_2 \cdots p_j$, kde $i \geqq 0$, $j \geqq 0$, $k \geqq 3$ jsou celá čísla a $p_1 p_2 \cdots p_j$ navzájem různá Fermatova prvočísla.*“ (Křížek, 1995)

Z tohoto vztahu plyne, že pravidelný mnohoúhelník je eukleidovsky konstruovatelný pro $k = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots$ a není konstruovatelný pro $k = 7, 9, 11, \ldots$.

Staří Řekové si věděli rady s konstrukcí pravidelného pětiúhelníku, marně se však snažili narýsovat pravidelný sedmiúhelník či devítiúhelník. Díky důkazu *Gaussovy věty* dnes již víme, že právě tyto mnohoúhelníky pouze za pomoci pravítka a kružítka konstruovat nelze. Konstrukci pravidelného sedmnáctiúhelníku (pro $i = 0$, $j = 1$, $k = p_1 = 17$) ukázal sám Gauss. (Křížek, 1995)

2.3 Wieferichova prvočísla

Arthur Wieferich (1884 – 1954), po němž jsou nazvána *Wieferichova prvočísla*, byl německý matematik.

Malá Fermatova věta říká, že pro každé prvočíslo p je splněn vztah $2^{p-1} \equiv 1 \pmod{p}$. Číslo p nazveme Wieferichovým prvočíslem právě tehdy, je-li splněna kongruence $2^{p-1} \equiv 1 \pmod{p^2}$.

I přes fakt, že bylo provedeno široké počítačové hledání Wieferichových prvočísel až do hranice $4 \cdot 10^{12}$, zatím známe jen dvě prvočísla, která splňují Wieferichovu kongruenci $2^{p-1} \equiv 1 \pmod{p^2}$.

Jedná se o prvočísla $p = 1\,093$ a $p = 3\,511$. První z uvedených prvočísel bylo objeveno W. Meissnerem roku 1913 a druhé N. G. W. M. Beegerem o 9 let později roku 1922. (Křížek, 2018)

2.4 Prvočísla Sophie Germainové

Sophie Germain (1776 – 1831), po níž jsou nazvána *prvočísla Sophie Germainové*, byla francouzská matematička a fyzička.

Pokud čísla p a $2p + 1$ jsou obě prvočísla, pak p nazveme prvočíslem Sophie Germainové.

Najdeme všechna prvočísla Sophie Germainové, která jsou menší než 100.

p	***2p + 1***	***Je 2p + 1 prvočíslo?***
2	*5*	*Ano*
3	*7*	*Ano*
5	*11*	*Ano*
7	*15*	*Ne*
11	*23*	*Ano*
13	*27*	*Ne*
17	*35*	*Ne*
19	*39*	*Ne*
23	*47*	*Ano*
29	*59*	*Ano*
31	*63*	*Ne*
37	*75*	*Ne*
41	*83*	*Ano*
43	*87*	*Ne*
47	*95*	*Ne*
53	*107*	*Ano*
59	*119*	*Ne*
61	*123*	*Ne*
67	*135*	*Ne*
71	*143*	*Ne*
73	*147*	*Ne*
79	*159*	*Ne*
83	*167*	*Ano*
89	*179*	*Ano*
97	*195*	*Ne*

Z tabulky můžeme vidět, že posloupnost prvočísel Sophie Germainové není nijak pravidelná. Dále je zřejmé, že prvočíslo Sophie Germainové nemůže nikdy končit cifrou 7, protože by výsledné číslo $2p + 1$ končilo cifrou 5, a dle kritéria dělitelnosti číslem 5 by se pak jednalo o číslo složené.

Nejvyšší dosud známé prvočíslo Sophie Germainové bylo nalezeno v únoru 2016, obsahuje 388 342 cifer a jedná se o číslo $2\,618\,163\,402\,417 \cdot 2^{1\,290\,000} - 1$. (Caldwell)

Prvočísla Sophie Germainové velmi úzce souvisí s *bezpečnými prvočísly*, která se využívají v kryptografii. Pokud p a $2p + 1$ jsou prvočísla, pak $q = 2p + 1$ nazveme

bezpečným prvočíslem. Jelikož číslo q – 1 má velkého prvočíselného dělitele p a je tak obtížnější pro faktorizaci, zvyšují bezpečná prvočísla spolehlivost šifrování.

2.5 Eukleidova prvočísla

Eukleidés z Alexandrie (asi 323 př. n. l. – asi 285 př. n. l.), po němž jsou nazvána *Eukleidova prvočísla*, byl řecký matematik.

Definice Eukleidových prvočísel je založena na úvaze, která nám říká, že prvočísel existuje nekonečně mnoho. Tuto větu a její jednoduchý důkaz si nyní ukážeme. S touto úvahou přišel sám Eukleidés.

Věta 2.6

Prvočísel existuje nekonečně mnoho.

Důkaz. Důkaz provedeme sporem. Předpokládejme naopak, že prvočísel existuje jen konečné množství a označme je $p_1, p_2, \ldots p_n$. Vezměme číslo, které je součinem všech prvočísel, přičtěme k němu 1 a označme ho $S = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Dělíme-li S libovolným prvočíslem p_i, dostaneme vždy zbytek 1, tudíž žádné p_i nedělí S. Číslo S je tedy dalším prvočíslem, anebo S je složeným číslem, které je dělitelné prvočíslem různým od $p_1, p_2, \ldots, p_n$, což je spor. (Fuchs, 1993)

□

Avšak číslo S nemusí být nutně nové prvočíslo, jak bývá mnohdy špatně interpretováno. Věta 2.6 nám říká, že existuje nekonečné množství prvočísel a že součin prvočísel $p_1, p_2, \ldots, p_n$ zvětšený o 1 může být buď nové prvočíslo, nebo číslo složené, které není dělitelné žádným z prvočísel $p_1, p_2, \ldots, p_n$. Uvažujme konečnou posloupnost prvočísel 2, 3, 5, 7, 11, 13. Pak $S = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$, což je číslo složené.

Právě pro tuto Eukleidovu úvahu jsou prvočísla tvaru $S = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ nazývána Eukleidova prvočísla.

Uvedeme si prvních pět Eukleidových prvočísel.

i	$p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$	S
1	$2 + 1$	3
2	$2 \cdot 3 + 1$	7
3	$2 \cdot 3 \cdot 5 + 1$	31
4	$2 \cdot 3 \cdot 5 \cdot 7 + 1$	211
5	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$	2 311

Označíme-li P jako součin všech prvočísel menších nebo rovných p, pak P +1 je Eukleidovým prvočíslem pro p = 2, 3, 5, 7, 11, 31, 379, 1 019, 1 021, 2 657, 3 229, 4 547, 4 787, 11 549, … . Za zmínku také stojí zajímavost, že první tři Eukleidovská prvočísla jsou stejná, jako první tři Mersennova prvočísla. (Křížek, 2018)

2.6 Wilsonova prvočísla

John Wilson (1741 – 1793), po němž jsou nazvána *Wilsonova prvočísla*, byl britský matematik.

Pro zavedení definice Wilsonových prvočísel musíme nejdřív uvést větu, která nese jméno Johna Wilsona, avšak nebyl to on, kdo ji objevil.

Věta 2.7

Wilsonova věta. *„Číslo $p > 1$ je prvočíslo právě tehdy, když*

$$(p-1)! \equiv -1 \pmod{p}.\text{“}$$ (Michal Křížek, 2018)

Když zaměníme v kongruenci z věty 2.7 modul p za p^2, dostaneme definici Wilsonových prvočísel.

Pokud platí kongruence $(p-1)! \equiv -1 \pmod{p^2}$, pak p nazveme Wilsonovým prvočíslem.

Doposud známá Wilsonova prvočísla jsou 5, 13 a 563, která byla nalezena roku 1953 za pomocí raného elektronického počítače.

Podle heuristického argumentu by se čtvrté Wilsonovo prvočíslo mohlo vyskytovat kolem čísla $5 \cdot 10^{23}$, pokud vůbec další takové prvočíslo existuje. Je však jisté, že je větší než $5 \cdot 10^{8}$. (Wells, 2005)

2.7 Gaussova prvočísla

Johann Carl Friedrich Gauss (1777 – 1855), po němž jsou nazvána *Gaussova prvočísla*, byl významný německý matematik a fyzik.

Prvočísla můžeme definovat i na jiných algebraických strukturách, než je množina přirozených čísel. Pro zavedení definice Gaussových prvočísel nejprve musíme definovat Gaussova čísla, která definujeme v komplexní rovině jako součty $Z[i] = a + bi$, kde $a, b \in Z$, a i je imaginární jednotka. Jsou to tedy čísla v komplexní rovině, která mají celočíselné souřadnice. Koeficient a se nazývá *reálná část komplexního čísla Re*, koeficient b se nazývá *imaginární část komplexního čísla Im*.

Dokážeme, že množina Gaussových čísel spolu s operací sčítání tvoří *komutativní grupu*. Tuto množinu označme $Z[i]$. Aby množina $Z[i]$ společně s operací sčítání mohla být nazvána komutativní grupou, musí splňovat následující axiomy:

1) Operace sčítání je neomezeně definována na $Z[i]$:

$\forall\, x, y \in Z[i]; x + y \in Z[i]$.

Nechť $x = a + bi$; $a, b \in Z$, $y = c + di$; $c, d \in Z$. Máme dokázat, že $x + y \in Z[i]$.

$x + y = (a + bi) + (c + di) = (a + c) + (b + d)i \in Z[i]$, což jsme měli dokázat.

2) Struktura je asociativní:

$\forall\, x, y, z \in Z[i]; x + (y + z) = (x + y) + z$.

Nechť $x = a + bi$; $a, b \in Z$, $y = c + di$; $c, d \in Z$, $z = f + gi$; $f, g \in Z$.

Máme dokázat, že $x + (y + z) = (x + y) + z$.

$x + (y + z) = (a + bi) + [(c + di) + (f + gi)] = (a + bi) + [(c + f) + (d + g)i] = (a + c + f) + (b + d + g)i = [(a + c) + (b + d)i] + (f + gi) = [(a + bi) + (c + di)] + (f + gi) = (x + y) + z,$ čímž jsme rovnost dokázali.

3) Existuje neutrální prvek vzhledem k operaci sčítání:

$\exists\, e \in Z[i]; \forall\, x \in Z[i]; x + e = e + x = x.$

Ukážeme, že neutrálním prvkem je $e = 0 + 0i$. Nechť x je libovolné Gaussovo číslo, pak má tvar $x = a + bi$.

$x + e = a + bi + 0 + 0i = (a + 0) + (b + 0)i = a + bi = x$

$e + x = 0 + 0i + a + bi = (0 + a) + (0 + b)i = a + bi = x$

Tím je existence neutrálního prvku pro sčítání dokázána.

4) Ke každému prvku existuje inverzní prvek vzhledem k operaci sčítání:

$\forall\, x \in Z[i]; \exists\, n \in Z[i]; x + n = n + x = e.$

Ukážeme, že ke každému prvku x existuje inverzní prvek n, který je prvkem opačným k x. Nechť x je libovolné Gaussovo číslo a n je číslo k němu opačné. Pak mají tvar $x = a + bi$ a $n = -a - bi$.

$x + n = a + bi + (-a - bi) = a + bi - a - bi = (a - a) + (b - b)i = 0 + 0i = e$

$n + x = -a - bi + a + bi = (-a + a) + (-b + b)i = 0 + 0i = e$

Tím je existence inverzních prvků pro sčítání na celé množině dokázána.

5) Struktura je komutativní:

$\forall\, x, y \in Z[i]; x + y = y + x.$

Nechť $x = a + bi$; $a, b \in Z$, $y = c + di$; $c, d \in Z$. Máme dokázat, že $x + y = y + x$.

$x + y = a + bi + c + di = c + di + a + bi = y + x$

□

Tím jsme dokázali komutativnost. Struktura splňující axiomy 1 – 4 se nazývá grupa, je-li navíc splněn axiom 5, pak hovoříme o *komutativní (Abelově) grupě*.

Množina Gaussových čísel $Z[i]$ spolu s operací násobení tvoří *monoid*. Aby Množina $Z[i]$ spolu s operací násobení mohla být nazvána monoidem, musí splňovat následující axiomy:

1) Operace násobení je neomezeně definována na $Z[i]$:

$\forall\, x, y \in Z[i]; x \cdot y \in Z[i]$.

Nechť $x = a + bi$; $a, b \in Z$, $y = c + di$; $c, d \in Z$. Máme dokázat, že $x \cdot y \in Z[i]$.

$x \cdot y = (a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = ac + adi + bci - bd = (ac - bd) + (ad + bc)i \in Z[i]$, což jsme měli dokázat.

2) Struktura je asociativní:

$\forall\, x, y, z \in Z[i]; x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Nechť $x = a + bi$; $a, b \in Z$, $y = c + di$; $c, d \in Z$, $z = f + gi$; $f, g \in Z$.

$x \cdot (y \cdot z) = (a + bi) \cdot [(c + di) \cdot (f + gi)] = (a + bi) \cdot (cf + cgi + dfi - dg) = (a + bi) \cdot [(cf - dg) + (cg + df)i] = a(cf - dg) + a(cg + df)i + b(cf - dg)i - b(\mathrm{cg} + df) = acf - adg + acgi + adfi + bcfi - bdgi - bcg - bdf = f(ac - bd) + f(ad + bc)i + g(ac - bd)i - g(ad + bc) = [(ac - bd) + (ad + bc)i] \cdot (f + gi) = (ac + adi + bci - bd) \cdot (f + gi) = [(a + bi) \cdot (c + di)] \cdot (f + gi) = (x \cdot y) \cdot z$, čímž jsme rovnost dokázali.

3) Existuje neutrální prvek vzhledem k operaci sčítání:

$\exists\, e \in Z[i] - \{0 + 0i\}; \forall\, x \in Z[i]; x \cdot e = e \cdot x = x$.

Ukážeme, že neutrálním prvkem je $e = 1 + 0i$. Nechť x je libovolné Gaussovo číslo, pak má tvar $x = a + bi$.

$x \cdot e = (a + bi) \cdot (1 + 0i) = a + bi = x$

$e \cdot x = (1 + 0i) \cdot (a + bi) = a + bi = x$

Tím je existence neutrálního prvku pro násobení dokázána.

Ukážeme, že struktura nesplňuje axiom o existenci inverzního prvku.

Má platit, že $\forall\, x \in Z[i] - \{0 + 0i\}; \exists\, n \in Z[i]; x \cdot n = n \cdot x = e$, tj. ke každému prvku x existuje inverzní prvek n takový, že $x \cdot n = n \cdot x = e$.

Ukážeme, že pro prvek $1 + 2i \in Z[i]$ neexistuje inverzní prvek n, který $\in Z[i]$. Nechť inverzní prvek $n = a + bi$. Má platit, že $(1 + 2i) \cdot (a + bi) = 1 + 0i$.

$(1 + 2i) \cdot (a + bi) = 1 + 0i$

$a + bi + 2ai + 2bi^2 = 1 + 0i$

$a + bi + 2ai - 2b = 1 + 0i$

$(a - 2b) + (2a + b) = 1 + 0i$, z této rovnice dostáváme soustavu dvou rovnic o dvou neznámých.

$a - 2b = 1$

$2a + b = 0$

Z této soustavy dostáváme řešení $a = \frac{1}{5}$ a $b = -\frac{2}{5}$.

Pak ale $\frac{1}{5} - \frac{2}{5}i \notin Z[i]$. Ukázali jsme, že prvek $1 + 2i$ nemá v $Z[i]$ inverzní prvek. Jelikož axiom o existenci inverzního prvku má platit pro všechny prvky, není tento axiom pro množinu $Z[i]$ spolu s operací násobení platný.

Tím jsme dokázali, že Gaussova čísla spolu s operací násobení tvoří *monoid*.

□

Velikost komplexního čísla $z = a + bi$ je dána vztahem $|z| = \sqrt{a^2 + b^2}$.

Nyní už nic nebrání tomu, abychom si uvedli definici Gaussových prvočísel.

„Jestliže číslo $z = a + bi$ splňuje jednu z následujících podmínek, pak ho nazveme Gaussovým prvočíslem.

1. *$a^2 + b^2$ je prvočíslo pro $a \neq 0$ a zároveň $b \neq 0$, nebo*
2. *$|z|$ je prvočíslo tvaru $4k - 1$ pro $a = 0$ nebo $b = 0$.“* (Michal Křížek, 2018)

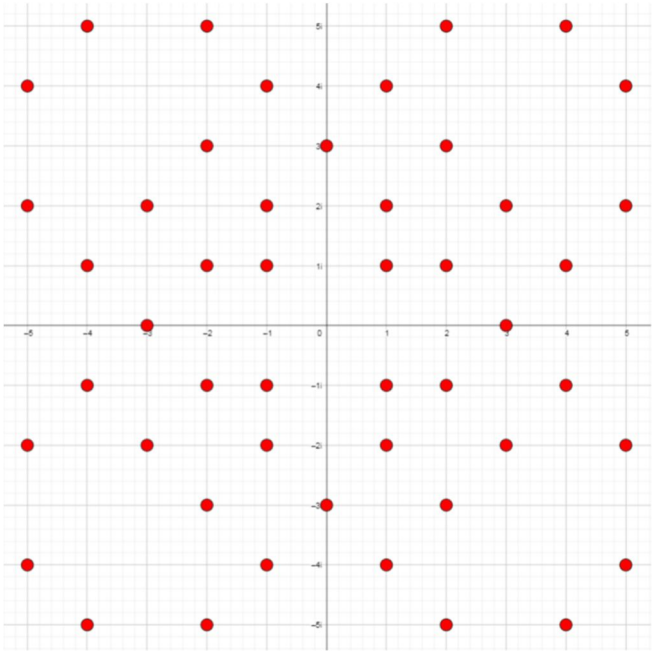
Z této definice vyplývá následující tvrzení:

Pokud $z = a + bi$ je Gaussovo prvočíslo, pak $z_1 = \pm a \pm bi$ a $z_2 = \pm b \pm ai$ jsou rovněž Gaussova prvočísla.

Reálné prvočíslo se v Gaussově oboru rozkládá právě tehdy, pokud ho můžeme zapsat jako součet dvou čtverců. Pojďme si toto tvrzení ukázat na jednoduchém příkladu. Vezměme reálné prvočíslo 2, které se zcela jednoznačně dá zapsat jako součet dvou čtverců $1^2 + 1^2 = 2$. Rozklad v Gaussově oboru je pak $2 = (1 + i)(1 - i)$. Oba činitelé jsou Gaussovými prvočísly.

Zaměříme se na další prvočíslo v pořadí, kterým je prvočíslo 3. Toto číslo se nedá zapsat jako součin dvou čtverců, nedá se tedy v Gaussově oboru rozložit, avšak splňuje druhou podmínku z definice, protože je ve tvaru $4k - 1$. Tudíž 3 je Gaussovo prvočíslo.

Na obrázku si ukážeme všechna Gaussova prvočísla, pro které platí $Re \leq 5$ a zároveň $Im \leq 5$.



Z obrázku je patrné, že rozložení Gaussových prvočísel v Gaussově rovině tvoří středově souměrný útvar se středem souměrnosti v bodě [0, 0].

Každé Mersennovo prvočíslo je zároveň Gaussovým prvočíslem, proto je největším známým Gaussovým prvočíslem prvočíslo $2^{82\,589\,933} - 1$, které je z oboru reálných prvočísel, zároveň se však nedá v Gaussově oboru rozložit na součin, tudíž spadá i do oboru Gaussových prvočísel. (Křížek, 2018)

2.8 Cullenova prvočísla

James Cullen (1867 – 1933), po něž jsou nazvána *Cullenova prvočísla*, byl irský matematik a katolický kněz.

Čísla ve tvaru $C_n = n \cdot 2^n + 1$ se nazývají Cullenova čísla. Pokud je C_n prvočíslo, pak ho nazveme Cullenovým prvočíslem.

Nejmenší Cullenovo prvočíslo je $C_1 = 3$ pro $n = 1$. Cullenova prvočísla jsou pro malá n velice vzácná, poněvadž další takové prvočíslo máme až pro $n = 141$.

Ukázalo se, že téměř všechna Cullenova čísla jsou složená, přesto je tu stále nevyřešená domněnka, zda existuje nekonečně mnoho Cullenových prvočísel. Zrovna tak nevíme, zda existuje nějaké prvočíslo C_n takové, že $n = p$, kde p je libovolné prvočíslo. Dosud známe šestnáct Cullenových prvočísel, které si uvedeme v tabulce.

#	Prvočíslo	Počet cifer
1	$1 \cdot 2^1 + 1$	1
2	$141 \cdot 2^{141} + 1$	45
3	$4\,713 \cdot 2^{4\,713} + 1$	1 423
4	$5\,795 \cdot 2^{5\,795} + 1$	1 749
5	$6\,611 \cdot 2^{6\,611} + 1$	1 994
6	$289 \cdot 2^{18\,502} + 1$	5 573
7	$8\,073 \cdot 2^{32\,294} + 1$	9 726
8	$32\,469 \cdot 2^{32\,469} + 1$	9 779
9	$7\,457 \cdot 2^{59\,659} + 1$	17 964
10	$90\,825 \cdot 2^{90\,825} + 1$	27 347
11	$262\,419 \cdot 2^{262\,419} + 1$	79 002
12	$361\,275 \cdot 2^{361\,275} + 1$	108 761
13	$481\,899 \cdot 2^{481\,899} + 1$	145 072
14	$338\,707 \cdot 2^{1\,354\,830} + 1$	407 850
15	$1\,582\,137 \cdot 2^{6\,328\,550} + 1$	1 905 090
16	$6\,679\,881 \cdot 2^{6\,679\,881} + 1$	2 012 852

Můžeme si všimnout, že ne každé prvočíslo uvedené v tabulce je ve tvaru $C_n = n \cdot 2^n + 1$. Dají se však převést na kanonický tvar. Například prvočíslo $1\,582\,137 \cdot 2^{6\,328\,550} + 1 = 6\,328\,548 \cdot 2^{6\,328\,548} + 1$. Uvedená prvočísla se vztahují pro

n = 1, 141, 4 713, 5 795, 6 611, 18 496, 32 292, 32 469, 59 656, 90 825, 262 419, 361 275, 481 899, 1 354 828, a 6 679 881.

Čísla tvaru $C_n = n \cdot b^n + 1$ nazveme zobecněná Cullenova čísla. Dostáváme tak další možnosti hledání prvočísel pro $b \in N - \{1\}$. (Caldwell)

2.9 Woodallova prvočísla

Herbert James Woodall (1893 – 1981), po němž jsou nazvána *Woodallova prvočísla*, byl britský matematik. Tato čísla s ním mimo jiné zkoumal i další britský matematik Allan Joseph Champneys Cunningham.

Čísla tvaru $W_n = n \cdot 2^n - 1$ se nazývají Woodallova čísla, někdy též pro svůj tvar Cullenova čísla druhého druhu. Pokud je W_n prvočíslo, pak ho nazveme Woodallovým prvočíslem.

Četnost Woodallových prvočísel pro malé n je poněkud vyšší, než je tomu u Cullenových prvočísel. O prvočísla se jedná, pokud n = 2, 3, 6, 30, 75, 81, 115, 123, 249, 362, 384, 462, 512, 751, 822, 5 312, 7 755, 9 531, 12 379, 15 822 a 18 885. Další čísla pro $n \leq 20\,000$ jsou složená. I zde panuje domněnka, že těchto prvočísel je nekonečně mnoho.

V tabulce si uvedeme pět největších dosud známých Woodallových prvočísel, přičemž některé z nich opět nejsou v kanonickém tvaru $W_n = n \cdot 2^n - 1$, ale dají se na tento tvar převést. Největší Woodallovo prvočíslo bylo nalezeno poměrně nedávno, a to v březnu roku 2018.

Pořadí	***Prvočíslo***	***Počet cifer***
1	$8\,508\,301 \cdot 2^{17\,016\,603} - 1$	*5 122 515*
2	$938\,237 \cdot 2^{3\,752\,950} - 1$	*1 129 757*
3	$1\,183\,953 \cdot 2^{2\,367\,907} - 1$	*712 818*
4	$251\,749 \cdot 2^{2\,013\,995} - 1$	*606 279*
5	$1\,467\,763 \cdot 2^{1\,467\,763} - 1$	*441 847*

Mersennovo prvočíslo $2^{521} - 1$ je zároveň Woodallovo prvočíslo, protože se dá převést na tvar $512 \cdot 2^{512} - 1$.

I zde se dá zkoumat obecnější tvar. Čísla tvaru $n \cdot b^n - 1$, kde $b \in N - \{1\}$, nazýváme zobecněná Woodallova prvočísla. (Wells, 2005), (Cadwell)

2.10 Wagstaffova prvočísla

Samuel Standfield Wagstaff Jr. (narozen roku 1945), po němž jsou nazvána *Wagstaffova prvočísla*, je americký matematik.

Nechť je dán předpis $q = \frac{2^p+1}{3}$, kde p je liché prvočíslo. Číslo q nazveme Wagstaffovo číslo. Pokud je navíc prvočíslo, pak ho nazveme Wagstaffovo prvočíslo.

Zkusíme si tento vztah ověřit pro několik prvních prvočísel.

Prvočíslo p	***Wagstaffovo číslo q***	***Je q prvočíslo?***
3	*3*	*Ano*
5	*11*	*Ano*
7	*43*	*Ano*
11	*683*	*Ano*

Pro první čtyři lichá prvočísla vztah platí. Mylně bychom však usuzovali, že to platí pro všechna prvočísla. Prvním prvočíslem, které negeneruje Wagstaffovo prvočíslo, je číslo 29. Pro která prvočísla tento vztah tedy platí?

K říjnu roku 2014 byla známa tato prvočísla p, která generují Wagstaffova prvočísla q: 3, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 79, 101, 127, 167, 191, 199, 313, 347, 701, 1 709, 2 617, 3 539, 5 807, 10 501, 10 691, 11 279, 12 391, 14 479, 42 737, 83 339.

Toto jsou všechny známé exponenty p, které generují Wagstaffova prvočísla. Máme tu však i další, u kterých prvočíselnost není dokázána, ovšem v některých zahraničních dokumentech se uvádí jako možná Wagstaffova prvočísla. Uvedeme si tři největší.

Prvočíslo $\frac{2^{4\,031\,399}+1}{3}$, které obsahuje 1 213 572 cifer, je třetím největším možným prvočíslem tohoto typu. Objevil ho v únoru 2010 Tony Reix.

Prvočísla $\frac{2^{13\,347\,311}+1}{3}$ a $\frac{2^{13\,372\,531}+1}{3}$, která byla objevena v září 2013 Ryanem Propperem, jsou dvě největší možná Wagstaffova prvočísla, z nichž druhé uvedené je vůbec největší. Obě obsahují více jak 4 000 000 cifer.

Není však jisté, zda mezi prvočísly 4 031 399 a 13 347 311 neexistuje další prvočíselný exponent, který by produkoval další možné Wagstaffovo prvočíslo.

Tato prvočísla mají uplatnění v kryptografii. (Marshall)

3 Další speciální typy prvočísel

První oddíl hlavní části byl zaměřen na speciální typy prvočísel, které nesou názvy slavných matematiků. Nyní se zaměříme na prvočísla, která jsou speciální pro svou určitou specifickou vlastnost.

3.1 Faktoriální prvočísla

Na začátek si připomeneme pár vlastností *faktoriálu*.

Nechť n je přirozené číslo. Výrazem $n!$ rozumíme součin přirozených čísel menších nebo rovno n.

Matematicky pak $n! = \prod_{k=1}^{n} k$. Například $5! = \prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$.

K ucelení definice je ještě potřeba definovat $0! = 1$.

Faktoriály se pak nejčastěji používají v kombinatorice, kde kombinační číslo je definováno jako $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ pro $n \geq k \geq 0$.

Nyní už ale k samotným prvočíslům.

Faktoriální prvočísla jsou prvočísla tvaru $n! \pm 1$.

Při variantě $n! + 1$ dostáváme prvočísla pro n = 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, 1 477, 6 380, 26 951 … .

Druhý výraz $n! - 1$ je prvočíselný pro n = 3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, 1 963, 3 507, 3 610, 6 917, 21 480, 34 790 … . (Wells, 2005)

Uvedeme deset největších dosud známých faktoriálních prvočísel.

Pořadí	***Prvočíslo***	***Počet cifer***	***Doba nalezení***
1	*208 003! – 1*	*1 015 843*	*Červenec 2016*
2	*150 209! + 1*	*712 355*	*Říjen 2011*
3	*147 855! – 1*	*700 177*	*Září 2013*
4	*110 059! + 1*	*507 082*	*Červen 2011*
5	*103 040! – 1*	*471 794*	*Prosinec 2010*
6	*94 550! – 1*	*429 390*	*Říjen 2010*
7	*34 790! – 1*	*142 891*	*Květen 2002*
8	*26 951! + 1*	*107 707*	*Květen 2002*
9	*21 480! – 1*	*83 727*	*Září 2001*
10	*6 917! – 1*	*23 560*	*Říjen 1998*

Tabulka největších faktoriálních prvočísel (Caldwell)

Ukázalo se, že některé faktoriálové sumy dávají prvočíslo.

Sumy v této posloupnosti generují prvočísla.

$n = 3$ $3! - 2! + 1! = \mathbf{5}$

$n = 4$ $4! - 3! + 2! - 1! = \mathbf{19}$

$n = 5$ $5! - 4! + 3! - 2! + 1! = \mathbf{101}$

$n = 6$ $6! - 5! + 4! - 3! + 2! - 1! = \mathbf{619}$

$n = 7$ $7! - 6! + 5! - 4! + 3! - 2! + 1! = \mathbf{4\,421}$

$n = 8$ $8! - 7! + 6! - 5! + 4! - 3! + 2! - 1! = \mathbf{35\,899}$

Pro $n = 10$ dostaneme také prvočíslo, avšak pro $n = 9$ vychází suma $326\,981 = 79 \cdot 4\,139$, což je číslo složené.

Od $n = 11$ do $n = 28$ máme pouze další dvě prvočísla, a tak to vypadá, že čím více budeme n zvyšovat, tím méně se budeme setkávat s prvočísly těchto sum. (Wells, 2005)

Na začátku jsme uvedli pojem faktoriál. Jelikož se pohybujeme v oblasti prvočísel, bylo by vhodné uvést pojem *primoriál*, který je spjatý právě s prvočísly.

Zatímco faktoriál je součin přirozených čísel menších nebo rovno *n,* primoriál je součin prvočísel menších nebo rovno *n*. To znamená, že ze součinu vyřadíme všechna čísla složená.

Primoriál

$n\# \equiv \prod_{i=1}^{\pi(n)} p_i$,

kde $\pi(n)$ je prvočíselná funkce, která udává počet prvočísel menších než *n.*

Například 14# = 2 · 3 · 5 · 7 · 11 · 13 = 30 030.

Primoriál se dá definovat i jako součin prvních *n* prvočísel.

$p_n\# \equiv \prod_{k=1}^{n} p_k$. (Weisstein)

Uvedeme si několik prvních členů posloupnosti primoriálu podle druhé definice.

n	***p_n#***	***Výsledek***
1	*2*	*2*
2	*2 · 3*	*6*
3	*2 · 3 · 5*	*30*
4	*2 · 3 · 5 · 7*	*210*
5	*2 · 3 · 5 · 7 · 11*	*2 310*
6	*2 · 3 · 5 · 7 · 11 · 13*	*30 030*

Dvojitý faktoriál čísla *n* rozumíme výraz *n*!! = *n*(*n* – 2)(*n* – 4) …, trojitý faktoriál čísla *n* je pak výraz *n*!!! = *n*(*n* – 3)(*n* – 6) … . Největší známé prvočíslo tvaru *n*!! – 1 je 9682!! – 1. Pro tvar *n*!!! – 1 známe nejvyšší prvočíslo 34 706!!! – 1. Dvojitý a trojitý faktoriál řadíme mezi takzvané multifaktoriály. (Wells, 2005)

3.2 Palindromická prvočísla

Palindrom (z řeckého *palindromos* "běžet opět nazpátek") je posloupnost znaků, která se čte zleva doprava stejně jako zprava doleva.

Příklady palindromických slov: Kajak, krk, radar, tahat.

Příklady palindromických vět: V elipse spí lev. Kája má maják. Nebude duben.

Zřejmě nejznámějším palindromem v českých zemích je číslo 135 797 531, které je spjato s položením základního kamene Karlova mostu podle juliánského kalendáře v roce 1357 dne 9. 7. v 5 hodin a 31 minut.

Palindromické prvočíslo je prvočíslo, které je zároveň palindromem.

Všechna jednociferná prvočísla 2, 3, 5, 7 jsou palindromy.

Z dvojciferných prvočísel je palindromem pouze prvočíslo 11.

Trojciferných palindromických prvočísel máme patnáct. Jedná se o prvočísla 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919 a 929.

Další prvočíselné palindromy pokračují až pěticiferným prvočíslem 10 301. Žádné čtyřciferné prvočíslo není palindrom, dokonce platí následující věta.

Věta 3.1

„Jediné palindromické prvočíslo se sudým počtem cifer je číslo 11.

Důkaz. Nechť číslo m = 9090…90 má 2k cifer. Vidíme, že

$$m \cdot 11 = 99999\ldots990,$$

a tudíž platí

$$11(m + 1) = 11m + 11 = 10^{2k+1} + 1. \qquad (3.1)$$

Uvažujme nyní palindromické číslo p se sudým počtem cifer 2n ve tvaru

$p = a_1 10^{2n-1} + a_2 10^{2n-2} + \cdots + a_2 10 + a_1$, *kde* $a_1 \neq 0$, $a_2, \ldots, a_n$ *jsou desítkové cifry.*

Odtud plyne, že

$$p = a_1(10^{2n-1} + 1) + a_2(10^{2n-2} + 10) + \cdots + a_n(10^n + 10^{n-1}) =$$

$$= a_1(10^{2n-1} + 1) + 10a_2(10^{2n-3} + 1) + \cdots + 10^{n-1}a_n(10 + 1).$$

Podle (3.1) jsou ale všechny členy dělitelné 11, a proto palindrom p se sudým počtem cifer je vždy složené číslo, pokud je p > 11.“ (Křížek, 2018)

□

Uvedeme si tři největší dosud známá palindromická prvočísla.

Pořadí	***Prvočíslo***	***Počet cifer***
1	$10^{474\,500} + 999 \cdot 10^{237\,249} + 1$	*474 501*
2	$10^{390\,636} + 999 \cdot 10^{195\,317} + 1$	*390 637*
3	$10^{362\,600} + 666 \cdot 10^{181\,299} + 1$	*362 601*

3.3 Cyklická a permutační prvočísla

Nejprve si řekneme něco k permutacím.

Permutací množiny M rozumíme každé bijektivní zobrazení množiny M na sebe. Uvažme třeba množinu $M = \{a, b, c\}$. Potom zobrazení f, pro které platí $f(a) = c$, $f(b) = a$, $f(c) = b$ je permutací.

Permutace množiny M je tedy uspořádání jejích prvků, kdy pro každou možnost využíváme všechny prvky z množiny M.

Počet všech možných permutací je $P(n) = n! = n \cdot (n - 1) \cdot (n - 2) \cdot \ldots \cdot 2 \cdot 1$.

Cyklická permutace množiny M je pak takové uspořádání, kdy její prvky tvoří nějaký cyklus. Mějme permutaci $(a_1, a_2, \ldots, a_n)$. Pak cyklické permutace tvaru $(a_1, a_2, \ldots, a_n)$, $(a_2, a_3, \ldots, a_n, a_1)$, …, $(a_n, a_1, \ldots, a_{n-2}, a_{n-1})$ představují stejnou cyklickou permutaci.

Ukážeme si princip cyklické permutace na jednoduchém příkladu a následně odvodíme vzorec.

Př. Kolika způsoby lze posadit n lidí ke kulatému stolu?

Na první židli máme na výběr n možností, na druhou židli máme $n - 1$ možností a tak dále. Těchto permutací je tedy $n \cdot (n - 1) \cdot \ldots \cdot 2 \cdot 1$. Ovšem při každé permutaci máme n možností, jak v dané permutaci mohou lidé rotovat, tudíž počet permutací bude n-krát menší. Způsobů, jak lze posadit n lidí ke stolu, a tedy počet cyklických permutací je $\frac{n \cdot (n - 1) \cdot (n - 2) \cdot \ldots \cdot 2 \cdot 1}{n} = = (n - 1) \cdot (n - 2) \cdot \ldots \cdot 2 \cdot 1 = (n - 1)!$

Prvočíslo nazveme *cyklické*, jestliže libovolná cyklická permutace jeho cifer dává opět prvočíslo.

Například číslo 3 779 je permutační prvočíslo, protože 3 779, 7 793, 7 937, 9 377 jsou prvočísla.

Další cyklická prvočísla jsou 2, 3, 5, 7, 13, 17, 37, 79, 113, 199, 337 a všechna prvočísla složená z jedniček. Například 11, 1 111 111 111 111 111 111, 11 111 111 111 111 111 111 111.

Prvočíslo nazveme *permutační*, pokud libovolná permutace jeho cifer dává opět prvočíslo. Oproti cyklickým prvočíslům požadujeme, aby byly všechny permutace prvočísly, kdežto u cyklických permutujeme pouze cifry v daném pořadí dokola. Permutačních prvočísel tak bude logicky méně, vypíšeme si všechna dosud známá: 2, 3, 5, 7, 11, 13, 17, 37, 79, 113, 199, 337 a všechna prvočísla složená z jedniček.

3.4 Siamská prvočísla

Krátce se zmíníme i o prvočíslech, která se nazývají siamská. *Siamská prvočísla* byla takto pojmenována v článku (Beauregard, Suryanarayan, 2001). Jedná se o dvojice čísel tvaru $n^2 - 2$ a $n^2 + 2$. Jsou to tedy dvojice prvočísel, které mezi sebou mají vzdálenost čtyři.

Uvedeme si několik prvních dvojic této posloupnosti:

(7, 11), (79, 83), (223, 227), (439, 443), (1 087, 1 091), (13 687, 13 691). (Křížek, 2018)

3.5 Jedinečná prvočísla

Dalšími prvočísly, kterými se budeme zabývat, jsou *jedinečná prvočísla*.

Pojďme se tedy podívat, co se za jejich jedinečností skrývá. Nechť p je prvočíslo, pak výraz $\frac{1}{p}$ nazveme *převrácenou hodnotou* prvočísla p.

Prvočíslo $p \notin \{2, 5\}$ nese název *jedinečné*, pokud neexistuje jiné prvočíslo q, jehož převrácená hodnota $\frac{1}{q}$ by měla stejně dlouhou periodu jako $\frac{1}{p}$.

U jedinečných prvočísel vyřazujeme prvočísla 2 a 5, protože jsou to dvě jediná prvočísla, jejichž převrácené hodnoty nemají nekonečný desetinný rozvoj. Ostatní převrácené hodnoty prvočísel mají nekonečný periodický desetinný rozvoj.

Uvedeme si prvních devět jedinečných prvočísel a jejich délky period.

Jedinečné prvočíslo	***Délka periody***
3	*1*
11	*2*
37	*3*
101	*4*
9 091	*10*
9 901	*12*
333 667	*9*
909 091	*14*
99 990 001	*24*

Můžeme si všimnout, že existují převrácené hodnoty prvočísel, které mají délku periody 1, 2, 3 a 4. Tato posloupnost číslem 5 dále nepokračuje, protože periody převrácených hodnot prvočísel 41 a 271 mají délku 5. A to konkrétně:

$$\frac{1}{41} = 0.\overline{02439}, \frac{1}{271} = 0.\overline{00369}.$$

Prvočísla 41 a 271 tedy nejsou jedinečná. Zrovna tak čísla $\frac{1}{7}$ a $\frac{1}{13}$ mají obě délku periody 6, tudíž 7 a 13 se taktéž neřadí mezi jedinečná prvočísla. (Křížek, 2018)

3.6 Pandigitální prvočísla

Pandigitální číslo je takové číslo, které ve svém zápisu obsahuje všechny cifry ze své číselné soustavy. Pokud se pohybujeme v dekadické soustavě, pak se jedná o cifry 0 – 9. Protože je těchto cifer deset, musí i nejmenší pandigitální číslo obsahovat ve svém zápisu nejméně deset cifer, přičemž nesmí začínat číslicí 0, protože by se pak

nejednalo o platnou číslici v číselném zápisu. Nejmenším pandigitálním číslem je tedy číslo 1 023 456 789.

Existuje i takové pandigitální číslo, v jehož zápisu se číslice neopakují, a jeho prvních *n* cifer dá takové číslo, které je dělitelné *n*. Tímto číslem je 3 816 547 290. V tabulce ukážeme, že tato vlastnost skutečně platí. Termín "*prvních n cifer*" označíme symbolem *N*.

n	***N***	***Podíl N/n***
1	*3*	*3*
2	*38*	*19*
3	*381*	*127*
4	*3 816*	*954*
5	*38 165*	*7 633*
6	*381 654*	*63 609*
7	*3 816 547*	*545 221*
8	*38 165 472*	*4 770 684*
9	*381 654 729*	*42 406 081*
10	*3 816 547 290*	*381 654 729*

Pandigitální číslo, které je navíc prvočíslem, se nazývá *pandigitální prvočíslo*.

Číslice 0 – 9 nelze uspořádat tak, aby vzniklo prvočíslo. Je to dáno tím, že součet těchto číslic je 45, což je dělitelné třemi. Abychom tedy měli možnost dostat prvočíslo, musíme přidat další cifru. Nejmenší pandigitální prvočíslo tedy obsahuje nejméně jedenáct cifer.

Uvedeme si několik nejmenších pandigitálních prvočísel: 10 123 457 689, 10 123 465 789, 10 123 465 897, 10 123 485 679, 10 123 485 769 … .

Pokud bychom definici upravili a vynechali bychom číslici 0, pak by nejmenším takovým prvočíslem bylo číslo 1 123 465 789.

Bylo objeveno prozatím nejmenší prvočíslo takové, které je pandigitální a zároveň palindromické. Jedná se o číslo 1 023 456 987 896 543 201 a na tomto objevu mají zásluhy Dubner a Ondrejka. (Wells, 2005)

3.7 Poloprvočísla

Nechť je dáno číslo $k \in N$. Pokud číslo k má pouze dva prvočíselné dělitele, pak se řadí mezi *poloprvočísla*.

Nejmenší poloprvočíslo je číslo 4, dále tato posloupnost pokračuje následovně: 6, 9 10, 14, 15, 21, 22, 25, 26, 33, 34, 35, 38, 39, 46, 49, 51, 55, … . Můžeme si povšimnout, že ve zmiňovaném výčtu se vyskytují poloprvočíselné páry, někdy i poloprvočíselné trojice. Jedná se o dvě, případně o tři po sobě jdoucí poloprvočísla.

Uvedeme si poloprvočíselné páry a trojice až do čísla 150.

Poloprvočíselné páry

9-10, 14-15, 21-22, 25-26, 38-39, 57-58, 118-119, 122-123, 133-134, 145-146.

Poloprvočíselné trojice

33-34-35, 85-86-87, 93-94-95, 141-142-143.

Pokud bychom požadovali, aby poloprvočíselný pár měl různé prvočíselné dělitele, pak první takový pár je 14 - 15. První po sobě jdoucí pár se třemi odlišnými prvočíselnými děliteli je 230 - 231. Číslo 230 je po rozložení na součin prvočísel $2 \cdot 5 \cdot 23$ a číslo 231 pak $3 \cdot 7 \cdot 11$.

Čtyři po sobě jdoucí poloprvočísla nemůžou existovat, protože jedno z nich bude dělitelné čtyřmi, tudíž bude mít nejméně tři prvočíselné dělitele.

Existuje 299 poloprvočísel, která jsou menší než 1 000. (Wells, 2005)

3.8 Sexy prvočísla

Nechť p je prvočíslo. Pokud $p + 6$ je také prvočíslo, pak p a $p + 6$ nazveme *sexy prvočísly*.

Jsou to tedy prvočísla, která jsou od sebe vzdálena o šest.

Název "*sexy*" vznikl zkomolením číslice 6, což se v angličtině nebo v latině překládá jako "*six*", odkud už k překroucení výslovnosti na slovo "*sex*" není daleko. Obzvlášť, pokud se toto slovo dostane do úst školáků.

Uvedeme si posloupnost dvojic sexy prvočísel až do čísla 200: 5-11, 11-17, 13-19, 17-23, 23-29, 31-37, 37-43, 47-53, 53-59, 61-67, 67-73, 73-79, 83-89, 97-103, 103-109, 107-113, 131-137, 151-157, 157-163, 167-173, 173-179, a 191-197.

Mezi těmito dvojicemi je deset dvojic tvaru $6n + 1$ a 12 dvojic tvaru $6n - 1$.

Posloupnost trojic sexy prvočísel začíná 7-13-19, 17-23-29, 31-37-43, 47-53-59… .

Z posloupnosti prvočíselných čtveřic uvedeme také prvních pár členů: 5-11-17-23, 11-17-23-29, 41-47-53-59, 61-67-73-79 … .

Pokud se zaměříme na pětice sexy prvočísel, existuje pouze jedna, a to 5-11-17-23-29, což si následně dokážeme.

Věta 3.2

"*Neexistují žádné další pětice sexy prvočísel kromě 5-11-17-23-29.*"

Důkaz. Nechť n je přirozené číslo. Uvažme další čtyři přirozená čísla, která jsou od n vzdálena postupně o šest. Posloupnost těchto čísel je n, $n + 6$, $n + 12$, $n + 18$, $n + 24$.

Zaměříme se na zbytek po dělení číslem 5. Mohou nastat tyto případy:

1) n je dělitelné 5, tudíž n je buď 5, nebo číslo složené.

2) $n \equiv 4 \bmod 5$, pak $n + 6 \equiv 10 \bmod 5$, tudíž n + 6 je dělitelné 5.

3) $n \equiv 3 \bmod 5$, pak $n + 12 \equiv 15 \bmod 5$, tudíž $n + 12$ je dělitelné 5.

4) $n \equiv 2 \bmod 5$, pak $n + 18 \equiv 20 \bmod 5$, tudíž $n + 18$ je dělitelné 5.

5) $n \equiv 1 \bmod 5$, pak $n + 24 \equiv 25 \bmod 5$, tudíž $n + 24$ je dělitelné 5.

Ukázali jsme, že žádná další pětice sexy prvočísel neexistuje, protože vždy mezi pěticí čísel vzdálených o šest bude číslo, které je dělitelné pěti.

□

Z důkazu zároveň vyplývá, že v případě čtveřic sexy prvočísel vždy musí čtveřice začínat číslem, které má zbytek po dělení 5 jedna (kromě samotné čtveřice, která začíná číslem 5), protože pak můžeme ještě třikrát přičíst číslo 6, než výsledné číslo bude dělitelné pěti.

Žádné šestice či početnější skupiny sexy prvočísel samozřejmě neexistují. (Wells,2005)

3.9 Prvočíselná dvojčata

Žádné dvě prvočísla nemohou přímo sousedit, protože každé prvočíslo s výjimkou prvočísla 2 je liché, tudíž sousední číslo musí být sudé, a proto se nejedná o prvočíslo. Jediná dvě prvočísla, která spolu přímo sousedí, jsou 2 a 3. (Gracián, 2017)

Nechť p je prvočíslo. Pokud i $p + 2$ je prvočíslo, pak p a $p + 2$ nazveme *prvočíselnými dvojčaty*.

Jsou to tedy dvojice prvočísel, jejichž rozdíl je 2.

Uvedeme si v tabulce všechny prvočíselná dvojčata, která jsou menší než 1 000 (Jsou uvedena i v díle (Gracián, 2017)).

(3, 5)	*(5, 7)*	*(11, 13)*	*(17, 19)*	*(29, 31)*
(41, 43)	*(59, 61)*	*(71, 73)*	*(101, 103)*	*(107, 109)*
(137, 139)	*(149, 151)*	*(179, 181)*	*(191, 193)*	*(197, 199)*
(227, 229)	*(239, 241)*	*(269, 271)*	*(281, 283)*	*(311, 313)*
(347, 349)	*(419, 421)*	*(431, 433)*	*(461, 463)*	*(521, 523)*
(569, 571)	*(599, 601)*	*(617, 619)*	*(641, 643)*	*(659, 661)*
(809, 811)	*(821, 823)*	*(827, 829)*	*(857, 859)*	*(881, 883)*

V tabulce můžeme zaregistrovat, že mezi dvojčaty *(659, 661) a (809, 811)* je poměrně velký skok. Nenalezneme zde žádná prvočíselná dvojčata, která by měla na řádu stovek číslo 7. V intervalu (900, 1 000) také nenalezneme žádná prvočíselná dvojčata. Čím dál postupujeme v množině přirozených čísel, tím méně se s prvočísly setkáváme, tudíž je menší i hustota zastoupení prvočíselných dvojčat.

Jedním ze známých problémů teorie čísel je, zda prvočíselných dvojčat existuje konečně či nekonečně mnoho. Již dávno víme, že prvočísel existuje nekonečně mnoho, zda se to ale týká i těchto prvočíselných dvojic, tím už si jistí nejsme. Díky moderní počítačové analýze víme, že se tyto dvojice vyskytují i mezi extrémně vysokými čísly, což matematiky snadno dovádí k domněnce, že prvočíselných dvojčat existuje nekonečně mnoho. Bez důkazu však zůstáváme pouze u domněnky. (Gracián, 2017)

Všechna prvočíselná dvojčata mají tvar $6n \pm 1$, s výjimkou (3, 5), protože prvočíslo 3 není v uvedeném tvaru.

Další zajímavostí je, že polynom $K(n) = 60n^2 + 30n - 30 \pm 1$ generuje prvočíselná dvojčata pro $n = 1$ až 13, což si zpřehledníme v tabulce.

N	***Polynom K(n)***	***Prvočíselná dvojčata***
1	$60 \cdot 1^2 + 30 \cdot 1 - 30 \pm 1$	*(59, 61)*
2	$60 \cdot 2^2 + 30 \cdot 2 - 30 \pm 1$	*(269, 271)*
3	$60 \cdot 3^2 + 30 \cdot 3 - 30 \pm 1$	*(599, 601)*
4	$60 \cdot 4^2 + 30 \cdot 4 - 30 \pm 1$	*(1 049, 1 051)*
5	$60 \cdot 5^2 + 30 \cdot 5 - 30 \pm 1$	*(1 619, 1 621)*
6	$60 \cdot 6^2 + 30 \cdot 6 - 30 \pm 1$	*(2 309, 2 311)*
7	$60 \cdot 7^2 + 30 \cdot 7 - 30 \pm 1$	*(3 119, 3 121)*
8	$60 \cdot 8^2 + 30 \cdot 8 - 30 \pm 1$	*(4 049, 4 051)*
9	$60 \cdot 9^2 + 30 \cdot 9 - 30 \pm 1$	*(5 099, 5 101)*
10	$60 \cdot 10^2 + 30 \cdot 10 - 30 \pm 1$	*(6 269, 6 271)*
11	$60 \cdot 11^2 + 30 \cdot 11 - 30 \pm 1$	*(7 559, 7 561)*
12	$60 \cdot 12^2 + 30 \cdot 12 - 30 \pm 1$	*(8 969, 8 971)*
13	$60 \cdot 13^2 + 30 \cdot 13 - 30 \pm 1$	*(10 499, 10 501)*

I v tomto případě nás budou zajímat rekordmani tohoto typu čísel, uvedeme si proto deset největších dosud známých prvočíselných dvojčat.

Pořadí	***Prvočíselná dvojčata***	***Počet cifer***	***Doba objevení***
1	$2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} \pm 1$	*388 342*	*Září 2016*
2	$3\,756\,801\,695\,685 \cdot 2^{666\,669} \pm 1$	*200 700*	*Prosinec 2011*
3	$6\,551\,648\,355 \cdot 2^{333\,333} \pm 1$	*100 355*	*Srpen 2009*
4	$12\,770\,275\,971 \cdot 2^{222\,225} \pm 1$	*66 907*	*Červenec 2017*
5	$70\,965\,694\,293 \cdot 2^{200\,006} \pm 1$	*60 219*	*Duben 2016*
6	$66\,444\,866\,235 \cdot 2^{200\,003} \pm 1$	*60 218*	*Duben 2016*

7	*$4\,884\,940\,623 \cdot 2^{198\,800} \pm 1$*	*59 855*	*Červenec 2015*
8	*$2\,003\,663\,613 \cdot 2^{195\,000} \pm 1$*	*58 711*	*Leden 2007*
9	*$38\,529\,154\,785 \cdot 2^{173\,250} \pm 1$*	*52 165*	*Červenec 2014*
10	*$194\,772\,106\,074\,315 \cdot 2^{171\,960} \pm 1$*	*51 780*	*Červen 2007*

Tabulka – prvočíselná dvojčata (Caldwell)

Prvočíslo 5 je jediné, které se vyskytuje ve dvou prvočíselných dvojčatech *(3, 5)*, *(5, 7)*, ale o tom více v následující kapitole.

3.10 Prvočíselná trojčata

Nechť p je prvočíslo. Pokud i $p + 2$ a $p + 4$ jsou prvočísla, pak p, $p + 2$ a $p + 4$ nazveme *prvočíselnými trojčaty*.

Ač uvádíme definici, jako by se mělo jednat o početnou množinu, existuje jenom jedna taková trojice prvočísel, ve které jsou sousední prvočísla vzdálena o 2. Jedná se o trojici (3, 5, 7), a že žádná jiná neexistuje, si nyní dokážeme.

Věta 3.3

"Neexistuje žádná další trojice prvočísel tvaru p, p + 2 a p + 4 kromě trojice (3, 5, 7)."

Důkaz. Nechť je dána trojice přirozených čísel n, $n + 2$, $n + 4$.

Zaměříme se na zbytek po dělení číslem 3. Mohou nastat následující tři případy.

1) n je dělitelné 3, tudíž n je buď 3, nebo číslo složené.

2) $n \equiv 1 \bmod 3$, pak $n + 2 \equiv 3 \bmod 3$, tudíž $n + 2$ je dělitelné 3.

3) $n \equiv 2 \bmod 3$, pak $n + 4 \equiv 6 \bmod 3$, tudíž $n + 4$ je dělitelné 3.

Tím jsme ukázali, že v dané trojici přirozených čísel n, $n + 2$, $n + 4$ je vždy jeden člen z trojice dělitelný třemi. Jelikož prvočísla jsou podmnožinou přirozených čísel, platí toto tvrzení i pro prvočísla.

□

Za zmínku určitě stojí i prvočísla, která jsou od sebe vzdálena o čtyři. V anglickém jazyce nesou název "*cousin primes*". Těchto dvojic prvočísel, která jsou menší než 1 000, existuje 40. Pro zajímavost si uvedeme prvních deset. (Wells, 2005)

(3, 7)	*(7, 11)*	*(13, 17)*	*(19, 23)*	*(37, 41)*
(43, 47)	*(67, 71)*	*(79, 83)*	*(97, 101)*	*(103, 107)*

4 Řešené i neřešené příklady

4.1 Řešené příklady

Příklad 1.

Nalezněte všechna čísla $k \in N_0$, pro která je mezi deseti po sobě jdoucími čísly $k + 1$, $k + 2$, … , $k + 10$ nejvíce prvočísel.

Řešení. Pro $k = 0$ dostáváme čtyři prvočísla: 2, 3, 5, 7. Pro $k = 1$ je mezi našimi čísly pět prvočísel : 2, 3, 5, 7, 11 a pro $k = 2$ pouze čtyři prvočísla: 3, 5, 7, 11. Pro $k \geq 3$ dostáváme deset po sobě jdoucích přirozených čísel, z nichž pět je sudých a pět lichých. Jelikož prvočíslo, které je větší než 3, nemůže být sudé, odpadá nám pět možností pro potenciální prvočísla. V naší posloupnosti deseti po sobě jdoucích přirozených čísel pro $k \geq 3$ je mezi lichými čísly alespoň jedno dělitelné třemi. Našli jsme tedy mezi čísly $k + 1$, $k + 2$, … , $k + 10$ alespoň šest složených čísel, vyskytují se tedy mezi nimi maximálně čtyři prvočísla. Zadání tedy vyhovuje jediné číslo $k = 1$.

Příklad 2.

Najdi prvočíslo p takové, aby pro přirozená čísla a, b platilo následující:

$D(a, b) = 91$

$n(a, b) = 210p$

$a \cdot b = 1\,470p^2$.

Řešení. U čísel 91, 210 a 1 470 provedeme faktorizaci.

$D(a, b) = 91 = 7 \cdot 13$

$n(a, b) = 210p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot p$

$a \cdot b = 1470p^2 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7 \cdot p^2$

Protože $D(a, b) = 7 \cdot 13$, je a i b dělitelné 13, tedy součin $a \cdot b$ je dělitelný 13^2. Jelikož $a \cdot b = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7 \cdot p^2$, musí nutně být $p = 13$. Předpoklad $n(a, b) = 210p = 3 \cdot 5 \cdot 7 \cdot 13$ je také splněn. Tím jsme našli hledané prvočíslo, kterým je číslo 13.

Příklad 3.

Dokažte, že existuje alespoň jedno takové přirozené číslo n, pro které existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslo.

Řešení. Zaměřme se na čísla $(n + 1)! + 2$, $(n + 1)! + 3$, …, $(n + 1)! + (n+ 1)$. Mezi těmito n po sobě jdoucími přirozenými čísly není žádné prvočíslo, protože pro libovolné $k \in \{2, 3, 4, \ldots, n + 1\}$ platí $k \mid (n + 1)!$, a tedy $k \mid (n + 1)! + k$, a proto $(n + 1)! + k$ nemůže být prvočíslo.

□

Příklad 4.

Dokažte následující tvrzení: *„Je-li číslo m složené, pak je vždy možno najít prvočíslo $p \leq \sqrt{m}$, které dělí číslo m.“*

Řešení. Každé složené číslo m můžeme vyjádřit ve tvaru $m = x \cdot y$, kde $x > 1$, $y > 1$, $x \geq y$. Kdyby bylo $y > \sqrt{m}$, bylo by také $x > \sqrt{m}$. Z těchto dvou nerovností by pak plynulo, $x \cdot y > (\sqrt{m})^2 = m$, tedy $x \cdot y > m$. Avšak tím bychom dostali spor s předpokladem $m = x \cdot y$, takže o čísle y můžeme říci, že platí $y \leq \sqrt{m}$. Pokud je y přímo prvočíslo, hledání pro nás skončilo. Je-li y číslo složené, pak můžeme najít prvočíslo p, které dělí y; přitom je $p < y$ a tedy i $p < \sqrt{m}$. Tím jsme našli prvočíslo p, jehož existenci jsme měli v tomto příkladu ukázat.

Příklad 5.

Rozhodněte, zda číslo 811 je složené číslo nebo prvočíslo.

Řešení. Přesvědčíme se, že 811 je prvočíslo. Abychom k takovému tvrzení dospěli, je třeba ukázat, že číslo 811 není dělitelné žádným prvočíslem p, pro které platí

$p \leq \sqrt{811}$. Jelikož $\sqrt{811} \doteq 28{,}5$, stačí nám ověřit prvočísla 2, 3, 5, 7, 11, 13, 17, 19, 23. Z našich prvočísel se na středních školách setkáváme s kritérii dělitelnosti čísly 2, 3, 5, a 7 proto si ověříme dělitelnost čísla 811 jednotlivými prvočísly právě přes zmíněná kritéria. Dělitelnost ostatními prvočísly ověříme přes klasický výpočet.

2: Číslo je dělitelné 2, je-li na místě jednotek sudé číslo. U našeho čísla 811 je na místě jednotek liché číslo 1, tudíž číslo 811 není dělitelné dvěma.

3: Číslo je dělitelné 3, je-li jeho ciferný součet dělitelný 3. Dostáváme 8 + 1 + 1 = 10, což není dělitelné 3, tudíž není ani číslo 811 dělitelné 3.

5: Číslo je dělitelné 5, je-li na místě jednotek 5 nebo 0. U čísla 811 je na místě jednotek číslo 1, není tedy dělitelné 5.

7: Číslo je dělitelné 7, je-li rozdíl zbývající části a posledního čísla vynásobeného dvakrát dělitelný 7. Zde dostáváme $81 - 1 \cdot 2 = 79$, což není dělitelné 7, tudíž ani číslo 811 není dělitelné 7.

11: 811/11 = 73 zbytek 8

13: 811/13 = 62 zbytek 5

17: 811/17 = 47 zbytek 12

19: 811/19 = 42 zbytek 13

23: 811/23 = 35 zbytek 6

Tím jsme ukázali, že 811 je prvočíslo.

Příklad 6.

Určete nejmenší čtyřciferné číslo, které je zároveň prvočíslem.

Řešení. Nejmenší čtyřciferné číslo je 1 000, které je zřejmě složené. V následujícím postupu nebudeme uvažovat sudá čísla, protože ta jsou také složená. Číslo 1 001 je dělitelné 11, číslo 1 003 je dělitelné 17, číslo 1 005 je zřejmě dělitelné 5 a číslo 1 007 je dělitelné 19. Ve všech těchto případech jde o čísla složená. Následující číslo, které

přichází do úvahy, je číslo 1 009 a jedná se o prvočíslo. Ověření je stejné jako v předchozím příkladě a ponecháme ho tak čtenáři. Opět bychom zkoumali dělitelnost čísla 1 009 prvočísly, která jsou menší než $\sqrt{1\,009} \doteq 31{,}8$. Tudíž posledním prvočíslem, kterým budeme dělit číslo 1 009 je prvočíslo 31. Dojdeme k závěru, že nejmenší čtyřciferné prvočíslo je skutečně číslo 1 009.

Příklad 7.

Pět prvočísel tvoří pět po sobě jdoucích členů aritmetické posloupnosti s diferencí $d = 6$. Určete tato prvočísla.

Řešení. V tomto příkladu využijeme tvrzení, jehož pravdivost je prokázána ve větě 3.2: Je-li a libovolné celé nezáporné číslo, pak alespoň jedno z čísel a, $a + 6$, $a + 12$, $a + 18$, $a + 24$ je dělitelné pěti. V naší posloupnosti je tedy jedno z čísel dělitelné pěti. Podle zadání však požadujeme, aby každý člen posloupnosti byl prvočíslem. Jediné prvočíslo, které je dělitelné pěti, je samotné číslo 5, tudíž musí figurovat v naší posloupnosti. Vzhledem k diferenci $d = 6$ musí být první člen posloupnosti $a_1 = 5$. Pokud $a_1 = 5$, pak $a_2 = 11$, $a_3 = 17$, $a_4 = 23$, $a_5 = 29$. Všechny tyto členy posloupnosti jsou prvočísly, takže jsme našli hledaných pět členů posloupnosti, totiž 5, 11, 17, 23, 29. (Tato pětice prvočísel, která jsou od sebe vzdálena o 6, je zároveň jedinou pěticí sexy prvočísel, která jsme zmiňovali v kapitole 3.8).

4.2 Neřešené příklady

Příklad 8.

Ukažte, že je možné najít tisíc po sobě jdoucích přirozených čísel, která jsou složená.

Příklad 9.

Rozhodněte, zda číslo 1 553 je prvočíslo, nebo číslo složené.

Příklad 10.

Proveďte faktorizaci u čísel 2 518, 3 724 a 111 111.

Příklad 11.

Najděte největší prvočíslo, kterým je dělitelné číslo 4 812.

Příklad 12.

Určete největší čtyřciferné prvočíslo.

Příklad 13.

Pět prvočísel tvoří pět po sobě jdoucích členů aritmetické posloupnosti s diferencí $d = 12$. Určete tato prvočísla.

Příklad 14.

Násobky kolika prvočísel je nutno vyškrtnout při hledání čísel, která jsou menší než 500, pomocí metody Eratosthenova síta?

Příklad 15.

Kolik prvočísel obsahuje interval od 200 do 300?

Příklad 16.

Napište sedm za sebou jdoucích složených čísel.

Příklad 17.

Najděte první dvojici prvočísel, která jsou větší než 1 000 a jsou od sebe vzdálena o 2. Totéž udělejte pro vzdálenost 4, 6, 8 a 10.

Příklad 18.

Kolik čtyřciferných čísel je dělitelných prvočíslem 7?

Příklad 19.

Jakou nejmenší délku v centimetrech má provázek, který lze rozstříhat na 15 stejných částí, a zároveň na 24 stejných částí?

Příklad 20.

Uveďte alespoň pět příkladů z běžného života, ve kterých figuruje libovolné prvočíslo.

Většina příkladů v této kapitole je inspirována příklady z publikací (Sedláček, 1961), (Bulant).

Závěr

Cílem této bakalářské práce bylo uvést čtenáře do oblasti prvočísel a následně vhodně interpretovat speciální typy prvočísel, na které byla zaměřena hlavní část práce.

Bakalářská práce „Zajímavá prvočísla a jejich vlastnosti“ se zaměřuje především na speciální typy prvočísel, které byly objevovány skrze celou historii od starověku až po současnost. Úvod je zaměřen na vymezení základních pojmů z oblasti prvočísel. V závěru je pozornost soustředěna na řešené i neřešené příklady, pomocí nichž lze upevnit vědomosti získané z celé práce. Text je koncipován tak, aby byl přehledný a pochopitelný pro všechny čtenáře, kteří mají alespoň základní znalosti z algebry. Jednotlivé typy prvočísel jsou většinou doplněny o tabulky dosud největších objevených prvočísel daného typu.

Jsem rád, že jsem si vypracováním této bakalářské práce mohl prohloubit matematické znalosti a udělat patřičný nadhled nad daným tématem.

Práce může sloužit jako pomůcka pro učitele ve škole nebo v zájmových kroužcích. Avšak je určena pro všechny, kteří se chtějí dozvědět o prvočíslech zajímavosti, které nejsou běžně zahrnuty při klasických hodinách matematiky.

Bibliografie

Bulant, M. Algebra 2 - Teorie čísel. *Přírodovědecká fakulta MU - Ústav matematiky a statistiky.* Retrieved from: https://www.math.muni.cz/~bulik/vyuka/Algebra-2/alg2-print.pdf.

Cadwell, C. (n. d.). . Retrieved from: https://primes.utm.edu/top20/page.php?id=7.

Cadwell, C. (n. d.). . Retrieved from: https://primes.utm.edu/top20/page.php?id=6.

Cadwell, C. (n. d.). . Retrieved from:https://primes.utm.edu/top20/page.php?id=30.

Cadwell, C. (n. d.). . Retrieved from:https://primes.utm.edu/top20/page.php?id=2.

Cadwell, C. (n. d.). . Retrieved from:https://primes.utm.edu/top20/page.php?id=1.

Fuchs, E. 1993. Co ještě nevíme o prvočíslech. [autor knihy] Fuchs Eduard Bečvář Jindřich. *Historie matematiky I.* Praha : Nakladatelství Prometheus, 1993.

Gracián, E. 2017. *Prvočísla - Dlouhá cesta do nekonečna.* místo neznámé : Dokořán, 2017. 978–80–7363–842–9.

Great Internet Mersenne Prime Search. (©1996-2020). Retrieved from: https://www.mersenne.org/primes/.

Halaš, R. (2014). *Úvod do teorie čísel.* Olomouc : Univerzita Palackého, 2014. 978-80-244-4068-2.

Křížek, Michal. (1995) O Fermatových číslech. *The Czech Digital Mathematics Library.* Retrieved from: https://dml.cz/handle/10338.dmlcz/138304.

Marshall, S. (n. d.). Number theory. *viXra.org.* Retrieved from: https://vixra.org/abs/1904.0033.

Křížek, M. (2018). *Kouzlo čísel.* Český Těšín : Nakladatelství Academia. ISBN 978-80-200-2840-2.

Sedláček, J. (1961). *Co víme o přirozených číslech.* Praha : Mladá fronta. D-14-10349.

Weisstein, E. . Retrieved from: https://mathworld.wolfram.com/Primorial.html.

Wells, D. (2005). *Prime numbers: The Most Mysterious Figures in Math.* New Jersey : John Wiley & Sons, 2005. 0471718920.