České vysoké učení technické v Praze
The Czech Technical University in Prague

RNDr. Alena Šolcová, Ph. D.

Praktické aplikace teorie čísel

Real-life applications of number theory

Habilitační přednáška

Obor: Aplikovaná matematika

Praha 2008

Summary

Real-life applications of number theory. The halilitation lecture is divided into four parts. In the first part, we present a brief survey of applications of number theory from monograph [7]. We shortly discuss, e.g., RSA method, error-correcting codes, hashing functions, connections between number theory, chaos, and fractals.

There are also practical applications of Fermat primes. In particular, in number-theoretic transforms; in modular arithmetic, which leads to fast multiplication of large numbers; in pseudorandom number generators; and in an analysis of the logistic equation by means of divisors of Fermat numbers. They are also used in digital signal processing (digital filtering).

Reed-Solomon error-correcting codes are employed to protect standard compact disks (CD's) against the effects of minor damage (e.g., scratching). They enable missing information to be reconstructed. Error-correcting codes are also employed in many other fields, for instance, to correct errors in signals (data) coming from interplanetary vehicles.

The second part of the habilitation lecture will be devoted to some real-live applications of the prime number 11 in error-detecting codes, e.g., in bank account numbers, ISBN and ISSN codes. We also briefly mention one-dimensional and two-dimensional codes.

In the third part, we examine a Diophantine equation that leads to the so-called Kepler's mosaics. We find all regular and semiregular tilings of the plane by regular polygons. Then we give some applications and generalizations to the three-dimensional space.

Finally, the fourth part of the habilitation lecture deals with the astronomical clock (horologe) of Prague. The origin of its mathematical model is attributed to Joannes Andreae, called *Šindel*. He invented this model approximately 600 years ago. In honour of this great achievement, we introduced and investigated in paper [11] a new term, the *Šindel sequence*. We show that there is a remarkable relationship between the triangular numbers T_k and the bellwork of this clock. Šindel sequences $\{a_i\} \subset \mathbb{N}$ of natural numbers are defined as those periodic sequences with period p that satisfy the following condition: for any $k \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that $T_k = a_1 + \cdots + a_n$. We found that this condition guarantees a functioning of the bellworks, which is controlled by the horologe. We indroduce a necessary and sufficient condition for a periodic sequence to be a Šindel sequence.

Souhrn

Praktické aplikace teorie čísel. Habilitační přednáška je rozdělena do čtyř částí. V první části uvedeme stručný přehled aplikací teorie čísel z monografie [7]. Krátce se zmíníme např. o metodě RSA, o samoopravných kódech, o hašovacích funkcích, o souvislostech mezi teorií čísel, chaosem a fraktály.

Též připomeneme praktické aplikace Fermatových prvočísel, zejména v číselněteoretických transformacích; v modulární aritmetice, která umožňuje rychlé násobení velkých čísel; při návrhu generátorů pseudonáhodných čísel a při analýze logistické rovnice pomocí dělitelů Fermatových čísel. Používají se též při úpravě digitálního signálu (digitální filtrování dat).

Reedovy-Solomonovy samoopravné kódy se používají k ochraně standardních kompaktních disků (CD) proti drobnému poškození (např. poškrábání). Umožňují totiž zrekonstruovat ztracenou informaci. Samoopravné kódy se používají i řadě dalších oblastí, například o opravám signálu (dat) přicházejících z meziplanetárních sond.

Druhá část habilitační přednášky bude věnována některým konkrétním aplikacím prvočísla 11 v samodetekujících kódech, např. číslech bankovních účtů, ISBN a ISSN kódech. Také se stručně zmíníme o jednorozměrných čárových kódech a dvourozměrných kódech.

Ve třetí části budeme vyšetřovat diofantskou rovnici, která vede na tzv. Keplerovy mozaiky. Určíme všechna pravidelná i polopravidelná pokrytí roviny pravidelnými mnohoúhelníky. Pak uvedeme několik aplikací a zobecnění do trojrozměrného prostoru.

Konečně ve čtvrté části habilitační přednášky se budeme zabývat pražským orlojem. Jan Ondřejův, zvaný *Šindel.* pravděpodobně vytvořil jeho matematický model před 600 lety. Na jeho počest jsme v [11] zavedli pojem nový pojem *šindelovské posloupnosti.* V přednášce ukážeme, že existuje pozoruhodná souvislost mezi trojúhelníkovými čísly T_k a bicím strojem pražského orloje. Šindelovské posloupnosti $\{a_i\} \subset \mathbb{N}$ přirozených čísel se definují jako periodické posloupnosti s periodou p, které splňují následující podmínku: pro každé $k \in \mathbb{N}$ existuje $n \in \mathbb{N}$ takové, že $T_k = a_1 + \cdots + a_n$. Zjistili jsme, že tato podmínka zaručuje dobré fungování bicího stroje, který je řízen hlavním strojem orloje. Představíme nutnou a postačující podmínku k tomu, aby daná periodická posloupnost byla šindelovská.

Klíčová slova

Teorie čísel, prvočíslo, ISBN kód, čísla bankovních kódů, pravidelné polygony, pravidelné a polopravidelné pokrytí, diofantská nerovnice, pražský orloj, pražská hodinová posloupnost, šindelovská posloupnost, trojúhelníková čísla, kongruence, kvadratický zbytek.

Keywords

Number theory, prime number, ISBN code, bank account numbers, regular polygons, regular and semiregular tilings, Diophantine inequalities, Prague's astronomical clock (horologe), Prague's clock sequence, Šindel sequence, triangular numbers, congruence, quadratic residue.

Obsah

1. Úvod

Studiem prvočísel se zabývá lidstvo již několik tisíciletí. Podle některých vědců to dokládají archeologické nálezy z území afrického Zaire, kde byla vykopána kost, na níž lze pozorovat 11, 13, 17 a 19 zářezů. Pomocí radiokarbonové metody (založené na uhlíkové chronometrii vycházející z poměru izotopů ^{12}C a ^{14}C) bylo zjištěno, že je stará 8 tisíc let. Někomu se tehdy asi zdála tato čísla poněkud zvláštní, a tak si je zaznamenal na kost. Samozřejmě odtud neplyne, že by se tehdy lidé vážně zabývali vlastnostmi prvočísel. Avšak již v 7. stol. př. n. l. pýthagorejci ve starém Řecku prvočísla prokazatelně studovali. Později Eukleides (4.–3. stol. př. n. l.) dokázal, že je jich nekonečně mnoho. Eratosthenes z Kyreny (3. stol. př. n. l.) se zase proslavil svým prvočíselným sítem pro vyhledávání prvočísel. Ale teprve ve 20. století se dospělo k tomu, že prvočísla mohou mít řadu zajímavých technických aplikací.

Kdysi se pro kontrolu správnosti na osmistopých děrných páskách používala tzv. parita, tj. osmá krajní stopa se doplňovala tak, aby byl počet dírek v každém řádku sudý. To sloužilo k odhalování chyb při děrování dat pro počítače. Podobný význam mají kontrolní součty pro ověřování správnosti různých datových souborů (např. sloupcové či řádkové součty nebo celkový součet čísel v nějaké tabulce). To jsou jednoduché příklady samodetekujících kódů. Jako příklad si ve 2. kapitole uvedeme praktické použití prvočísla 11 v samodetekujících kódech.

V pracích [3], [4], [5], [8] a [10] se zabýváme vlastnostmi několika typů speciálních tříd prvočísel. V monografii [7] pak uvádíme celou řadu praktických aplikací prvočísel, např.:

- šifrování tajných zpráv pomocí velkých prvočísel
- digitální podpis
- hašovací funkce
- generátory pseudonáhodných čísel
- konstrukce pravidelných mnohoúhelníků
- poselství mimozemským civilizacím
- Fermatova transformace
- chaos a bifurkace logistické rovnice
- konstrukce konečných algebraických těles
- rychlé násobení
- návrhy ozubených kol
- kódování aminokyselin

V [7] jsou uvedeny i další aplikace teorie čísel, které nutně nevyužívají pojem prvočísla, např. samoopravné kódy či šifrování pomocí symetrického klíče. V poslední době se ukazuje, že teorie čísel je nečekaně potřebná i v dalších vzdálených oborech, např. při digitálním zpracování řeči, při studiu vlnových jevů v kvantové mechanice, teorii grup, teorii grafů nebo při řešení akustiky koncertních sálů.

2. Prvočíslo 11 v kódování

V této kapitole ukážeme praktické použití nejmenšího dvojciferného prvočísla 11 v samodetekujících kódech (viz [9]).

2.1 Rodná čísla

V naší republice jsou všechna rodná čísla od roku 1986 dělitelná prvočíslem 11. Poslední čtyřčíslí je totiž voleno tak, aby celé deseticiferné rodné číslo (odhlédneme-li od lomítka) bylo dělitelné 11. Zkuste si např., že rodné číslo

(1) 975811/0428

(odpovídající narození děvčete dne 11. 8. 1997) je dělitelné 11.

Jakou výhodu má skutečnost, že jsou rodná čísla takto volena? Počítač totiž okamžitě odhalí chybu, jakmile se při zadávání rodného čísla zmýlíme v jedné jeho cifře. Pak rozdíl mezi správným a špatně zadaným rodným číslem bude $\pm c \cdot 10^n$, kde $c \in \{1, 2, \ldots, 9\}$, což nikdy není dělitelné 11, ale může být dělitelné složenými čísly $12, 14, 15, 16, \ldots$. Napíšeme-li např. omylem 975811/0728 místo čísla v (1), počítač by při dělení dvanácti chybu neodhalil, protože obě čísla jsou dělitelná 12. Složená čísla proto nejsou pro tyto účely vhodná. Protože číslo 11 nám umožňuje detekovat chybu, hovoříme o *jedenáctkovém samodetekujícím kódu*.

Představme si, že dříve zvolený příklad rodného čísla (1) má hospodářka zapsat do školní databáze. Jestliže se splete např. ve třetí cifře takto: 860811/0428 (tj. „změní děvče na chlapce“), pak rozdíl obou čísel je $5 \cdot 10^7$, což jistě není dělitelné 11. Jestliže se zmýlí ve více cifrách, potom s velkou pravděpodobností přibližně $\frac{10}{11}$ počítač rovněž odhalí chybu. Kvalitní software je ovšem schopen najít i další nesrovnalosti. Například musí umět zkontrolovat počet vkládaných cifer nebo vyřadit uměle vytvořené rodné číslo 830229/0425, které je sice dělitelné 11, ale odpovídá neexistujícímu 29. únoru roku 1983.

Jedenáct je nejmenší dvojciferné prvočíslo. Uvědomme si dále, že jednociferná prvočísla se pro detekci chyb nehodí. Při jejich použití by se totiž obecně nedala odhalit chyba při vložení jedné nesprávné cifry. Na druhé straně bychom mohli použít i větší prvočísla. Pak bychom ale měli méně možností volby rodných čísel, protože deseticiferných čísel, která jsou dělitelná 11, je více než deseticiferných čísel, která jsou dělitelná např. 13. Proto je prvočíslo 11 pro desítkovou soustavu „optimální“ ve uvedeném smyslu. Poznamenejme ještě, že podobný jedenáctkový kód, který se liší jen v jednom detailu, byl zaveden pro rodná čísla již od 1. ledna 1954. Tehdy se devíticiferné číslo dělilo 11 a jednociferný zbytek byla poslední desátá cifra (takto vzniklé rodné číslo je dělitelné 11). Pokud ale zbytek vyšel 10, jako desátá cifra se volila nula a taková rodná čísla se po roce 1986 už nezavádějí.

2.2. ISBN a ISSN kódy

Podobně jako rodná čísla jsou chráněny proti případné chybě i kódy ISBN knižních publikací. Používají se od roku 1972. Skládají se z deseti cifer $x_1 x_2 \ldots x_{10}$, které jsou rozděleny do čtyř částí, mezi nimiž jsou 3 spojovníky. Přitom první tři části mají proměnnou délku:

ISBN kód země-nakladatelství-identifikační číslo knihy-kontrolní cifra x_{10}.

Například pro knihu [1] je

(2) ISBN 80-7196-274-0,

kde ISBN je zkratka anglického názvu *The International Standard Book Number,* první číslo 0 odpovídá zemi, popř. jazyku (anglosaské země mají kromě 0 vyhrazenu ještě 1, frankofonní 2, německy mluvící země 3, Japonsko 4, ... , Česká i Slovenská republika 80 apod.), 7196 je kód nakladatelství Prometheus, následují identifikační číslo knihy a poslední cifra x_{10}, která se volí tak, aby číslo

$$x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} \tag{3}$$

bylo dělitelné jedenácti, tj.

$$x_{10} \equiv \sum_{k=1}^{9} kx_k \pmod{11},$$

přitom pro $x_{10} = 10$ se místo kontrolní cifry píše římská desítka X.

Pro kód (2) po dosazení do (3) dostáváme

$$1 \cdot 8 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 1 + 5 \cdot 9 + 6 \cdot 6 + 7 \cdot 2 + 8 \cdot 7 + 9 \cdot 4 + 10 \cdot x_{10} = 220 + 10x_{10}.$$

Toto číslo je dělitelné 11 pro $x_{10} = 0$. Jestliže se spleteme v jedné cifře nebo omylem prohodíme dvě nestejné cifry, pak takto zadané ISBN nebude dělitelné 11 a snadno odhalíme, že někde nastala chyba. Nově vydávané ISBN kódy jsou třináctimístné. Začínají trojciferným číslem 978 (EAN Prefix).

ISSN kódy (angl. *International Standard Serial Number*) slouží k identifikaci periodik (časopisů). Zapisují se jako dvě čtveřice cifer oddělených spojovníkem: $y_1y_2y_3y_4$-$y_5y_6y_7y_8$. Poslední kontrolní cifra y_8 se volí tak, aby číslo

$$8y_1 + 7y_2 + \cdots + 2y_7 + y_8$$

bylo dělitelné 11 (pokud na místo kontrolní číslice patří 10, používá opět se znak římské číslice X). Například pro časopis Pokroky matematiky, fyziky a astronomie je CS-ISSN-0032-2423, což vyhovuje výše uvedenému kritériu, neboť $\frac{55}{11} = 5$. Podobně pro mezinárodní časopis Applications of Mathematics s ISSN 0862-7940 dostaneme, že $\frac{165}{11} = 15$. Před ISSN kódy se v současnosti předkládá trojciferné číslo 977 (EAN Prefix).

2.3. Identifikační čísla organizací

Ve veřejné správě se setkáváme s identifikačními čísly organizací, která mají osm cifer (podobně jako ISSN kódy) a jsou tvaru IČO $y_1y_2 \ldots y_8$. Starší kratší čísla se doplňují nulami zleva na osm cifer. Poslední cifra y_8 je kontrolní. K jejímu určení se nejprve stanoví zbytek po vydělení součtu

$$8y_1 + 7y_2 + \cdots + 2y_7$$

jedenácti. Zbytek odečtený od 11 se položí roven s. V případě, že vyjde $s = 10$, je kontrolní cifra 0, pro $s = 11$ je kontrolní cifra 1. Jinak definujeme $y_8 = s$. Opět vidíme, že většina chyb může být eliminována, je-li do kódu zavedena jedna kontrolní cifra, která slouží k ověřování správnosti ostatních číslic. Můžete si vyzkoušet, že uvedený algoritmus funguje např. pro IČO Stavební fakulty ČVUT, které je 68 407 700.

2.4. Čísla bankovních účtů

Čísla účtů u Komerční banky se skládají ze dvou částí. První část čísla obsahuje 0 až 6 cifer b_i, druhá část 5 až 10 cifer a_i, tj.

$$\text{číslo účtu: } b_5b_4b_3b_2b_1b_0\text{-}a_9a_8a_7a_6a_5a_4a_3a_2a_1a_0$$

(jiné peněžní ústavy mohou mít čísla účtů utvářena jiným způsobem). Kvůli jednoduché kontrole správnosti jsou čísla účtů navíc volena tak, aby

$$11 \mid \Big(\sum_{i=0}^{5} b_i 2^i\Big), \quad 11 \mid \Big(\sum_{i=0}^{9} a_i 2^i\Big). \tag{4}$$

Uvažujme například číslo účtu

$$158\text{-}3214151.$$

V tomto případě se cifry b_5, b_4, b_3 a a_9, a_8, a_7 neuvádějí (jsou nahrazeny prázdnými znaky). Pak pro první část čísla účtu podle (4) máme $1 \cdot 4 + 5 \cdot 2 + 8 \cdot 1 = 22$, což je dělitelné 11. Podobně zjistíme dělitelnost jedenácti i druhé části čísla účtu,

$$3 \cdot 64 + 2 \cdot 32 + 16 + 4 \cdot 8 + 4 + 5 \cdot 2 + 1 = 319.$$

2.5. Závěrečné poznámky

Velká rozmanitost jedenáctkových kódů vznikla spíše estetickým cítěním jejich tvůrců než podstatnými teoretickými přednostmi některého z nich. Pro jednoduchou detekci chyb jsou podobně konstruovány např. kódy ISMN (*International Standard Music Number*), kódy obsahující biometrické údaje, kódy na platebních a telefonních kartách či přímo kódy na mobilních telefonech, i když ne vždy se používá zrovna jedenáctkový kód. Také čárový kód, s nímž se dnes setkáváme doslova na každém kroku, umožňuje detekovat chybu. Například v naší zemi nejpoužívanější kód EAN-13 obsahuje 13 číslic $a_0a_1a_2 \ldots a_{12}$, z nichž každá je kódována dvěma černými čarami a dvěma mezerami různých šířek (viz obr. 1 vlevo). První kontrolní cifra a_0 je definována tak, aby součet

$$a_0 + 3(a_1 + a_3 + \cdots + a_{11}) + a_2 + a_4 + \cdots + a_{12}$$

byl dělitelný deseti. Čárový kód byl poprvé patentován v USA již v roce 1949. Jeho masové použití je však spojeno až s obrovským pokrokem optoelektrotechniky. V supermarketech zvyšuje rychlost prodeje až o 400 %. Největší dvojciferné prvočíslo 97 se používá k zabezpečení kódu IBAN (International Bank Account Number).

Obr. 1. Jednorozměrné a dvourozměrné čárové kódy.

Při použití samodetekujících kódů můžeme sice zjistit, že se někde vyskytla chyba, ale obecně nevíme, ve které cifře. Tento nedostatek lze odstranit pomocí tzv. samoopravných kódů (viz [7]). Ty nám umožňují pomocí redundantní (nadbytečné) informace obsažené v kódových slovech stanovit, ve kterém bitu (znaku) došlo k chybě, a opravit jej. Používají se mj. pro spolehlivé přenosy dat zajišťujících bezpečnost železniční dopravy, např. aby nebyly současně otevřené závory a návěstidlo pro vlak. Samoopravné (též nazývané samoopravující se) kódy se také používají v moderních automobilech, kde zajišťují případnou opravu údajů procházejících sériovou sběrnicí, která slouží k distribuci dat a povelů k jednotlivým elektrickým přístrojům.

Velká budoucnost je vkládána do nové generace čárových kódů – tzv. dvourozměrných kódů s velmi vysokou informační kapacitou (přes 1 kB) a schopností detekce a oprav chyb. Můžeme se s nimi setkat např. na pražských tramvajenkách (viz obr. 1 vpravo), amerických řidičských průkazech, nejrůznějších identifikačních kartách. Lze je využít i pro zakódování diagnózy pacientů. Tisknou se a přenášejí na papíru, což je jistě nejlevnější médium. Další jejich výhoda spočívá v možnosti přenosu dat bez nutnosti vkládání z klávesnice, kdy často vznikají překlepy.

3. Keplerovy mozaiky

3.1. Pravidelná pokrytí

Německý matematik a astronom Johannes Kepler se ve svém stěžejním díle *Harmonices mundi* (1619) zabýval otázkou, jaká pokrytí (tj. mozaiky, parketáže) lze vytvořit z pravidelných n-úhelníků tak, aby sousední n-úhelníky vždy sousedily celou stranou (viz [1]). Navíc požadoval, aby každý vrchol byl stejného typu $(n_1, n_2, \ldots, n_k)$, tj. aby byl obklopen postupně pravidelným n_1-úhelníkem, n_2-úhelníkem atd. Přitom k-tici $(n_1, n_2, \ldots, n_k)$ budeme považovat za ekvivalentní $(n_k, \ldots, n_2, n_1)$, tj. nebude nám záležet na tom, zda vrcholy n-úhelníků kolem daného vrcholu číslujeme po směru či proti směru hodinových ručiček. Rovněž k-tice $(n_1, n_2, \ldots, n_k)$ a $(n_2, \ldots, n_k, n_1)$ budeme považovat za ekvivalentní, tj. nebude záležet na tom, odkud začneme n-úhelníky číslovat. Takové pokrytí nazveme *polopravidelné*. Pokud speciálně $n_1 = n_2 = \cdots = n_k$, pak hovoříme o *pravidelném pokrytí*. Dvě pokrytí budeme považovat za ekvivalentní, pokud jedno dostaneme z druhého pomocí posunutí, otočení a dilatace.

3.2. Řešení Keplerovy diofantské rovnice

Věta. *Existuje právě* 12 *různých polopravidelných pokrytí roviny, z toho jsou* 3 *pravidelná.*

D ů k a z . Vnitřní úhel v pravidelném n_i-úhelníku je roven $(n_i - 2)180°/n_i$. Proto pro vrchol typu $(n_1, n_2, \ldots, n_k)$ platí následující nutná (nikoliv však postačující) podmínka existence polopravidelného pokrytí

$$\frac{n_1 - 2}{n_1}180 + \frac{n_2 - 2}{n_2}180 + \cdots + \frac{n_k - 2}{n_k}180 = 360.$$

Odtud jednoduchými úpravami dostaneme diofantskou rovnici

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k} = \frac{k-2}{2}. \tag{5}$$

Pravá strana (5) musí být kladná, a tedy $k \geq 3$. Protože bod lze obklopit 6 rovnostrannými trojúhelníky a všechny ostatní n-úhelníky mají vnitřní úhly větší, získáme další nutnou podmínku $k \leq 6$. Srovnáme-li složky výsledné k-tice pro přehlednost podle velikosti, dostaneme následujících 17 řešení rovnice (5).
Trojice:

$$(3,7,42), \quad (3,8,24), \quad (3,9,18), \quad (3,10,15), \quad (3,12,12),$$
$$(4,5,20), \quad (4,6,12), \quad (4,8,8), \quad (5,5,10), \quad (6,6,6);$$

čtveřice:

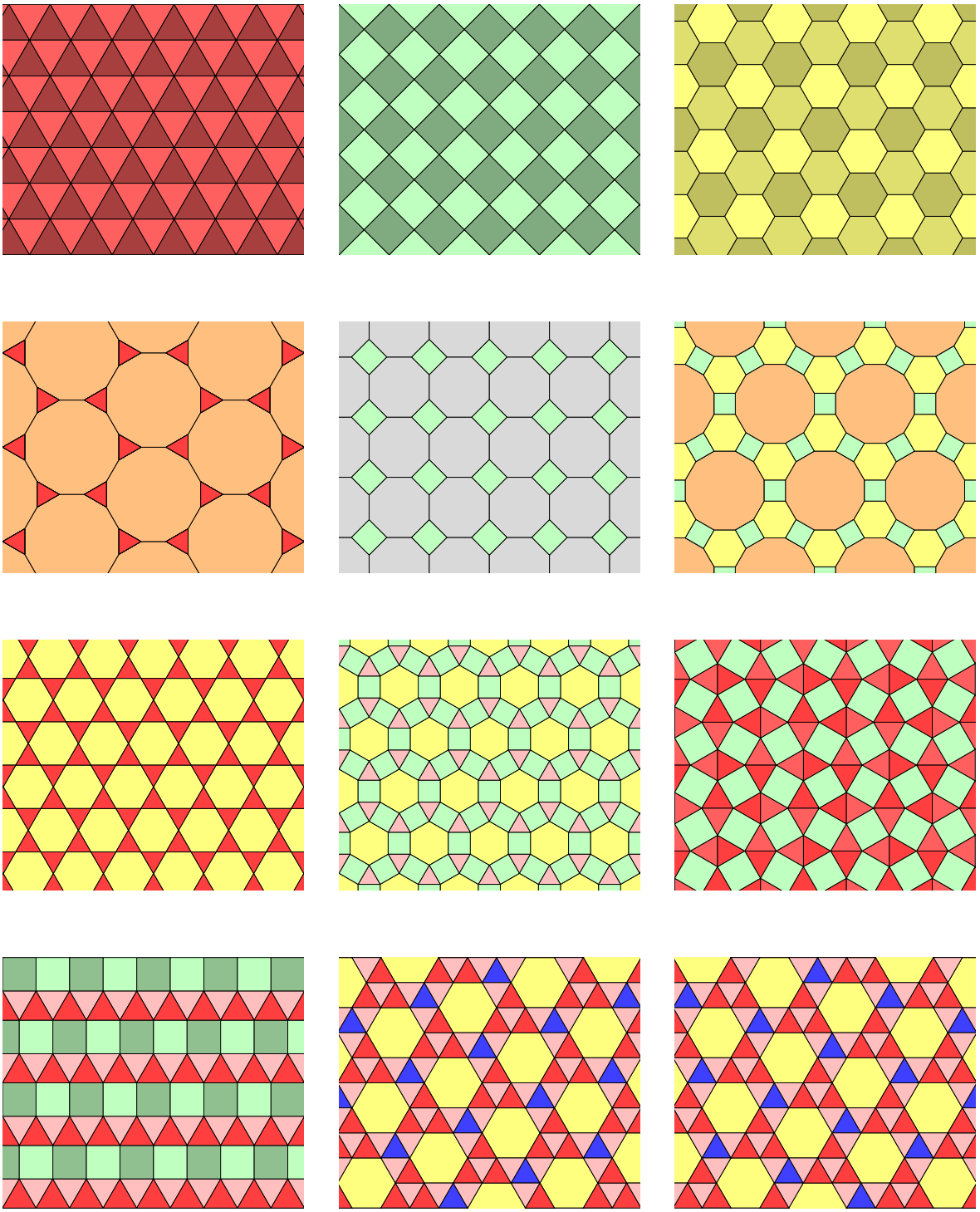
$$(3,3,4,12), \quad (3,3,6,6), \quad (3,4,4,6), \quad (4,4,4,4);$$

pětice:

$$(3,3,3,3,6), \quad (3,3,3,4,4);$$

šestice:

$$(3,3,3,3,3,3).$$



Obr. 2. Keplerovo pravidelné a polopravidelné pokrytí roviny pravidelnými mnohoúhelníky.

Ne všechna ale odpovídají polopravidelným pokrytím celé roviny. Například bod lze obklopit dvěma pětiúhelníky a jedním desetiúhelníkem, ale snadno můžeme ověřit, že to nestačí na pokrytí celé roviny. Navíc složky uvedených sedmnácti k-tic byly srovnány podle velikosti, což v dalším už nebudeme požadovat.

Postupným prověřováním předchozích případů získáme jen následujících 12 ře-

šení (viz obr. 2)

$$
\begin{array}{lll}
(3,3,3,3,3,3), & (4,4,4,4), & (6,6,6), \\
(3,12,12), & (4,8,8), & (4,6,12), \\
(3,6,3,6), & (3,4,6,4), & (3,3,4,3,4), \\
(3,3,3,4,4), & (3,3,3,3,6), & (3,3,3,3,6).
\end{array}
$$

Poslední dvě řešení jsou číselně stejná. Všimněte si ale na obr. 2, že poslední pokrytí je zrcadlovým obrazem předposledního. Ostatních 10 pokrytí má osu souměrnosti. □

Keplerovy polopravidelné mozaiky se používají k ozdobnému dláždění některých chodníků, pro parketáže a umělecké mozaiky, jako vzory na tapety a látky, v počítačové grafice, ale i při popisu uhlíkových nanotrubic.

Podobně jako jsme vyšetřovali pravidelná a polopravidelná pokrytí roviny pravidelnými mnohoúhelníky, lze studovat i tzv. polopravidelná tělesa (viz [1]). *Polopravidelné těleso* je konvexní mnohostěn, jehož všechny stěny jsou pravidelné mnohoúhelníky a všechny prostorové úhly ve vrcholech mnohostěnu jsou přímo či nepřímo[1] shodné. Speciálním případem polopravidelných těles jsou platónská pravidelná tělesa, jejichž povrch je tvořen pravidelnými mnohoúhelníky jednoho typu. Polopravidelná tělesa, jejichž povrch je tvořen pravidelnými mnohoúhelníky dvou či více typů, se dělí na tzv. archimédovská tělesa, pravidelné hranoly a pravidelné antihranoly. Jejich existenci lze vyšetřovat podobně jako v předchozí větě. Pravidelné hranoly (resp. pravidelné antihranoly) mají dvě protilehlé stěny tvořeny stejným pravidelným n-úhelníkem a ostatní stěny jsou čtverce (resp. rovnostranné trojúhelníky). Speciálním případem pravidelného hranolu (resp. pravidelného antihranolu) je krychle (resp. pravidelný osmistěn). Přehled třinácti archimédovských těles podává Johannes Kepler ve druhé kapitole *Harmonií světa.* Tato tělesa jsou pojmenována po antickém mysliteli Archimédovi.

Pravidelná a polopravidelná tělesa mají řadu použití v krystalografii a teorii bodových grup. Používají se i pro dekorační účely (např. na nástupišti stanice Lužiny Metra B v Praze). Také fotbalový míč připomíná archimédovské těleso o 12 pětiúhelníkových a 20 šestiúhelníkových stěnách. Tento mnohostěn má 60 vrcholů a nalezl uplatnění též v chemii. Ukázalo se totiž, že existuje stabilní molekula uhlíku, tzv. fulleren C_{60}, která má 60 atomů umístěných právě ve vrcholech takového polopravidelného tělesa. Pravidelné triangulace trojúhelníkových stěn pravidelného dvacetistěnu se zase používají ke konstrukci triangulace povrchu koule.

[1] Prostorový úhel je nepřímo shodný se svým zrcadlovým obrazem.

4. Teorie čísel ukrytá v pražském orloji

4.1. Jan Šindel – autor matematického modelu orloje

V této kapitole uvidíme, že teorie čísel sehrála důležitou úlohu i při konstrukci pražského orloje. Podle výzkumů Zdeňka Horského a Emanulela Procházky orloj vznikl v době mistra Jana Husa kolem roku 1410. Jeho matematický model navrhl Jan Ondřejův, zvaný *Šindel,* který se zabýval matematikou a astronomií na pražské univerzitě. Jeho starší kolega Křišťan z Prachatic již kolem roku 1406 zde přednášel o konstrukci astrolábu. To je starověký astronomický úhloměrný přístroj k určování poloh nebeských těles a místního času. Unikátní stroj orloje vytvořil Mikuláš z Kadaně. V průběhu staletí byla konstrukce orloje vícekrát zdokonalována, např. pověstným Janem z Růže (mistrem Hanušem). V 16. století pečoval o orloj Jan Táborský z Klokotské Hory. Ten je také autorem nejstaršího známého popisu orloje z roku 1570.

Jan Ondřejův, zvaný Šindel (cca 1375 – cca 1457), se roku 1399 stal mistrem svobodných umění na pražské univerzitě a v roce 1410 zde ve funkci rektora vystřídal mistra Jana Husa. Napsal několik matematických a astronomických pojednání – např. *De notitia triangulorum cum notis Iohannis Schindel; Canones pro eclipsibus Solis et Lune.* Na univerzitě přednášel podle Thabita Ptolemaiův *Almagest.* Šindel byl též osobním lékařem krále Václava IV (viz [2]). Na jeho počest jsme v [11] zavedli pojem šindelovské posloupnosti, který níže představíme. S jeho pomocí uvidíme, jaká podivuhodná matematika se skrývá v bicím stroji pražského orloje a jak tento stroj souvisí s trojúhelníkovými čísly.

4.2. Pražská hodinová posloupnost

Genialitu tehdejších hodinářů můžeme demonstrovat na konstrukci zařízení pro přesnou stabilizaci úderů zvonu. Bicí stroj obsahuje velké oběžné kolo (tzv. závěrkové kolo) s 24 zářezy na vnějším obvodu, jejichž vzdálenosti postupně narůstají (viz obr. 3). To umožňuje periodické opakování 1–24 úderů zvonu během každého dne. Počet úderů zvonu odpovídá SEČ, tj. v letním čase orloj odbíjí vždy o hodinu méně. Součástí bicího stroje je i pomocné kolečko, jehož obvod je rozdělen 6 zářezy na segmenty o délkách oblouku 1, 2, 3, 4, 3, 2 (viz obr. 3). Tyto délky se periodicky opakují po každé otočce a jejich součet je

$$s = 15.$$

Na začátku každé hodiny se zvedne západka, obě kola se začnou otáčet a zvon odbíjí příslušný počet hodin. Kola se zastaví, jakmile západka zapadne současně do zářezů na obou kolech. Každý den udeří zvon celkem

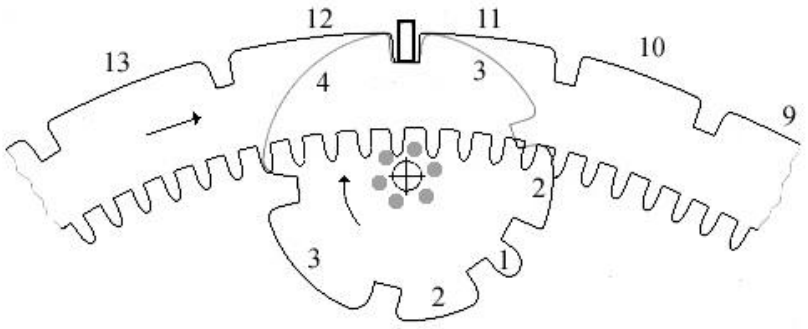
$$1 + 2 + \cdots + 24 = 300$$

krát, a protože trojúhelníkové číslo $T_{24} = 300$ je dělitelné $s = 15$, bude pomocné kolečko na počátku každého dne vždy ve stejné poloze.

Závěrkové kolo má 120 vnitřních zubů, které zapadají do cévového kola se 6 vodorovnými tyčkami, jež obklopují střed pomocného kolečka (viz obr. 3). Protože se

závěrkové kolo otočí jednou denně, pomocné kolečko se otočí za tu dobu 20krát. Obě kola se otáčejí pouze během odbíjení. Přitom je ale obvodová rychlost pomocného kolečka přibližně 4krát větší, protože jeho obvod je 5krát menší, než obvod závěrkového kola. To umožňuje dostatečně přesnou stabilizaci počtu úderů zvonu zejména při opotřebení zářezů závěrkového kola. Bez pomocného kolečka by totiž mohl zvon udeřit např. jen 11krát místo 12krát, pokud by segment označený 12 na obr. 3 měl již příliš zaoblené konce. Pro jeden úder zvonu hodinu po půlnoci, je dokonce pomocné kolečko nezbytné, neboť na závěrkovém kole schází příslušný segment (viz obr. 3).

Pražský orloj je pravděpodobně nejstarší a stále fungující hodinový stroj, který obsahuje takové důmyslné zařízení pro přesnou stabilizaci počtu úderů zvonu.



Obr. 3. Počet úderů zvonu je označen čísly $\ldots, 9, 10, 11, 12, 13, \ldots$ po vnějším obvodu velkého závěrkového kola. Za ním je umístěno pomocné kolečko, jehož obvod je zářezy rozdělen na segmenty o délkách oblouku 1, 2, 3, 4, 3, 2. Západka je znázorněna malým obdélníčkem nahoře uprostřed.

Když se pomocné kolečko otáčí, vytváří pomocí délek segmentů mezi jednotlivými zářezy periodickou posloupnost, jejíž částečné součty odpovídají počtu úderů zvonu v každou celou hodinu,

(6)
$$1\,2\,3\,4\,\underbrace{3\,2}_{5}\;\underbrace{1\,2\,3}_{6}\;\underbrace{4\,3}_{7}$$

$$\underbrace{2\,1\,2\,3}_{8}\;\underbrace{4\,3\,2}_{9}\;\underbrace{1\,2\,3\,4}_{10}\;\underbrace{3\,2\,1\,2\,3}_{11}\;\underbrace{4\,3\,2\,1\,2}_{12}$$

$$\underbrace{3\,4\,3\,2\,1}_{13}\;\underbrace{2\,3\,4\,3\,2}_{14}\;\underbrace{1\,2\,3\,4\,3\,2}_{15}\ldots$$

V další kapitole ukážeme, že bychom takto mohli pokračovat až do nekonečna. Všechny periodické posloupnosti ale takovou pěknou součtovou vlastnost nemají. Například je patrno, že nelze použít periodu 1, 2, 3, 4, 5, 4, 3, 2, protože pro 6 úderů zvonu je $6 < 4+3$. Rovněž perioda 1, 2, 3, 2 se k tomuto účelu nehodí, neboť pro 4 údery máme $2+1 < 4 < 2+1+2$.

Sloane ve své The on-line encyclopedia of integer sequences:

`http://www.research.att.com/~njas/sequences/`

nazývá periodickou posloupnost

$$1,\ 2,\ 3,\ 4,\ 3,\ 2,\ 1,\ 2,\ 3,\ 4,\ 3,\ 2,\ldots$$

pražská hodinová posloupnost díky zajímavé součtové vlastnosti uvedené v (6).

V následujících kapitolách se budeme věnovat zobecnění této posloupnosti. Budeme se zajímat o to, jak navrhnout nepravidelné ozubení pomocného kolečka i pro obecně jiné hodnoty součtu s.

4.3. Trojúhelníková čísla a šindelovské posloupnosti

V článku [6] jsme odvodili překvapivou souvislost mezi *trojúhelníkovými čísly*

$$T_k = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}, \quad k = 0, 1, 2, \ldots, \tag{7}$$

a pražskou hodinovou posloupností, která byla použita při konstrukci bicího stroje pražského orloje. V této kapitole se budeme zabývat dalšími periodickými posloupnostmi, které mají podobnou vlastnost jako posloupnost 1, 2, 3, 4, 3, 2, ... v (6), tj. které by mohly být použity při konstrukci podobného pomocného kolečka jako je na obr. 3.

Posloupnost $(a_i)_{i=1}^{\infty}$ se nazývá *periodická,* jestliže existuje $p \in \mathbb{N}$ tak, že

$$\forall\, i \in \mathbb{N} : \quad a_{i+p} = a_i. \tag{8}$$

Konečná posloupnost $a_1, \ldots, a_p$ se nazývá *perioda* a p *délka periody.* Nejmenší p splňující (8) se nazývá *minimální délka periody* a jemu odpovídající posloupnost $a_1, \ldots, a_p$ *minimální perioda.*

Nechť $(a_i) \subset \mathbb{N}$ je periodická posloupnost. Řekneme, že trojúhelníkové číslo T_k pro $k \in \mathbb{N}$ je *dosažitelné* pomocí (a_i), jestliže existuje $n \in \mathbb{N}$ tak, že

$$T_k = \sum_{i=1}^{n} a_i. \tag{9}$$

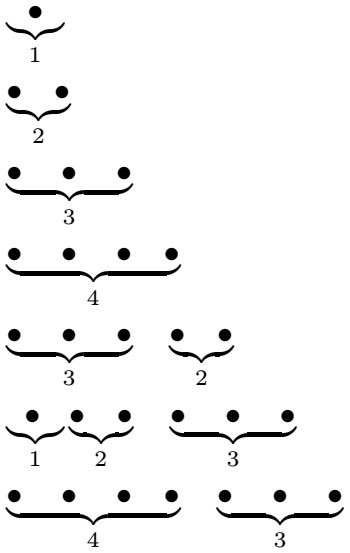
Periodickou posloupnost (a_i) nazveme *šindelovskou,* je-li T_k dosažitelné pomocí (a_i) pro všechna $k \in \mathbb{N}$, tj.

$$\forall\, k \in \mathbb{N} \quad \exists\, n \in \mathbb{N} : T_k = \sum_{i=1}^{n} a_i. \tag{10}$$

Trojúhelníkové číslo T_k na levé straně je rovno součtu $1 + \cdots + k$ hodin na velkém závěrkovém kole, zatímco součet na pravé straně odpovídá celkovému pootočení pomocného kolečka (viz obr. 3). Přitom pro k-tou hodinu platí

$$k = T_k - T_{k-1} = \sum_{i=m+1}^{n} a_i, \tag{11}$$

kde $T_{k-1} = \sum_{i=1}^{m} a_i$. Protože $a_i > 0$, je číslo n v (10) závisející na k určeno jednoznačně. Z (7) a (9) je také patrno, že $a_1 = 1$, je-li (a_i) šindelovská posloupnost.



Obr. 4. Schematické znázornění trojúhelníkového čísla T_7. Černé puntíky v k-tém řádku znázorňují počet úderů zvonu v k-té hodině (viz (11)). Čísly jsou označeny délky segmentů mezi zářezy na pomocném kolečku.

Následující věta ukazuje, že podmínku (10) lze zaměnit mnohem jednodušší podmínkou, jež obsahuje pouze konečný počet čísel k. To nám umožňuje provést jen konečný počet aritmetických operací, abychom zjistili, zda zvolená perioda $a_1, \ldots, a_p$ dává šindelovskou posloupnost. Součet prvků periody budeme nadále označovat

$$s = \sum_{i=1}^{p} a_i. \tag{12}$$

Věta. *Periodická posloupnost (a_i) je pro liché s šindelovská, jestliže T_k je dosažitelné pomocí (a_i) pro $k = 1, 2, \ldots, \frac{1}{2}(s-1)$.*

Důkaz této věty je uveden v [6].

Poznámka. Číslo $\frac{1}{2}(s-1)$ v předchozí větě nelze zmenšit, je-li p délka minimální periody odpovídající s. Abychom se o tom přesvědčili, stačí uvažovat posloupnost (a_i) s minimální periodou $1, 2, 2, 1, 4, 1, 4$ a $s = 15$. Pak podle definice jsou trojúhelníková čísla $T_1, \ldots, T_6$ dosažitelná pomocí (a_i), ale T_7 není.

Příklady. Význam předchozí věty můžeme demonstrovat na pražské hodinové posloupnosti (6) pro $s = 15$. Stačí totiž ověřit vztah (10) pouze pro $k \leq \frac{1}{2}(s-1) = 7$, tedy jen první řádek v (6). (Přitom $T_7 = 28$ z obr. 4 je dokonalé číslo.) Dosažitelnost celých čísel $k > 7$ na dalších řádcích (6) pak vyplývá z předchozí věty.

Podobně můžeme ověřit předpoklady věty i pro další periody:

1, 2 pro $p = 2$ a $s = 3$,

1, 2, 2 pro $p = 3$ a $s = 5$,

1, 2, 3, 1 pro $p = 4$ a $s = 7$,
1, 2, 3, 3 pro $p = 4$ a $s = 9$,
1, 2, 2, 1, 4, 1, 4, 1, 4, 1, 4 pro $p = 11$ a $s = 25$.

Existují šindelovské posloupnosti i pro s sudá. Jednu takovou můžeme zkonstruovat např. z periody 1, 2, 1, 1, 1:

$$1\ 2\ \underbrace{1\ 1\ 1}_{3}\ \ \underbrace{1\ 2\ 1}_{4}\ \ \underbrace{1\ 1\ 1\ 2}_{5}\ \ \underbrace{1\ 1\ 1\ 1\ 2}_{6}\ldots \tag{13}$$

Činitel $\frac{1}{2}(s-1)$ na pravé straně (8.9) ale není celočíselný. Proto příslušné prvky posloupnosti vyjadřující číslo $s = 6$ v (13) nejsou ve stejném pořadí jako daná perioda.

4.4. Podmínka pro existenci šindelovské posloupnosti

Nechť $n \geq 2$ a a jsou pevně daná celá čísla. Připomeňme nejprve pojmy kvadratického rezidua a nerezidua. Jestliže kvadratická kongruence

$$x^2 \equiv a \pmod{n}$$

má řešení x, pak a se nazývá *kvadratický zbytek* (*kvadratické reziduum*) *modulo* n. V opačném případě se a nazývá *kvadratické nereziduum modulo* n.

Na závěr uveďme nutnou a postačující podmínku pro existenci šindelovské posloupnosti, která se opírá o pojem kvadratického zbytku.

Věta *Periodická posloupnost* (a_i) *je šindelovská právě tehdy, když pro každé* $n \in \{1, \ldots, p\}$ *a* $j \in \{1, 2, \ldots, a_n - 1\}$, *pro něž* $a_n \geq 2$, *číslo*

$$w = 8\Big(\sum_{i=1}^{n} a_i - j\Big) + 1$$

není kvadratický zbytek modulo s.

V důkazu této věty (viz [11]) je obsažen numerický algoritmus pro vytváření tzv. primitivních šindelovských posloupností. Pomocí počítače lze prověřit, že žádná primitivní šindelovská posloupnost pro $s \leq 1000$ a $s \neq 15$ nemá takovou pěknou „palindromickou“ vlastnost jako pražská hodinová posloupnost (6), která byla použita při konstrukci bicího stroje pražského orloje. Tuto posloupnost generuje při otáčení pomocné kolečko znázorněné na obr. 3.

V práci [12] uvádíme další matematické věty (celkem 10), které se bezprostředně týkají konstrukce pražského orloje.

Literatura

[1] Šolcová, A., *Johannes Kepler, zakladatel nebeské mechaniky*, Prometheus, Praha, 2004.

[2] Šolcová, A., *Jan Šindel a matematika ukrytá v pražském orloji*, 28. mezinárodní konference Historie matematiky, Jevíčko, JČMF, Matfyzpress, Praha, 2007, 96–99.

[3] Šolcová, A., Křížek, M., *Fermat and Mersenne numbers in Pepin's test*, Demonstratio Math. **39** (2006), 737–742.

[4] Šolcová, A., Křížek, M., *Elitné prvočísla*, Obzory mat. fyz. inf. **35** (2006), č. 4, 1–6.

[5] Šolcová, A., Křížek, M., Mink, G. (eds.), *Matematik Pierre de Fermat*, Cahiers du CEFRES, no. 28, Praha, 2002.

[6] Křížek, M., Somer, L., Šolcová, A., *Jaká matematika se ukrývá v pražském orloji?*, Matematika-fyzika-informatika **16** (2006), 129–137.

[7] Křížek, M., Somer, L., Šolcová, A., *Kouzlo čísel*, Edice Galileo, Academia, Praha, 2009.

[8] Křížek, M., Šolcová, A., *Marin Mersenne a jeho prvočísla*, Matematika – fyzika – informatika **11** (2001/02), 204–212.

[9] Křížek, M., Šolcová, A., *Prvočíslo 11 v kódování*, Rozhledy mat.-fyz. **78** (2004), 208–214.

[10] Křížek, M., Šolcová, A., *Jak spolu souvisí chaos, fraktály a teorie čísel*, Sborník semináře: Determinismus a chaos, Herbertov (ed. L. Herrmann), SF ČVUT, Praha, 2005, 96–113.

[11] Křížek, M., Šolcová, A., Somer, L., *Construction of Šindel sequences*, Comment. Math. Univ. Carolin. **48** (2007), 373–388.

[12] Křížek, M., Šolcová, A., Somer, L., *Ten theorems on the astronomical clock of Prague*, Proc. Internat. Conf. Presentation of Mathematics '07 (eds. J. Příhonská, K. Segeth, D. Andrejsová), Tech. Univ. Liberec, 2007, 53–62.

Seznam literatury obsahuje jen vlastní práce týkající se problematiky aplikací teorie čísel. Stovky odkazů na práce dalších autorů jsou uvedeny v např. [7].

RNDr. Alena Šolcová, Ph. D.

RNDr. Alena Šolcová, Ph. D. (1950) studovala v letech 1968–1973 matematiku na Matematicko-fyzikální fakultě UK a zároveň v letech 1968–1972 filosofii na Filosofické fakultě UK. Titul RNDr. získala v roce 1983.

Doktorské studium Matematika ve stavebním inženýrství absolvovala v letech 2002–2005 a ukončila obhajobou dizertační práce na téma: *Fermat's Ideas Revived in Mathematics Applied in Engineering* na FSv ČVUT Praha v roce 2005.

Je autorkou více než 150 matematických článků zaměřených převážně na historii matematiky, aplikace matematiky, didaktiku matematiky, teorii čísel, některé numerické metody, astronomii a informatiku. Získala mnoho pozvání k přednáškám na zahraničních univerzitách: Harvard University v Cambridge Mass. (USA), Roma, Viterbo, Trieste (Itálie), Paris VIII (Francie), Wroclaw (Polsko), Shandong University in Jinan, Hong Kong Baptiste University (Čína) a na mezinárodních symposiích a konferencích (např. UNAM Mexico City v Mexiku, Kolobrzeg v Polsku, Zaragoza ve Španělsku, Uppsala ve Švédsku, Beijing v Číně).

Dosud vedla 11 diplomových prací z informatiky, historie matematiky, historie astronomie a praktického uplatnění některých metod ve výuce. Od roku 1994 vyučuje matematiku a základy informatiky a programování na FSv ČVUT. Je pověřována převážně cvičeními a semináři. Od roku 1996 přednáší pro zahraniční studenty ČVUT (převážně z FS ČVUT) anglicky The History of Technology (ZS 2/0) se zaměřením na užití matematických method ve vývoji techniky.

Již 17 let vede na FSv ČVUT seminář pro dějiny matematiky a astronomie (SEDMA). Je členkou Českého komitétu pro dějiny vědy a techniky při AV ČR a členkou mezinárodní komise pro dějiny techniky ICOHTEC. Je předsedkyní Historické sekce České astronomické společnosti.

Od roku 1995 je členkou České matematické společnosti. V roce 1999 obdržela čestné uznání Jednoty českých matematiků a fyziků. Od roku 2002 je zasloužilou členkou JČMF, místopředsedkyní matematického oddělení a tajemnicí Pražské pobočky JČMF. Věnuje se též popularizaci exaktních věd, mj. realizovala několik interaktivních výstav matematických a fyzikálních experimentů. Je držitelkou medaile Jana Marka Marci a dvou medailí Jana A. Komenského za návrhy a realizace výstav: Experimentem k poznání v Národním technickém muzeu v Praze a v Moravském zemském muzeu v Brně, a Descartes a Komenský ve Valdštejnském paláci v Praze.

V roce 2007 pojmenovala Mezinárodní astronomická unie na její počest planetku č. 58 682 Alenašolcová.