Věnováno našim rodičům a prarodičům

OBSAH

Přirozená čísla jsou prvotním pramenem celé matematiky.

Hermann Minkowski

Úvodní slovo 11

Seznam symbolů 15

Předmluva 19

1. Dělitelnost a kongruence 27
- **1.1. Přirozená čísla** 27
- **1.2. Jednoduchá kritéria dělitelnosti** 29
- **1.3. Nejmenší společný násobek a největší společný dělitel** 32
- **1.4. Nesoudělná čísla** 34
- **1.5. Eukleidův algoritmus*** 36
- **1.6. Lineární diofantské rovnice*** 37
- **1.7. Kongruence*** 39
- **1.8. Čínská věta o zbytcích*** 42
- **1.9. Dirichletův princip*** 47

2. Prvočísla a čísla složená 50
- **2.1. Základní věta aritmetiky*** 50
- **2.2. Eukleidova věta o nekonečnosti prvočísel*** 52
- **2.3. Pythagorejské trojice*** 54
- **2.4. Fermatova metoda nekonečného sestupu**** 57
- **2.5. Velká Fermatova věta** 63
- **2.6. Malá Fermatova věta*** 66
- **2.7. Eulerova–Fermatova věta*** 70
- **2.8. Carmichaelova věta**** 73
- **2.9. Legendrův a Jacobiho symbol**** 76
- **2.10. Rozklad na prvočísla** 81

3. Vlastnosti prvočísel 86
- **3.1. Kritéria prvočíselnosti*** 86

3.2. Wilsonova věta* 89
3.3. Dirichletova věta* 93
3.4. Fermatova vánoční věta** 94
3.5. Polynomy generující prvočísla 99
3.6. Riemannova hypotéza** 103
3.7. Další vlastnosti prvočísel* 104

4. Speciální typy prvočísel 109
4.1. Mersennova prvočísla* 109
4.2. Fermatova prvočísla* 119
4.3. Wieferichova prvočísla* 134
4.4. Elitní prvočísla** 136
4.5. Regulární a iregulární prvočísla* 140
4.6. Prvočísla Sophie Germainové** 142
4.7. Eukleidova prvočísla* 149
4.8. Další speciální typy prvočísel* 154

5. Aplikace prvočísel 163
5.1. Prvočíslo 11 v kódování 163
5.2. Šifrování tajných zpráv pomocí velkých prvočísel** 171
5.3. Digitální podpis* 178
5.4. Hašovací funkce* 180
5.5. Generátory pseudonáhodných čísel* 182
5.6. Eukleidovská konstrukce pravidelných mnohoúhelníků** 184
5.7. Poselství mimozemským civilizacím 195
5.8. Fermatova transformace** 198
5.9. Jak spolu souvisí chaos, fraktály a teorie čísel** 199
5.10. Další aplikace 209

6. Pseudoprvočísla 212
6.1. Co je pseudoprvočíslo?* 212
6.2. Historické poznámky 213
6.3. Hustota rozložení pseudoprvočísel* 217
6.4. Carmichaelova čísla* 218
6.5. Mersennova a Fermatova pseudoprvočísla* 219

7. Speciální typy přirozených čísel **222**
7.1. Fibonacciho a Lucasova čísla* **222**
7.2. Mnohoúhelníková čísla **243**
7.3. Dokonalá čísla* **249**
7.4. Deficientní a abundantní čísla* **253**
7.5. Spřátelená čísla* **256**
7.6. Fermatova čísla* **259**
7.7. Sierpińského čísla** **265**
7.8. Další speciální typy přirozených čísel* **268**

8. Jaká matematika se ukrývá v pražském orloji? **273**
8.1. Jan Šindel – autor matematického modelu orloje **273**
8.2. Co ukazuje pražský orloj? **274**
8.3. Pražská hodinová posloupnost **281**
8.4. Trojúhelníková čísla a šindelovské posloupnosti* **284**
8.5. Podmínka pro existenci šindelovské posloupnosti** **291**
8.6. Konstrukce primitivní šindelovské posloupnosti** **296**
8.7. Která šindelovská posloupnost je nejkrásnější? **299**

9. Další aplikace teorie čísel **304**
9.1. Samoopravné kódy* **304**
9.2. Šifrování pomocí symetrického klíče **307**
9.3. Keplerovy mozaiky **310**
9.4. Penrosovy mozaiky* **312**
9.5. Platónská tělesa **314**
9.6. Vykrývací čtyřstěny* **318**
9.7. Triky s čísly* **320**
9.8. Latinské čtverce* **326**
9.9. Magické čtverce **331**

Tabulky **335**

Literatura **347**

Odkazy na internetové stránky **358**

Rejstřík **359**

Počet hvězdiček označuje míru obtížnosti dané kapitoly.

Úvodní slovo

Matematické věty a jejich důkazy
jsou pro nás jako valouny zlata
pro zlatokopy.

Autoři

S čísly se setkáváme denně, doslova na každém kroku. Není možné se bez nich obejít, nevšímat si jich a být k nim lhostejný. Pojďme se tedy společně podívat do světa čísel, seznámit se s jejich fascinujícími a někdy až magickými vlastnostmi. Dokážeme si některé překvapivé souvislosti mezi teorií čísel a geometrií (viz např. kapitoly 1, 4, 7 a 9). Uvidíme, jakými zákonitostmi se řídí celá čísla. Ukážeme si také, že teorie čísel má mnohé praktické aplikace, bez nichž si ani nelze představit moderní technický svět.

Toto pojednání o číslech vzniklo na základě našich více než 50 popularizačních a vědeckých článků o elementární a algebraické teorii čísel. O většině z nich se referovalo na semináři *Aktuální problémy numerické matematiky,* který probíhá v Matematickém ústavu Akademie věd ČR [www1], na semináři *Dějiny matematiky a astronomie* na ČVUT v Praze [www2] a na mnoha domácích i mezinárodních konferencích věnovaných teorii čísel.

Kniha je určena nejširší matematické veřejnosti – zejména těm, kteří dokáží ocenit kouzlo abstraktní i aplikované matematiky. Předpokládáme pouze, že čtenář je seznámen se základními pravidly aritmetiky a že mu nečiní potíže algebraické úpravy. Jen zcela výjimečně bude potřebovat k porozumění několika vztahům znalost lineární algebry či matematické analýzy. Většinu kapitol lze číst nezávisle na předchozím výkladu. Přitom některé části jsou vcelku jednoduché, jiné složitější. Pokud bude pro vás nějaká partie příliš náročná, není problém ji přeskočit. Obtížnější kapitoly jsou v obsahu označeny jednou hvězdičkou * nebo dvěma hvězdičkami ** podle stupně obtížnosti.

V závěru knihy jsou tabulky a poměrně rozsáhlý seznam literatury, jehož účelem je upozornit na některé práce z teorie čísel.

Pro inspiraci je zde také několik odkazů na internetové stránky, i když jsme si dobře vědomi, že nepodléhají recenzi a často se mění. Nově definované pojmy jsou v textu pro pohodlí čtenáře zvýrazněny kurzívou. Lze je nalézt také v rejstříku.

Při čtení jednotlivých kapitol se prosím nezalekněte poměrně velkého množství matematických vět. Je jich více než 160. Matematikové totiž formulují své myšlenky právě formou matematických vět, které obsahují jen to, co je na daném problému podstatné. Téměř u všech tvrzení podáváme důkaz (u složitějších důkazů jen odkaz na příslušnou literaturu), abyste se sami mohli přesvědčit o platnosti předkládaných tvrzení. Na teorii čísel je nejkrásnější to, že důkaz každého tvrzení se obvykle liší od ostatních důkazů. Přitom formulace uvedených matematických vět se vejde většinou jen na jednu či dvě řádky, což umožňuje poměrně snadno pochopit, co daná věta vlastně říká.

Matematická tvrzení platí věčně. Nejsou závislá na poloze a času. O jejich platnosti nerozhoduje parlament hlasováním, ani náboženský či politický systém v dané zemi, ani nezávisí na kulturních zvyklostech apod. Například Pythagorova věta platí na Zemi stejně tak jako ve vzdálené galaxii M31 a bude platit i za milion let. Definice matematických pojmů nedovolují dvojí výklad. Rovněž naprosto přesné formulace matematických problémů nepřipouštějí více interpretací. Vágní vyjadřování, jehož jsme denně svědky, má za následek řadu nedorozumění. Jen malé procento naší veřejnosti se dokáže vyjadřovat přesně a vnímat krásu matematiky. Výstižně to vyjádřil významný maďarský matematik Cornelius Lanczos (1893–1974):

Většina umění, jako je malířství, sochařství a hudba, vyvolává ve veřejnosti emocionální dojem. Je to tím, že tato umění jsou vnímána jedním či více z našich smyslů. Tak tomu není s uměním matematickým, které může být doceněno pouze matematiky. A stát se matematikem vyžaduje dlouhé období usilovné přípravy. Matematická komunita je podobná jakési imaginární společnosti hudebních skladatelů, jejichž jediným uspokojením je vzájemná výměna hudebních skladeb, které komponují.

Další slavný maďarský matematik Paul Erdős (1913–1996) se o číslech vyjádřil takto:

Proč jsou čísla krásná? To je podobné, jako ptát se, proč je Beethovenova Devátá krásná. Když to nevidíte, nikdo vám to nemůže říct. Já vím, že čísla jsou krásná. A pokud ne, tak není krásné nic.

V české a slovenské matematické literatuře najdeme několik knih o teorii čísel. Zmiňme se o znamenitých monografiích (Grošek, Porubský, 1992), (Lepka, 2000), (Rychlík, 1950), (Sedláček, 1997), (Šalát, 1969) a (Znám, 1987). V naší knize ale naleznete některá zcela nová témata. Například uvidíte, jak trojúhelníková čísla souvisí s bicím strojem pražského orloje, o jakou matematiku se opírá tradiční čínský kalendář, nebo jak lze zkonstruovat pravidelný sedmnáctiúhelník pomocí pravítka a kružítka. Ukážeme, jak byla použita základní věta aritmetiky při návrhu poselství mimozemským civilizacím a jak teorie čísel souvisí s teorií grafů. Seznámíme se také s nejnovějšími výsledky při honbě za největšími prvočísly a poznáme, k čemu jsou nám vůbec prvočísla dobrá. Uvedeme řadu jejich rozličných praktických aplikací v naprosto odlišných odvětvích. Představíme si kódy, které detekují případné chyby, a tzv. samoopravné kódy, které navíc chyby automaticky opravují. Také vám předvedeme, jak spolu souvisí chaos, fraktály a teorie čísel.

V řadě diskusí nám pomohli zdokonalit obsah knihy především Jan Brandts, Karel Břinda, Yann Bugeaud, Pavel Burda, Walter Carlip, Karl Dilcher, Alena Hadravová, Helena Holovská, Václav Holub, Jan Chleboun, František Katrnoška, Martin Klazar, Sergej Korotov, Pavel a Filip Křížkovi, Florian Luca, Karel Micka, Jaroslav Mlýnek, Pavla Pavlíková, Štefan Porubský, Ladislav Skula, László Szalay, Bedřich Šofr, Jakub Šolc, Pavel Trojovský, Jana Vlášková a Václav Vopravil. Jejich pomoci si velice vážíme a patří jim náš velký dík. Dále jsme zavázáni univerzitní knihovně v Göttingen za povolení publikovat kopii části dopisu z pozůstalosti C. F. Gausse (obr. 4.5) a Národní knihovně ČR v Klementinu za umožnění studia kodexu XIII.F.1, jehož část je na obrázku 8.7.

Také bychom rádi poděkovali Akademii věd ČR a Ministerstvu školství, mládeže a tělovýchovy za udělení grantů IAA 100190803 a 1P05ME749, bez nichž by tato knížka jen těžko vznikla. Náš velký dík patří zvláště nakladatelství Academia, Ediční radě Akademie věd za finanční podporu a panu redaktoru Aleši Baďurovi za velice cenné připomínky a významnou pomoc při závěrečné úpravě práce a Jakubu Šolcovi za pečlivou grafickou úpravu.

Michal Křížek
Lawrence Somer
Alena Šolcová

3.14	desetinné číslo
$\mathbb{N} = \{1, 2, 3, \dots\}$	množina přirozených čísel
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	množina celých čísel
$\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}$	množina racionálních čísel
$\mathbb{R}$	množina reálných čísel
$\mathbb{C}$	množina komplexních čísel
A_n	čtyřstěnná čísla
B_n	Bernoulliova čísla
C_n	Cullenova čísla
F_m	Fermatova čísla
K_n	Fibonacciho čísla
L_n	Lucasova čísla
M_p	Mersennova čísla
$P_{k,n}$	mnohoúhelníková čísla
P_n	pětiúhelníková čísla
S_n	čtvercová čísla
T_n	trojúhelníková čísla
W_n	Woodallova čísla
$(n_1, n_2, \dots, n_k)$	největší společný dělitel čísel $n_1, n_2, \dots, n_k$
$[n_1, n_2, \dots, n_k]$	nejmenší společný násobek čísel $n_1, n_2, \dots, n_k$
$\{n_1, n_2, \dots, n_k\}$	množina k čísel $n_1, n_2, \dots, n_k$ (nezáleží na pořadí)
$\langle n_1, n_2, \dots, n_k \rangle$	uspořádaná k-tice čísel $n_1, \dots, n_k$ (záleží na pořadí)
(a_i)	posloupnost
$\lfloor a \rfloor$	celá část reálného čísla a
$\lvert S \rvert$	počet prvků množiny S
$\approx$	přibližná rovnost
$n \equiv k \pmod{m}$	n je kongruentní k modulo m

$n \not\equiv k \pmod{m}$	n není kongruentní k modulo m
$m \mid n$	m dělí n
$m \nmid n$	m nedělí n
$m^j \parallel n$	m^j přesně dělí n pro $1 < m \leq n$
$\max(m, n)$	maximum z čísel m a n
$\min(m, n)$	minimum z čísel m a n
$\mathrm{ord}_d n$	řád n modulo d
$n!$	součin $1 \cdot 2 \cdots n$, n-faktoriál
det	determinant
$\log_b$	logaritmus o základu b
log	přirozený logaritmus
e	Eulerovo číslo
π	Ludolfovo číslo
$\pi(x)$	počet prvočísel nepřevyšujících x
$G(n)$	orientovaný graf na n vrcholech
$\tau(n)$	počet všech kladných dělitelů čísla n
$\omega(n)$	počet všech prvočíselných dělitelů čísla n
$\sigma(n)$	součet všech kladných dělitelů čísla n
$s(n)$	součet všech kladných dělitelů n menších než n
φ	Eulerova funkce
Φ_n	cyklotomický polynom stupně n
λ	Carmichaelova funkce
$\left(\frac{a}{p}\right)$	Legendrův symbol pro liché prvočíslo p
$\left(\frac{a}{m}\right)$	Jacobiho symbol pro liché číslo m
$\binom{n}{k}$	kombinační číslo n nad k (binomický koeficient)
Re z	reálná část komplexního čísla z
Im z	imaginární část komplexního čísla z

$\overline{z}$	číslo komplexně sdružené k z
i	imaginární jednotka
$i,\ j,\ k$	celočíselné indexy
$\exists$	existuje
$\forall$	pro všechna
$\mathcal{O}(\cdot)$	Landauův symbol: $f(\alpha) = \mathcal{O}(g(\alpha))$, pokud $\lvert f(\alpha)\rvert \leq C\lvert g(\alpha)\rvert$ pro $\alpha \to 0$ nebo $\alpha \to \infty$
$\emptyset$	prázdná množina
$\prod$	součin
$\sum$	součet
$\cap$	průnik
$\cup$	sjednocení
$\setminus$	rozdíl množin
$\subset$	je podmnožinou
$\in$	je prvkem
$\notin$	není prvkem
$\{x \in A;\ \mathcal{P}(x)\}$	množina všech prvků x z A majících vlastnost $\mathcal{P}(x)$
$f : A \to B$	zobrazení (funkce) f z množiny A do množiny B
$\Rightarrow$	implikace
$\Leftrightarrow$	ekvivalence
$:=$	přiřazení
$\square$	Halmosův symbol označující konec důkazu

V knize zapisujeme desetinná čísla, na rozdíl od české literatury, s tečkou.

Předmluva

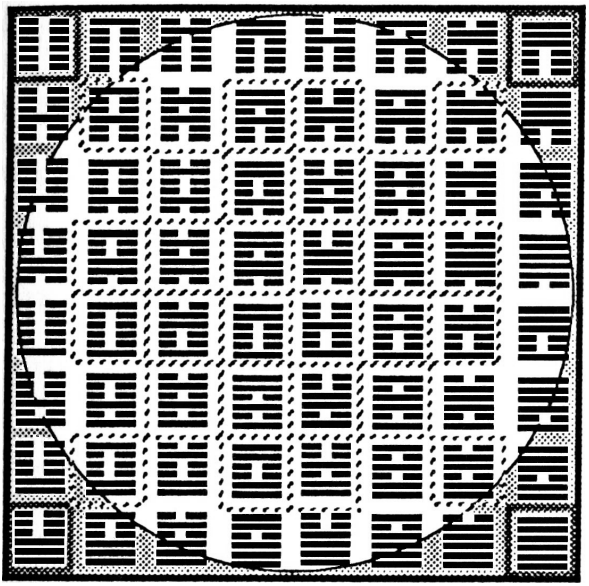
Podle staročínské filosofie všechny jevy vznikly z prachaosu, který se rozštěpil ve dva naprosté protiklady, ***jin*** *a* ***jang.***

V jedné z nejstarších čínských knih *I-ťing (Kniha proměn),* která vznikla přibližně v 8. stol. př. n. l., je uveden obrázek (tzv. hexagram) obsahující 8 × 8 políček. Uvnitř každého z nich je šest přerušovaných nebo plných horizontálních čar (obr. 1). Přerušená čára znamená starý čínský princip *jin* a plná princip *jang*, jež jsou v protikladu. *Jin* je spojováno s Měsícem, vlhkostí, tmou, zemí, ženou a pasivitou, *jang* naproti tomu se Sluncem, suchem, světlem, nebesy, mužem a aktivitou.

Významný německý matematik Gottfried Wilhelm Leibniz (1646–1716) spojoval uvedený hexagram s objevem dvojkové soustavy. Budeme-li totiž místo přerušené čáry uvažovat nulu a místo plné čáry jedničku, pak symboly v políčkách zleva doprava (horním řádkem počínaje) lze postupně interpretovat jako čísla 0, 1, 2, 3, . . . zapsaná ve dvojkové soustavě. První číslo v levém horním políčku je tedy nula, i když tento její zápis nebyl v 8. století př. n. l. používán pro operace s čísly. Poslední číslo v pravém dolním rohu odpovídá 63, které se ve dvojkové soustavě zapisuje šesti jedničkami. Použití nuly se nám dnes zdá zcela přirozené, ale její samotný objev a zejména způsob jejího zápisu znamenal v evropské matematice obrovský pokrok.

I když staří Číňané neprováděli se symboly *jin* a *jang* žádné aritmetické operace, nelze jim upřít prioritu ve znázornění čísel zapsaných ve dvojkové soustavě. Tento fenomenální objev našel

praktické uplatnění až v dnešní době počítačů, tj. téměř o tři tisíce let později. Počítače totiž zobrazují a zpracovávají veškerou informaci (včetně čísel) právě ve dvojkové soustavě. Je to nejjednodušší způsob jak v elektronických obvodech počítače zpracovávat data. A tak i fungování celosvětové sítě internetu, e-mailu, faxu, skenerů, kopírek, digitálních kamer, kompaktních disků CD a DVD či mobilních telefonů je vlastně založeno na principech *jin* (= 0) a *jang* (= 1).



Obr. 1. První znázornění dvojkové soustavy z 8. století př. n. l.

Příroda ale v průběhu evoluce objevila dvojkovou (nebo chceteli čtyřkovou) soustavu již před více než třemi miliardami let. Na dvojšroubovici kyseliny deoxyribonukleové (DNA), která je obsažena v každé buňce, se nacházejí čtyři druhy bází: adenin *A*, cytosin *C*, guanin *G* a thymin *T*. Nahradíme-li je postupně dvojicemi 00, 01, 10 a 11, bude každému vláknu DNA odpovídat posloupnost nul a jedniček, která tak vlastně představuje genetickou informaci

zapsanou ve dvojkové soustavě. Přitom je genetický kód univerzální pro celou rostlinnou i živočišnou říši (až na několik drobných výjimek).

Obr. 2. Symboly *jin* a *jang* lze nalézt na dnešní vlajce Korejské republiky.

Pomocí replikace $R(A) = T$, $R(C) = G$, $R(G) = C$ a $R(T) = A$ dochází k vytvoření druhého vlákna kyseliny DNA, čímž tato kyselina získává tvar dvojšroubovice (Katrnoška, Křížek, 2003). Příroda tak vlastně objevila i jednoduchou logickou unární operaci negace. Například nukleotidy $\ldots AGTCCT \ldots$ na horním vláknu z obr. 3 odpovídající posloupnosti

$$\ldots 001011010111 \ldots$$

přejdou při replikaci DNA na $\ldots TCAGGA \ldots$ odpovídající „komplementární“ posloupnosti

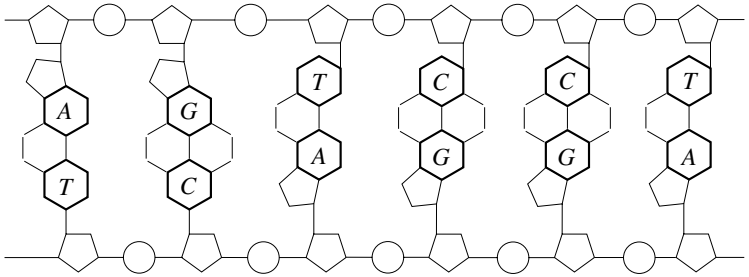
$$\ldots 110100101000 \ldots,$$

kde $A = 00$, $C = 01$, $G = 10$ a $T = 11$.

Pokud bychom položili $A = 0$, $C = 1$, $G = 2$ a $T = 3$, pak je genetická informace převedena do čtyřkové soustavy. Součet těchto numerických hodnot je pro všechny možné přípustné páry A–T, C–G, G–C a T–A vždy roven 3. Nositel Nobelovy ceny James D. Watson ve své knize *Geny, ženy a Gamow* z roku 2001 píše:

> *Nejvýznamnějším Gamowovým zjištěním bylo, že celý jazyk DNA je vytvořen ze čtyř písmen, bází A, C, G a T. Upoutala ho myšlenka, že k osvětlení fungování genů by mohla být využita teorie čísel.*

Zde dovolte malé odbočení. Při návrhu modelu struktury DNA v roce 1953 sehrála jistě důležitou roli skutečnost, že jeden z au-



Obr. 3. Schematické znázornění struktury DNA. Nukleotidy jsou označené písmeny *A*, *C*, *G* a *T*. Molekuly cukru deoxyribózy (označené pětiúhelníky) a molekuly kyseliny fosforečné (označené kroužky) jsou spojené silnými kovalentními vazbami a chrání tak genetickou informaci před poškozením. Celá molekula DNA je ve skutečnosti zkroucená do dvojité pravotočivé šroubovice.

torů, Francis H. C. Crick, byl fyzikem s abstraktním matematicko-fyzikálním myšlením. Crick si již v roce 1950 uvědomil, že když budeme stejné molekuly spojovat naprosto stejným způsobem, budou ležet na prostorové šroubovici (v mezních případech na kružnici či přímce). Za tento objev získal společně s Jamesem D. Watsonem Nobelovu cenu. Podobně zakladatel genetiky Johann Gregor Mendel ovládal matematické metody a dokonce matematiku vyučoval ve Znojmě a Brně. A jen precizní práce se statistickými daty z křížení hrachu mu umožnila objevit známé zákony dědičnosti (Katrnoška, Křížek, 2004/05). Matematika tak hraje důležitou roli při odkrývání a popisu zákonitostí přírody.

Ve starověku a středověku se používaly číselné soustavy o různých základech. Například je doloženo, že staří Babyloňané a Mayové používali soustavu o základu 60. Původ českých slov tucet (12), kopa (60) a veletucet (144) také svědčí o tom, že se u nás nepoužívala jen desítková soustava.

Připomeňme, že celé kladné číslo n v soustavě o základu b lze jednoznačně napsat ve tvaru

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

kde jeho cifry (číslice) $c_i \in \{0, 1, \ldots, b-1\}$, tj. množina cifer má

právě b prvků, a $c_k \neq 0$. (Existenci takového vyjádření lze dokázat indukcí a jednoznačnost podobně jako ve větě 2.2.) Pokud $b \geq 10$, roli dalších cifer mohou hrát písmena. Například v šestnáctkové (tj. hexadecimální) soustavě se používají tyto cifry: 0, 1, 2, . . . , 9, A, B, C, D, E, F. V této knížce ale budeme dále pracovat jen v desítkové či dvojkové soustavě.

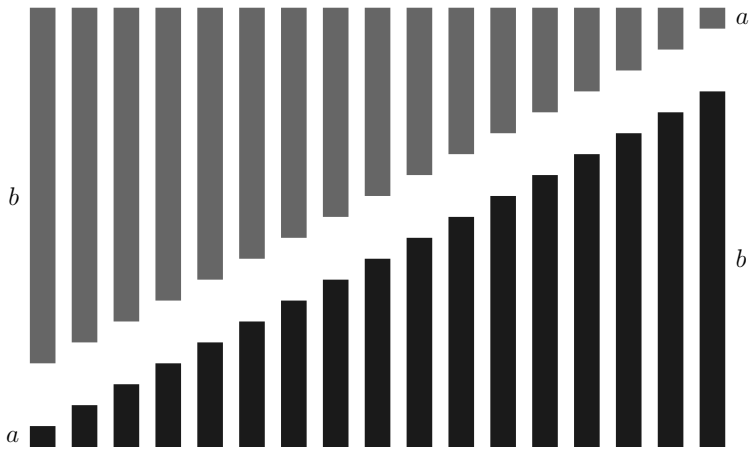
Vydáme se po cestě za tajemstvím přirozených čísel a představíme si jejich některé doslova kouzelné a nečekané vlastnosti. Chceme vám zejména ukázat, že čísla nejsou jen pro zábavu a s ní spojeným dobrodružstvím, ale že teorie čísel má také obrovské množství praktických aplikací. V minulosti Eukleides, Fermat, Euler a mnozí další si vlastně s čísly pouze „hráli“, dokazovali o nich nejrůznější tvrzení, aniž by tušili, jakou obrovskou revoluci svými výsledky způsobí a jaké praktické využití jejich matematické věty budou mít. Navíc tentýž výsledek se dá často použít v řadě naprosto rozličných situací. V této knize to uvidíme například u Čínské věty o zbytcích či Malé Fermatovy věty. Většina tvrzení z teorie čísel na své praktické použití teprve čeká a mnohé z nich uplatnění patrně nikdy nenajdou. To ale nic neubírá na jejich kráse.

Studiem prvočísel a jejich mnohdy překvapivými vlastnostmi se zabývá lidstvo už několik tisíciletí. Ale teprve ve 20. století se přišlo na to jak využít prvočísel v řadě užitečných aplikací. Například rodná čísla jsou od roku 1986 utvářena tak, aby byla dělitelná prvočíslem 11. Počítač totiž okamžitě odhalí chybu, jakmile se při zadávání rodného čísla zmýlíme v jedné jeho cifře. Jestliže se zmýlíme ve více cifrách, potom s velkou pravděpodobností počítač rovněž odhalí chybu. To je jeden z příkladů tzv. samodetekujících kódů. Poněkud komplikovanějším jedenáctkovým kódem jsou chráněna proti možné chybě i čísla bankovních účtů, identifikační čísla organizací, čísla ISSN časopisů, čísla ISBN publikací aj.

Větší prvočísla, jež mají až sto cifer, se používají v moderních kryptografických systémech s veřejným šifrovacím klíčem (např. v metodě RSA pro přenos tajných zpráv). Také digitální podpis, jehož zavedení do života schválil náš parlament, je založen na velkých prvočíslech. Pomocí prvočísel lze konstruovat efektivní

generátory pseudonáhodných čísel nebo navrhovat algoritmy pro velmi rychlé násobení velkých čísel. Prvočísla mají řadu aplikací i při zpracování signálu či obrazu pomocí číselně teoretických transformací, např. při filtrování dat získaných z radarů, sonarů, modemů apod.

Vydáním základní Gaussovy práce *Disquisitiones arithmeticae*, srov. (Gauss, 1986), na počátku 19. století se teorie čísel konstituovala jako systematická matematická disciplína, jejímž hlavním předmětem je studium vlastností celých čísel. Ve 20. století pak našla široké uplatnění v nejrůznějších oborech lidské činnosti. Používá se v řadě softwarových produktů, v informační bezpečnosti, při kompresi dat, matematické genetice, ve fyzice, astronomii, robotice, krystalografii aj. S čárovými kódy se dnes běžně setkáváme v komerční sféře díky obrovskému pokroku optoelektrotechniky. Jejich zavedení v obchodech zvyšuje rychlost prodeje až o 400 %. Samoopravné kódy se zase používají při přenosu dat z meziplanetárních sond nebo na železnici pro zabezpečení jejího spolehlivého provozu. Také fungování digitálních fotoaparátů, telekomunikačních družic, hudebních přehrávačů aj. je založeno na teorii čísel.



Obr. 4. Geometrická interpretace známého Gaussova vztahu pro součet prvních n členů aritmetické posloupnosti $a + (a + d) + (a + 2d) + \cdots + b = \frac{1}{2}n(a + b)$, kde $b = a + (n - 1)d$ a d je rozdíl (diference) dvou sousedních členů.

Tyto moderní výdobytky civilizace by bez teorie čísel nikdy nevznikly. I když zde v 19. století nebyly, asi jen těžko bychom se jich dnes vzdávali. Širší veřejnost si je bohužel neuvědomuje (nebo ani uvědomovat nechce) a považuje je za samozřejmost. Netuší, kolik lidského důmyslu, intelektuálního úsilí a matematických výsledků je ukryto v těchto technických zařízeních. Například počítačové tomografy by nefungovaly bez komplexních čísel. O ně se totiž opírá rychlá Fourierova transformace, která je potřebná k velice rychlému výpočtu Radonovy inverzní transformace v reálném čase (Křížek, 1999).

V následujících kapitolách se při výkladu zaměříme na geometrickou představivost, která může do značné míry usnadnit chápání některých algebraických tvrzení, vztahů a základních pojmů z teorie čísel, např. známých algebraických identit $(a \pm b)^2 = a^2 \pm 2ab + b^2$, $a^2 - b^2 = (a + b)(a - b)$, Pythagorovy věty (obr. 2.1), vztahu pro součet aritmetické posloupnosti (obr. 4) apod. Celkem je v této knize kolem 100 obrázků. Najdete zde i poznámky o historickém pozadí některých pojmů a metod.

1. DĚLITELNOST A KONGRUENCE

Jeden obrázek řekne více
než tisíc slov.

Staré čínské přísloví

1.1. Přirozená čísla

Lidé od pradávna používají čísla 1, 2, 3,... k vyjádření počtu nějakých předmětů. Nejstarší použití nuly bylo zaznamenáno v Indii. Postupně byla zavedena mezi celá čísla v poziční číselné soustavě.

Občas se setkáváme s otázkou, zda nula je či není přirozené číslo. Na tento dotaz bohužel nelze dát jednoznačnou odpověď typu ANO/NE, neboť to, zda budeme nulu považovat za přirozené číslo či nikoliv, je věcí definice. Nulu je vhodné zahrnout do množiny přirozených čísel například při určování počtu prvků konečných množin, protože počet prvků prázdné množiny je nula.

Na druhou stranu existují dobré důvody, kdy naopak není výhodné nulu zahrnovat do množiny přirozených čísel. Je to například při umocňování přirozených čísel na přirozenou mocninu. Symbolu 0^0 totiž nelze jednoznačně přiřadit nějakou hodnotu, která by přirozeně korespondovala s operacemi v reálném oboru. Vidíme například, že pro $n = 1, 2, \ldots$ je $0^n = 0$, zatímco $n^0 = 1$. Rovněž nelze rozumně definovat nejmenší společný násobek například čísel 0 a 3, jak uvidíme v oddílu 1.3. Proto se častěji nula za přirozené číslo nepovažuje. Také v této knížce množina přirozených čísel nebude nulu obsahovat.

Množinu přirozených čísel označíme

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Úmluva. Přirozená čísla budeme většinou značit $i, j, k, \ell, m, n, p, q, r, s, \ldots$, pokud nebude stanoveno jinak.

Poměrně dlouho trvalo, než si matematikové ujasnili, jak lze vlastně přirozená čísla zavést. Mezi několika možnostmi se nakonec prosadily čtyři axiomy, které teprve roku 1891 formuloval pomocí funkce „následníka“ italský matematik Giuseppe Peano (1858–1932). Výstižně charakterizují množinu přirozených čísel a nazývají se po něm *Peanovy axiomy:*

A1. *Existuje přirozené číslo, které není následníkem žádného přirozeného čísla.* Toto číslo budeme označovat symbolem 1.
A2. *Každé přirozené číslo má právě jednoho následníka.*
A3. *Každé přirozené číslo je následníkem nejvýše jednoho přirozeného čísla.*
A4. *Každá množina, která obsahuje přirozené číslo* 1 *a s každým přirozeným číslem obsahuje i jeho následníka, je množinou přirozených čísel.*

Na těchto axiomech je založena hlavní myšlenka principu matematické indukce. Pokud chceme dokázat, že nějaká vlastnost $V(n)$ platí pro všechna přirozená čísla n, pak nejprve dokážeme, že $V(n)$ platí pro $n = 1$. Potom dokážeme, že když vlastnost $V(n)$ platí pro nějaké přirozené číslo n, platí i $V(n+1)$ pro následníka $n+1$ čísla n. Odtud již plyne, že vlastnost platí pro všechna přirozená n.

Množinu celých čísel označíme

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Tato množina se tedy skládá z přirozených čísel, k nim opačných čísel (tj. se znaménkem minus) a nuly. Je uzavřena vůči operaci sčítání a násobení, tj. pro libovolná $m, n \in \mathbb{Z}$ je $m + n \in \mathbb{Z}$ a $m \cdot n \in \mathbb{Z}$. Na $\mathbb{Z}$ se zavádějí relace $=, <, >, \leq$ a $\geq$.

Množina přirozených čísel $\mathbb{N}$ je *dobře uspořádaná,* což znamená, že libovolná její neprázdná podmnožina má nejmenší prvek. Podobnou vlastnost nemá ani množina celých čísel $\mathbb{Z}$, ani množina racionálních čísel $\mathbb{Q}$ či reálných čísel $\mathbb{R}$. To, že je množina přirozených čísel dobře uspořádaná, je ekvivalentní principu matematické indukce, viz např. (Tattersall, 2005, s. 40). Je to vlastně axiom, tj. tvrzení, které se přijímá bez důkazu, protože neodporuje intuici.

Už v antice si Archimédes (287–212 př. n. l.) uvědomoval, že množina přirozených čísel je dobře uspořádaná.

Archimédův axiom. *Pro libovolná přirozená čísla j a k existuje přirozené číslo n tak, že $nj \geq k$.*

Archimédův axiom lze dokázat. Je to tedy matematická věta, ale z historických důvodů hovoříme o axiomu. Kdyby totiž nebyl pravdou, pak by existovala $j, k \in \mathbb{N}$ tak, že $nj < k$ pro každé $n \in \mathbb{N}$. Z dobrého uspořádání množiny $M = \{k - nj\,;\, n \in \mathbb{N}\} \subset \mathbb{N}$ plyne existence nejmenšího prvku m množiny M. Prvek $k-(m+1)j$ ale také leží v M a platí pro něj

$$k - (m+1)j = (k - mj) - j < k - mj,$$

což je ve sporu s minimalitou $k - mj$.

Archimédův axiom má hezkou geometrickou interpretaci. Říká vlastně, kolik úseček o délce j pokryje úsečku o délce k.

1.2. Jednoduchá kritéria dělitelnosti

Řekneme, že přirozené číslo d *dělí* (beze zbytku) přirozené číslo n, jestliže existuje $k \in \mathbb{N}$ tak, že $n = d \cdot k$. V tomto případě budeme psát

$$d \mid n,$$

např. $3 \mid 6$. Číslo d se nazývá *dělitel* čísla n a čísla 1 a n se nazývají *triviální* (*samozřejmí*) *dělitelé* čísla n. Jestliže $1 < d < n$, pak d se nazývá *netriviální dělitel,* a jestliže $d < n$, pak se d nazývá *vlastní dělitel* čísla n. Pokud m nedělí n, budeme psát $m \nmid n$, např. $5 \nmid 6$. Podobné definice lze zavést i pro celá záporná čísla. Celé číslo dělitelné dvěma se nazývá *sudé,* v opačném případě *liché.*

Věta 1.1. *Přirozené číslo n je dělitelné:*

a) *dvěma, je-li jeho poslední cifra sudá,*
b) *třemi, je-li jeho ciferný součet dělitelný* 3,

c) *čtyřmi, je-li jeho poslední dvojčíslí dělitelné* 4,
d) *pěti, je-li jeho poslední cifra* 0 *nebo* 5,
e) *šesti, je-li sudé a dělitelné* 3,
f) *sedmi, je-li dvojnásobek počtu stovek zvětšený o poslední dvojčíslí dělitelný* 7,
g) *osmi, je-li poslední trojčíslí dělitelné* 8,
h) *devíti, je-li jeho ciferný součet dělitelný* 9,
i) *desíti, je-li jeho poslední cifra* 0.

D ů k a z. Nechť n je libovolné přirozené číslo. V desítkové soustavě je lze jednoznačně napsat ve tvaru

$$n = c_k 10^k + \cdots + c_2 10^2 + c_1 10 + c_0, \qquad (1.1)$$

kde jeho cifry $c_k, \ldots, c_2, c_1, c_0$ jsou z množiny $\{0, 1, 2, \ldots, 9\}$ a $c_k \neq 0$. Z vyjádření (1.1) okamžitě plynou tvrzení a), c), d), g) a i).

Označme s ciferný součet čísla n, tj.

$$s = c_k + \cdots + c_2 + c_1 + c_0.$$

Pak

$$n - s = c_k(10^k - 1) + \cdots + c_2\, 99 + c_1\, 9,$$

kde každý sčítanec na pravé straně je dělitelný devíti. Proto je n dělitelné třemi, popř. devíti, právě tehdy, když s je dělitelné třemi, popř. devíti. Tedy platí b) a h).

Z a) a b) okamžitě plyne e). Zbývá dokázat f). Důkaz tohoto kritéria pochází od Václava Holuba. Dvojnásobek stovek čísla n zvětšený o poslední dvojčíslí je roven

$$m = 2c_k 10^{k-2} + \cdots + 2c_2 + 10c_1 + c_0.$$

Podle (1.1) vidíme, že rozdíl

$$n - m = 98c_k 10^{k-2} + \cdots + 98c_2$$

je dělitelný sedmi, protože $7 \mid 98$. Jestliže nyní 7 dělí m, potom 7 také dělí součet $m + (n - m) = n$. □

Příklad. Podle věty 1.1 okamžitě vidíme, že $7 \mid 1239$, protože 7 dělí $2 \cdot 12 + 39 = 63$.

Příklad. Pro větší čísla je většinou nutné použít příslušné pravidlo vícekrát za sebou. Například

$$3 \mid 188887777788885,$$

jelikož ciferný součet 105 je dělitený třemi a $3 \mid 6$.

Dělitelnosti číslem 11 se budeme věnovat v oddílu 5.1. Uveďme si ještě pravidla pro dělitelnost čísly 13, 17 a 19. Příslušné důkazy lze provést analogicky jako v důkazu věty 1.1.

Přirozené číslo n je dělitelné 13, jestliže čtyřnásobek poslední cifry přičtený k desítkám je dělitelný 13. Například $13 \mid 507$, protože 13 dělí $4 \cdot 7 + 50 = 78$.

Přirozené číslo n je dělitelné 17, jestliže pětinásobek poslední cifry odečtený od desítek je dělitelný 17. Například $17 \mid 357$, protože 17 dělí $35 - 5 \cdot 7 = 0$.

Přirozené číslo n je dělitelné 19, jestliže dvojnásobek poslední cifry přičtený k desítkám je dělitelný 19. Například $19 \mid 1026$, protože snadno zjistíme, že 19 dělí $2 \cdot 6 + 102 = 114$ a 19 dělí $11 + 2 \cdot 4 = 19$.

Připomeňme, že *kombinační číslo* $\binom{n}{m}$ (čti n nad m) je definováno vztahem

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} \quad \text{pro celá } n \geq m \geq 0,$$

kde

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n \quad \text{pro } n \in \mathbb{N}, \quad 0! = 1,$$

symbolu $n!$ říkáme *n faktoriál.*

Poznámka. Nechť $k = n - m$ je přirozené číslo. Pak platí

$$k!\binom{n}{m} = k!\frac{n!}{m!k!} = \frac{n!}{m!} = (m+1)(m+2)\cdots(m+k).$$

Vidíme tedy, že součin k po sobě jdoucích čísel na pravé straně je vždy dělitelný $k!$.

Navíc lze dokázat, že $(m+1)(m+2)\cdots(m+k)$ se pro $k>1$ nikdy nerovná mocnině n^j pro $j \geq 2$ a n přirozené (Erdős, Selfridge, 1975).

1.3. Nejmenší společný násobek a největší společný dělitel

Nechť m a n jsou libovolná přirozená čísla. Označme $M \subset \mathbb{N}$ množinu všech společných násobků čísel m a n. Množina M je zřejmě neprázdná, neboť obsahuje například součin mn. Protože je $\mathbb{N}$ dobře uspořádaná, musí M obsahovat svůj nejmenší prvek, který označíme $[m,n]$ a nazveme *nejmenším společným násobkem* čísel $m,n \in \mathbb{N}$. Je to tedy nejmenší přirozené číslo, které je dělitelné čísly m i n.

Podobně *největším společným dělitelem* dvou celých čísel m a n, která nejsou současně 0, je největší přirozené číslo, které dělí m i n. Největší společný dělitel čísel m a n budeme označovat (m,n).

Základní vlastností největšího společného dělitele a nejmenšího společného násobku je zřejmě

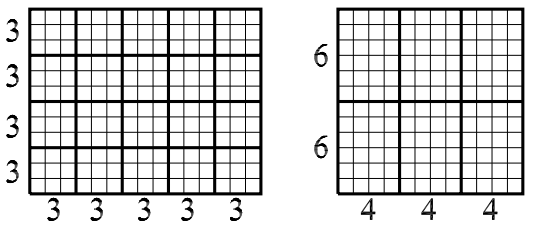
$$(m,n)=(n,m), \quad [m,n]=[n,m].$$

Pro $k,m,n \in \mathbb{N}$ platí též následující distributivní vlastnosti

$$[k,(m,n)]=([k,m],[k,n]) \quad \text{a} \quad (k,[m,n])=[(k,m),(k,n)].$$

Na obrázku 1.1 vidíme geometrickou interpretaci největšího společného dělitele a nejmenšího společného násobku. Levá část obrázku ukazuje, proč je největší společný dělitel čísel $m=12$ a $n=15$ roven 3. Čtverec o délce strany $(m,n)=3$ je největším čtvercem, kterým lze zcela vyplnit obdélník, jehož délky stran jsou 12 a 15. Můžeme si to též představit jako úlohu, v níž je zapotřebí rozstříhat čtverečkovaný papír o rozměrech 12×15 na co možná největší stejně velké čtverce. Délka jejich strany je pak největším společným dělitelem.

Podobně pravá část obrázku ilustruje, proč je nejmenší společný násobek čísel $m = 6$ a $n = 4$ roven 12. Čtverec o délce strany $[m, n] = 12$ je tak vlastně nejmenším čtvercem, který lze vyplnit shodnými obdélníky o délkách stran 6 a 4.



Obr. 1.1. Geometrická interpretace největšího společného dělitele a nejmenšího společného násobku. Obrázek znázorňuje, proč (12, 15) = 3 a [6, 4] = 12.

Věta 1.2. *Pro každá dvě přirozená čísla m a n platí*

$$mn = (m, n)[m, n]. \tag{1.2}$$

D ů k a z. Označme $d \geq 1$ libovolný společný dělitel čísel m a n. Pak $\frac{m}{d}$ i $\frac{n}{d}$ jsou přirozená čísla, $\frac{m}{d}n$ je celočíselný násobek čísla n a $\frac{n}{d}m$ je celočíselný násobek čísla m. Tudíž $\frac{mn}{d}$ je společný násobek čísel m a n. Jestliže je nyní d největší společný dělitel čísel m a n, musí být $\frac{mn}{d}$ nejmenší společný násobek m a n. □

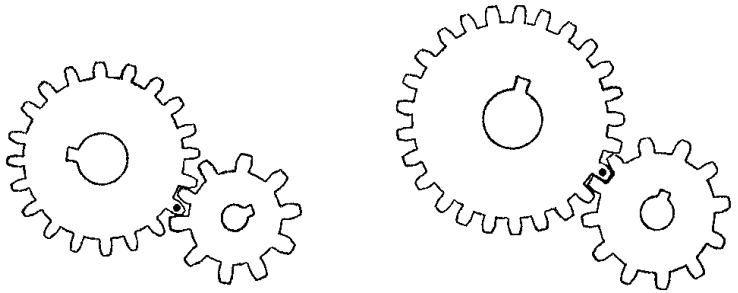
Příklad. Pro $m = 18$ a $n = 27$ je $(m, n) = 9$, $[m, n] = 54$, a tedy $18 \cdot 27 = 9 \cdot 54$.

Největší společný dělitel a nejmenší společný násobek více než dvou čísel lze definovat indukcí podobně jako pro dvě čísla. Pro $k > 2$ a celá čísla $n_1, \ldots, n_k$ položíme

$$(n_1, \ldots, n_{k-1}, n_k) = \big((n_1, \ldots, n_{k-1}), n_k\big),$$
$$\text{jestliže } n_j \neq 0 \text{ pro nějaké } j \in \{1, \ldots, k-1\},$$
$$[n_1, \ldots, n_{k-1}, n_k] = \big[[n_1, \ldots, n_{k-1}], n_k\big],$$
$$\text{jestliže } n_1 n_2 \cdots n_k \neq 0.$$

1.4. Nesoudělná čísla

Přirozená čísla m a n nazveme *nesoudělná,* jestliže $(m, n) = 1$. Zajímavá aplikace nesoudělných čísel se uvádí v příručce (Sedláček, 1977, s. 38). Na obrázku 1.2 vidíme dva převody ozubených kol. V levé části obrázku má větší kolo 20 zubů a menší 10 zubů. Bude-li jeden zub většího kola mírně poškozený (na obr. 1.2 je označen tečkou), pak po každé otáčce většího kola zapadne přesně do stejné mezery menšího kola a v tomto místě se menší kolo bude velmi rychle opotřebovávat. Naproti tomu v pravé části obrázku 1.2 má větší kolo 25 zubů a menší 12 zubů. Protože $(25, 12) = 1$, bude docházet ke zcela rovnoměrnému opotřebovávání. Přitom poměr počtu zubů je v obou případech téměř stejný: 2 a 2.083.



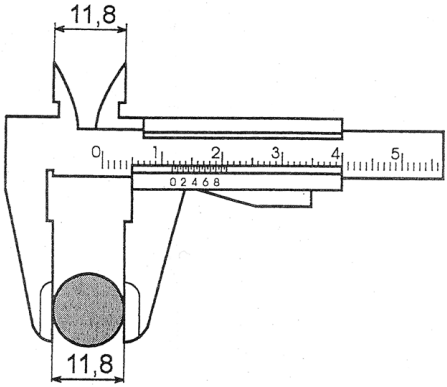
Obr. 1.2. Pro počet zubů levého převodu platí $(20, 10) = 10$, pro pravý máme $(25, 12) = 1$.

Na obrázku 1.3 vidíme automobilové kolo s poklicí uchycenou 4 šrouby, která má 5 otvorů pro ventilek. To, že jsou čísla 4 a 5 nesoudělná, má opět jistou výhodu. Pokud se při nasazování poklice přímo netrefíme s ventilkem do příslušného otvoru, pak poklici postupně zkoušíme nasadit při otočkách o 90°, popř. 180° nebo 270°, přičemž poloha otvorů vzhledem k ventilku bude pokaždé jiná. To nám umožňuje v jedné z těchto poloh prostrčit ventilek otvorem skrze poklici. Můžete si vyzkoušet, že při otočení poklice o 90° se celá konfigurace otvorů pro ventilek zdánlivě pootočí

o $18° = 90° - 72° = 72°/4 = 360°/(4 \times 5)$. Pokud by byl počet otvorů 2, 4, 6 nebo 8 (tj. soudělný s počtem šroubů 4), pak tolik různých možností nasazení poklice nedostaneme.

Obr. 1.3. Pro počet šroubů a otvorů platí $(4, 5) = 1$.

Uveďme další praktické použití nesoudělných čísel. Pevná část posuvného měřítka je vybavena stupnicí, v níž každý centimetr je rozdělen na 10 mm. Na pohyblivé části k ní těsně přiléhá tzv. nonius rozdělený na 10 stejně dlouhých dílků, které mají dohromady 9 milimetrů (obr. 1.4). To, že jsou délky 9 mm a 10 mm nesoudělné, nám umožňuje zjišťovat rozměry drobných předmětů s přesností na desetiny milimetru. Při měření určujeme, kolikátý dílek nonia splynul s některým dílkem milimetrové stupnice. Tolik desetin milimetru pak přičteme k naměřeným milimetrům (tj. k jejich největší celočíselné hodnotě). Kdybychom místo 9 mm zvolili délku soudělnou s 10 mm, pak by se současně krylo několik rysek a nevěděli bychom, který údaj platí. Autorem této vtipné myšlenky je portugalský královský kosmograf Pedro Nunes (1502–1578), který ji poprvé použil pro přesná měření úhlu. Zařízení podobné noniu se používá také u mikrometrů.



Obr. 1.4. Nonius na posuvném měřítku.

1.5. Eukleidův algoritmus

Pro výpočet největšího společného dělitele (m, n) dvou velkých přirozených čísel $m \geq n$ se s oblibou používá známý *Eukleidův algoritmus,* který lze stručně charakterizovat takto:

Jestliže n dělí m, pak $(m, n) = n$. V opačném případě je

$$(m, n) = (n, z),$$

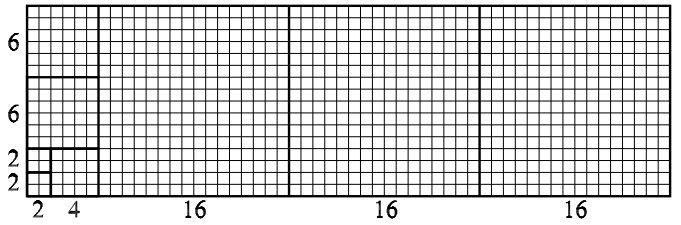
kde $z \geq 1$ je zbytek při dělení čísla m číslem n. Protože $z < m$, větší problém se tak převádí na menší. Další kroky algoritmu pak probíhají obdobně. Problém se redukuje na menší a menší, dokud nedostaneme zbytek 0.

Například pro $m = 54$ a $n = 16$ pomocí Eukleidova algoritmu dostáváme

$$(54, 16) = (16, 6) = (6, 4) = (4, 2) = 2.$$

Nyní si opět představme, že máme čtverečkovaný papír o rozměrech 54×16 (obr. 1.5). Z něj budeme postupně odstřihávat co možná největší čtverce, dokud to půjde, tj. v prvním kroku odstřihneme 3 čtverce o délce strany 16, v dalším kroku odstřihneme 2 čtverce o délce strany 6 atd. Délka strany čtverce, který nám zů-

stane, je výsledkem Eukleidova algoritmu, tj. největším společným dělitelem čísel 54 a 16.



Obr. 1.5. Geometrické znázornění redukce při použití Eukleidova algoritmu pro výpočet největšího společného dělitele (54, 16).

Pokud jsou čísla m a n nesoudělná, Eukleidův algoritmus končí nejmenším možným čtvercem 1×1. Například dvě po sobě jdoucí čísla jsou vždy nesoudělná.

Pro výpočet nejmenšího společného násobku $[m, n]$ je také vhodné aplikovat nejprve Eukleidův algoritmus, protože $(m, n) \leq [m, n]$, a pak použít vztah (1.2). K Eukleidovu algoritmu se ještě vrátíme v oddílu 7.1.

1.6. Lineární diofantské rovnice

Název diofantská rovnice je odvozen od jména řeckého matematika *Diofanta,* který žil v Alexandrii ve 3. století našeho letopočtu a zabýval se řešením rozličných úloh z teorie čísel. Diofantské rovnice jsou rovnice s celočíselnými koeficienty, jejichž řešení se hledá mezi celými čísly. Při řešení soustav diofantských rovnic máme většinou více neznámých než rovnic. V tomto oddílu se budeme zabývat jen jednou lineární diofantskou rovnicí se dvěma celočíselnými neznámými. Poznamenejme, že se někdy používá i termín diofantovská, diofantická či neurčitá rovnice.

Věta 1.3. *Nechť* $k = (m, n)$ *pro nějaká celá čísla* m *a* n, *která*

nejsou současně nulová. Pak existují celá čísla x a y tak, že

$$mx + ny = k. \tag{1.3}$$

D ů k a z. Nechť S je množina všech celých čísel tvaru $ma + nb$, kde a a b jsou celá čísla. Číslo m nebo n není nula, a tudíž množina S obsahuje nenulová celá čísla. Protože $t = ma + nb$ je v S, číslo $-t = (-m)a + (-n)b$ je také v S. Tedy S obsahuje přirozená čísla. Protože množina přirozených čísel je dobře uspořádaná (viz oddíl 1.1), existuje nejmenší přirozené číslo d v S tvaru $d = mx + ny$. Tvrdíme, že $d = (m, n)$.

Nejprve ukážeme, že d je společný dělitel m a n. Buď $u = ma_0 + nb_0$ libovolný prvek S. Dělením zjistíme, že $u = qd + r$, kde $0 \leq r < d$ je zbytek. Tedy platí

$$ma_0 + nb_0 = q(mx + ny) + r,$$

tj.

$$r = m(a_0 - qx) + n(b_0 - qy)$$

a $r \in S$. Protože $r \geq 0$ a $r < d$, platí, že $r = 0$ díky volbě d. Tudíž d dělí u pro každé $u \in S$. Avšak $m = m \cdot 1 + n \cdot 0 \in S$ a $n = m \cdot 0 + n \cdot 1 \in S$, což znamená, že d dělí jak m, tak n.

Konečně nechť e je libovolný společný dělitel čísel m a n. Pak e dělí $mx + ny = d$, a proto $d = (m, n) = k$. □

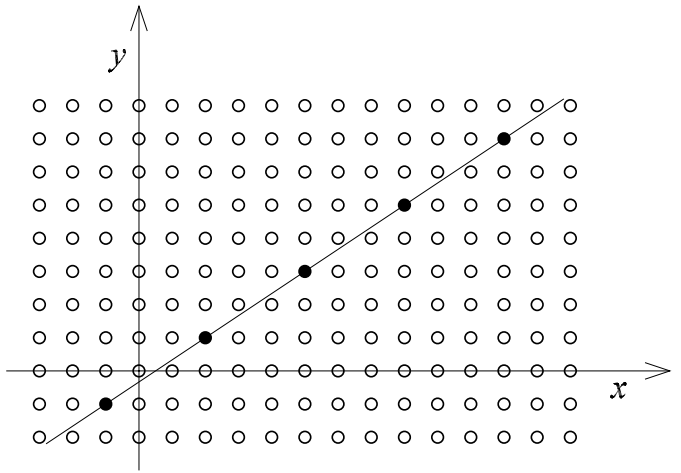
Věta 1.3, viz (Burton, 1998, s. 22), má velice pěknou geometrickou interpretaci. Každá přímka $mx + ny = k$ totiž prochází mřížovými body (x, y), které jsou řešením lineární diofantské rovnice (obr. 1.6 pro $m = 2$, $n = -3$ a $k = 1$).

Příklad. Ukažme, jak vyřešit následující diofantskou rovnici

$$8x - 27y = 1$$

metodou podobnou Eukleidovu algoritmu. Protože $(8, 27) = 1$, má podle věty 1.3 tato rovnice řešení a platí

$$x = 3y + \frac{3y + 1}{8}.$$



Obr. 1.6. Přímka odpovídající lineární diofantské rovnici $2x - 3y = 1$ prochází body o souřadnicích $\ldots, (-1, -1), (2, 1), (5, 3), (8, 5), (11, 7), \ldots$.

Abychom dostali celočíselné řešení, musí být $3y + 1$ násobkem 8, tj. existuje celé číslo v tak, že

$$3y + 1 = 8v, \quad \text{a tedy } y = 2v + \frac{2v - 1}{3}.$$

Můžeme tedy zvolit $v = 2$ a pomocí zpětné substituce dostaneme, že dvojice $y = 5$ a $x = 17$ je řešení. Pro $v = 5, 8, 11, \ldots$ a $v = -1, -4, -7, \ldots$ získáme další dvojice řešení.

1.7. Kongruence

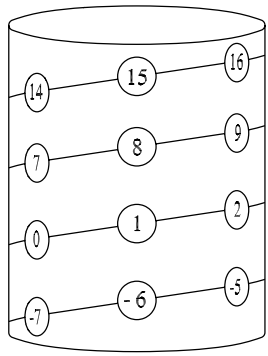
V tomto oddílu se zmíníme o pojmu kongruence, který zavedl německý matematik Carl Friedrich Gauss. Používal jej k nejrůznějším výpočtům, např. k výpočtu, na který den připadne velikonoční neděle (viz poznámka v dalším textu). Kongruence mají mnoho dalších praktických aplikací v kryptografii, v astronomii při sestavování kalendářů (Burton, 1998, s. 122), při generování pseudonáhodných čísel aj., jak ostatně ještě uvidíme v kapitole 5.

Nechť n, z jsou celá čísla a $m \in \mathbb{N}$. Pak říkáme, že *n je kongruentní se z modulo m* a píšeme

$$n \equiv z \pmod{m},$$

jestliže $n - z$ je dělitelné m. Číslo m se nazývá *modul.*

Předpokládejme například, že $m = 7$. Představme si, že na nekonečně dlouhý válec rovnoměrně navineme provázek, který má na sobě rovnoměrně rozložené očíslované značky, jak je znázorněno na obrázku 1.7. Čísla, která jsou ve svislých řadách pod sebou, jsou vzájemně kongruentní. Například $16 \equiv -5 \pmod{7}$, jelikož $16 - (-5) = 21$ je dělitelné sedmi. Na ciferníku klasických hodin lze podobně demonstrovat kongruenci modulo 12.



Obr. 1.7. Geometrická interpretace kongruence modulo 7.

Nyní odvodíme některá početní pravidla pro počítání s kongruencemi. Zřejmě $a \equiv a \pmod{m}$ pro každé celé číslo a. Jestliže $a \equiv b \pmod{m}$, pak pro libovolná celá čísla a, b, c a $k \geq 0$ snadno nahlédneme, že

$$\begin{aligned} b &\equiv a \pmod{m}, \\ a \pm c &\equiv b \pm c \pmod{m}, \\ ac &\equiv bc \pmod{m}, \\ a^k &\equiv b^k \pmod{m}, \end{aligned} \tag{1.4}$$

kde poslední kongruence plyne z rovnosti

$$a^k - b^k = (a-b)\big(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}\big), \quad k > 1.$$

Z uvedených vztahů je patrné, že relace „$\equiv$“ modulo m je reflexivní a symetrická. Protože platí i tranzitivita, je to vlastně relace ekvivalence na množině celých čísel.

Jestliže $(c, m) = 1$, potom v kongruenci $ac \equiv bc \pmod{m}$ můžeme krátit c, tj. $a \equiv b \pmod{m}$. Pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, pak zřejmě

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

a navíc

$$ac \equiv bd \pmod{m}. \tag{1.5}$$

Pro $a = b + im$ a $c = d + jm$ vskutku platí $ac = bd + (jb + id + ijm)m$, a proto kongruence (1.5) je splněna.

Poznámka. Gaussův algoritmus výpočtu, na který den v roce r připadne velikonoční neděle, probíhá takto: Pro období 1900–2099 zvolíme $m = 24$ a $n = 5$. Nechť a, b, c, d, e jsou nejmenší nezáporná čísla splňující kongruence[1)] $a \equiv r \pmod{19}$, $b \equiv r \pmod{4}$, $c \equiv r \pmod{7}$, $d \equiv (m + 19a) \pmod{30}$ a $e \equiv (n + 2b + 4c + 6d) \pmod{7}$. Pak pro $d + e < 10$ připadá velikonoční neděle na březnový den, který vypočteme jako $(22 + d + e)$, pro $d + e = 35$ připadá na $(d + e - 16)$-tý den dubnu a ve zbývajících případech měsíce dubna na $(d + e - 9)$.

Tento algoritmus má ale dvě výjimky. V letech 1954 a 2049 není velikonoční neděle 25. dubna, ale o týden dříve, podrobnosti viz (www13).

Uveďme ještě několik zajímavých kongruencí. Snadno lze ověřit, že

$$n^5 \equiv n \pmod{10} \quad \forall n \in \mathbb{N},$$

[1)] Zde $a + 1$ je tzv. *zlaté číslo* (pořadové číslo roku v Metonově devatenáctiletém cyklu, v němž se téměř přesně vystřídá 235 synodických měsíců, tj. od novu k novu).

tj. pátá mocnina každého přirozeného čísla n končí na stejnou cifru jako samotné n. Pro libovolnou cifru c navíc platí

$$c^{2k} \equiv (10 - c)^{2k} \pmod{10}$$

a

$$c^{2k-1} + (10 - c)^{2k-1} \equiv 10 \pmod{10}.$$

Odtud například vidíme, že třetí mocnina čísla, jež končí na $c = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, bude končit na $0, 1, 8, 7, 4, 5, 6, 3, 2, 9$.

1.8. Čínská věta o zbytcích

Staročínský matematik Sun Zi kolem 4.–5. století formuloval ve své knize o aritmetice následující úlohu (Martzloff, 1977, s. 90, 310):

Nechť x označuje určitý počet předmětů. Počítáme-li je po trojicích, zbudou dva, počítáme-li je po pěticích, zbudou tři, a konečně počítáme-li je po sedmicích, zbudou dva. Kolik je x?

Tuto úlohu můžeme zřejmě převést na soustavu tří kongruencí pro neznámou hodnotu x:

$$x \equiv 2 \pmod{3}, \tag{1.6}$$

$$x \equiv 3 \pmod{5}, \tag{1.7}$$

$$x \equiv 2 \pmod{7}. \tag{1.8}$$

Úlohu (1.6)–(1.8) lze též formulovat takto: Mám určitý počet jüanů. Kdybych si koupil slepice po třech jüanech, zbyly by mi 2 jüany, kdybych si koupil králíky po pěti jüanech, zbyly by mi 3 jüany, a kdybych si koupil krocany po sedmi jüanech, zbyly by mi 2 jüany. Kolik mám jüanů? Proto Číňané úlohám podobného typu říkají „peněžní problém“. Yang Hui ve své knize z roku 1275 uvádí dalších pět podobných příkladů, viz opět (Martzloff, 1977, s. 311).

Než ukážeme, jaká je geometrická interpretace soustavy (1.6)–(1.8), budeme se zabývat jednodušší úlohou:

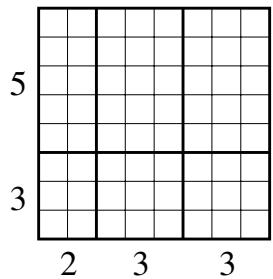
Před domem stojí schodiště. Jdu-li nahoru po třech schodech, zbudou mi dva. Jdu-li po pěti schodech, zbudou mi nahoře tři. Kolik má schodiště schodů?

Vidíme, že tato úloha se dá napsat pomocí kongruencí (1.6) a (1.7), tj.

$$x \equiv 2 \pmod 3,$$
$$x \equiv 3 \pmod 5,$$

kde x je počet schodů. Odečteme-li od sebe odpovídající rovnice $x = 3i+2$ a $x = 5j+3$, dostaneme $0 = 3i-5j-1$, tj. $j = \dfrac{3i-1}{5}$ a volba $i = 2 + 5n$ dává řešení $x = 8 + 15n$ pro $n \geq 0$, neboť schodiště nemůže mít záporný počet schodů.

Na obrázku 1.8 je znázorněn čtverec, jehož délku strany $x = 8$ hledáme. Ta odpovídá nejmenšímu řešení pro $n = 0$. Vidíme, že čtverec je rozdělen na několik obdélníků. V levé dolní části je obdélník, jehož délky stran odpovídají zbytkům 2 a 3. V pravé horní části jsou dva obdélníky, jejichž délky stran odpovídají modulům 3 a 5. Rozměry zbývajících obdélníků jsou zkombinovány ze zbytků a modulů. Počty dílků vyznačené na vodorovné straně čtverce jsou obsaženy v první kongruenci, na svislé straně pak ve druhé.



Obr. 1.8. Geometrická interpretace úlohy (1.6)–(1.7).

Nyní uvedeme jednu z nejpoužívanějších vět teorie čísel, která umožňuje řešit úlohy těchto typů, jež vedou na soustavy lineárních kongruencí o jedné neznámé (viz např. (1.6)–(1.8)). Je velice po-

dobná Eukleidovu algoritmu. Na mnoha dalších místech této knihy uvidíme její užitečnost. Protože důkaz bude konstruktivní, lze příslušný algoritmus použít k řešení konkrétní soustavy lineárních kongruencí.

Věta 1.4 (Čínská věta o zbytcích). *Nechť $m_1, m_2, \ldots, m_k$ jsou po dvojicích nesoudělná přirozená čísla. Pak pro soustavu kongruencí*

$$\begin{aligned} x &\equiv r_1 \pmod{m_1}, \\ x &\equiv r_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv r_k \pmod{m_k}, \end{aligned} \tag{1.9}$$

kde r_i jsou celá čísla, existuje právě jedno řešení x modulo m, kde

$$m = m_1 m_2 \cdots m_k.$$

D ů k a z. Nejprve dokážeme existenci řešení x. Definujme n_i pomocí rovnic

$$m = m_1 n_1 = m_2 n_2 = \cdots = m_k n_k. \tag{1.10}$$

Protože m_i a n_i jsou nesoudělná, existují podle věty 1.3 celá čísla y_i, $i = 1, 2, \ldots, k$, tak, že

$$n_i y_i \equiv 1 \pmod{m_i}. \tag{1.11}$$

Tvrdíme, že obecné řešení systému (1.9) má tvar

$$x \equiv r_1 n_1 y_1 + r_2 n_2 y_2 + \cdots + r_k n_k y_k \pmod{m}. \tag{1.12}$$

Abychom ověřili, že takové číslo x řeší soustavu (1.9), zvolíme $i \in \{1, \ldots, k\}$. Ze vztahu (1.10) vidíme, že všechny členy kromě i-tého členu na pravé straně (1.12) obsahují činitel m_i, a tedy

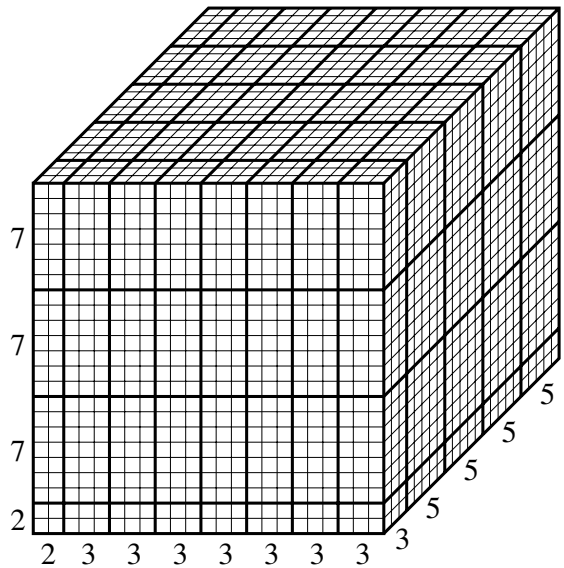
$$x \equiv r_1 n_1 y_1 + r_2 n_2 y_2 + \cdots + r_k n_k y_k \equiv r_i n_i y_i \equiv r_i \pmod{m_i},$$

kde poslední ekvivalenci dostaneme vynásobením kongruence (1.11) číslem r_i.

Abychom dokázali jednoznačnost, předpokládejme, že x_1 a x_2 jsou dvě řešení soustavy (1.9). Pak $x_1 \equiv x_2 \pmod{m_i}$ pro každé

$i = 1, \ldots, k$. Protože m_i jsou po dvojicích nesoudělná čísla, máme $x_1 \equiv x_2 \pmod{m}$. Tudíž řešení (1.9) je určeno jednoznačně modulo m. □

Použijeme-li větu 1.4 na systém (1.6)–(1.8), kde $(3, 5, 7) = 1$, najdeme nejmenší kladné řešení $x = 23$. Jeho geometrické znázornění lze nalézt na krychli z obrázku 1.9. Tato krychle o hraně délky 23 je rozdělena na množství menších kvádrů. Přední levý dolní kvádr má rozměry $2 \times 3 \times 2$ odpovídající zbytkům soustavy (1.6)–(1.8). Zadní pravá horní část krychle je rozdělena na kvádry o rozměrech $3 \times 5 \times 7$, které odpovídají modulům. Rozměry zbývajících kvádrů jsou opět zkombinovány ze zbytků a modulů.



Obr. 1.9. Geometrická interpretace Čínské věty o zbytcích pro systém kongruencí (1.6)–(1.8).

V 13. století řešil Qin Jiushao kongruence (1.11) pomocí metody připomínající Eukleidův algoritmus, viz (Martzloff, 1977, s. 317) nebo příklad v oddílu 1.6. Úloha nalezení y_i splňující kongruenci

(1.11) totiž může být převedena na řešení diofantské rovnice

$$n_i y_i - m_i v_i = 1$$

pro neznámé y_i a v_i.

Uspořádané n-tice budeme v této knize psát do lomených závorek, protože kulaté závorky jsou již vyhrazeny pro největší společný dělitel. Čínská věta o zbytcích vlastně říká, že každé přirozené číslo x nepřevyšující $m = m_1 m_2 \cdots m_k$ lze jednoznačně určit pomocí k-tice zbytků $\langle r_1, r_2, \ldots, r_k \rangle$ po dělení čísly $m_1, m_2, \ldots, m_k$, kde

$$0 \leq r_i < m_i, \quad i = 1, 2, \ldots, k.$$

Říká se tomu sinoreprezentace (Schroeder, 2006). Například pro $k = 2$, $m_1 = 3$ a $m_2 = 5$ dostaneme tabulku:

r_2	0	1	2	3	4
$r_1 = 0$	0	6	12	3	9
$r_1 = 1$	10	1	7	13	4
$r_1 = 2$	5	11	2	8	14

Vidíme, že vnitřek tabulky obsahuje každé z čísel od 0 do 14 právě jednou. Povšimněme si dále, že tato čísla se zvětšují o jednu ve směru diagonál. Podobná struktura založená na sinoreprezentaci sehrála důležitou roli též při vytvoření tradičního čínského kalendáře, který má šedesátiletý cyklus, viz obr. 1.10.

Řádky odpovídají 12 zemským větvím a sloupce 10 nebeským kmenům. Každý řádek je zasvěcen nějakému zvířeti a každý dvojsloupec odpovídá některému z pěti prvků, z nichž je složen vesmír. Více podrobností o čínském kalendáři naleznete v článcích (Křížek, Liu, 1996) a (Křížek, Liu, Šolcová, 2005/06).

Čínská věta o zbytcích má řadu dalších praktických aplikací (Schroeder, 2006) při výpočtu konvolucí, Fourierovy transformace, kvadratických kongruencí apod.

	ťia	i	ping	ting	wu	ťi	keng	sin	žen	kuej	
c’	1		13		25		37		49		myš
čchou		2		14		26		38		50	kráva
jin	51		3		15		27		39		tygr
mao		52		4		16		28		40	králík
čchen	41		53		5		17		29		drak
s’		42		54		6		18		30	had
wu	31		43		55		7		19		kůň
wej		32		44		56		8		20	ovce
šen	21		33		45		57		9		opice
jou		22		34		46		58		10	kuře
sü	11		23		35		47		59		pes
chaj		12		24		36		48		60	prase
	dřevo		oheň		země		kov		voda		

Obr. 1.10. Tradiční čínský kalendář.

1.9. Dirichletův princip

Pomocí Dirichletova principu většinou dokazujeme existenci takových objektů, které nelze zkonstruovat, anebo je jejich konstrukce velice obtížná.

Věta 1.5 (Dirichletův princip). *Nechť $n \in \mathbb{N}$. Je-li více než n předmětů rozděleno do n skupin, pak v alespoň jedné skupině se nacházejí alespoň dva předměty.*

Důkaz. Nechť k_i je počet předmětů v i-té skupině pro $i = 1, 2, \ldots, n$. Kdyby v každé skupině byl nejvýše jeden předmět, tj. $k_i \leq 1$ pro všechna $i = 1, 2, \ldots, n$, potom by počet všech předmětů byl

$$k_1 + k_2 + \cdots + k_n \leq 1 + 1 + \cdots + 1 = n,$$

což je spor. □

Dirichletův princip lze dokázat i matematickou indukcí (Rychlík, 1950, s. 150). Na první pohled vypadá jako velice jednoduché tvrzení. Jeho vhodným použitím však lze získat velice silné výsledky, jak ostatně ještě uvidíme při důkazu Fermatovy vánoční věty 3.12. Pomocí něj lze například snadno dokázat, že v Praze existují alespoň dva lidé, kteří mají stejný počet vlasů.

Je známo, že žádný člověk nemá více než $n = 100\,000$ vlasů a že Praha má více než jeden milion obyvatel. Její obyvatele rozdělme do skupin tak, že do i-té skupiny dáme všechny obyvatele Prahy, kteří mají právě i vlasů, kde $i = 0, 1, \ldots, n$. Protože Pražanů je více než počet skupin, musí být podle Dirichletova principu v alespoň jedné skupině alespoň dva občané (ve skutečnosti mnohem více) se stejným počtem vlasů.

Tento příklad názorně ukazuje, jak se Dirichletův princip používá. Přitom najít konkrétní dva občany, kteří mají stejný počet vlasů, by bylo v praxi velice obtížné.

Věta 1.6. *Je-li dáno $n + 1$ přirozených čísel, pak mezi nimi existují dvě, jejichž rozdíl je dělitelný n.*

D ů k a z. Rozdělme čísla do n skupin podle toho, jaký zbytek dávají při dělení n, tj. do první skupiny dáme ta čísla, která dávají zbytek 0, do druhé skupiny ta, která dávají zbytek 1 atd. Do poslední skupiny dáme čísla, která dávají zbytek $n - 1$. Podle věty 1.5 existuje alespoň jedna skupina obsahující dvě čísla, která dávají stejný zbytek při dělení n. Jejich rozdíl je tedy dělitelný n. □

Příklad. Dokážeme, že existuje mocnina čísla 37, která končí na 00001. Uvažujme čísla

$$37,\ 37^2,\ 37^3, \ldots,\ 37^{100001},$$

jež rozdělíme do $n = 10^5$ skupin tak, že do i-té skupiny dáme ty mocniny 37^k, které dávají po vydělení číslem n zbytek i pro $i = 0, 1, 2, \ldots, n - 1$. (Nulový zbytek přitom dostat nemůžeme, protože čísla 37^m a n jsou nesoudělná.) Pak ale podle věty 1.6

existují dvě přirozená čísla $j > m$ tak, že

$$37^j - 37^m = 37^m\,(37^{j-m} - 1)$$

je dělitelné n. Protože $(37^m, n) = 1$, rozdíl $37^{j-m} - 1$ je dělitelný n, a tedy 37^{j-m} dává po dělení n zbytek 1.

Množství podobných příkladů lze nalézt např. v knížce (Bukovský, Kluvánek, 1970).

2. PRVOČÍSLA A ČÍSLA SLOŽENÁ

Prvočísla jsou surovinou,
z níž máme postavit aritmetiku,
a Eukleidova věta je zárukou,
že pro tento úkol máme
dostatečné množství materiálu.

G. H. Hardy
Obrana matematikova, 1999

2.1. Základní věta aritmetiky

Přirozené číslo p se nazývá *prvočíslo,* jestliže p má právě dva různé dělitele. Každé prvočíslo p je tedy větší než jedna a je dělitelné sebou samým a jednou. Přirozená čísla větší než jedna, která nejsou prvočísly, se nazývají *složená.*

Přirozená čísla se tak dělí na jednotku 1, prvočísla (např. 2, 3, 5, 7, 11, 13, ...) a čísla složená (např. 4, 6, 8, 9, 10, 12, 14, ...).

Věta 2.1 (První Eukleidova věta). *Je-li p prvočíslo a $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.*

Důkaz. Jestliže $p \mid a$, jsme hotovi. Pokud $p \nmid a$, pak $(a, p) = 1$ a podle věty 1.3 existují celá čísla x a y tak, že $ax + py = 1$, a tedy

$$abx + pby = b.$$

Protože $p \mid ab$ a $p \mid p$, vidíme, že $p \mid b$. □

Jako důsledek dostáváme následující Základní větu aritmetiky, která tvrdí, že každé přirozené číslo $n > 1$ lze jednoznačně napsat jako součin přirozených mocnin prvočísel $p_1 < p_2 < \cdots < p_r$:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}, \tag{2.1}$$

kde $\alpha_i \in \mathbb{N}$ pro $i \in \{1, \ldots, r\}$ a symbol $\prod$ označuje součin. Čísla p_i se nazývají *prvočinitelé.*

Věta 2.2 (Základní věta aritmetiky). *Jestliže*

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

kde $p_1 < p_2 < \cdots < p_r$, $q_1 < q_2 < \cdots < q_s$ *jsou prvočísla a* $r, s, \alpha_i, \beta_i \in \mathbb{N}$, *pak*

$$r = s, \quad p_i = q_i, \quad \alpha_i = \beta_i$$

pro každé $i = 1, \ldots, r$.

D ů k a z. Nechť $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ a nechť $m = n$. Jestliže nějaké prvočíslo p dělí m, pak podle První Eukleidovy věty 2.1 prvočíslo p musí dělit p_k pro nějaké $k \in \{1, \ldots, r\}$. Z definice prvočísla však plyne, že $p = p_k$. Protože $m = n$, musí p dělit také nějaké q_ℓ pro $\ell \in \{1, \ldots, s\}$ a stejným způsobem dostaneme, že $p = q_\ell$. Odtud plyne, že $p_k = q_\ell$. Protože prvočísla p_i a q_j jsou srovnána podle velikosti, musí platit $p_1 = q_1, \ldots, p_r = q_r$ a $r = s$.

Předpokládejme dále, že $\alpha_i > \beta_i$ pro nějaké $i \in \{1, \ldots, r\}$. Vydělíme-li rovnost $m = n$ mocninou p^{β_i}, dostaneme

$$p_1^{\alpha_1} \cdots p_i^{\alpha_i - \beta_i} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_i^0 \cdots p_r^{\beta_r},$$

což je spor, neboť levá strana rovnice je dělitelná p_i, zatímco pravá strana nikoliv. Podobně dojdeme ke sporu i v případě, kdy $\alpha_i < \beta_i$. Tedy $\alpha_i = \beta_i$ pro všechna $i \in \{1, \ldots, r\}$. □

Základní věta aritmetiky měla neobvyklé praktické použití v poselství mimozemským civilizacím, jak ještě uvidíme v oddílu 5.7.

Poznámka. Analogická věta o jednoznačnosti rozkladu v jiných algebraických strukturách vůbec nemusí platit. Například v tělese $Q(\mathrm{i}\sqrt{5})$, bližší informace o tomto tělese lze nalézt např. v (Hardy, Wright, 1979, s. 211), můžeme rozložit číslo 21 dvěma odlišnými způsoby na součin dvou ireducibilních (tj. dále nerozložitelných)

prvků

$$21 = 3 \cdot 7 \quad \text{a} \quad 21 = 1 + 2^2 \cdot 5 = (1 + 2\mathrm{i}\sqrt{5})(1 - 2\mathrm{i}\sqrt{5}).$$

Poznámka. Jedním z důvodů, proč 1 není prvočíslem, je ten, že bychom neměli jednoznačnost exponentů v (2.1), např. $1 = 1^2 = 1^3$. Dalším důvodem je vyjádření tzv. Riemannovy ζ-funkce pomocí součinu přes všechna prvočísla, viz (3.19).

Podle Základní věty aritmetiky 2.2 pro $m, n \in \mathbb{N}$ můžeme psát

$$m = \prod_{i=1}^{\infty} p_i^{k_i}, \quad n = \prod_{i=1}^{\infty} p_i^{\ell_i},$$

kde p_i je i-té prvočíslo a $k_i, \ell_i \geq 0$ pro všechna $i \in \mathbb{N}$ (speciálně když $m = 1$, pak všechna $k_i = 0$). Největší společný dělitel a nejmenší společný násobek dvou přirozených čísel m a n lze vypočítat takto

$$(m, n) = \prod_{i=1}^{\infty} p_i^{\min(k_i, \ell_i)}, \quad [m, n] = \prod_{i=1}^{\infty} p_i^{\max(k_i, \ell_i)}.$$

2.2. Eukleidova věta o nekonečnosti prvočísel

Je zajímavé, že můžeme najít libovolně dlouhé úseky po sobě jdoucích složených čísel. Ukažme si to na jednoduchém příkladu.

Příklad. Pro libovolné $n > 1$ uvažujme konečnou posloupnost

$$n! + 2,\ n! + 3, \ldots,\ n! + n,$$

která obsahuje $n - 1$ po sobě jdoucích čísel. Vidíme, že první člen této posloupnosti je dělitelný dvěma, druhý třemi atd. Konečně poslední člen je dělitelný n. Například pro $n = 1001$ dostáváme 1000 po sobě následujících složených čísel. Na druhé straně platí tvrzení, které lze nalézt už u starořeckého matematika Eukleida v jeho třináctidílném spisu *Základy*.

Věta 2.3 (Druhá Eukleidova věta). *Prvočísel je nekonečně mnoho.*

D ů k a z. Předpokládejme naopak, že existuje jen konečně mnoho prvočísel $p_1, p_2, \ldots, p_n$ a položme

$$m = p_1\, p_2 \cdots p_n + 1. \tag{2.2}$$

Protože podíl m/p_i dá vždy zbytek 1, žádné p_i nedělí m. Podle Základní věty aritmetiky 2.2 je tedy číslo m dalším prvočíslem, anebo je m dělitelné prvočíslem různým od $p_1, p_2, \ldots, p_n$, což je spor. □

Složených čísel je také nekonečně mnoho, jak plyne z věty 2.3 i z předchozího příkladu.

Poznámka. V některých publikacích se nesprávně píše, že m z předchozí věty musí být nové prvočíslo. To ovšem není pravda. Stačí uvažovat konečnou posloupnost prvočísel 2, 3, 5, 7, 11 a 13. Pak vidíme, že

$$m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509. \tag{2.3}$$

Čili m je složené a není dělitelné žádným prvočíslem z posloupnosti 2, 3, 5, 7, 11, 13. K tomuto tématu se vrátíme v oddílu 4.7.

Připomeňme ještě, že všechna prvočísla v daném omezeném intervalu začínajícím od 1 lze najít pomocí známého *Eratosthenova síta,* v němž se vyškrtává číslo 1 a všechna složená čísla z tohoto intervalu. To jest škrtají se nejprve čísla dělitelná dvěma kromě 2, třemi kromě 3, pěti kromě 5 atd., až zbudou jen prvočísla:

$$\not{1},\ 2,\ 3,\ \not{4},\ 5,\ \not{6},\ 7,\ \not{8},\ \not{9},\ \not{1}0,\ 11,\ \not{1}2,\ 13, \ldots \tag{2.4}$$

Toto síto se nazývá podle řeckého matematika a astronoma Eratosthena z Kyreny (276–194 př. n. l.), který též přibližně vypočetl obvod Země.

Poznámka. Ruský matematik Pafnutij Lvovič Čebyšev (1821 až 1894) dokázal, že pro každé přirozené číslo n vždy existuje prvočíslo p takové, že

$$n \leq p \leq 2n.$$

2.3. Pythagorejské trojice

Nejprve si připomeňme známou větu.

Věta 2.4. *Nechť a, b, c jsou délky stran trojúhelníku. Pak je tento trojúhelník pravoúhlý s přeponou délky c právě tehdy, když platí*

$$a^2 + b^2 = c^2.$$

Implikace $\Rightarrow$ je klasická Pythagorova věta. Obrácená implikace $\Leftarrow$, která je z praktického hlediska mnohem důležitější, se v řadě učebnic bohužel opomíjí. Navíc se v nich často setkáváme s historkou o tom, jak staří Egypťané používali k vyměřování pyramid provaz se stejně vzdálenými uzly a vytvořili z nich trojúhelník o délkách stran $a = 3$, $b = 4$ a $c = 5$. To, že tento trojúhelník je pravoúhlý, však vůbec neplyne z Pythagorovy věty, jak se často argumentuje, ale z obrácené implikace, která je zahrnuta ve větě 2.4.

Nechť pro uspořádanou trojici $\langle a, b, c\rangle$ přirozených čísel platí $a^2 + b^2 = c^2$. Pak se tato trojice nazývá *pythagorejská trojice* a příslušný pravoúhlý trojúhelník z věty 2.4 se nazývá *pythagorejský trojúhelník.* Je-li $\langle a, b, c\rangle$ pythagorejská trojice, pak zřejmě $\langle b, a, c\rangle$ je také pythagorejská trojice. Jestliže navíc a, b, c nemají společného dělitele $d > 1$, pak se $\langle a, b, c\rangle$ nazývá *primitivní pythagorejská trojice.*

Následující věta je uvedena v Diofantově *Aritmetice*, jejíž latinská verze byla publikována v roce 1621.

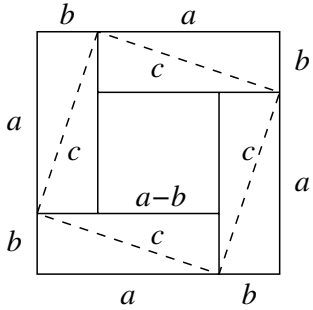
Věta 2.5. *Uspořádaná trojice $\langle a, b, c\rangle$ přirozených čísel je primitivní pythagorejská trojice právě tehdy, když existují nesoudělná přirozená čísla $m > n$, z nichž jedno je sudé a druhé liché, tak, že buď*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2, \tag{2.5}$$

anebo

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2. \tag{2.6}$$

Čísla m a n jsou určena jednoznačně.



Obr. 2.1. Vizuální důkaz Pythagorovy věty podle staročínského matematika Liu Hui (3. stol.): Obsahy čtverců o stranách $a+b$ a c splňují rovnice $(a+b)^2 = c^2+2ab$ a $2ab+(a-b)^2 = c^2$. Každá z těchto identit po úpravě dává $a^2+b^2 = c^2$.

D ů k a z. $\Rightarrow$: Nechť $\langle a, b, c\rangle$ je primitivní pythagorejská trojice. Pak jen nejvýše jedno z těchto čísel může být sudé. Předpokládejme na okamžik, že a i b jsou obě lichá. Pak a^2 i b^2 jsou o jednu větší než nějaký násobek 4, protože

$$(2j+1)^2 = 4j^2+4j+1.$$

Tedy a^2+b^2 je o 2 větší než nějaký násobek 4. Odtud ale plyne, že druhá mocnina je dělitelná dvěma, ale není dělitelná čtyřmi, což není možné. Proto právě jedno z čísel a nebo b musí být sudé. Bez újmy na obecnosti můžeme tedy předpokládat, že $b = 2k$ a že čísla a a c jsou lichá. Potom

$$k^2 = \frac{c^2-a^2}{4} = \frac{c+a}{2}\cdot\frac{c-a}{2}.$$

Protože a a c jsou lichá, jsou čísla $(c+a)/2$ a $(c-a)/2$ přirozená. Musí být navíc nesoudělná, protože každý jejich společný dělitel dělí jejich součet (což je c) i jejich rozdíl (což je a) a o těchto číslech jsme předpokládali, že jsou nesoudělná.

Každé prvočíslo p, které dělí $(c-a)/2$, také dělí k^2, a proto i p^2 dělí k^2. Jelikož p nedělí $(c+a)/2$, musí p^2 dělit $(c-a)/2$. Rozklad $(c-a)/2$ na prvočísla má tedy jen sudé exponenty, což znamená, že číslo $(c-a)/2$ je čtverec. Podobně zjistíme, že $(c+a)/2$ je

rovněž čtverec. Můžeme tedy psát

$$\frac{c+a}{2} = m^2 \quad \text{a} \quad \frac{c-a}{2} = n^2.$$

Vidíme, že čísla m a n jsou nesoudělná, jsou určena jednoznačně a $m > n$. Jelikož $c = m^2 + n^2$ je liché, jedno z čísel m a n musí být liché a druhé sudé. Dále vidíme, že $a = m^2 - n^2$, a tudíž

$$b = \sqrt{c^2 - a^2} = 2mn.$$

$\Leftarrow$: Nechť obráceně $m > n$ jsou nesoudělná přirozená čísla, z nichž jedno je liché a druhé sudé. Položme nejprve

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Pak zřejmě a a c jsou lichá, b je sudé a

$$a^2 + b^2 = (m^2 - n^2) + (2mn)^2 = (m^2 + n^2)^2 = c^2.$$

Tudíž $\langle a, b, c\rangle$ je pythagorejská trojice. Kdyby čísla a, b, c byla všechna dělitelná nějakým lichým prvočíslem p, pak by také čísla $c + a = 2m^2$ a $c - a = 2n^2$ byla dělitelná p, což je ve sporu s tím, že m a n jsou nesoudělná. Odtud plyne, že $\langle a, b, c\rangle$ je primitivní pythagorejská trojice.

Případ, kdy a je sudé a b je liché, lze vyšetřit analogicky. □

Mezi nejznámější primitivní pythagorejské trojice patří

$$\langle 3, 4, 5\rangle, \quad \langle 5, 12, 13\rangle, \quad \langle 7, 24, 25\rangle, \quad \langle 8, 15, 17\rangle, \quad \langle 9, 40, 41\rangle.$$

Poznamenejme ještě, že pro všechna přirozená čísla d dávají volby

$$a = d(m^2 - n^2), \quad b = d(2mn), \quad c = d(m^2 + n^2)$$

a

$$a = d(2mn), \quad b = d(m^2 - n^2), \quad c = d(m^2 + n^2)$$

všechny pythagorejské trojice (Sierpiński, 1950). Jsou-li $\langle a,\ b,\ c\rangle$ a $\langle a',\ b',\ c'\rangle$ pythagorejské trojice, pak je $\langle aa' - bb',\ ab' + a'b,\ cc'\rangle$ také pythagorejská trojice pro $aa' > bb'$.

Pomocí *Lebesgueovy identity*

$$(m^2+n^2-r^2-s^2)^2+(2ms-2nr)^2+(2mr+2ns)^2 \\ =(m^2+n^2+r^2+s^2)^2$$

se hledají čtveřice přirozených čísel splňujících diofantskou rovnici

$$a^2+b^2+c^2=d^2.$$

Například pro $m=n=s=2$ a $r=1$ dostáváme

$$3^2+4^2+12^2=13^2.$$

Na závěr oddílu si dokažme ještě jednu větu, jejímž autorem je Pierre de Fermat.

Věta 2.6 (Fermatova). *Žádné číslo tvaru* $4k-1$ *pro* $k\in\mathbb{N}$ *není součtem dvou čtverců celých čísel.*

D ů k a z. Čtverec sudého čísla je tvaru $4k$. Čtverec lichého čísla $2j+1$ je tvaru $4j^2+4j+1=4k+1$. (Speciálně tedy $4k-1$ není nikdy čtvercem celého čísla.) Tudíž součet dvou čtverců je tvaru $4k$ nebo $4k+1$ nebo $4k+2$, ale nikdy není tvaru $4k+3=4(k+1)-1$. □

2.4. Fermatova metoda nekonečného sestupu

Význačný francouzský matematik Pierre de Fermat (1601–1665) se proslavil nejen Velkou Fermatovou větou a Malou Fermatovou větou (viz oddíly 2.5 a 2.6), ale též množstvím dalších důležitých matematických výsledků. Fermat (viz obr. XIV z barevné přílohy a obr. 2.2) zavedl celou řadu nových pojmů a objevil několik užitečných metod, jež nyní nesou jeho jméno, viz (Křížek, Luca, Somer, 2001), (Mahoney, 1994), (Šolcová, Křížek, Mink, 2002). Jsou to například Fermatova čísla, Fermatova metoda rozkladu, Fermatova spirála, Fermatova funkce, Fermatovy kvocienty, Fermatova transformace, Fermatův bod. Fermat přispěl k základům diferenciálního

a integrálního počtu. Dovedl hledat minima a maxima funkcí a integrovat polynomy dříve než Isaac Newton (1642–1727) a Gottfried Wilhelm Leibniz (1646–1716), viz (Šolcová, 2001). Fermat také patří k zakladatelům analytické geometrie, variačních metod, teorie pravděpodobnosti a zejména moderní teorie čísel. Je též objevitelem známého Fermatova principu, podle něhož se světlo pohybuje po té dráze, po které se šíří v nejkratším čase. Proto se v opticky různorodém prostředí světlo nepohybuje po přímce, ale láme se. Fermatův princip se uplatňuje i v seismice.

Obr. 2.2. Pierre de Fermat – zakladatel moderní teorie čísel.

V tomto oddílu si přiblížíme Fermatovu metodu nekonečného sestupu, která je blízká principu matematické indukce. Opírá se o vlastnost, že množina přirozených čísel $\mathbb{N}$ je dobře uspořádaná, což znamená, že její libovolná neprázdná podmnožina má nejmenší prvek.

Fermatova metoda nekonečného sestupu je založena na následující větě.

Věta 2.7. *Nechť M je podmnožina množiny přirozených čísel $\mathbb{N}$ a nechť pro libovolné $m \in M$ existuje $n \in M$ tak, že $n < m$. Potom je množina M prázdná.*

D ů k a z. Předpokládejme naopak, že M je neprázdná. Protože je množina přirozených čísel $\mathbb{N}$ dobře uspořádaná, existuje nejmenší prvek m množiny M. Pak ale podle předpokladu věty existuje prvek $n \in M$, který je menší než m, což je spor s minimalitou m. Tedy $M = \emptyset$. □

Věta 2.7 se používá hlavně k důkazům neexistence přirozených čísel jistých vlastností. Její užitečnost si ukážeme na dvou tvrzeních, kterými se zabýval sám Pierre de Fermat již kolem roku 1640. Důkazy obou tvrzení budou ilustrovat, jak se Fermatova metoda nekonečného sestupu vlastně používá. První tvrzení se týká pythagorejských trojúhelníků.

Protože a nebo b ve větě 2.5 je sudé, obsah

$$P = \frac{ab}{2} \tag{2.7}$$

pythagorejského trojúhelníka je vždy přirozené číslo. Věty 2.5 a 2.7 nyní použijeme k důkazu následující vlastnosti.

Věta 2.8. *Neexistuje pythagorejský trojúhelník, jehož obsah je čtvercem přirozeného čísla.*

D ů k a z. Předpokládejme naopak, že existují $a, b, c \in \mathbb{N}$ tak, že $a^2 + b^2 = c^2$ a že obsah P pythagorejského trojúhelníku je čtvercem nějakého přirozeného čísla. Lze předpokládat, že $\langle a, b, c \rangle$ je primitivní pythagorejská trojice. To znamená, že největší společný dělitel čísel a, b, c je jedna, což je ekvivalentní vlastnosti, že čísla a a b jsou nesoudělná. Kdyby totiž tomu tak nebylo, pak bychom položili $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ a $c' = \frac{c}{d}$, kde d je největší společný dělitel čísel a, b, c. Trojice $\langle a', b', c' \rangle$ by pak opět byla pythagorejská a obsah příslušného pythagorejského trojúhelníku by byl opět

čtvercem, jak plyne z (2.7). Podle věty 2.5 je zřejmě právě jedno z čísel a a b sudé. Bez újmy na obecnosti můžeme předpokládat, že b je sudé. Existují tedy přirozená čísla $m > n$ tak, že

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2. \tag{2.8}$$

Ze vztahu (2.8) a nesoudělnosti čísel a, b, c okamžitě plyne, že i čísla m a n jsou nesoudělná. Proto jsou po dvojicích nesoudělná také čísla m, n, $m+n$ a $m-n$.

Obsah uvažovaného pythagorejského trojúhelníku podle (2.7) a (2.8) je

$$P = mn(m+n)(m-n). \tag{2.9}$$

Protože P je čtverec, musí být čtverce i jednotliví činitelé v (2.9), tj. existují $u, v, k, \ell \in \mathbb{N}$ tak, že

$$m = u^2, \quad n = v^2, \quad m+n = u^2+v^2 = k^2, \quad m-n = u^2-v^2 = \ell^2. \tag{2.10}$$

Sečtením a odečtením dvou posledních rovnic dostaneme

$$2m = 2u^2 = k^2 + \ell^2, \quad 2n = 2v^2 = k^2 - \ell^2 = (k+\ell)(k-\ell). \tag{2.11}$$

Protože předpokládáme, že $a = m^2 - n^2$ je liché (viz (2.8)), čísla $k^2 = m+n$ a $\ell^2 = m-n$ ze vztahu (2.10) jsou rovněž lichá. Tedy k a ℓ jsou také lichá čísla.

Označme symbolem j největšího společného dělitele čísel $k+\ell$ a $k-\ell$. Zřejmě $j \geq 2$, protože $k+\ell$ a $k-\ell$ jsou čísla sudá. Vidíme, že j dělí (beze zbytku) $2k$ i 2ℓ. Čili j^2 dělí $4(k^2+\ell^2) = 8m$ i $4(k^2-\ell^2) = 8n$. Protože jsou čísla m a n nesoudělná, je $j \leq 2$. Čísla $k+\ell$ a $k-\ell$ tedy nemají kromě 2 žádného společného dělitele. Proto podle (2.11) existují $r \in \mathbb{N}$ a sudé číslo $s \in \mathbb{N}$ tak, že buď

$$k+\ell = 2r^2 \quad \text{a} \quad k-\ell = s^2,$$

anebo

$$k+\ell = s^2 \quad \text{a} \quad k-\ell = 2r^2.$$

Odtud a z (2.11) dostaneme

$$\left(r^2\right)^2 + \left(\frac{s^2}{2}\right)^2 = \left(\frac{k+\ell}{2}\right)^2 + \left(\frac{k-\ell}{2}\right)^2 = \frac{k^2+\ell^2}{2} = u^2.$$

Vidíme, že trojice $\langle r^2, s^2/2, u\rangle$ je novou pythagorejskou trojicí. Obsah odpovídajícího trojúhelníku je $P' = r^2 s^2/4$, což je zřejmě čtverec přirozeného čísla, neboť s je sudé. Obsah P' je však menší než obsah P, tj.

$$P' = \frac{r^2 s^2}{4} = \frac{k^2-\ell^2}{8} < k^2 < u^2 v^2 k^2 \ell^2 = P,$$

kde poslední rovnost plyne z (2.9) a (2.10).

Ověřili jsme tak předpoklady věty 2.7 pro množinu

$$M = \{P \in \mathbb{N};\ \exists\, a, b, c, i \in \mathbb{N} :\ P = i^2 = \frac{ab}{2},\ a^2 + b^2 = c^2\},$$

kde symbol $\exists$ označuje existenční kvantifikátor (a čte se „existuje“). Tedy platí $M = \emptyset$. □

Fermat použil metodu nekonečného sestupu i při důkazu následujícího tvrzení.

Věta 2.9. *Rovnice tvaru $x^4 + y^4 = w^2$ nemá řešení pro přirozená čísla x, y a w.*

D ů k a z. Předpokládejme naopak, že existuje řešení rovnice $x^4 + y^4 = w^2$ v množině přirozených čísel. Pak

$$(x^2)^2 + (y^2)^2 = w^2. \tag{2.12}$$

Zřejmě můžeme předpokládat, že největší společný dělitel čísel x^2, y^2 a w je 1. Kdyby totiž byl jejich největší společný dělitel $d > 1$, pak bychom mohli rovnici (2.12) vydělit d^2 a získat tak jiná nesoudělná čísla splňující (2.12).

Protože $\langle x^2, y^2, w\rangle$ je pythagorejská trojice nesoudělných čísel, právě jedno z čísel x, nebo y je sudé. Bez újmy na obecnosti můžeme předpokládat, že x je liché a y je sudé. Podle věty 2.5 tedy existují přirozená čísla $m > n$ tak, že

$$x^2 = m^2 - n^2, \quad y^2 = 2mn, \quad w = m^2 + n^2. \tag{2.13}$$

Kdyby čísla m a n byla soudělná, pak by x^2, y^2 a w ve vztahu (2.13) byla soudělná čísla, což je spor. Čísla m a n jsou proto nesoudělná. Ze vztahu (2.13) vidíme, že

$$x^2 + n^2 = m^2.$$

Protože x je liché, podle věty 2.5 existují přirozená čísla $r > s$ tak, že

$$x = r^2 - s^2, \quad n = 2rs, \quad m = r^2 + s^2. \tag{2.14}$$

Čísla r a s jsou opět nesoudělná. Kdyby totiž byla soudělná, největší společný dělitel čísel x, m a n by byl větší než jedna, což je spor s tím, že m a n jsou nesoudělná. Podle (2.13) je $2mn$ čtverec přirozeného čísla. Protože m a n jsou nesoudělná, existují přirozená čísla u a v tak, že

$$n = 2u^2, \quad m = v^2. \tag{2.15}$$

Odtud a z (2.14) je $2u^2 = 2rs$, z čehož plyne existence přirozených čísel g a h tak, že $r = g^2$ a $s = h^2$. Ze vztahu $m = v^2$ a (2.14) dostaneme

$$g^4 + h^4 = v^2.$$

Tato rovnice má tentýž tvar jako původní rovnice (2.12), ale $v < w$, protože podle (2.13) a (2.15)

$$v = \sqrt{m} < m^2 + n^2 = w.$$

Opět jsou splněny předpoklady věty 2.7 pro množinu

$$M = \{w \in \mathbb{N};\ \exists x, y \in \mathbb{N} :\ x^4 + y^4 = w^2\},$$

a tedy $M = \emptyset$. □

Podobným způsobem jako větu 2.9 lze dokázat, že rozdíl dvou čtvrtých mocnin přirozených čísel nikdy není čtvercem žádného přirozeného čísla.

Fermat používal metodu nekonečného sestupu s nadšením k důkazům i jiných hypotéz. Rozhodl se ji používat, jak se sám vyjádřil, protože obvyklé metody, které se vyskytovaly v učebnicích, nedostačovaly k demonstraci obtížnějších výroků. Své návrhy různých

postupů důkazů posílal Fermat v dopisech svým přátelům P. Carcavimu a B. Fréniclu de Bessy. Jeho důkazy však často nebyly provedeny důsledně.

Proč vůbec Fermat nazval svůj myšlenkový postup právě metodou nekonečného sestupu (franc. *descente infinie*)? Jak jsme viděli v předchozích důkazech, z existence alespoň jednoho řešení v množině M vyplývala existence jiného menšího řešení v M. Zdá se, že takto bychom mohli pokračovat v množině M v nekonečném sestupu, ale množina přirozených čísel je ohraničená zdola číslem 1, což vede ke sporu.

Fermatova metoda nekonečného sestupu je příbuzná dnes známé metodě matematické indukce. Implicitně použil metodu indukce již Eukleides při důkazu věty 2.3 o nekonečném počtu prvočísel. Její použití se rozšířilo až v 16. století díky Francescu Maurolicovi a později Johnu Wallisovi, s nímž Fermat vedl vědeckou korespondenci. Fermatovu metodu nekonečného sestupu lze zobecnit i na mnohem obecnější algebraické struktury, než jsou přirozená čísla.

2.5. Velká Fermatova věta

V roce 1670 Samuel de Fermat (1630–1690), syn Pierra de Fermata, publikoval ve francouzském Toulouse Diofantovu *Aritmetiku* rozšířenou o poznámky, které jeho otec připisoval na okraje svého exempláře Bachetova vydání *Aritmetiky* z roku 1621. V jedné z těchto poznámek Fermat bez důkazu napsal větu, které se dnes všeobecně říká Velká Fermatova věta.

Věta 2.10 (Velká Fermatova věta). *Neexistují přirozená čísla* $n \geq 3$, x, y *a* z *tak, že*

$$x^n + y^n = z^n. \tag{2.16}$$

Je to jeden z nejslavnějších matematických problémů všech dob. Exponent $n \geq 3$ je buď dělitelný lichým prvočíslem, nebo je n mocninou 2. Ukážeme, že větu stačí dokázat jen, je-li exponent n

liché prvočíslo nebo $n = 4$. Pokud by totiž měla rovnice (2.16) řešení pro nějaké $n = pq$, kde p je liché prvočíslo a $q > 1$, pak

$$x^{pq} + y^{pq} = \left(x^q\right)^p + \left(y^q\right)^p = \left(z^q\right)^p = z^{pq}.$$

Tudíž stačí položit $x' = x^q$, $y' = y^q$, $z' = y^q$ a vidíme, že rovnice (2.16) má řešení i pro $n = p$.

Podobně lze ukázat, že kdyby existovalo nějaké řešení rovnice (2.16) pro $n = 2^k$, kde $k > 2$, pak by muselo existovat řešení i pro $n = 4$,

$$x^{2^k} + y^{2^k} = \left(x^{2^{k-2}}\right)^4 + \left(y^{2^{k-2}}\right)^4 = \left(z^{2^{k-2}}\right)^4 = z^{2^k}.$$

Sám Fermat však dokázal neexistenci řešení (2.16) jen pro $n = 4$ a to svojí oblíbenou metodou nekonečného sestupu. Rovnice (2.16) tedy nemá řešení ani pro $n = 8, 16, 32, \ldots$

Věta 2.11. *Velká Fermatova věta platí pro $n = 4$, tj. rovnice*

$$x^4 + y^4 = z^4 \tag{2.17}$$

nemá řešení v množině přirozených čísel.

D ů k a z. Předpokládejme naopak, že existují přirozená čísla x, y, z splňující (2.17). Položíme-li $w = z^2$, dostaneme ihned spor s Fermatovým tvrzením z věty 2.9. □

O století později použil metodu nekonečného sestupu k důkazu Velké Fermatovy věty L. Euler pro $n = 3, 4$. V původním Eulerově důkazu pro $n = 3$ z roku 1770 však byla nalezena chyba, kterou se později podařilo opravit. Případu $n = 3$, který je podrobně vyšetřen například v práci (Hardy, Wright, 1979), se věnoval i Christian Huygens. V roce 1825 G. P. L. Dirichlet a o tři roky později i A. M. Lagrange dokázali Velkou Fermatovu větu pro $n = 5$. Případ $n = 7$ rozřešili G. Lamé a V. A. Lebesgue v roce 1840. V roce 1983 Gerhard Faltings dokázal Mordellovu domněnku, která tvrdí, že rovnice (2.16) má pro každý exponent $n > 3$ jen konečně mnoho řešení takových, že $(x, y, z) = 1$. Podrobný historický přehled obsahující řadu speciálních tvrzení, která se týkají řešení rovnice (2.16), je podán v článku (Terjanian, 2002).

Matematikům trvalo více než 350 let, než byla Velká Fermatova dokázána i pro libovolný prvočíselný exponent. Anglický matematik Andrew Wiles z univerzity v Princetonu našel způsob jak větu dokázat. V červnu 1993 nastínil její důkaz během tří přednášek na Newton Institute v Cambridge před zraky asi padesáti specialistů na teorii čísel. Později sice byla nalezena v jeho důkazu mezera, ale poměrně brzy se ji podařilo odstranit. V roce 1995 společně s Richardem Taylorem zveřejnil úplný důkaz tvrzení, ze kterého Velká Fermatova věta vyplývá, viz (Wiles, 1995), (Taylor, Wiles, 1995). Metodu, kterou tito autoři použili, však Fermat nemohl znát, neboť řada pojmů (jako například modulární formy, eliptické křivky, grupy) nebyla tehdy ještě zavedena. V článku (Pradlová, Křížek, 1999, s. 265) se popisují vlastnosti grupy, která se opírá o eliptické křivky, má jednotkový prvek v nekonečnu a byla použita při důkazu Velké Fermatovy věty. Metody, které Wiles použil, jsou vysvětleny v knize (Hellegouarch, 2002) nebo v článku (Nekovář, 1994). Populární knížka o řešení Fermatovy věty existuje i v českém jazyce – viz (Singh, 2000). Velké Fermatově větě se budeme ještě věnovat v oddílech 4.3 a 4.5.

Existuje celá řada problémů podobných Velké Fermatově větě. Například Američan Andrew Beal formuloval následující domněnku, na jejíž řešení je vypsána velká finanční odměna, viz (Mauldin, 1998).

Bealova domněnka. *Rovnice*

$$x^k + y^m = z^n$$

nemá řešení v přirozených číslech k, m, n, x, y *a* z*, kde* k, m *a* n *jsou větší než* 2 *a čísla* x, y *a* z *jsou vzájemně nesoudělná.*

Během osmdesátých let 20. století formulovali W. Masser, J. Oesterlé a L. Szpiro diofantskou nerovnost známou pod názvem Domněnka abc. Její rozřešení by mělo mnoho aplikací (např. pro důkaz Bealovy domněnky). Označme pro přirozená čísla a, b a c symbolem $N(a, b, c)$ součin prvočíselných dělitelů čísel a, b a c, kde se každý dělitel vyskytuje jen jednou.

Domněnka abc. *Ke každému reálnému číslu $\varepsilon > 0$ existuje konstanta $\mu > 1$ taková, že pro každá dvě vzájemně nesoudělná čísla a a b a jejich součet $c = a + b$ platí*

$$\max(|a|, |b|, |c|) \leq \mu N(a, b, c)^{1+\varepsilon}.$$

Catalanova domněnka. *Neexistují po sobě jdoucí přirozená čísla kromě* 8 *a* 9*, která jsou obě mocninami.*

Nedávno Catalanovu domněnku dokázal rumunský matematik Preda Mihăilescu, podrobnosti najde zájemce v článku (Bugeaud, Mignotte, 2005). Ukázal, že rovnice

$$x^m - y^n = 1, \quad \text{kde } m, n, x, y \geq 2,$$

má jen jediné řešení $m = y = 2$, $n = x = 3$. Poznamenejme ještě, že v 7. století indický matematik Brahmagupta našel nejmenší řešení $x = 151$ a $y = 120$ speciálního případu tzv. *Pellovy rovnice* $x^2 - 94y^2 = 1$. Více o této rovnici a jejím řešení je například v knize (Burton, 1998).

2.6. Malá Fermatova věta

Číslo $n^3 - n$ pro $n \in \mathbb{N}$ je dělitelné třemi (ale i dvěma), protože ho lze napsat jako součin tří po sobě jdoucích přirozených čísel

$$n^3 - n = (n-1)n(n+1).$$

Toto jednoduché tvrzení zobecníme v Malé Fermatově větě, která patří mezi nejpoužívanější prostředky v teorii čísel, jak ostatně uvidíme i v této knize (viz rejstřík). K jejímu důkazu budeme potřebovat následující implikaci, která bezprostředně plyne z První Eukleidovy věty 2.1:

Je-li p prvočíslo a $ab \equiv 0 \pmod{p}$, pak

$$a \equiv 0 \pmod{p} \quad \text{nebo} \quad b \equiv 0 \pmod{p}. \tag{2.18}$$

Věta 2.12 (Malá Fermatova věta). *Jestliže $a \in \mathbb{N}$ a p je prvočíslo, pak $p \mid \left(a^p - a\right)$.*

D ů k a z. Případ $p = 2$ je zřejmý. Nechť p je prvočíslo větší než 2. Jestliže $p \mid a$, pak p také dělí číslo $a^p - a = a(a^{p-1} - 1)$. Nechť čísla p a a jsou nesoudělná, tj.

$$(p, a) = 1.$$

Ukážeme, že $p \mid \left(a^{p-1} - 1\right)$. Uvažujme konečnou posloupnost

$$a,\ 2a,\ 3a, \ldots,\ (p-1)a. \tag{2.19}$$

Vydělíme-li čísla ia a ja, $1 \leq j < i < p$, prvočíslem p, nemůžeme dostat stejný zbytek, protože pak by $p \mid (i - j)a$, což je podle (2.18) spor s tím, že $(a, p) = 1$. Posloupnost (2.19) proto dává $p - 1$ různých nenulových zbytků při dělení prvočíslem p. Stejné zbytky (až na pořadí) dostaneme, když budeme dělit posloupnost $1, 2, \ldots, p - 1$ prvočíslem p. Vynásobme mezi sebou tato čísla a pak také čísla v (2.19). Odtud pomocí (1.5) a následnou indukcí dospějeme ke kongruenci $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Tedy

$$(a^{p-1} - 1)(p-1)! \equiv 0 \pmod{p}$$

a první činitel na levé straně je dělitelný prvočíslem p podle (2.18), jelikož platí $p \nmid (p-1)!$. □

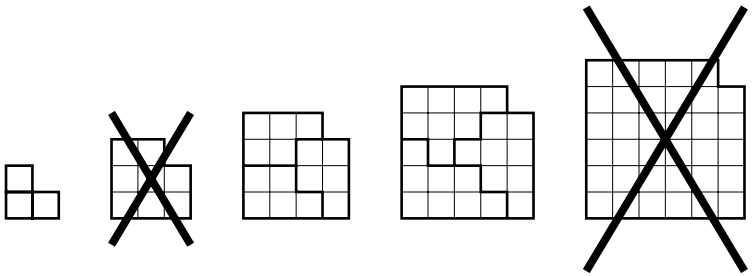
Existuje několik dalších důkazů Malé Fermatovy věty. Nejstarší důkaz z roku 1736 pochází od Eulera. Jeden z velice zajímavých důkazů je podán v (Gutfreund, Little, 1982), viz též (Skula, 2002). Opírá se o jisté symetrické vlastnosti fyzikálních částic, které mají určitý typ spinu.

Jiný důkaz uvažuje náramek s p korálky o a barvách, viz (Golomb, 1956). Počet všech množných obarvení náramku je a^p. Počet jednobarevných náramků je a (obr. I barevné přílohy). Pokud ale všechny korálky nemají stejnou barvu, pak p pootočení o $360°/p$ náramku dává p různých možností obarvení, protože p je prvočíslo. (Kdyby p bylo složené, mohli bychom při vhodném pootočení a obarvení více barvami dostat tutéž konfiguraci.) Tedy $a^p = a + pn$ pro nějaké $n \in \mathbb{N}$, tj. $p \mid a^p - a$.

Speciální případ Malé Fermatovy věty byl znám Janu Brožkovi (1585–1652) z Krakovské akademie, viz Johannes Broscius:

De Numeris Perfectis Disceptationes Duae, 1637. Přehled výsledků týkajících se Malé Fermatovy věty je podán také v knížce (Lepka, 2000). Vyšetřují se zde i vlastnosti *Fermatova kvocientu* $(a^{p-1}-1)/p$.

Malá Fermatova věta se často formuluje pomocí kongruence tak, jak říká věta 2.13 (srov. obr. 2.3).



Obr. 2.3. Geometrická interpretace Malé Fermatovy věty daná kongruencí (2.20) pro $p = 3$. Jestliže $(3, a) = 1$, pak $3 \mid \left(a^2 - 1\right)$; tj. čtverec a^2 zmenšený o jednu může být rozdělen na tři části o stejném celočíselném obsahu. Jestliže $3 \mid a$, pak podobný rozklad není možný.

Věta 2.13 (Malá Fermatova věta). *Jestliže p je prvočíslo a platí $(a, p) = 1$, pak*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.20}$$

Nechť d a a jsou nesoudělná přirozená čísla. Nejmenší kladný exponent e, pro který $d \mid \left(a^e - 1\right)$ (tj. $a^e \equiv 1 \pmod{d}$), se nazývá (*multiplikativní*) *řád čísla a modulo d,* což budeme zapisovat takto: $e = \mathrm{ord}_d a$.

Podle Malé Fermatovy věty $p \mid \left(a^{p-1} - 1\right)$ pro libovolné prvočíslo p nesoudělné s a. Odtud plyne existence řádu $e \leq p - 1$. Například můžeme ověřit, že $\mathrm{ord}_7 2 = 3$, $\mathrm{ord}_5 3 = 4$. Speciálně $\mathrm{ord}_1 a = 1$ pro každé $a \in \mathbb{N}$.

Věta 2.14. *Jestliže $e = \mathrm{ord}_d a$, pak*

$$d \mid \left(a^n - 1\right) \tag{2.21}$$

pro $n = ke$, $k \in \{1, 2, \dots\}$ *a vztah* (2.21) *platí pouze pro tyto exponenty.*

Důkaz. Jestliže $n = ke$, pak

$$a^n - 1 = a^{ke} - 1 = \left(a^e - 1\right)\left(a^{e(k-1)} + \cdots + a^e + 1\right),$$

a proto (2.21) platí díky předchozí definici.

Předpokládejme nyní, že $d \mid \left(a^{ke+h} - 1\right)$ pro nějaké $k \in \{1, 2, \dots\}$ a $0 < h < e$. Pak

$$\left(a^{ke+h} - 1\right) - \left(a^{ke} - 1\right) = a^{ke}\left(a^h - 1\right).$$

Protože obě čísla v závorkách na levé straně jsou podle předpokladu dělitelná d a podle (2.21) platí $(d, a^{ke}) = 1$, dostaneme, že $a^h - 1$ je dělitelné číslem d. To ale odporuje minimalitě exponentu e. □

Nechť p je prvočíslo. Podle Malé Fermatovy věty řád modulo p čísla a nesoudělného s p je $p-1$ nebo menší. Číslo $g \not\equiv 0 \pmod{p}$ nazveme *primitivním kořenem modulo* p, jestliže

$$\operatorname{ord}_p g = p - 1.$$

Přitom většinou volíme g tak, aby $0 < g < p$. Takové číslo g je tedy primitivním kořenem, jestliže $g^k \not\equiv 1 \pmod{p}$ pro všechna $k \in \{1, \dots, p-1\}$ (srov. tab. 8, str. 344).

Například číslo 3 je primitivním kořenem modulo 17 (viz obr. 2.4), protože $3^k \not\equiv 1 \pmod{17}$ pro všechna $k = 1, \dots, 15$ a $3^{16} \equiv 1 \pmod{17}$. V tomto případě řád čísla 3 modulo 17 je 16, tj. $\operatorname{ord}_{17} 3 = 16$.

Na druhé straně 4 není primitivním kořenem, neboť $4^4 \equiv 1 \pmod{17}$.

Primitivní kořeny mají řadu aplikací např. v kryptografii, a při konstrukci generátorů pseudonáhodných čísel a pravidelných mnohoúhelníků (viz oddíly 5.3, 5.5 a 5.6). Pro existenci primitivních kořenů platí následující věta.

Věta 2.15. *Jestliže* p *je prvočíslo, pak existuje primitivní kořen modulo* p.

Důkaz je uveden např. v (Gauss, 1986, article 55) nebo (Burton, 1998, s. 156–157). Zobecnění tohoto výsledku uvedeme ve větě 2.18.

Jestliže g je primitivní kořen modulo p, kde p je prvočíslo, pak g je generátorem množiny všech nenulových zbytků modulo p, tj. $\{g,\ g^2,\ g^3,\ldots,\ g^{p-1}\}$ se skládá ze všech $p-1$ nenulových zbytků modulo p. Tudíž pro každé přirozené číslo $a \not\equiv 0 \pmod{p}$ existuje exponent $n \in \{1,\ldots,p-1\}$ tak, že $g^n \equiv a \pmod{p}$. Tato myšlenka je dále rozvinuta v knize (Burton, 1998, s. 165–169).

2.7. Eulerova–Fermatova věta

Leonhard Euler (1707–1783) zobecnil Malou Fermatovu větu 2.13 i pro neprvočíselný modul. K tomuto účelu si nejprve zavedeme *Eulerovu funkci* φ. Pro každé $n \in \mathbb{N}$ je hodnota $\varphi(n)$ definována jako počet všech přirozených čísel nepřevyšujících n, která jsou s n nesoudělná, tj.

$$\varphi(n) = |\{m \in \{1,\ldots,n\};\ (m,n) = 1\}|,$$

kde $|\cdot|$ označuje počet prvků. Snadno zjistíme, že

$$\varphi(1) = 1,\ \ \varphi(2) = 1,\ \ \varphi(3) = 2,\ \ \varphi(4) = 2,$$
$$\varphi(5) = 4,\ \ \varphi(6) = 2,\ \ \varphi(7) = 6,\qquad \ldots$$

Další hodnoty φ uvádíme v tabulce 7 na str. 343. Z definice funkce φ dále vidíme, že její hodnoty jsou pro $n > 2$ sudé. Pokud je p prvočíslo, pak zřejmě

$$\varphi(p) = p - 1 \tag{2.22}$$

a

$$\varphi\big(p^k\big) = (p-1)p^{k-1} \tag{2.23}$$

pro každé $k \in \mathbb{N}$.

Eulerova funkce má následující důležitou vlastnost:

$$(m,n) = 1 \quad \Longrightarrow \quad \varphi(mn) = \varphi(m)\varphi(n). \tag{2.24}$$

Důkaz je podán například v knihách (Gauss, 1986, article 38), (Burton, 1998, s. 125) nebo (Niven, Zuckerman, Montgomery, 1991, s. 69). Pokud je tedy prvočíselný rozklad čísla n dán vztahem

$$n = \prod_{i=1}^{r} p_i^{k_i},$$

kde $p_1 < p_2 < \cdots < p_r$, $k_i \in \mathbb{N}$, pak podle (2.23) a (2.24)

$$\varphi(n) = \prod_{i=1}^{r}(p_i - 1)p_i^{k_i-1} = n\prod_{i=1}^{r}\frac{(p_i-1)p_i^{k_i-1}}{p_i^{k_i}} = \\ = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right). \qquad (2.25)$$

Všimněte si, že na pravé straně musí být celé číslo, protože $\varphi(n)$ na levé straně je celé.

C. F. Gauss odvodil důležitý vztah

$$\sum_{d|n}\varphi(d) = n \quad \text{pro všechna } n \in \mathbb{N},$$

kde sčítáme přes všechny dělitele d čísla n. Důkaz je uveden například v (Gauss, 1986, article 39) nebo (Burton, 1998, s. 134).

Poznámka. V knížce (Rademacher, Toeplitz, 1970, kap. 27) je dokázáno, že 30 je největší číslo takové, že všechna čísla s ním nesoudělná jsou prvočísla. Původní důkaz, který podal ruský matematik Pafnutij Lvovič Čebyšev (1821–1894), později značně zjednodušil student H. Bonse.

Věta 2.16. *Nechť $n > 1$. Pak $\varphi(n) < n - 1$ právě tehdy, když n je složené; $\varphi(n) = n - 1$ právě tehdy, když n je prvočíslo.*

D ů k a z. Tvrzení věty okamžitě plyne ze vztahů (2.22), (2.23) a (2.25). □

Věta 2.17 (Eulerova–Fermatova). *Nechť $a, n \in \mathbb{N}$. Pak*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad (2.26)$$

právě tehdy, když $(a, n) = 1$.

Tato věta vlastně udává nutnou a postačující podmínku k tomu, aby čísla a a n byla nesoudělná. Na tomto místě ji ale dokazovat nebudeme, neboť bude přímým důsledkem silnější Carmichaelovy věty 2.20 a vztahu (2.27).

Ze vztahů (2.22) a (2.20) vidíme, že věta 2.17 je přímým zobecněním Malé Fermatovy věty 2.13.

Nyní definujeme primitivní kořeny modulo libovolné přirozené číslo $n \geq 2$ podobně jako pro prvočísla. Podle Eulerovy–Fermatovy věty 2.17 největší možný řád modulo n čísla a nesoudělného s n je roven $\varphi(n)$. Jestliže a je přirozené číslo takové, že $(a, n) = 1$, pak a se nazývá *primitivní kořen modulo n*, pokud

$$\mathrm{ord}_n a = \varphi(n).$$

Následující věta určuje všechna přirozená čísla $n \geq 2$, která mají primitivní kořeny.

Věta 2.18. *Nechť $n \geq 2$. Pak existují primitivní kořeny modulo n právě tehdy, když $n \in \{2,\ 4,\ p^k,\ 2p^k\}$, kde p je liché prvočíslo a $k \in \mathbb{N}$. Jestliže navíc n má primitivní kořen, pak má n přesně $\varphi(\varphi(n))$ nekongruentních primitivních kořenů.*

Důkaz je uveden například v knize (Burton, 1998, s. 160–164) nebo (Niven, Zuckerman, Montgomery, 1991, s. 102–104). Je-li tedy p prvočíslo, pak má p právě $\varphi(p-1)$ nekongruentních primitivních kořenů (obr. 2.4). Například 3 má jen jeden primitivní kořen, neboť $\varphi(\varphi(3)) = \varphi(2) = 1$, a tento kořen je 2. Prvočíslo 7 má dva primitivní kořeny, protože $\varphi(\varphi(7)) = \varphi(6) = 2$. Metody pro vyhledávání primitivních kořenů jsou uvedeny v knize (Vinogradov, 1953).

Podle věty 2.18 existuje primitivní kořen modulo p^k, kde p je prvočíslo a $k \in \mathbb{N}$, kromě případu, kdy $p = 2$ a zároveň $k \geq 3$. Následující věta určuje největší možný řád modulo 2^k pro $k \geq 3$.

Věta 2.19. *Nechť a je liché přirozené číslo a $k \geq 3$. Pak*

$$\mathrm{ord}_{2^k} a \mid 2^{k-2} \quad a \quad 2^{k-2} < \varphi(2^k) = 2^{k-1}.$$

Speciálně

$$\operatorname{ord}_{2^k} 5 = 2^{k-2}.$$

Důkaz je uveden v (Niven, Zuckerman, Montgomery, 1991, s. 103 až 105).

Poznamenejme ještě, že v roce 1875 H. J. Smith dokázal následující překvapivý vztah, viz (Lovász, 1979),

$$\det\big((i,j)\big)_{i,j=1}^{n} = \prod_{k=1}^{n} \varphi(k),$$

tj. determinant matice největších společných dělitelů je roven součinu hodnot Eulerovy funkce.

Podle (Luca, 2004, s. 5) pro každé $n \in \mathbb{N}$ existuje k tak, že $\varphi(k) = n!$.

2.8. Carmichaelova věta

Podle Eulerovy–Fermatovy věty 2.17 a vět 2.14 a 2.18 platí: jestliže a a n jsou nesoudělná přirozená čísla, pak $\operatorname{ord}_n a \mid \varphi(n)$ a existuje přirozené číslo b tak, že $\operatorname{ord}_n b = \varphi(n)$ pro $n \in \{2, 4, p^k, 2p^k\}$, kde p je liché prvočíslo a $k \in \mathbb{N}$. Jak ale uvidíme z dalšího textu, největší možný řád modulo n může být podstatně nižší než $\varphi(n)$, pokud n není mocninou prvočísla. K tomuto účelu nejprve zavedeme Carmichaelovu funkci $\lambda(n)$, jež se poprvé objevila v článku (Carmichael, 1912). Její definice je vlastně pouhou modifikací Eulerovy funkce $\varphi(n)$.

Pro přirozené n je *Carmichaelova funkce* $\lambda(n)$ definována takto:

$$\lambda(1) = 1 = \varphi(1),$$
$$\lambda(2) = 1 = \varphi(2),$$
$$\lambda(4) = 2 = \varphi(4),$$

$$\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k) \text{ pro } k \geq 3,$$

$$\lambda(p^k) = (p-1)p^{k-1} = \varphi(p^k) \text{ pro libovolné liché prvočíslo } p \text{ a } k \geq 1,$$

$$\lambda\left(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\right) = \left[\lambda\left(p_1^{k_1}\right),\ \lambda\left(p_2^{k_2}\right), \ldots,\ \lambda\left(p_r^{k_r}\right)\right],$$

kde $p_1,\ p_2, \ldots,\ p_r$ jsou různá prvočísla a $k_i \in \mathbb{N}$ pro $1 \leq i \leq r$.

Hodnoty funkce $\lambda(n)$ pro $n \leq 32$ uvádíme v tabulce 7 uvedené na str. 343. Pomocí vět 2.18 a 2.19 tedy vidíme, že když p je prvočíslo a $k \in \mathbb{N}$, pak $\lambda\left(p^k\right)$ se rovná největšímu možnému řádu p^k. Z definice funkce $\lambda(n)$ je dále patrné, že

$$\lambda(n) \mid \varphi(n) \tag{2.27}$$

pro všechna přirozená n a že $\lambda(n) = \varphi(n)$ právě tehdy, když $n \in \{1,\ 2,\ 4,\ p^k,\ 2p^k\}$, kde p je liché prvočíslo a $k \in \mathbb{N}$ (srov. větu 2.18).

Povšimněme si, že $\lambda(n)$ může být mnohem menší než $\varphi(n)$, pokud má n hodně prvočinitelů. Nechť například $n = 2^6 \cdot 11 \cdot 17 \cdot 41 = 490\,688$. Potom

$$\lambda(n) = \left[\lambda\left(2^6\right), \lambda(11), \lambda(17), \lambda(41)\right] = [16, 10, 16, 40] = 80,$$

zatímco

$$\varphi(n) = \varphi\left(2^6\right)\varphi(11)\varphi(17)\varphi(41) = 32 \cdot 10 \cdot 16 \cdot 40 = 204\,800.$$

Následující věta zobecňuje Eulerovu–Fermatovu větu 2.17. Tvrdí vlastně, že $\lambda(n)$ je univerzální řád modulo n.

Věta 2.20 (Carmichaelova). *Nechť $a, n \in \mathbb{N}$. Pak*

$$a^{\lambda(n)} \equiv 1 \pmod{n} \tag{2.28}$$

právě tehdy, když $(a, n) = 1$. Navíc existuje $b \in \mathbb{N}$ tak, že

$$\operatorname{ord}_n b = \lambda(n). \tag{2.29}$$

D ů k a z. $\Rightarrow$: Jestliže $(a, n) = d > 1$, pak $d \nmid \left(a^{\lambda(n)} - 1\right)$, a tedy (2.28) neplatí.

$\Leftarrow$: Nechť obráceně $(a, n) = 1$. Kongruence (2.28) zřejmě platí pro $n = 1$. Předpokládejme tedy, že $n \geq 2$. Abychom ukázali platnost kongruence (2.28), stačí podle věty 2.14 ukázat, že

$$\operatorname{ord}_n a \mid \lambda(n). \tag{2.30}$$

Uvažujme následující rozklad n na prvočinitele

$$n = \prod_{i=1}^{r} p_i^{k_i}, \tag{2.31}$$

kde $p_1 < p_2 < \cdots < p_r$, $k_i \in \mathbb{N}$, a nechť $q_i = p_i^{k_i}$ pro $1 \leq i \leq r$. Protože mocniny různých prvočísel jsou nesoudělné, dostáváme

$$\operatorname{ord}_n a = \left[\operatorname{ord}_{q_1} a,\ \operatorname{ord}_{q_2} a, \ldots,\ \operatorname{ord}_{q_r} a\right]. \tag{2.32}$$

Na druhé straně platí

$$\operatorname{ord}_{q_i} a \mid \lambda(q_i) \tag{2.33}$$

pro $1 \leq i \leq r$ díky (2.27) a větě 2.14. Podle definice funkce $\lambda(n)$, (2.32) a (2.33) vidíme, že vztah (2.30) je splněn.

Dále ukážeme existenci $b \in \mathbb{N}$ tak, aby platilo (2.29). Uvažujme rozklad (2.31). Podle Čínské věty o zbytcích 1.4 a vět 2.18 a 2.19 existuje přirozené b tak, že pro $1 \leq i \leq r$ platí

$$b \equiv g_i \pmod{p_i^{k_i}}, \tag{2.34}$$

kde g_1 je primitivní kořen modulo $p_1^{k_1}$, je-li p_1 liché nebo $p_1 = 2$ a $1 \leq k_1 \leq 2$, $g_1 = 5$, je-li $p_1 = 2$ a $k_1 \geq 3$, a g_i je primitivní kořen modulo $p_i^{k_i}$ pro $2 \leq i \leq r$. Protože $\left(g_i, p_i^{k_i}\right) = 1$ pro $1 \leq i \leq r$, platí $(b, n) = 1$. Tvrdíme, že $\operatorname{ord}_n b = \lambda(n)$. Podle (2.34), (2.27) a věty 2.19 máme

$$\operatorname{ord}_{q_i} b = \lambda(q_i) \tag{2.35}$$

pro $1 \leq i \leq r$. Jelikož

$$\operatorname{ord}_n b = \left[\operatorname{ord}_{q_1} b,\ \operatorname{ord}_{q_2} b, \ldots,\ \operatorname{ord}_{q_r} b\right],$$

vidíme z (2.35) a z definice funkce λ, že $\operatorname{ord}_n b = \lambda(n)$. □

2.9. Legendrův a Jacobiho symbol

Francouzský matematik Adrien Marie Legendre (1752–1813) zavedl do teorie čísel velice užitečný symbol $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$. Dříve než si jej představíme a seznámíme se s jeho vlastnostmi, definujeme kvadratické zbytky modulo prvočíslo.

Nechť $n \geq 2$ a a jsou nesoudělná celá čísla. Pokud má kvadratická kongruence

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

celočíselné řešení x, pak a se nazývá *kvadratický zbytek* nebo *kvadratické reziduum modulo n.* V opačném případě říkáme, že a není *kvadratický zbytek modulo n*, přičemž a budeme nazývat *kvadratické nereziduum* – někdy se mu též říká *nezbytek*, viz (Apfelbeck, 1968).

Nechť p je liché prvočíslo. Pak *Legendrův symbol* $\left(\frac{a}{p}\right)$ je roven

$$\begin{aligned} 1,&\ \text{jestliže } a \text{ je kvadratický zbytek modulo } p,\\ -1,&\ \text{jestliže } a \text{ není kvadratický zbytek modulo } p,\\ 0,&\ \text{jestliže } p \mid a. \end{aligned}$$

Kvadratický charakter a vzhledem k prvočíslu p je tak vyjádřen pomocí Legendrova symbolu. Je zřejmé, že posloupnost $\left(\left(\frac{a}{p}\right)\right)_{a=0}^{\infty}$ je periodická, např.

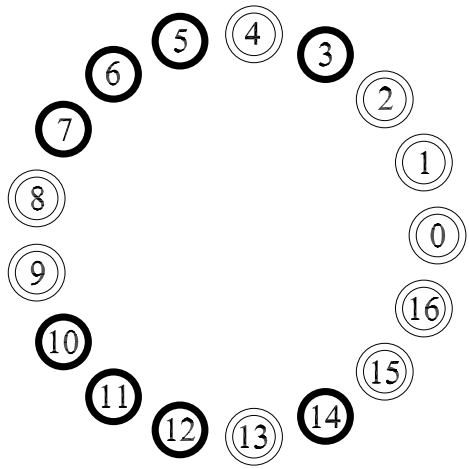
$$\left(\frac{0}{7}\right) = 0, \quad \left(\frac{1}{7}\right) = 1, \quad \left(\frac{2}{7}\right) = 1, \left(\frac{3}{7}\right) = -1, \left(\frac{4}{7}\right) = 1,$$

$$\left(\frac{5}{7}\right) = -1, \left(\frac{6}{7}\right) = -1, \left(\frac{7}{7}\right) = 0, \left(\frac{8}{7}\right) = 1, \quad \left(\frac{9}{7}\right) = 1, \ldots$$

Je-li p liché prvočíslo, pak počet kvadratických reziduí se rovná počtu kvadratických nereziduí, což je rovno $\frac{p-1}{2}$ (důkaz je např.

v (Riesel, 1985, s. 279)). Na obrázku 2.4 vidíme hodnoty Legendrova symbolu pro $p = 17$.

Legendrův symbol má důležité použití při testování prvočíselnosti a výpočtu primitivních kořenů. V kapitole 5 uvidíme některé jeho praktické aplikace. Leonhard Euler navrhl jednoduchou metodu, jak Legendrův symbol $\left(\frac{a}{p}\right)$ počítat.



Obr. 2.4. Černé kroužky označují hodnotu (-1) Legendrova symbolu pro $p = 17$. V tomto případě shodou okolností splývají s primitivními kořeny. Ostatní kroužky odpovídají nezáporným hodnotám Legendrova symbolu $\left(\frac{a}{p}\right)$, přitom jeho nulová hodnota je pouze v bodě 0.

Věta 2.21 (Eulerovo kritérium). *Je-li p liché prvočíslo, pak*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{2.36}$$

Důkaz. Jestliže $p \mid a$, potom zřejmě platí (2.36). Předpokládejme tedy, že $p \nmid a$. Podle Malé Fermatovy věty 2.13 je,

$$a^{p-1} - 1 = \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod{p}.$$

Protože p je prvočíslo, pak buď $a^{(p-1)/2} \equiv 1 \pmod{p}$, nebo

$a^{(p-1)/2} \equiv -1 \pmod{p}$, viz (2.18). Stačí tedy dokázat, že $a^{(p-1)/2} \equiv 1 \pmod{p}$ právě tehdy, když a je kvadratický zbytek modulo p.

Nechť a je kvadratický zbytek modulo p, tj. $a \equiv b^2 \pmod{p}$ pro nějaké b takové, že $b \not\equiv 0 \pmod{p}$. Pak podle Malé Fermatovy věty 2.13 platí

$$a^{(p-1)/2} \equiv \left(b^2\right)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Předpokládejme obráceně, že $a^{(p-1)/2} \equiv 1 \pmod{p}$ a nechť q je primitivní kořen modulo p. Pak $a \equiv q^t \pmod{p}$ pro nějaké t tak, že $1 \leq t \leq p-1$. Tudíž

$$q^{t(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Platí však $\mathrm{ord}_p q = p-1$, a proto $(p-1) \mid t(p-1)/2$. Odtud vyplývá, že $2 \mid t$. Nechť tedy $t = 2j$. Pak

$$(q^j)^2 = q^t \equiv a \pmod{p}$$

a $\left(\frac{a}{p}\right) = 1$. □

V následujícím výkladu uvádíme některé základní vlastnosti Legendrova symbolu, které využijeme v dalších kapitolách.

Věta 2.22. *Nechť p je liché prvočíslo. Pak pro celá čísla a a b platí:*

(I) *jestliže* $a \equiv b \pmod{p}$, *pak* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(II) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(III) *jestliže* $(a,p) = 1$, *pak* $\left(\frac{a^2}{p}\right) = 1, \quad \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$;

(IV) $\left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;

(V) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Důkaz této věty lze nalézt v knihách (Burton, 1998, s. 178–183) a (Niven, Zuckerman, Montgomery, 1991, s. 132–135).

Následující zákon kvadratické reciprocity jako první dokázal Gauss. Nazval jej *Theorema aureum* (Zlatá věta). Je to velice užitečný nástroj pro výpočet Legendrova symbolu $\left(\frac{p}{q}\right)$ pro lichá prvočísla p a q, viz (Gauss, 1986, articles 135–144).

Věta 2.23 (Zákon kvadratické reciprocity). *Jestliže p a q jsou lichá prvočísla, pak*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Důkaz je uveden například v (Burton, 1998, s. 188–190), (Koblitz, 1994, s. 45–46) a (Niven, Zuckerman, Montgomery, 1991, s. 137–138).

Věty 2.22 a 2.23 nám umožňují podstatně zjednodušit výpočet Legendrova symbolu. Například pro prvočíslo $p = 1999$ podle vlastnosti (II), zákona kvadratické reciprocity a vlastností (I) a (IV) máme

$$\begin{aligned}\left(\frac{111}{1999}\right) &= \left(\frac{3\cdot 37}{1999}\right) = \left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right) = \\ &= (-1)^{999}\left(\frac{1999}{3}\right) \times (-1)^{999\cdot 18}\left(\frac{1999}{37}\right) = \\ &= (-1)\left(\frac{1}{3}\right)\left(\frac{1}{37}\right) = -1.\end{aligned}$$

Legendrův symbol $\left(\frac{a}{p}\right)$, kde p je prvočíslo, zobecnil německý matematik Carl Gustav Jacobi (1804–1851) takto:

Nechť a je celé číslo a nechť $n \geq 3$ je liché. Nechť $n = p_1 p_2 \cdots p_r$, kde p_i jsou lichá prvočísla ne nutně různá. Pak *Jacobiho symbol* $\left(\frac{a}{n}\right)$ je definován vztahem

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right), \tag{2.37}$$

kde $\left(\frac{a}{p_i}\right)$ je Legendrův symbol.

Vlastnosti Jacobiho symbolu jsou podobné vlastnostem Legendrova symbolu. Například opět platí zákon kvadratické reciprocity. Pro lichá prvočísla se oba symboly rovnají.

Věta 2.24. *Nechť $m > 1$ a $n > 1$ jsou lichá čísla. Pak pro celá čísla a, b platí:*

(I) *jestliže* $a \equiv b \pmod{n}$, *pak* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$;

(II) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;

(III) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$;

(IV) *jestliže* $(a, n) = 1$, *pak* $\left(\frac{a^2}{n}\right) = \left(\frac{a}{n^2}\right) = 1$;

(V) *jestliže* $(ab, mn) = 1$, *pak* $\left(\frac{a^2 b}{m^2 n}\right) = \left(\frac{b}{n}\right)$;

(VI) $\left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$;

(VII) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$;

(VIII) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ (*zákon kvadratické reciprocity*).

Důkaz je v (Niven, Zuckerman, Montgomery, 1991, s. 143–146).

Jestliže Jacobiho symbol $\left(\frac{a}{n}\right) = 1$, pak a není nutně kvadratický zbytek modulo n, když n je složené. Například

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

ale 2 není kvadratický zbytek modulo 15.

Věta 2.25. *Je-li $n \geq 3$, pak každý primitivní kořen je kvadratické nereziduum modulo n.*

Důkaz. Nechť $n \geq 3$, nechť $a \in \{1, \ldots, n-1\}$ je kvadratické reziduum modulo n a $(a, n) = 1$. Pokud ukážeme, že a není primitivním kořenem, bude věta dokázána.

Podle předpokladu existuje přirozené číslo x tak, že

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

Tuto kongruenci můžeme pomocí (1.4) umocnit na $\varphi(n)/2$, protože $n \geq 3$ a číslo $\varphi(n)$ je tedy sudé. Podle Eulerovy–Fermatovy věty 2.17 proto platí

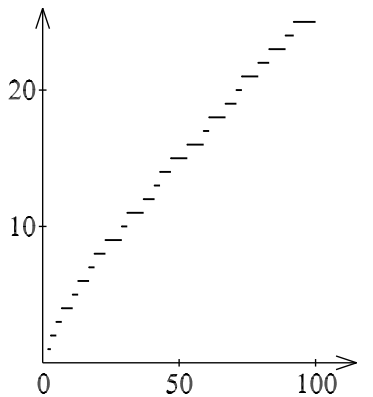
$$a^{\varphi(n)/2} \equiv x^{\varphi}(n) \equiv 1 \pmod{n}.$$

Odtud vyplývá, že a není primitivní kořen. □

Pro úplnost ještě dodejme, že pro $n = 2$ je 1 primitivní kořen modulo 2, ale množina kvadratických nereziduí je prázdná. Pro $n = 1$ jsou množiny primitivních kořenů i kvadratických nereziduí modulo n prázdné.

2.10. Rozklad na prvočísla

Malou Fermatovu větu 2.13 můžeme použít k tomu, abychom ukázali, že dané číslo $p > 1$ je složené, aniž bychom znali nějakého netriviálního dělitele. Pokud totiž nalezneme a nesoudělné s p tak, že kongruence (2.20) neplatí, pak p není prvočíslo. Jestliže například ukážeme, že p nedělí $2^{p-1} - 1$, pak p je složené.



Obr. 2.5. Graf funkce $\pi(x)$.

Zde je třeba zdůraznit, že rozklad daného čísla n na prvočinitele je mnohem obtížnější než zjišťovat, zda je n prvočíslo či číslo složené. C. F. Gauss pokládá rozklad na prvočinitele za velice důležitou základní úlohu aritmetiky (Gauss, 1986, article 329).

Nejstarší metoda rozkladu čísla n na prvočinitele postupně zkouší dělit n všemi prvočísly nepřevyšujícími $\sqrt{n}$, viz (Sedláček, 1977, s. 20). Například k tomu, abychom touto metodou prokázali, že 283 je prvočíslo, je třeba prověřit, že není dělitelné 2, 3, 5, 7, 11 a 13. Zde je ale nutné zdůraznit, že tato metoda není příliš efektivní. Předpokládejme, že jsme schopni provést miliardu dělení za sekundu. Pak bychom potřebovali pro rozložení čísla $n = pq$, kde p a q jsou neznámá třiceticiferná prvočísla, více času, než je stáří vesmíru ($\approx 13.7 \cdot 10^9$ let).

Abychom se o tom přesvědčili, označme $\pi(x)$ počet prvočísel nepřevyšujících x (obr. 2.5). Pak podle Gaussova vztahu, viz např. (Hardy, Wright, 1979), (Schroeder, 2006), je hodnota funkce $\pi(x)$ přibližně rovna $\frac{x}{\log x}$. Přitom chyba je menší než 15 % pro každé $x \geq 3000$. V roce 1896 Jacques Hadamard (1865–1963) a nezávisle též Charles-Jean de la Vallée Poussin (1866–1962) dokázali dokonce asymptotickou rovnost pro $x \to \infty$,

$$\pi(x) \approx \frac{x}{\log x} \qquad (\textit{prvočíselná věta}). \tag{2.38}$$

Protože celá část $\sqrt{n}$ má 30 cifer, existuje alespoň

$$10^{29}/(29 \log 10) \approx 1.5 \cdot 10^{27}$$

prvočísel menších než $\sqrt{n}$. Protože rok má $3.2 \cdot 10^7$ sekund, můžeme za tuto dobu učinit $3.2 \cdot 10^{16}$ dělení. Abychom ale vyzkoušeli všechna prvočísla menší než $\sqrt{n}$, potřebovali bychom k rozkladu n alespoň $47 \cdot 10^9$ roků, což je více než trojnásobek stáří vesmíru. Matematikové přirovnávají takový algoritmus k úsilí rozbít atom kladivem.

Pokud máme nějakou dodatečnou informaci o čísle, jež má být rozkládáno, nebo o jeho prvočinitelích, rozklad lze provést mnohem efektivněji (viz např. věty 4.3 a 4.17).

Při rozkladu daného čísla n na prvočinitele se obvykle n hledá jako součin dvou či více netriviálních dělitelů ne nutně prvočíselných. Ty se pak opět zkoušejí rozložit na další netriviální dělitele tak dlouho, dokud nedostaneme prvočíselný rozklad.

Dále budeme předpokládat, že n je liché a složené, protože mocniny dvojky lze snadno oddělit.

Jedna z metod pro rozklad čísla n je pokusit se n napsat jako rozdíl čtverců. Tak okamžitě dostaneme rozklad na dva netriviální činitele

$$n = a^2 - b^2 = (a + b)(a - b), \tag{2.39}$$

pokud $a - b > 1$. Jestliže obráceně $n = qr$, kde $q \geq r \geq 1$, pak n lze napsat jako rozdíl dvou čtverců

$$n = \left(\frac{q + r}{2}\right)^2 - \left(\frac{q - r}{2}\right)^2,$$

kde čísla v závorkách jsou celá nezáporná, protože q a r jsou lichá.

Pomocí vztahu (2.39) Fermat navrhl metodu, kterou dnes nazýváme *Fermatovou metodou rozkladu.* Nutno dodat, že jeho metoda je efektivní, jen pokud je n součin dvou skoro stejně velkých činitelů. Algoritmus metody probíhá takto:

Jestliže n je čtverec, jsme hotovi. Pokud není čtverec, definujeme

$$a = \lfloor \sqrt{n} \rfloor + 1,$$

kde $\lfloor \sqrt{n} \rfloor$ označuje celou část $\sqrt{n}$. Dále položíme

$$x = a^2 - n.$$

Pokud je x čtverec, jsme hotovi, protože $n = (a + \sqrt{x})(a - \sqrt{x})$. V opačném případě vypočítáme dalšího možného kandidáta

$$(a + 1)^2 - n = a^2 + 2a + 1 - n = x + 2a + 1$$

a prověříme, zda je čtvercem či nikoliv. Pokud ano, jsme opět hotovi, jinak zvětšíme a o dvě a pokračujeme stejným způsobem dále. Po konečně mnoha krocích najdeme dva netriviální dělitele, viz např. (Beran, 1995), (Burton, 1998, s. 97–99), (Koblitz, 1994, s. 143–144).

Následující metoda rozkladu se připisuje Leonhardu Eulerovi. Nechť n lze vyjádřit jako součet dvou nenulových čtverců dvěma různými způsoby, tj.

$$n = a^2 + b^2 = c^2 + d^2, \tag{2.40}$$

kde bez újmy na obecnosti můžeme předpokládat, že $a > c \geq d > b \geq 1$. Pak n je složené číslo, neboť

$$\begin{aligned} n &= \frac{(a^2 - d^2)(c^2 + d^2)}{a^2 - d^2} = \frac{a^2c^2 - d^2(c^2 - a^2 + d^2)}{a^2 - d^2} \\ &= \frac{a^2c^2 - d^2b^2}{a^2 - d^2} = \frac{(ac + bd)(ac - bd)}{(a + d)(a - d)}. \end{aligned} \tag{2.41}$$

Protože n je celé, můžeme vykrátit všechny činitele ve jmenovateli, a tak dostaneme, že n je součin dvou netriviálních činitelů. K této metodě se ještě vrátíme ve větě 3.13.

Francouzská matematička Sophie Germainová (1776–1831) zjistila, že každé číslo tvaru $a^4 + 4$ je složené pro $a > 1$, protože se dá rozložit na dva netriviální činitele,

$$a^4 + 4 = \left(a^2 + 2\right)^2 - 4a^2 = \left(a^2 + 2 + 2a\right)\left(a^2 + 2 - 2a\right). \tag{2.42}$$

Rovnost (2.42) je speciálním případem vztahu

$$a^4 + 4b^2 = \left(a^2 + 2b^2\right)^2 - 4a^2b^2 = \left(a^2 + 2b^2 + 2ab\right)\left(a^2 + 2b^2 - 2ab\right).$$

Další jednoduchý rozklad pro $m > 1$ nalezl Léon François Antoine Aurifeuille v roce 1873

$$2^{4m-2} + 1 = (2^{2m-1} + 2^m + 1)(2^{2m-1} - 2^m + 1). \tag{2.43}$$

Fortuné Landry strávil mnoho let hledáním rozkladu čísla $2^{58} + 1$, který nalezl v roce 1869. Znalost vztahu (2.43) by mu ale ušetřila mnoho času, neboť

$$2^{58} + 1 = \left(2^{29} + 2^{15} + 1\right)\left(2^{29} - 2^{15} + 1\right).$$

Rovnost (2.43) lze zobecnit na tvar

$$a^{4m-2} + 1 = (a^{2m-1} + a^m + 1)(a^{2m-1} - a^m + 1). \tag{2.43}$$

Uveďme ještě další známé rozklady na dva činitele

$$a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1}).$$

Pokud je $m = 2k$ sudé, platí také obecně jiný rozklad

$$a^{2k} - b^{2k} = (a+b)(a^{2k-1} - a^{2k-2}b + a^{2k-3}b^2 - \cdots - b^{2k-1}).$$

Pro liché $m = 2k+1$ zase máme

$$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - a^{2k-3}b^3 + \cdots + b^{2k})$$

a jako speciální případ dostáváme

$$a^{2m} + b^{2m} = (a^2)^m + (b^2)^m = \\ = (a^2 + b^2)(a^{2m-2} - a^{2m-4}b^2 + \cdots + b^{2m-2}).$$

Rozklad na tři činitele má každé číslo tvaru

$$3^{6k-3} + 1 = \left(3^{2k-1} + 1\right)\left(3^{2k-1} - 3^k + 1\right)\left(3^{2k-1} + 3^k + 1\right).$$

Další příklady speciálních typů čísel, která lze apriori rozložit na menší činitele, jsou uvedeny v knize (Wells, 2005, s. 15).

Jak již bylo řečeno, je mnohem obtížnější rozložit složené číslo na dva netriviální činitele než jenom zjistit, že je složené. Známá metoda RSA pro šifrování tajných zpráv pomocí dvou velkých prvočísel je založena právě na této skutečnosti (viz oddíl 5.2). Počet aritmetických operací pro rozklad velkého čísla na dvě prvočísla totiž roste exponenciálně. Pokud má takové číslo například 200 cifer, pak je téměř nemožné jej dnešními prostředky rozložit. Na druhé straně pro ověření prvočíselnosti libovolného čísla o 200 cifrách na počítači stačí jen několik minut.

Přehled nejlepších algoritmů na prvočíselné rozklady čísel je podán například v (Crandall, Pomerance, 2005), (Lenstra, Lenstra, Manasse, Pollard, 1993) a (Pomerance, 1998). Mezi nejefektivnější patří Pollardův algoritmus, který je vhodný pro rozklad těch čísel, pro jejichž nějakého dělitele existuje „blízké“ číslo (± 10) složené pouze z „malých“ činitelů menších než 20 000. Za jeden z nejúčinnějších algoritmů je také považován Lenstrův algoritmus (a jeho různé modifikace), v němž je grupa čísel modulo p nahrazena grupou bodů na eliptické křivce.

3. VLASTNOSTI PRVOČÍSEL

Matematika je královnou věd
a aritmetika je královnou matematiky.

Carl Friedrich Gauss

3.1. Kritéria prvočíselnosti

Pro přirozená čísla j, m, n řekneme, že m^j *přesně dělí* n, a budeme psát $m^j \parallel n$, jestliže $m^j \mid n$, ale $m^{j+1} \nmid n$. Pro $j = 0$ bude symbol $m^0 \parallel n$ znamenat, že $m \nmid n$.

Věta 3.1. *Přirozené číslo n je prvočíslem právě tehdy, když $n \mid \binom{n}{k}$ pro všechna $k \in \{1, \ldots, n-1\}$.*

D ů k a z. $\Rightarrow$: Pro $k \in \{1, \ldots, n-1\}$ je $n-k$ také mezi čísly 1 a $n-1$. Jelikož n je prvočíslo, $n \nmid k!$ a $n \nmid (n-k)!$. Vidíme tedy, že

$$n \mid \binom{n}{k} = \frac{n!}{k!(n-k)!},$$

neboť $n \mid n!$.

$\Leftarrow$: Nechť naopak n je složené a nechť p je nejmenší prvočíslo, které dělí n. Tedy $1 < p < n$ a platí

$$\binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)\cdots 2 \cdot 1}. \tag{3.1}$$

Předpokládejme, že $p^j \parallel n$ pro nějaké přirozené číslo j. Mezi p postupně jdoucími čísly $n, n-1, \ldots, n-p+1$ je právě jedno dělitelné p. Protože $p \mid n$, platí

$$p \nmid (n-1)(n-2)\cdots(n-p+1).$$

Tudíž $p^j \parallel n(n-1)\cdots(n-p+1)$ a zřejmě $p \parallel p(p-1)\cdots 2 \cdot 1$. Podle (3.1) tedy dostaneme, že $p^{j-1} \parallel \binom{n}{p}$. Ale $n \nmid \binom{n}{p}$, protože $p^j \parallel n$. □

Jako důsledek věty 3.1 dostáváme následující pravidlo, které umožňuje snadněji manipulovat s mocninami a kongruencemi. Jestliže p je prvočíslo, pak

$$(a+b)^p \equiv a^p + b^p \pmod{p}. \tag{3.2}$$

Z $p+1$ členů získaných rozvojem $(a+b)^p$ modulo p pomocí binomické věty

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + b^p$$

zůstanou jen a^p a b^p, protože všechny ostatní členy jsou podle věty 3.1 dělitelné p, tj. $p \mid \binom{p}{k}$ pro $1 \leq k \leq p-1$, což můžeme také zapsat takto:

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Věta 3.1 má řadu dalších aplikací. Byla kupříkladu použita v průlomovém článku (Agrawal, Kayal, Saxena, 2004), kde je popsán nový deterministický algoritmus pro testování prvočíselnosti, který je polynomický v čase. Pro zadané číslo n je jeho výpočetní složitost $\mathcal{O}\big((\log n)^{12}\big)$, kde $\log n$ je úměrný počtu cifer čísla n. Zatím se však tento algoritmus pro praktické účely nepoužívá, protože exponent 12 je příliš velký.

Francouzský matematik François Proth (1852–1879) během svého krátkého života publikoval následující tvrzení (Proth, 1878).

Věta 3.2 (Prothova). *Nechť* $q = k2^n + 1$, $k < 2^n$ *a nechť* $\left(\frac{a}{q}\right) = -1$. *Pak* q *je prvočíslo právě tehdy, když*

$$a^{(q-1)/2} \equiv -1 \pmod{q}. \tag{3.3}$$

Důkaz je uveden například v (Křížek, Luca, Somer, 2001, s. 70). Prothova věta má důležité použití při testování prvočíselnosti, jak ještě uvidíme v oddílech 4.2 a 7.6.

Věta 3.3. *Nechť p je liché prvočíslo. Pak*

$$p \equiv 1 \pmod 4 \quad \Longleftrightarrow \quad \left(\frac{-1}{p}\right) = 1,$$

$$p \equiv -1 \pmod 4 \quad \Longleftrightarrow \quad \left(\frac{-1}{p}\right) = -1.$$

D ů k a z. Pro prvočíslo tvaru $p = 4k + 1$ podle věty 2.22 platí

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2k} = 1.$$

Podobně pro $p = 4k - 1$ dostáváme

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2k-1} = -1.$$

Odtud též plynou obrácené implikace. □

Věta 3.4. *Nechť p je prvočíslo. Je-li a přirozené číslo menší než p, pak existuje právě jedno přirozené číslo x menší než p, které je řešením kongruence*

$$ax \equiv 1 \pmod p. \tag{3.4}$$

D ů k a z. Podle Malé Fermatovy věty 2.13

$$a^{p-1} = a(a^{p-2}) \equiv 1 \pmod p,$$

neboť $(a, p) = 1$. Za x tedy můžeme zvolit přirozené číslo menší než p kongruentní s a^{p-2} modulo p.

Dále dokážeme jednoznačnost řešení x. Nechť tedy existují dvě řešení kongruence (3.4), tj. $ax \equiv ay \equiv 1 \pmod p$. Protože

$$ax - ay = a(x - y) \equiv 0 \pmod p,$$

vidíme podle První Eukleidovy věty 2.1, že $p \mid a$ nebo $p \mid (x - y)$. Prvočíslo p ale nemůže dělit a, protože $(a, p) = 1$, a tedy platí $p \mid (x - y)$, tj. $x \equiv y \pmod p$. Protože obě přirozená čísla x a y jsou menší než p, dostáváme, že $x = y$. □

Přirozené číslo x z věty 3.4 nazveme *inverzním prvkem* k a modulo prvočíslo p.

Věta 3.5. *Je-li $p > 2$ prvočíslo a $a^2 \equiv 1 \pmod{p}$, pak buď*

$$a \equiv 1 \pmod{p}, \quad \text{nebo} \quad a \equiv -1 \pmod{p}.$$

Důkaz. Protože platí $(a-1)(a+1) \equiv 0 \pmod{p}$, máme $p \mid (a-1)(a+1)$. Podle První Eukleidovy věty 2.1 pro prvočíslo $p > 2$ platí buď $p \mid (a-1)$, nebo $p \mid (a+1)$. □

Dalším důležitým kritériem prvočíselnosti se budeme zabývat v oddílu 3.2.

3.2. Wilsonova věta

John Wilson (1741–1793) byl vynikající britský matematik z univerzity v Cambridge. Následující větu, která nese jeho jméno, ale neobjevil.

Věta 3.6 (Wilsonova). *Číslo $p > 1$ je prvočíslo právě tehdy, když*

$$(p-1)! \equiv -1 \pmod{p}. \tag{3.5}$$

V roce 1770 Edward Waring poprvé publikoval v *Meditationes algebraicae* na s. 288 bez důkazu implikaci $\Rightarrow$ a věnoval ji Johnu Wilsonovi. Doslova napsal, že pokud je p prvočíslem, pak součet $(p-1)! + 1$ je dělitelný p. Tehdy totiž ještě nebyl zaveden pojem kongruence. Podle (Hardy, Wright, 1979, s. 81) a (Porubský, 2002) implikaci $\Rightarrow$ v poněkud modifikované formě znal již dříve G. W. Leibniz (1646–1716). Obrácenou implikaci $\Leftarrow$ později dokázal J.-L. Lagrange v roce 1773. Proto se větě 3.6 někdy také říká Wilsonova–Lagrangeova věta.

Poznamenejme ještě, že předpoklad $p > 1$ se v mnoha učebnicích opomíjí. Pro $p = 1$ je ale kongruence (3.5) splněna, zatímco 1 není podle definice prvočíslo.

Důkaz věty 3.6 $\Rightarrow$: Jestliže $p = 2$, pak kongruence (3.5) zřejmě platí. Nechť tedy $p > 2$ je prvočíslo a nechť a je libovolné přirozené číslo menší než p. Podle věty 3.4 existuje právě jedno přirozené číslo $b < p$ tak, že $ab \equiv 1 \pmod{p}$. Z věty 3.5 potom

dostáváme, že když $ab \equiv 1 \pmod{p}$ a $b \equiv a \pmod{p}$, pak $a \equiv 1 \pmod{p}$, anebo $a \equiv p-1 \pmod{p}$. Odtud plyne, že přirozená čísla $2, 3, \ldots, p-2$ lze přerovnat na posloupnost $a_2, a_3, \ldots, a_{p-2}$ tak, aby po dvojicích platilo

$$a_i a_{i+1} \equiv 1 \pmod{p}$$

pro $i = 2, 4, 6, \ldots, p-3$. Mezi 2 a $p-2$ je právě $p-3$ čísel, tj. sudý počet. Proto

$$(p-1)! \equiv 1 \cdot (p-1) a_2 \cdots a_{p-2} \equiv (p-1) 1^{(p-3)/2} \equiv -1 \pmod{p}.$$

$\Leftarrow$: Ukážeme, že pokud je n složené, pak $(n-1)! \equiv 2 \pmod{n}$ pro $n = 4$ a $(n-1)! \equiv 0 \pmod{n}$ pro $n > 4$. Okamžitě vidíme, že

$$(4-1)! = 6 \equiv 2 \pmod{4}.$$

Předpokládejme nyní, že $n > 4$ je složené číslo a nechť není čtvercem. Pak můžeme rozložit n takto:

$$n = dk,$$

kde $2 \leq d < k < n-1$. Tudíž $dk \mid (n-1)!$ a $(n-1)! \equiv 0 \pmod{n}$.

Konečně předpokládejme, že $n > 4$ a $n = k^2$. Pak $3 \leq k < 2k \leq n-1$, a tedy $k(2k) \mid (n-1)!$. Protože $2k^2 \equiv 0 \pmod{n}$, v tomto případě také máme $(n-1)! \equiv 0 \pmod{n}$. □

Jako důsledek předchozího důkazu Wilsonovy věty dostáváme následující tvrzení.

Věta 3.7. *Přirozené číslo $n > 4$ je složené právě tehdy, když*

$$(n-1)! \equiv 0 \pmod{n}. \tag{3.6}$$

Wilsonovu větu 3.6 lze dokázat mnoha způsoby, viz např. (Dickson, 1919, Chapt. III), (Robbins, 1993, s. 89). Důkazem implikace $\Rightarrow$ se také zabýval významný český matematik Karel Petr (1868 až 1950) v roce 1905. Stručně si naznačíme hlavní myšlenku jeho důkazu, protože má neobvykle krásnou geometrickou interpretaci, viz (Petr, 1905).

V Petrově důkazu se uvažují orientované, po částech lineární uzavřené křivky, které procházejí všemi vrcholy pravidelného p-úhelníku, kde p je prvočíslo. Přitom křivky s opačnou orientací se považují za odlišné. Dohromady je všech křivek právě $(p-1)!$. Začneme-li totiž od libovolného vrcholu, pak můžeme projít zbývajícími $p-1$ vrcholy právě tolika způsoby, kolik je permutací z $p-1$ prvků.

Regulární křivky budou ty, které se nezmění při otočení o úhel $2\pi/p$ kolem středu pravidelného p-úhelníku. Ostatní křivky nazveme *neregulárními* (obr. 3.1).

Počet regulárních křivek je zřejmě $p-1$. Například pro $p=5$ je jedna z těchto křivek nakreslena vlevo na obr. 3.1, další má opačnou orientaci a zbývající dvě regulární křivky mají tvar pravidelného pětiúhelníku s hranami orientovanými po směru a proti směru hodinových ručiček. Petr ukazuje, že počet neregulárních křivek je pm pro nějaké vhodné přirozené číslo m. Odtud pro celkový počet všech křivek plyne, že

$$(p-1)! = p - 1 + pm,$$

což implikuje dokazovanou kongruenci (3.5).

Obr. 3.1. Příklad regulární (vlevo) a neregulární křivky (vpravo) pro $p = 5$.

Zatím neznáme efektivní algoritmus pro výpočet faktoriálu. Proto je Wilsonova věta velice nepraktická pro testování prvočíselnosti p na počítačích. Je to ale dobrý teoretický prostředek v důkazové technice.

Faktoriál na levé straně kongruence (3.5) lze podstatně zredukovat, jak uvidíme v následujících větách.

Věta 3.8. *Je-li p prvočíslo tvaru $p = 4k + 1$, pak*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}.$$

D ů k a z. Podle Wilsonovy věty 3.6 je

$$(p-1)! = 1\cdot 2\cdot 3\cdots\frac{p-1}{2}\frac{p+1}{2}\frac{p+3}{2}\cdots(p-1) \equiv -1 \pmod{p}, \tag{3.7}$$

kde prostřední zlomky jsou celá čísla, protože p je liché. Dále vidíme, že platí modulo p

$$p-1 \equiv -1, \quad p-2 \equiv -2, \ldots, \quad \frac{p+1}{2} \equiv -\frac{p-1}{2}.$$

Vztah (3.7) můžeme tedy po dvojicích přerovnat tak, že

$$(p-1)! \equiv 1(-1)2(-2)\cdots\frac{p-1}{2}\left(-\frac{p-1}{2}\right) =$$
$$= \left(\left(\frac{p-1}{2}\right)!\right)^2(-1)^{(p-1)/2} \pmod{p}.$$

Odtud a z Wilsonovy věty 3.6 dostaneme, že

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{2}} = -1 \pmod{p}, \tag{3.8}$$

protože $p = 4k + 1$. □

Z předchozí věty tedy plyne, že kongruence

$$x^2 \equiv -1 \pmod{p}$$

má řešení, je-li p tvaru $4k + 1$.

Věta 3.9. *Je-li p prvočíslo tvaru $p = 4k - 1$, pak*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p} \tag{3.9}$$

a

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}. \tag{3.10}$$

D ů k a z. Nechť $p = 4k - 1$. Celý důkaz je stejný jako důkaz věty 3.8, jen poslední ekvivalence v (3.8) bude rovna 1, a tedy platí (3.9). Protože však p je liché prvočíslo, můžeme podle věty 3.5 obě strany odmocnit a dostaneme (3.10). □

V článku (Mordell, 1961) se uvádí, jaké konkrétní znaménko v (3.10) platí pro prvočísla tvaru $p = 4k - 1$.

3.3. Dirichletova věta

V roce 1837 Peter Gustav Lejeune Dirichlet (1805–1859) dokázal zajímavou větu, která používá velice důmyslné analytické metody v teorii čísel.

Věta 3.10 (Dirichletova). *Nechť $a, d \in \mathbb{N}$ jsou nesoudělná čísla. Pak existuje nekonečně mnoho prvočísel v aritmetické posloupnosti*

$$a,\ a+d,\ a+2d,\ a+3d,\ \ldots$$

Důkaz této věty je v původní práci (Dirichlet, 1837). Ekvivalentně můžeme větu 3.10 formulovat tak, že množina

$$S = \{p \in \mathbb{N};\ p \text{ je prvočíslo a } p \equiv a \pmod{d}\}$$

má nekonečně mnoho prvků. Navíc hustota množiny S v množině prvočísel je $1/\varphi(d)$, kde φ je Eulerova funkce, tj.

$$\lim_{x\to\infty} \frac{|\{p\in\mathbb{N};\ p \text{ je prvočíslo, } p\equiv a \pmod{d} \text{ a } p\le x\}|}{|\{p \in \mathbb{N};\ p \text{ je prvočíslo a } p \le x\}|} = \frac{1}{\varphi(d)}.$$

Důkaz tohoto tvrzení je například v (Ireland, Rosen, 1990, s. 251–261).

Mnohem překvapivější tvrzení však bylo zveřejněno v roce 2004 na preprintovém serveru [www3].

Věta 3.11 (Greenova–Taova). *Pro každé $k \in \mathbb{N}$ množina prvočísel obsahuje aritmetickou posloupnost délky k.*

Podrobný téměř padesátistránkový důkaz se uvádí v (Green, Tao, 2008). Jeho hlavní myšlenka je obsahem článku (Klazar, 2004).

Například aritmetická posloupnost

$$5,\ 11,\ 17,\ 23,\ 29$$

délky 5 obsahuje pouze prvočísla. Jiná aritmetická posloupnost prvočísel délky 10 je tato:

$$199,\ 409,\ 619,\ 829,\ 1039,\ 1249,\ 1459,\ 1669,\ 1879,\ 2089$$

(srov. s tab. 1 na str. 335–336). Ještě delší posloupnost prvočísel je

$$(223092870n + 2236133941)_{n=0}^{15}.$$

Greenova–Taova věta ale tvrdí, že ať si zvolíme přirozené číslo k jakkoliv velké, vždy budou existovat prvočísla

$$p_1 < p_2 < \cdots < p_k$$

taková, že

$$p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1}.$$

3.4. Fermatova vánoční věta

Dne 25. prosince 1640 napsal Pierre de Fermat dopis Marinu Mersennovi, v němž jej informoval o svém novém objevu. Fermat přišel na to, že každé prvočíslo tvaru $4k + 1$ pro $k \in \mathbb{N}$ se dá jednoznačně napsat jako součet dvou čtverců přirozených čísel a že takové prvočíslo je přeponou právě jednoho pythagorejského trojúhelníku o stranách $a < b < c$. V dopise doslova (ve starofrancouzštině) píše:

Tout nombre premier, qui sourpasse de l'unité un multiple du quaternaire, est une seul fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle.

Například prvočísla 5, 13 a 17 můžeme napsat jako součet dvou čtverců takto:

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2 \quad \text{a} \quad 17 = 1^2 + 4^2.$$

Tomuto významnému objevu se začalo říkat Fermatova vánoční věta, protože Fermat napsal svůj dopis Mersennovi o Vánocích právě na Boží hod. Dále vidíme, že čísla 5, 13 a 17 jsou přepony pythagorejských trojúhelníků o stranách $\langle 3,4,5\rangle$, $\langle 5,12,13\rangle$ a $\langle 8,15,17\rangle$. K této zajímavé vlastnosti se vrátíme později.

Každé liché přirozené číslo větší než 1 je zřejmě tvaru $4k\pm 1$ pro nějaké $k\in\mathbb{N}$. Z věty 2.6, která také přísluší Fermatovi, již víme, že žádné číslo tvaru $4k-1$ pro $k\in\mathbb{N}$ není součtem dvou čtverců celých čísel. Ve větách 3.12 a 3.13 se budeme zabývat čísly tvaru $4k+1$.

Už v době svého pobytu v Bordeaux v roce 1629 byl Fermat hodně ovlivněn dílem Françoise Viète. Zde studoval Viètovy traktáty *Isagoge* (Tours, 1591) a *De recognitione et emendatione aequationum* (Paris, 1615). Při dokazování vánoční věty Fermat použil následující rovnosti, které pocházejí právě od Viète,

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2=(ac-bd)^2+(ad+bc)^2, \tag{3.11}$$

a nazývají se *Viètovy identity.* Podrobný důkaz vánoční věty ale podal až Euler.

Věta 3.12 (Fermatova vánoční věta). *Každé prvočíslo tvaru $p=4k+1$ lze jednoznačně napsat jako součet dvou čtverců přirozených čísel.*

D ů k a z. Nejprve dokážeme jednoznačnost takového rozkladu. Předpokládejme tedy, že prvočíslo p lze napsat dvěma způsoby jako součet dvou čtverců

$$p=a^2+b^2=c^2+d^2,$$

kde a,b,c,d jsou přirozená čísla. (Ani není nutné předpokládat, že je tvaru $4k+1$.) Pak

$$\begin{aligned} a^2c^2-b^2d^2 &= a^2(a^2+b^2-d^2)-d^2(c^2+d^2-a^2)= \\ &= a^2(a^2+b^2)-d^2(c^2+d^2)=p(a^2-d^2)\equiv 0 \pmod p, \end{aligned}$$

a tedy podle První Eukleidovy věty 2.1 platí

$$ac \equiv bd \pmod{p} \quad \text{nebo} \quad ac \equiv -bd \pmod{p}.$$

Protože a, b, c, d jsou všechna menší než $\sqrt{p}$, platí

$$ac - bd = 0 \quad \text{nebo} \quad ac + bd = p.$$

Pokud platí druhá rovnost, pak podle Viètových rovností (3.11) máme

$$p^2 = (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 = p^2+(ad-bc)^2,$$

tj. $ad - bc = 0$. Tudíž dohromady

$$ac = bd \quad \text{nebo} \quad ad = bc.$$

Předpokládejme například, že $ac = bd$. Pak $a \mid d$, protože $a \mid bd$ a $(a, b) = 1$. Proto existuje přirozené m tak, že $d = ma$. Odtud plyne, že $c = mb$, a proto

$$p = c^2 + d^2 = m^2(a^2 + b^2),$$

což dává $m = 1$, $a = d$ a $b = c$.

Kdybychom předpokládali, že $ad = bc$, pak zcela analogicky dostaneme, že $a = c$ a $b = d$. Tím jsme dokázali jednoznačnost rozkladu prvočísla p na dva čtverce (až na pořadí sčítanců).

Dále se budeme věnovat důkazu existence tohoto rozkladu. Nechť

$$z \equiv \Big(\frac{p-1}{2}\Big)! \pmod{p},$$

kde $0 \le z \le p - 1$. Protože p je tvaru $4k + 1$, podle věty 3.8 platí

$$z^2 \equiv -1 \pmod{p}. \tag{3.12}$$

Uvažujme uspořádanou dvojici $\langle x, y\rangle$, kde $x, y \in \{0, 1, \ldots, n-1\}$, $n = \lfloor\sqrt{p}\rfloor + 1$ a $\lfloor r\rfloor$ označuje celou část reálného čísla r (tj. největší celé číslo menší nebo rovno r). Takových dvojic je právě n^2, a proto existuje n^2 čísel typu $x - zy$ pro $x, y \in \{0, 1, \ldots, n - 1\}$, neboť z je pevné číslo. Protože máme právě p různých zbytků modulo p a $n^2 > p$, z Dirichletova principu (viz věta 1.5) plyne, že existují

dvě různé uspořádané dvojice $\langle x', y' \rangle$ a $\langle x'', y'' \rangle$ takové, že

$$x' - zy' \equiv x'' - zy'' \pmod{p},$$

kde $x', y', x'', y'' \in \{0, 1, \ldots, n-1\}$. Tedy

$$x' - x'' \equiv z(y' - y'') \pmod{p}. \tag{3.13}$$

Položíme-li

$$a = |x' - x''| \quad \text{a} \quad b = |y' - y''|,$$

pak $a, b \in \{0, 1, \ldots, n-1\}$ a podle (3.13), (1.4) a (3.12) platí

$$a^2 \equiv z^2 b^2 \equiv -b^2 \pmod{p},$$

tj.

$$a^2 + b^2 \equiv 0 \pmod{p}. \tag{3.14}$$

Obě čísla a a b se ale současně nerovnají nule, protože $\langle x', y' \rangle$ a $\langle x'', y'' \rangle$ jsou různé uspořádané dvojice. Jelikož p je prvočíslo, $\sqrt{p}$ není celé číslo. Proto podle (3.14) platí $0 \leq a < \sqrt{p}$ a $0 \leq b < \sqrt{p}$. Odtud plyne, že

$$0 < a^2 + b^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p.$$

Mezi čísly $1, 2, \ldots, 2p-1$ ale existuje pouze jediné číslo dělitelné prvočíslem p, a tím je právě číslo p. Z (3.14) tedy plyne, že

$$a^2 + b^2 = p. \qquad \square$$

Poznámka. Předpokládejme, že p je prvočíslo tvaru $p = 4k + 1$. V monografii (Bressoud, Wagon, 2000, s. 281) se předkládá Smithův algoritmus, jak vypočítat jednoznačně určená přirozená čísla a a b z věty 3.12 taková, že $p = a^2 + b^2$. K tomu stačí zvolit z tak, že $z^2 \equiv -1 \pmod{p}$, a použít Eukleidův algoritmus na dvojici (p, z). První dva zbytky, které jsou menší než $\sqrt{p}$, jsou právě hledaná čísla a a b.

Zvolme například $p = 61$, tj. $7 < \sqrt{61} < 8$. Vidíme, že $z = 11$ splňuje kongruenci

$$z^2 \equiv -1 \pmod{61}.$$

Pak podle Eukleidova algoritmu z oddílu 1.4 dostáváme

$$(61, 11) = (11, 6) = (6, 5),$$

a tedy

$$61 = 6^2 + 5^2.$$

Poznámka. Číslo z splňující kongruenci $z^2 \equiv -1 \pmod{p}$ lze pro „malá“ p najít pomocí věty 3.8. Pro „větší“ p lze postupovat takto: Protože $p = 4k+1$, je $(p-1)/2$ sudé číslo. Pomocí Eulerova kritéria (2.36) najdeme kvadratické nereziduum a, tj. $a^{(p-1)/2} \equiv -1 \pmod{p}$. To lze udělat zkusmo, neboť počet kvadratických reziduí je stejný jako počet kvadratických nereziduí. Nyní stačí vzít zbytek z, $0 \leq z < p$ takový, že $z \equiv a^{(p-1)/4} \pmod{p}$.

Věta 3.13. *Je-li n číslo složené, které lze napsat jako součin dvou čísel tvaru $4k + 1$, pak lze n napsat jako součet dvou čtverců přirozených čísel více způsoby.*

D ů k a z. Nechť nejprve $n = qr$ pro nějaká prvočísla $q > 1$ a $r > 1$ tvaru $4k + 1$. Z Fermatovy vánoční věty 3.12 a z Viètových rovností (3.11)

$$\begin{aligned} n = qr &= (a^2 + b^2)(c^2 + d^2) \qquad (3.15) \\ &= (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

plyne, že každé číslo, které je součinem dvou prvočísel kongruentních 1 modulo 4, lze napsat jako součet dvou čtverců, kde a, b, c, d jsou přirozená čísla. Indukcí se pak můžeme přesvědčit, že každé číslo, které je součinem dvou či více prvočísel kongruentních 1 modulo 4, je součtem dvou čtverců.

Musíme ještě ukázat, že čtverce v (3.15), jejichž součet dává n, jsou různé. Zřejmě

$$ac + bd \neq ac - bd.$$

Předpokládejme tedy, že $ac + bd = ad + bc$ a $ac - bd = ad - bc$. Jejich sečtením pak dostaneme $2ac = 2ad$, tj. $c = d$. To ale odporuje skutečnosti, že r je liché. □

Obecná věta určující, kolika způsoby lze rozložit libovolné přirozené číslo na součet dvou čtverců, je uvedena v (Hardy, Wright, 1979, s. 241). V oddílech 4.7 (na straně 158) a 5.10 (na straně 210) upozorníme na dvě zajímavé aplikace Fermatovy vánoční věty 3.12 v algebře a bioinformatice. O dalším jejím použití v geometrii věděl už Fermat:

Věta 3.14. *Pro každé prvočíslo tvaru $p = 4k + 1$ existuje právě jedna pythagorejská trojice, jejíž největší číslo* (*odpovídající přeponě*) *je p.*

D ů k a z. Nechť p je prvočíslo. Podle Fermatovy vánoční věty 3.12 je $p = m^2 + n^2$. Protože p je liché, čísla m a n nemohou být současně obě lichá ani obě sudá, tj. jsou rozdílné parity. Protože p je prvočíslo, platí $(m, n) = 1$. Tedy p je přepona odpovídající primitivní pythagorejské trojici podle vztahů (2.5) a (2.6). □

3.5. Polynomy generující prvočísla

V roce 1772 L. Euler píše J. Bernoullimu, že objevil kvadratický polynom

$$p(x) = x^2 + x + 41, \tag{3.16}$$

jenž dává následující posloupnost prvočísel (srov. tab. 1 uvedenou na str. 335) pro $x = 0, 1, \ldots, 39$:

41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197,
223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593,
641, 691, 743, 797, 853, 911, 971, 1033, 1097,
1163, 1231, 1301, 1373, 1447, 1523, 1601. (3.17)

Teprve číslo $p(40) = 40^2 + 40 + 41 = 40 \cdot 41 + 41 = 41^2$ je složené. Je pozoruhodné, že prvočísla dostaneme i pro záporné argumenty $x = -40, -39, \ldots, -1$ polynomu (3.16). Celkem tedy 80 po sobě jdoucích celočíselných argumentů x dává prvočísla.

Jiný kvadratický polynom

$$q(x) = x^2 + x + 17$$

generuje prvočísla pro $x = -16, -15, \ldots, 15$. Russell Ruby objevil polynom

$$r(x) = 36x^2 - 810x + 2753,$$

který dává prvočísla pro $x = 0, 1, \ldots, 44$. Podobných polynomů jsou v literatuře desítky ($2x^2 + 29$, $x^2 - 79x + 1601$, $36x^2 - 810x + 2753$, $103x^2 - 3945x + 34381$ aj.).

91	90	89	88	87	86	85	84	83	82
92	57	56	55	54	53	52	51	50	81
93	58	31	30	29	28	27	26	49	80
94	59	32	13	12	11	10	25	48	79
95	60	33	14	3	2	9	24	47	78
96	61	34	15	4	1	8	23	46	77
97	62	35	16	5	6	7	22	45	76
98	63	36	17	18	19	20	21	44	75
99	64	37	38	39	40	41	42	43	74
100	65	66	67	68	69	70	71	72	73

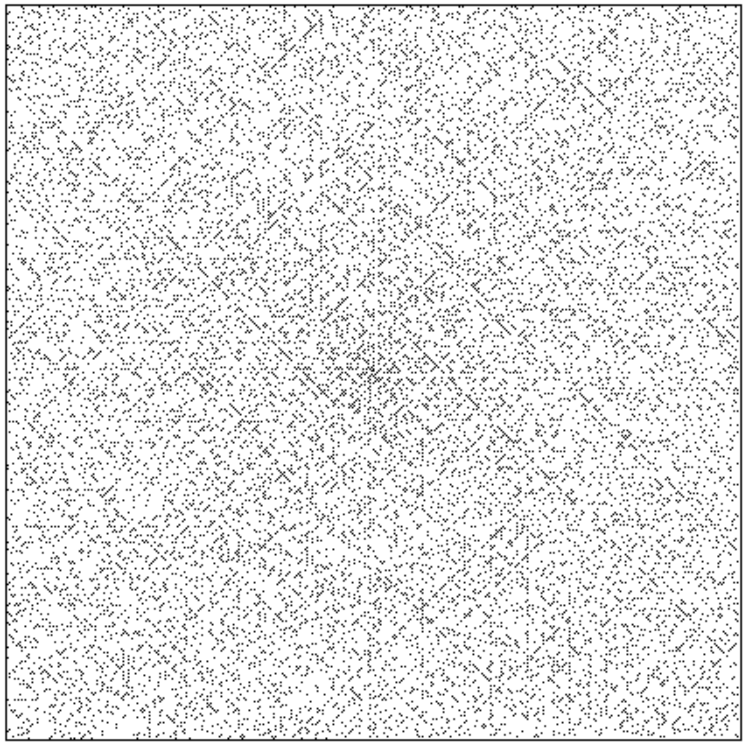
Obr. 3.2. Ulamova čtvercová spirála přirozených čísel. Prvočísla jsou pro odlišení znázorněna na černém podkladě.

Na obrázku 3.2 je znázorněna Ulamova čtvercová spirála, kterou v roce 1963 navrhl polský matematik Stanislaw Marcin Ulam (1909–1984). Prvočísla jsou v ní napsána pro odlišení na černých čtverečcích. Na obrázku 3.3 pak vidíme, jak je rozmístěno prvních 16 000 prvočísel v Ulamově spirále. Povšimněte si zajímavé struktury obsahující řady úseček o směrnicích ± 1, které odpoví-

dají kvadratickým polynomům tvaru $4x^2 + bx + c$. Například pro polynom

$$u(x) = 4x^2 + 10x + 5$$

dostáváme prvočísla $u(0) = 5$, $u(1) = 19$, $u(2) = 41$ a $u(3) = 71$, která leží na úsečce o směrnici -1 (obr. 3.2). Podobně pro polynom $v(x) = 4x^2 + 10x + 7$ platí $v(-4) = 31$, $v(-3) = 13$, $v(-2) = 3$ apod. Pokud bychom spirálu „odvíjeli“ od čísla 41, pak bychom podobným způsobem dostali pro uvedený Eulerův polynom (3.16) úsečku se směrnicí -1 obsahující 80 po sobě jdoucích prvočísel.



Obr. 3.3. Rozložení prvních 16 000 prvočísel na Ulamově spirále.

Profesor matematiky na pražské univerzitě Jakub Filip Kulik (1793–1863) přišel s podobným nápadem již mnohem dříve. Studoval totiž rozložení prvočísel (jsou vyznačena půltučně) mezi přirozenými čísly uspořádanými do trojúhelníku:

$$
\begin{array}{ccccccccccccccccccc}
 & & & & & & & 1 & & & & & & & & & & & \\
 & & & & & & \mathbf{2} & \mathbf{3} & 4 & & & & & & & & & & \\
 & & & & & \mathbf{5} & 6 & \mathbf{7} & 8 & 9 & & & & & & & & & \\
 & & & & 10 & \mathbf{11} & 12 & \mathbf{13} & 14 & 15 & 16 & & & & & & & & \\
 & & & \mathbf{17} & 18 & \mathbf{19} & 20 & 21 & 22 & \mathbf{23} & 24 & 25 & & & & & & & \\
 & & 26 & 27 & 28 & \mathbf{29} & 30 & \mathbf{31} & 32 & 33 & 34 & 35 & 36 & & & & & & \\
 & \mathbf{37} & 38 & 39 & 40 & \mathbf{41} & 42 & \mathbf{43} & 44 & 45 & 46 & \mathbf{47} & 48 & 49 & & & & & \\
50 & 51 & 52 & \mathbf{53} & 54 & 55 & 56 & 57 & 58 & \mathbf{59} & 60 & \mathbf{61} & 62 & 63 & 64 & & & & \\
65 & 66 & \mathbf{67} & 68 & 69 & 70 & \mathbf{71} & 72 & \mathbf{73} & 74 & 75 & 76 & 77 & 78 & \mathbf{79} & 80 & 81 & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

Také sestavil rozsáhlé tabulky prvočíselných dělitelů všech přirozených čísel do sto milionů. Dodnes obdivujeme, jak mohl toto úctyhodné dílo vykonat.

V roce 1976 J. P. Jones, D. Sato, H. Wada a D. Wiens publikovali polynom 25. stupně o 26 proměnných $a, b, \ldots, z$, jehož všechny kladné hodnoty v celočíselných nezáporných bodech jsou prvočísly, blíže viz (Wells, 2005, s. 150),

$$
\begin{aligned}
&(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-\\
&[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]-\\
&[2n+p+q+z-e]^2-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-\\
&u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy^2)+1-(x+cu)^2]^2-[n+l+\\
&v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-\\
&1)+b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+\\
&2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}.
\end{aligned}
$$

Počítat takto prvočísla je ale velmi nepraktické. Povšimněte si, že polynom ve složených závorkách je kladný pouze tehdy, když výrazy v hranatých závorkách jsou nulové. Pak je hodnota složené závorky 1 a hledané prvočíslo je rovno $k + 2$.

3.6. Riemannova hypotéza

Položme

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}, \tag{3.18}$$

kde suma konverguje pro libovolné komplexní číslo z takové, že $\mathrm{Re}(z) > 1$. Funkce ζ má komplexně sdružené kořeny a nazývá se *Riemannova ζ-funkce.* Přitom platí, že $\zeta(1) = \infty$, což je součet harmonické řady, a $\zeta(2) = \pi^2/6$.

Lze dokázat následující překvapivou rovnost obsahující na pravé straně součin přes všechna prvočísla p,

$$\zeta(z) = \prod_{p} \frac{1}{1 - p^{-z}}. \tag{3.19}$$

Už Leonhard Euler uměl odvodit, že (3.18) a (3.19) se rovnají pro z reálná.

Označíme-li i-té prvočíslo p_i, pak podle vzorečku pro součet geometrické posloupnosti máme

$$\sum_{j=0}^{\infty} \left(\frac{1}{p_i}\right)^j = \frac{1}{1 - p_i^{-1}}$$

pro každé $i = 1, 2, \ldots$ Vynásobíme-li mezi sebou prvních m takových rovnic, pak ze Základní věty aritmetiky 2.2 dostaneme

$$\prod_{i=1}^{m} \frac{1}{1 - p_i^{-1}} =$$

$$\left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \ldots\right) \ldots \left(1 + \frac{1}{p_m} + \frac{1}{p_m^2} + \ldots\right) = \sum \frac{1}{n},$$

kde v poslední sumě sčítáme přes všechna přirozená čísla, která nemají žádného prvočinitele většího než p_m. Odtud je již patrné, jak asi Euler přišel ke svému výsledku.

Německý matematik Bernhard Riemann (1826–1866) odvodil pro ζ-funkci další užitečný vztah

$$\pi^{-z/2}\,\Gamma\left(\frac{z}{2}\right)\zeta(z) = \pi^{-(1-z)/2}\,\Gamma\left((1-z)/2\right)\zeta(1-z), \tag{3.20}$$

tj. z lze zaměnit za $1-z$. Zde Γ-funkce je přirozeným rozšířením faktoriálu

$$\Gamma(n) = (n-1)!$$

do množiny komplexních čísel. Funkce $\zeta(1-z)$ na pravé straně (3.20) má pól pro $z=0$ (tj. $\zeta(1)=\infty$) a $\Gamma\left(\frac{1-z}{2}\right)$ má póly v bodech $z = 1, 3, 5, 7, \ldots$. Pravá strana (3.20) se tedy musí anulovat pro $z = 3, 5, 7, \ldots$, a proto

$$0 = \zeta(-2) = \zeta(-4) = \zeta(-6) = \ldots .$$

Tyto kořeny se nazývají *triviální*. Funkci ζ lze spojitě a hladce rozšířit na celou komplexní rovinu kromě bodu 1, v němž má funkce pól.

Riemannova hypotéza říká, že všechny netriviální kořeny mají imaginární část rovnou 0.5. Rozřešení této hypotézy je dnes pokládáno za jeden z nejtěžších a nejdůležitějších problémů teorie čísel, neboť úzce souvisí s otázkou rozložení prvočísel (srov. (3.19)). Na jeho vyřešení byla vypsána odměna 1 000 000 dolarů (viz [www4]). Navíc se ukazuje, že rozdělení vzdáleností netriviálních sousedních kořenů zcela odpovídá spektrální statistice jistého kvantového chaotického systému, viz (Cejnar, 2007).

3.7. Další vlastnosti prvočísel

Následující věta tvrdí, že součet převrácených hodnot všech prvočísel je divergentní.

Věta 3.15. *Nechť $p_1 < p_2 < \ldots$ jsou všechna prvočísla. Pak*

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty. \tag{3.21}$$

D ů k a z. Předpokládejme naopak, že řada v (3.21) je konvergentní. Pak můžeme pevně zvolit přirozené číslo j tak, že zbytek

řady po j členech je menší než $1/2$, tj.

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots < \frac{1}{2}. \tag{3.22}$$

Nechť $N(x)$ označuje počet přirozených čísel n nepřevyšujících x, která nejsou dělitelná žádným prvočíslem $p > p_j$. Pokud vyjádříme takové n ve tvaru

$$n = n_1^2 m, \tag{3.23}$$

kde m není dělitelné žádným čtvercem prvočísla, pak

$$m = 2^{b_1} 3^{b_2} \cdots p_j^{b_j},$$

kde $b_i \in \{0, 1\}$. Existuje tedy 2^j možností různých hodnot m. Z (3.23) vidíme, že

$$n_1 \leq \sqrt{n} \leq \sqrt{x},$$

a tedy existuje nejvýše $\sqrt{x}$ různých hodnot n_1. Odtud plyne, že

$$N(x) \leq 2^j \sqrt{x}. \tag{3.24}$$

Nechť

$$x \geq 2^{2j+2} \tag{3.25}$$

je libovolné kladné číslo a p prvočíslo. Pak počet těch přirozených čísel $n \leq x$, která jsou dělitelná p, je nejvýše $\frac{x}{p}$. Tudíž rozdíl $x - N(x)$ (tj. počet těch $n \leq x$ dělitelných jedním či více prvočísly $p_{j+1}, p_{j+2}, \ldots$) není větší než

$$\frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \cdots < \frac{x}{2}.$$

Z (3.24) však máme

$$\frac{x}{2} < N(x) \leq 2^j \sqrt{x},$$

tj. $x < 2^{2j+2}$, což je spor s (3.25). Řada (3.21) proto diverguje. □

Prvočíselnými dvojčaty nazýváme takovou dvojici prvočísel $\langle p, q\rangle$, pro něž $p < q$ a $q - p \leq 2$. Jsou to například dvojice

$$\langle 2,3\rangle, \quad \langle 3,5\rangle, \quad \langle 5,7\rangle, \quad \langle 11,13\rangle, \quad \langle 17,19\rangle, \quad \langle 10^9+7, 10^9+9\rangle.$$

Z věty 3.15 víme, že pokud sčítáme převrácené hodnoty všech prvočísel, roste tento součet nade všechny meze. Na druhé straně v roce 1919 Viggo Brun ukázal, že součet převrácených hodnot prvočíselných dvojčat (kromě první dvojice)

$$\sum_q \frac{1}{q} = \left(\frac{1}{3}+\frac{1}{5}\right) + \left(\frac{1}{5}+\frac{1}{7}\right) + \left(\frac{1}{11}+\frac{1}{13}\right) + \cdots$$

konverguje k číslu 1.90216057783278…, jež se nazývá *Brunova konstanta.* To tedy znamená, že prvočíselná dvojčata se v posloupnosti všech prvočísel vyskytují velice „řídce". Zatím ale nevíme, zda jich existuje nekonečně mnoho. Nicméně v roce 1949 P. Clement dokázal následující větu, viz (Tattersall, 2005, s. 120).

Věta 3.16 (Clementova). *Číslo* $p(p+2)$ *dělí* $4((p-1)!+1)+p$ *právě tehdy, když* $\langle p,\ p+2\rangle$ *jsou prvočíselná dvojčata.*

Čtveřici prvočísel $\langle p, q, r, s\rangle$ nazveme *prvočíselná čtyřčata,* jestliže $p < q < r < s$ a $s - p \leq 8$. Jsou to například čtveřice $\langle 2,3,5,7\rangle$, $\langle 11,13,17,19\rangle$ nebo

$$10013950 + i \quad \text{pro } i = 1,3,7,9.$$

Pokud by existoval jen konečný počet prvočíselných dvojčat, byl by zřejmě i konečný počet prvočíselných čtyřčat.

Na závěr si ještě položme otázku:

Lze každé sudé číslo větší než 2 *napsat jako součet dvou prvočísel?*

Tato otázka vznikla během vzájemné korespondence mezi Leonhardem Eulerem a Christianem Goldbachem v roce 1742. Skutečně vidíme, že $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5 = 3+7$ apod. Domněnce, že alespoň jeden takový rozklad vždy existuje, se říká *Goldbachova hypotéza.* Do roku 2008 ji nikdo neroz-

řešil. Podle některých pramenů ji poprvé vyslovil Euler inspirován Goldbachem. V roce 1937 ruský matematik Ivan Matvejevič Vinogradov (1891–1983) dokázal, že existuje přirozené číslo n_0 takové, že každé liché $n > n_0$ lze vyjádřit jako součet tří prvočísel.

Na závěr si uveďme ještě jedno pozoruhodné kritérium prvočíselnosti z článku (Mann, Shanks, 1972) opírající se o známý Pascalův trojúhelník, který předložil francouzský matematik Blaise Pascal (1623–1662),

$$
\begin{array}{ccccccccccccccccccc}
 & & & & & & & & 1 & & & & & & & & & & \\
 & & & & & & & 1 & & 1 & & & & & & & & & \\
 & & & & & & 1 & & 2 & & 1 & & & & & & & & \\
 & & & & & 1 & & 3 & & 3 & & 1 & & & & & & & \\
 & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & & \\
 & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & & \\
 & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & & \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & & & \\
1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

Jeho řádky tvoří kombinační čísla $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}$ pro $n = 0, 1, 2, \ldots$ V čínské literatuře je tento trojúhelník pojmenován po matematikovi Yang Huiovi, který jej publikoval ve své knize již z roku 1261 pro $n = 6$ – viz (Křížek, Liu, 1997), (Martzloff, 1997, s. 230).

Věta 3.17. *Přirozené číslo $k > 1$ je prvočíslo právě tehdy, když*

$$n \,\Big|\, \binom{n}{k-2n} \quad \text{pro všechna } n \text{ taková, že } \frac{k}{3} \le n \le \frac{k}{2}.$$

Abychom si přiblížili, co tato věta vlastně říká, utvořme si názornou tabulku. Její horní řádek bude obsahovat pořadová čísla sloupců $k = 0$, 1, **2, 3,** 4, …, kde prvočísla jsou zvýrazněna. Do dalších řádek napišme Pascalův trojúhelník tak, že následující řádek je vždy posunut o dvě místa doprava vzhledem k předchozímu

řádku. Levý sloupec tabulky bude obsahovat pořadová čísla řádků $n = 0,\ 1,\ 2, \ldots$ Pokud je binomický koeficient dělitelný číslem řádku, napíšeme jej také půltučně:

$n \backslash k$	0	1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	12	**13**	14	15	
0	1																
1			**1**	**1**													
2					1	**2**	1										
3						1	**3**	**3**	1								
4							1	**4**	6		**4**		1				
5											1	**5**	**10**	**10**	**5**	1	
6													1	**6**	15	20	...

Věta 3.17 tvrdí, že sloupec obsahuje jen půltučně psané binomické koeficienty právě tehdy, když odpovídá nějakému prvočíslu.

4. SPECIÁLNÍ TYPY PRVOČÍSEL

Přirozená čísla jsou bezpochyby od Boha,
ale ďábel je prošpikoval prvočísly.

Parafrázovaný výrok Leopolda Kroneckera

4.1. Mersennova prvočísla

Kdo byl Marin Mersenne? Francouzský matematik a fyzik Marin Mersenne se proslavil zejména svými objevy v teorii čísel, mechanice a optice. Zasloužil se o zprostředkování komunikace mezi významnými evropskými vědci. Jeho pozůstalost zachycuje 78 různých korespondentů, např. Pierra de Fermata, Christiana Huygense, Johna Pella, René Descarta, Galilea Galileiho, Evangelistu Torricelliho, Giovanna Pieroniho i našeho Jana Ámose Komenského. Tehdy se ještě nevydávaly žádné odborné matematické časopisy, takže písemně informovat Marina Mersenna o svém objevu vlastně nahrazovalo dnešní vědeckou publikaci (viz oddíl 3.4).

Marin Mersenne se narodil 8. září 1588 v Bourg d'Oizé v departementu Sarthe (dříve dépt. Maine) ve Francii. Pamětní deska věnovaná jeho osobě (obr. 4.1) je umístěna na stěně kostela, který přiléhá k náměstí Marina Mersenna v Oizé. V letech 1604–1609 studoval Mersenne na jezuitské koleji v nedalekém La Flèche, i když nikdy do jezuitského řádu nevstoupil. Další dva roky se věnoval studiu teologie na pařížské Sorboně a v roce 1611 vstoupil do řádu minimů. Od roku 1614 několik let vykládal filosofii v klášteře tohoto řádu v Nevers. Později bydlel ve středu Paříže v ulici Rue des Minimes v blízkosti náměstí Place des Vosges (dříve Place Royale). Zde ve svém bytě od roku 1623 pořádal schůzky učenců, mezi nimiž byli mj. Étienne a Blaise (otec a syn) Pascalové, Pierre Gassendi, René Descartes, Gilles Personne de Roberval, Isaac Beeckmann, Thomas Hobbes a též muzikolog Giovanni Battista Doni. Sám Mersenne je také autorem několika hudebních skladeb a rozsáh-

lého muzikologického díla (Mersenne, 1627). Soustřeďoval kolem sebe významné vědce, kteří později v Paříži vytvořili jádro Akademie věd, viz (Křížek, Šolcová, 2001/02).

Mersenne navrhl Huygensovi, aby použil kyvadlo k měření času. Podal také první přesnou definici cykloidy a stanovil její základní vlastnosti. Hledal dokonalý jazyk k popisu přírody. Podporoval racionální a logické uvažování. René Descartes jej pojmenoval „le bon père Mersenne". Pro Gassendiho znamenal největšího z minimů – „Maxime de Minimis". Marin Mersenne zemřel 1. září 1648 v Paříži.

Obr. 4.1. Pamětní deska v Oizé připomíná, že M. Mersenne byl duchovním otcem Akademie věd. Deska byla odhalena ke 400. výročí jeho narození.

Mersennova čísla. Mersennovy matematické zájmy se týkaly především teorie čísel. Studoval mj. čísla tvaru

$$M_p = 2^p - 1,$$

kde p je prvočíslo, která se po něm nazývají *Mersennova čísla.* Jestliže $2^p - 1$ je samo prvočíslo, nazývá se *Mersennovo prvočíslo*.

Poznamenejme, že v české literatuře se občas používá i termín Mersenneovo (prvo)číslo.

Povšimněme si, že číslo $2^{ij} - 1$ pro celá čísla $i > 1$ a $j > 1$ lze napsat jako součin dvou netriviálních činitelů

$$2^{ij} - 1 = (2^i - 1)(2^{i(j-1)} + 2^{i(j-2)} + \cdots + 2^i + 1). \qquad (4.1)$$

Proto požadujeme, aby exponent p Mersennova čísla $2^p - 1$ byl prvočíslem. Sporem snadno z rozkladu (4.1) odvodíme následující větu, kterou znal již Pierre de Fermat, viz (Dickson, 1919, s. 12), (Mahoney, 1994, s. 294).

Věta 4.1. *Je-li $2^p - 1$ prvočíslo, pak p je také prvočíslo.*

D ů k a z. Nechť $2^p - 1$ je prvočíslo a předpokládejme naopak, že p je složené, tj. existují přirozená čísla $i > 1$ a $j > 1$ tak, že $p = ij$. Pak oba činitelé na pravé straně rovnice (4.1) jsou větší než jedna, a tedy číslo $2^p - 1$ je složené, což je ve sporu s předpokladem. □

Vidíme, že první čtyři prvočíselné exponenty $p = 2, 3, 5, 7$ dávají Mersennova prvočísla 3, 7, 31, 127. Avšak pro $p = 11$ je číslo $2^{11} - 1 = 2047$ dělitelné 23. Podobně $2^{23} - 1 = 47 \cdot 178481$ a $2^{29} - 1 = 233 \cdot 2304167$. Obrácená věta 4.1 tedy neplatí. K dělitelům Mersennových čísel se vrátíme ještě ve větách 4.3 a 4.4.

Přestože do roku 2007 bylo objeveno 44 Mersennových prvočísel, málo je známo o jejich skutečném rozložení (několik empirických vztahů se uvádí například v knihách (Schroeder, 2006) a (Wagstaff, 1983). Číslo M_p je prvočíslem, když

$p =$ 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, ...

Sám Marin Mersenne v předmluvě ke své práci *Cogitata Physica-Mathematica* z roku 1644 nesprávně tvrdí, že čísla $2^n - 1$ jsou prvočísla pro n =2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 a jsou složená pro všechna ostatní přirozená čísla $n < 257$, viz (Dickson, 1919, s. 12–13).

K případu $n = 67$ existuje známá historka, viz např. (Porubský, 2002), (Wells, 2005). Frank Nelson Cole (1861–1926) totiž rozložil číslo M_{67} na dvě prvočísla, čemuž věnoval mnoho let. V roce 1903 přednesl na půdě Americké matematické společnosti legendární přednášku beze slov, kterou Eric Temple Bell popsal slovy:

Cole, beztak málomluvný člověk, přistoupil k tabuli, beze slov vzal křídu a spočítal 2^{67}. *Pak starostlivě odečetl* 1 *a jako výsledek získal číselné monstrum*

$$147\,573\,952\,589\,676\,412\,927.$$

Poté pořád beze slov vyhledal ještě volné místo na tabuli a ručně vynásobil krok za krokem

$$193\,707\,721 \cdot 761\,838\,257\,287.$$

Když oba výpočty souhlasily, dostalo se mu bouřlivých ovací. Cole se vrátil na své místo, stále bez jediného slova. Mersennova domněnka tak zmizela ve hlubinách matematických hrdinných ság.

Podle článku (Kraïtchik, 1952) Pierre de Fermat rozložil $2^p - 1$ na prvočísla pro $p = 11,\ 23,\ 37$. Tyto výsledky jej vedly k objevu Malé Fermatovy věty 2.13, která má ve speciálním případě tvar

$$2^{q-1} \equiv 1 \pmod{q} \tag{4.2}$$

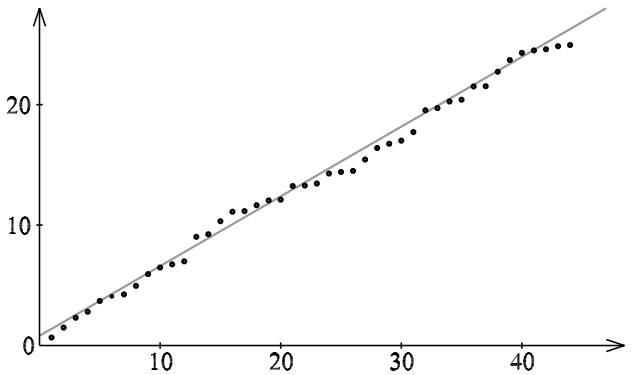
pro každé prvočíslo $q > 2$. Tato kongruence vyjadřuje, že prvočíslo q dělí (beze zbytku) rozdíl $2^{q-1} - 1$.

Věta 4.2 (Lucasův–Lehmerův test). *Nechť* $y_1 = 4$ *a* $y_{k+1} = y_k^2 - 2$ *pro* $k = 1, 2, \ldots$. *Pak pro* $p > 2$ *je Mersennovo číslo* $M_p = 2^p - 1$ *prvočíslem právě tehdy, když* M_p *dělí* y_{p-1}.

Důkaz je uveden např. v (Křížek, Luca, Somer, 2001, s. 214) nebo (Riesel, 1994, s. 126). Vidíme, že posloupnost y_i roste po-

měrně rychle: 4, 14, 194, 37 634, 1 416 317 954, ... Lucasův–Lehmerův test vlastně tvrdí, že M_p je prvočíslo pro $p > 2$ právě tehdy, když $y_{p-1} \equiv 0 \pmod{M_p}$.

Označme n-té Mersennovo prvočíslo symbolem $M(n)$, tj. $M(1) = 2^2 - 1 = 3$, $M(2) = 2^3 - 1 = 7$, $M(3) = 2^5 - 1 = 31$, $M(4) = 2^7 - 1 = 127, \ldots$. Na obrázku 4.2 je znázorněno velice pozoruhodné rozložení dosud objevených Mersennových prvočísel $M(n)$. Na základě tohoto rozložení S. S. Wagstaff předpověděl, viz (Wagstaff, 1983, s. 388), že očekávaný počet Mersennových prvočísel M_p s exponentem p mezi m a $2m$ je roven $\mathrm{e}^\gamma = 1.781\,072\,418\ldots$, kde $\mathrm{e} = \lim_{k\to\infty} \left(1 + \frac{1}{k}\right)^k = 2.718\,281\,828\ldots$ je *Eulerovo číslo* a $\gamma = \lim_{k\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} - \log k\right) = 0.577\,215\,665\ldots$ je *Eulerova konstanta*. Tento odhad podstatně usnadňuje hledání dalších Mersennových prvočísel.



Obr. 4.2. Hodnoty $\log_2(\log_2 M(n))$ pro $n = 1, 2, 3, \ldots$

Největší známá prvočísla. V roce 1996 vznikl síťový projekt GIMPS (Great Internet Mersenne Prime Search), v němž tisíce matematiků a počítačových odborníků z celého světa s podporou sítě internet hledají Mersennova prvočísla s velkým počtem cifer (viz [www5], [www6]). Nápad vytvořit bezplatný software, který

využívá Lucasův–Lehmerův test (viz věta 4.2), pochází od George Woltmana, který celý projekt založil. Příslušné programy, které lze stáhnout ze sítě, vytvořila firma Scotta Kurowského. Využívají tzv. rychlé násobení, srov. (Schönhage, Strassen, 1971), které podstatně šetří počet prováděných elementárních aritmetických operací.

V rámci projektu GIMPS již byla nalezeno několik vskutku obrovských Mersennových prvočísel. Například v roce 1998 devatenáctiletý student Roland Clarkson objevil na svém domácím počítači třicáté sedmé Mersennovo prvočíslo

$$M(37) = M_{3021377} = 2^{3021377} - 1,$$

které má více než devět set tisíc cifer. Další velké Mersennovo prvočíslo $2^{6972593} - 1$, které díky projektu GIMPS nalezl Nayan Hajratwala v roce 1999, má více než dva miliony cifer. Bylo to první známé prvočíslo, které má více než milion cifer. Nayan Hajratwala za tento vynikající výsledek dostal odměnu 50 000 amerických dolarů (USD). Pro prvního objevitele prvočísla, které bude mít více než 10 milionů (100 milionů, popř. miliardu) cifer, má společnost The Electronic Frontier Foundation připravenu odměnu 100 000 USD (150 000 USD, popř. 250 000 USD). Řešením problémů teorie čísel lze tak získat docela slušný finanční obnos. Do roku 2007 bylo zatím největší známé Mersennovo prvočíslo

$$M_{32582657} = 2^{32582657} - 1,$$

které má 9 808 358 cifer. Je to zároveň vůbec největší známé prvočíslo.[1)] Tabulka objevitelů Mersennových prvočísel společně s příslušným rokem objevu je uvedena například v (Ribenboim, 1996, s. 94) nebo na stránce [www6].

Úplný seznam prvočinitelů Mersennových čísel M_p pro prvočíselné exponenty $p \leq 257$ lze nalézt v (Riesel, 1994), viz též (Brillhart et al., 1988) pro větší p. Obecný tvar dělitelů Mersennových čísel je dán následující větou, jež byla známa již Fermatovi, viz (Dickson, 1919, s. 12), (Mahoney, 1994, s. 294).

[1)] V roce 2008 byla objevena další dvě prvočísla $M_{37156667}$ a $M_{43112609}$.

Věta 4.3. *Je-li $p > 2$ prvočíslo, pak každý prvočinitel čísla M_p má tvar $2kp + 1$.*

Důkaz. Nechť q je prvočinitel čísla $2^p - 1$. Pak $2^p \equiv 1 \pmod{q}$. Protože p je prvočíslo a $2^1 \not\equiv 1 \pmod{q}$, vidíme, že p je nejmenší exponent, pro který $2^p \equiv 1 \pmod{q}$. Podle speciálního případu Malé Fermatovy věty (4.2) je $2^{q-1} \equiv 1 \pmod{q}$. Tedy p dělí $q - 1$, tj. existuje j tak, že $jp = q - 1$. Protože p je liché a $q - 1$ je sudé, platí $j = 2k$ pro nějaké přirozené číslo k. □

Věta 4.4. *Jestliže n dělí M_p pro nějaké prvočíslo $p > 2$, pak $n \equiv \pm 1 \pmod{8}$.*

Důkaz viz (Ribenboim, 1991, s. 66).

Hledání sudých dokonalých čísel. Mezi Mersennovými prvočísly a tzv. dokonalými čísly existuje překvapivá souvislost. Přirozené číslo n se nazývá *dokonalé*, jestliže se rovná součtu všech svých dělitelů menších než n. Například 6 a 28 jsou dokonalá čísla, protože

$$6 = 1 + 2 + 3 \quad \text{a} \quad 28 = 1 + 2 + 4 + 7 + 14.$$

Podrobný přehled dalších dokonalých čísel a jejich objevitelů je uveden v (Bezuszka, Kenney, 1997).

Nechť n je libovolné přirozené číslo. Označme $\sigma(n)$ součet všech jeho kladných dělitelů, tj.

$$\sigma(n) = \sum_{d|n} d.$$

Například $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$. Další hodnoty σ pro $n \leq 32$ uvádíme v tabulce 7 na str 343. Pomocí funkce σ můžeme vyslovit ekvivalentní definici: n je *dokonalé*, jestliže

$$\sigma(n) = 2n.$$

Navíc platí

$$\sigma(mn) = \sigma(m)\,\sigma(n),$$

jsou-li m a n nesoudělná přirozená čísla.

Nutná a postačující podmínka pro to, aby sudé číslo n bylo dokonalé, je, že má tvar $n = 2^{p-1}(2^p - 1)$ pro přirozené číslo $p > 1$ takové, že $2^p - 1$ je prvočíslo (tj. p musí být podle věty 4.1 také prvočíslem). Eukleides (4.–3. stol. př. n. l.) věděl, že tato podmínka je postačující, ale nevěděl, zda je též nutná. Odpověď byla nalezena až o dvě tisíciletí později Eulerem, který dokázal její nutnost.

Věta 4.5 (Eukleidova). *Je-li $2^p - 1$ prvočíslo, pak je číslo $n = 2^{p-1}(2^p - 1)$ dokonalé.*

D ů k a z. Protože jsou čísla 2^{p-1} a $2^p - 1$ nesoudělná, platí

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p-1) = \frac{2^p - 1}{2 - 1}(1+2^p-1) = (2^p-1)2^p = 2n,$$

a tedy n je dokonalé. □

Věta 4.6 (Eulerova). *Všechna sudá dokonalá čísla mají tvar*

$$n = 2^{p-1}(2^p - 1),$$

kde $p > 1$ a $2^p - 1$ je prvočíslo.

D ů k a z. Jestliže n je sudé, můžeme psát $n = 2^{p-1}u$, kde $p > 1$ a u je liché. Protože 2^{p-1} a u jsou nesoudělná, součet dělitelů čísla n se rovná

$$\sigma(n) = \sigma(2^{p-1})\sigma(u) = (2^p - 1)\sigma(u).$$

Je-li n dokonalé, máme

$$\sigma(n) = 2n = 2^p u,$$

a tedy

$$(2^p - 1)\sigma(u) = 2^p u.$$

Jelikož $2^p - 1$ a 2^p jsou nesoudělná, vidíme, že $\sigma(u) = 2^p t$ a $u = (2^p - 1)t$, kde t je přirozené číslo. Protože však u má alespoň tyto dělitele: 1, t, $2^p - 1$ a $t(2^p - 1)$ pro $t > 1$, součet dělitelů u splňuje nerovnost

$$\sigma(u) \geq 1 + t + 2^p - 1 + t(2^p - 1) = 2^p(1 + t),$$

která odporuje rovnosti $\sigma(u) = 2^p t$. Tudíž $t = 1$. Pak ale $\sigma(u) \geq 1 + 2^p - 1 = 2^p$ a požadovaná rovnost $n = 2^{p-1}(2^p - 1)$ platí jen, když $u = 2^p - 1$ je prvočíslo. □

Položíme-li $q = 2^p - 1$ a $m = p - 1$, můžeme Eukleidovu a Eulerovu větu dohromady formulovat takto:

Číslo $q = 1 + 2 + 2^2 + \cdots + 2^m$ je prvočíslo právě tehdy, když je $2^m q$ dokonalé.

Z vět 4.5 a 4.6 také dostáváme další zajímavou souvislost mezi sudými dokonalými čísly n a Mersennovými prvočísly M_p,

$$n = 2^{p-1}(2^p - 1) = \frac{2^p}{2}(2^p - 1) = 1 + 2 + \cdots + (2^p - 1) = \sum_{i=1}^{M_p} i.$$

Věta 4.7. *Sečtěme cifry libovolného sudého dokonalého čísla kromě 6. Pak sečtěme cifry tohoto součtu a opakujme celý proces tak dlouho, až dostaneme jedinou cifru. Potom je výsledná cifra jednička.*

Důkaz. Nejprve ukážeme, že pro sudé dokonalé číslo $n > 6$ platí kongruence $n \equiv 1 \pmod 9$. Nechť p je liché prvočíslo. Protože $2 \equiv -1 \pmod 3$ a číslo $p - 1$ je sudé, podle (1.4) máme $2^{p-1} \equiv 1 \pmod 3$, tj.

$$2^{p-1} = 3k + 1$$

pro nějaké přirozené číslo k. Podle Eulerovy věty 4.6 proto platí,

$$n = 2^{p-1}(2^p - 1) = (3k+1)\big(2(3k+1)-1\big) = (3k+1)(6k+1)$$
$$= 18k^2 + 9k + 1 \equiv 1 \pmod 9.$$

Číslo n můžeme zapsat ve tvaru

$$n = c_k 10^k + c_{k-1} 10^{k-1} + \cdots + 10c_1 + c_0,$$

kde cifra $c_k \neq 0$. Protože $10 \equiv 1 \pmod 9$, podle (1.4) platí

$$10^j \equiv 1^j = 1 \pmod 9$$

pro libovolné $j \geq 0$. Tedy pro součet všech cifer dostaneme

$$n \equiv c_k + \cdots c_1 + c_0 \equiv 1 \pmod 9.$$

Nyní budeme opakovat tento postup tak dlouho, až dostaneme jedinou cifru, která bude zřejmě rovna 1. □

Následující větu lze nalézt v (Kraïtchik, 1952).

Věta 4.8 (Heathova). *Každé sudé dokonalé číslo* $2^{p-1}(2^p-1)$ *pro* $p>2$ *je součtem třetích mocnin* $2^{(p-1)/2}$ *lichých čísel.*

D ů k a z. Nejprve si povšimněme, že podle vět 4.1 a 4.7 je p prvočíslem. Nechť $p>2$. Položme $k=(p-1)/2$, $m=2^k$ a $s=1^3+3^3+5^3+\cdots+(2m-1)^3$. Pak pomocí matematické indukce dostaneme

$$\begin{aligned} s &= \sum_{k=1}^{m}(2k-1)^3 = \sum_{k=1}^{m}(8k^3-12k^2+6k-1) \\ &= 8\frac{m^2(m+1)^2}{4} - 12\frac{m(m+1)(2m+1)}{6} + 6\frac{m(m+1)}{2} - m \\ &= m^2(2m^2-1). \end{aligned}$$

Zde jsme mj. použili vztah

$$1^3+2^3+\cdots+m^3 = (1+2+\cdots+m)^2 = \frac{1}{4}m^2(m+1)^2,$$

který pochází od řeckého učence Nikomacha z jeho stěžejního díla *Úvod do aritmetiky.* Nyní vidíme, že $s=2^{2k}(2^{2k+1}-1)=2^{p-1}(2^p-1)$. □

K dokonalým číslům se ještě vrátíme v oddíle 7.3.

Otevřené problémy. Existuje celá řada nezodpovězených otázek týkajících se Mersennových čísel M_p. Například jedna z domněnek říká, že je nekonečně mnoho Mersennových prvočísel, a tedy také nekonečně mnoho sudých dokonalých čísel. Dosud ale nevíme, zda vůbec existuje nějaké liché dokonalé číslo. Ví se ale, že pokud by existovalo, pak by bylo větší než 10^{300} a mělo alespoň devět různých prvočinitelů, z nichž jeden je alespoň 10^7, viz (Jenkins, 2003), (Nielsen, 2007).

Také není známo, zda posloupnost $m_{k+1}=2^{m_k}-1$ začínající $m_1=2$ obsahuje jen prvočísla. Prvních pět členů $m_1=2$, $m_2=$

$2^2 - 1 = 3$, $m_3 = 2^3 - 1 = 7$, $m_4 = 2^7 - 1 = 127$ a

$m_5 = 2^{127} - 1 = 170141183460469231731687303715884105727$

jsou skutečně prvočísla M_1, M_2, M_3, M_7 a M_{127}. Charakter m_6 zatím není znám. Kdyby však m_k bylo složené pro nějaké k, pak podle (4.1) by m_{k+1} bylo také složené. Nevíme rovněž, zda existuje nekonečně mnoho složených Mersennových čísel.

Na závěr poznamenejme, že Mersennova čísla se používají při zpracování digitálních signálů – (Crandall, Fagin, 1994), (Dimitrov, Cooklev, Donevsky, 1994), (Elliott, Rao, 1982, s. 425), (Gorshkov, 1994b). Více informací o Marinu Mersennovi a jeho prvočíslech lze najít např. v (Dickson,1919), (Ribenboim, 1996).

4.2. Fermatova prvočísla

Fermatova čísla. Od narození dalšího velkého francouzského matematika Pierra de Fermata uplynulo již více než 400 let – viz (Křížek, Luca, Somer, 2001), (Šolcová, 2001), (Šolcová, Křížek, Mink, 2002). Jedno z jeho mylných tvrzení doslova způsobilo revoluci v teorii čísel i geometrii. Fermat se totiž domníval, že všechna čísla tvaru

$$F_m = 2^{2^m} + 1 \quad \text{pro } m = 0,\ 1,\ 2,\ldots \tag{4.3}$$

jsou prvočísla. Prvních pět členů této posloupnosti

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537 \tag{4.4}$$

prvočísly skutečně jsou. V roce 1732 však Leonhard Euler, viz (Euler, 1738, s. 104), zjistil, že

$$F_5 = 641 \cdot 6700417,$$

a tak vyvrátil Fermatovu domněnku (obr. 4.3). Tak vznikla přirozená otázka, zda existuje nekonečně mnoho prvočísel tvaru (4.3).

Čísla F_m se nazývají *Fermatova čísla.* Je-li F_m prvočíslo, řekneme, že je *Fermatovým prvočíslem*.

Uveďme nejprve nutnou podmínku k tomu, aby pro $n \in \mathbb{N}$ bylo číslo 2^n+1 prvočíslem. Tato podmínka nám napovídá, proč Fermat zvolil exponent v (4.3) v exponenciálním tvaru.

Věta 4.9. *Nechť n je přirozené číslo. Je-li $2^n + 1$ prvočíslo, pak $n = 2^m$ pro nějaké $m \in \{0,\ 1,\ 2, \dots\}$.*

D ů k a z. Jestliže k je přirozené číslo a $\ell \geq 3$ liché, pak

$$2^{k\ell} + 1 = \big(2^k + 1\big)\big(2^{k(\ell-1)} - 2^{k(\ell-2)} + \cdots - 2^k + 1\big). \quad (4.5)$$

Odtud plyne, že číslo $2^n + 1$ je složené, je-li exponent n dělitelný lichým přirozeným číslem $\ell \geq 3$. To ale v posloupnosti (4.3) nenastává. Proto n musí být mocninou dvojky. □

Poznamenejme ještě, že pro $n = 4r + 2$ platí *Lucasova formule,* viz (Kraïtchik, 1952)

$$2^n + 1 = \big(2^{2r+1} - 2^{r+1} + 1\big)\big(2^{2r+1} + 2^{r+1} + 1\big).$$

Z (4.3) vyplývá následující rekurentní vztah

$$F_{m+1} = (F_m - 1)^2 + 1, \quad (4.6)$$

a proto

$$F_{m+1} - 2 = F_m(F_m - 2).$$

Odtud indukcí dostáváme zajímavou vlastnost

$$F_{m+1} - 2 = F_m F_{m-1} \cdots F_1 F_0,$$

ze které vyplývá, že $F_{m+1} - 2$ je dělitelné všemi menšími Fermatovými čísly. Tedy

$$F_k \mid (F_m - 2) \quad \text{pro všechna } k = 0, 1, \dots, m-1. \quad (4.7)$$

Konstrukce pravidelných mnohoúhelníků. Do roku 1796 byla Fermatova čísla spíše matematickou kuriozitou. Zájem o ně vzrostl, když Carl Friedrich Gauss objevil až neuvěřitelnou souvislost mezi Fermatovými prvočísly a eukleidovskou konstrukcí (tj. pomocí kružítka a pravítka) pravidelných mnohoúhelníků. Gauss ve svých necelých devatenácti letech zcela nečekaně nalezl eukleidovskou

Eukleides (4.–3. stol. př. n. l.):
Pravidelný n-úhelník lze zkonstruovat pomocí pravítka a kružítka, jestliže

$$n = 2^i 3^j 5^k,$$

kde $n \geq 3$ *a* $i \geq 0$ *jsou celá čísla a* $j, k \in \{0, 1\}$.

Pierre de Fermat (1601–1665):
Pro $m = 0, 1, 2, \ldots$ *je posloupnost*

$$F_m = 2^{2^m} + 1$$

tvořena prvočísly.
(Nepravdivé tvrzení.)

Leonhard Euler (1707–1783):

$$F_5 = 641 \cdot 6700417.$$

Carl Friedrich Gauss (1777–1855):
Pravidelný n-úhelník lze zkonstruovat pomocí pravítka a kružítka právě tehdy, když

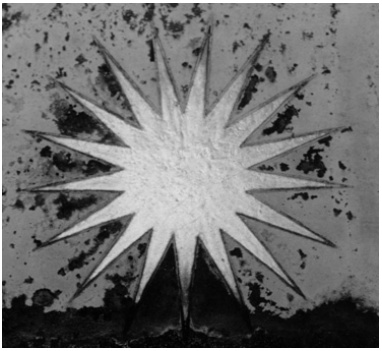
$$n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j},$$

kde $n \geq 3$, $i \geq 0$, $j \geq 0$ *a* $F_{m_1}, \ldots, F_{m_j}$ *jsou vzájemně různá Fermatova prvočísla.*

Obr. 4.3. Historické milníky eukleidovské konstrukce pravidelných mnohoúhelníků.

konstrukci pravidelného sedmnáctiúhelníku. Na počest tohoto zásadního objevu je na podstavci Gaussovy sochy (viz obrázky 4.4 a 5.4) v jeho rodném Braunschweigu znázorněna pravidelná sedmnácticípá hvězda (nikoli na jeho hrobce v Göttingen, jak si Gauss původně přál). Hvězda byla zvolena proto, že pravidelný sedmnáctiúhelník vypadá téměř jako kružnice. Konstrukci sedmnáctiúhelníku a dalších pravidelných mnohoúhelníků se budeme podrobně věnovat v oddíle 5.6.

Zanedlouho Gauss formuloval nutnou a postačující podmínku (obr. 4.3) udávající, kdy je pravidelný mnohoúhelník eukleidovsky konstruovatelný. Její původní důkaz, který má více než 50 stránek, viz (Gauss, 1986, Sect. VII), ale není zcela úplný. Nutnost Gaussovy podmínky byla dokázána později v roce 1837 P. L. Wantzelem, viz (Wantzel, 1837) a též (Pierpont, 1895/96).



Obr. 4.4. Zlatá sedmnácticípá hvězda na podstavci Gaussovy sochy v německém Braunschweigu.

Věta 4.10 (Gaussova). *Pravidelný n-úhelník lze eukleidovsky konstruovat právě tehdy, když počet jeho vrcholů je roven*

$$n = 2^i \, p_1 \, p_2 \, \cdots \, p_j,$$

kde $i \geq 0$, $j \geq 0$, $n \geq 3$ *jsou celá čísla a* $p_1, p_2, \ldots, p_j$ *jsou navzájem různá Fermatova prvočísla.*

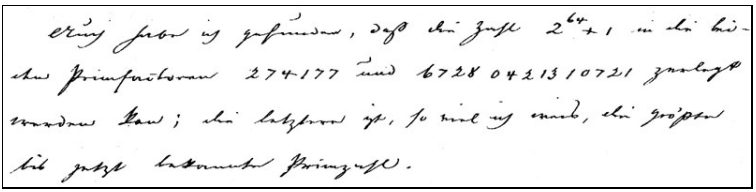
Důkaz této věty založený na Galoisově teorii je podán například v (Křížek, Luca, Somer, 2001, kap. 16).

Pravidelný n-úhelník s lichým počtem vrcholů lze tedy zkonstruovat pro

$$n = 3,\ 5,\ 15,\ 17,\ 51,\ 85,\ 255,\ 257, \ldots, \tag{4.8}$$

kde $15 = 3 \cdot 5$, $51 = 3 \cdot 17$, $85 = 5 \cdot 17$, $255 = 3 \cdot 5 \cdot 17, \ldots$, jsou součiny Fermatových prvočísel. Podobně například volba $i = 2$, $j = 2$, $p_1 = 3$ a $p_2 = 5$ v Gaussově větě dává možnost zkonstruovat pravidelný šedesátiúhelník pomocí kružítka a pravítka.

Vyšetřování prvočíselnosti Fermatových čísel se vzhledem ke Gaussově větě stalo poměrně důležitým úkolem. Německý astronom Thomas Clausen 1. ledna 1855 píše Gaussovi, viz (Biermann, 1964, s. 185), že číslo F_6 je složené. Na obr. 4.5 je kopie části jeho dopisu, který je uložen v knihovně univerzity v Göttingen. Stejný výsledek publikoval nezávisle Fortuné Landry až v roce 1880. Když mu bylo 82 let, podařilo se mu rozložit dvaceticiferné číslo F_6 na dva prvočinitele, viz (Landry, 1880).



Obr. 4.5. Část dopisu T. Clausena, ve kterém Gaussovi oznamuje, že se mu podařilo najít rozklad čísla F_6: *„Auch habe ich gefunden, daß die Zahl $2^{64}+1$ in die beiden Primfactoren 274177 und 67280421310721 zerlegt werden kann; die letztere ist, so viel ich weiß, die größte bis jetzt bekannte Primzahl.“*

Díky moderním matematickým metodám a výkonné výpočetní technice dnes již víme, že

$$F_m \text{ je složené pro } 5 \leq m \leq 32,$$

i když pro F_{14}, F_{20}, F_{22} a F_{24} zatím neznáme žádného netriviálního dělitele. Číslo F_{24} má přes 5 milionů cifer. Důkaz toho, že je to číslo složené, si vyžádal provedení 10^{17} aritmetických operací, viz (Crandall, Mayer, Papadopoulos, 2003). Byl to zatím nejrozsáhlejší výpočet, jehož výsledkem byla jednobitová informace typu ANO/NE. Do roku 2007 nebylo známo, zda F_{33} je číslo složené či prvočíslo. Zatím tedy ani nevíme, zda je současný seznam eukleidovsky konstruovatelných pravidelných mnohoúhelníků již úplný.

Přestože je dnes známo přes dvě stě prvočinitelů různých Fermatových čísel, stále se nedaří mezi nimi vysledovat takovou zákonitost, která by vedla k definitivní odpovědi na otázku, zda je F_4

největší Fermatovo prvočíslo. Otevřeným problémem také stále zůstává, zda je Fermatových prvočísel konečně či nekonečně mnoho.

Pro testování prvočíselnosti Fermatových čísel se nejčastěji používá následující věta – viz (Pépin, 1877), (Šolcová, Křížek, 2006a), která je speciálním případem Prothovy věty 3.2.

Věta 4.11 (Pépinův test). *Pro $m \geq 1$ je Fermatovo číslo F_m prvočíslem právě tehdy, když*

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}. \tag{4.9}$$

Francouzský matematik Jean François Théofile Pépin (1826–1904) dokázal tuto větu v roce 1877, kde místo základu 3 stojí 5. Určitě by jej potěšilo, kolik matematiků použilo a stále používá jeho test po více než jednom století. Poznamenejme ještě, že J. F. T. Pépin vstoupil do jezuitského řádu v roce 1846. Proto jsou jeho články publikovány pod jménem *le P. Pépin, S. J.,* což znamená: Pater Pépin, Societatis Jesu.

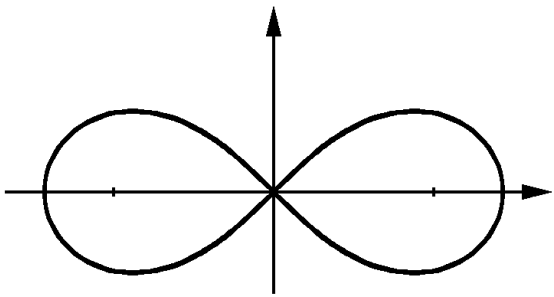
O dalších souvislostech Fermatových čísel s geometrií. C. F. Gauss rovněž objevil způsob, jak rozdělit lemniskátu na pět stejně dlouhých částí, viz (Rosen, 1981). V následující větě ukážeme, jak tento Gaussův výsledek zobecnil Niels Henrik Abel (1802–1829). Tento významný norský matematik mj. také dokázal, že neexistuje obecné řešení algebraické rovnice pátého stupně a zobecnil binomickou větu pro libovolný reálný exponent. Na jeho počest byla zřízena Abelova cena za matematiku (obdoba Nobelovy ceny za fyziku), která je spojena s částkou 6 000 000 norských korun. Cenu uděluje Norská Akademie věd (podrobnosti viz (Křížek, 2004)) podobně jako Nobelovu cenu za mír.

Věta 4.12 (Abelova). *Lemniskáta může být rozdělena na n stejně dlouhých částí pomocí pravítka a kružítka, když*

$$n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j},$$

kde $i \geq 0$ a $j \geq 0$ jsou celá čísla a F_{m_1}, $F_{m_2}, \ldots$, F_{m_j} jsou vzájemně různá Fermatova prvočísla.

Podrobný důkaz tohoto tvrzení je uveden v (Rosen, 1981). Připomeňme, že (Bernoulliova) lemniskáta je uzavřená křivka, jejíž body mají od dvou pevných bodů $(\pm(a/2)\sqrt{2}, 0)$ konstantní součin vzdáleností rovný $a^2/2$, kde $a > 0$ je reálný parametr ($a = \sqrt{2}$ na obr. 4.6). Lemniskáta je také průnikem povrchu toroidu s rovinou tečnou k jeho otvoru a rovnoběžnou s jeho rotační osou. Je pojmenována po švýcarském matematikovi Jacobu Bernoullim (1654–1705).



Obr. 4.6. Lemniskáta $(x^2 + y^2)^2 = a^2(x^2 - y^2)$.

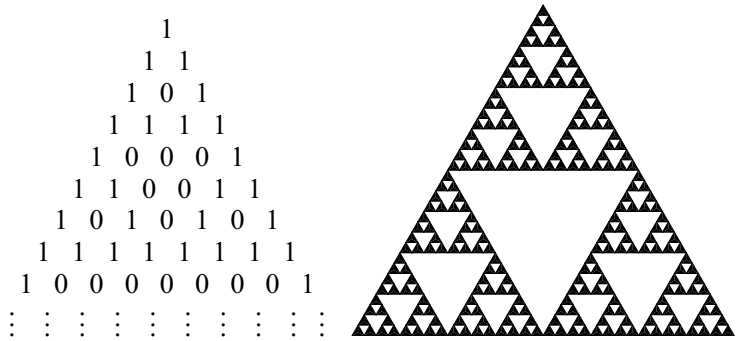
Ukažme si další pozoruhodný vztah mezi teorií čísel a konstrukcí pravidelných mnohoúhelníků. Připomeňme, že Pascalův trojúhelník je trojúhelník sestavený z binomických koeficientů. Uvažujme jej modulo 2, tj. sudá čísla v Pascalově trojúhelníku nahradíme nulou a lichá jedničkou (obr. 4.7).

Každý řádek tak představuje číslo zapsané ve dvojkové soustavě. Převedeme-li nyní tato čísla do desítkové soustavy, dostaneme posloupnost

$$1, 3, 5, 15, 17, 51, 85, 255, 257, \ldots, \qquad (4.10)$$

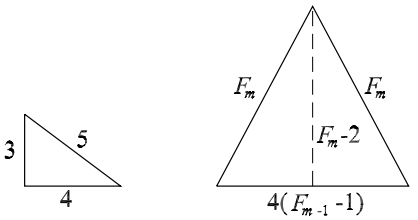
která je rostoucí, protože každý řádek v trojúhelníku z obr. 4.7 začíná 1 a je o jednu dvojkovou cifru delší než předchozí řádek. Porovnejme nyní posloupnosti (4.8) a (4.10). Není to malý zázrak? Důkaz této zajímavé shody je uveden v (van der Waall, 1976), viz též (Křížek, Luca, Somer, 2001, s. 80). Navíc si povšimněte,

že Pascalův trojúhelník modulo 2 má podobnou strukturu jako známá Sierpińského fraktální množina (obr. 4.7). Jedničky odpovídají černě obarveným trojúhelníkům a nuly trojúhelníkům bílým.



Obr. 4.7. Pascalův trojúhelník modulo 2 a Sierpińského fraktální množina.

I Heronův trojúhelník úzce souvisí s Fermatovými prvočísly. Připomeňme, že trojúhelník, jehož délky stran i obsah jsou celočíselné, se nazývá *Heronův trojúhelník.* Následující tvrzení (srov. obr. 4.8) je dokázáno v (Luca, 2002).



Obr. 4.8. Jediné možné Heronovy trojúhelníky, jejichž délky stran jsou mocniny prvočísel.

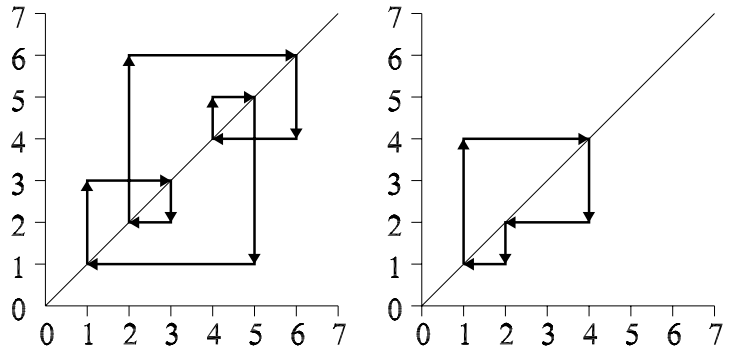
Věta 4.13 (Lucova). *Nechť délky stran Heronova trojúhelníku jsou mocniny prvočísel. Potom jsou jsou tyto délky stran buď rovny pythagorejské trojici* $\langle 3, 4, 5\rangle$*, nebo* $\langle F_m, F_m, 4(F_{m-1}-1)\rangle$ *pro nějaké* $m \geq 1$*, pro něž je* F_m *prvočíslo.*

Prvočíselnost F_m má i další překrásnou geometrickou interpretaci, kterou v roce 2000 objevili R. Jones a J. Pearce. Nejprve si ale popíšeme algoritmus, jak lze graficky zobrazovat zlomky tvaru $\frac{1}{n}$.

Nechť $b > 1$ a n jsou celá čísla. Jestliže r_i je zbytek v i-tém kroku při výpočtu zlomku $\frac{1}{n}$ vzhledem k základu b číselné soustavy, pak zbytek v následujícím kroku $i + 1$ splňuje kongruenci

$$r_{i+1} \equiv br_i \pmod{n}.$$

Začneme-li s $r_0 = 1$, dostaneme posloupnost zbytků $r_0, r_1, r_2, \ldots$ pro $\frac{1}{n}$ odpovídajících základu b. Tuto skutečnost můžeme v rovině graficky znázornit takto (obr. 4.9): z bodu (r_0, r_0) veďme úsečku nejprve vertikálně a pak horizontálně do bodu (r_1, r_1). Odtud opět vedeme úsečku nejprve vertikálně a pak horizontálně do bodu (r_2, r_2) atd. Pokud v i-tém kroku dostaneme nulový zbytek, algoritmus ukončíme. Posloupnost zbytků tak jednoznačně určuje výsledný graf.

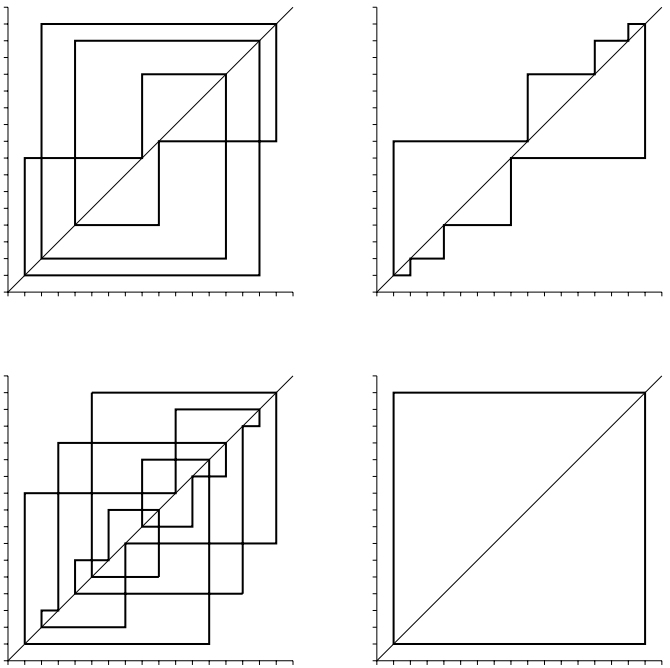


$b = 10$ $b = 11$

Obr. 4.9. Grafické znázornění zlomku $\frac{1}{7}$ pro dva různé základy.

Uvažujme například zlomek $\frac{1}{7}$, který má v desítkové soustavě (tj. pro $b = 10$) rozvoj $0.\overline{142857}$. Odpovídající posloupnost zbytků je periodická,

$$\begin{aligned} r_0 &= 1, \\ r_1 &= 3 \equiv 10 \pmod 7, \\ r_2 &= 2 \equiv 30 \pmod 7, \\ r_3 &= 6 \equiv 20 \pmod 7, \\ r_4 &= 4 \equiv 60 \pmod 7, \\ r_5 &= 5 \equiv 40 \pmod 7, \\ r_0 = r_6 &= 1 \equiv 50 \pmod 7 \end{aligned}$$



Obr. 4.10. Grafy odpovídající zlomku $\frac{1}{17}$ při základech $b = 8,\ 9,\ 10$ a 16.

atd. Z obr. 4.9 je patrné, že příslušný graf je středově symetrický vzhledem k bodu $\left(\frac{7}{2}, \frac{7}{2}\right)$ při základu $b = 10$. Je ale nesymetrický při základu $b = 11$, neboť

$$\begin{aligned} r_0 &= 1, \\ r_1 &= 4 \equiv 11 \pmod 7, \\ r_2 &= 2 \equiv 44 \pmod 7, \\ r_0 = r_3 &= 1 \equiv 22 \pmod 7. \end{aligned}$$

Přirozené číslo $n > 1$ nazveme *perfektně symetrické,* jestliže graf odpovídající zlomku $\frac{1}{n}$ je středově symetrický vzhledem k bodu $\left(\frac{n}{2}, \frac{n}{2}\right)$ pro každý základ b, pro který $b \not\equiv 0 \pmod n$ a $b \not\equiv 1 \pmod n$. V roce 2000 Jones a Pearce dokázali následující nutnou a postačující podmínku, viz (Jones, Pearce, 2000).

Věta 4.14. *Přirozené číslo $n > 1$ je perfektně symetrické právě tehdy, když n je Fermatovo prvočíslo nebo $n = 2$.*

Na obrázku 4.10 jsou znázorněny grafy odpovídající zlomku $\frac{1}{F_2}$ pro několik různých základů.

Souvislost Fermatových prvočísel s teorií grafů. Nechť

$$H = \{0, 1, \ldots, n-1\},$$

kde $n > 1$. Předpokládejme, že f je zobrazení z množiny H do sebe. Začneme-li od libovolného prvku x_0 z H, můžeme definovat posloupnost prvků z H pomocí vztahu

$$x_{i+1} = f(x_i), \quad i = 0, 1, \ldots .$$

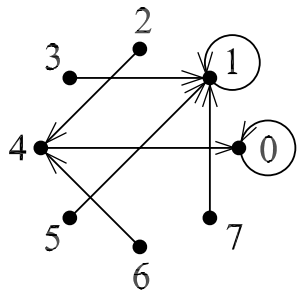
Protože H je konečná množina, posloupnost (x_i) je od jistého

indexu počínaje periodická. Pokud $x_k, x_{k+1}, \ldots, x_t$ jsou různé a

$$\begin{aligned} x_{k+1} &= f(x_k), \\ &\vdots \\ x_t &= f(x_{t-1}), \\ x_k &= f(x_t), \end{aligned}$$

pak prvky $x_k, x_{k+1}, \ldots, x_t$ tvoří *cyklus*. Cyklus délky 1 nazveme *pevný bod*.

Iterační graf zobrazení f je orientovaný graf, jehož vrcholy jsou prvky z H, a takový, že existuje orientovaná hrana z x do $f(x)$ pro všechna $x \in H$.



Obr. 4.11. Iterační graf funkce *f* definované vztahem (4.11) pro $n = 8$.

Iterační graf se nazývá *binární,* jestliže jeho symetrizace má právě dvě komponenty (tj. příslušný neorientovaný graf se skládá ze dvou souvislých podgrafů) a platí:

1. Vrchol 0 je izolovaný pevný bod.
2. Vrchol 1 je pevný bod a existuje orientovaná hrana z vrcholu $n - 1$ do 1.
3. Pro každý vrchol z množiny $\{1, 2, \ldots, n-1\}$ existují buď dvě orientované hrany, nebo žádná hrana směřující do tohoto vrcholu.

Dále budeme uvažovat speciální diskrétní iterace. Pro každé

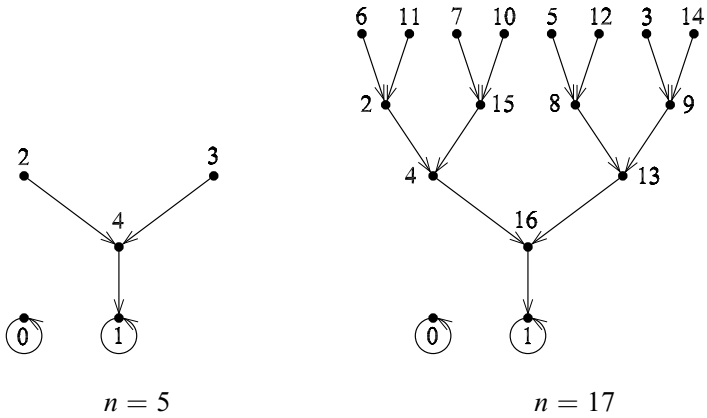
$x \in H$ nechť $f(x)$ je zbytek x^2 modulo n, tj.

$$f(x) \in H \quad \text{a} \quad f(x) \equiv x^2 \pmod{n}. \tag{4.11}$$

To odpovídá iteračnímu schématu $x_{i+1} \equiv x_i^2 \pmod{n}$.

V článku (Szalay, 1992) je dokázána následující věta (srov. s obrázky 4.11 a 4.12).

Věta 4.15 (Szalayova). *Iterační graf zobrazení f definovaný* (4.11) *je binární právě tehdy, když modul n je Fermatovo prvočíslo.*



Obr. 4.12. Binární grafy odpovídající Fermatovým prvočíslům.

Szalayova věta názorně ilustruje, proč jsou grafy z obr. 4.12 binární. Větší komponenta je binární strom, pokud odejmeme orientovanou uzavřenou hranu (smyčku) s počátkem i koncem ve vrcholu 1.

V článku (Křížek, Somer, 2001) je dokázáno, že mezi prvočísly pouze Fermatova prvočísla mají vlastnost, že množina primitivních kořenů je rovna právě množině kvadratických nereziduí modulo F_m (srov. větu 2.25).

Na obrázku 2.4 jsou vyznačeny všechny primitivní kořeny modulo 17. Nyní si povšimněme, že primitivní kořeny modulo n leží v „horní části“ každého grafu z obr. 4.12. Je-li F_m prvočíslem, pak

podle Pépinova testu (4.9) je číslo 3 vždy primitivním kořenem modulo F_m pro $m \geq 1$. Obrázek 4.12 tak krásně graficky znázorňuje Pépinův test. V tomto testu však může místo čísla 3 stát libovolný primitivní kořen modulo n. Následující věta je převzata z článku (Šolcová, Křížek, 2006a).

Věta 4.16. *Nechť b je libovolný primitivní kořen modulo Fermatovo prvočíslo F_m pro $m \geq 0$. Pak b^{2k-1} pro $k = 1, \ldots, (F_m - 1)/2$ jsou všechny vzájemně nekongruentní primitivní kořeny modulo F_m.*

D ů k a z. Snadno nahlédneme, že tvrzení platí pro $m \leq 1$.

Nechť tedy $m > 1$. Podle (Křížek, Somer, Luca, 2001, s. 42) může být báze 3 v Pépinově testu (4.9) nahrazena libovolným přirozeným číslem b takovým, že pro Jacobiho symbol platí $\left(\frac{b}{F_m}\right) = -1$ pro všechna $m > 1$. Jinými slovy, F_m je prvočíslem právě tehdy, když

$$b^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

Odtud dostaneme

$$\left(b^{2k-1}\right)^{(F_m-1)/2} = \left(b^{(F_m-1)/2}\right)^{2k-1} \equiv (-1)^{2k-1} = -1 \pmod{F_m},$$

tj. b^{2k-1} pro $k = 1, \ldots, (F_m - 1)/2$ jsou primitivní kořeny modulo F_m. Dále vidíme, že tyto kořeny nejsou vzájemně kongruentní, protože pro $1 \leq k < \ell \leq (F_m - 1)/2$ máme

$$\begin{aligned} b^{2k-1} - b^{2\ell-1} &= b^{2\ell-1}\left(b^{2(k-\ell)} - 1\right) \\ &= b^{2\ell-1}\left(b^{k-\ell} + 1\right)\left(b^{k-\ell} - 1\right) \not\equiv 0 \pmod{F_m}, \end{aligned}$$

kde poslední nekongruence plyne přímo z definice primitivního kořenu. □

V práci (Křížek, Somer, 2003b) je uvedeno několik dalších nutných a postačujících podmínek na prvočíselnost F_m. O souvislosti Fermatových prvočísel s pěti platónskými tělesy (pravidelnými mnohostěny – viz obr. II barevné přílohy) je pojednáno v článku (Křížek, Křížek, 1997). K Fermatovým číslům se ještě dostaneme

v následujících kapitolách. Nyní si řekneme ještě něco o jejich dělitelích.

Prvočíselní dělitelé Fermatových čísel. V roce 1878 francouzský matematik François Édouard Anatole Lucas (1842 až 1891) dokázal následující větu, která se stala mocným nástrojem pro hledání prvočinitelů Fermatových čísel, viz (Lucas, 1878).

Věta 4.17 (Lucasova). *Jestliže prvočíslo p dělí F_m pro $m > 1$, pak existuje přirozené číslo k tak, že*

$$p = k\,2^{m+2} + 1.$$

Její důkaz je uveden v (Křížek, Luca, Somer, 2001, s. 59). Užitečnost Lucasovy věty si ukažme na úloze, kterou se zbýval A. E. Western v roce 1903. Šlo o to zjistit, zda F_{18} je číslo složené. Počet jeho cifer je úctyhodný – téměř 80 000, protože

$$\log_{10}(2^{2^{18}} + 1) + 1 \approx \log_{10} 2^{2^{18}} + 1 = 2^{18} \log_{10} 2 + 1 \approx 78\,914.$$

Podle Lucasovy věty je třeba najít přirozené číslo k tak, aby $k\,2^{20} + 1$ dělilo F_{18} a aby $k\,2^{20} + 1$ bylo prvočíslem. Tímto způsobem Western poměrně snadno zjistil, že hledané číslo k je 13, protože pro menší hodnoty k (kromě případu $k = 7$) jsou čísla $k\,2^{20} + 1$ složená.

Jak ale můžeme ověřit, že $p = 13 \cdot 2^{20} + 1 = 13631489$ skutečně dělí obrovské Fermatovo číslo F_{18}? To lze snadno zjistit pomocí následujícího řetězce kongruencí:

$$\begin{aligned}
2^{2^5} &= 65536^2 \equiv 1048261 \pmod{p},\\
2^{2^6} &\equiv 1048261^2 \equiv 3164342 \pmod{p},\\
2^{2^7} &\equiv 3164342^2 \equiv 9153547 \pmod{p},\\
&\vdots \qquad\qquad \vdots\\
2^{2^{17}} &\equiv 1598622^2 \equiv 1635631 \pmod{p},\\
2^{2^{18}} &\equiv 1635631^2 \equiv 13631488 \pmod{p},
\end{aligned}$$

kde na pravých stranách stojí zbytky při dělení prvočíslem p. Tudíž

$$2^{2^{18}} + 1 \equiv 0 \pmod{13631489}.$$

V roce 1828 anonymní pisatel vyslovil hypotézu, viz (Dickson, 1919, s. 376), že všechna čísla tvaru

$$2 + 1, \quad 2^2 + 1, \quad 2^{2^2} + 1, \quad 2^{2^{2^2}} + 1, \ldots$$

jsou prvočísla. V roce 1953 J. Selfridge na počítači ukázal, že $(3150 \cdot 2^{18} + 1) \mid F_{16}$, čímž tuto starou hypotézu vyvrátil. Existuje ale množství dalších otevřených domněnek týkajících se prvočísel F_m, viz (Křížek, Luca, Somer, 2001).

4.3. Wieferichova prvočísla

Jestliže $p^2 \mid F_m$, kde p je prvočíslo, pak můžeme říci mnohem více o tvaru p, než je v Lucasově větě 4.17. Následující věta je dokázána v (Ribenboim, 1979a, s. 88).

Věta 4.18. *Nechť $m \geq 2$ a $p^2 \mid F_m$, kde p je prvočíslo. Pak existuje k liché a $r \geq m + 2$ tak, že*

$$p = k2^r + 1 \quad a \quad \frac{k^{p-1} - 1}{p} \equiv 1 \pmod{p}.$$

Zatím ale nejsou známa žádná Fermatova čísla, která by byla dělitelná čtvercem prvočísla (více informací o této problematice je v (Křížek, Luca, Somer, 2001)). Následující věta se většinou používá k testování, zda F_m je dělitelné čtvercem prvočísla, viz (Ribenboim, 1979a).

Věta 4.19. *Jestliže prvočíslo p dělí F_m, pak*

$$p^2 \mid F_m \iff 2^{p-1} \equiv 1 \pmod{p^2} \quad (\textit{Wieferichova kongruence}). \tag{4.12}$$

D ů k a z. Platí-li $p^2 \mid F_m$, potom

$$2^{2^m} \equiv -1 \pmod{p^2}.$$

Odtud podle (1.4) vidíme, že $2^{2^{m+2}} \equiv 1 \pmod{p^2}$, a tedy $2^{k2^{m+2}} \equiv 1 \pmod{p^2}$ pro každé $k \in \mathbb{N}$. Protože podle Lucasovy věty 4.17 $p = k2^{m+2} + 1$ pro nějaké k, dostaneme $2^{p-1} \equiv 1 \pmod{p^2}$.

Předpokládejme obráceně, že $2^{p-1} \equiv 1 \pmod{p^2}$. Z binomické věty lze snadno dokázat – viz (LeVeque, 1996), že když $a \geq 2$ je celé a t je největší celé číslo takové, že $\mathrm{ord}_{p^t}(a) = \mathrm{ord}_p(a)$, pak $\mathrm{ord}_{p^r}(a) = \mathrm{ord}_p(a)$ pro $r \in \{1, \ldots, t\}$ a $\mathrm{ord}_{p^t}(a) = p^{r-t}\mathrm{ord}_p(a)$ pro $r > t$. Protože $p \nmid (p-1)$, platí $\mathrm{ord}_{p^2}(2) = \mathrm{ord}_p(2)$. Odtud plyne, že $2^k \equiv 1 \pmod{p^2}$ právě tehdy, když $2^k \equiv 1 \pmod{p}$. Jelikož $p \mid F_m$, máme $2^{2^m} \equiv -1 \pmod{p}$. Tedy $2^{2^{m+1}} \equiv 1 \pmod{p}$, což implikuje, že $2^{2^{m+1}} \equiv 1 \pmod{p^2}$. Jinými slovy,

$$p^2 \mid \left(2^{2^{m+1}} - 1\right) = \left(2^{2^m} + 1\right)\left(2^{2^m} - 1\right).$$

Protože $p \mid F_m = 2^{2^m} + 1$ a $\left(2^{2^m} + 1\right) - \left(2^{2^m} - 1\right) = 2$, vidíme, že $p \nmid \left(2^{2^m} - 1\right)$. Tudíž $\left(p^2, 2^{2^m} - 1\right) = 1$, a proto $p^2 \mid \left(2^{2^m} + 1\right) = F_m$. □

Poznámka. Přestože bylo provedeno rozsáhlé počítačové hledání, viz (Crandall, Dilcher, Pomerance, 1997), až do hranice $4 \cdot 10^{12}$, zatím známe jen dvě prvočísla, která splňují Wieferichovu kongruenci na pravé straně ekvivalence (4.12),

$$p = 1093 \quad \text{a} \quad p = 3511.$$

Elementární důkaz toho, že tato čísla splňují Wieferichovu kongruenci, je uveden v (Guy, 1967) (viz též tabulka v (Montgomery, 1993) získaná na počítači). Prvočísla 1093 a 3511 se nazývají *Wieferichova prvočísla.* První z nich bylo objeveno W. Meissnerem v roce 1913 a druhé N. G. W. M. Beegerem v roce 1922, tedy mnohem dříve, než začala éra elektronických počítačů, viz (Ribenboim, 1996, s. 334). Tato dvě prvočísla však nedělí žádné Fermatovo číslo F_m, neboť žádné z nich nemá tvar $k2^{m+2} + 1$ pro $m > 1$, jak vyžaduje Lucasova věta 4.17.

Dříve než byla dokázána Velká Fermatova věta 2.10 – viz (Wiles, 1995) a (Taylor, Wiles, 1995), matematici vyšetřovali rovnici

$$x^p + y^p = z^p, \tag{4.13}$$

kde p je liché prvočíslo, $xyz \neq 0$ a $(x, y, z) = 1$. Velká Fermatova věta se tradičně dělí na dva případy. V *prvním případě Velké Fermatovy věty* se předpokládá, že $p \nmid xyz$. Ve druhém případě, který je mnohem těžší, se požaduje, aby $p \mid xyz$. V další větě ukážeme, že ekvivalence (4.12) vyjadřuje úzkou souvislost mezi prvním případem Velké Fermatovy věty a Fermatovými čísly.

Věta 4.20 (Wieferichova). *Jestliže první případ Velké Fermatovy věty neplatí pro lichý prvočíselný exponent p, pak p splňuje Wieferichovu kongruenci*

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Tato věta německého matematika Arthura J. A. Wiefericha (1884 až 1954) je obsažena v článku (Wieferich, 1909), viz též (Ribenboim, 1979b). Tvrdí, že pokud by rovnice (4.13) měla řešení pro nějaké liché prvočíslo $p \nmid xyz$, pak by platila Wieferichova kongruence. Protože ale Velká Fermatova věta již byla dokázána, má Wieferichova věta spíše jen historický význam. V monografiích (Křížek, Luca, Somer, 2001, s. 69) a (Ribenboim, 1996, s. 333–346) jsou uvedeny další zajímavé souvislosti mezi Fermatovými čísly a Wieferichovými prvočísly.

4.4. Elitní prvočísla

Co je elitní prvočíslo? Prvočíslo p se nazývá *elitní,* jestliže pouze konečný počet Fermatových čísel jsou kvadratické zbytky modulo p.

Jinými slovy prvočíslo p je elitní, jestliže existuje index k tak, že pro všechna $m > k$ kvadratická kongruence

$$x^2 \equiv F_m \pmod{p}$$

nemá řešení, tj. pro Jacobiho symbol platí, viz (Křížek, Luca,

Somer, 2001, s. 42)

$$\left(\frac{p}{F_m}\right) = -1 \quad \text{pro všechna } m > k.$$

Elitní prvočísla jsou tak úzce svázána s Fermatovými čísly, viz (Šolcová, Křížek, 2006b).

Příklad. Ukážeme, že čísla 3, 5 a 7 jsou elitní prvočísla. Ze vztahů (4.4) a (4.7) vidíme, že pro $m \geq 1$ je $F_m \equiv 2 \pmod 3$. Protože $F_m \equiv 1 \pmod 4$, podle zákona kvadratické reciprocity (viz věta 2.23) platí

$$\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Tato skutečnost je základem Pépinova testu.

Podle (4.7) je $F_m \equiv 2 \pmod 5$ pro $m \geq 2$, neboť $F_1 = 5$. Pak použitím zákona kvadratické reciprocity (viz věty 2.23 a 2.24) dostáváme

$$\left(\frac{5}{F_m}\right) = \left(\frac{F_m}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Jak již bylo řečeno, Pépin ve svém původním článku (Pépin, 1877) použil právě bázi 5 místo báze 3, která je ve vztahu (4.9). Podle (Aigner, 1986) lze báze 3 a 5 v Pépinově testu také zaměnit číslem 7. K tomu stačí ukázat, že Jacobiho symbol $\left(\frac{7}{F_m}\right)$ je roven -1 pro všechna m větší než nějaké k. Ukážeme, že $\left(\frac{7}{F_m}\right) = -1$ pro všechna $m \geq 1$. Protože

$$F_m = 16^{2^{m-2}} + 1 \equiv F_{m-2} \pmod 7,$$

platí (srov. např. (van Maanen, 1981/82, s. 349))

$$\begin{aligned} F_m &\equiv F_0 \equiv 3 \pmod 7 \quad \text{pro } m \text{ sudé} \\ \text{a} \quad F_m &\equiv F_1 \equiv 5 \pmod 7 \quad \text{pro } m \text{ liché.} \end{aligned}$$

Jelikož $F_m \equiv 1 \pmod 4$ pro $m \geq 1$, vidíme podle zákona kvadratické reciprocity pro Jacobiho symbol (viz vlastnost (VIII)

věty 2.24), že

$$\left(\frac{7}{F_m}\right) = \left(\frac{F_m}{7}\right) = \left(\frac{3}{7}\right) = -1 \quad \text{pro každé sudé } m \geq 2$$

a $\left(\frac{7}{F_m}\right) = \left(\frac{F_m}{7}\right) = \left(\frac{5}{7}\right) = -1 \quad$ pro každé liché $m \geq 1$.

Stručně ještě naznačíme, jak se ověří, že 41 je elitní prvočíslo. K tomu stačí ukázat, že $\left(\frac{41}{F_m}\right) = -1$ pro všechna F_m, pro něž $m \geq 2$. Nejprve se dokáže, že

$$\left(\frac{41}{F_{m+4}}\right) = \left(\frac{41}{F_m}\right) \quad \text{pro } m \geq 2.$$

Přímým výpočtem je pak nutné ještě prověřit, že $\left(\frac{41}{F_m}\right) = -1$ pro $2 \leq m \leq 5$.

Elitní prvočísla tedy mohou nahrazovat číslo 3 nebo 5 v klasickém Pépinově testu.

Díky rekurentnímu vztahu (4.6) lze dokázat, viz (Müller, 2006), že pro každé přirozené číslo p je posloupnost $\left(F_m \pmod p\right)_{m=0}^{\infty}$ periodická od jistého indexu k. V článku (Aigner, 1996) je dokázáno, že pro každé prvočíslo zapsané ve tvaru $p = 2^r h + 1$, kde $h \geq 1$ je liché a $r \in \mathbb{N}$, tato perioda začíná v F_r nebo dříve. Délku ℓ nazveme *Fermatovou periodou,* jestliže ℓ je nejmenší přirozené číslo splňující kongruenci

$$F_{r+\ell} \equiv F_r \pmod p.$$

Členy F_{r+s} pro $s = 0, \ldots, \ell - 1$ se nazývají *Fermatovy zbytky modulo p.*

Elitní prvočísla poprvé definoval a studoval rakouský matematik Alexander Aigner v článku (Aigner, 1986). Objevil jich 14 menších než 35 milionů. Později Tom Müller s použitím počítačů nalezl další dvě menší než jedna miliarda, viz (Müller, 2006). Prvních 16 elitních prvočísel je:

3, 5, 7, 41, 15 361, 23 041, 26 881, 61 441, 87 041, 163 841, 544 001, 604 801, 6 684 673, 14 172 161, 159 318 017, 446 960 641.

Müller objevil ještě dalších 26 elitních prvočísel větších než jedna miliarda. Z nich největší $2^{3888} \cdot 15 + 1$ má 1172 cifer. K tomu Müller použil následující větu.

Věta 4.21 (Müllerova). *Nechť $p = 2^r h + 1$ je prvočíslo, kde h je liché. Pak p je elitní právě tehdy, když multiplikativní řád každého Fermatova zbytku modulo p je násobkem 2^r.*

Alain Chaumont a Tom Müller (Chaumont, Müller, 2005) nalezli ještě dalších 5 elitních prvočísel menších než 250 miliard:

$$1\,151\,139\,841, \qquad 3\,208\,642\,561, \qquad 38\,126\,223\,361,$$
$$108\,905\,103\,361, \qquad 171\,727\,482\,881.$$

Otevřené problémy. Kolem elitních prvočísel existuje celá řada domněnek. Uveďme jen ty nejdůležitější.

Domněnka 1. Počet elitních prvočísel je nekonečný.

Nicméně v článku (Křížek, Luca, Somer, 2002) je dokázáno, že

$$\sum_{p \in \mathbb{E}} \frac{1}{p} \tag{4.14}$$

konverguje, kde $\mathbb{E}$ je množina elitních prvočísel. To jest množina $\mathbb{E}$ není dostatečně „hustá“, aby způsobila divergenci sumy (4.14), jako je tomu v případě všech prvočísel (viz věta 3.15). Označíme-li $E(x)$ počet elitních prvočísel menších nebo rovných x, pak platí

$$E(x) = \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big) \quad \text{pro } x \to \infty,$$

viz (Křížek, Luca, Somer, 2002). Zde $\mathcal{O}$ označuje *Landauův symbol,* který v tomto případě znamená, že existuje konstanta $C > 0$ tak, že $E(x) \leq C\frac{x}{(\log x)^2}$ pro $x \to \infty$. Tento horní odhad je ale pravděpodobně dosti hrubý. Müller (Müller, 2006) na základě numerických testů vyslovil další tři domněnky.

Domněnka 2.

$$E(x) = \mathcal{O}(\log x) \quad \text{pro } x \to \infty.$$

Domněnka 3. Počet elitních prvočísel tvaru $2^r \cdot 15 + 1$ je nekonečný.

Domněnka 4. Délka Fermatovy periody ℓ není ohraničená, tj. existují elitní prvočísla s libovolně velkou Fermatovou periodou.

4.5. Regulární a iregulární prvočísla

Regulární prvočísla, která si definujeme v dalším výkladu, zavedl německý matematik Ernst Eduard Kummer (1810–1893) při pokusu dokázat Velkou Fermatovu větu 2.10. Tato věta tvrdí, že rovnice

$$x^n + y^n = z^n \tag{4.15}$$

nemá řešení v přirozených číslech, když $n > 2$. Sám Fermat vlastní metodou nekonečného sestupu dokázal, že diofantská rovnice (4.15) nemá řešení pro $n = 4$ (viz věta 2.11).

Kolem roku 1850 Kummer učinil velký pokrok v úsilí dokázat Velkou Fermatovu větu v případě, že p je regulární prvočíslo. Pro definici regulárních prvočísel si nejprve uvedeme, jak jsou definována Bernoulliova čísla B_k. Ta vystupují v koeficientech mocninné řady funkce

$$\frac{x}{\mathrm{e}^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}, \tag{4.16}$$

přitom

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \ldots,$$

kde *Bernoulliova čísla* B_k jsou definována rekurentně vztahem

$$\binom{k+1}{k} B_k + \binom{k+1}{k-1} B_{k-1} + \cdots + \binom{k+1}{1} B_1 + B_0 = 0.$$

Jsou pojmenována po Jacobu Bernoullim. Snadno nahlédneme, že všechna B_k jsou racionální čísla. Lze také odvodit, že $B_{2k+1} = 0$ pro libovolné $k \in \mathbb{N}$.

Řekneme, že liché prvočíslo je *regulární,* jestliže nedělí žádného čitatele Bernoulliových čísel $B_0, B_2, B_4, \ldots, B_{p-3}$. Prvočíslo, které není regulární, se nazývá *iregulární.*

Například prvočísla

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 41,\ \ldots$$

jsou regulární, zatímco prvočísla

$$37,\ 59,\ 67,\ 101,\ 103,\ 131,\ 149,\ldots$$

jsou iregulární.

Jestliže p je iregulární, jeho *index iregularity* je roven počtu přirozených čísel k takových, že p dělí čitatele B_{2k} pro $2 \leq 2k \leq p-3$. Největší do roku 2007 známý index iregularity je 7. Tento index má například iregulární prvočíslo 3 238 481. Přesto se všeobecně věří, že index iregularity může být libovolně velký.

Pomocí poněkud heuristických argumentů se odvodilo, že poměr počtu všech regulárních prvočísel menších než n ku počtu všech prvočísel menších než n konverguje k $e^{-1/2} \approx 0.60653$. Pro podporu této domněnky hovoří skutečnost odvozená v článku (Buhler, Crandall, Ernvall, Metsänkylä, 1993). Tvrdí se zde, že z 283 145 prvočísel menších než $4 \cdot 10^6$ je jich 171 548 regulárních (tedy 60.587 %). Přesto dodnes není známo, zda existuje nekonečně mnoho regulárních prvočísel. K. L. Jensen v roce 1915 dokázal, že existuje nekonečně mnoho iregulárních prvočísel. Největší do roku 2007 známé iregulární prvočíslo má 5083 cifer. Dělí čitatele Bernoulliova čísla B_{2370} a bylo objeveno v roce 2003.

Za obětavé úsilí dokázat Velkou Fermatovu větu získal Kummer od Francouzské akademie věd cenu 3000 franků.

4.6. Prvočísla Sophie Germainové

Základní vlastnosti. V roce 1819 se francouzská matematička Marie-Sophie Germainová proslavila částečným důkazem tzv. prvního případu Velké Fermatovy věty (srov. větu 4.20), tj. rovnice $x^p+y^p=z^p$ nemá řešení v přirozených číslech pro prvočíselný exponent $p > 2$ takový, že p nedělí součin xyz. Dokázala, že pokud p a $2p+1$ jsou současně prvočísly, pak první případ Velké Fermatovy věty platí pro exponent p.

Liché prvočíslo p, pro něž $2p + 1$ je také prvočíslem, se proto nazývá *prvočíslo Sophie Germainové.* Jsou to například prvočísla 5, 11 a 23.

Tato prvočísla mají řadu zajímavých vlastností. Je-li kupříkladu p prvočíslo Sophie Germainové, pak v (Křížek, Somer, 2001) dokazujeme, že všechna kvadratická nerezidua jsou primitivní kořeny modulo $2p + 1$ kromě jediného čísla $2p$, které je kvadratickým nereziduem, ale není primitivním kořenem. K této vlastnosti se ještě vrátíme ve větě 4.28.

Další věta, kterou znal již Fermat, ukazuje úzkou souvislost mezi Mersennovými čísly a prvočísly Sophie Germainové. Byla dokázána později Leonhardem Eulerem a nezávisle též Josephem Louisem Lagrangem.

Věta 4.22. *Nechť p je prvočíslo takové, že $p \equiv 3 \pmod 4$. Pak $2p + 1$ dělí Mersennovo číslo M_p právě tehdy, když $2p + 1$ je prvočíslo.*

Důkaz je uveden například v (Ribenboim, 1996, s. 90–91) a (Robbins, 1993, s. 149). Jestliže tedy $p = 11, 23, 83, \ldots$, pak M_p má prvočinitele 23, 47, 167, ... Další souvislost Mersennových prvočísel s prvočísly Sophie Germainové uvedeme ve větě 4.27.

Dosud nevíme, zda existuje nekonečně mnoho prvočísel Sophie Germainové. Pokud by existovalo nekonečně mnoho prvočísel Sophie Germainové p, pro něž $p \equiv 3 \pmod 4$, pak by také podle věty 4.22 existovalo nekonečně mnoho složených Mersennových čísel, neboť $2p + 1$ dělí $2^p - 1$.

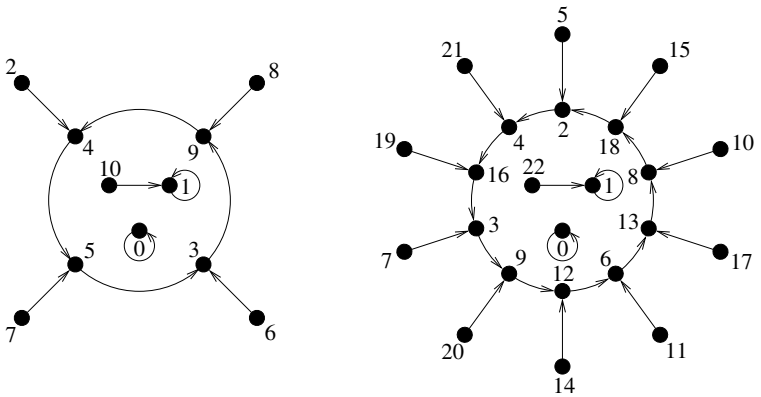
Pokud má množina prvočísel Sophie Germainové určitou hustotu, pak existuje deterministický polynomický algoritmus šestého stupně, který zjistí, zda je dané číslo prvočíslem, viz (Agrawal, Kayal, Saxena, 2004). Pro praktické účely je ale třeba najít algoritmus, který je nejvýše kubický[2)] v čase, jinak se dále budou pro testování prvočíselnosti používat pravděpodobnostní algoritmy založené na Malé Fermatově větě 2.13.

Největší známé prvočíslo Sophie Germainové do roku 2007 bylo

$$p = 7068555 \cdot 2^{121301} + 1,$$

tj. $2p + 1$ je také prvočíslo.

Struktura iteračních grafů. Pro každé přirozené číslo n uvažujme orientovaný graf $G(n)$ s vrcholy $0, 1, 2, \ldots, n-1$, jehož definice je stejná jako v oddílu 4.2, viz (4.11). Ukážeme, že když p je prvočíslo Sophie Germainové, pak má graf $G(2p+1)$ velice zajímavou strukturu. Jeho netriviální komponenty budou totiž připomínat sluníčka nebo kormidelní kolo, jímž se řídí loď – viz (Rogers, 1996, s. 323) a obrázky 4.13, 4.14 a 4.15.

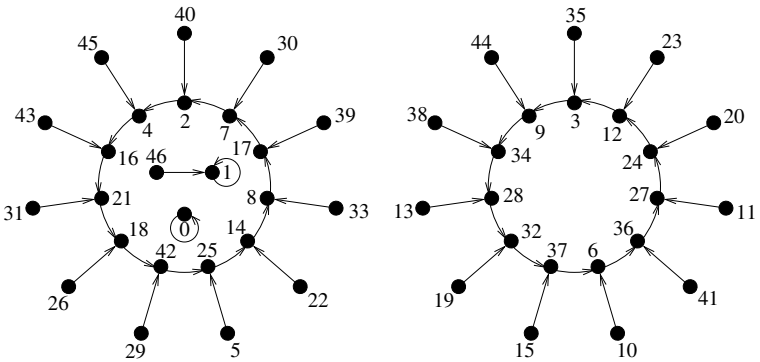


Obr. 4.13. Iterační orientované grafy odpovídající $n = 11$ a $n = 23$.

[2)] Pokud je pro zjištění prvočíselnosti daného čísla o n cifrách zapotřebí řádově n^3 aritmetických operací, pak se algoritmus nazývá *kubický*.

V práci (Rogers, 1996) se popisuje struktura každé komponenty grafu $G(n)$, je-li n prvočíslo. V článcích (Křížek, Somer, 2004) a (Somer, Křížek, 2004, 2006, 2007) vyšetřujeme strukturu $G(n)$ i pro n složená.

Nechť $\omega(n)$ označuje počet různých prvočísel, která dělí n. V příspěvku (Szalay, 1992) se dokazuje, že počet pevných bodů grafu $G(n)$ je roven $2^{\omega(n)}$. To vede k následujícímu tvrzení (srov. obr. 4.13 a 4.14).



Obr. 4.14. Iterační graf pro $n = 47$.

Věta 4.23. *Jestliže n je prvočíslo, pak existují právě dva pevné body grafu $G(n)$, totiž* 0 *a* 1.

Následující tvrzení jsou převzata z článku (Křížek, Somer, 2004). Využívají vlastností Carmichaelovy funkce λ, viz oddíl 2.8.

Věta 4.24. *V grafu $G(n)$ existuje cyklus délky t právě tehdy, když $t = \mathrm{ord}_d 2$ pro nějaký lichý kladný dělitel d čísla $\lambda(n)$.*

D ů k a z. Předpokládejme, že a je vrchol t-cyklu v $G(n)$. Pak t je nejmenší přirozené číslo, pro něž

$$a^{2^t} \equiv a \pmod{n}.$$

Odtud plyne, že t je nejmenší přirozené číslo, pro které

$$a^{2^t} - a \equiv a\left(a^{2^t-1} - 1\right) \equiv 0 \pmod{n}. \tag{4.17}$$

Protože $(a, a^{2^t-1} - 1) = 1$, ze vztahu (4.17) plyne, že když $n_1 = (a, n)$ a $n_2 = n/n_1$, pak t je nejmenší přirozené číslo takové, že

$$\begin{aligned} a &\equiv 0 \pmod{n_1}, \\ a^{2^t-1} &\equiv 1 \pmod{n_2}. \end{aligned} \tag{4.18}$$

Tudíž $(n_1, n_2) = 1$ a podle Čínské věty o zbytcích 1.4 dostaneme existenci celého čísla b takového, že

$$\begin{aligned} b &\equiv 1 \pmod{n_1}, \\ b &\equiv a \pmod{n_2}. \end{aligned} \tag{4.19}$$

Z výrazů (4.18) a (4.19) dále plyne, že t je nejmenší přirozené číslo, pro něž

$$b^{2^t-1} \equiv 1 \pmod{n}. \tag{4.20}$$

Nechť $d = \mathrm{ord}_n b$. Pak $d \mid \left(2^t - 1\right)$. Protože podle (4.20) je t nejmenší přirozené číslo, pro něž $d \mid \left(2^t - 1\right)$, vidíme, že $t = \mathrm{ord}_2 d$. Zřejmě je d liché, neboť $d \mid \left(2^t - 1\right)$. Navíc $d \mid \lambda(n)$, jak plyne z Carmichaelovy věty 2.20, protože podle (4.20) platí $(b, n) = 1$.

Předpokládejme obráceně, že d je lichý kladný dělitel $\lambda(n)$ a nechť $t = \mathrm{ord}_d 2$. Podle Carmichaelovy věty 2.20 existuje zbytek g modulo n tak, že $\mathrm{ord}_n g = \lambda(n)$. Nechť $h = g^{\lambda(n)/d}$. Pak $\mathrm{ord}_n h = d$. Jelikož $d \mid \left(2^t - 1\right)$ (ale $d \nmid \left(2^k - 1\right)$, kdykoliv $1 \leq k < t$), vidíme, že t je nejmenší přirozené číslo, pro které platí

$$h^{2^t-1} \equiv 1 \pmod{n}. \tag{4.21}$$

Potom

$$h \cdot h^{2^t-1} = h^{2^t} \equiv h \pmod{n},$$

a tedy h je vrcholem v t-cyklu $G(n)$. □

Věta 4.25. *Nechť p je prvočíslo Sophie Germainové. Pak $G(2p+1)$ má dvě triviální komponenty: izolovaný pevný bod 0 a komponentu*

$\{1, 2p\}$, *jejíž pevný bod je* 1. *Každá ostatní komponenta má* $2t$ *vrcholů a obsahuje* t*-cyklus, kde* $t = \mathrm{ord}_p 2$. *Počet orientovaných hran přicházejících do každého z vrcholů* t*-cyklu je právě* 2.

D ů k a z. Protože $n = 2p + 1$ je prvočíslo, podle definice Carmichaelovy lambda funkce (viz oddíl 2.8) dostáváme

$$\lambda(2p + 1) = 2p.$$

Číslo $2p$ má právě dva liché dělitele 1 a p. Položíme-li $d = 1$ ve větě 4.24, dostaneme podle věty 4.23, že existují právě dva pevné body 0 a 1. Zřejmě 0 je jediné řešení kongruence $x^2 \equiv 0 \pmod{n}$, a tedy 0 je izolovaný pevný bod. Navíc $x = 1$ a $x = 2p$ jsou jediná řešení kongruence $x^2 \equiv 1 \pmod{n}$, neboť n je prvočíslo. Máme ukázat, že odpovídající komponenta obsahující $\{1, 2p\}$ nemá žádné jiné vrcholy. Protože p a n jsou lichá čísla, vidíme, že $n \equiv 3 \pmod 4$. Tedy $2p$ není kvadratický zbytek modulo n, což znamená, že kongruence $x^2 \equiv 2p \pmod{n}$ nemá řešení.

Položme nyní $d = p$ ve větě 4.24. Každá další komponenta $G(2p+1)$ tedy obsahuje cyklus délky $t = \mathrm{ord}_p 2$ pro $t > 1$. Jestliže vrchol a patří do tohoto t-cyklu, pak kongruence $x^2 \equiv a \pmod{n}$ má řešení, a tudíž a je kvadratický zbytek modulo n. Protože n je liché prvočíslo, má tato kongruence právě dvě řešení c a $-c$. Jedno z nich leží na t-cyklu a druhé mimo něj. Jelikož $n = 2p + 1 \equiv 3 \pmod 4$, jeden ze zbytků c nebo $-c$ musí být kvadratické reziduum a ten druhý kvadratické nereziduum modulo n.

Předpokládejme, že c není kvadratický zbytek modulo n. Pak c leží mimo t-cyklus a orientovaná hrana vycházející z c vstupuje do a. Protože c není kvadratický zbytek modulo n, neexistuje hrana vstupující do c. Proto má příslušná komponenta právě $2t$ vrcholů.

□

V článku (Křížek, Somer, 2004) se zabýváme též obrácenou větou 4.25.

Je-li p prvočíslo Sophie Germainové, pak všechny komponenty grafu $G(2p + 1)$, které neobsahují vrcholy 0 a 1, budeme nazývat *sluníčka Sophie Germainové.*

Jako důsledek dostáváme tuto větu.

Věta 4.26. *Nechť p je prvočíslo Sophie Germainové. Pak počet sluníček Sophie Germainové grafu $G(2p+1)$ je roven*

$$\frac{p-1}{\mathrm{ord}_p 2}. \tag{4.22}$$

D ů k a z. Z věty 4.25 víme, že počet vrcholů grafu $G(2p+1)$, které leží mimo triviální komponenty, je roven $2p-2$. Podle věty 4.25 každé sluníčko Sophie Germainové má $2\,\mathrm{ord}_p 2$ vrcholů, což dokazuje tvrzení. □

Poznámka. Jestliže $2p+1$ je prvočíslo a $p > 1$, pak $2p-2$ není dělitelné 3. Tudíž podle (4.22) není počet sluníček Sophie Germainové nikdy dělitelný 3 a délka všech příslušných t-cyklů také není dělitelná 3.

Nyní dokážeme poněkud obecnější tvrzení, a to, že $G(2p+1)$ nikdy neobsahuje q-cyklus pro $q = 3, 5, 7, 13, 17, 19, \ldots$, což jsou exponenty všech Mersennových prvočísel $M_q = 2^q - 1$ s $q > 2$. (Poznamenejme, že $G(7)$ obsahuje 2-cyklus.)

Věta 4.27. *Nechť M_q je Mersennovo prvočíslo pro $q > 2$. Pak neexistuje prvočíslo Sophie Germainové p tak, že $G(2p+1)$ obsahuje q-cyklus.*

D ů k a z. Předpokládejme naopak, že existuje prvočíslo Sophie Germainové p a Mersennovo prvočíslo M_q pro $q > 2$ tak, že $G(2p+1)$ obsahuje q-cyklus. Pak podle věty 4.25 je $q = \mathrm{ord}_p 2$, a tudíž $p = 2^q - 1$. Číslo

$$2p + 1 = 2^{q+1} - 1 = (2^{(q+1)/2} + 1)(2^{(q+1)/2} - 1)$$

je ale složené pro prvočíslo $q > 2$, což je spor. □

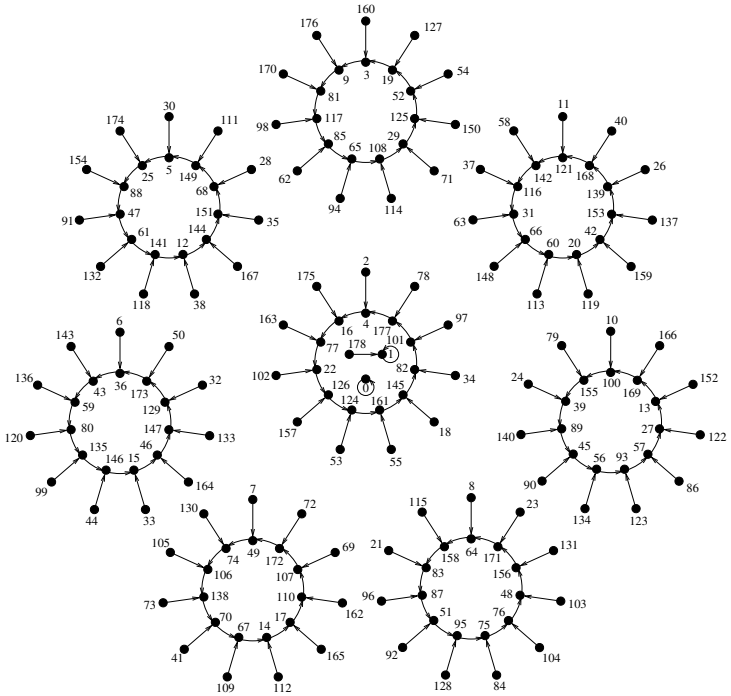
Toto tvrzení tedy opět svazuje Mersennova prvočísla s prvočísly Sophie Germainové.

Příklad. Nechť $p = 89$. Protože $2^{11} \equiv 1 \pmod{89}$, vidíme, že

$\mathrm{ord}_{89}2 = 11$. Tudíž podle věty 4.26 počet sluníček Sophie Germainové grafu $G(179)$ je $88/11 = 8$ (obr. 4.15).

Poznamenejme ještě, že orientované grafy $G(n)$ odpovídající Mersennovým číslům n se vyšetřují v článku (Szalay, 1992). V článcích (Somer, Křížek, 2006, 2007) vyšetřujeme strukturu orientovaných grafů odpovídající kongruenci $f(x) \equiv x^k \pmod{n}$ pro $k \geq 2$, která je obecnější než (4.11).

Z věty 4.16 víme, že počet primitivních kořenů Fermatových prvočísel je roven počtu kvadratických nereziduí. Jiná prvočísla tuto vlastnost nemají. Předpokládejme nyní, že p je prvočíslem Sophie Germainové. Následující věta ukazuje, že počet primitivních kořenů prvočísla $2p + 1$ je jen o jednu menší než počet kvadratických nereziduí, kterých je p.



Obr. 4.15. Iterační orientovaný graf pro $n = 179$.

Věta 4.28. *Je-li p prvočíslem Sophie Germainové, pak prvočíslo $q = 2p + 1$ má $p - 1$ primitivních kořenů modulo q.*

D ů k a z. Prvočíslo Sophie Germainové p je podle definice liché, a proto platí $(2, p) = 1$. Pomocí věty 2.18, výrazu (2.24) a dvojnásobným použitím vztahu (2.22) zjistíme, že počet primitivních kořenů prvočísla q je

$$\varphi(\varphi(q)) = \varphi(2p) = \varphi(2)\varphi(p) = \varphi(p) = p - 1. \qquad \square$$

Podle věty 2.25 je každý primitivní kořen kvadratickým nereziduem modulo q. Následující věta udává, že kvadratické nereziduum $q - 1$ není primitivním kořenem (srov. obrázky 4.13 až 4.15).

Věta 4.29. *Je-li p prvočíslem Sophie Germainové, pak číslo $2p$ je jediné kvadratické nereziduum, které není primitivním kořenem modulo $q = 2p + 1$.*

D ů k a z. Vidíme, že

$$(2p)^2 = (q - 1)^2 \equiv 1 \pmod{q}.$$

Odtud a z nerovnosti $q \geq 7$ plyne, že $2p$ není primitivním kořenem modulo q, neboť $\varphi(q) \geq 2$.

Prvočíslo q je tvaru $4k - 1$, protože p je liché prvočíslo. Podle věty 3.3 kongruence

$$x^2 \equiv 2p \equiv -1 \pmod{q}$$

nemá řešení, a tedy $2p$ je kvadratické nereziduum. $\square$

4.7. Eukleidova prvočísla

Druhá Eukleidova věta 2.3 nám zaručuje, že existuje nekonečně mnoho prvočísel. Její důkaz byl veden sporem. Předpokládalo se, že existuje jen konečně mnoho prvočísel $p_1, p_2, \ldots, p_n$, a přitom se vyšetřovalo číslo (srov. (2.2))

$$m = p_1 p_2 \cdots p_n + 1. \qquad (4.23)$$

Z tohoto důvodu se prvočísla tvaru (4.23) nazývají *Eukleidova prvočísla.* Například

$$2+1=3, \quad 2\cdot 3+1=7, \quad 2\cdot 3\cdot 5+1=31,$$
$$2\cdot 3\cdot 5\cdot 7+1=211, \quad 2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311$$

jsou Eukleidova prvočísla. Povšimněte si, že první tři Eukleidova prvočísla jsou stejná jako první tři Mersennova prvočísla.

Podle (2.3) každé číslo tvaru (4.23) ale prvočíslem být nemusí. Označíme-li symbolem $p\#$ součin všech prvočísel menších nebo rovných p, pak $p\# + 1$ je Eukleidovým prvočíslem pro

$$p = 2,\ 3,\ 5,\ 7,\ 11,\ 31,\ 379,\ 1019,\ 1021,$$
$$2657,\ 3229,\ 4547,\ 4787,\ 11549,\ \ldots,$$

viz např. (Borning, 1972), (Caldwell, Gallot, 2002). Podobně lze vyšetřovat i čísla tvaru $p\# - 1$ (angl. *primorial numbers*), která jsou prvočísly pro

$$p = 3,\ 5,\ 11,\ 13,\ 41,\ 89,\ 317,\ 337,\ 991,$$
$$1873,\ 2053,\ 2377,\ 4093,\ 4297,\ 4583,\ \ldots$$

Nechť $A(p)$ označuje počet primitivních kořenů modulo prvočíslo p. Z věty 4.16 víme, že počet nekongruentních primitivních kořenů Fermatových prvočísel je téměř roven $p/2$, přesněji řečeno platí

$$\frac{A(p)}{p-1} = \frac{1}{2}.$$

Všechna ostatní prvočísla mají počet primitivních kořenů relativně menší. Podle věty 4.28 je počet primitivních kořenů prvočísel tvaru $2p+1$, kde p je prvočíslo, také roven téměř 50 %,

$$\frac{A(2p+1)}{2p-2} = \frac{1}{2},$$

srov. tab. 8 na str 344. Z důkazu následující věty a věty 4.31 bude naopak patrné, že Eukleidova prvočísla mají počet primitivních kořenů velice malý vzhledem k velikosti p.

Věta 4.30. *Pro libovolné $\varepsilon > 0$ existuje p tak, že*

$$\frac{A(p)}{p} < \varepsilon.$$

D ů k a z. Podle věty 2.18 a vztahu (2.22) je $A(p) = \varphi(p-1)$. Symbolem p_i označme i-té prvočíslo. Z Dirichletovy věty 3.10 plyne, že pro libovolné $n \in \mathbb{N}$ existuje $r \in \mathbb{N}$ tak, že $rp_1p_2\cdots p_n+1$ je rovno nějakému prvočíslu p. Pak $p-1$ můžeme rozložit takto:

$$p - 1 = sp_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}, \tag{4.24}$$

kde $(s, p_1, p_2, \ldots, p_n) = 1$ a $k_i \geq 1$ pro $i = 1, \ldots, n$. Odtud z (4.24), (2.23) a (2.24) plyne, že

$$\begin{aligned}\frac{\varphi(p-1)}{p} < \frac{\varphi(p-1)}{p-1} &= \frac{\varphi(s)\varphi(p_1^{k_1})\cdots\varphi(p_n^{k_n})}{p-1} \\ &= \frac{\varphi(s)}{s}\frac{p_1^{k_1-1}(p_1-1)}{p_1^{k_1}}\cdots\frac{p_n^{k_n-1}(p_n-1)}{p_n^{k_n}} \\ &= \frac{\varphi(s)}{s}\frac{p_1-1}{p_1}\cdots\frac{p_n-1}{p_n} \leq \Big(1-\frac{1}{p_1}\Big)\cdots\Big(1-\frac{1}{p_n}\Big),\end{aligned}$$

neboť $\varphi(s) \leq s$. Zbývá dokázat, že

$$\lim_{n\to\infty} a_n = 0, \tag{4.25}$$

kde

$$a_n = \prod_{i=1}^{n}\Big(1-\frac{1}{p_i}\Big).$$

Ze vzorečku pro součet geometrické posloupnosti plyne, že

$$\sum_{j=0}^{\infty}\Big(\frac{1}{p_i}\Big)^j = \frac{1}{1-{p_i}^{-1}},$$

a tedy

$$\frac{1}{a_n} = \prod_{i=1}^{n} \frac{1}{1 - {p_i}^{-1}} = \prod_{i=1}^{n} \sum_{j=0}^{\infty} \Big(\frac{1}{p_i}\Big)^j =$$

$$= \prod_{i=1}^{n} \big(1 + p_1^{-1} + p_1^{-2} + \cdots\big) \cdots \big(1 + p_n^{-1} + p_n^{-2} + \cdots\big) = \sum_{m} \frac{1}{m},$$

kde v poslední sumě sčítáme přes všechna přirozená čísla m, která jsou dělitelná pouze prvočísly $p_1, p_2, \ldots, p_n$. Pro $n \to \infty$ ale pravá strana přechází podle Základní věty aritmetiky 2.2 v harmonickou řadu $\sum_{m=1}^{\infty} \frac{1}{m}$, která je divergentní. Čili levá strana diverguje do nekonečna pro $n \to \infty$, a proto platí (4.25). □

Z důkazu předchozí věty pro Eukleidova prvočísla

$$p = p_1 p_2 \cdots p_n + 1$$

dostáváme následující horní odhad

$$\frac{A(p)}{p} < \Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_n}\Big).$$

Poznamenejme, že součin na pravé straně konverguje velice pomalu monotónně k nule pro $n \to \infty$. Podíl na levé straně pro malá p lze poměrně snadno vypočítat. Prvočíslo 3 má jediný primitivní kořen 2 a prvočíslo 7 má dva primitivní kořeny 3 a 5. Určení počtu primitivních kořenů dalších Eukleidových prvočísel je lepší svěřit počítači: $A(31) = 8$, $A(211) = 48$ a $A(2311) = 480$. Vidíme, že podíly $\frac{A(p)}{p}$ odpovídající prvním pěti Eukleidovým prvočíslům $p = 3,\ 7,\ 31,\ 211,\ 2311$, tj. $\frac{1}{3} \approx 0.333$, $\frac{2}{7} \approx 0.285$, $\frac{8}{31} \approx 0.258$, $\frac{48}{211} \approx 0.227$, $\frac{480}{2311} \approx 0.207$ tvoří pomalu klesající posloupnost.

Věta 4.31. *Je-li p Eukleidovo prvočíslo, pak pro všechna prvočísla*

$q < p$ *platí*

$$\frac{A(q)}{q} > \frac{A(p)}{p}.$$

D ů k a z. Nechť $p = p_1 p_2 \cdots p_n + 1$ je Eukleidovo prvočíslo a nechť $q < p$ je libovolné prvočíslo. Věta zřejmě platí pro $q = 2$, protože

$$\begin{aligned} \frac{A(p)}{p} = \frac{\varphi(p-1)}{p} &< \frac{\varphi(p-1)}{p-1} = \frac{\varphi(p_1)\cdots\varphi(p_n)}{p_1\cdots p_n} \\ &= \frac{p_1-1}{p_1}\cdots\frac{p_n-1}{p_n} \le \frac{1}{2} = \frac{A(q)}{q}. \end{aligned} \tag{4.26}$$

Můžeme tedy předpokládat, že $q > 2$. Pak $q-1$ má méně než n různých prvočísel ve svém prvočíselném rozkladu

$$q - 1 = q_1^{\ell_1} q_2^{\ell_2} \cdots q_m^{\ell_m},$$

kde $q_1 < q_2 < \cdots < q_m$ jsou prvočísla a $\ell_i \ge 1$. Protože $m < n$, platí

$$p_i \le q_i \quad \text{pro } i = 1, \ldots, m.$$

Z vlastností Eulerovy funkce (2.23) a (2.24) dále víme, že

$$\frac{\varphi(q_i^{\ell_i})}{q_i^{\ell_i}} = \frac{\varphi(q_i)}{q_i} = \frac{q_i - 1}{q_i} \quad \text{pro } i = 1, \ldots, m.$$

Odtud, ze vztahu (4.26) a z nerovnosti

$$\frac{p_i - 1}{p_i} \le \frac{q_i - 1}{q_i} \text{ pro } i = 1, \ldots, m,$$

dostaneme

$$\begin{aligned} \frac{A(p)}{p} &< \frac{p_1-1}{p_1}\cdots\frac{p_n-1}{p_n} \le \frac{q_1-1}{q_1}\cdots\frac{q_m-1}{q_m}\frac{q-1}{q} \\ &= \frac{\varphi(q_1^{\ell_1})}{q_1^{\ell_1}}\cdots\frac{\varphi(q_m^{\ell_m})}{q_m^{\ell_m}}\frac{q-1}{q} = \frac{\varphi(q-1)}{q-1}\frac{q-1}{q} = \frac{A(q)}{q}, \end{aligned}$$

kde poslední nerovnost plyne ze skutečnosti, že p_i jsou po sobě jdoucí prvočísla, $m < n$ a $q_m < q$. □

4.8. Další speciální typy prvočísel

Faktoriální prvočísla. V důkazu Druhé Eukleidovy věty 2.3 lze zaměnit vztah (4.23) vztahem

$$m = p! + 1, \tag{4.27}$$

kde p je největší prvočíslo, pokud je jich jen konečný počet. Protože pro každé přirozené číslo $q \leq p$ dá podíl m/q vždy zbytek 1, žádné prvočíslo menší nebo rovné p nedělí m. Podle Základní věty aritmetiky 2.2 je tedy číslo m další prvočíslo, anebo je m dělitelné prvočíslem větším než p, což je spor. Tento poněkud odlišný důkaz Eukleidovy věty se ale v literatuře objevuje méně často.

Prvočísla tvaru (4.27) se nazývají *faktoriální prvočísla*, viz (Borning, 1972), (Caldwell, Gallot, 2002); přitom nepožadujeme, aby p bylo prvočíslo. Například pro

$$n = 1,\ 2,\ 3,\ 11,\ 27,\ 37,\ 41,\ 73,\ 77,\ 116,$$
$$154,\ 320,\ 340,\ 399,\ 427,\ 872,\ 1477, \ldots$$

je $n! + 1$ prvočíslem. Prvočísla tvaru $n! - 1$ se také nazývají *faktoriální.* Dostaneme je například pro

$$n = 3,\ 4,\ 6,\ 7,\ 12,\ 14,\ 30,\ 32,\ 33,\ 38,\ 94,$$
$$166,\ 324,\ 379,\ 469,\ 546,\ 974,\ 1963, \ldots$$

Studují se i další podobné typy prvočísel, např. multifaktoriální prvočísla, viz (Caldwell, Dubner, 1993/94).

Palindromická prvočísla. Slovo palindrom pochází z řečtiny a znamená „běžet opět nazpátek“. *Palindromem* rozumíme řetězec znaků, který se čte zleva doprava stejně jako zprava doleva. Například „kobyla má malý bok“ (odhlédneme-li od délek samohlásek). Snad nejznámějším palindromem v českých zemích je číslo 135797531, které je spojeno s položením základního kamene Karlova mostu v roce 1357 juliánského kalendáře dne 9. 7. v 5 hodin a 31 minut. Diskuse o tom, co tehdy znamenala minuta, je v práci (Horský, 1979, s. 202).

Palindromické prvočíslo je prvočíslo, které je zároveň palindromem, např.

$$3,\ 5,\ 7,\ 11, 101,\ 131,\ 151,$$
$$181,\ 191,\ 313,\ 353,\ 373,\ 383,\ 727,\ 757,\ 787,$$
$$797,\ 919,\ 10301,\ 10501,\ \ldots$$

Povšimněte si, že v tomto seznamu nefigurují žádná čtyřciferná čísla. Platí dokonce mnohem obecnější tvrzení.

Věta 4.32. *Jediné palindromické prvočíslo se sudým počtem cifer je číslo* 11.

D ů k a z. Nechť číslo $m = 9090\ldots90$ má $2k$ cifer. Vidíme, že

$$m \cdot 11 = 99999\ldots990,$$

a tudíž platí

$$11(m+1) = 11m + 11 = 10^{2k} + 1. \tag{4.28}$$

Uvažujme nyní palindromické číslo p se sudým počtem cifer $2n$ ve tvaru

$$p = a_1 10^{2n} + a_2 10^{2n-1} + \cdots + a_2 10 + a_1,$$

kde $a_1 \neq 0$, $a_2, \ldots, a_n$ jsou desítkové cifry. Odtud plyne, že

$$\begin{aligned} p &= a_1(10^{2n}+1) + a_2\,(10^{2n-1}+10) + \cdots + a_n\,(10^{n+1}+10^{n-1}) \\ &= a_1(10^{2n}+1) + 10a_2(10^{2n-2}+1) + \cdots + 10^{n-1}a_n(10^2+1). \end{aligned}$$

Podle (4.28) jsou ale všechny členy dělitelné 11, a proto palindrom p se sudým počtem cifer je vždy složené číslo, pokud je $p > 11$. □

Největším známým palindromickým prvočíslem v roce 2007 bylo číslo

$$10^{175108} + 230767032 \cdot 10^{87550} + 1,$$

které má 175 109 cifer. Speciálními případy těchto čísel jsou prvočísla složená jen z jedniček (angl. *repunit* od slova repeating unit),

která musí mít podle věty 4.32 lichý počet cifer (kromě čísla 11). Například

$$11,\ 1111111111111111,\ 11111111111111111111111 \tag{4.29}$$

jsou prvočísla s 2, 19 a 23 ciframi. Další taková známá prvočísla

$$\frac{10^{317}-1}{9}, \quad \text{resp.} \quad \frac{10^{1031}-1}{9} \tag{4.30}$$

mají lichý počet 317, resp. 1031 cifer.

Cyklická a permutační prvočísla. Prvočíslo se nazývá *cyklické*, jestliže libovolná cyklická permutace jeho cifer dává opět prvočíslo. Například 3779 je permutační prvočíslo, protože

$$3779, \quad 7793, \quad 7937 \quad \text{a} \quad 9377$$

jsou prvočísla. Další cyklická prvočísla jsou

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 37,\ 79,\ 113,\ 197,\ 199,$$
$$337,\ 1193,\ 11939,\ 19937,\ 193939,\ 199933,$$

ale i čísla uvedená v (4.29) a (4.30).

Prvočíslo se nazývá *permutační*, pokud libovolná permutace jeho cifer dává opět prvočíslo. Zatím jsou známa jen tato permutační prvočísla

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 37,\ 79,\ 113,\ 199,\ 337$$

a všechna prvočísla složená z jedniček.

Wilsonova prvočísla. Zaměníme-li v kongruenci ve Wilsonově větě 3.6 modul p za p^2, dostaneme následující definici. Prvočíslo p se nazývá *Wilsonovo*, jestliže platí

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

Dosud byla objevena jen tři Wilsonova prvočísla: 5, 13 a 563.

Siamská prvočísla. V článku (Beauregard, Suryanarayan, 2001) byla zavedena *siamská prvočísla* jako dvojice prvočísel tvaru n^2-2

a n^2+2. Posloupnost takovýchto párů začíná takto:

$$\langle 7,11\rangle,\quad \langle 79,83\rangle,\quad \langle 223,227\rangle,\quad \langle 439,443\rangle,$$
$$\langle 1087,1091\rangle,\quad \langle 13687,13691\rangle.$$

Jedinečná prvočísla. Převrácené hodnoty prvočísel jsou racionální čísla, tj. mají periodický desetinný rozvoj. Délku této periody lze předem určit pomocí věty 4.33. Například zlomky

$$\frac{1}{7}=0.142857142857\ldots,\quad \frac{1}{13}=0.076923076923\ldots$$

mají oba periodu délky 6.

Prvočíslo $p\notin\{2,5\}$ se nazývá *jedinečné,* pokud neexistuje jiné prvočíslo q, jehož převrácená hodnota $1/q$ by měla stejnou délku periody jako $1/p$ (v desítkové soustavě). Jedinečnými prvočísly jsou například čísla

3, 11, 37, 101, 9091, 9901, 333667, 909091, 99990001,...,

jejichž délka periody je postupně:

1, 2, 3, 4, 10, 12, 9, 14, 24,...

Tedy například 1/37 má délku minimální periody 3 a žádné jiné prvočíslo tuto vlastnost nemá. Palindromická prvočísla (4.29) jsou rovněž jedinečnými prvočísly (angl. *unique primes*).

Věta 4.33. *Nechť $n=2^\alpha 5^\beta q$, kde $\alpha\geq 0$, $\beta\geq 0$, $q>1$, $(q,10)=1$ a $\mu=\max(\alpha,\beta)$. Nechť k je nejmenší přirozené číslo takové, že $q\mid(10^k-1)$. Jestliže $m<n$ jsou nesoudělná přirozená čísla, pak desetinný rozvoj zlomku $\frac{m}{n}$ má μ neopakujících se cifer a k opakujících se cifer.*

Důkaz této věty lze nalézt např. v (Hardy, Wright, 1979, s. 111).

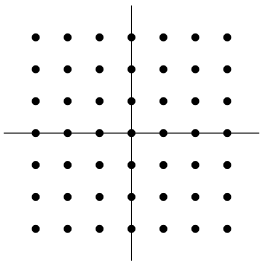
Gaussova prvočísla. Prvočísla lze definovat i v jiných algebraických strukturách než jen na množině přirozených čísel. V komplexní rovině nejprve definujme *Gaussova čísla* jako součty $a+\mathrm{i}b$,

kde $a, b \in \mathbb{Z}$ a i je imaginární jednotka (obr. 4.16). Velikost $z = a + \mathrm{i}b$ je dána vztahem $|z| = \sqrt{a^2 + b^2}$.

Vidíme, že součet i součin dvou Gaussových čísel $a + \mathrm{i}b$ a $c + \mathrm{i}d$ dá opět Gaussovo číslo,

$$(a + \mathrm{i}b) + (c + \mathrm{i}d) = (a + c) + \mathrm{i}(b + d),$$
$$(a + \mathrm{i}b)(c + \mathrm{i}d) = (ac - bd) + \mathrm{i}(ad + bc).$$

Absolutní hodnotu 1 mají právě čtyři Gaussova čísla: ± 1 a $\pm \mathrm{i}$ (obr. 4.16). Množinu Gaussových čísel označme $\mathbb{Z}[\,\mathrm{i}\,]$. Dále si ukážeme, jak se na $\mathbb{Z}[\,\mathrm{i}\,]$ zavádějí tzv. Gaussova prvočísla.



Obr. 4.16. Gaussova čísla v komplexní rovině mají celočíselné souřadnice.

Podle Fermatovy vánoční věty 3.12 lze každé prvočíslo tvaru $4k+1$ napsat jako součet čtverců, který lze ale v komplexní aritmetice rozložit na součin dvou komplexně sdružených Gaussových čísel, jejichž absolutní hodnoty jsou $\sqrt{4k+1}$, tj. leží mezi 1 a $4k + 1$, například

$$13 = 3^2 + 2^2 = (3 - 2\mathrm{i})(3 + 2\mathrm{i}), \quad 17 = 4^2 + 1^2 = (4 - \mathrm{i})(4 + \mathrm{i}).$$

Rovněž prvočíslo 2 lze v komplexní rovině rozložit na součin dvou Gaussových čísel, jejichž absolutní hodnoty jsou $\sqrt{2}$,

$$2 = (1 - \mathrm{i})(1 + \mathrm{i}).$$

To jsou příklady Gaussových složených čísel. Pro prvočísla tvaru $4k - 1$ ale podobný rozklad udělat nelze (viz věta 2.6). To nám umožňuje vyslovit následující definici.

Gaussovo číslo $z = a + \mathrm{i}b$ se nazývá *Gaussovo prvočíslo*, jestliže $|z| > 1$ a z nelze vyjádřit jako součin dvou Gaussových čísel v absolutní hodnotě větších než 1.

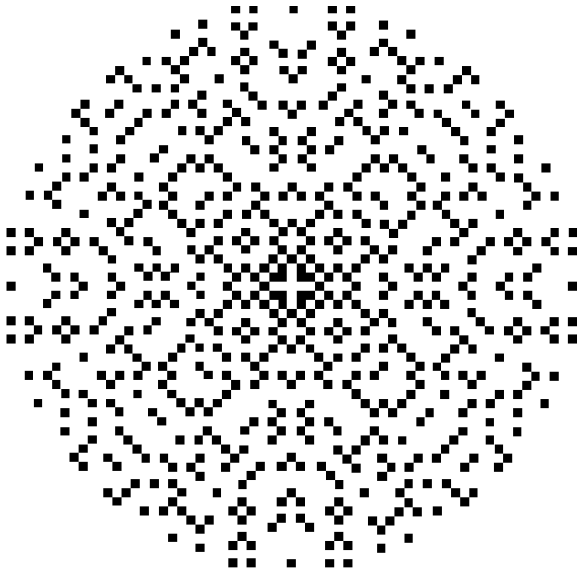
V knize (Wells, 2005, s. 112) se uvádí tato věta.

Věta 4.34. *Číslo $z = a + \mathrm{i}b$, kde $a, b \in \mathbb{Z}$, je Gaussovo prvočíslo právě tehdy, když*

1. $a^2 + b^2$ *je prvočíslo pro* $a \neq 0 \neq b$, *nebo*
2. $|z|$ *je prvočíslo tvaru* $4k - 1$ *pro* $a = 0$ *nebo* $b = 0$.

Na obrázku 4.17 jsou znázorněna Gaussova prvočísla, jejichž absolutní hodnota je menší než $\sqrt{1000}$. Všechna Gaussova prvočísla, jejichž absolutní hodnota nepřevyšuje 7 a $0 < \mathrm{Im}\, z \leq \mathrm{Re}\, z$, jsou tvaru

$1+\mathrm{i}, \quad 2+\mathrm{i}, \quad 3, \quad 3+2\mathrm{i}, \quad 4+\mathrm{i}, \quad 5+2\mathrm{i}, \quad 5+4\mathrm{i}, \quad 6+\mathrm{i}, \quad 7.$



Obr. 4.17. Schematické znázornění Gaussových prvočísel v komplexní rovině. Délka strany jednotlivých čtverečků je rovna 1. Střed obrázku odpovídá nulovému Gaussovu číslu $0 + \mathrm{i}\,0$.

Gaussova prvočíselná čtyřčata jsou čtveřice Gaussových prvočísel tvaru

$$\langle a-1+\mathrm{i}b,\ a+\mathrm{i}(b-1),\ a+\mathrm{i}(b+1),\ a+1+\mathrm{i}b\rangle, \quad a,b\in\mathbb{Z},$$

např.

$$4+5\mathrm{i}, \quad 5+4\mathrm{i}, \quad 5+6\mathrm{i}, \quad 6+5\mathrm{i}.$$

Na obrázku 4.17 je toto čtyřče umístěno nedaleko od středu severovýchodním směrem. Jistě zde objevíte i další Gaussova prvočíselná čtyřčata.

Každé Mersennovo prvočíslo je zároveň i Gaussovým prvočíslem. A tak největší známé reálné Gaussovo prvočíslo do roku 2008 bylo $M_{43112609}$. Řada dalších vlastností Gaussových prvočísel je uvedena v knize (Bressound, Wagon, 2000).

Eisensteinova prvočísla. Jeden z Gaussových žáků Ferdinand Gotthold Max Eisenstein (1823–1852) definoval podobný typ prvočísel v komplexní rovině. Položme

$$\omega=\frac{-1+\mathrm{i}\sqrt{3}}{2}.$$

Vidíme, že ω je třetí odmocnina z jedné, tj. je řešením rovnice $z^3=1$ v komplexním oboru a navíc platí

$$1+\omega+\omega^2=0 \quad \text{a} \quad \omega^2=\overline{\omega}, \tag{4.31}$$

kde $\overline{\omega}$ označuje číslo komplexně sdružené k ω.

Čísla tvaru $a+\omega b$, kde $a,b\in\mathbb{Z}$, se nazývají *Eisensteinova čísla* (obr. 4.18).

Pomocí (4.31) lze ukázat, že součet i součin dvou takových čísel dá opět Eisensteinovo číslo. Absolutní hodnotu 1 má právě těchto šest Eisensteinových čísel: ±1, $\pm\omega$, $\pm\overline{\omega}$ (obr. 4.18).

Použitím (4.31) můžeme rozložit číslo

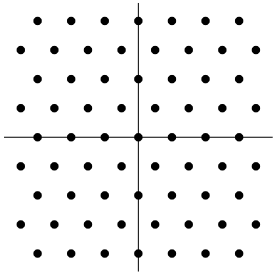
$$3=1-\omega-\omega^2+\omega^3=(1-\omega)(1-\omega^2)=(1-\omega)(1-\overline{\omega})$$

na součin dvou Eisensteinových čísel, jejichž absolutní hodnota je $\sqrt{3}$.

Z Eratosthenova síta (2.4) plyne, že každé prvočíslo větší než 3 je pouze tvaru $6k \pm 1$ pro nějaké vhodné $k \in \mathbb{N}$. Prvočísla tvaru $p = 6k + 1$ ale mohou být rozložena na součin dvou Eisensteinových čísel, jejichž absolutní hodnota je větší než 1. (Přitom se využívá toho, že p je tvaru $a^2 - ab + b^2$, viz (Hardy, Wright, 1979, s. 221).) Například

$$7 = (2-\omega)(2-\overline{\omega}),\ 13 = (3-\omega)(3-\overline{\omega}) \text{ a } 19 = (3-2\omega)(3-2\overline{\omega}).$$

Na druhé straně podobný rozklad nelze udělat pro prvočíslo 2 a prvočísla tvaru $6k - 1$.



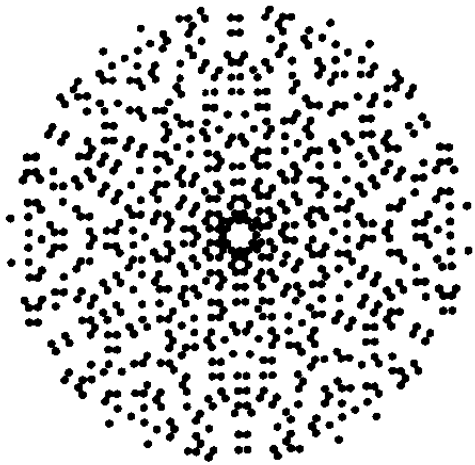
Obr. 4.18. Eisensteinova čísla v komplexní rovině.

Eisensteinovo číslo z se nazývá *Eisensteinovo prvočíslo*, jestliže $|z| > 1$ a z nelze vyjádřit jako součin dvou Eisensteinových čísel v absolutní hodnotě větších než 1.

Rozložení Eisensteinových prvočísel v Gaussově rovině (obr. 4.19) má zajímavou šestičetnou symetrii. Všimněte si šesti malých šestiúhelníčků, které obklopují středový šestiúhelník. To jsou Eisensteinova prvočíselná šesterčata, např.

$$3 + 2\omega, \quad 3 + \omega, \quad 4 + \omega, \quad 5 + 2\omega, \quad 5 + 3\omega, \quad 4 + 3\omega.$$

Zatím ale není známo, zda existují další Eisensteinova prvočíselná šesterčata s větší absolutní hodnotou. Největší známé reálné Eisensteinovo prvočíslo do roku 2007 bylo $27653 \cdot 2^{9167433} + 1$.



Obr. 4.19. Schematické znázornění Eisensteinových prvočísel v komplexní rovině.

Existuje velké množství dalších typů prvočísel, viz např. (Wells, 2005). Hledají se prvočísla, která při „ořezávání“ zprava či zleva dávají opět prvočísla, např. 73 939 133, 7 393 913, 739 391, 73 939, 7393, 739, 73 a 7 nebo 632 647, 32 647, 2547, 647, 47 a 7. Největší známé prvočíslo, které při ořezávání zleva dává jen prvočísla, je 357 686 312 646 216 567 629 137. V kapitole 7 se ještě zmíníme o Fibonacciho, Lucasových, Thabitových, Cullenových a Woodallových prvočíslech.

5. APLIKACE PRVOČÍSEL

Čísla jsou jediná univerzální
řeč ve vesmíru.

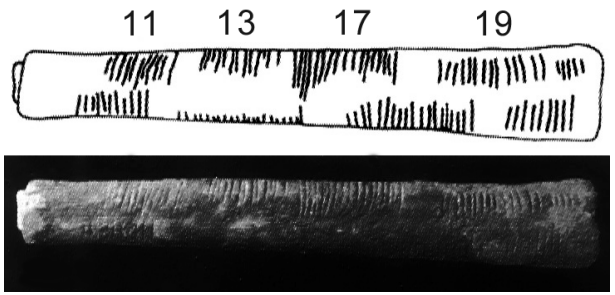
Nathanael West

Nejvyšším posláním matematiky je nalézat skrytý
pořádek v chaosu, který nás všude obklopuje.

Norbert Wiener

5.1. Prvočíslo 11 v kódování

Úvod. Studiem prvočísel se zabývá lidstvo již několik tisíciletí. Podle některých vědců to dokládají archeologické nálezy z území afrického Zairu, kde byla vykopána kost (obr. 5.1), 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 osm tisíc let. Někomu se tehdy asi zdála tato čísla poněkud zvláštní, a tak si je zaznamenal na kost. Samozřejmě se tehdy ještě lidé vážně nezabývali vlastnostmi prvočísel. Avšak již v 7. stol. př. n. l. ve starém Řecku



Obr. 5.1. Znázornění prvočísel na kosti staré 8 tisíc let.

prvočísla prokazatelně studovali. Později Eukleides (4.–3. stol. př. n. l.) dokázal, že je jich nekonečně mnoho (viz věta 2.3). Eratosthenes z Kyreny (3. stol. př. n. l.) se zase proslavil svým prvočíselným sítem (viz (2.4)). Ale teprve ve 20. století se dospělo k tomu, že prvočísla mohou mít řadu zajímavých technických aplikací. V tomto oddílu si ukážeme praktické použití prvočísla 11 v tzv. *samodetekujících kódech.*

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.

Dříve než si ukážeme, jak se prvočíslo 11 vlastně používá, odvodíme jednoduché kritérium pro dělitelnost 11. Podle něho stačí střídavě odečítat a přičítat jednotlivé cifry daného čísla (srov. vztah (5.6)) a pak zjistit, zda je výsledný součet dělitelný 11, viz (Křížek, Šolcová, 2004).

Věta 5.1. *Nechť* $k \in \{0, 1, 2, \dots\}$ *a*

$$m = \sum_{n=0}^{k} c_n 10^n \quad \textit{pro} \quad c_n \in \{0, 1, \dots, 9\}, \quad c_k \neq 0,$$

tj. $c_k, \dots, c_0$ *jsou cifry přirozeného čísla* m *v desítkové soustavě. Pak*

$$11 \mid m \iff 11 \mid \Big(\sum_{n=0}^{k} (-1)^n c_n\Big). \tag{5.1}$$

D ů k a z. Podle vzorce pro rozdíl dvou n-tých mocnin platí

$$10^n - (-1)^n = (10+1)\big[10^{n-1} + 10^{n-2}(-1) + \cdots \\ \cdots + 10(-1)^{n-2} + (-1)^{n-1}\big], \tag{5.2}$$

kde hranatá závorka obsahuje právě n sčítanců. Rozdíl $10^n - (-1)^n$ je tedy dělitelný 11.

Nechť m je dělitelné 11, tj.

$$11 \mid (c_k 10^k + c_{k-1} 10^{k-1} + \cdots + c_1 10 + c_0). \qquad (5.3)$$

Použijeme-li nyní vzorec (5.2) na každý sčítanec v (5.3) kromě posledního, pak dostaneme

$$11 \mid ((-1)^k c_k + (-1)^{k-1} c_{k-1} + \cdots - c_1 + c_0). \qquad (5.4)$$

Podobně zjistíme, že když platí (5.4), je splněn i vztah (5.3). □

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 například, že rodné číslo

$$975811/0428 \qquad (5.5)$$

(odpovídající narození děvčete dne 11. 8. 1997) je dělitelné 11. Podle kritéria (5.1) totiž platí

$$-9 + 7 - 5 + 8 - 1 + 1 - 0 + 4 - 2 + 8 = 11, \qquad (5.6)$$

což 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 například omylem 975811/0728 místo čísla uvedeného v (5.5), počítač by při dělení dvanácti chybu neodhalil, protože obě čísla jsou dělitená 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 (5.5) má hospodářka zapsat do školní databáze. Jestliže se splete například ve třetí cifře takto: 970811/0428 (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 například 13. Proto je prvočíslo 11 pro desítkovou soustavu „optimální“ v 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.

Obr. 5.2. Dvoukoruna má tvar pravidelného jedenáctiúhelníku.

K praktickému použití kritéria (5.1) můžete použít obyčejnou dvoukorunu. Její průmět je totiž pravidelný jedenáctiúhelník (s mírně zaoblenými rohy). Zkuste si ekvivalenci (5.1) prověřit na příkladu (5.5). Minci umístěte do základní polohy (obr. 5.2). Pak jí postupně střídavě otáčejte po směru a proti směru hodinových ruči-

ček o tolik vrcholů, kolik je příslušná cifra. Pokud jste se nezmýlili, mince se nakonec musí opět nalézat v základní poloze (vzhledem k (5.6)).

Kódy ISBN a ISSN. Podobně jako rodná čísla jsou chráněny proti možné chybě i kódy ISBN knižních publikací. Skládají se z deseti cifer $x_1x_2\ldots x_{10}$, které jsou rozděleny do čtyř částí, mezi nimiž jsou tři spojovníky. Přitom první tři části mají proměnnou délku. Celosvětový knižní kód má tvar:

ISBN kód země-nakladat.-identifik. číslo knihy-kontrol. cifra x_{10}.

Například pro knihu (Křížek, Luca, Somer, 2001) je

$$\text{ISBN } 0\text{-}387\text{-}95332\text{-}9, \tag{5.7}$$

kde ISBN je zkratka anglického názvu *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.), 387 je kód nakladatelství Springer, následují identifikační číslo knihy a poslední cifra x_{10}, která se volí tak, aby číslo

$$x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} \tag{5.8}$$

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. Další podrobnosti jsou uvedeny na adrese [www7].

Pro kód (5.7) po dosazení do (5.8) dostáváme

$$2\cdot 3+3\cdot 8+4\cdot 7+5\cdot 9+6\cdot 5+7\cdot 3+8\cdot 3+9\cdot 2+10\cdot 9 = 286,$$

což po vydělení 11 dá přesně 26. 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 kódy ISBN jsou třináctimístné. Začínají trojciferným číslem 978 (EAN Prefix).

Kódy ISSN (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 je na místě kontrolní číslice potřeba 10, používá se znak X). Například pro časopis Pokroky matematiky, fyziky a astronomie je CS-ISSN-0032-2423, což vyhovuje 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 kódy ISSN se v současnosti předkládá trojciferné číslo 977 (EAN Prefix). Více podrobností je uvedeno na adrese [www8].

Identifikační čísla organizací. Ve veřejné správě se setkáváme s identifikačními čísly organizací, která mají osm cifer (podobně jako kódy ISSN) 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 například pro IČO Matematického ústavu Akademie věd ČR, které je 67 985 840.

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

má 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

$$11 \mid \Big(\sum_{i=0}^{5} b_i 2^i\Big), \quad 11 \mid \Big(\sum_{i=0}^{9} a_i 2^i\Big). \tag{5.9}$$

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 (5.9) máme $1 \cdot 4 + 5 \cdot 2 + 8 \cdot 1 = 22$, což je dělitelné 11. Podobně zjistíme dělitelnost jedenácti i druhé části čísla účtu,

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

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 například 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 (obr. 5.3 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). O různých typech dalších kódů se můžete dočíst na stránkách [www9] a [www10].

Obr. 5.3. 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 oddíl 9.1). 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, například aby nebyly současně otevřené závory a návěstidlo pro vlak na volno. 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 (obr. 5.3 vpravo). Můžeme se s nimi setkat například na amerických řidičských průkazech a 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.

5.2. Šifrování tajných zpráv pomocí velkých prvočísel

Metoda RSA pro šifrování zpráv. Při přenosu tajných vojenských zpráv, bankovních údajů, strategických dat a dalších důvěrných a citlivých informací je nutné dodržovat maximální obezřetnost. Například obchodní transakce dnes běžně prováděné prostřednictvím internetu si může někdo nepovolaný přečíst, a pak je zneužít. Proto je třeba takové údaje při přenosu zašifrovat.

Základní rozdíl mezi pojmy *šifrování* a *kódování* spočívá v tom, že při šifrování se využívá nějaká tajná informace (klíč), bez jejíž znalosti v podstatě nelze získat ze zašifrované zprávy její obsah, viz (Mlýnek, 2006). Naproti tomu kódování je transformace jedné formy zápisu informace do jiné formy, která je z nějakého důvodu pro danou situaci výhodnější (např. kódy ASCII, Morseova abeceda, genetický kód nebo kódy z oddílu 5.1).

Návrhem vhodných šifrovacích metod a problémy bezpečného přenosu, ochrany a uchovávání dat se zabývá věda nazývaná *kryptografie.* Naproti tomu *kryptoanalýza* je zaměřena na studium metod pro luštění šifer. Kdysi se k šifrování používalo tzv. tajného klíče. Jeho nevýhodou bylo, že jej musely znát všechny komunikující strany, a tak mohlo snadno dojít k jeho prozrazení. Jakmile je totiž jednou tajný klíč znám, přenos zprávy již není tajný. Pěkný historický přehled o problematice šifrování je uveden v knize (Grošek, Porubský, 1992).

V článku (Rivest, Shamir, Adelman, 1978) byla publikována metoda (nyní nazývaná metoda RSA podle počátečních písmen příjmení autorů), která k šifrování používá veřejně známý klíč. Šifrovat zprávy tedy může kdokoliv, ale odšifrovat je dokáže jen ten, kdo navíc zná tajný dešifrovací klíč. Dnes je to bezesporu jedna z nejbezpečnějších šifrovacích technik. Její hlavní myšlenka je založena na tom, že umíme-li zprávu zašifrovat, neznamená to ještě, že ji umíme odšifrovat. Jinými slovy, předností metody RSA je, že ze znalosti šifrovacího klíče nelze odvodit klíč dešifrovací. To vyplývá z vlastností tzv. jednosměrných funkcí, jejichž hodnotu lze jednoduše vypočítat, zato je však téměř nemožné tyto funkce

invertovat. Utajovaná zpráva se nejprve převede na řetěz číslic (tj. přirozené číslo). Hlavní trik metody RSA spočívá v tom, že vynásobit dvě prvočísla, která mají, řekněme, okolo sta cifer, trvá i na běžném osobním počítači jen zlomek sekundy. Naproti tomu zpětně rozložit tento součin na dva prvočinitele by trvalo pomocí nejlepších známých metod a nejmodernějších počítačů mnohem déle, než je stáří vesmíru. Proto je metodám rozkladu věnována značná pozornost a za posledních třicet let byl učiněn skutečně obrovský pokrok. Přehled těchto metod je podán v (Pomerance, 1998). Nejefektivnější z nich umožňují v „přiměřeném" čase rozkládat na prvočinitele přirozená čísla až o 200 cifrách. V následujících odstavcích se seznámíme pouze se základní myšlenkou metody RSA (nikoli s její praktickou realizací).

Šifrování a odšifrování utajovaných zpráv. Nejprve si připomeňme (viz oddíl 1.7), že zápis

$$x \equiv y \pmod{n}$$

znamená, že $x - y$ je dělitelné n beze zbytku. Přitom předchozí kongruenci můžeme násobit i mocnit, tj.

$$cx \equiv cy \pmod{n} \quad \text{a} \quad x^k \equiv y^k \pmod{n}$$

pro c celé a k přirozené.

Utajovanou zprávu nejprve převedeme na přirozené číslo x. K tomu nám může posloužit například známá tabulka kódů ASCII (A=65, B=66, . . . , Z=90, . . .), ale existují i jiné mnohem efektivnější možnosti.

Dále budeme předpokládat, že

$$x < n,$$

kde n je součin dvou různých prvočísel, která nejsou veřejně známa a mají více než 100 cifer. Pokud by byla zpráva delší, rozdělíme ji na několik kratších tak, aby předchozí nerovnost byla splněna pro každou z nich.

Vlastní algoritmus šifrování je relativně jednoduchá operace, při níž se umocňuje x na přirozený exponent e modulo n. Zašifrovanou

zprávu označme symbolem x^*. Je to přirozené číslo x^*, které je jednoznačně definováno nerovností $x^* < n$ a kongruencí

$$x^* \equiv x^e \pmod{n} \qquad \text{(zašifrovaná zpráva)}, \tag{5.10}$$

kde e se nazývá *šifrovací exponent* (od angl. slova *encryption*) a obě čísla e a n jsou veřejně známa, a jen tato dvě čísla stačí k zašifrování. Proto může šifrovat kdokoliv.

Odšifrování probíhá zcela analogicky. Opět se definuje číslo $(x^*)\hat{} \in \mathbb{N}$ splňující nerovnost $(x^*)\hat{} < n$ tak, aby

$$(x^*)\hat{} \equiv (x^*)^d \pmod{n} \qquad \text{(odšifrovaná zpráva)}. \tag{5.11}$$

Dešifrovací exponent d (od angl. slova *decryption*) ale není veřejně znám. Na straně 174 ukážeme, jak volit exponenty e a d tak, aby $(x^*)\hat{} = x$, tj. aby zašifrovaná zpráva byla po odšifrování totožná s původní zprávou x.

Eulerova funkce. Připomeňme (viz oddíl 2.7), že pro každé $n \in \mathbb{N}$ je hodnota Eulerovy funkce $\varphi(n)$ definována jako počet těch přirozených čísel nepřevyšujících n, která jsou nesoudělná s n, tj.

$$\varphi(n) = |\{m \in \mathbb{N};\ 1 \le m \le n,\ (m, n) = 1\}|, \tag{5.12}$$

kde symbol $|\cdot|$ označuje počet prvků. Snadno se můžeme přesvědčit, že

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

je-li p prvočíslo. Navíc lze dokázat, že pro i-tou mocninu prvočísla p platí

$$\varphi(p^i) = (p-1)p^{i-1}, \quad i \in \mathbb{N}. \tag{5.13}$$

Nás ale bude hlavně zajímat hodnota Eulerovy funkce pro

$$n = pq, \tag{5.14}$$

kde p a q jsou různá prvočísla. Číslo n je tedy dělitelné p i q a počet všech přirozených čísel menších než n je zřejmě $pq - 1$. V nich je ale obsaženo $p - 1$ násobků q a $q - 1$ násobků p, které

jsou vzájemně různé a soudělné s n. Tedy

$$\varphi(n) = (pq-1)-(p-1)-(q-1) = pq-p-q+1 = (p-1)(q-1). \tag{5.15}$$

Důležitou vlastností Eulerovy funkce je implikace

$$(m,n) = 1 \quad \Longrightarrow \quad \varphi(mn) = \varphi(m)\varphi(n), \tag{5.16}$$

která je vlastně jen zobecněním toho, že z (5.14) plyne (5.15).

Jak již bylo řečeno v oddílu 2.7, pomocí funkce φ Leonhard Euler zobecnil Malou Fermatovu větu, aniž by tušil, jaké obrovské uplatnění bude za několik století mít. Metodu RSA, opírající se o Eulerovu–Fermatovu větu 2.17, totiž používá například americká armáda či banky k bezpečnému přenosu tajných či důvěrných dat. Tuto větu si nyní pro úplnost připomeneme.

Věta 5.2 (Eulerova–Fermatova). *Pro $x, n \in \mathbb{N}$ platí*

$$(x,n) = 1 \tag{5.17}$$

právě tehdy, když

$$x^{\varphi(n)} \equiv 1 \pmod{n}. \tag{5.18}$$

Kdy platí $(x^*)\hat{} = x$? Nejprve dokážeme následující větu, která stanovuje postačující podmínky pro existenci inverzního prvku modulo $\varphi(n)$.

Věta 5.3. *Jestliže $e \in \mathbb{N}$ splňuje rovnost*

$$(e, \varphi(n)) = 1, \tag{5.19}$$

pak existuje právě jedno $d \in \mathbb{N}$ menší než $\varphi(n)$ takové, že

$$ed \equiv 1 \pmod{\varphi(n)}. \tag{5.20}$$

Důkaz. Pro přirozená čísla $k = 1, \ldots, \varphi(n) - 1$ definujme zbytky $z_k \in \{1, \ldots, \varphi(n) - 1\}$ pomocí kongruence

$$ek \equiv z_k \pmod{\varphi(n)}.$$

Pokud se dva zbytky rovnají, tj. $z_{k_1} = z_{k_2}$, potom

$$e(k_1 - k_2) \equiv 0 \pmod{\varphi(n)}.$$

Podobným způsobem jako v důkazu První Eukleidovy věty 2.1 nejprve dokážeme, že $k_1 = k_2$.

Podle předpokladu (5.19) a věty 1.3 existují celá čísla v a y tak, že $ev + \varphi(n)y = 1$, tj.

$$e(k_1 - k_2)v + \varphi(n)(k_1 - k_2)y = k_1 - k_2.$$

Odtud plyne, že $k_1 - k_2 \equiv 0 \pmod{\varphi(n)}$, neboli $k_1 = k_2$. Vidíme tedy, že všechna z_k jsou vzájemně různá, a proto existuje právě jedno d odpovídající zbytku 1, které splňuje (5.20). □

Dále dokážeme, že zašifrovaná zpráva x^* je po odšifrování totožná s původní zprávou x.

Věta 5.4. *Jestliže platí* (5.19)*, pak*

$$(x^*)\hat{} = x. \tag{5.21}$$

D ů k a z. Z kongruence (5.20) plyne existence takového čísla r, že

$$ed = 1 + r\varphi(n). \tag{5.22}$$

Rozlišujme dva případy:

1. Nechť platí předpoklad (5.17). Pak lze Eulerův vztah (5.18) umocnit na r-tou a vynásobíme-li jej poté x, dostaneme

$$x^{1+r\varphi(n)} \equiv x \pmod{n}. \tag{5.23}$$

Nyní postupně z (5.11), (5.10), (5.22) a (5.23) plyne, že

$$(x^*)\hat{} \equiv (x^*)^d \equiv x^{ed} \equiv x^{1+r\varphi(n)} \equiv x \pmod{n}. \tag{5.24}$$

Vztah (5.21) tedy platí, neboť obě přirozená čísla x i $(x^*)\hat{}$ jsou menší než n.

2. Nechť naopak předpoklad (5.17) neplatí. Potom podle (5.14) je buď $x = p$, anebo $x = q$. Předpokládejme například, že $x = q$ (případ $x = p$ by se vyšetřoval analogicky). Protože $(q, p) = 1$,

můžeme umocnit Fermatův vztah $x^{p-1} \equiv 1 \pmod{p}$ na $r(q-1)$, tj.

$$x^{r(p-1)(q-1)} \equiv 1 \pmod{p}.$$

Podle (5.15) je $\varphi(n) = (p-1)(q-1)$, a tedy snadno nahlédneme, že platí

$$x^{1+r\varphi(n)} \equiv x \pmod{px}.$$

To je ale opět vztah (5.23), jelikož $px = pq = n$. Důkaz rovnosti (5.21) je potom stejný jako v (5.24). □

Volba šifrovacího a dešifrovacího exponentu. Šifrovací exponent e se volí tak, aby $3 \leq e < \varphi(n)$ a aby platil předpoklad (5.19). To lze ovšem snadno splnit vzhledem k (5.15). Navíc je třeba zvolit e tak, aby $e^m \not\equiv 1 \pmod{\varphi(n)}$ pro „nevelká“ m. Jinak by totiž, vzhledem k relaci (5.20), mohl kdokoliv odšifrovat zprávy pro $d = e^{m-1}$.

V kongruencích (5.10) a (5.11) přímo nefigurují hodnoty prvočísel p a q, a pokud je neznáme, je téměř nemožné stanovit hodnotu dešifrovacího exponentu d. Z věty 5.3 však víme, že existuje právě jedno přirozené číslo $d < \varphi(n)$ splňující kongruenci (5.20). Jak však stanovit jeho hodnotu v konkrétním případě, jestliže známe p a q?

Pokud umíme rozložit $\varphi(n)$ z (5.15) na prvočísla,[1)] pak pomocí (5.13) a (5.16) lze jednoduše vypočítat hodnotu $\varphi(\varphi(n))$, viz např. (5.26). Stanovení exponentu d je potom relativně snadné. Z Eulerovy–Fermatovy věty 5.2, kde místo x píšeme e a místo n píšeme $\varphi(n)$, plyne implikace

$$(e, \varphi(n)) = 1 \quad \Longrightarrow \quad e^{\varphi(\varphi(n))} \equiv 1 \pmod{\varphi(n)}.$$

Vynásobíme-li předchozí kongruenci d a využijeme-li (5.20), pak dostaneme explicitní vyjádření pro dešifrovací exponent $d < \varphi(n)$,

$$d \equiv de^{\varphi(\varphi(n))} \equiv ede^{\varphi(\varphi(n))-1} \equiv e^{\varphi(\varphi(n))-1} \pmod{\varphi(n)}. \quad (5.25)$$

[1)] Najít prvočíselný rozklad čísel $p-1$ a $q-1$ je mnohem snazší než rozkládat n, protože mají zhruba jen poloviční počet cifer, než má n, a navíc jsou sudá.

Pokud $\varphi(n)$ neumíme rozložit na prvočísla, lze d počítat přímo z kongruence (5.20), a to například Eukleidovým algoritmem z oddílu 1.5, anebo prostě zvolíme jiné p či q.

Ilustrační příklad. Nechť $p = 491$ a $q = 701$ jsou prvočísla z rozkladu (5.14). Pak $n = 344\,191$ a podle (5.15) je $\varphi(n) = 343\,000$. Zvolíme-li šifrovací exponent $e = 3$, pak (5.19) zřejmě platí, protože 343 000 není dělitelné třemi.

Nechť „tajná" zpráva, kterou chceme poslat, zní: SOS. Položíme-li například A=01, B=02, C=03, ..., O=15, ..., S=19, ..., Z=26, zprávu převedeme na číslo $x = 191\,519$. Hodnotu x zašifrujeme veřejným klíčem (5.10) na $x^* = 224\,717$, neboť

$$191519^3 \equiv 224717 \pmod{344191}.$$

Dále se zabývejme výpočtem d. Opakovaným užitím vztahů (5.16) a (5.13) dostaneme

$$\varphi(\varphi(n)) = \varphi(343000) = \varphi(2^3 5^3 7^3) = \varphi(2^3)\varphi(5^3)\varphi(7^3) = \\ = 4 \cdot 100 \cdot 294 = 117600. \tag{5.26}$$

Na počítači můžeme ověřit, že

$$3^{117599} \equiv 228667 \pmod{343000},$$

a tak podle (5.25) je $d = 228667$. Aby výpočet předchozí kongruence probíhal rychle, exponent se rozloží na mocniny dvou, tj.

$$117599 = 2^0+2^1+2^2+2^3+2^4+2^6+2^8+2^9+2^{11}+2^{14}+2^{15}+2^{16}.$$

Pak totiž lze pro výpočet mocnin 3^{2^k} použít již spočtené nižší mocniny $3^{2^{k-1}}$ modulo $\varphi(n)$, a příslušné z nich pak pronásobit opět modulo $\varphi(n)$.

Konečně z (5.11) a (5.21) (nebo opět na počítači) dostaneme, že

$$224717^{228667} \equiv 191519 \pmod{344191},$$

tj. $(x^*)\hat{} = 191519$, což znamená SOS.

Závěr. Matematický popis metody RSA vlastně vynalezli W. Diffie

a M. E. Hellman již v roce 1976 tím, že zavedli pojem tzv. jednosměrné funkce. S tímto pojmem se seznámíme v oddílu 5.3. I když Diffie a Hellman jako první předložili vztah (5.10) pro šifrování – viz (Diffie, Hellman, 1976), neuvedli žádný ilustrační příklad jako Rivest, Shamir a Adleman. Posledně jmenovaní se pak proslavili zejména tím, že zveřejnili algoritmus výpočtu kongruence (5.10), podrobně a srozumitelně popsali řadu výhod a vlastností metody RSA, navrhli, jak volit prvočísla p a q atd. Detailní analýza metody RSA je uvedena také v (Grošek, Porubský, 1992, s. 205). Metoda RSA je v současnosti považována za jednu z nejbezpečnějších šifer.

Zopakujme si ještě význam některých použitých symbolů:

- p, q – dvě různá prvočísla, která nejsou veřejně známa,
- n – součin p a q, který je veřejně znám (je součástí veřejného klíče),
- e – šifrovací exponent, který je veřejně znám (je součástí veřejného klíče),
- d – dešifrovací exponent, který není veřejně znám (tzv. soukromý klíč),
- x – zpráva převedená na přirozené číslo menší než n,
- x^* – zpráva zašifrovaná pomocí exponentu e.

5.3. Digitální podpis

Protože e a d je podle (5.20) dvojice vzájemně inverzních prvků modulo $\varphi(n)$, můžeme jednoduše ověřit, že také platí (srov. s (5.21))

$$(x\hat{})^* = x \tag{5.27}$$

za předpokladu (5.19). Rovnost (5.27) se používá pro tzv. *digitální podpis*, jenž zaručuje pravost zprávy.

Například velitel vojenského útvaru použije na nějakou důležitou (ale ne tajnou) zprávu nejprve svůj soukromý klíč (5.11), který zná jen on. Díky platnosti vztahu (5.27) pak mohou podřízené jednotky tuto zprávu odšifrovat pomocí veřejného klíče (5.10), a tak

jsou si jisty, že celou zprávu skutečně poslal jejich velitel a ne někdo jiný.

Digitální podpis je tak mnohem spolehlivější než „originál" pravého podpisu či otisk prstů, protože jej nelze zfalšovat. Navíc podepsaný nemůže později popřít, že to je právě jeho podpis. Jinou možnost uvedeme v oddílu 5.4.

Digitální podpisy hrají též důležitou roli při projektování počítačových systémů proti nežádoucím vstupům a manipulacím, ochraně dat před „nepovolanými čtenáři", falzifikaci nebo destrukci rozličných souborů.

Metoda RSA našla široké uplatnění zejména ve vojenství a při provádění větších bankovních transakcí. Používá se i pro přenos tajných klíčů (viz oddíl 9.2), čísel PIN a všude tam, kde je nutné zajistit vysokou důvěrnost. Až se zrychlí technika šifrování, pak podle (Rivest, Shamir, Adelman, 1978) bude možné telefonovat tak, že každé vyřčené slovo bude nejprve „podepsáno".

Dále si přiblížíme pojem jednosměrné funkce. Nechť A a B jsou nějaké podmnožiny celých čísel. Pak funkci $f : A \to B$ nazveme *jednosměrnou,* jestliže pro každé $x \in A$ je „snadný" výpočet funkční hodnoty $f(x)$, avšak pro libovolnou hodnotu y z oboru hodnot $f(A) = \{y \in B;\ \exists x \in A : y = f(x)\}$ je „velice obtížné" (technicky neproveditelné) najít $x \in A$ tak, aby platilo

$$y = f(x).$$

Současně k danému $x_1 \in A$ není možné v reálném čase určit takové $x_2 \in A$, $x_2 \neq x_1$, aby platilo

$$f(x_1) = f(x_2). \tag{5.28}$$

Za příklad jednosměrné funkce lze považovat funkci danou vztahem

$$f(x) \equiv g^x \pmod{p}, \tag{5.29}$$

kde p je velké prvočíslo, g je primitivní kořen modulo p a $0 \leq f(x) < p$ je zbytek. I pro velké přirozené číslo x lze poměrně snadno vypočítat hodnotu $f(x)$, avšak zpětné určení hodnoty x

z $f(x)$ (tj. výpočet diskrétního logaritmu) není v reálném čase možné, i když p a g jsou veřejně známé.

Jednosměrné funkce se také používají k vytváření digitálního podpisu, viz např. (Mlýnek, 2007). Právními aspekty tzv. elektronického podpisu, který je vymezen poněkud šířeji, se zabývá knížka (Bosáková a kol., 2002).

5.4. Hašovací funkce

Speciálním případem jednosměrných funkcí jsou tzv. funkce hašovací (z angl. slova *hash* = otisk), které přiřazují datům libovolné délky řetězec bitů pevně stanovené délky, např. 128 bitů = 16 bytů (čti bajtů), což je řetězec nul a jedniček délky 128. V současnosti se hodně používají také délky 20 bytů a více. Přiřazenou hodnotu budeme nazývat *otisk* (říká se ji též *haš*). Přitom je hašovací funkce konstruována tak, aby nebylo možné v reálném čase najít dva různé vstupní soubory dat, kterým by byla přiřazena stejná hodnota hašovací funkce (viz (5.28)). Hašovací funkce se používá také při realizaci digitálního podpisu, při kryptografických kontrolních součtech při přenosu dat aj.

Například při kontrole shodnosti dvou databází se vzájemně neporovnávají všechny soubory, ale místo složitého přenášení se porovnají jen jejich otisky $f(x_1)$ a $f(x_2)$. Pokud $f(x_1) = f(x_2)$, jsou s pravděpodobností téměř rovnou 1 obě databáze shodné.

Hašovací funkce se také může použít k pozdějšímu prokázání původnosti nějakého dokumentu x, aniž byl z nějakého důvodu zveřejněn. Stačí, pokud je uveřejněna jen jeho hodnota $f(x)$. Kdykoliv je pak možné dodatečně ověřit, že otisk $f(x)$ odpovídá souboru x. Například autor závěti zapsané v elektronické formě může zveřejnit pouze její otisk. Po úmrtí autora a zveřejnění závěti si může kdokoliv ověřit, že nejde o podvržený nebo dodatečně upravený elektronický dokument, tj. že do závěti nebylo nic připisováno či z ní vyškrtáváno.

Uveďme příklad početní náročnosti získání souboru x, jehož

otisk je roven zadané hodnotě y, tj. $f(x) = y$. Předpokládejme pro jednoduchost, že x budeme vybírat pouze ze souborů délky 16 bytů (= 128 bitů). Uvažujme hašovací funkci s délkou výstupu také 16 bytů a předpokládejme, že k získání hledaného souboru x bude zapotřebí kolem 2^{127} pokusů. Při rychlosti 10^6 pokusů za sekundu by k provedení uvedeného počtu pokusů bylo zapotřebí asi $5.4 \cdot 10^{24}$ let, což je mnohem více, než je současné stáří vesmíru ($13.7 \cdot 10^9$ let).

V tomto příkladu je digitální podpis vlastně stejně velký jako celá zpráva, což je nevýhodné z hlediska výpočetní náročnosti.

V knize (Křížek, Luca, Somer, 2001, s. 174) ukazujeme, jak lze použít Eulerovu–Fermatovu větu 5.2 a Fermatova prvočísla ke konstrukci hašovacích funkcí pro efektivní ukládání datových souborů a hledání potřebné informace v nich. Na zobrazení dané množiny datových souborů do množiny adres v paměti počítače můžeme totiž pohlížet také jako na hašovací funkci. Nechť je každý soubor jednoznačně určen svým klíčem k. (Termín klíč má zde poněkud jiný význam než v oddílech 5.2 a 5.3.) Hašovací funkce má tvar

$$h : k_j \in K = \{k_1, k_2, \ldots, k_n\} \mapsto j \in \{1, 2, \ldots, n\}.$$

Přitom soubor kromě klíče k ještě obsahuje nějakou další informaci INFO(k) tak, jak je znázorněno na tomto schématu:

Množina klíčů s dodatečnou informací			adresa
k_1,	INFO(k_1)	$\mapsto$	1
k_2,	INFO(k_2)	$\mapsto$	2
	$\vdots$		$\vdots$
k_n,	INFO(k_n)	$\mapsto$	n

Například k může být poznávací značka automobilu a INFO(k) může obsahovat další údaje o majiteli, barvě automobilu, jeho velikosti, výkonu motoru atd. Všechny soubory lze uspořádat a definovat hašovací funkci tak, že pro daný klíč k můžeme přímo nalézt odpovídající soubor, aniž bychom museli prohledávat všechny klíče.

5.5. Generátory pseudonáhodných čísel

Pročísla lze také využít ke konstrukci generátorů pseudonáhodných čísel, jež mají například tvar

$$r_i \equiv k r_{i-1} \pmod{m}, \quad i = 1, 2, \ldots,$$

kde modul m je prvočíslo nebo mocnina prvočísla, r_0 a k jsou vhodně zvolené konstanty a $0 \leq r_i < m$. Aby takový generátor nevytvářel pořád stejnou posloupnost při každém svém spuštění, je třeba jej restartovat pokaždé obecně z jiné hodnoty r_0, čehož se většinou dosahuje hardwarově.

Generátory pseudonáhodných čísel se používají k získávání prvočíselných rozkladů, při testování prvočíselnosti, při simulaci některých fyzikálních procesů, při řešení parciálních diferenciálních rovnic metodou Monte Carlo (zejména ve vícerozměrném prostoru), v kryptografii pro generování pseudonáhodných posloupností bitů (viz kap. 9.2), ale i ve všech počítačových hrách, kde je zapotřebí nějaké nahodilosti, aj.

Posloupnost pseudonáhodných čísel $x_i \in \langle 0, 1)$ lze definovat například takto:

$$x_i = \frac{r_i - 1}{F_4 - 1} \quad \text{pro } i = 1, 2, \ldots,$$

kde F_4 je Fermatovo prvočíslo, $r_i \in \{1, \ldots, F_4 - 1\}$ je zbytek takový, že

$$r_i \equiv 75 r_{i-1} \pmod{F_4} \quad \text{a} \quad r_0 = 1. \tag{5.30}$$

Délka periody této posloupnosti je $2^{16} = 65\,536$, což je maximální možná délka pro prvočíselný modul F_4.

Posloupnost zbytků mocnin $75,\ 75^2,\ 75^3, \ldots$ se tedy nejprve dělí Fermatovým prvočíslem $F_4 = 2^{16} + 1$ a zbytky se pak normují tak, že se dělí $F_4 - 1$. Periodická posloupnost x_i pseudonáhodných čísel tak nabývá hodnot mezi 0 a 1 (včetně 0, ale kromě 1). Konstanta u r_{i-1} ve vztahu (5.30) byla zvolena 75 z toho důvodu, že je to primitivní kořen modulo F_4. Abychom se o tom přesvědčili,

použijeme nejprve větu 2.22 (II), (III), (V), větu 2.23 a vztah (4.7),

$$\left(\frac{75}{F_4}\right) = \left(\frac{3}{F_4}\right)\left(\frac{5^2}{F_4}\right) = \left(\frac{3}{F_4}\right) = \left(\frac{F_4}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Z definice Legendrova symbolu nyní vidíme, že 75 je kvadratické nereziduum modulo F_4. Podle Carmichaelovy věty 2.20 dále dostaneme, že 75 je také primitivní kořen modulo F_4, tj. $\mathrm{ord}_{F_4} 75 = F_4 - 1$. (Lze též použít vět 2.25 a 4.16.)

V osmdesátých letech se generátor psedonáhoných čísel (5.30) používal v některých domácích počítačích, např. ZX Spectrum. Jisté slabiny tohoto jednoduchého generátoru se popisují v monografii (Ripley, 1987, s. 40).

Velice se osvědčil následující generátor s mnohem delší periodou

$$s_i \equiv 279470273 s_{i-1} \pmod{p},$$

kde $p = F_5 - 6$ je deseticiferné prvočíslo. Výsledky jsou sice zcela deterministické, ale vypadají velice náhodně.

Na druhé straně jako příklad nevhodné volby konstant uveďme generátor, který se používal v sedmdesátých letech. Tento generátor definovaný vztahem

$$w_i \equiv (2^{16} + 3) w_{i-1} \pmod{2^{31}}$$

a začínající od nějakého lichého čísla dává zdánlivě náhodné výsledky. Později se přišlo na to, že když jím postupně generujeme souřadnice bodů v trojrozměrném prostoru, tyto body leží v 15 rovinách, viz (Knuth, 1997).

Podobným nedostatkům lineárních generátorů tvaru

$$y_{i+1} \equiv b y_i + c \pmod{m}, \quad i = 0, 1, 2, \ldots,$$

lze předejít, použijeme-li kvadratické generátory, viz (Strauch, Porubský, 2005, Sec. 2.25.5), které definují posloupnost pseudonáhodných čísel x_i pomocí vztahu

$$x_i = \frac{y_i}{m},$$

v němž

$$y_{i+1} \equiv a y_i^2 + b y_i + c \pmod{m}, \quad i = 0, 1, 2, \ldots,$$

a kde modul m je prvočíslo nebo mocnina prvočísla, $0 \leq y_i < m$ a y_0, a, b, c jsou vhodně zvolená celá čísla. V (Knuth, 1981, s. 34) jsou uvedeny nutné a postačující podmínky na tyto konstanty tak, aby posloupnost x_i měla největší možnou periodu délky m.

Poznámka. V pracích (Koubková, Pavelka, 1998, s. 97) a (Schroeder, 2006, s. 212) se popisuje, jak lze po telefonu simulovat házení mincí.

Poznámka. Posloupnost pseudonáhodných čísel $(x_i)_{i=1}^{\infty}$ vytvořená uvedenými generátory nabývá po normalizaci hodnot mezi 0 a 1. Nechť $F = F(x)$ je distribuční funkce nějakého pravděpodobnostního rozdělení, $F(x) \to 0$ pro $x \to -\infty$ a $F(x) \to 1$ pro $x \to \infty$. Pokud je F rostoucí, má smysl uvažovat inverzní funkci F^{-1} (např. pro normální Gaussovo rozdělení). Pak $(F^{-1}(x_i))_{i=1}^{\infty}$ je posloupnost psedonáhodných čísel odpovídajících uvažovanému rozdělení pravděpodobnosti.

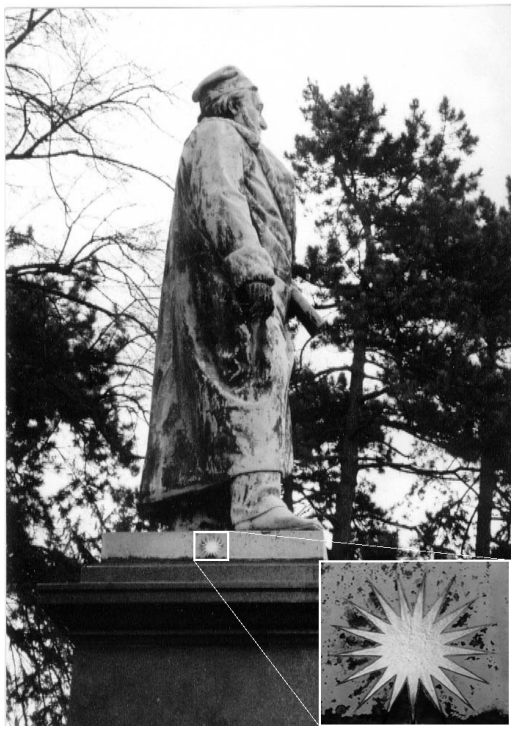
5.6. Eukleidovská konstrukce pravidelných mnohoúhelníků

Již Eukleides věděl, jak lze pomocí pravítka a kružítka konstruovat pravidelné mnohoúhelníky s n vrcholy pro

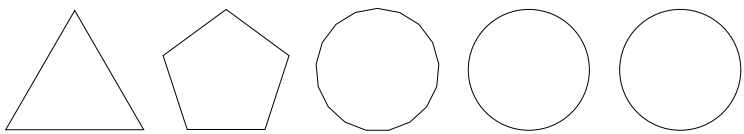
$$n = 2^i 3^j 5^k,$$

kde $n \geq 3$ a $i \geq 0$ jsou celá čísla a j a k jsou 0 nebo 1. Nevěděl však, zda je možné zkonstruovat pravidelný sedmiúhelník či devítiúhelník. Přibližně za dva tisíce let mu na tuto otázku odpověděl (viz Gaussova věta 4.10) Carl Friedrich Gauss. Ten již ve věku necelých devatenácti let napsal krátké pojednání o tom, jak pomocí pravítka a kružítka zkonstruovat pravidelný sedmnáctiúhelník. Gaussův fundamentální objev je znázorněn na podstavci jeho sochy v Braunschweigu (obr. 5.4). Protože však pravidelný sedmnáctiúhelník vypadá téměř jako kružnice (obr. 5.5), je místo něj na Gaussově památníku nakreslena pravidelná sedmnácticípá hvězda.

Gauss v popisu své konstrukce podstatně využil toho, že 17 je Fermatovo prvočíslo. Na obrázku 5.5 jsou zatím známé eukleidovsky konstruovatelné pravidelné mnohoúhelníky s prvočíselným počtem vrcholů.

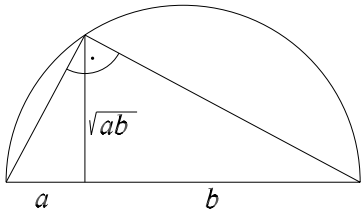


Obr. 5.4. Socha C. F. Gausse v jeho rodném Braunschweigu v Německu. Zlatá sedmnácticípá hvězda je umístěna uprostřed podstavce (detail viz též obr. 4.4).



Obr. 5.5. Rovnostranný trojúhelník a pravidelný pětiúhelník, sedmnáctiúhelník, 257úhelník a 65537úhelník.

V důkazu věty 5.5 uvidíme, jak konstrukce pravidelných mnohoúhelníků souvisí s komplexními čísly. I když je důkaz poněkud delší, k jeho pochopení stačí znát několik trigonometrických identit a umět řešit kvadratické rovnice. Eukleidovské konstrukce jsou obvykle založeny na následující skutečnosti. Jestliže a, b, c jsou délky tří úseček, pak pomocí pravítka a kružítka umíme zkonstruovat úsečky o délkách $a \pm b$, ab/c a $\sqrt{ab}$, a tedy také $\sqrt{a}$ pro $b = 1$. K tomuto účelu se výborně hodí například podobnost trojúhelníků a Eukleidova věta známá z geometrie (obr. 5.6).



Obr. 5.6. Eukleidova věta o výšce v pravoúhlém trojúhelníku.

Tak můžeme zkonstruovat úsečku, jejíž délku lze vyjádřit pomocí konečného počtu druhých odmocnin. Speciálně pro středový úhel pravidelného trojúhelníku, pětiúhelníku a sedmnáctiúhelníku (jejichž počet vrcholů je F_0, F_1 a F_2) dostáváme následující větu.

Věta 5.5. *Platí:*

$$\cos\frac{2\pi}{3} = -\frac{1}{2}, \tag{5.31}$$

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4} \tag{5.32}$$

$$\cos\frac{2\pi}{17} = \frac{1}{16}\Big(-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+ \\ +2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17+\sqrt{17})}}\Big). \tag{5.33}$$

D ů k a z. Kořeny binomické rovnice $z^n - 1 = 0$ v komplexní rovině $\mathbb{C}$ jsou rovnoměrně rozloženy na jednotkové kružnici se

středem v počátku. Podle Základní věty algebry je jich n. Mají tvar (obr. 5.7 pro $n = 17$)

$$z_k = \mathrm{e}^{\mathrm{i}k\alpha} = \cos k\alpha + \mathrm{i}\,\sin k\alpha \quad \text{pro } k = 0, \ldots, n-1, \quad (5.34)$$

kde

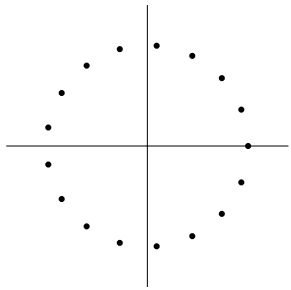
$$\alpha = \frac{2\pi}{n}.$$

Zřejmě $z_0 = 1$ a součet všech kořenů je nula,

$$z_{n-1} + z_{n-2} + \cdots + z_1 + 1 = 0. \quad (5.35)$$

Navíc podle (5.34) pro součet dvou komplexně sdružených kořenů platí

$$z_k + z_{n-k} = 2\cos k\alpha, \quad k = 1, \ldots, n-1. \quad (5.36)$$



Obr. 5.7. Kořeny rovnice $z^n - 1 = 0$ leží na jednotkové kružnici v komplexní rovině $\mathbb{C}$. Obrázek odpovídá případu $n = 17$.

Zvolíme-li nejprve $n = 3$, vidíme z (5.36), že $z_1 + z_2 = 2\cos\alpha$. Odtud a z (5.35) dostáváme (5.31).

Dále nechť $n = 5$. Položíme-li

$$x_1 = z_1 + z_4, \quad (5.37)$$

$$x_2 = z_2 + z_3, \quad (5.38)$$

pak snadno zjistíme, že $x_1 > 0 > x_2$. Odtud a z (5.35) máme

$$x_1 + x_2 = -1. \quad (5.39)$$

Pomocí (5.37), (5.38), (5.36) a vztahu

$$2\cos k\alpha\cos\ell\alpha=\cos(k+\ell)\alpha+\cos(k-\ell)\alpha, \tag{5.40}$$

opět z (5.36) a (5.35) dostaneme

$$x_1x_2=4\cos\alpha\cos 2\alpha=2(\cos 3\alpha+\cos\alpha)=z_3+z_2+z_1+z_4=-1.$$

Odtud a z (5.39) vyplývá, že x_1 a x_2 jsou kořeny kvadratické rovnice

$$x^2+x-1=0,$$

tj.

$$x_1=\frac{-1+\sqrt{5}}{2}. \tag{5.41}$$

Tato rovnost a vztahy (5.37) a (5.36) dávají (5.32).

Konečně nechť $n=17$. Položíme-li

$$x_1=z_1+z_2+z_4+z_8+z_9+z_{13}+z_{15}+z_{16}, \tag{5.42}$$

$$x_2=z_3+z_5+z_6+z_7+z_{10}+z_{11}+z_{12}+z_{14}, \tag{5.43}$$

snadno zjistíme, že $x_1>0>x_2$. Díky rovnosti (5.35) obdržíme

$$x_1+x_2=-1. \tag{5.44}$$

Užitím (5.42), (5.43), (5.36), (5.40), opět (5.36) a (5.35) máme

$$\begin{aligned}
x_1x_2&=4(\cos\alpha+\cos 2\alpha+\cos 4\alpha+\cos 8\alpha)\cdot\\
&\quad\cdot(\cos 3\alpha+\cos 5\alpha+\cos 6\alpha+\cos 7\alpha)\\
&=2(\cos 4\alpha+\cos 2\alpha+\cos 6\alpha+\cos 4\alpha+\cos 7\alpha+\cos 5\alpha+\\
&\quad+\cos 8\alpha+\cos 6\alpha+\cos 5\alpha+\cos\alpha+\cos 7\alpha+\cos 3\alpha+\\
&\quad+\cos 8\alpha+\cos 4\alpha+\cos 9\alpha+\cos 5\alpha+\cos 7\alpha+\cos\alpha+\\
&\quad+\cos 9\alpha+\cos\alpha+\cos 10\alpha+\cos 2\alpha+\cos 11\alpha+\\
&\quad+\cos 3\alpha+\cos 11\alpha+\cos 5\alpha+\cos 13\alpha+\cos 3\alpha+\\
&\quad+\cos 14\alpha+\cos 2\alpha+\cos 15\alpha+\cos\alpha)\\
&=4(z_1+z_2+\cdots+z_{16})=-4.
\end{aligned}$$

Odtud a z (5.44) vyplývá, že x_1 a x_2 jsou kořeny kvadratické rovnice

$$x^2 + x - 4 = 0,$$

tj.

$$x_1 = \frac{-1 + \sqrt{17}}{2}, \quad x_2 = \frac{-1 - \sqrt{17}}{2}.$$

Položíme-li

$$\begin{aligned} y_1 &= 2(\cos\alpha + \cos 4\alpha), \\ y_2 &= 2(\cos 2\alpha + \cos 8\alpha), \\ y_3 &= 2(\cos 3\alpha + \cos 5\alpha), \\ y_4 &= 2(\cos 6\alpha + \cos 7\alpha), \end{aligned}$$

vidíme, že $y_1 > y_2$ a $y_3 > y_4$. Z (5.42) a (5.36) vyplývá, že

$$y_1 + y_2 = x_1.$$

Použijeme-li opět (5.36) a (5.35), dostaneme

$$\begin{aligned} y_1 y_2 &= 4(\cos\alpha + \cos 4\alpha)(\cos 2\alpha + \cos 8\alpha) = 2(\cos 3\alpha + \\ &\quad + \cos\alpha\cos 9\alpha + \cos 7\alpha\cos 6\alpha + \cos 2\alpha\cos 12\alpha + \cos 4\alpha) \\ &= z_3 + z_{14} + z_1 + z_{16} + z_6 + z_{11} + z_2 + z_{15} + z_9 + z_8 + \\ &\quad + z_7 + z_{10} + z_{12} + z_5 + z_4 + z_{13} = -1. \end{aligned}$$

Odtud a ze vztahu $y_1 + y_2 = x_1$ získáme další kvadratickou rovnici

$$y^2 - x_1 y - 1 = 0,$$

tj.

$$\begin{aligned} y_1 &= \frac{x_1 + \sqrt{x_1^2 + 4}}{2} = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{4}, \\ y_2 &= \frac{x_1 - \sqrt{x_1^2 + 4}}{2}. \end{aligned} \tag{5.45}$$

Podobně dostaneme

$$\begin{aligned} y_3 + y_4 &= x_2, \\ y_3 y_4 &= 4(\cos 3\alpha + \cos 5\alpha)(\cos 7\alpha + \cos 6\alpha) = -1. \end{aligned}$$

Tyto vztahy nám opět dávají kvadratickou rovnici pro y_3 a y_4:

$$y^2 - x_2 y - 1 = 0,$$

tj.

$$y_3 = \frac{x_2 + \sqrt{x_2^2 + 4}}{2} = \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4},$$
$$y_4 = \frac{x_2 - \sqrt{x_2^2 + 4}}{2}. \tag{5.46}$$

Zřejmě

$$y_1 = 2\cos\alpha + 2\cos 4\alpha,$$
$$y_3 = 2(\cos 5\alpha + \cos 3\alpha) = 4\cos\alpha\cos 4\alpha,$$

kde poslední rovnost plyne z (5.40). Čili

$$w_1 = 2\cos\alpha \quad \text{a} \quad w_2 = 2\cos 4\alpha$$

($w_1 > w_2$) jsou kořeny kvadratické rovnice

$$w^2 - y_1 w + y_3 = 0.$$

A tedy

$$w_1 = \frac{y_1 + \sqrt{y_1^2 - 4y_3}}{2} = 2\cos\frac{2\pi}{17}.$$

Dosazením z (5.45) a (5.46) dostáváme, že

$$2\cos\frac{2\pi}{17} = -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34 - 2\sqrt{17}}$$
$$+\frac{1}{4}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Tudíž (5.33) platí. □

Poznamenejme, že rozklady (5.42) a (5.43) pocházejí přímo od Gausse, který uspořádal mocniny z^k do periody podle mocnin 3 modulo 17 takto:

$$z_3, z_9, z_{10}, z_{13}, z_5, z_{15}, z_{11}, z_{16}, z_{14}, z_8, z_7, z_4, z_{12}, z_2, z_6, z_1, \tag{5.47}$$

protože

$$3^1 \equiv 3 \pmod{17},\ 3^2 \equiv 9 \pmod{17},\ 3^3 \equiv 10 \pmod{17},\ldots$$
$$3^{14} \equiv 2 \pmod{17},\ 3^{15} \equiv 6 \pmod{17},\ 3^{16} \equiv 1 \pmod{17}.$$

Přitom báze 3 byla zvolena proto, že je to primitivní kořen modulo 17, což umožňuje generovat všechny nenulové zbytky modulo 17, tj. nejmenší řešení kongruence

$$3^j \equiv 1 \pmod{17}$$

pro $j \in \mathbb{N}$ je $j = 17 - 1 = 16$. Pro $j = 1, \ldots, 16$ totiž dostaneme 16 různých zbytků $r_j \in \{1, \ldots, 16\}$ tak, že

$$3^j = 17q_j + r_j$$

pro vhodné celé číslo q_j.

Poznamenejme ještě, že

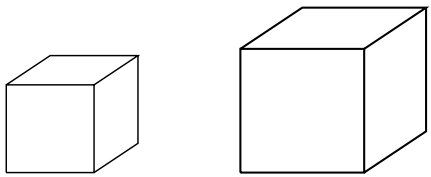
$$z_{r_j} = z_1^{r_j} = z_1^{3^j},$$

a tedy

$$z_{r_{j+1}} = z_1^{3^{j+1}} = \left(z_1^{3^j}\right)^3 = (z_{r_j})^3.$$

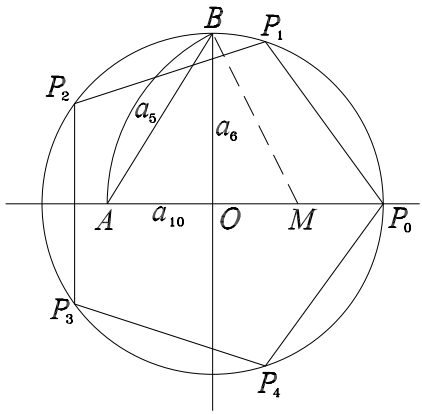
Tudíž v posloupnosti komplexních kořenů (5.47) je každý z nich třetí mocninou předcházejícího kořene. Členy z rozkladů (5.42) a (5.43) se objevují na sudých, popř. lichých, pozicích posloupnosti (5.47).

Sám Gauss v knize (Gauss, 1986) prohlásil, že rozložení primitivních kořenů je hluboké mystérium (srov. tab. 8 na str. 344). Jejich rozložení pro Fermatova prvočísla je dáno větou 4.16.



Obr. 5.8. Pro danou krychli nelze zkonstruovat pomocí kružítka a pravítka hranu krychle s dvojnásobným objemem.

Pro danou úsečku, jejíž délka je a, obecně není možné najít eukleidovskou konstrukci úsečky délky $\sqrt[k]{a}$, pokud k není mocninou 2. Poznamenejme, že již staří Řekové se marně pokoušeli zkonstruovat úsečku délky $\sqrt[3]{2}$ (tzv. problém zdvojení krychle – viz obr. 5.8). Nemožnost takové konstrukce je dokázána například v monografii (Kořínek, 1956, kap. 52,6).



Obr. 5.9. Při eukleidovské konstrukci pravidelného pětiúhelníku se sestrojuje pravoúhlý trojúhelník *ABO* tak, aby $|BM| = |AM|$, kde *M* je střed úsečky OP_0. Pak $a_5 = |AB|$, $a_6 = |BO|$ a $a_{10} = |AO|$ jsou postupně strany pravidelného pětiúhelníku, šestiúhelníku a desetiúhelníku.

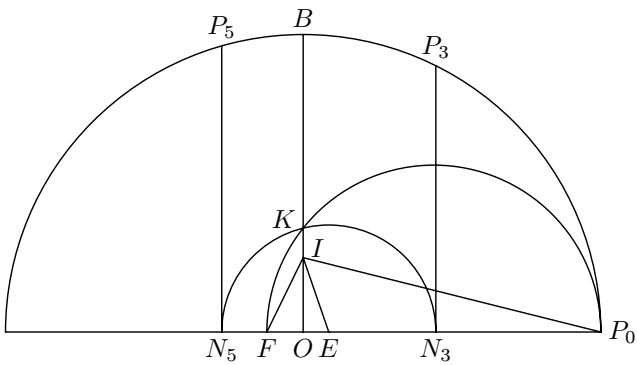
Praktické provedení konstrukce pravidelného pětiúhelníku je popsáno například v knížkách (Fabián, 2005), (Šofr, 1976) a na obr. 5.9. Navíc je známo, že délka strany pravidelného pětiúhelníku a_5 je větší částí jeho úhlopříčky rozdělené *zlatým řezem,* tj.

$$\frac{d}{a_5} = \frac{a_5}{d - a_5} = \frac{1 + \sqrt{5}}{2} = 1.6180339887\ldots,$$

kde d označuje délku úhlopříčky (srov. (5.32)).

Popišme si ještě eukleidovskou konstrukci pravidelného sedmnáctiúhelníku z článku (Richmond, 1909). Označme $P_0, P_1, \ldots, P_{16}$ jeho neznámé vrcholy na kružnici se středem v O. Nechť P_0 je

dáno (obr. 5.10). Budeme konstruovat pouze P_3 odpovídající úhlu $6\pi/17$, popř. P_5 náležející $10\pi/17$, protože pak snadno sestrojíme ostatní vrcholy. (Přitom zde nebudeme přímo používat vztah (5.33) pro $\alpha = 2\pi/17$, protože nebudeme konstruovat bod P_1.) Nechť B je koncový bod poloměru, který je kolmý na OP_0. Zkonstruujeme bod I úsečky OB tak, že $|OI| = \frac{1}{4}|OB|$. Dále nalezneme bod E na úsečce OP_0 tak, aby $|\sphericalangle OIE| = \frac{1}{4}|\sphericalangle OIP_0|$. Na polopřímce opačné k OP_0 sestrojíme bod F takový, že $|\sphericalangle FIE| = \frac{1}{4}\pi$. Nyní označíme K průnik úsečky OB a kružnice o průměru FP_0. Další kružnice se středem E a poloměrem $|EK|$ protíná přímku OP_0 v bodech N_3 (mezi body O a P_0) a N_5. To jsou ortogonální projekce vrcholů P_3 a P_5 na přímku OP_0.



Obr. 5.10. Eukleidovská konstrukce pravidelného sedmnáctiúhelníku.

Původní eukleidovská konstrukce pravidelného 257úhelníku se uvádí na více než osmdesáti stránkách v (Richelot, 1832). Mnohem kratší analýza tohoto problému je podána v (Gottlieb, 1999). Zde je též zmínka o konstrukci pravidelného 65537úhelníku.

Odpověď na otázku, jak konstruovat další pravidelné n-úhelníky, se opírá o věty 5.6 a 5.7. Následující věta 5.6 je vlastně speciálním případem věty 1.3. Dokážeme ji ale poněkud jednodušším způsobem.

Věta 5.6. *Nechť $p \geq 2$ a $q \geq 2$ jsou nesoudělná přirozená čísla. Pak existují přirozená čísla x a y tak, že*

$$px - qy = 1.$$

D ů k a z. Pro každé $k = 1, \ldots, q-1$ definujme $r_k \in \{1, \ldots, q-1\}$ pomocí kongruence

$$pk \equiv r_k \pmod{q},$$

tj. q dělí rozdíl $pk - r_k$. Sporem snadno zjistíme, že všechna r_k jsou vzájemně různá. Čili kongruence

$$px \equiv 1 \pmod{q} \tag{5.48}$$

má právě jedno řešení x v množině $\{1, \ldots, q-1\}$. Tudíž existuje přirozené číslo y takové, že $px - 1 = qy$. □

Věta 5.7. *Nechť $n = pq$, kde $p \geq 2$ a $q \geq 2$ jsou nesoudělná přirozená čísla. Pak existuje eukleidovská konstrukce kořenů rovnice $z^n - 1 = 0$ tehdy a jen tehdy, když existuje eukleidovská konstrukce kořenů rovnic $z^p - 1 = 0$ a $z^q - 1 = 0$.*

D ů k a z. Nechť $p \geq 2$ a $q \geq 2$ jsou nesoudělná. Pak podle věty 5.6 existují přirozená čísla x, y, pro něž $xp - yq = 1$. Odtud plyne, že

$$\frac{x}{q} - \frac{y}{p} = \frac{1}{pq},$$

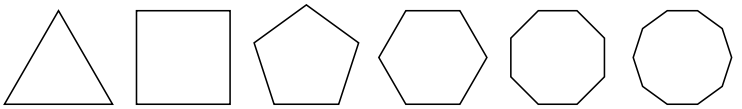
tj. jestliže umíme zkonstruovat části $\frac{1}{q}$ a $\frac{1}{p}$ plného úhlu 2π, pak také umíme zkonstruovat jeho část $\frac{1}{pq}$.

Opačná implikace je triviální. □

Příklad. Nechť $p = 5$ a $q = 3$. Pak z (5.17) snadno zjistíme, že $x = 2, y = 3$ a $2/3 - 3/5 = 1/15$. Tudíž umíme zkonstruovat jednu patnáctinu plného úhlu 2π, a tedy i pravidelný patnáctiúhelník.

Poznámka. Protože jakýkoliv kruhový oblouk lze pomocí pravítka a kružítka rozdělit na dva stejné díly, lze jej rozdělit i na

$2, 4, 8, \ldots, 2^i$ stejných dílů. Pokud tedy umíme zkonstruovat pravidelný n-úhelník, umíme zkonstruovat i pravidelný $2^i n$-úhelník.



Obr. 5.11. Všechny eukleidovsky konstruovatelné pravidelné mnohoúhelníky pro $n \leq 10$.

Starý geometrický problém konstrukce pravidelných mnohoúhelníků se tak transformuje na algebraický problém. Pravidelný n-úhelník pro $n < 100$ může být zkonstruován pomocí pravítka a kružítka tehdy a jen tehdy, když $n = 3$, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96. I když jsou dnes známy stovky netriviálních dělitelů Fermatových čísel, stále neumíme stanovit nějaký obecný princip, který by dal definitivní odpověď na otázku, zda je F_4 největší Fermatovo prvočíslo. Dosud tedy nevíme, zda je současný seznam eukleidovsky konstruovatelných mnohoúhelníků již kompletní.

5.7. Poselství mimozemským civilizacím

Roku 1974 bylo z největšího radioteleskopu světa Arecibo o průměru 305 m nacházejícího se na Portoriku vysláno ke kulové hvězdokupě M13 v souhvězdí Herkula poselství mimozemským civilizacím. Tehdy se předpokládalo, že v tomto obrovském množství milionů hvězd by mohla existovat na nějaké exoplanetě vyspělá civilizace. Podle dnešních dnešních poznatků je však existence takové civilizace velice nepravděpodobná, neboť v kulových hvězdokupách nejsou rozšířeny těžší prvky a případné exoplanety mají nestabilní dráhy.

Poselství bylo ve dvojkové soustavě (místo nul a jedniček byly vysílány krátké signály na dvou různých blízkých kmitočtech) a

obsahovalo právě 1679 bitů. Pokud zprávu zachytí nějaká dostatečně vyspělá civilizace, pak se předpokládá, že zná Základní větu aritmetiky 2.2 a rozloží si číslo 1679 na součin dvou prvočísel

$$1679 = 73 \times 23.$$

To umožňuje vytvořit obdélníkový obrázek sestavený ze čtverečků (obr. 5.12), který má výrazné uspořádání, tj. má nízkou entropii. Bílý čtvereček přitom odpovídá 0 a černý čtvereček 1 vyslané zprávy. Pokud bychom sestavili jednotlivé bity do podélného obdélníku 23×73, dostaneme obrázek, viz (Mišoň, 1975, s. 335) s vysokou entropií, který připomíná spíše rozsypaný čaj. Proto se také uvažovalo o poselství, jehož délka by se rovnala nějakému čtvercovému číslu, tj. kdy by na pořadí činitelů nezáleželo.

Při sestavování jednotlivých bitů do obdélníku na výšku 73×23 můžeme postupovat několika způsoby. Na obr. 5.12 je nakreslen jeden ze způsobů, kdy je třeba číst poselství zprava doleva, jako čtou Arabové. (Bity lze uspořádat i do zrcadlového obrazu, a pak by se poselství četlo odleva doprava, což je zase běžné pro nás.)

Na prvních třech řádcích obrázku 5.12 jsou zapsána čísla 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ve dvojkové soustavě. Nápadným se jeví obsazení políčka ve čtvrtém řádku pod každým číslem, které označuje jakési návěští (např. desetinnou tečku), odkud se má číslo číst. Autoři označují tuto část poselství jako úvodní lekci.

Další skupina znaků na řádcích 6 až 10 nám tak určuje pět čísel

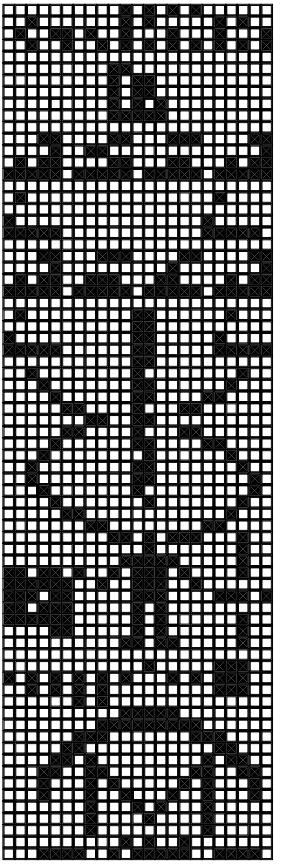
$$1, 6, 7, 8, 15,$$

která odpovídají atomovým číslům biogenních prvků

$$\mathrm{H, C, N, O, P.}$$

Na dalších řádcích jsou zakódovány složky kyseliny DNA (podrobnosti viz (Mišoň, 1975)). Samotná struktura dvojité šroubovice DNA je znázorněna zhruba uprostřed obrázku. Mezi oběma vlákny je informace o počtu nukleotidů v DNA. Pod ní nalezneme siluetu člověka, a pak Slunce s devíti planetami (tehdy ještě s Plutem), přičemž Země je pro zvýraznění posunuta o jeden řádek blíže k člověku. Obří planety Jupiter a Saturn jsou vyznačeny třemi černými čtverečky, Uran a Neptun dvěma čtverečky.

Obr. 5.12. Poselství mimozemským civilizacím.



V dolní části obrázku je znázorněn radioteleskop, z nějž bylo poselství vysláno. Paprsky směřující od ohniska jsou po odrazu od anténního zrcadla rovnoběžné. Na posledních dvou řádcích je zakódován přibližný průměr zrcadla, vyjádřený ve vlnové délce 12.6 cm vysílaného signálu. Autoři tohoto poselství tehdy pracovali v National Astronomy and Ionosphere Center.

V knize (Delahaye, 2000, s. 106) se uvádí podobné poselství obsahující $31 \times 41 = 1271$ bitů. Od roku 1974 bylo vysláno ještě několik dalších mnohem komplikovanějších poselství, která se ale vždy opírala o teorii čísel.

5.8. Fermatova transformace

Fermatova prvočísla F_m mají zajímavé použití při digitálním zpracování signálů. Nechť $\alpha \in \{2, 3, \ldots, F_m - 1\}$ je dáno a nechť N je zvoleno tak, že N dělí řád $e = \mathrm{ord}_{F_m}\alpha$, tj. nejmenší exponent, pro který $\alpha^e \equiv 1 \pmod{F_m}$.

Číslo N se nazývá *délka transformace* a $\mathrm{ord}_{F_m}\alpha$ *maximální délka transformace*. Například pro $m \geq 1$ a $\alpha = 3$ je maximální délka transformace rovna 2^{2^m}, jak plyne z Pépinova testu (věta 4.11). Jestliže $\alpha = 2$, pak je $\mathrm{ord}_{F_m}\alpha = 2^{m+1}$ pro $m = 0, 1, \ldots$.

Fermatova transformace pro rychlé zpracování digitálních signálů byla poprvé navržena v (Schönhage, Strassen, 1971). Digitální signál je reprezentován vektorem $x = (x(0), x(1), \ldots, x(N-1))$ celých čísel takových, že $x(k) \in \{0, 1, \ldots, F_m - 1\}$ pro $k = 0, 1, \ldots, N-1$. Jednorozměrná *Fermatova transformace* a její inverze jsou pak dány vztahy

$$\begin{aligned} X(j) &\equiv \sum_{k=0}^{N-1} x(k)\alpha^{jk} \pmod{F_m}, \qquad j = 0, 1, \ldots, N-1, \\ x(k) &\equiv N^- \sum_{j=0}^{N-1} X(j)\alpha^{-jk} \pmod{F_m}, \quad k = 0, 1, \ldots, N-1, \end{aligned} \tag{5.49}$$

kde $X(j) \in \{0, 1, \ldots, F_m - 1\}$ pro všechna $j \in \{0, 1, \ldots, N-1\}$ a $N^- \in \mathbb{N}$ označuje inverzní prvek, pro nějž $NN^- \equiv 1 \pmod{F_m}$.

Fourierova a Laplaceova transformace jsou definovány pro spojité signály, viz (Koukal, Křížek, Potůček, 2002, kap. 4), které musí být pro počítačovou implementaci nejprve diskretizovány. Pro porovnání s (5.49) připomeňme, že *diskrétní Fourierova transformace* a její inverze jsou dány v komplexním oboru vztahy

$$\begin{aligned} Y(j) &= \sum_{k=0}^{N-1} y(k)\,\mathrm{e}^{-2\pi\mathrm{i}jk/N}, \qquad j = 0, 1, \ldots, N-1, \\ y(k) &= N^{-1} \sum_{j=0}^{N-1} Y(j)\,\mathrm{e}^{2\pi\mathrm{i}jk/N}, \quad k = 0, 1, \ldots, N-1. \end{aligned}$$

Diskrétní Fourierova transformace vyžaduje N^2 násobení komplexních čísel. Poznamenejme ale, že počet násobení lze značně zredukovat na $\mathcal{O}(N \log N)$, pokud N je mocnina 2 (viz tzv. rychlá Fourierova transformace zavedená v (Cooley, Tukey, 1965)). Naproti tomu Fermatova transformace a její inverze vyžaduje provedení pouze $\mathcal{O}(N \log N)$ sčítání, odečítání, posunů o bit, ale žádné násobení. V počítačové aritmetice modulo F_m lze totiž převést příslušná násobení jen na „bitové“ posuny, viz (Agarwal, Burrus, 1973).

Fermatova transformace umožňuje jednoduše počítat konvoluce digitálních signálů, viz (Schönhage, Strassen, 1971), pomocí podobných vztahů jako pro diskrétní Fourierovu transformaci. Důležité však je, že nedochází k žádným zaokrouhlovacím chybám, protože se výpočet odehrává v celočíselné aritmetice.

Pro výpočet Fermatovy transformace (5.49) se používá binární aritmetika modulo F_m. V (Křížek, Luca, Somer, 2001) je podrobně popsáno, jak efektivně provádět základní operace v této aritmetice.

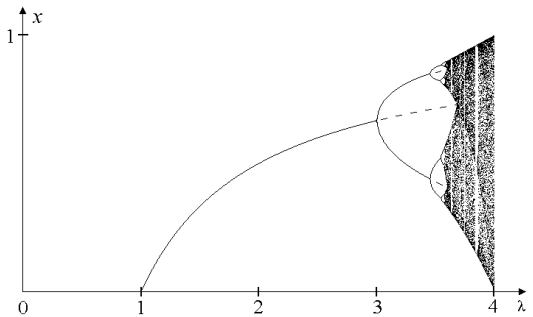
V roce 1978 Reed, Truong a Welch publikovali efektivní algoritmus pro rychlé dekódování Reedových–Solomonových kódů pomocí Fermatovy transformace – (Reed, Truong, Welch, 1978). Poznamenejme například, že kompaktní disky CD jsou chráněny proti drobnému poškrábání pomocí známých Reedových–Solomonových samoopravných kódů, které umožňují dodatečně vypočítat ztracenou informaci, viz (Rao, Fujiwara, 1989).

5.9. Jak spolu souvisí chaos, fraktály a teorie čísel

V tomto oddílu se zmíníme o překvapivé souvislosti Mersennových a Fermatových čísel s logistickou rovnicí, která způsobila bouřlivý rozvoj teorie chaosu a fraktálů. V sedmdesátých letech M. J. Feigenbaum řešil iteračně na běžné kapesní kalkulačce tzv. *logistickou rovnici*, viz (Feigenbaum, 1978)

$$x_{n+1} = \lambda x_n(1 - x_n), \quad n = 1, 2, \ldots, \tag{5.50}$$

jež popisuje například evoluci dynamického biologického systému. Lineární člen λx_n charakterizuje růst jisté populace, zatímco kvadratický člen $(-\lambda x_n^2)$ reprezentuje její úbytek v důsledku nějakého procesu. Pro pevný parametr λ a zadanou počáteční hodnotu $x_1 \in \langle 0, 1\rangle$ může mít posloupnost (x_n) různý počet hromadných bodů.



Obr. 5.13. Feigenbaumova cesta k chaosu. Pro vzrůstající hodnotu řídicího parametru $\lambda \in \langle 0, 4\rangle$ obrázek ilustruje množinu odpovídajících hromadných bodů všech posloupností (x_n) pro všechny počáteční hodnoty $x_1 \in \langle 0, 1\rangle$.

Z obr. 5.13 je patrné, že chování i poměrně jednoduchého nelineárního matematického modelu (5.50) může být velice komplikované pro měnící se λ a příslušné hromadné body posloupnosti (x_n) mohou mít značně komplikovanou strukturu s množstvím bifurkací (tj. rozvětvení). První z nich je v bodě $\lambda_1 = 1$. Odpovídající „větev řešení" je dána funkcí $f(\lambda) = 1 - \lambda^{-1}$ pro $\lambda \in \langle 1, 4\rangle$, která popisuje stabilní rovnovážný stav až do druhého bifurkačního bodu $\lambda_2 = 3$. Další bifurkační body jsou v $\lambda_3 \approx 3.44949$, $\lambda_4 \approx 3.54409$ atd. V nich dochází k tzv. „zdvojování period", o němž se zmíníme později.

Pro $\lambda > \lambda_2$ existuje konstantní (ale nestabilní) řešení s počáteční podmínkou $x_1 = x_1(\lambda)$ ležící na grafu funkce f, např. $x_n = 0.7$ pro všechna přirozená n a $\lambda = \dfrac{10}{3}$. Podobně pro $\lambda > \lambda_3$ existují

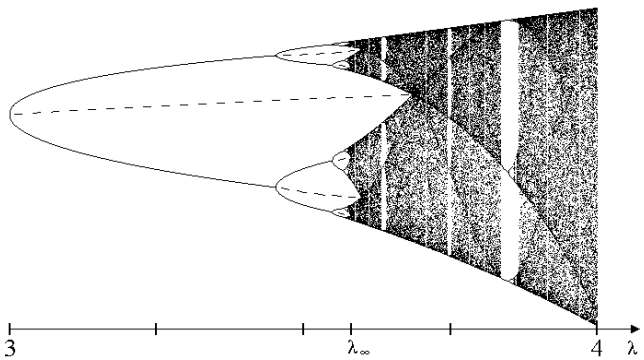
další nestabilní řešení. Například $x_n = \frac{6}{7}$ pro n liché, $x_n = \frac{3}{7}$ pro n sudé a $\lambda = \frac{7}{2}$. Tato nestabilní řešení jsou znázorněna v obr. 5.13 přerušovanou čarou.

Jestliže počáteční hodnota $x_1 \in (0, 1\rangle$ neleží na grafu funkce f, dostaneme 2 hromadné body pro $\lambda \in (\lambda_2, \lambda_3\rangle$. Podobně hodnotě $\lambda \in (\lambda_3, \lambda_4\rangle$ obecně odpovídají 4 hromadné body atd. Jak uvidíme později, tyto hromadné body budou generovat nekonstantní periodická řešení. Zvolíme-li například $\lambda \in (\lambda_2, \lambda_3\rangle$ a počáteční hodnotu x_1 na horní nebo dolní větvi, bude odpovídající posloupnost (x_n) oscilovat mezi těmito dvěma hodnotami.

Feigenbaum objevil jednu velice překvapivou vlastnost posloupnosti λ_j. Zjistil totiž, že

$$\delta = \lim_{j\to\infty} \frac{\lambda_j - \lambda_{j-1}}{\lambda_{j+1} - \lambda_j} = 4.669201609102990671853203820 47\ldots,$$

tj. vzdálenosti $\lambda_{j+1} - \lambda_j$ tvoří téměř geometrickou posloupnost. Limita δ se nazývá *Feigenbaumova konstanta* (*Feigenbaumovo číslo*) a opakující se zdvojování period v bodech $\lambda_1, \lambda_2, \lambda_3, \ldots$ se nazývá *Feigenbaumovy kaskády.*



Obr. 5.14. Při bližším pohledu na Feigenbaumův přechod k chaosu dynamického systému (5.50) pro $\lambda \in \langle 3, 4\rangle$ jsou zřetelně patrná tzv. okna za bodem λ_∞.

Pro λ přesahující hodnotu $\lambda_\infty = \lim_{n\to\infty} \lambda_n \approx 3.5699456$, vidíme velice chaotické chování, ale též oblasti s konečně mnoha hromadnými body (viz obrázky 5.13 a 5.14). To znamená, že pro určité hodnoty parametru $\lambda \in \langle \lambda_\infty, 4\rangle$ se objevují tzv. okna, kde se chaotické chování hromadných bodů posloupností (x_n) mění na pravidelné.

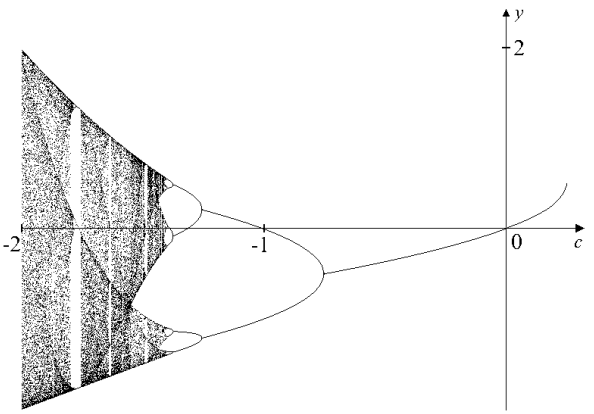
Pomocí jednoduché transformace

$$x_n = \frac{1}{2} - \frac{y_n}{\lambda} \tag{5.51}$$

lze logistickou rovnici (5.50) přepsat do kanonického tvaru (srov. obr. 5.15)

$$y_{n+1} = y_n^2 + c, \tag{5.52}$$

kde $c = \lambda/2 - \lambda^2/4$.



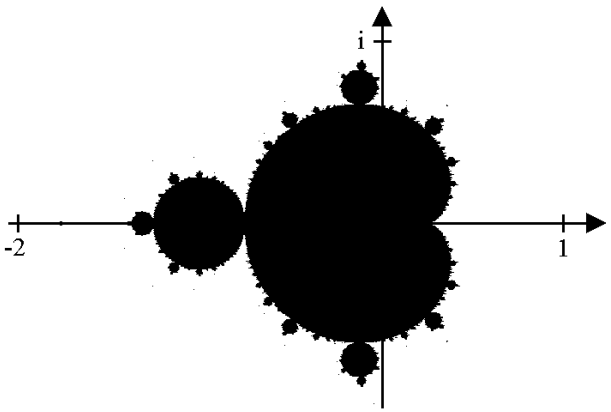
Obr. 5.15. Množina hromadných bodů posloupností (y_n) s počáteční podmínkou $y_1 = 0$, když parametr c probíhá interval $\langle -2, 0.25\rangle$. Nestabilní řešení nejsou znázorněna.

Rovnici (5.52) je výhodné vyšetřovat v komplexní rovině $\mathbb{C}$, tj. $c, y_n \in \mathbb{C}$. Poznamenejme, že některé fraktální objekty v komplexní rovině jsou popsány pomocí stejné rovnice jako chaos v reálné proměnné. Označme závislost posloupnosti (5.52) na parametru

c obvyklým způsobem: $y_n = y_n(c)$. Pak *Mandelbrotova množina* $\mathcal{M}$ je množina všech parametrů $c \in \mathbb{C}$, pro něž je posloupnost $\{y_n(c)\}_{n=1}^{\infty}$ s počáteční podmínku $y_1(c) = 0$ ohraničená, tj.

$$\mathcal{M} = \{c \in \mathbb{C};\ \exists C > 0\ \forall n \in \{1, 2, \ldots\} : |y_n(c)| \leq C \ \text{ a } \ y_1(c) = 0\}$$

(obr. 5.16). Pokud každému bodu $c \in \mathbb{C} \setminus \mathcal{M}$ přiřadíme jistý barevný odstín podle „rychlosti divergence" posloupnosti $(y_n(c))_{n=1}^{\infty}$, získáme tak známé barevné obrázky okolí Mandelbrotovy množiny (viz např. obr. III). Tento postup později vedl ke vzniku nového oboru *počítačové výtvarné tvorby* (angl. *computer painting*).



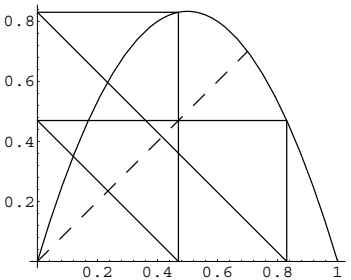
Obr. 5.16. Mandelbrotova množina všech komplexních čísel c, pro něž je posloupnost $y_1(c) = 0$, $y_2(c)$, $y_3(c)$,..., definovaná vztahem (5.52), ohraničená.

Řešení $(y_n)_{n=1}^{\infty}$ rovnice (5.52) se nazývá *periodické*, jestliže existuje přirozené číslo p tak, že $y_{n+p} = y_n$ pro všechna přirozená čísla n a $y_{n+r} \neq y_n$ pro všechna $r \in \{1, \ldots, p-1\}$. Číslo p se pak nazývá *minimální perioda* a jakýkoliv její přirozený násobek *perioda.* Ostatní řešení se nazývají *neperiodická.*

Podobně se definují i periodická a neperiodická řešení logistické rovnice (5.50). Například již zmíněné řešení $x_n = 0.7$ pro všechna přirozená n a $\lambda = \dfrac{10}{3}$ má periodu $p = 1$, protože $x_{n+1} = x_n$ (viz

průnik čárkované přímky s grafem paraboly $f(x) = \frac{10}{3}x(1-x)$ na obr. 5.17).

Pro $\lambda \geq \lambda_\infty$ vidíme, že existují malé periody, které nejsou mocninami 2 v oblastech nazývaných okna. Například $p = 3$ pro $\lambda = 3.83$, $p = 5$ pro $\lambda = 3.74$ nebo $p = 7$ pro $\lambda = 3.702$ (obr. 5.13).



Obr. 5.17. Geometrická interpretace periodických řešení rovnice (5.50) s minimální periodou $p = 2$ pro $\lambda = \frac{10}{3}$ a $x_1 = \left(13 - \sqrt{13}\right)/20 \approx 0.4697224$, $x_2 = \left(13 + \sqrt{13}\right)/20 \approx 0.8302776$, $x_3 = x_1$, $x_4 = x_2$ atd. Začneme-li v bodě x_1, pak odpovídající hodnota je $x_2 = f(x_1)$ a $x_3 = f(x_2) = x_1$.

Obrázek IV barevné přílohy ukazuje vztah mezi Mandelbrotovou množinou $\mathcal{M}$ a chaotickým chováním dynamického systému (5.52) pro $c \in \langle -2, 0.25 \rangle$. Vznikl kombinací obrázků 5.15 a 5.16. Z něj je patrná souvislost mezi $\mathcal{M}$ a bifurkačními větvemi řešení rovnice (5.52). Rovina, v níž je znázorněn bifurkační diagram z obrázku 5.15, prochází reálnou osou a je kolmá na komplexní rovinu obsahující $\mathcal{M}$. Kruhové podoblasti Mandelbrotovy množiny rozmístěné podél reálné osy odpovídají jednotlivým bifurkačním větvím. Okna příslušející periodám 3, 5, 7 apod., blíže viz (Křížek, Šolcová, 2005), odpovídají malým „kopiím“ $\mathcal{M}$, které jsou částí fraktální množiny $\mathcal{M}$.

Vyšetřujme nejprve nejjednodušší případ rovnice (5.52) pro $c = 0$, tj.

$$y_{n+1} = y_n^2 . \tag{5.53}$$

Zvolíme-li $y_1 = a \in \mathbb{C}$ libovolně, pak $y_2 = a^2$, $y_3 = a^4$ atd. Vidíme tedy, že všechna řešení (periodická i neperiodická) rovnice (5.53) mají tvar

$$y_n = a^{2^{n-1}}, \quad a \in \mathbb{C}.$$

Každé periodické řešení rovnice (5.52) je samozřejmě ohraničené. Všechna řešení rovnice (5.53) s periodou p (ale i periodou q, která dělí p) splňují rovnici

$$y^{2^p} - y = 0, \tag{5.54}$$

jež má zřejmě triviální řešení $y_n = 0$. Abychom určili ostatní (netriviální) periodická řešení, zavedeme si nejprve tzv. cyklotomické polynomy.

Jestliže $k \geq 1$ a $\zeta = \mathrm{e}^{2\pi \mathrm{i}/k}$ (tj. ζ je k-tým primitivním kořenem jedničky), pak *k-tý cyklotomický polynom* Φ_k je definován vztahem

$$\Phi_k(y) = \prod_{\substack{j=1 \\ (j,k)=1}}^{k} \left(y - \zeta^j\right).$$

Přímým výpočtem se lze přesvědčit, že

$$\begin{aligned}
&\Phi_1(y) = y - 1, && \Phi_2(y) = y + 1,\\
&\Phi_3(y) = y^2 + y + 1, && \Phi_4(y) = y^2 + 1,\\
&\Phi_5(y) = y^4 + y^3 + y^2 + y + 1, && \Phi_6(y) = y^2 - y + 1,\\
&\Phi_7(y) = y^6 + y^5 + y^4 + y^3 + y^2 + y + 1, && \Phi_8(y) = y^4 + 1,\\
&\Phi_9(y) = y^6 + y^3 + 1, && \Phi_{10}(y) = y^4 - y^3 + y^2 - y + 1.
\end{aligned}$$

Stupeň cyklotomického polynomu Φ_k je roven hodnotě Eulerovy funkce $\varphi(k)$. Navíc pro cyklotomické polynomy a $n \in \mathbb{N}$ platí vztah, viz např. (Křížek, Luca Somer, 2001, s. 150),

$$y^n - 1 = \prod_{d|n} \Phi_d(y). \tag{5.55}$$

Například pro $n = 17$ platí (obr. 5.7)

$$y^{17} - 1 = \Phi_1(y)\,\Phi_{17}(y) = (y-1)(y^{16} + y^{15} + \cdots + 1).$$

Ze vztahu (5.55) plyne, že netriviální periodická řešení rovnice (5.54) leží na jednotkové kružnici a splňují rovnici

$$y^{2^p-1} - 1 = \prod_{d|(2^p-1)} \Phi_d(y) = 0. \tag{5.56}$$

Všechna periodická řešení (5.53) s periodou $p = 1$ jsou tudíž dána rovnicemi $\Phi_0(y) \equiv y = 0$ a $\Phi_1(y) = 0$. Všechna periodická řešení s minimální periodou $p > 1$ jsou dána rovnicemi $\Phi_d(y) = 0$, kde podle (Antonyuk, Stanyukovich, 1990a) platí (srov. příklad na konci tohoto oddílu)

$$d \parallel \left(2^p - 1\right) \quad \text{a} \quad d \nmid \left(2^q - 1\right) \ \text{ pro } q \mid p \text{ takové, že } 1 < q < p. \tag{5.57}$$

Při tzv. zdvojování period se vyšetřují všechna periodická řešení s periodou $p = 2^m$, $m = 0, 1, 2, \ldots$ (nebo periodou q, která dělí p). Ta jsou definována rovnicí

$$y^{2^{2^m}} - y = 0.$$

Vyloučíme-li triviální řešení $y_n = 0$, dostaneme

$$y^{2^{2^m}-1} - 1 = 0. \tag{5.58}$$

Periodická řešení splňující (5.58) zřejmě musí ležet na jednotkové kružnici v komplexní rovině.

Věta 5.8. *Periodické řešení rovnice* (5.53) *s minimální periodou p je dáno právě jednou rovnicí pro cyklotomický polynom*

$$\Phi_{M_p}(y) \equiv y^{M_p-1} + y^{M_p-2} + \cdots + y + 1 = 0 \tag{5.59}$$

tehdy a jen tehdy, když M_p je Mersennovo prvočíslo.

Dříve než větu 5.8 dokážeme, uvedeme jednoduchý příklad.

Příklad. Jestliže $p = 3$, pak $M_3 = 7$ a $\Phi_7(y) = y^6 + y^5 + \cdots + y + 1 = 0$. Pro

$$y_n = \cos\frac{2^n\pi}{7} + \mathrm{i}\sin\frac{2^n\pi}{7}, \quad n = 1, 2, \ldots,$$

dostaneme pomocí (5.53), že $y_4 = y_1$, $y_5 = y_2$ atd., což potvrzuje, že perioda je 3.

Důkaz věty 5.8. Je-li $M_p = 2^p - 1$ prvočíslo, pak podle věty 4.1 je také p prvočíslem. Pouze $d = 1$ a $d = 2^p - 1$ dělí $2^p - 1$, a tudíž ze vztahu (5.56) plyne, že

$$y^{2^p-1} - 1 = \Phi_1(y)\,\Phi_{M_p}(y) = 0.$$

Periodické řešení rovnice (5.53) je identická nula, nebo musí jeho hodnoty ležet na jednotkové kružnici v komplexní rovině. Stacionární posloupnost $y_n = 1$ odpovídající rovnici $\Phi_1(y) = y - 1 = 0$ zřejmě nemá minimální periodu p. Proto položíme

$$y_n = \cos\frac{2^n\pi}{M_p} + \mathrm{i}\sin\frac{2^n\pi}{M_p}, \quad n \in \mathbb{N}. \tag{5.60}$$

Pak podle (5.60) pro libovolné přirozené číslo r platí

$$\begin{aligned} y_{p+r} &= \cos\frac{2^{p+r}\pi}{2^p-1} + \mathrm{i}\sin\frac{2^{p+r}\pi}{2^p-1} \\ &= \cos\frac{2^r(2^p-1)\pi + 2^r\pi}{2^p-1} + \mathrm{i}\sin\frac{2^r(2^p-1)\pi + 2^r\pi}{2^p-1} \\ &= \cos\frac{2^r\pi}{2^p-1} + \mathrm{i}\sin\frac{2^r\pi}{2^p-1} = y_r. \end{aligned}$$

Vidíme tedy, že $y_{p+r} = y_r$, tj. posloupnost (y_n) má periodu p. Tato posloupnost je definována jedinou rovnicí (5.59).

Nechť obráceně M_p je číslo složené, tj. $M_p = d_1 d_2$ pro $d_1 > 1$ a $d_2 > 1$. Všechna periodická řešení s periodou $p > 1$ jsou dána vztahem (5.56), tj. rovnicemi $\Phi_d(y) = 0$ pro $d \mid M_p$. Musíme ukázat, že kromě rovnice (5.59) existují ještě další rovnice, které dávají periodu p. Je-li p prvočíslo, pak jistě neexistuje q splňující (5.57) a rovnice $\Phi_{d_1}(y) = 0$ a $\Phi_{d_2}(y) = 0$ tudíž také dávají řešení s periodou p. Je-li $p = qk$ pro $q > 1$ a $k > 1$, pak druhý činitel

na pravé straně rovnosti (4.1) (pro $q = i$) není tvaru $2^q - 1$. Označíme-li jej d_2, pak $\Phi_{d_2}(y) = 0$ je další rovnicí, která opět dává řešení s periodou p, neboť (5.57) platí. □

Příklad. Užijeme-li prvočíselné rozklady čísla $2^p - 1$ pro $p \leq 9$ a vztah (5.57), pak odpovídající periodická řešení lze vyjádřit pomocí rovnic

$$\begin{aligned}
&p = 1, \quad \Phi_0(y) = 0, \quad \Phi_1(y) = 0,\\
&p = 2, \quad \Phi_3(y) = 0,\\
&p = 3, \quad \Phi_7(y) = 0,\\
&p = 4, \quad \Phi_5(y) = 0, \quad \Phi_{15}(y) = 0,\\
&p = 5, \quad \Phi_{31}(y) = 0,\\
&p = 6, \quad \Phi_9(y) = 0, \quad \Phi_{21}(y) = 0, \quad \Phi_{63}(y) = 0,\\
&p = 7, \quad \Phi_{127}(y) = 0,\\
&p = 8, \quad \Phi_{17}(y) = 0, \quad \Phi_{51}(y) = 0, \quad \Phi_{85}(y) = 0, \quad \Phi_{255}(y) = 0,\\
&p = 9, \quad \Phi_{73}(y) = 0, \quad \Phi_{511}(y) = 0.
\end{aligned}$$

Periody $p = 2, 3, 5, 7$ tedy odpovídají cyklotomickým polynomům prvních čtyř Mersennových prvočísel $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ a $M_7 = 127$. Naproti tomu periodu $p = 4$ dostaneme řešením rovnice $\Phi_5(y) = 0$, ale také rovnice $\Phi_{15}(y) = 0$, protože jen dělitelé $d = 5$ a $d = 15$ čísla $2^4 - 1$ splňují podmínky (5.57). Pro

$$y_n = \cos\frac{2^n\pi}{5} + \mathrm{i}\sin\frac{2^n\pi}{5}, \quad y'_n = \cos\frac{2^n\pi}{15} + \mathrm{i}\sin\frac{2^n\pi}{15}, \ n = 1, 2, \ldots,$$

dostaneme pomocí (5.53), že $y_5 = y_1$, $y_6 = y_2, \ldots$ a $y'_5 = y'_1$, $y'_6 = y'_2, \ldots$, a tedy obě posloupnosti mají periodu 4.

Matematickou indukcí můžeme odvodit velice užitečný vztah (srov. (4.6)–(4.7))

$$F_m - 2 = 2^{2^m} - 1 = \prod_{k=0}^{m-1}(2^{2^k} + 1) = \prod_{k=0}^{m-1} F_k.$$

Exponent v rovnici (5.58) lze tedy napsat jako součin Fermatových

čísel. To nám umožňuje rozložit polynom na levé straně (5.58) na nerozložitelné (tj. ireducibilní) cyklotomické polynomy nižšího řádu. Hledání těchto polynomů je proto spojeno s rozkladem Fermatových čísel na prvočísla.

Pokud F_m a F_{m+1} jsou dvě po sobě následující prvočísla, počet „bifurkačních větví" se zdvojnásobí, viz (Antonyuk, Stanyukovich, 1990b). To nastává pro hodnoty $p = 2, 4, 8, 16, 32$. Značně komplikovanou situaci však dostaneme pro další Fermatova čísla, která mají více netriviálních dělitelů. Počet cyklotomických polynomů závisí poněkud komplikovaným způsobem na počtu prvočíselných dělitelů, který se běžně označuje τ. Pro složená Fermatova čísla je $\tau(F_5) = \tau(F_6) = \tau(F_7) = \tau(F_8) = 2$, $\tau(F_9) = 3$, $\tau(F_{10}) = 4$ a $\tau(F_{11}) = 5$. Hodnota $\tau(F_{12})$ zatím není známa. Ví se jen, že je alespoň 7.

Případ rovnice (5.52) pro $c \neq 0$ se v (Antonyuk, Stanyukovich, 1990a) vyšetřuje pomocí teorie perturbací.

5.10. Další aplikace

Konstrukce konečných algebraických těles. Uvažujme množinu

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$$

pro $p > 1$ s operací sčítání a násobení modulo p. Je-li p prvočíslo, pak podle věty 3.4 ke každému nenulovému prvku množiny $\mathbb{Z}_p$ existuje prvek inverzní. Taková algebraická struktura se nazývá *konečné těleso.* Pokud p není prvočíslo (nebo jeho mocnina), inverzní prvek nelze definovat. Například pro $\mathbb{Z}_6$ dostáváme netriviální dělitele nuly, protože $2 \cdot 3 \equiv 0 \pmod 6$. Algebraická tělesa mají celou řadu aplikací například v kvantových logikách, kombinatorice či v teorii okruhů. Nezapomeňme také, že přibližně od roku 1940 je architektura elektronických obvodů v počítačích budována právě na aritmetice modulo prvočíslo $p = 2$, tj. pomocí tělesa $\mathbb{Z}_2$.

Rychlé násobení. V aritmetice modulo 2^n nebo $2^n \pm 1$ lze velice jednoduše definovat tzv. rychlé násobení. Například násobení dvěma lze převést na posun o jeden bit vlevo – (Křížek, Luca, Somer, 2001, s. 172). A. Schönhage a V. Strassen[2)] v roce 1971 předložili rychlý algoritmus pro násobení dvou velkých čísel o N cifrách, který vyžaduje provedení jen $\mathcal{O}(N \log N \log\log N)$ aritmetických operací, viz (Schönhage, Strassen, 1971). Poznamenejme, že běžný algoritmus pro násobení dvou čísel, který se děti učí ve škole, vyžaduje $\mathcal{O}(N^2)$ operací. Pokud máte mezi sebou vynásobit například dvě tisíciciferná čísla, výhody rychlého algoritmu se zřetelně projeví, viz (Gorshkov, 1994a).

Prvočísla v přírodě. Biologové popisují zajímavý druh cikád (rodu Magicicada), jejichž kukly žijí 17 let pod zemí, viz (Crandall, Pomerance, 2005, Sec. 8.6), (Singh, 2000, s. 70) a (Wells, 2005, s. 27). Pak se vylíhnou, během několika týdnů dospějí, nakladou vajíčka a zemřou. Jistý parazit, který ohrožuje dospělé jedince, má dvouletý či tříletý životní cyklus. V prvém případě se s cikádou potká každých 34 let a ve druhém každých 51 let, protože prvočísla jsou nesoudělná. Svým neobvyklým životním cyklem se tak cikáda chrání proti parazitům. Kukly jiných typů cikád žijí pod zemí 7 nebo 13 let.

Ozubená kola. Prvočísla a nesoudělná čísla hrají důležitou roli při návrhu ozubených kol u nejrůznějších soustrojí, jako jsou např. jízdní kola, převodovky, mechanické hodinové strojky, faktorizační stroje – viz například (Delahaye, 2000, s. 112), (Hayes, 2000).

Kódování aminokyselin. V článku (Yan, Yan, Yan, 1991) je uveden zajímavý způsob kódování aminokyselin, který se opírá o skutečnost, že každé prvočíslo tvaru $4k+1$ lze jednoznačně napsat jako součet dvou čtverců $a^2 + b^2$ (viz Fermatova vánoční věta 3.12).

[2)] V. Strassen se již dříve proslavil překvapivým výsledkem, že Gaussova eliminace pro řešení soustavy lineárních algebraických rovnic nemá asymptoticky optimální počet operací – viz Numer. Math. **13** (1969), 354–356.

Za včlenění určité aminokyseliny do proteinového řetězce odpovídá vždy trojice nukleotidů (tzv. triplet). M. W. Nirenberg sestavil v roce 1966 tabulku genetického kódu – např. (Katrnoška, Křížek, 2003, 2004/05), kde každému tripletu DNA je přiřazena bílkovinotvorná aminokyselina. Tripletů je celkem $4^3 = 64$, zatímco aminokyselin je jen 20 (k nim jsou přidány ještě 3 terminační kodony označující ukončení syntézy). Většina aminokyselin je tak kódována 2, 4 nebo 6 triplety (např. leucin a serin 6 triplety). Rozdíly mezi malými prvočísly jsou ale také většinou 2, 4 nebo 6. Proto se jednotlivým aminokyselinám a kodonům nejprve vhodným způsobem přiřazují prvočísla menší než 64 a čísla 0, 1, 25, 45. Například leucinu $17 = 1^2 + 4^2$, serinu $29 = 2^2 + 5^2$, valinu $41 = 4^2 + 5^2$, alaninu $53 = 2^2 + 7^2$, glycinu[3)] $61 = 5^2 + 6^2$ a terminačním kodonům $0 = 0^2 + 0^2$. Tím se každé bílkovinotvorné aminokyselině a terminačním kodonům místo tripletu přiřazují jen dvě čísla $a \leq b$ z množiny $\{0, 1, \ldots, 7\}$ a šetří se tak paměť počítače. Jádro lidské buňky totiž obsahuje přibližně $3 \cdot 10^9$ nukleotidových párů, a proto je důležité dbát na co možná nejúspornější uchovávání biometrických údajů lidského genomu. Na tento ojedinělý způsob kódování získali autoři dokonce americký patent, i když je v tomto případě aplikace prvočísel poněkud nepřirozená.

Další použití. Prvočísla se uplatňují při rozpoznávání řeči, při použití paprsků X v astronomii, při řešení akustiky koncertních sálů, při návrhu směrové antény – viz (Schroeder, 2006).

A ještě jedna aplikace na závěr. Kdyby počet poslanců v našem parlamentu byl 199, nedocházelo by k tolika patových situacím, kterých jsme v poslední době svědky. Protože 199 je prvočíslo, nelze je napsat jako součet dvou (ani tří, čtyř, ...) stejně velkých čísel.

[3)] Charakteristická spektra glycinu byla detekována dokonce v mezihvězdném prostoru.

6. PSEUDOPRVOČÍSLA

Číselní teoretici jsou jako milovníci kaviáru,
jakmile jej jednou okusí, nemohou přestat.

Howard Eves

6.1. Co je pseudoprvočíslo?

V této kapitole si představíme speciální třídu složených čísel – pseudoprvočísla, která vykazují některé vlastnosti jako prvočísla (Křížek, Somer, 2003a). Podáme přehled jejich základních charakteristik, uvedeme mj. tvrzení o jejich asymptotické hustotě a ukážeme, že jejich výskyt je mnohem vzácnější než výskyt prvočísel. Například jen 3 pseudoprvočísla[1)] (o základu 2) jsou menší než 1000, zatímco ve stejném intervalu je 168 prvočísel (viz tabulka prvočísel na str. 335). Zavedeme také zajímavou množinu Carmichaelových čísel a popíšeme některé algoritmy pro generování pseudoprvočísel.

Pro definování pojmu „pseudoprvočíslo“ budeme potřebovat Malou Fermatovu větu 2.13, která určuje základní vlastnosti prvočísel a na níž je založena většina pravděpodobnostních algoritmů pro testování prvočíselnosti. Malá Fermatova věta tak hraje klíčovou roli v teorii čísel. Většinou se uvádí ve dvou ekvivalentních verzích. První verze říká, že když p je prvočíslo, pak

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

pro všechna celá čísla a (jinými slovy, p dělí $a^p - a$ beze zbytku). Podle druhé verze, když p je prvočíslo nesoudělné s a, pak

$$a^{p-1} \equiv 1 \pmod{p}. \tag{6.1}$$

[1)] Jejich definici uvedeme na další stránce.

Obrácené tvrzení Malé Fermatovy věty bohužel neplatí. Pro libovolný základ $a > 1$ existuje složené číslo n nesoudělné s a tak, že

$$a^n \equiv a \pmod{n}. \tag{6.2}$$

Například složené číslo $n = 341 = 31 \cdot 11$ splňuje (6.2) pro $a = 2$, pro něž $(a, n) = 1$. Snadno totiž vypočteme, že $2^{10} \equiv 1 \pmod{341}$. Umocněním na třicátou čtvrtou dostaneme $2^{340} \equiv 1 \pmod{341}$, tj. platí (6.1). Vynásobíme-li nyní ještě poslední kongruenci dvěma, dostaneme

$$2^{341} \equiv 2 \pmod{341}, \tag{6.3}$$

tj. platí i vztah (6.2).

Pro jiný základ $a = 3$ můžeme obdobně dokázat, že $3^{340} \equiv 56 \pmod{341}$ a $(3, 341) = 1$, což podle (6.1) znamená, že 341 je složené číslo (aniž bychom prováděli jeho rozklad na prvočísla).

Složené přirozené číslo n se nazývá *pseudoprvočíslo o základu a,* jestliže platí (6.2), tj. když n dělí $a^n - a$.

Poznamenejme ještě, že pokud jsou čísla a a n nesoudělná, pak (6.2) platí právě tehdy, když

$$a^{n-1} \equiv 1 \pmod{n}. \tag{6.4}$$

6.2. Historické poznámky

První pseudoprvočíslo 341 o základu 2 bylo nalezeno v roce 1819 Pierrem F. Sarrusem (viz Annales de Math. 10 (1819), 184–187 nebo (Dickson, 1919, s. 92)), který ukázal platnost kongruence (6.3). Pierre Frédérique Sarrus (1798–1861) je známý zejména svými jednoduchými vztahy pro výpočet determinantů čtvercových matic řádu 2 nebo 3.

Podle (Porubský, 2002) vlastnost (6.3) čísla 341 byla rovněž zaznamenána anonymním autorem článku *Théorèmes et problèmes*

sur les nombres, který byl publikován v Journal für die reine und angewandte Mathematik 6 (1830), 100–106.

Také János Bólyai (1802–1860), jeden ze zakladatelů neeukleidovských geometrií, informoval svého otce, viz (Kiss, 1985) o objevu pseudoprvočísla 341 v dopise z května 1855. Navíc podle (Kiss, 1985, s. 72) byl Bólyai první, kdo ukázal, že složené Fermatovo číslo $F_5 = 2^{32} + 1 = 641 \cdot 6700417$ je pseudoprvočíslo o základu 2. Jeho důkaz byl založen na kongruenci

$$2^{2^{32}} \equiv 1 \pmod{F_5}.$$

Abychom se přesvědčili, že tento vztah platí, umocníme na druhou nejprve kongruenci $2^{32} \equiv -1 \pmod{F_5}$, viz (1.4),

$$2^{64} \equiv 1 \pmod{F_5}.$$

Využijeme-li rovnosti $2^{32} = 64 \cdot 2^{26}$, můžeme v umocňování pokračovat

$$2^{2^{32}} = \left(2^{64}\right)^{2^{26}} \equiv 1 \pmod{F_5}.$$

Vynásobíme-li dvěma levou i pravou stranu této kongruence, dostaneme

$$2^{F_5} = 2 \cdot 2^{2^{32}} \equiv 2 \pmod{F_5},$$

a tedy F_5 je pseudoprvočíslo o základu 2.

V roce 1909 Tadeusz Banachiewicz publikoval 5 pseudoprvočísel o základu 2 menších než 2000 a později objevil ještě dvě zbývající v tomto intervalu, viz (Banachiewicz, 1909), (Dickson, 1919, s. 94), (Sierpiński, 1948). Jejich úplný seznam má tvar:

$$\begin{aligned} 341 &= 11 \cdot 31, \\ 561 &= 3 \cdot 11 \cdot 17, \\ 645 &= 3 \cdot 5 \cdot 43, \\ 1105 &= 5 \cdot 13 \cdot 17, \\ 1387 &= 19 \cdot 73, \\ 1729 &= 7 \cdot 13 \cdot 19, \\ 1905 &= 3 \cdot 5 \cdot 127. \end{aligned}$$

Pseudoprvočísla o základu 2 byla objevena nejdříve a jsou také nejčastěji studována. Proto se dohodněme na následujícím.

Úmluva. Pro jednoduchost budeme pseudoprvočísla o základu 2 nazývat jen *pseudoprvočísla.*

Pseudoprvočísla o jiných základech jsou tabelována například v (Ribenboim, 1988).

Příklad. Ukážeme, že $91 = 7 \cdot 13$ je pseudoprvočíslo o základu 3. Podle Malé Fermatovy věty 2.13 platí $3^6 \equiv 1 \pmod 7$, a tedy podle (1.4) máme, že $3^{90} \equiv 1 \pmod 7$. Dále vidíme, že $3^3 \equiv 1 \pmod{13}$, tj. $3^{90} \equiv 1 \pmod{13}$. Dohromady dostáváme, že $3^{90} \equiv 1 \pmod{91}$, tj. 91 je pseudoprvočíslo o základu 3. Navíc lze prověřit, že je to nejmenší pseudoprvočíslo o tomto základu. (Další takové pseudoprvočíslo je 286.)

Pseudoprvočíslům se kdysi také říkalo „skoro prvočísla“ (angl. *almost primes*), viz (Erdős, 1950), nebo též *Pouletova čísla*, viz (Duparc, 1953), neboť byla intenzivně studována P. Pouletem v (Poulet, 1938), kde jsou tabelována všechna pseudoprvočísla až do 10^8. Viz též (Lehmer, 1936).

V řadě publikací – např. (Banachiewicz, 1909), (Dickson, 1919, s. 59), (Jeans, 1897/98) – se uvádí, že staří Číňané již 500 let př. n. l. věřili, že

$$2^n \equiv 2 \pmod n \tag{6.5}$$

platí právě tehdy, když je n prvočíslo.[2)] Zajímavé vysvětlení, jak tato téměř jistě nepravdivá historka vznikla, je popsáno v (Ribenboim, 1996, s. 103–105) či v (Ribenboim, 1988, s. 86). Hlavní protiargument je ten, že staří Číňané nikdy neformulovali pojem „prvočísla“. Tato chyba se poprvé objevila pravděpodobně v článku (Jeans, 1897/98) a byla pak opakována mnoha autory.

[2)] Při vší úctě ke starým čínským matematikům by asi jen těžko mohli na svých abacích zjistit, že $341 \mid (2^{341} - 2)$, tj. že implikace $\Rightarrow$ neplatí, neboť číslo $2^{341} - 2$ má přes 100 cifer a pravidla pro počítání s kongruencemi tehdy nebyla ještě známa.

Podle D. Mahnkeho (Mahnke, 1913) v letech 1680–1681 G. W. Leibniz rovněž chybně tvrdil, že kongruence (6.5) platí, jen když je n prvočíslo.

Následující větu, jež je uvedena v (Sierpiński, 1948) a (Steuerwald, 1947), lze použít k rekurzivnímu generování nekonečně mnoha pseudoprvočísel.

Věta 6.1. *Jestliže n je liché pseudoprvočíslo, pak $2^n - 1$ je také liché pseudoprvočíslo.*

D ů k a z. Protože n je složené, existuje přirozené číslo m, $1 < m < n$, které dělí n. Pak $2^m - 1$ dělí podle (4.1) číslo $2^n - 1$, tj.

$$\left(2^m - 1\right) \mid \left(2^n - 1\right),$$

a tudíž $2^n - 1$ je také složené. Nyní stačí dokázat, že

$$\left(2^n - 1\right) \mid \left(2^{2^n - 2} - 1\right). \tag{6.6}$$

Jelikož n je liché pseudoprvočíslo, podle kongruence (6.4) platí

$$\left(2^n - 2\right)/2 = 2^{n-1} - 1 = kn$$

pro nějaké celé číslo k. Potom číslo $2^n - 1$ dělí $2^{kn} - 1 = 2^{(2^n-2)/2} - 1$ a vztah (6.6) je tedy splněn, neboť

$$2^{2^n-2} - 1 = \left(2^{(2^n-2)/2} - 1\right)\left(2^{(2^n-2)/2} + 1\right). \qquad \square$$

Díky této větě můžeme explicitně stanovit pseudoprvočíslo, které je větší než libovolné předem zadané přirozené číslo. Podobné tvrzení pro prvočísla prozatím není známo, i když víme, že prvočísel je nekonečně mnoho. Do roku 2008 největší známé prvočíslo bylo Mersennovo prvočíslo $2^{43112609} - 1$, jež má téměř 13 milionů cifer (viz oddíl 4.1). Poznamenejme ještě, že v roce 1903 větu 6.1 dokázal E. Malo (Malo, 1903) pro případ, že n je prvočíslo a $2^n - 1$ je složené.

První sudé pseudoprvočíslo (o základu 2)

$$161\,038 = 2 \cdot 73 \cdot 1103$$

bylo nalezeno D. H. Lehmerem v roce 1950, viz (Erdős, 1950). O rok později potom N. G. W. H. Beeger dokázal, že existuje nekonečně mnoho sudých pseudoprvočísel – viz (Beeger, 1951).

6.3. Hustota rozložení pseudoprvočísel

I když je pseudoprvočísel nekonečně mnoho (viz věta 6.1), je jich mnohem méně než prvočísel. Například K. Szymiczek (Szymiczek, 1967) dokázal, že pokud n-té pseudoprvočíslo (o základu 2) označíme P_n, pak je řada

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

konvergentní, zatímco je dobře známo, že když p_n značí n-té prvočíslo, pak je řada

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

divergentní (viz věta 3.15). Později však A. Mąkowski ve své publikaci (Mąkowski, 1974) pro pseudoprvočísla ukázal, že řada

$$\sum_{n=1}^{\infty} \frac{1}{\log P_n}$$

je divergentní.

Jestliže si náhodně zvolíme číslo $n \leq 10^{10}$, pro něž $2^{n-1} \equiv 1 \pmod{n}$, pak pravděpodobnost, že n je prvočíslo, bude více než 30 000krát větší než pravděpodobnost toho, že n je pseudoprvočíslo. Více podrobností je v článku (Křížek, Somer, 2003a).

Zajímavá vlastnost, která je společná jak prvočíslům, tak i pseudoprvočíslům, je vyjádřena v následující větě, viz (Rotkiewicz, 1963) a (Rotkiewicz, 1967).

Věta 6.2 (Rotkiewiczova). *Nechť $a, d \in \mathbb{N}$ jsou nesoudělná čísla. Pak existuje nekonečně mnoho pseudoprvočísel v aritmetické posloupnosti $(a + kd)_{k=0}^{\infty}$.*

Podobný výsledek pro prvočísla udává Dirichletova věta 3.10, která má stejné znění jako věta 6.2, když vypustíme předponu „pseudo“.

6.4. Carmichaelova čísla

Obrovská řídkost pseudoprvočísel o pevném základu a ve srovnání s prvočísly poskytuje rozumný důvod používat Malou Fermatovu větu 2.13 pro testování prvočíselnosti, viz (Porubský, 2002, s. 81). Existují však složená čísla n, nazývaná *Carmichaelova čísla* nebo též *absolutní pseudoprvočísla,* která jsou pseudoprvočísly pro každý základ a, tj. kongruence

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

platí pro všechna přirozená čísla a.

Počítačová prvočíselná síta založená na Malé Fermatově větě nám tedy kromě prvočísel propustí i složená Carmichaelova čísla. Proto se příslušné testy prvočíselnosti musí jistým způsobem modifikovat. Jak již bylo řečeno, Wilsonova ekvivalence (viz věta 3.6): „p *je prvočíslo* $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$“ se k testování prvočíselnosti nehodí, neboť není znám efektivní způsob výpočtu faktoriálu modulo p.

V roce 1899 A. Korselt dokázal následující nutnou a postačující podmínku pro to, aby složené přirozené číslo n bylo absolutním pseudoprvočíslem, viz (Korselt, 1899).

Věta 6.3 (Korseltova). *Složené číslo n je absolutní pseudoprvočíslo právě tehdy, když n není dělitelné čtvercem žádného přirozeného čísla většího než jedna a $p-1$ dělí $n-1$ pro všechny prvočinitele p čísla n.*

Je zajímavé, že když Korselt dokázal tuto větu, neuvedl ani jeden příklad absolutního pseudoprvočísla. Z Korseltovy věty 6.3 například okamžitě plyne, že

$$561 = 3 \cdot 11 \cdot 17$$

je absolutní pseudoprvočíslo, neboť $3 - 1 = 2$, $11 - 1 = 10$, $17 - 1 = 16$ a všechna tato tři čísla dělí 560.

Na druhé straně $341 = 11 \cdot 31$ není absolutní pseudoprvočíslo, neboť $31 - 1 = 30$ nedělí 340.

R. D. Carmichael, který zavedl funkci λ (viz oddíl 2.8), nezávisle objevil Korseltovo uvedené kritérium a přeformuloval je následujícím způsobem, i když nepoužil termínu „Carmichaelovo číslo“ (Carmichael, 1910).

Věta 6.4 (Carmichaelova). *Složené číslo n je Carmichaelovo číslo, právě když n není dělitelné čtvercem žádného přirozeného čísla většího než jedna a $\lambda(n) \mid (n - 1)$.*

V článku (Carmichael, 1910) se také ukazuje, že každé Carmichaelovo číslo má alespoň tři prvočíselné dělitele, a uvedl jejich čtyři příklady, které obsahovaly i dvě nejmenší: 561 a 1105. V dalším jeho článku (Carmichael, 1912) je uvedeno již patnáct Carmichaelových čísel. Podle (Pomerance, Selfridge, Wagstaff, 1980) existuje jen 2163 Carmichaelových čísel menších než $25 \cdot 10^9$.

V práci (Alford, Granville, Pomerance, 1994) je ukázáno, že existuje nekonečně mnoho Carmichaelových čísel. Navíc je dokázáno, že pokud $C(x)$ označuje počet Carmichaelových čísel nepřevyšujících x, pak pro dostatečně velké x platí

$$C(x) > x^{2/7}.$$

6.5. Mersennova a Fermatova pseudoprvočísla

Následující věta tvrdí, že každé složené *Mersennovo číslo* $M_p = 2^p - 1$, kde p je prvočíslo, je pseudoprvočíslo (o základu 2).

Věta 6.5. *Všechna Mersennova čísla jsou buď prvočísla, anebo pseudoprvočísla.*

Důkaz. Nechť $M_p = 2^p - 1$, kde p je prvočíslo, je složené

Mersennovo číslo. Pak p je liché prvočíslo. Stačí dokázat, že

$$2^{M_p-1} \equiv 1 \pmod{M_p},$$

neboli ekvivalentně

$$M_p \mid \left(2^{M_p-1} - 1\right). \tag{6.7}$$

My však dokážeme silnější tvrzení, a to

$$M_p \mid \left(2^{(M_p-1)/2} - 1\right), \tag{6.8}$$

které implikuje (6.7).

Podle Malé Fermatovy věty 2.13 platí

$$\frac{M_p - 1}{2} = 2^{p-1} - 1 \equiv 0 \pmod{p}.$$

Tudíž $(M_p - 1)/2 = kp$ pro nějaké přirozené číslo k. Protože

$$\left(2^p - 1\right) \mid \left(2^{kp} - 1\right),$$

vidíme, že (6.8) platí. □

Existuje také několik souvislostí mezi Fermatovými čísly $F_m = 2^{2^m} + 1$, $m = 0, 1, 2, \ldots$, a pseudoprvočísly. Například v roce 1904 M. Cipolla odvodil, že $n \mid \left(2^n - 2\right)$ pro $n = 2^{2^m} + 1$, $m = 0, 1, 2, \ldots$ O pět let později Banachiewicz dokázal, že všechna Fermatova čísla jsou buď prvočísla, anebo pseudoprvočísla o základu 2 (důkaz je uveden např. v (Křížek, Luca, Somer, 2001, s. 36)).

Věta 6.6. *Všechna Fermatova čísla jsou buď prvočísla, anebo pseudoprvočísla. Jestliže navíc* $2^n + 1$ *je pseudoprvočíslo, pak n je mocnina* 2.

Možná, že právě tato věta vedla Fermata k jeho nesprávné domněnce, že všechna Fermatova čísla jsou prvočísla.

Fermatova čísla použilo několik autorů, viz (Cipolla, 1904), (Jarden, 1950), (Jeans, 1897/98), (Rotkiewicz, 1964) a (Szymiczek, 1966) ke generování nekonečně mnoha pseudoprvočísel. Následující věta z roku 1904 dokázaná v (Cipolla, 1904) ukazuje, jak lze Fermatova čísla použít k vytvoření nekonečně mnoha pseudoprvočísel, která mají libovolně velký počet prvočinitelů.

Věta 6.7 (Cipollova). *Jestliže* $a > b > \cdots > s > 1$ *a* $n = F_a F_b \cdots F_s$, *pak n je pseudoprvočíslo právě tehdy, když* $2^s > a$. *Pro libovolně velké* $m > 1$ *tedy existuje nekonečně mnoho pseudoprvočísel, která mají alespoň m různých prvočinitelů.*

V roce 1949 P. Erdős dokázal, že pro každé $m > 1$ existuje nekonečně mnoho pseudoprvočísel, která mají právě m různých prvočinitelů. Je zajímavé, že první důkaz nekonečného počtu pseudoprvočísel podal astronom J. H. Jeans už v roce 1897. V práci (Jeans, 1897/98) ukázal, že když $a > b$ a $2^b > a$, pak $F_a F_b$ je pseudoprvočíslo. Tento výsledek je speciálním případem věty 6.7.

Věta 6.8 (Mickova). *Každé přirozené číslo, které není prvočíslem, je pseudoprvočíslem pro vhodně zvolený základ.*

D ů k a z. Pro libovolné složené přirozené číslo n je podle binomické věty rozdíl $a^n - a$ dělitelný n pro $a = n + 1$,

$$(n+1)^n - n - 1 = n^n + \binom{n}{1} n^{n-1} + \cdots + \binom{n}{n-2} n^2.$$

Odtud a ze vztahu (6.2) plyne, že n je pseudoprvočíslo o základu $n + 1$. □

Výzkum v oblasti pseudoprvočísel je nyní značně rozsáhlý. Existuje celá řada rozličných tříd pseudoprvočísel (viz (Baillie, Wagstaff, 1980), (Joo, Phong, 1990), (Kiss, 1999), (Křížek, Luca, Somer, 2001), (Phong, 1988), (Somer, 1989), (Szymiczek, 1966)), např. již zmíněná absolutní pseudoprvočísla, Eulerova, Frobeniova, Lehmerova a silná pseudoprvočísla, Fermatova a Lucasova d-pseudoprvočísla, superpseudoprvočísla aj. Pseudoprvočísla mají praktické uplatnění v kryptografii a algebře – viz (Flaut, 2007). Teprve čas ukáže, zda někdy najdou uplatnění také v dalších praktických situacích podobně jako prvočísla.

7. SPECIÁLNÍ TYPY PŘIROZENÝCH ČÍSEL

Vesmír je řízen čísly.

Motto pythagorejců

7.1. Fibonacciho a Lucasova čísla

Fibonacciho čísla. Posloupnost *Fibonacciho čísel* $(K_n)_{n=0}^{\infty}$ začíná hodnotami $K_0 = 0$ a $K_1 = 1$ a splňuje rekurenci[1)]

$$K_{n+2} = K_{n+1} + K_n \qquad \text{pro všechna } n = 0, 1, 2, \ldots \tag{7.1}$$

Několik jejích prvních členů je tedy

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,$$
$$233,\ 377,\ 610,\ 987,\ 1597,\ 2584,\ \ldots$$

Tato čísla se poprvé objevila ve druhém rozšířeném vydání knihy *Liber Abaci* z r. 1228 italského matematika Fibonacciho a nesou proto jeho jméno. Poprvé je ale nazval Fibonacciho čísly Édouard Lucas až kolem roku 1870. Leonardo z Pisy (asi 1180 – asi 1250), nazývaný Fibonacci,[2)] tj. syn Bonaccia, byl jedním z největších matematiků středověku. Vděčíme mu mimo jiné za to, že do evropské matematiky zavedl nulu díky svým kontaktům s Arábií.

Ve 12. kapitole jmenované knihy (srov. (Pisano, 2002, s. 404)) se vyšetřuje úloha, jak rychle se mohou množit králíci za jistých velice specifických a idealizovaných podmínek. Předpokládejme, že jeden nově narozený pár je umístěn do prázdného výběhu, králíci se mohou pářit již po měsíci, doba březosti je také 1 měsíc, každá samice porodí každý měsíc právě jeden pár a konečně že králíci neumírají. V rovnici (7.1) pak K_n značí počet králičích párů v ohrádce v n-tém měsíci. První, kdo napsal rekurenci (7.1) pro

[1)] V literatuře se Fibonacciho čísla standardně označují symbolem F_n, který je ale v této knize již vyhrazen pro Fermatova čísla.

[2)] Někdy též Leonardo Pisánský.

Fibonacciho čísla, byl Albert Girard (1595–1632), a tedy nikoli Fibonacci, viz (Tanton, 2005).

Bylo by obtížné vyjmenovat všechny aktivity, které zájem o Fibonacciho čísla vyvolal. Omezíme se jen na konstatování, že existuje specializovaný časopis *The Fibonacci Quarterly* vycházející čtyřikrát ročně a také společnost *Fibonacci Association*, jež pořádá velké mezinárodní konference o Fibonacciho číslech každé dva roky.

O Fibonacciho číslech byla napsána celá řada monografií, viz například (Hoggatt, 1969), (Jarden, 1973), (Koshy, 2001), (Livio, 2002), (Vajda, 1989), (Vorobiev, 2002). Fibonacciho čísla jsou tak populární, že ve finském Turku připevnili na vysoký elektrárenský komín pod sebe dva metry vysoká neonová Fibonacciho čísla od 1 až do 55.

V tomto oddílu podáme stručný přehled o zajímavých vlastnostech Fibonacciho čísel, o zcela nových výsledcích i otevřených problémech. Uvidíme, že Fibonacciho čísla se objevují v některých naprosto nečekaných souvislostech.

Příklad. Vydělíme-li postupně atomová čísla vzácných plynů ($_2$He, $_{10}$Ne, $_{18}$Ar, $_{36}$Kr, $_{54}$Xe, $_{86}$Rn) číslem 5π, pak po zaokrouhlení na celá čísla dostaneme posloupnost 0, 1, 1, 2, 3, 5. V tomto Fibonacciho růstu můžeme pokračovat i dále. Pro hypotetický vzácný plyn $_{118}$Uuo, tzv. ununoktinium, pak dostaneme 8.

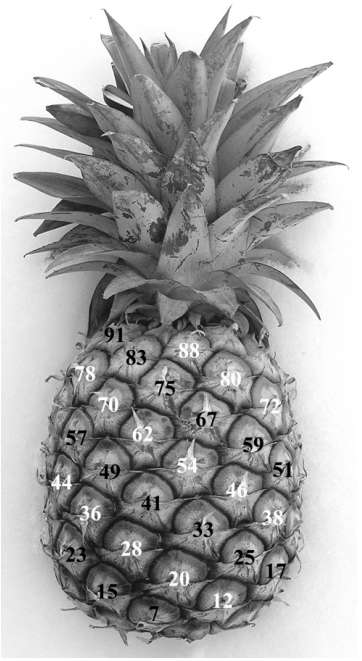
Příklad. Také v biologii se setkáváme s častým výskytem Fibonacciho čísel. Například semínka smrkových či borovicových šišek jsou uspořádána do dvou typů (pravotočivých a levotočivých) šroubovic, jejichž počty jsou obvykle 13 a 8. Podobné spirály lze spatřit také u artyčoků nebo ananasů. Na obrázku 7.1 vidíme, že šroubovice (spirály) na povrchu ananasu jsou tvořené útvary, které připomínají kosodélníky.

Obrázek 7.2 pak schematicky znázorňuje rozvinutý povrch tohoto ananasu. Kosodélníky lze očíslovat tak, že čísla na jednotlivých šroubovicích tvoří aritmetické posloupnosti s diferencemi

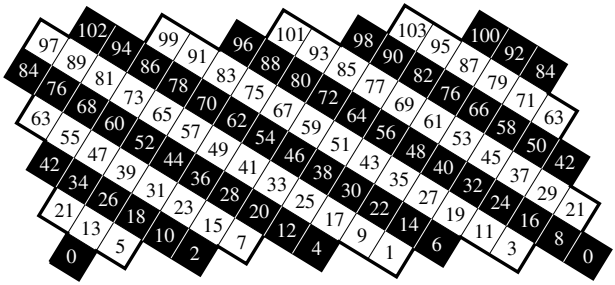
8 a 13. Čísla kosodélníků, které se dotýkají právě jedním vrcholem, mají zase diferenci rovnou 5 nebo 21 (v absolutní hodnotě). Je pozoruhodné, že zhruba každý druhý ananas má šroubovice na svém povrchu umístěné zrcadlově, tj. má 13 levotočivých a 8 pravotočivých šroubovic. Existuje domněnka, že tato složitá struktura šroubovic není zakódována v DNA, ale že se vytváří automaticky při růstu, přičemž nový kosodélník se vytváří tam, kde je nejvíce místa. Další ukázky výskytu Fibonacciho čísel v přírodě lze nalézt např. v (Koshy, 2001).

Příklad. V roce 1876 francouzský matematik Édouard Lucas odvodil formuli

$$\sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} = K_{n+1},$$



Obr. 7.1. Soustavy pravotočivých a levotočivých šroubovic na povrchu ananasu.



Obr. 7.2. Osm levotočivých šroubovic na rozvinutém plášti ananasu je pro rozlišení obarveno střídavě černě a bíle. Přibližně kolmo na tento směr máme třináct pravotočivých šroubovic. (Pravý a levý okraj nákresu je třeba ztotožnit.)

která udává, jak jsou Fibonacciho čísla ukryta v Pascalově trojúhelníku.[3)] Zapíšeme tento trojúhelník tak, jak je znázorněno na obr. 7.3. Je patrné, že součty kombinačních čísel podle diagonál se sklonem asi 45° jsou rovny právě číslům K_{n+1}, viz (Calda, 1993). Například $1+1=2$, $1+2=3$, $1+3+1=5$, $1+4+3=8$ atd.

$$
\begin{array}{ccccccccc}
1 & & & & & & & & \\
1 & & 1 & & & & & & \\
1 & & 2 & & 1 & & & & \\
1 & & 3 & & 3 & & 1 & & \\
1 & & 4 & & 6 & & 4 & & 1 \\
1 & & 5 & & 10 & & 10 & & 5 \\
1 & & 6 & & 15 & & 20 & & 15 \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
\qquad
\begin{array}{ccc}
& & \\
& & \\
& & \\
& & \\
1 & & \\
1 & & \\
6 & & 1 \\
\vdots & & \vdots
\end{array}
$$

Obr. 7.3. Pascalův trojúhelník ve zkoseném tvaru.

Příklad. Lze dokázat, že počet podmnožin množiny $A=\{1,\ldots,n\}$, které neobsahují dvě po sobě následující čísla, je K_{n+2}. Například pro $n=4$ jsou to podmnožiny $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1,3\}$, $\{1,4\}$ a $\{2,4\}$.

[3)] Poněkud odlišným způsobem jsou skryta v Pascalově trojúhelníku také Fermatova čísla, viz odstavec *O dalších souvislostech Fermatových čísel s geometrií* v oddílu 4.2.

Rovněž počet možností, kdy při n hodech mincí za sebou nepadnou dvě panny, je K_{n+2}. Například pro $n = 4$ jsou to možnosti

(O,O,O,O), (P,O,O,O), (O,P,O,O), (O,O,P,O),
(O,O,O,P), (P,O,P,O), (P,O,O,P), (O,P,O,P),

kde O značí orla a P pannu. To, že v obou případech dostáváme stejný počet možností, plyne z následujícího přiřazení. Nechť B je podmnožina A, která neobsahuje dvě po sobě následující čísla. Pak odpovídající n-tice složená z O a P má na i-tém místě P právě tehdy, když $i \in B$.

Příklad. Uvažujme dvě tabule okenního skla na sobě. Sluneční paprsek se uvnitř této dvojité vrstvy může různě lámat. V knize (Livio, 2002, s. 99) se ukazuje, že paprsek může projít buď přímo, nebo se uvnitř jednou odrazí dvěma způsoby, nebo se dvakrát odrazí třemi způsoby, nebo se třikrát odrazí pěti způsoby, nebo se čtyřikrát odrazí osmi způsoby atd. Opět dostáváme Fibonacciho posloupnost.

Příklad. Klasickou Fibonacciho úlohu s králíky lze ekvivalentně formulovat takto: Uvažujme posloupnost řetězců tvořených číslicemi 0 a 1, které jsou definovány rekurentně tak, že číslici 0 zaměníme v následujícím řetězci za 1 (tj. nově narozený králičí pár dospěje) a číslici 1 zaměníme za 10 (tj. dospělému páru se narodí jeden nový pár). Pokud začneme od jedničky, dostaneme tuto posloupnost řetězců:

1,
10,
101,
10110,
10110101,
1011010110110,
10110101101101011010110101,
⋮

Lze dokázat, že délka n-tého řetězce je rovna K_{n+1} pro $n = 1, 2, 3, \ldots$ a že n-tý řetěz pro $n > 2$ vznikne spojením dvou předchozích řetězců tak, že n-tý řetěz začíná vždy předchozím řetězcem. Tímto způsobem můžeme zkonstruovat nekonečnou posloupnost nul a jedniček

$$10110101101101011010110110101101101\ldots, \qquad (7.2)$$

která se nazývá *zlatý řetězec*. Posloupnost (7.2) má fraktální charakter. Libovolný její konečný podřetězec se v ní totiž vyskytuje nekonečněkrát, i když posloupnost (7.2) není periodická. Fibonacci tak poprvé představil úlohu, která vede k fraktálním strukturám.

Fibonacciho čísla a Mandelbrotova množina. Fibonacciho čísla jsou „ukryta“ i v Mandelbrotově fraktální množině (podrobnosti viz (Křížek, Šolcová, 2005)). Největší část Mandelbrotovy množiny $\mathcal{M}$ definované vztahem (viz oddíl 5.9)

$$\mathcal{M} = \{c \in \mathbb{C};\ \exists\, C > 0\ \forall n \in \{1, 2, \ldots\} : |y_n(c)| \leq C \quad \text{a} \quad y_1(c) = 0\}$$

tvoří oblast ohraničenou křivkou srdcovkou (tzv. tělo). V našem případě srdcovku opisuje bod na kružnici o poloměru 1/4, která se kotálí po stejně velké kružnici se středem v nule. Srdcovka (neboli kardioida) je speciálním případem prosté epicykloidy. K tělu Madelbrotovy množiny oblasti přiléhá, viz (Peitgen, Jürgens, Saupe, 1992, s. 857), nekonečně mnoho kruhových oblastí s dalšími kruhovými výstupky, kterých je rovněž nekonečně mnoho (viz obr. III barevné přílohy).

Různobarevné obrázky okolí Mandelbrotovy fraktální množiny lze získat například následujícím způsobem: Každému bodu $c \in \mathbb{C} \setminus \mathcal{M}$ přiřadíme jistý barevný odstín podle „rychlosti divergence“ posloupnosti $(y_n(c))_{n=1}^{\infty}$ definované vztahem (5.52). Na obr. III barevné přílohy zelená barva označuje interval s největší rychlostí divergence, tyrkysová interval s o něco menší rychlostí, fialová interval s ještě menší rychlostí divergence atd. Množství podobných obrázků lze nalézt v literatuře i na internetu.

Mnohem přirozenější je ale obarvovat vnitřek Mandelbrotovy množiny $\mathcal{M}$ podle počtu hromadných bodů posloupnosti (y_n) (viz obr. V barevné přílohy). Pro $k \in \mathbb{N}$ položme

$$\mathcal{M}(k) = \{c \in \mathcal{M};\ (y_n(c))_{n=1}^{\infty} \text{ má právě } k \text{ hromadných bodů}\}.$$

Na obrázcích V a VI barevné přílohy žlutá barva vyznačuje množinu $\mathcal{M}(1)$ (kdy posloupnost $(y_n(c))_{n=1}^{\infty}$ má limitu) a fialová barva vyznačuje množinu $\mathcal{M}(2)$ (tj. kdy odpovídající posloupnost má právě 2 hromadné body). Další barvy jsou přiřazeny takto: 3 – červená, 4 – blankytně modrá, 5 – zelená, 6 – světle modrá, 7 – tmavě šedivá, 8 – světle šedivá, 9 – hnědá, 10 – tmavě fialová, 11 – tmavě červená, 12 – modrá, 13 – tmavě zelená, 14 – tmavě modrá, 15 a více hromadných bodů – černá. Bíle je obarvena oblast, kde posloupnost $(y_n(c))$ diverguje pro $n \to \infty$. Takto zavedené barevné označení nám umožní vystopovat Fibonacciho čísla i v Mandelbrotově množině.

Na obr. V barevné přílohy vidíme, že po obvodu srdcovky jsou rozmístěné různě obarvené kruhy (v kulatých závorkách budeme označovat příslušný počet hromadných bodů). Všimněme si, že největší kruh mezi fialovým (2) a horním (popř. dolním) červeným kruhem (3) je zelený (5). Podobně na obr. VI největší kruh mezi červeným (3) a zeleným (5) je světle šedivý (8). Největší kruh mezi zeleným (5) a světle šedivým (8) je tmavě zelený (13) apod. Čísla v závorkách jsou ale Fibonacciho čísla. Důkaz této vlastnosti a další zajímavé souvislosti mezi Mandelbrotovou množinou a Fibonacciho čísly jsou uvedeny v (Devaney, 1999), (Peitgen, Jürgens, Saupe, 1992, s. 688), (Zhu, Cao, Liu, Zhu, 2001) aj.

Zlatý řez a Lucasova čísla. Označme

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \text{a} \qquad \beta = \frac{1-\sqrt{5}}{2} \tag{7.3}$$

kořeny charakteristické rovnice[4)]

$$x^2 - x - 1 = 0$$

odpovídající diferenční rovnici (7.1). Číslo

$$\alpha = 1.6180339887\ldots$$

se nazývá *zlatý řez* (lat. sectio aurea). Všimněme si, že kořen β je až na znaménko stejný jako kořen (5.41), který hraje důležitou roli při eukleidovské konstrukci pravidelného pětiúhelníku. Konstanty

$$\alpha = \alpha^2 - 1 \quad \text{a} \quad \beta = -\frac{1}{\alpha}$$

mají důležitou úlohu při analýze Fibonacciho čísel díky vztahu

$$K_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{pro všechna } n = 0, 1, 2, \ldots, \tag{7.4}$$

který se nazývá *Binetova formule* (přitom $\alpha - \beta = \sqrt{5}$ a $\alpha + \beta = 1$). Formuli (7.4) publikoval již v roce 1765 Leonhard Euler. V roce 1843 ji ale znovu „objevil" francouzský matematik Jacques Philippe Marie Binet (1786–1856). Povšimněme si, že (7.4) generuje pouze přirozená čísla, i když obsahuje několik iracionálních čísel. Ze vztahu (7.4) navíc plyne, že K_n je nejbližší celé číslo k číslu $\alpha^n/\sqrt{5}$.

Zlatý řez představuje již od antiky základní estetický poměr. Obdélník, jehož délky stran jsou v poměru α, je pokládán za nejkrásnější. Takový obdélník vznikne například jako konvexní obal dvou protilehlých hran pravidelného dvacetistěnu (viz obr. II barevné přílohy). Poměr délek úhlopříčky a strany pravidelného pětiúhelníku je α; přitom se i samotné úhlopříčky rovněž dělí v poměru zlatého řezu. Poloměr kružnice opsané pravidelnému desetiúhelníku k délce jeho strany je rovněž v poměru α. Johannes Kepler (1571–1630) popsal třicetistěn (tzv. *Keplerův třicetistěn*), který je průnikem pěti různě natočených krychlí o stejném středu, viz (Šolcová, 2004, s. 32). Všech třicet stěn tvoří shodné kosočtverce a poměr jejich úhlopříček je také roven α.

[4)] Řešení lineárních diferenčních rovnic k-tého řádu je popsáno např. v (Henrici, 1962, s. 213).

Zlatý řez má celou řadu zajímavých algebraických vyjádření, např.

$$\alpha = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\dots}}}}\,.$$

Každé reálné číslo $y \neq 0$ lze zapsat ve tvaru řetězového zlomku

$$y = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}, \quad a_i \in \mathbb{Z},$$

což se někdy označuje $[a_1, a_2, a_3, \dots]$. Přitom platí

$$\alpha^{-1} = [1, 1, 1, \dots] = (\sqrt{5} - 1)/2.$$

Poznámka. Pomocí čísel $[2, 2, 2, \dots] = \sqrt{2} - 1$, resp. $[3, 3, 3, \dots] = (\sqrt{13} - 3)/2$ lze analogicky definovat též tzv. *stříbrný řez,* resp. *bronzový řez.*

K posloupnosti K_n existuje důležitá (též celočíselná) doprovodná posloupnost

$$L_n = \alpha^n + \beta^n = \alpha^n + (-1)^n \alpha^{-n} \qquad \text{pro všechna } n = 0, 1, 2, \dots, \tag{7.5}$$

která se nazývá *Lucasova posloupnost*. Její prvky, tzv. *Lucasova čísla*, splňují také rekurenci (7.1), pokud zaměníme K_n za L_n, tj.

$$L_{n+2} = L_{n+1} + L_n \qquad \text{pro všechna } n = 0, 1, 2, \dots \tag{7.6}$$

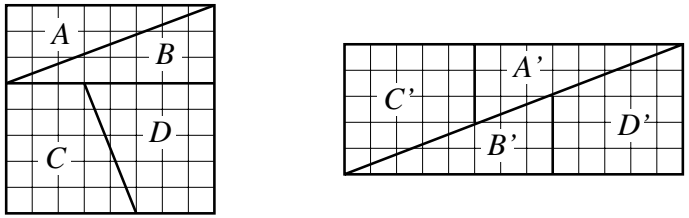
s počátečními hodnotami $L_0 = 2$ a $L_1 = 1$. Několik jejích prvních členů je

$$2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ 76, \dots$$

Rovnosti obsahující Fibonacciho a Lucasova čísla. V roce 1680 francouzský matematik a astronom italského původu Giovanni Domenico Cassini zjistil, že (viz (Koshy, 2001, s. 74))

$$K_{n+1}K_{n-1} - K_n^2 = (-1)^n. \tag{7.7}$$

Tato identita pro $n = 6$ je základem pozoruhodného geometrického paradoxu z obrázku 7.4 (viz poznámka na konci oddílu 7.1).



Obr. 7.4. Čtverec 8×8 a obdélník 13×5, jež mají různé obsahy, jsou rozděleny na oblasti A, B, C, D a A', B', C', D', které mají po řadě zdánlivě stejné obsahy.

Ze vztahů (7.1), (7.4), (7.5) a (7.6) můžeme odvodit řadu zajímavých identit:

$$\begin{aligned}
K_{n+1} + K_{n-1} &= L_n, \\
L_{n+1} + L_{n-1} &= 5K_n, \\
K_n^2 - K_{n+k}K_{n-k} &= (-1)^{n+k}K_k^2, \\
L_n^2 - L_{n+1}L_{n-1} &= (-1)^n 5, \\
L_n^2 - 5K_n^2 &= (-1)^n 4, \\
K_{n+1}^2 - K_{n-1}^2 &= K_n L_n = K_{2n}, \\
K_{n+1}^2 + K_n^2 &= K_{2n+1}, \\
K_m K_{n+1} + K_{m-1}K_n &= K_{m+n}.
\end{aligned}$$

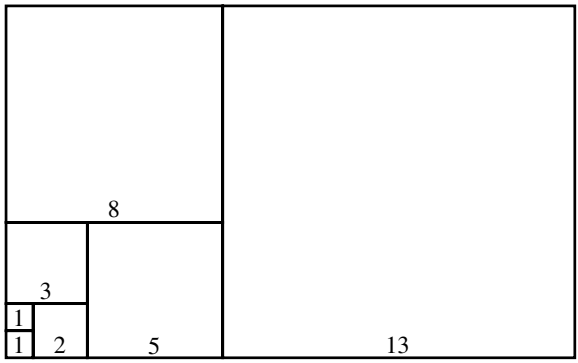
Rovnosti na posledních třech řádcích lze rekurentně použít pro výpočet Fibonacciho čísel s velkými indexy. Pomocí matematické indukce z nich lze též odvodit další elegantní vztah

$$\begin{pmatrix} K_{n+1} & K_n \\ K_n & K_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n, \quad n = 1, 2, \ldots$$

Povšimněte si, že (7.7) vlastně vyjadřuje rovnost determinantů těchto matic. Více než stovku podobných vztahů mezi Fibonacciho

a Lucasovými čísly lze nalézt v (Hoggatt, 1969), (Koshy, 2001) a (Vajda, 1989). Uveďme ještě některé z nich (viz též obr. 7.5):

$$\sum_{i=1}^{n} K_i = K_{n+2} - 1, \qquad \prod_{i=0}^{n-1} L_{2^i} = K_{2^n}, \qquad \sum_{i=0}^{n} \binom{n}{i} K_i = K_{2n}.$$



Obr. 7.5. Geometrická interpretace vztahu $\sum_{i=1}^{n} K_i^2 = K_n K_{n+1}$.

Determinanty tridiagonálních matic typu $n \times n$

$$T(n) = \begin{pmatrix} 3 & 1 & & & \\ 1 & 3 & 1 & & \\ & 1 & 3 & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & 1 & 3 \end{pmatrix}, \qquad U(n) = \begin{pmatrix} 1 & \mathrm{i} & & & \\ \mathrm{i} & 1 & \mathrm{i} & & \\ & \mathrm{i} & 1 & \ddots & \\ & & \ddots & \ddots & \mathrm{i} \\ & & & \mathrm{i} & 1 \end{pmatrix},$$

kde i je imaginární jednotka, jsou Fibonacciho čísly. Indukcí lze totiž odvodit, viz (Strang, 1998), (Cahill, D'Errico, Spence, 2003), že

$$\det T(n) = K_{2n+2} = \prod_{k=1}^{n} \Big(3 - 2\cos\frac{k\pi}{n+1}\Big),$$

$$\det U(n) = K_{n+1} = \prod_{k=1}^{n} \Big(1 - 2\mathrm{i}\cos\frac{k\pi}{n+1}\Big).$$

Tyto rozklady na činitele v reálné i komplexní aritmetice jsou dále zobecněny v (Seibert, Trojovský, 2007).

Slavný ruský matematik Jurij Matijasevič (Matiyasevich, 1992, s. 40) pomocí Fibonacciho čísel též negativně rozřešil desátý Hilbertův problém, který se týká řešitelnosti diofantských rovnic pomocí konečného počtu aritmetických operací, viz (Matiyasevich, 1970), (Jones, Matiysevich, 1991). V roce 1985 odvodil další překvapivý vztah (viz (Matiyasevich, Guy, 1986)) mezi Fibonacciho čísly a *Ludolfovým číslem* $\pi = 3.141\,592\,653\,589\ldots$, které je transcendentní (tj. není řešením žádné algebraické rovnice s celočíselnými koeficienty),

$$\pi = \lim_{n\to\infty} \sqrt{\frac{6\ln(K_1K_2\cdots K_n)}{\ln[K_1,K_2,\ldots,K_n]}},$$

kde $[K_1,K_2,\ldots,K_n]$ označuje nejmenší společný násobek Fibonacciho čísel $K_1,K_2,\ldots,K_n$.

James P. Jones v článku (Jones, 1975) dokázal, že množina všech kladných Fibonacciho čísel je totožná s množinou všech kladných hodnot následujícího polynomu pátého stupně ve dvou celočíselných proměnných:

$$p(x,y) = -x^4y - 2x^3y^2 + x^2y^3 + 2xy^4 - y^5 + 2y.$$

Například $p(1,1) = 1$, $p(2,3) = 3$, $p(8,13) = 13$.

Belgický matematik Eugène Charles Catalan (1814–1894) zavedl tzv. *Fibonacciho polynomy* pomocí rekurence podobné (7.1):

$$f_{n+2}(x) = x\,f_{n+1}(x) + f_n(x) \qquad \text{pro všechna } n = 0,1,2,\ldots,$$

kde $f_0(x) = 0$ a $f_1(x) = 1$. Přitom vidíme, že

$$f_n(1) = K_n.$$

Podobně lze definovat i Lucasovy polynomy. Jejich vlastnosti jsou uvedeny v knize (Koshy, 2001).

Ze vztahů (7.4) a (7.5) lze snadno dokázat, že platí

$$\alpha = \lim_{n\to\infty} \frac{K_{n+1}}{K_n} = \lim_{n\to\infty} \frac{L_{n+1}}{L_n}. \tag{7.8}$$

Zlatý řez α má celou řadu důležitých aplikací. Například jej lze použít k hledání minima spojité reálné (obecně nediferencovatelné) funkce J na uzavřeném intervalu $\langle a, b\rangle \subset \mathbb{R}$ (angl. *golden section search algorithm* – viz (Křížek, Neittaanmäki, 1990, s. 177)). Nechť bod minima x^* leží uvnitř $\langle a, b\rangle$ a pro jednoduchost předpokládejme, že J je na intervalu $\langle a, x^*\rangle$ klesající a na $\langle x^*, b\rangle$ rostoucí. Počáteční hodnoty algoritmu jsou dány takto $x_0 := a$, $x_3 := b$,

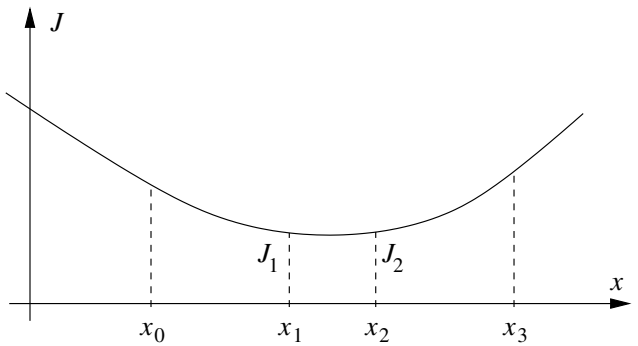
$$x_1 := \gamma x_3 - \beta x_0, \quad J_1 := J(x_1),$$
$$x_2 := \gamma x_0 - \beta x_3, \quad J_2 := J(x_2),$$

kde $\beta = \dfrac{1-\sqrt{5}}{2} = -\dfrac{1}{\alpha}$ a $\gamma = \beta^2 = \dfrac{3-\sqrt{5}}{2}$. Pokud $J_1 < J_2$, položíme (srov. obr. 7.6)

$$x_3 := x_2,\ x_2 := x_1,\ x_1 := x_0 + x_3 - x_2,\ J_2 := J_1,\ J_1 := J(x_1);$$

v opačném případě

$$x_0 := x_1,\ x_1 := x_2,\ x_2 := x_0 + x_3 - x_1,\ J_1 := J_2,\ J_2 := J(x_2).$$



Obr. 7.6. Hledání minima funkce *J* pomocí zlatého řezu.

Tento iterační proces opakujeme tak dlouho, až je rozdíl $x_3 - x_0$ dostatečně malý. Přitom v intervalu $\langle x_0, x_3\rangle$ bude ležet bod minima x^*. Poměry délek příslušných úseček během iteračního procesu

budou stále v poměru zlatého řezu α, viz (7.3). Vidíme například, že

$$\frac{x_3 - x_0}{x_3 - x_1} = \frac{x_3 - x_0}{x_3 - \beta^2 x_3 + \beta x_0} = \frac{x_3 - x_0}{-\beta x_3 + \beta x_0} = \alpha.$$

Podobně platí, že

$$\frac{x_3 - x_0}{x_2 - x_0} = \frac{x_2 - x_0}{x_2 - x_1} = \frac{x_3 - x_1}{x_2 - x_1} = \alpha.$$

Díky této vlastnosti lze ukázat, že počet vyhodnocení funkční hodnoty J (což může být někdy výpočetně velice náročné) je obecně nejmenší možný.

Fibonacciho čísla mají použití i v teorii her, v genetice, v hudbě,[5] pro třídicí algoritmy (angl. *Fibonacci sorting algorithm*), pro problém bankovních depozitů, pro řešení speciálních elektrických obvodů aj. Tyto aplikace lze nalézt například v knížkách (Hoggatt, 1969), (Koshy, 2001), (Schroeder, 2006).

Nejkrásnější vlastnosti Fibonacciho a Lucasových čísel. Na prvním místě uveďme Zeckendorfovu větu o úplnosti.

Věta 7.1 (Zeckendorfova). *Každé přirozené číslo lze jednoznačně vyjádřit jako součet různých Fibonacciho čísel K_i pro $i \geq 2$ tak, že žádné dva indexy i po sobě nenásledují.*

Její důkaz je uveden v (Brown, 1964). Na základě Zeckendorfovy věty můžeme tedy každé přirozené číslo napsat jako součet Fibonacciho čísel. To, že tento součet neobsahuje dvě po sobě následující Fibonacciho čísla, lze splnit díky vztahu (7.1). Budeme-li pro přirozené $n \geq 2$ psát 10^{n-2} místo K_n, pak všem celým nezáporným číslům můžeme přiřadit následující řetězce složené z nul

[5] Například chromatická stupnice na klavíru má 13 kláves, z toho 8 bílých a 2+3=5 černých.

a jedniček

$$0 \mapsto \underline{0}, \quad 1 \mapsto \underline{1}, \quad 2 \mapsto 1\underline{0}, \quad 3 \mapsto 10\underline{0}, \quad 4 = 3 + 1 \mapsto 10\underline{1},$$
$$5 \mapsto 100\underline{0}, \quad 6 = 5 + 1 \mapsto 100\underline{1}, \quad 7 = 5 + 2 \mapsto 101\underline{0},$$
$$8 \mapsto 1000\underline{0}, \quad 9 = 8 + 1 \mapsto 1000\underline{1}, \quad 10 = 8 + 2 \mapsto 1001\underline{0},$$
$$11 = 8 + 3 \mapsto 1010\underline{0}, \quad 12 = 8 + 3 + 1 \mapsto 1010\underline{1}, \ldots$$

Všimněte si, že z posledních cifer (jsou podtržené) lze sestavit řetězec, který je inverzní ke zlatému řetězci (7.2), tj. nuly a jedničky jsou prohozené. Není to malý zázrak?

Věta 7.2. *Každé přirozené číslo lze vyjádřit jako součet různých Lucasových čísel L_i pro $i \geq 0$.*

Důkaz je uveden například v knížce (Hoggatt, 1969, s. 73). Není těžké ukázat (viz (Koshy, 2001, s. 136), (Vorobiev, 2002, s. 57)), že každá dvě po sobě následující Fibonacciho čísla jsou nesoudělná, tj.

$$(K_{n+1}, K_n) = 1.$$

Tento výsledek lze zobecnit tak, jak uvádí věta 7.3.

Věta 7.3. *Pro libovolná přirozená čísla m a n platí*

$$(K_m, K_n) = K_{(m,n)},$$
$$K_m \mid K_n \iff m \mid n \tag{7.9}$$

a

$$L_m \mid L_n \iff \exists k \in \{1, 2 \ldots\} : \; m = (2k-1)n, \quad n > 1.$$

Důkazy jednotlivých tvrzení lze najít např. v (Hoggatt, 1969, s. 39–40), (Koshy, 2001, s. 198–200), (Vorobiev, 2002, s. 51–58).

Věta 7.4. *Číslo K_{mn} je dělitelné $K_m K_n$, právě když $(m, n) = 1, 2$ nebo 5.*

Věta 7.5. *Nechť $m > 1$ a $n > 1$. Pak je číslo L_{mn} dělitelné $L_m L_n$ právě tehdy, když m a n jsou lichá nesoudělná čísla.*

Důkazy předcházejících dvou vět lze najít v (Jarden, 1973, s. 1 a 3). Další pozoruhodná věta je uvedena v (Koshy, 2001, s. 422).

Věta 7.6. *Jestliže $p \geq 5$ je prvočíslo, pak $K_{p^2} \equiv p^2 \pmod{100}$, tj. dvě poslední cifry čísel p^2 a K_{p^2} jsou stejné.*

Následující tvrzení pochází od významného francouzského matematika Gabriela Lamého (1795–1870), viz (Koshy, 2001, s. 138–140).

Věta 7.7. *Nechť $2 \leq k \leq m$. Pak Eukleidův algoritmus pro (k, m) nepotřebuje více kroků, než je pětinásobek počtu cifer k. Dále platí, že $k \geq K_{n+1}$ a $m \geq K_{n+2}$, pokud Eukleidův algoritmus spotřebuje n kroků.*

Eukleidův algoritmus (viz oddíl 1.5) pro výpočet největšího společného dělitele spotřebuje nejvíce kroků, jestliže k a m jsou dvě po sobě následující Fibonacciho čísla. Je-li tedy $n \geq 2$, pak pro určení (K_{n+1}, K_{n+2}) je zapotřebí právě n dělení (srov. obr. 7.5).

Na závěr této části uveďme ještě jednu větu. Důkaz, který pro ukázku předvedeme, je podstatně jednodušší než původní důkaz J. H. Haltona z článku (Halton, 1964).

Věta 7.8 (Haltonova). *Nechť $n \geq m$ a nechť r je zbytek při dělení K_n číslem K_m. Pak buď r, nebo $K_m - r$ je Fibonacciho číslo.*

D ů k a z. Podle (7.4)

$$\begin{aligned} K_n &= \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= \frac{\alpha^m - \beta^m}{\alpha - \beta}(\alpha^{n-m} + \beta^{n-m}) - (\alpha\beta)^{\min(m,n-m)} \frac{\alpha^{|n-2m|} - \beta^{|n-2m|}}{\alpha - \beta} \\ &= K_m L_{n-m} - (-1)^{\min(m,n-m)} K_{|n-2m|}. \end{aligned}$$

Jestliže $|n-2m| < m$, potom $r = K_{|n-2m|}$ nebo $K_m - r = K_{|n-2m|}$. Pokud $|n-2m| \geq m$, pak dělíme $K_{|n-2m|}$ číslem K_m a pokračujeme tak dlouho, až bude zbytek menší než K_m. □

Prvočinitelé Fibonacciho čísel. Fibonacciho čísla 2, 3, 5, 13, 89, 233, 1597 aj. jsou prvočísla. Dodnes ovšem není známo, zda je jich nekonečně mnoho. Také Lucasova čísla 3, 7, 11, 29, 47, 199, 521 aj. jsou prvočísla a nevíme, zda jich je nekonečně mnoho. Protože platí ekvivalence (7.9), každé prvočíslo K_n s $n > 4$ musí mít index n prvočíselný. Naproti tomu $K_{19} = 37 \cdot 113$ je číslo složené, i když má prvočíselný index. Tabulky všech prvočinitelů Fibonacciho a Lucasových čísel pro $n \leq 385$ jsou obsaženy například v (Jarden, 1973).

Zajímavý objev učinil J. M. Zenger. Všiml si, že součin prvních sedmi prvočísel je roven

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = K_7 K_8 K_9 K_{10}. \tag{7.10}$$

V následující větě (viz (Křížek, Luca, Somer, 2006)) ukážeme, že tento pěkný příklad již nelze „zvětšit".

Věta 7.9. *Největší součin po sobě následujících prvočísel, který je roven součinu alespoň tří po sobě jdoucích Fibonacciho čísel, je* $K_7 K_8 K_9 K_{10}$.

D ů k a z. Nechť n je přirozené číslo. Označme $z(n)$ nejmenší přirozené číslo j takové, že $n \mid K_j$. Je známo, že takové $z(n)$ vždy existuje (Ribenboim, 1996, s. 60). Nejprve ukážeme, že platí

$$n \mid K_m \iff z(n) \mid m. \tag{7.11}$$

$\Rightarrow$: Nechť $n \mid K_m$ a označme $k = (z(n), m)$. Pak podle věty 7.3 je $(K_{z(n)}, K_m) = K_k$ a $k \leq z(n)$. Pokud $k < z(n)$, pak $n \mid K_k$, protože $n \mid K_{z(n)}$ a $n \mid K_m$. To je ale ve sporu s tím, že $z(n)$ je nejmenší přirozené číslo j takové, že $n \mid K_j$. Tudíž $k = z(n)$ a $z(n) \mid m$.

$\Leftarrow$: Nechť $z(n) \mid m$. Pak podle (7.9) platí $K_{z(n)} \mid K_m$. Protože n podle definice dělí $K_{z(n)}$, máme $n \mid K_m$.

Nyní dokážeme vlastní tvrzení věty. Pokud máme alespoň tři po sobě jdoucí indexy, pak alespoň jeden z nich je dělitelný třemi. Jestliže $3 \mid n$, pak pomocí ekvivalence (7.9) platí $K_3 \mid K_n$. Tedy K_n je sudé, protože $K_3 = 2$, a součin prvočísel na levé straně musí začínat 2.

Pokud by existoval příklad s ještě větším počtem činitelů, než je v (7.10), pak by levá strana musela obsahovat prvočíslo 19. Nejmenší Fibonacciho číslo dělitelné 19 je $K_{18} = 2584$. Podle (7.11) musí proto součin Fibonacciho čísel na pravé straně obsahovat index n dělitelný $z(19) = 18$, což je násobek 6. Avšak podle (7.9) je $K_6 \mid K_n$ a přitom $K_6 = 8 = 2^3$. Součin na levé straně tedy nemůže být součinem po sobě jdoucích prvočísel. □

Věta 7.10. *Pro každé $n \in \mathbb{N}$ je posloupnost zbytků $(K_i \pmod n)_{i=0}^{\infty}$ periodická.*

D ů k a z. Posloupnost $(K_i \pmod n)_{i=0}^{\infty}$ obsahuje nejvýše n různých zbytků. Podle Dirichletova principu (věta 1.5) tedy existuje $j \in \{0, 1, \ldots, n^2-1\}$ tak, že se uspořádaná dvojice $\langle K_j, K_{j+1}\rangle$ opakuje v posloupnosti Fibonacciho čísel modulo n, neboť takových dvojic je n^2. Posloupnost $(K_i \pmod n)_{i=0}^{\infty}$ je proto periodická pro $i \geq j$.

Sporem ukážeme, že $j = 0$. Nechť $j \geq 1$ je nejmenší číslo takové, že posloupnost $(K_i \pmod n)_{i=0}^{\infty}$ je periodická pro $i \geq j$ a nechť ℓ je perioda této posloupnosti. Pak $K_i \equiv K_{i+\ell} \pmod n$ pro všechna $i \geq j$. Speciálně $K_j \equiv K_{j+\ell} \pmod n$ a $K_{j+1} \equiv K_{j+1+\ell} \pmod n$. Pak ale

$$K_{j-1} = K_{j+1} - K_j \equiv K_{j+1+\ell} - K_{j+\ell} = K_{j-1+\ell} \pmod n$$

a $(K_i \pmod n)_{i=0}^{\infty}$ je tedy periodická i pro $i \geq j-1$, což je spor. Tedy $j = 0$ a posloupnost $(K_i \pmod n)_{i=0}^{\infty}$ je periodická od samého počátku. □

Navíc D. D. Wall dokázal, že délka periody posloupnosti zbytků $(K_i \pmod n)_{i=0}^{\infty}$ je pro $n > 2$ vždy sudá. Pro $n = 2, 3, 4$ jsou délky minimálních period postupně 3, 8 a 6. Snadno se můžete přesvědčit, že pro $n = 24$ je délka minimální periody také 24.

Prvočinitel p čísla K_n se nazývá *primitivní*, jestliže p nedělí K_m pro žádné přirozené $m < n$. Například $K_{12} = 144 = 2^4 \cdot 3^2$ nemá žádného primitivního prvočinitele, protože $2 \mid K_3$ a $3 \mid K_4$. Robert Daniel Carmichael, viz (Carmichael, 1913), dokázal následující velmi silnou větu.

Věta 7.11 (Carmichaelova). *Číslo K_n má alespoň jednoho primitivního prvočinitele pro všechna $n > 12$.*

Poznamenejme ještě, že primitivní prvočinitelé musí být poměrně velcí. Jestliže totiž $p \neq 5$ je primitivní prvočinitel K_n, pak $p \equiv 1 \pmod{n}$ pro $p \equiv 1, 4 \pmod 5$ a $p \equiv -1 \pmod{n}$ pro $p \equiv 2, 3 \pmod 5$. Tedy $p \geq n - 1$.

V. Drobot v článku (Drobot, 2000) dokázal pozoruhodnou souvislost Fibonacciho čísel s prvočísly p, pro něž $2p - 1$ je také prvočíslo (srov. oddíl 4.6). Je-li $p \equiv 2, 4 \pmod 5$ takové prvočíslo, pak $2p - 1 \mid K_p$, a tedy K_p není prvočíslo.

Wayne McDaniel odvodil, že K_n pro $n > 48$ má vždy alespoň jednoho prvočinitele tvaru $p \equiv 1 \pmod 4$, viz (McDaniel, 2002). Odtud mj. plyne, že všechna Fibonacciho prvočísla kromě 2 a 3 mají také tento tvar. Pravděpodobnost, že K_n má prvočinitele tvaru $p \equiv 3 \pmod 4$, je právě $\frac{1}{2}$, viz (Luca, 2003a). Naproti tomu hustota množiny prvočinitelů Lucasových čísel je jen $\frac{2}{3}$ (podrobnosti viz (Křížek, Luca, Somer, 2005)).

Další vlastnosti Fibonacciho čísel. Nejprve připomeňme (viz oddíl 4.8, strana 154), že přirozené číslo m se nazývá *palindromem v číselné soustavě o základu b*, jestliže řetězec jeho cifer je stejný, když se čte zleva doprava jako zprava doleva. Například $K_{10} = 55$, $L_5 = 11$ a $L_{25} = 167761$ jsou palindromy v desítkové soustavě. Označíme-li $\mathcal{P}_b$ množinu přirozených čísel n, pro něž K_n nebo L_n je palindrom v bázi $b > 1$, pak asymptotická hustota množiny $\mathcal{P}_b$ je nula, viz (Luca, 2003b), tj.

$$\lim_{m\to\infty} \frac{|\{n \in \mathcal{P}_b;\ n \leq m\}|}{m} = 0,$$

kde $|\cdot|$ značí počet prvků. Tento výsledek ale není tak silný, aby z něj šlo odvodit, že suma převrácených hodnot prvků z $\mathcal{P}_b$ je konvergentní.

I. J. Good ve své práci (Good, 1974) zjistil, že

$$\sum_{n=0}^{\infty} \frac{1}{K_{2^n}} = \frac{7-\sqrt{5}}{2}.$$

Toto iracionální číslo je algebraické, neboť je kořenem polynomu s celočíselnými koeficienty.

Pro β z (7.3) a všechna komplexní čísla z taková, že $|z| < |\beta|$, je splněna rovnost (viz (Schroeder, 2006, s. 225))

$$\sum_{i=1}^{\infty} K_i z^i = \frac{z}{1-z-z^2}. \tag{7.12}$$

Racionální funkce na pravé straně (7.12) se nazývá *vytvořující funkce* Fibonacciho posloupnosti. Speciálně pro $z = \frac{1}{2}$ mocninná řada v (7.12) konverguje a platí

$$\sum_{i=1}^{\infty} \frac{K_i}{2^i} = 2.$$

Největší přirozené číslo n takové, že $K_n = x^2$ pro nějaké celé x, je $n = 12$, viz (Ljunggren, 1951). Je tedy přirozené se ptát, jaké jsou všechny mocniny ve Fibonacciho posloupnosti. Díky vztahu (7.9) stačí uvažovat jen prvočíselné exponenty. Vznikla domněnka, že $K_{12} = 144$ je největší taková mocnina. H. London a R. Finkelstein ji dokázali pro exponent 3 (viz (London, Finkelstein, 1969)) a J. McLaughlin pro exponenty 5, 7, 11, 13 a 17, viz (McLaughlin, 2002). V roce 2004 byla nakonec domněnka dokázána pro všechny exponenty, viz (Bugeaud, Mignotte, Siksek, 2004).

Fibonacciho čísla se objevují zcela nečekaně při řešení některých diofantských rovnic. Ilustrujme to na následující úloze. *Diofantská čtveřice* je množina čtyř racionálních čísel takových, že součin libovolných dvou čísel z této čtveřice zvětšený o jednu je čtvercem racionálního čísla. Diofantos z Alexandrie jednu takovou čtveřici nalezl $\left\langle \frac{1}{16}, \frac{33}{16}, \frac{68}{16}, \frac{105}{16} \right\rangle$. První, kdo zkonstruoval podobné

řešení s celočíselnými hodnotami

$$\langle 1, 3, 8, 120\rangle,$$

byl Pierre de Fermat. Skutečnost, že první tři členy této čtveřice jsou Fibonacciho čísla, umožnila odhalit mnohem obecnější řešení. Pro $k \geq 1$ je

$$\langle K_{2k},\ K_{2k+2},\ K_{2k+4},\ 4K_{2k+1}\,K_{2k+2}\,K_{2k+3}\rangle$$

vždy diofantskou čtveřicí. Je-li totiž x takové, že $xK_i + 1$ je čtverec pro všechna $i \in \{2k,\ 2k+2,\ 2k+4\}$, pak (viz (Dujella, 1999))

$$x = 4K_{2k+1}\,K_{2k+2}\,K_{2k+3}.$$

D. A. Lind hledal řešení diofantské rovnice pro binomické koeficienty (viz (Lind, 1968))

$$\binom{n}{k} = \binom{n-1}{k+1} \tag{7.13}$$

a překvapivě našel nekonečnou třídu řešení

$$\langle n, k\rangle = \langle K_{i+2}\,K_{2i+3}, K_i\,K_{2i+3}\rangle \ \text{ pro } \ i = 0,\ 1,\ \ldots$$

Existuje domněnka, že diofantská rovnice

$$\binom{n}{k} = \binom{m}{\ell} \qquad \text{pro } n > m,\ k \leq n/2,\ \ell \leq m/2$$

má jen konečně mnoho celočíselných řešení $\langle n, k, m, \ell\rangle$ kromě těch, která tvoří již zmíněnou nekonečnou třídu řešení rovnice (7.13) ve Fibonacciho číslech.

Na závěr se zmíníme o Fibonacciho číslech dalších tvarů. V článku (Luca, 1999) je dokázáno, že $K_{12} = 3!4!$ je největší Fibonacciho číslo, které je součinem faktoriálů. Navíc

$$K_1\,K_2\,K_3\,K_4\,K_5\,K_6\,K_8\,K_{10}\,K_{12} = 11!$$

je největším faktoriálem, který je součinem různých Fibonacciho čísel. Poznamenejme ještě, že existuje jen konečně mnoho Fibonacciho čísel, která lze vyjádřit jako sumu nejvýše k faktoriálů pro každé pevné k, ale stanovit takovou sumu pro $k \geq 3$ je z výpočetního hlediska velice obtížné.

Poznámka. Pokud vám v hlavě stále vrtá geometrický paradox z obr. 7.4, pak vám napovíme, že nejmenší z úhlů trojúhelníku A je $\operatorname{arctg}\frac{3}{8} = 20,56°$, zatímco u trojúhelníku A' je to $\operatorname{arctg}\frac{5}{13} = 21,04°$ (srov. též (7.8)). Tento malý rozdíl v obrázku 7.4 není téměř vidět. Autorem paradoxu je matematik C. L. Dodgson, známý jako Lewis Carroll, autor knížky *Alenka v říši divů*.

7.2. Mnohoúhelníková čísla

Pro přirozené k definujme *k-úhelníková* (*polygonální* nebo též *figurální*) *čísla* $P_{k,n}$ jako součet prvních n členů aritmetické posloupnosti $((m-1)(k-2)+1)_{m=1}^{\infty}$ s počátečním členem 1 a diferencí $k-2$, tj.

$$P_{k,n} = 1+(k-1)+(2k-3)+(3k-5)+\cdots+((n-1)(k-2)+1). \tag{7.14}$$

Většinou se uvažují jen pro případ $k \geq 3$, který odpovídá pravidelným mnohoúhelníkům. Například pro $k = 3,4,5$ a $n = 1,2,3,4$ jsou mnohoúhelníková čísla $P_{k,n}$ na obrázku 7.7 znázorněna pravidelnými mnohoúhelníky s k stranami a n puntíky na každé straně, přičemž celkový počet puntíků je $P_{k,n}$.

Označme T_n *trojúhelníková čísla* $P_{3,n}$. Podobně můžeme definovat symbol S_n pro *čtvercová čísla* $P_{4,n}$ nebo P_n pro *pětiúhelníková čísla* $P_{5,n}$. Užijeme-li vzorec pro součet prvních n členů aritmetické posloupnosti (7.14), vidíme, že

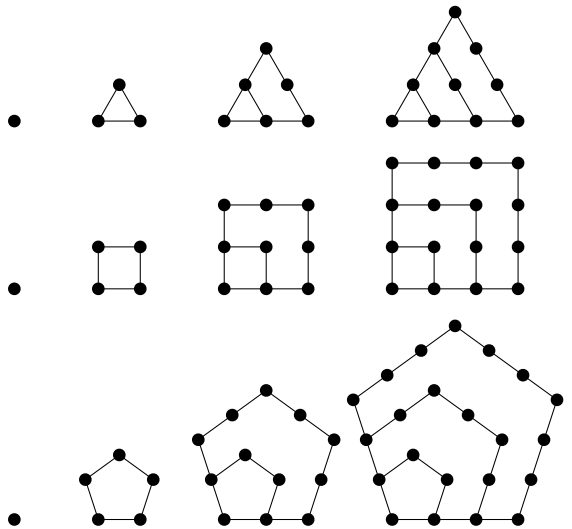
$$P_{k,n} = \frac{n}{2}[1+(1+(n-1)(k-2))] = \frac{n}{2}[(n-1)(k-2)+2]. \tag{7.15}$$

Speciálně tedy

$$\begin{aligned} T_n &= \frac{n(n+1)}{2} = 1+2+\cdots+n, \qquad (7.16)\\ S_n &= n^2,\\ P_n &= \frac{n(3n-1)}{2}, \end{aligned}$$

a pro $n = 1, 2, 3, 4, 5, 6, \ldots$ dostaneme

1, 3, 6, 10, 15, 21,... (trojúhelníková čísla),
1, 4, 9, 16, 25, 36,... (čtvercová čísla),
1, 5, 12, 22, 35, 51,... (pětiúhelníková čísla).



Obr. 7.7. Geometrická interpretace trojúhelníkových, čtvercových a pětiúhelníkových čísel.

Z prostředního řádku obr. 7.7 také vidíme, že každé čtvercové číslo je součtem po sobě následujících lichých čísel.

$$n^2 = 1 + 3 + 5 + \cdots + (2n - 3) + (2n - 1),$$

což lze ostatně přímo dokázat i ze vzorce pro součet konečného počtu členů aritmetické posloupnosti. Dále snadno zjistíme, že

$$T_n = n + T_{n-1},$$
$$S_n = n + 2T_{n-1},$$
$$P_n = n + 3T_{n-1}$$

a obecně

$$P_{k,n} = n + (k-2)T_{n-1}.$$

S mnohoúhelníkovými čísly se setkáváme v řadě situací. Například v Bohrově modelu atomu vodíku mají dráhy, po nichž může obíhat elektron jádro, poloměry úměrné $S_n = n^2$. V následující kapitole 8 ukážeme, jak trojúhelníková čísla (7.16) souvisí s bicím strojem pražského orloje. Uveďme si tedy některé jejich zajímavé vlastnosti. Tak například Luo (viz (Luo, 1989)) dokázal, že největší Fibonacciho trojúhelníkové číslo je $K_{10} = 55$. Ze vztahu (7.16) pro $n = 8$ se zase snadno sami můžete přesvědčit, že čtvercové číslo $36 = 6^2$ je zároveň i trojúhelníkové.

Nyní rozšíříme posloupnost mnohoúhelníkových čísel o členy $P_{0,0} = P_{1,0} = P_{2,0} = \cdots = 0$, tedy

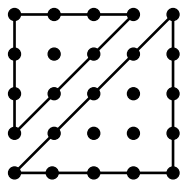
$$T_0 = 0, \quad S_0 = 0 \quad \text{a} \quad P_0 = 0.$$

Pak platí věty, které uvádíme dále.

Věta 7.12. *Součet dvou po sobě následujících trojúhelníkových čísel je čtvercem přirozeného čísla.*

D ů k a z. Pro přirozené n máme

$$T_{n-1} + T_n = \frac{n(n-1)}{2} + \frac{n(n+1)}{2} = n^2. \qquad \square$$



Obr. 7.8. Geometrická interpretace věty 7.12.

Jiná věta ukazuje, že k-úhelníkové číslo je součtem $(k-1)$-úhelníkového čísla a trojúhelníkového čísla.

Věta 7.13. *Pro libovolné $k, n \in \mathbb{N}$ platí*

$$P_{k,n} = P_{k-1,n} + T_{n-1}.$$

D ů k a z. Ze vztahů (7.15) a (7.16) plyne

$$\begin{aligned} P_{k,n} &= \frac{n}{2}(n(k-2)+4-k) \\ &= \frac{n}{2}(n(k-3)+5-k) + \frac{n}{2}(n-1) = P_{k-1,n} + T_{n-1}. \end{aligned}$$ □

Věta 7.14. *Pro libovolné $k, n \in \mathbb{N}$ platí*

$$8(k-2)P_{k,n} + (k-4)^2 = (2kn - 4n - k + 4)^2.$$

D ů k a z. Ze vztahu (7.15) plyne

$$\begin{aligned} 8(k-2)P_{k,n} + (k-4)^2 &= 8(k-2)\frac{n}{2}(n(k-2)+4-k) + (k-4)^2 \\ &= [(2n)(k-2)]^2 + 4n(k-2)(4-k) + (4-k)^2 \\ &= (2kn - 4n - k + 4)^2. \end{aligned}$$ □

Speciálně pro $k = 3$ obdržíme

$$8T_n + 1 = (2n+1)^2,$$

a tedy $8T_n + 1$ je čtvercem přirozeného čísla (srov. obr. 8.8 v další kapitole). Pro $k = 5$ dostaneme

$$24P_n + 1 = (6n-1)^2 \quad \text{a} \quad P_n = n^2 + T_{n-1}.$$

Pro $k = 6$ je $P_{6,n} = T_{2n-1}$.

Věta 7.15. *Každé přirozené číslo lze vyjádřit jako součet k-úhelníkových čísel s nejvýše k sčítanci.*

Tuto větu vyslovil již Pierre Fermat. Tvrdil, že má i její důkaz, který ale nikdy nebyl nalezen. Větu 7.15 pro případ $k = 4$ (tzv. čtvercovou větu) znal již Diofantos, ale dokázal ji až C. G. Jacobi, J. L. Lagrange (1772) a L. Euler: *Každé přirozené číslo je součtem čtyř čtverců.* C. F. Gauss v roce 1796 podal důkaz věty 7.15 pro případ trojúhelníkových čísel. Úplný důkaz pro libovolné k však

podal až A. L. Cauchy v roce 1813, viz (Guy, 1994a). Podle věty 7.15 pro $k = 3$ například platí, že

$$18 = 0 + 3 + 15 = T_2 + T_5.$$

Podobně pro $k = 4$ máme

$$1634 = 1^2 + 9^2 + 16^2 + 36^2 = S_1 + S_9 + S_{16} + S_{36}.$$

Zabývejme se nyní pozoruhodnou větou pocházející od Eulera, která svazuje tzv. zobecněná pětiúhelníková čísla a rozklady čísel na sčítance. Označme $p(n)$ počet vzájemně různých způsobů, kterými můžeme vyjádřit číslo n jako součet jednoho či více přirozených čísel bez ohledu na pořadí sčítanců (přitom klademe $p(0) = 1$). Tak například $p(4) = 5$, protože

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1.$$

Zobecněná pětiúhelníková čísla definujme vztahem

$$P_j = \frac{3j^2 - j}{2} \quad \text{pro } j = 0, 1, 2, \ldots,$$
$$P_j = \frac{3j^2 + j}{2} \quad \text{pro } j = -1, -2, \ldots$$

Vidíme tedy, že jejich definice souhlasí s běžnými pětiúhelníkovými čísly pro j přirozené.

Věta 7.16 (Eulerova). *Pro každé přirozené číslo n platí*

$$\begin{aligned} p(n) &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) \\ &\quad + p(n-15) - p(n-22) - \ldots \\ &= \sum_j (-1)^{j+1} p\Big(n - \frac{3j^2 + j}{2}\Big) + \sum_j (-1)^{j+1} p\Big(n - \frac{3j^2 - j}{2}\Big), \end{aligned}$$

kde sčítáme přes všechna přirozená čísla j, pro něž argumenty v $p(\cdot)$ jsou nezáporné.

Důkaz této věty je uveden v (Hardy, Wright, 1979, s. 284) a (Niven, Zuckerman, Montgomery, 1991, s. 456).

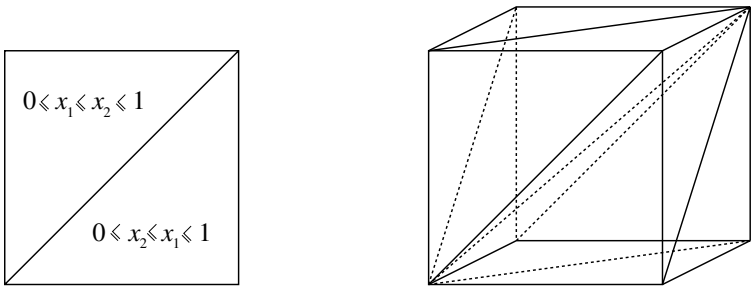
Podobně jako mnohoúhelníková (polygonální) čísla lze definovat i čísla polyedrická. Například podle věty 7.12 a (7.16) platí

$$2T_{n-1} = n^2 - n,$$

což lze zobecnit do trojrozměrného prostoru takto: Krychli rozdělíme na 6 čtyřstěnů o stejném objemu, které mají společnou prostorovou úhlopříčku (obr. 7.9). Proto platí

$$6A_{n-1} = n^3 - n,$$

kde $A_n = \frac{1}{6}n(n+1)(n+2)$ jsou čtyřstěnná (tetraedrální) čísla, $A_1 = 1$, $A_2 = 4$, $A_3 = 10$ atd.



Obr. 7.9. Dělení jednotkového čtverce na dva trojúhelníky a dělení jednotkové krychle na 6 čtyřstěnů. Souřadnice bodů jednoho z nich splňují nerovnosti $0 \leq x_1 \leq x_2 \leq x_3 \leq 1$.

Analogickým způsobem můžeme vyšetřovat i další polyedrická čísla. Například *pyramidální čísla* 1, 5, 14, 30, 55, 91, 140,... dostaneme jako částečné součty čtvercových čísel

$$S_1 + S_2 + \cdots + S_n = \frac{1}{6}n(n+1)(2n+1).$$

Jistě si sami odvodíte podobné vztahy pro čísla krychlová, osmistěnná (oktaedrální) apod. Taková zobecnění lze dále ještě rozšiřovat i do d-rozměrných prostorů a získat tak čísla polytopická (např. d-krychlová).

7.3. Dokonalá čísla

Dokonalými čísly jsme se zabývali již v oddílu 4.1, kde jsme ukázali, jak úzce souvisí s Mersennovými prvočísly. Připomeňme, že přirozené číslo n se nazývá *dokonalé*, jestliže se rovná součtu všech svých dělitelů menších než n. Například

$$\begin{aligned} 6 &= 1+2+3,\\ 28 &= 1+2+4+7+14,\\ 496 &= 1+2+4+8+16+31+62+124+248,\\ 8128 &= 1+2+4+8+16+32+64+127+254+508\\ &\quad +1016+2032+4064. \end{aligned}$$

Tato čtyři dokonalá čísla znal již novopythagorejec Nikomachos z Gerasy (kolem roku 100 n. l.). Díky Eukleidově větě 4.5 a Eulerově větě 4.6 můžeme snadno stanovit další dokonalá čísla

$$33\,550336,\ \ 8589\,869056,\ \ 137438\,691328,$$
$$2\,305843\,008139\,952128,\ldots$$

Zatím známe právě tolik dokonalých čísel, kolik je Mersennových prvočísel. Povšimněme si, že pro součet převrácených hodnot všech dělitelů dokonalých čísel platí

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=2,$$

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{7}+\frac{1}{14}+\frac{1}{28}=2$$

apod. Tuto vlastnost si nyní dokážeme pro libovolné dokonalé číslo. Podobně jako v oddílu 4.1 budeme symbolem $\sigma(n)$ nadále značit součet všech kladných dělitelů n (včetně n), tj.

$$\sigma(n)=\sum_{d|n} d. \tag{7.17}$$

Věta 7.17. *Přirozené číslo n je dokonalé právě tehdy, když*

$$\sum_{d|n} \frac{1}{d} = 2.$$

D ů k a z. Podle definice dokonalého čísla platí

$$2n = \sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d},$$

což dokazuje větu. □

Jako přímý důsledek dostáváme následující tvrzení, viz (Burton, 1998, s. 204).

Věta 7.18. *Jestliže n je dokonalé, $m < n$ a $m \mid n$, pak m není dokonalé.*

Z Eukleidovy věty 4.5 a Eulerovy věty 4.6 lze odvodit další poněkud překvapivou vlastnost sudých dokonalých čísel.

Věta 7.19. *Všechna sudá dokonalá čísla jsou trojúhelníková.*

D ů k a z. Z vět 4.5 a 4.6 dostáváme následující souvislost mezi sudými dokonalými čísly n a Mersennovými prvočísly M_p,

$$n = 2^{p-1}(2^p - 1) = \frac{2^p}{2}(2^p - 1) = 1 + 2 + \cdots + (2^p - 1). \quad (7.18)$$

Odtud a z (7.16) je již vidět, že n je trojúhelníkové číslo. □

Dokažme si nyní několik dalších jednoduchých vlastností dokonalých čísel.

Věta 7.20. *Jestliže n je dokonalé, pak n není mocninou prvočísla.*

D ů k a z. Předpokládejme naopak, že $n = p^k$, kde p je prvočíslo a k je přirozené číslo. Pak

$$\sigma(n) = 1 + p + p^2 + \cdots + p^k = 1 + p(1 + p + \cdots + p^{k-1}),$$

a tedy $p \nmid \sigma(n)$. Tudíž $\sigma(n) \neq 2p^k$. □

Pro libovolná nesoudělná přirozená čísla r a s z definice (7.17) plyne, že

$$\sigma(rs) = \sigma(r)\sigma(s). \tag{7.19}$$

Tento vztah dále několikrát využijeme.

Věta 7.21. *Jestliže n je dokonalé, pak n není čtvercem.*

Důkaz. Předpokládejme naopak, že $n = m^2$. Pak

$$n = \prod_{i=1}^{r} p_i^{k_i},$$

kde $2 \mid k_i$ pro $i = 1, 2, \ldots, r$. Odtud a z (7.19) indukcí plyne, že

$$\sigma(n) = \sigma\Big(\prod_{i=1}^{r} p_i^{k_i}\Big) = \prod_{i=1}^{r} \sigma\big(p_i^{k_i}\big).$$

Vidíme ale, že

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \tag{7.20}$$

je liché pro $i = 1, 2, \ldots, r$, protože k_i je sudé. Tudíž v (7.20) je lichý počet členů a $\sigma(n)$ je také liché číslo. Proto $\sigma(n) \neq 2n$. □

Věta 7.22. *Pokud je n sudé dokonalé číslo tvaru* (7.18)*, pak n lze binárně zapsat takto:*

$$111\ldots1000\ldots0,$$

kde je p jedniček a $p-1$ nul.

Důkaz. Tvrzení věty plyne okamžitě z vyjádření (7.18) jako speciálního trojúhelníkového čísla.

Věta 7.23. *Číslo n dané* (7.18) *končí buď na* 6*, nebo* 8*. Pokud navíc končí na* 8*, musí končit na* 28*.*

Důkaz. Nejprve ukážeme, že $n \equiv 6$ nebo $8 \pmod{10}$. Je-li $p = 2$, pak podle (7.18) je $n = 6$. Předpokládejme tedy, že p je liché, tj. $p - 1$ je sudé. Nyní snadno prověříme, že $2^{p-1} \equiv 6$

(mod 10), pokud $p-1 = 4k$, a $2^{p-1} \equiv 4 \pmod{10}$, pokud $p-1 = 4\ell + 2$ pro nějaká přirozená čísla k a ℓ.

Jestliže $2^{p-1} \equiv 6 \pmod{10}$, pak podle (7.18) je

$$n = 2^{p-1}(2^p - 1) \equiv 6(2 \cdot 6 - 1) \equiv 6 \cdot 11 \equiv 6 \pmod{10}.$$

Jestliže $2^{p-1} \equiv 4 \pmod{10}$, pak podobně dostaneme

$$n = 4(2 \cdot 4 - 1) \equiv 4 \cdot 7 \equiv 8 \pmod{10}.$$

Zbytek tvrzení o posledním dvojčíslí je dokázán v (Burton, 1998, s. 203–204). □

V Heatově větě 4.8 jsme ukázali, že každé sudé dokonalé číslo kromě 6 lze vyjádřit jako součet třetích mocnin lichých čísel. Na druhé straně v článku (Mąkowski, 1962) je ukázáno, že

$$28 = 2^2(2^3 - 1) = 3^3 + 1^3$$

je jediné sudé dokonalé číslo, které je tvaru $m^3 + 1$, kde m je přirozené číslo.

Věta 7.24 (Mąkowského). *Jediné sudé dokonalé číslo tvaru* m^3+1 *je* 28.

D ů k a z. Všechna sudá dokonalá čísla jsou tvaru (7.18). Tudíž pro prvočíslo $p \geq 3$ máme $2^{p-1} \equiv 1 \pmod{3}$, $2^p - 1 \equiv 1 \pmod{3}$, což dává $2^{p-1}(2^p - 1) \equiv 1 \pmod{3}$. Jestliže $2^{p-1}(2^p - 1) = m^3 + 1$, pak m je dělitelné 3, tj. $m = 3y$ a

$$2^{p-1}(2^p - 1) = (m + 1)(m^2 - m + 1).$$

Vidíme, že

$$(m+1, m^2-m+1) = (m+1, -2m+1) = (m+1, 3) = (3y+1, 3) = 1.$$

Protože $m > 2$, platí $m^2 - m + 1 > m + 1 > 1$. Ale jediné vyjádření sudého dokonalého čísla jako součinu dvou nesoudělných kladných čísel větších než 1 je dáno vztahem (7.18). Tudíž $m + 1 = 2^{p-1}$ a $m^2 - m + 1 = 2^p - 1$. Odečteme-li od poslední rovnice $2m + 2 = 2^p$, dostaneme $m^2 - 3m - 1 = -1$. Tedy $m(m - 3) = 0$, odkud plyne, že $m = 3$. □

Jako důsledek dostáváme následující tvrzení.

Věta 7.25. *Jediné sudé dokonalé číslo tvaru* $m^m + 1$ *je* 28.

D ů k a z. Pokud je $m^m + 1$ sudé dokonalé číslo, pak m je dělitelné 3, tj. $m = 3k$ a $[(3k)^k]^3 + 1$ je sudé dokonalé číslo. Podle předchozí věty $(3k)^k = 3$, a tudíž $k = 1$, $m = 3$ a $m^m + 1 = 28$. □

Odtud plyne další věta.

Věta 7.26. *Neexistuje sudé dokonalé číslo tvaru* $m^{m^{\cdot^{\cdot^{\cdot^m}}}} + 1$.

Tento výsledek je dále rozšířen v (Sinha, 1974) na čísla tvaru $a^{m^{\cdot^{\cdot^{\cdot^m}}}} + 1$. V tomto článku je též ukázáno, že 28 je jediné dokonalé číslo tvaru $a^n + b^n$, kde $n \geq 2$ a $(a, b) = 1$, což zobecňuje Mąkowského větu 7.24.

Otevřených problémů týkajících se dokonalých čísel je celá řada, viz poslední odstavec oddílu 4.1 a (Šalát, 1964).

7.4. Deficientní a abundantní čísla

Pro přirozené číslo n položme

$$s(n) = \sigma(n) - n = \sum_{\substack{d|n \\ d<n}} d, \tag{7.21}$$

kde $\sigma(n)$ je definováno vztahem (7.17). Hodnota $s(n)$ je součtem tzv. *alikvotních částí*, tj. součtem všech dělitelů čísla n menších než n. Dokonalé číslo je tak plně charakterizováno vztahem (obr. 7.10)

$$s(n) = n.$$

Přirozené číslo n se nazývá *deficientní,* popř. *abundantní,* jestliže

$$s(n) < n, \quad \text{popř.} \quad s(n) > n.$$

Podle této definice jsou

$1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19, \ldots$ deficientní čísla a

$12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 60, \ldots$ abundantní čísla.

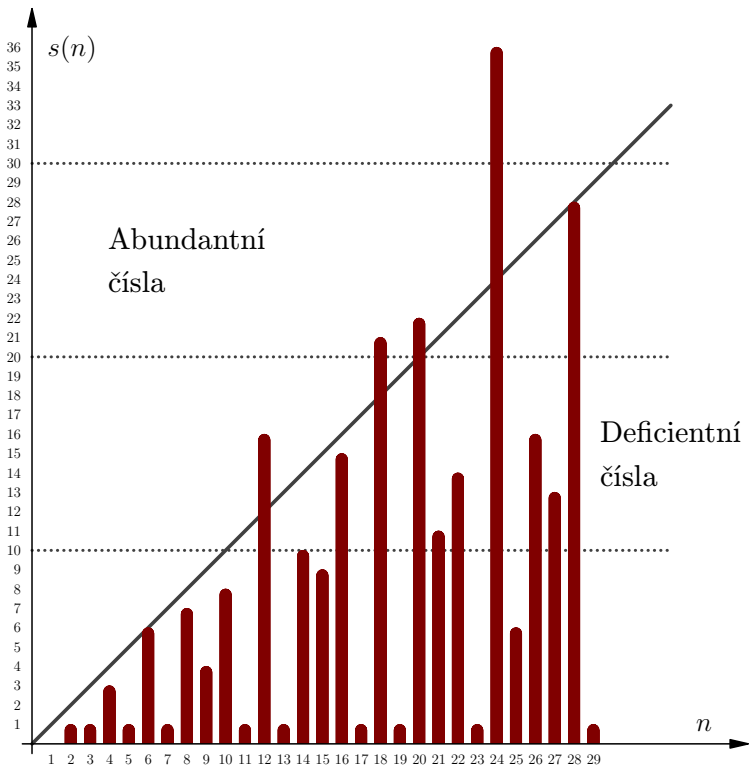
Například $14 = 2 \cdot 7$ je deficientní, protože

$$s(14) = 1 + 2 + 7 < 14.$$

Na druhé straně číslo $12 = 2^2 \cdot 3$ je abundantní, neboť

$$s(12) = 1 + 2 + 3 + 4 + 6 > 12.$$

Nejmenší liché abundantní číslo je 945.



Obr. 7.10. Graf závislosti *s*(*n*) na *n*. Diagonála odpovídá dokonalým číslům.

Symbolem $\sigma(n)$ budeme nadále opět značit součet všech kladných dělitelů n (bez násobnosti). Jak již bylo řečeno v části 4.1, zatím nevíme, zda existuje nekonečně mnoho sudých dokonalých čísel, žádné liché dokonalé číslo neznáme. Naproti tomu platí následující věta.

Věta 7.27. *Existuje nekonečně mnoho sudých i lichých deficientních i abundantních čísel.*

D ů k a z. Budeme rozlišovat následující čtyři případy:

a) Všechna čísla 2^k pro $k \geq 1$ jsou sudá a deficientní, neboť
$$s(2^k) = 2^k - 1 < 2^k.$$

b) Nechť p je liché prvočíslo a $k \geq 1$. Pak p^k je liché a deficientní, neboť
$$s(p^k) = 1 + p + p^2 + \cdots + p^{k-1} = \frac{p^k - 1}{p - 1} < \frac{p^k}{p - 1} < p^k.$$

c) Všechna čísla dělitelná 12 jsou sudá a abundantní, protože
$$\frac{s(n)}{n} > \frac{1}{2} + \frac{1}{3} + \frac{1}{4} > 1.$$

d) Nechť $n = 945\,k$, kde k je libovolné liché přirozené číslo, které není dělitelné 3, 5 a 7. Protože $945 = 3^3 \cdot 5 \cdot 7$, vidíme, že $(945, k) = 1$, a tedy podle (7.19)
$$\begin{aligned}\sigma(n) &= \sigma(945)\,\sigma(k) = \sigma(3^3)\,\sigma(5)\,\sigma(7)\,\sigma(k)\\ &= 40 \cdot 6 \cdot 8 \cdot \sigma(k) \geq 1920\,k > 2 \cdot 945\,k,\end{aligned}$$
protože $\sigma(k) \geq k$. Každé n uvedeného tvaru je podle (7.21) abundantní a zřejmě i liché. □

Poznamenejme, že Claude Gaspard Bachet de Méziriac podal poměrně zdlouhavý důkaz Eukleidovy věty 4.5 s dodatkem: *Je-li* $2^q - 1$ *číslo složené, pak je číslo* $n = 2^{q-1}(2^q - 1)$ *abundantní,* viz (Porubský, 2002, s. 54). Označíme-li $A(x)$ počet abundantních čísel nepřevyšujících x, pak
$$0.241x < A(x) < 0.314x,$$
což znamená, že většina přirozených čísel je deficientních.

7.5. Spřátelená čísla

Přirozená čísla m a n se nazývají *spřátelená,* jestliže každé z nich je rovné součtu všech kladných dělitelů druhého čísla kromě jeho samotného, tj. jestliže

$$\sum_{\substack{d|m\\ d<m}} d = n \quad \text{a} \quad \sum_{\substack{d|n\\ d<n}} d = m.$$

Další ekvivalentní vyjádření spřátelených čísel m a n je dáno rovnostmi

$$\sigma(m) = m + n = \sigma(n). \tag{7.22}$$

Každé dokonalé číslo je tedy samo se sebou spřátelené. Snadno lze ověřit, že $220 = 2^2 \cdot 5 \cdot 11$ a $284 = 2^2 \cdot 71$ jsou spřátelená čísla, první z nich je abundantní a druhé deficientní a přitom platí

$$220 = 1 + 2 + 4 + 71 + 142,$$
$$284 = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110.$$

Je to nejmenší známý pár takových čísel, která nejsou dokonalá. Řecký učenec Iamblichos (250–330 n. l.) připsal znalost této dvojice již pythagorejcům, viz též (Burton, 1998, s. 213). Kdybychom rozšířili graf z obrázku 7.10 až do 284, pak by přímka spojující funkční hodnoty $s(220)$ a $s(284)$ měla směrnici -1.

První explicitní pravidlo pro vyjádření speciálních spřátelených čísel nalezl proslulý arabský matematik Abu-l-Hasan Thabit ibn Qurra z Bagdádu již v 9. století, viz (Porubský, 2002).

Věta 7.28 (Thabitova). *Jestliže jsou čísla* $p = 3 \cdot 2^{k-1} - 1$, $q = 3 \cdot 2^k - 1$ *a* $r = 9 \cdot 2^{2k-1} - 1$ *prvočísly pro* $k \geq 2$, *pak* $2^k pq$ *a* $2^k r$ *jsou spřátelená čísla.*

D ů k a z. Položíme-li $m = 2^k pq$ a $n = 2^k r$, pak

$$\begin{aligned} m+n &= 2^k(3\cdot 2^{k-1}-1)(3\cdot 2^k-1)+2^k(9\cdot 2^{2k-1}-1)\\ &= 2^k(9\cdot 2^{2k-1}-3\cdot 2^{k-1}-3\cdot 2^k+1)+2^k(9\cdot 2^{2k-1}-1)\\ &= 9\cdot 2^{3k-1}-3\cdot 2^{2k-1}-3\cdot 2\cdot 2^{2k-1}+2^k+9\cdot 2^{3k-1}-2^k\\ &= 2\cdot 9\cdot 2^{3k-1}-9\cdot 2^{2k-1} = 9\cdot 2^{2k-1}(2^{k+1}-1). \end{aligned} \tag{7.23}$$

Protože pro $k \geq 2$ jsou čísla 2^k, p a q nesoudělná, můžeme použít vztah (7.19),

$$\sigma(m) = \sigma(2^k)\,\sigma(p)\,\sigma(q). \tag{7.24}$$

Jelikož p a q jsou prvočísla, platí $\sigma(p) = p+1$ a $\sigma(q) = q+1$. Dále použijeme vztah pro součet geometrické řady

$$\sigma(2^k) = 1+2+2^2+\cdots 2^k = \frac{2^{k+1}-1}{2-1} = 2^{k+1}-1.$$

Dohromady tedy ze (7.24) a (7.23) plyne, že

$$\sigma(m) = (2^{k+1}-1)(3\cdot 2^{k-1})(3\cdot 2^k) = (2^{k+1}-1)9\cdot 2^{2k-1} = m+n. \tag{7.25}$$

Protože r je také prvočíslo, platí

$$\sigma(n) = \sigma(2^k r) = \sigma(2^k)\sigma(r) = (2^{k+1}-1)9\cdot 2^{2k-1} = m+n. \tag{7.26}$$

Ze vztahů (7.25) a (7.26) tedy dostáváme, že (7.22) platí, a proto jsou čísla m a n spřátelená. □

Čísla tvaru $3\cdot 2^k - 1$ se nazývají *Thabitova čísla.* Je-li $3\cdot 2^k - 1$ pro nějaké $k \geq 0$ prvočíslem, nazývá se *Thabitovo prvočíslo,* např.

2, 5, 11, 23, 47, 191, 383, 6143, 786431, 51539607551.

Vidíme, že pro $k = 2$ Thabitova věta 7.28 dává spřátelená čísla 220 a 284, viz (Borho, 1972). Není ale známo, zda Thabit použil větu i pro $k > 2$. Druhý nejmenší pár spřátelených čísel $\{1184, 1210\}$ nalezl teprve šestnáctiletý Nicolo Paganini v roce 1866. V tomto případě však nelze použít větu 7.28, protože ta udává jen postačující podmínku pro existenci spřátelených čísel. Pierru de

Fermatovi se přisuzuje dvojice $\{17296, 18416\}$, který Thabitovu větu 7.28 znovu „objevil“. Tato dvojice odpovídá případu $k = 4$. Před ním ale objevil stejnou dvojici arabský matematik al-Banna z Marakeše v Maroku na přelomu 13. a 14. století. V jeho díle nalezneme tento výrok, viz (Porubský, 2002, s. 60):

Čísla 17 296 *a* 18 416 *jsou spřátelená; první z nich je abundantní, druhé deficientní. Alláh je všemohoucí.*

Také Fermatův vrstevník René Descartes nalezl dvojici poměrně velkých spřátelených čísel $\{9363584, 9437056\}$, jež odpovídá případu $k = 7$ ve větě 7.28.

Nejmenší dvojice spřátelených čísel jsou tyto:

$$\{220, 284\},\quad \{1184, 1210\},\quad \{2620, 2924\},\quad \{5020, 5564\},$$
$$\{6232, 6368\},\quad \{10744, 10856\},\quad \{12285, 14595\},$$
$$\{17296, 18416\},\quad \{63020,76084\},\quad \{66928, 66992\},$$
$$\{67095, 71145\},\quad \{69615, 87633\},\quad \{79750, 88730\},\ \ldots$$

Leonhard Euler nalezl celkem 60 párů spřátelených čísel. Také zobecnil (viz (Euler, 1915)) Thabitovu větu 7.28 na případ, že $p = 2^{k-\ell} f - 1$, $q = 2^k f - 1$ a $r = 2^{2k-\ell} f^2 - 1$ jsou prvočísla, $f = 2^\ell + 1$ a $k > \ell \geq 1$. Důkaz tohoto tvrzení je zcela podobný důkazu věty 7.28. Přitom případ $\ell = 1$ odpovídá právě Thabitově větě. Pro $\ell = 7$ a $k = 8$ dostáváme pár

$$\{2172649216, 2181168896\}.$$

Další pár získáme pro $\ell = 11$ a $k = 40$ (viz (te Riele, 1974))

$$m = 272491804039370655778575224081940584857 6,$$
$$n = 272491804039618485630625803878723590553 6,$$

přitom poměr $m : n$ je zhruba $1 - 2^{-40}$.

Díky počítačové technice je v současné době známo přes 7 milionů takových dvojic, přičemž největší z nich mají přes 3000 cifer.

Věta 7.29. *Jestliže m a n jsou spřátelená čísla, pak platí*

$$\Big(\sum_{d|m}\frac{1}{d}\Big)^{-1}+\Big(\sum_{d|n}\frac{1}{d}\Big)^{-1}=1.$$

D ů k a z. Podle (7.22) vidíme, že

$$m+n=\sigma(m)=\sum_{d|m}d=\sum_{d|m}\frac{m}{d}=m\sum_{d|m}\frac{1}{d},$$
$$m+n=\sigma(n)=\sum_{d|n}d=\sum_{d|n}\frac{n}{d}=n\sum_{d|n}\frac{1}{d}.$$

Tedy

$$\sum_{d|m}\frac{1}{d}=\frac{m+n}{m}\quad\text{a}\quad\sum_{d|n}\frac{1}{d}=\frac{m+n}{n},$$

odkud plyne, že

$$\Big(\sum_{d|m}\frac{1}{d}\Big)^{-1}+\Big(\sum_{d|n}\frac{1}{d}\Big)^{-1}=\frac{m}{m+n}+\frac{n}{m+n}=1.\qquad\square$$

Na závěr oddílu ještě uvedeme některé otevřené problémy:

1. *Existuje nekonečně mnoho párů spřátelených čísel?*
2. *Existuje spřátelený pár nesoudělných čísel?*
3. *Existuje spřátelený pár rozdílné parity* (*tj. m liché a n sudé*)*?*
4. *Existuje spřátelený pár čísel, z nichž jedno je čtvercem?*

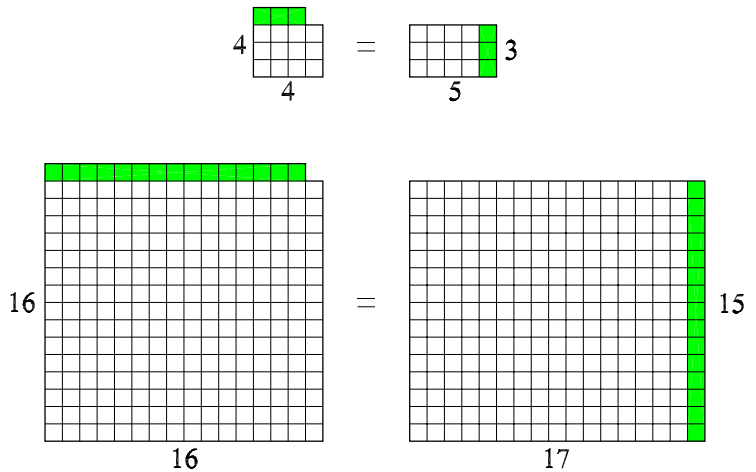
7.6. Fermatova čísla

Jak jsme viděli v 5. kapitole, Fermatova čísla hrají důležitou roli v aplikacích. Připomeňme, že jsou definována vztahem (viz (4.3))

$$F_m=2^{2^m}+1\quad\text{pro } m=0,\ 1,\ 2,\ \ldots\qquad(7.27)$$

V oddílu 4.2 jsme uvedli řadu vět, které se týkají především Fermatových prvočísel. V tomto oddílu se budeme zabývat dalšími vlastnostmi Fermatových čísel.

Fermatova čísla F_m pro $m \geq 2$ mají vždy poslední cifru 7, protože 2^{2^m} končí na 6, jak lze snadno zjistit indukcí.



Obr. 7.11. Geometrická interpretace vztahu $F_m - 2 = F_0 F_1 \cdots F_{m-1}$ pro $m = 2$ a $m = 3$.

Podle vztahu (4.7) platí

$$F_m - 2 = F_0 F_1 \cdots F_{m-1} \tag{7.28}$$

pro všechna $m \geq 1$. Jeden ze zakladatelů neeukleidovské geometrie János Bólyai užil (7.28) k důkazu následujícího tvrzení.

Věta 7.30 (Bólyaiova). *Každé Fermatovo číslo F_m pro $m \geq 1$ je tvaru $6n - 1$.*

D ů k a z. Podle (7.28) je

$$F_m + 1 = F_0 F_1 \cdots F_{m-1} + 3 = 3(F_1 \cdots F_{m-1} + 1),$$

kde číslo v závorkách je evidentně sudé. Pravá strana je proto dělitelná šesti. □

Vidíme tedy, že žádné Fermatovo číslo F_m není dělitelné 3 pro $m \geq 1$. V následující větě 7.31 dokážeme mnohem silnější tvrzení.

Mocnina dvou zvětšená o jednu může dělit jinou mocninu dvou zvětšenou o jednu, např. $(2+1) \mid (8+1)$ nebo $(4+1) \mid (64+1)$. Eulerův současník Christian Goldbach (1690–1764) však dokázal, že největší společný dělitel dvou různých Fermatových čísel je jedna.

Věta 7.31 (Goldbach). *Každá dvě různá Fermatova čísla jsou nesoudělná.*

D ů k a z. Nechť

$$q \mid F_m \quad \text{a} \quad q \mid F_{m-k} \tag{7.29}$$

pro $m \geq k \geq 1$. Odtud a z (7.28) dostaneme, že $q \mid (F_m - 2)$. Tedy podle (7.29) máme $q \mid 2$. Protože ale F_m je liché, platí $q = 1$. □

Poznamenejme ještě, že z Goldbachovy věty lze jiným způsobem dokázat Druhou Eukleidovu větu 2.3 o nekonečnosti prvočísel (Hardy, Wright, 1979, s. 14).

D ů k a z. Podle věty 7.31 je každé číslo z posloupnosti $F_0, F_1, F_2, \ldots, F_m$ dělitelné prvočíslem, které nedělí žádné jiné Fermatovo číslo. Proto pro libovolné m vždy existuje alespoň $m+1$ různých prvočísel nepřevyšujících F_m. □

Jako důsledek dostáváme, že číslo $F_m - 2$ ze (7.28) má alespoň m různých prvočíselných dělitelů.

Dále si všimněme, že Fermatovo číslo $F_1 = 5$ lze napsat jako součet dvou prvočísel 2 a 3. Následující věta uvedená v (Sierpiński, 1970) se zabývá případem $m > 1$.

Věta 7.32. *Žádné Fermatovo číslo F_m pro $m > 1$ nemůže být vyjádřeno jako součet dvou prvočísel.*

D ů k a z. Čísla F_m jsou lichá. Pokud by F_m bylo součtem dvou prvočísel, pak jedno z nich musí být 2 a druhé $F_m - 2$. Vidíme však, že číslo

$$F_m - 2 = 2^{2^m} - 1 = \left(2^{2^{m-1}} - 1\right)\left(2^{2^{m-1}} + 1\right)$$

je složené pro $m > 1$, jelikož $2^{2^{m-1}} - 1 \geq 3$. □

Každé liché číslo lze vyjádřit jako rozdíl čtverců,

$$2n + 1 = (n + 1)^2 - n^2.$$

Tudíž i každé Fermatovo číslo lze takto napsat:

$$F_m = 2^{2^m} + 1 = \left(2^{2^m - 1} + 1\right)^2 - \left(2^{2^m - 1}\right)^2.$$

Pokud je F_m složené, existují i jiné možnosti, jak je vyjádřit jako rozdíl dvou čtverců, viz (Křížek, Luca, Somer, 2001).

Věta 7.33. *Žádné Fermatovo číslo nemůže být vyjádřeno jako rozdíl dvou p-tých mocnin, kde p je liché prvočíslo.*

D ů k a z. Předpokládejme, že p je liché prvočíslo a že

$$F_m = a^p - b^p = (a - b)\left(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}\right),$$

kde $a > b$. Jelikož F_m je prvočíslo, platí $a - b = 1$. Podle Malé Fermatovy věty 2.13

$$F_m = a^p - b^p \equiv a - b \equiv 1 \pmod{p}.$$

Tedy p dělí $F_m - 1 = 2^{2^m}$, což není možné. Tudíž F_m nelze vyjádřit jako rozdíl dvou p-tých mocnin. □

Pro $m \geq 1$ může být podle Fermatovy vánoční věty 3.12 napsáno Fermatovo prvočíslo F_m jako součet dvou čtverců právě jedním způsobem, a to

$$F_m = \left(2^{2^{m-1}}\right)^2 + 1^2.$$

Sophie Germainová objevila (viz (2.42)), že každé číslo tvaru $a^4 + 4$ je složené pro $a > 1$, neboť

$$a^4 + 4 = \left(a^2 + 2a + 2\right)\left(a^2 - 2a + 2\right).$$

Položíme-li $a = 2^{2^{m-2}}$ pro $m \geq 2$, pak $a^2 + 1 = F_{m-1}$, $a^4 + 1 = F_m$, a tedy

$$F_m + 3 = \left(F_{m-1} + 2F_{m-2} - 1\right)\left(F_{m-1} - 2F_{m-2} + 3\right),$$

kde oba činitelé jsou sudá čísla větší než 2 pro $m > 2$.

Dokažme si nyní speciální Eulerovo tvrzení, že číslo F_5, které má deset cifer, je složené (srov. obr. 4.3).

Věta 7.34. *Číslo F_5 je dělitelné* 641.

D ů k a z. Protože

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$$

dělí čísla $5^4\,2^{28} + 2^{32}$ a $5^4\,2^{28} - 1$, musí dělit i jejich rozdíl, což je F_5. □

Abychom se mohli snadno přesvědčit, že nalezený dělitel čísla F_m je prvočíselný, můžeme použít například Prothovu větu 3.2 nebo následující Suyamovu větu. Její předpoklady jsou splněny pro většinu (asi 85 %) všech známých prvočinitelů Fermatových čísel (srov. tabulky 3 a 5 na stránkách 339 a 341). Obecný tvar dělitelů Fermatových čísel je dán Lucasovou větou 4.17.

Věta 7.35 (Suyamova). *Jestliže $p = k2^n + 1$ dělí F_m a $k2^{n-(m+2)} < 9 \cdot 2^{m+2} + 6$, pak je p prvočíslo.*

D ů k a z. Předpokládejme naopak, že p je součinem dvou netriviálních činitelů. Pomocí Lucasovy věty 4.17 lze dokázat, viz (Křížek, Chleboun, 1994), že každý z těchto činitelů je větší než $3 \cdot 2^{m+2} + 1$. Proto $k2^n + 1 \geq (3 \cdot 2^{m+2} + 1)^2$. Odtud plyne, že $k2^{n-(m+2)} \geq 9 \cdot 2^{m+2} + 6$, což je spor. □

Jako příklad použití věty 7.35 uvažujme dělitele $45592577 = 11131 \cdot 2^{12} + 1$ čísla F_{10} (viz tab. 3). V tomto případě máme $n = 12$, $m = 10$ a $n - (m + 2) = 0$. Protože $k = 11131$ je menší než $9 \cdot 2^{12} + 6 = 36870$, musí být tento dělitel prvočíslem.

Do roku 2007 bylo známo, že čísla F_m jsou složená pro $m = 5, 6, \ldots, 32$ a pro $F_5, F_6, \ldots, F_{11}$ navíc známe úplné prvočíselné rozklady (viz tab. 3, str. 339).

V roce 1984 Wilfrid Keller objevil, že Fermatovo číslo F_{23471} je složené. Počítačovou analýzou dokázal (viz (Keller, 1992)), že je dělitelné číslem $5 \cdot 2^{23473} + 1$. Číslo F_{23471} má více než 10^{7000} cifer. Velikost tohoto Fermatova čísla prosím nezaměňujte s relativně

malým číslem 10^{7000}, které má „jen“ 7001 cifer. Pro porovnání dodejme, že počet elementárních částic v pozorovatelné části vesmíru se odhaduje na 10^{80} plus minus několik řádů.

V roce 2003 bylo největším známým složeným Fermatovým číslem $F_{2145351}$. Jeho prvočinitele $3 \cdot 2^{2145353} + 1$, který má 645817 cifer, objevil J. B. Cosgrave. Je to zatím největší známé nemersenovské prvočíslo. Další prvočinitele Fermatových čísel lze najít na adrese [www11].

V roce 2004 vyšel článek (Hill, 2004), jehož tvrzení nyní mírně zobecníme.

Věta 7.36 (Hillova). *Nechť p je prvočíslo tvaru $k2^n + 1$, kde $k > 1$ je liché, $n \geq m + 2$ a p dělí F_m. Pak*

$$k^{2^{m+1}} \equiv 1 \pmod{p}.$$

D ů k a z. Jednoduchými úpravami modulo p dostáváme, že

$$1 = (-1)^{2^{m+1}} \equiv (k2^n)^{2^{m+1}} = k^{2^{m+1}} \left(2^{2^m}\right)^{2n} \equiv k^{2^{m+1}} (-1)^{2n} = k^{2^{m+1}}.$$

□

Poznamenejme dále, že každé Fermatovo číslo F_m v dvojkové soustavě má tvar

$$1000\ldots0001$$

s $2^m - 1$ nulami uvnitř. Více tvrzení o Fermatových číslech je uvedeno v monografii (Křížek, Luca, Somer, 2001).

Na závěr tohoto oddílu uveďme ještě nejdůležitější nerozřešené problémy týkající se Fermatových čísel:

1. *Je složených Fermatových čísel nekonečně mnoho?*
2. *Existuje F_m, které je dělitelné druhou mocninou nějakého prvočísla?*
3. *Jaký je úplný rozklad čísel F_{12}, $F_{13}, \ldots$ na prvočísla?*
4. *Jaký je nejmenší prvočinitel složených čísel F_{14}, F_{20}, F_{22} a F_{24}?*
5. *Jestliže F_{m+1} je prvočíslo, je také F_m prvočíslo?*

K prověřování otázky 2. na počítačích se používá věta 4.19. Existuje však domněnka podložená pravděpodobnostním důkazem, viz (Hardy, Wright, 1979, s. 15), že neexistuje F_m splňující bod 2.

Pokud by se podařilo problém 5. pozitivně rozřešit, bylo by F_4 největším Fermatovým prvočíslem a zároveň bychom dostali i pozitivní odpověď na otázku 1. Další otevřené problémy jsou například v článcích (Guy, 1994a), (Křížek, 1994a, 1995).

7.7. Sierpińského čísla

Následující věta je uvedena v (Sierpiński, 1960) a (Sierpiński, 1970, problém 128). Její důkaz obsahuje zajímavou aplikaci Fermatových čísel.

Věta 7.37 (Sierpińského). *Existuje nekonečně mnoho přirozených čísel k takových, že všechna čísla $k2^n + 1$, $n = 1, 2, \ldots$, jsou složená.*

Důkaz. Víme, že Fermatova čísla $F_0, \ldots, F_4$ jsou prvočísly a podle věty 7.34 $F_5 = 641\, p$. Není těžké prověřit, že p je prvočíslo, pro něž $p > 2^{16} + 1 = F_4$. Protože $p \mid F_5$, vidíme navíc, že

$$(p, F_5 - 2) = (p, 2^{32} - 1) = 1.$$

Tudíž $\left(p, 641\left(2^{32} - 1\right)\right) = 1$. Podle Čínské věty o zbytcích 1.4 existuje nekonečně mnoho přirozených čísel k tak, že

$$k \equiv 1 \pmod{641(2^{32} - 1)}, \tag{7.30}$$

$$k \equiv -1 \pmod{p}. \tag{7.31}$$

Nyní dokážeme, že když k je přirozené číslo větší než p, které splňuje systém kongruencí (7.30)–(7.31), pak všechna čísla $k2^n + 1$ ($n = 1, 2, \ldots$) jsou složená. Zřejmě můžeme vyjádřit číslo n ve tvaru $n = 2^m(2t + 1)$, kde m a t jsou nezáporná celá čísla. Nejprve nechť $m \in \{0, 1, 2, 3, 4\}$. Pak z (7.30) máme

$$k2^n + 1 \equiv 2^{2^m(2t+1)} + 1 \pmod{(2^{32} - 1)}. \tag{7.32}$$

Protože $F_m \mid \left(2^{32}-1\right)$ pro $m = 0, 1, 2, 3, 4$ a $F_m \mid \left(2^{2^m(2t+1)}+1\right)$, podle (7.32) platí, že $F_m \mid (k2^n+1)$, a tedy nerovnosti $k2^n+1 > k > p > F_4$ implikují, že číslo $k2^n+1$ je složené.

Nechť dále $m = 5$. Potom ze vztahu (7.30) dostáváme

$$k2^n + 1 \equiv 2^{2^5(2t+1)} + 1 \pmod{641}$$

pro nezáporné celé číslo t. Jelikož $k > p > 641$ a $641 \mid \left(2^{2^5}+1\right) \mid \left(2^{2^5(2t+1)}+1\right)$, podle (4.5) vidíme, že číslo $k2^n+1$ je složené.

Zbývá vyšetřit případ $m \geq 6$. Platí $2^6 \mid n$, což implikuje, že $n = 2^6 h$ pro nějaké přirozené číslo h. Podle (7.31) máme

$$k2^n + 1 \equiv -2^{2^6 h} + 1 \pmod{p},$$

a protože $p \mid \left(2^{2^5}+1\right) \mid \left(2^{2^6}-1\right) \mid \left(2^{2^6 h}-1\right)$, dostaneme $p \mid (k2^n+1)$. Jelikož

$$k2^n + 1 > k > p,$$

číslo $k2^n+1$ je složené. □

Přirozené číslo k se nazývá *Sierpińského číslem,* jestliže posloupnost $(k2^n+1)_{n=1}^{\infty}$ obsahuje pouze složená čísla.

Všechna známá Sierpińského čísla k byla nalezena pomocí metody *pokrývacích množin.* V této metodě se hledá konečná množina prvočísel $p_1, p_2, \ldots, p_r$ takových, že každé číslo posloupnosti $k2^n+1$, $n = 1, 2, \ldots$, je dělitelné alespoň jedním z těchto prvočísel. Kupříkladu pro každé přirozené číslo k splňující kongruence (7.30)–(7.31) v důkazu Sierpińského věty je

$$\{3,\ 5,\ 17,\ 257,\ 641,\ 65537,\ 6\,700417\} \tag{7.33}$$

pokrývací množina. Podle (1.12) nejmenší přirozené číslo k, které vyhovuje (7.30)–(7.31), splňuje kongruenci

$$k \equiv m_1 y_1 - m_2 y_2 \pmod{m},$$

kde $m_1 = 6\,700417$, $m_2 = 2\,753074\,036095$, $m = m_1 m_2 = 18\,446744\,073709\,551615$, $y_1 = 1\,157493\,686323$ a $y_2 = 3\,883315$ splňují kongruence (srov. (1.11))

$$m_i y_i \equiv 1 \pmod{(m/m_i)}, \quad i = 1, 2,$$

jež mohou být vyřešeny pomocí Eukleidova algoritmu (viz oddíl 1.5). Tímto způsobem nalezneme nejmenší kladné řešení

$$k = 15\,511380\,746462\,593381$$

systému (7.30)–(7.31).

Nejmenší Sierpińského číslo se stejnou pokrývací množinou jako v (7.33) je

$$k = 201446\,503145\,165177$$

(viz (Baillie, Cormack, Williams, 1981)). Nejmenší známé Sierpińského číslo je

$$78\,557.$$

Bylo objeveno Selfridgem v roce 1962. Jeho pokrývací množina je

$$\{3, 5, 7, 13, 19, 37, 73\}.$$

Do roku 2007 je známo 11 lichých Sierpińského čísel menších než 10^6:

$$78\,557,\ 271\,129,\ 271\,577,\ 327\,739,\ 482\,719,\ 575\,041,$$
$$603\,713,\ 808\,247,\ 903\,983,\ 934\,909,\ 965\,431.$$

V článku (Jaeschke, 1983, s. 382) jsou tato čísla uvedena společně s jejich pokrývacími množinami. Povšimněme si, že Sierpińského čísla, která jsou v uvedeném seznamu na druhém a třetím místě, jsou téměř stejně velká. Navíc mají stejnou pokrývací množinu $\{3, 5, 7, 13, 17, 241\}$.

Všeobecně se soudí, že neexistuje liché Sierpińského číslo menší než 78 557. Až do roku konce 2007 bylo známo jen 6 lichých čísel menších než 78 557, o nichž nebylo známo, zda jsou či nejsou Sierpińského čísly. Jsou to tato čísla k (viz [www12]):

$$10\,223,\ 21\,181,\ 22\,699,\ 24\,737,\ 55\,459,\ 67\,607.$$

Pro každé z těchto čísel k byla testována prvočíselnost $k2^n + 1$ pro všechny hodnoty n až do 300 000.

Problém nalezení nejmenšího Sierpińského čísla je všeobecně nazýván *Sierpińského problém.* Někteří autoři požadují, aby příslušné číslo k bylo liché. Sám Waclaw Sierpiński ale ve své původní práci (Sierpiński, 1960, s. 74) tento předpoklad nevyslovuje. Píše doslova:

Le problème reste ouvert quel est le plus petit nombre naturel k tel que les nombres $k \cdot 2^n + 1$, où $n = 1, 2, \ldots$ sont tous composés. (*Zůstává otevřený problém najít nejmenší přirozené číslo k takové, že všechna čísla $k \cdot 2^n + 1$, $n = 1, 2, \ldots$, jsou složená.*)

Sierpiński tedy připouští i sudá k. V budoucnu se možná ukáže, že F_4 je největší Fermatovo prvočíslo. Zatím je to jen hypotéza, kterou označíme (H).

Věta 7.38. *Pokud platí* (H), *pak* $F_4 - 1 = 65536$ *je Sierpińského číslo.*

D ů k a z. Uvažujme posloupnost $(2^{16+n} + 1)_{n=1}^{\infty}$. Jestliže exponent $16 + n$ není tvaru 2^m, pak je číslo $2^{16+n} + 1$ složené, jak plyne ze (4.5). Jestliže $2^{16+n} + 1$ je tvaru 2^m, pak $m > 4$, a tedy $65536 \cdot 2^n + 1$ je složené podle hypotézy (H). □

Číslo 65 536 je menší než 78 557. Jeho pokrývací množina je zřejmě nekonečná, jak okamžitě plyne z Goldbachovy věty 7.31. Pokud platí (H), pak další sudá Sierpińského čísla jsou $2^{17}, 2^{18}, \ldots$.

7.8. Další speciální typy přirozených čísel

Zobecněná Lucasova čísla. V tomto odstavci ukážeme, že řešení rovnice (5.52) pro jednu konkrétní nenulovou hodnotu c úzce souvisí se zobecněnými Lucasovými čísly. Místo rekurence (7.6) budeme uvažovat rekurenci

$$L_{n+2} = rL_{n+1} + sL_n \qquad \text{pro všechna } n = 0, 1, 2, \ldots$$

pro daná celá čísla r a s a nějaké počáteční podmínky L_0 a L_1. Taková čísla nazveme *zobecněná Lucasova čísla.*

Je patrné, že rovnice (5.50) s kritickou hodnotou $\lambda = 4$ (tj. maximální možnou hodnotou λ, pro niž jsou ještě všechna řešení s počáteční podmínkou $x_1 \in \langle 0, 1\rangle$ ohraničená) je ekvivalentní rovnici (5.52) s $c = -2$.

Věta 7.39. *Řešení rovnice* (5.52) *pro* $c = -2$ *má tvar*

$$y_n = a^{2^{n-1}} + a^{-2^{n-1}}, \quad a \in \mathbb{C}, \quad a \neq 0. \tag{7.34}$$

D ů k a z. Podle (7.34) platí

$$y_{n+1} = a^{2^n} + 2 + a^{-2^n} - 2 = \left(a^{2^{n-1}} + a^{-2^{n-1}}\right)^2 - 2 = y_n^2 - 2.$$

Posloupnost definovaná vztahem (7.34) tedy splňuje rovnici (5.52) pro $c = -2$.

Musíme ještě ukázat, že neexistují jiná řešení. Jestliže počáteční člen y_1 posloupnosti je libovolné komplexní číslo, pak existuje nenulové číslo $a \in \mathbb{C}$ takové, že $y_1 = a + a^{-1}$. (K tomu stačí vyřešit kvadratickou rovnici $a^2 - ay_1 + 1 = 0$, jejíž obě řešení dávají $y_1 \in \mathbb{C}$.) Dalšími členy posloupnosti (5.52) jsou $y_2 = a^2 + a^{-2}$, $y_3 = a^4 + a^{-4}$ atd. □

Vztah (7.34) nám umožňuje explicitně určit posloupnost definovanou rekurentně takto:

$$y_{n+1} = y_n^2 - 2, \quad y_1 = 4. \tag{7.35}$$

Ze vztahu (7.34) pro $a = 2 + \sqrt{3}$ pak dostaneme

$$y_n = \left(2 + \sqrt{3}\right)^{2^{n-1}} + \left(2 - \sqrt{3}\right)^{2^{n-1}} = \left\lfloor \left(2 + \sqrt{3}\right)^{2^{n-1}} \right\rfloor + 1,$$

kde $\lfloor \cdot \rfloor$ označuje celou část. Přitom platí $y_n = L_{2^{n-1}}$, kde zobecněná Lucasova čísla L_k splňují rekurenci konkrétního tvaru (viz (Riesel, 1994, s. 131))

$$L_{k+2} = 4L_{k+1} - L_k \tag{7.36}$$

s počátečními podmínkami $L_1 = 4$ a $L_2 = 14$ (tj. $L_k = a^k + a^{-k}$).

Poznamenejme ještě, že některá ze zobecněných Lucasových čísel definovaných pomocí (7.36) se vyskytují i v následujícím Lucasově–Lehmerově testu (srov. větu 4.2 a vztah (7.35)), který

slouží k hledání těch největších známých prvočísel – Mersennových prvočísel. Modifikovaná verze věty 4.2 tedy zní:

Věta 7.40. *Je-li $p > 2$, pak Mersennovo číslo $M_p = 2^p - 1$ je prvočíslem právě tehdy, když $M_p \mid L_{p-1}$.*

Zobecněná Fermatova a Mersennova čísla. Zajímavé zobecnění Fermatových a Mersennových čísel je uvedeno v článku (Ligh, Jones, 1982). Jeho autoři studovali čísla tvaru

$$Z_{p,m} = \frac{2^{p^{m+1}}-1}{2^{p^m}-1} = \sum_{j=1}^{p} 2^{p^m(j-1)},$$

odkud pro Fermatova čísla vidíme, že

$$F_m = Z_{2,m} = 2^{2^m} + 1.$$

Pro $m = 0$ zase máme

$$M_p = Z_{p,0} = 2^p - 1,$$

což jsou Mersennova čísla. *Zobecněná Fermatova čísla* se však většinou definují vztahem

$$F_{b,m} = b^{2^m} + 1.$$

Je patrné, že $F_m = F_{2,m}$. Nejrůznější zobecnění Fermatových čísel se uvádějí v kapitole 13 knihy (Křížek, Luca, Somer, 2001). Studují se například čísla tvaru $a^{2^m} + b^{2^m}$.

Cunninghamova čísla. Počátkem 20. století byl zahájen velký projekt, který se zabývá rozklady *Cunninghamových čísel*, tj. čísel tvaru $b^n \pm 1$, kde b je „malé“ (obvykle $b \leq 12$) a n je „velké“.

Je-li $b \geq 2$ a $b^n + 1$ je prvočíslo, pak nutně $n = 2^m$. To plyne ze vztahu (4.5), kde zaměníme základ 2 za b. Podobně můžeme také ve vztahu (4.1) zaměnit základ 2 za b. Pro $i > 1$ a $j > 1$ pak plyne, že k tomu, aby číslo $b^n + 1$ bylo prvočíslem, je nutné, aby exponent n byl prvočíslem.

V současnosti se každý měsíc na počítačích nalézají desítky prvočíselných dělitelů Cunninghamových čísel. Tabulky jejich dělitelů pro $b \leq 12$ jsou obsahem knihy (Brillhart et al., 1988). Největší přínos Cunninghamova projektu ale spočívá v tom, že dal podnět k vytváření nových vysoce efektivních metod pro testování prvočíselnosti, hledání prvočíselných rozkladů apod. Vyšetřují se i zobecněná Cunninghamova čísla tvaru $b^n \pm a^n$.

Cullenova čísla. Zatím nevíme, zda posloupnost Fermatových čísel F_m obsahuje nekonečně mnoho složených čísel. Na druhé straně je dokázáno, že v posloupnosti

$$C_n = n\,2^n + 1$$

je nekonečně mnoho složených čísel pro $n = 1, 2, \ldots$, viz (Crandall, Pomerance, 2005, s. 71).

V roce 1905 reverend J. Cullen dokázal, že C_n je složené pro $n \in \{2, 3, \ldots, 100\}$ kromě jediného případu $n = 53$ (viz (Cullen, 1905)), a proto se čísla C_n nazývají *Cullenova čísla.* O rok později A. J. Cunningham zjistil, že prvočíslo 5591 dělí C_{53} a dokázal, že C_n je složené pro všechna $n \in \{2, 3, \ldots, 200\}$ kromě případu $n = 141$, který neuměl rozhodnout. Zhruba o padesát let později Robinson v roce 1957 ukázal, že C_{141} je prvočíslo. Do konce roku 2007 bylo známo, že C_n jsou prvočísla pouze pro

$$n = 1,\ 141,\ 4713,\ 5795,\ 6611,\ 18\,496,\ 32\,292,\ 32\,469,$$
$$59\,656,\ 90\,825,\ 262\,419,\ 361\,275,\ 4\,811\,899.$$

Tato čísla se nazývají *Cullenova prvočísla.* Zatím není známo, zda je jich nekonečně mnoho.

Cullenova čísla C_n se podobají Fermatovým číslům v tom, že $C_n - 1$ jsou dělitelná vysokými mocninami dvojky pro velká n a že Cullenova prvočísla jsou patrně velice řídká, blíže (Křížek, Luca, Somer, 2001, s. 157). Studují se i zobecněná Cullenova čísla tvaru $nb^n + 1$.

Woodallova čísla. V roce 1917 se A. J. Cunningham a H. J. Woodall zabývali vlastnostmi čísel

$$W_n = n\,2^n - 1,$$

kterým se v současnosti říká *Woodallova čísla.* Někdy se též nazývají *Cullenova čísla druhého druhu.*

Existuje nekonečně mnoho složených Woodallových čísel. Pro

$$n = 2,\ 3,\ 6,\ 30,\ 75,\ 81,\ 115,\ 123,\ 249,\ 362,\ 384,\ 462,$$
$$512,\ 751,\ 822,\ \ldots$$

jsou W_n prvočísla (tzv. *Woodallova prvočísla*).

Rieselova čísla. Pokud je pro každé $n \in \mathbb{N}$ číslo

$$k\,2^n - 1$$

složené, nazývá se *k Rieselovo číslo.* Jeho definice je tedy podobná definici Sierpińského čísla z oddílu 7.7. Existuje domněnka, že $k = 509\,203$ je nejmenší Rieselovo číslo.

8. JAKÁ MATEMATIKA SE UKRÝVÁ V PRAŽSKÉM ORLOJI?

Orloj ten jest rozprávky a chvály hodný ve všech krajinách nad jiné všecky veliké orloje na světě . . .

Jan Táborský z Klokotské Hory
Zpráva o orloji pražském, 1570

8.1. 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 Emanuela Procházky (Horský, Procházka, 1964) a (Horský, 1988) 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 (viz obr. VIII barevné přílohy) 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, viz (Táborský, 1901).

Jan Šindel (asi 1375 – asi 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*, viz (Spunar, 1985, s. 136). Na univerzitě přednášel podle Thabita Ptolemaiův *Almagest.* Šindel byl též osobním lékařem krále Václava IV. Na jeho počest jsme v (Křížek, Somer, Šolcová, 2006) zavedli pojem šindelovské posloupnosti, který představíme v oddílu 8.4. S jeho pomocí uvidíme, jaká podivuhodná matematika

se skrývá v bicím stroji pražského orloje a jak tento stroj souvisí s trojúhelníkovými čísly.

Poznamenejme ještě, že Šindel se pravděpodobně narodil v Hradci Králové. Proto dalekohled na zdejší hvězdárně nese jeho jméno. Také planetka č. 3847 dostala jméno Šindel.

8.2. Co ukazuje pražský orloj?

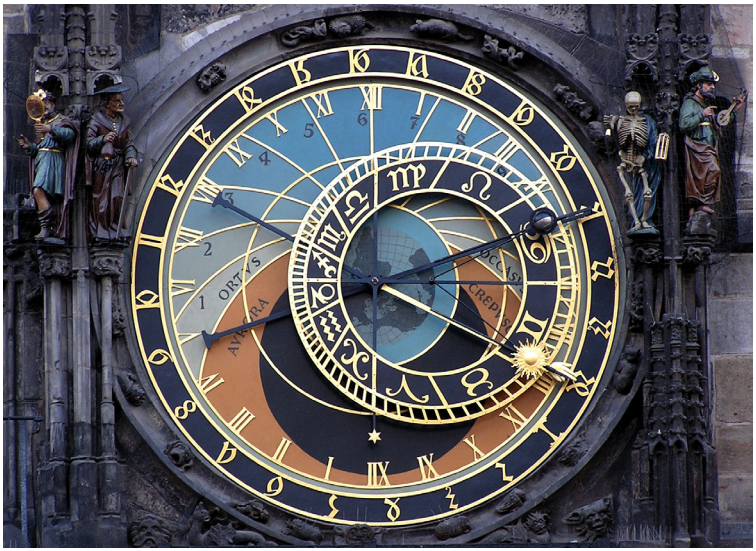
Pražský orloj je umístěn v dolní části Staroměstské radniční věže vysoké přibližně 59 metrů.[1)] Jeho astronomický ciferník (obr. 8.1) je astroláb poháněný hodinovým strojem. Znázorňuje geocentrický model vesmíru s nehybnou Zemí uprostřed, kolem níž obíhá Slunce, Měsíc a znamení zvěrokruhu nebeské sféry.[2)] Orloj tak vlastně představuje jeden z prvních analogových počítačů, neboť ukazuje pohyby nebeských těles. Někdy se dokonce hovoří o „high technology" 15. století.

Při návrhu astronomického ciferníku byla použita stereografická projekce nebeské sféry na rovinu. V případě pražského orloje si nebeskou sféru představme jako kulovou plochu o poloměru asi 40 cm (obr. 8.2). Střed promítání S je umístěn v severním pólu[3)] kulové plochy a projekční rovina je k ní tečná s bodem dotyku v jižním pólu J. Střed astronomického ciferníku (obr. 8.1) tedy odpovídá jižnímu pólu nebeské sféry. Nejmenší vnitřní kružnice se středem v jižním pólu znázorňuje obratník Kozoroha na nebeské sféře, zatímco vnější soustředná kružnice obratník Raka. Mezi těmito kružnicemi je na ciferníku ještě umístěna další sou-

[1)] Tato výška je rovna stu pražských loktů, což byla tehdejší jednotka míry. Některé prameny uvádějí nesprávnou výšku věže 70 metrů. Etalon pražského lokte 59.1 cm je umístěn na Novoměstské radnici a též na bývalé Hradčanské radnici v Loretánské ulici č. 1/173.

[2)] Naproti tomu olomoucký orloj znázorňuje po rekonstrukcích v 19. a 20. století heliocentrický model vesmíru – viz (Čermák, 2005).

[3)] Většina orlojů a astrolábů, které vznikly po roce 1450, má střed promítání v jižním pólu nebeské sféry, aby bylo možné znázorňovat polohy hvězd v okolí severního pólu. Při tomto způsobu promítání ale sluneční ukazatel vykonává v létě krátké kruhové oblouky, zatímco v zimě dlouhé.



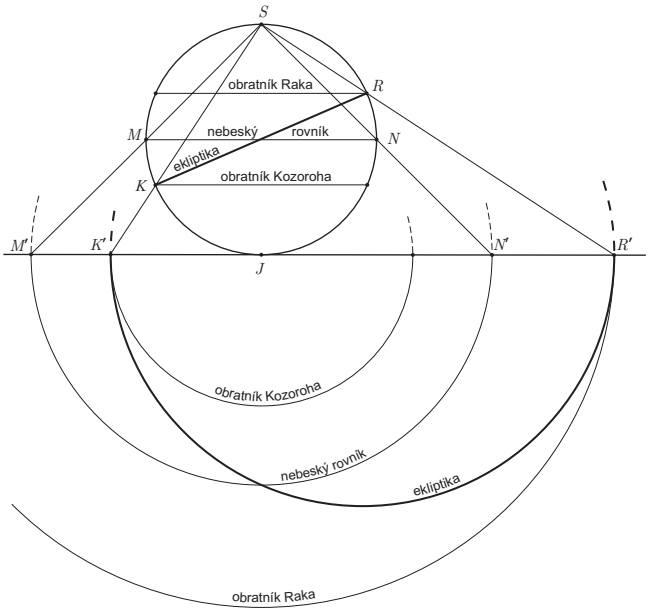
Obr. 8.1. Astronomický ciferník pražského orloje.

středná kružnice představující rovník nebeské sféry (viz obrázky 8.1 a 8.2).

Důležitou vlastností stereografické projekce je, že *každá kružnice, jež neprochází severním pólem, se opět zobrazí na kružnici*, viz (Křížek, Šolc, Šolcová, 2007/08). Proto se ekliptika, tj. dráha Slunce po nebeské sféře, zobrazuje na kružnici (obr. 8.2). Její střed není ve středu ciferníku, ale celá ekliptika se kolem tohoto bodu excentricky otáčí (obr. VII barevné přílohy). Ekliptika je na ciferníku orloje znázorněna zlatým prstencem. Po jeho vnitřní straně je na černém podkladu rozmístěno 12 znamení zvěrokruhu (tj. zodiaku nebo též zvířetníku). Na ekliptice lze pozorovat přibližnou polohu Slunce, Měsíce[4)] a jeho fáze. Sluneční i měsíční ukazatel je posuvně uchycen na příslušné rafii hodinového stroje a je tenkou ojnicí spojen se středem ekliptiky, aby na ní stále zůstával. Astronomický ciferník orloje také umožňuje zjišťovat východy, kulmi-

[4)] Dráha Měsíce neleží v rovině ekliptiky, ale je od ní odkloněna přibližně o úhel $i = 5°$, což se na astronomickém ciferníku pro jednoduchost zanedbává.

nace a západy jednotlivých znamení zvěrokruhu. Shodou okolností střed naší Galaxie leží v souhvězdí Střelce, jehož znamení je na prstenci ekliptiky znázorněno zlatou šipkou (obr. 8.1). Z postavení prstence tedy můžeme také přibližně určit, kde se právě nachází střed Galaxie. Ekliptika se dotýká obou obratníků ve dvou protilehlých bodech K a R (viz obrázky 8.1 a 8.2). Její střed leží ve středu spojnice těchto bodů.



Obr. 8.2. Stereografická projekce obratníků Raka a Kozoroha, nebeského rovníku a ekliptiky (nahoře bokorys, dole půdorys). Průměr $|JS|$ dané koule je roven poloměru $|JN'|$ stereografické projekce rovníku.

V době zimního slunovratu dne 21. prosince se sluneční ukazatel nachází na obratníku Kozoroha. Pak se od něj po spirále postupně vzdaluje, až o letním slunovratu 21. června dosáhne obratníku Raka. Dalšího půl roku se zase pomalu přibližuje k obratníku Kozoroha. V době jarní a podzimní rovnodennosti je sluneční ukazatel na nebeském rovníku.

Rafie, na jejímž konci je uchycena pozlacená ruka, ukazuje *středoevropský čas* (SEČ) na stupnici s římskými číslicemi.[5] Sluneční ukazatel, který je posuvně upevněn na téže rafii, tak oběhne Zemi nakreslenou uprostřed ciferníku jednou za den. Zlaté arabské číslice na vnějším černém prstenci slouží k označení *staročeského času*, který se počítal od západu Slunce, viz (Horský, 1988, s. 50). Tento prstenec se v průběhu roku pozvolna kývavě natáčí o $\pm 30°$. Černé arabské číslice u zlatých kruhových oblouků označují planetní hodiny, pro něž je jedna hodina definována jako 1/12 doby mezi východem a západem Slunce. Sluneční ukazatel pak určuje odpovídající *babylonský čas*, jenž se počítá od východu Slunce. Konečně ručička s malou šesticípou hvězdičkou (viz obr. 8.1 dole), která je umístěna mezi znameními Berana a Ryb a pevně spojena s prstencem ekliptiky, ukazuje na stupnici s římskými číslicemi *hvězdný čas*.[6] To je hodinový úhel *jarního bodu*, tj. bodu, v němž Slunce přechází nebeský rovník z jižní polokoule nebeské sféry na severní polokouli. V důsledku precese zemské osy se ale jarní bod posunuje podél ekliptiky o $50.26''$ za rok. Proto se poloha znamení zvěrokruhu na nebeské sféře mění, zatímco poloha zvířetníkových a dalších souhvězdí je v podstatě neměnná. Jarní bod se tak v současnosti nachází v souhvězdí Ryb.

Černě vybarvený kruh v dolní části ciferníku znázorňuje astronomickou noc, kdy je Slunce níže než $18°$ pod horizontem. Načervenalá oblast (viz obr. VII barevné přílohy) označená AVRORA odpovídá svítání a CREPVSCVLVM stmívání (soumraku). Východ Slunce je označen ORTVS a západ OCCASVS. Modře obarvená oblast znamená den.

Součástí hlavního hodinového stroje je stroj ukazovací, jenž obsahuje 3 stejně velká souosá ozubená kola o průměru 117 cm z počátku 15. století s ručně vypilovanými zuby (obr. 8.3). Země se za rok (tj. přibližně za 365 dní) otočí kolem své osy zhruba 366krát.

[5] Poznamenejme, že rozdíl mezi SEČ a původním pražským časem je jen 138 sekund, neboť Praha leží v blízkosti patnáctého poledníku.

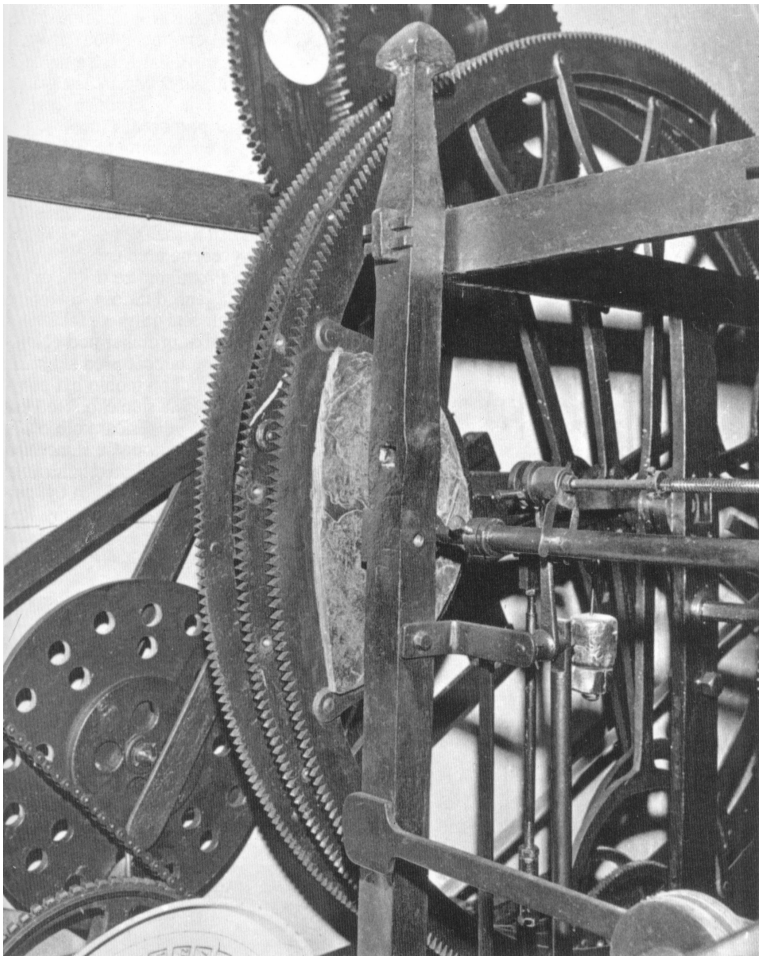
[6] Hvězdný den začíná okamžikem, kdy jarní bod prochází místním poledníkem (vrcholí).

Této skutečnosti jsou přizpůsobeny i počty zubů na prvních dvou kolech. První kolo má 365 zubů a otočí prstencem ekliptiky přibližně jednou za hvězdný den (tj. za 23 hodin 56 minut a 4 sekundy) a 366krát za rok. Druhé kolo, které má 366 zubů, otočí sluneční ukazatel jednou za střední sluneční den (tj. za 24 hodin) a 365krát za rok. Sluneční ukazatel se tedy posune vzhledem ke zvěrokruhu o jeden zub denně. Třetí kolo má 379 zubů a rotuje v souladu se středním zdánlivým pohybem Měsíce, jak uvidíme dále.

Záhadou zůstává, jak mohli tehdejší konstruktéři orloje vypilovat po obvodu velkých oběžných kol tak přesně 379, 366 a 365 zubů (s přesností na desetiny milimetru). Podle Gaussovy věty 4.10 nelze pomocí kružítka a pravítka rozdělit kružnici na $n = 379$ (ani na 366 či 365) stejně dlouhých dílů, protože prvočíslo 379 není tvaru $2^{2^m} + 1$. Kdyby si tehdejší konstruktéři vypočítali vzdálenost dvou zubů s přesností na setinu milimetru a postupně ji nanášeli na obvod kola, pak by po 379 krocích chyba mohla vzrůst na téměř 4 mm, což by znemožňovalo tento postup použít. Jedna z možností, jak mohlo být rovnoměrně rozmístěno po obvodu měsíčního kola $n = 379$ zubů, je vzít pevný provázek (nebo drát) stejně dlouhý jako obvod kola. Natažený provázek lze pomocí podobnosti rozdělit značkami na n stejně dlouhých dílků. Pak stačí provázek obtočit kolem kola a značky na kolo přenést (podrobnosti viz (Křížek, Šolcová, Somer, 2007b)). Je známo, že zuby se nejprve ručně vysekaly, a pak se postupně opilovaly na požadovanou vzdálenost.

Protože oběh Měsíce kolem Země není nikterak synchronizován s rotací Země kolem vlastní osy ani s dobou oběhu Země kolem Slunce, zmíněné počty zubů 365, 366 a 379 umožňují jen přibližně znázornit skutečné polohy těchto těles. Hlavní hodinový stroj od počátku otáčel prodlouženou hřídelí, na které byla pevně umístěna tři kolečka o 24 zubech, jež zabírala do tří velkých kol. Tím se dosáhlo toho, že se zvěrokruh, sluneční a měsíční ukazatel otáčejí kolem středu ciferníku vzájemně různými úhlovými rychlostmi.

Měsíc dorazí do téže polohy se Sluncem jednou za 29.53 dne, což je tzv. *synodický měsíc* (od novu k novu). Tomu jsou přizpů-



Obr. 8.3. Ukazovací stroj orloje obsahuje tři ozubená souosá kola otáčející prstencem ekliptiky, slunečním a měsíčním ukazatelem. Na prvním kole, které otáčí excentricky umístěnou ekliptikou, je připevněna olověná protiváha.

sobeny počty zubů na třetím kole. Měsíční ukazatel se opozdí za slunečním o $379 - 366 = 13$ zubů za den. To odpovídá úhlu $(1 - \frac{366}{379}) \cdot 360° = 12.348°$, což poměrně dobře vystihuje skuteč-

nost, že se Měsíc každý den posune podél ekliptiky od Slunce[7] směrem na východ v průměru o $12.191° = 360°/29.53$. Snadno se můžete přesvědčit, že 378 nebo 380 zubů měsíčního kola by nevystihovalo tak dobře skutečný posun Měsíce. V roce 1865 začalo být měsíční kolo poháněno tzv. diferenčním (opravovacím) strojem, který pohyb měsíčního ukazatele ještě více zpřesnil. Přesto se poloha tohoto ukazatele musí vícekrát ročně mírně upravovat, mj. také proto, že dráha Měsíce je eliptická.

Jelikož je i dráha Země mírně eliptická, Slunce se nepohybuje po ekliptice rovnoměrně. Z tohoto důvodu se v současnosti také natočení prstence ekliptiky dvakrát do roka přizpůsobuje skutečné poloze Slunce.

Kolo poháněj ící ekliptiku má plnou osu. Sluneční kolo má dutou osu, která obklopuje osu prvního kola. Třetí měsíční kolo má rovněž dutou osu obklopující osy prvních dvou kol.

Měsíční ukazatel je dutá koule (obr. 8.1), jejíž jedna polovina je natřena černě. Uvnitř je skryt důmyslný mechanismus s ozubeným kolem a olověným závažíčkem, který otáčí Měsícem a ukazuje tak jeho fáze. Energie potřebná k jeho otáčení se získává z pohybu prstence ekliptiky.

Při rekonstrukci astronomického ciferníku orloje kolem roku 1865 restaurátoři omylem vyrobili prstenec ekliptiky stejně velký jako nebeský rovník a ekliptika se přitom nedotýkala žádného z obratníků. Na sféře reprezentující hvězdnou oblohu má sice ekliptika i nebeský rovník stejný průměr $|KR| = |MN|$ – viz obr. 8.2, ale pro stereografické průměty platí $|K'R'| > |M'N'|$. Až po zásahu matematika Františka Josefa Studničky a astronoma Karla Hornsteina byla k prstenci ekliptiky přinýtována větší zlatá obruč tak, že každé znamení zvěrokruhu je rozděleno na 6 dílků po pěti stupních, a to umožňuje přibližně stanovit i datum. I když se takto zvětšená ekliptika již začala dotýkat obou obratníků, poloha slu-

[7] Za hodinu se Měsíc posune podél ekliptiky od Slunce zhruba o půl stupně a za minutu o 30″. Za 40 sekund se tedy posune o úhel 20″, který odpovídá aberaci slunečního světla. Proto při úplném zatmění Slunce jsou Země, Měsíc a Slunce v přímce až 40 sekund po středu zatmění.

nečního a měsíčního ukazatele dodnes zůstala na nesprávné kružnici (obr. 8.1). Přitom by stačilo prodloužit ojnice slunečního a měsíčního ukazatele jen o 7 cm.

Dolní ciferník orloje obsahující kopie 12 velkých a 12 malých kruhových Mánesových obrazů (tzv. lunet) představuje kalendář. Otáčí se velice pomalu – jedna otočka trvá celý rok. Originál kalendářní desky je uložen v Městském muzeu v Praze. Kopii umístěnou na orloji v dnešní době zhotovil Bohumír Číla. Pozlacená střelka v horní části ciferníku ukazuje příslušný den v roce, informuje o svátcích aj., viz (Horský, 1988, s. 58). Například lze také zjistit, ve kterém znamení se právě Slunce nachází.

8.3. 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 obrázky 8.4 a 8.5). 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 obrázky 8.4 a 8.5). Tyto délky se periodicky opakují po každé otočce a jejich součet je

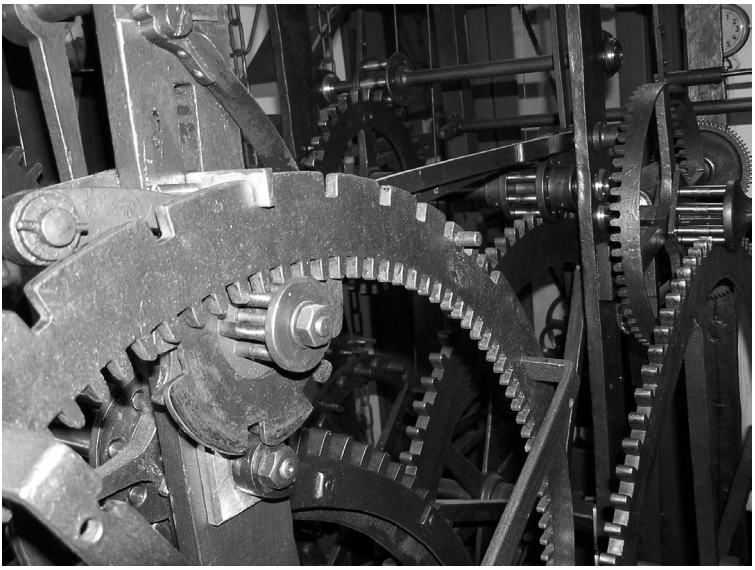
$$s = 15.$$

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

$$1 + 2 + \cdots + 24 = 300\text{krát},$$

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

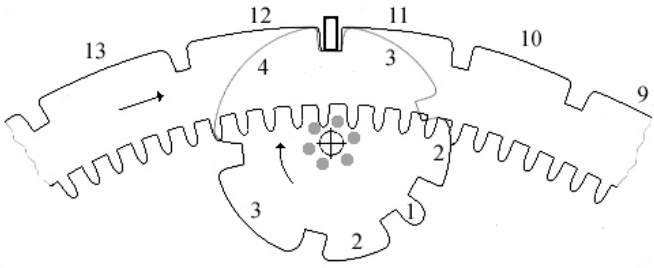
Závěrkové kolo má 120 vnitřních zubů, které zapadají do cévového kola se 6 vodorovnými tyčkami, jež obklopují střed pomocného kolečka (viz obrázky 8.4 a 8.5). Protože se závěrkové kolo otočí jednou denně, pomocné kolečko se otočí za tu dobu 20krát.



Obr. 8.4. Detail bicího stroje pražského orloje ukazující umístění pomocného kolečka. Západka je v poloze mezi segmenty odpovídajícími 8. a 9. hodině ranní.

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 například jen 11krát místo 12krát, pokud by segment označený 12 na obr. 8.5 měl již příliš zaoblené konce. Pro jeden úder zvonu hodinu po půlnoci bylo kdysi pomocné kolečko dokonce nezbytné, neboť na závěrkovém kole schází příslušný segment (viz obr. IX barevné přílohy a obr. 8.4). Byl by totiž tak tenký, že by se brzy zlomil.

Pražský orloj je pravděpodobně nejstarší a stále fungující hodinový stroj, který obsahuje takové důmyslné zařízení pro přesnou stabilizaci počtu úderů zvonu, viz (Horský, 1988, s. 78).



Obr. 8.5. Počet úderů zvonu je označen čísly . . . , 9, 10, 11, 12, 13, . . . 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,

$$1\,2\,3\,4\,\underbrace{3\,2}_{5}\;\underbrace{1\,2\,3}_{6}\;\underbrace{4\,3}_{7} \tag{8.1}$$

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

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

V další kapitole ukážeme, že bychom takto mohli pokračovat až do nekonečna. Všechny periodické posloupnosti ale takovou pěknou součtovou vlastnost nemají. Například je patrné, 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 v (Sloane, 2002, 2007) 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 (8.1).

V následujících oddílech dokážeme řadu matematických vět týkajících se zobecnění této posloupnosti. Budeme se vlastně zajímat o to, jak navrhnout nepravidelné ozubení pomocného kolečka i pro obecně jiné hodnoty součtu s.

8.4. Trojúhelníková čísla a šindelovské posloupnosti

V článku (Křížek, Šolcová, Somer, 2007a) jsme odvodili překvapivou souvislost mezi *trojúhelníkovými čísly*

$$T_k = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}, \quad k = 0, 1, 2, \ldots, \tag{8.2}$$

a pražskou hodinovou posloupností, která byla použita při konstrukci bicího stroje pražského orloje. V tomto oddílu se budeme zabývat dalšími periodickými posloupnostmi, které mají podobnou vlastnost jako posloupnost 1, 2, 3, 4, 3, 2,... v (8.1), tj. které by mohly být použity při konstrukci podobného pomocného kolečka, jako je znázorněno na obr. 8.4.

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

$$\forall\, i \in \mathbb{N} : \quad a_{i+p} = a_i. \tag{8.3}$$

Konečná posloupnost $a_1, \ldots, a_p$ se nazývá *perioda* a p *délka periody.* Nejmenší p splňující (8.3) 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

$$T_k = \sum_{i=1}^{n} a_i. \tag{8.4}$$

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

$$\forall\, k \in \mathbb{N} \quad \exists\, n \in \mathbb{N} \,:\, T_k = \sum_{i=1}^{n} a_i. \tag{8.5}$$

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 (obr. 8.6). Přitom pro k-tou hodinu platí

$$k = T_k - T_{k-1} = \sum_{i=m+1}^{n} a_i, \tag{8.6}$$

kde $T_{k-1} = \sum_{i=1}^{m} a_i$. Protože $a_i > 0$, je číslo n v (8.5) závisející na k určeno jednoznačně. Z (8.2) a (8.4) je také patrné, že $a_1 = 1$, je-li (a_i) šindelovská posloupnost.

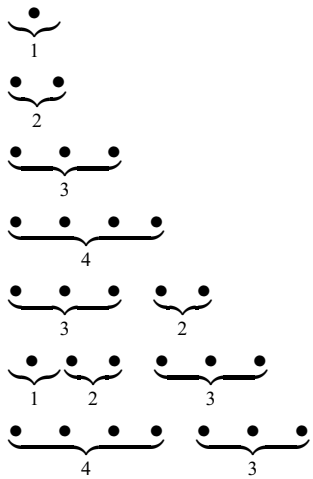
Následující věta ukazuje, že podmínku (8.5) lze zaměnit mnohem jednodušší podmínkou, jež obsahuje pouze konečný počet čísel k. To nám umožňuje provést jen konečný počet aritmetických operací, abychom zjistili, zda zvolená perioda $a_1, \ldots, a_p$ dává šindelovskou posloupnost. Součet prvků periody budeme nadále označovat

$$s = \sum_{i=1}^{p} a_i. \tag{8.7}$$

Věta 8.1. *Periodická posloupnost (a_i) je pro liché s šindelovská, jestliže T_k je dosažitelné pomocí (a_i) pro $k = 1, 2, \ldots, (s-1)/2$.*

Důkaz. Případ $s = 1$ je triviální. Nechť tedy $s \geq 3$ je liché a nechť

$$\forall\, k \in \{1, 2, \ldots, (s-1)/2\} \quad \exists\, n \in \mathbb{N} \,:\, T_k = \sum_{i=1}^{n} a_i. \tag{8.8}$$



Obr. 8.6. Schematické znázornění trojúhelníkového čísla T_7. Černé puntíky v k-tém řádku znázorňují počet úderů zvonu v k-té hodině (viz (8.6)). Celkový počet úderů zvonu od jedné hodiny po půlnoci do k-té hodiny je T_k. Čísly jsou označeny délky segmentů mezi zářezy na pomocném kolečku.

Podle (8.7) platí

$$1 + 2 + \cdots + (s-1) = \frac{s-1}{2} \sum_{i=1}^{p} a_i, \tag{8.9}$$

kde p je délka periody a $(s-1)/2$ je celé. Pro odpovídající posloupnost

$$\underbrace{a_1, a_2, \ldots, a_p}_{s}, \underbrace{a_1, a_2, \ldots, a_p}_{s}, \ldots, \underbrace{a_1, a_2, \ldots, a_p}_{s}, \tag{8.10}$$

pak vztah (8.9) vyjadřuje, že se perioda $a_1, a_2, \ldots, a_p$ v posloupnosti (8.10) opakuje $(s-1)/2$krát.

Musíme ověřit rovnost (8.4) pro všechna $k \geq (s+1)/2$ za předpokladu (8.8). Pro $k = s-1$, které je sudé, pomocí (8.2),

(8.9) a (8.3) dostáváme

$$T_k = T_{s-1} = \frac{k}{2}\sum_{i=1}^{p} a_i = \sum_{i=1}^{pk/2} a_i,$$

neboli $n = pk/2$ v (8.4) a číslo T_{s-1} je tedy dosažitelné.

Předpokládejme nyní, že $k = s-1-k'$, kde $1 \le k' \le (s-3)/2$ a $s > 3$. Podle předpokladu (8.8) existuje $n' \in \mathbb{N}$ tak, že

$$\frac{k'(k'+1)}{2} = \sum_{i=1}^{n'} a_i. \tag{8.11}$$

Ze vztahu (8.2) plyne, že

$$\begin{aligned} T_k = T_{s-1-k'} &= \frac{(s-1-k')(s-k')}{2} \\ &= \frac{s(s-1-2k')}{2} + \frac{k'(k'+1)}{2}. \end{aligned} \tag{8.12}$$

Protože s je liché a $1 \le k' \le (s-3)/2$, je $m = s-1-2k'$ sudé přirozené číslo. Tedy podle (8.12), (8.7), (8.11) a (8.3) platí

$$T_k = \frac{s-1-2k'}{2}\sum_{i=1}^{p} a_i + \sum_{i=1}^{n'} a_i = \sum_{i=1}^{pm/2+n'} a_i.$$

Dále nechť $k = qs + k'$ pro $q \in \mathbb{N}$ a $0 \le k' < s$. Potom z (8.2) a (8.7) dostaneme, že

$$T_k = \frac{(qs+k')(qs+k'+1)}{2} = sj + \frac{k'(k'+1)}{2} = \sum_{i=1}^{pj} a_i + T_{k'},$$

kde $j = q(qs+1)/2 + qk'$ je celé číslo a $T_{k'} = 0$ pro $k' = 0$. Z předchozí části důkazu již ale víme, že $T_{k'} = \sum_{i=1}^{n'} a_i$ pro nějaké $n' \in \mathbb{N}$ a $0 < k' < s$. □

Poznámka. Číslo $(s-1)/2$ v (8.8) 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 věty 8.1 můžeme demonstrovat na pražské hodinové posloupnosti (8.1) pro $s = 15$. Stačí totiž ověřit vztah (8.5) pouze pro $k \leq (s-1)/2 = 7$, tedy jen první řádek v (8.1). (Přitom $T_7 = 28$ z obr. 8.6 je dokonalé číslo.) Dosažitelnost celých čísel $k > 7$ na dalších řádcích (8.1) pak vyplývá z věty 8.1.

Podobně můžeme ověřit předpoklady věty 8.1 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 například z periody 1, 2, 1, 1, 1:

$$1\ 2\ \underbrace{1\ 1\ 1}_{3}\quad \underbrace{1\ 2\ 1}_{4}\quad \underbrace{1\ 1\ 1\ 2}_{5}\quad \underbrace{1\ 1\ 1\ 1\ 2}_{6}\ldots \tag{8.13}$$

Činitel $(s-1)/2$ na pravé straně (8.9) ale není celočíselný. Proto příslušné prvky posloupnosti vyjadřující číslo $s = 6$ v (8.13) nejsou ve stejném pořadí jako daná perioda. Později ve větě 8.6 ukážeme, jak lze nalézt pro dané s šindelovskou posloupnost.

Věta 8.2. *Periodická posloupnost* (a_i) *je pro sudé* s *ve vztahu* (8.7) *šindelovská, jestliže* T_k *je dosažitelné pomocí* (a_i) *pro* $k = 1, 2, \ldots, s-1$.

D ů k a z. Nechť s v (8.7) je sudé a nechť

$$\forall\, k \in \{1, 2, \ldots, s-1\} \quad \exists\, n \in \mathbb{N} : \; T_k = \sum_{i=1}^{n} a_i. \tag{8.14}$$

Ze vztahů (8.7) a (8.3) vyplývá, že

$$T_{2s-1} = (2s-1)\sum_{i=1}^{p} a_i = \sum_{i=1}^{(2s-1)p} a_i.$$

Nechť $k = 2s - 1 - k'$, kde $1 \leq k' \leq s-1$. Podle předpokladu (8.14) existuje $n' \in \mathbb{N}$ tak, že

$$\frac{k'(k'+1)}{2} = \sum_{i=1}^{n'} a_i.$$

Potom z (8.2) máme

$$\begin{aligned} T_k = T_{2s-1-k'} &= \frac{(2s-1-k')(2s-k')}{2} \\ &= s(2s-1-2k') + \frac{k'(k'+1)}{2}, \end{aligned}$$

a tudíž

$$T_k = (2s-1-2k')\sum_{i=1}^{p} a_i + \sum_{i=1}^{n'} a_i = \sum_{i=1}^{pm+n'} a_i,$$

kde $m = 2s - 1 - 2k'$.

Zbytek důkazu pro $k \geq 2s-1$ je podobný důkazu věty 8.1. □

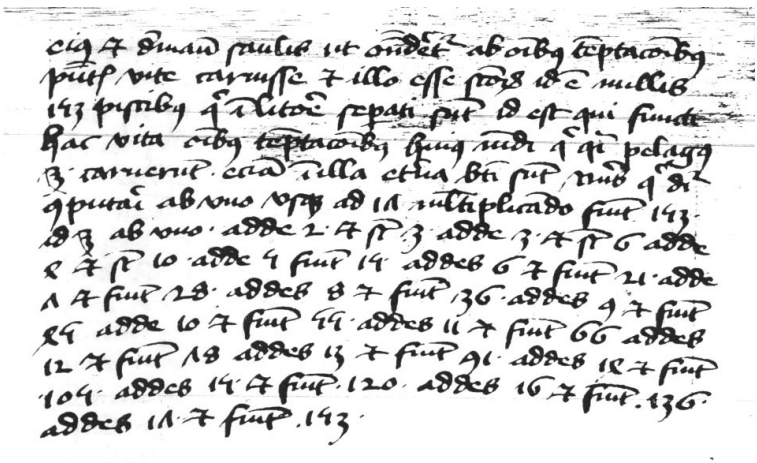
Poznámka. Číslo $s-1$ v (8.14) opět nelze zmenšit, je-li p délka minimální periody odpovídající s. Abychom to ověřili, stačí uvažovat periodickou posloupnost (a_i) s minimální periodou $1, 2, 1$ a $s = 4$. Pak trojúhelníková čísla T_1 a T_2 jsou dosažitelná pomocí (a_i), ale T_3 není.

Poznámka. Traduje se historka, že učitel zadal ve třídě, kterou navštěvoval mladý Gauss, vypočítat součet $1+2+\cdots+100$. Gauss si uvědomil, že když sečte první sčítanec s posledním, dostane číslo 101 stejně tak, jako když sečte druhý sčítanec s předposledním atd. Ke stanovení celkového součtu mu tedy stačilo vynásobit číslo 101

polovičním počtem sčítanců:

$$1 + 2 + \cdots + 100 = (1 + 100) + (2 + 99) + \cdots + (50 + 51)$$
$$= 101 \cdot 50 = 5050.$$

Gauss tak místo zdlouhavého postupného přičítání $1 + 2 + 3 + \cdots$ použil vlastně vztah (8.2) a odvodil, že $T_{100} = 5050$ (srov. též obr. 4 z předmluvy).



Obr. 8.7. Ukázka z díla *Liber de numeris* (viz folio 151r), kde se na řádcích 5 a 6 popisuje, jak vynásobit čísla $9 \times 17 = 153$. Cifry 4, 5 a 7 jsou psány podobným způsobem jako na vnějším ciferníku orloje – srov. obr. 8.1. Od sedmé řádky je pak (volně přeloženo) napsáno: *... k jedné přidej* 2, *dostaneš* 3. *K nim přidej* 3, *budeš mít* 6. *K nim přičti* 4, *dostaneš* 10, *dále přidej* 5 *a budeš mít* 15. *K* 15 *přidaných* 6 *dává* 21, *k nim přičti* 7, *dostaneš* 28. *Přidej* 8 *a to dává* 36, *k nim připočítej* 9, *dostaneš* 45. *Pak přidej* 10 *a budeš mít* 55. *Po přičtení* 11 *je součet* 66, *tak přidej* 12 *a dostaneš* 78. *Přičti* 13 *a máš* 91. *Přidej* 14, *dostaneš* 105, *k nim přičti* 15, *budeš mít* 120. *Po přidání* 16 *to dává* 136 *a k nim přičti* 17 *a dostaneš* 153.

Podobné úvahy pro lichý počet sčítanců lze ale vysledovat i v pojednání *Liber de numeris,* které vzniklo zhruba o 350 let dříve a je uloženo v odd. XIII.F.I. pražského Klementina. Šindel podle tohoto textu (viz folio 153r) přednášel matematiku na pražské univerzitě

v roce 1437 a není vyloučeno, že je i jeho autorem, viz (Spunar, 1985, s. 135), (Urbánková, 1962, s. 88). I když tehdy neexistovaly vzorce typu (8.2), Šindel věděl, že součet po sobě následujících čísel lze napsat jako součin dvou přirozených čísel. Ukažme si to na příkladu z obrázku 8.7, kde se ukazuje, že[8)]

$$1 + 2 + \cdots + 17 = 17 \cdot 9 = 153,$$

jinými slovy $T_{17} = 153$. Srovnej s obr. 4 z předmluvy pro $a = 1$ a $b = 17$ (viz též (8.2)).

8.5. 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*.

Nežli uvedeme nutnou a postačující podmínku pro existenci šindelovské posloupnosti, která se bude opírat o pojem kvadratického zbytku, dokážeme důležitou vlastnost, kterou později využijeme při důkazu vět 8.4 a 8.9.

Věta 8.3. *Jestliže f a h jsou celá nezáporná čísla, pak $8f + 1$ je kvadratický zbytek modulo 2^h.*

Důkaz. Jestliže $h \in \{0, 1, 2, 3\}$, pak $8f + 1 \equiv 1 \pmod{2^h}$. Odtud plyne, že levá strana kongruence $8f + 1$ je kvadratický zbytek, a tedy pravá strana je kvadratický zbytek, neboť $3^2 \equiv 1 \pmod{2^h}$.

[8)] Číslo 153 má celou řadu dalších zajímavých vlastností, např. $153 = 1! + 2! + 3! + 4! + 5!$, $153 = 1^3 + 3^3 + 5^3$, viz též věta 9.8.

Předpokládejme nyní, že $h \geq 4$. Nechť f a c jsou nezáporná celá čísla taková, že $0 \leq c \leq 2^{h-3} - 1$ a $f \equiv c \pmod{2^{h-3}}$, tj. $2^{h-3} \mid (f-c)$. Protože číslo $8 \cdot 2^{h-3} = 2^h$ dělí $(8f+1)-(8c+1) = 8(f-c)$, dostáváme, že $8f+1 \equiv 8c+1 \pmod{2^h}$. Celkem máme 2^{h-3} zbytků $8\ell+1$ modulo 2^h, které nejsou vzájemně kongruentní, pro $0 \leq \ell \leq 2^{h-3} - 1$, neboť $0 \leq 8\ell + 1 < 2^n$. Proto bez újmy na obecnosti můžeme předpokládat, že $8f + 1$ je prvkem množiny

$$A = \{0 \cdot 8 + 1,\ 1 \cdot 8 + 1,\ 2 \cdot 8 + 1,\ \ldots,\ (2^{h-3} - 1)8 + 1\},$$

která má 2^{h-3} prvků. V knize (Niven, Zuckerman, Montgomery, 1991, s. 105) je dokázáno, že množina $\{1, 3, 5, \ldots, 2^h - 1\}$ lichých zbytků je totožná s $\{(-1)^i 5^j\}$ modulo 2^h, kde $0 \leq i \leq 1$ a $0 \leq j \leq 2^{h-2} - 1$. Zřejmě $5^{2j} = (5^j)^2$ je lichý kvadratický zbytek modulo 2^h pro celé nezáporné j. Podle našich předchozích úvah 2^{h-3} lichých kvadratických zbytků 5^{2j} modulo 2^h nejsou vzájemně kongruentní pro $0 \leq j \leq 2^{h-3} - 1$, neboť $0 \leq 2j \leq 2^{h-2} - 1$. Dále vidíme, že

$$5^2 = 25 = 3 \cdot 8 + 1.$$

Podle binomické věty tedy platí

$$\begin{aligned} 5^{2j} &= (3 \cdot 8 + 1)^j \\ &= 3^j 8^j + \binom{j}{1} 3^{j-1} 8^{j-1} + \cdots + \binom{j}{j-1} 3 \cdot 8 + 1 \\ &\equiv 1 \pmod{8} \end{aligned}$$

pro $0 \leq j \leq 2^{h-3} - 1$. Protože obě množiny A a $\{5^{2j} \mid 0 \leq j \leq 2^{h-3} - 1\}$ obsahují stejný počet prvků, věta je dokázána. □

Věta 8.4. *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 kvadratickým zbytkem modulo s.

D ů k a z. $\Leftarrow$: Nechť periodická posloupnost (a_i) není šindelovská. Pak podle (8.5) existují přirozená čísla ℓ a m tak, že $a_m \geq 2$ a

$$\sum_{i=1}^{m-1} a_i < T_\ell < \sum_{i=1}^{m} a_i,$$

tj. existuje přirozené číslo $j \leq a_m - 1$ tak, že

$$T_\ell = \sum_{i=1}^{m} a_i - j. \tag{8.15}$$

Nechť $n \in \{1, \ldots, p\}$ je takové, že $n \equiv m \pmod{p}$. Pak z (8.2), (8.15), (8.7) a (8.3) vyplývá

$$(2\ell+1)^2 = 4\ell^2 + 4\ell + 1 = 8T_\ell + 1 = 8\Big(\sum_{i=1}^{m} a_i - j\Big) + 1$$
$$\equiv 8\Big(\sum_{i=1}^{n} a_i - j\Big) + 1 \pmod{s},$$

tj. $8\big(\sum_{i=1}^{n} a_i - j\big) + 1$ je čtverec modulo s.

$\Rightarrow$: Nechť (a_i) je šindelovská posloupnost a $s = 2^c d$, kde $c \geq 0$ a d je liché. Předpokládejme obráceně, že existují přirozená čísla n, j a x tak, že $n \leq p$, $a_n \geq 2$, $j \leq a_n - 1$, $x \leq s$ a

$$w = 8\Big(\sum_{i=1}^{n} a_i - j\Big) + 1 \equiv x^2 \pmod{s}. \tag{8.16}$$

Z věty 8.3 a vztahu (8.16) plyne existence y takového, že

$$x^2 \equiv w \pmod{d}, \tag{8.17}$$
$$y^2 \equiv w \pmod{2^{c+3}}.$$

Podle Čínské věty o zbytcích 1.4 existuje přirozené číslo $u \geq 3$ tak,[9] že $u \equiv x \pmod{d} \wedge u \equiv y \pmod{2^{c+3}}$. Tedy podle (8.17)

[9] Zde požadujeme $u \geq 3$, abychom se vyhnuli případu $w = u = 1$ v (8.16).

platí

$$u^2 \equiv x^2 \equiv w \pmod{d},$$
$$u^2 \equiv y^2 \equiv w \pmod{2^{c+3}}.$$

Protože $(d, 2^{c+3}) = 1$, máme

$$u^2 \equiv w \pmod{2^{c+3}d}. \tag{8.18}$$

Zřejmě je u liché, neboť w je liché. Nechť tedy $u = 2\ell + 1$, kde $\ell \geq 1$. Potom ze vztahu (8.18) dostáváme $u^2 = 4\ell^2 + 4\ell + 1 = w + 2^{c+3}dg$ pro nějaké celé číslo g. Protože $u \geq 3$, ze vztahů (8.2), (8.18) a (8.16) platí, že

$$T_\ell = \frac{u^2 - 1}{8} = \frac{w - 1}{8} + 2^c dg \equiv \sum_{i=1}^{n} a_i - j \pmod{s}.$$

Tedy existuje přirozené číslo m tak, že $m \equiv n \pmod{p}$ a

$$T_\ell = \sum_{i=1}^{m} a_i - j,$$

což je spor s předpokladem, že (a_i) je šindelovská posloupnost. □

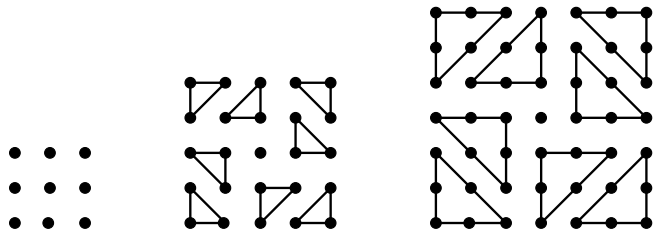
Jako vedlejší výsledek důkazu věty 8.4 dostáváme další známé tvrzení, viz (Burton, 1998, s. 15) a obr. 8.8.

Věta 8.5. *Přirozené číslo r je trojúhelníkové právě tehdy, když je $8r + 1$ je čtvercové.*

D ů k a z. Pokud $r = T_\ell = \ell(\ell + 1)/2$, pak $8r + 1 = 4\ell^2 + 4\ell + 1 = (2\ell + 1)^2$.

Jestliže obráceně $8r + 1$ je čtverec, pak $8r + 1 = (2\ell + 1)^2$ pro nějaké celé číslo ℓ, protože $8r + 1$ je liché. Potom

$$r = \frac{(2\ell + 1)^2 - 1}{8} = \frac{4\ell(\ell + 1)}{8} = \frac{\ell(\ell + 1)}{2} = T_\ell. \qquad \square$$



Obr. 8.8. Již staří pythagorejci věděli, že když r je trojúhelníkové číslo, pak $8r+1$ je čtverec. Tento výsledek byl zaznamenán řeckým historikem Plútarchem kolem roku 100, viz (Tattersall, 2005, s. 4).

Poznámka. Ve větě 8.4 požadujeme, aby

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

nebylo kvadratickým zbytkem modulo s pro různé hodnoty n a j, když (a_i) je šindelovská posloupnost. Postačující podmínka pro to je, že w není kvadratický zbytek pro nějaké liché prvočíslo q dělící s. K tomu, abychom viděli, že tato podmínka není nutná, uvažujme periodickou posloupnost (a_i) z příkladů uvedených za větou 8.1 s $p = 11$, $s = 25$ a periodou 1, 2, 2, 1, 4, 1, 4, 1, 4, 1, 4. Pak

$$8\Big(\sum_{i=1}^{5} a_i - 2\Big) + 1 = 65$$

není kvadratický zbytek modulo 25, ale je kvadratický zbytek modulo 5. Přitom 5 je jediné liché prvočíslo, které dělí $s = 25$.

Poznámka. Uvažujme posloupnost (a_i) s periodou $1, 2, 1, 1, \ldots, 1$ a povšimněme si, že

$$w = 8\Big(\sum_{i=1}^{2} a_i - 1\Big) + 1 = 17.$$

Z věty 8.4 a zákona kvadratické reciprocity (viz věta 2.23) je patrné,

že pokud s je liché prvočíslo a

$$s \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17}, \tag{8.19}$$

pak w je také kvadratický zbytek modulo s, a tedy (a_i) není šindelovská posloupnost (kvadratické zbytky včetně nuly jsou na obr. 2.4 znázorněny bílými kroužky). Protože ale $s = 15$ není prvočíslem, je posloupnost s periodou $1, 2, 1, 1, \ldots, 1$ šindelovská. Periody dalších posloupností (a_i) lze vyšetřovat obdobně.

8.6. Konstrukce primitivní šindelovské posloupnosti

Nejprve si zavedeme pojem složené a primitivní šindelovské posloupnosti. Pak uvedeme větu, která nám bude zaručovat existenci jediné primitivní šindelovské posloupnosti pro dané s (viz (8.7)).

Šindelovská posloupnost (a'_i) s minimální délkou periody $p + 1$ se nazývá *složená*, jestliže existuje posloupnost (a_i) a $\ell \in \mathbb{N}$ tak, že

$$\begin{aligned} a_i &= a'_i, \quad i = 1, \ldots, \ell - 1, \\ a_\ell &= a'_\ell + a'_{\ell+1}, \\ a_i &= a'_{i+1}, \quad i = \ell + 1, \ldots, p. \end{aligned}$$

Příklad. Perioda 1, 2, 3, 2, 2, 3, 2 odvozená z periody $1, 2, 3, 4, 3, 2$ posloupnosti (8.1) dává složenou šindelovskou posloupnost. Jinými slovy, pomocné kolečko (s jedním zářezem navíc) by fungovalo i pro tuto složenou šindelovskou posloupnost.

Šindelovská posloupnost (a_i) se nazývá *primitivní,* jestliže není složená.

Příklad. Snadno lze ověřit, že všechny posloupnosti z příkladů uvedených za větou 8.1 jsou primitivní.

Důkaz následující věty obsahuje explicitní algoritmus pro nalezení primitivní šindelovské posloupnosti pro dané s.

Věta 8.6. *Pro každé $s \in \mathbb{N}$ existuje jediná primitivní šindelovská posloupnost (a_i) tak, že platí (8.7) pro nějakou (ne nutně minimální) délku periody p.*

Důkaz. Nechť $1 \leq b_1 < b_2 < \cdots < b_t \leq s$ jsou všechna přirozené čísla taková, že $8b_n + 1$ je čtverec modulo s pro $n = 1, \ldots, t$. Vidíme, že $b_1 = 1$ a $b_t = s$. Zvolme nyní periodu takto: $a_1 = b_1$ a $a_n = b_n - b_{n-1}$ pro $n = 2, 3, \ldots, t$. Pak

$$\forall n \in \{1, 2, \ldots, t\} : \quad b_n = \sum_{i=1}^{n} a_i.$$

Tvrdíme, že (a_i) je šindelovská posloupnost. Vidíme, že pokud $n \in \{1, \ldots, t\}$, $a_n \geq 2$ a $j \in \{1, 2, \ldots, a_n - 1\}$, pak

$$b_{n-1} < \sum_{i=1}^{n} a_i - j < b_n.$$

Tedy $8(\sum_{i=1}^{n} a_i - j) + 1$ je kvadratické nereziduum modulo s, protože

$$8b_1 + 1, \ldots, 8b_t + 1$$

jsou všechny kvadratické zbytky modulo s. Podle věty 8.4 je (a_i) šindelovská posloupnost.

Navíc vidíme, že (a_i) je primitivní šindelovská posloupnost s délkou periody $p = t$ splňující (8.7). Z konstrukce periody je také zřejmé, že (a_i) je jediná primitivní šindelovská posloupnost, která vyhovuje (8.7) pro nějakou délku periody p. □

Posloupnost $1, 1, 1, \ldots$ se nazývá *triviální* šindelovská posloupnost.

Věta 8.7. *Primitivní šindelovská posloupnost (a_i) je triviální právě tehdy, když $s = 2^h$ pro $h \geq 0$.*

Důkaz. $\Longleftarrow$: Z konstrukce periody v důkazu předchozí věty 8.6 vyplývá, že primitivní šindelovská posloupnost odpovídající s je netriviální právě tehdy, když existuje přirozené číslo $f \leq s$ takové, že $8f + 1$ není kvadratický zbytek modulo s. Podle věty 8.3

je $8f + 1$ vždy kvadratický zbytek modulo $s = 2^h$ pro $h \geq 0$. Tudíž primitivní šindelovská posloupnost odpovídající $s = 2^h$ je triviální.

$\Longrightarrow$: Nechť obráceně s má lichý prvočíselný dělitel q a nechť d není kvadratický zbytek modulo q. Předpokládejme, že $8z \equiv 1 \pmod{q}$, tj. z je inverzní prvek k 8 modulo q. Pro $f \equiv z(d-1) \pmod{q}$ je tedy $8f+1 \equiv d \pmod{q}$. Odtud vyplývá, že primitivní šindelovská posloupnost odpovídající s je netriviální. □

Z vět 8.6 a 8.7 okamžitě plyne následující tvrzení.

Věta 8.8. *Nechť (a_i) je periodická posloupnost s minimální délkou periody p a $s = 2^m$, kde m je nezáporné celé číslo. Pak (a_i) je šindelovská posloupnost právě tehdy, když (a_i) je triviální.*

Dále dokážeme větu, která nám zaručuje, že pro libovolné dané přirozené číslo k lze vždy najít šindelovskou posloupnost, která jej bude obsahovat.

Věta 8.9. *Pro každé $k \in \mathbb{N}$ existuje $\ell \in \mathbb{N}$ a šindelovská posloupnost (a_i) taková, že $a_\ell = k$.*

Důkaz. Číslo $8r + 1$ je čtverec právě tehdy, když r je trojúhelníkové číslo (viz věta 8.5). Budiž $k = T_k - T_{k-1}$ dáno (viz (8.6)). Podle věty 8.6 stačí nalézt přirozené číslo $s \geq T_k$ tak, že $8(T_{k-1} + j) + 1$ není kvadratický zbytek modulo s pro $j = 1, 2, \ldots, k-1$.

Pro pevné $j \in \{1, \ldots, k-1\}$ nechť

$$8(T_{k-1} + j) + 1 = \prod_{i=1}^{v} p_i^{\alpha_i}$$

je prvočíselný rozklad. Protože $8(T_{k-1} + j) + 1$ není čtverec, musí být některé α_i liché. Bez újmy na obecnosti můžeme předpokládat, že α_1 je liché. Nechť c_1 není kvadratický zbytek modulo p_1. Podle Čínské věty o zbytcích 1.4 a Dirichletovy věty 3.10 o nekonečnosti prvočísel v aritmetických posloupnostech můžeme najít prvočíslo $q_j \geq T_k$ takové, že $q_j \equiv 1 \pmod{4}$, $q_j \equiv c_1 \pmod{p_1}$ a $q_j \equiv 1 \pmod{p_i}$ pro $i \in \{2, \ldots, v\}$.

Protože $q_j \equiv 1 \pmod 4$, z vlastností Legendrova symbolu a zákona kvadratické reciprocity (viz věty 2.22 a 2.23) dostaneme

$$\left(\frac{p_1}{q_j}\right) = \left(\frac{q_j}{p_1}\right) = \left(\frac{c_1}{p_1}\right) = -1$$

a

$$\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1 \quad \text{pro } i = 2, 3, \ldots, v,$$

kde $\left(\frac{p}{q}\right)$ je Legendrův symbol pro lichá prvočísla p a q. Jelikož je Jacobiho symbol multiplikativní (viz (2.37)), vidíme, že

$$\left(\frac{8(T_{k-1}+j)+1}{q_j}\right) = \prod_{i=1}^{v}\left(\frac{p_i}{q_j}\right)^{\alpha_i} = (-1)^{\alpha_1}\prod_{i=2}^{v} 1^{\alpha_i} = -1,$$

a tudíž, $8(T_{k-1}+j)+1$ je kvadratické nereziduum modulo q_j. Nyní stačí definovat s jako součin různých q_j pro $j \in \{1, \ldots, k-1\}$. □

Příklad. Perioda 1, 2, 3, 4, 5, 3, 3, 7, 2, 3, 3, 9 s minimální délkou periody $p = 12$ a $s = 45$ dává primitivní šindelovskou posloupnost (a_i) s poměrně velkou hodnotou $a_{12} = 9$ vzhledem k s (viz věta 8.6).

8.7. Která šindelovská posloupnost je nejkrásnější?

V důkazu věty 8.6 je obsažen numerický algoritmus pro vytváření primitivních šindelovských posloupností. Následující tabulka udává periody těchto posloupností pro $s = 1, \ldots, 25$. 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 (8.1), která byla použita při konstrukci bicího stroje pražského orloje. Tuto posloupnost generuje při otáčení pomocné kolečko znázorněné na obrázcích IX a X barevné přílohy a na obrázcích 8.4 a 8.5.

s	**Periody primitivních šindelovských posloupností**															
1	1															
2	1	1														
3	1	2														
4	1	1	1	1												
5	1	2	2													
6	1	2	1	2												
7	1	2	3	1												
8	1	1	1	1	1	1	1	1								
9	1	2	3	3												
10	1	2	2	1	2	2										
11	1	2	1	2	4	1										
12	1	2	1	2	1	2	1	2								
13	1	1	1	3	2	2	3									
14	1	2	3	1	1	2	3	1								
15	**1**	**2**	**3**	**4**	**3**	**2**										
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	1	1	1	2	4	1	4	2							
18	1	2	3	3	1	2	3	3								
19	1	1	1	3	1	2	1	5	2	2						
20	1	2	2	1	2	2	1	2	2	1	2	2				
21	1	2	3	1	3	3	2	6								
22	1	2	1	2	4	1	1	2	1	2	4	1				
23	1	2	2	1	3	1	3	2	5	1	1	1				
24	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
25	1	2	2	1	4	1	4	1	4	1	4					

Z tabulky dále vidíme, že triviální primitivní šindelovské posloupnosti vznikají pro $s = 2^h$ a nějaké $h \geq 0$, jak jsme již dokázali ve větě 8.7.

O struktuře šindelovských posloupností pro případ $s = 13$ a $s = 19$, kdy $a_2 = 1$, se diskutuje v poznámce ke vztahu (8.19). Pokud by zvon zvonil

$$1 + 2 + \cdots + 12 = 78 = 6 \times 13$$

za každý půlden, pak by pomocné kolečko bylo nejspíše voleno tak, že $s = 13$, přičemž další možnosti jsou $s \in \{2, 3, 6, 26, 39\}$. Jejich příslušné primitivní šindelovské posloupnosti ale nejsou tak „hezké“, jako je pražská hodinová posloupnost (8.1).

Z tabulky je také patrné, že neexistuje primitivní šindelovská posloupnost, jejíž perioda je minimální pro $s < 25$ sudé. Tuto vlastnost si nyní dokážeme pro s libovolně velké.

Věta 8.10. *Existuje jediná primitivní šindelovská posloupnost s minimální periodou právě tehdy, když s ve vztahu* (8.7) *je liché.*

Důkaz. $\Rightarrow$: Nechť $s = 2^c d$, kde $c \geq 1$ a d je liché. Protože podle věty 8.3 je $8f + 1$ kvadratický zbytek modulo 2^c pro všechna nezáporná celá čísla f, podle Čínské věty o zbytcích 1.4 je $8f + 1$ čtverec modulo s právě tehdy, když $8f + 1$ je čtverec modulo d. Z konstrukce v důkazu věty 8.6 plyne, že primitivní šindelovská posloupnost odpovídající $s = 2^c d$ má stejnou periodu (ne nutně minimální), jako je perioda primitivní šindelovské posloupnosti odpovídající $s = d$. Vidíme tedy, že pro s sudé nemá primitivní šindelovská posloupnost odpovídající součtu s příslušnou periodu jako minimální.

$\Leftarrow$: Buď nyní s liché číslo. Jestliže $s = 1$, tvrzení je triviální. Nechť tedy $s \geq 3$ a nechť (a_i) je jediná (viz věta 8.6) primitivní šindelovská posloupnost odpovídající s s délkou periody p. Předpokládejme, že p' je minimální délka periody posloupnosti (a_i) a nechť

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

Předpokládejme naopak, že $p' < p$, tj. $s' < s$. Pro $k \in \mathbb{N}$

položme $w_k = \sum_{i=1}^{k} a_i$. Abychom obdrželi spor, stačí podle věty 8.6 najít přirozené číslo $n \leq p$ tak, že $8w_n + 1$ je kvadratické nereziduum modulo s. K tomu stačí najít dělitele f čísla s tak, aby $8w_n + 1$ bylo kvadratické nereziduum modulo f.

Protože $(8, s) = 1$, existuje jediné celé číslo b tak, že $0 \leq b \leq s - 1$ a $8b + 1 \equiv 0 \pmod{s}$. Nechť $b \equiv -z \pmod{s}$, kde z je inverze prvku 8 modulo s. Jelikož 0 je čtvercem modulo s, vidíme z konstrukce z důkazu věty 8.6, že $8w_k + 1 \equiv 0 \pmod{s}$ pro nějaké $k \in \{1, 2, \ldots, p\}$. Nechť m je přirozené číslo takové, že $m \leq p'$ a $m \equiv k \pmod{p'}$. Pak $8w_m + 1 \equiv 0 \pmod{s'}$. Protože $s' < s$, existuje liché prvočíslo q tak, že $q \mid \frac{s}{s'} = \frac{p}{p'}$. Předpokládejme nejprve, že $q \nmid s'$, a uvažujme q čísel

$$8w_m + 1, 8w_{m+p'} + 1, 8w_{m+2p'+1}, \ldots, 8w_{m+(q-1)p'} + 1. \quad (8.20)$$

Povšimněme si, že

$$(8w_{m+jp'} + 1) - (8w_{m+ip'} + 1) = 8(j - i)s' \quad (8.21)$$

pro $0 \leq i < j \leq q - 1$ a že $(8s', q) = 1$, vidíme, že q čísel (8.20) není vzájemně kongruentních modulo q. Nechť e je kvadratické nereziduum modulo q. Pak $8w_{m+jp'} + 1 \equiv e \pmod{q}$ pro nějaké $j \in \{0, 1, 2, \ldots, q - 1\}$, což je spor, neboť $q \mid s$ a $m + jp' \leq m + (q - 1)p' \leq p$.

Nakonec se budeme zabývat zbývajícím případem, v němž $q^\alpha \| s'$ pro nějaké liché prvočíslo q a přirozené číslo α, kde $q^\alpha \| s'$ znamená, že $q^\alpha \mid s'$, ale $q^{\alpha+1} \nmid s'$. Potom $8w_m + 1 \equiv 0 \pmod{q^\alpha}$. Podle (8.21) a vztahu $q^\alpha \| s'$ vidíme, že q čísel v (8.20) je kongruentních s čísly

$$0,\ q^\alpha,\ 2q^\alpha,\ \ldots,\ (q - 1)q^\alpha \pmod{q^{\alpha+1}} \quad (8.22)$$

v nějakém pořadí. Abychom zakončili důkaz, stačí ukázat, že alespoň jedno z q čísel v (8.22) je kvadratické nereziduum modulo $q^{\alpha+1}$. Pokud je α liché, pak zřejmě q^α je kvadratické nereziduum modulo $q^{\alpha+1}$.

Nyní předpokládejme, že α je sudé přirozené číslo, $q^{\alpha} \| r$ a r je kvadratický zbytek modulo $q^{\alpha+1}$. Potom

$$r \equiv \left(aq^{\alpha/2}\right)^2 = a^2 q^{\alpha} \pmod{q^{\alpha+1}}$$

pro nějaké a takové, že $q \nmid a$. Jestliže

$$a^2 q^{\alpha} \equiv h q^{\alpha} \pmod{q^{\alpha+1}},$$

pak

$$a^2 \equiv h \pmod{q}.$$

Nechť u je kvadratické nereziduum modulo q a předpokládejme, že $0 \leq u \leq q-1$. Pak uq^{α} je kvadratické nereziduum modulo $q^{\alpha+1}$. □

9. DALŠÍ APLIKACE TEORIE ČÍSEL

Matematika nám neslúži len na poznávanie prírody,
ale je tiež mohutným nástrojom na jej ovládnutie.

Štefan Schwarz
Matematika v b mol, 1999, str. 30
ed. K. Nemoga, B. Riečan

9.1. Samoopravné kódy

Praktickému užití prvočísel jsme věnovali celou 5. kapitolu. Teorie čísel má ale použití i v dalších oblastech (viz (Borho, Zagier, Rohlfs, Kraft, Jantzen, 1981), (Schroeder, 2006), (Znám, 1987) aj.), např. při kódování a dekódování televizního signálu, v astronomii, při řešení diferenčních a diferenciálních rovnic, při vytváření formátů JPG či PNG, v teorii grup a svazů, v mnoha dalších matematických disciplínách, v informatice, při zpracování signálu z GPS, při studiu struktury atomu nebo rezonance v teorii kmitání. Může ale sloužit i pro zábavu, viz např. (Cihlář, Vopravil, 1995).

Z oddílu 5.1 dále víme, že nová rodná čísla jsou dělitelná 11, abychom mohli snadno zkontrolovat, zda se v nich nevyskytuje chyba. Podobně se pro ověření správnosti u velkých datových souborů používají různé kontrolní součty. To jsou příklady tzv. samodetekujících kódů. Jejich použitím sice můžeme zjistit, že v daném souboru dat vznikla chyba, ale obecně nevíme, který bit se přenesl či zobrazil nesprávně. Pomocí teorie čísel však můžeme tento nedostatek odstranit. Boj se šumem je otázkou tzv. *samoopravných kódů*, jejichž hlavní myšlenku použil již v roce 1947 Richard Wesley Hamming (1915–1998) na tehdejších reléových počítačích, aby ošetřil následky jejich značné nespolehlivosti.

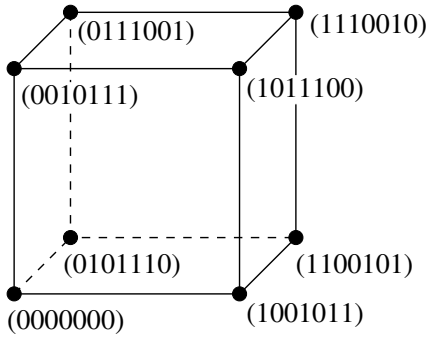
Definujme *Hammingovu vzdálenost* $d(u, v)$ mezi vektory $u = (u_1, u_2, \ldots, u_k)$ a $v = (v_1, v_2, \ldots, v_k)$, $u_i, v_i \in \{0, 1\}$, jako počet míst, ve kterých se u liší od v.

Například pro $k = 3$ je $d((000), (011)) = 2$ nebo $d((101), (010)) = 3$, kde čárky mezi složkami vektorů pro přehlednost vynecháváme.

Jednoduchý samoopravný kód používá následujících osmi *kódových slov*, což jsou vektory délky $k = 7$,

$$\begin{array}{l}(0000000),\\(0010111),\\(1001011),\\(1100101),\\(1110010),\\(0111001),\\(1011100),\\(0101110).\end{array} \tag{9.1}$$

Je vidět, že se nenulové prvky v (9.1) postupně cyklicky posunují vždy o jeden bit vpravo. Dále si povšimněme, že první 3 bity (cifry) v každém řádku (9.1) jsou vzájemně různé a že žádná jiná taková trojice bitů už neexistuje, neboť $2^3 = 8$. První tři bity tedy reprezentují souřadnice vrcholů jednotkové krychle (obr. 9.1). Zbylé 4 bity jsou voleny tak, aby Hammingova vzdálenost mezi libovolnými dvěma řádky v (9.1) byla právě 4.



Obr. 9.1. První tři složky kódových slov jsou souřadnice vrcholů krychle. Hammingova vzdálenost libovolných dvou kódových slov je 4.

Označme G množinu všech osmi kódových slov z (9.1) s operací

$$u \oplus v = (u_1 \oplus v_1, u_2 \oplus v_2, \ldots, u_7 \oplus v_7),$$

kde jednotlivé složky sčítáme podle pravidla:

$$0 \oplus 0 = 0, \quad 1 \oplus 0 = 1, \quad 0 \oplus 1 = 1, \quad 1 \oplus 1 = 0.$$

Tato operace je zřejmě asociativní. Protože Hammingova vzdálenost každých dvou různých prvků z G je 4, jejich sečtením získáme kódové slovo složené ze čtyř jedniček a tří nul. Snadno můžeme ověřit, že toto kódové slovo opět patří do G. Například

$$\begin{aligned}(0101110) &= (1001011) \oplus (1100101) = (1011100) \oplus (1110010) \\ &= (0010111) \oplus (0111001) = (0101110) \oplus (0000000).\end{aligned}$$

Poznamenejme, že množina G spolu s operací sčítání $\oplus$ tvoří tzv. grupu (podrobnosti viz (Pradlová, Křížek, 1999)), jejíž neutrální prvek je první kódové slovo v (9.1) složené ze samých nul a každý prvek je sám k sobě inverzní.

Stručně si nyní popišme vlastní metodu samoopravných kódů, kterou se odstraňují chyby například při přenosu dat z meziplanetárních sond. Používá ji i americká armáda. Nutnost používat samoopravné kódy totiž vzniká tam, kde existuje jistá (ne příliš velká) pravděpodobnost výskytu chyby při přenosu informace, např. při průchodu rádiových vln oblakem meziplanetárního prachu nebo pásem planetek.

Příklad. Přenos dat v případě kodových slov (9.1) probíhá takto: První 3 bity přenášené informace se jednoznačně doplní o další 4 bity podle (9.1) a příslušné kódové slovo se odešle. Pak se vezmou další tři bity přenášené informace, opět se doplní na sedmici podle (9.1) a odešlou atd. Pokud při přenosu informace dojde ke změně jednoho bitu v nějakém kódovém slovu, bude jeho Hammingova vzdálenost od původního kódového slova 1, zatímco od ostatních slov 3 nebo 5. Tak přijímací strana okamžitě zjistí, který bit se špatně přenesl, a opraví jej. Při ztrátě dvou ze sedmice bitů se pouze pozná, že došlo k chybě, a celé kódové slovo se musí vyslat

znovu. Z každého kódového slova se ale při příjmu využijí jen první 3 bity, které nesou původní informaci. Zbylé 4 bity redundantní (tj. přebytečné) informace se pak již mohou vypustit.

Pokud by přenos dat byl ještě méně spolehlivý, je třeba použít jiný samoopravný kód s větší délkou slova (viz (Thompson, 1983)) nebo větší anténu apod. Například první orbitální družice Marsu Mariner 9 byla již v roce 1971 vybavena kódem s možností až sedminásobných oprav na jedno kódové slovo o délce 32 bitů. Každý bod přenášené fotografie povrchu Marsu byl ohodnocen $2^6 = 64$ stupni jasu. Odpovídajících 6 bitů bylo doplněno 26 bity redundantní informace umožňující opravit případné chyby způsobené šumem při přenosu dat meziplanetárním prostorem. Více podrobností o tomto kódu lze nalézt v (Adámek, 1982, s. 90).

Samoopravné kódy se také používají k zabezpečení správného fungování některých pamětí počítačů. Stejně tak známé kompaktní disky jsou jimi „chráněny" před mechanickým poškozením. Například když se povrch disku poškrábe, chybějící informace se patřičně doplní. Jedny z nejúčinnějších samoopravných kódů jsou založeny na použití Leechovy mřížky, která odpovídá nejhustšímu uspořádání koulí ve dvacetičtyřrozměrném prostoru, viz (Thompson, 1983). Poznamenejme ještě, že příroda objevila samoopravné kódy a samoopravné procesy již před mnoha miliardami let. Pokud je například jedno vlákno kyseliny DNA poškozeno, ztracená informace se doplní podle komplementárního vlákna, menší poškození živého organismu se většinou také „samoopraví" apod.

9.2. Šifrování pomocí symetrického klíče

Kryptografie je součástí širšího vědního oboru kryptologie, který zahrnuje též oblast kryptoanalýzy, tj. analýzy bezpečnostních algoritmů. Kryptografie se zabývá ochranou přenosu a uchování dat, především zajištěním jejich důvěrnosti, integrity dat (tj. obsahové neporušenosti), autentičnosti informací a nepopiratelností jejich původu. Prudký rozvoj kryptografie lze spojit s počátkem 20. sto-

letí, kdy se značně rozšířil telegrafní a později rádiový přenos informací. Například německá armáda používala elektromechanický šifrovací stroj Enigma. Jeho kód v roce 1932 rozšifrovali matematici Marian Rejewski, Jerzy Rozycki a Hendryk Zygalski pracující pro polskou tajnou službu. Koncem druhé světové války pak zdokonalený kód rozšifroval geniální matematik Alan Turing (1912–1954), což pomohlo zkrátit válku a ušetřit tak mnoho lidských životů.

V této kapitole představíme velice jednoduchou metodu šifrování pomocí symetrického klíče (tzv. Vernamovy šifry). Symetrické šifry s tajným klíčem se užívají k šifrování rozsáhlých souborů, neboť jsou podstatně rychlejší než asymetrické šifry (jako je například metoda RSA). K odeslání tajné zprávy potřebujeme šifrovací klíč, bez jehož znalosti nelze zprávu rozluštit. Klíč generujeme jako dostatečně dlouhou posloupnost zcela náhodně zvolených nul a jedniček (např. házením mince či pomocí generátorů pseudonáhodných čísel). Níže ukážeme, že takto zvolený tajný klíč se stane klíčem šifrovacím i dešifrovacím zároveň. Proto se mu říká *symetrický klíč.*

Na množině $G = \{0, 1\}$ definujme operaci sčítání $\oplus$ podobně jako v předchozí kapitole:

$$0 \oplus 0 = 0, \quad 1 \oplus 0 = 1, \quad 0 \oplus 1 = 1, \quad 1 \oplus 1 = 0. \qquad (9.2)$$

Tato aritmetická pravidla nyní použijeme k velice jednoduchému šifrování a odšifrování tajné zprávy následujícím postupem:

Text zprávy nejprve překódujeme na posloupnost nul a jedniček. Z oddílu 5.2 již víme, jaký je rozdíl mezi kódováním a šifrováním, což se často zaměňuje. Při kódování se převádí jedna forma zápisu na jinou, avšak nedochází k jejímu utajování. Algoritmus převodu je znám (např. čárový kód na zboží, kód ASCII, radiotelegrafní kód Q apod.). Kódování tedy slouží jen k usnadnění přenosu informace. Naproti tomu šifrování slouží k utajení zprávy. Zprávu ve dvojkové soustavě pak „sečteme“ se šifrovacím klíčem tak, že na jednotlivé cifry postupně používáme vztahy (9.2) – viz první tři

řádky následujícího příkladu:

100001110... tajná zpráva,
000101101... šifrovací klíč,
100100011... přenášená zašifrovaná zpráva,
000101101... dešifrovací klíč,
100001110... odšifrovaná zpráva.

Přijímající strana k zašifrované zprávě přičte dešifrovací klíč – viz poslední tři řádky příkladu. Všimněte si ještě, že součet šifrovacího a dešifrovacího klíče je nula, tj. šifrovací (i dešifrovací) klíč je sám k sobě inverzní. Pokud byl šifrovací klíč zvolen jako skutečně náhodná posloupnost nul a jedniček, pak je samotná zašifrovaná zpráva opět zcela náhodná posloupnost (tj. nenese žádnou informaci).

Věta 9.1. *Zašifrovaná zpráva je po odšifrování totožná s původní zprávou.*

D ů k a z. Ze vztahů (9.2) plyne, že

$$u \oplus v \oplus v = u \oplus 0 = u \quad \text{pro všechna } u, v \in G,$$

a proto musí být po dvojitém použití symetrického klíče dešifrovaná zpráva totožná se zprávou původní. □

Tento způsob šifrování se používá mj. v našich bankách v kombinaci s metodou RSA, která na rozdíl od metody tajného symetrického klíče je metodou s veřejným šifrovacím klíčem. Výhodou symetrického klíče ale je to, že neklade v podstatě žádné nároky na výpočetní čas, zatímco šifrování zpráv metodou RSA je značně časově náročné.

Popišme si jednoduchý způsob použití kombinace metody RSA a symetrického klíče, při kterém probíhá odeslání delší důvěrné zprávy: Náhodně je vygenerován jeden symetrický klíč určité délky, např. 128 bytů (1024 bitů). Důvěrná zpráva se pak rozdělí po osmibytových blocích a každý blok se zašifruje vygenerovaným symetrickým klíčem. Samotný symetrický klíč je zašifrován veřej-

ným RSA klíčem příjemce a odešle se společně se zašifrovanou zprávou. Tak získá příjemce symetrický klíč, aniž by došlo k jeho prozrazení, a může si důvěrnou zprávu odšifrovat.

9.3. Keplerovy mozaiky

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 (Šolcová, 2004). 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.

Věta 9.2 (Keplerova). *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

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k} = \frac{k-2}{2}. \tag{9.3}$$

Pravá strana (9.3) 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 $k \leq 6$ řešitelnosti (9.3). Srovnáme-li složky výsledné k-tice pro přehlednost podle velikosti, dostaneme následujících 17 řešení rovnice (9.3):

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

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

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 nadále už nebudeme požadovat.

Postupným prověřováním předchozích případů získáme jen následujících 12 řešení (viz obr. XI barevné přílohy)

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

Poslední dvě řešení jsou číselně stejná. Všimněte si ale na obr. XI, 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 apod.

9.4. Penrosovy mozaiky

Počátkem sedmdesátých let 20. století britský matematik a fyzik Roger Penrose objevil pokrytí roviny dvěma typy dlaždic, které má lokální pětičetnou symetrii a úzce souvisí se zlatým řezem (viz obr. XII barevné přílohy). Obě dlaždice mají tvar kosočtverce a jejich strany jsou stejně dlouhé. První dlaždice má ostrý úhel roven 72° a druhá 36°. Nazývají se *Penrosovy dlaždice.* Podle (5.32) a (7.3) je

$$\cos 72^\circ = \frac{1}{2\alpha} = -\frac{\beta}{2}, \tag{9.4}$$

kde α je zlatý řez a β je jeho převrácená hodnota s opačným znaménkem. Předpokládejme, že dlaždice mají jednotkové délky stran. Pak první dlaždice má obsah $\sin 72^\circ = 2 \sin 36^\circ \cos 36^\circ$ a druhá dlaždice $\sin 36^\circ$. Poměr jejich obsahů je tedy roven zlatému řezu

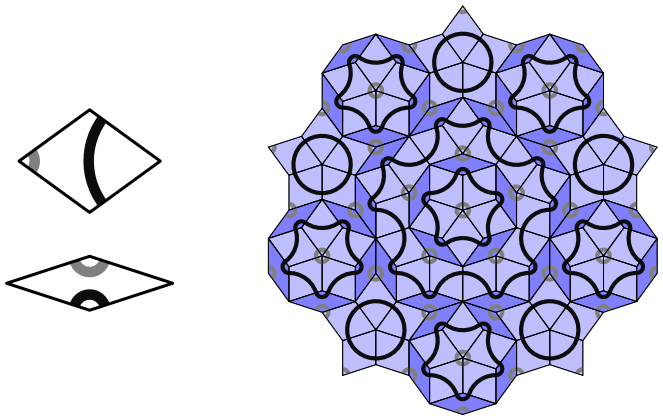
$$\sin 72^\circ : \sin 36^\circ = 2 \cos 36^\circ = \alpha = \frac{1 + \sqrt{5}}{2}.$$

Penrose přiznává, že se inspiroval Keplerovým dílem *Harmonices mundi,* kde se vyšetřují možnosti pokrytí kolem pětiúhelníkových dlaždic. Pro konstrukci Penrosova pokrytí je třeba, aby všechny dlaždice splňovaly tzv. *Penrosovo pravidlo:*

Dlaždice je třeba napojovat tak, aby na sebe spojitě navazovaly oblouky stejné barvy nakreslené na dlaždicích (obr. 9.2).

Nejpřekvapivější vlastností Penrosových pokrytí roviny je skutečnost, že nejsou nikdy periodická (obr. XII). Pokud tedy takové pokrytí posuneme o nějaký vektor, nikdy se nebude shodovat s pů-

vodním pokrytím, i když existuje jen konečný počet možností jak obklopit daný vrchol Penrosovými dlaždicemi.[1)]



Obr. 9.2. K vytvoření aperiodického pokrytí je třeba napojovat Penrosovy dlaždice tak, aby na sebe spojitě navazovaly vyznačené oblouky stejné barvy.

O Penrosově pokrytí existuje velké množství literatury. Zde připomeneme jen jeho původní článek (Penrose, 1974), v němž se dlaždice z obr. 9.2 objevují poprvé, a větu nesoucí jeho jméno.

Věta 9.3 (Penrosova). *Žádné pokrytí roviny Penrosovými dlaždicemi splňující Penrosovo pravidlo není periodické.*

Důkaz lze nalézt např. v (Grünbaum, Shephard, 1987, s. 534–542).

Poznámka. Z Penrosových dlaždic můžeme sestavit i periodická pokrytí, když porušíme Penrosovo pravidlo. Například, když pospojujeme dlaždice jednoho či druhého typu do nekonečně dlouhých pásů, z nichž pak lze vytvářet různá periodická pokrytí. K tomu, abychom dostali aperiodické pokrytí, bohužel nestačí požadovat, aby dvě sousední dlaždice netvořily rovnoběžník. Napří-

[1)] Penrosovo pokrytí lze zobecnit i do vícerozměrných prostorů.

klad lze sestavit periodické pokrytí Penrosovými dlaždicemi, kde každý vrchol je obklopen čtyřmi dlaždicemi s vrcholovými úhly vždy ve stejném pořadí: 36°, 72°, 144° a 108°. V tomto případě také není splněno Penrosovo pravidlo, viz (Křížek, Šolc, 2009).

V roce 1986 nalezl André Katz aperiodické pokrytí roviny vykazující lokální sedmičetnou symetrii. Jeho tři typy dlaždic mají opět tvar kosočtverců, jejichž ostré úhly jsou postupně $180°/7$, $360°/7$ a $540°/7$ (viz obr. XIII barevné přílohy).

Rovinu lze také aperiodicky vyplnit pouze jedním typem dlaždic, které mají tvar například rovnoramenného pravoúhlého trojúhelníku. K tomu stačí uvažovat Ulamovu spirálu z obrázku 3.2. Čtverce odpovídající prvočíslům rozdělíme diagonálou se sklonem 1 na dva trojúhelníky. Ostatní čtverce rozdělíme diagonálou se sklonem (-1).

9.5. Platónská tělesa

Řecký filosof Platón (427–347 př. n. l.) vykládal kosmologii na základě čistě geometrických představ. Přitom zkoumal vlastnosti 5 pravidelných mnohostěnů v trojrozměrném prostoru (viz obr. II barevné přílohy). Připomeňme, že *pravidelný mnohostěn* (též tzv. *platónské těleso*) je konvexní mnohostěn, jehož všechny stěny jsou shodné pravidelné mnohoúhelníky a v jehož každém vrcholu se stýká stejný počet stěn. Dvě pravidelná tělesa budeme považovat za ekvivalentní, pokud jedno dostaneme z druhého pomocí posunutí, otočení a dilatace. Přímým výpočtem se lze přesvědčit, že souřadnice vrcholů pravidelných mnohostěnů jsou například:

pravidelný čtyřstěn $\left(-\frac{\sqrt{2}}{2}, \pm 1, 0\right)$ a $\left(\frac{\sqrt{2}}{2}, \pm 1, 0\right)$,

krychle $(\pm 1, \pm 1, \pm 1)$,

pravidelný osmistěn $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ a $(0, 0, \pm 1)$,

pravidelný dvacetistěn $(\pm\alpha, \pm 1, 0)$, $(0, \pm\alpha, \pm 1)$ a $(\pm 1, 0, \pm\alpha)$, kde α je zlatý řez,

a vrcholy pravidelného dvanáctistěnu jsou ve středech trojúhelníkových stěn pravidelného dvacetistěnu.

Věta 9.4 (Platónova). *Existuje právě* 5 *pravidelných mnohostěnů.*

D ů k a z. Ukážeme, že existuje nejvýše 5 platónských těles, tj. že neexistuje žádné další, které by nebylo na obr. II bar. přílohy. Vnitřní úhel v pravidelném n-úhelníku je roven $(n-2)\,180°/n$. Protože platónské těleso je konvexní mnohostěn, součet všech úhlů kolem jednoho vrcholu mnohostěnu je menší než 360°. Označíme-li k počet pravidelných mnohoúhelníků kolem libovolného vrcholu, dostaneme diofantskou nerovnici

$$k\frac{n-2}{n}180 < 360,$$

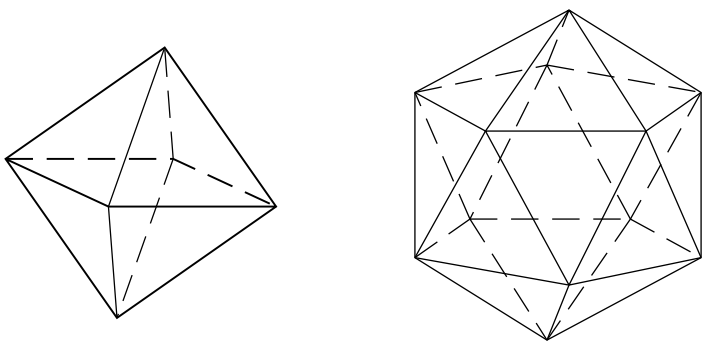
kde zřejmě $k \geq 3$. Odtud po úpravě plyne, že

$$3(n-2) \leq k(n-2) < 2n, \tag{9.5}$$

a tedy

$$n < 6.$$

Pro $n = 3$ má pravá nerovnice v (9.5) právě tři řešení $k \in \{3, 4, 5\}$, která odpovídají pravidelnému čtyřstěnu, osmistěnu a dvacetistěnu.



Obr. 9.3. Pravidelný osmistěn a dvacetistěn.

Pro $n = 4$ má nerovnice (9.5) jediné řešení $k = 3$, jež vede ke krychli. Také pro $n = 5$ dostáváme jen jedno řešení $k = 3$ odpovídající pravidelnému dvanáctistěnu. Každé z těchto pěti řešení je tedy realizovatelné. □

Krychle, jež má 8 vrcholů a 6 stěn, je duální k osmistěnu, protože ten má 6 vrcholů a 8 stěn. Podobně dvanáctistěn, který má 20 vrcholů, je duální k dvacetistěnu, který má 12 vrcholů. Čtyřstěn je duální sám k sobě. Pro každý konvexní mnohostěn platí známý *Eulerův vztah* (který znal René Descartes již v první polovině 17. století)

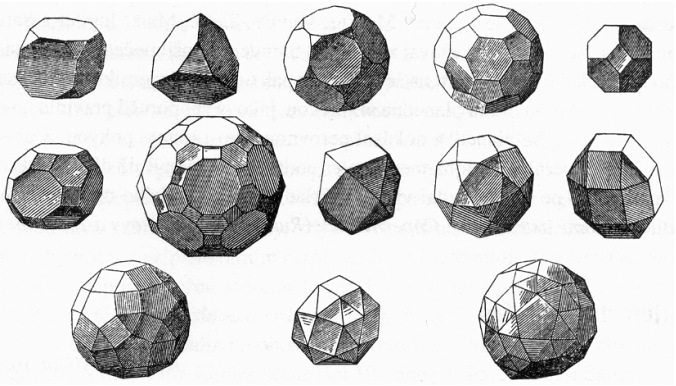
$$v + s = h + 2,$$

kde v je počet vrcholů, h je počet hran a s je počet stěn.

Podobně, jako jsme vyšetřovali pravidelná a polopravidelná pokrytí roviny pravidelnými mnohoúhelníky, lze studovat i tzv. polopravidelná tělesa, viz (Šolcová, 2004). *Polopravidelné těleso* je konvexní mnohostěn, jehož všechny stěny jsou tvořeny pravidelnými mnohoúhelníky a všechny prostorové úhly ve vrcholech mnohostěnu jsou přímo či nepřímo[2)] 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 (obr. 9.4), pravidelné hranoly a pravidelné antihranoly. Jejich existenci lze vyšetřovat podobně jako ve větě 9.4. Pravidelné hranoly mají dvě protilehlé stěny tvořené stejným pravidelným n-úhelníkem a ostatní stěny jsou čtverce (u pravidelných antihranolů pak rovnostranné trojúhelníky). Speciálním případem pravidelného hranolu je krychle (u pravidelných antihranolů pak pravidelný osmistěn). Přehled třinácti archimédovských těles podává Johannes Kepler ve druhé kapitole *Harmonií světa* (Harmonices mundi). Tato tělesa jsou pojmenována po antickém mysliteli Archimédovi. Kolem roku 1905 bylo objeveno ještě čtrnácté archi-

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

médovské těleso, které vznikne otočením „horní vrstvy“ desátého tělesa z obr. 9.4 o 45° a není středově symetrické. Další dvě archimédovská tělesa můžeme dostat jako zrcadlové obrazy posledních dvou těles z obr. 9.4. Terminologie ale není jednotná.

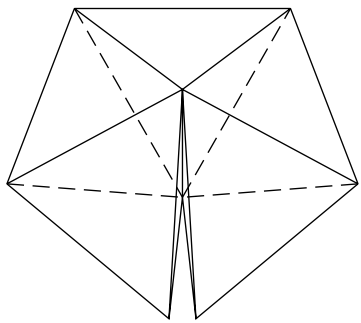


Obr. 9.4. Archimédovská tělesa z Keplerova díla Harmonices mundi.

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 trasy B v Praze). Také fotbalový míč připomíná archimédovské těleso o 12 pětihúhelníkových a 20 šestiúhelníkových stěnách (viz čtvrté těleso na obr. 9.4). 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. Pravidelný dvacetistěn (obr. 9.3) lze také použít k rozdělení trojrozměrného prostoru na ostroúhlé čtyřstěny, viz (Brandts, Korotov, Křížek, 2005). Prostor lze vyplnit i pravidelnými čtyřstěny a osmistěny, které se střídají, anebo krychlemi, které mají celou řadu praktických použití.

9.6. Vykrývací čtyřstěny

V roce 1900 si slavný německý matematik David Hilbert (1862 až 1943) položil otázku: Jaké existují mnohostěny, jejichž shodnými exempláři lze vhodným naskládáním vedle sebe bez mezer vyplnit celý trojrozměrný prostor? Tato dosud ne zcela vyřešená otázka úzce souvisí s tzv. osmnáctým Hilbertovým problémem. Velké množství částečných řešení objevili krystalografové při studiu struktury mřížek monokrystalů. V tomto oddílu se budeme zabývat nejjednodušším případem, kdy mnohostěnem je čtyřstěn. Čtyřstěn, jehož shodnými kopiemi lze vyplnit bez mezer celý prostor, nazveme *vykrývací.*



Obr. 9.5. Shodnými pravidelnými čtyřstěny nelze vyplnit prostor. K dané stěně pravidelného čtyřstěnu lze totiž „připojit" celou stěnou stejně velký pravidelný čtyřstěn právě jedním způsobem. Pokud takto „obtočíme" 5 pravidelných čtyřstěnů kolem jedné společné hrany, objeví se malá mezera.

Řecký učenec Aristotelés inspirován myšlenkami svého učitele Platóna se ve svém díle *O nebi* (350 let př. n. l.) mylně domníval, že prostor lze bez mezer vyplnit pravidelnými čtyřstěny stejné velikosti, viz (Aristote, 1965, sv. 3, kap. 8), což by vyžadovalo, aby úhel mezi dvěma stěnami pravidelného čtyřstěnu byl 72°. Mohli bychom tedy rozdělit pravidelný dvacetistěn na 20 pravidelných čtyřstěnů, jejichž společný bod leží ve středu dvacetistěnu. Protože

Aristotelés byl uznávanou osobností, o jeho tvrzení nikdo nepochyboval. Až arabský matematik Averroes (1126–1198) zjistil, že hrana pravidelného dvacetistěnu (obr. 9.3) vepsaného do koule o poloměru 1 má velikost $\frac{1}{5}\sqrt{10(5-\sqrt{5})} \approx 1.05$ a nerovná se tak 1, jak by plynulo z Aristotelovy domněnky. Aristotelés se tedy mýlil. Stěnové úhly pravidelného čtyřstěnu jsou rovny $\arccos \frac{1}{3}$, což zaokrouhleno na celé stupně je 71°.

Položme si nyní otázku, viz (Křížek, 1994b), zda existuje vykrývací čtyřstěn, jehož všechny hrany mají celočíselné délky. Odpověď se bude opírat o konstrukci, kterou navrhl v roce 1974 Michael Goldberg. V článku (Goldberg, 1974) rozdělil prostor na nekonečně dlouhé trojboké hranoly, jejichž průřez je rovnostranný trojúhelník s délkou strany e. Na třech rovnoběžných hranách jednoho pevně zvoleného hranolu umístíme body A, B, C, D, E a F (obr. 9.6), jejichž souřadnice ve směru svislé osy jsou postupně: 0, a, $2a$, $3a$, $4a$ a $5a$, kde $a > 0$ je libovolné reálné číslo. Snadno nahlédneme, že šikmo seříznutým trojbokým hranolem $ABCDEF$ lze vykrýt celý prostor, neboť jeho stěny ABC a DEF jsou rovnoběžné.

Z obrázku 9.6 je dále patrné, že hranol $ABCDEF$ lze rozdělit na tři shodné čtyřstěny $ABCD$, $BCDE$ a $CDEF$. Označíme-li délku hrany AB jako b a délku AC jako c, pak zřejmě platí

$$b^2 = e^2 + a^2, \quad c^2 = e^2 + 4a^2. \tag{9.6}$$

Vidíme, že hrany BC, CD, DE a EF mají délku b a hrany BD, DF a CE mají délku c. Protože poměr a/e lze udělat libovolný kladný, vykrývacích čtyřstěnů existuje nekonečně mnoho.

Věta 9.5. *Existuje nekonečně mnoho vykrývacích čtyřstěnů, jejichž délky stran jsou celočíselné.*

D ů k a z. Vyloučíme-li e^2 z rovnic (9.6), dostaneme diofantskou rovnici

$$3a^2 + b^2 = c^2. \tag{9.7}$$

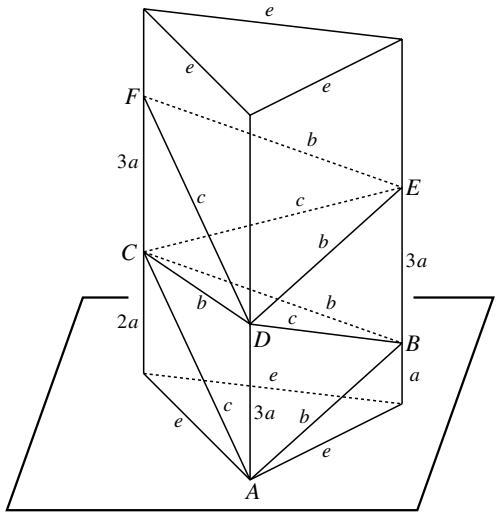
Podobně jako ve větě 2.5 se lze přesvědčit, že rovnice (9.7) má kladná celočíselná řešení tvaru

$$a = 2kmn, \quad b = k(im^2 - jn^2), \quad c = k(im^2 + jn^2),$$

kde i, j, k, m, n jsou libovolná přirozená čísla taková, že $im^2 > jn^2$ a $ij = 3$. □

Například pro $n = 1$ a $m = 2, 3, 4, 5$ dostaneme postupně následující trojice $\langle 3a, b, c\rangle$:

$$\langle 12, 11, 13\rangle, \quad \langle 9, 13, 14\rangle, \quad \langle 24, 13, 19\rangle \quad \text{a} \quad \langle 15, 11, 14\rangle.$$



Obr. 9.6. Goldbergovo dělení nekonečného trojbokého hranolu na shodné čtyřstěny.

9.7. Triky s čísly

Trik s číslem 1089. Proč tolik lidí říká, že *nenávidí* matematiku? Pravda je taková, že mnohdy ani nevědí, co matematika je. Britský matematik David Acheson se domnívá, že matematici by tuto situ-

aci mohli změnit například tím, že zprostředkují široké veřejnosti některé své myšlenky a ukáží, že mají ze své profese radost.

Jednou z cest, jak to udělat, je použít moment *překvapení*, který matematické úlohy často doprovází. A příjemná překvapení má přece každý rád. Takových překvapení si v oddílu 9.7 ukážeme hned několik. Sám Acheson v článku (Acheson, 2004) popisuje, jak zažil svoje první matematické překvapení, když mu bylo 10 let. V té době se mu líbily různé kouzelnické triky. Jednoho dne narazil na následující „trik s čísly“:

Zvolte si libovolné trojciferné číslo tak, aby první a poslední číslice se lišily alespoň o dvě. Utvořte číslo, jehož cifry jsou v opačném pořadí, a odečtěte menší z těchto čísel od většího (např. $782 - 287 = 495$). Výsledek nyní sečtěte s číslem, jehož cifry jsou opět v opačném pořadí (v našem případě $495 + 594 = 1089$).

Pozoruhodné je, že výsledek vyjde *vždy* 1089, ať si zvolíte jakékoliv trojciferné číslo. Acheson říká: „Uvidíte-li tento trik poprvé jako desetileté dítě, doslova vás okouzlí.“

Věta 9.6. *Předchozí trik s trojciferným čísly dává vždy* 1089.

D ů k a z. Stačí uvažovat cifry a, b, c takové, že $a \geq c + 2$. Pak

$$\begin{aligned} 100a + 10b + c - 100c - 10b - a &= 100(a - c) - a + c \\ &= 100(a - c - 1) + 90 + (10 - a + c). \end{aligned}$$

Přičteme-li k tomuto výsledku číslo $100(10-a+c)+90+(a-c-1)$, dostaneme $900 + 180 + 9 = 1089$. □

Trik s číslem 11. Zvolme si dvě libovolná přirozená čísla. Utvořme posloupnost definovanou podobně, jako je Fibonacciho posloupnost daná vztahem (7.1). Zvolíme-li například 5 a 6, potom odpovídající posloupnost bude

$$5,\ 6,\ 11,\ 17,\ 28,\ 45,\ \mathbf{73},\ 118,\ 191,\ 309, \ldots$$

V tomto speciálním případě vidíme, že součet prvních deseti čísel je

roven jedenáctinásobku sedmého čísla (srov. (Livio, 2002, s. 104)),

$$5+6+11+17+28+45+73+118+191+309 = 803 = 11 \cdot 73.$$

Můžeme se tedy ptát: *Jaké číslo dostaneme, když součet prvních deseti čísel podobně vytvořených ze dvou libovolných počátečních hodnot vydělíme sedmým z nich?* Odpověď bude vždy 11, jak plyne z následující věty.

Věta 9.7. *Nechť* $(f_i)_{i=1}^{10}$ *je posloupnost, kde* f_1 *a* f_2 *jsou libovolná přirozená čísla a* $f_i = f_{i-1} + f_{i-2}$ *pro* $i > 2$. *Pak*

$$\frac{1}{f_7} \sum_{i=1}^{10} f_i = 11.$$

D ů k a z. Položme $m = f_1$ a $n = f_2$. Pak vidíme, že

$$\begin{aligned}
f_1 &= m, \\
f_2 &= n, \\
f_3 &= m + n, \\
f_4 &= m + 2n, \\
f_5 &= 2m + 3n, \\
f_6 &= 3m + 5n, \\
f_7 &= 5m + 8n, \\
f_8 &= 8m + 13n, \\
f_9 &= 13m + 21n, \\
f_{10} &= 21m + 34n,
\end{aligned}$$

a tedy

$$\sum_{i=1}^{10} f_i = 55m + 88n = 11 f_7. \qquad \square$$

Poznámka. Počáteční hodnoty f_1 a f_2 v předchozí větě mohou být i libovolná komplexní čísla, pro něž je $f_7 \neq 0$.

Trik s číslem 153. Uvažujme přirozené číslo

$$n = c_k 10^k + \cdots + c_1 10 + c_0, \tag{9.8}$$

kde $c_k, \ldots, c_1, c_0$ jsou jeho cifry z množiny $\{0, 1, 2, \ldots, 9\}$ a $c_k > 0$. Předpokládejme, že n je dělitelné třemi a utvořme číslo

$$m = c_k^3 + \cdots + c_1^3 + c_0^3. \tag{9.9}$$

Položme nyní $n := m$ a předchozí postup opakujme. Pak po konečném počtu kroků dostaneme číslo 153.

Příklady.

$$\begin{aligned}
3 &\mapsto 3^3 = 27 \mapsto 2^3 + 7^3 = 351 \mapsto 3^3 + 5^3 + 1^3 = 153,\\
18 &\mapsto 1^3 + 8^3 = 513 \mapsto 5^3 + 1^3 + 3^3 = 153,\\
153 &\mapsto 1^3 + 5^3 + 3^3 = 153,\\
9876 &\mapsto 9^3 + 8^3 + 7^3 + 6^3 = 1800 \mapsto 1^3 + 8^3 = 513\\
&\qquad\qquad\qquad\qquad\qquad\qquad \mapsto 5^3 + 1^3 + 3^3 = 153.
\end{aligned}$$

Věta 9.8. *Když budeme opakovaně sčítat třetí mocniny jednotlivých cifer libovolného přirozeného čísla dělitelného třemi, pak vždy dostaneme číslo* 153.

D ů k a z. Nejprve ukážeme, že když $3 \mid n$, pak $3 \mid m$. Podle věty 1.1 b) a (9.8) je $n \equiv \sum_{i=0}^{k} c_i \pmod 3$ a podle Malé Fermatovy věty 2.12 máme $c_i^3 \equiv c_i \pmod 3$. Odtud a z (9.9) plyne, že

$$m = \sum_{i=0}^{k} c_i^3 \equiv \sum_{i=0}^{k} c_i \equiv n \pmod 3.$$

Dále dokážeme, že pro $n \geq 10^4$ je $n > m$. Protože $c_k > 0$ a $k \geq 4$, podle (9.8) a (9.9) platí

$$n = \sum_{i=0}^{k} c_i 10^i \geq c_k 10^k \geq 10^k > (k+1)9^3 \geq \sum_{i=0}^{k} c_i^3 = m,$$

tj. pro $n \geq 10^4$ je m vždy menší než n. Tento postup opakujeme tak dlouho, dokud nedostaneme číslo menší než 10^4. Pak ale zbývá jen konečný počet možností a na počítači v celočíselné aritmetice lze ověřit, že všechny vedou na číslo 153. □

Poznámka. Předpoklad dělitelnosti třemi ve větě 9.8 je podstatný. Existují totiž jiná přirozená čísla, která se rovnají součtu třetích mocnin svých cifer: $1 = 1^3$, $370 = 3^3+7^3+0^3$, $371 = 3^3+7^3+1^3$ a $407 = 4^3 + 0^3 + 7^3$. Mezi čísly dělitelnými třemi je ale číslo 153 jediné s touto vlastností.

Trik s čísly 6174 a 495. Indický matematik D. R. Kaprekar objevil, že číslo 6174 má následující zajímavou vlastnost, viz (Kaprekar, 1955). Zvolme libovolné čtyřciferné číslo n_1, jehož cifry nejsou všechny stejné. Uvažujme nyní dvě čtyřciferná čísla složená z těchto cifer, které jsou srovnané podle velikosti od největší k nejmenší a od nejmenší k největší. Nechť n_2 je rozdíl těchto dvou čísel. Pokud má tři cifry, doplníme jej zpředu nulou. Opakujeme-li tento proces, pak po nejvýše sedmi krocích dostaneme vždy číslo 6174, nazývané *Kaprekarova konstanta*.

Příklad. Zvolme $n_1 = 1470$. Pak

$$\begin{aligned} n_2 &= 7410 - 0147 = 7263, \\ n_3 &= 7632 - 2367 = 5265, \\ n_4 &= 6552 - 2556 = 3996, \\ n_5 &= 9963 - 3699 = 6264, \\ n_6 &= 6642 - 2466 = 4176, \\ n_7 &= 7641 - 1467 = 6174. \end{aligned}$$

Pro trojciferná čísla je podobná konstanta rovna 495. Důkaz těchto pozoruhodných vlastností pro trojciferná i čtyřciferná čísla lze provést na počítači v celočíselné aritmetice.

Trik s reálnými čísly. V (Hančl, Rucki, 2007) je uvedeno následující tvrzení.

Věta 9.9. *Jestliže* $x + \dfrac{1}{x}$ *je celé číslo pro nějaké reálné* $x \neq 0$*, pak* $x^n + \dfrac{1}{x^n}$ *je také celé číslo pro každé* $n \in \mathbb{N}$.

D ů k a z. Tvrzení dokážeme matematickou indukcí. Zřejmě platí pro $n = 2$, protože

$$x^2 + x^{-2} = (x + x^{-1})(x + x^{-1}) - 2.$$

Nechť nyní $n \geq 2$ a nechť tvrzení platí pro všechna $k = 1, 2, \ldots, n$. Pak

$$x^{n+1} + \frac{1}{x^{n+1}} = \left(x^n + \frac{1}{x^n}\right)\left(x + \frac{1}{x}\right) - \left(x^{n-1} + \frac{1}{x^{n-1}}\right),$$

kde číslo vpravo je podle indukčního předpokladu celé. □

Trik s komplexními čísly. Eulerovi se připisuje snad nejkrásnější matematická formule

$$\mathrm{e}^{\mathrm{i}\pi} + 1 = 0,$$

která svazuje pět nejpoužívanějších matematických konstant 0, 1, imaginární jednotku i, Eulerovo číslo e a Ludolfovo číslo π. Odtud plyne, že

$$\mathrm{e}^{\mathrm{i}\pi} = -1 = (-1)^3 = \left(\mathrm{e}^{\mathrm{i}\pi}\right)^3 = \mathrm{e}^{3\mathrm{i}\pi}.$$

Protože se levá a pravá strana rovnají, můžeme obě části odlogaritmovat a dostaneme rovnost exponentů $\mathrm{i}\pi = 3\mathrm{i}\pi$. Vydělíme-li obě strany nenulovým číslem iπ, obdržíme jiný zajímavý trik

$$1 = 3. \tag{9.10}$$

Další triky s čísly. V následujících větách uvádíme některé zajímavé vlastnosti přirozených čísel, které lze využít k dalším kouzlům s čísly.

Věta 9.10. *Zvolme dvě cifry* $a, b \in \{1, 2, \ldots, 9\}$ *tak, aby* $a + b = 10$*. Pak pro libovolné* $n \in \mathbb{N}$ *čísla* a^{2n} *a* b^{2n} *končí na tutéž cifru.*

D ů k a z. Protože $b \equiv -a \pmod{10}$, podle (1.4) platí

$$b^{2n} \equiv (-a)^{2n} \equiv a^{2n} \pmod{10}. \qquad \square$$

Věta 9.11. *Zvolme dvě cifry* $a, b \in \{1, 2, \ldots, 9\}$ *tak, aby* $a + b = 10$. *Pak pro libovolné* $n \in \mathbb{N}$ *číslo* $a^{2n+1} + b^{2n+1}$ *končí na nulu.*

D ů k a z. Protože $b \equiv -a \pmod{10}$, podle (1.4) platí

$$b^{2n+1} \equiv (-a)^{2n+1} = -a^{2n+1} \pmod{10},$$

a tedy $a^{2n+1} + b^{2n+1} \equiv 0 \pmod{10}$. $\square$

Věta 9.12. *Zvolme dvojciferné číslo končící na* 5. *Jeho čtverec dostaneme tak, že vynásobíme jeho první cifru a číslem* $a + 1$ *a na konec připíšeme* 25.

D ů k a z. Zřejmě

$$(10a + 5)^2 = 100a^2 + 100a + 25 = 100a(a + 1) + 25. \qquad \square$$

Například $65^2 = 6 \cdot 7 \cdot 100 + 25 = 4225$.

Příklad. Vyzkoušejte si, že prvních šest násobků čísla 142 857 má vždy stejné cifry, které se cyklicky vyskytují ve stejném pořadí a začínají pokaždé jinou cifrou.

Poznámka. Pokud vám v hlavě stále vrtá paradoxní rovnost (9.10), pak vám napovíme, že logaritmus v komplexní rovině není jednoznačná funkce, a tedy odlogaritmování v komplexním oboru nelze (na rozdíl od reálného oboru) obecně provádět.

9.8. Latinské čtverce

Pojem latinský čtverec zavedl Leonhard Euler roku 1782 takto: *Latinský čtverec řádu n je schéma o n řádcích a n sloupcích, kde v každém řádku a v každém sloupci se každý prvek nějakého souboru o n prvcích objevuje právě jednou.* Prvky latinského čtverce mohou být různé objekty, např. hrací karty, šachové figurky, osoby

či přirozená čísla. Proslulou úlohou, která stála u zrodu pojmu latinského čtverce, byla úloha o 36 důstojnících, kterou zformuloval Euler r. 1779:

Seřaďte 36 *důstojníků šesti různých hodností ze šesti různých pluků do čtvercového útvaru složeného ze* 6 *řad po* 6 *důstojnících tak, aby v každé řadě a v každém zástupu byly zastoupeny všechny hodnosti a všechny pluky.*

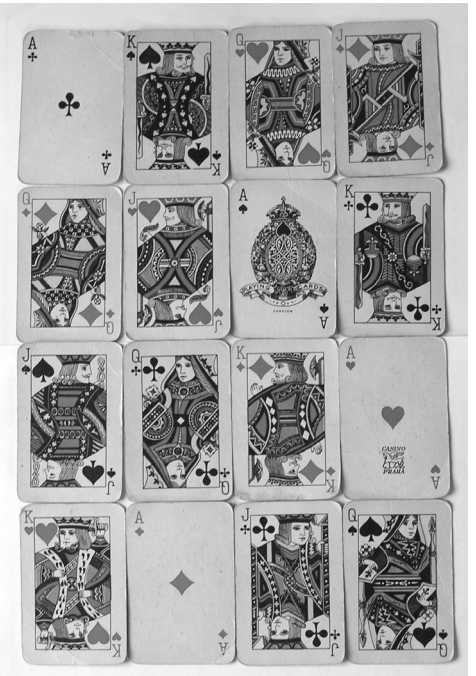
Euler se domníval, že úloha nemá řešení, avšak neuměl své tvrzení dokázat. Trvalo pak dlouhých 118 let, než roku 1900 G. Tarry systematickým výpočtem dokázal, že tato úloha skutečně nemá řešení, viz (Katrnoška, 2007). Je třeba poznamenat, že mnoho prací věnovaných latinským čtvercům se týkalo úloh souvisejících s kartami. Například to byla úloha o seřazení 16 bridžových karet předložená Jacquesem Ozanamem už koncem 17. století (obr. 9.7).

Nechť jsou dány dva latinské čtverce L_1 a L_2, kde $L_1 = (a_{ij})$, $L_2 = (b_{ij})$, $i, j = 1, 2, \ldots, n$. Pak L_1 a L_2 nazýváme *ortogonální*, jestliže jsou všechny dvojice (a_{ij}, b_{ij}), $i, j = 1, 2, \ldots, n$, navzájem různé.

Zavedení pojmu ortogonality má svůj původ v Eulerově úloze o 36 důstojnících. Její řešení spočívalo v nalezení dvou vzájemně ortogonálních latinských čtverců šestého řádu. Jestliže jsou totiž latinské čtverce $L_1 = (a_{ij})$ a $L_2 = (b_{ij})$ ortogonální, pak v množině dvojic $E = (a_{ij}, b_{ij})$ se každá tato dvojice vyskytne právě jednou. Takový čtverec se pak nazývá *Eulerův čtverec.* Snadno se zjistí, že neexistují ortogonální latinské čtverce řádu 2. Neexistence ortogonálních čtverců řádu 6 je vlastně zdůvodněním neřešitelnosti úlohy o 36 důstojnících.

L. Euler vyslovil domněnku, že když $n \equiv 2 \pmod 4$, pak neexistují vzájemně ortogonální čtverce řádu n. Mýlil se ale. Roku 1960 byl totiž v práci (Bose, Parker, Shrikhande, 1960) publikován důkaz, že ortogonální latinské čtverce existují pro všechna přirozená čísla n kromě případů $n = 2$ a $n = 6$. K danému latinskému čtverci však obecně nemusí existovat latinský čtverec k němu ortogonální, což dokázal H. B. Mann, viz (Mann, 1944). Zobecnění této

věty je v článku (Parker, Somer, 1988). V teorii ortogonality latinských čtverců jsou dva základní problémy, problém existence ortogonálního latinského čtverce k danému latinskému čtverci a s tím související jeho konstrukce.



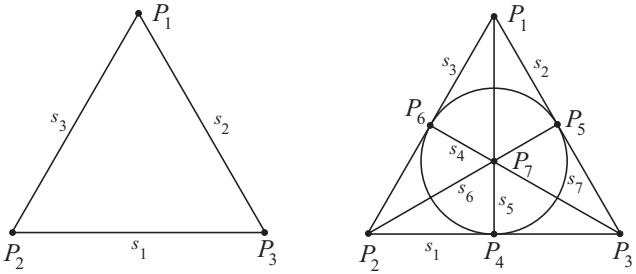
Obr. 9.7. Příklad dvou ortogonálních latinských čtverců. V každém řádku a v každém sloupci (i na obou diagonálách) se nachází právě jedna z hodností: A, K, Q, J a zároveň právě jedna z barev: srdce, kára, piky, kříže (trefy).

Když se A. Cayley zabýval multiplikačními tabulkami konečných grup, zjistil, že tyto tabulky jsou latinskými čtverci. Na druhé straně latinský čtverec nemusí být multiplikační tabulkou grupy. Později se ukázalo, že latinské čtverce lze používat jako prostředek ke stanovení existence konečných projektivních rovin různých řádů. Proto se nyní o těchto rovinách, které připomínají klasické nekonečné projektivní roviny, stručně zmíníme.

Konečná projektivní rovina řádu $n \in \{1, 2, 3, \dots\}$ je množina, která se skládá z $n^2 + n + 1$ bodů a z $n^2 + n + 1$ přímek splňujících následující axiomy:

A1. Každý bod leží na $n + 1$ přímkách.
A2. Každá přímka obsahuje $n + 1$ bodů.
A3. Libovolné dva různé body leží na právě jedné přímce.
A4. Každé dvě různé přímky se protínají vždy jen v jednom bodě.

Existují i jiné ekvivalentní definice konečné projektivní roviny.



Obr. 9.8. Konečné projektivní roviny pro $n = 1$ (trojúhelník) a pro $n = 2$ (Fanova rovina).

Předložený systém axiomů konečné projektivní roviny se ukazuje jako nejvhodnější, neboť výstižně charakterizuje dualitu mezi přímkami a body. Zaměníme-li totiž v systému axiomů A1 až A4 mezi sebou slova „bod“ a „přímka“ a zaměníme-li zároveň slova „leží“ a „protíná“, pak se systém axiomů nezmění.

Důsledkem toho je, že když zaměníme v pravdivém tvrzení týkajícím se projektivní roviny řádu n všude navzájem uvedené termíny, pak dostaneme opět pravdivý výrok. Snadno se zjistí, že nejmenší konečnou projektivní rovinou je trojúhelník (obr. 9.8). Méně triviálním příkladem projektivní roviny řádu $n = 2$ je tzv. *Fanova rovina*, která má podle definice 7 bodů a 7 přímek. Zajímavost této roviny spočívá v tom, že nelze všechny její „přímky“ umístit na běžné úsečky. Proto se jedna z jejích „přímek“ zobrazuje na kružnici (obr. 9.8).

Ukázalo se, že existence konečné projektivní roviny řádu n úzce souvisí s existencí $n-1$ vzájemně ortogonálních čtverců řádu n. Poznamenejme ještě, že existuje-li $n-1$ vzájemně ortogonálních latinských čtverců řádu n, pak tento systém čtverců se nazývá *úplný*. Uveďme nyní následující větu, jejíž důkaz lze nalézt v práci (Rybnikov, 1985).

Věta 9.13. *Nechť $n \geq 2$. Projektivní rovina řádu n existuje právě tehdy, když existuje úplná množina $n-1$ vzájemně ortogonálních latinských čtverců řádu n.*

V roce 1938 R. C. Bose v článku (Bose, 1938) ukázal, proč neexistují projektivní roviny řádu 6. Vzhledem k tomu, že neexistují vzájemně ortogonální latinské čtverce řádu 6, plyne z věty 9.13 rovněž neexistence konečné projektivní roviny řádu 6. Pro existenci projektivní roviny řádu n platí následující věta, viz (Rybnikov, 1985).

Věta 9.14. *Je-li n mocninou prvočísla, pak existuje konečná projektivní rovina řádu n.*

Je známo, že pro $n = 2,\ 3,\ 4,\ 5,\ 7$ a 8 je konečná projektivní rovina určena jednoznačně. Pro $n = 9$ ale existují 4 vzájemně neizomorfní konečné projektivní roviny. Roku 1949 byla dokázána následující věta, viz (Bruck, Ryser, 1949).

Věta 9.15 (Bruckova–Ryserova). *Nechť $n \equiv 1, 2 \pmod 4$. Jestliže existuje konečná projektivní rovina řádu n, pak existují celá čísla x a y tak, že $n = x^2 + y^2$.*

Podmínka, že existují x a y, pro něž $n = x^2 + y^2$, ale není postačující. Zvolíme-li totiž $n = 10$, pak $10 \equiv 2 \pmod 4$, $10 = 1^2 + 3^2$ a neexistence konečné projektivní roviny řádu 10 byla dokázána neobyčejně rozsáhlými výpočty na počítačích. Bruckova–Ryserova věta také nic netvrdí o případu $n = 12$, který zatím není rozřešen. Na druhé straně okamžitě implikuje neexistenci konečné projektivní roviny například pro $n = 14$, neboť $14 \equiv 2 \pmod 4$

a číslo 14 nelze vyjádřit jako součet dvou čtverců. Všimněte si, že Fermatova vánoční věta 3.12 je speciálním případem Bruckovy–Ryserovy věty, protože prvočísla tvaru $n \equiv 1 \pmod 4$ (pro něž podle věty 9.14 projektivní rovina řádu p existuje) lze jednoznačně rozložit na součet dvou čtverců. Pro další zobecnění věty 9.15 odkazujeme na práci (Somer, 1993).

S aplikacemi latinských čtverců se lze setkat při kódování tajných dokumentů, při plánování experimentů v operačním výzkumu nebo při pěstování několika odrůd zemědělských plodin na menších čtvercových políčkách s různou bonitou půdy, viz (Bosák, 1976). Matici 8×8 sestavenou ze všech možných tripletů nukleotidů DNA (adeninu, cytosinu, guaninu a uracylu) lze také interpretovat jako latinský čtverec, viz (Katrnoška, 2007). Latinské čtverce se používají i při organizaci golfových, bridžových či tenisových turnajů. Jako kuriózní příklad latinského čtverce 9×9 je též každé výsledné postavení populární hry sudoku, viz (Herzberg, Murty, 2007), (Katrnoška, Křížek, Somer, 2008).

9.9. Magické čtverce

Magickým čtvercem řádu n rozumíme čtvercovou matici řádu n, která obsahuje vzájemně různá přirozená čísla, a přitom je součet čísel v libovolném řádku, v libovolném sloupci i na obou úhlopříčkách týž.

Magické čtverce hledali již staří Číňané. Na obrázku 9.9 je ukázka magického čtverce 3×3, který byl vyryt do želvího krunýře. Albrecht Dürer na svém slavném obrazu *Melencolia I* z roku 1514 zase znázornil magický čtverec 4×4, který uprostřed dolního řádku udává rok vzniku obrazu,

$$\begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix}. \tag{9.11}$$

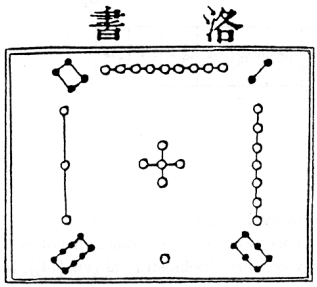
Věta 9.16. *Obsahuje-li magický čtverec $n \times n$ po sobě jdoucí při-*

rozená čísla $1, 2, \ldots, n^2$*, pak součet čísel v každém řádku, sloupci i na obou diagonálách je* $(n^3 + n)/2$.

D ů k a z. Označme s řádkový součet daného magického čtverce $n \times n$. Protože tento čtverec má n řádek, platí

$$s = \frac{1}{n}\sum_{k=1}^{n^2} k = \frac{1}{n}\frac{n^2(n^2+1)}{2} = \frac{1}{2}n(n^2+1). \qquad \square$$

Například pro magický čtverec znázorněný na obr. 9.9 (popř. v (9.11)) platí $s = 15$ (popř. $s = 34$).



$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}$$

Obr. 9.9. Magický čtverec nebeské želvy.

Při hledání obecných magických čtverců pro $n \geq 3$ máme jistou libovůli, protože je třeba najít n^2 přirozených čísel splňujících soustavu $2n + 2$ lineárních diofantských rovnic. Proto si lidé odedávna pro zábavu vymýšlejí nejrůznější magické čtverce s dalšími zajímavými vlastnostmi. Například

$$\begin{bmatrix} 96 & 64 & 37 & 45 \\ 39 & 43 & 98 & 62 \\ 84 & 76 & 25 & 57 \\ 23 & 59 & 82 & 78 \end{bmatrix} \quad \text{a} \quad \begin{bmatrix} 69 & 46 & 73 & 54 \\ 93 & 34 & 89 & 26 \\ 48 & 67 & 52 & 75 \\ 32 & 95 & 28 & 87 \end{bmatrix}$$

je dvojice magických čtverců, z nichž první má cifry jednotlivých čísel v opačném pořadí než čtverec druhý.

Jiný bizarní magický čtverec objevil argentinský matematik Rodolfo Marcelo Kurchan. Cifry jeho prvků jsou vzájemně různé a stejnou vlastnost má i řádkový (sloupcový) součet 4 129 607 358,

$$\begin{bmatrix} 1037956284 & 1036947285 & 1027856394 & 1026847395 \\ 1026857394 & 1027846395 & 1036957284 & 1037946285 \\ 1036847295 & 1037856294 & 1026947385 & 1027956384 \\ 1027946385 & 1026957384 & 1037846295 & 1036857294 \end{bmatrix}.$$

Allan W. Johnson objevil tzv. *apokalyptický magický čtverec* 6×6,

$$\begin{bmatrix} 3 & 107 & 5 & \mathbf{131} & 109 & 311 \\ 7 & 331 & 193 & 11 & \mathbf{83} & 41 \\ 103 & 53 & 71 & 89 & 151 & \mathbf{199} \\ \mathbf{113} & 61 & 97 & 197 & 167 & 31 \\ 367 & \mathbf{13} & 173 & 59 & 17 & 37 \\ 73 & 101 & \mathbf{127} & 179 & 139 & 47 \end{bmatrix},$$

který má vskutku pozoruhodné vlastnosti, viz (Pickover, 2001). Povšimněte si, že jeho prvky jsou vzájemně různá prvočísla. Součet čísel v každém řádku, sloupci a na obou diagonálách je roven *apokalyptickému číslu* 666, o němž je zmínka ve Zjevení Janově v Novém zákonu v kap. 13 o šelmě. Součet 666 je ale i na tzv. přerušených diagonálách v obou směrech. Jedna z nich je pro zvýraznění vytištěna tučně a pro ni máme $113 + 13 + 127 + 131 + 83 + 199 = 666$. Jiná taková přerušená diagonála dává $3 + 101 + 173 + 197 + 151 + 41 = 666$ atd.

Samotné apokalyptické číslo 666 má řadu zvláštních reprezentací. Například je součtem čtverců po sobě jdoucích prvočísel

$$666 = 2^2 + 3^2 + 5^2 + 7^2 + 11^2 + 13^2 + 17^2,$$

je největším trojúhelníkovým číslem, které má stejné cifry, tj.

$$666 = 1 + 2 + 3 + \cdots + 36 = T_{36}.$$

Jeho cifry jsou dokonalá čísla. Je také tzv. *Smithovým číslem*. To znamená, že součet cifer čísla 666 je roven součtu cifer všech jeho prvočinitelů (včetně násobnosti), čili $666 = 2 \cdot 3 \cdot 3 \cdot 37$, a přitom platí

$$6 + 6 + 6 = 2 + 3 + 3 + 3 + 7.$$

Číslo 666 je také součtem dvou palindromických prvočísel $666 = 313 + 353$,

$$666 = 1^6 - 2^6 + 3^6, \quad 666 = 6 + 6 + 6 + 6^3 + 6^3 + 6^3 \text{ aj.}$$

Pokud jej zapíšeme římskými číslicemi DCLXVI, vidíme, že všechna písmena jsou různá a v klesajícím pořadí.

Další zajímavostí je, že hodnota Eulerovy funkce je

$$\varphi(666) = 6 \cdot 6 \cdot 6.$$

Věta 9.17. *Pro libovolné $n \geq 3$ existuje magický čtverec řádu n obsahující pouze prvočísla.*

D ů k a z. Podle Greenovy–Taovy věty 3.11 můžeme najít n^2 prvočísel $p_1, p_2, \ldots, p_{n^2}$, která tvoří aritmetickou posloupnost s počátečním členem $a = p_1$ a diferencí $d = p_2 - p_1$. Podle práce (Pickover, 2001) existuje magický čtverec řádu n obsahující po sobě jdoucí přirozená čísla $1, 2, \ldots, n^2$. Vynásobíme-li jej nejprve číslem d a přičteme k němu konstantní čtverec, jehož prvky jsou $a-d$, dostaneme opět magický čtverec. Jinými slovy, čísla $1, 2, \ldots, n^2$ nahradíme ve stejném pořadí prvočísly $p_1, p_2, \ldots, p_{n^2}$, čímž dostaneme hledaný magický čtverec. □

Na závěr ještě uveďme výsledné postavení hry sudoku (viz podrobněji (Katrnoška, Křížek, Somer, 2008)), v jehož středu je magický čtverec nebeské želvy, okolní bloky 3×3 mají řádkové i sloupcové součty 15 a na každé hlavní diagonále jsou vzájemně různá čísla.

$$\left[\begin{array}{ccc|ccc|ccc}
1 & 6 & 8 & 9 & 2 & 4 & 5 & 7 & 3 \\
9 & 2 & 4 & 5 & 7 & 3 & 1 & 6 & 8 \\
5 & 7 & 3 & 1 & 6 & 8 & 9 & 2 & 4 \\
\hline
8 & 1 & 6 & 4 & 9 & 2 & 3 & 5 & 7 \\
4 & 9 & 2 & 3 & 5 & 7 & 8 & 1 & 6 \\
3 & 5 & 7 & 8 & 1 & 6 & 4 & 9 & 2 \\
\hline
6 & 8 & 1 & 2 & 4 & 9 & 7 & 3 & 5 \\
2 & 4 & 9 & 7 & 3 & 5 & 6 & 8 & 1 \\
7 & 3 & 5 & 6 & 8 & 1 & 2 & 4 & 9
\end{array}\right]$$

Magické čtverce se zobecňují nejrůznějšími způsoby na magické hvězdy, kruhy, šestiúhelníky apod. V literatuře se také můžeme setkat s magickými krychlemi a vícerozměrnými hyperkrychlemi, viz např. (Pickover, 2001, s. 238).

Tabulka 1. Prvních tisíc prvočísel

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987

1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831

4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693
5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857
5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053
6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221
6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367
6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571
6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761
6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917
6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103
7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297
7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499
7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643
7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829
7841	7853	7867	7873	7877	7879	7883	7901	7907	7919

Tabulka 2. Fermatova čísla

$$F_0 = 3,$$

$$F_1 = 5,$$

$$F_2 = 17,$$

$$F_3 = 257,$$

$$F_4 = 65537,$$

$$F_5 = 4294967297,$$

$$F_6 = 18446744073709551617,$$

$$F_7 = 340282366920938463463374607431768211457,$$

$$F_8 = 115792089237316195423570985008687907853\\269984665640564039457584007913129639937,$$

$$F_9 = 134078079299425970995740249982058461274\\793658205923933777235614437217640300735\\469768018742981669034276900318581864860\\508537538828119465699464336490060840 97,$$

$$F_{10} = 179769313486231590772930519078902473361\\797697894230657273430081157732675805500\\963132708477322407536021120113879871393\\357658789768814416622492847430639474124\\377767893424865485276302219601246094119\\453082952085005768838150682342462881473\\913110540827237163350510684586298239947\\245938479716304835356329624224137217.$$

Tabulka 3. Úplný rozklad složených Fermatových čísel F_m pro $5 \leq m \leq 11$

m	prvočinitel	rok	objevitel
5	641	1732	Euler
5	6700417	1732	Euler
6	274177	1855	Clausen
6	67280421310721*	1855	Clausen
7	59649589127497217	1970	Morrison, Brillhart
7	5704689200685129054721	1970	Morrison, Brillhart
8	1238926361552897	1980	Brent, Pollard
8	p_{62}^{**}	1980	Brent, Pollard
9	2424833	1903	Western
9	p_{49}	1990	Lenstra, Lenstra, Jr., Manasse, Pollard
9	p_{99}^{***}	1990	Lenstra, Lenstra, Jr., Manasse, Pollard
10	45592577	1953	Selfridge
10	6487031809	1962	Brillhart
10	p_{40}	1995	Brent
10	p_{252}	1995	Brent
11	319489	1899	Cunningham
11	974849	1899	Cunningham
11	167988556341760475137	1988	Brent
11	3560841906445833920513	1988	Brent
11	p_{564}^{****}	1988	Brent

Prvočíselnost dokázal * Landry, Le Lasseur a Gérardin; ** Williams; *** Odlyzko; **** Morain. Čísla p_j označují prvočísla o j cifrách, která uvádíme v tomto přehledu:

$$p_{62} = 93461639715357977769163558199606896584051237541638188580280321,$$

$$p_{49} = 7455602825647884208337395736200454918783366342657,$$

$$p_{99} = 741640062627530801524787141901937474059940781097519023905821316144415759504705008092818711693940737,$$

$$p_{40} = 4659775785220018543264560743076778192897,$$

$$\begin{aligned} p_{252} = {} & 1304398744054881897274847687965099039466085308416118921868952957768324162514718635741402279775731048958987839288429238448311490329137987290886016179460941194490105959067101305319061710183544916096191939124885381160807122996723228062178207531270144245 77, \end{aligned}$$

$$\begin{aligned} p_{564} = {} & 1734624471791475554302589708643097783774218447236640846493470190613635791928791088575910383304088371779838108684515464219407129783061341898642808260145427587085892438736855639731189488693991585455506611147420216132557017260564139394366945793220968665108959685482705388072645828554151936401912464931182546092879815733057795573358504982279280090942872567591518912118622751714319229788100979251036035496917279912663527358783236647193154777091427745377038294584918917590325110939381322486044298573971650711059244462177542540706913047034664643603491382441723306598834177. \end{aligned}$$

Tabulka 4. Složená Fermatova čísla, pro něž v roce 2007 nebyl znám žádný prvočinitel

m	status	rok	objevitel
14	složené číslo	1961	Selfridge, Hurwitz
20	složené číslo	1987	Young, Buell
22	složené číslo	1993	Crandall, Doenias, Norrie, Young
24	složené číslo	1999	Crandall, Mayer, Papadopoulos

Tabulka 5. Prvočinitelé Fermatových čísel F_m, $12 \leq m \leq 30$

m	prvočinitel	rok	objevitel
12	114689	1877	Lucas, Pervouchine
12	26017793	1903	Western
12	63766529	1903	Western
12	190274191361	1974	Hallyburton, Brillhart
12	1256132134125569	1986	Baillie
13	2710954639361	1974	Hallyburton, Brillhart
13	2663848877152141313	1991	Crandall
13	3603109844542291969	1991	Crandall
13	319546020820551643220672513	1995	Brent
15	1214251009	1925	Kraïtchik
15	2327042503868417	1987	Gostin
15	168768817029516972383024127016961	1997	Crandall, Van Halewyn
16	825753601	1953	Selfridge
16	188981757975021318420037633	1996	Crandall, Dilcher
17	31065037602817	1978	Gostin
18	13631489	1903	Western
18	81274690703860512587777	1999	McIntosh, Tardif
19	70525124609	1962	Riesel
19	646730219521	1963	Wrathall
21	4485296422913	1963	Wrathall
23	167772161	1878	Pervouchine
25	25991531462657	1963	Wrathall
25	204393464266227713	1985	Gostin
25	2170072644496392193	1987	McLaughlin
26	76861124116481	1963	Wrathall
27	151413703311361	1963	Wrathall
27	231292694251438081	1985	Gostin
28	1766730974551267606529	1997	Taura
29	2405286912458753	1980	Gostin, McLaughlin
30	640126220763137	1963	Wrathall
30	1095981164658689	1963	Wrathall

Tabulka 6. Prvočinitelé tvaru $p = k2^n + 1$ Fermatových čísel F_m, $5 \leq m \leq 30$

(Prvočísla p_j jsou uvedena za tabulkou 3.)

m	p	k	n
5	641	5	7
5	6700417	52347	7
6	274177	1071	8
6	67280421310721	262814145745	8
7	59649589127497217	116503103764643	9
7	5704689200685129054721	11141971095088142685	9
8	1238926361552897	604944512477	11
8	p_{62}	[59 cifer]	11
9	2424833	37	16
9	p_{49}	[46 cifer]	11
9	p_{99}	[96 cifer]	11
10	45592577	11131	12
10	6487031809	395937	14
10	p_{40}	[37 cifer]	12
10	p_{252}	[248 cifer]	13
11	319489	39	13
11	974849	119	13
11	167988556341760475137	10253207784531279	14
11	3560841906445833920513	434673084282938711	13
11	p_{564}	[560 cifer]	13
12	114689	7	14
12	26017793	397	16
12	63766529	973	16
12	190274191361	11613415	14
12	1256132134125569	76668221077	14
13	2710954639361	41365885	16
13	2663848877152141313	20323554055421	17
13	3603109844542291969	6872386635861	19
13	319546020820551643220672513	609485665932753836099	19
15	1214251009	579	21
15	2327042503868417	17753925353	17
15	168768 . . . 016961	128760388969052865892810155 5	17
16	825753601	1575	19
16	188981757975021318420037633	180227048850079840107	20
17	31065037602817	59251857	19
18	13631489	13	20
18	81274690703860512587777	9688698137266697	23

m	p	k	n
19	70525124609	33629	21
19	646730219521	308385	21
21	4485296422913	534689	23
23	167772161	5	25
25	25991531462657	48413	29
25	204393464266227713	1522849979	27
25	2170072644496392193	16168301139	27
26	76861124116481	143165	29
27	151413703311361	141015	30
27	231292694251438081	430816215	29
28	1766730974551267606529	25709319373	36
29	2405286912458753	1120049	31
30	640126220763137	149041	32
30	1095981164658689	127589	33

Tabulka 7. Hodnoty některých aritmetických funkcí

Značení: $\tau(n)$ je počet dělitelů čísla n, $\sigma(n)$ je součet dělitelů n, $\varphi(n)$ je Eulerova funkce, $\lambda(n)$ je Carmichaelova funkce a $\omega(n)$ je počet různých prvočísel, jež dělí n.

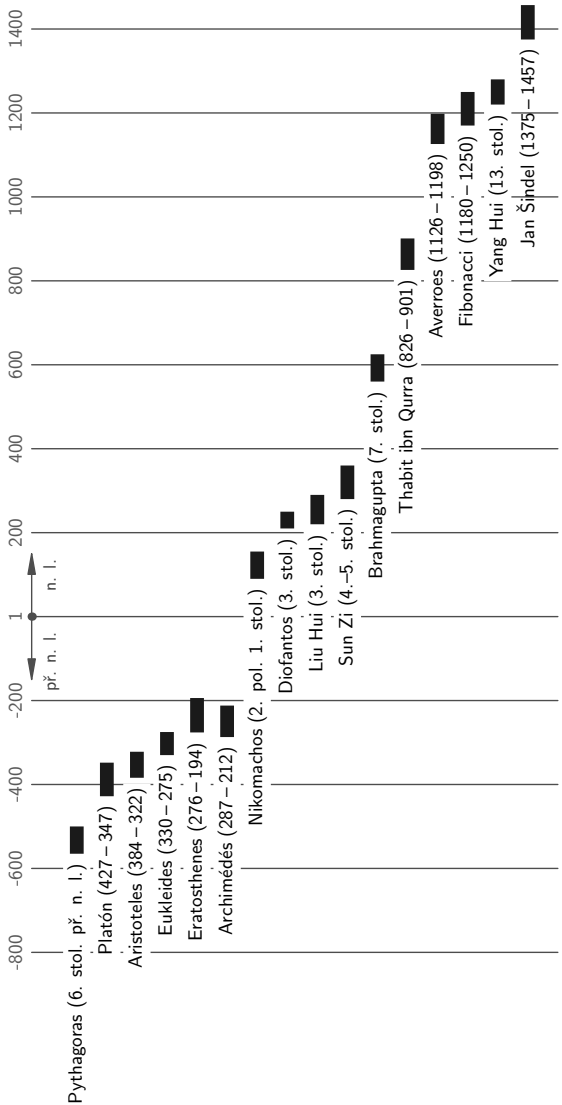
n	$\tau(n)$	$\sigma(n)$	$\varphi(n)$	$\lambda(n)$	$\omega(n)$
1	1	1	1	1	0
2	2	3	1	1	1
3	2	4	2	2	1
4	3	7	2	2	1
5	2	6	4	4	1
6	4	12	2	2	2
7	2	8	6	6	1
8	4	15	4	2	1
9	3	13	6	6	1
10	4	18	4	4	2
11	2	12	10	10	1
12	6	28	4	2	2
13	2	14	12	12	1
14	4	24	6	6	2
15	4	24	8	4	2
16	5	31	8	4	1

n	$\tau(n)$	$\sigma(n)$	$\varphi(n)$	$\lambda(n)$	$\omega(n)$
17	2	18	16	16	1
18	6	39	6	6	2
19	2	20	18	18	1
20	6	42	8	4	2
21	4	32	12	6	2
22	4	36	10	10	2
23	2	24	22	22	1
24	8	60	8	2	2
25	3	31	20	20	1
26	4	42	12	12	2
27	4	40	18	18	1
28	6	56	12	6	2
29	2	30	28	28	1
30	8	72	8	4	3
31	2	32	30	30	1
32	6	63	16	8	1

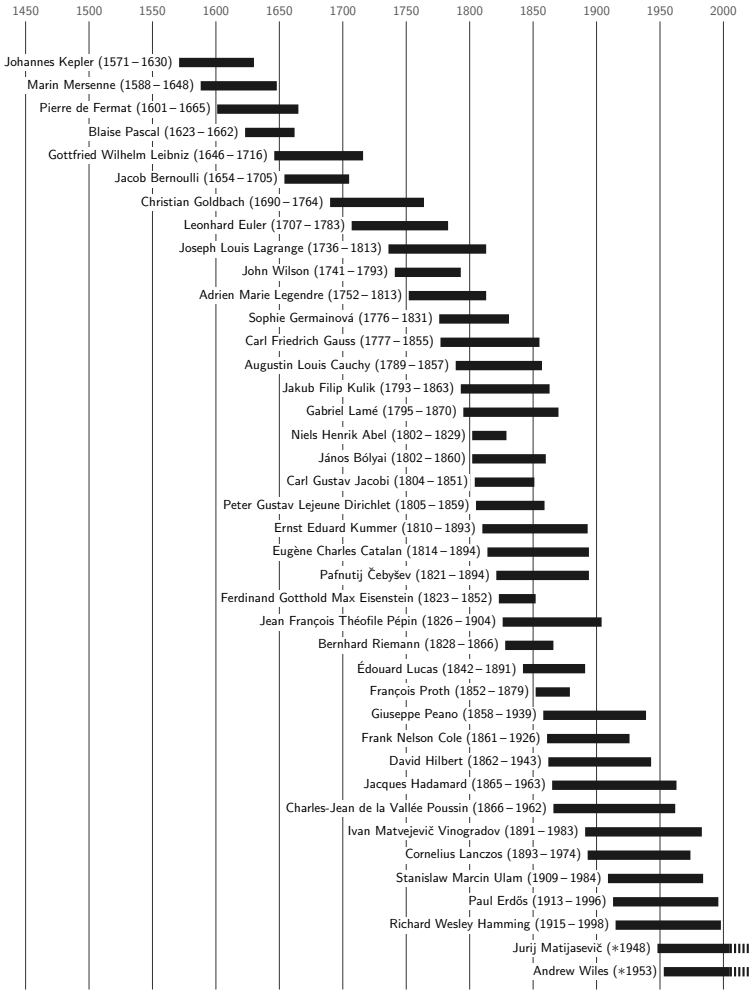
Tabulka 8. Primitivní kořeny mocnin lichých prvočísel menších než 50

3	5	7	9	11	13	17	19	23	25	27	29	31	37	41	43	47	49
2	2	3	2	2	2	3	2	5	2	2	2	3	2	6	3	5	3
	3	5	5	6	6	5	3	7	3	5	3	11	5	7	5	10	5
				7	7	6	10	10	8	11	8	12	13	11	12	11	10
				8	11	7	13	11	12	14	10	13	15	12	18	13	12
						10	14	14	13	20	11	17	17	13	19	15	17
						11	15	15	17	23	14	21	18	15	20	19	24
						12		17	22		15	22	19	17	26	20	26
						14		19	23		18	24	20	19	28	22	33
								20			19		22	22	29	23	38
								21			21		24	24	30	26	40
											26		26	26	33	29	45
											27		32	28	34	30	47
													35	29		31	
														30		33	
														34		35	
														35		38	
																39	
																40	
																41	
																43	
																44	
																45	

Tabulka 9. Chronologická tabulka významných osobností předfermatovské éry teorie čísel (přesná životní data nejsou jistá)



Tabulka 10. Chronologická tabulka významných osobností novodobé teorie čísel



Literatura

Adámek J.: *Kódování.* SNTL, Praha 1982.

Agarwal R. C., Burrus C. S.: *Fast digital convolution using Fermat transforms.* Southwest IEEE Conf. Rec., Houston, Texas 1973, s. 538–543.

Agrawal M., Kayal N., Saxena N.: *Primes is in P.* Ann. of Math. (2) **160** (2004), s. 781–793.

Acheson D.: 1089 *a vše, co s tím souvisí. Moment překvapení v matematice.* Pokroky mat. fyz. astronom. **49** (2004), s. 24–31.

Aigner A.: *On prime numbers for which (almost) all Fermat numbers are quadratic nonresidues* (německy). Monatsh. Math. **101** (1986), s. 85–93.

Alford W. R., Granville A., Pomerance C.: *There are infinitely many Carmichael numbers.* Ann. of Math. **140** (1994), s. 703–722.

Antonyuk P. N., Stanyukovich K. P.: *Periodic solutions of the logistic difference equation* (rusky). Dokl. Akad. Nauk SSSR **313** (1990a), s. 1033–1036, English translation in Soviet Math. Dokl. **42** (1991), s. 116–119.

Antonyuk P. N., Stanyukovich K. P.: *The logistic difference equation. Period doublings and Fermat numbers* (rusky). Dokl. Akad. Nauk SSSR **313** (1990b), s. 1289–1292, English translation in Soviet Math. Dokl. **42** (1991), s. 138–141.

Apfelbeck A.: *Kongruence.* Škola mladých matematiků, sv. 21, Mladá fronta, Praha 1968.

Aristote: *Du ciel.* Text établi et traduit par Paul Moraux, Les Belles Lettres, Paris 1965.

Baillie R., Cormack G., Williams H. C.: *The problem of Sierpiński concerning* $k \cdot 2^n + 1$. Math. Comp. **37** (1981), s. 229–231; Corrigenda ibid. **39** (1982), s. 308.

Baillie R., Wagstaff S. S.: *Lucas pseudoprimes.* Math. Comp. **35** (1980), s. 1391–1417.

Banachiewicz T.: *O związku pomiędzy pewnym twierdzeniem matematyków chińskich a formą Fermata na liczby pierwsze.* Spraw. Tow. Nauk, Warszawa **2** (1909), s. 7–11.

Beauregard R. A., Suryanarayan E. R.: *Square-plus-two primes.* Math. Gazette **85** (2001), s. 90–91.

Beeger N. G. W. H.: *On even numbers m dividing* $2^m - 2$. Amer. Math. Monthly **58** (1951), s. 553–555.

Beran L.: *Fermatova metoda rozkladu v retrospektivě.* Rozhledy mat.-fyz. **72** (1995), s. 113–115.

Beran L.: *Fermatova metoda rozkladu ve vašich rukách.* Rozhledy mat.-fyz. **72** (1995), s. 277–283.

Bezuszka S. J., Kenney M. J.: *Even perfect numbers: (update)*^{2}. The Mathematics Teacher **90** (1997), s. 628–633.

Biermann K.-R.: *Thomas Clausen, Mathematiker und Astronom.* J. Reine Angew. Math. **216** (1964), s. 159–198.

Borho W.: *On Thabit ibn Kurrah's formula for amicable numbers.* Math. Comp. **26** (1972), s. 571–578.

Borho W., Zagier D., Rohlfs J., Kraft H., Jantzen J. C.: *Živá čísla.* Mir, Moskva 1985; Birkhäuser, Basilej 1981.

Borning A.: *Some results for* $k! \pm 1$ *and* $2 \cdot 3 \cdot 5 \cdots p \pm 1$. Math. Comp. **26** (1972), s. 567–570.

Bosák J.: *Latinské štvorce.* Škola mladých matematiků, sv. 38, Praha 1976.

Bosáková D. a kol.: *Elektronický podpis.* Grada, Praha 2002.

Bose R. C.: *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares.* Sankya **3** (1938), s. 323–338.

Bose R. C., Parker E. T., Shrikhande S. S.: *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture.* Canad. Math. J. **12** (1960), s. 189–203.
Brandts J., Korotov S., Křížek M.: *O triangulacích bez tupých úhlů.* Pokroky mat. fyz. astronom. **50** (2005), s. 193–207.
Bressoud D., Wagon S.: *Computational number theory.* Key College Publ., Springer, New York 2000.
Brillhart J., Lehmer D. H., Selfridge J. L., Tuckerman B., Wagstaff S. S.: *Factorization of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers.* Contemporary Math., vol. 22, second edition, Amer. Math. Soc., Providence 1988.
Brown J. L.: *Zeckendorf's theorem and some applications.* Fibonacci Quart. **2** (1964), s. 163–168.
Bruck R. H., Ryser H. J.: *On the non-existence of certain finite projective planes.* Canad. Math. J. **1** (1949), s. 88–93.
Bugeaud Y., Mignotte M.: *Catalanova domněnka dokázána.* Pokroky mat. fyz. astronom. **50** (2005), s. 280–285.
Bugeaud Y., Mignotte M., Siksek S.: *Sur les nombres de Fibonacci de la forme* $q^k y^p$. C. R. Math. Acad. Sci. Paris **339** (2004), s. 327–330.
Buhler J., Crandall R., Ernvall R., Metsänkylä T.: *Irregular primes and cyclotomic invariants to four million.* Math. Comp. **61** (1993), s. 151–153.
Bukovský L., Kluvánek I.: *Dirichletov princíp.* ÚV MO, Mladá fronta, Praha 1970.
Burton D. M.: *Elementary number theory.* fourth edition, McGraw-Hill, New York 1998.
Cahill N. D., D'Errico J. R., Spence J. P.: *Complex factorizations of the Fibonacci and Lucas numbers.* Fibonacci Quart. **41** (2003), s. 13–19.
Calda E.: *Fibonacciova čísla a Pascalův trojúhelník.* Rozhledy mat.-fyz. **71** (1993), s. 15–19.
Caldwell C., Dubner H.: *Primorial, factorial and multifactorial primes.* Math. Spectrum **26** (1993/94), s. 1–7.
Caldwell C., Gallot Y.: *On the primality of* $n! \pm 1$ *and* $2 \times 3 \times 5 \times \cdots \times p \pm 1$. Math. Comp. **71** (2002), s. 441–448.
Carmichael R. D.: *Note on a new number theory function.* Bull. Amer. Math. Soc. **16** (1910), s. 232–238.
Carmichael R. D.: *On composite numbers P which satisfy the Fermat congruence* $a^{P-1} \equiv 1 \pmod{P}$. Amer. Math. Monthly **19** (1912), s. 22–27.
Carmichael R. D.: *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$. Ann. Math. **15** (1913), s. No. 2, 30–70.
Cejnar P.: *Kvantový chaos.* Čs. čas. fyz. **57** (2007), s. 268–277.
Cihlář J., Vopravil V.: *Hry a čísla.* Pedagogická fakulta, Ústí nad Labem 1983, 1995.
Cipolla M.: *Sui numeri composti P, che verificano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$. Annali di Matematica (3) **9** (1904), s. 139–160.
Cooley J. W., Tukey J. W.: *An algorithm for the machine calculation of complex Fourier series.* Math. Comp. **19** (1965), s. 297–301.
Crandall R., Dilcher K., Pomerance C.: *A search for Wieferich and Wilson primes.* Math. Comp. **66** (1997), s. 433–449.
Crandall R., Fagin B.: *Discrete weighted transforms and large-integer arithmetic.* Math. Comp. **62** (1994), s. 305–324.
Crandall R. E., Mayer E., Papadopoulos J.: *The twenty-fourth Fermat number is composite.* Math. Comp. **72** (2003), s. 1555–1572.
Crandall R. E., Pomerance C.: *Prime numbers. A computational perspective.* Springer, New York 2001, 2005.
Cullen J.: *Question* 15897. Math. Quest. Educ. Times **9** (1905), s. 534.
Čermák M.: *Olomoucký orloj.* Memoria, Olomouc 2005.

Delahaye J. P. *Merveilleux nombres premiers. Voyage au cœur de l'arithmétique.* Belin – Pour la Science, Paříž 2000.
Devaney R. L.: *The Mandelbrot set, the Farey tree, and the Fibonacci sequence.* Amer. Math. Monthly **106** (1999), s. 289–302.
Dickson L. E. *History of the theory of numbers, vol. I, Divisibility and primality.* Carnegie Inst., Washington 1919.
Diffie W., Hellman M. E.: *New directions in cryptography.* IEEE Trans. Inform. Theory **22** (1976), s. 644–654..
Dimitrov V. S., Cooklev T. V., Donevsky B. D.: *Generalized Fermat–Mersenne number theoretic transform.* IEEE Trans. Circuits and Systems II, Analog Digit. Signal Process. **41** (1994), s. 133–139.
Dirichlet P. G. L.: *Beweis des Satzes dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.* Abh. d. Königl. Akad. d. Wiss. 1837, s. 45–81; reprinted in Werke, vol. 1, s. 315–350, G. Reimer, Berlín 1889.
Drobot V.: *On primes in the Fibonacci sequence.* Fibonacci Quart. **38** (2000), s. 71–72.
Dujella A.: *A proof of the Hoggatt-Bergum conjecture.* Proc. Amer. Math. Soc. **127** (1999), s. 1999–2005.
Duparc H. J. A.: *On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers.* Rapport ZW 1953-004, Math. Centrum Amsterdam, 1953, s. 1–7.
Elliott D. F., Rao K. R.: *Fast transforms. Algorithms, analyses, applications.* Academic Press, Londýn 1982.
Erdős P.: *On almost primes.* Amer. Math. Monthly **57** (1950), s. 404–407.
Erdős P., Selfridge J. L.: *The product of consecutive integers is never a power.* Illinois J. Math. **19** (1975), s. 292–301.
Euler L.: *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus.* Comment. Acad. Sci. Petropol. **6,** ad annos 1732–33 (1738), s. 103–107.
Euler L.: *De numeris amicabilibus. Leonahardi Euleri Opera Omnia.* Teubner, Leipzig and Berlin, Ser. I., vol. 2 , 1915, s. 63–162.
Fabián J.: *Pětiúhelník.* Lupus, Hradec Králové, Trutnov 2005.
Feigenbaum M. J.: *Quantitative universality for a class of nonlinear transformations.* J. Stat. Phys. **19** (1978), s. 25–52.
Flaut C.: *Some primality and factoring tests.* Creative Math. & Inf. **16** (2007), s. 20–26.
Gauss C. F.: *Disquisitiones arithmeticae.* Springer, Berlín 1986.
Goldberg M.: *Three infinite families of tetrahedral space-fillers.* J. Combin. Theory Ser. A **16** (1974), s. 348–354.
Golomb S. W.: *Combinatorial proof of Fermat's "little" theorem.* Amer. Math. Monthly **63** (1956), s. 718.
Good I. J.: *A reciprocal series of Fibonacci numbers.* Fibonacci Quart. **12** (1974), s. 346.
Gorshkov A. S.: *Method of fast multiplication modulo Fermat primes* (rusky). Dokl. Akad. Nauk SSSR **336** (1994a), s. 175–178, English translation in Soviet Phys. Dokl. **39** (1994a), s. 314–317.
Gorshkov A. S.: *On the method of the number-theoretic Mersenne transform* (rusky). Dokl. Akad. Nauk **336** (1994b), s. 33–34, English translation in Phys. Dokl. **39** (1994b), s. 312–313.
Gostin G. B., McLaughlin P. B.: *Six new factors of Fermat numbers.* Math. Comp. **38** (1982), s. 645–649.
Gottlieb C.: *The simple and straightforward construction of the regular 257-gon.* Math. Intelligencer **21** (1999), s. 31–37.
Green B., Tao T.: *The primes contain arbitrarily long arithmetic progressions.* Ann. of Math. **167** (2008), s. 481–547.
Grošek O., Porubský Š.: *Šifrovanie – algoritmy, metódy, prax.* Grada, Praha 1992.

Grünbaum B., Shephard G. C.: *Tilings and patterns.* W. H. Freeman and Company, New York 1987.
Gutfreund H., Little W. A.: *Physicist's proof of Fermat's theorem of primes.* Amer. J. Phys. **50** (1982), s. 219–220.
Guy R. K.: *The primes* 1093 *and* 3511. Math. Student **35** (1967), s. 205–206.
Guy R. K.: *The strong law of small numbers.* Amer. Math. Monthly **95** (1988), s. 697–712.
Guy R. K.: *The second strong law of small numbers.* Math. Mag. **63** (1990), s. 3–20.
Guy R. K.: *Every number is expressible as the sum of how many polygonal numbers?* Amer. Math. Monthly. **101** (1994a), s. 169–172.
Guy R. K.: *Unsolved problems in number theory.* second edition, Springer, Berlín 1994b.
Halton J. H.: *On Fibonacci residues.* Fibonacci Quart. **2** (1964), s. 217–218.
Hančl J., Rucki P.: *Increase your mathematical intelligence.* PF Ostravské Univerzity, Ostrava 2007.
Hardy G. H.: *Obrana matematikova.* Prostor, Praha 1999.
Hardy G. H., Wright E. M.: *An introduction to the theory of numbers.* Clarendon Press, Oxford, fourth edition 1960; other editions: 1938, 1945, 1954, 1979.
Hayes J. H.: *On the teeth of wheels.* Amer. Scientist **88** (2000), s. 296–300.
Hellegouarch Y.: *Invitation to the mathematics of Fermat–Wiles.* Academic Press, Londýn 2002.
Henrici P.: *Discrete variable methods in ordinary differential equations.* John Wiley & Sons, New York 1962.
Herzberg A. L., Murty M. R.: *Sudoku squares and chromatic polynomials.* Notices Amer. Math. Soc. **54** (2007), s. 708–717.
Hill C.: *Solution to Problem* 10997. Amer. Math. Monthly **111** (2004), s. 917–918.
Hogben L.: *An introduction to mathematical genetics.* Norton, New York 1946.
Hoggatt V. E.: *Fibonacci and Lucas numbers.* Houghton Mifflin Company, Boston 1969.
Horský Z.: *Založení Karlova mostu a kosmologická symbolika Staroměstské mostecké věže.* Staletá Praha IX, Panorama, Praha 1979, s. 197–212.
Horský Z.: *Pražský orloj.* Panorama, Praha 1988.
Horský Z., Procházka E.: *Pražský orloj.* Sborník pro dějiny přírodních věd a techniky **9** (1964), s. 83–146.
Chaumont A., Müller T.: *All elite primes up to* 250 *billions.* J. Integer Seq. **9** (2005), s. Article 06.3.8, 1–5.
Ireland K., Rosen M.: *A classical introduction to modern number theory.* second edition, Springer, New York 1990.
Jarden D.: *Existence of an infinitude of composite n for which* $2^{n-1} \equiv 1 \pmod{n}$. Riveon Lematematika **4** (1950), s. 65–67.
Jarden D.: *Recurring sequences: a collection of papers.* Riveon Lematematika, Jeruzalém 1973.
Jaeschke G.: *On the smallest k such that all* $k \cdot 2^N + 1$ *are composite.* Math. Comp. **40** (1983), s. 381–384; Corrigendum ibid. **45** (1985), s. 637.
Jeans J. H.: *The converse of Fermat's theorem.* Messenger of Mathematics **27** (1897/98), s. 174.
Jenkins P.: *Odd perfect numbers have a prime factor exceeding* 10^7. Math. Comp. **72** (2003), s. 1549–1554.
Jones J. P.: *Diophantine representation of the Fibonacci numbers.* Fibonacci Quart. **13** (1975), s. 84–88.
Jones J. P., Matiyasevich Y. V.: *Proof of recursive unsolvability of Hilbert's tenth problem.* Amer. Math. Monthly **98** (1991), s. 689–709.
Jones R., Pearce J.: *A postmodern view of fractions and the reciprocals of Fermat primes.* Math. Mag. **73** (2000), s. 83–97.

Joo I., Phong B. M.: *On super Lehmer pseudoprimes.* Studia Sci. Math. Hungar. **25** (1990), s. 121–124.
Kaprekar D. R.: *An interesting property of the number* 6174. Scripta Math. **15** (1955), s. 244–245.
Katrnoška F.: *Latinské čtverce a genetický kód.* Pokroky mat. fyz. astronom. **52** (2007), s. 177–187.
Katrnoška F., Křížek M.: *Genetický kód a teorie monoidů aneb* 50 *let od objevu struktury DNA.* Pokroky mat. fyz. astronom. **48** (2003), s. 207–222.
Katrnoška F., Křížek M.: *Významné milníky matematické genetiky.* Matematika – fyzika – informatika **14** (2004/05), s. 1–12.
Katrnoška F., Křížek M., Somer L.: *Magické čtverce a sudoku.* Pokroky mat. fyz. astronom. **53** (2008), s. 113–124.
Keller W.: *Factors of Fermat numbers and large primes of the form* $k \cdot 2^n + 1$*, II.* Preprint Univ. of Hamburg 1992, s. 1–40.
Kiss E.: *Notes on János Bólyai's researches in number theory.* Historia Math. **26** (1999), s. 68–76.
Kiss P.: *Some results on Lucas pseudoprimes.* Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **28** (1985), s. 153–159.
Klazar M.: *Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti.* Pokroky mat. fyz. astronom. **49** (2004), s. 177–188.
Knuth D. E.: *Seminumerical algorithms. The art of computer programming.* Vol. 2, second edition, Addison Wesley, Reading 1981.
Knuth D. E.: *The art of computer programming.* Addison Wesley, Boston 1997.
Koblitz N.: *A course in number theory and cryptography.* Springer, New York 1994.
Korselt A.: *Problème chinois.* L'Interm. des Math. **6** (1899), s. 143.
Kořínek V.: *Základy algebry.* ČSAV, Praha 1953, 1956.
Koshy T.: *Fibonacci and Lucas numbers with applications.* John Wiley & Sons, Inc., New York 2001.
Koubková A., Pavelka J.: *Úvod do teoretické informatiky.* Matfyzpress, Praha 1998.
Koukal S., Křížek M., Potůček R.: *Fourierovy trigonometrické řady a metoda konečných prvků v komplexním oboru.* Academia, Praha 2002.
Kraïtchik M.: *On the factorization of* $2^n \pm 1$. Scripta Math. **18** (1952), s. 39–52.
Křížek M.: *Deset otevřených problémů z teorie čísel.* Rozhledy mat.-fyz. **71** (1994a), s. 4–10.
Křížek M.: *Jak dělit prostor na shodné čtyřstěny?* Rozhledy mat.-fyz. **71** (1994b), s. 27–33.
Křížek M.: *O Fermatových číslech.* Pokroky mat. fyz. astronom. **40** (1995), s. 243–253.
Křížek M.: *Gaussův příspěvek k eukleidovské geometrii.* Rozhledy mat.-fyz. **74** (1997), s. 254–258.
Křížek M.: *Metoda RSA pro šifrování zpráv pomocí velkých prvočísel.* Rozhledy mat.-fyz. **75** (1998), s. 101–107.
Křížek M.: *Má ryze teoretická matematika uplatnění v technické praxi?* Pokroky mat. fyz. astronom. **44** (1999), s. 14–24.
Křížek M.: *Od Fermatových čísel ke geometrii.* Pokroky mat. fyz. astronom. **46** (2001), s. 179–191.
Křížek M.: *Od Fermatových prvočísel ke geometrii.* Cahiers du CEFRES **28** (2002), s. 131–161.
Křížek M.: *Abelova cena za matematiku.* Pokroky mat. fyz. astronom. **49** (2004), s. 11–14.
Křížek M.: *O geometrické interpretaci některých pojmů z teorie čísel.* Pokroky mat. fyz. astronom. **50** (2005), s. 75–79.
Křížek M.: *From Fermat primes to geometry.* Proc. Internat. Conf. Presentation of Mathematics '05 (eds J. Přívratská, J. Příhonská, D. Andrejsová), Tech. Univ. Liberec 2006, s. 45–52.

Křížek M., Chleboun J.: *A note on factorization of the Fermat numbers and their factors of the form* $3h\,2^n + 1$. Math. Bohem. **119** (1994), s. 437–445.
Křížek M., Chleboun J.: *Is any composite Fermat number divisible by the factor* $5h\,2^n + 1$*?* Tatra Mt. Math. Publ. **11** (1997), s. 17–21.
Křížek M., Křížek P.: *Kouzelný dvanáctistěn pětiúhelníkový.* Rozhledy mat.-fyz. **74** (1997), s. 234–238.
Křížek M., Liu L.: *Struktura tradičního čínského kalendáře.* Rozhledy mat.-fyz. **73** (1996), s. 270–275.
Křížek M., Liu L.: *Matematika ve starověké Číně.* Pokroky mat. fyz. astronom. **42** (1997), s. 223–233.
Křížek M., Liu L., Šolcová A.: *Fundamental achievements of ancient Chinese mathematicians.* Math. Spectrum **38** (2005/2006), s. 99–107.
Křížek M., Luca F., Somer L.: 17 *lectures on Fermat numbers: From number theory to geometry.* CMS Books in Mathematics, vol. 9, Springer-Verlag, New York 2001.
Křížek M., Luca F., Somer L.: *On the convergence of series of reciprocals of primes related to the Fermat numbers.* J. Number Theory **97** (2002), s. 95–112.
Křížek M., Luca F., Somer L.: *Algebraické vlastnosti Fibonacciových čísel.* Pokroky mat. fyz. astronom. **50** (2005), s. 127–140.
Křížek M., Luca F., Somer L.: *From Fermat numbers to geometry.* Math. Spectrum **38** (2005/2006), s. 56–63.
Křížek M., Luca F., Somer L.: *Arithmetic properties of Fibonacci numbers.* Proc. Internat. Conf. Presentation of Mathematics '06 (eds J. Přívratská, J. Příhonská, Z. Andres), Tech. Univ. Liberec 2006, s. 7–18.
Křížek M., Luca F., Somer L.: *Desde los números de Fermat hasta la geometría.* La Gaceta de la Realm Sociedad Mathematica Española **10.2** (2007), s. 463–475.
Křížek M., Neittaanmäki P.: *Finite element approximation of variational problems and applications.* Longman, Harlow; John Wiley & Sons, New York 1990.
Křížek M., Somer L.: *A necessary and sufficient condition for the primality of Fermat numbers.* Math. Bohem. **126** (2001), s. 541–549.
Křížek M., Somer L.: *Pseudoprvočísla.* Pokroky mat. fyz. astronom. **48** (2003a), s. 143–151.
Křížek M., Somer L.: 17 *necessary and sufficient conditions for the primality of Fermat numbers.* Acta Math. Inf. Univ. Ostraviensis **11** (2003b), s. 73–79.
Křížek M., Somer L.: *Sophie Germain little suns.* Math. Slovaca **54** (2004), s. 433–442.
Křížek M., Somer L.: *Euclidean primes have the minimum number of primitive roots.* J. Algebra Number Theory Appl. **12** (2008), s. 121–127.
Křížek M., Somer L., Šolcová A.: *Jaká matematika se ukrývá v pražském orloji?* Matematika – fyzika – informatika **16** (2006), s. 129–137.
Křížek M., Šolc J.: *Od Keplerových mozaik k pětičetné symetrii.* Pokroky mat. fyz. astronom. **54** (2009), s. 41–56.
Křížek M., Šolc J., Šolcová A.: *Pražský orloj a stereografická projekce.* Matematika – fyzika – informatika **17** (2007/2008), s. 129–139.
Křížek M., Šolcová A.: *Marin Mersenne a jeho prvočísla.* Matematika – fyzika – informatika **11** (2001/02), s. 204–212.
Křížek M., Šolcová A.: *Prvočíslo 11 v kódování.* Rozhledy mat.-fyz. **78** (2004), s. 208–214.
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, s. 96–113.
Křížek M., Šolcová A., Somer L.: *Construction of Šindel sequences.* Comment. Math. Univ. Carolin. **48** (2007a), s. 373–388.
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, (2007b), s. 53–62.
Landry F.: *Sur la décomposition du nombre* $2^{64} + 1$. C. R. Acad. Sci. Paris **91** (1880), s. 138.
Lehmer D. H.: *An extended theory of Lucas' functions.* Ann. of Math. **31** (1930), s. 419–448.
Lehmer D. H.: *On the converse of Fermat's theorem.* Amer. Math. Monthly **43** (1936), s. 346–354.
Le Lionnais F.: *Les nombres remarquables.* Hermann, Paříž 1983.
Lenstra A. K., Lenstra H. W., Jr., Manasse M. S., Pollard J. M.: *The factorization of the ninth Fermat number.* Math. Comp. **61** (1993), s. 319–349. Addendum ibid. **64** (1995), s. 1357.
Lepka K.: *Historie Fermatových kvocientů.* Dějiny matematiky sv. 14, Prometheus, Praha 2000.
LeVeque W. J.: *Fundamentals of number theory.* Dover, Mineola, New York 1996.
Ligh S., Jones P.: *Generalized Fermat and Mersenne numbers.* Fibonacci Quart. **20** (1982), s. 12–16.
Lind D. A.: *The quadratic field* $\mathbb{Q}[\sqrt{5}]$ *and a certain diophantine equation.* Fibonacci Quart. **6** (1968), s. 86–93.
Livio M.: *The golden ratio.* Headline Book Publ., Londýn 2002.
Ljunggren W.: *On the diophantine equation* $x^2 + 4 = Ay^2$. Det. Kgl. Norske Vid.-Selsk. Forh. **24** (1951), s. 82–84.
London H., Finkelstein R.: *On Fibonacci and Lucas numbers which are perfect powers.* Fibonacci Quart. **7** (1969), s. 476–481, 487; Errata ibid. **8** (1970), s. 248.
Lovász L.: *Combinatorial problems and exercises.* North-Holland, Amsterdam 1979.
Luca F.: *Products of factorials in binary recurrence sequences.* Rocky Mountain J. Math. **29** (1999), s. 1387–1411.
Luca F.: *Fermatova čísla ve speciálních trojúhelnících.* Cahiers du CEFRES **28** (2002), s. 107–122.
Luca F.: *Proposed problem H-*596. Advanced Problem Section, Fibonacci Quart. **41** (2003a), s. 187.
Luca F.: *Palindromes in Lucas sequences.* Monatsh. Math. **138** (2003b), s. 209–223.
Luca F.: *Números primos y aplicaciones.* Soc. Mat. Mexicana, Mexiko 2004.
Luca F., Křížek M.: *On the solutions of the congruence* $n^2 \equiv 1 \pmod{\varphi^2(n)}$. Proc. Amer. Math. Soc. **129** (2001), s. 2191–2196.
Lucas E.: *Théorèmes d'arithmétique.* Atti della Reale Accademia delle Scienze di Torino **13** (1878), s. 271–284.
Luo M.: *On triangular Fibonacci numbers.* Fibonacci Quart. **27** (1989), s. 98–108.
Mahnke D.: *Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung.* Bibliotheca Math. **13** (1913), s. 29–61.
Mahoney M. S.: *The mathematical career of Pierre Fermat (1601–1665).* Princeton Univ. Press, Princeton, New Jersey 1973, 1994.
Mąkowski A.: *Remark on perfect numbers.* Elem. Math. **17** (1962), s. 109.
Mąkowski A.: *On a problem of Rotkiewicz on pseudoprime numbers.* Elem. Math. **29** (1974), s. 13.
Malo E.: *Nombres qui sans être premiers, verifient exceptionnellement une congruence de Fermat.* L'Interm. des Math. **10** (1903), s. 88.
Mann H. B.: *On orthogonal Latin squares.* Bull. Amer. Math. Soc. **50** (1944), s. 249–257.
Mann H. B., Shanks D.: *A necessary and sufficient condition for primality, and its source.* J. Combin. Theory Ser. A **13** (1972), s. 131–134.
Martzloff J.-C.: *The history of Chinese mathematics.* Springer, Berlín 1997.
Matiyasevich Y.: *Enumerable sets are diophantine.* Soviet Math. Dokl. **11** (1970), s. 354–358.

Matiyasevich Y.: *My collaboration with Julia Robinson.* Math. Intell. **14** (1992), s. no. 4, 38–45.
Matiyasevich Y. V., Guy R. K.: *A new formula for* π. Amer. Math. Monthly **93** (1986), s. 631–635.
Mauldin R. D.: *Zobecnění Velké Fermatovy věty: Bealova domněnka a problém o cenu.* Pokroky mat. fyz. astronom. **43** (1998), s. 104–107.
McDaniel W.: *On Fibonacci and Pell numbers of the form* kx^2. Fibonacci Quart. **40** (2002), s. 41–42.
McLaughlin J.: *Small prime powers in the Fibonacci sequence.* ArXiv:math/0110150.
Mersenne M.: *Traité d'harmonie universelle.* Paříž 1627.
Mišoň K.: *Netradiční aplikace dyadické soustavy.* Pokroky mat. fyz. astronom. **XX** (1975), s. 332–339.
Mlýnek J.: *Informační bezpečnost.* Pokroky mat. fyz. astronom. **51** (2006), s. 89–98.
Mlýnek J.: *Zabezpečení obchodních informací.* Computer Press, Brno 2007.
Montgomery P. L.: *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$. Math. Comp. **61** (1993), s. 361–363.
Mordell L. J.: *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod{p}$. Amer. Math. Monthly **68** (1961), s. 145–146.
Moree P., Soli P.: *Around Pelikan's conjecture on very odd sequences.* Manuscripta Math. **117** (2005), s. 219–238.
Müller T.: *Searching for large elite primes.* Experimental Math. **15** (2006), s. 183–186.
Nekovář J.: *Modulární křivky a Fermatova věta.* Math. Bohem. **119** (1994), s. 79–96.
Nielsen P.: *Odd perfect numbers have at least nine distinct prime factors.* Math. Comp. **76** (2007), s. 2109–2126.
Niven I., Zuckerman H. S., Montgomery H. L.: *An introduction to the theory of numbers.* fifth edition, John Wiley & Sons, New York 1991.
Parker E. T., Somer L.: *A partial generalization of Mann's theorem concerning orthogonal Latin squares.* Canad. Math. Bull. **31** (1988), s. 409–413.
Peitgen H. O., Jürgens H., Saupe D.: *Chaos and fractals: New frontiers of science.* Springer, New York 1992.
Penrose R.: *Role of aesthetics in pure and applied mathematical research.* Bull. Inst. Maths. Appl. **10** (1974), s. 266–271.
Pépin P.: *Sur la formule* $2^{2^n} + 1$. C. R. Acad. Sci. **85** (1877), s. 329–331.
Petr K.: *Geometrický důkaz poučky Wilsonovy.* Časopis Pěst. Mat. Fyz. **34** (1905), s. 164–166.
Phong B. M.: *On super Lucas and super Lehmer pseudoprimes.* Studia Sci. Math. Hungar. **23** (1988), s. 435–442.
Pickover C. A.: *Wonders of numbers.* Oxford Univ. Press, Oxford 2001.
Pierpont J.: *On an undemostrated theorem of the Disquisitiones Arithmeticæ.* Bull. Amer. Math. Soc. **2** (1895/96), s. 77–83.
Pisano L.: *Fibonacci's Liber abaci.* A translation into modern English of Leonardo Pisano's *Book of calculation*. Translated by L. E. Sigler, Springer, New York 2002.
Pomerance C.: *On the distribution of pseudoprimes.* Math. Comp. **37** (1981), s. 587–593.
Pomerance C.: *A new lower bound for the pseudoprime counting function.* Illinois J. Math. **26** (1982), s. 4–9.
Pomerance C.: *Vyprávění o dvou sítech.* Pokroky mat. fyz. astronom. **43** (1998), s. 9–29.
Pomerance C., Selfridge J. L., Wagstaff S. S.: *The pseudoprimes to* $25 \cdot 10^9$. Math. Comp. **35** (1980), s. 1003–1026.
Porubský Š.: *Fermat a teorie čísel aneb Problematika dělitelů a dokonalá čísla.* Matematik Pierre de Fermat (eds A. Šolcová, M. Křížek, G. Mink), Cahiers du CEFRES **28** (2002), s. 49–86.

Poulet P.: *Table des nombres composés vérifiant le théorème de Fermat pour le module* 2 *jusqu'à* 100.000.000. Sphinx **8** (1938), s. 42–52; Errata in Math. Comp. **25** (1971), s. 944–945, Math. Comp. **26** (1972), s. 814.
Pradlová J., Křížek M.: *Grupy kolem nás I–III.* Rozhledy mat.-fyz. **76** (1999), s. 209–216, 261–267; **77** (2000), s. 5–12.
Proth F.: *Théorèmes sur les nombres premiers.* C. R. Acad. Sci. Paris **87** (1878), s. 926.
Rademacher H., Toeplitz O.: *The enjoyment of mathematics.* Princeton Univ. Press, New Jersey 1957, 1966, 1970.
Rao T. R. N., Fujiwara E.: *Error-control coding for computer systems.* Prentice-Hall, Inc., Englewood Cliffs, New Jersey 1989.
Reed I. S., Truong T. K., Welch L. R.: *The fast decoding of Reed-Solomon codes using Fermat transforms.* IEEE Trans. Inform. Theory **24** (1978), s. 497–499.
Ribenboim P.: *On the square factors of the numbers of Fermat and Ferentinou–Nicolacopoulou.* Bull. Greek Math. Soc. **20** (1979a), s. 81–92.
Ribenboim P.: 13 *lectures on Fermat's last theorem.* Springer, New York 1979b.
Ribenboim P.: *The little book of big primes.* Springer, Berlín 1991.
Ribenboim P.: *The book of prime number records.* Springer, New York 1988, 1989.
Ribenboim P.: *The new book of prime number records.* Springer, New York 1996.
Ribenboim P.: *Fermat's last theorem for amateurs.* Springer, New York 1999.
Richelot F. J.: *De resolutione algebraica aequationis* $x^{257} = 1$. Crelle's Journal IX (1832), s. 1–26, 146–161, 209–230, 337–356.
Richmond H. W.: *To construct a regular polygon of* 17 *sides.* Math. Ann. **67** (1909), s. 459–461.
Riesel H.: *Prime numbers and computer methods for factorization.* Birkhäuser, Boston–Basilej–Stuttgart 1985, 1994.
Ripley B. D.: *Stochastic simulations.* John Wiley & Sons, New York 1987.
Rivest R. L., Shamir A., Adelman L. M.: *A method for obtaining digital signatures and public key cryptosystems.* Comm. ACM **21** (1978), s. 120–126.
Robbins N.: *Beginning number theory.* Dubuque, IA: Wm. C. Brown Publishers 1993.
Rogers T. D.: *The graph of the square mapping on the prime fields.* Discrete Math. **148** (1996), s. 317–324.
Rosen M.: *Abel's theorem on the lemniscate.* Amer. Math. Monthly **88** (1981), s. 387–395.
Rotkiewicz A.: *Sur les nombres pseudopremiers de la forme* $ax + b$. C. R. Acad. Sci. Paris Sér. I Math. **257** (1963), s. 2601–2604.
Rotkiewicz A.: *Sur les formules donnant des nombres pseudopremiers.* Colloq. Math. **12** (1964), s. 69–72.
Rotkiewicz A.: *Sur les nombres de Mersenne dépourvus de facteurs carres et sur les nombres naturels n tells que* $n^2 \mid 2^n - 2$. Mat. Vesnik **2 (17)** (1965), s. 78–80.
Rotkiewicz A.: *On the pseudoprimes of the form* $ax + b$. Proc. Cambridge Philos. Soc. **63** (1967), s. 389–392.
Rotkiewicz A.: *Pseudoprime numbers and their generalizations.* Stud. Assoc. Fac. Sci. Univ. Novi Sad 1972.
Rybnikov K. A.: *Vveděnije v kombinatornyj analiz.* Izd. Moskovskogo Univ., Moskva 1985.
Rychlík K.: *Úvod do elementární číselné theorie.* JČMF, Praha 1931, 1950.
Sedláček J.: *Co víme o přirozených číslech.* ÚV MO, Mladá fronta, Praha 1977.
Seibert J., Trojovský P.: *On factorization of the Fibonacci and Lucas numbers.* Preprint, 2007.
Schönhage A., Strassen V.: *Fast multiplication of large numbers* (německy). Computing **7** (1971), s. 281–292.
Schroeder M. R.: *Number theory in science and communication.* Springer, Berlín 1984, 1986, 1997, 2006.

Sierpiński W.: *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n–2)/n$. Colloq. Math. **1** (1948), s. 9.
Sierpiński W.: *Teoria liczb.* Warszawa 1950.
Sierpiński W.: *Sur un problème concernant les nombres* $k \cdot 2^n + 1$. Elem. Math. **15** (1960), s. 73–74.
Sierpiński W.: 250 *problems in elementary number theory.* American Elsevier, New York 1970.
Singh S.: *Velká Fermatova věta.* Academia, Praha 2000.
Sinha T. N.: *Note on perfect numbers.* Math. Student **42** (1974), s. 336.
Skula L.: *Malá Fermatova věta.* Matematik Pierre de Fermat (eds A. Šolcová, M. Křížek, G. Mink), Cahiers du CEFRES **28** (2002), s. 163–171.
Sloane N. J. A.: *My favorite integer sequences.* arXiv:math.C0/0207175v1 (2002), s. 1–28.
Sloane N. J. A.: *The on-line encyclopedia of integer sequences.* 2007, A028355, A028356, viz `http://www.research.att.com/~njas/sequences/`.
Somer L.: *On Fermat d-pseudoprimes* In: Théorie des nombres (éds J.-M. De Koninck, C. Levesque), Walter de Gruyter, Berlín, New York 1989, s. 841–860.
Somer L.: *A note on Parker's paper on mutually orthogonal Latin squares.* Proc. of the 24th Internat. Conf. on Combinatorics, Graph Theory, and Computing, Congr. Numer. **98** (1993), s. 188–190.
Somer L.: *On Lucas d-pseudoprimes.* In: Applications of Fibonacci numbers, vol. 7 (eds G. E. Bergum, A. N. Philippou, A. F. Horadam), Kluwer Academic Publishers, Dordrecht 1998, s. 369–375.
Somer L., Křížek M.: *On a connection of number theory with graph theory.* Czechoslovak Math. J. **54** (2004), s. 465–485.
Somer L., Křížek M.: *Structure of digraphs associated with quadratic congruences with composite moduli.* Discrete Math. **306** (2006), s. 2174–2185.
Somer L., Křížek M.: *On semiregular digraphs of the congruence* $x^k \equiv y \pmod{n}$. Comment. Math. Univ. Carolin. **48** (2007), s. 41–58.
Spunar P.: *Repertorium auctorum Bohemorum provectum idearum post Universitatem Pragensem conditam illustrans, Tomus 1.* Studia Copernicana XXV, Wydawnictwo Polskiej Akademii nauk Vratislav, Varšava 1985.
Steuerwald R.: *Über die Kongruenz* $2^{n-1} \equiv 1 \pmod{n}$. S.–B. Math.-Nat. Kl., Bayer. Akad. Wiss., (1947), s. 177.
Strang G.: *Introduction to linear algebra.* Second edition, Wellesley MA, Wellesley-Cambridge 1998.
Strauch O., Poruský Š.: *Distribution of sequences: A sampler.* Peter Lang Publ. Group, Frankfurt am Main 2005.
Szalay L.: *Egy diszkrét iteráció a számelméletben (Diskrétní iterace v teorii čísel).* BDTF Tud. Közl. VIII. Természettudományok 3., Szombathely, (1992), s. 71–91.
Szymiczek K.: *Note on Fermat numbers.* Elem. Math. **21** (1966), s. 59.
Szymiczek K.: *On pseudoprimes which are products of distinct primes.* Amer. Math. Monthly **74** (1967), s. 35–37.
Šalát T.: *O dokonalých číslach.* Pokroky mat. fyz. astronom. **IX** (1964), s. 1–13.
Šalát T.: *Vybrané kapitoly z elementárnej teórie čísel.* SPN, Bratislava 1969.
Šofr B.: *Euklidovské geometrické konštrukcie.* Alfa, Bratislava 1976.
Šolcová A.: *D'Artagnan mezi matematiky — pocta Pierru Fermatovi k* 400. *výročí narození.* Pokroky mat. fyz. astronom. **46** (2001), s. 286–298.
Šolcová A.: *Johannes Kepler, zakladatel nebeské mechaniky.* Prometheus, Praha 2004.
Šolcová A., Křížek M.: *Fermat and Mersenne numbers in Pepin's test.* Demonstratio Math. **39** (2006a), s. 737–742.
Šolcová A., Křížek M.: *Elitné prvočísla.* Obzory mat. fyz. inf. **35** (2006b) č. 4, s. 1–6.

Šolcová A., Křížek M., Mink G. (eds): *Matematik Pierre de Fermat.* Cahiers du CEFRES, no. 28, Praha 2002.
Táborský J.: *Zpráva o orloji pražském.* Josef Teige, Praha 1570, 1901.
Tanton J.: *A dozen questions about Fibonacci numbers.* Math. Horizons, Feb.(2005), s. 5–31.
Tattersall J. J.: *Elementary number theory in nine chapters.* Cambridge Univ. Press, Cambridge 2005.
Taylor R., Wiles A.: *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. **141** (1995), s. 553–572.
te Riele: *Four large amicable pairs.* Math. Comp. **28** (1974), s. 309–312.
Terjanian G.: *Velká Fermatova věta.* Cahiers du CEFRES **28** (2002), s. 87–106.
Thompson T. M.: *From error-correcting codes through sphere packing to simple groups.* Math. Assoc. Amer., Washington 1983.
Urbánková E.: *Zbytky knihovny snad M. Jana Šindela v Universitní knihovně.* Ročenka Universitní knihovny v Praze 1960–1961, SPN, Praha 1962, s. 87–97.
Vajda S.: *Fibonacci & Lucas numbers, and the golden section: Theory and applications.* John Wiley & Sons, New York 1989.
van der Waall R. W.: *Oplossing.* Nieuw archief voor wiskunde **XXIV** (1976), s. 262–263.
van Maanen J.: *Euler and Goldbach on Fermat's numbers:* $F_n = 2^{2^n} + 1$ (holandsky). Euclides (Groningen) **57** (1981/82), s. 347–356.
Vasiga T., Shallit J.: *On the iteration of certain quadratic maps over* GF(p). Discrete Math. **277** (2004), s. 219–240.
Vasilenko O. N.: *On some properties of Fermat numbers* (rusky). Vestnik Moskov. Univ. Ser. I Mat. Mekh., no. **5** (1998), s. 56–58.
Vinogradov I. M.: *Základy theorie čísel.* Nakl. ČSAV, Praha 1953.
Vorobiev N. N.: *Fibonacci numbers.* Birkhäuser, Basilej 2002; Nauka, Moskva 1992.
Wagstaff S. S.: *Divisors of Mersenne numbers.* Math. Comp. **40** (1983), s. 385–397.
Wantzel P. L.: *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas.* J. Math. **2** (1837), s. 366–372.
Warren L. R. J., Bray H. G.: *On the square-freeness of Fermat and Mersenne numbers.* Pacific J. Math. **22** (1967), s. 563–564.
Weil A.: *Number theory, an approach through history.* Birkhäuser, Basilej 1984.
Wells D.: *Prime numbers: The most mysterious figures in math.* John Wiley & Sons, New Jersey 2005.
Wieferich A.: *Beweis des Satzes, dass sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen lässt.* Math. Ann. **66** (1909), s. 95–101.
Wiles A.: *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. **141** (1995), s. 443–551.
Yan J. F., Yan A. K., Yan B. C.: *Prime numbers and the amino acid code: analogy in coding properties.* J. Theor. Biol. **151** (1991), s. 333–341.
Zhu Z., Cao L., Liu X., Zhu W.: *Topological invariance of the Fibonacci sequences of the periodic buds in general Mandelbrot sets.* J. Northeast Univ. Nat. Sci. **22** (2001), s. 497–500.
Znám Š.: *Teória čísel.* ALFA, Bratislava 1987.

Databáze Mathematical Reviews eviduje přibližně 3000 mezinárodních matematických časopisů. Mezi nejdůležitější pro teorii čísel patří: *Journal of Number Theory, The Fibonacci Quarterly, Acta Arithmetica, Journal of Integer Sequences, Mathematics of Computation, International Journal of Number Theory, Indian Journal for Number Theory and Its Applications, Experimental Mathematics, Journal de Théorie des Nombres de Bordeaux, The Ramanujan Journal* a též elektronický časopis *Integers* (*Electronic Journal of Combinatorial Number Theory*).

Odkazy na internetové stránky

[www1] http://www.math.cas.cz
[www2] http://mat.fsv.cvut.cz/sedm
[www3] http://www.arxiv.org/
[www4] http://www.claymath.org/millennium
[www5] http://www.mersenne.org
[www6] http://primes.utm.edu/mersenne/index.html
[www7] http://www.isbn.org
[www8] http://www.issn.org
[www9] http://www.kolej.mff.cuni.cz/∼dan/kody.html
[www10] http://www.kodys.cz
[www11] http://www.prothsearch.net/fermat.html
[www12] http://www.prothsearch.net/sierp.html
[www13] http://aa.usno.navy.mil/data/docs/easter.php
[www14] http://www.mathpages.com/home/inumber.htm
[www15] http://www.mathworld.wolfram.com/topics/NumberTheory.html
[www16] http://www.mathepedia.de
[www17] http://www.mcs.surrey.ac.uk/Personal/R.Knott
[www18] http://www.research.att.com/~njas/sequences

Rejstřík

A

Abel N. H. 124
Acheson D. 320
Aigner A. 138
al-Banna 258
algoritmus bezpečnostní 307
– deterministický 87, 143
– Eukleidův 36, 38, 44, 45, 98, 177, 237, 267
– explicitní 296
– Gaussův 41
– kubický 143
– Lenstrův 85
– numerický 299
– Pollardův 85
– polynomický 143
– pravděpodobnostní 212
– rychlý 210
– Smithův 97
– šifrování 172
Archimédes 316
Aristotelés 319
astroláb 274
Aurifeuille, L. 84
Averroes 319
axiom Archimédův 29
axiomy Peanovy 28

B

Banachiewicz T. 214, 220
Beal A. 65
Beeckmann I. 109
Begger N. 135, 217
Bell E. T. 112
Bernoulli J. 99, 125
bifurkace 199
Binet P. M. 229
bod Fermatův 57
– pevný 130, 145
Bólyai J. 260
Bonse H. 71
Brahmagupta 66
Broscius J. 68
Brun V. 106

C

Carcavi P. 63
Carmichael R. D. 219, 239
Carrol L. 243
Cassini G. D. 230
Catalan E. Ch. 233
Cauchy A. L. 247
Cayley A. 328
Clarkson R. 114
Clausen T. 123
Clement P. 106
Cole F. N. 112
Cosgrave J. B. 264
Crick F. 22

Č

čas babylonský 277
– hvězdný 277
– letní 281
– staročeský 277
– středoevropský 277
část alikvotní 253
Čebyšev P. L. 53, 71
čísla nesoudělná 34, 37, 62, 194, 251, 259
– soudělná 62
– spřátelená 256, 258, 259
číslo abundantní 253, 255, 258
– algebraické 241
– apokalyptické 333
– bankovního účtu 168
– Bernoulliovo 140, 141
– Carmichaelovo 218
– Cullenovo 271
– – druhého druhu 272
– Cunninghamovo 270
– čtvercové 243, 294
– čtyřstěnné 248
– deficientní 253, 255, 258
– *d*-krychlové 248
– dokonalé 115, 249, 250, 256, 288
– Eisensteinovo 160
– Eulerovo 113, 325
– Feigenbaumovo 201
– Fermatovo 57, 119, 195, 199, 209, 220, 259, 261, 263, 264, 265, 338, 340

– Fibonacciho 222, 225, 232, 235, 238, 242, 245
– figurální 243
– Gaussovo 157
– identifikační organizace 168
– iracionální 229, 241
– kombinační 31, 107
– komplexní 269
– krychlové 248
– *k*-úhelníkové 243, 245
– liché 29
– Lucasovo 222, 228, 230, 236
– Ludolfovo 233, 325
– Mersennovo 110, 118, 142, 199, 219, 270
– oktaedrální 248
– osmistěnné 248
– palindromické 155
– perfektně symetrické 129
– pětiúhelníkové 243
– polyedrické 248
– polygonální 243
– polytopické 248
– Pouletovo 215
– přirozené 27, 109
– pseudonáhodné 39, 69, 182
– pyramidální 248
– racionální 157, 241
– Rieselovo 272
– rodné 165
– Sierpińského 265, 266, 268
– složené 50, 266, 340
– Smithovo 333
– sudé 29
– – dokonalé 115, 118, 252
– tetraedrální 248
– Thabitovo 257
– trojciferné 321
– trojúhelníkové 243, 245, 246, 250, 284, 285, 294, 298, 333
– Woodallovo 272
– zlaté 41
– zobecněné Fermatovo 270
– – Lucasovo 268
– – Mersennovo 270
– – pětiúhelníkové 247
čtverce latinské ortogonální 327, 330
čtverec apokalyptický magický 333
– Eulerův 327
– latinský 326, 331
– magický 331, 332, 334
čtveřice diofantská 241
čtyřčata Gaussova prvočíselná 160
– prvočíselná 106
čtyřstěn 248, 317
– pravidelný 314, 319
– vykrývací 318, 319

D

de Bessy F. 63
de la Vallée Poussin 82
de Méziriac 255
de Roberval G. P. 109
dělitel 29
– největší společný 32, 36, 52, 60
– netriviální 29, 81, 83
– společný 38
– triviální 29
– vlastní 29
Descartes R. 109, 316
Diffie W. 178
Diofantos 37, 241, 246
Dirichlet P. L. 64, 93
DNA 20, 211, 224, 307, 331
Dodgson C. L. 243
domněnka abc 65
– Aristotelova 319
– Bealova 65
– Catalanova 66
– Mordellova 64
Doni G. B. 109
Drobot V. 240
Dürer A. 331
dvojčata prvočíselná 106

E

Eisenstein M. 160
ekvivalence Wilsonova 218
eliminace Gaussova 210
Eratosthenes 53, 164
Erdős P. 13, 221
Eukleides 63, 116, 121, 164, 184
Euler L. 70, 77, 84, 99, 103, 106, 116, 119, 121, 142, 174, 246, 258, 326
exponent dešifrovací 173
– šifrovací 177

F

faktoriál 31, 104, 242
Faltings G. 64
Feigenbaum M. J. 199
Fermat P. 57, 59, 62, 64, 83, 109, 111, 112, 114, 119, 121, 140, 220, 242, 246, 258, obr. XIV bar. př.

Fermat S. 63
Finkelstein R. 241
formule Binetova 229
– Lucasova 120
funkce Carmichaelova λ 73, 144, 146, 343
– Eulerova φ 70, 153, 173, 205, 334, 343
– Fermatova 57
– hašovací 180
– gama Γ 104
– jednosměrná 179, 180
– racionální 241
– Riemannova ζ 52, 103
– vytvořující 241

G

Galileo G. 109
Gassendi P. 109
Gauss C. F. 24, 71, 79, 82, 86, 121, 123, 124, 184, 190, 191, 246, 289
Germainová S. 84, 142, 262
GIMPS 113
Girard A. 223
Goldbach Ch. 106, 261
Goldberg M. 319
Good I. J. 241
graf binární 130
– iterační 130, 143

H

Hadamard J. 82
Hajratwala N. 114
Halton J. H. 237
Hamming R. W. 304
Hardy G. H. 50
Hellman M. E. 178
Hilbert D. 318
Hobbes T. 109
Holub V. 30
Horský Z. 273
Hus J. 273
hypotéza Goldbachova 106
– Riemannova 103
Huygens C. 64, 109

Ch

chaos 199, 200, 202
Chaumont A. 139

I

Iamblichos 256
IBAN 170
identity Lebesgueovy 57
– Viètovy 95
index regularity 141
indukce matematická 28, 48, 58, 208, 231, 325
informace redundantní 170
ISBN 167

J

Jacobi C. G. 79, 246
Jan z Růže 273
Jeans J. H. 221
jednotka imaginární 232, 325
Jones J. P. 102, 233
Jones R. 127

K

kalendář 281
– čínský 46
Kaprekar D. R. 324
Katz A. 314
Keller W. 263
Kepler J. 229, 310, 316
klíč 181
– dešifrovací 309
– soukromý 178
– symetrický 308
– šifrovací 309, 310
– veřejný 177
kód ASCII 308
– čárový 169, 308
– dvourozměrný 170
– jedenáctkový 165, 169
– jednorozměrný 170
– radiotelegrafní 308
– Reedův–Solomonův 199
– samodetekující 164
– samopravný 304, 307
kódování 171, 308
koeficient binomický 108, 125, 242
Komenský J. A. 109
kongruence 39, 45, 215
– kvadratická 76, 136
– Wieferichova 134
konstanta Brunova 106
– Eulerova 113
– Feigenbaumova 201

– Kaprekarova 324
konstrukce eukleidovská 122, 186
Korselt A. 218
kořen primitivní 69, 75, 77, 81, 132, 142, 149, 150, 183, 191, 344
– triviální 104
kritérium Eulerovo 77, 98
Kronecker L. 109
krychle 45, 305, 314, 317, obr. II bar. př.
– magická 334
kryptoanalýza 171
kryptografie 39, 69, 171, 182, 221, 307
Křišťan z Prachatic 273
křivka neregulární 91
– regulární 91
– uzavřená 125
Kulik J. F. 102
Kummer E. E. 140
Kurchan R. M. 332
Kurowski S. 114
kvocient Fermatův 68

L

Lagrange A. M. 64, 142, 246
Lamé G. 64, 237
Lanczos C. 12
Landry F. 123
Lebesgue V. A. 64
Legendre A. M. 76
Lehmer D. H. 217
Leibniz G. 19, 58, 89, 216
lemniskáta 125
Leonardo z Pisy 223
Lind D. A. 242
Liu Hui 55
London H. 241
Lucas É. A. 133, 224

M

Mahnke D. 216
Mąkowski A. 217
Malo E. 216
Masser D. 65
Matijasevič J. 233
Maurolici F. 63
McDaniel W. 240
McLaughlin J. 241
Meissner W. 135
Mersenne M. 94, 109, 119
Mendel G. 22
metoda Fermatova nekonečného sestupu 59, 63
– – rozkladu 57, 83
– nekonečného sestupu 140
– pokrývacích množin 266
– rozkladu 82
Mihăilescu P. 66
Mikuláš z Kadaně 273
Minkowski H. 7
mnohoúhelník pravidelný 120, 125, 185, 243, obr. XI bar. př.
mnohostěn konvexní 314
– pravidelný 69, 314
množina celých čísel 28
– elitních prvočísel 139
– fraktální 204
– komplexních čísel 104
– Mandelbrotova 203, 227, obr. III–VI bar. př.
– pokrývací 267
– přirozených čísel 27, 38, 58
– racionálních čísel 28
– reálných čísel 28
– Sierpińského fraktální 126
model geocentrický 274
– heliocentrický 274
modul 40, 70
– prvočíselný 182
mozaika Keplerova 310
– Penrosova 312
Müller T. 138

N

násobek nejmenší společný 27, 32, 37, 52, 233
nereziduum kvadratické 76, 98, 142, 148, 183, 291, 299, 302
nerovnice diofantská 315
nerovnost diofantská 65
Newton I. 58
Nikomachos 118, 249
Nirenberg M. W. 211
nula 19, 27
Nunes P. 35

O

Oesterlé J. 65
Ondřejův J. 273

P

Paganini N. 257
palindrom 154, 240
Pascal B. 107, 109
Pascal É. 109
Peano G. 28
Pearce J. 127
Pell J. 109
Penrose R. 312
Pépin J. F. 124, 137
perioda 203, 284, 296
– Fermatova 138, 140
– minimální 203, 284
pětiúhelník 186, 192, 311
Petr K. 90
Pieroni G. 109
Platón 314
Plútarchos 295
podpis digitální 178
– elektronický 180
pokrytí aperiodické 313
– Katzovo – obr. XIII bar. přílohy
– Keplerovo – obr. XI bar. přílohy
– Penrosovo 313, obr. XII bar. př.
– periodické – v obr. příloze
– polopravidelné 310
– pravidelné 310
polynom cyklotomický 205, 209
– Eulerův 101
– Fibonacciho 233
– kvadratický 99
– Lucasův 233
posloupnost aritmetická 25, 217, 243, 244, 334
– Fibonacciho 226, 241, 321
– geometrická 103, 151
– Lucasova 230
– náhodná 309
– periodická 239, 283, 284, 285, 289, 292, 295
– primitivní šindelovská 296, 298, 299
– pražská hodinová 281, 284, 288
– složená šindelovská 296
– šindelovská 285, 288, 291, 292, 296, 298, 299
– triviální šindelovská 297, 300
princip Dirichletův 47, 239
– Fermatův 58
– matematické indukce 58
problém Hilbertův 233, 318
– Sierpińského 268
Procházka E. 273
projekce stereografická 274, 276
Proth F. 87
prvek biogenní 196
– inverzní 88
prvočinitel 51, 341
– primitivní 239
prvočísla siamská 156
prvočíslo 23, 50, 69, 108, 109, 238, 278, 334, 335
– Cullenovo 271
– cyklické 156
– dvojciferné 166, 170
– elitní 136
– Eisensteinovo 161
– Eukleidovo 150, 152
– faktoriální 154
– Fermatovo 119, 121, 126, 129, 150, 182, 185, 191, 195, 198, 260, 265
– Fibonacciho 238
– Gaussovo 159, 160
– iregulární 141
– jedinečné 157
– liché 63, 77, 88
– Lucasovo 238
– Mersennovo 111, 114, 118, 142, 147, 150, 160, 206, 216, 249, 270
– multifaktoriální 154
– nemersennovské 264
– palindromické 155, 157, 333
– permutační 156
– regulární 140
– Sophie Germainové 142, 145
– Thabitovo 257
– Wieferichovo 134, 135
– Wilsonovo 156
– Woodallovo 272
pseudoprvočíslo 213, 215, 221
– absolutní 218, 221
– Eulerovo 221
– Fermatovo 219, 221
– Frobeniovo 221
– Lehmerovo 221
– Lucasovo 221
– Mersennovo 219
– o základu *a* 213
– silné 221
pythagorejci 222, 256

Q

Qin Jiushao 45

R

reziduum kvadratické 76, 80, 291
Riemann B. 103

Rotkiewicz A. 217
rovina Fanova 329
– komplexní 104, 159, 206
– konečná projektivní 329
rovnice binomická 186
– diofantská 37, 57, 233, 242, 310, 319, 332
– charakteristická 229
– kvadratická 186, 188, 189, 190, 269
– lineární diofantská 38
– logistická 199
– Pellova 66
rozdělení normální Gaussovo 184
– pravděpodobnostní 184
rozklad na prvočinitele 75
– prvočíselný 71
RSA 23, 85, 171, 178, 179, 308, 309
Ruby R. 100

Ř

řád čísla 68
řada geometrická 257
– harmonická 152
řešení neperiodické 205
– periodické 203, 205
– triviální 206
řetězec zlatý 227
řez bronzový 230
– stříbrný 230
– zlatý 192, 229, 235, 312, 314

S

Sarrus P. F. 213
Sato D. 102
sedmnáctiúhelník 186, 192
Selfridge J. 134, 267
Schönhage A. 210
Schwarz Š. 304
slovo kódové 305
soustava číselná 127
– čtyřková 20, 21
– desítková 22, 30, 125, 164
– dvojková 19, 20, 23, 125, 264
– kongruencí 42, 44
– šestnáctková 23
spirála Fermatova 57
– Ulamova 100
srdcovka 227
Strassen V. 210
stroj bicí 245, 274, 281, 284, 299, obr. IX, X bar. př.
– diferenční 280
– hlavní hodinový 277, obr. VIII bar. př.
– hodinový 274, 275, 283
– opravovací 280
– ukazovací 277
sudoku 331, 334
Sun Zi 42
superpseudoprvočíslo 221
symbol Halmosův 17
– Jacobiho 79, 136
– Landauův 139
– Legendrův 76, 78, 299
Szpiro L. 65
Szymiczek K. 217

Š

šesterčata Eisensteinova prvočíselná 161
šifrování 171, 308
Šindel J. 273

T

Táborský J. 273
Taylor R. 65
těleso archimédovské 316
– konečné 209
– platónské 132, 314, obr. II bar. př.
– polopravidelné 316
test Lucasův–Lehmerův 112, 269
– Pépinův 124, 132
Thabit ibn Qurra 256, 257, 273
toroid 125
Torricelli E. 109
transformace diskrétní Fourierova 198
– Fermatova 198
– Fourierova 25, 198
– Laplaceova 198
– Radonova 25
trojice primitivní pythagorejská 54, 59, 99
– pythagorejská 54, 61, 99
trojúhelník Heronův 126
– Pascalův 107, 125, 225
– pythagorejský 54, 59, 94
– rovnostranný 311
třicetistěn Keplerův 229
Turing A. 308

U

Ulam S. M. 100

V

věta binomická 87, 292
– Bólyaiova 260
– Bruckova–Ryserova 330
– Carmichaelova 72, 74, 219, 240
– Cipollova 221
– Clementova 106
– Čínská o zbytcích 44, 46, 75, 145, 265, 293, 298
– čtyřčtvercová 246
– Dirichletova 93, 151, 218, 298
– Druhá Eukleidova 53, 149, 154, 261
– Eukleidova 116, 249, 255
– – o výšce 186
– Eulerova 116, 117
– Eulerova–Fermatova 71, 73, 74, 81, 174, 176
– Fermatova vánoční 48, 57, 95, 98, 99, 158, 210, 262, 331
– Gaussova 122, 184, 278
– Goldbachova 261, 268
– Greenova–Taova 93, 334
– Haltonova 237
– Heatova 118, 252
– Hillova 264
– Keplerova 310
– Korseltova 218
– Lucasova 133, 134, 135, 263
– Lucova 126
– Mąkowského 252
– Malá Fermatova 57, 66, 70, 77, 81, 88, 112, 115, 143, 174, 212, 215, 218, 220, 262, 323, obr. I bar. př.
– Mickova 221
– Müllerova 139
– Penrosova 313
– Platónova 315
– Prothova 124, 263
– První Eukleidova 51, 66, 88, 96, 175
– prvočíselná 82
– Pythagorova 12, 25, 54
– Rotkiewiczova 217
– Sierpińského 265, 266
– Suyamova 263
– Szalayova 131
– Thabitova 256, 258
– Velká Fermatova 57, 63, 65, 135, 140
– Wieferichova 136
– Wilsonova 89, 92
– Wilsonova–Lagrangeova 89
– Základní algebry 187
– – aritmetiky 13, 50, 51, 53, 103, 152, 196
– Zeckendorfova 235
– Zlatá 79
Viète F. 95
Vinogradov I. M. 107
vzdálenost Hammingova 304, 306
vztah Eulerův 175, 316
– Fermatův 176
– Gaussův 24, 82
– rekurentní 120

W

Wada H. 102
Wagstaff S. S. 113
Wall D. D. 239
Wallis J. 63
Wantzel P. L. 121
Waring E. 89
Watson J. 21
West N. 163
Western A. E. 133
Wieferich A. J. A. 136
Wiener N. 163
Wiens 102
Wiles A. 65
Wilson J. 89
Woltman G. 114

Y

Yang Hui 42, 107

Z

zákon kvadratické reciprocity 79, 80, 137, 295, 299
zbytek Fermatův 138
– kvadratický 76, 78, 291, 298, 303
zpráva zašifrovaná 173
– odšifrovaná 173