ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

ÚLOHY O DĚLITELNOSTI

BAKALÁŘSKÁ PRÁCE

Martin Pašek

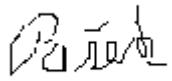
Matematika se zaměřením na vzdělávání

Vedoucí práce: Doc. RNDr. Jaroslav Hora CSc.

Plzeň, 2022

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

V Plzni dne 20. 6. 2023



vlastnoruční podpis

Obsah

SEZNAM ZKRATEK

NSD – Největší společný dělitel

ÚSZ – Úplná soustava zbytků

FÚSZ – Fundamentální úplná soustava zbytků

RSZ – Redukovaná soustava zbytků

Úvod

Dělení čísel a dělitelnost je znalost, se kterou se seznamují již děti na základní škole. Jsou to poznatky nesporně důležité. Jde o základy, na kterých jsou potom stavěny další a další pilíře matematiky. Využití těchto zákonitostí může být nápomocné při řešení velkého počtu problémů. Tento argument je potvrzen nespočetným množstvím úloh zabývající se touto tematikou v Matematických olympiádách, Klokanovi nebo přijímacích zkouškách.

Teorie dělitelnosti jakožto podmnožina teorie čísel se ale zabývá i složitějšími příklady, na které již nenarazíme na žádné základní či střední škole. Jejich důležitost či využití ale nemusí být o nic menší. Některé z těchto příkladů jsou tak obtížné, že jejich vyřešení vyžadovalo nejprve objevit úplně jiné poznatky a založit nové, dříve neznámé okruhy matematiky.

V této práci se v jednotlivých kapitolách podíváme na několik problémů z teorie dělitelnosti.

Závěrečná část práce obsahuje také několik příkladů vybraných z matematických olympiád společně s vlastním řešením. Vypracované příklady slouží jako demonstrace využití nejrůznějších poznatků z oboru dělitelnosti.

VELIKONOČNÍ PROBLÉM

Na začátek se podíváme na křesťanský svátek spojený s oslavou zmrtvýchvstání Ježíše Krista. Tento svátek je oblíbený především u dětí, a přestože se jedná o původně náboženský svátek, spousta lidí ho má spíše spojený s vítáním jara. Řeč je samozřejmě o Velikonocích. Dalším důvodem, proč je tento svátek tak zajímavý, je jeho datum. Jedná se totiž o jediný svátek v našem kalendáři, který své datum mění. Jelikož existuje několik různých náboženství a každé slaví Velikonoce podle svých tradic, o to víc se může konkrétní datum lišit. Jelikož se ale jedná hlavně o křesťanský svátek, budeme vycházet z křesťanské tradice. Podle ní připadá datum velikonoční neděle na první neděli po prvním jarním úplňku. Takto se může tedy určení data oslav zdát jako velmi prosté. Přesto byl ve středověku na univerzitách vyčleněn předmět, ve kterém se učenci učili metodě, jejímž cílem bylo spočítat přesné datum Velikonoc. Proč je tedy tento výpočet tak obtížný a jak to vše souvisí s teorií dělitelnosti?

JULIÁNSKÝ KALENDÁŘ

Pro první odpověď se musíme vrátit do minulosti. Nacházíme se v době Julia Caesara v prvním století před naším letopočtem. V platnost právě přichází nový systém určující strukturu roku, který se bude později nazývat juliánský kalendář. Jedná se o druh solárního kalendáře. To znamená, že se řídí dobou, za kterou oběhne země slunce. Celý rok v něm tedy trvá 365 dní, což je stejný počet, na který jsme zvyklí i dnes. Solární rok ale ve skutečnosti netrvá 365 dní, ale přibližně 365 a čtvrt dne. Proto se jednou za 4 roky navíc přidává jeden přestupný den. Výhodou tohoto kalendáře je dodržení spojitosti mezi čtyřmi ročními obdobími tak, jak to známe v současnosti. Jeho nevýhodou je neslučitelnost s délkou jednotlivých měsíčních cyklů. Délky jednotlivých měsíců jsou tedy dány pouze dohodou. Vraťme se zpět k Velikonocům. Pokud chceme spočítat přesné datum velikonoční neděle, stačí zjistit datum a den prvního jarního úplňku. V případě, že by úplněk připadnul na neděli, pak se budou Velikonoce slavit až následující neděli. V historii se pro zjištění přesného dne prvního jarního úplňku využívalo různých cyklů. Jejich výhoda spočívala v opakování se určité skutečnosti, a tak začala platit po jejich uplynutí stejná pravidla opět od začátku.

Jedna z metod využívala tzv. Metonova cyklu. Ten trval 19 let a po jeho uplynutí

připadnou měsíční fáze opět na stejné dny v roce. Pokud bychom ale chtěli dosáhnout větší přesnosti kvůli výskytu přestupných dnů, musíme zřetězit několik těchto cyklů za sebe. Kallippův cyklus vznikl složením 4 Metonových cyklů. Trval tedy 76 let, a jelikož je číslo 76 dělitelné čtyřmi, je počet přestupných dní vždy 19. U Metonova cyklu to mohly být celkem 4, ale také 5 přestupných dnů. Nejpřesnějším byl pak Hipparchův cyklus, který se skládal ze 4 Kallippových cyklů a jednoho odečteného dne. Počítat Velikonoce podle tohoto cyklu znamená, že musíme provést opravu data pouze o jeden den každých 304 let. Další metoda využívala např. slunečního kruhu, což je cyklus dlouhý 28 let. Po jeho uplynutí se začnou opakovat dny v týdnu pro určité datum.

Gregoriánský kalendář

Přesuneme se o několik století vpřed. Za ten obrovský počet uplynulých let se nedalo nevšimnout narůstající nepřesnosti Juliánského kalendáře. Např. jarní rovnodennost se oficiálně odchýlila od data 21. března o celých 10 dní. Výše zmíněný Metonův cyklus se také začal lišit od reality, a to o 4 dny. Proto byl roku 1582 zaveden Gregoriánský kalendář pojmenovaný podle papeže Řehoře XIII.. Došlo ke korekci všech přestupných dnů, vyrovnání fází Měsíce a byl převeden počet dní některých měsíců. Podoba tohoto nového kalendáře přetrvává až dodnes, neboť je to přesně ten kalendář, podle kterého se každý rok řídíme. Dalším opravným aspektem je vypouštění přestupného roku třikrát za 400 let, přičemž v roce 2000 zrovna vypuštěn nebyl. Znamená to tedy, že roku 2100 nebude přestupný rok. S novými změnami se změnil i přístup k výpočtu přesného data Velikonoc. Byla zavedena veličina s názvem epakta, která reprezentuje stáří Měsíce na začátku roku. Pomalu se ale dostáváme k osobě, která vytvořila metodu, jejíž proměnné založené na dělitelnosti se dají zapsat šikovně do tabulek. S její pomocí může každý člověk spočítat datum Velikonoc bez nutnosti chápat jednotlivé astronomické cykly. Stačí se v této tabulce správně orientovat. Touto osobou byl Carl Friedrich Gauss.

Carl Friedrich Gauss

Carl Friedrich Gauss se narodil v Německu roku 1777. Jeho matematického nadání si všiml ve škole jeho učitel. Jeho obrovskou předností byla schopnost neskutečně rychlých výpočtů, které prováděl z hlavy. Nejednalo se ale pouze o jednoduché výpočty, ale jeho mysl zvládala i složitější kalkulace. Přestože byli jeho rodiči spíše chudí, jeho matka a

učitelé ho doporučili vévodovi z Brunšviku. Ten mu poskytl potřebné finance na další studium. Díky tomu se dostal na univerzitu v Göttingenu v roce 1795. Zpočátku se zabýval hodně geometrií mnohoúhelníků. Věnoval se ale i teorii čísel, aritmetice, polynomům, a dokonce i astronomii. Z jeho raných prací v teorii dělitelnosti lze například uvést aritmetiku zbytkových tříd a také velikonoční algoritmus.

Jeden z problémů, které Gausse trápily, byla neznalost přesného dne narození. Jeho rodiče si totiž přesný den nepamatovali. Jeho matka ale věděla, že se narodil 8 dní před svátkem Nanebevstoupení Páně roku 1777. O tomto svátku víme, že se koná vždy ve čtvrtek, 40 dní po velikonoční sobotě. Potřeboval tedy zjistit přesný den, kdy se ten rok konaly Velikonoce. Potom už by byl jednoduše schopen dopočítat datum svého narození. Problém vyřešil již ve svých osmnácti letech, a později v roce 1800 svůj algoritmus pro výpočet velikonoční neděle veřejně publikoval. Zjistil, že velikonoční neděle v roce 1777 nastala 30. března. Svátek Nanebevstoupení tedy připadl na 8. května, a tak se Gauss narodil 30. dubna.

Algoritmus

Nesmírnou výhodou Gaussova algoritmu je absence pomocných veličin. Nepotřebujeme znát ani epaktu, nedělní písmeno, nebo zlaté číslo, což byly veličiny, které se kdysi používaly, ale pouze rok a speciální parametry. Nejdříve se podíváme na tento algoritmus obecně a potom postup aplikujeme pro výpočet konkrétního data Velikonoc.

Označme si rok proměnnou R. Do našeho výpočtu budou vstupovat celkem tři cykly. Prvním z nich je devatenáctiletý Metonův cyklus. Druhým je čtyřletý cyklus, ve kterém se do kalendáře vkládá přestupný rok. Posledním cyklem je doba sedmi let, víme totiž, že rok má celkem 52 týdnů a jeden den. V případě, že by nebyl zahrnut přestupný rok, začaly by se po těchto sedmi letech opět opakovat jednotlivé dny v týdnu přiřazené ke konkrétnímu datu. Využijeme tedy funkci modulo, která nám vrací zbytek po dělení přirozeným číslem. Vypočítáme si tři proměnné a, b, $c \in N$.

- $a = R \bmod 19 \Rightarrow a \in (0, 18)$
- $b = R \bmod 4 \Rightarrow b \in (0, 3)$
- $c = R \bmod 7 \Rightarrow c \in (0, 6)$

Teď se podíváme na datum prvního jarního úplňku. Ten může být nejdříve 21. března. Velikonoční neděle může být tedy nejdříve 22. března. Napřed tedy musíme spočítat datum prvního úplňku. Toto datum si označme d. Začínat budeme od čísla 21. To budeme následně zvětšovat o hodnotu M, která souvisí s počtem dní v Metonově cyklu. Pro juliánský kalendář je hodnota M v čase konstantní, konkrétně 15. Od doby zavedení gregoriánského kalendáře ale dochází k úpravě hodnoty M, která se nyní mění v čase. Konkrétní hodnoty M pro jednotlivé roky si ukážeme později. Vraťme se zpět k proměnné d. Pokud by proměnná d vzrostla nad 30, musíme ji o 30 snížit, nebudeme se poté nacházet v březnu, ale v dubnu. Konkrétní hodnota d je dána následujícím vztahem:

- $d = (19a + M) \bmod 30$

Dostáváme se k poslední proměnné, kterou budeme potřebovat. Nazveme ji e. Hodnota je spjata se sedmiletým cyklem, ve kterém by se opakovaly jednotlivé dny ke konkrétnímu datu, pokud bychom nepřidávali přestupný den. Pro juliánský kalendář bude e vždy rovno 6. Po gregoriánské reformě se ale hodnoty e také mění v čase, konkrétně od 0 do 6. Konkrétní hodnotu pro jednotlivé roky si ukážeme později v tabulce. Gaussův vzorec pro e vypadá následovně:

- $e = (2b + 4c + 6d + N) \bmod 7$

Teď už jen stačí dopočítat výsledné datum Velikonoc, které bude závislé na součtu d + e.

- Pokud je $d + e < 10$, potom připadá velikonoční neděle na datum $(22 + d + e)$. března.
- Pokud je $d + e > 9$, potom připadá velikonoční neděle na datum $(d + e – 9)$. dubna.

Vzhledem k zavedené konvenci si musíme dovolit zmínit 2 výjimky. Pokud nám vyjde d = 28, snížíme ho o jedna, a pokud vyjde d = 27 také ho ponížíme o jedna. Důvodem je fakt, že pokud vyjde úplněk na neděli 18. nebo 19. dubna, počítá se s ním, jako by proběhl již předchozí den.

Přestože je dnes k výpočtu data Velikonoc oficiálně využívána Liliova – Claviova metoda, Gaussův algoritmus je s ním ekvivalentní. Velká výhoda Gaussova algoritmu spočívá ve snadnější implementaci do počítačového programu.

KONKRÉTNÍ VÝPOČTY

Nyní se podíváme na několik konkrétních výpočtů data velikonoční neděle. Abychom mohli tyto výpočty provést, potřebujeme napřed dohledat v následující tabulce konkrétní hodnoty M a N pro náš rok.

od roku	do roku	M	N
1582	1699	22	2
1700	1799	23	3
1800	1899	23	4
1900	1999	24	5
2000	2099	24	5
2100	2199	24	6
2200	2299	25	0

(tabulka č. 1 – hodnoty proměnných M a N)

PŘÍKLAD Č. 1

Na začátek se podíváme na datum Velikonoc roku 1999, na rok, kdy jsem se narodil. Dne 14. března jsem se poprvé podíval na tento svět a mojí otázkou zůstává, kolik dní jsem byl starý, když jsem slavil své první Velikonoce?

Výchozí číslo R je pro nás 1999. Spočítáme proměnné a, b, c.

- a = 1999 mod 19 = 4
- b = 1999 mod 4 = 3
- c = 1999 mod 7 = 4

Pro tento rok budou hodnoty M = 24, N = 5. Dosadíme do vzorce pro výpočet proměnné d.

- d = (19a + M) mod 30 = 100 mod 30 = 10

Teď, když známe přesnou hodnotu d, vypočítáme hodnotu proměnné e.

- e = (2b + 4c + 6d + N) mod 7 = (6 + 16 + 60 + 5) mod 7 = 87 mod 7 = 3

Součet d + e > 10, proto naším hledaným měsícem bude duben.

- (d + e – 9) = (3 + 10 – 9) = 4

V roce 1999 se Velikonoce slavily 4. dubna. Byl jsem tedy starý přesně 3 týdny.

PŘÍKLAD Č. 2

Teď se podíváme na datum Velikonoc z opačného úhlu pohledu. Pokusíme se zjistit, v jakém roce se slavily Velikonoce přesně 22. března.

Jelikož se jedná o první možný den intervalu, ve kterém lze Velikonoce slavit, musí být součet d + e = 0.

Musí tedy platit následující rovnice:

- (19a + M) mod 30 = 0
- (2b + 4c + N) mod 7 = 0

Nejprve se podíváme na první rovnici. Proměnná a může dosahovat pouze celočíselných hodnot od 0 do 18. Po odečtení čísla M zjišťujeme, že 19a mod 30 = 30 – M. Hodnoty M mohou od roku 1582 dosahovat 22 až 24. Řešíme tedy tyto 3 případy:

- 19a mod 30 = 8
- 19a mod 30 = 7
- 19a mod 30 = 6

Musíme ověřit tuto množinu násobků: {19 · 2; 19 · 12; 19 · 3; 19 · 13; 19 · 4; 19 · 14}. Ověření provedeme dosazením. Zjišťujeme, že podmínku splňují násobky 19 · 2 a 19 · 13. Dostáváme tedy dvojici a = 2, M = 22 nebo a = 13, M = 23. Budeme se tedy pohybovat mezi roky 1582 a 1899. Díky tomu N ∈ {2; 3; 4}.

Teď se podíváme na všechny rovnice s proměnnou e podle konkrétní hodnoty N.

- (2b + 4c + 2) mod 7 = 0; (2b + 4c + 3) mod 7 = 0; (2b + 4c + 4) mod 7 = 0

Provedeme úpravu:

- (2b + 4c) mod 7 = 5; (2b + 4c) mod 7 = 4; (2b + 4c) mod 7 = 3

O hodnotách b, c víme: b ∈ {0; 1; 2; 3}; c ∈ {0; 1; 2; 3; 4; 5; 6}. Jelikož se jedná o velký počet kombinací, podíváme se pouze na několik možností. Začneme s hodnotou c = 0. Ve výsledku to tedy znamená, že náš hledaný rok bude dělitelný 7. Teď dosadíme do rovnice

postupně všechny hodnoty b. Pouze pro hodnotu b = 2 je jedna z rovnic pravdivá, konkrétně prostřední rovnice. Tím dostáváme také hodnotu N = 3. Můžeme tedy zahodit dvojici a = 2, M = 22, neboť N je rovné dvěma pouze v letech, kdy M = 23. Náš rok budeme hledat pouze v intervalu od roku 1700 do roku 1799.

Dostáváme se k poslednímu kroku. Potřebujeme vyřešit tuto soustavu tří rovnic o jedné neznámé:

- R mod 19 = 13
- R mod 4 = 2
- R mod 7 = 0

Hledáme sudé roky, které nejsou dělitelné 4, po dělení 19 dávají zbytek 13 a jsou dělitelné 7 beze zbytku. Žádný takový rok těmto kritériím nevyhovuje. Budeme tedy muset v hodnotách b, c hledat dál. Jak již bylo řečeno, těchto možností spousta, přeskočíme tedy rovnou k vyhovující dvojici. Zvolíme c = 1 a z rovnice (2b + 4c) mod 7 = 3 získáváme b = 3. Hodnota N se rovná 4. Interval potenciálně vyhovujících let připadá mezi roky 1800 a 1899.

Dostáváme opět soustavu tří rovnic o jedné neznámé:

- R mod 19 = 13
- R mod 4 = 1
- R mod 7 = 3

Konečně se dostáváme k výsledku. Tuto podmínku splňuje rok 1837. Znamená to tedy, že v roce 1837 se slavily Velikonoce 22. března.

UPLATNĚNÍ VE ŠKOLE

Aplikace algoritmu na základní škole může být zajímavým zpestřením hodiny matematiky. Každé dítě si tak může vypočítat datum Velikonoc pro jimi zvolený rok. Naučí se tak pracovat s algoritmy, získají kulturní přesah a aplikují matematickou operaci modulo.

Druhý příklad už je složitější. Než na základní školu, se hodí spíše na střední školu. Studenti se tak v příkladu naučí využívat algoritmus opačným směrem. Dojde k rozvíjení kritického myšlení a kompetencí k řešení problému.

KONGRUENCE

V této kapitole se zaměříme na kongruenci celých čísel a její základní vlastnosti. Následně se podíváme na její využití v praxi.

Definice 1: Mějme dvě celá čísla a, b. Číslo a je kongruentní s b podle modulu m, kde m je přirozené číslo větší než 1, právě tehdy, když platí $m|a - b$.

Tuto kongruenci značíme $a \equiv b \pmod{m}$. Pro názornou ukázku zapíšeme kongruencí výraz 12:5. Víme, že zbytkem po dělení bude číslo 2. Proto tedy $5|12 - 2$. Tento vztah přepíšeme do tvaru $12 \equiv 2 \pmod{5}$.

VLASTNOSTI

Víme, že pro každé celé číslo m platí vztah $m|0$. Pokud si 0 přepíšeme jako $a - a$ dostaneme tvrzení $m|a - a$. Z definice pojmu kongruence tedy platí vztah $a \equiv a \pmod{m}$.

Mějme následující tvrzení o dělitelnosti celých čísel: pokud $m|a - b$, potom $m|b - a$. Toto tvrzení můžeme aplikovat i na kongruenci. Pokud $a \equiv b \pmod{m}$, potom $b \equiv a \pmod{m}$.

Mějme $a \equiv b \pmod{m}$ a také $b \equiv c \pmod{m}$. Zapíšeme tyto kongruence vztahem dělitelnosti. Platí tedy $m|a - b$, a zároveň $m|b - c$. Z vlastnosti dělitelnosti celých čísel bude také platit vztah $m|(a - b) + (b - c)$, což je po úpravě ekvivalentní s výrazem $m|a - c$. Pokud tedy $(a \equiv b \pmod{m} \wedge b \equiv c \pmod{m})$, potom $a \equiv c \pmod{m}$.

ZBYTKOVÉ TŘÍDY

Kongruence modulo m rozděluje množinu celých čísel na tzv. zbytkové třídy. Ty se označují písmenem Z_x, kde celé číslo x je konkrétní označení této třídy. Celkový počet těchto tříd je přesně m a index x začíná od 0 až do $m - 1$. Ve zbytkové třídě Z_0 budou všechna čísla, která jsou dělitelná m. V ostatních třídách Z_x jsou potom tedy všechna čísla, která dávají po dělení číslem m zbytek x.

Pro ukázku si vypíšeme zbytkové třídy modulo 4.

$Z_0 = \{..., -12, -8, -4, 0, 4, 8, 12...\}$

$Z_1 = \{..., -11, -7, -3, 1, 5, 9, 13...\}$

$Z_2 = \{..., -10, -6, -2, 2, 6, 10, 14...\}$

$Z_3 = \{..., -9, -5, -1, 3, 7, 11, 15...\}$

Vybereme z každé této třídy právě jedno číslo a utvoříme z těchto vybraných čísel množinu. Tuto množinu nazveme úplnou soustavou zbytků podle modulu m. (dále jen ÚSZ). Např. ÚSZ modulu 4 může být {8, 1, 6, –9}

Speciální množinu ÚSZ = {0, 1, …, m – 1} pak nazýváme fundamentální úplnou soustavou zbytků (dále jen FÚSZ).

Operace s kongruencí

Mějme libovolná celá čísla a, b, c. Dále přirozené číslo m > 1. Potom platí následující implikace:

- $a \equiv b \pmod m \Rightarrow a + c \equiv b + c \pmod m$
- $a \equiv b \pmod m \Rightarrow a \cdot c \equiv b \cdot c \pmod m$

Mějme libovolná celá čísla a, b, c, d. Dále celé číslo m > 1.

- $(a \equiv b \pmod m \wedge c \equiv d \pmod m) \Rightarrow a + c \equiv b + d \pmod m$ (věta o sčítání kongruencí)
- $(a \equiv b \pmod m \wedge c \equiv d \pmod m) \Rightarrow a \cdot c \equiv b \cdot d \pmod m$ (věta o násobení kongruencí)

Všechna tato tvrzení platí pro 2 ale i více kongruencí.

Pokud ve větě o násobení položíme a = c, b = d, dostaneme větu o umocnění kongruence:

$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$, kde n je přirozené číslo

Využití kongruence

Jedním z využití kongruence je počítání zbytků po dělení u čísel, jejichž hodnoty vysoko přesahují limity našich kalkulátorů.

Příklad č. 1: pomocí vlastností kongruence celých čísel spočítejte zbytek po dělení čísla 12^{144} číslem 65.

Nejprve si vyjádříme nejmenší mocninu 12, která je větší než 65 a provedeme kongruenci.

$$12^2 \equiv 144$$

$$12^2 \equiv 14 \pmod{65}$$

Budeme pokračovat v umocňování kongruence. Našim cílem je se dostat umocňováním až na exponent 144.

$$12^4 \equiv 14^2 \pmod{65} \Rightarrow 12^4 \equiv 1 \pmod{65}$$

Nyní jsme dostali jako výsledek kongruence číslo 1. Umocňování pravé strany teď bude jednoduché, neboť jakákoliv mocnina čísla 1 je vždy 1. Pokračujeme v umocňování:

$$(12^4)^{36} \equiv 1^{36} \pmod{65} \Rightarrow 12^{144} \equiv 1 \pmod{65}$$

Číslo 12^{144} dává po dělení číslem 65 zbytek 1.

Pokud nemůžeme najít takovou mocninu, pro kterou se kongruence modulo m rovná 1, potom se pokusíme rozdělit mocninu na součet mocnin čísla 2. Např. 312^{15} bychom rozložili jako $312^{1+2+4+8}$. Poté bychom spočítali čtyři různé kongruence pro čísla 312, 312^2, 312^4 a 312^8. Tyto čtyři kongruence mezi sebou pak jen vynásobíme a získáme hledaný zbytek po dělení modulo m.

Pokud bychom chtěli vypočítat např. zbytek, který dostaneme, když vydělíme číslo ($312^{15} + 120^{13} \cdot 95^9$) číslem 28, rozdělíme si celý příklad na menší příklady. Vypočítáme kongruenci modulo 28 u čísel 312^{15}, 120^{13} a 95^9 samostatně. Vynásobíme výsledky kongruence čísel 120^{13} a 95^9, přičteme výsledek kongruence čísla 312^{15}. Dostáváme náš hledaný výsledek.

Na závěr se ještě podíváme na věty o krácení. Mějme celá čísla a, b, c. Také mějme přirozené číslo m větší než 1. Potom platí následující implikace.

- $a + c \equiv b + c \pmod{m} \Rightarrow a \equiv b \pmod{m}$

Nyní přidáme kromě proměnných a, b, c, m ještě výraz D(m, c), který reprezentuje největší společný dělitel čísel m a c. Pokud je výraz D(m, c) roven jedné, pak platí následující věta.

- $a \cdot c \equiv b \cdot c \pmod{m} \Rightarrow a \equiv b \pmod{m}$

Pokud je výraz D(m, c) větší než 1, potom můžeme zjednodušit výraz $(m:d) \mid (a - b) \cdot (c:d)$ na výraz $(m:d) \mid (a - b)$, proto musíme předchozí větu upravit následovně:

- $a \cdot c \equiv b \cdot c \pmod{m} \Rightarrow a \equiv b \pmod{m:d}$

DIOFANTICKÉ ROVNICE

Definice 2: Diofantická rovnice je lineární neurčitá rovnice o dvou neznámých x, y. Tato rovnice je dána předpisem: $a \cdot x + b \cdot y = c$; přičemž koeficienty a, b, c jsou celá čísla a zároveň a, b nesmí být nula. Neznámé x, y, jsou též z množiny celých čísel.

Na začátek uvažujme, že rovnice má řešení x, y. Není pro nás důležité, kolik tyto neznámé přesně jsou. Víme ale určitě, že bude existovat přirozené číslo D, které bude největším společným dělitelem koeficientů a, b. Číslo D tedy dělí jako číslo a, tak i číslo b. Z toho vyplývá vztah $D|(a \cdot x + b \cdot y)$ a tím pádem i $D|c$, neboť se musí obě strany rovnice rovnat. Získali jsme nutnou podmínku, aby byla rovnice řešitelná. Největší společný dělitel čísel a, b musí dělit číslo c.

K nalezení všech řešení využijeme pravidel kongruence, vlastnosti dělitelnosti celých čísel a Euklidův algoritmus. Postup si ukážeme na následujícím příkladu.

Příklad č. 2: Najděte řešení rovnice $16x + 7y = 2$

Začneme Euklidovým algoritmem a nalezneme NSD(16,7)

$16 = 2 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

NSD(16,7) = 1

Ověříme nutnou podmínku řešitelnosti. NSD(16,7) dělí pravou stranu rovnice, můžeme tedy uvažovat o řešení. Teď se pokusíme postupovat zpětně v algoritmu. Vyjádříme si poslední číslo v algoritmu jako kombinaci čísel předešlých. Důležité pro nás budou násobné koeficienty u těchto čísel. Postup končí až bude číslo 1 vyjádřeno jako kombinace čísel 16 a 7.

$1 = 1 \cdot 7 – 3 \cdot 2$

Další číslo v pořadí bude 2.

$2 = 16 – 2 \cdot 7$, a proto $1 = 1 \cdot 7 – 3 \cdot (16 – 2 \cdot 7)$

$1 = 1 \cdot 7 – 3 \cdot 16 + 6 \cdot 7 = 7 \cdot 7 – 3 \cdot 16$

Víme tedy, že s koeficienty 7 a –3 jsme schopni vytvořit číslo 1. Pravá strana má ale hodnotu 2. Proto vynásobíme oba koeficienty dvěma. Bude tedy platit vztah $14 \cdot 7 – 6 \cdot 16 = 2$. Jedním z hledaných řešení je kombinace $x = –6$, $y = 14$.

Z postupu tedy plyne, že pro nesoudělná čísla a, b vždy existují celá čísla x, y taková, že platí vztah $a \cdot x + b \cdot y = 1$

Vynásobením jsme schopni docílit výsledku i pro jinou pravou stranu než jedna. Pokud ovšem existuje celé číslo $D = NSD(a, b) \wedge D > 1$, pak existují celá čísla x,y pro které platí následující rovnice: $a \cdot x + b \cdot y = D$.

Nyní nalezneme ostatní řešení. Využijeme předchozích poznatků a budeme předpokládat, že existuje ještě jiné řešení $x´$ a $y´$. Stejně jako naše první řešení musí splňovat rovnici $(a:D) \cdot x + (b:D) \cdot y = c:D$, tak i všechna další budou tuto rovnici splňovat. Pokud bychom tedy tyto dvě rovnice odečetli, výsledek musí být nulový:

$(a:D) \cdot (x – x´) + (b:D) \cdot (y – y´) = 0$

Po úpravě rovnice získáme parametrické vyjádření všech ostatních řešení. Všechna tato řešení se budou lišit o parametr $t \in Z$:

$x´ = x + (b:D) \cdot t$

$y´ = y – (a:D) \cdot t$

Pokud tedy nejsou v příkladu omezeny hodnoty x, y na menší definiční obor než celá čísla, potom je počet řešení nekonečný. Výsledek z našeho příkladu zapsán parametricky bude pak vypadat následovně:

$x´ = –6 + 7t$

$y´ = 14 – 16t$

Pro $t = 0$ dostaneme prvotní řešení, pro $t = 1$ bude $x = 1$, $y = –2$, pro $t = 2$ bude $x = 8$, $y = 18$ atd…

LINEÁRNÍ KONGRUENCE O JEDNÉ NEZNÁMÉ

Definice 3: Mějme čísla a, b $\in$ Z, m $\in$ N, m > 1. Lineární kongruencí o jedné neznámé označíme rovnici ve tvaru $a \cdot x + b \equiv 0 \pmod{m}$. Přičemž číslo a nesmí být dělitelné číslem m.

Vraťme se zpět k pojmům fundamentální úplná soustava zbytků FÚSZ a úplná soustava zbytků ÚSZ. Pokud bude mít lineární kongruence o jedné neznámé nějaké řešení, zajímá nás toto řešení obsažené právě v těchto dvou soustavách.

Počet řešení závisí na NSD(a, m) a také jeho vztahu k číslu b. Vycházejme ze základní rovnice lineární kongruence o jedné neznámé.

$a \cdot x + b \equiv 0 \pmod{m}$

- Za předpokladu, že NSD(a, m) = d, d > 0 a zároveň číslo d nedělí b, kongruence nemá řešení v FÚSZ, a tím pádem nemá řešení ani v ÚSZ.
- Za předpokladu, že NSD(a, m) = 1, potom má kongruence právě jedno řešení v FÚSZ, a tím pádem i jedno řešení v jakékoliv ÚSZ.
- A nakonec pokud platí NSD(a, m) = d, d > 0 a zároveň $d \mid b$, pak má kongruence v FÚSZ právě d řešení a tím pádem i řešení v libovolné ÚSZ.

Všechna řešení lze zapsat ve tvaru $x = x' + (m:d) \cdot t$. Je nutné ale napřed nalézt všechna různá nekongruentní řešení. Tím dosáhneme omezením hodnot t = 0, 1, 2, …, d – 1.

Pro vyřešení lineární kongruence o jedné neznámé lze využít dva postupy. Metodu tabulkového zápisu a řešení kongruence jako rovnice, pro kterou budeme dodržovat pravidla kongruence.

Příklad č. 3: Řešte lineární kongruenci $2x + 4 \equiv 0 \pmod{8}$ tabulkovou metodou

NSD(2, 8) = $2 \wedge 2 \mid 4$, rovnice bude mít v FÚSZ tedy 2 řešení.

Vytvoříme si tabulku o třech řádcích. V prvním budou všechny hodnoty, kterých může nabývat proměnná x. V druhém vypočítáme odpovídající hodnotu rovnice pro dané x. V posledním řádku provedeme operaci modulo m, a budeme zde hledat případ, ve kterém je modulo m rovno nule.

x	0	1	2	3	4	5	6	7
2x + 4	4	6	8	10	12	14	16	18
2x + 4 (mod 8)	4	6	0	2	4	6	0	2

(tabulka č. 2 – řešení příkladu č. 3)

Pro hodnoty x = 2, x = 6 vychází 2x + 4 (mod 8) = 0. V FÚSZ bude mít tedy rovnice dvě řešení $x_1 = 2$, $x_2 = 6$.

Všechna řešení pak zapíšeme ve tvaru $x = 2 + 4t$, $t \in N$

Teď vyřešíme ten samý příklad, ale budeme s kongruencí pracovat jako s rovnicí řídící se pravidly kongruence.

$2x + 4 \equiv 0 \pmod 8$

Přepíšeme číslo 4 na druhou stranu rovnice.

$2x \equiv -4 \pmod 8$

Využijeme zbytkovou třídu, do které patří číslo –4 modulo 8, a upravíme pravou stranu rovnice následovně:

$2x \equiv 4 \pmod 8$

NSD(2, 4) = 2 a zároveň $2 \mid 8$. Zkrátíme tedy rovnici dvěma, ale nesmíme zapomenout zkrátit i (mod 8). Využili jsme větu: $a \cdot c \equiv b \cdot c \pmod m \Rightarrow a \equiv b \pmod{m:d}$.

$x \equiv 2 \pmod 4$

Všechna řešení zapíšeme ve tvaru $x = 2 + 4t$, $t \in N$. K nalezení všech řešení v FÚSZ dosadíme za t = 0, 1 a tak dostáváme dvě řešení $x_1 = 2$, $x_2 = 6$.

POKROČILEJŠÍ PROBLÉMY A VZORCE

EULEROVA FUNKCE

Definice 3: Eulerova funkce $\varphi(m)$ je taková funkce, která nenulovému přirozenému číslu m přiřadí nenulové přirozené číslo x. Hodnota čísla x je rovna počtu všech přirozených čísel menších než m, která jsou s číslem m nesoudělné.

Pro představu např. $\varphi(6) = 2$ neboť podmínku splňuje množina {1, 5}.

VLASTNOSTI FUNKCE

Pro výpočet této funkce budeme potřebovat znát několik vlastností.

1. $\varphi(1) = 1$
2. $\varphi(p) = p - 1$, kde p je prvočíslem
3. $\varphi(p^k) = p^{(k-1)} \cdot (p - 1)$, kde p je opět prvočíslem, k je kladnou mocninou prvočísla p.
4. $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$, pokud jsou čísla m_1, m_2 nesoudělná.

Pro výpočet budeme potřebovat, aby byly čísla m_1 a m_2 nesoudělná. Dvojice různých prvočísel bude tuto vlastnost splňovat vždy. Pokud tedy číslo m není prvočíslem, provedeme jeho rozklad na prvočísla a využijeme 4. vlastnosti Eulerovy funkce. Následně použijeme 2. a 3. vlastnosti k finálnímu výpočtu.

Příklad č. 4: Vypočítejte $\varphi(1260)$.

1. Přepíšeme číslo 1260 jako součin prvočísel $2^2 \cdot 3^2 \cdot 5 \cdot 7$
2. Využijeme 4. vlastnosti: $\varphi(1260) = \varphi(2^2) \cdot \varphi(3^2) \cdot \varphi(5) \cdot \varphi(7)$
3. S pomocí ostatních vlastností dostáváme: $\varphi(1260) = 2 \cdot (2-1) \cdot 3 \cdot (3-1) \cdot (5-1) \cdot (7-1)$
4. Roznásobíme celý výraz: $\varphi(1260) = 2 \cdot 6 \cdot 4 \cdot 6 = 288$, což je náš hledaný výsledek.

REDUKOVANÁ SOUSTAVA ZBYTKŮ

Redukovaná soustava zbytků (RSZ) podle modulu m je množina přirozených čísel splňující dvě vlastnosti:

- Všechna čísla množiny jsou spolu nekongruentní podle modulu m
- Všechna čísla množiny jsou také zároveň nesoudělná s modulem m

Z vlastností vyplývá, že počet čísel množiny RSZ bude přímo odpovídat hodnotě Eulerovy

funkce.

Mějme množinu čísel M = {1, 2, 3, 4, 5, 6, 7, 8}. Upravíme množinu tak, aby splňovala vlastnosti redukované soustavy zbytků modulo 6. Napřed odstraníme všechna soudělná čísla s modulem 6. Množina M tedy bude vypadat takto: {1, 5, 7}. Teď odstraníme všechna kongruentní čísla. V množině tedy zůstanou pouze čísla 1 a 5. Jak jsme již zjistili $\varphi(6) = 2$, což odpovídá i počtu prvků v redukované množině M.

Pokud vynásobíme všechny prvky RSZ přirozeným číslem a, které je nesoudělné s modulem m, nově vzniklá množina bude také RSZ.

Vynásobíme šesti množinu M = {1, 5}, dostáváme novou množinu M' = {11, 55}. $11 \equiv 5 \pmod 6$. $55 \equiv 1 \pmod 6$. Vidíme, že nová množina je plně kongruentní s původní množinou. Proto i množina M' je RSZ podle modulu 6.

Eulerova věta

Označíme si prvky množiny RSZ jako $x_1, x_2, ..., x_{\varphi(m)}$. Pokud všechny prvky vynásobíme číslem a nesoudělným s modulem m, dostaneme soustavu kongruencí:

$$a \cdot x_1 \equiv x_1'; a \cdot x_2 \equiv x_2'; \dots ; a \cdot x_{\varphi(m)} \equiv x_{\varphi(m)}' \pmod m$$

Vynásobíme všechny kongruence a dostáváme rovnici:

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdot \dots \cdot x_{\varphi(m)} \equiv x_1' \cdot x_2' \cdot \dots \cdot x_{\varphi(m)}' \pmod m$$

V kongruenci modulo m jsou součiny čárkovaných a nečárkovaných čísel x totožné. Nahradíme je tedy číslem c. Dostáváme výraz $a^{\varphi(m)} \cdot c \equiv c \pmod m$. Protože jsou čísla c, m nesoudělná, zjednodušíme celý výraz: $a^{\varphi(m)} \equiv 1 \pmod m$. Tato odvozená kongruence se označuje jako Eulerova věta.

Definice 4: Jestliže je číslo a nesoudělné s modulem m, potom platí následující kongruence:

$a^{\varphi(m)} \equiv 1 \pmod m$, kde $\varphi(m)$ je Eulerovou funkcí.

Malá věta Fermatova

Malá věta Fermatova vychází z Eulerovy věty $a^{\varphi(m)} \equiv 1 \pmod m$, pokud za číslo m dosadíme prvočíslo.

Definice 5: Mějme prvočíslo p, které zároveň nedělí číslo a. Pak platí následující kongruence:

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

Funkce $\Theta(n)$ a $\sigma(n)$

Definice 6: $\Theta(n)$ je funkce, která přirozenému číslu n přiřadí počet všech přirozených dělitelů čísla n.

Pro ukázku si vypíšeme všechny dělitele čísla 20. Těmi jsou čísla 1, 2, 4, 5, 10 a 20, což dává celkový počet šesti čísel. Dostáváme tedy $\Theta(20) = 6$.

Definice 7: σ(n) je funkce, která pro přirozené číslo n vrací přirozené číslo, které udává součet všech dělitelů čísla n.

Spočítáme σ(20). Všechny dělitele čísla 20 jsme si již vypsali. Provedeme jejich součet. 1 + 2 + 4 + 5 + 10 + 20 = 42. Z toho vyplývá σ(20) = 42.

Pro malá čísla lze hodnotu obou funkcí spočítat pouhým výčtem dělitelů, jako jsme to udělali u čísla 20. Je ale jasné, že u větších čísel se tento způsob stane velice pracným a obtížným. Proto potřebujeme najít obecnou metodu pro výpočet $\Theta(n)$ a σ(n).

Pro odvození si spočítáme dělitele čísla 32. Rozložením na prvočísla zjistíme, že $32 = 2^5$. Přirozenými děliteli 32 jsou tedy všechna čísla ve tvaru 2^x, kde x je přirozeným číslem od 0 do 5 ($2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 8$; $2^4 = 16$; $2^5 = 32$). Je tedy jasné, že $\Theta(32) = \Theta(2^5) = 1 + 5 = 6$. Součet je pak vyjádřen jako $1 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5$. Místo umocnění a mechanického součtu se ale na sčítance podíváme jako na geometrickou řadu s kvocientem q = 2. Využijeme vzorec pro výpočet n–tého členu geometrické řady $\frac{q^n - 1}{q - 1}$. Jelikož exponent číslujeme již od 0, dosadíme za n = 6, a tak $\sigma(20) = (2^6 - 1) : (2 - 1) = 63$.

Některá čísla ale nelze rozložit na mocninu pouze jednoho přirozeného čísla. Podíváme se tedy na výpočet théta a sigma funkce u čísla 72. Nejprve číslo rozložíme na součin prvočísel. $72 = 2^3 \cdot 3^2$. Opět si vyjádříme všechny dělitele jako 2^x a 3^y, kde x náleží intervalu od 0 do 3, y náleží intervalu od 0 do 2. Zvolíme y = 0 a dostaneme 4 dělitele, konkrétně $3^0 \cdot 2^0$, $3^0 \cdot 2^1$, $3^0 \cdot 2^2$, $3^0 \cdot 2^3$. Pro y = 1 opět 4 dělitele, a nakonec pro y = 2 také 4 dělitele. Z toho snadno posoudíme, že celkový počet dělitelů čísla 72 je 4 + 4 + 4 = 12. Tento poznatek

přetvoříme do vzorečku. Nesmíme ale zapomenout, že exponent počítáme od 0. $\Theta(72) = \Theta(2^3 \cdot 3^2) = (1 + 3) \cdot (1 + 2) = 4 \cdot 3 = 12$. Obecně tedy získáme vztah, kdy lze vypočítat $\Theta(n)$ jako součin nejvyšších mocnin všech přirozených čísel, která dostaneme prvočíselným rozkladem čísla n, ale zvýšených o 1. Pro funkci σ(72) opět využijeme vzorec pro geometrickou řadu. $\frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} = 15 \cdot 13 = 195 = \sigma(72)$. Pokud tedy zobecníme postup pro výpočet σ(n), provedeme rozklad čísla n na prvočísla. U každého prvočísla spočítáme součet geometrické řady tvořenou jeho mocninami. A nakonec tyto součty vynásobíme.

Pokud za číslo n dosadíme přirozené číslo p, je očividné, že σ(p) = p + 1, a také $\Theta(p) = 2$.

Podle hodnoty sigma funkce lze každé přirozené číslo rozdělit do třech kategorií:

- σ(n) < 2n, těchto přirozených čísel existuje nekonečně mnoho
- σ(n) > 2n, i těchto přirozených čísel je nekonečný počet
- σ(n) = 2n, tato čísla jsou výjimečná, nevíme, zda je jejich počet konečný či nikoliv

DOKONALÁ ČÍSLA

Označme si všechna přirozená čísla n, pro něž platí σ(n) = 2n, jako čísla dokonalá. Jedním z těchto čísel je např. 6, pro které platí σ(n) = 1 + 2 + 3 + 6 = 12 = 2 · 6. Dalším příkladem je 28, neboť opět platí σ(n) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 · 28.

Jak zjistit, zda je dané číslo dokonalé, aniž bychom potřebovali vždy spočítat jeho odpovídající sigma funkci? O to se pokoušel už samotný Euklides ve svém díle Základy. Nakonec přišel s postačující podmínkou, u které o dvě milénia později dokázal L. Euler, že je zároveň nutnou podmínkou. Tato podmínka říká: Aby sudé číslo bylo dokonalým, musí jít zapsat ve tvaru $2^{n-1}(2^n-1)$ a zároveň aby číslo (2^n-1) bylo prvočíslem. Například již zmíněné dokonalé číslo 6 lze zapsat ve tvaru $2^{2-1}(2^2-1) = 2 \cdot 3$. Číslo 28 potom ve tvaru $2^{3-1}(2^3-1) = 4 \cdot 7$.

Důkladnějším průzkumem bylo zjištěno, že prvočíselná podmínka je sice nutná, ale není dostačující. Tento argument potvrzuje následující příklad: $2^{11} - 1 = 2047 = 23 \cdot 89$.

Nebudeme se teď ale zabývat čísly, která podmínku porušují. Pojďme se podívat na čísla, které podmínku splňují. Takovým číslům se věnoval matematik Marin Mersenne. A tak se dnes označují výrazem M_n všechna přirozená čísla ve tvaru $2^n - 1$, která jsou zároveň

prvočísly. Během historie postupně došlo k objevování několika těchto čísel a jejich počet tedy postupně rostl. Se zvyšujícím se exponentem n ale roste i obtížnost kontroly, zda je daný výraz prvočíslem. Než nastoupily na scénu počítače, zůstalo největším objeveným Mersennovým číslem po dobu více jak polovinu století číslo M_{127}. Počítací stroje pak začaly používat speciálně naprogramované algoritmy pro ověření, zda je dané číslo prvočíslem, a při tom zvládly pracovat efektivněji než nejlepší a nejrychlejší matematici světa.

Dodnes je oficiální počet známých Mersennových čísel 48, ale můžeme předpokládat, že se jejich počet bude v budoucnu kvůli zlepšující se technice zvyšovat. Posledním tímto číslem je ($2^{57885161}$–1), které má celkem 17 425 170 cifer [8, cit. 14.5.2023].

VELKÁ VĚTA FERMATOVA

ZNĚNÍ

Mějme celá čísla x, y, z, n, kde n > 2, potom rovnice $x^n + y^n = z^n$ nemá žádné kladné celočíselné řešení. [9, str. 43, cit. 23.3.2023].

Takto zní úryvek myšlenky, kterou její stvořitel Pierre de Fermat zaznamenal na okraj své knihy v 17. století. V té době jistě netušil. že potrápí v následujících staletích nejednoho matematika. Na první pohled se může tato formulace zdát velmi krátkou a jednoduchou. Důkaz její pravdivosti ale lidstvo hledalo po více než 300 let. Teprve v roce 1994 geniální matematik Andrew Wiles definitivně potvrdil její pravdivost.

Proč je ale toto tvrzení pro svět matematiky tak důležité? Čím je přesně tato věta zajímavější než jiné matematické věty? A je objevení důkazu skutečně tak obrovským úspěchem?

Pro zodpovězení těchto otázek se budeme muset podívat hluboko do historie.

PYTHAGORAS

V 6. století př. n. l. se na světové scéně objevil Pythagoras ze Samu. Je jasné, že tento obrovský časový skok do minulosti znamená, že si nemůžeme být jisti vším co o něm víme, neboť některé informace mohou být pouze legendou a mýtem. Přesto se tento člověk stal jednou z nejinspirativnějších postav matematiky.

Víme, že svého vzdělání dosáhl cestováním po celém známém světě. Nejvíce ho ale fascinovali Egypťané a Babyloňané svým přístupem k řešení problémů. Ti vyjádřili každý výpočet ve tvaru předpisu. Ten potom stačilo pouze krok po kroku následovat. Proto pro další generace nikdy nebylo nutné hledat znovu ty samé odpovědi. Nikdo se ale nezabýval tím, jaké myšlenky se za těmito předpisy skrývají. V té době ani Pythagora moc nezajímala odpověď na otázku proč.

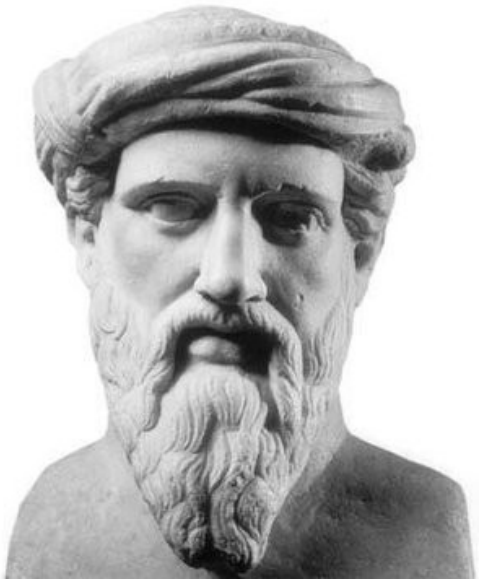
Poté co v Řecku objevil dlouho vyhledávaného mecenáše jménem Milos, získal dostatek finančních prostředků založit si svoji vlastní školu, které říkal Bratrstvo. [9, str. 25, cit. 26.3.2023]. Každý z této školy složil přísahu, že nevyzradí žádný z objevů lidem z venčí. A tak spoustu vědomostí zůstalo v naprosté izolaci kruhu Bratrstva. Víme ale, že se v té

době změnilo Pythagorovo chápání matematiky. Jeho škola byla velmi úzce spojena s náboženstvím. Jeho členové začali věřit, že porozuměním vztahům mezi čísly odhalí tajemství vesmíru a dostanou se tak blíže bohům. Nově dochází ke studiu racionálních čísel ve zlomkovém tvaru. Jedním z dalších okruhů čísel, která školu zajímala byla například i dokonalá čísla již zmíněná v předchozí kapitole.

Kromě vztahů mezi čísly začaly Pythagora zajímat i souvislosti čísel s okolním světem. Začal si uvědomovat, že jsou některé jevy řízeny přírodními zákony, které se dají sepsat do matematických rovnic. Jedním z prvních jeho objevů byl vztah mezi harmonií v hudbě a harmonií mezi čísly. [9, str. 29, cit. 26.3.2023].

A pak se to stalo. Bratrstvo objevilo větu nesoucí jméno zakladatele tohoto spolku. Pythagorova věta se brzy stala slavnou a svoji slávu přestála až do dnešní doby, kdy se o ní učí děti ve škole. Přitom její matematický i geometrický význam je jednoduchý. V pravém trojúhelníku je druhá mocnina délky přepony rovna součtu druhých mocnin obou odvěsen. [9, str. 33, cit. 26.3.2023]. Tento vztah se dá také zapsat jako $x^2 + y^2 = z^2$, kde x, y reprezentují velikost odvěsen a z velikost přepony. Přestože tato věta byla známá již dříve, byl to právě Pythagoras, který dokázal její platnost pro všechny pravoúhlé trojúhelníky.

Pythagorova věta je zásadní pro další rozvoj problematiky i pro vznik samotné Fermatovy věty.



(obrázek č. 1 – Pythagorova busta)

PYTHAGOREJSKÉ TROJICE

Pythagorejskou trojicí označíme celá čísla a, b, c, která splňují Pythagorovu větu. Nejmenší takovou trojicí jsou čísla 3, 4, 5. Podívejme se, co se stane s rovnicí, pokud do ní dosadíme dvojnásobky těchto hodnot. $6^2+8^2=10^2$. I tato trojice splňuje Pythagorovu větu. Znamená to tedy, že jsme schopni vygenerovat jakékoliv množství řešení pouze z jedné trojice. Geometricky by byly všechny trojúhelníky generované těmito trojicemi podobné. V praxi i ve škole je ale důležité nepoužívat pořád s podobnými trojúhelníky. A proto všechny takové trojice, které nejsou násobkem žádné jiné nazveme primitivními, či základními. Jak tyto trojice ale vytvoříme? Na jeden z algoritmů se nyní podíváme.

Přepíšeme si Pythagorovu větu do tvaru $c^2-a^2=b^2$. Podle vzorce upravíme rovnici do tvaru: $(c - a) \cdot (c + a) = b^2$. Jelikož jsou všechny celá čísla větší než 0, vydělíme rovnici číslem b, zároveň rovnici vydělíme výrazem (c – a). Rovnice bude vypadat následovně:

$$\frac{c+a}{b}=\frac{b}{c-a}$$

Označíme si levou stranu jako podíl dvou nenulových celých čísel $\frac{m}{n}$. Jelikož se obě strany rovnice musí rovnat, potom i pravá strana rovnice musí být rovna $\frac{m}{n}$. Převrácením zlomku zjišťujeme, že zlomky $\frac{c+a}{b}$ a $\frac{b}{c-a}$ jsou také převrácené. Rozložíme tyto dva složené zlomky a položíme je rovné podílu čísel m, n. Dostáváme dvojici rovnic:

- $\frac{c}{b}+\frac{a}{b}=\frac{m}{n}$
- $\frac{c}{b}-\frac{a}{b}=\frac{n}{m}$

Pokusíme se vyřešit tuto soustavu dvou rovnic o dvou neznámých. Napřed eliminujeme výraz $\frac{a}{b}$ sčítací metodou:

- $\frac{c}{b}=\frac{1}{2}\left(\frac{m}{n}+\frac{n}{m}\right)=\frac{m^2+n^2}{2mn}$

Teď sčítací metodou eliminujeme výraz $\frac{c}{b}$:

- $\frac{a}{b}=\frac{1}{2}(\frac{m}{n}-\frac{n}{m})=\frac{m^2-n^2}{2mn}$

Dříve než se podíváme na jednotlivé koeficienty, pojďme se zaměřit na vlastnosti čísel a, b, c. Všechna tři čísla musí být navzájem nesoudělná. To znamená, že největší společný dělitel čísel a, b, c musí být číslo 1. Z toho také plyne, že každá dvě čísla musí být navzájem nesoudělná. Pokud bude číslo a liché, potom číslo b je sudé a opačně. Označme tedy číslo a jako liché, b jako sudé. Aby byla dodržena kongruence s číslem c, tedy rovnice měla řešení, potom musí být číslo c liché. Tyto vlastnosti jsou dobře vidět i na již uvedené trojici 3, 4, 5. Nyní přeneseme tyto vlastnosti na parametry m, n.

Aby byly dodrženy předem stanovené sudosti a lichosti čísel, jedno z čísel m, n musí být liché, zatímco druhé musí být sudé. Také platí vztah m > n. Podíváme se zpět do posledního kroku řešení soustavy rovnic. Z dvojice zlomků $\frac{c}{b}=\frac{m^2+n^2}{2mn}$ a $\frac{a}{b}=\frac{m^2-n^2}{2mn}$ vyjádříme čísla a, b, c:

- $a=m^2-n^2$
- $b=2mn$;
- $c=m^2+n^2$

Tento algoritmus pro hledání všech primitivních pythagorejských trojic, který je tvořen těmito třemi rovnicemi vymyslel Euklides. Pokud chceme najít i jiné než primitivní trojice, potom stačí všechny koeficienty a, b, c vynásobit stejnou celočíselnou kladnou konstantou.

Tyto tři rovnice lze odvodit i jiným způsobem, například přes umocnění komplexního čísla na čtverec, či přes jednotkovou kružnici.

VYUŽITÍ

Algoritmus pro hledání primitivních pythagorejských trojic se stane neocenitelným nástrojem, až nastoupím do školy jako pedagog. Lze ho využít nejen k tvorbě testů, ale také k vymýšlení nejrůznějších geometrických úloh na Pythagorovu větu a goniometrické funkce v pravoúhlém trojúhelníku.

Zobecnění pro vyšší mocniny

Jak čas ubíhal, začala se Pythagorova věta více zkoumat v pozměněném tvaru. Světové matematiky začalo zajímat, zda se najde i celočíselné řešení pro rovnici se třetími mocninami: $x^3 + y^3 = z^3$. Najít ale tři celá čísla, která by tuto rovnici splňovala, se zdálo nemožné. Neexistoval žádný matematický důkaz, že rovnice má nebo nemá řešení. Znamená to, že se úloha změnila ze snadné na nemožnou pouhým zvýšením mocniny o jedna. Pokud bychom ale mocniny zvyšovali dále, v hledání řešení si nijak nepomůžeme. Nalezení celých čísel splňující $x^n + y^n = z^n$ kde n je celé číslo větší než 2 tedy bylo za hranicí dobových znalostí. V 17. století ale francouzský matematik Pierre de Fermat způsobil překvapující zvrat. Prohlásil, že zatím nikdo nenašel žádné řešení, neboť žádné takové řešení neexistuje. [9, str. 42, cit. 28.3.2023]

Pierre de Fermat

Pierre de Fermat se narodil na samém začátku 17. století. Jeho otec byl vcelku zámožný, a tak se synovi dostalo dobrého vzdělání. Přestože ve svých 30 letech vstoupil do politiky, nijak zvlášť velké ambice v tomto odvětví neměl. Všechen svůj volný čas věnoval matematice. Ta se teprve postupně začala vracet do podvědomí veřejnosti z temných časů středověku. Tento přístup se snažil změnit Marin Mersenne, zmíněný v kapitole o Mersennových číslech. Na svých cestách přesvědčoval kolegy, aby své znalosti sdíleli s ostatními a spolupracovali na nových objevech. Nakonec se setkal s Pierrem de Fermat a stal se jediným člověkem, jehož prostřednictvím Fermat udržoval spojení s ostatními matematiky. I přes Mersennovo prosby se ale se světem nikdy nepodělil o své důkazy. Naopak se přímo vyžíval v tom, sdělovat někomu ze svých kolegů své objevy bez jejich důkazu. Následně je vyzval k tomu, aby důkaz jeho tvrzení našli. Nejspíš jediným, s kým si Fermat vyměňoval názory byl Blaise Pascal. Oba společně napsali první zákony teorie pravděpodobnosti.

I přes jeho dobrovolnou izolaci se ale některé jeho objevy dostaly do světa. Jmenujme například položení základů diferenciálního a integrálního počtu. Překvapivě ovlivnil ale i odvětví ekonomie a osvětlil problematiku inflace. Přesto jeho nejoblíbenější láskou byla teorie čísel. A právě zde navázal na práci antických matematiků, jakými byli Pythagoras, Euklides a další. Důvod, proč zmiňuji právě Euklida, je jeho nesporná důležitost v teorii

dělitelnosti. Zabýval se iracionálními čísly, což jsou taková čísla, která nelze zapsat ve zlomku v základním tvaru. Nejznámějšími iracionálními čísly jsou například π, $\sqrt{2}$ nebo Eulerovo číslo e. O práci těchto antických géniů se dozvěděl Fermat v Diofantově knize Aritmetika (Právě po Diofantovi jsou pojmenovány diofantické rovnice, které jsme v této práci také rozebírali). V této knize objevil spoustu problémů, které souvisely právě s Pythagorovou větou. Začal si hrát s variacemi věty. Druhou mocninu nahrazoval jiným číslem a hledat řešení. A tak se stalo, že v roce 1637 sepsal právě do svého výtisku Aritmetiky svůj objev. V tu dobu ještě netušil, že bude navždy označován jako Velká Fermatova věta. Také zde napsal, že důkaz tohoto tvrzení má, ale že je okraj stránky příliš malý, aby se tam vešel. Když o 30 let později zemřel, hrozilo, že všechny jeho objevy a zápisky přijdou vniveč. Naštěstí se nejstarší Fermatův syn Clément Samuel postaral o to, aby jeho odkaz pokračoval dál. Vydává knihu Diofantova Aritmetika doplněná o pozorování Pierra de Fermat. A tak mohl svět matematiky konečně spatřit problém, který ho bude trápit ještě po více než 300 let.

(obrázek č. 2 – Pierre de Fermat)

Pokusy o důkaz

Poté co byla Fermatova věta vypuštěna do světa, strhla se vlna zájmu. Správný matematik nebere pouhé slovo jako důkaz, i když bylo vyřčeno z úst Fermata. Bylo povinností důkaz objevit. Matematika jako exaktní věda nestaví své hypotézy na experimentech, ale na nesporně dokázaných tvrzení. Bez tohoto důkazu si nikdy nemůžete být jisti, co je pravdou, a co je pouze výmyslem. Pokud bychom další a další poznatky stavěli na základech, které se nakonec ukážou jako mylné, důsledky mohou být katastrofální. Zatímco se ostatní Fermatova tvrzení ukázala být pravdivá, právě ona Velká věta zůstala pořád bez důkazu. Nespočet matematiků se tedy snažilo nalézt důkaz. Většina ale na své cestě přestala věřit ve své schopnosti a bádání ukončili. Ostatně nikdo nevěděl, zda tato cesta vůbec má nějaký cíl. Nikdo nechtěl zbytečně vynaložit svůj čas na dokázání něčeho, co nemusela být vůbec pravda.

Leonhard Euler

Jedním z těch, kteří se o důkaz pokusili a zaslouží si pozornost byl v 18. století Leonhard Euler. Využil své znalosti z dokazování pravidel grafů. Pokud by se mu povedlo dokázat tvrzení pro nejjednodušší případ $x^3 + y^3 = z^3$, možná by pak zvládl větu potvrdit postupným zobecňováním pro vyšší mocniny. Také se pokusil pracovat s Fermatovým náčrtem důkazu pro mocninu 4, což byla jediná pomůcka, kterou génius po sobě v tomto problému zanechal. Úpravou metody nekonečného sestupu tedy nakonec úspěšně dokázal tvrzení pro mocninu 3 a 4. Stal se po sto letech prvním člověkem, který dosáhl nějakého úspěchu. Při dokazování využil imaginárních čísel, vět z teorie dělitelnosti a odmocnin.

Krátce se podíváme, jak vlastně důkaz metodou nekonečného sestupu funguje. Zvolíme si vztah pro který chceme důkaz provést. V tomto případě se jedná o vztah $x^4 + y^4 = z^4$. Budeme uvažovat, že existuje přirozené číslo, pro které tento vztah platí. Stejně jako u Pythagorejských trojic, i zde musí existovat nejmenší přirozené číslo z, které rovnici splňuje. Pokud ale dokážeme, že existuje ještě menší přirozené číslo, které splňuje zadanou rovnost, můžeme tento proces dokazování opakovat nespočetněkrát. Dojde tedy ke sporu, a tudíž můžeme prohlásit, že neexistuje žádné přirozené číslo, které rovnici splňuje.

Ukažme si konkrétněji první krok důkazu. Přepíšeme si z^4 jako novou proměnnou ve tvaru Z^2. Potom tedy hledáme přirozená čísla, která splňují rovnici $x^4 + y^4 = Z^2$. Trojice čísel x^2, y^2, Z je pak určitě Pythagorejskou trojicí a lze ji přepsat dle algoritmu pro nalezení všech primitivních Pythagorejských trojic následovně:

- $y^2 = m^2 - n^2$
- $x^2 ¿ 2mn;$
- $Z = m^2 + n^2$

První rovnice je Pythagorovou větou. Zopakujeme tedy první krok a opět vytvoříme Pythagorejskou trojici y, m, n. Proměnné si znovu přepíšeme:

- $y = p^2 - q^2$
- $n ¿ 2pq;$
- $m = p^2 + q^2$

Pokud bychom pokračovali v úpravách a přepisu, došlo by k nekonečnému sestupu a tím pádem k důkazu Fermatovy věty pro n = 4.

Pokračování v dokazování

Přestože dokazování po Eulerově smrti postupovalo velmi pomalu, ve špatném stavu tento proces nebyl. Protože např. každé číslo osmé mocniny lze napsat také jako číslo 4. mocniny. Třeba 256 = 2^8 = 4^4. Každý důkaz pro 4 mocninu tedy zároveň platí pro libovolnou mocninu, která je násobkem čtyř. To samé se dá pak říct i o mocnině tří. Výhodou čísla 3 je ale jeho vlastnost prvočísla. Všechna ostatní čísla, která nejsou prvočísly se dají zapsat jako součin prvočísel. Tím jsme tedy schopni snížit počet rovnic, které potřebujeme ověřit. Je nutné si ale uvědomit, že přestože jsme spoustu případů eliminovali, celkový počet rovnic je stále nekonečno.

Počátkem 19. století se věta stala nejznámějším číselně teoretickým problémem. Na matematické scéně se objevila nová osoba. Byla to žena, a tak musela bojovat se spoustou předsudků a sociálních problémů. Tato Francouzka nesla jméno Sophie Germainová, ale tajně studovala pod mužským jménem jako pan Le Blanc. Poté co matematik Lagrange objevil její výjimečnost, trval na osobním setkání. Sophie musela s pravdou ven. Pravda ale matematika neodradila a stal se jejím učitelem a přítelem. Již

několik let se věnovala problému Fermatovy věty až nakonec učinila důležitý objev. Zaměřila se na prvočísla, která lze zapsat ve tvaru 2p + 1, kde p je také prvočíslem. Díky jejím metodám, které převzali kolegové, Fermatova věta platí pro mocniny 5 a 7.

1. března 1847 se konalo velice dramatické zasedání francouzské Akademie. Dva vysoce postavení matematikové zde oba prohlásili, že se dostávají ke kompletaci důkazu. Jedná se o Cauchyho a Lamého. Jejich soutěž ale zhatil německý kolega Ernst Kummer. Zjistil, že oba staví svůj důkaz na chybně pochopeném faktu. Sám se tedy pustil do dokazování. Při objevení chyby zavedl tzv. ideální čísla v kruhových tělesech. Nakonec v roce 1857 provedl obrovský skok vpřed, když dokázal Fermatovu větu pro mocniny n < 100 [10, str. 246, cit. 19.6.2023].

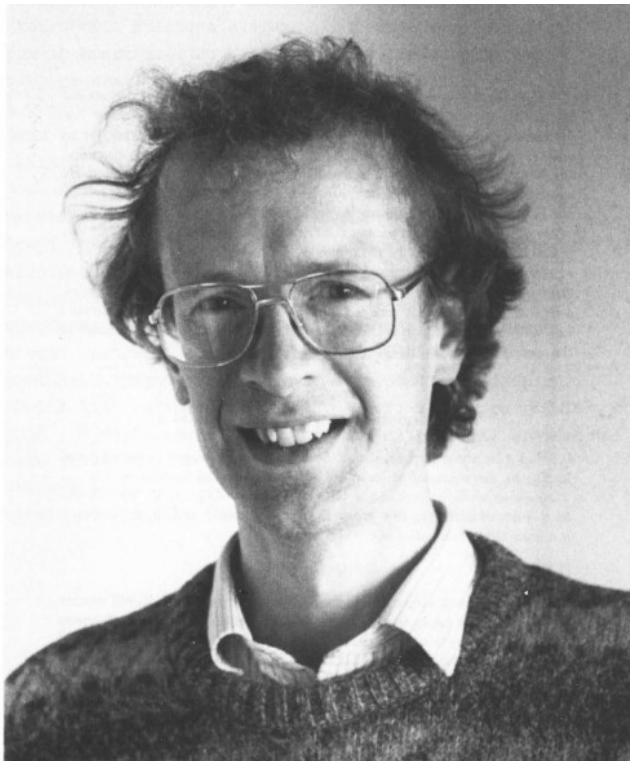
Vyhlášené odměny z několika zdrojů zvyšují všeobecnou motivaci, která se ale stává zároveň kontraproduktivní. Věta začala přitahovat spoustu zbytečně otravujících amatérů a podvodníků. Nejznámější odměnou byla soutěž, kterou odstartoval v r. 1908 Paul Wolfskehl. Po své smrti ve své závěti uvádí, že odkáže odměnu 100 000 marek tomu, kdo dokáže Velkou Fermatovu větu. Soutěž měla být platná až do roku 2007.

Během druhé světové války se zaměřili nejlepší matematici pracující v oboru teorie čísel na dešifrování a šifrování tajných zpráv. Dokazování Fermatovy věty v té době dosáhlo mocniny n < 619 díky matematikovi Vandiverovi. Na scénu přichází první stroje, které se po válce s každým rokem více a více zdokonalují. Počítače tak najednou zvládají spočítat za krátkou dobu více výpočtů než jeden matematik za celý život.

Zatím nejblíže se dostáváme k důkazu pro takzvané zvláštní případy. V nich nesmí být žádné z čísel x, y, z dělitelné prvočíselným exponentem n. Pro tyto případy se tak posouvá platnost Fermatovy věty až k exponentu n < 253 747 889 [10, str. 247, cit. 19.6.2023].

Naděje pro důkaz Velké Fermatovy věty

Dostáváme se k člověku, který dokázal nemožné. Jeho jméno je Andrew Wiles. Již jako desetiletý se zajímal o matematiku. Právě v tomto věku poprvé narazil na problém Fermatovy věty. Byl tak jednoduchý, že ho dokázal i jako malý pochopit. A přitom zatím nikdo nebyl schopný Fermatova slova dokázat. Zapřísáhl se, že až bude větší a chytřejší, musí větu vyřešit.



(obrázek č. 3 – Andrew Wiles)

V roce 1975 nastoupil na univerzitu v Cambridgi. Brzy se ukázal jako velice schopný. Poté co se stal profesionálním matematikem, začal se zabývat eliptickými křivkami. Tento název je ve své podstatě lehce zavádějící. Ve skutečnosti se totiž nejedná o elipsy. A nejsou to v pravém slova smyslu ani křivky. Eliptické křivky můžeme označit následující rovnicí:

$y^2 = x^3 + ax^2 + bx + c$, kde a, b, c jsou libovolná celá čísla.

Podobně jako u Fermatovy věty, je cílem nalézt celočíselná řešení různých eliptických rovnic. Počet těchto rovnic je nekonečný, každá je ale jedinečná. Aby ale mohl Wiles propojit svůj obor s Fermatovou větou, musíme napřed zmínit dva další důležité objevy.

V Japonsku několik let předtím se objevili dva velice talentovaní matematici. Oba náhodou řešili stejný problém a shodli se, že by se měli o tento problém spolu podělit. Šlo o duo Jutaka Tanijama a Goru Šimura. Zabývali se modulárními formami. Jedná se o jeden z nejpodivnějších matematických objektů. Hlavním rysem modulárních forem je jejich obrovská míra symetrie. Symetrií je myšleno schopnost předmětu jevit se pořád stejně i po jeho transformaci. Touto transformací může být například otočení. Čtverec je krásným

příkladem takové symetrie, neboť je bodově, osově i úhlově symetrický. Představit si modulární formu ale není tak jednoduché jako čtverec, neboť se nachází ve čtyřrozměrném prostoru. Každá tato forma se vyznačuje obsahem různých složek označovaných jako M_i. Všechny tyto složky lze zahrnout pak do takzvané modulární řady pojmenované jako M–řada. V přeneseném slova smyslu se jedná o DNA modulárních forem.

Existuje ale také E–řada fungující skoro jako DNA eliptických křivek. Tanijama objevil, že se M–řada jisté modulární formy shoduje s jednou konkrétní E–řadou. A domníval se, že tento vztah lze zobecnit pro všechny případy. Pokud bychom tedy znali M–řadu, nemuseli bychom již počítat E–řadu odpovídají příslušné eliptické rovnici. K jeho domněnce se připojil i kolega a kamarád Šimura. A tak se jí začalo říkat Tanijamova–Šimurova domněnka.

Dostáváme se nyní k druhému poznatku. Během Sympozia v Oberwolfachu roku 1984 vystoupil s novým tvrzením Gerhard Frey. Tvrzení sice nedokázal, ale tvrdil, že ten, kdo ho prokáže, dokáže vyvrátit Velkou Fermatovu větu. Zjistil totiž, že se dá Fermatova rovnice přepsat do tvaru $y^2 = x^3 + (A^n - B^n) \cdot x^2 + bx - (A^n \cdot B^n)$. Jedná se tedy o eliptickou křivku s koeficienty $a = A^n - B^n$, $b = 0$, $c = -(A^n \cdot B^n)$. Tím tedy propojil Wilesovu práci, domněnku i Fermatovu větu. Pokud řešení existuje, není možné, aby měla rovnice vztah k modulárnímu světu, a tím by tedy došlo k vyvrácení Tanijamovy–Šimurovy domněnky. Ta totiž tvrdí, že každá eliptická rovnice je modulární. Důležitější otázkou tedy zůstává, pokud se domněnka potvrdí, pak nemá Freyova rovnice nárok na existenci. Z toho vyplývá, že Fermatova věta nemá řešení, a proto tedy bez pochyby platí [9, str. 191, cit. 31.3.2023].

Velké finále

Wilesovi se tím dětský sen proměnil v konkrétní problém, na kterém mohl pracovat. Odebral se do ústraní a veškerý svůj čas věnoval studiu veškeré problematiky. V následujících letech učinil mnoho významných objevů, ale žádný nepublikoval, ne dokud nedokončí důkaz. Tři dlouhé roky a Wilesova nespokojenost a frustrace vzrůstaly. Opět se tedy vydal na průzkum literaturou a rozhodl se využít novou metodu. A pak se to stalo. Andrew Wiles přišel na důkaz Tanijamovy–Šimurovy domněnky. Potřeboval ale někoho, kdo mu jeho postupy zkontroluje, než provede oficiální odhalení. Rozhodl se pro

konzultaci s profesorem Nickem Katzem. Katzův průzkum žádnou chybu neodhalil, a tak po dlouhých sedmi letech, v květnu 1993 byl Andrew přesvědčen, že má v rukou celý důkaz Velké Fermatovy věty. V červnu se konala v Cambridgi konference. Wiles zde vystoupil se svými třemi přednáškami. Postupně se propracovával do velkého finále svého odhalení. Konečně přišla na řadu poslední přednáška. A na jejím konci Andrew opravdu napsal důkaz Fermatovy věty. Světový tisk začal rozšiřovat tuto novinu. Dokonce i sám profesor Šimura se dozvěděl z novin o potvrzení jeho a kolegovi domněnky.

Přestože vše vypadalo dokonale, protokol vyžadoval pořádné prozkoumání autorovy práce. Nakonec se drobné problémy přece jen objevily. Metoda, kterou Wiles přizpůsobil svým potřebám, možná ve skutečnosti nefungovala tak, jak matematik zamýšlel. Sám Katz se podivil, že si toho nevšiml, když vše s Andrewem studovali. Před Andrewem tedy vyvstala nová výzva. Rozhodl se chybu odstranit ještě dříve, než dojde k odhalení chyby zbytku světa. Skulina se ale postupně začala dostávat na světlo. Radost a zaujetí vystřídaly rozpaky a zoufalství.

Nakonec se Wiles rozhodl spojit své síly s Richardem Taylorem. A pak se to opět stalo. Andrew si všiml spojitosti mezi předchozí metodou, kterou používal a tou současnou. Každá sama o sobě nestačila, ale dohromady se doplnily. A tak došlo opět k oznámení, že Velká Fermatova věta byla dokázána a chyba v důkazu opravena. O důkazu, který se nacházel na neuvěřitelných 130 stranách nikdo nepochyboval. Tentokrát ne.

Přestože to byl Andrew Wiles, který konečně dokázal najít důkaz Velké Fermatovy věty po více než 350 letech od její formulace, nesmíme zapomenout na všechny nové poznatky, které byly sepsány při zkoumání pouze této jedné věty. A také na všechny matematiky, kteří se o tyto poznatky zasloužili, ten obrovský čas a úsilí, které je to stálo. Bez toho všeho bychom dnes nebyli tam, kde jsme. Dokazování Fermatovy věty ukazuje neskutečné odhodlání lidí, dokázat neuvěřitelné věci, i když se na první pohled vše zdá nemožné.

Zbývá již jen jedna otázka. Jaký byl ale Fermatův důkaz? Odpověď nám samozřejmě není známá. Je jisté, že Fermat nevymyslel a nedokázal všechny vědomosti, které Wiles na důkaz použil. Jejich důkazy se tedy musely bezesporu lišit. Matematici se v této otázce rozdělili na dva tábory. Jedni věří, že Fermat našel pouze chybný důkaz. Druzí optimisté věří Fermatovu tvrzení, že správný důkaz skutečně měl. Znamenalo by to, že byl založen

na poznatcích ze 17. století a úvahy, které za ním stáli byly tak brilantní, že i po 350 letech zůstaly bez povšimnutí všemy matematiky od Eulera až po Wilese. A tak i přes Wilesův objev se stále najde nespočet zapálených lidí, kteří dychtí najít původní Fermatův důkaz.

Odkaz

V roce 2000 byla u nás v České republice vydána speciální poštovní známka ku příležitosti Světového dne matematiky [11, cit. 19.6.2023]. Tato známka je zajímavá právě tím, že oslavuje důkaz Velké Fermatovy věty. Její vzhled si můžeme prohlédnout na dalším obrázku.

(Obrázek č. 4 – Poštovní známka 0260 – Světový rok matematiky)

SEZNAM PŘÍKLADŮ PRAKTICKÉ ČÁSTI

V této kapitole se nachází celkem 10 příkladů vybraných z matematické olympiády. K řešení každého z nich je aspoň částečně využito poznatků spojených s teorií dělitelnosti. U každého příkladu je uveden též jeho zdroj a autor.

PŘ. 1. (71. ročník, Z6–I–4, M. Petrová)

ZADÁNÍ

Kuba si zapsal čtyřmístné číslo, jehož dvě číslice byly sudé a dvě liché. Pokud by v tomto čísle vyškrtl obě sudé číslice, dostal by číslo čtyřikrát menší, než kdyby v tomtéž čísle vyškrtl obě liché číslice.

Které nejvyšší číslo s těmito vlastnostmi si mohl Kuba zapsat?

ŘEŠENÍ

Rozdělme si čtyři cifry na dvě dvojciferná čísla a označme si je pomocí neznámé x, y. Číslo x bude tvořeno pouze ze sudých číslic, y pak z lichých číslic. Ze zadání víme, že musí platit vztah 4y = x, nebo jinak také x : y = 4. Číslo x musí být tedy dělitelné 4. U y používáme pouze liché číslice, proto nabývá hodnot pouze od 11 do 19. Vyšší hodnoty použít nemůžeme. Podle vztahu 4y = x bychom dosáhli trojmístných hodnot čísla x, to ale musí být dvouciferné.

Je jasné, že pokud liché číslo vynásobíme 4, výsledný výraz bude vždy sudý. Nás ale zajímá i cifra na místě desítek, která musí být také sudá. Tím tedy ještě více eliminujeme množinu y. V úvahu tedy přichází pouze množina y = {11, 15, 17}. Prověříme postupně všechny možnosti.

- 4 · 11 = 44, dostáváme tedy cifry 4, 4, 1, 1. Z nich jde nejvýše poskládat číslo 4411.
- 4· 15 = 60, poskládáme maximální číslo 6150, neboť musíme dodržet pořadí cifer. Jednička musí být před pětkou, aby po vyškrtnutí sudých číslic zbylo číslo 15.
- 4 · 17 = 68, zde dostáváme nejvýše 6817. Číslo 6 musí být před 8 a jednička před sedmičkou, aby po vyškrtnutí byla dodržena čísla 68 a 17.

Z těchto tří čísel je největší 6817.

Př. 2. (71. ročník, Z7–I–2, L. Hozová)

Zadání

Součin věků všech dětí pana Násobka je 1408. Věk nejmladšího dítěte je roven polovině věku nejstaršího dítěte.

Kolik dětí má pan Násobek a kolik je jim let?

Řešení

U čísla 1408 provedeme rozklad na prvočísla. Tako prvočísla nebo jejich součiny pak budou věky jednotlivých dětí. Rozkladem získáme tvar $1408 = 2^7 \cdot 11$. Jedno z dětí musí být tedy staré 11 let. Nejmladší dítě má poloviční věk oproti nejstaršímu. Jedenáctileté dítě tedy není nejmladší ani nejstarší, neboť dvojnásobek ani polovina 11 nelze vyjádřit mocninou čísla 2.

Zbývá nám tedy číslo 2^7. Různé součiny nabízí možnosti $2 \cdot 2^3 \cdot 2^3$, $2 \cdot 2 \cdot 2^5$, $2^2 \cdot 2^2 \cdot 2^3$, $2^3 \cdot 2^4$. Postupně všechny prověříme. První tři možnosti nesplňují podmínku mezi nejstarším a nejmladším dítětem. Poslední možnost $2^3 \cdot 2^4$ naše kritéria splňuje.

Pan Násobek má tedy celkem 3 děti a jsou staré 8, 11 a 16 let.

Př. 3. (71. ročník, Z6–I–3, V. Hucíková)

Zadání

Míša zkoumá čísla, která lze vyjádřit jako součet alespoň dvou po sobě jdoucích přirozených čísel. Obzvlášť ji zajímají čísla, která se takto dají vyjádřit vícero způsoby (např. 18 = 5 + 6 + 7 = 3 + 4 + 5 + 6). Číslům, která lze takto vyjádřit alespoň třemi způsoby říká velkolepá.

Najděte alespoň tři Míšina velkolepá čísla.

Řešení

Rozdělíme si hledání na dvě kategorie. Velkolepá čísla, která jsou sudá a která jsou lichá. Pokusíme se najít algoritmus, který by rozkládal dané číslo na součet po sobě jdoucích přirozených čísel.

Sudé přirozené číslo nelze vyjádřit jako součet dvou po sobě jdoucích přirozených čísel.

Pokud bude součet tvořen ze 3 čísel, uvažujme tyto čísla jako x, x+1, x–1. Součet tedy bude 3x. Pokud naše sudé číslo bude dělitelné třemi, lze rozložit na tři po sobě jdoucí přirozená čísla. Pokud půjde rozložit sudé číslo na 4 po sobě jdoucí přirozená čísla, budou to určitě 2 sudá a 2 lichá čísla, a tak součet bude opravdu sudý. Tyto čísla nalezneme vydělením čtyřmi, ale samotné číslo nesmí být dělitelné 4. Výsledek je aritmetický průměr oněch 4 hledaných přirozených čísel, která jsou v jeho těsném okolí (Např. č. 40 rozdělit nelze, ale 42 ano. 42:4 = 10,5. Na okolí se nachází čtveřice 9, 10, 11, 12 jejíž průměr je opravdu 10,5.). Pro rozložení na 5 přirozených čísel užijeme stejného postupu jako u 3 čísel. Součet bude x–2 + x–1 + x + x+1 + x+2 = 5x. Stačí tedy aby bylo číslo dělitelné 5.

Spojíme tato tři kritéria. Dostaneme například sudé číslo 30. To je dělitelné 5, 3, ale není dělitelné 4. 30 = 9 + 10 + 11 = 6 + 7 + 8 + 9 = 4 + 5 + 6 + 7 + 8

Druhým číslem může být například 90. Abychom se ale nedívali pouze na sudá velkolepá čísla odvodíme si podobná pravidla i pro lichá čísla.

Každé přirozené liché číslo lze rozložit na dvě po sobě jdoucí přirozená čísla. Vydělíme ho dvěma a výsledek dělení je aritmetickým průměrem těchto dvou po sobě jdoucích přirozených čísel. U rozkladu na 3 přirozená čísla stačí ověřit dělitelnost třemi. Výsledek po dělení 3 je jedno z nich. Od výsledku následně stačí přičíst a odečíst jedničku a získáme zbývající dvě. Už u příkladu se sudými čísly jsme zjistili, že součet dvou sudých a dvou lichých čísel je vždy lichý. Proto nemůžeme sudé číslo rozložit na 4 po sobě jdoucí přirozená čísla. U rozkladu na 5 čísel provedeme zkoušku na dělitelnost 5. Pokud je číslo dělitelné 5, výsledek po dělení označíme např. d. Potom rozklad bude tvořen čísly d–2, d–1, d, d+1, d+2. Opět poskládáme všechna tři kritéria dohromady. Nejmenší takové číslo je 15, které lze vyjádřit jako 1 + 2 + 3 + 4 + 5 = 4 + 5 + 6 = 7 + 8.

Druhým sudým číslem může být např. 105 = 52 + 53 = 34 + 35 + 36 = 19 + 20 + 21 +22 + 23. Hledaná velkolepá čísla mohou být třeba 105, 15, 30, 90…

PŘ. 4. (71. ročník, Z6–II–2, E. Novotná)

ZADÁNÍ

Myslím si tři přirozená čísla. Součin prvního a druhého je 24, součin druhého a třetího 32, součin prvního a třetího 48.

Která čísla si myslím?

ŘEŠENÍ

Přepíšeme si zadání do jednotlivých rovnic.

- $x \cdot y = 24$
- $y \cdot z = 32$
- $x \cdot z = 48$

Z těchto rovnic získáváme následující poznatky:

- $x \cdot y < y \cdot z \Rightarrow x < z$
- $x \cdot z > y \cdot z \Rightarrow x > y$
- $x \cdot y < x \cdot z \Rightarrow y < z$
- $y < x < z$
- $2(x \cdot y) = x \cdot z \Rightarrow z = 2y$
- $x, y, z \neq 0 \wedge x, y, z \neq 1$

Nyní můžeme využít dva různé postupy, jak se dopracovat k výsledku.

Normálně bychom řešili soustavu 3 rovnic o třech neznámých. Využijeme ale vztahu $z = 2y$, a upravíme druhou rovnici dosazením tohoto vztahu. $2y^2 = 32$ a dostáváme tedy výsledek $y = \pm 4$. Jelikož ale uvažujeme řešení pouze na oboru přirozených čísel, přípustnou možností je pouze $y = 4$. Nyní dosadíme do 1. rovnice. $4x = 24 \Rightarrow x = 6$. Dosadíme výsledek do poslední rovnice. $6z = 48$. Odtud $z = 8$. Dostáváme tedy trojici čísel $x = 6, y = 4, z = 8$.

Druhým řešením je rozklad pravých stran rovnice na součin dvou přirozených čísel a ty porovnáme s pravidly, která jsme si zapsali výše.

- $24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6$
- $32 = 2 \cdot 16 = 4 \cdot 8$
- $48 = 2 \cdot 24 = 3 \cdot 16 = 4 \cdot 12 = 6 \cdot 8$

Například ze druhé rovnice lze poznat, že neznámé z, y mohou nabývat hodnot 2, 16 nebo 8, 4. Zároveň ale musí platit vztah $y < z$. Stačí tedy pouze prověřit pro které hodnoty platí i ostatní rovnice. Pokud zvolíme dvojici $y = 2, z = 16$, z první rovnice musí být x rovno 12, ale

ze třetí rovnice 3. Zkusíme tedy druhou možnost y = 4, z = 8. Pro tento případ je x rovno v první rovnici 6, stejně jako v rovnici třetí. Našli jsme tedy naši trojici x = 6, y = 4, z = 8.

Př. 5. (71. ročník, Z7–II–3, E. Novotná)

Zadání

Eva měla šest kartiček s číslicemi 1, 2, 3, 4, 5, 6 (na každé kartičce byla jedna číslice). Přeskupováním všech šesti kartiček tvořila skupiny čísel a sledovala jejich vlastnosti. Zjistila, že umí různými způsoby poskládat trojice čísel, z nichž každé je dělitelné šesti.

Určete všechny takové trojice.

Řešení

Aby bylo číslo dělitelné 6, musí být dělitelné třemi a dvěma. Hledáme tedy sudá čísla, jejichž ciferný součet je dělitelný třemi. Z cifer, která máme k dispozici je nejmenší takové možné číslo 6 a hned po něm 12. Na tyto dvě čísla jsme spotřebovali 3 cifry, poslední číslo musí být tedy v tomto případě trojciferné. Můžeme ale také vytvořit 3 dvojciferná čísla.

Nyní postupně ověříme všechny varianty.

Zvolme jedno z čísel 6. Hledáme tedy jedno dvojciferné a jedno trojciferné číslo. Pokud bychom obě sudé číslice 2 a 4 užili na dvojciferné číslo, pak trojciferné číslo nebude nikdy dělitelné 6. Můžeme tedy vypustit dvojice 24 a 48. Zbývá prověřit čísla 12 a 54.

- Pokud je druhé číslo 12 ⇒ Třetí vznikne z cifer 3, 4, 5 a musí být dělitelné 6. Dostáváme dvojici 354, 534
- Pokud je druhé číslo 54 ⇒ Třetí složíme z cifer 1, 2, 3. Dvojice takových čísel, která jsou navíc dělitelná šesti, je 312, 132

Nyní se podíváme na možnost, že jsou všechna tři čísla dvojciferná. Napřed si vypíšeme ale všechny dvojciferné násobky 6, které jsme schopni složit z dostupných cifer. Jsou jimi čísla 12, 24, 36, 54. Z těchto čísel potřebujeme vybrat takovou trojici, aby se žádná z cifer neopakovala ve více číslech. Číslo 24 tedy nelze použít v kombinaci s číslem 12 nebo 54. Můžeme tedy číslo 24 vyškrtnout. Ostatní 3 čísla už jsou společně v pořádku.

Sepíšeme tedy všechny kombinace a dostaneme celkem 5 možností:

- 12, 36, 54 6, 12, 354 6, 12, 534 6, 54, 132 6, 54, 312

PŘ. 6. (71. ročník, Z8–II–1, M. Petrová)

ZADÁNÍ

Na tabuli byl zadán příklad na dělení dvou kladných čísel. David si všiml, že pokud by dělenec zvětšil o dva a dělitel o sedm, podíl by se nezměnil.

O kolik by se musel zvětšit dělitel, aby při zvětšení dělence o tři vyšel opět stejný podíl?

ŘEŠENÍ

Označme si dělenec x a dělitel y. Naše číslo tedy bude vypadat takto: $\frac{x}{y}$.Obě čísla jsou kladná, a tak i výsledek zlomku je kladný. Také víme, že mohou být 2 zlomky ekvivalentní. Např. $\frac{2}{3}=\frac{4}{6}$. Můžeme si tedy všimnout, že jsou oba dělenec i dělitel dvojnásobné. Musí tedy být libovolným *k* násobkem zlomku v základním tvaru.

Zadání lze přepsat do rovnice $\frac{x}{y} = \frac{x+2}{y+7}$. Vynásobíme rovnici výrazem y · (y+7). Převedeme neznámé na jednu stranu a čísla na druhou. Dostáváme řešení $\frac{x}{y} = \frac{2}{7}$. Toto řešení lze nalézt také pouhým pozorováním rovnice, neboť víme, že musí být dodržena rovnost zlomků. Pokud by čísla x, y byla rovna číslům, která přičítáme, pak by byl zlomek v nezkráceném tvaru roven $\frac{2x}{2y}$ což odpovídá $\frac{x}{y}$. Odtud tedy x = 2, y = 7.

Teď už jen vytvoříme poslední rovnici z otázky úkolu: $\frac{2}{7} = \frac{2+3}{7+z}$. Zde lze použít opět dva postupy. Buď vypočteme rovnici o jedné neznámé, nebo se stačí zamyslet o hodnotě z. Čitatel vzrostl ze 2 na 5, což je 2,5násobek. Pokud tedy přičítáme k 7 neznámou z, výsledek dělitele musí být také 2,5násobek. 7 · 2,5 = 17,5. Odtud z = 17,5 – 7 = 10,5.

Odpověď tedy zní: Dělitel se musí zvýšit o 10,5.

PŘ. 7. (70. ročník, Z8–I–1, M. Mach)

ZADÁNÍ

Myslím si pětimístné číslo, které není dělitelné třemi ani čtyřmi. Pokud každou číslici zvětším o jedna, získám pětimístné číslo, které je dělitelné třemi. Pokud každou číslici

zmenším o jedna, získám pětimístné číslo dělitelné čtyřmi. Pokud prohodím libovolné dvě číslice, číslo se zmenší.

Jaké číslo si můžu myslet? Najděte všechny možnosti.

ŘEŠENÍ

Představím si pětimístné číslo tvořené z pěti cifer a, b, c, d, e. Pořadí cifer je stejné jako pořadí neznámých. Žádné dvě cifry nejsou stejné a zároveň $a > b > c > d > e$. Tyto neznámé budeme zvyšovat a snižovat o jedna. Je definitivní, že $a < 9$, $e > 0$.

Aby bylo číslo dělitelné třemi, musí být ciferný součet dělitelný třemi. Ciferný součet našeho čísla odpovídá $a + b + c + d + e$. My ale potřebujeme, aby tento součet dělitelný třemi nebyl. Zároveň nesmí být součet $d + e$ dělitelný 4. Tak zaručíme, že celé pětimístné číslo nebude dělitelné 4.

Nyní se podíváme, co se stane, když zvýšíme všechny cifry o jedna. Ciferný součet bude roven $a + b + c + d + e + 5$ a musí být dělitelný 3. Z toho jsme schopni říct, že zbytek našeho původního čísla po dělení třemi bude 1.

Teď zmenšíme všechny cifry o 1. Ciferný součet bude ve tvaru $a + b + c + d + e – 5$. Pro nás je ale důležité poslední dvojčíslí, $d – 1 + e – 1$ totiž musí být dělitelné 4. Jelikož číslo d může být maximálně pět a zároveň $d > e$, vyhovují kritériu celkem 3 čísla, a to 31, 43, 51.

Podíváme se na každý případ zvlášť. Začneme s 51. Zbylé cifry, které lze použít jsou 8, 7, 6, přesně v tomto pořadí. Pokud u celého čísla 87651 zvýšíme každou cifru o 1, zjistíme, že 98762 není dělitelné třemi.

Pokud naše hledané číslo končí na dvojčíslí 43, je jasné, že jeho zvětšená verze 54 je dělitelná 3. Stačí tedy aby první tři cifry pětimístného čísla byly také dělitelné třemi. Pokud zvolíme trojici $a = 8$, $b = 7$, $c = 6$, přijdeme na číslo 87643, které splňuje naše kritéria. Ponížením všech cifer o jedna je dodržena dělitelnost 3. Vyhovuje tedy i číslo 76543. Pro ostatní možnosti $a = 8$, $b = 7$, $c = 5$ nebo $a = 8$, $b = 6$, $c = 5$ není splněna dělitelnost třemi.

Naposledy zvolíme poslední dvojčíslí 31. Zvýšíme všechny cifry pětimístného čísla o 1. Dvojčíslí 42 bude vždy dělitelné 3. Bude tedy záležet na dělitelnosti součtu prvních 3 cifer. Z předchozího případu víme, že čísla 8, 7, 6 kritériu vyhovují, stejně tak 7, 6, 5. Nově také 6, 5, 4. Musí platit $a < 9$, $c > 3$. Když tedy položíme $a = 8$, $c = 4$, potom musí být

bezpodmínečně b = 6. Jiné další možnosti již nevyhovují podmínkám.

Celkem tedy existuje 6 těchto čísel: 87643, 76543, 87631, 76531, 65431, 86431.

PŘ. 8. (70. ročník, Z9–I–1, M. Petrová)

ZADÁNÍ

Slavěna si napsala barevnými fixy čtyři přirozená čísla: červené, modré, zelené a žluté. Když červené vydělí modrým, dostane neúplný podíl zelené číslo a žluté představuje zbytek po tomto dělení. Když vydělí modré číslo zeleným, vyjde jí dělení beze zbytku a podílem je číslo žluté. Slavěna prozradila, že dvě z jejich čísel jsou 97 a 101.

Určete ostatní Slavěnčina čísla a přiřaďte jednotlivým číslům jejich barvy. Najděte všechny možnosti.

ŘEŠENÍ

Označme si čísla podle prvního písmene jejich barvy č, m, z, ž. Musí platit vztahy:

- $č : m = z$ (zbytek ž) $\Rightarrow č = m \cdot z + ž$
- $m : z = ž \Rightarrow m = z \cdot ž$

Z toho se dá dále vyvodit:

- $č > m$
- $č = ž \cdot (z^2 + 1)$ pro $m = z \cdot ž$

Z těchto 4 bodů lze provést závěr, že č, m jsou čísla složená. Jelikož 97 a 101 jsou prvočísla, potom platí $z = 97$, $ž = 101$ nebo také $ž = 97$, $z = 101$.

Stačí jen čísla dosadit do druhého vztahu, $m = 97 \cdot 101 = 9797$. Nakonec dosadíme do první rovnice pro zjištění červeného čísla.

- $č_1 = 9797 \cdot 101 + 97 = 989594$
- $č_2 = 9797 \cdot 97 + 101 = 950410$

Výsledek má celkem 2 možnosti:

- Červené = 989594, modré = 9797, zelené = 101, žluté = 97
- Červené = 950410, modré = 9797, zelené = 97, žluté = 101

PŘ. 9. (70. ročník, Z9–I–2, K. Pazourek)

ZADÁNÍ

Najděte všechny dvojice nezáporných celých čísel x a jednomístných přirozených čísel y, pro která platí: $\frac{x}{y} + 1 = x,\overline{y}$

Zápis na pravé straně rovnice značí periodické číslo.

ŘEŠENÍ

Víme:

- $\frac{x}{y} > 0 \Rightarrow \frac{x}{y} + 1 > 1$
- Pokud $x > y \Rightarrow \frac{x}{y} > 1$
- $\frac{x}{y} + 1 = \frac{x+y}{y}$

Periodické číslo můžeme přepsat do tvaru $x,\overline{y} = x + 0,\overline{y}$. Navíc $0,\overline{y}$ lze přepsat do zlomkového tvaru. Projdeme všech 9 hodnot, kterých může y nabývat. Zjistíme, že pouze pro 3, 6, 9 je zlomek $\frac{1}{y}$ periodický. Musíme tedy prověřit tyto tři možnosti.

Pro y = 3 odpovídá $\frac{1}{y} = 0,\overline{y} = \frac{1}{3} = 0,\overline{3}$. Můžeme tedy celou rovnici ze zadání upravit do tvaru $\frac{x}{3} + 1 = x + \frac{1}{3}$. Vynásobíme rovnici 3. Převedeme čísla na jednu stranu a neznámou x na druhou stranu. Dostáváme výsledek x = 1

Pro y = 6 přepíšeme $\frac{1}{y} = 0,1\overline{6}$. My ale potřebujeme na pravou stranu dostat pouze periodické číslo 6 a ne $1\overline{6}$. Můžeme ale upravit výraz následovně. $10 \cdot 0,1\overline{6} = 1,\overline{6}$, což odpovídá $10 \cdot \frac{1}{6} = \frac{10}{6}$. Po odečtení 1 dostáváme hodnotu $\frac{2}{3} = 0,\overline{6}$. Nyní můžeme opět přepsat úvodní rovnici. $\frac{x}{6} + 1 = x + \frac{2}{3}$. Po úpravě získáváme hodnotu $x = \frac{2}{5}$. Proměnná může ale dosahovat pouze celých hodnot, a tak pro y = 6 řešení neexistuje.

Posledním případem je y = 9. Opět si přepíšeme zlomek do periodického rozvoje $\frac{1}{y} = 0,\overline{1}$. Vynásobíme rozvoj 9 a převedeme do zlomkového tvaru. Dosadíme do úvodní rovnice a dostaneme vztah $\frac{x}{9} + 1 = x + \frac{9}{9}$. Tato rovnice má řešení x = 0. Je ale důležité se pozastavit nad tím, zda toto řešení uznat. Pokud se totiž podíváme na zlomek 9/9 v jeho základním tvaru, je roven 1. Ale v případě $9 \cdot 0,\overline{1}$ je hodnota rovna $0,\overline{9}$. Pravá strana rovnice jde tedy přepsat do dvou rozdílných podob a to x + 1 nebo $x + 0,\overline{9}$. V první podobě řešení uznat nemůžeme, v druhé ano. V oficiálním řešení je tato možnost uznána.

Řešením rovnice je dvojice x = 1, y = 3 nebo x = 0, y = 9.

Př. 10. (69. ročník, Z9–I–3, L. Hozová)

Zadání

Pro která celá čísla x je podíl $\frac{x+11}{x+7}$ celým číslem? Najděte všechna řešení.

Řešení

Pokud má být zlomek celým číslem, potom musí být čitatel roven jmenovateli, nebo jakémukoliv celočíselnému násobku jmenovatele. Toto tvrzení lze přepsat následovně:

- $x + 11 = k \cdot (x + 7), k \in \mathbb{Z}$

Je ale jasné, že jmenovat nesmí být roven nule $\Rightarrow x \neq -7$

Rozdělíme tedy definiční obor neznámého čísla x na část větší než –7 a část menší než –7. Pokusíme se dále systematicky zredukovat definiční obor, neboť máme stále nekonečně mnoho možností. Dosaďme x = 0, získáme výsledek $\frac{11}{7}$. Nejedná se o celé číslo. Důležité ale je, že pokud x > 0, potom zlomek musí být vždy > 0. Postupně budeme zvyšovat x. Vypíšeme si následující tři hodnoty.

- $x = 1 \Rightarrow \frac{x+11}{x+7} = \frac{12}{8}$
- $x = 2 \Rightarrow \frac{x+11}{x+7} = \frac{13}{9}$
- $x = 3 \Rightarrow \frac{x+11}{x+7} = \frac{14}{10}$

Můžeme si všimnout, že jsou všechny zlomky větší než 1. V podstatě pokaždé zvyšujeme čitatel i jmenovatel o 1. To znamená, pro obrovské hodnoty x se postupně přibližujeme k výsledku 1, nikdy této hodnoty ale nedosáhneme. Jmenovatel nikdy nebude celočíselným dělitelem čitatele. Proto můžeme s jistotou tvrdit, že pro x > 0 nebude zlomek nikdy celočíselný.

Dosadíme x = –11, získáme výsledek 0. Máme tedy naše první řešení. Podívejme se, co se stane, pokud budeme volit x < –11.

- x = –12 $\Rightarrow \frac{x+11}{x+7} = \frac{1}{5}$
- x = –13 $\Rightarrow \frac{x+11}{x+7} = \frac{2}{6}$
- x = –14 $\Rightarrow \frac{x+11}{x+7} = \frac{3}{7}$

Pro x < –11 bude tedy zlomek vždy < 0. Postupným snižování x se budeme přibližovat k nule, nikdy této hodnoty ale nedosáhneme. Zlomek může být nulový pouze pokud je čitatel nulový, ten je ale vždy různý od nuly pro x < –11. Také nemůže být výsledek nějaké z celých čísel. Čitatel bude vždy menší než jmenovatel, a tak nemůže být nikdy násobkem jmenovatele. Proto můžeme s jistotou tvrdit, že pro x < –11 nebude zlomek nikdy celočíselný.

Zbývá tedy prověřit pouze několik možností. Konkrétně x = {–10, –9, –8, –6, –5, –4, –3, –2, –1}

Výsledky těchto hodnot jsou znázorněny následující tabulkou:

x =	–10	–9	–8	–6	–5	–4	–3	–2	–1
$\frac{x+11}{x+7}$ =	$\frac{-1}{3}$	–1	–3	5	3	$\frac{7}{3}$	2	$\frac{9}{5}$	$\frac{10}{6}$

(tabulka č. 3 – dosazení hodnot)

Z tabulky lze vyčíst celkem 5 vyhovujících hodnot. Celkem budeme mít tedy 6 řešení.

Zlomek $\frac{x+11}{x+7}$ je celým číslem pro x = {–9, –8, –6, –5, –3, 0}.

ZÁVĚR

Výpočet data Velikonoc, Diofantické rovnice, či důkaz Fermatovy věty, na který se čekalo více než 300 let. Zpočátku se mohou tyto tři problémy zdát jako naprosto odlišné. Přesto byly u řešení každého z nich použity znalosti z teorie dělitelnosti. Je tedy jasné, že teorie dělitelnost je široký matematický obor, který své uplatnění nalezne v nejrůznějších koutech matematiky, což nesporně dokazuje jeho důležitost a potenciál.

RESUMÉ

V této práci jsem popsal několik zajímavých problémů z teorie dělitelnosti. Pro odlehčení jsem tuto práci začal algoritmem pro výpočet data Velikonoc. V dalších kapitolách jsem se zabýval kongruencí celých čísel. Následuje několik zajímavých funkcí, které operují s děliteli celých čísel. Na konci teoretické části popisuji Pythagorovu větu a algoritmus pro hledání Pythagorejských trojic. Také v této kapitole vyprávím příběh Velké Fermatovy věty. Do praktické části jsem zahrnul vlastní řešení deseti vybraných příkladů z matematické olympiády.

Při psaní této práce jsem si zopakoval látku, se kterou jsem se již na školách v minulosti setkal. Také jsem si ale rozšířil vědomosti o nové okruhy z oblasti dělitelnosti a částečně prostudoval i jejich minulost. Naučil jsem se konstruovat své myšlenky a využívat správného matematického zápisu. Z praktického hlediska určitě využiji během pedagogické činnosti algoritmus pro tvorbu Pythagorejských trojic. Do hodin matematiky také pro odlehčení látky zakomponuji výpočet data Velikonoc.

RESUME

In this thesis, I wrote about several interesting problems from the theory of divisibility. I started this work with an algorithm for calculating the date of Easter. In other chapters, I dealt with the congruence of integers. Then I follow with some interesting functions that operate on integer divisors. At the end of the theoretical part, I describe the Pythagorean theorem and the algorithm for finding Pythagorean triples. Moreover in this chapter, I tell the story of Fermat's Great Theorem. In the practical part, I included my solutions to ten selected examples from the Mathematical Olympiad.

While writing this work, I reviewed material that I had already encountered at schools in the past. However, I also expanded my knowledge of new circuits in the theory of divisibility and partially studied their past. I learned to structure my thoughts and use correct mathematical notation. From a practical point of view, I will use the algorithm for creating Pythagorean triples during my teaching activities. I will also incorporate the calculation of the date of Easter into the mathematics lessons to lighten the subject.

SEZNAM POUŽITÉ LITERATURY

[1] *Bečvář, J. (editor); Fuchs, E. (editor): Historie matematiky. I. Seminář pro vyučující na středních školách, Jevíčko, 19.8.–22.8.1993, Sborník. Brno: Jednota českých matematiků a fyziků, 1993. str. 140–161, dostupné online z: https://dml.cz/handle/10338.dmlcz/400592*

[2] *ŘEHÁČEK, Jan. Jan Řeháček Blog iDNES. IDNES Blog [online]. Praha: MAFRA, c 1999–2023, 9.6.2017 [cit. 2023–06–02]. Dostupné z: https://janrehacek.blog.idnes.cz/blog.aspx?c=603423*

[3] *Pythagorean triple. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001–, 16. května 2005 [cit. 2023–06–02]. Dostupné z: https://en.wikipedia.org/wiki/Pythagorean_triple*

[4] *Fermat's Method of Infinite Descent. Brilliant [online]. Kalifornie: Brilliant Worldwide, c 2023 [cit. 2023–06–03]. Dostupné z: https://brilliant.org/wiki/general–diophantine–equations–fermats–method–of/*

[5] *ŠOLCOVÁ, Alena. D'Artagnan mezi matematiky – pocta Pierru Fermatovi k 400. výročí narození. In: Pokroky matematiky, fyziky a astronomie [online]. Praha: Union of Czech Mathematicians and Physicists, 2001, 2001, s. 286–298 [cit. 2023–06–03]. ISSN 0032–2423. Dostupné z: https://dml.cz/bitstream/handle/10338.dmlcz/141095/PokrokyMFA_46–2001–4_3.pdf*

[6] *HONZÍK, Lukáš. Kongruence a neurčité rovnice. Courseware [pdf, online]. Plzeň: Lukáš Honzík, c2007–2023, s. 15 [cit. 2023–03–04]. Dostupné z: https://courseware.zcu.cz/portal/studium/courseware/kmt/ela*

[7] *VESELÝ, František. O dělitelnosti čísel celých [online]. Praha: Mladá Fronta, 1966, (Škola mladých matematiků, sv. 14), [cit. 2023–03–15]. Dostupné z: https://dml.cz/handle/10338.dmlcz/403573*

[8] *List of Known Mersenne Prime Numbers. Great Internet Mersenne Prime Search [online]. State of California: Mersenne Research, ©1996–2023 [cit. 2023–03–16]. Dostupné z: https://www.mersenne.org/primes/*

[9] *SINGH, Simon. Velká Fermatova věta: dramatická historie řešení největšího matematického problému. V českém jazyce vyd. 4., V upr. a dopl. podobě 2. Přeložil Luboš PICK, přeložil Jiří RÁKOSNÍK, přeložil Mirko ROKYTA. Praha: Argo, 2010. Aliter (Argo: Dokořán). ISBN 978–80–7363–315–8.*

[10] SCHWARZ, Štefan. *Algebraické čísla*. Sv. XVI.. Praha: Přírodovědecké nakladatelství, 1950. Kruh.

[11] *Světový rok matematiky. Česká dáma [online]. Hradec Králové: Filatelie Česká Dáma, 2000 [cit. 2023-06-19]. Dostupné z: https://www.ceskadama.cz/product.php?id_product=453*

SEZNAM OBRÁZKŮ A TABULEK

OBRÁZKY

TABULKY