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

TESTOVÁNÍ PRVOČÍSELNOSTI

BAKALÁŘSKÁ PRÁCE

Gabriela Stulíková
Přírodovědná studia, obor Matematická studia

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

Plzeň 2017

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 28.června 2017

.....

vlastnoruční podpis

Děkuji vedoucímu mé bakalářské práce Doc. RNDr. Jaroslavu Horovi, CSc. za odborné vedení, cenné rady a čas, který mi věnoval.

originální zadání

OBSAH

ÚVOD

Práce na téma testování prvočíselnosti, která je rozdělena na tři části a každá část pojednává o určitém problému.

V první kapitole se zaměřím na malou Fermatovu větu a její důkazy. Nejprve se věnuji obecnější teorii. Zprvu Vás seznámím s velkou Fermatovou větou, která je jednou z nejslavnějších vět matematiky. Dále představím hlavního protagonistu Pierra de Fermata a poté se již budu věnovat malé Fermatově větě a jejím důkazům. V této kapitole se objeví jak elementární důkaz, tak důkaz pomocí teorie grup nebo například matematickou indukcí. Všechny důkazy budou rozepsány a okomentovány. S malou Fermatovou větou úzce souvisí i Eulerova věta, která je součástí této kapitoly.

V druhé části probírám základní pojmy jako prvočíslo a kongruence či postupné vysvětlení Eukleidova algoritmu s podrobným výkladem a příklady. Název kapitoly testování prvočíselnosti již napovídá, že popisuji jednotlivé algoritmy či testy, které se k prvočíselnému rozkladu mohou použít. Zmiňuji například nejjednodušší algoritmus zkusmé dělení, Eratosthenovo síto, Solovayův-Strassenův test, Lucasův-Lehmerův test, pravděpodobnostní Millerův-Rabinův test, Solovay-Strassenův a hlavní test Fermatův, se kterým souvisí Pépinův test. V této části se věnuji i Fermatovým pseudoprvočíslům při základu a.

V třetí kapitole s názvem Carmichaelova čísla a objev prvních sedmi Carmichaelových čísel se odkazuji na malou Fermatovu větu, která s tímto pojmem velmi úzce souvisí.

Ve své práci se snažím sepsat ucelený text, který se týká testování prvočíselnosti a všeho, co k tomuto tématu náleží. Veškeré definice se snažím s menšími úpravami zachovávat a ke každé uvádět příklad pro snadnější pochopení, u některých i se slovním postupem.

KAPITOLA PRVNÍ – MALÁ FERMATOVA VĚTA A JEJÍ DŮKAZY

Než se budeme věnovat malé Fermatově větě, uvedeme si větu snad ještě známější. Velká Fermatova věta je v historii matematiky jedna z nejslavnějších vět.

Definice 1.1: velká Fermatova věta

Neexistují přirozená čísla kladná $x, y, z,$ a přirozené $n > 2$, pro něž platí: $x^n + y^n = z^n$.

Tuto větu si nejprve Pierre de Fermat zaznamenal jako poznámku ve své knize přibližně v 17. století.

„Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exigitas non caperet.“[1]

„(Je nemožné rozdělit krychli do dvou krychlí, či čtvrtou mocninu do dvou čtvrtých mocnin, nebo obecně jakoukoli mocninu vyšší než druhou do dvou stejných mocnin. Objevil jsem opravdu tak podivuhodný důkaz, že tento okraj je příliš malý, aby se do něj vešel.)“

Tato věta nebyla dokázána za jeho života, ale až v následujících staletí se dokázaly některé případy. Například Euler dokázal případ s mocnitelem tři. Definitivní důkaz Fermatovy velké věty podal až v roce 1994 matematik Andrew Wiles, pocházející z Velké Británie. Jde o jeden z nejsložitějších důkazů matematiky.

O velké Fermatově větě existuje řada knih i v českém jazyce. Příkladem může být kniha Velká Fermatova věta od Simona Singha. Tato věta je tak populární, že se objevuje i v povídce Karla Matěje Čapka nazvaná $x^n + y^n = z^n$, nebo v seriálu The Simpsons v čarodějnickém díle VI (sedmá série, šestá epizoda). Další citace můžeme zpozorovat například v seriálu Star Trek, či v knize Stiega Larssona – Milénium - Dívka, která si hrála s ohněm. Pro filatelisty je zajímavé, že existuje i česká známka věnované této větě.

Nyní si představíme hlavního protagonistu Pierra de Fermata a poté se budeme věnovat již malé Fermatově větě.

[1] Nagell, T. „Fermat's Last Theorem.“ §68 in Introduction to Number Theory. New York: Wiley, pp. 251-253, 1951

Pierre de Fermat


Obrázek 1: Pierre de Fermat

Narodil se 17. srpna 1601 v Beaumont de Lomagne a zemřel 12. ledna 1665 v Castres. Francouzský matematik, občanským povoláním právník. Svůj život strávil v Toulouse a stal se královským soudcem. Matematické problémy řešil jen ve volném čase. Svými myšlenkami přispěl k rozkvětu matematiky v několika oborech.

Byl spoluzakladatelem teorie čísel a studoval otázky týkající se prvočísel. V teorii pravděpodobnosti spolu s Pascalem vlastně založili tento obor s úvahami o pravděpodobnosti výher v hazardu. V matematické analýze a analytické geometrii odhalil metodu hledání extrémů funkce, pozdější diferenciální a integrální počet. Zde se vyskytuje i vymezení Fermatova principu. Jde o fyzikální tvrzení šíření světla v prostoru z jednoho bodu do druhého po dráze tak, aby potřebná doba nabývala extrémní hodnotu.

Jeho čísla, tzv. Fermatova čísla, jsou ve tvaru $2^n + 1$, *kde* $n = 2^m, m = 0,1,2,\ldots$ *jsou prvočísla. Tento výrok platí pouze pro prvních pět čísel, což dokázal Leonhard Euler v 18. století. V 19. století i Carl Friedrich Gauss použil v geometrii Fermatova čísla pro důkaz euklidovské konstrukce (pomocí kružítka a pravítka) pravidelného mnohoúhelníku s lichým počtem vrcholů.*

Největší dosud známé Fermatovo prvočíslo (dělitelné jedničkou a samo sebou) je $F_4 = 65\,537$. *Čísla* $F_5 - F_{23}$ *mají důkaz, že jsou složená. Existuje pouze úplný rozklad pro čísla* $F_5, F_6, F_7, F_8, F_9, F_{10}, F_{11}$.

$F_0 = 2^{2^0} + 1 = 3 = P$

$F_1 = 5 = P$

$F_2 = 17 = P$

$F_3 = 257 = P$

$F_4 = 65537 = P$

$F_5 = 641 \cdot 6700417$

$F_6 = 274177 \cdot 67280421310721$

$F_7 = 59649589127497217 \cdot 5704689200685129054721$

$F_8 = 1238926361552897 \cdot P$

$F_9 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P$

$F_{10} = 45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P$

$F_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 35608419064458339205 13 \cdot P$

$F_{12} = 114689 \cdot 26017793 \cdot 63766529 \cdot 190274191361 \cdot 1256132134125569 \cdot C$

$F_{13} = 2710954639361 \cdot 2663848877152141313 \cdot 3603109844542291969 \cdot$
$\cdot 319546020820551643220672513 \cdot C$

$F_{14} = C$

$F_{15} = 1214251009 \cdot 2327042503868417 \cdot 1687688170295169723830241270169 61 \cdot C$

$F_{16} = 825753601 \cdot 188981757975021318420037633 \cdot C$

$F_{17} = 31065037602817 \cdot C$

$F_{18} = 13631489 \cdot 81274690703860512587777 \cdot C$

$F_{19} = 70525124609 \cdot 646730219521 \cdot C$

$F_{20} = C$

$F_{21} = 4485296422913 \cdot C$

$F_{22} = C$

$F_{23} = 167772161 \cdot C$

$F_{24} = C$

Toto je prvních 25 Fermatových čísel známých k dubnu 2005. P je prvočíslo, C je kompozitní (složené) číslo. Nejmenší Fermatovo číslo neznámého charakteru je F_{33}.

Definice 1.2: malá Fermatova věta

Pro každé prvočíslo p (tedy přirozené číslo, které je dělitelné pouze jedničkou a sebou samým) a každé celé číslo k, kde největší společný dělitel $(k, p) = 1$ platí:

$k^{p-1} \equiv 1 \pmod{p}$ nebo $k^p \equiv k \pmod{p}$, tj.

$(k^p - k)$ je dělitelné prvočíslem p.

Elementární důkaz:

Uvažme, že máme x různých písmen abecedy $X_1,....X_a$ a množinu slov o p písmenech patřící téže abecedě, kde platí, že p je prvočíslo.

Vznikne x^p slov. Mějme množinu $\nu(X_{i1}X_{i2}...X_{ip}) = X_{i2}X_{i3}...X_{ip}X_{i1}$.

Tuto množinu rozdělíme na menší podmnožiny Z tak, že slovo (označíme písmenkem O) $O \in Z \Leftrightarrow \nu(O) \in Z$.

Vezměme k nejmenší číslo tak, aby $\nu^k O = O$. Očividně $k \mid p \Leftrightarrow k = 1 \vee k = p$.

Každá podmnožina Z má jeden prvek, anebo p prvků. Počet prvků záleží na opakování písmen ve slově, jestliže máme ve slově p krát jedno písmeno, máme jeden prvek.

Množin jednoprvkových je x tj. $\{X_1X_1...X_1\},...,\{X_x,...,X_x\}$. Ostatní slova lze rozdělit do podmnožin o p prvcích, což představuje $p \mid (k^p - k)$.

Důkaz pomocí teorie grup

Buď dáno prvočíslo p. Je dobře známo, že množina zbytkových tříd $\mathbb{Z}_p$ je těleso (libovolná množina s binárními operacemi $\oplus, \otimes$) Nenulové prvky patřící $\mathbb{Z}_p$ vytvářejí grupu (množina s binární operací násobení splňující axiomy grupy) $\mathbb{Z}^*_p$ řádu $p-1$. Buď $k \in \mathbb{Z}^*_p$ nějaký prvek této grupy. Tento prvek generuje cyklickou podgrupu (grupa, generovaná jediným prvkem) řádu l, kde l je nejmenší číslo, pro které platí $k^l = 1$. Nyní podle důsledku Lagrangeovy věty, že řád každého prvku či podgrupy dělí řád grupy, kdy tato věta je základním tvrzením v teorii grup, dostaneme $p - 1 = lm$.

Spojením těchto tvrzení vznikne $k^{p-1} = k^{lm} = (k^l)^m = 1^m = 1$ v $\mathbb{Z}^*_p$. Platí pro $k \in \mathbb{Z}_p \neq 0$ vzniká $k^{p-1} = 1$ v $\mathbb{Z}_p$, tj. $k^{p-1} \equiv 1 \pmod{p}$.

Důkaz pomocí součinu zbytkových tříd

Mějme p prvočíslo v množině zbytkových tříd označenou $\mathbb{Z}_p$, kde její nenulové prvky tvoří grupu $\mathbb{Z}_p^*$ řádu $p-1$. Násobením nenulovým číslem k vzniká permutace prvků $\mathbb{Z}_p$, z čehož vyplívá, že součin všech prvků se nemění.

$$\prod_{a\in\mathbb{Z}_p^*} a = \prod_{a\in\mathbb{Z}_p^*} ka = k^{p-1}\prod_{a\in\mathbb{Z}_p^*} a,$$

jelikož je každý prvek násobení nesoudělný s p, tak je i součin na levé i na pravé straně nesoudělný s naším prvočíslem p a můžeme krátit. Dostáváme rovnici

$$k^{p-1} = 1 \text{ v } \mathbb{Z}_p.$$

Důkaz pomocí matematické indukce

Zvolme libovolné $a < p-1$. Víme, že $k^{p-1} \equiv 1 \pmod p$. V přirozených číslech, což je množina, obsahující kladná celá čísla, označující se $\mathbb{N}$, platí nerovnice $1 \le k \le a.$ dále $(a+1)^p \equiv a^p + 1^p \pmod p$ - (binomický rozvoj, kde ostatní členy jsou dělitelné p).

Pro důkaz matematickou indukcí, zvolíme

1. indukční předpoklad $a^p \equiv a \pmod p$, pak
2. $(a+1)^p \equiv a+1 \pmod p$ = $(a+1)^{p-1} \equiv 1 \pmod p$

   toto tvrzení platí pro $k = 1,\ldots, p-1$
3. pomocí binomického rozvoje dostáváme pro $z\in\mathbb{Z}$ $(y+pz)^p \equiv k^p \pmod p$
4. nakonec pro jakékoliv číslo $x\in\mathbb{Z}$ takové, že není násobkem p platí: $x = y + zp; y = \{1,2,\ldots, p-1\} \Rightarrow x^{p-1} \equiv k^{p-1} \equiv 1 \pmod p$.

Důkaz pomocí faktoriálu

Vezměme si množinu $\{k, 2k, ..., (p-1)k\}$.

Z těchto čísel vzniká po dělení prvočíslem p po dvou různý zbytek. Pokud tento předpoklad není splněn, tj. $kn \equiv km \pmod{p}$ pro $n, m \in 1, 2, ..., p-1 \wedge n > m$ vznikne tvrzení, že:

$$p \mid (nk - mk) \vee p \mid (n-m)k \text{ tj.}$$

prvočíslo p dělí buď k nebo $n - m$, kdy ale $n - m < p$, což představuje spor.

Povšimněme si, že všechna tvoří nenulový zbytek po dělení p, proto platí

$$(p-1)! = 1 \cdot 2 \cdots 3 \equiv k \cdot 2k \cdots (p-1)k = (p-1)! \cdot k^{p-1} \pmod{p}.$$

Faktoriály $(p-1)!$ jsou nesoudělné s prvočíslem p, lze kongruence krátit a vznikne definice 1.2 $\rightarrow$ $k^{p-1} \equiv 1 \pmod{p}$.

S malou Fermatovou větou velmi úzce souvisí Eulerova věta, která představuje zobecnění malé Fermatovy věty.

Věta 1.3: Eulerova věta

Nechť dvě k, n jsou dvě nesoudělná přirozená čísla a $\varphi(n)$ představuje počet čísel menších nebo rovných n, opět nesoudělná s n. Pak platí:

$k^{\varphi(n)} \equiv 1 \pmod{n}$, kde

$\varphi(n)$ je Eulerova funkce čísla n.

Vlastnosti Eulerovy funkce φ

pro p prvočíslo platí: $\varphi(p) = p - 1$, protože všechna čísla menší než p jsou nesoudělná s p.

Druhou vlastností je důsledek čínské zbytkové věty, která řeší vlastnosti čísel v grupách kongruence modulo n. Pro n, m nesoudělná dostáváme vztah $\varphi(nm) = \varphi(n)\varphi(m)$.

Dále platí pro p prvočíslo a $\alpha \in \mathbb{N}$, kdy nesoudělné jsou násobky $p < p^{\alpha}$, kterých je právě $p^{\alpha-1}$ následující tvrzení: $\varphi(p^{\alpha}) = (p-1)p^{\alpha-1}$.

Důsledkem těchto vlastností získáváme tvrzení:

Je – li $n = p_1^{\alpha 1}, ..., p_n^{\alpha n}$ prvočíselný rozklad čísla n, pak

$$\varphi(n) = p_1^{\alpha 1-1}(p_1-1)p_2^{\alpha 2-1}(p_2-1)p_3^{\alpha 3-1}(p_3-1)\cdots p_n^{\alpha n-1}(p_n-1) =$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\cdots\left(1-\frac{1}{p_n}\right)$$

Důkaz Eulerovy věty

Libovolné číslo od 0 do $n-1$, nesoudělné s n, má inverzi v Z_n a přesně $\varphi(n)$ invertibilních prvků (takový prvek, pro který existuje inverzní prvek) s označením $a_1, \ldots, a_m$.

Pro každou dvojici prvků a_i a a_j, kdy $i, j \in \{0,1,2,...,\varphi(n)\}$ platí: $a_i k \neq a_j k$ v Z_n

Rovnost nemůže platit, jelikož čísla a_i, a_j jsou nesoudělná s n.

Nyní si představme posloupnost $a_1k, a_2k, ..., a_{\varphi(n)}k$ a druhou posloupnost $a_1, a_2, \ldots, a_{\varphi(n)}$.

Nyní vytkneme z první posloupnosti k a dostáváme

$k^{\varphi(n)}(a_1, a_2, ..., a_{\varphi(n)}) = a_1, a_2, ..., a_{\varphi(n)}$ v Z_n.

Nyní jen vykrátíme a dostáváme tvrzení

$k^{\varphi(n)} = 1 \pmod{n}$.

Příklad 1.4 Určete, kolik je 7^{3822} v Z_{15} ?

Řešení:

Nejprve si určíme největšího společného dělitele čísel 7,15.

$$NSD(7,15)=1$$

$$7=1\cdot 7$$
$$15=1\cdot 3\cdot 5$$

Nyní dosadíme do vzorce, který je pro náš příklad je upraven takto

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$$

$$\varphi(15)=15\cdot\left(1-\frac{1}{5}\right)\cdot\left(1-\frac{1}{3}\right)=8\,.$$

Podle Eulerovy věty tedy platí $7^8\equiv 1\,(\mathrm{mod}15)$. To je důležité tvrzení. Vydělením exponentu 3822 číslem 8 dostaneme neúplný podíl 477 a zbytek 6, tedy

3822 = 8.477 + 6.

Tím víme, že číslo 7^{3822} lze rozložit jako

$(7^8)^{477}\cdot 7^6 = 1^{477}\cdot 7^6$, kdy 7^6 lze vyjádřit jako

$7^2\cdot 7^2\cdot 7^2 = 1\cdot 49\cdot 49\cdot 49 = 4\cdot 4\cdot 4 = 16\cdot 4 = 1\cdot 4 = 4$ v Z_{15}

Poznámka: Užili jsme toho, že $49=145\cdot 3+4$.

Odpověď na otázku, kolik je 7^{3822} v Z_{15} je 4.

Abychom si více představili, jak je Eulerova věta v dané situaci důležitá, uveďme výpočet z programu Mathematica:

QuotientRemainder[7^3822,15]
{614635549379898810637336305503223282420984510160848246492194400708366606
911320299129323754753743695060356988026623079715469228221356979605457351 2
515234119866326250703611875445338466727987160364907639492252419440335403 3
980414875092982015310884095410819543776752302447951903840324162330342089 2
814491675602943778855976542662770634166755880353992320106717413277123282 9

074262530600802170087535183145137371162396231353976786276063373120046092422934341353624363971864319335843525707181861263524774289806886829236463880818400744757982630564934424764261912864713660769855976990019734562736984278926736874747992958157970157627624543436354213528013468710889197562991181004677937594275674379416676864801267059697631596853122823017237315754684395231500478045603104168780763915352938962928820737159981349342277535395877908144680856347316381804086743825562030681014808749308691062465101491926332973666511325062980002675563106854011728766392990789113707729537107728969470732545243410634670404317600936156454216054242258705103444337631662263045134474362490361937119976984143243376064213329922710853468240524143464323584128248519757284196003687504261600995968921910251058294889529671384624595214223266262740001520883083584583272408679405750387957693787622860601280859683319605680808914674980219157499830848556887094582099935653455698114581287573462974501602861131852688818260684379314941259196702771471228142373857966858904921856804339307569929526401906120066560379971579426137379759652160932056038756900541024282840478306990119961874923257427007600456850282947839820745515760512192617182535152631455259216861818673250811529262727945769904743569110562152794710075111860077584543903909570840303872124050902499480326825288732762000203342830267996163501233358043384170842774892086502966626076047310972101162195893063122233149841949232333630384413250295011791362960334467354649322791700521484927688554735584947936991127822415715491038590082110015844016870061344977853599938150389247914117727728769420405167096706577930917119944632398744058172174863537424824776853282288318316818156660682778416433007737771845080953446707077757010139594029756093327020853912539638558308652135566298923215106321894751861408748580224447339904923820200723755831518003958023940638142552331401137792209517665682500262692963845532067985495555915464289572146319452056175666462326538160526183266624017738552108721158671298115239195059836548985511282366339280732990580524982241615982750425112324806161841111112619125248066465408822013292901059438686181208913332461820447359250002745916052681405816474919788158439578054589320074215581656821318967231269408662454347499261976110042857032500977005301723098135262686856968237045389371335529030169596081103457542526114664957247635202865928015695797303883972043902671458677381 1

2386747514753425092394155258084636136716448093628913085345421642113549059
7434030233592817100283824193185057232452194396710957558042653280563992530
1551168665158465655217584622933932334369648031692191146388552023337844323
1018842078179345261765404708898366439311769455405686179285340527084796288
9227941697308557057418103722044672073133256179283147803102466251096972103
9463895094720591423014219438968187946600150960837780309783995120378250746
614975425498047203, 4}

Povel QuotientRemainder skutečně exaktně vyčíslil mocninu 7^3822, což je podle očekávání obrovské číslo a poté i zbytek při dělení tohoto čísla číslem 15.

Příklad 1.5. Určete hodnotu Eulerovy funkce pro číslo 735.

Řešení:

Rozložíme číslo 735 na prvočíselný součin.

$$735 = 3 \cdot 245 = 3 \cdot 5 \cdot 49 = 3 \cdot 5 \cdot 7 \cdot 7$$

Nyní dosadíme do příslušného vzorce, nebo můžeme použít jejich vhodnou kombinaci

$$\varphi(735) = \varphi(3) \cdot \varphi(5) \cdot \varphi(7^2)$$

$$\varphi(p) = p - 1$$

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1}$$

$$\varphi(3) = 3 - 1 = 2, \varphi(5) = 5 - 1 = 4,$$

$$\varphi(7^2) = (7-1)7^{2-1} = 6 \cdot 7$$

$$\varphi(735) = 2 \cdot 4 \cdot 42 = 336$$

Eulerova funkce nabývá pro číslo 735 hodnoty 336.

Příklad 1.6: malá Fermatova věta – ověření pro malá čísla

Řešení:

a) Vezměme si prvočíslo $p = 5$ a $k = 2$. Číslo dvě není násobkem prvočísla 5, tato čísla jsou nesoudělná.

Nyní můžeme dosadit do malé Fermatovy věty a rozepsat

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

V našem příkladě je

$$2^{5-1} \equiv 1 \pmod{5}$$

$$2^4 \equiv 1 \pmod{5}.$$

b) Mějme $p = 5, k = 2$. Jsou takto čísla dělitelná 5?

Stejně jako v předchozím bodě a) číslo 5 není násobkem čísla 2. Můžeme proto použít i jiný postup:

$$k^p - k$$

$$2^5 - 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 - 2 = 32 - 2 = 30,$$

ano, číslo 30 lze vydělit 5 s výsledkem 6.

Shrnutí: V obou případech lze odpovědět, že pokud zvolíme prvočíslo $p = 5$ a $k = 2$ vyjde nám rovnost jak v bodě za a) tak i za b).

Příklad 1.7: další důsledek malé Fermatovy věty

Řešení:

a) Zvolme prvočíslo $p = 3$, $k = 4$.

Čtyřka není násobkem čísla 3, proto lze pokračovat a chceme ověřit, že číslo $k^p - k = 4^3 - 4$ je dělitelné 4.

$$4^3 - 4 = 4 \cdot 4 \cdot 4 - 4 = 16 \cdot 4 - 4 = 64 - 4 = 60,$$

$$\frac{60}{4} = 15(zbytek 0),$$

pokud vyjde zbytek 0, respektive číslo 4 dělí číslo 60 beze zbytku, máme malou Fermatovu větu.

b) Ukažme si dosazení do kongruence

P = 3, k= 4

NSD(3,4) =1

Dosadíme do malé Fermatovy věty

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

V našem příkladě tj.

$$4^{3-1} \equiv 1 \pmod{3}$$

$$4^2 \equiv 1 \pmod{5}$$

Poznámka: $4^2 = 16 \Rightarrow \frac{16}{5} = 3(zbytek\ 1)$, což odpovídá kongruenci ve vzorci malé Fermatovy věty.

Leonhard Euler

Narodil se 15. dubna 1707 v Basileji ve Švýcarsku a zemřel 18. září 1789 v Petrohradě v Rusku. Své dětství prožil v Riehen se svojí rodinou. Zde navštěvovat školu, kde se již jako malý zajímal o matematiku, které rozuměl i jeho otec. Ve svých čtrnácti letech začal studovat basilejskou univerzitu. Jeho talent zaujal i Johanna Bernoullia, který mu dával soukromé hodiny.

V roce 1723 se stal Euler magistrem filozofie a na přání

Obrázek 2: Leonhard Euler

svého otce se začal věnovat studium teologie. Díky Johannu Bernoulli, který přesvědčil Paula Eulera (otce Leonharda Eulera), začal studovat matematiku. V roce 1726 úspěšně ukončil toto studium a o rok později vyhrál 2. místo v soutěži pařížské akademie Velké cena s tématem lodních stožárů.

Od roku 1727 působil jako učitel matematiky a mechaniky v Petrohradě. V letech 1727-1730 působil v ruském námořnictvu jako poručík zdravotní služby a v roce 1730 se stal i profesorem fyziky a řádným akademikem. V této době se zabýval hlavně teorií čísel, diferenciálními rovnicemi, variačním počtem a mechanikou.

Po tomto období se roku 1733 vrátil zpět do Švýcarska a o rok později si vzal za ženu Katharinu Gsell a měl třináct dětí. Dva roky na to onemocněl a tyto zdravotní problémy ho doprovázely až do konce života. V roce 1838 pravděpodobně kvůli šedému zákalu oslepl na jedno oko.

V roce 1737 vydal svou první knihu Mechanica, která souvisí s Newtonovou dynamikou. Získal Velkou cenu Pařížské akademie a rok poté navštívil Berlín. Zde působil 25 let a stále spolupracoval s petrohradskou akademií. Roku 1744 byl jmenován ředitelem matematického oddělení Akademie věd, kde měl na starost i botanickou zahradu nebo například publikaci map.

V roce 1748 publikoval vlnovou rovnici, která popisuje kmitání strun v čase a prostoru. O 11 let později odvodil rovnici pro kmitající plochu s pevným okrajem (buben).

Také se účastnil prací na úpravách říčního kanálu Finow a pracoval i jako poradce vlády pro loterii, pojištění, úroky, důchody a dělostřelectvo. V Berlíně publikoval okolo 380 článků a velké množství knih například o výpočtech drah planet, o dělostřelectvu a balistice, o analýze nebo pohybu Měsíce.

Spory s Fridrichem II ho přiměly k návratu zpět do Petrohradu roku 1766. V roce 1771, již slepý, přišel o část rukopisů při požáru svého domu. I přesto stále pokračoval ve své vědecké práci a studiu optiky a algebry. 18. září umírá v Petrohradě na záchvat mrtvice. Jeho práce se publikovaly ještě 50 let po jeho smrti.

Jeho dílem se inspiroval i Carl Fridrich Gauss

KAPITOLA DRUHÁ – TESTOVÁNÍ PRVOČÍSELNOSTI. PSEUDOPRVOČÍSLA PŘI ZÁKLADU a

Nejprve si musíme představit základní pojmy a výpočty. V první kapitole jsme si uvedli znění malé Fermatovy věty a její důkazy, kde se vyskytly určité pojmy jako prvočíslo, kongruence apod. Než začneme s její aplikací, řekněme si něco více o některých pojmech použitých v předchozí kapitole, patřící do teorie čísel.

Definice 2.1: Prvočíslo

Prvočísla jsou čísla větší než 1, dělitelná beze zbytku jedničkou a sama sebou, patřící do množiny přirozených čísel. Pokud má číslo i další dělitele, nazývá se složené číslo. Jsou to všechna čísla $p \geq 2$.

Některé z jejich vlastností jsou běžné a známé, jiné velice pozoruhodné:

Prvočísel je nekonečně mnoho.

Je- li p prvočíslo, $p|(k \cdot l) \Rightarrow p|k \vee p|l$.

Každé číslo složené můžeme vyjádřit jako součin prvočísel.

Pokud $a \in \mathbb{Z} \wedge a > 1 \Rightarrow \exists p : a < p < 2a$ (Bertrandův postulát)

Je-li grupa konečná a existuje nejvyšší mocnina prvočísla p, která dělí řád grupy, existuje v grupě podgrupa nejvyššího řádu

$\sum \frac{1}{p}$ diverguje.

Na úlohy na hledání rozkladu přirozeného čísla v součin prvočísel narazíme již na základní škole.

Příklad 2.2: Rozklad na součin prvočísel u jednoduchého čísla 12.

Řešení:

Rozklad se nalezne postupným dělením (beze zbytku) samozřejmě s využitím toho, že děti znají několik nejmenších prvočísel. Tento proces probíhá tak dlouho, dokud nedostaneme číslo 1. Je dobré znát prvočinitele do hodnoty druhé odmocniny, pokud se jedná o složené číslo. Jde o nejjednodušší způsob testování prvočíselnosti.

$$12 = 2 \cdot 6$$
$$6 = 2 \cdot 3$$

Čísla 2,3 jsou prvočísla, která již nejde rozložit, proto $12 = 2 \cdot 2 \cdot 3$.

Složitější zadání může vypadat například takto:

Příklad 2.3: Nalezněte taková prvočísla, která lze vyjádřit součtem i rozdílem prvočísel.

Řešení:

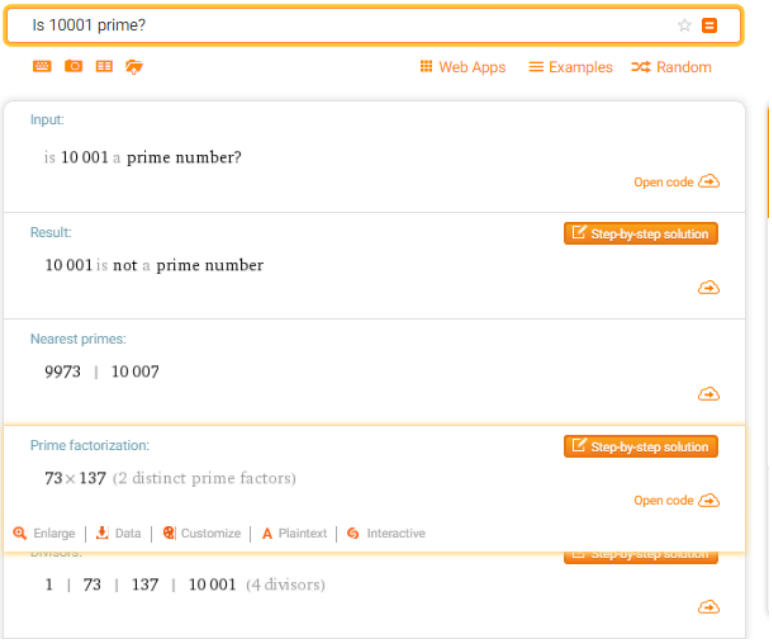
Je-li p prvočíslo, které lze zapsat jako součet i rozdíl, určitě platí $p > 2$, p je liché. Jestliže operace sčítání a rozdílu má dát prvočíslo, což je liché číslo, jedno z prvočísel musí být sudé (rovno 2).

$$p = x + 2 = y - 2, \ p, x, y \text{ jsou prvočísla}$$

Jediná prvočísla jdoucí za sebou v aritmetické posloupnosti s diferencí 2 jsou $3, 5, 7$. Tedy pouze prvočíslo 5 lze vyjádřit jako $5 = 3 + 2 = 7 - 2$.

Vrátíme se ještě jednou k faktorizaci (rozkladu) přirozeného čísla v součin prvočísel. Nalezení rozkladu přirozeného čísla v součin prvočísel je zřejmě fundamentální aritmetickou úlohou. I proto existuje velké množství počítačových programů či mobilních aplikací, které vypočítají rozklad na prvočísla.

Příkladem takového programu volně dostupného na internetu je program WolframAlpha, program Mathematica či jiné.



Obrázek 3: WolframAlpha

Rozklad na součin se používá i pro výpočet největšího společného dělitele (NSD) nebo pro nejmenší společný násobek (NSN). Pro výpočet nejmenšího společného dělitele dvou přirozených čísel lze efektivně využít tzv. Eukleidův algoritmus.

Věta 2.4: Eukleidův (Euklidův) algoritmus

Slouží k určování největšího společného dělitele (*NSD*) dvou přirozených čísel tak, že výsledné číslo je největší číslem, které dělí obě čísla beze zbytku. Používá se u vyšších čísel, kde není hned poznat rozklad na prvočísla. Algoritmus lze použít i pro nejmenší společný násobek (NSN), kde součin dvou čísel, pro která chceme nejmenší společný násobek znát, se vydělí největším společným dělitelem.

Příklad 2.5. Určete největší společný dělitel čísel 945,729.

Řešení:

Postup si ukážeme pomocí Eukleidova algoritmu.

$$D(945,729) = ?$$

Vezmeme větší číslo, tj. 945 a rozložme ho na součin prvočísla + zbytek.

$$945 = 1 \cdot 729 + 216$$

Nyní vezmeme opět větší číslo z rozkladu a rozložíme ho pomocí zbytku.

$$729 = 3 \cdot 216 + 81$$

Opět opakujeme stejný postup, až se dostaneme ke zbytku, který již nelze rozložit, tj. máme prvočíslo.

$$216 = 2 \cdot 81 + 54$$
$$81 = 1 \cdot 54 + 27$$
$$54 = 2 \cdot 27 + 0$$

V našem příkladě již vidíme, že vyšel zbytek nula, proto $NSD(945,729) = 27$.

$$\text{NSN}(945,729) = \frac{945 \cdot 729}{27} = 25515,$$

Po dosazení do podílu pro výpočet NSN, získávám $\text{NSN}(945,729) = 25515$.

Příklad 2.6: Určete největší společný dělitel čísel 55567, 32399.

Řešení:

Na tomto příkladě si ukážeme rozepsaný postup Eukleidova algoritmu u vyšších čísel, jelikož rozklad na prvočísla by byl opravdu zdlouhavý.

$$NSD(55567, 32399)$$

$$55567 - 32399 = 23168$$

$$32399 - 23268 = 9231$$

$$23168 - 9231 \cdot 2 = 4706$$

$$9231 - 4706 = 4525$$

$$4706 - 4525 = 181$$

$$4525 - 181 \cdot 25 = 0$$

$$NSD(55567, 32399) = 181$$

$$NSN(55567, 32399) = \frac{55567 \cdot 32399}{181} = 9946493.$$

Největší společný dělitel zadaných čísel je 181 a nejmenší společný násobek 9 946 493.

Podle Eukleidova algoritmu máme 6 dělení se zbytkem. U rozkladu na součin prvočísel je zapotřebí použít seznam prvočísel a 42 dělení.

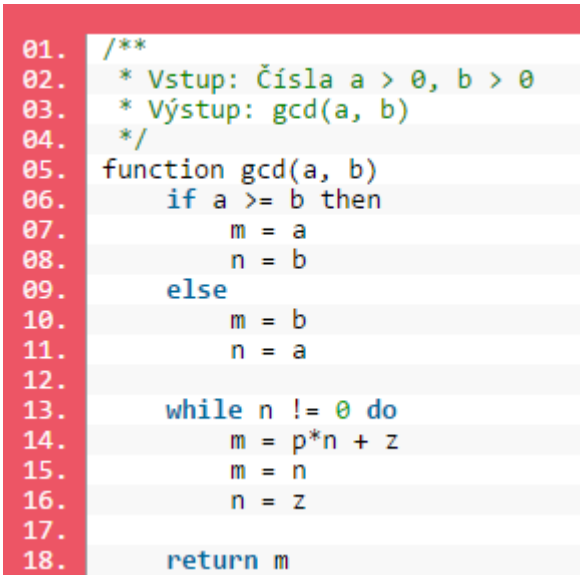
Ukažme si, jak zapsat Euklidův algoritmus jako návod pro výpočet v počítači.

Pseudocode pro Javu zapsán v programovacím jazyce:

```
/**
 * Vstup: Čísla a > 0, b > 0
 * Výstup: gcd(a, b)
 */
function gcd(a, b)
    if a >= b then
        m = a
        n = b
    else
        m = b
        n = a

    while n != 0 do
        m = p*n + z
        m = n
        n = z

    return m
```



Obrázek 4: Pseudocode Eukleidova algoritmu

Zbytek po dělení se každým krokem snižuje a je nazýván variantem. Dvojice čísel $n, z \wedge m, n$ jsou invariantem a splňují rovnici tohoto algoritmu $m = p \cdot n + z$. Jestliže číslo v našem případě a dělí levou stranu rovnice, musí zároveň dělit i pravou stranu rovnice.

Potřebujeme získat největší společný dělitel a tak vidíme, že pokud $a \mid m \Rightarrow a \mid n$ z těchto tvrzení spojených dohromady vyplívá, že i $a \mid z$.

Jedním z dalších pojmů je kongruence.

Definice 2.7: Kongruence

Celé číslo a je kongruentní s celým číslem b podle modulu m, kdy $m \in \mathbb{N} \wedge m \geq 1$. Označujeme $a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$.

Čteme jako a je kongruentní s b modulo m. Toto tvrzení platí právě tehdy, když rozdíl $(a-b)$ dělí m.

Kongruence na množině celých čísel je relací ekvivalence, která způsobí, že základ množiny celých čísel se dělí na třídy navzájem ekvivalentních prvků, tzv. zbytkové třídy označující se $Z_0, Z_1, ..., Z_{n-1}$.

Jelikož je relací ekvivalence, platí i reflexivita, symetrie a tranzitivita.

Důkaz reflexivita: $a \overset{?}{\equiv} a \pmod{m} \Leftrightarrow$

$m \mid a - a$

$m \mid 0$

Důkaz symetrie: $(a \equiv b \pmod{m} \wedge a \neq b) \Rightarrow b \equiv a \pmod{m}$

$a \equiv b \pmod{m} \Rightarrow m \mid (a-b) \Leftrightarrow m \mid (b-a) \Leftrightarrow b \equiv a \pmod{m}$

Důkaz tranzitivity: $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

$a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$
$b \equiv c \pmod{m} \Leftrightarrow m \mid (b-c)$ } $m \mid [(a-b)+(b-c)] \Rightarrow m \mid (a-c) \Rightarrow$
$\Rightarrow a \equiv c \pmod{m}$

Věta 2.8: O sčítání a násobení kongruencí

$$(\forall a,b,c,d \in \mathbb{Z})(\forall m \in \mathbb{N}, m>1): a \equiv b (\mathrm{mod}\, m) \wedge c \equiv d (\mathrm{mod}\, m) \Rightarrow$$
$$\Rightarrow \quad a+c \equiv b+d (\mathrm{mod}\, m)$$
$$a \cdot c \equiv b \cdot d (\mathrm{mod}\, m)$$

Tato věta platí i pro n kongruencí a zároveň platí i věta o mocnění: $a^n \equiv b^n (\mathrm{mod}\, m)$.

Příklad 2.9: Určete zbytek po dělení čísla 12^{144} číslem 65.

Řešení:

Pro tuto kongruenci použijeme větu o mocnění.

$$12 \equiv 12 (\mathrm{mod}\, 65)$$
$$12^2 \equiv 14 (\mathrm{mod}\, 65)$$

Jak jsme dostali číslo 14?. $12^2 = 144$, jelikož máme kongruenci $(\mathrm{mod}\, 65)$, od čísla 144 odečteme 65. Výsledné číslo je pořád nad náš zadaný modul, můžeme opět odečítat. Postup: $144-65=79; 79-65=14$. Kongruenci opět umocníme na druhou.

$$\left(12^2\right)^2 \equiv 14^2 (\mathrm{mod}\, 65)$$

Opět použijeme postup, který je popsán výše $14^2 = 196; 196-65=131-65=66-65=1$.

$$12^4 \equiv 1 (\mathrm{mod}\, 65)$$

Pokud opět umocníme na potřebnou mocninu, pak jednička umocněná na libovolné číslo je stále číslo jedna.

$$12^{144} \equiv 1 (\mathrm{mod}\, 65)$$

Zbytek po dělení čísla 12^{144} číslem 65 je 1.

Příklad 2.10: Dokažte, že číslo 65 dělí součet $12^{163} + 47^2$.

Řešení:

Použijeme větu o sčítání kongruencí, nejprve vypočteme každou kongruenci zvlášť, poté je sečteme, doupravíme a máme hledaný výsledek.

$$12 \equiv 12 (\mathrm{mod}\, 65)$$
$$12^2 \equiv 14 (\mathrm{mod}\, 65) / ()^2$$
$$12^4 \equiv 1 (\mathrm{mod}\, 65) / ()^{34}$$
$$12^{136} \equiv 1 (\mathrm{mod}\, 65)$$

$$47 \equiv (-18) (\mathrm{mod}\, 65)$$

Pokud zapíšeme tuto kongruenci jako $47 \equiv 47 (\mathrm{mod}\, 65)$, tak po umocnění získáváme zbytečně velké číslo, proto je jednodušší zkusit spočítat $47 - 65 = -18$. Pokud umocníme (-18) na druhou, získáme výsledek 324, který v $(\mathrm{mod}\, 65)$ tvoří výsledek $4 \cdot 65 + 64$.

$$47^2 \equiv 64 (\mathrm{mod}\, 65)$$

Nyní obě kongruence sečteme a zjistíme výsledek.

$$12^{136} + 47^2 \equiv 1 + 64 (\mathrm{mod}\, 65)$$
$$12^{136} + 47^2 \equiv 0 (\mathrm{mod}\, 65)$$

Ano, číslo 65 dělí součet $12^{163} + 47^2$.

Definice 2.11: Testy prvočíselnosti

Všechny testy prvočíselnosti řeší otázku, zda zadané přirozené číslo je prvočíslo, obvykle bez použití prvočíselného rozkladu.

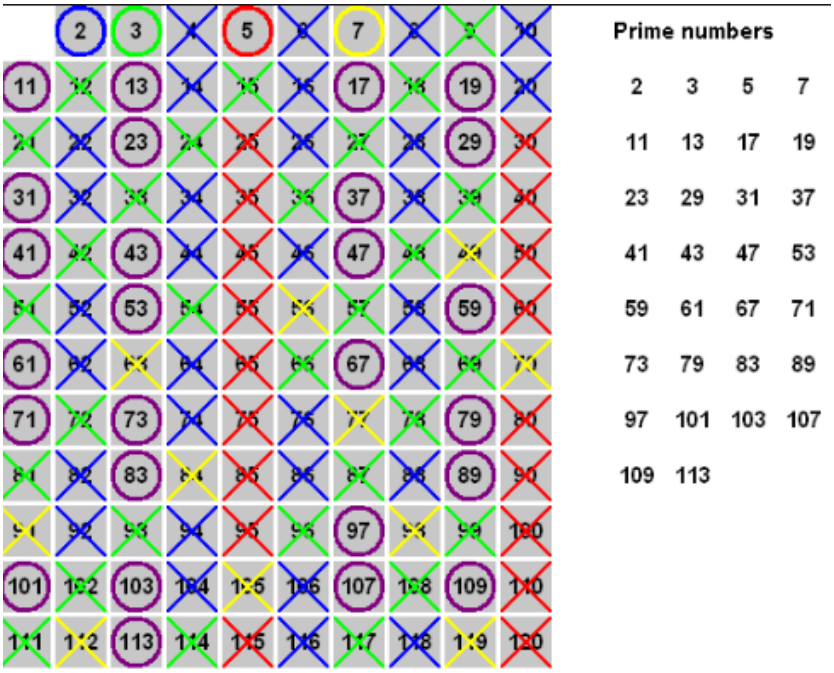
Nejjednodušší algoritmus pro testování je **zkusmé dělení**. Jde o princip postupného dělení testovaného čísla možnými děliteli. Může se dělit všemi přirozenými čísly menšími než je zadané číslo, nebo například jen prvočíslem dva či lichými čísly. Lze provádět zkusmé dělení i jen s prvočísly menšími nebo rovnými odmocnině ze zadaného čísla. Je vhodný pro testování malých čísel, řádově do milionu, pokud použijeme počítačový program.

Dalším příkladem algoritmu, lze použít tzv. **Eratosthenovo síto**. Jedná se o jednoduchý výpočet směřující k nalezení všech prvočísel, která jsou menší než horní mez. Funguje jako síto, jak již napovídá název. Na začátku máme všechna přirozená čísla, z dané horní meze, se vyjme první číslo, které je prvočíslem a odstraní se jeho násobky. Toto

opakujeme do té doby, až je v seznamu odstraněno poslední číslo. Také můžeme končit, když je prvočíslo číslo vyšší než odmocnina maximálního čísla.

V následující tabulce můžeme vidět, jak celý princip funguje. Nejprve odstraníme modrá čísla (násobky 2), poté zelené násobky 3, následují násobky čísla 5 vyznačená červeně, dále žluté násobky 7, a nakonec zůstávají prvočísla vyznačená fialově.

Eratosthenovo síto je běžným školním postupem. Umožní školákům prožít radost z nalezení menší „sbírky“ prvočísel, jenže jde nepochybně o metodu velice pomalou a neefektivní. Stejně tak je tomu i s metodou zkusmého dělení. Bylo by proto dobré mít nějaký test, který by odhalil, zda dané (a velké) přirozené číslo je prvočíslem nejlépe po několika početních operacích.



Obrázek 5: Prvočísla

Věta 2.12: Motivace Fermatova testu

Podle malé Fermatovy věty platí pro každé prvočíslo p a každé celé číslo a konguence

$$a^p \equiv a(\text{mod p})$$

Pokud je a nesoudělné s p, lze v předchozí kongruenci krátit a platí

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

Poslední kongruencí budeme testovat čísla p větší než 2 pro základ $a = 2$. Máme

3 je prvočíslo - 3 dělí $2^2 - 1$;
4 není prvočíslo - 4 nedělí $2^3 - 1$;
5 je prvočíslo - 5 dělí $2^4 - 1$;
6 není prvočíslo - 6 nedělí $2^5 - 1$;
7 je prvočíslo - 7 dělí $2^6 - 1$;
8 není prvočíslo - 8 nedělí $2^7 - 1$;
9 není prvočíslo - 9 nedělí $2^8 - 1$;
10 není prvočíslo - 10 nedělí $2^9 - 1$;
11 je prvočíslo - 11 dělí $2^{10} - 1$ atd.

Vypadá to idylicky, pokud je p prvočíslem, je výraz dělitelný p, pokud ne, není výraz dělitelný číslem p. Nemohli bychom na základě platnosti či neplatnosti jedné kongruence „třídit“ prvočísla a čísla složená?

Pokud je $p > 2$ prvočíslo, pak zřejmě p dělí $2^{p-1} - 1$. To vyplývá z malé Fermatovy věty. Platí i obrácená implikace? Zřejmě se tomu dlouho věřilo. Jenže se nakonec přišlo na to, že pro $n = 341$, kdy jde o číslo složené ($341 = 11 \cdot 31$), ale 341 dělí $2^{340} - 1$. Tak byla objevena složená čísla, která procházejí tzv. 2 – prvočíselným testem (tzv. pseudoprvočísla o základu 2). Je jich jen 7 menších než 2 000, konkrétně 341, 561, 645, 1 105, 1 387, 1 729, 1 905.

Věta 2.13: Fermatovská pseudoprvočísla při základu a

Fermatova pseudočísla opět vycházejí z malé Fermatovy věty, kterou máme nadefinovanou v úvodu této práce takto: $k^{p-1} \equiv 1 \pmod{p}$, $NSD(k, p) = 1$, p ještě nemusí představovat prvočíslo, Lucas[2] dokázal příkladem $x = 2701 = 73 \cdot 37$, kdy $2^9 \equiv 1 (\mathrm{mod}\, 73) \Rightarrow 2^{36} \equiv 1 (\mathrm{mod}\, 73) \wedge 2^{36} \equiv 1 (\mathrm{mod}\, 37)$. Pokud tyto tvrzení spojením získáváme $2^{36} \equiv 1 (\mathrm{mod}\, x)$, protože $x - 1 = 36 \cdot 75$, platí protipříklad. Pro číslo $341 = 11 \cdot 31$ platí $2^{340} \equiv 1 (\mathrm{mod}\, 341)$ a vlastnost čísla 341 je nejmenším protipříkladem.

[2] F. E. A. Lucas, Théorie des nombres, 1891, str. 422

Díky logickému dokončení malé Fermatovy věty vzniká „ fermatovský test složenosti“, který zní:

Pokud neplatí $k^{\alpha-1} \equiv 1(\mathrm{mod}\,\alpha)$, kde k je libovolné číslo a splňuje podmínku $(k,\alpha)=1$ $\Rightarrow \alpha$ je složené číslo. Tento test vyžaduje maximálně $2\log_2 \alpha$ násobení dvou čísel modul α a jeho následnou redukci.

Jestliže $k^d (\mathrm{mod}\,\alpha)$ závisí na binárním rozvoji d a počtu jedniček v něm, který se v průměru pohybuje okolo $1,5\lfloor \log_2 d \rfloor$, kdy $d=\alpha-1$ získáváme počet nutných redukcí a násobení $\mathrm{mod}(\alpha) = 1,5\lfloor \log_2 \alpha \rfloor$. Celý tento proces se nazývá algoritmus polynomiálního řádu.

Definice 2.14: Pseudoprvočísla při základu *a*

Pseudoprvočísla jsou celá čísla složená, která splňují podmínky některých testů umožňující rozklad na prvočísla. Vychází z MFV.

Pro α liché, složené číslo platí:

$$a^{\alpha-1} \equiv 1(\mathrm{mod}\,\alpha).$$

Příklad 2.15: Je číslo 4 se základem 5 pseudoprvočíslo?

Řešení:

Použijeme vzorec $a^{\alpha-1} \equiv 1(\mathrm{mod}\,\alpha)$ a dosadíme za $a=5, \alpha=4$.

$$5^{4-1} \overset{?}{\equiv} 1(\mathrm{mod}\,4)$$

$$5^3 = 125$$

$$125 \equiv 1(\mathrm{mod}\,4)$$

Ano, číslo 4 je pseudoprvočíslem.

Definice 2.16: Silná pseudoprvočísla

Nechť $m = 2^s \cdot d + 1$ je složené číslo a platí alespoň jedna z následujících podmínek, nazýváme toto číslo silným pseudočíslem.

$$k^d \equiv 1 (\mathrm{mod}\ p) \vee$$

$$k^{2^t d} \equiv -1 (\mathrm{mod}\ p), \text{ kde } 0 \leq t \leq s-1.$$

Věta 2.17: Fermatův test prvočíselnosti

Slouží k určování prvočísel, nebo čísel složených. Vychází z malé Fermatovy věty a funguje pravděpodobnostně.

$$k^{p-1} \equiv 1 \pmod{p}\ ,\ 0 < k < p$$

Pro všechna k , kde rovnost neplatí, p není prvočíslem. U některých složených čísel rovnost může platit (Fermatova pseudoprvočísla). Pokud rovnost platí, může být p prvočíslo a nemusí. To jsou tzv. Carmichaelova čísla o kterých si povíme v následující kapitole a jsou nedostatkem ve Fermatově testu prvočíselnosti.

Příklad 2.18: Otestujte číslo 17 a zvolte $k = 2$.

Řešení:

Pokud dosadíme do vzorce $k^{p-1} \equiv 1 \pmod{p}$

$$2^{17-1} \equiv 1 \pmod{17}$$

$$2^{16} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 = 16 \cdot 16 \cdot 16 \cdot 16 = (-1) \cdot (-1) \cdot (-1) \cdot (-1) = 1 \text{ v } Z_{17},$$

zjistili jsme, že číslo 17 je opravdu prvočíslo. Svědkem je zde použito číslo 2.

Příklad 2.19: Otestujte číslo 15 a zvolte a) $k = 2$ a za b) $k = 4$.

Řešení:

Použijeme v obou případech stejný postup jako je v příkladě 2.18.

a) $k^{p-1} \equiv 1 \pmod{p}$ b) $k^{p-1} \equiv 1 \pmod{p}$

$2^{15-1} \equiv 1 (\mathrm{mod} 15)$ $4^{15-1} \equiv 1 (\mathrm{mod} 15)$

$2^{14} \equiv 4 (\mathrm{mod} 15)$ $4^{14} \equiv 1 (\mathrm{mod} 15)$

V případě za a) si můžeme povšimnout, že kongruence není rovna 1, proto 15 není prvočíslo. Naopak v druhém případě vidíme, že číslo 15 je prvočíslem, proto číslo 4 označujeme za tzv. Fermatova lháře. V praxi se příliš neobjevuje a spíše se používá již zmíněný Millerův-Rabinův test, Solovay-Strassenův test.

Představíme si algoritmus s názvem **Solovayův-Strassenův test**, který se používá s Eulerovou větou. Ověřuje se pouze platnost rovnice $k^{(p-1)/2} \equiv \left(\frac{k}{p}\right) (\mathrm{mod}\, p)$. Jestliže k nesplňuje rovnici je prvočíslo p číslo složené. Pokud tato rovnice platí i pro složené číslo nazveme ho Eulerovo pseudoprvočíslo.

Věta 2.20: Millerův-Rabinův test prvočíselnosti

Jeden z algoritmů, který se zabývá otázkou, zda je dané číslo prvočíslo. Jde o test, který má pravděpodobnostní verzi. Slouží k testování složených čísel a vychází z malé Fermatovy věty. Stejně jako Fermatův a Solovayův-Strassenův test je založen na existenci rovností, které obecně neplatí, ale prvočísla je splňují.

Jestliže zapíšeme $p-1=2^s d$, d je liché $\wedge$ $k < p$:

$k^d \equiv 1 (\mathrm{mod}\, p) \vee k^{2^t d} \equiv -1 (\mathrm{mod}\, p)$, kde $0 \le t \le s-1$.

Příklad 2.21: Otestujte číslo 49.

Řešení:

V algoritmu si vybereme libovolné $k < p$. Následně podmínky z uvedené definice. Jestliže podmínky neplatí p je číslo složené, pokud je tomu naopak, testujeme další k.

$$p-1=48 \Rightarrow 48=2^4 \cdot 3$$

$$k=3, s=4, d=3$$

Teď již dosadíme do vzorů a budeme pozorovat výsledek.

$$3^3 = 27 \rightarrow 27(\text{mod}\,49) = 27 \rightarrow 27 \neq \pm 1(\text{mod}\,49)$$

$$3^{2\cdot 3} = 729 \rightarrow 729(\text{mod}\,49) = 43 \rightarrow 43 \neq -1(\text{mod}\,49)$$

$$3^{4\cdot 3}(\text{mod}\,49) = 36 \rightarrow 36 \neq -1(\text{mod}\,49)$$

$$3^{8\cdot 3}(\text{mod}\,49) = 22 \rightarrow 22 \neq -1(\text{mod}\,49)$$

Z těchto výpočtů je jasné, že 49 je složené číslo.

Za zmínku stojí i jeden test pro určování prvočísel, který souvisí s Fermatovým testem. Nazývá se **Pépinův test**. Tento test byl objeven v roce 1877 a bylo zjištěno, že platí pro základ pět, později i pro základ číslo tři. $3^{((Fn-1)/2)} \equiv -1 \pmod{F_n}$, $n \in \mathbb{N}$.

Za zmínění stojí i **Wilsonův test**. Používá faktoriály a používá se hlavně v důkazech. Platí tvrzení, že $\forall p \in \mathbb{N} : p \geq 2$ je prvočíslo $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$. Jestliže můžeme p rozložit na $p = 4x+1$, pak platí $(((p-1)/2)!)2 \equiv -1$. Pokud je tato podmínka platná, nevíme však, zda je p prvočíslo. Vznikají tzv. pseudotesty, což jsou testy, které neřeknou, zda číslo je prvočíslo nebo složené.

Poslední zmíněný test se nazývá **Lucasův-Lehmerův test.** Tento test využívají Mersennova čísla, což jsou prvočísla ve tvaru $M_p = 2^p - 1$. Zapisuje se jako rovnice a příkladem může být otázka, zda je číslo 15 prvočíslo. Odpověď je zjevně jasná. Patnáct je číslo složené, protože $15 = 2^4 - 1$, tato rovnice je nepravdivá.

KAPITOLA TŘETÍ – CARMICHAELOVA ČÍSLA.
V. ŠIMERKA - OBJEV PRVNÍCH SEDMI CARMICHAELOVÝCH ČÍSEL

Definice 3.1: Carmichaelova čísla

Číslo, které splňuje zadanou podmínku: $a^{n-1} \equiv 1 \bmod(n), n \in \mathbb{N}$. Podmínka platí pro všechna a nesoudělná s n.

Tato definice je již obsažena v malé Fermatově větě. Pro zjištěním zda se jedná i Charmichaelova čísla nelze požít Fermatův test prvočíselnosti. S tímto pojmem souvisí V. Šimerka a jeho objev prvních sedmi Carmichaelových čísel.

Václav Šimerka

Obrázek 6: Václav Šimerka

Narodil se 20. prosince 1819 ve Vysokém Veselí a zemřel 26. prosince 1887 v obci Praskačka.

Pocházel ze sedmi dětí. V útlém věku navštěvoval farní základní školu ve Vysokém Veselí, následně studoval gymnázium v Jičíně. Na přelomu let 1839/40 a 1840/41 navštěvoval filozofickou fakultu pražské univerzity, kde absolvoval výuku náboženství, filosofie, matematiky, přírodovědy, fyziky, latinské filologie, morální filosofie a dějin, přednášky z vyšší matematiky, astronomie a geometrie. Následně pokračoval studiem teologického semináře v Hradci Králové a 25.7.1845 byl vysvěcen na kněze. O pět let později, kdy byly zavedeny státní zkoušky se přihlásil a získal aprobaci na matematiku pro gymnázium v českém i německém jazyce, z fyziky neuspěl. V toce 1851 působil rok jako kaplan ve Slatinách a poté odešel do Prahy dostudovat fyziku. Na druhý pokus 27.6.1853 u státní zkoušky prošel.

Na podzim roku 1853 byl jmenován suplujícím učitelem na gymnáziu v Českých Budějovicích. První rok učil fyziku a český jazyk později i matematiku. V tomto období

vyšla jeho první vědecká pojednání. V roce 1862 se vrátil zpět a stal se farářem ve Slatině u Žamberka, poté odešel po čtyřech letech na dvacet let života do Jenišovic.

K učitelství se již nevrátil, ale o matematiku se zajímal stále. Byl zakladatelem Jednoty českých matematiků a roku 1870 jmenován jejím čestným členem. Přispíval časopisu Krok. Svůj poslední život prožil v obci Praskačka.

Věta 3.2. Objev prvních sedmi Carmichaelových čísel

Václav Šimerka s použitím Fermatovy věty nalezl prvních sedm Carmichaelových čísel ve své práci nazvané Zbytky z aritmetické posloupnosti.

Ukažme si jeho myšlenku:

Poučka tato dle vynálezce řečená Fermatovou jest jednou z nejdůležitějších v neurčité analytice; neudává však charakteristickou známku kmenných čísel, (jíž by se tato ode všech ostatních lišila), ježto podobně i při některých dělitelných číslech bývá. Tak na př. při $561 = 3 . 11 . 17$, $b = 2$ nalezneme

$$2_{10} = -98,\ 2_{20} = 67,\ 2_{40} = 1,\ (2_{40})^{14} = 2_{560} = 1.$$

Tolikéž u čísel

$1105 = 5 . 13 . 17$, $1729 = 7 . 13 . 19$, $2465 = 5 . 17 . 29$,
$2821 = 7 . 13 . 31$, $6601 = 7 . 23 . 41$, $8911 = 7 . 19 . 67$ a j. v.,

kdykoli b s modulem nesoudělné jest.

Obrázek 7: Zbytky z aritmetické posloupnosti

Závěrem si ujasněme, že prvních sedm Carmichaelových čísel představují 2 - pseudoprvočísla $561, 1105, 1729, 2465, 2821, 6601, 8911$.

ZÁVĚR

Cílem této práce bylo přednést základní informace o testování prvočíselnosti. Toto téma zahrnuje v mé práci malou Fermatovu větu. Tato věta je jednou ze základních vět teorie čísel. Příklady, které jsem zvolila, doplňují definice a veškerý výklad pro přesnější představu.

Ve své práci jsem neobsáhla veškeré otázky z oboru teorie čísel, ale snažila jsem se zaměřit pouze na ty, které přímo souvisí s malou Fermatovou větou. Účelně jsem se věnovala problematice důkazů, testů prvočíselnosti a možnosti zjištění prvočísel s volně dostupnými počítačovými aplikacemi.

RESUMÉ

Cílem této práce je seznámit čtenáře s problematikou testování prvočíselnosti. Jednou z nejznámějších vět teorie čísel je velká Fermatova věta a malá Fermatova věta. Tato práce se zabývá právě malou Fermatovou větou a důkazy v první kapitole. Druhá část je o testování prvočíselnosti a pseudoprvočísel o základu *a*. Poslední část řeší Carmichaelova čísla a Václava Šimerku - objev prvních sedmi Carmichaelových čísel. Celá práce je doplněna příklady s postupy a vysvětlením tak, aby čtenář pochopil snadněji danou problematiku.

Summary

The aim of this work is to acquaint the reader with the issue of first-order testing. One of the most well-known sentences of numbers theory is the big Fermat theorem and the little Fermat theorem. This paper deals with the little Fermat sentence and the evidence in the first chapter. The second part is about the testing of prime numbers and pseudo-numbers on the basis of *a*. The last part deals with Carmichael's numbers and Václav Šimerka - the discovery of the first seven Carmichael numbers. The whole work is supplemented with examples of procedures and explanations so that the reader can understand the issue more easily.

SEZNAM POUŽITÉ LITERATURY

Bečvář, J.; Fuchs, E.: Historie matematiky. I., Co ještě nevíme o prvočíslech, Brno:Jednota českých matematiků a fyziků, 1993. pp. 140-161, Dostupné z: http://dml.cz/dmlcz/400592

Childs, L.N.: „ A Concrete Introduction to Higher Algebra “, 2. ed., Springer, 1996.

Crandall, R., Pomerance, C.: „ Prime Numbers. A Computational Perspective “, Second Edition, Springer, 2005.

Hykšová, M.: „ Filosofická pojetí pravděpodobnosti v pracích českých myslitelů “, Praha, Matfyzpress, vydavatelství Matematicko-fyzikální fakulty Univerzity Karlovy v Praze, 2011. p. 142–146.

Růžička, J.: „ Teorie čísel, diplomová práce “, Masarykova univerzita, Brno 2006, Dostupná z: https://is.muni.cz/th/42653/fi_m/DIPLOMKA.pdf.

Singh,S.: „ Velká Fermatova věta “, 1. vydání., Praha 2000.

Šimerka, V.:“ Zbytky z aritmetické posloupnosti “, Časopis pro pěstování matematiky a fysiky, r. 1885, 14(5) p. 221–225.

SEZNAM OBRÁZKŮ

ZDROJE OBRÁZKŮ

Obrázky, které nemají uvedený zdroj jsou vytvořené v programu Microsoft Malování nebo Microsoft Word.

Obrázek1: Mahoney, Michael S., The Mathematical Career of Pierre de Fermat (1601–1665), 1973, z: http://www.nndb.com/people/768/000087507/

Obrázek2: Leonhard Euler. [online] [citováno 10. 6 2017] z : http://www.mensa.cz/volny-cas/hlavolamy/sifry/sifra-33/

Obrázek3: Matematický program Wolframalpha [online][citováno 10.6.2017] z : http://www.wolframalpha.com/input/?i=is+1001+prime

Obrázek5: Revisitons le crible d'Ératosthène (1ère partie) [online] [citováno 10.6.2017] z: https://blogdemaths.wordpress.com/2012/07/03/revisitons-le-crible-deratosthene/

Obrázek6: Hykšová, M:„Filosofická pojetí pravděpodobnosti v pracích českých myslitelů", Praha, Matfyzpress, vydavatelství Matematicko-fyzikální fakulty Univerzity Karlovy v Praze, 2011. p. 142–146.

Obrázek7: Šimerka, V.:" Zbytky z aritmetické posloupnosti ", Časopis pro pěstování matematiky a fysiky, r. 1885, 14(5) p. 221–225.