ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ

ÚLOHY Z OBLASTI TEORIE ČÍSEL VE ŠKOLNÍCH SOUVISLOSTECH

Bakalářská práce

Plzeň 2020

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

Autor práce: Tereza Soukupová

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

V Plzni dne 2. 7. 2020

.....

vlastnoruční podpis

Poděkování :

Děkuji vedoucímu mé bakalářské práce doc. RNDr. Jaroslavu Horovi, CSc. za ochotnou spolupráci a také za všechny rady a připomínky, které mi během psaní práce poskytl.

Anotace

Tato bakalářská práce pojednává o úlohách z oblasti teorie čísel ve školních souvislostech. Cílem této práce je přiblížit čtenáři pojem prvočísla, kongruence, kritéria dělitelnosti a mimo jiné i šifrování. Nejprve popíši prvočísla a také prvočíselný rozklad. Tento rozklad se dále využívá v kapitolách jako je největší společný dělitel a nejmenší společný násobek. V dalších kapitolách se zabývám kongruencí a kritérii dělitelnosti. Na konci práce se zmiňuji o speciálních prvočíslech jako jsou Mersennova a Fermatova prvočísla, také okrajově nastíním testy prvočísel a šifrování.

Annotation

This Bachelor thesis deals with subjects from areas number theory in context with school. The main goal of this thesis is to introduce terms like prime numbers , congruence, criteria of divisibility, and also encryption. First I will describe the prime numbers and prime factorization of numbers. This decomposition is used in a few other chapters for example in greatest common divisor and the least common multiple . In the next chapters, I address the congruence and the criteria of divisibility. At the end of I mention special prime numbers like Mersenn's or Fermat's prime numbers. I also briefly mention tests of prime numbers and encryption.

Klíčová slova

Prvočísla, kongruence, Kritéria dělitelnosti, Mersennova a Fermatova prvočísla, testy prvočíselnosti, šifrování

Keywords

Prime numbers , congruence, criteria of divisibility, Mersenn's and Fermat's prime numbers, tests of prime numbers, encryption

Obsah

1.Úvod

Pro svou bakalářskou práci jsem si vybrala téma Úlohy z oblasti teorie čísel ve školních souvislostech. Pro výběr toho tématu jsem se rozhodla především proto, že mě velice zajímá téma teorie čísel a především prvočísel. Tato bakalářská práce má za úkol seznámit čtenáře s pojmem teorie čísel, prvočísla a kongruence. Jen na úvod bych chtěla zmínit, že zvolené příklady nejsou vybrány z žádné literární předlohy, nýbrž jsou navržené a vypočítané jen mnou. Celý text této bakalářské práce je rozdělen do deseti kapitol.

Druhá kapitola s názvem historie matematiky se zabývá historií v odlišných dobách a také na odlišných území. Je zde jasně uveden rozvoj matematiky v jednotlivých obdobích. Dále je také zmíněn Pythagoras z ostrova Sámos, který byl velmi důležitým matematikem v celé historii oboru.

Třetí kapitola je věnovaná prvočíslům, je zde vysvětleno, jak se prvočísla poznají a také základní operace s nimi.

Ve čtvrté kapitole se zmiňuji o největším společném násobku a nejmenším společném děliteli. Je zde vysvětleno, jak s těmito tématy pracovat a také zde uvádím řešení vybraných příkladů.

Pátá kapitola se věnuje kongruenc9m, kde nejdříve pro upřesnění zmiňuji pojem ekvivalence. Dále jsou zde vybrané příklady a také jejich řešení na toto téma.

Šestá kapitola má název kritéria dělitelnosti. Jsou zde vysvětlena kritéria a také důkazy dělitelnosti pro čísla dva, tři, čtyři, pět, šest, sedm, osm a devět.

Sedmá kapitola s názvem Mersennova a Fermantova prvočísla se věnuje těmto speciálním případům prvočísel. Je zde uvedený vzorec a také příklady těchto prvočísel.

Osmá kapitola se věnuje testům prvočíselnosti. Uvádím zde Elementární test a jeho princip. Jsou zde zmíněny také vybrané příklady pro tento test. Dále zde uvádím Eratosthenovo síto, které je názorně vysvětleno na určitém příkladu. Jsou zde uvedeny také další testy, jako je:

Fermatův test prvočíselnosti, Lehmannův test prvočíselnosti a Rabin-Milleruv test prvočísel.

V deváté kapitole se věnuji šifrováním pomocí velkých prvočísel. Jsou zde popsány tři základní šifrování a to RSA šifra, šifrování ElGamal a Diffieho – Helmanovo šifrování. V této kapitole poukazuji na to, proč je šifrování pomocí prvočísel tak důležité a jaké má šifrování využití.

V poslední desáté kapitole zmiňuji velkou prvočíselnou větu, dále její vzorec a také Riemannovu domněnku.

2. Historie matematiky

Historie matematiky sahá až do paleolitu, kde se poprvé objevují takzvané vrubovky. Tento název dostaly díky zářezům neboli vrubům. Jednalo se o hůlku, která sloužila k počítání. Již na vrubovce se zaznamenávaly primitivní počty. Ať už to bylo obyčejné počítání, a nebo záznamy dluhů. Tato lišta (většinou šlo o kost) se rozřízla napůl, z čehož jednu půlku obdržel dlužník, kdežto druhá byla přidělena věřiteli. Nález vrubovky byl také objeven i u nás v České republice a to konkrétně na Moravě v okolí Dolních Věstonic. Jednalo se o vrubovku, která byla vytvořena z lýtkové kosti vlka. Na kosti bylo nalezeno celkem 55 zářezů. Tento objev se datuje do doby 30 tisíc let před naším letopočtem.

Nyní se budeme zabývat jejími charakteristickými znaky. V případě, že se na vrubovce nacházel pouze jeden znak, což byla většinou čárka nebo zářez, jednalo se o číslo jedna. Znak se mohl opakovat, tudíž například tři zářezy představovaly číslo 3. Zajímavostí je, že pokud bylo více jak 5 zářezů, tak byly pro přehlednost znaky oddělovány mezerami.

V neolitu zřejmě lidé využívali i elementárních poznatků z geometrie, jelikož v této době již docházelo k vyměřování pozemků a staveb. Rozvíjel se zde obchod, zemědělství a mimo jiné i řemesla.

2.1. Čína

Jedním z prvních národů, který se pokusil o zapsání čísel, byli Číňané přibližně v 8. století před naším letopočtem. Číňané si nakreslili obrázek, který obsahoval 8 x 8 políček. Každé ze zmíněných políček bylo rozděleno na 6 přerušovaných či plných čar. Přerušovaná čára znamenala jin a plná jang, které jsou v protikladu. Jin znamená měsíc a představuje negativní stranu, kdežto jang je spojován se

Sluncem, světlem a aktivitou. Německý matematik Gottfried Wilhem Leibniz tvrdil, že Číňané díky tomuto hexagramu objevili zápis dvojkové soustavy. (Pokud si představíme, že přerušované čáry značí 0 a plné čáry zase symbol 1).
I přesto, že staří Číňané neprováděli se symboly aritmetické operace jin a jang, byl tento hexagram vzestupným bodem zapisování čísel.

2.2. Egypt

Nejstarší záznamy z Egypta, které se týkají počtu prvků, pochází z roku 3 300 před naším letopočtem. Jednalo se o vyčíslení vojenské síly.

Dále byly objeveny dva papyry, a to Moskevský a Rhindův. V moskevském papyru, který pochází z doby 1 890 před naším letopočtem, bylo nalezeno celkem 25 úloh. Tento papyrus byl v roce 1912 darován do moskevského muzea umění. Rhindův papyrus obsahoval dokonce 84 úloh, později v něm však byly nalezeny chyby. Tento papyrus se však nezachoval v originále, ale byl z něho zhotoven opis, který je nyní uložen v Britském muzeu v Londýně. Tyto papyry byly po dlouhou dobu hlavními prameny pro studium matematiky ve starém Egyptě.

Dále se našly také matematické tabulky, které byly zapsány na kůži. Ve starověkém Egyptě se již pracovalo s čísly, které byly větší než 10. Podobně jako v pravěku pro malá čísla používali čárky, kdežto pro cifru deset měli již speciální znaky. Tyto symboly dále pokračovaly s čísly 100 až 1 000 000. Zajímavostí je, že například pro číslo 1 000 byl symbolem lotosový květ a například pro číslo 1 000 000 to byl žasnoucí muž. Pro číslo 10 byl použit symbol zahnuté kosti, a tak pokud chtěli zapsat číslo 7, použili zahnutou kost a k tomu dvě čárky.

V oblasti geometrie se zde začaly využívat provazy s uzly.

2.3. Mezopotámie

V Mezopotámii zapisovali čísla jiným způsobem, než v Číně. Zde se nepoužívaly jednoduché čárky, nýbrž otiskli trojhrannou dřevěnou tyčinku na hliněnou tabulku. Jeden otisk trojúhelníku označoval číslo jedna. Opakováním těchto znaků vznikla číselná tabulka. Tento objev pochází z doby 3 000 před našim letopočtem.

2.4. Řecko

Pythagoras, který pocházel z ostrova Sámos, který se narodil okolo roku 570 před našim letopočtem. Prosazoval studium kvadrivia, což bylo studium zabývající se čtyřmi základními vědami. Jednalo se o geometrii, aritmetiku, astronomii a hudbu. Vyslovil větu, která je základem matematiky: „Věci jsou čísla, číslo 1 je základní stavební kámen aritmetiky, není to obyčejné číslo, ale pochází přímo od Boha, jako základ všech dalších čísel“. Dále vyslovil například Pythagorovu větu. Její podstata byla známá již v Mezopotámii nebo v Egyptě, ale on ji jako první opravdu dokázal. Matematika se od té doby stala vědou, která vyžaduje zdůvodňování a důkazy. Poprvé se zde také objevují kvantifikátory a věty typu „pro všechny … platí … “. Pythagoras dále založil školu, jejíž členové se v historii matematiky označují jako pythagorejci a mezi nejznámější objevy této školy patří prvočísla a také dva pravidelné mnohostěny.

Mezi další představitele řecké matematiky patří Erastosthenes z Kyrény, což byla starověká řecká osada na severním pobřeží Afriky. Erastothenes žil kolem roku 230 před naším letopočtem. Jednalo se o matematika, astronoma a také geografa. Byl prvním, kdo popsal metodu nalézání prvočísel. Tuto metodu známe pod názvem Erasthenovo síto. Nyní si vysvětlíme, jak toto síto fungovalo. Jako první krok si vypíšeme tabulku všech čísel od 1 do 100. Číslo 1 není prvočíslo ani číslo složené, z toho důvodu si jej nebudeme všímat. Dále následuje číslo 2, toto číslo si

podtrhneme a nejdříve budeme vyškrtávat všechny násobky dvou, tedy čísla : 4, 6, 8, 10, … .Pokud jsou násobky vyškrtané až dokonce, tedy do čísla 100, vrátíme se opět na začátek a pokračujeme u nejmenšího čísla, které není podtržené ani přeškrtnuté. Objevíme číslo 3, proces je opět stejný jako u čísla 2, tedy vyškrtáváme všechny násobky 3, tedy čísla: 6 (které už je ovšem škrtnuté), 9, 12, 15, . Stejnou operaci provedeme také u čísel 5 a 7. Všechna čísla, která jsou podtržená a nejsou přeškrtnutá jsou prvočísla. Tato metoda vyžaduje pracný postup a proto se nepoužívá pro vyhledávání velkých prvočísel.

Ukázka Eratosthenova síta:
1, 2, 3, 4, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23 , ~~24~~ ,~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~, 31, ~~32~~, ~~33~~, ~~34~~, ~~35~~, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~, 41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, ~~49~~, ~~50~~

Z ukázky lze jednoduše prvočísla vypsat: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

Jako posledního z představitelů řecké matematiky zde uvedeme Thaléta z Milétu. Díky jeho důkazu již žáci na základní škole vědí o Thaletově větě, která zní: „Všechny obvodové úhly sestrojené nad průměrem kružnice jsou pravé.“ V původním znění: „Středový úhel je dvojnásobek obvodového“. Kdybychom tuto větu vysvětlovali žákům na základní škole, uvedli bychom obsáhlejší vysvětlení. Sestrojíme kružnici s libovolným průměrem. Nyní si narýsujeme úsečku průměru a její body označíme A a B. Dále si zvolíme libovolný bod na kružnici a označíme ho písmenem C. Sestrojíme trojúhelník ABC, kde bude platit, že tento trojúhelník je pravoúhlý s pravým úhlem u vrcholu C.

Jako zdroje pro historii matematiky jsem užila textů z: [1], [2], [3], [4]

3. Prvočísla

Abychom pochopili podstatu prvočísel, nejdříve si vysvětlíme základní principy rozkladu. Ukážeme si rozklad na čísle 12. Vyjádříme ho třemi následujícími způsoby jako součin dalších čísel:

$$12 = 2 \cdot 6$$

$$12 = 3 \cdot 4$$

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

Číslům na pravé straně se říká dělitelé, v našem případě číslo 3 je tedy dělitelem čísla 12. Dělitel je takové číslo, které je „obsaženo ve velkém čísle beze zbytku“. Jako další příklad uvedeme číslo 15, podobně jako v předchozím případě vidíme, že 5 je dělitelem 15, jelikož číslo 5 je obsaženo v 15.Pokud používáme termín je obsaženo, vysvětlíme to tak, že když 15 dělíme 5, získáme přirozené číslo, v tomto případě 3. Dále si všimneme, že zbytek po dělení je nulový. Zde se vracíme ke starořecké geometrické představě. Kdybychom reprezentovali číslo 15 jako úsečku o délce 15 dílků (15 cm v moderní době) a číslo 5 jako úsečku o délce 5 dílků, bylo by patrné, že popsanou úsečku musíme nanést přesně třikrát.

Nyní se podíváme na to, kolik dělitelů mohou mít konkrétní čísla. Vezmeme si již zmiňované číslo 12. Zjistíme, že mezi dělitele 12 patří čísla 2, 3, 4 a 6, pokud těmito čísly dělíme, dostaneme celé číslo. Tyto čísla budeme nazývat množinou dělitelů. Do této množiny patří samozřejmě i číslo samotné a číslo 1, jelikož každé číslo je dělitelné jedničkou. Najdeme tak mnoho čísel, například číslo 24, jehož dělitelé pak budou: 1, 2, 3, 4, 6, 8, 12, 24.

V případě, že budeme chtít nalézt dělitele čísla 5, nalezneme pouze číslo 1 a 5. Tento jev platí i pro čísla: 2, 3, 7, 11 a 13. Pokud si zvolíme libovolné přirozené číslo $n > 1$, poté vždy nalezneme minimálně dvě čísla, která budou dělit číslo n, tato dvě čísla jsou také přirozená a nazývají se samozřejmí dělitelé. V případě, že číslo $p > 1$ nemá žádné

jiné dělitele, kromě samozřejmých dělitelů se nazývá prvočíslo. Naopak, pokud číslo s > 1 není prvočíslo, nazývá se složené číslo. [5]

V publikaci [5], příklad 16, máme rozhodnout, zda číslo 2 437 je prvočíslem, či číslem složeným, totéž máme zodpovědět pro číslo 2 771.
1) Pokud číslo 2437 má být prvočíslem, nesmí být dělitelné žádným prvočíslem menším než naše zvolené číslo. Dále si odmocníme číslo 2 437. √ 2 437 = 49.37. tudíž budeme zkoumat dělitelnost těmito prvočísly: 2, 3, 5, 7, 11 ,13, 17, 19, 23, 29, 31, 37, 41, 43, 47. 2 437 / 2 =1 218.5, 2 437 / 3 = 812.3, 2 437 / 5 = 487.4, 2 437 / 7 = 348.1, 2 437 / 11 = 221.6, 2 437 / 13 = 187.5, 2 437 / 17 =143.4, 2 437 / 19 = 128.3, 2 437 / 23 = 105.96, 2 437 / 29 = 84.03, 2 437 / 31 = 78.6, 2 437 / 37 = 65.86, 2 437 / 41 = 59.44, 2 437 / 43 = 56.67, 2 437 / 47 = 51. 85.
Všechny tyto případy nám ukazují, že číslo 2 437 není dělitelné žádným vybraným prvočíslem. Odpověď tedy zní: Číslo 2 437 je prvočíslo.

2) Nyní zkoumáme číslo 2 771. Postup je stejný jako u předcházejícího příkladu. √2 771 = 52.64, tedy budeme počítat dělitelnost prvočísly 2, 3, 5, 7, 11 ,13, 17, 19, 23, 29, 31, 37, 41, 43, 47. 2 771 / 2 = 1385.5, 2 771 / 3 = 923.67, 2 771 / 5 = 554.2, 2 771 / 7 = 395. 86, 2 771 / 11 = 251.91, 2 771 / 13 = 213.15, **2 771 / 17 =163**, 2 771 / 19 = 145.84, 2 771 / 23 = 120.48, 2 771 / 29 = 95.55, 2 771 / 31 = 89.39, 2 771 / 37 = 74.89, 2 771 / 41 = 67.59, 2 771 / 43 = 64.44, 2 771 / 47 = 58.96.
Tučně zvýrazněný výpočet dokazuje, že číslo 2 771 je dělitelné číslem 17 beze zbytku, tudíž v tomto případě číslo 2 771 není prvočíslem**.**

3.1. Nekonečný počet prvočísel

Počet prvočísel v každém bloku 100 přirozených čísel klesá. Prvočísla však postupně nevymizí úplně, protože prvočísel je nekonečně mnoho. [6]

Dokážeme, že prvočísel je konečný počet, tudíž důkaz provedeme sporem. [7]

Mějme $a_1, a_2, a_3, \ldots, a_n$, což je posloupnost všech existujících prvočísel. Pokud máme v této posloupnosti obsažena všechna prvočísla, tak už nemůže existovat žádné, které by v této posloupnosti nebylo obsaženo. Nyní uvažujeme číslo $q = a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n + 1$. Je patrné, že toto číslo není dělitelné žádným z prvočísel $a_1, a_2, a_3, \ldots, a_n$. Je tedy dalším prvočíslem. To je ale ve sporu s tím, že prvočísel je konečný počet, jak jsme předpokládali: mělo jich být nejvýše n, tudíž prvočísel je nekonečně mnoho.

3.2. Prvočíselný rozklad

Číslo 1 má jednoho dělitele a nazývá se jednotkou ve smyslu dělitelnosti. Nejde ani o prvočíslo ani o číslo složené. Každé prvočíslo má právě dva dělitele a to číslo 1 a samo sebe. Každé složené číslo má více než dva různé dělitele.

Přirozená čísla můžeme napsat ve tvaru součinu:

$$1 = 1 \cdot 1$$

$$5 = 5 \cdot 1 \text{ nebo } 5 = 5 \cdot 1$$

$$70 = 5 \cdot 14 \text{ nebo } 70 = 10 \cdot 7$$

$$108 = 12 \cdot 9 \text{ nebo } 108 = 2 \cdot 54$$

Jestliže rozkládáme číslo 5 zjistíme, že činitelé jsou pouze 2 a to jednička a pětka. Avšak u zbývajících čísel jsou u rozkladu obsažena i složená čísla. První číslo 70 nalezneme činitele 14 a 5. Číslo 5 je již prvočíslo, ale číslo 14 není. Tudíž musíme opět udělat rozklad $14 = 2 \cdot 7$. Nyní máme oba činitele, kteří jsou prvočíslo. Při konečném rozkladu

budeme činitele zapisovat od nejmenšího až po největší, tudíž 70 = 2 · 5 · 7. Takto vypadá zápis součinu pomocí prvočísel.

Nyní se podíváme na druhé číslo 108. Rozdíl je patrný na první pohled, a to, že oba činitelé jsou čísla složená. Nyní budeme postupovat po částech, nejdříve rozložíme číslo 12. 12 = 2 · 6. všimneme si, že opět máme dva činitele z toho jeden je opět složené číslo, tudíž pokračujeme s číslem 6. 6= = 2 · 3, teď již máme jen prvočísla, takže můžeme pokračovat s druhým činitelem čísla 108, a to s číslem 9. 9 = = 3 · 3, číslo 3 je již prvočíslo, takže 9 už je rozloženo a nemusíme pokračovat. Nyní spojíme všechny součiny prvočísel z čísla 12 a 9. Konečný zápis součinu zapíšeme takto: 108 = 2 · 2 · 3 · 3 · 3.

Tímto způsobem jsme schopni rozložit malá čísla na rozklad prvočinitelů, jelikož je tento způsob jednoduchý a rychlý. Pro větší čísla se již používá jiný rozklad, který je založen na tom, že všechna prvočísla jsou zapsaná ve sloupečku pod sebou, a taktéž je založen na stejném principu jako první rozklad. Prvočísla jsou seřazena od nejmenšího po největší a opět je nazýváme činitelé. [8]

Nyní si tento způsob ukažme na číslu 520.

520	2
260	2
130	2
65	5
13	13
1	

Tento příklad si upřesníme, abychom lépe porozuměli druhému rozkladu na prvočinitele. Na levé straně můžeme nalézt výsledky a na pravé straně od svislé čáry vidíme čísla, kterými dělíme čísla na pravé straně. Jediné co je důležité je to, že se vždy snažíme dělit tím nejmenším prvočíslem. Začneme tedy s číslem 520 a hledáme nejmenší prvočíslo, kterým můžeme dělit. Najdeme číslo 2. Tudíž napíšeme číslo

2 vpravo od svislé čáry ve stejné úrovni jako číslo 520. Nyní zapíšeme výsledek pod číslo 520 tedy 260 a můžeme pokračovat dále. Opět hledáme nejmenší prvočíslo, kterým lze dělit. Takto postupujeme až do té doby, dokud nedostaneme na levé straně číslo 1. Pokud na pravé straně nemáme již čím dělit je příklad vyřešený. Některé publikace ještě doporučují napsat výsledek prvním způsobem rozkladu. V našem případě je tedy výsledek : $520 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 13 =$
$= 2^3 \cdot 5 \cdot 13$

Vybrané příklady na rozklad na prvočinitele. Rozložíme si tato čísla: a) 704, b) 872, c) 944 d) 999, e) 3 675

Řešení:

a) 704

704 | 2
352 | 2
176 | 2
88 | 2
44 | 2
22 | 2
11 | 11
1 |

$704 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 11 = 2^6 \cdot 11$

b) 872

872 | 2
436 | 2
218 | 2
109 | 109
1 |

$872 = 2 \cdot 2 \cdot 2 \cdot 109 = 2^3 \cdot 109$

c) 944

944 | 2
472 | 2
236 | 2
118 | 2
 59 | 59
  1 |

$944 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 59 = 2^4 \cdot 59$

d) 999

999 | 3
333 | 3
111 | 3
 37 | 37
  1 |

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

e) 3 675

3 675 | 3
1 225 | 5
 245 | 5
  49 | 7
   7 | 7
   1 |

$3\,675 = 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 = 3 \cdot 5^2 \cdot 7^2$

Publikace [5] uvádí příklad 17: rozložte na prvočinitele a) 3 248, b) 2 418, c) 3 819.

a) 3 248

3 248 | 2
1624 | 2
812 | 2
406 | 2
203 | 7
29 | 29
1 |

$3\,248 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 7 \cdot 29 = 2^4 \cdot 7 \cdot 29$

b) 2 418

2 418 | 2
1 209 | 3
403 | 13
31 | 31
1 |

$2\,418 = 2 \cdot 3 \cdot 13 \cdot 31$

c) 3 819

3 819 | 3
1 273 | 19
67 | 67
1 |

$3\,819 = 3 \cdot 19 \cdot 67$

4. Největší společný dělitel a nejmenší společný násobek

4.1 Největší společný dělitel

Největšího společného dělitele si nejdříve ukážeme na příkladu a až poté vyslovíme definici. Jako ukázkový příklad jsou zde dvě čísla a to číslo 60 a 90. U každého z nich provedeme rozklad na prvočinitele. Tudíž rozklad čísla 60 = 2 · 2 · 3 · 5. Tuto operaci provedeme také u čísla 90. Dostaneme rozklad 90 = 2 ·3 · 3 · 5. Nyní hledáme prvočísla, která jsou v obou rozkladech, v našem případě jsou to čísla 2, 3 a 5. Největší společný dělitel je součin těchto čísel: 2 · 3 · 5 = 30. Výsledek zapisujeme D(60,90) = 30.

Dalším řešením není rozklad na prvočinitele, nýbrž hledáme všechny čísla, kterými je naše zvolené číslo dělitelné. Číslo 60 je dělitelné čísly 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 a 60. Číslo 90 je dělitelné čísly 1, 2, 3, 5, 6, 9, 15, 30 a 90. Nyní vybereme společné dělitele obou čísel. To znamená, že dostaneme čísla 1, 2, 3 a 30. Číslo 30 je ze seznamu společných dělitelů největší, tudíž se nazývá největším společným dělitelem. D(60,90) = 30.

4.2. Příklady Největšího společného dělitele

Nyní si uvedeme pár příkladů na toto téma.

a) D(25, 85) b) D(60, 75) c) D(96, 128) d) D(150, 225)

Řešení:

a) D(25, 85)

25 | 5 85 | 5

5 | 5 17 | 17

1 | 1|

25= 5 · 5 85 = 5 · 17

D(25, 85) = 5

b) D(60, 75)

60 | 2 — 75 | 3

30 | 2 — 25 | 5

15 | 5 — 5 | 5

3 | 3 — 1 |

1 |

60 = 2 · 2 · 3 · 5 75= 3 · 5 · 5

D(60,75) = 3 · 5 = 15

c) D(96, 128)

96 | 2 — 128 | 2

48 | 2 — 64 | 2

24 | 2 — 32 | 2

12 | 2 — 16 | 2

6 | 2 — 8 | 2

3 | 3 — 4 | 2

1 | — 2 | 2

1

96 = 2 · 2 · 2 · 2 · 2 · 3 128 =2 · 2 · 2 · 2 ·2 · 2 · 2

D(96,128) = 2 · 2 · 2 · 2 · 2 = 32

d)D(150, 225)

150 | 2 — 225 | 3

75 | 3 — 75 | 3

25 | 5 — 25 | 5

5 | 5 — 5 | 5

1 | — 1 |

150 = 2 · 3 · 5 · 5 — 225 = 3 · 3 · 5 · 5

D(150, 225) = 3 · 5 · 5 = 75

Teď již můžeme vyslovit definici největšího společného dělitele. „Společným dělitelem přirozených čísel $a_1, a_2, a_3, ..., a_k$ nazýváme to přirozené číslo d, kterým je každé z čísel $a_1, a_2, ..., a_k$ dělitelné. Je-li dána skupina přirozených čísel

$a_1, a_2, a_3, ..., a_k$, je vždy možno vyhledat největší z jejich společných dělitelů. Toto číslo se nazývá největší společný dělitel čísel $a_1, a_2, a_3, ..., a_k$ a označuje se $D(a_1, a_2, a_3, ..., a_k)$.“ [9]

4.3. Nejmenší společný násobek

Jak zjistíme nejmenší společný násobek, si ukážeme na stejných číslech jako u největšího společného dělitele, tudíž na číslech 60 a 90. Jako v předchozím případě si čísla opět zapíšeme jako součin prvočísel. 60 = 2 · 2 · 3 · 5, totéž provedeme u čísla 90. 90 = 2 · 3 · 3 · 5. U prvního čísla využijeme celý prvočíselný rozklad, kdežto u druhého čísla jen ty, která se již nevyskytují v prvním rozkladu. Pro lepší orientaci si čísla u prvního rozkladu podtrhneme a u druhého rozkladu vyškrtáme již vyskytující se čísla z prvního rozkladu a zbylá čísla následně také podtrhneme. Nejmenším společným násobkem poté budou všechna podtržená čísla z obou dvojic a následně jejich součin. [9]

60 = $\underline{2} \cdot \underline{2} \cdot \underline{3} \cdot \underline{5}$

90 = $\cancel{2} \cdot \cancel{3} \cdot \underline{3} \cdot \cancel{5}$

n(60,90) = 2 · 2· 3 · 5 · 3 = 2 · 2 · 3 · 3 · 5 = 180

nejmenší společný násobek čísel 60 a 90 je číslo 180.

4.4. Příklady nejmenšího společného násobku

Následuje několik příkladů. Vezmeme stejná čísla, se kterými jsme pracovali u největšího společného dělitele.

a) n(25, 85) b) n(60, 75) c) n(96, 128) d) n(150, 225)

Řešení:

a) n(25, 85)

25	5	85	5
5	5	17	17
1		1	

25= 5 · 5

85 = ~~5~~ · 17

n(25,85) = 5 · 5 · 17 = 425

b) n(60, 75)

60	2	75	3
30	2	25	5
15	5	5	5
3	3	1	
1			

60 = 2 · 2 · 3 · 5

75= ~~3~~ · ~~5~~ · 5

n(60, 75) = 2 · 2 · 3 · 5 · 5 = 300

c) n(96, 128)

96	2	128	2
48	2	64	2
24	2	32	2
12	2	16	2
6	2	8	2
3	3	4	2
1		2	2
		1	

96 = 2 · 2 ·2 ·2 ·2 · 3

128 =~~2~~ · ~~2~~ · ~~2~~ · ~~2~~ ·~~2~~ ·2 ·2

n (96, 128) = 2 · 2 · 2 · 2 · 2 · 2 · 2 · 3 = 384

d) n(150, 225)

150	2	225	3
75	3	75	3
25	5	25	5
5	5	5	5
1		1	

150 = 2 · 3 · 5 · 5

225 = ~~3~~ · 3 · ~~5~~ · ~~5~~

n(150, 225) = 2 · 3 · 5 · 5 · 3 = 450

4.5. Slovní úlohy na nejmenší společný násobek a největší společný dělitel

V této podkapitole následují slovní úlohy na největší společný dělitel a nejmenší společný násobek.

a) Papírový obdélník s rozměry 69 cm a 46 cm se má rozstříhat na co nejmenší počet shodných čtverců. Vypočítejte délku strany čtverce.

Řešení:

69	3	46	2
23	23	23	23
1		1	

69 = 3 · 23

46 = 2 · 23

D(69, 46) = 23

Odpověď: Délka strany čtverce bude 23 cm.

b) Maminka rozdělila svým dětem 24 jablek a 15 hrušek. Každé dítě dostalo stejný počet jablek a stejný počet hrušek jako jeho sourozenci. Kolik dětí měla maminka a kolik jablek a hrušek každé dítě dostalo?

Řešení:

24 | 2 15 | 3
12 | 2 5 | 5
6 | 2 1 |
3 | 3
1 |

24 = 2 · 2 · 2 · 3 15 = 3 · 5

D(24, 15) = 3

24/3 = 8

15/3 = 5

Odpověď: Maminka měla 3 děti. Každé dítě dostalo 8 jablek a 5 hrušek.

c) V květinářství dostali 144 bílých a 192 červených růží. Kolik kytic mohou svázat, má-li mít každá kytice stejný počet červených a stejný počet bílých růží? Kolik bílých a červených růží bude každá kytice obsahovat?

Řešení:

144 | 2 192 | 2
72 | 2 96 | 2
36 | 2 48 | 2
18 | 2 24 | 2
9 | 3 12 | 2
3 | 3 6 | 2
1 | 3 | 3
1 |

144 = 2 · 2 · 2 · 2 · 3 · 3192 = 2 · 2 · 2 · 2 · 2 · 2 · 3

D (144, 192) = 2 · 2 · 2 · 2 · 3 = 48

144/48 = 3

192/48 = 4

Odpověď: V květinářství mohou svázat 48 kytic. V každé kytici budou 3 růže bílé a 4 růže červené barvy.

d) Z autobusové zastávky vyjely v 10 . 10 hod současně autobusy dvou linek. Autobus č. 1 vyjíždí z této zastávky každých 20 minu, autobus č. 2 každých 16 minut. Za jak dlouho se opět sejdou autobusy obou linek v této zastávce? V kolik hodin se sejdou?

Řešení:

20	2	16	2
10	2	8	2
5	5	4	2
1		2	2
		1	

$20 = \underline{2} \cdot \underline{2} \cdot \underline{5}$

$16 = \cancel{2} \cdot \cancel{2} \cdot \underline{2} \cdot \underline{2}$

$n(20, 16) = 2 \cdot 2 \cdot 5 \cdot 2 \cdot 2 = 80$

10. 10 hod + 80 minut = 11. 30 hod

Odpověď: Autobusy se opět setkají za 80 min, tudíž v 11. 30 budou oba na zastávce, ze které vyjeli.

e) Jan a Jirka šli na procházku. Vykročili ze stejného místa. Jan dělal kroky dlouhé 66 cm, Jirka pouze 42 cm. Po kolika metrech Jirka došlápne přesně do Janovy stopy? Kolik kroků každý z nich udělá?

Řešení:

66	2	42	2
33	3	21	3
11	11	7	7
1		1	

$66 = \underline{2} \cdot \underline{3} \cdot \underline{11}$

$42 = \cancel{2} \cdot \cancel{3} \cdot \underline{7}$

$n(66, 42) = 2 \cdot 3 \cdot 11 \cdot 7 = 462$ cm = 4, 62 m

462/66 = 7

462/42 = 11

Odpověď: Jirka došlápne do Janovy stopy přesně za 4, 62 metrů. Jirka udělá 11 kroků a Jan pouze 7 kroků.

f) Karel a Vojta četli stejnou knihu. Karel denně přečetl 24 stránek, Vojta pouze 15 stránek. Kolik stránek měla kniha, pokud ji oba přečetli za celý počet dní? Kolik dní ji četl Karel a kolik dní Vojta?

Řešení:

24 | 2 15 | 3
12 | 2 5 | 5
6 | 2 1 |
3 | 3
1 |

$24 = \underline{2} \cdot \underline{2} \cdot \underline{2} \cdot \underline{3}$

$15 = \cancel{3} \cdot \underline{5}$

$n(24, 15) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 120$

$120/24 = 5$

$120/15 = 8$

Odpověď: Kniha měla celkem 120 stránek. Karel ji přečetl za 5 dní, kdežto Vojta ji přečetl za 8 dní.

5. Kongruence

Kongruence je pojem, který označuje v algebře ekvivalenci. Tato ekvivalence je slučitelná se všemi operacemi. Tedy pokud jsou prvky ekvivalentní a jejich operativní výsledek je též ekvivalentní, poté bude existovat kongruence pro tyto zvolené prvky. Abychom lépe pochopili kongruenci, měli bychom si nejdříve říci něco o ekvivalenci.

5.1. Ekvivalence

Binární relace ekvivalence slouží k vytvoření tříd navzájem ekvivalentních prvků. Máme zde několik podmínek ekvivalence. Mezi první podmínku patří reflexivita. Tento pojem vysvětlíme jednoduše a to tak, že pro každý prvek *a* z množiny X platí, že je v relaci sám se sebou. Mezi reflexivní relace patří například „je rovno“, „je podmnožinou“ nebo dělitelnost. Další podmínka pro existenci ekvivalence je symetrie. Symetrie říká, že pro každý prvek *a* a *b* z množiny X platí, pokud prvek *a* je v relaci s prvkem *b*, tak i prvek *b* je v relaci s prvkem *a*. Symetrická relace je například „je menší než“. Poslední operace, která se řadí mezi ekvivalenci, je tranzitivnost. Tato operace je složitější než již dvě zmíněné. Tranzitivnost říká, že pro každé *a*, *b* a *c* z množiny X platí, pokud *a* je v relaci s prvkem *b* a prvek *b* je v relaci s prvkem *c*, tak i prvek *a* je v relaci s prvkem *c*. Tato operace platí například pro „je větší než“, „je větší nebo rovno“, „je menší nebo rovno“ a také pro dělitelnost. Relace, která má vlastnosti tranzitivnosti a reflexnosti se nazývá kvaziuspořádání. Pokud je kvaziuspořádání navíc symetrické, potom můžeme mluvit o relaci ekvivalence.

Formální zápis pro operace zní:

reflexivní: $\forall\ a \in X : [a, a] \in R$

symetrická: $\forall\ a,b \in X : [a, b] \in R \rightarrow [b, a] \in R$

tranzitivní: $\forall\ a, b, c \in X: ([a, b] \in R \wedge [b, c] \in R) \rightarrow \rightarrow [a\ c] \in R$

Abychom lépe pochopili co pojem ekvivalence znamená, ukážeme si jednoduchý příklad, který zní: Jiří, Petr a Franta chodí do stejné třídy. Jako konkrétní příklad si zvolíme devátou třídu. Nyní si projdeme všechny tři typy operací. Začneme reflexivitou. Reflexivita musí být v relaci sama se sebou, takže je jasné, že Jiří chodí sám se sebou do deváté třídy. První operaci máme dokázanou.
Druhou operací je symetrie. Jestliže Jiří chodí do deváté třídy jako Petr, tak i Petr musí chodit do deváté třídy jako Jiří. Tato operace je také vyřešená.
Dále nám zbývá poslední operace a tou je tranzitivita.
V případě, že Jiří chodí do deváté třídy společně s Petrem a dále Petr chodí do deváté třídy společně s Frantou, tak i Jiří chodí do té stejné třídy jako Franta. Poslední operaci jsme vyřešili. V této chvíli jsme schopny na sto procent prohlásit, že se jedná o relaci ekvivalance.

V neposlední řadě musíme uvést další tři operace, abychom lépe pochopili kongruenci. Je-li a = b, tak pro libovolné číslo c platí následující tvrzení:

$$a + c = b + c$$

$$a – c = b – c$$

$$a \cdot c = b \cdot c$$

Z těchto operací je zřejmé, že jednotlivé operace můžeme sčítat, odečítat a nebo násobit. Na tomto principu je založena teorie algebry, nebo také teorie rovnicových soustav. Jediná operace, která zde není obsažena je dělitelnost. V této chvíli se již dostáváme k samotné podstatě kongruence. Půjde tedy o dělitelnost.

5.2. Vlastní pojem kongruence

Kongruence je relace, kde důležitou roli hraje modulo m. Modulo m představuje číslo, kterým budeme následovně dělit. Relaci můžeme chápat jako vztah mezi dvěma čísly, které mají stejný zbytek po dělení modulem. Poté říkáme, že *a* je kongruentní s *b* podle modulu m. Zápis zní: a ≡ b mod(m). Pokud tento vztah neplatí, zapisujeme jednoduše pomocí přeškrtnuté čáry. Jinými slovy můžeme říci, že čísla *a* a *b* jsou kongruentní podle modulu m, pokud m dělí a – b.

Jak už jsme si mohli všimnout na začátku této kapitoly, tak kongruence je relace ekvivalence. To znamená, že má vlastnost reflexivní, symetrickou a také tranzitivní. Jelikož jsme již s těmito pojmy obeznámeni, můžeme si je aplikovat přímo na pojem kongruence. Začneme tedy u prvního pojmu, pokud říkáme, že je kongruence reflexivní, rozumíme tím, že prvek *a* je kongruentní s *a* podle modulu m. Následuje operace symetrie, kongruence je symetrická, jestliže *a* je kongruentní s *b* podle modulu m, poté také *b* je kongruentní s *a* podle modulo m. Poslední operace je tranzitivnost. Tento pojem pojednává o vztahu tří prvků. Tedy pokud *a* je kongruentní s *b* podle modulu m a zároveň *b* je kongruentní s *c* podle modulu m, potom platí, že také *a* je kongruentní s *c* podle modulu m. Tyto operace jsme nyní schopny zapsat formálními symboly.

reflexivní: a ≡ a mod(m)

symetrická: a ≡ b mod(m) → b ≡ a mod(m)

tranzitivní: (a ≡ b mod(m) ∧ b ≡ c mod(m)) → a ≡ c mod(m)

V předešlém případě jsme si také uvedli ještě další tři operace, které se u kongruence objevují, avšak zde jsou více obsáhlejší. Mějme a ≡ b mod(m) a zároveň c ≡ d mod(m), pak operace znějí:

$a \equiv b \bmod(m) \rightarrow k \cdot a \equiv k \cdot b \bmod(m)$

$(a + c) \equiv (b + d) \bmod(m)$

$(a - c) \equiv (b - d) \bmod(m)$

$ac \equiv b \cdot d \bmod(m)$

Je tedy jasné, že kongruence, které mají stejný modulo se dají sčítat a také násobit. Při násobení je možno také vynásobit stejným číslem *k* obě strany kongruence.
V případě dělení je možno vydělit kongruence dělitelem, který bude jejich společný, ale tento dělitel nesmí být soudělný s modulem.

Jestliže bude $m > 1$, tak číslo *a* bude kongruentní právě s jedním číslem množiny $\{0, 1, \ldots, m - 1\}$

Jev $a \cdot b \equiv 0 \bmod(p)$, je pravdivý jen pokud $a \equiv 0 \bmod(p)$, nebo $b \equiv 0 \bmod(p)$, kde *p* je prvočíslo.

5.3. Příklady kongruence

Následné vybrané příklady kongruence, ve kterých máme zjistit, zda jsou správné: a) $916 \equiv 76 \bmod(42)$, b) $-326 \equiv 22 \bmod(29)$, c) $615 \equiv -86 \bmod(14)$

Řešení:

a) Jako první krok si spočteme 916 – 76

$916 - 76 = 840$

Dále zjišťujeme zda číslo 42 dělí náš vypočítaný výsledek po odečítání.

$840/42 = 20$

Můžeme si všimnout, že po dělení těchto dvou čísel nám vyšel zbytek, který je celé číslo.

Tudíž jsme vypočítali příklad a zjistili jsme, že kongruence $916 \equiv 76 \bmod(42)$ je správná.

b) Opět si jako první krok vypočteme rozdíl dvou čísel, a to čísel -326 a 22.

$-326 - 22 = -348$

Druhým krokem je otázka, zda číslo 29 dělí již vypočítaný výsledek.

(-348) / 29 = -12

Výsledek je znovu celé číslo, tím pádem kongruence - 326 ≡ 22mod(29) je správná.

c) 615 ≡ -86 mod(14)

Opakujeme kroky jako v předchozích řešení příkladů.

615 - (-86) = 701

Dělí číslo 14 číslo 701?

701/14 = 50, 07

V této chvíli si povšimneme, že výsledek nevyšel celé číslo, nýbrž desetinné. Odpověď je tedy v tomto případě odlišná. Kongruence 615 ≡ -86 mod (14) není správná.

6. Kritéria dělitelnosti

Kritérium dělitelnosti dvěma:
Každé číslo *n*, které je přirozené, je dělitelné dvěma, pokud cifra, která se nachází na místě nultého řádu, je dělitelná dvěma. Sudá čísla jsou dělitelná dvěma, kdežto lichá čísla dávají zbytek 1, tudíž nejsou dělitelná dvěma.

Kritérium dělitelnosti třemi:
Pokud je ciferný součet čísla n dělitelný třemi, poté je přirozené číslo n dělitelné třemi.

Kritérium dělitelnosti čtyřmi:
Každé přirozené číslo n je dělitelné čtyřmi, pokud je čtyřmi dělitelné poslední jeho dvojčíslí.

Kritérium dělitelnosti pěti:
Přirozené číslo n je dělitelné pěti pokud, cifra, která se nachází na místě nultého řádu je dělitelná pěti. **[10]**

Kritérium dělitelnosti šesti:
Číslo n, které je přirozené, je dělitelné šesti, pokud se jedná o číslo sudé a také je dělitelné třemi.

Kritérium dělitelnosti sedmi:
Přirozené číslo n je dělitelné sedmi, pokud je sedmi dělitelný i jeho rozdíl součtu sudých a lichých trojčíslí. **[10]**

Kritérium dělitelnosti osmi:
Číslo n je dělitelné osmi, jestliže je osmi dělitelné jeho poslední trojčíslí.

Kritérium dělitelnosti devíti:
Přirozené číslo n je dělitelné devíti, když je i devíti dělitelný jeho ciferný součet.

Kritérium dělitelnosti deseti:

Číslo n, které je přirozené, je dělitelné deseti, pokud se na místě nultého řádu nachází 0.

6.1. Důkazy dělitelnosti

Každé přirozené číslo *a* lze zapsat ve tvaru: $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \dots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$, a_0 reprezentuje počet jednotek a jedná se o cifru nultého řádu,

a_1 reprezentuje počet desítek a je cifrou prvního řádu,

a_2 představuje počet stovek a je cifrou druhého řádu,

a_3 představuje počet tisíců a je cifrou třetího řádu, dále platí:

$0 \leq a_0, a_{n-1} \leq 10$, tedy koeficienty jsou celá a nezáporná čísla od jedné do devíti.

Důkaz dělitelnosti dvěma:

Budeme mít přirozené číslo ve tvaru:

$a = a_0 + a_1 \cdot 10 + + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \dots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$,

Nyní z druhého a následujících sčítanců vytkneme číslo 10, takže nám vznikne tvar : $a = a_0 + 10 \cdot (a_1 + a_2 \cdot 10 + a_3 \cdot 10^2 + \dots + a_n \cdot 10^{n-1})$, celou závorku si označíme písmenem Y, jelikož v tomto důkazu není až tak důležitá. Tím vznikne: $a = a_0 + 10 \cdot Y$, již jsme schopni říci, že část $10 \cdot Y$ je dělitelná čísly 2, 5 a 10, jelikož číslo 2 dělí 10, číslo 5 dělí 10 a také číslo 10 dělí 10. V této chvíli nám zbude jen a_0. Pokud je číslo dělitelné dvěma, poté tato cifra nultého řádu musí být sudé číslo, to znamená, že cifry 0, 2, 4, 6, 8 musí být na místě jednotek.

Důkaz dělitelnosti pěti a deseti:

Tento důkaz je obdobný jako důkaz dělitelnosti dvěma, opět vycházíme ze tvaru: $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + + ... + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$, poté znovu vytkneme číslo 10 a vznikne nám tvar: $a = a_0 + 10 \cdot (a_1 + a_2 \cdot 10 + a_3 \cdot 10^2 + \ldots + a_n \cdot 10^{n-1})$, nyní si celou závorku označíme písmenem Y a dostaneme $a = a_0 + 10 \cdot Y$, výraz $Y \cdot 10$ je zajisté dělený čísly pět a deset, jelikož číslo pět dělí deset a deset dělí deset. Pokud přirozené číslo je dělitelné pěti, poté a_0 musí být nula nebo pět, pokud je dělitelné deseti, tak a_0 musí být nula.

Důkaz dělitelnosti čtyřmi:

Opět vycházíme ze tvaru pro zápis přirozeného čísla: $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \ldots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$. Dále budeme vytýkat číslo 100. Vznikne nám tedy tvar: $a = a_0 + + a_1 \cdot 10 + 100 \cdot (a_2 \cdot 1 + a_3 \cdot 10 + \ldots + a_{n-1} \cdot 10^{n-4} + a_n \cdot 10^{n-3})$. Celou závorku si označíme písmenem Y, tak nám vznikne tvar: $a = a_0 + a_1 \cdot 10 + 100 \cdot Y$. Výraz $100 \cdot Y$ je zajisté dělitelný čtyřmi, jelikož čtyři dělí sto. Jestliže je přirozené číslo dělitelné čtyřmi, poté také jeho poslední dvojčíslí je dělitelné čtyřmi.

Důkaz dělitelnosti osmi:

Důkaz dělitelnosti osmi vychází z důkazu dělitelnosti čtyřmi. Vycházíme ze tvaru pro zápis přirozeného čísla:

$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \ldots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n$. Nyní ale budeme vytýkat číslo 1000. Vznikne nám tedy tvar: $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + 1000(a_3 \cdot 1 + \ldots + a_{n-1} \cdot 10^{n-4} + + a_n \cdot 10^{n-3})$. Závorku si označíme písmenem Y, jelikož pro tento důkaz není podstatná, dostáváme tvar: $a = a_0 + a_1 \cdot 10 + + a_2 \cdot 10^2 + 1000 \cdot Y$. Výraz $1000 \cdot Y$ je dělitelný osmi, jelikož číslo osm dělí tisíc. Aby bylo číslo dělitelné osmi, musí být také jeho poslední trojčíslí dělitelné osmi.

Důkaz dělitelnosti devíti:

Budeme vycházet ze tvaru pro zápis přirozeného čísla: $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \ldots + a_{n-1} \cdot 10^{n-1} + + a_n \cdot 10^n$. Dále si čísla $10, 10^2, 10^3, \ldots$ rozepíšeme, a vznikne nám tvar: $a = a_0 + a_1 \cdot (9 \cdot 1 + 1) + a_2 \cdot (9 \cdot 11 + 1) + a_3 \cdot (9 \cdot 111 + 1) + + \ldots a_{n-1} \cdot (9 \cdot 11...1 + 1) + a_n \cdot (9 \cdot 11...1 + 1)$, dále si výraz upravíme : $a = a_0 + (a_1 \cdot 9 \cdot 1 + a_1 \cdot 1) + (a_2 \cdot 9 \cdot 11 + a_2 \cdot 1) + + (a_3 \cdot 9 \cdot 111 + a_3 \cdot 1) + \ldots + (a_{n-1} \cdot 9 \cdot 11...1 + a_{n-1} \cdot 1) + + (a_n \cdot 9 \cdot 11...1 + a_n \cdot 1)$. Vytkneme číslo devět. Dostáváme tak tvar: $a = (a_0 + a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n) + + 9 \cdot (a_1 \cdot 1 + a_2 \cdot 11 + + a_3 \cdot 111 + \ldots + a_{n-1} \cdot 11...1 + a_n \cdot 11...1)$.

Druhou závorku si označíme písmenem Y, získáme tak: $a = (a_0 + a_1 + a_2 + a_3 + \ldots + + a_{n-1} + a_n) + 9 \cdot Y$. Výraz $9 \cdot Y$ je zajisté dělitelný devíti. Nyní nám zbývá pouze první závorka neboli ciferný součet. Aby bylo číslo dělitelné devíti, musí být také jeho ciferný součet dělitelný devíti.

Důkaz dělitelnosti třemi:

Tento důkaz je podobný, jako důkaz dělitelnosti devíti. Po úpravách nám opět vznikne tvar: $a = (a_0 + a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n) + 9 \cdot (a_1 \cdot 1 + a_2 \cdot 11 + a_3 \cdot 111 + \ldots + a_{n-1} \cdot 11...1 + a_n \cdot 11...1)$, druhou závorku si opět označíme písmenem Y: $a = (a_0 + a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n) + 9 \cdot Y$. Výraz $9 \cdot Y$ je zajisté dělitelný třemi jelikož číslo tři dělí devět, tudíž nás zajímá jen ciferný součet. Přirozené číslo je dělitelné třemi, pokud je jeho ciferný součet dělitelný třemi.

7. Mersennova a Fermantova prvočísla

7.1. Mersennova prvočísla

Martin Mersenne byl francouzského původu. Zabýval se výhradně teorií čísel, mechanikou a optikou. Byl velmi důležitým článkem mezi významnými vědci, jako byli otec a syn Pascalovi, René Descartesý, a nebo Isaac Beckmann. Pro tuto skupinu lidí pořádal v roce 1623 schůzky, kde se probíraly různé disciplíny věd. Mersenne se narodil v roce 1588 ve Francii, kde také ve svých 60 letech zemřel, tedy v roce 1648. Na počest jeho památky byla zhotovena pamětní deska, která je umístěna na stěně kostela. Jednalo se o člověka, který se také zabýval teologií, filosofií, hudbou a mimo jiné navrhl Huygensovi, aby k měření času použil kyvadlo. Jako první upřesnil definici cykloidy a její charakteristické vlastnosti. Jeho jméno je však známé díky jinému pojmu, a tím jsou Mersennova čísla a prvočísla, na která se nyní podíváme. [11]

Mersennova čísla vyložil ve tvaru $M_p = 2^p - 1$, kde p je prvočíslo, tato čísla se týkají v první řadě teorie čísel. Pokud ovšem číslo $2^p - 1$ je samo prvočíslo, je nazýváno Mersennovo prvočíslo. Můžeme si všimnout, že pokud p =2, 3, 5, 7, tedy pokud dosadíme za proměnou p první čtyři prvočísla, dostaneme Mernsennova prvočísla 3, 7, 31, 127. Tento vzorec $2^p - 1$ však neplatí pro všechna prvočísla, například pro p = 11, jelikož $2^{11} - 1 = 2\,047$, číslo 2 047 není prvočíslo, jelikož je dělitelné číslem 23. Podobě je to u čísel 23 a 29, tedy $2^{23} - 1 = 47 \cdot 178\,481$ a $2^{29} - 1 = 233 \cdot 2\,304\,167$. Od roku 2007 je známo celkem 44 Mersennových prvočísel. Nalezené číslo M_p je prvočíslem pokud: p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253, 4 423, 9 689, 9 941, 11 213, 19 937, 21 701, 23 209, 44 497, 86 243, 110 503, 132 049, 216 091,

756 839, 859 433, 1 257 787, 1 398 269, 2 976 221, 3 021 377, 6 972 593, 13 466 917, 20 996 011, 24 036 583, 25 964 951, 30 402 457, 32 582 657, … [11]

Sám Mersenn tvrdil ve své práci, že čísla $2^p - 1$ pro p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 jsou prvočísla, avšak tato práce byla publikovaná v roce 1644 a my nyní již víme, že to není pravdivé tvrzení.

Matematici z celého světa hledají Mersennova prvočísla s velkým počtem cifer díky síťovému projektu s názvem GIMPS (Great Internet Mersenne Prime Search), který vznikl v roce 1996. Tento projekt byl navržen Georgem Woltmanem a je založen na principu rychlého násobení.

Doposud bylo největší Mersennovo prvočíslo nalezeno v roce 207 a to číslo $M_{32582657} = 2^{32582657} - 1$, které tvoří neuvěřitelných 9 808 358 cifer. [11]

7.2. Fermantova prvočísla

Celým jménem Pierre Fermat byl francouzským matematikem, který se také zabýval prvočísly. Domníval se, že všechna čísla ve tvaru: $F_m = 2^n + 1$, kde $n = 2^m$ jsou prvočísla s tím, že m = 0, 1, 2, … Tato domněnka však není pravdivá a již v roce 1732 ji Leonhard Euler vyvrátil, když objasnil Fermatovo číslo 5, tedy $F_5 = 641 \cdot 6\,700\,417$. V této chvíli posloupnost $F_m = 2^n + 1$, kde $n = 2^m$ poskytuje pouze prvních pět prvočíselných členů: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Fermatova čísla se označují symbolem F_m, dále je-li výraz $2^n + 1$, kde $n = 2^m$ prvočíslo, nazýváme ho Fermatovo prvočíslo.

Největší zájem o Fermatova čísla měl Carl Friedrich Gauss, který roku 1796 objevil souvislost mezi těmito

prvočísly a euklidovskou konstrukcí pravidelných mnohoúhelníků. Gauss objevil konstrukci sedmnáctiúhelníku již ve svých osmnácti letech a v dalších letech se tomuto tématu věnoval. Aby bylo možné pravidelný n-úhelník euklidovsky zkonstruovat, musí se počet vrcholů n-úhelníka rovnat číslu $n = 2^{k} \cdot p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_j$, kde čísla *p* tvoří Fermatova čísla. Takový n-úhelník lze konstruovat pro *n* = 3, 5, 15, 17, 51, 85, 255, 257 ,…, a tudíž bude mít lichý počet vrcholů.

Doposud je známo více než dvě stě prvočinitelů Fermantových čísel, avšak stále neznáme souvislosti, které by vedly k definitivní odpovědi, zda je opravdu F4 největší Fermatovo číslo. Například pro čísla F_{14}, F_{20}, F_{22} a F_{24}, nejsme schopni nalézt netriviálního dělitele. Víme však, že jsou to čísla složená jako již zmíněné číslo F_{14}, které má přes pět milionů cifer. [11]

8. Testy prvočíselnosti

Existuje mnoho testů prvočíselnosti, já zde uvedu jen několik z možných příkladů. Jednoduché testy pro pochopení vysvětlím i s příklady, kdežto testy složitější pouze uvedu jako možnosti na odhalování prvočísel.

8.1. Elementární test

Nejjednodušší ze všech testů je jistě elementární test prvočíselnosti, jedná se o základní test, kde se u testovaného čísla zkouší, zda někteří dělitelé dělí toto číslo. Pokud nenajdeme žádné číslo, které by dělilo zvolené pevné číslo, poté se jedná o prvočíslo. Princip tohoto testu spočívá v odmocnině z námi testovaného čísla. Pokud si tento test rozebereme více do hloubky, zjistíme, že pokud je číslo menší nebo rovno 1, poté zajisté nebude prvočíslem. Dále, jestliže testované číslo je sudé a není dva, také nebude prvočíslem. Nyní nám stačí testovat pouze lichá čísla. Tento test bohužel není použitelný pro velká čísla, a proto se využívá jen pro malá čísla, které mají maximálně 24 číslic.

Příklady:

Uvedeme si první příklad a to na čísle 211. Nejdříve musíme toto číslo odmocnit.

$\sqrt{211} = 14.53$

Nadále je zřejmé, že námi uvedené číslo 211 budeme dělit prvočísly 2, 3, 5, 7, 11 a 13.

211 / 2 = 105.5

211 / 3 = 70.33

211 / 5 = 42.2

211 / 7 = 30.14

211 / 11 =1 9.18

211 / 13 = 16.23

Jak vidíme, tak ani jeden výsledek po dělení šesti prvočísly nevyšel beze zbytku, tudíž naše číslo 211 je opravdu prvočíslem.

Jako náš další příklad bude číslo 821.

V prvním kroku toto číslo musíme odmocnit: $\sqrt{821} = 28.65$,

Ve druhém kroku budeme číslo dělit těmito prvočísly: 2, 3, 5, 7, 11, 13, 17,19, 23.

821 /2 = 410.5

821 / 3 = 273.66

821 / 5 = 164.2

821 / 7 = 117.29

821 / 11 = 74.64

821 / 13 = 63.15

821 / 17 = 48.29

821 / 19 = 43.21

821 / 23 = 35.70

Každý z vypočítaných výsledků vyšel se zbytkem, jsme schopni říci, že číslo 821 je prvočíslo.

Posledním ukázkovým příkladem je číslo 505. Na první pohled je již zřejmé, že se nebude jednat o prvočíslo. Pojďme ale postupovat podle elementárního testu. Číslo 505 není sudé a nerovná se číslu dva, tudíž stále může být prvočíslem. Zkusme tedy toto číslo odmocnit: $\sqrt{505} = 22.47$, nadále budeme zkoumat, zda je dělitelné těmito prvočísly: 2, 3, 5, 7, 11, 13, 17 a 19.

505 / 2 = 252.5

505 / 3 = 168.33

505 / 5 = 101

505 / 7 = 72.14

505 / 11 = 45.91

505 / 13 = 38.85

505 / 17 = 29.71

505 / 19 = 26.58

Jen jediné prvočíslo a to číslo 5 dělí námi zvolené číslo 505, to ovšem znamená, že 505 nemůže být prvočíslem, i přesto, že má pouze jednoho dělitele z řady prvočísel.

8.2. Eratosthenovo síto

O tomto principu jsme si již říkali v kapitole historie matematiky. Jedná se o algoritmus, který je datován do roku 200 před naším letopočtem, a je pojmenován po svém objeviteli Eratosthenovi. Tento test se provádí jen u hledání prvočísel do 1 0000 000. Nyní si ho připomeneme jen jedním příkladem. Našim cílem je najít všechna prvočísla do 30. Prvním krokem je podtržení čísla 2 a následné vyškrtání všech jeho násobků.

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~~

Dále potrháme číslo 3 a také vyškrtáme jeho násobky.

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~~

Ten samý krok uděláme i u čísla 5.

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~~

Nyní jsme hotovi, zbyly nám jen podtržená čísla, tyto čísla jsou prvočísla.

8.3. Fermatův test prvočíselnosti

Tento test bývá někdy uváděn i jako test složenosti, a to proto, že nedokáže rozlišit prvočísla od speciálních složených čísel, která se nazývají Carmichaelova čísla. Test vychází z Fermatovy věty, tudíž pro každé prvočíslo musí platit: $a^{p-1} \equiv 1 \bmod(p)$. Jestliže tato rovnost nebude pravdivá, poté tento vztah stačí jako důkaz složenosti čísla *p*, a tudíž nemůže být prvočíslem, avšak pokud bude pravdivá, číslo může být prvočíslem, ale také nemusí. Test tak musíme provést znovu, ale nyní s jiným číslem *a*. Nejmenší Carmichaelovo číslo je číslo 561, dalšími jsou například 1 105,1 729,2 465 a 2 821, tyto čísla se také někdy označují jako pseudočísla. Z důvodu těchto pseudočísel se Fermatův test v praxi nepoužívá.

8.4. Lehmannův test prvočíselnosti

Tento test vychází z malé Fermatovy věty, kterou jsme si již uvedli. Princip e založený na tom, že cíleně nevíme, zda jsme našli prvočíslo, ale určitě víme, zda jsme prvočíslo nenašli, algoritmus Lehmannova testu se stále opakuje a my jsme schopni snížit každým opakováním procento složených čísel až o padesát procent.

8.5. Rabin-Millerův test prvočísel

Jedná se o pravděpodobnostní test, který je postaven na na faktu: máme-li celé číslo *n*, které je prvočíslo, poté má právě dvě odmocniny jedničku a modulo n. Tento test se v praxi využívá nejčastěji, a je založený také na Fermatově větě jako test Lehmannův. Stanoví nám na sto procent, že se o prvočíslo nejedná, a tudíž se jedná o složené číslo.

9. Šifrování pomocí velkých prvočísel

9.1. RSA šifra

RSA šifra je pojmenovaná podle Ronalda Rivesta, Adi Shamira a Leonarda Adlemanna. Byla vymyšlena v roce 1997 a v této době se řadí mezi nejpoužívanější asymetrické šifry. Rozdíl asymetrické šifry od té symetrické je prostý, jelikož se přijímatel a odesílatel nemusí setkat a tím pádem se také nemusí dohodnout na společném klíči, zpráva je v tomto případě šifrovaná i dešifrovaná. Pokud zpráva není dostatečně zašifrovaná, mohl by jí kdokoliv otevřít a vzniknout tak veliký problém, jelikož se tato metoda šifrování používá v bankovnictví. Pro tento důvod se častěji využívá asymetrické šifrování, kde máme dva klíče, první je soukromý a pomocí něho se zpráva šifruje a druhý je veřejný, ten slouží k dešifrování zprávy. Tyto dva klíče jsou velice úzce matematicky propojené. Pokud neznáme klíč k dešifrování zprávy je v podstatě nemožné ji otevřít.

Pojďme si toto šifrování ukázat na příkladě. Karel vlastní asymetrickou šifru, tedy obdrží vygenerované dva klíče. Jak již jsme uvedli, první klíč je soukromý a druhý veřejný. Karel poté chce napsat zprávu, kterou následně zašifruje svým soukromým klíčem, to znamená, že nikdo ostatní tuto zprávu nemůže nijak upravit, jelikož nikdo nemá přístup ke Karlovu soukromému klíči. Karel poté zprávu zveřejní, avšak každý příjemce má přístup k této zprávě, jelikož mají veřejný klíč ke Karlově zprávě. Každý může Karlovu zprávu otevřít a přečíst, ale nemůže ji nijak změnit, jak už bylo uvedeno. Toto je princip, který se hojně využívá v praxi, například takto fungují digitální podpisy.

Zkusme tento příklad provést z druhé strany. Například Petr by chtěl poslat Karlovi zprávu, problém je v tom, že si přeje aby tuto zprávu viděl pouze Karel a nikdo jiný. Petr tudíž nemůže použít postup z předchozího příkladu, jelikož kdyby zašifroval svojí zprávu, kdokoli z ostatních by si ji mohl přečíst. Petr tedy použije Karlův veřejný klíč k zašifrování své

zprávy. Karel jako jediný tuto zprávu může dešifrovat, jelikož jen on má přístup ke svému soukromému klíči.

Poslední příklad uvádí situaci, kdy si Karel a Petr chtějí navzájem posílat tajné zprávy, aniž by se střetli, tudíž musí využít tento šifrovací systém. Nevyhovujícím principem bude zkombinovat oba dva předcházející příklady dohromady. To znamená, že Karel svoji zprávu zašifruje jeho soukromým klíčem, a tak zaručí, že tuto zprávu nebude moci někdo jiný upravit. Dále zašifruje danou zprávu i s Petrovým veřejným klíčem, tudíž nikdo jiný kromě Petra si ji nebude moci přečíst. Ten jistý postup podstoupí i Petr, jakmile bude psát svou zprávu Karlovi. Nejdříve si zašifruje svou zprávu soukromým klíčem a následně ji zašifruje Karlovým veřejným klíčem.

Šifra RSA se nepoužívá pouze v bankovním systému, ale také zabezpečuje datové přenosy na internetu.

Prvočísla jsou velice důležitá v tomto procesu šifrování, jelikož prvočíslo *p* a každé číslo od jedné do *p – 1* mají největší společný dělitel rovný, a tedy má převrácenou hodnotu v modulo(p). Prvočísla se vyskytují také v Eulerově funkci, která je při tomto šifrování také důležitá, její rovnice zní : $\varphi(n) = p - 1, p \in P$,

P označuje množinu prvočísel, φ (n) značí Eulerovu funkci, která je zobrazením a udává počet všech čísel k takových, že $1 \leq k \leq n$ a dále D(k, n) = 1, například φ (5) = 4.

Eulerova věta nám říká : $a^{\varphi(n)} = 1 \bmod(n)$. Pokud za φ (n) dosadíme p-1, což je Eulerova funkce, dostaneme:

$$a^{p-1} = 1 \bmod(p),$$

tato rovnice je speciálním případem Eulerovy věty a říká se jí Malá Fermatova věta.

Vytvoření klíče je algoritmus, který nám vygeneruje jak veřejný tak i soukromý klíč. Generování probíhá ve třech krocích:

- zvolení n(modulus), zvolíme dvě různá prvočísla a poté rovnici $n = p \cdot q$
- volba e (veřejný klíč), e musí patřit do oboru hodnot
- zvolení d(soukromý klíč), pro volbu d musí platit: $e \cdot d \bmod \varphi(n) = 1$ [12]

K šifrování zprávy se tak používá vzorec $F(m,k) = m^k \bmod(n)$

Zašifrování soukromého klíče:

$F(x,y) = x^y \bmod(n) = z$, kde x je zpráva, y je soukromý klíč a z je zašifrovaná zpráva

Zašifrování veřejného klíče:

$F(x,e) = x^e \bmod(n) = z$, kde x je zpráva, e je veřejný klíč a z je zašifrovaná zpráva.

Bezpečnost šifry RSA rozloží velké číslo na součin prvočísel, na takzvanou faktorizaci. Proto je důležité, aby čísla *p* a *q* byly velmi daleko od sebe a jednalo se o velmi velká prvočísla. V současné době se považuje za bezpečné, aby se modus skládal minimálně z 309 cifer, to znamená, aby klíč měl velikost alespoň 1 024 bitů. Například pro rozluštění RSA šifry, která by měla 1 024 bitů je vypsaná odměna neuvěřitelných 1 000 000 dolarů.

9.2. Šifrování ElGamal

Taher ElGamal navrhl tento algoritmus v roce 1895. Jedná se o šifrování, kde se využívá asymetrický princip. Skládá se ze šifrovacích dat, která jsou ale dvakrát delší než otevřená data, a proto se nevyužívá často. I přes jeho nepříliš hojné využití se vyskytuje v mnoha programech, a také se využívá jako alternativa k jiným algoritmům.

V tomto šifrování se generují dva klíče, veřejný a soukromý. Princip pracuje na počítání diskrétních logaritmů.
Vzorec k vytvoření klíče zní:

$$y = g^{a} \bmod(p)$$

Tento vzorec se používá k vytvoření veřejného klíče, je potřeba si zvolit vysoké prvočíslo *p*, číslo *a* představuje náhodně vybrané číslo, které je zároveň i soukromým klíčem, a *g* představuje hodnotu generátoru, který je zastoupený v multiplikativní skupině.

9.3. Diffieho – Hellmanovo šifrování

Toto šifrování se stalo první metodou, jak sdílet informace na nezabezpečeném komunikačním kanále. Navrhli ho roku 1976 Whitfield Diffe a Martin Hellman, po kterých je i pojmenován. Jelikož se jedná o symetrický princip, tak si dvě strany nejdříve vytvoří šifrovací klíč. Tento klíč je posílán po částech, avšak je posílán na základě informací, tudíž v případě odposlechu třetí osoby není možné zjistit šifrovací klíč, který slouží pro šifrovací komunikaci.

Pokud osoba A vlastní veřejný klíč osoby B, použije následující vzorec: $K_A = y_B^{xA} \bmod(p)$. Pro osobu B je tento vzorec podobný: $K_B = y_A^{xB} \bmod(p)$, aby mohli tento vzorec uživatelé používat, musí si nejdříve domluvit číslo *p,* v tomto šifrování se jedná o prvočíslo, dále také *x*, které tvoří tajný klíč. Číslo y_A či y_B tvoří veřejný klíč, který si navzájem přepošlou. Celé hodnoty K_A a K_B je přeposílaná zpráva, ze které se vytvoří symetrický šifrovací klíč.

10. Velká prvočíselná věta

První, kdo se o tuto větu zajímal, byl již Carl Friedrich Gauss, který v 18. století vyjádřil četnost prvočísel. Dále se jí také věnoval Pafnutij Lvovič Čebyšev a Bernhard Riemann. První důkazy této prvočíselné věty dokázal v roce 1896 Charles Jean de la Vallée-Poussin a Jacques Hadamard, kteří použili metody matematické analýzy. Ve 20. století se podařilo Edmundovi Landauovi o jednodušší důkaz této věty.

Jedná se o větu, která se zabývá oborem teorie čísel. Platí že, π (x) je prvočíselná funkce. Touto funkcí rozumíme počet prvočísel, které jsou menší nebo rovno *x*, myšleno reálné *x.*

Vzorec prvočíselné věty zní:

$$\lim_{x \to \infty} \pi(x) / (x / \ln(x)) = 1.$$

Slovy tento vzorec můžeme popsat jako limitu, pokud x jde k nekonečnu, poté podíl funkce π(x) a x / ln(x) se rovná jedné. Jinými slovy zjišťujeme pravděpodobnost při náhodném výběru čísla, která by vyjadřovala, že se jedná o prvočíslo. Tato pravděpodobnost je rovna 1 / ln(x). Mezi dvěma prvočísly je tak mezera rovna ln(x). Mějme například prvočíselnou funkci π(14). Již víme, že existuje šest prvočísel menších nebo rovných číslu 14 a ty jsou: 2, 3, 5, 7, 11 a13, tudíž prvočíselná funkce π(14) bude rovna číslu 6.

Pro zajímavost kolem čísla 10 000 je jedno z devíti čísel prvočíslem, avšak kolem čísla 1 000 000 je už jen jedno z 21 čísel prvočíslem.

Velká prvočíselná věta však neudává informace o rozdílu funkcí, jelikož je to velice komplikované nalézt. Tento rozdíl patří k nejzákladnějším a nevyřešeným problémům matematiky, jedná se o Riemannovu domněnku, která nese jméno po německém matematikovi Bernhardu Riemannovi a je zařazena mezi sedm nevyřešených matematických problémů. Do tohoto seznamu byla vložena v roce 2000.

Závěr

Teorie čísel je velká kapitola matematiky. Myslím, že tuto kapitolu lze studovat mnohem podrobněji. Cílem této bakalářské práce bylo seznámit čtenáře s pojmem prvočíslo a kongruence, s jejich základními vlastnostmi a metodami. Proto bylo důležité zmínit také pojmy, jako jsou největší společný dělitel, nejmenší společný násobek a také kritéria dělitelnosti. Uvedla jsem také méně známá témata, která zajisté jdou studovat více do podrobna, jako byly testy pročíselnosti či šifrování pomocí velkých prvočísel. Těchto témat jsem se však dotkla jen okrajově, jelikož rozsáhlost této tématiky by byla pro některé čtenáře příliš vyčerpávající.

Charakter mé práce je čistě informativní. Bylo nutné shromáždit veškeré materiály a postupně se propracovávat k jednotlivým pojmům, aby čtenář pochopil návaznost a orientoval se v této práci bez obtíží.

Po celý čas psaní bakalářské práce bylo zajímavé sledovat jak je celá problematika matematiky provázaná, a jak je důležité pochopit veškeré souvislosti mezi tématy. Jen díky tomuto jsem mohla tyto informace předat čtenáři. Závěrem bych chtěla říci, že výběru tématu nelituji. Musím také uvést, že přínos informací mne velice obohatil.

Seznam literatury:

[1] GRACIÁN, Prvočísla, dlouhá cesta do nekonečna. Vyd. 1. Praha, 2017, 20 s.

[2] BEČVÁŘ, Jindřich a Eduard FUCHS. Historie matematiky I: seminář pro vyučující na středních školách: Jevíčko, 19.8.-22.8.1993 : sborník. 1. vyd. Brno: Jednota českých matematiků a fyziků, 1994, 241 s.

[3] MAREŠ, Milan. Příběhy matematiky: stručná historie královny věd. 1. vyd. Příbram: Pistorius & Olšanská, 2008, 334 s. ISBN 9788087053164.

[4] VYMAZALOVÁ Hana. Staroegyptská matematika. Hieratické matematické texty. Praha: Český egyptologický ústav FF UK, 2006.

[5] Sedláček: Co víme o přirozených číslech Praha: Mladá fronta, 1961.

[6] DERBYSHIRE, John. Posedlost prvočísly. Vyd. 1. Praha: Academia, 2007, 407 s.

[7] Důkaz sporem. Matematika.cz [online]. 2014 [cit. 2015-02-28]. Dostupné z: http://www.matematika.cz/dukaz-sporem#dukaz-nekonecnosti-prvocisel

[8] [9] BIALAS, Aleksander. O dělitelnosti čísel. 1. vyd. Praha: Státní pedagogické nakladatelství, 1966, 97 s.

[9] SEDLÁČEK, Jiří. Co víme o přirozených číslech. 2. vyd. Praha: Mladá fronta, 1965, 53 s.

[10] DRÁBEK, Jaroslav, VIKTORA, Václav, KŘIŽALKOVIČ, Karol, LIŠKA, Jan. Základy elementární aritmetiky pro učitelství 1. stupně ZŠ. 1. vyd. Praha: SPN, 1985, 223 s.

[11] Křížek Michal, Somer Lawrence, Šolcová Alena. Kouzlo čísel 1. vydání. Akademia. 2009

[12] Cleverandsmart, generovanie kľúču, http://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-rsa/