ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

PRVOČÍSLA A FAKTORIZACE CELÝCH ČÍSEL

DIPLOMOVÁ PRÁCE

Bc. Stanislav Hefler
Učitelství pro 2. stupeň ZŠ, obor Ma-Inf

Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

Plzeň, 2015

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 14. dubna 2015

.....

vlastnoruční podpis

Děkuji mému vedoucímu diplomové práce doc. RNDr. Jaroslavu Horovi, CSc., za jeho cenné rady, připomínky a metodické vedení práce.

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: **2013/2014**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Stanislav HEFLER**
Osobní číslo:	**P13N0006P**
Studijní program:	**N7503 Učitelství pro základní školy**
Studijní obory:	**Učitelství informatiky pro základní školy**
	Učitelství matematiky pro základní školy
Název tématu:	**Prvočísla a faktorizace celých čísel**
Zadávající katedra:	**Katedra matematiky, fyziky a technické výchovy**

Zásady pro vypracování:

Prostudovat základní fakta o prvočíslech, testy prvočíselnosti, pseudoprvočísla. Základní algoritmy pro faktorizaci přirozených čísel. Ukázky výpočtů v programu Mathematica, příp. v dalších prostředcích počítačové algebry.

1. Prvočísla - úvodní informace, klasické výsledky. Testy prvočíselnosti.
2. p-pseudoprvočísla, příklady silnějších prvočíselných testů, ukázky výpočtů v programu Mathematica.
3. Metoda opakovaného dělení. Fermatova a Eulerova faktorizační metoda, příp. další klasické faktorizační metody. Moderní faktorizační metody.

Rozvržení práce:

1. Seznámení s literaturou knižní i časopiseckou, překlady textů - do 30. 6. 2014
2. Příprava konceptu DP (včetně výpočetních ukázek v programu Mathematica) - do 31. 12. 2014
3. Závěrečné úpravy a definitivní uzavření textu - do 31. 3. 2015

Rozsah grafických prací:

Rozsah pracovní zprávy: **40 - 60**

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

Crandall, R., Pomerance, C. B. Prime Numbers. A Computational Perspective. 2. vydání, Springer, 2005.
Childs, L. A Concrete Introduction to Higher Algebra. 2. vydání, Springer, 2009.
Další knižní a časopisecké prameny, zdroje na Internetu, manuál k počítačovému programu Mathematica.

Vedoucí diplomové práce: **Doc. RNDr. Jaroslav Hora, CSc.**
Katedra matematiky, fyziky a technické výchovy

Datum zadání diplomové práce: **25. listopadu 2013**
Termín odevzdání diplomové práce: **15. dubna 2015**

Doc. PaedDr. Jana Coufalová, CSc.
děkanka

L.S.

Doc. PaedDr. Jarmila Honzíková, Ph.D.
vedoucí katedry

V Plzni dne 2. prosince 2013

OBSAH

ÚVOD

Tato diplomová práce se zabývá prvočísly, testováním prvočíselnosti a faktorizací celých čísel. Tyto matematické operace spadají do matematické disciplíny algebra, kterou se zabývají matematici od nepaměti. Mezi nejvýznamnější matematiky řešící problematiku prvočíselných testů a faktorizace patřili v neposlední řadě Euklidés z Alexandrie, Pierre de Fermat a Leonhard Euler, po kterých jsou pojmenovány prvočíselné testy a metody faktorizace. Mezi moderní matematiky řešící tuto problematiku patří Michael Morrison, John Brillhart, Carl Pomerance, John M. Pollard, Daniel Shanks a Hendrik William Lenstra.

Hlavním tématem této práce je prvočíselnost a faktorizace celých čísel. Proto je největší část práce věnována právě prvočíselným testů, klasickým metodám faktorizace a moderním faktorizačním metodám. Pro zajímavost jsem do své práce umístil ukázku určení prvočíselnosti v různých matematických softwarech.

Tato práce obsahuje vymezení pojmů prvočíslo, pseudoprvočíslo, prvočíselný test a faktorizace celých čísel. Dále ukázky klasických i moderních prvočíselných testů a metod faktorizace celých čísel. Práce je rozdělena do pěti kapitol.

První kapitola se zabývá vymezením pojmu prvočíslo a historickému vývoji těchto čísel. Dále zde najdeme vysvětlení pojmu prvočíselný test a klasické prvočíselné testy.

Druhá kapitola obsahuje vysvětlení pojmu pseudoprvočíslo a ukázky moderních prvočíselných testů. Zde také nalezneme ukázku určení prvočíselnosti pomocí matematických programů Wolfram Mathematica, Maple, MATLAB, GNU OCTAVE a Wolfram|Alpha.

Třetí kapitola je věnována klasickým metodám faktorizace. Jedná se o metodu postupného dělení, Fermatovu faktorizační metodu, Eulerovu faktorizační metodu a využití Euklidova algoritmu pro faktorizaci celých čísel.

Ukázky vybraných moderních metod faktorizace nalezneme ve čtvrté kapitole. Jedná se především o metody Johna M. Pollarda a Hendrika W. Lenstra.

Poslední pátá kapitola se věnuje využití prvočísel a prvočíselných testů v dnešní době, především šifrovacímu algoritmu RSA a elektronickému podpisu.

1 PRVOČÍSLA

Definice: Číslo 1 je dělitelné jediným přirozeným číslem, a to sebou samým. Libovolné přirozené číslo $n > 1$ je dělitelné 1 a sebou samým. Těmto dělitelům se říká **samozřejmí dělitelé**. Přirozené číslo, které kromě samozřejmých dělitelů nemá již žádné další dělitele, se nazývá **prvočíslo**. Přirozené číslo, které není prvočíslem, se nazývá **číslo složené.** (1)

Prvočísla se nejčastěji označují písmenem p.

1.1 HISTORICKÝ VÝVOJ PRVOČÍSEL

Množina čísel nazývaná prvočísla byla známá už matematiky ve starověkém Řecku. Matematici Pythagorejské školy (asi 500 př. n. l. až 300 př. n. l.) studovali čísla kvůli vlastnostem, které vycházely z jejich numerologického a mystického vědění. Z těchto důvodů se zajímali o prvočísla a čísla dokonalá (perfektní), která byla důležitá především pro jejich mystické záhady.

Definice: **Dokonalé číslo** je takové číslo, jehož součet jeho vlastních dělitelů je roven tomuto číslu. Vlastním dělitelem čísla a se nazývá každý dělitel tohoto čísla a, pro který platí, že je menší než číslo a. (2)

Číslo 6 má vlastní dělitele $1, 2$ a 3, a zároveň platí $1 + 2 + 3 = 6$. Číslo 6 je tedy dokonalé číslo.

Platí také, že dokonalé číslo je rovno polovině součtu všech jeho dělitelů, tedy

$$6 = \frac{(1 + 2 + 3 + 6)}{2}.$$

Dalšími dokonalými čísly jsou čísla 28, 496 a 8128.

Prvočíslům se věnoval i řecký matematik Euklidés z Alexandrie v jeho díle Stoicheia (česky Základy, anglicky The Euclid´s Elements), ve kterém popisuje základy matematiky a geometrie. Dílo Stoicheia je rozděleno do třinácti knih.

Obrázek 1 Euklidés z Alexandrie

V Euklidových Základech napsaných kolem roku 300 př. n. l. je uvedeno několik důležitých vlastností prvočísel a také nechybí jejich důkazy. V 9. knize (v této knize Euklidés využívá výsledky z předchozích dvou knih, ve kterých se zabývá teorií čísel a dává jednotlivým pojmům hlubší význam) Euklidés dokázal základní větu aritmetiky.

Věta: Základní věta aritmetiky. Každé přirozené číslo $n > 1$ lze zapsat jako součin prvočísel p a to jediným způsobem (až na pořadí činitelů):

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_i^{a_i} = \prod_{j=1}^{i} p_j^{a_j}. \quad (3)$$

Euklidés se zabýval určením počtu všech prvočísel. Určil, že prvočísel je více než jakékoli dané množství prvočísel. V dnešní době je známější podoba této věty, prvočísel je nekonečně mnoho, ale v době, kdy Euklidés tuto větu vyslovil, byl pojem nekonečno pouze potenciální (je zajímavé, že tato situace trvala až do 19. století). Své tvrzení o počtu prvočísel dokázal a jedná se o první známý důkaz sporem. Pro ukázku, jak v Euklidově době vypadal „geometrický" jazyk, v němž byla formulována tehdejší matematika a to včetně aritmetiky, uvedu tuto větu a její důkaz, jak byla publikována v 9. knize Euklidových Základů.

Věta: Prvočísel jest více než jakékoli dané množství prvočísel.

Důkaz: Buďte dána prvočísla A, B, C. Tvrdím, že jest více prvočísel než A, B, C. Uvažme nejmenší číslo dělitelné čísly A, B, C, nechť to je DE a přičtěme k DE jednotku DF. Číslo EF tedy buďto prvočíslo je nebo není.

Nechť nejprve prvočíslem jest; jsou tedy nalezena prvočísla A, B, C, EF jejichž počet jest více než A, B, C.

Nechť tedy EF není prvočíslo; je tedy některým prvočíslem dělitelné. Nechť ho dělí prvočíslo G. Tvrdím, že G není rovno žádnému z čísel A, B, C. Nuže, připusťme, že je některému z těchto čísel rovno. Avšak A, B, C dělí číslo DE. Tedy číslo G rovněž dělí DE. Pak ale dělí i číslo EF. G pak ale dělí i zbývající jednotku DF, ačkoliv je číslem a to jest nesmysl. G tedy není rovno žádnému z čísel A, B, C a přitom jest prvočíslem. Jest tedy nalezeno více prvočísel než je dané množství A, B, C, totiž A, B, C, G, což právě bylo dokázati. (4)

Euklidés také dokázal, že číslo $2^n - 1$ je prvočíslo, pokud číslo $2^{n-1} \cdot (2^n - 1)$ je dokonalé číslo. V roce 1747 Leonhard Euler dokázal, že pro všechna sudá dokonalá čísla tato vlastnost platí. Zatím se nepovedlo dokázat, zda existují nějaká lichá dokonalá čísla.

Obrázek 2 Eratosthenés z Kyrény

Kolem roku 200 př. n. l. řecký matematik Eratosthenés z Kyrény přišel na jeden z prvních postupů pro výpočet prvočísel, který nese jeho jméno, **Eratosthenovo síto**. Pomocí tohoto algoritmu byla objevena řada dalších prvočísel (jednalo se především o čísla s více ciframi).

Tento algoritmus sestává ze čtyř kroků:

1) Sepíšeme čísla 2 až n (až po jaké číslo chceme zjistit prvočísla).
2) Označíme číslo 2 (případně nejnižší neoznačené číslo) jako prvočíslo.
3) Škrtneme všechny násobky čísla 2 (označeného čísla z předchozího kroku).
4) Pokračujeme znovu od kroku 2, dokud nejsou všechna čísla označena nebo škrtnuta. Označená čísla jsou všechna prvočísla, pro která platí $p < n$.

	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~~

Obrázek 3 Ukázka Eratosthenova síta

Dalším matematikem, který se zabýval prvočísly, byl počátkem 17. století Pierre de Fermat. Vyslovil větu, že každé prvočíslo tvaru $4n + 1$ ($n \in \mathbb{N}$) lze zapsat jediným způsobem jako součet dvou čtverců (druhých mocnin) přirozených čísel. Tuto Fermatovu větu později dokázal Leonhard Euler.

Fermat je také autorem metody pro rozklad čísla na jeho prvočinitele. Dokázal to rozkladem čísla $2\,027\,651\,281$, kde $2\,027\,651\,281 = 44\,021 \cdot 46\,061$. Fermatovou faktorizační metodou se budeme zabývat podrobně později.

Obrázek 4 Pierre de Fermat

Pierre de Fermat také vyslovil Fermatovu malou větu.

Věta: Nechť p je prvočíslo a přirozené číslo a je nesoudělné s p. Pak platí:

$$a^{p-1} \equiv 1\ (mod\ p),$$

nebo ekvivalentně:

$$a^{p} \equiv a\ (mod\ p).\ (3)$$

Definice: Říkáme, že celé číslo a je kongruentní s celým číslem b podle modulu m (kde m je libovolné přirozené číslo větší než 1), značíme $a \equiv b\ (mod\ m)$ právě tehdy, když platí $m|a - b$. Symbolicky

$$a \equiv b \Leftrightarrow m|a - b.\ (5)$$

Fermatova malá věta se stala základem řady dalších výsledků v teorii čísel a využívá se také v počítačových metodách určování, zda je dané číslo prvočíslem.

Pierre de Fermat si při ověřování svých domněnek dopisoval s dalšími matematiky. Jedním z nich byl také mnich Marin Mersenne. V jednom ze svých dopisů Mersennovi vyslovil Fermat domněnku, že číslo tvaru $2^n + 1$ je prvočíslem, pokud číslo n je mocninou čísla 2. Tuto domněnku ověřil pro $n = \{1, 2, 4, 8, 16\}$. Dále ověřil, že pokud n nebylo mocninou čísla 2, číslo $2^n + 1$ nebylo prvočíslem. Čísla tohoto tvaru se nazývají Fermatova čísla.

Věta: Čísla ve tvaru $F_n = 2^{2^n} + 1$ se nazývají **Fermatova čísla**. (3)

Fermat věřil, že všechna čísla v tomto tvaru jsou prvočísla, ale tato domněnka nebyla dokázána.

Teprve Leonhard Euler po více jak sto letech dokázal, že $2^{32} + 1 = 4\,294\,967\,297$, které je dělitelné číslem 641, není prvočíslem.

Také čísla tvaru $2^n - 1$ přitahovala pozornost a to hlavně mnicha Marina Mersenna. Marin Mersenne dokázal, že pokud číslo n není prvočíslem, pak číslo $2^n - 1$ musí být složené. Tato čísla se označují jako Mersennova čísla M_n.

Obrázek 5 Marin Mersenne

Věta: Čísla ve tvaru $M_n = 2^n - 1$ se nazývají **Mersennova čísla**. (2)

Sám Mersenne věděl, že pokud má být Mersennovo číslo $M_n = 2^n - 1$ prvočíslem, musí být n prvočíslem. Ne však všechna čísla tvaru $2^p - 1$ jsou prvočísly. Například číslo

$$M_{11}: 2^{11} - 1 = 2047 = 23 \cdot 89$$

a tudíž není prvočíslem. Řadu let se pomocí Mersennových čísel vypočítávala mnohociferná čísla, u kterých se prokazovalo, zdali jsou prvočísly nebo čísly složenými.

V roce 1603 Pietro Antonio Cataldi dokázal, že Mersennova čísla $M_{17}: 2^{17} - 1 = 131\,071$ a $M_{19}: 2^{19} - 1 = 524\,287$ jsou prvočísly. Téměř 150 let bylo číslo M_{19} největším známým prvočíslem.

V roce 1644 vyslovil Mersenne domněnku, že Mersennova čísla M_1 (Mersenne považoval číslo 1 za prvočíslo), M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{67}, M_{127} a M_{257} jsou prvočísly (bylo to však dokázáno jen do čísla M_{19}).

Až v roce 1750 Leonhard Euler dokázal, že také $M_{31}: 2^{31} - 1 = 2\,147\,486\,647$ je prvočíslem. V roce 1876 Eduard Lucas přidal důkaz pro číslo $M_{127}: 2^{127} - 1$, toto prvočíslo má 39 cifer. V roce 1883 Ivan Mikheevich Pervushin doplnil seznam Mersenových čísel, která jsou prvočísly, o číslo M_{61}.

První chybu v Mersennově domněnce objevil až v roce 1903 americký matematik Frank Nelson Cole. Určil, že $M_{67}: 2^{67} - 1 = 193\,707\,721 \cdot 761\,838\,257\,287$ a není tedy prvočíslem.

V roce 1952 Raphael Mitchel Robinson pomocí jednoho z prvních elektronických počítačů dokázal, že Mersennova čísla M_{521}, M_{607}, M_{1279}, M_{2203} a M_{2281} jsou prvočísly. Číslo M_{2281} má 687 cifer.

V roce 1998 bylo dokázáno, že celkem 37 Mersennových čísel jsou prvočísly a největším známým prvočíslem nalezeným 27. ledna 1998 skupinou GIMPS (Great Internet Mersenne Prime Search) bylo 37. Mersennovo prvočíslo $M_{3\,021\,377}$, které má $909\,526$ cifer.

Dalším cílem skupiny GIMPS bylo najít Mersennovo prvočíslo, které bude mít více jak milion cifer. S vývojem výpočetní techniky tato „výzva“ netrvala dlouho a již 1. června roku 1999 nalezl Nayan Hajratwala 38. Mersennovo prvočíslo $M_{6\,972\,593}$, které má $2\,098\,960$ cifer.

Obrázek 6 Curtis Cooper

V současnosti (březen 2015) je největším známým prvočíslem 48. Mersennovo prvočíslo $M_{57\,885\,161}$, které má $17\,425\,170$ cifer. Bylo objeveno matematikem Curtisem Cooperem z University of Central Missouri 25. ledna 2013. (5)

Eulerova práce měla značný dopad na celou teorii čísel, byl prvním, kdo začal studovat teorii čísel pomocí nástrojů analýzy a tím založil analytickou teorii čísel. Leonhard Euler nejen dokázal, že harmonická řada

$$\sum_{n=0}^{\infty} \frac{1}{n}$$

je divergentní, ale také že řada

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots,$$

která je nekonečným součtem převrácených hodnot prvočísel, je také divergentní.

Obrázek 7 Leonhard Euler

Na první pohled je rozložení prvočísel mezi všemi celými čísly náhodné. Například mezi stovkou čísel, která bezprostředně následují za číslem 10^7, je devět prvočísel, zatímco mezi další stovkou čísel jsou jen dvě prvočísla.

Avšak ve velkém měřítku jsou prvočísla rozložena velmi rovnoměrně. Adrien Marie Legendre a Carl Friedrich Gauss jako první provedli výpočet hustoty prvočísel. Odhadli, že hustota prvočísel je asi $\frac{1}{log\, n}$. Během 19. století se pokusili toto tvrzení dokázat Pafnuty Lvovich Chebyshev (Čebyšev) a Bernhard Riemann, který tento problém dal do souvislosti s Riemannovou hypotézou. Riemannova hypotéza souvisí s nulovými body Riemannovy funkce ζ („zéta“) v komplexní rovině. V roce 1896 tuto hypotézu dokázal Jacques Hadamard a Louis de La Vallée Poussin s použitím složitých metod komplexní analýzy.

V teorii čísel dodnes existuje řada nevyřešených problémů s prvočísly. Jedná se o vyslovené hypotézy matematiků, kteří se zabývali teorií čísel. Jednou z nejznámějších je Goldbachova hypotéza, která říká, že každé sudé celé číslo větší než 2 lze zapsat jako součet dvou prvočísel. Poprvé byla tato hypotéza uvedena v dopise, který psal Christian Goldbach 7. 7. 1742 Leonhardu Eulerovi.

Obrázek 8 Christian Goldbach

Přes snahu mnoha matematiků se dodnes nepovedlo Goldbachovu hypotézu potvrdit ani vyvrátit. Podařilo se však prokázat řadu dílčích výsledků, od kterých je cesta k prokázání či vyvrácení Goldbachovy hypotézy stále daleká.

Například Ivan Matvejevič Vinogradov dokázal, že existuje číslo n_0, pro které platí, že každé liché číslo větší než n_0 je součtem tří prvočísel. Bohužel však ještě nebylo určeno, jak velké musí být toto číslo n_0. Jedná se však o částečné vyřešení tzv. ternárního Goldbachova problému (každé liché číslo $n > 7$ je součtem tří prvočísel), který je důsledkem Goldbachovy hypotézy.

Mezi další nevyřešené hypotézy (problémy) s prvočísly patří například:

- Prvočíselná dvojčata – domněnka prvočíselných dvojčat tvrdí, že existuje nekonečně mnoho dvojic prvočísel vzdálených od sebe o číslo 2.
- Existuje nekonečně mnoho prvočísel tvaru $n^2 + 1$?
- Je-li p prvočíslo, je $2^p - 1$ nedělitelné druhou mocninou prvočísla?
- Obsahuje Fibonacciho posloupnost nekonečně mnoho prvočísel?

1.2 PRVOČÍSELNÝ ROZKLAD

Prvočíselným rozkladem myslíme nejzákladnější metodu pro faktorizaci přirozených čísel, která se vyučuje již v 6. ročníku na základní škole (ZŠ). Jedná se však o nejhorší metodu při použití počítačového algoritmu z hlediska časové náročnosti, jakou můžeme zvolit.

Definice: Každé celé číslo a, kde $|a| > 1$, se dá vyjádřit jako součin prvočísel.

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n. \quad (5)$$

Například číslo 80 lze vyjádřit jako součin $80 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$.

Prvočíselný rozklad se na ZŠ určuje několika způsoby. Jedná se o tabulkovou, řádkovou a grafickou metodu.

1.2.1 METODA TABULKOVÁ

Při tabulkové metodě se používají dva sloupce. Do levého sloupce napíšeme na první řádek číslo, které chceme rozložit na součin prvočísel. Pomocí postupného dělení (zkoušíme prvočísla od čísla 2) pak napíšeme do pravého sloupce nalezeného prvočíselného dělitele (do prvního řádku). Rozkládané číslo vydělíme nalezeným prvočíselným dělitelem a výsledek zapíšeme do druhého řádku v levém sloupci. Znovu hledáme prvočíselného dělitele, který dělí nově získané číslo, a tohoto dělitele zapíšeme do pravého sloupce. Tento postup opakujeme, dokud nedostaneme v levém sloupci číslo 1. V tu chvíli je prvočíselný rozklad dokončen a v pravém sloupci máme zapsána prvočísla, která v součinu tvoří hledaný prvočíselný rozklad. Tento postup si ukážeme na prvočíselném rozkladu složeného čísla 210.

210	**2**
105	**3**
35	**5**
7	**7**
1	

Obrázek 9 Tabulková metoda

Prvočíselný rozklad čísla $210 = 2 \cdot 3 \cdot 5 \cdot 7$.

1.2.2 METODA ŘÁDKOVÁ

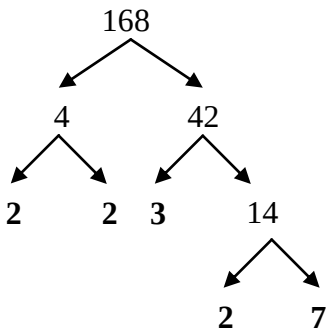
V řádkové metodě zapisujeme postupný rozklad do řádky. Zapíšeme rozkládané číslo a za něho rovnítko (symbol $=$). Hledáme prvního prvočíselného dělitele. Po jeho nalezení zapíšeme rozkládané číslo jako součin nalezeného prvočíselného dělitele a rozkládaného čísla vyděleného tímto prvočíselným dělitelem. Za tento součin opět napíšeme rovnítko a hledáme dalšího dělitele. Postupujeme tak dlouho, dokud za rovnítkem není pouze součin prvočísel. Metodu si ukážeme na rozkladu složeného čísla 330.

$$330 = 2 \cdot 165 = 2 \cdot 3 \cdot 55 = \underline{2 \cdot 3 \cdot 5 \cdot 11}$$

Prvočíselný rozklad čísla $330 = 2 \cdot 3 \cdot 5 \cdot 11$.

1.2.3 METODA GRAFICKÁ

V této metodě, někdy nazývaná strom, si napíšeme rozkládané číslo a zapíšeme pod něho dvě šipky, které tvoří obrácené písmeno V (∧). Pod první šipku napíšeme nalezeného dělitele a pod druhou šipku napíšeme výsledek po dělení rozkládaného čísla nalezeným dělitelem. Pokud tato čísla nejsou prvočísla, tak pod tyto čísla opět zapíšeme šipky a postup opakujeme. Na konci nám pod šipkami zůstanou pouze prvočísla, která tvoří hledaný prvočíselný rozklad. Metodu si ukážeme na rozkladu složeného čísla 168.



Obrázek 10 Grafická metoda (strom)

Prvočíselný rozklad čísla $168 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7$.

1.3 PRVOČÍSELNÝ TEST

Jednou z velmi důležitých vlastností v teorii čísel je určit, zda je dané číslo prvočíslem nebo číslem složeným. Mohlo by nás napadnout, že je cílem zjistit, jestli lze určit faktorizaci (rozložit číslo na součin prvočísel) a pokud tuto faktorizaci nelze určit, učiníme závěr, že je dané číslo prvočíslem. Tento postup ale nepatří k nejrychlejším a nejjednodušším. K potvrzení či vyvrácení prvočíselnosti nám pomohou tzv. prvočíselné testy (někdy také označovány testy prvočíselnosti), které se nespoléhají na faktorizaci. Je nutné říci, že prvočíselné testy nám nedají žádnou informaci o faktorech (činitelé vyskytující se ve faktorizaci daného čísla). Protože všechna známá prvočísla jsou až na prvočíslo 2 lichá, budeme v následujících testech a metodách uvažovat, že prvočísla jsou obecně lichá čísla. Dalo by se říci, že všechny testy prvočíselnosti mají následující podobu.

Pokud dané číslo splňuje určité podmínky (má určitou vlastnost, lze zapsat určitým způsobem), je prvočíslem, jinak je číslem složeným. (3)

Většina prvočíselných testů je poměrně složitá nebo použitelná pouze pro některá čísla, která lze vyjádřit v nějakém speciálním tvaru. Tímto je například Prothova věta.

Věta: Předpokládejme, že číslo x má tvar $x = h \cdot 2^n + 1$, kde $2^n > h$ a h je liché číslo. Pokud existuje celé číslo a takové, že platí:

$$a^{\left(\frac{x-1}{2}\right)} \equiv -1 \ (mod\ x),$$

tak je číslo x prvočíslem. (2)

Naštěstí existují i prvočíselné testy, které jsou po matematické stránce jednoduché, a jejich výpočet je rychlý. Bohužel mohou v určitých případech selhat. Vždy se jedná o selhání, kdy je složené číslo označeno jako prvočíslo, opačně se tato chyba nevyskytuje (někdy proto bývají tyto testy označovány jako testy složených čísel). Tímto testem je například Fermatův prvočíselný test.

1.3.1 FERMATŮV PRVOČÍSELNÝ TEST

Fermatovým prvočíselným testem je tzv. Fermatova malá věta.

Fermatova malá věta: Nechť p je prvočíslo a přirozené číslo a je nesoudělné s p. Pak platí:

$$a^{p-1} \equiv 1 \ (mod\ p) \ (5).$$

Ukázku testování prvočíselnosti pomocí Fermatova prvočíselného testu si ukážeme na číslu 67.

$$a^{p-1} \equiv 1 \ (mod\ p)$$

$$2^{66} \equiv x \ (mod\ 67)$$

$$2^5 \equiv 32 \ (mod\ 67)$$

$$2^6 \equiv 64 \ (mod\ 67)$$

$$2^6 \equiv -3 \ (mod\ 67)$$

$$2^5 \cdot 2^6 \equiv 32 \cdot (-3) \ (mod\ 67)$$

$$2^{11} \equiv -96 \ (mod\ 67)$$

$$2^{11} \equiv 38 \ (mod\ 67)$$

$$(2^{11})^3 \equiv 38^3 \ (mod\ 67)$$

$$2^{33} \equiv 54\,872 \ (mod\ 67)$$

$$2^{33} \equiv 66 \ (mod\ 67)$$

$$2^{33} \equiv -1 \ (mod\ 67)$$

$$(2^{33})^2 \equiv (-1)^2 \ (mod\ 67)$$

$$\underline{\underline{2^{66} \equiv 1 \ (mod\ 67)}}$$

Pomocí Fermatova prvočíselného testu jsme určili, že číslo 67 je prvočíslem.

Jak již bylo řečeno dříve, tento test není naprosto spolehlivý. Například pro číslo $341 = 11 \cdot 31$ (je vidět, že jde o číslo složené) platí Fermatova malá věta:

$$2^{340} \equiv 1 \ (mod\ 341).$$

Pro ukázku provedeme výpočet.

$$2^{340} \equiv x \ (mod\ 341)$$

$$2 \equiv 2 \ (mod\ 341)$$

$$2^5 \equiv 2^5 \ (mod\ 341)$$

$$2^5 \equiv 32 \ (mod\ 341)$$

$$(2^5)^2 \equiv 32^2 \ (mod\ 341)$$

$$2^{10} \equiv 1 \ (mod\ 341)$$

$$(2^{10})^{34} \equiv 1^{34} \ (mod\ 341)$$

$$\underline{\underline{2^{340} \equiv 1 \ (mod\ 341)}}$$

$2^{340} \equiv 1 \ (mod\ 341)$, přesto $341 = 11 \cdot 31$.

Z tohoto důvodu bývá někdy používána věta opačná označovaná jako Fermatův test složených čísel.

Věta: Pokud je N liché číslo a existuje celé číslo a takové, pro které platí $nsd(a, N) = 1$, a platí:

$$a^{N-1} \not\equiv 1 \ (mod\ N),$$

pak je N složené číslo. (3)

1.3.2 EULERŮV PRVOČÍSELNÝ TEST

Eulerův prvočíselný test vychází z tzv. Eulerova kritéria.

Eulerovo kritérium: Nechť je $nsd(a,p)=1$. Pokud platí:

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

tak je p prvočíslo. (3)

V Eulerovu kritériu nám $\left(\frac{a}{p}\right)$ značí Legendreův symbol, který je multiplikativní funkcí s hodnotami $1, 0, -1$.

Definice: Nechť p je liché prvočíslo. Celé číslo a se označuje kvadratický zbytek, pokud je modulo kongruentní druhé mocnině nějakého celého čísla x ($x^2 \equiv a\ (mod\ p)$), v opačném případě se nazývá kvadratický nezbytek. Legendreův symbol je funkce dvou proměnných p a a definovaná následovně:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ pokud } a \text{ je kvadratický zbytek modulo } p \text{ a } a \not\equiv 0\ (mod\ p) \\ -1 \text{ pokud } a \text{ je kvadratický nezbytek modulo } p \\ 0 \text{ pokud } a \equiv 0\ (mod\ p). \end{cases} (6)$$

Protože jsou v našem případě a a p nesoudělné, může Legendreův symbol $\left(\frac{a}{p}\right)$ nabývat pouze hodnot 1 a -1. Drobnou úpravou Eulerova kritéria získáme Eulerův prvočíselný test.

Eulerův prvočíselný test: Pokud je p prvočíslo, pak existuje celé číslo a takové, pro které platí $nsd(a,p)=1$ a platí:

$$a^{\left(\frac{p-1}{2}\right)} \equiv \pm 1\ (mod\ p).\ (3)$$

Ukázku testování prvočíselnosti pomocí Eulerova prvočíselného testu si ukážeme na číslu 61.

$$a^{\left(\frac{p-1}{2}\right)} \equiv \pm 1 \ (mod\ p)$$

$$2^{30} \equiv x \ (mod\ 61)$$

$$2^{5} \equiv 32 \ (mod\ 61)$$

$$(2^{5})^{2} \equiv 32^{2} \ (mod\ 61)$$

$$2^{10} \equiv 48 \ (mod\ 61)$$

$$2^{5} \cdot 2^{10} \equiv 32 \cdot 48 \ (mod\ 61)$$

$$2^{15} \equiv 11 \ (mod\ 61)$$

$$(2^{15})^{2} \equiv 11^{2} \ (mod\ 61)$$

$$2^{30} \equiv 121 \ (mod\ 61)$$

$$\underline{\underline{2^{30} \equiv -1 \ (mod\ 61)}}$$

Pomocí Eulerova prvočíselného testu jsme určili, že je číslo 61 prvočíslem.

Stejně jako Fermatův test prvočíselnosti, není Eulerův test prvočíselnosti zcela spolehlivý.

Například pro číslo $561 = 3 \cdot 11 \cdot 17$ (je vidět, že jde o číslo složené) vychází Eulerův test prvočíselnosti: $2^{280} \equiv 1 \ (mod\ 561)$.

$$2^{280} \equiv x \ (mod\ 561)$$

$$2^{10} \equiv 463 \ (mod\ 561)$$

$$(2^{10})^{2} \equiv 463^{2} \ (mod\ 561)$$

$$2^{20} \equiv 67 \ (mod\ 561)$$

$$(2^{20})^{2} \equiv 67^{2} \ (mod\ 561)$$

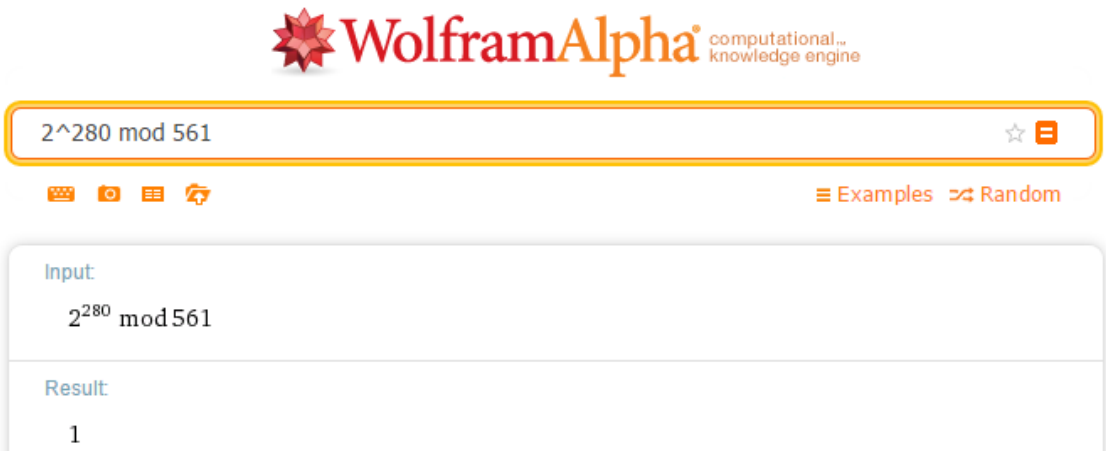
$$2^{40} \equiv 1 \ (mod\ 561)$$

$$(2^{40})^{7} \equiv 1^{7} \ (mod\ 561)$$

$$\underline{\underline{2^{280} \equiv 1 \ (mod\ 561)}}$$

$2^{280} \equiv 1 \ (mod\ 561)$, přesto $561 = 3 \cdot 11 \cdot 17$.

Výsledek můžeme překontrolovat pomocí nástroje Wolfram|Alpha. Jedná se o matematický nástroj, který je dostupný na internetové stránce www.wolframalpha.com. Zde stačí zadat příklad jako příkaz do vstupního pole a nástroj Wolfram|Alpha nám zobrazí výsledek v kolonce Result (u řady výpočtů nám nabídne i graf, případně zjednodušenou formu výrazu). Pro zobrazení našeho výsledku použijeme příkaz $2\text{^}280\ mod\ 561$. Symbol ^ se používá pro zapsání mocniny do matematických programů, kde nám odděluje základ mocniny (mocněnec) a exponent (mocnitel), například 2^5 zapíšeme jako $2\text{^}5$.



Obrázek 11 Ukázka výpočtu v nástroji Wolfram|Alpha

Protože u některých složených čísel dojde u Eulerova testu prvočíselnosti k označení složeného čísla prvočíslem, bývá někdy používána věta opačná označovaná jako Eulerův test složených čísel.

Věta: Pokud je N liché číslo a existuje celé číslo a takové, pro které platí $nsd(a, N) = 1$ a platí:

$$a^{\left(\frac{N-1}{2}\right)} \not\equiv \pm 1\ (mod\ N),$$

pak je N složené číslo. (3)

2 PSEUDOPRVOČÍSLA A SILNĚJŠÍ PRVOČÍSELNÉ TESTY

V předchozí kapitole jsme rozlišovali pouze prvočísla a čísla složená. Nyní se zaměříme na čísla, která jsou čísla složená, ale podle testu prvočíselnosti jsou označena za prvočísla. Příkladem jsou již dříve zmiňovaná čísla 341 a 561. Další je například číslo 645 (ověříme Fermatovým testem prvočíselnosti).

$$2^{644} \equiv x \ (mod\ 645)$$

$$2^{11} \equiv 2048 \ (mod\ 645)$$

$$2^{11} \equiv 113 \ (mod\ 645)$$

$$(2^{11})^2 \equiv 113^2 \ (mod\ 645)$$

$$2^{22} \equiv 12\,769 \ (mod\ 645)$$

$$2^{22} \equiv 514 \ (mod\ 645)$$

$$2^{22} \cdot 2 \equiv 514 \cdot 2 \ (mod\ 645)$$

$$2^{23} \equiv 1028 \ (mod\ 645)$$

$$2^{23} \equiv 383 \ (mod\ 645)$$

$$(2^{23})^2 \equiv 383^2 \ (mod\ 645)$$

$$2^{46} \equiv 146\,689 \ (mod\ 645)$$

$$2^{46} \equiv 274 \ (mod\ 645)$$

$$(2^{46})^2 \equiv 274^2 \ (mod\ 645)$$

$$2^{92} \equiv 75\,076 \ (mod\ 645)$$

$$2^{92} \equiv 256 \ (mod\ 645)$$

$$(2^{92})^7 \equiv 256^7 \ (mod\ 645)$$

$$\underline{\underline{2^{644} \equiv 1 \ (mod\ 645)}}$$

$2^{644} \equiv 1 \ (mod\ 645)$, přesto $645 = 3 \cdot 5 \cdot 43$.

2.1 PSEUDOPRVOČÍSLA

Složená čísla, která jsou Fermatovým testem prvočíselnosti (případně jiným testem prvočíselnosti) označena jako prvočísla, například číslo 341, se nazývají pseudoprvočísla (falešná prvočísla). Pro úplnou přesnost uvedeme definici.

Definice: Liché složené číslo N, pro něž platí:

$$a^{N-1} \equiv 1 \ (mod\ N),$$

se nazývá **pseudoprvočíslo** pro základ (bázi) a. (3)

Obecně se před termín pseudoprvočíslo dává označení podle toho, kterým testem bylo označeno za prvočíslo. V tomto případě se tedy jedná o Fermatova pseudoprvočísla. Pokud nalezneme na výraz pseudoprvočíslo, předpokládá se, že se jedná o Fermatovo pseudoprvočíslo.

V tabulce je ukázka pseudoprvočísel (do 1000) pro základy do čísla 22.

Základ	Fermatova pseudoprvočísla
2	341, 561, 645
3	91, 121, 286, 671, 703, 949
4	15, 85, 91, 341, 435, 451, 561, 645, 703
5	4, 124, 217, 561, 781
6	35, 185, 217, 301, 481
7	6, 25, 325, 561, 703, 817
8	9, 21, 45, 63, 65, 105, 117, 133, 153, 231, 273, 341, 481, 511, 561, 585, 645, 651, 861, 949
9	4, 8, 28, 52, 91, 121, 205, 286, 364, 511, 532, 616, 671, 697, 703, 946, 949
10	9, 33, 91, 99, 259, 451, 481, 561, 657, 703, 909
11	10, 15, 70, 133, 190, 259, 305, 481, 645, 703, 793
12	65, 91, 133, 143, 145, 247, 377, 385, 703
13	4, 6, 12, 21, 85, 105, 231, 244, 276, 357, 427, 561
14	15, 39, 65, 195, 481, 561, 781, 793, 841, 985
15	14, 341, 742, 946
16	15, 51, 85, 91, 255, 341, 435, 451, 561, 595, 645, 703
17	4, 8, 9, 16, 45, 91, 145, 261, 781
18	25, 49, 65, 85, 133, 221, 323, 325, 343, 425, 451, 637, 931
19	6, 9, 15, 18, 45, 49, 153, 169, 343, 561, 637, 889, 905, 906
20	21, 57, 133, 231, 399, 561, 671, 861, 889
21	4, 10, 20, 55, 65, 85, 221, 703, 793
22	21, 69, 91, 105, 161, 169, 345, 483, 485, 645, 805

Tabulka 1 - Pseudoprvočísla do 1000 pro základy do 22

Fermatova pseudoprvočísla se základem 2 se nazývají Pouletova čísla.

Definice: Pouletova čísla jsou Fermatova 2–pseudoprvočísla, tedy lichá složená čísla N, pro která platí:

$$2^{N-1} \equiv 1\ (mod\ N).\ (6)$$

První Pouletova čísla jsou $341, 561, 645, 1105, 1387$ …

Nyní, když známe čísla, ve kterých Fermatův test prvočíselnosti selže, se nabízí myšlenka dokonalejšího prvočíselného testu. Pokud projde číslo Fermatovým testem jako prvočíslo, stačí porovnat, zda není pseudoprvočíslem. Tímto testem se budeme zabývat v části Příklady silnějších prvočíselných testů 2.2.

2.1.1 CARMICHAELOVA ČÍSLA

Pro složená čísla N nebývá složité nalezení čísla a, nejčastěji metodou experimentu, které splňuje rovnost $a^{N-1} \not\equiv 1\ (mod\ N)$. Proto ve většině případů pro malé a vrací Fermatův test prvočíselnosti N jako číslo složené. Ovšem existují složená čísla N taková, že $a^{N-1} \equiv 1\ (mod\ N)$ pro všechna a, pro která platí $nsd(a, N) = 1$. Tato speciální čísla se nazývají Carmichaelova čísla (jsou pojmenována po americkém matematikovi Robertu Danielovi Carmichaelovi). Nejmenším z těchto čísel je číslo 561.

Definice: Složená čísla N, taková že platí $a^{N-1} \equiv 1\ (mod\ N)$ pro všechna a splňující $nsd(a, N) = 1$, se nazývají **Carmichaelova čísla**. (3)

Všechna Carmichaelova čísla jsou Fermatovým testem prvočíselnosti označena jako prvočísla. Další Carmichaelova čísla jsou například čísla $1105, 1729, 2465, 2821$ a 6601.

V současné době existuje nespočet vzorců (předpisů), podle kterých lze najít Carmichaelova čísla. Nejznámějším vzorcem je $N = (6t + 1) \cdot (12t + 1) \cdot (18t + 1)$, ve kterém musí platit, že každý z faktorů ($6t + 1, 12t + 1$ a $18t + 1$) musí být prvočíslem pro stejný parametr t. Například pokud $t = 1$, dostaneme $N = 7 \cdot 13 \cdot 19 = 1729$. Žádná z těchto formulí pro získání Carmichaelových čísel není bohužel schopna vygenerovat všechna tato čísla.

Musíme však říci, že jsou Carmichaelova čísla spíše vzácná. Existuje pouze 2163 Carmichaelových čísel, která jsou menší jak $25 \cdot 10^9$ (25 miliard).

2.1.2 EULEROVA PSEUDOPRVOČÍSLA

Stejně jako v případě jiných pseudoprvočísel, tak i termín Eulerova pseudoprvočísla označuje složená čísla, která Eulerův prvočíselný test označí chybně za prvočísla.

Definice: Lichá složená čísla N, pro která platí:

$$a^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$

a zároveň platí $nsd(a, N) = 1$, se nazývají **Eulerova prvočísla** se základem a.

Eulerovým pseudoprvočíslem je například číslo 1729.

2.1.3 SILNÁ PSEUDOPRVOČÍSLA

Myšlenka použití Eulerova kritéria místo Fermatova testu prvočíselnosti v rozlišování mezi prvočíslem a číslem složeným nás posune ještě o kousek dále. Přitom se dostáváme k pojmu silné pseudoprvočíslo.

Definice: Liché složené číslo N, pro které platí:

$$N - 1 = d \cdot 2^s,$$

kde d je liché číslo a $nsd(a, N) = 1$, je nazýváno **silným pseudoprvočíslem** pro základ a, jestliže platí jedna z podmínek:

$$a^d \equiv 1 \ (mod\ N),$$

$$a^{d \cdot 2^r} \equiv -1 \ (mod\ N),$$

pro nějaké $r = 0, 1, 2, \dots, s - 1$. (3)

Silná pseudoprvočísla pro základ 2 jsou například čísla $2047, 3277$ a 4033.

2.2 PŘÍKLADY SILNĚJŠÍCH PRVOČÍSELNÝCH TESTŮ

Nyní se zaměříme na úpravy prvočíselných testů a silné prvočíselné testy, které odhalují prvočísla a čísla složená téměř bez chyb (jsou bezchybné do určitého čísla).

2.2.1 KOMBINACE FERMATOVA TESTU A SEZNAMU PSEUDOPRVOČÍSEL

Nastala myšlenka, že pokud bychom znali všechna pseudoprvočísla určité báze, pak by bylo možné spojit Fermatův test prvočíselnosti pro tuto bázi se seznamem pseudoprvočísel. Výsledkem by byl rychlý a spolehlivý prvočíselný test (při použití na počítači).

Bohužel je tento test rychlý pouze pro čísla omezené velikosti (řádově do 10^7).

Na tuto myšlenku přišel Derrick Henry Lehmer (test bývá někdy označen jako Lehmerův test prvočíselnosti), který jako první sestavil přehled Fermatových pseudoprvočísel menších než 10^7 pro základ 2.

Pro větší čísla ($10^7 - 2 \cdot 10^8$) připravil Lehmer následující schéma (zkoumané číslo je označeno jako N):

1. Použijte metodu postupného dělení 65 prvočísly, která jsou menší než 313. Pokud je nalezen nějaký dělitel, je N složeným číslem.
2. Vypočtěte $2^{N-1}\ (mod\ N)$, pokud je výsledek různý od čísla 1,
$$2^{N-1} \not\equiv 1\ (mod\ N),$$
tak je N složeným číslem.
3. Zjistěte, zda je N v seznamu pseudoprvočísel. Pokud seznam obsahuje N, pak je N složené číslo. Jinak je N prvočíslem.

Tento test později rozšířili Carl Pomerance, John Selfridge a Samuel Wagstaff. Šlo o rozšíření seznamu pseudoprvočísel o další báze ($3, 5$ a 7). Také bylo možné test použít pro čísla do $25 \cdot 10^9$.

2.2.2 SILNÝ PSEUDOPRVOČÍSELNÝ TEST

Dalším velmi spolehlivým testem, který téměř nechybuje, je silný pseudoprvočíselný test. Tento test vychází z Eulerova prvočíselného testu. Využívá ovšem testování více základů. Prověřování tohoto testu ukázalo, že testováním pomocí Eulerova testu až do základu 11 jsou správně určena všechna čísla menší než $2\,152\,302\,898\,747$.

Při testování i dalších základů 13 a 17 test selže až u čísla $341\,550\,071\,728\,321$.

V samotném testu se samozřejmě rovnou neprovádí testování všech těchto základů $(2, 3, 5, 7, 11, 13, 17)$. Testování se provádí postupně, nejdříve na základu 2. Pokud by základ 2 tímto testem prošel, testuje se další základ.

Obecné schéma tohoto testu, který lze spolehlivě použít pro čísla menší jak $341\,550\,071\,728\,321$, vypadá následovně:

1. Zkontrolujte, zda číslo N splňuje Eulerovo kritérium pro základ 2.
$$2^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$
Pokud ne, pak je N složeným číslem.

2. Zkontrolujte, zda číslo N splňuje Eulerovo kritérium pro základ 3.
$$3^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$
Pokud ne, pak je N složeným číslem.

3. Je-li $N < 1\,373\,653$, pak N je prvočíslem. Je-li $N \geq 1\,373\,653$, zkontrolujte, zda splňuje Eulerovo kritérium pro základ 5.
$$5^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$
Pokud ne, pak je N složeným číslem.

4. Je-li $N < 25\,326\,001$, pak N je prvočíslem. Je-li $N \geq 25\,326\,001$, zkontrolujte, zda splňuje Eulerovo kritérium pro základ 7.

$$7^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$

Pokud ne, pak je N složeným číslem.

5. Je-li $N < 3\,215\,031\,751$, pak N je prvočíslem. Je-li $N \geq 3\,215\,031\,751$, zkontrolujte, zda splňuje Eulerovo kritérium pro základ 11.

$$11^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$

Pokud ne, pak je N složeným číslem.

6. Je-li $N < 2\,152\,302\,898\,747$, pak N je prvočíslem. Je-li $N \geq 2\,152\,302\,898\,747$, zkontrolujte, zda N splňuje Eulerovo kritérium pro základ 13.

$$13^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$

Pokud ne, pak je N složeným číslem.

7. Je-li $N < 3\,474\,749\,660\,383$, pak N je prvočíslem. Pokud $N \geq 3\,474\,749\,660\,383$, zkontrolujte, zda splňuje Eulerovo kritérium pro základ 17.

$$17^{\left(\frac{N-1}{2}\right)} \equiv \pm 1 \ (mod\ N)$$

Pokud ne, pak N je složeným číslem.

Ze schématu je vidět, že pokud testujeme malé číslo, nemusíme využít všechny kroky.

Ukázku testování pomocí tohoto testu si předvedeme na testování složeného čísla 341, které Fermatův prvočíselný test chybně označil za prvočíslo.

1. Zkontrolujeme, zda číslo 341 splňuje Eulerovo kritérium pro základ 2.

$$2^{\left(\frac{341-1}{2}\right)} \equiv^{?} \pm\ 1\ (mod\ 341)$$

$$2^{170} \equiv x\ (mod\ 341)$$

$$2^{10} \equiv 1024\ (mod\ 341)$$

$$2^{10} \equiv 1\ (mod\ 341)$$

$$(2^{10})^{17} \equiv 1^{17}\ (mod\ 341)$$

$$\underline{\underline{2^{170} \equiv 1\ (mod\ 341)}}$$

Zde Eulerovo kritérium platí. Přejdeme na další krok.

2. Zkontrolujte, zda číslo 341 splňuje Eulerovo kritérium pro základ 3.

$$3^{\left(\frac{341-1}{2}\right)} \equiv^{?} \pm\ 1\ (mod\ 341)$$

$$3^{170} \equiv x\ (mod\ 341)$$

$$3^{6} \equiv 729\ (mod\ 341)$$

$$3^{6} \equiv 47\ (mod\ 341)$$

$$(3^{6})^{2} \equiv 47^{2}\ (mod\ 341)$$

$$3^{12} \equiv 163\ (mod\ 341)$$

$$3^{12} \cdot 3^{5} \equiv 163 \cdot 3^{5}\ (mod\ 341)$$

$$3^{17} \equiv 53\ (mod\ 341)$$

$$(3^{17})^{5} \equiv 53^{5}\ (mod\ 341)$$

$$3^{85} \equiv 254\ (mod\ 341)$$

$$(3^{85})^{2} \equiv 254^{2}\ (mod\ 341)$$

$$\underline{\underline{3^{170} \equiv 67\ (mod\ 341) \Rightarrow}}\ 3^{170} \not\equiv \pm 1\ (mod\ 341)$$

Zde Eulerovo kritérium neplatí, a proto je číslo 341 číslem složeným.

K určení tohoto čísla nám stačili pouze dva kroky ze sedmi kroků tohoto prvočíselného testu. Jedná se proto o rychlý test. S většími čísly se časová náročnost zvětšuje, ale oproti jiným prvočíselným testům je stále nízká.

2.3 MODERNÍ PRVOČÍSELNÉ TESTY

V této části se zaměříme na dva moderní prvočíselné testy, které jsou implementovány do řady matematických softwarů, jako je například Maple, Wolfram Mathematica a MATLAB (pouze MATLAB nám na svých internetových stránkách uvádí informaci o používaném prvočíselném testu, ostatní uvádí pouze informaci, že využívají jeden z moderních prvočíselných testů). Většina těchto testů je založena na existenci rovností, které neplatí obecně, ale pouze pro prvočísla. Předností těchto testů je rychlost.

2.3.1 MILLER-RABINŮV TEST PRVOČÍSELNOSTI

Jedná se o jeden z prvních „moderních“ počítačových testů prvočíselnosti vyvinutý Gary Lee Millerem a Michaelem Ozer Rabinem.

Autorem první verze tohoto testu je Gary Lee Miller. Tato verze byla rychlá, bohužel však závislá na Riemannově hypotéze (všechny netriviální nulové body Riemannovy „zéta“ funkce mají reálnou část rovnu $\frac{1}{2}$.), která nebyla dosud dokázána ani vyvrácena.

Michael O. Rabin na základě verze Gary L. Millera vyvinul dnes používanou verzi tohoto testu, která nezávisí na ničem nedokázaném. Jedná se však o pravděpodobnostní test, tedy čím vícekrát ho provedeme, tím je výsledek pravděpodobnější.

Jako většina testů prvočíselnosti, tak i Miller-Rabinův test je založen na platnosti rovností pro testované číslo a zcela jisti si můžeme být pouze v případě výsledku, že testované číslo je číslem složeným. Miller-Rabinův test určuje prvočíselnost čísla N následujícím způsobem.

Předpokladem je testování lichého čísla (až na číslo 2, jsou všechna sudá čísla složenými čísly, a tedy jedním z faktorů je právě číslo 2). Pokud je N liché, je možné jej vyjádřit ve tvaru $2^s \cdot d + 1$, kde s a d jsou celá čísla a d je liché.

Tento test je založen na pokusu o nalezení čísla $a < n$, pro které by platily následující kongruence:

$$a^d \not\equiv 1 \ (mod\ N) \text{ a}$$

$$a^{2^r d} \not\equiv -1 \ (mod\ N), \text{ pro všechna } 0 \leq r \leq s - 1.$$

Pokud je takové a nalezeno, je číslo N složeným číslem. Pro tento test si číslo a volíme, takže je možné pro různé volby čísla a dospět k různým výsledkům. Jedná tedy o nedeterministický test (při stejné vstupní hodnotě nám může dát různé výsledky).

Ukázku testování si ukážeme na složeném číslu 221.

$$N = 221 = 2^2 \cdot 55 + 1,$$

takže $s = 2$ a $d = 55$. Zvolíme $a = 174$ a určíme, zda platí kongruence uvedené výše.

$$174^{55} \equiv 47\ (mod\ 221) \Rightarrow a^d \not\equiv 1\ (mod\ N)$$

$$174^{2^0 \cdot 55} \equiv 47\ (mod\ 221) \Rightarrow a^{2^r d} \not\equiv -1\ (mod\ N)$$

$$174^{2^1 \cdot 55} \equiv 220\ (mod\ 221)$$

$$174^{2^1 \cdot 55} \equiv -1\ (mod\ 221) \Rightarrow a^{2^r d} \equiv -1\ (mod\ N)$$

Vidíme, že poslední kongruence $a^{2^r d} \not\equiv -1\ (mod\ N)$, pro $r = 1$ neplatí. Takže je číslo 221 pravděpodobně prvočíslem (jde o výsledek testu, víme že $221 = 13 \cdot 17$ a je složeným číslem), ale abychom měli jistotu, zvolíme ještě jinou hodnotu čísla $a = 137$.

$$137^{55} \equiv 188\ (mod\ 221) \Rightarrow a^d \not\equiv 1\ (mod\ N)$$

$$137^{2^0 \cdot 55} \equiv 188\ (mod\ 221) \Rightarrow a^{2^r d} \not\equiv -1\ (mod\ N)$$

$$137^{2^1 \cdot 55} \equiv 205\ (mod\ 221) \Rightarrow a^{2^r d} \not\equiv -1\ (mod\ N)$$

Pro $a = 137$ platí všechny kongruence a výsledkem testu je, že číslo 221 je složeným číslem.

V matematických softwarech dochází k náhodnému zvolení 25 různých hodnot čísla a (pokud je to vzhledem k podmínce $a < N$ možné) a je prokázáno, že pokud je pro všechny testované hodnoty a číslo N vyhodnoceno prvočíslem, je to s pravděpodobností téměř 100% (s pravděpodobností $\frac{1}{4^{25}}$ se jedná o pseudoprvočíslo).

2.3.2 AGRAWAL–KAYAL–SAXENŮV TEST PRVOČÍSELNOSTI

Dalším moderním prvočíselným testem je AKS test, který je pojmenován po svých tvůrcích. Jedná se o matematiky a informatiky Manindra **A**grawala, Neeraje **K**ayala a Nitina **S**axena z Indie. Tento test je prvním deterministickým testem (má pro dané vstupní hodnoty vždy stejnou výslednou hodnotu). Svůj algoritmus pro AKS test autoři publikovali 6. srpna 2002 v dokumentu „PRIMES is in P“ (Prvočísla jsou v P), kde P označuje třídu složitosti řešení problémů, které jsou počítačem řešitelné v polynomiálním čase. Jde o problémy, které jsou řešeny efektivně (dalšími matematickými problémy spadajícími do této třídy složitosti jsou například nalezení nejmenšího společného násobku a největšího společného dělitele). Jedná se také o první zcela nezávislý test prvočíselnosti na Riemannově hypotéze v polynomiálním čase. V roce 2006 autoři přišli s novou zjednodušenou verzí svého testu.

Tento test může být použit k ověření jakéhokoliv čísla, není zde omezení velikostí ani vlastnostmi čísla (třeba Lucas-Lehmerův test lze použít pouze na Mersennova prvočísla).

Test je založen na platnosti následující věty.

Věta: Je-li N prvočíslo, pak platí:

$$g(x)^N \equiv g(x^N)\ (mod\ N),$$

pro všechny polynomy $g(x) \in \mathbb{Z}[x]$. Konkrétně platí:

$$(x + a)^N \equiv x^N + a\ (mod\ N),$$

pro všechny $a \in \mathbb{Z}$. (3)

Pokud tato věta platí jen pro jednu hodnotu a, kde $nsd(a,\ N) = 1$, pak je N prvočíslo. Jedná se o větu, která je zobecněním Fermatovy malé věty pro polynomy.

Protože by však výpočet trval příliš dlouho, je v testu použit následující upravený tvar kongruence:

$$(x + a)^N \not\equiv x^N + a\ \big(mod\ (x^r - 1, N)\big),$$

který je řešitelný v polynomiálním čase (původní kongruence je řešitelná v exponenciálním čase).

Samotná podoba testu má následující tři části:

1. Power test (test mocnin)

   V této části se testuje, jestli číslo N není čtvercem nebo vyšší mocninou. Pokud by bylo, tak je test ukončen a číslo N je vyhodnoceno jako složené číslo.

2. Nastavení hodnoty r.

   Zde dochází nejprve k nalezení nejmenší hodnoty r, pro kterou platí: $O_r(N) > log^2 N$.

   $O_r(N)$ značí multiplikativní řád prvku a výsledkem je nejmenší kladné číslo k, které vyhovuje kongruenci:

   $$N^k \equiv 1 \ (mod\ r),$$

   za podmínky $nsd(N,\ r) = 1$.

   Následně dochází k ověření, zda má číslo N vlastního dělitele z intervalu $\left[2, \sqrt{\varphi(r)} \cdot \log(N)\right]$ (symbol φ značí Eulerovu funkci). Pokud je vlastní dělitel nalezen, test končí a číslo N je vyhodnoceno složeným číslem.

   Pod Eulerovo číselně-teoretickou funkcí $\varphi(m)$ rozumíme funkci na množině nenulových přirozených čísel přiřazující každému nenulovému přirozenému číslu m číslo představující počet nenulových přirozených čísel menších než toto číslo, která jsou s tímto číslem nesoudělná.

3. Binomická kongruence

   V poslední části tohoto testu dochází k testování, zda platí následující kongruence:

   $$(x + a)^N \not\equiv x^N + a \ \left(mod\ (x^r - 1, N)\right),$$

   pro všechny hodnoty $a \in \left[2, \sqrt{\varphi(r)} \cdot \log(N)\right]$.

   Pokud nějaká hodnota a kongruenci vyhovuje, tak je N číslem složeným. Jinak je N prvočíslem.

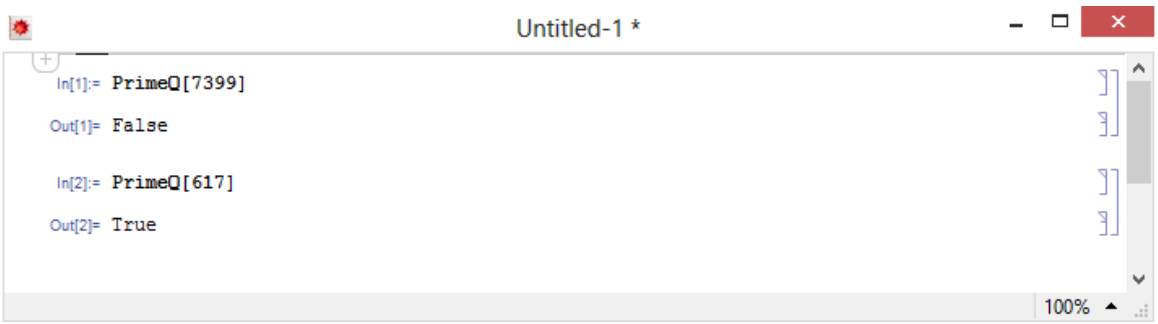
Je obdivuhodné, že na tento test přišli autoři v době, kdy Kayal a Saxena zakončovali bakalářské studium na vysoké škole Indian Institute of Technology Kanpur.

2.4 URČENÍ PRVOČÍSELNOSTI V MATEMATICKÝCH SOFTWARECH

V následující části si ukážeme, jak lze pomocí matematických softwarů rozhodnout o prvočíselnosti celého čísla. Za matematické softwary jsem zvolil ty nejrozšířenější, tedy Wolfram Mathematica, Wolfram|Alpha, Maple, MATLAB a GNU OCTAVE (nepatří mezi nejrozšířenější, ale je volně dostupnou obdobou programu MATLAB).

2.4.1 WOLFRAM MATHEMATICA

Wolfram Mathematica je jeden z nejznámějších matematických softwarů. Jako většina nejrozšířenějších matematických softwarů bohužel nemá bezplatnou verzi (za určitou formou bezplatné verze se může považovat nástroj Wolfram|Alpha). Wolfram Mathematica nám nabízí řadu přednastavených matematických operací, které se vyvolávají příkazy. Mezi příkazy nalezneme i ty, díky kterým se dozvíme, zda je nějaké číslo prvočíslem. Jedná se o příkaz $PrimeQ$. Použití si ukážeme na určení čísel 7399 a 617. Zkoumané číslo zadáváme za příkaz do hranatých závorek ($PrimeQ[7399]$).

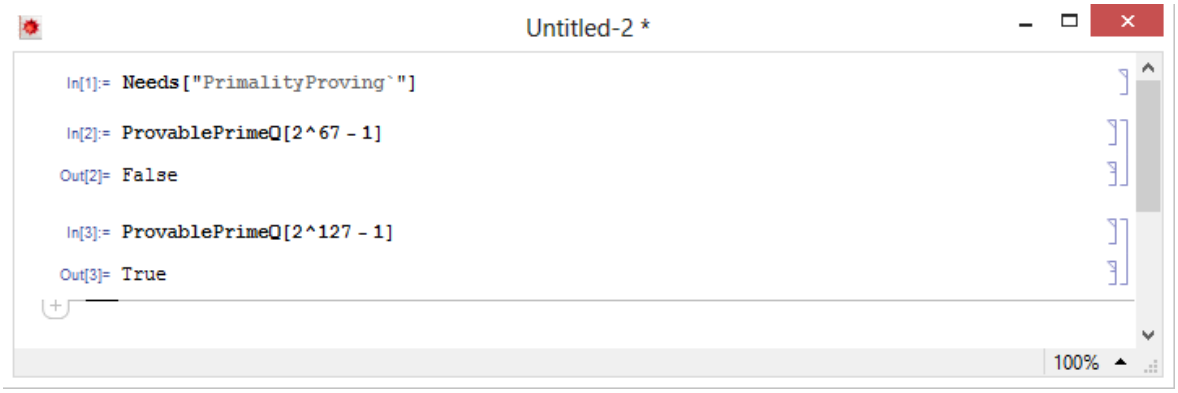


Obrázek 12 Určení prvočíselnosti v programu Wolfram Mathematica

Na obrázku vidíme, že pokud je testované číslo prvočíslem, tak nám program vrátí hodnotu True (pravda). V opačném případě je vrácená hodnota False (nepravda).

Stejně jako u testů prvočíselnosti zde platí, že test není zcela bezchybný (pro mnohaciferná čísla). Wolfram Mathematica nám nabízí rozšířenou operaci, která není součástí základní instalace (u verze Wolfram Mathematica 8), ale můžeme ji získat. Získání dalších funkcí se provádí stažením package (balíček operací). Balíček pro testy prvočíselnosti se jmenuje $PrimalityProving$. Stažení se provede vložením příkazu $Needs["PrimalityProving`"]$. Po stažení tohoto balíčků máme dostupnou operaci $ProvablePrimeQ$, která nám říká, zda je u námi testovaného čísla prokazatelné, že je prvočíslem.

Ukázku si provedeme na Mersennových číslech M_{67} a M_{127}. Na obrázku je také vidět vložení balíčku $PrimalityProving$.



Obrázek 13 Prokázání prvočíselnosti v programu Wolfram Mathematica

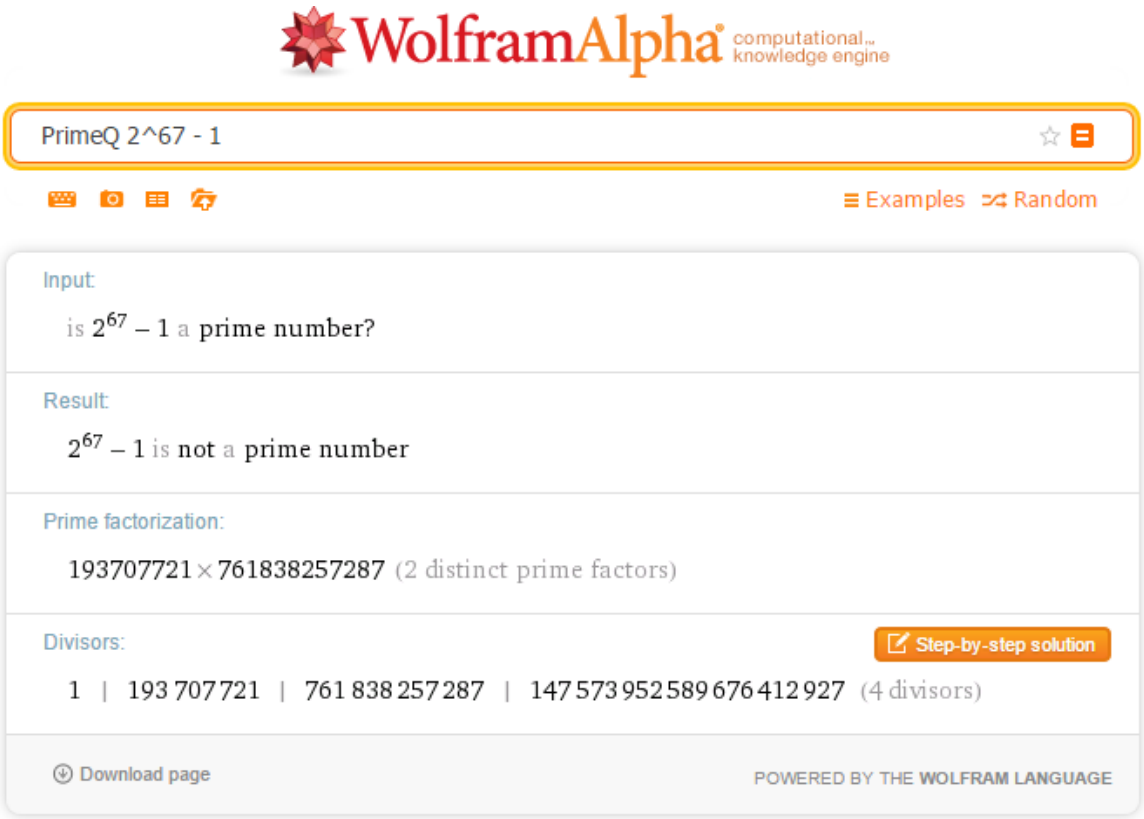
Na obrázku vidíme, že u čísla $M_{67} = 2^{67} - 1$ je hodnota False (nelze prokázat, že je prvočíslem) a u čísla $M_{127} = 2^{127} - 1$ je hodnota True (lze prokázat, že je prvočíslem).

2.4.2 WOLFRAM|ALPHA

Wolfram|Alpha je internetový server, který umožňuje řadu matematických operací. Jedná se o obdobu programu Wolfram Mathematica, která je volně dostupná na internetu. Ve své bezplatné verzi umožňuje přístup k předdefinovaným funkcím, které nám zobrazí výsledek zvolené operace. Placená verze dále zobrazuje postup výpočtu a umožňuje další užitečné funkce.

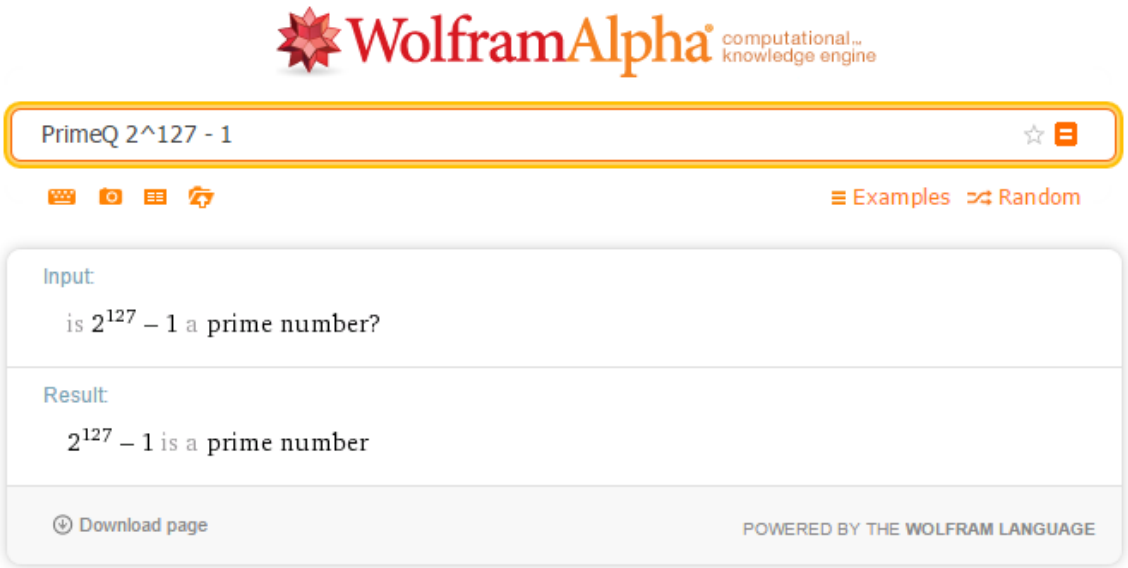
Při určení prvočíselnosti čísla zadáváme stejný příkaz, jako v programu Wolfram Mathematica ($PrimeQ$). Testované číslo za příkazem nemusí být vloženo do závorek.

Použití si ukážeme na Mersennových číslech M_{67} a M_{127}.



Obrázek 14 Určení prvočíselnosti ve Wolfram|Alpha

V řádce Result vidíme, že číslo M_{67} není prvočíslem (is not a prime number) a v následujících řádkách vidíme faktorizaci (Prime factorization) tohoto čísla a jeho dělitele (Divisors).



Obrázek 15 Určení prvočíselnosti ve Wolfram|Alpha 2

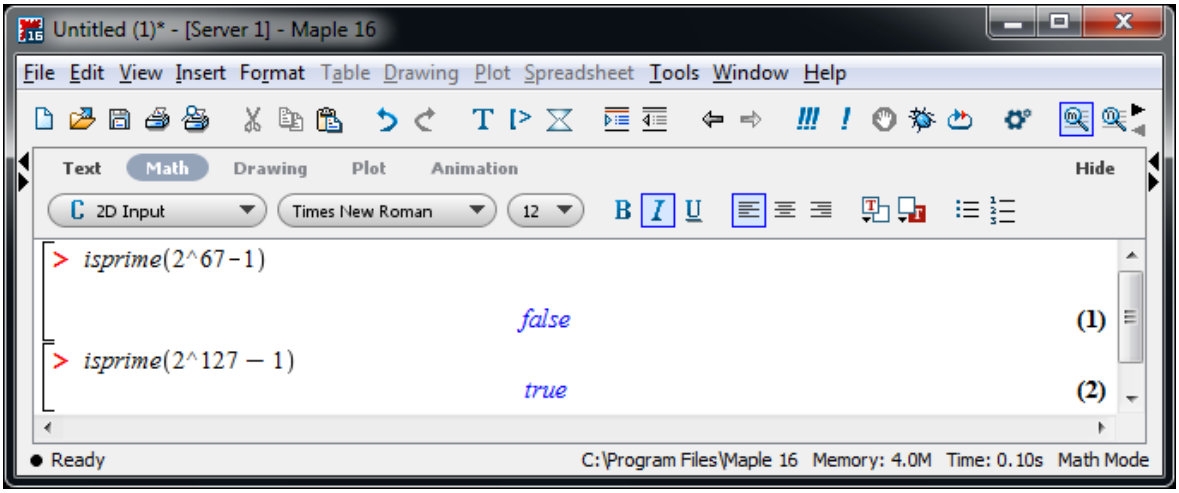
V případě čísla M_{127} dostaneme výsledek, že je prvočíslem (is a prime number).

2.4.3 MAPLE

Maple je dalším z nejrozšířenějších matematických softwarů. Stejně jako Wolfram Mathematica nám Maple nenabízí bezplatnou verzi. Pracuje na základě předdefinovaných funkcí, které se používají pomocí příkazů. Příkaz zapíšeme do jednoho řádku a ve druhém nám program Maple zobrazí výsledek.

Pro určení, zda je zadané číslo prvočíslem, nám v tomto programu slouží příkaz $isprime()$ (jedná se vlastně o otázku „Je prvočíslem?“). Do kulaté závorky za příkaz zapíšeme testované číslo (můžeme zadat i výpočet). Pro zapsání exponentu v matematických programech používáme znak ^, který vkládáme mezi základ a exponent.

Použití si ukážeme, jako v předchozím případě, na Mersennových číslech M_{67} (příkaz: $isprime(2\text{^}67-1)$) a M_{127} (příkaz: $isprime(2\text{^}127-1)$).



Obrázek 16 Určení prvočíselnosti v programu Maple 16

V řádce pod námi zadaným příkazem $isprime(2\text{^}67-1)$ vidíme, že nám program Maple vrátil výsledek $\boldsymbol{false}$ (nepravda), takže číslo M_{67} není prvočíslem. Pro Mersennovo číslo M_{127} nám Maple vrátil výsledek $\boldsymbol{true}$ (pravda), takže číslo M_{127} je prvočíslem.

2.4.4 MATLAB

MATLAB je dalším z nejrozšířenějších matematických programů. Stejně jako předchozí programy, tak i MATLAB nemá bezplatnou verzi. Najdeme zde však program GNU OCTAVE, který je téměř shodný s programem MATLAB a je bezplatný. Programem GNU OCTAVE se budeme zabývat v další podkapitole.

V programu MATLAB najdeme opět řadu předdefinovaných funkcí, které vyvoláme příkazem. Pro určení prvočíselnosti nám MATLAB nabízí příkaz $isprime()$, kde do závorky zapíšeme testované číslo. Jako jediný z komerčních programů nám MATLAB poskytne informaci o způsobu testování. Pro testování prvočíselnosti využívá od verze 7 AKS test, ve starších verzích využíval Miller-Rabinův test.

Oproti předchozím programům nám nevrací program MATLAB hodnoty true nebo false, ale jejich obdobu ve formě čísel 0 (nepravda) a 1 (pravda). Na začátek řádku s návratovou hodnotou navíc přidává označení ans (zkratka pro answer, což značí odpověď nebo řešení).

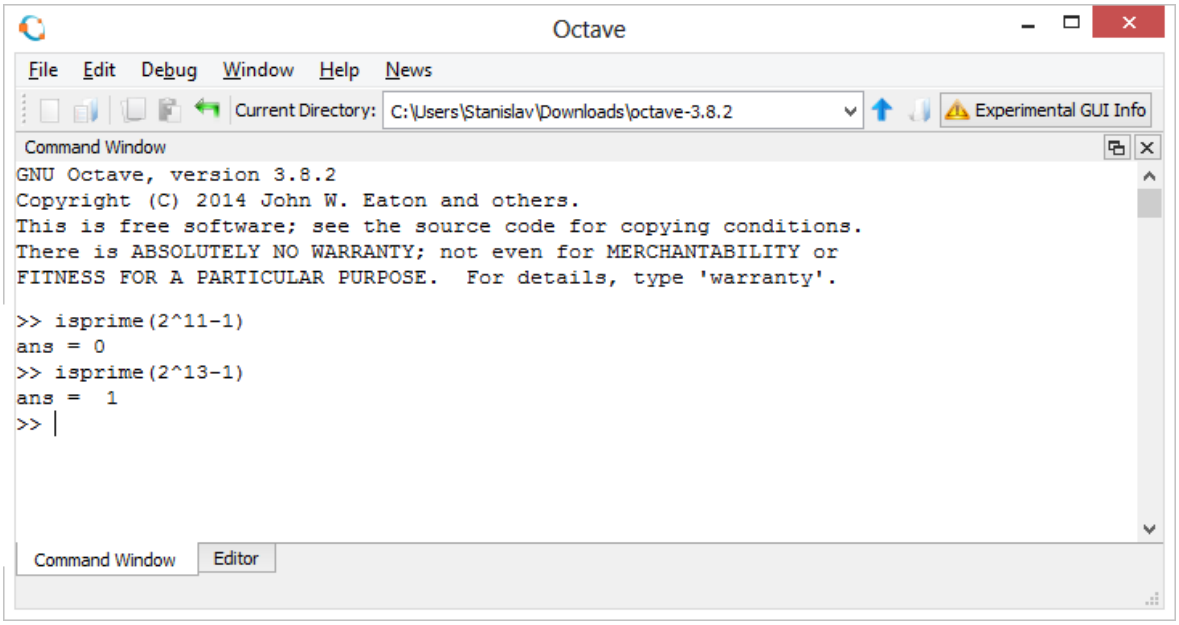
Ukázku si opět ukážeme na Mersennových číslech M_{67} a M_{127}.

Obrázek 17 Určení prvočíselnosti v programu MATLAB

Na obrázku vidíme, že pro číslo M_{67} (příkaz: $isprime(2\text{^}67-1)$) nám program MATLAB vrátil v dalším řádku $ans = 0$. To znamená, že toto číslo není prvočíslem. Druhé číslo M_{127} nám program MATLAB označil prvočíslem ($ans = 1$ značí pravdu).

2.4.5 GNU OCTAVE

Jak již bylo uvedeno v předchozím textu, tak program GNU OCTAVE je bezplatnou obdobou programu MATLAB, který je šířen pod licencí Open Source. Navíc nám program GNU OCTAVE nabízí verzi portable. Většina příkazu se shoduje s příkazy programu MATLAB. I zde máme pro test prvočíselnosti příkaz $isprime()$. Musíme však počítat s tím, že má tento program v základní verzi omezenou velikost paměti pro výpočty. Proto si ukázku ukážeme na Mersennových číslech M_{11} a M_{13}.



Obrázek 18 Určení prvočíselnosti v programu GNU OCTAVE

Na obrázku vidíme, že pro číslo M_{11} (příkaz: $isprime(2\text{^}11-1)$) nám program GNU OCTAVE vrátil v dalším řádku $ans = 0$ (ans značí výsledek a hodnota 0 nepravdu). To znamená, že toto číslo není prvočíslem. Druhé číslo M_{13} nám program GNU OCTAVE označil prvočíslem ($ans = 1$ značí pravdu).

3 KLASICKÉ METODY FAKTORIZACE

Pojem faktorizace označuje v matematice rozklad čísla na součin několika menších čísel. Jedná se tedy například o prvočíselný rozklad. Jako u prvočíselného rozkladu, tak i faktorizace nejčastěji slouží k rozkladu čísla na součin prvočísel a tím prokázání, že rozkládané číslo je složeným číslem.

Přesto, že řada metod faktorizace je známá již stovky let, tak k největšímu rozvoji tohoto matematického problému došlo s rozvojem výpočetní techniky, tedy moderních počítačů.

Některé faktorizační metody, dnes označované jako klasické metody faktorizace, znali již Euklidés, Euler a Fermat. Ale množství početních operací a celková složitost početní práce tyto významné matematiky odradila od faktorizace mnohociferných čísel. Proto je skupina matematiků, kteří se pustili do faktorizace mnohociferných čísel před příchodem výpočetní techniky velmi malá.

Matematikem, který do této malé skupiny patří, je americký matematik Frank Nelson Cole, který dokázal určit faktorizaci 67. Mersennova čísla $M_{67}: 2^{67} - 1$.

$$2^{67} - 1 = 147\,573\,952\,589\,676\,412\,927 = 193\,707\,721 \cdot 761\,838\,257\,287$$

Tento výpočet provedl bez použití počítače a ukazoval ho svým studentům během přednášek na tabuli.

V předchozí kapitole jsme si ukázali, že prokázání prvočíselnosti pomocí prvočíselných testů je poměrně rychlá matematická operace. Naproti tomu faktorizační metody bohužel tak rychlé nejsou. Proto se nejčastěji prováděla faktorizace u čísel, u kterých již bylo prokázáno, že jsou složenými čísly. V následujících podkapitolách si představíme některé metody faktorizace, které jsou označovány za klasické faktorizační metody. Zjistíme, že některé mohou být v určitých případech poměrně rychlé a v jiných může jít o nejhorší možný způsob faktorizace z hlediska časové náročnosti výpočtu.

S rozvojem výpočetní techniky došlo k zabudování algoritmů (postupu výpočtu) těchto metod do matematických programů a faktorizace se stala dostupnější (v případě těchto metod ale nemůžeme mluvit o dostupnosti z hlediska času, tedy časové složitosti). Musíme však říci, že už jsou v dnešní době překonané.

3.1 METODA OPAKOVANÉHO DĚLENÍ

Metoda opakovaného dělení, také označována jako trial division, je jedna z nejstarších metod pro určení faktorů (dělitelů) daného čísla. Bývala také používána jako prvočíselný test, ale vzhledem k časové náročnosti výpočtu, která se s každou další cifrou ve faktorizovaném čísle zvětšuje, bývá označována za nejhorší možnou faktorizační metodu.

Jedná se o postup, kterým se snažíme postupně hledat faktory faktorizovaného čísla pomocí zkušebních dělitelů, dokud nenalezne všechny faktory daného čísla. Prvním zkušebním dělitelem je první prvočíslo, tedy číslo 2. Tímto zkušebním dělitelem dělíme faktorizované číslo, dokud je to možné. Poté zkusíme další prvočíslo, číslo 3, na zbývající část faktorizovaného čísla a tak dále. Tento postup opakujeme, dokud je zbývající část faktorizovaného čísla větší než druhá mocnina zkušebního dělitele.

Výpočet si ukážeme na faktorizaci (hledání faktorů, dělitelů) čísla 7399.

1. Za zkušebního dělitele označíme první prvočíslo 2.

   Máme dělit číslo 7399 číslem 2. Na první pohled vidíme, že číslo 7399 není dělitelné číslem 2 (7399 není sudé). Proto číslo 2 není faktorem čísla 7399.

2. Za zkušebního dělitele označíme další prvočíslo, číslo 3.

   Máme dělit číslo 7399 číslem 3. Na první pohled vidíme, že číslo 7399 není dělitelné číslem 3 (ciferný součet čísla 7399 (28) není dělitelný číslem 3). Proto číslo 3 není faktorem čísla 7399.

3. Za zkušebního dělitele označíme další prvočíslo, číslo 5.

   Máme dělit číslo 7399 číslem 5. Na první pohled vidíme, že číslo 7399 není dělitelné číslem 5 (číslo 7399 nemá na posledním místě cifru 0 nebo 5). Proto číslo 5 není faktorem čísla 7399.

4. Za zkušebního dělitele označíme další prvočíslo, číslo 7.

   Máme dělit číslo 7399 číslem 7. Pomocí kritéria pro dělitelnost sedmi vidíme, že je číslo 7399 dělitelné číslem 7 (Rozdíl zbývající části a dvojnásobku poslední cifry musí být dělitelný 7).

   $$7399 \Rightarrow 739 - 2 \cdot 9 = 739 - 18 = 721 \Rightarrow 72 - 2 \cdot 1 = 72 - 2 = 70$$

Protože je číslo 70 dělitelné číslem 7, je i číslo 7399 dělitelné číslem 7.

Číslo 7 je faktorem čísla 7399. Zbývající část faktorizovaného čísla 7399 je 1057. Protože je i číslo 1057 dělitelné sedmi, je číslo 7 dvojnásobným faktorem čísla 7399. A zbývající částí je číslo 151 ($7399 = 7^2 \cdot 151$).

5. Za zkušebního dělitele označíme další prvočíslo, číslo 11.

   Máme dělit číslo 151 číslem 11. Na první pohled vidíme, že číslo 151 není dělitelné číslem 11 (rozdíl součtu cifer na sudém a lichém místě není dělitelný 11).

   $$-1 + 5 - 1 = 3$$

   Číslo 3 není dělitelné číslem 11 a proto i číslo 151 není dělitelné číslem 11.

   Proto číslo 11 není faktorem čísla 7399.

6. Za zkušebního dělitele označíme další prvočíslo, číslo 13.

   Protože číslo 151 je menší než druhá mocnina čísla 13 ($13^2 = 169$) je číslo 151 prvočíslem a faktorizace zde končí.

   Výsledkem faktorizace čísla 7399 pomocí metody opakovaného dělení je:

   $$\underline{\underline{7399 = 7 \cdot 7 \cdot 151}}.$$

3.2 FERMATOVA FAKTORIZAČNÍ METODA

Fermatova faktorizační metoda je po metodě postupného dělení druhou nejstarší metodou pro faktorizaci daného celého čísla. I když není tato metoda nejefektivnější, má praktický význam pro řadu dalších metod faktorizace i jiných matematických postupů.

Myšlenkou Fermatovy faktorizační metody je pokus o zapsání lichého složeného čísla N jako součinu dvou kladných čísel a a b ($N = a \cdot b$), tak aby platilo, že součin $a \cdot b$ odpovídá rozdílu dvou čtverců $x^2 - y^2 = (x - y) \cdot (x + y)$, kde jednotliví činitelé odpovídají číslům a a b ($a = x - y$, $b = x + y$). Aby byla tato faktorizace netriviální, musí platit $x - y > 1$.

V některých případech (hlavně u menších čísel) můžeme faktorizaci uhodnout, ale jak určíme faktorizaci čísel, u kterých to na první pohled patrné není?

Je patrné, že x musí být větší než $\sqrt{N}$ (v případě, kdy bude N čtvercem, tak získáme ve vyjádření $N = x^2 - 0^2$) a proto je nejmenší možná hodnota čísla $x = \lceil\sqrt{N}\rceil + 1$. Tuto hodnotu označíme m. Nyní musíme vzít v úvahu, že $z = m^2 - N$ a musíme ověřit, zda je číslo z druhou mocninou nějakého čísla. Pokud je z čtvercem, nalezli jsme čísla $x = m$ a $y = z$, která vyhovují rovnosti:

$$N = a \cdot b = (x - y) \cdot (x + y) = x^2 - y^2$$

a faktorizace je u konce.

Pokud číslo z čtvercem není, použijeme další možné m, tedy číslo $m_2 = m_1 + 1$. Musíme znovu dopočítat možné y tedy $z_2 = m_1^2 - N$. Abychom pokaždé nemuseli vypočítávat hodnotu z pomocí čtverce, provedeme drobnou úpravu výrazu $m_n^2 - N$.

$$m_n^2 - N = (m_{n-1} + 1)^2 - N = {m_{n-1}}^2 + 2m_{n-1} + 1 - N = z_{n-1} + 2m_{n-1} + 1$$

Vidíme, že číslo $z_n = z_{n-1} + 2m_{n-1} + 1$ a je možné jeho určení z předchozího výpočtu pro z_{n-1}.

Tento postup opakujeme, dokud není nalezené číslo z_n čtvercem.

Výpočet pomocí Fermatovy faktorizační metody lze zapsat do tří kroků.

1. Určíme druhou odmocninu daného čísla N a označíme $m = \lceil\sqrt{N}\rceil + 1$.
2. Určíme $z = m^2 - N$, pokud z není čtvercem, přičteme k číslu m číslo 1 a postup opakujeme.
3. Dopočteme čísla a a b, kde $a = m - \sqrt{z}$ a $b = m + \sqrt{z}$.

Výpočet si ukážeme na faktorizaci čísla 7399. Podle předchozí metody opakovaného dělení víme, že $7399 = 7 \cdot 7 \cdot 151$. Uvidíme, zda i Fermatovou metodou dospějeme ke stejnému výsledku.

1. Určíme druhou odmocninu čísla 7399 a označme $m = \lceil\sqrt{7399}\rceil + 1$.

$$m = \lceil\sqrt{7399}\rceil + 1 = [86{,}02] + 1 = 86 + 1 = \underline{\underline{87}}.$$

2. Určíme $z = m^2 - N$ a zjistíme, zda je z čtvercem.

$$z = m^2 - N = 87^2 - 7399 = 7569 - 7399 = \underline{\underline{170}}$$

Protože $z = 170$ není čtvercem ($\sqrt{170} = 13{,}04$ není celým číslem) zvýšíme m o číslo 1 a určíme z_2.

$$z_2 = z_1 + 2m_1 + 1 = 170 + 2 \cdot 87 + 1 = \underline{\underline{345}}$$

Ani $z_2 = 345$ ($\sqrt{345} = 18{,}57$ není celým číslem) není čtvercem. Postup opakujeme.

Pro zjednodušení uvedeme tabulku dalších hodnot z, které jsou počítány ze vztahu $z_n = z_{n-1} + 2m_{n-1} + 1$.

Krok	m	$2m + 1$	z	$\sqrt{z}$
1	87	175	170	13,038
2	88	177	345	18,574
3	89	179	522	22,847
4	90	181	701	26,476
5	91	183	882	29,698
6	92	185	1065	32,634
7	93	187	1250	35,355
8	94	189	1437	37,908
9	95	191	1626	40,324
10	96	193	1817	42,626
11	97	195	2010	44,833
12	98	197	2205	46,957
13	99	199	2402	49,010
14	**100**	**201**	**2601**	**51**

Tabulka 2 - Faktorizace čísla 7399 Fermatovou metodou

Z tabulky vidíme, že až 14. krok nám dává $m = 100$ a $z = 2601$, které je čtvercem čísla 51.

3. Dopočteme čísla a a b, kde $a = m - \sqrt{z}$ a $b = m + \sqrt{z}$.

$$a = m - \sqrt{z} = 100 - \sqrt{2601} = 100 - 51 = \underline{\underline{49}}$$

$$b = m + \sqrt{z} = 100 + \sqrt{2601} = 100 + 51 = \underline{\underline{151}}$$

Vidíme, že faktory čísla 7399 jsou čísla 49 a 151.

Dospěli jsme ke stejnému výsledku jako u metody postupného dělení.

Jako každá numerická metoda, tak i Fermatova faktorizační metoda je pro některá čísla rychlá a pro jiná pomalá. Například pro číslo $632\,143$ potřebujeme k nalezení čísla z celkem 637 dílčích kroků a pro číslo $632\,145$, které je pouze o dva větší, nám stačí 22 kroků.

Faktorizaci čísla $632\,145$ pomocí Fermatovy metody určíme následovně.

1. $m = \left[\sqrt{632\,145}\right] + 1 = [795{,}08] + 1 = 795 + 1 = \underline{\underline{796}}$
2. $z = 796^2 - 632\,145 = 633\,616 - 632\,145 = \underline{\underline{1471}}$.

   Další dílčí kroky jsou uvedeny v tabulce.

Krok	m	$2m+1$	z	$\sqrt{z}$
1	796	1593	1471	38,354
2	797	1595	3064	55,353
3	798	1597	4659	68,257
4	799	1599	6256	79,095
5	800	1601	7855	88,628
6	801	1603	9456	97,242
7	802	1605	11 059	105,162
8	803	1607	12 664	112,534
9	804	1609	14 271	119,461
10	805	1611	15 880	126,016
11	806	1613	17 491	132,254
12	807	1615	19 104	138,217
13	808	1617	20 719	143,941
14	809	1619	22 336	149,452
15	810	1621	23 955	154,774
16	811	1623	25 576	159,925
17	812	1625	27 199	164,921
18	813	1627	28 824	169,776
19	814	1629	30 451	174,502
20	815	1631	32 080	179,109
21	816	1633	33 711	183,606
22	**817**	**1635**	**35 344**	**188**

Tabulka 3 - Faktorizace čísla 632 145 Fermatovou metodou

Z tabulky vidíme, že 22. krok nám dává $m = 817$ a $z = 35\,344$, které je čtvercem čísla 188.

3. A nyní už stačí jen dopočítat jednotlivé faktory.

$$a = m - \sqrt{z} = 817 - \sqrt{35\,344} = 817 - 188 = \underline{\underline{629}}$$

$$b = m + \sqrt{z} = 817 + \sqrt{35\,344} = 817 + 188 = \underline{\underline{1005}}$$

Vidíme, že faktory čísla $632\,145$ jsou čísla 629 a 1005.

$$\underline{\underline{632\,145 = 629 \cdot 1005}}$$

Také vidíme, že získané faktory nejsou obecně prvočíselné, avšak byl učiněn podstatný pokrok pro nalezení prvočíselného rozkladu. Opětovnou aplikací Fermatovy faktorizační metody na získané faktory 1005 a 629 získáme $1005 = 67 \cdot 15$ (další aplikací dále $15 = 3 \cdot 5$) a $629 = 17 \cdot 37$. Pro faktorizaci čísla 1005 použijeme deset kroků, pro číslo 629 stačí dva kroky a pro číslo 15 pouze jeden krok na určení hodnoty z.

Faktorizaci čísla $632\,143$ pomocí Fermatovy metody určíme následovně.

1. $m = \left[\sqrt{632\,143}\right] + 1 = [795{,}07] + 1 = 795 + 1 = \underline{\underline{796}}$
2. $z = 796^2 - 632\,143 = 633\,616 - 632\,143 = \underline{\underline{1469}}$

   Další dílčí kroky jsou uvedeny v souboru FermatovaFaktorizacniMetoda.xlsx na přiloženém CD.

   V tomto případě nám výsledek dává až 637. krok.

   $m = 1432$ a $z = 1\,418\,481$, které je čtvercem čísla 1191.

3. A nyní už stačí jen dopočítat jednotlivé faktory.

$$a = m - \sqrt{z} = 1432 - \sqrt{1\,418\,481} = 1432 - 1191 = \underline{\underline{241}}$$

$$b = m + \sqrt{z} = 1432 + \sqrt{1\,418\,481} = 1432 + 1191 = \underline{\underline{2623}}$$

Vidíme, že faktory čísla $632\,143$ jsou čísla 2623 a 241.

$$\underline{\underline{632\,143 = 241 \cdot 2623}}$$

Zde je prvočíselným faktorem číslo 241. Pro získání dalších prvočíselných faktorů použijeme na číslo 2623 znovu Fermatovu faktorizační metodu. Pro určení faktorizace $2623 = 43 \cdot 61$ potřebujeme pouze jeden krok na nalezení hodnoty z.

3.3 EULEROVA FAKTORIZAČNÍ METODA

Eulerova faktorizační metoda vychází z Fermatovy faktorizační metody a odlišuje se tím, že ji lze použít pouze na celá čísla N, která lze zapsat ve tvaru:

$$N = a^2 + Db^2$$

a to dvěma různými způsoby pro stejnou hodnotu čísla D.

To vychází z rovnosti, kterou objevil Joseph Louis Lagrange:

$$(x^2 + Dy^2) \cdot (u^2 + Dv^2) = \begin{cases} (xu + Dyv)^2 + D(yu - xv)^2 \\ (xu - Dyv)^2 + D(yu + xv)^2. \end{cases} (7)$$

Tato rovnost ukazuje, že součin dvou různých celých čísel, která můžeme obě zapsat ve tvaru $N = a^2 + Db^2$, je opět celým číslem stejného tvaru, a má dvě různá vyjádření tvaru $r^2 + Ds^2$ ($r = xu \pm Dyv, s = yu \mp xv$).

Leonhard Euler dokázal rovnost opačnou, že pokud číslo N lze zapsat dvěma různými vyjádřeními tvaru $r^2 + Ds^2$, tedy $N = a^2 + Db^2$ a $N = c^2 + Dd^2$, kdy $nsd(bd, N) = 1$, pak je možné číslo N zapsat jako součin těchto čísel ve stejném tvaru.

Tyto faktory čísla N ($N = f_1 \cdot f_2$) lze určit následujícím výpočtem:

$$f_1 = nsd(N, ad - bc) \text{ a}$$

$$f_2 = nsd(N, ad + bc).$$

Postup pro nalezení dvou různých vyjádření čísla N ve tvaru $r^2 + Ds^2$, je analogický s postupem pro nalezení čísel m a z ve Fermatově faktorizační metodě.

Bohužel všechna celá čísla nemají více vyjádření ve tvaru $r^2 + Ds^2$ (některá nemají dokonce žádné) pro stejnou hodnotu D. Proto se tato metoda používá u čísel, kde je již jedno vyjádření tvaru $r^2 + Ds^2$ známé a pokoušíme se nalézt vyjádření druhé.

Faktorizaci pomocí Eulerovy faktorizační metody si ukážeme na rozkladu čísla $34\,889$, kde již známe jedno vyjádření tvaru $r^2 + Ds^2$ a to $34\,889 = 143^2 + 10 \cdot 38^2$.

Pro určení druhého vyjádření tvaru $r^2 + Ds^2$ použijeme postup podobný jako ve Fermatově faktorizační metodě pro nalezení hodnoty z.

1. Nejdříve určíme první hodnotu čísla s (ve Fermatově faktorizační metodě bylo číslo m), která se vypočítá takto:

$$s = \left[\sqrt{\frac{N}{D}}\right].$$

$$s = \left[\sqrt{\frac{N}{D}}\right] = \left[\sqrt{\frac{34\,889}{10}}\right] = [59{,}07] = \underline{\underline{59}}$$

2. Nyní potřebujeme určit hodnotu z. Zde bude $z = N - Ds^2$. Pro další dílčí kroky použijeme vztah $z_n = z_{n-1} + D \cdot (2 \cdot s_{n-1} - 1)$. Oproti Fermatově faktorizační metodě, zde v dalších dílčích krocích odečítáme od hodnoty s číslo 1.

$$z = N - 10s^2 = 34\,889 - 10 \cdot 59^2 = 34\,889 - 34\,810 = \underline{\underline{79}}$$

Protože číslo $z = 79$ není čtvercem, zmenšíme hodnotu s o číslo 1 a spočteme z_2.

$$z_2 = z_1 + D \cdot (2 \cdot s_1 - 1) = 79 + 10 \cdot (2 \cdot 59 - 1) = 79 + 1170 = \underline{\underline{1249}}$$

Ani číslo $z_2 = 1249$ není čtvercem ($\sqrt{1249} = 35{,}34$), zmenšíme hodnotu s_2 o číslo 1 a spočteme z_3. Následující hodnoty z jsou uvedeny v tabulce.

Krok	s	$10(2s-1)$	z	$\sqrt{z}$
1	59	1170	79	8,888
2	58	1150	1249	35,341
3	57	1130	2399	48,980
4	56	1110	3529	59,405
5	55	1090	4639	68,110
6	54	1070	5729	75,690
7	53	1050	6799	82,456
8	52	1030	7849	88,595
9	51	1010	8879	94,228
10	50	990	9889	99,443
11	49	970	10 879	104,302
12	48	950	11 849	108,853

13	47	930	12 799	113,133
14	46	910	13 729	117,171
15	45	890	14 639	120,992
16	44	870	15 529	124,615
17	43	850	16 399	128,059
18	42	830	17 249	131,335
19	41	810	18 079	134,458
20	40	790	18 889	137,437
21	39	770	19 679	140,282
22	**38**	**750**	**20 449**	**143**

Tabulka 4 - Eulerova faktorizační metoda 1

Z tabulky vidíme, že 22. krok nám dává hodnoty $s = 38$ a $z = 20\,449$ ($\sqrt{z} = r = 143$). Ovšem vidíme, že jsme získali vyjádření, které již známe ($34\,889 = 143^2 + 10 \cdot 38^2$). Musíme pokračovat ve výpočtu.

Krok	s	$10(2s-1)$	z	$\sqrt{z}$
22	**38**	**750**	**20 449**	**143**
23	37	730	21 199	145,599
24	36	710	21 929	148,084
25	35	690	22 639	150,463
26	34	670	23 329	152,738
27	33	650	23 999	154,916
28	**32**	**630**	**24 649**	**157**

Tabulka 5 - Eulerova faktorizační metoda 2

Z tabulky vidíme, že 28. krok nám dává hodnoty $s = 32$ a $z = 24\,649$ ($\sqrt{z} = r = 157$), které jsou odlišné od hodnot v 22. kroku. Získali jsme druhé vyjádření čísla $34\,889$ ve tvaru $r^2 + 10 \cdot s^2$, konkrétně $34\,889 = 157^2 + 10 \cdot 32^2$.

3. Nyní máme dva tvary $N = a^2 + Db^2$ a $N = c^2 + Dd^2$, kde:

$$a = 143, b = 38, c = 157 \text{ a } d = 32.$$

Stačí dopočítat faktory čísla N ($N = f_1 \cdot f_2$), které určíme následujícími vzorci:

$$f_1 = nsd(N, ad - bc) \text{ a}$$

$$f_2 = nsd(N, ad + bc)$$

$$f_1 = nsd(34\,889, 143 \cdot 32 - 38 \cdot 157) = nsd(34\,889, -1390) = \underline{\underline{139}}$$

$$f_2 = nsd(34\,889, 143 \cdot 32 + 38 \cdot 157) = nsd(34\,889, 10\,542) = \underline{\underline{251}}$$

Pomocí Eulerovy faktorizační metody jsme určili za faktory čísla $34\,889$ čísla 139 a 251.

$$\underline{\underline{34\,889 = f_1 \cdot f_2 = 139 \cdot 251}}.$$

3.4 EUKLIDŮV ALGORITMUS JAKO POMŮCKA FAKTORIZACE

Před rozvojem výpočetní techniky a objevením nových a účinnějších faktorizačních metod, byl používán i Euklidův algoritmus pro nalezení faktorů celého čísla N.

Euklidův algoritmus: Nechť jsou a a b dva nenulové prvky. Pak existují prvky $\eta_0, \eta_1, \dots, \eta_n$, $v_1, v_2, \dots, v_n$ tak, že $v_n = nsd(a, b)$ a platí:

$$\begin{aligned}
a &= b \cdot \eta_0 + v_1 && N(v_1) < N(b) \\
b &= v_1 \cdot \eta_1 + v_2 && N(v_2) < N(v_1) \\
v_1 &= v_2 \cdot \eta_2 + v_3 && N(v_3) < N(v_2) \\
&\vdots && \vdots \\
v_{i-1} &= v_i \cdot \eta_i + v_{i+1} && N(v_{i+1}) < N(v_i) \\
&\vdots && \vdots \\
v_{n-2} &= v_{n-1} \cdot \eta_{n-1} + v_n && N(v_n) < N(v_{n-1}) \\
v_{n-1} &= v_n \cdot \eta_n + 0. && (7)
\end{aligned}$$

Metoda použití Euklidova algoritmu je následující. Aby bylo možné najít faktory čísla N, je potřeba znát součin všech prvočísel, která jsou menší než $\sqrt{N}$. Protože bychom u mnohociferných čísel získávali obrovská čísla, je potřeba tuto množinu prvočísel (možných faktorů) rozdělit na více částí a tím i hledání faktorů rozdělit na více částí. K tomuto účelu sloužily známé součiny prvočísel $\prod_2^{97} p$, $\prod_{101}^{199} p$, …(součin prvočísel od 2 do 97, součin prvočísel od 101 do 199, …).

Například součin prvočísel menších než 100 je označován P_0.

$$P_0 = \prod_{2}^{97} p = 2\,305\,567\,963\,945\,518\,424\,753\,102\,147\,331\,756\,070$$

Samozřejmě si můžeme tyto množiny prvočísel určit sami a vypočítat jejich příslušné součiny $\prod_g^G p$, kde provádíme součin prvočísel od g (dolní limit) do G (horní limit).

Po určení součinu prvočísel použijeme Euklidův algoritmus pro nalezení faktorů, kde prvky a a b jsou součin prvočísel $\prod_g^G p$ a číslo N.

Ukázku použití si ukážeme na faktorizaci nám již z předchozích kapitol známého čísla 7399.

1. Určíme množinu prvočísel, mezi kterými budeme hledat jeden z faktorů, tedy hodnotu dolního a horního limitu. Za horní limit nemusíme volit hodnotu čísla N, stačí nám volit za $G = \lfloor \sqrt{N} \rfloor = 86$. Dále volme $g = 2$.

   Protože víme, že faktory jsou čísla 7 (dvojnásobný faktor) a 151, zvolíme za horní limit $G = 19$ (i s $G = 86$ dospějeme ke stejnému výsledku, bude však zapotřebí více kroků Euklidova algoritmu a získali bychom za součin $\prod_2^{86} p$ číslo o 32 cifrách).

2. Určíme součin $\prod_2^{19} p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9\,699\,690$. Tento součin označíme jako a.

   Za hodnotu b použijeme číslo pro faktorizaci $N = 7399$.

3. Nyní zbývá určit faktor pomocí Euklidova algoritmu s čísly $a = 9\,699\,690$ a $b = 7399$.

   V prvním kroku Euklidova algoritmu dělíme číslo $a = 9\,699\,690$ číslem $b = 7399$, abychom určili čísla η_0 a zbytek v_1.

   $$a = b \cdot \eta_0 + v_1$$

   $$9\,699\,690 = 7399 \cdot 1310 + 7000$$

   V následujícím kroku budeme dělit číslo 7399 pomocí zbytku z předchozího kroku.

   $$b = v_1 \cdot \eta_1 + v_2$$

   $$7399 = 7000 \cdot 1 + 399$$

   Euklidův algoritmus opakujeme, dokud nedostaneme nulový zbytek.

Pro názornost sepíšeme celý Euklidův algoritmus.

$$a = b \cdot \eta_0 + v_1$$

$$9\,699\,690 = 7399 \cdot 1310 + 7000$$

$$7399 = 7000 \cdot 1 + 399$$

$$7000 = 399 \cdot 17 + 217$$

$$399 = 217 \cdot 1 + 182$$

$$217 = 182 \cdot 1 + 35$$

$$182 = 35 \cdot 5 + \boxed{7}$$

$$35 = 7 \cdot 5 + 0$$

Posledním nenulovým zbytkem je číslo 7, které je jedním z faktorů čísla 7399. Při vydělení čísla 7399 faktorem 7, získáme druhý faktor, tedy číslo 1057.

Pomocí Euklidova algoritmu jsme určili faktorizaci čísla $7399 = 7 \cdot 1057$. Víme, že i číslo 1057 lze faktorizovat. Budeme tedy pokračovat v Euklidově algoritmu s čísly $a = \prod_2^{19} p$ a $b = 1057$.

$$9\,699\,690 = 9176 \cdot 1057 + 658$$

$$1057 = 1 \cdot 658 + 399$$

$$658 = 1 \cdot 399 + 259$$

$$399 = 1 \cdot 259 + 140$$

$$259 = 1 \cdot 140 + 119$$

$$140 = 1 \cdot 119 + 21$$

$$119 = 5 \cdot 21 + 14$$

$$21 = 1 \cdot 14 + \boxed{7}$$

$$14 = 2 \cdot 7 + 0$$

Posledním nenulovým zbytkem je číslo 7, které je jedním z faktorů čísla 1057. Při vydělení čísla 1057 faktorem 7, získáme druhý faktor, tedy číslo 151.

Dospěli jsme tedy ke stejnému výsledku jako v předchozích metodách $\underline{7399 = 7 \cdot 7 \cdot 151}$.

4 MODERNÍ METODY FAKTORIZACE

S narůstajícími nároky na rychlost faktorizace a také na zvyšující se počet cifer bylo zapotřebí nových a rychlejších metod. Z potřeby umění rozkládat velká celá čísla na prvočinitele (prvočíselné faktory) za relativně krátkou dobu nastal v této oblasti matematiky v posledních 40 letech značný pokrok. Je to dáno nástupem vysokorychlostních počítačů. Tento pokrok můžeme rozdělit na dvě základní linie.

První se zabývala analýzou již známých metod (označovány jako klasické metody faktorizace) a jejich zdokonalením. Samozřejmě bylo zapotřebí je částečně upravit a vytvořit z nich počítačové algoritmy, případně moduly, které se vložily do již existujících matematických programů. Mezi matematiky a informatiky, kteří převedli do počítačových algoritmů nejstarší faktorizační metody, patří Michael Morrison, John Brillhart, Maurice Kraitchik, Derrick Henry Lehmer a Ralph Ernest Powers. Dosažený pokrok v této oblasti byl příčinnou rozvoje druhé linie počítačové faktorizace celých čísel, která kladla důraz hlavně na rychlost a univerzálnost použití (Eulerova metoda požaduje, aby faktorizované číslo šlo zapsat ve dvou vyjádřeních tvaru $r^2 + Ds^2$, takže tato metoda univerzální není).

Druhá linie se zabývala nalezením nových postupů faktorizace celých čísel, které v řadě případů vychází z klasických metod faktorizace. Nechá se rozdělit na několik dalších částí (vývoj nových metod vycházejících z již známých faktorizačních metod, rozvoj prvočíselných sít, vytvoření nových metod z nově objevených matematických souvislostí…). V této linii jsou nejznámějšími jmény Carl Pomerance, John M. Pollard, Daniel Shanks a Hendrik William Lenstra. Hlavně poslední dva jmenovaní D. Shanks a H. W. Lenstra se zasloužili o objevení zcela nových faktorizačních metod.

V důsledku tohoto velkého rozvoje v této oblasti matematiky nelze poskytnout kompletní přehled o všech výsledcích a kompletní klasifikaci moderních faktorizačních metod. Proto se v této kapitole zaměříme hlavně na jedny z prvních moderních faktorizačních metod, a to na metody Johna M. Pollarda. Metody ostatních zde zmíněných matematiků si pouze představíme a naznačíme jejich hlavní myšlenku. Podrobný popis algoritmu (způsobu výpočtu) těchto metod není z důvodu jejich rozsahu možný. Každá by byla na samostatnou práci. Nebudu zde ani ukazovat faktorizace podle těchto metod s výjimkou metod Johna M. Pollarda a H. W. Lenstra.

4.1 POLLARDOVA $p-1$ METODA

Pollardova $p-1$ metoda je algoritmus objevený Johnem Pollardem v roce 1974. Jedná se o metodu, která nefunguje obecně, ale pouze pro určitý typ faktorů. Podmínkou pro nalezení faktoru p je, aby číslo předcházející faktoru, $p-1$, bylo velmi hladkým číslem.

Pojem hladké číslo, označuje takové celé číslo, které nemá prvočíselného dělitele většího než číslo B. Takové číslo je označováno jako B-hladké. Například číslo $117 = 3^2 \cdot 13$ je 13-hladké.

Podobně pojem velmi hladké číslo, označuje číslo m, pokud pro všechny mocniny jeho prvočíselných faktorů, které jsou soudělné s číslem m, platí $p^i \leq B$. Takové číslo označujeme jako B-velmi hladké. Například číslo $360 = 2^3 \cdot 3^2 \cdot 5$ je 9-velmi hladké ($2^3 = 8, 3^2 = 9$). Také ho můžeme označit jako 5-hladké.

Pollardova $p-1$ metoda využívá Fermatovu malou větu a následující myšlenku. Víme, že pokud je p prvočíslo, pak platí:

$$2^{p-1} \equiv 1 \ (mod\ p).$$

Pokud je $p-1$ soudělné s číslem M, tak platí:

$$2^M \equiv 1 \ (mod\ p).$$

Takže pokud je p prvočíselným faktorem celého čísla N, tak $p \mid nsd(2^M - 1, N)$.

Nápadem Johna Pollarda bylo vybrat číslo M s mnoha děliteli ve tvaru $p-1$ (podmínkou je, aby $p-1 < B$) a tím hledat najednou větší množství prvočísel jako možné faktory čísla N. Pro ještě rychlejší průběh faktorizace a zbytečnému navyšování počtu cifer je M definováno jako nejmenší společný násobek prvků $p_i - 1$, kde $p_i - 1 < B$.

Určení faktorizace si ukážeme na číslu $N = 7399$.

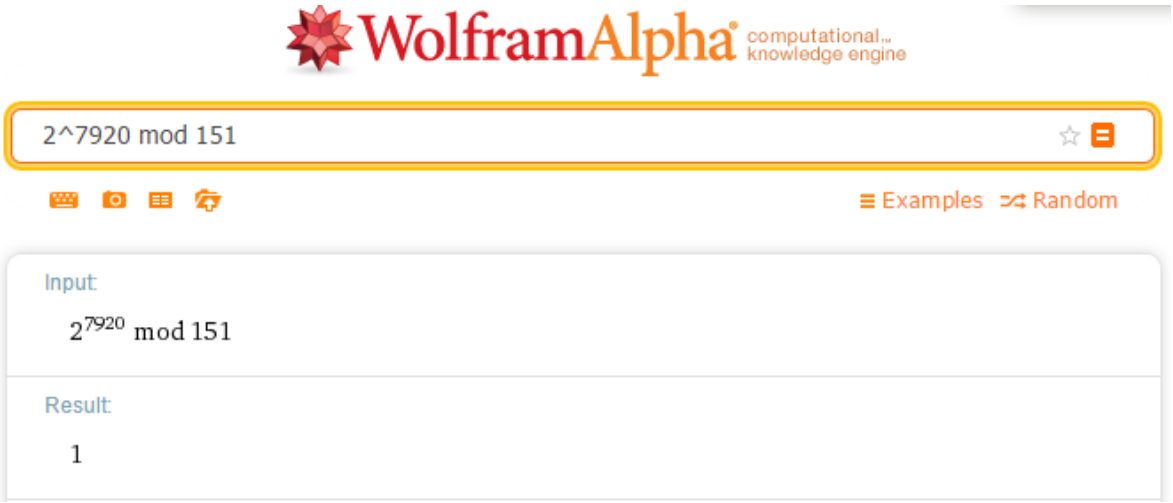
1. Prvním krokem je nalezení hodnoty B. Z předchozích faktorizací víme, že jedním z faktorů je číslo 151. Samotná metoda faktorizace využívá metody pro zjištění čísla B nebo bývá hodnota B nahrazována hodnotou $\sqrt{N}$.

   Protože víme, že $p = 151$, tak $p - 1 = 150$. Dále $150 = 2 \cdot 3 \cdot 5^2$ a je tedy 25-velmi hladké ($B = 25$).

2. Spočteme hodnotu $M = nsn(\{p-1\}_{p=2}^{p \leq B})$.

   $$M = nsn(1, 2, 4, 6, 10, 12, 16, 18, 22) = \underline{\underline{7920}}$$

   Zde ověříme pomocí nástroje Wolfram|Alpha platnost kongruence $2^M \equiv 1 \ (mod\ p)$ (v samotné faktorizaci k tomuto výpočtu nedochází).



Obrázek 19 Výpočet kongruence

3. Nyní musíme ověřit, jestli $p = 151$ dělí $nsd(2^{7920} - 1, 7399)$

   $$nsd(2^{7920} - 1, 7399) = \underline{\underline{1057}}$$

   $$1057 = 7 \cdot 151 \Longrightarrow 151|1057$$

   Protože je číslo 151 soudělné s číslem 1057, tak je faktorem čísla 7399.

   Tato metoda nepatří mezi nejrychlejší a univerzální metody, proto byla brzy překonána a to samotným autorem Pollardovou ρ metodou.

4.2 POLLARDOVA ρ METODA

Pollardova „ró“ metoda (Pollard´s rho method) je velice efektivní metoda pro faktorizaci složených čísel s malými prvočíselnými faktory. Jedná se o metodu ze skupiny metod označovaných jako Monte Carlo.

Metody ze skupiny Monte Carlo jsou algoritmy, které využívají pseudonáhodná čísla. Jde o čísla, která se zdají být náhodná, ale jsou generována určitým počítačovým generátorem. Tyto metody se využívají převážně pro složité výpočty, kde ostatní metody selžou.

Algoritmus Pollardovy ρ metody očekává na vstupu složené číslo N. Výstupem je netriviální faktor čísla N nebo oznámení o neúspěšné faktorizaci. Algoritmus je následující:

1. Zvolení náhodných čísel.

   V tomto kroku dochází ke zvolení náhodných čísel a z nich určení funkce a čísel U a V. Samotný algoritmus by měl obecně následující podobu (může se lišit v souvislosti s programovacím jazykem):

   $a = RandomInteger[1, N-3]$; (zvolení náhodného čísla a z intervalu $[1, N-3]$)

   $s = RandomInteger[1, N-1]$; (zvolení náhodného čísla s z intervalu $[1, N-1]$)

   $U = s$; (přiřazení hodnoty s hodnotě U)

   $V = s$; (přiřazení hodnoty s hodnotě V)

   $F(x) := (x^2 + a)\ (mod\ N)$ (nadefinování funkce pro další výpočet).

2. Hledání faktoru g.

   V tomto kroku dochází k výpočtu funkčních hodnot $F(U)$ a $F(F(V))$. Následně k výpočtu hodnoty g, která je nejmenším společným dělitelem rozdílu funkčních hodnot $F(U)$ a $F(F(V))$ a složeného čísla N ($nsd\big(F(U) - F\big(F(V)\big),\ N\big)$. Samotný algoritmus by měl obecně následující podobu (může se lišit v souvislosti s programovacím jazykem).

   $U = F(U)$; (funkční hodnota pro U)

   $V = F(V)$; (funkční hodnota pro V)

   $V = F(V)$; (funkční hodnota pro $F(V)$)

   $g = nsd(U - V, N)$; (určení hodnoty g jako nejmenšího společného dělitele hodnot $U - V$ a N)

   Následuje ověření, zda je $g \neq 1$. Pokud nastane $g = 1$ tak se tento krok (hledání faktoru g) opakuje (došlo k nalezení triviálního faktoru).

3. Špatně zvolené náhodné veličiny.

   V tomto kroku se ověřuje, zda nenastala rovnost $g = N$ (došlo k nalezení triviálního faktoru). Pokud tato rovnost nastala, došlo ke zvolení nevhodných hodnot a a s. Je nutné začít s algoritmem od začátku (od kroku zvolení náhodných čísel).

4. Výsledek

   Pokud se dostaneme v algoritmu až sem, tak je g faktorem čísla N.

Faktorizaci pomocí této metody si ukážeme na již známém čísle 7399.

1. Zvolení náhodných čísel.

   Zvolíme hodnoty $a = 5$, $s = 3$. Dále získáme funkci $F(x)$ a hodnoty U a V.

   $$a = 5 \Rightarrow F(x) := (x^2 + 5)\ (mod\ 7399)$$

   $$s = 3 \Rightarrow U = V = 3$$

2. Hledání faktoru g.

   $$U := F(U)$$

   $$F(U) \equiv (3^2 + 5)\ (mod\ 7399)$$

   $$F(U) \equiv 14\ (mod\ 7399)$$

   $$\underline{\underline{\boldsymbol{U := F(U) = 14}}}$$

   $$V := F\big(F(V)\big)$$

   $$F(V) \equiv (3^2 + 5)\ (mod\ 7399)$$

   $$F(V) \equiv 14\ (mod\ 7399)$$

   $$F\big(F(V)\big) \equiv (14^2 + 5)\ (mod\ 7399)$$

   $$F\big(F(V)\big) \equiv 201\ (mod\ 7399)$$

   $$\underline{\underline{\boldsymbol{V := F\big(F(V)\big) = 201}}}$$

   $$g = nsd(U - V, 7399)$$

   $$g = nsd(14 - 201, 7399)$$

   $$\underline{\underline{\boldsymbol{g = 1}}}$$

   Protože $g = 1$ (byl nalezen triviální faktor), tak tento krok opakujeme s hodnotami $U = 14$ a $V = 201$.

$$U \coloneqq F(U)$$

$$F(U) \equiv (14^2 + 5)\ (mod\ 7399)$$

$$F(U) \equiv 201\ (mod\ 7399)$$

$$\underline{\underline{\boldsymbol{U} := \boldsymbol{F}(\boldsymbol{U}) = \mathbf{201}}}$$

$$V := F\big(F(V)\big)$$

$$F(V) \equiv (201^2 + 5)\ (mod\ 7399)$$

$$F(V) \equiv 40\ 406\ (mod\ 7399)$$

$$F(V) \equiv 3411\ (mod\ 7399)$$

$$F\big(F(V)\big) \equiv (3411^2 + 5)\ (mod\ 7399)$$

$$F\big(F(V)\big) \equiv 11\ 634\ 926\ (mod\ 7399)$$

$$F\big(F(V)\big) \equiv 3698\ (mod\ 7399)$$

$$\underline{\underline{\boldsymbol{V} := \boldsymbol{F}\big(\boldsymbol{F}(\boldsymbol{V})\big) = \mathbf{3698}}}$$

$$g = nsd(U - V, 7399)$$

$$g = nsd(201 - 3698, 7399)$$

$$\underline{\underline{\boldsymbol{g} = \mathbf{1}}}$$

Protože $g = 1$ (byl nalezen triviální faktor), musíme tento krok opakovat pro hodnoty $U = 201$ a $V = 3698$.

$$U := F(U)$$

$$F(U) \equiv (201^2 + 5)\ (mod\ 7399)$$

$$F(U) \equiv 40\ 406\ (mod\ 7399)$$

$$F(U) \equiv 3411\ (mod\ 7399)$$

$$\underline{\underline{\boldsymbol{U} := \boldsymbol{F}(\boldsymbol{U}) = \mathbf{3411}}}$$

$$V := F\big(F(V)\big)$$

$$F(V) \equiv (3698^2 + 5)\ (mod\ 7399)$$

$$F(V) \equiv 13\ 675\ 209\ (mod\ 7399)$$

$$F(V) \equiv 1857\ (mod\ 7399)$$

$$F\big(F(V)\big) \equiv (1857^2 + 5)\ (mod\ 7399)$$

$$F\big(F(V)\big) \equiv 3\ 448\ 454\ (mod\ 7399)$$

$$F\big(F(V)\big) \equiv 520\ (mod\ 7399)$$

$$\underline{\underline{\boldsymbol{V} := \boldsymbol{F}\big(\boldsymbol{F}(\boldsymbol{V})\big) = \mathbf{520}}}$$

$$g = nsd(U - V, 7399)$$

$$nsd(3698 - 520, 7399)$$

$$\underline{\underline{\boldsymbol{g} = \mathbf{49}}}$$

Druhá část algoritmu nám odhalila za podezřelý faktor čísla 7399 číslo 49.

3. Špatně zvolené náhodné veličiny.

   Protože $g = 49 \neq 7399 = N$, bude v následující části označena hodnota g faktorem čísla 7399.

4. Výsledek

   Číslo $g = 49$ je netriviálním faktorem čísla 7399.

Tato metoda je na výpočet velice jednoduchá a je možné ji vytvořit i v programu MS Excel. Jeden z možných způsobů řešení si můžete prohlédnout na přiloženém CD v souboru PollardovaRoMetoda.xlsx. Je nutné zadat N, a a s do příslušných buněk. Pokud bychom ve žlutém sloupečku neviděli jiná čísla než 1, je zapotřebí poslední řádek roztáhnout (označení buněk A6 - E6, myší kliknout a držet čtvereček v pravém dolním rohu označené oblasti a táhnout směrem dolu).

4.3 SQUFOF

SQUFOF je faktorizační metoda Daniela Shankse objevená v roce 1975 a v originále se nazývá Shanks´s method **Squ**are **Fo**rms **F**actorization (SQUFOF) a do češtiny se nechá přeložit jako Shanksova faktorizační metoda čtvercových rozkladů. Jedná se o moderní faktorizační metodu, která je z části vylepšením Fermatovy faktorizační metody, a dále využívá binární kvadratické formy. Využití binárních kvadratických forem se ukázalo jako velmi úspěšné a řada moderních metod faktorizace tyto formy využívá. Většina těchto metod je však velmi komplikovaná a jsou určeny hlavně pro faktorizaci na počítači a není ideální je používat pro počítání na papíře (bez počítače).

Podrobný popis toho, jak SQUFOF funguje je uveden v knize Dalea Husemöllera Elliptic Curves (8). Je však možné tuto metodu popsat pomocí řetězových zlomků bez jakékoliv zmínky o binárních kvadratických formách.

Řetězový zlomek je výraz typu:

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{a_4 + \cdots,}}}}$$

kde a_i a b_i jsou buď racionální, reálná nebo komplexní čísla. Pokud platí $b_i = 1$ pro všechny i, tak mluvíme o základním řetězovém zlomku. Pokud výraz obsahuje konečný počet členů, jde o konečný řetězový zlomek. Pokud výraz obsahuje nekonečný počet členů, nazývá se nekonečným řetězovým zlomkem. (3)

Shanksova metoda pro faktorizaci čísla N využívá řetězového zlomku pro hodnotu $\sqrt{N}$.

Základní myšlenkou metody SQUFOF je Legendreova kongruence:

$$x^2 \equiv y^2 \ (mod\ N),$$

pro jejíž řešení se využívá kongruence:

$$A_{n-1}^2 \equiv (-1)^n Q_n \ (mod\ N).$$

Jediné, co je nutné, je řetězit $\sqrt{N}$ dokud není nalezen čtverec $Q_n = R^2$ pro sudé n. Legendreova kongruence má pak řešení:

$$x \equiv A_{n-1} \text{ a}$$

$$y \equiv R.$$

Pokud se nejedná o triviální řešení, pak lze faktory f_1 a f_2 najít pomocí Euklidova algoritmu pro hodnoty N a $A_{n-1} \pm R$.

Tento postup pro hledání čtverce v řetězovém zlomku pro $\sqrt{N}$ je znán již dlouho, ovšem nebyl před příchodem počítačů používán kvůli množství kroků potřebných k nalezení tohoto čtverce.

Vzhledem k rozsáhlosti výpočtu zde ukázku nepoužijeme. Nechá se však najít v knize Hanse Riesela Prime Numbers and Computer Methods for Factorization (3).

Shanks také přišel na to, že nalezený čtverec ve jmenovateli řetězeného zlomku musí být nalezen v sudém kroku řetězení a nesmí být čtvercem jiného jmenovatele, který se v řetězení objevil. Pak je zaručeno, že nedojde k nalezení triviálních řešení.

4.4 CFRAC

CFRAC je počítačová metoda faktorizace vyvinutá Michaelem Morrisonem a Johnem Brillhartem. V originále se jmenuje Morrison and Brillhart´s **C**ontinued **Frac**tion Method (CFRAC). Dala by se přeložit jako metoda řetězových zlomků. Jedná se o jednu z nejefektivnějších metod faktorizace, která je univerzální (není zapotřebí speciální tvar faktorů ani faktorizovaného čísla).

Stejně jako v metodě SQUFOF je hlavní myšlenkou Legendreova kongruence:

$$x^2 \equiv y^2 \ (mod\ N),$$

pro jejíž řešení se zde využívá kongruence:

$$A_{n-1}^2 \equiv (-1)^n Q_n \ (mod\ N).$$

Vidíme, že tato část je shodná s předchozí metodou. Další postup je však odlišný.

Zatímco u metody SQUFOF je nutné ve jmenovateli řetězeného zlomku pro $\sqrt{N}$ najít čtverec $Q_n = R^2$ pro sudé n, tak Morrison a Brillhart se snaží vytvořit čtverce, které vznikají násobením kvadratických zbytků. Tím dochází k rychlejšímu nalezení čtverce.

Vzhledem k rozsáhlosti výpočtu zde ukázku nepoužiji. Nechá se však najít v knize Hanse Riesela Prime Numbers and Computer Methods for Factorization (3).

4.5 KVADRATICKÉ SÍTO

Kvadratické síto (Quadratic sieve) je jedním z nejrychlejších algoritmů pro faktorizaci složených čísel. Bohužel je také velice náročný na výpočet a na paměť počítače. Autorem této metody je Carl Pomerance. Jedná se o univerzální metodu, u které nezáleží na tvaru a vlastnostech faktorizovaného čísla ani jeho faktorech. Délka výpočtu je však závislá na počtu cifer faktorizovaného čísla.

Ve skutečnosti se jedná o úpravu metody CFRAC. Jedinou změnou je, že na nalezení kvadratických zbytků, vymyslel Carl Pomerance nový postup, který výrazně zkrátil dobu faktorizace. V metodě CFRAC zabíralo nalezení kvadratických zbytků většinu času výpočtu.

Kvadratické zbytky jsou dány v této metodě rovnicí:

$$Q(x) = (x + m)^2 - N, m = \sqrt{N}, x \in \mathbb{Z}.$$

Stejně jako u předchozích metod, zde vzhledem k rozsáhlosti výpočtu ukázku faktorizace neprovedu. Lze jí opět najít v knize Hanse Riesela. (3)

4.6 ECM

ECM (Elliptic curve method) je metoda do češtiny překládána jako metoda eliptických křivek. Někdy bývá pojmenována po svém autorovi Henriku Lenstrovi, jako Lenstrova faktorizační metoda. Jedná se v současnosti o jednu z nejrychlejších univerzálních metod pro faktorizaci celých čísel. V případě, kdy mají faktory čísla N méně jak 25 cifer, se jedná dokonce o nejrychlejší metodu, proto bývá používána pro zjištění menších faktorů a následně je zapojena metoda, která je naopak rychlejší v hledání velkých faktorů (některé z kvadratických sít). Je to dáno tím, že složitost výpočtu nezáleží na samotném čísle N, ale pouze na velikosti faktorů. V současnosti největším nalezeným faktorem pomocí této metody bylo 83 ciferné číslo v roce 2013.

Z důvodu rozsáhlosti problematiky eliptických křivek, zde uvedeme pouze výpočet pomocí počítačového algoritmu (jde o zjednodušenou variantu, která je ovšem plně funkční).

Na začátku se vybere náhodná eliptická křivka tvaru $y^2 \equiv x^3 + ax + b \ (mod\ N)$ a určí se hodnota b $(b \equiv y^2 - x^3 - ax \ (mod\ N))$. Náhodný výběr probíhá generováním náhodných hodnot a, x a y z intervalu $[0, N-1]$. Je to z důvodu, aby bylo zajištěno, že bod $P = (x, y)$ náleží eliptické křivce $E_{a,b}(\mathbb{Z}_n)$.

Následně dojde k určení hodnoty $g = nsd\ (4a^3 + 27b^2, N)$ a ověří se, zda platí $0 < g < N$. Pokud je g mimo tento interval, musí se zvolit jiná eliptická křivka (jiné hodnoty a, x a y z intervalu $[0, N-1]$).

Faktorizaci si ukážeme na hledání faktoru čísla $N = 7399$.

Zvolíme náhodně hodnoty:

$$a = 2,$$

$$x = 4,$$

$$y = 3.$$

Dopočteme hodnotu b.

$$b \equiv y^2 - x^3 - ax \ (mod\ N)$$

$$b \equiv 3^2 - 4^3 - 2 \cdot 4 \ (mod\ 7399)$$

$$b \equiv 7336 \ (mod\ 7399)$$

$$\underline{\underline{b = 7366}}$$

Spočteme hodnotu g.

$$g = nsd(4a^3 + 27b^2, N) = nsd(4 \cdot 2^3 + 27 \cdot 7366^2, 7399) = 1$$

$$\underline{\underline{g = 1}}$$

Protože nám vyšlo $g = 1$, což ukazuje na triviální faktor, musíme zvolit jiné hodnoty a, x a y pro eliptickou křivku $E_{a,b}(\mathbb{Z}_n)$.

Zvolíme náhodně hodnoty:

$$a = 9,$$

$$x = 18,$$

$$y = 75.$$

Dopočteme hodnotu b.

$$b \equiv y^2 - x^3 - ax \ (mod\ N)$$

$$b \equiv 75^2 - 18^3 - 9 \cdot 18 \ (mod\ 7399)$$

$$b \equiv 7030 \ (mod\ 7399)$$

$$\underline{\underline{b = 7030}}$$

Spočteme hodnotu g.

$$g = nsd(4a^3 + 27b^2, N) = nsd(4 \cdot 9^3 + 27 \cdot 7030^2, 7399) = 49$$

$$\underline{\underline{g = 49}}$$

Vidíme, že $0 < g < N$ a jedná se tedy o faktor čísla 7339.

V samotném algoritmu ECM dochází maximálně k tisíci opakování generování hodnot, pokud ani jedna varianta neuspěje, je výpočet ukončen a je zapotřebí použít jinou metodu, případně spustit ECM znovu.

5 VYUŽITÍ PRVOČÍSEL

V poslední části této práce si ukážeme příklady ze „světa počítačů“, kde se využívají jedny z nejmodernějších prvočíselných testů a metod faktorizace celých čísel. Můžeme říci, že bez spolehlivých a rychlých prvočíselných testů bychom v dnešní době nevyužívali například zabezpečené internetové stránky vyžadující nějaký druh autorizace. Příkladem mohou být elektronická bankovnictví, elektronické podpisy, datové schránky, ale například i studentům Západočeské univerzity známé studijní portály STAG a Portál ZČU. Dále jsou prvočísla nezbytná pro většinu počítačových algoritmů pro šifrování.

Využití prvočísel nenajdeme pouze v „počítačovém světě“, ale třeba také u rodných čísel. Každé rodné číslo musí být dělitelné prvočísly 11 a 13 beze zbytku. Toho se využívá pro ověření pravosti rodného čísla, jedná se však pouze o jedno z pravidel (vlastností), které musí mít každé rodné číslo.

5.1 RSA

RSA je šifrovací algoritmus, který se kromě šifrování využívá i v jiných oblastech (např. elektronický podpis). Tento algoritmus je pojmenován po svých autorech Ronaldu Lorin Rivestovi, Adi Shamirovi a Leonardu Max Adlemanovi. Jedná se o šifrování s pomocí klíčů (veřejný a soukromý), které jsou tvořeny s pomocí prvočísel. Tento algoritmus pro šifrování patří mezi nejvyužívanější a při dostatečné délce klíčů je považován za bezpečný.

Bezpečnost tohoto algoritmu je postavena na faktorizaci celých čísel, což je v případě mnohaciferných čísel a podmínky, že celé číslo N musí mít právě dva (různé) prvočíselné faktory (p a q), které jsou také mnohaciferné (některá literatura uvádí pro případ bezpečného zašifrování více jak 200 cifer), velice obtížné. Oproti tomu, pokud si zvolíme dva takové faktory, zjištění tohoto čísla N (součin dvou faktorů) je pro počítač snadným úkolem. Právě zde se využívají prvočíselné testy k ověření, zda jsou zvolené faktory prvočísly. Tento šifrovací algoritmus má tři části. Jedná se o generování klíčů, šifrování a dešifrování.

5.1.1 GENEROVÁNÍ KLÍČŮ

V této první části algoritmu je nutné určit veřejný a soukromý klíč. Veřejný klíč je nutný pro zašifrování zprávy a soukromý klíč pro její dešifrování. Generování klíčů probíhá následujícím způsobem.

1. Volba p a q, výpočet N.

   Zvolíme dvě různá náhodná prvočísla p a q. Následně spočteme jejich součin a dostaneme číslo $N = p \cdot q$.

   Například zvolíme $p = 5, q = 11$ a spočteme $N = p \cdot q = 5 \cdot 11 = 55$ (pro jednoduchost ukázky jsem zvolil malá čísla).

2. Generování veřejného klíče.

   Spočteme hodnotu Eulerovy funkce pro N, $\varphi(N) = (p-1) \cdot (q-1)$, a zvolíme číslo E z intervalu $[2, N-2]$, které bude nesoudělné s $\varphi(N)$. Tím dostáváme veřejný klíč, kterým je dvojice čísel (N, E).

   Pro názornost budeme pokračovat v generování pomocí malých čísel zvolených v předchozím kroku.

   $$\varphi(N) = (p-1) \cdot (q-1) = 4 \cdot 10 = \underline{\underline{40}}$$

   Zvolíme $E = 3$ (opět volíme pro názornost malé číslo), které je nesoudělné s $\varphi(N) = 40$. Máme tedy veřejný klíč $(55, 3)$.

3. Generování soukromého klíče.

   Soukromý klíč tvoří dvojice (N, D). Číslo D určíme pomocí kongruence:

   $$ED \equiv 1 \left(mod\ \varphi(N)\right).$$

   V našem ukázkovém příkladě musí platit:

   $$3D \equiv 1\ (mod\ 40)\ \Rightarrow D = 27.$$

   Jde o jednu z možností, další může být třeba $67, 107, \ldots$

   Máme tedy soukromý klíč $(55, 27)$.

Výsledkem části generování klíčů je klíč veřejný (N, E) a klíč soukromý (N, D), které jsou nezbytné pro zašifrování a dešifrování zprávy. V naší ukázce $(55, 3)$ a $(55, 27)$.

5.1.2 ZAŠIFROVÁNÍ ZPRÁVY

V tomto kroku dochází k zašifrování zprávy pomocí veřejného klíče (N, E). Samotný text zprávy je zakódován pomocí kódovací metody jako číslo X (tyto metody jsou například Shannon-Fanovo kódování či Huffmanovo kódování). Podmínkou je, aby $X < N$. Výsledkem šifrování je pak opět číslo Y.

Získání čísla Y je jednoduché, stačí, aby Y vyhovovalo následující kongruenci:

$$Y \equiv X^E \ (mod\ N).$$

Pro naši ukázku zvolíme $X = 5$ a veřejný klíč (N, E) je $(55, 3)$.

$$Y \equiv 5^3 \ (mod\ 55)$$

$$Y \equiv 125 \ (mod\ 55) \Rightarrow \underline{\underline{Y = 15}}$$

Získali jsme tedy číslo $Y = 15$. To odpovídá zašifrované zprávě, kterou odešleme příjemci, který musí zprávu dešifrovat.

5.1.3 DEŠIFROVÁNÍ ZPRÁVY

K dešifrování zprávy dochází pomocí soukromého klíče (N, D) (tento klíč má pouze příjemce zprávy, kterému je určena, naproti tomu veřejný klíč je dostupný všem). Cílem je získat ze zašifrované zprávy Y dešifrovanou (původní) zprávu X.

Stejně jako bylo jednoduché získání Y z X, tak je jednoduché získání X z Y. X musí vyhovovat kongruenci:

$$X \equiv Y^D \ (mod\ N).$$

Pro naši ukázku máme přijatou zašifrovanou zprávu $Y = 15$ a soukromý klíč (N, D) je $(55, 27)$.

$$X \equiv 15^{27} \ (mod\ 55)$$

Pomocí matematického softwaru dospějeme k výsledku:

$$X \equiv 5 \ (mod\ 55) \ \Rightarrow \underline{\underline{X = 5}}.$$

Získali jsme tedy číslo $X = 5$, které odpovídá původní zprávě.

5.2 ELEKTRONICKÝ PODPIS

Elektronický podpis (někdy digitální podpis) je označení dat, které slouží jako náhrada vlastnoručního podpisu v elektronické komunikaci. Elektronický podpis obsahuje identifikaci jeho autora. K ověření, zda se jedná o platný elektronický podpis, se kromě dalších zabezpečení používá i několik matematických operací. Tyto matematické operace odpovídají šifrování pomocí RSA. Jedinou odlišností je, že probíhá obráceně.

Odesílatel má soukromý klíč a příjemce pomocí veřejného klíče ověří, zda se jedná o platný elektronický podpis. Místo textové zprávy (čísla u RSA) je zde šifrován takzvaný hash (otisk dokumentu), který tvoří nějaké číslo. Po vytvoření datové zprávy (dokumentu), který chceme odeslat a podepsat elektronickým podpisem, vypočteme hash (slouží k tomu takzvaná hashovací funkce) a následně ho zašifrujeme soukromým klíčem, tím vznikne elektronický podpis.

Při ověření podpisu příjemce určí opět hash datové zprávy a porovná ho s hashem, který určí dešifrováním elektronického podpisu. Pokud se oba hashe shodují, je z matematického hlediska elektronický podpis platný a zpráva byla přijata ve stejné podobě jako byla odeslána (nedošlo k manipulaci se zprávou). Ovšem nelze říci, že patří právě odesílateli, to je nutné dále ověřit pomocí certifikační autority.

Na stejném principu fungují i časové razítko (neoznačuje odesílatele, ale pouze garantovaný údaj o čase vzniku datové zprávy) a elektronická značka (oproti elektronickému podpisu ji mohou používat i právnické osoby a organizační složky státu).

ZÁVĚR

Ve své práci jsem se snažil ukázat zajímavou část odvětví matematické algebry, kterou je teorie čísel, především prvočíselnost a faktorizace celých čísel.

Příklady v mé práci jsou pouze úvodem do nespočtu prvočíselných testů a metod faktorizace celých čísel.

Cílem této práce bylo seznámení se s problematikou určování prvočíselnosti a faktorizace celých čísel pomocí klasických a moderních metod. Snažil jsem se ukázat použití jednotlivých testů prvočíselnosti a metod faktorizace celých čísel nejen Pierre de Fermata a Leonharda Eulera, ale i matematiků, kteří jsou autory moderních metod a testů, jako jsou M. Agrawal, N. Kayl, N. Saxena, J. M. Pollard a H. W. Lenstra.

Své poznatky získané studiem testů prvočíselnosti a metod faktorizace celých čísel mohu použít ve své budoucí profesi a seznámit mladé nadšené matematiky s jiným způsobem faktorizace, než je prvočíselný rozklad.

Závěrem bych chtěl ještě jednou poděkovat mému vedoucímu diplomové práce doc. RNDr. Jaroslavu Horovi, CSc., za jeho cenné rady, připomínky a metodické vedení práce.

RESUMÉ

This thesis (Prime numbers and integer factorization) deals with the area of mathematics, which is called algebra. More precisely, it is a part of algebra, which is called number theory.

The main idea of this thesis is prime numbers, primality proving (testing) and integer factorization.

It mainly deals with prime numbers, history of prime numbers, Merssene´s numbers, pseudoprimes, classical primality tests, modern primality tests, classical factorization methods and modern methods of integer factorization.

The first part of my thesis is devoted to history of primes, to finding of the greatest primes, Mersenne´s number and classical primality tests (Fermat´s and Euler´s primality test).

The second part of this thesis focuses on modern primality tests (Miller-Rabin´s primality test, AKS test) and examples of primality proving in mathematical software like the Wolfram Mathematica, the MATLAB, the Wolfram|Alpha, the Maple and the GNU OCTAVE.

The next part of my thesis is devoted to classical methods of integer factorization such as trial divisors, Fermat´s factoring method, Euler´s factoring method and Euclid´s algorithm as aid to factorization.

The fourth part of this thesis deals with modern methods of factorization like Pollard´s method (p-1 method and rho method), Shank´s method square forms factorization (SQUFOF), Morrison and Brillhart´s continued fraction method (CFRAC), Quadratic sieves and Lenstra´s elliptic curve method (ECM).

The final part of this thesis focuses on examples of using prime numbers and primality proving at present, especially in computer encryption.

SEZNAM LITERATURY

1. **Josef, Polák.** *Přehled středoškolské matematiky.* Praha : SPN, 1972.
2. **David, WELLS.** *PRIME NUMBERS - The Most Mysterious Figures in Math.* Hoboken, New Jersey : John Wiley & Sons, 2005. 0-471-46234-9.
3. **Hans, RIESEL.** *Prime Numbers and Computer Methods for Factorization.* Cambridge : Birkhäuser, 1994. 3-7643-3743-5.
4. **Fuchs, Eduard.** *Historie matematiky I.* Brno : Jednota českých matematiků a fyziků, 1993. stránky 140-161. Sv. Co ještě nevíme o prvočíslech.
5. Wikipedia: The Free Encyclopedia. *Mersenne prime.* [Online] [Citace: 10. 11 2014.] http://en.wikipedia.org/w/index.php?title=Mersenne_prime&oldid=633205806.
6. PouletNumber. *WolframMathWorld .* [Online] Wolfram Research, Inc. . [Citace: 21. 1 2015.] http://mathworld.wolfram.com/PouletNumber.html.
7. **Blažek, J. a kol.** *Algebra a teoretická aritmetika: Celost. a vysokoškolská učebnice pro studenty matematicko-fyzikálních, přírodověd. a pedagog. fakult.* Praha : SPN, 1985. str. 278.
8. **Husemöller, Dale.** *Eliptic Curves.* New Yourk : Spinger-Verlag, 1987.
9. **Bressoud, David M.** *Factorization and Primality Testing.* New York : Springer-Verlag, 1989. str. 237. ISBN 03-879-7040-1.
10. **Emerson, David.** *Primality testing and Sub-exponential Factorization.* Boston : Boston College Computer Science Senior Thesis, 2009.
11. **Guy, Richard K.** *Unsolved problems in number theory.* 3. edice. New York : Springer, 2004. str. 437. ISBN 0-387-20860-7.
12. **Peterka, Jiří.** *Báječný svět elektronického podpisu.* místo neznámé : CZ.NIC, 2010.
13. **Petr, Budiš.** *Elektronický podpis a jeho aplikace v praxi.* místo neznámé : ANAG, 2008. ISBN 978-80-7263-465-1.
14. **Rivest, R. L., Shamir, A. a Adleman, L.** *A method for obtaining Digital signatures and public-key cryptosystems.* Cambridge, MA : MIT Lab. for Computer Sciencis, 1978.
15. Přispěvatelé Wikipedie, Legendreův symbol [online], Wikipedie: Otevřená encyklopedie, Datum poslední revize 20. 01. 2014, 09:46 UTC, [citováno 2. 03. 2015] <http://cs.wikipedia.org/w/index.php?title=Legendre%C5%AFv_symbol&oldid=11122433>. [Online]
16. Maplesoft. *Support and user resources.* [Online] 2015. [Citace: 20. 2 2015.] http://www.maplesoft.com/support/.
17. MathWorks. *Support.* [Online] 2015. [Citace: 2. 3 2015.] http://www.mathworks.com/support.
18. Wolfram. *SUPPORT.* [Online] 2015. [Citace: 15. 2 2015.] http://www.wolfram.com/support.
19. GIMPS - Finding World Record Primes Since 1996. *GIMPS Discovers 48th Mersenne Prime.* [Online] Mersenne Research, Inc, 2015. [Citace: 10. 3 2015.] http://www.mersenne.org/primes/?press=M57885161.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

PŘÍLOHY

Všechny materiály k diplomové práci (DP) jsou vypáleny na přiloženém CD, které obsahuje:

- DP_Hefler_PrvocislaAFaktorizace.pdf (DP ve formátu pdf)
- DP_Hefler_PrvocislaAFaktorizace.docx (DP ve formátu docx)
- FermatovaFaktorizacniMetoda.xlsx (ukázka použití Fermatovy metody v programu Microsoft Office Excel 2007)
- PollardovaRoMetoda.xlsx (ukázka použití Pollardovy ρ metody v programu Microsoft Office Excel 2007).