# Obsah


**1 Úvod** **3**
1.1 Úvod . . . 3
1.2 Sylaby a literatúra . . . 3
1.3 Označenia a pomocné tvrdenia . . . 4

**2 Prvočísla** **6**
2.1 Deliteľnosť . . . 6
2.2 Prvočísla . . . 12
2.2.1 Základné vlastnosti prvočísel . . . 12
2.2.2 Základná veta aritmetiky, kanonický rozklad . . . 13
2.3 Rozloženie prvočísel . . . 14
2.3.1 Medzery v množine prvočísel . . . 14
2.3.2 Rad prevrátených hodnôt prvočísel . . . 14
2.3.3 Prvočíselná funkcia . . . 18
2.3.4 Čebyševove nerovnosti . . . 19
2.3.5 Bertrandov postulát . . . 23
2.4 Prvočísla špeciálneho tvaru . . . 26
2.4.1 Prvočísla v aritmetických postupnostiach . . . 26
2.4.2 Ďalšie typy prvočísel a niektoré známe otvorené problémy . . . 26

**3 Aritmetické funkcie** **29**
3.1 Kongruencie . . . 29
3.1.1 Definícia a základné vlastnosti . . . 29
3.1.2 Lineárne kongruencie . . . 31
3.1.3 Čínska veta o zvyškoch . . . 33
3.2 Aritmetické funkcie, multiplikatívne funkcie . . . 37
3.3 Eulerova funkcia . . . 41
3.3.1 Eulerova funkcia, Malá Fermatova veta . . . 41
3.3.2 Wilsonova a Lagrangeova veta . . . 47
3.4 Möbiova funkcia . . . 51

**4 Kvadratické kongruencie** **55**
4.1 Kvadratické zvyšky . . . 55
4.2 Legendrov symbol . . . 56
4.3 Zákon kvadratickej reciprocity . . . 60
4.4 Jacobiho symbol . . . 68
4.5 Kvadratické kongruencie modulo zložené čísla . . . 71





**5 Hustoty podmnožín prirodzených čísel** **74**
5.1 Asymptotická hustota . . . 74
5.2 Schnireľmannova hustota . . . 83
5.3 Logaritmická hustota . . . 85
5.3.1 Ďalšie zovšeobecnenia . . . 89
5.4 Štatistická konvergencia . . . 90
5.5 $\mathcal{I}$-konvergencia . . . 93

**6 Diofantické rovnice** **94**
6.1 Lineárne diofantické rovnice . . . 94
6.2 Pytagorovské trojuholníky . . . 95
6.3 Diofantická rovnica $x^4 + y^4 = z^4$ . . . 98
6.4 Diofantické rovnice a deliteľnosť . . . 100
6.5 Gaussovské a eisensteinovské celé čísla . . . 101
6.6 Diofantická rovnica $x^3 + y^3 = z^3$ . . . 106

**7 Aditívne vlastnosti prirodzených čísel** **109**
7.1 Bázy množiny $\mathbb{N}$ . . . 109
7.2 Súčty druhých mocnín prirodzených čísel . . . 110
7.2.1 Súčty dvoch štvorcov . . . 111
7.2.2 Súčty štyroch štvorcov . . . 115
7.2.3 Súčet troch štvorcov . . . 117
7.3 Goldbachova hypotéza, aditívne vlastnosti prvočísel . . . 118

**A Euklidov algoritmus** **119**

**B Rady** **121**
B.1 Harmonický rad . . . 121
B.2 Rad prevrátených hodnôt druhých mocnín . . . 122

**C Zložitosť niektorých teoreticko-číselných algoritmov** **124**
C.1 Základné operácie . . . 124
C.2 Euklidov algoritmus . . . 124
C.3 Výpočet Jacobiho symbolu . . . 125

**Register** **131**

**Zoznam symbolov** **133**

# Kapitola 1

# Úvod

Verzia: 26. septembra 2008

*You teach best what you most need to learn.*
Patrick Bach, Illusions

*Die Zahlentheorie ist nützlich, weil man mit ihr promovieren kann.*
Edmund Landau

## 1.1 Úvod

Teória čísel je v súčasnosti matematická disciplína, ktorá obsahuje veľa hlbokých a zaujímavých výsledkov ale aj otvorených problémov a hypotéz. Teória čísel využíva metódy najrôznejších matematických odvetví, v súvislosti s tým hovoríme o algebraickej, analytickej, pravdepodobnostnej, kombinatorickej či geometrickej teórii čísel. (Fakt, že poznatky z algebry často nachádzajú uplatnenie v teórii čísel, si je možné všimnúť aj na niektorých miestach v týchto poznámkach – pre viaceré vety sme podali algebraický aj „čisto“ teoreticko-číselný dôkaz.) Samozrejme teóriu čísel ovplyvňuje aj súčasný rozvoj výpočtovej techniky, ako nové odvetvie vznikla algoritmická teória čísel (computational number theory). V súvislosti s nasadením počítačov vystupujú do popredia napríklad otázky výpočtovej zložitosti teoreticko-číselných algoritmov. Mnohé teoreticko-číselné hypotézy sa dajú vďaka počítačom overiť pre pomerne veľké čísla. Môžeme spomenúť aj známy projekt hľadania veľkých prvočísel pomocou distribuovaných výpočtov. Aplikácie teórie čísel v oblasti computer science môžeme nájsť hlavne v kryptografii.

Samozrejme, nie je možné pokryť v priebehu 2 semestrov takú obrovskú oblasť. V skutočnosti tieto prednášky neobsahujú ani zďaleka všetko, čo by sa dalo zaradiť do „základného kurzu“. O tom, že sa zaoberáme skutočne len najzákladnejšími vecami svedčí napríklad aj to, že viaceré výsledky, ktoré ukážeme, sú pomerne staré (niekoľko storočí až niekoľko tisícročí).

Napriek tomu verím, že v tomto texte nájdete viacero zaujímavých vecí a poskytne Vám dobrý základ k prípadnému ďalšiemu štúdiu teórie čísel.

## 1.2 Sylaby a literatúra

**Sylaby predmetu:** Zima: Deliteľnosť v obore $\mathbb{Z}$, prvočísla. Prvočíselná veta. Základné aritmetické funkcie. Dokonalé čísla. Kongruencie. Eulerova veta. Kvadratické kongruencie a zákony reciprocity.



Leto: Cantorove rozvoje reálnych čísel. Kritériá iracionálnosti. Iracionálnosť čísel e a p. Pojem hustoty vteórii čísel. Základné typy hustôt; Schnireľmannova, asymptotická a logaritmická hustota. Pytagorovské trojuholníky.

Zvyčajne v zime stihnem prebrať veci po kapitolu 4 (vrátane), ostatné kapitoly patria do letného semestra.

**Literatúra:** Na tomto mieste by som rád uviedol jednak odporúčanú literatúru, ktorej prečítaním získate určite viac ako z týchto prednášok alebo z poznámok k ním, a dvak, ako káže človeku slušnosť, aj literatúru, ktorú som použil pri príprave tohoto textu.

V podstate všetko, čo bude obsahom tejto prednášky, môžete nájsť v učebniciach [ŠHHK] a [KLŠZ]. Z kníh v slovenskom jazyku je výborná aj kniha [Zn]. V češtine vyšla kniha [PS].

Ďalšie zdroje použité pri príprave týchto poznámok sú [An], [Ap], [AZ], [B], [BD], [C], [Č], [CP], [DSV], [DD], [DMR], [ES], [HW], [HS], [IR], [JJ], [KPW], [KLS], [Kos], [Lem2], [Lem1], [Lev1], [Lo], [MSC], [ME], [Nat], [NZM], [Po], [Pr], [Ri], [Ro], [Sie3], [Sie1], [Š3], [VR] a v neposlednom rade aj internetové zdroje [WIK] a [PLA].

Súčasne by som rád poďakoval Milošovi Zimanovi, ktorý prednášal tú istú prednášku v predchádzajúcich rokoch – viaceré témy som zaradil do prednášky na jeho podnet. Každopádne však na tomto mieste nemožno nepripomenúť profesora Tibora Šaláta, ktorý tento predmet prednášal dlhé roky a vlastne on dal tejto prednáške súčasnú podobu (témy z tejto prednášky spracoval v príslušných kapitolách kníh [ŠHHK] a [KLŠZ]). Za viaceré pripomienky k obsahu prednášky ďakujem Pavlovi Zlatošovi, Ladislavovi Kvaszovi, Martinovi Mačajovi a Martinovi Niepelovi. Bohužiaľ väčšinu z nich sa mi nepodarilo do tejto prednášky zaradiť – aj to svedčí o tom, že ak Vás teória čísel zaujme, ľahko môžete nájsť veľa ďalších fascinujúcich tém, o ktorých sa tu nezmienime. Takisto sa chcem poďakovať svojim študentom za mnohé zaujímavé poznámky na prednáškach, ako aj za upozornenie na viaceré preklepy aj vecné chyby. Menovite spomeniem aspoň (sorry, ako som na niekoho zabudol) O. Budáča, M. Burgera, J. Holosa a M. Višňovského.

Samozrejme, ako každý iný text, aj tu nájde množstvo chýb, nepresností a preklepov. Za akékoľvek návrhy a opravy budem vďačný. Budem sa snažiť tieto poznámky priebežne opravovať a dopĺňať, aktuálnu verziu nájdete na `http://thales.doa.fmph.uniba.sk/sleziak/vyuka/`.

Zrejme každý, kto si pozeral knihu [KLŠZ] určite získal dojem, že niektoré časti sú týchto poznámok takmer okopírované z príslušných kapitol spomenutej knihy. Preto sa môže zdať otázne, či nebolo zbytočné takéto pracné prepisovanie. Myslím si, že nie a to z dvoch dôvodov. Jednak takto majú študenti celý text pokope a nemusia kombinovať štúdium vo viacerých knihách – niektoré kapitoly študovať odtiaľto, iné z [KLŠZ] a ďalšie možno z celkom inej knihy. Ďalší dôvod je, že v takejto forme sa text ľahšie upravuje – a snáď keď to budem prednášať v ďalších rokoch, vždy nájdem niečo nové a zaujímavé, čo by sa tam dalo doplniť. Každopádne som považoval za moju povinnosť spomenúť, že niektoré kapitoly a prezentácia niektorých tém pochádza z [KLŠZ] – aby som nevyvolal dojem, že si chcem privlastňovať cudziu prácu.

## 1.3 Označenia a pomocné tvrdenia

Pre číselné obory budeme používať nasledujúce označenia:
$\mathbb{Z}$ = množina celých čísel
$\mathbb{N} = \{1, 2, \ldots\}$ = množina prirodzených čísel (Nulu nepovažujeme za prirodzené číslo.)
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.
$\mathbb{R}$=reálne čísla, $\mathbb{C}$=komplexné čísla

Označenie logaritmov: $\ln x$ označuje prirodzený logaritmus, $\log x$ je logaritmus so základom 10 a $\lg x$ je logaritmus so základom 2.

**Landauova notácia**

**Definícia 1.3.1.** Nech $f$ a $g$ sú funkcie s oborom $\mathbb{N}$ alebo $\mathbb{R}$ a s hodnotami v $\mathbb{R}$.

Budeme používať symbol $f(x) \sim g(x)$ na vyjadrenie faktu, že

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Ak je podiel $\frac{f(x)}{g(x)}$ ohraničený, zapíšeme to označením $f(x) = O(g(x))$.

Ak

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

píšeme $f(x) = o(g(x))$.

**Dolná a horná celá časť**

**Definícia 1.3.2.** Ak $x \in \mathbb{R}$, tak *dolná celá časť* $x$ je jediné celé číslo také, že $z \le x < z + 1$. Označujeme ju $\lfloor x \rfloor$.

Podobne *horná celá časť čísla* $x$ je celé číslo také, že $z - 1 < x \le z$. Hornú celú časť označujeme $\lceil x \rceil$.

*Zlomkovou časťou čísla* $x$ nazývame číslo $\{x\} = x - \lfloor x \rfloor$.

Napríklad $\lfloor \pi \rfloor = 3$, $\lceil \pi \rceil = 4$, $\{\pi\} = 0.141592\ldots$

{prelim:LMDCC2}

**Lema 1.3.3.** *Pre ľubovoľné $x \in \mathbb{R}$ platí $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$. Presnejšie,*

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0, & \text{ak } 0 \le \{x\} < \frac{1}{2}; \\ 1, & \text{ak } \frac{1}{2} \le \{x\}. \end{cases}$$

*Dôkaz.* Číslo $x$ môžeme zapísať v tvare $x = \lfloor x \rfloor + \{x\}$, pričom $0 \le \{x\} < 1$. Chceme vyjadriť dolnú celú časť čísla $2x = 2\lfloor x \rfloor + 2\{x\}$

Ak $0 \le \{x\} < \frac{1}{2}$, tak $2\{x\} < 1$ a $\lfloor 2x \rfloor = 2\lfloor x \rfloor$. V tomto prípade teda máme $\lfloor 2x \rfloor - 2\lfloor x \rfloor$.

Ak $\frac{1}{2} \le \{x\} < 1$, tak $1 \le 2\{x\} < 1$, z čoho dostaneme $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$ a $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 1$. □



# Kapitola 2

# Prvočísla

Tematika prvočísel patrí k najfascinujúcejším oblastiam nielen teórie čísel ale aj matematiky vôbec. Je známe množstvo dodnes nerozriešených hypotéz a problémov súvisiacich s prvočíslami. Príťažlivosť tejto oblasti pre „amatérskych matematikov“ je v tom, že na formulovanie týchto problémov často stačia vedomosti so základnej školy – to platí aj o mnohých iných problémoch v teórii čísel, veľa nematematikov sa napríklad pokúšalo dokázať známu Veľkú Fermatovu vetu. Pre „skutočných matematikov“ by čaro tejto problematiky mohlo byť skôr v tom, že prvočísla sa objavujú v najrôznejších oblastiach a najnečakanejších súvislostiach.

## 2.1 Deliteľnosť

{SECTDELIT}

Mnohé veci z tejto časti už poznáte (zo strednej školy, z iných prednášok), preto niektoré spomenieme iba stručnejšie. S podobnými výsledkami, aké uvedieme tu pre celé čísla, ste sa stretli aj na prednáškach o polynómoch (pozri [KGGS, Kapitola 5]). Mnohé z nich sa dajú zovšeobecniť na tzv. okruhy s jednoznačným rozkladom a Euklidovské okruhy (pozri [KGGS, Kapitola 7]).

Nasledujúca pomerne jednoduchá veta bude mať dôležité dôsledky.

{delit:VTLONGDIV}

**Veta 2.1.1 (Veta o delení so zvyškom).** *Nech $p, q$ sú celé čísla, $q > 0$. Potom existujú celé čísla $n$ a $r$ také, že*

$$p = n.q + r \qquad a \qquad 0 \le r < q.$$

*Navyše, $n$ a $r$ sú týmito podmienkami jednoznačne určené.*

Číslo $r$ z predchádzajúcej vety sa nazýva *zvyšok $p$ po delení číslom $q$* a označuje sa $p$ mod $q$.

*Dôkaz. Existencia:* Množina $\{k; kq \le p\}$ je zhora ohraničená. Preto existuje $n := \max\{k; kq \le p\}$. Položme $r = p - nq$. Očividne $r \ge 0$.

Tvrdíme, že $r < q$. Nech by to tak nebolo. Z nerovnosti $r \ge q$ dostaneme $p \ge (n + 1)q$, čo je spor s definíciou čísla $n$.

*Jednoznačnosť:* Predpokladajme, že $p = n.q + r = n'.q + r'$, kde $0 \le r, r' < q$. Potom

$$(n - n').q = r' - r.$$

Predpokladajme, že by $|n - n'| > 0$. Potom $|r - r'| \ge q$, čo je spor s tým, že $0 \le r, r' < q$.

Preto platí

$$(n - n').q = r - r' = 0,$$

a $n = n'$, $r = r'$. □

**Definícia 2.1.2.** Ak $a, b$ sú celé čísla, tak hovoríme, že $a$ *delí* $b$ ak existuje také $c \in \mathbb{Z}$, že $b = a.c$. Označujeme $a \mid b$.

Ak $a$ nedelí $b$, použijeme označenie $a \nmid b$. Napríklad $3 \mid 9$, ale $3 \nmid -7$.
Ľahko sa overia nasledujúce vlastnosti relácie $\mid$.

{delit:VTZAKDEL}

**Veta 2.1.3.** *Nech $a, b, c, m, n \in \mathbb{Z}$.*

(i) $a \mid 0$, $1 \mid a$, $a \mid a$.

(ii) *Ak $a \neq 0$, tak $0 \nmid a$.*

(iii) *Ak $a \mid b$ a $b \mid c$, tak $a \mid c$.*

(iv) *Ak $a \mid b$ a $a \mid c$, tak $a \mid m.b + n.c$.*

(v) *Ak $a \mid b$ a $b \mid a$, tak $a = \pm b$.*

(vi) *$a \mid b$ práve vtedy, keď $|a| \mid |b|$.*

(vii) *Ak $a, b \in \mathbb{N}$ a $a \mid b$, tak $a \leq b$.*

{delit:item7}

(viii) *Ak $a, b \in \mathbb{N}$ sú také, že $a \mid b$ a $b \mid a$, tak $a = b$.*

(ix) *Ak $ab \mid ac$ a $a \neq 0$, tak $b \mid c$.*

Uvedené tvrdenia budeme v ďalšom používať bez explicitnej odvolávky. Časť (viii) budeme veľmi často používať na dôkaz, že sa dve prirodzené čísla rovnajú.

{delit:DEFGCD}

**Definícia 2.1.4.** Nech $a, b \in \mathbb{Z}$. Prirodzené číslo $d$ sa nazýva *najväčší spoločný deliteľ* čísel $a$ a $b$, ak

*(i)* $d \mid a$, $d \mid b$,

*(ii)* pre všetky čísla $c \in \mathbb{Z}$ také, že $c \mid a$, $c \mid b$ platí $c \leq d$.

Najväčší spoločný deliteľ čísel $a$ a $b$ označujeme $(a, b)$.
Používame síce rovnaké označenie pre n.s.d. ako pre usporiadané dvojice, z kontextu by vždy malo byť zrejmé, o ktorý z týchto 2 pojmov ide (n.s.d. sa bude v týchto poznámkach vyskytovať oveľa častejšie ako usporiadaná dvojica).
Ak $(a, b) = 1$, čísla $a$ a $b$ voláme *nesúdeliteľné,* v opačnom prípade hovoríme, že sú *súdeliteľné.*

**Lema 2.1.5.** *Ak $a \neq 0$ alebo $b \neq 0$, tak existuje najväčší spoločný deliteľ čísel $a$ a $b$.*

*Dôkaz.* Bez ujmy na všeobecnosti nech $a \neq 0$. Uvažujme množinu $S$ všetkých spoločných deliteľov $a$ a $b$. Pre každé $s \in S$ platí $s \leq |a|$. Teda množina $S$ je zhora ohraničená a má maximálny prvok $d$. Tento prvok je najväčším spoločným deliteľom $a$ a $b$. □

Všimnite si, že n.s.d. $(0, 0)$ neexistuje (pretože každé prirodzené číslo je deliteľom nuly). Priamo z definície 2.1.4 je zrejmé, že ak n.s.d. $(a, b)$ existuje, tak je určený jednoznačne.



{delit:PRIKLGCD}

**Príklad 2.1.6.** Počítajme hodnoty polynómu $f(n) = n^4 + n^2 + 1$ pre $n \in \mathbb{N}$:
$f(1) = 3$
$f(2) = 21 = 3.7$
$f(3) = 91 = 7.13$
$f(4) = 273 = 3.7.13$
$f(5) = 651 = 3.7.31$
Z prvých vypočítaných hodnôt sa zdá, že po sebe idúce čísla majú vždy spoločného deliteľa väčšieho ako 1, teda, že sú súdeliteľné. Ľahko sa môžeme presvedčiť o tom, že to tak bude skutočne pre ľubovoľné $n$. Platí totiž
$f(n) = n^4 + n^2 + 1 = (n^2 - n + 1)(n^2 + n + 1)$,
$f(n+1) = [(n+1)^2 - (n+1) + 1][(n+1)^2 + (n+1) + 1] = (n^2 + n + 1)(n^2 + 3n + 3)$.
Preto $n^2 + n + 1 \geq 3$ je spoločným deliteľom čísel $f(n)$ a $f(n+1)$.

Nasledujúca charakteristika n.s.d. bude dôležitá vo viacerých dôkazoch.
Nazýva sa podľa francúzskeho matematika Étienne Bézouta, ktorý dokázal podobné tvrdenie pre polynómy. Pre prirodzené čísla však možno toto tvrdenie nájsť už v práci iného francúzskeho matematika, Claude Gaspard Bachet de Méziriaca, publikovanej v prvej polovici 17-teho storočia. Tento istý matematik je autorom prekladu Diofantovej Aritmetiky z Gréčtiny do Latinčiny – práve v tomto preklade sa nachádza známa Fermatova poznámka o tom, že našiel veľmi pekný dôkaz Veľkej Fermatovej vety, ale je naň na okraji knihy primálo miesta.

{delit:GCDLINKOM}

**Veta 2.1.7 (Bézoutova identita).** *Nech $a, b \in \mathbb{Z}$, aspoň jedno z nich je nenulové. Nech $d = (a, b)$. Potom existujú čísla $u, v \in \mathbb{Z}$ také, že*

$$d = au + bv.$$

*Navyše $d$ je najmenšie prirodzené číslo, ktoré možno zapísať v takomto tvare.*

*Dôkaz.* V prípade, že niektoré z čísel $a$, $b$ je nulové, tvrdenie očividne platí. Budeme preto predpokladať, že $a, b \neq 0$.
Označme $M := \{ax + by; x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Nech $m = \min M$. Zrejme $m = au + bv$ pre nejaké $u, v \in \mathbb{Z}$. Chceme ukázať, že $m = d$.
Pretože $d \mid a, b$, platí aj $d \mid ax + by$ pre ľubovoľné celé čísla $x$, $y$. Špeciálne platí $d \mid m$. Keďže $d$ aj $m$ sú kladné, vyplýva z toho $d \leq m$.
Na overenie opačnej nerovnosti stačí ukázať, že $m \mid a$ a $m \mid b$. Podľa vety 2.1.1 existujú $q$ a $r$ také, že $a = mq + r$, $0 \leq r < m$. Ak by platilo $r > 0$, tak dostaneme $r = a - mq = a(1 - mu) - bv \in M$, čo je v spore s tým, že $m$ je najmenší prvok množiny $M$. Preto musí platiť $r = 0$, z čoho dostaneme $a = mq$ a $m \mid a$. Podobne sa overí $m \mid b$. □

Všimnime si, že množina $\{ax + by; x, y \in \mathbb{Z}\}$ tvorí ideál v okruhu $(\mathbb{Z}, +, \cdot)$. Vieme, že $(\mathbb{Z}, +, \cdot)$ je okruh hlavných ideálov. Podľa predchádzajúcej vety je tento ideál generovaný číslom $(a, b)$.

**Dôsledok 2.1.8.** *Nech $a, b, c \in \mathbb{Z}$ a aspoň jedno z čísel je nenulové. Ak $c \mid a$ a $c \mid b$, tak $c \mid (a, b)$.*

*Dôkaz.* Podľa vety 2.1.7 sa dá najväčší spoločný deliteľ čísel $a$ a $b$ vyjadriť v tvare $(a, b) = ua + vb$, kde $u, v \in \mathbb{Z}$. Z toho, že $c \mid a$ a $c \mid b$ dostaneme $c \mid ua + vb = (a, b)$. □

Definícia najväčšieho spoločného deliteľa hovorí, že $(a, b)$ je najväčší prvok množiny spoločných deliteľov $a$ a $b$ vzhľadom na usporiadanie $\leq$. Všimnite si, že veta 2.1.3 nám okrem

iného hovorí, že relácia | na množine prirodzených čísel je čiastočné usporiadanie. Podľa predchádzajúceho dôsledku je $(a, b)$ najväčší prvok množiny (kladných) spoločných deliteľov $a$ a $b$ aj vzhľadom na toto čiastočné usporiadanie.

{delit:LMEUKLID}

**Lema 2.1.9 (Euklidova lema).** *Ak $a, b, c \in \mathbb{Z}$, $a \mid bc$ a $(a, b) = 1$, tak $a \mid c$.*

*Dôkaz.* Podľa vety 2.1.7 existujú $u, v \in \mathbb{Z}$ také, že $au + bv = 1$. Z toho dostaneme $c = (au + bv)c = a.uc + bc.v$. Číslo $a$ delí oba sčítance, a teda $a \mid c$. □

Uvedieme ešte jednu lemu, ktorá hovorí o deliteľnosti v súvislosti s nesúdeliteľnými číslami.

{delit:LMAKOEUKLID}

**Lema 2.1.10.** *Ak $a, b, c \in \mathbb{Z}$, $(a, b) = 1$, $a \mid c$ a $b \mid c$, tak $ab \mid c$.*

*Dôkaz.* Máme $c = ka$ pre nejaké $k \in \mathbb{Z}$. Pretože $b \mid ka$ a $(a, b) = 1$, použitím Euklidovej lemy dostaneme $b \mid k$, z čoho už ľahko vyplýva $ab \mid ka = c$. □

{delit:LMNSD}

**Lema 2.1.11 (Základné vlastnosti n.s.d.).** *Vo všetkých častiach predpokladáme, že čísla vystupujúce v jednotlivých rovnostiach sú také, že obe strany rovnosti sú definované.*

{delit:item1}

(i) *Ak $c = k.b + a$, tak $(a, b) = (b, c)$.*

{delit:NSDit2}

(ii) *Ak $(a, b) = 1$ a $(a, c) = 1$, tak $(a, bc) = 1$.*

{delit:NSDit3}

(iii) *Ak $(a, b_i) = 1$ pre každé $i = 1, \ldots, k$, tak $(a, b_1 \ldots b_k) = 1$.*

{delit:NSDit4}

(iv) *Ak $(a, c) = 1$, tak $(a, bc) = (a, b)$.*

{delit:NSDitem4}

(v) *Ak $d = (a, b)$, tak $(\frac{a}{d}, \frac{b}{d}) = 1$.*

{delit:NSDit6}

(vi) $(ka, kb) = k(a, b)$

*Dôkaz.* (i) Pre čísla $x$, $y$ označme $M_{x,y}$ množinu ich spoločných deliteľov. N.s.d. 2 čísel je najväčší prvok tejto množiny.

Zrejme $d \mid a \wedge d \mid b \Rightarrow d \mid c = kb + a$.

Obrátene $d \mid c = kb + a \wedge d \mid b \Rightarrow d \mid a = c - kb$.

Dokázali sme $M_{a,b} = M_{c,b}$, z čoho vyplýva $(a, b) = (b, c)$

(ii) Označme $d = (a, bc)$. Podľa vety 2.1.7 existujú $x, y, x', y' \in \mathbb{Z}$ také, že $ax + by = ax' + cy' = 1$. Z toho dostaneme $ax+by = ax+by.1 = ax+by.(ax'+cy') = a.(x+byx')+bc.yy'$. Získali sme vyjadrenie $1 = au + bv$, kde $u$ a $v$ sú celé čísla. Z toho vyplýva, že $d \mid 1$ a, keďže $d$ je prirodzené číslo, $d = 1$.

(iii) Vyplýva z (ii) matematickou indukciou vzhľadom na $k$.

(iv) Stačí nám ukázať, že každý spoločný deliteľ $d$ čísel $a$ a $bc$ musí deliť $b$. Z toho, že $d \mid a$ a $(a, c) = 1$ máme $(d, c) = 1$. Potom podľa Euklidovej lemy $d \mid bc$ implikuje $d \mid b$.

(v) Podľa vety 2.1.7 platí $ax + by = d$ pre nejaké $x, y \in \mathbb{Z}$. Z toho dostaneme $\frac{a}{d}x + \frac{b}{d}y = 1$. Pretože 1 je najmenšie prirodzené číslo a $(\frac{a}{d}, \frac{b}{d})$ je najmenšie prirodzené číslo, ktoré možno získať celočíselnou kombináciou čísel $\frac{a}{d}$ a $\frac{b}{d}$, musí platiť $(\frac{a}{d}, \frac{b}{d}) = 1$.

(vi) Stačí si uvedomiť, že ak $a$, $b$ vynásobíme rovnakým číslom $k$, zväčšia sa všetky prvky množiny $M_{a,b}$ práve $k$-krát. Teda aj najmenší prvok tejto množiny bude $k$-krát väčší. □

Vlastnosť (i) je základom Euklidovho algoritmu na výpočet najväčšieho spoločného deliteľa. (Euklidovým algoritmom súčasne vypočítame aj koeficienty $u$ a $v$ z vety 2.1.7.) Tento algoritmus poznáte pre prípad polynómov, pre celé čísla funguje analogicky (pozri napríklad Dodatok A, [KGGS, Veta 5.3.2], [Č, Veta 1.1.7], [C, Theorem 1C]).

Pomocou uvedených vlastností môžeme ukázať, že n.s.d. čísel z príkladu 2.1.6 je buď $n^2 + n + 1$ alebo $7(n^2 + n + 1)$.



{delit:PRIKLNSD}

**Príklad 2.1.12.** V príklade 2.1.6 sme zistili, že $f(n) = n^4 + n^2 + 1 = (n^2 - n + 1)(n^2 + n + 1)$ a $f(n + 1) = [(n + 1)^2 - (n + 1) + 1][(n + 1)^2 + (n + 1) + 1] = (n^2 + n + 1)(n^2 + 3n + 3)$, teda $n^2 + n + 1$ je spoločným deliteľom čísel $f(n)$ a $f(n + 1)$. Na zistenie ich n.s.d. nám stačí určiť n.s.d. čísel $a(n) = n^2 - n + 1$ a $b(n) = n^2 + 3n + 3$. Dostávame

$$(a(n), b(n)) = (a(n), b(n) - a(n)) = (n^2 - n + 1, 4n + 2) \overset{(1)}{=} (n^2 - n + 1, 2n + 1) =$$

$$(n^2 - n + 1 - (2n + 1), 2n + 1) = (n^2 - 3n, 2n + 1) = (n(n - 3), 2n + 1) \overset{(2)}{=} (n - 3, 2n + 1) =$$
$$(n - 3, (2n + 1) - 2(n - 3)) = (n - 3, 7)$$

V rovnosti (1) sme využili, že $n^2 - n + 1$ je nepárne (a lemu 2.1.11(iv)). V rovnosti (2) sme využili fakt, že $(n, 2n + 1) = 1$ a tú istú lemu. Takisto sme (vo väčšine rovností) používali lemu 2.1.11(i)).

Zistili sme, že $(a(n), b(n)) \mid 7$ a teda $(f(n), f(n + 1)) \mid 7(n^2 + n + 1)$. Dokonca vieme, že $(a(n), b(n)) = 7$ iba v prípade, že $7 \mid n - 3$, čiže $n = 7k + 3$. To znamená, že

$$(f(n), f(n + 1)) = \begin{cases} 7(n^2 + n + 1), & \text{ak } n = 7k + 3, \\ n^2 + n + 1, & \text{inak.} \end{cases}$$

Ešte uvedieme niektoré vlastnosti n.s.d., ktoré budeme potrebovať neskôr.

{delit:LMCOPRIME}

**Lema 2.1.13.** *Nech $m, n \in \mathbb{N}$. Ak $(m, n) = 1$ a $d \mid mn$, tak existujú jednoznačne určené čísla $u, v \in \mathbb{N}$ také, že $d = uv$, $u \mid m$ a $v \mid n$. (Konkrétne sú to čísla $u = (d, m)$ a $v = (d, n)$.)*

*Dôkaz. Existencia:* Ukážeme, že čísla $u := (d, m)$ a $v := (d, n)$ spĺňajú uvedené podmienky.

Pretože platí $u \mid m$ a $v \mid n$, pričom $m$ a $n$ sú nesúdeliteľné, platí aj $(u, v) = 1$. Súčasne $u, v \mid d$ a podľa lemy 2.1.10 dostaneme $uv \mid d$.

Podľa vety 2.1.7 existujú celé čísla $x_1$, $x_2$, $y_1$, $y_2$ také, že

$$u = dx_1 + my_1,$$
$$v = dx_2 + ny_2.$$

Preto

$$u.v = d^2x_1x_2 + d(nx_1y_2 + mx_2y_1) + mny_1y_2.$$

Z toho, že $d \mid mn$ vidíme, že $d \mid uv$.

Ukázali sme, že $d \mid uv$ aj $uv \mid d$. Pretože ide o prirodzené čísla, máme $d = uv$.

*Jednoznačnosť:* Je zrejmé, že pre čísla $u$, $v$, ktoré spĺňajú podmienky z tvrdenia lemy platí $u \mid (d, m)$ a $v \mid (d, n)$.

Prepokladajme, že by neplatilo $u = (d, m)$. Potom $u < (d, m)$ a $uv < (d, m)(d, n) = d$ (poslednú rovnosť sme ukázali v prvej časti dôkazu), čo je spor. □

{delit:DOSCOPRIME}

**Dôsledok 2.1.14.** *Ak $a, b, c \in \mathbb{N}$ a $(a, b) = 1$, tak $(ab, c) = (a, c)(b, c)$.*

*Dôkaz.* Označme $d := (ab, c)$. Pretože $d \mid ab$, na základe predchádzajúcej lemy $d = (d, a)(d, b)$. Teraz si stačí všimnúť, že $(d, a) = ((ab, c), a) = (a, c)$, a takisto $(d, b) = ((ab, c), b) = (b, c)$. Preto $(ab, c) = d = (a, c)(b, c)$. □

Duálny pojem k najväčšiemu spoločnému deliteľu je najmenší spoločný násobok.

**Definícia 2.1.15.** Nech $a, b \in \mathbb{Z}$. Prirodzené číslo $n$ sa nazýva *najmenší spoločný násobok* čísel $a$ a $b$, ak

*(i)* $a \mid n$, $b \mid n$,

*(ii)* pre všetky čísla $c \in \mathbb{N}$ také, že $a \mid c$, $b \mid c$ platí $n \leq c$.

Najmenší spoločný násobok čísel $a$ a $b$ označujeme $[a, b]$.

**Veta 2.1.16.** *Ak $a, b$ sú ľubovoľné prirodzené čísla rôzne od 0, tak*

$$[a, b] = \frac{ab}{(a, b)}.$$

*Dôkaz.* Označme $d := (a, b)$ $n := \frac{ab}{d}$. Pretože $d \mid a$, $n$ je celé číslo. Overíme, že $n$ spĺňa podmienky z definície n.s.n.

Číslo $n$ je celočíselným násobkom $a$, pretože $n = a\frac{b}{d}$. To znamená, že $a \mid n$. Podobne sa ukáže $b \mid n$.

Zostáva nám overiť druhú podmienku z definície nsn. Nech teda $c$ je prirodzené číslo také, že $a \mid c$, $b \mid c$. Potom zrejme platí aj $\frac{a}{d} \mid \frac{c}{d}$ a $\frac{b}{d} \mid \frac{c}{d}$. Pretože $(\frac{a}{d}, \frac{b}{d}) = 1$ (Lema 2.1.11(v)) dostaneme podľa Euklidovej lemy, že aj $\frac{ab}{d^2} \mid \frac{c}{d}$, z čoho už vyplýva (po vynásobení číslom $d$), že $n = \frac{ab}{d} \mid c$. □

Najmenší spoločný násobok a najväčší spoločný deliteľ môžeme definovať indukciou aj pre viacero čísel. Budeme používať označenie $(a_1, \ldots, a_n)$ a $[a_1, \ldots, a_n]$.

**Cvičenia**

1. Je relácia | čiastočné usporiadanie na niektorej z množín $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{N}_0$? Ak áno, čo sú v jednotlivých prípadoch maximálne a minimálne prvky? Existujú v tejto usporiadanej množine supréma a infima konečného počtu čísel?

2. Kde sme použili v dôkaze vety 2.1.1 fakt, že množina prirodzených čísel je *dobre usporiadaná* (každá neprázdna podmnožina má najmenší prvok)?

3. Dokážte, že ak $a, b \in$ a $\frac{1}{a} + \frac{1}{b} \in \mathbb{N}$, tak $a = b$ a $a = 1$ alebo $a = 2$.

4. Fibonacciho postupnosť je určená predpisom $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$. Dokážte, že pre každé $n \in \mathbb{N}$ platí $(F_n, F_{n+1}) = 1$.

5. Dokážte, že $(F_n, F_{n+3}) \in \{1, 2\}$ pre každé $n \in \mathbb{N}$.

6. Ak $n \in \mathbb{N}$, dokážte $(14n + 3, 21n + 4) = 1$.

7. Dokážte, že súčin 3 po sebe idúcich prirodzených čísel je deliteľný 6.

8. Dokážte, že súčin $n$ po sebe idúcich prirodzených čísel je deliteľný $n!$. {delitcvic:NSD}

9. Dokážte, že ak $(a, b) = 1$, tak a) $(a+b, a-b)$ je 1 alebo 2; b) $(2a+b, a+2b)$ je 1 alebo 3; c) $(a+b, a^2-ab+b^2)$ je 1 alebo 3; d) pre ľubovoľné $m, n \in \mathbb{N}$ platí $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$.

10. Dokážte, že $(a, (ab, c)) = (a, c)$ (predpokladáme, že čísla $a$, $b$, $c$ sú také, že všetky n.s.d. vystupujúce v tomto vzťahu existujú).

11. Nájdite všetky prirodzené čísla, pre ktoré číslo a) $n^2 - 1$, b) $n^2 + 1$ je mocninou dvojky.

12. Ako $N_n$ označme číslo, ktorého zápis v desiatkovej sústave pozostáva z $n$ jednotiek, (teda $N_n = 10^0 + 10^1 + \ldots + 10^{n-1}$). Dokážte, že $N_n \mid N_m$ práve vtedy, keď $n \mid m$.



13. Dokážte: Nepárne prirodzené číslo $N \geq 3$ je zložené práve vtedy, keď existujú nezáporné celé čísla $n, m \in \mathbb{N} \cup \{0\}$ také, že $n - m > 1$ a $N = n^2 - m^2$. Nájdite čísla, $m$ a $n$ pre zložené čísla $N = 39, 161, 737$.

## 2.2 Prvočísla

V tejto časti si povieme definíciu a základné vlastnosti prvočísel a dokážeme základnú vetu aritmetiky, ktorá hovorí, že každé číslo sa dá jednoznačne zapísať ako súčin prvočísel.

**Definícia 2.2.1.** Nech $n > 1$ je prirodzené číslo. Ak $n = m.k$ pre nejaké celé čísla $1 < m, k < n$, tak hovoríme, že $n$ je *zložené číslo*. V opačnom prípade hovoríme, že $p$ je prvočíslo.

Množinu všetkých prvočísel budeme označovať $\mathbb{P}$.

Inými slovami, $n > 1$ je prvočíslo ak nemá v $\mathbb{N}$ iných deliteľov ako 1 a $n$. Podľa obvyklej konvencie prirodzené číslo 1 nepovažujeme za zložené číslo ani za prvočíslo.

Prvočíslami sú napríklad $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$

### 2.2.1 Základné vlastnosti prvočísel

{prvoc:LMEXPRDEL}

**Lema 2.2.2.** *Pre každé prirodzené číslo $n > 1$ existuje prvočíslo $p$ také, že $p \mid n$.*

*Dôkaz.* Indukciou vzhľadom na $n$. Pre $n = 2$ tvrdenie zrejme platí.

Predpokladajme, že tvrdenie lemy platí pre všetky čísla menšie ako $n$, ukážeme, že platí aj pre $n$.

Ak $n$ je prvočíslo, tak stačí položiť $p = n$. Ak $n$ je zložené, tak $n = mk$ pre nejaké prirodzené čísla $1 < m, k < n$. Podľa indukčného predpokladu existuje prvočíslo $p$ také, že $p \mid m$. Zrejme potom aj $p \mid n$. □

Ľahko sa dá overiť, že ak $n$ je zložené číslo, tak musí existovať prvočíslo $p$, ktoré delí $n$ také, že $p \leq \sqrt{n}$ (pozri cvičenie 8). To znamená, že na určenie, či $n$ je zložené, stačí vyskúšať či je deliteľné niektorým z prvočísel veľkosti najviac $\sqrt{n}$. Toto pozorovanie je základom najjednoduchšieho algoritmu na testovanie prvočíselnosti, ktorý sa nazýva *Eratostenovo sito*. V súčasnosti sa používajú na testovanie prvočíselnosti hlavne rôzne pravdepodobnostné algoritmy. Pomerne nedávno sa podarilo trom indickým matematikom [AKS] objaviť prvý deterministický algoritmus na testovanie prvočíselnosti, ktorý beží v polynomiálnom čase. (Pod polynomiálnou časovou zložitosťou tu rozumieme časovú zložitosť vzhľadom na dĺžku vstupu. Dĺžka vstupu je vlastne počet cifier zadaného čísla, t.j. $\lg n$.)

Dôkaz nasledujúcej vety možno nájsť už v Euklidových Základoch.

**Veta 2.2.3 (Euklides).** *Množina $\mathbb{P}$ je nekonečná.*

*Dôkaz.* Sporom. Nech by $p_1, \ldots, p_n$ boli všetky prvočísla. Nech $n = p_1 p_2 \ldots p_n + 1$. Pre žiadne z čísel $p_1, \ldots, p_n$ neplatí $p_k \mid n$, čo je spor s lemou 2.2.2. □

{prvoc:LMZVPRV}

**Lema 2.2.4.** *Nech $p$ je prvočíslo.*

(i) *Nech $a \in \mathbb{Z}$. Potom $(a, p) = 1$ alebo $(a, p) = p$.*

(ii) *Nech $a, b \in \mathbb{Z}$. Ak $p \mid ab$, tak $p \mid a$ alebo $p \mid b$.*

(iii) *Nech $a_1, \ldots, a_n \in \mathbb{Z}$. Ak $p \mid a_1 \ldots a_n$, tak $p \mid a_k$ pre niektoré $k = 1, \ldots, n$.*

*Dôkaz.* (i): Nech $d = (a, p)$. Pretože $d \mid p$ a $p$ je prvočíslo, môže to byť iba 1 alebo $p$.

(ii): Ak $(a, p) = p$, tak máme $p \mid a$. V opačnom prípade dostaneme z Euklidovej lemy (lema 2.1.9) $p \mid b$.

(iii): Vyplýva z (ii) pomocou indukcie. □

### 2.2.2 Základná veta aritmetiky, kanonický rozklad

**Veta 2.2.5 (Základná veta aritmetiky).** *Každé prirodzené číslo $n > 1$ je možné zapísať ako súčin prvočísel $n = p_1 \dots p_k$.*

*Tento zápis je jednoznačný až na poradie.*

*Dôkaz. Existencia:* Indukciou. Pre $n = 2$ tvrdenie platí.

Ak $n > 2$ tak podľa lemy 2.2.2 existuje prvočíslo $p$ také, že $p \mid n$. Ak $p = n$, tak zápis čísla $n$ v tvare súčinu prvočísel pozostáva z tohto jediného prvočísla. V opačnom prípade je $\frac{n}{p} > 1$ a môžeme použiť indukčný predpoklad. Z neho dostaneme, že $\frac{n}{p} = p_1 \dots p_{k-1}$ a $n = p.p_1 \dots p_{k-1}$.

*Jednoznačnosť:* Nech $n = p_1 \dots p_k = q_1 \dots q_m$ sú rozklady toho istého čísla $n$. Chceme ukázať, že prvočísla $p_1, \dots, p_k$, $q_1, \dots, q_m$ sa líšia nanajvýš usporiadaním (z toho súčasne vyplýva, že $m = k$.)

Opäť budeme postupovať indukciou. Pre $n = 2$ je to pravda. Predpokladajme, že tvrdenie platí pre všetky prirodzené čísla menšie ako $n$ a väčšie ako 1.

Pretože $p_1 \mid q_1 \dots q_m$, existuje podľa lemy 2.2.4 $q_i$, kde $i \in \{1, 2, \dots, m\}$, také, že $p_1 \mid q_i$. Pretože $q_i$ je prvočíslo, platí potom $p_1 = q_i$.

Položme $s = p_2 \dots p_k = q_1 \dots q_{i-1}.q_{i+1} \dots q_m$. Ak $s = 1$, tak tvrdenie vety platí. Ak $s > 1$, tak podľa indukčného predpokladu prvočísla $q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_m$ sú len preusporiadaním prvočísel $p_2, \dots, p_k$, a teda to iste platí aj pre $p_1, \dots, p_k$ a $q_1, \dots, q_m$. □

Z predchádzajúcej vety vyplýva, že každé prirodzené číslo $n > 1$ možno jednoznačne zapísať v tvare $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, kde $p_1, \dots, p_k$ sú navzájom rôzne prvočísla a $\alpha_1, \dots, \alpha_k \in \mathbb{N}$. (Tento zápis je jednoznačný až na preusporiadanie prvočísel $p_1, \dots, p_k$.)

**Definícia 2.2.6.** Jednoznačný zápis čísla $n$ v tvare $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, kde $p_1, \dots, p_k$ sú navzájom rôzne prvočísla a $\alpha_1, \dots, \alpha_k \in \mathbb{N}$, nazývame *kanonický rozklad* čísla $n$.

Príklady kanonického rozkladu:
$1125 = 5^2.7^2$,
$5! = 120 = 2^3.3.5$,
$1400 = 2^3.5^2.7$.

Pri hľadaní kanonického rozkladu je tiež často užitočné už spomenuté pozorovanie, že ak $n$ je zložené, tak má prvočíselného deliteľa veľkosti nanajvýš $\sqrt{n}$ (cvičenie 8).

#### Cvičenia

1. Nech $a, b \in \mathbb{N}$ a $p_1, \dots, p_n$ sú všetky prvočísla, ktoré delia $a$ alebo $b$. Potom máme jednoznačné vyjadrenie $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \dots p_n^{\beta_n}$. Dokážte, že $a \mid b$ práve vtedy, keď $\alpha_i \leq \beta_i$ pre všetky $i = 1, \dots, n$.

2. Nech $m, n \in \mathbb{N}$ a $p_1, \dots, p_n$ sú všetky prvočísla, ktoré delia $m$ alebo $n$. Potom máme jednoznačné vyjadrenie $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, $n = p_1^{\beta_1} \dots p_n^{\beta_n}$, kde $\alpha, \beta \in \mathbb{N}_0$. Dokážte, že

$$(m, n) = p_1^{\min(\alpha_1, \beta_1)} \dots p_n^{\min(\alpha_n, \beta_n)} \qquad [m, n] = p_1^{\max(\alpha_1, \beta_1)} \dots p_n^{\max(\alpha_n, \beta_n)}.$$



3. Nájdite všetky čísla $p$ také, že $p$, $p + 2$ aj $p + 4$ sú prvočísla.

4. Dokážte, že pre všetky prirodzené čísla $n > 1$ je číslo $n^4 + 4$ zložené.

5. Dokážte, že pre všetky prirodzené čísla $n > 1$ je číslo $n^4 + n^2 + 1$ zložené.

6. Dokážte, že ak $2^n - 1$ je prvočíslo, tak $n$ je prvočíslo.

7. Dokážte, že ak $2^n + 1$ je prvočíslo, tak $n$ je mocnina 2. Pre aké $n$ sú $2^n - 1$ aj $2^n + 1$ prvočísla?

{prvoc:CVICSQRT}

8. Dokážte, že ak $n \in \mathbb{N}$ je zložené číslo, tak existuje prvočíslo $p$ také, že $p \mid n$ a $p \leq \sqrt{n}$. Nech $n \in \mathbb{N}$ a $p$ je najmenšie prvočíslo, ktoré delí $n$. Dokážte, že ak $p > \sqrt[3]{n}$, tak $\frac{n}{p}$ je prvočíslo alebo 1.

9. Dokážte, že ak $p$ aj $p^2 + 2$ sú prvočísla, tak aj $p^3 + 2$ je prvočíslo. Koľko takých trojíc existuje?

10. Dokážte, že pre $n > 1$ súčet $\sum_{k=1}^{n} \frac{1}{k}$ nie je celé číslo.

## 2.3 Rozloženie prvočísel

Už vieme, že prvočísel je nekonečne veľa. Môžeme si však položiť otázku, akých čísel je viac – zložených čísel alebo prvočísel. Z hľadiska kardinality ich je rovnako veľa – obe množiny sú nekonečné spočítateľné. Zrejme teda kardinalita nebude vhodné kritérium na porovnávanie veľkosti podmnožín množiny $\mathbb{N}$ – s výnimkou konečných množín majú všetky podmnožiny $\mathbb{N}$ rovnakú mohutnosť. Mohli by sme sa pokúsiť nájsť iné kritériá na posúdenie toho, či podmnožina $\mathbb{N}$ je „veľká“ alebo „malá“.

### 2.3.1 Medzery v množine prvočísel

**Veta 2.3.1.** *Existuje ľubovoľne dlhá postupnosť po sebe idúcich zložených čísel.*

*Dôkaz.* Nech $n \in \mathbb{N}$, $n \geq 2$. Uvažujme čísla $n! + 2, n! + 3, \dots, n! + n$. Pre každé z týchto čísel platí $k \mid n! + k$, čiže každé z nich má vlastného deliteľa. Uvedené čísla tvoria teda postupnosť $n - 1$ po sebe idúcich zložených čísel. □

### 2.3.2 Rad prevrátených hodnôt prvočísel

Ako sme už spomenuli, existuje množstvo kritérií na to, ktoré podmnožiny prirodzených čísel môžeme považovať za veľké a ktoré za malé, pričom v rôznych situáciach môžu byť vhodné rôzne kritériá.

Jednou z možností je zistiť, či rad zostavený z prevrátených hodnôt danej množiny konverguje alebo diverguje. Je napríklad známe, že harmonický rad $\sum \frac{1}{n}$ diverguje, čo zodpovedá tomu, že množina všetkých prirodzených čísel je veľká. Naopak, rad $\sum \frac{1}{n!} = e$ konverguje, čo zodpovedá tomu, že množina $\{n!; n \in \mathbb{N}\}$ je pomerne riedka. Ukážeme, že množina všetkých prvočísel je v tomto zmysle veľká.

Hoci rad $\sum \frac{1}{p_n}$ diverguje, jeho divergencia je extrémne pomalá. Aj o harmonickom rade vieme, že diverguje veľmi pomaly – rastie zhruba ako logaritmická funkcia (B.2). Je známe, že pre rad prevrátených hodnôt prvočísel platí $\sum_{p \leq x} \frac{1}{p} \sim \ln \ln x$.

Uvedieme niekoľko rôznych dôkazov. V prvom z nich budeme potrebovať pojem čísla bez kvadratických deliteľov.

**Definícia 2.3.2.** Hovoríme, že číslo $n \in \mathbb{N}$ je *číslo bez kvadratických deliteľov,* ak neexistuje prirodzené číslo $k > 1$ také, že $k^2 \mid n$.

O tom, či dané číslo je bez kvadratických deliteľov sa možno ľahko presvedčiť na základe jeho kanonického rozkladu. Číslo nemá kvadratických deliteľov práve vtedy, keď jeho kanonický rozklad obsahuje iba prvé mocniny prvočísel, t.j. $n = p_1 \dots p_k$.

Z toho tiež vidno, že každé číslo možno jednoznačne napísať v tvare $n = j.k^2$, kde $j$ nemá kvadratických deliteľov. Ak totiž $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla $n$ a $q_1, \dots, q_m$ sú tie prvočísla, ktoré sa vyskytujú v kanonickom rozklade čísla $n$ v nepárnej mocnine, tak platí $n = j.k^2$, kde $j = q_1 \dots q_m$ a $k = p_1^{\lfloor \frac{\alpha_1}{2} \rfloor} \dots p_k^{\lfloor \frac{\alpha_k}{2} \rfloor}$.

Napríklad pre $n = 2^3.3^2.5.7^7$ máme rozklad $n = (2.5.7).(2.3.7^3)^2$.

V ďalšom budeme ako $p_n$ označovať $n$-té prvočíslo, t.j. množinu všetkých prvočísel možno zapísať v tvare $\mathbb{P} = \{p_1 < p_2 < \dots\}$.

Budeme tiež používať nerovnosť

$$e^x > 1 + x.$$

(Sú to prvé 2 členy Taylorovho rozvoja funkcie $e^x$ v bode 0.)

{rozloz:PREVR}

**Veta 2.3.3.** *Rad prevrátených hodnôt prvočísel diverguje, t.j.*

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty.$$

Uvedenú vetu ako prvý dokázal L. Euler. Nasledujúci dôkaz je z článku [Niv2], dá sa tiež nájsť v knihách [KLŠZ] a [DD]. Prehľad viacerých ďalších dôkazov podáva článok [E].

*Dôkaz.* Pre $n \in \mathbb{N}$ označme $S_n$ čiastočný súčet

$$S_n = \sum_{k=1}^{n} \frac{1}{p_k},$$

kde $p_k$ označuje $k$-té prvočíslo. Platí

$$e^{S_n} = \prod_{k=1}^{n} e^{\frac{1}{p_k}} > \prod_{k=1}^{n} \left(1 + \frac{1}{p_k}\right).$$

Po roznásobení pravej strany dostaneme prevrátené hodnoty všetkých čísel tvaru $q_1 \dots q_k$, kde $q_1, \dots, q_k$ sú navzájom rôzne prvočísla veľkosti nanajvýš $p_n$. To znamená, že uvedený výraz je súčet prevrátených hodnôt všetkých čísel bez kvadratických deliteľov, ktoré obsahujú vo svojom rozklade len prvočísla $p_1, \dots, p_n$.

Označme $B$ množinu všetkých čísel bez kvadratických deliteľov. Z predchádzajúceho odhadu teda vyplýva, že

$$e^{S_n} > \sum_{\substack{k \le p_n \\ k \in B}} \frac{1}{k}.$$

(Čísla veľkosti najviac $p_n$ určite neobsahujú vo svojom rozklad väčšie prvočísla, než je $p_n$.)

Predpokladajme, že by existovala limita $\lim_{n\to\infty} S_n = S < +\infty$ (rastúca postupnosť musí mať limitu, ak je ohraničená). Keďže postupnosť $S_n$ je rastúca a $e^x$ je rastúca funkcia, pre všetky $n \in \mathbb{N}$ platí $e^S > e^{S_n}$.



Pretože každé prirodzené číslo možno zapísať v tvare $t = j^2 k$, kde $k \in B$, dostaneme nerovnosť

$$\left(\sum_{\substack{k \le p_n \\ k \in B}} \frac{1}{k}\right)\left(\sum_{j=1}^{p_n} \frac{1}{j^2}\right) \ge \sum_{t=1}^{p_n} \frac{1}{t}.$$

(Nerovnosť platí, pretože každé $t$ na pravej strane sa vyskytne ako menovateľ v niektorom zo zlomkov, ktoré vzniknú roznásobením ľavej strany.)

Je známe, že $\sum_{n=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}$ (pozri dodatok B). Dostávame teda

$$\frac{\pi^2}{6} e^S > \sum_{t=1}^{\infty} \frac{1}{t},$$

čo je spor s tým, že rad na pravej strane nerovnosti diverguje. □

Iný dôkaz vety 2.3.3, ktorého autorom je P. Erdös, je uvedený v knihe [AZ]. Prvá kapitola tejto knihy je venovaná šiestim zaujímavým dôkazom, že množina $\mathbb{P}$ je nekonečná. Nasledujúci dôkaz je práve jeden z nich – aj keď samozrejme tvrdenie, že rad prevrátených hodnôt prvočísel diverguje je podstatne silnejšie tvrdenie.

*Dôkaz vety 2.3.3.* Predpokladajme, že rad $\sum_{n=1}^{\infty} \frac{1}{p_k}$ konverguje. Potom existuje $k \in \mathbb{N}$ také, že

$$\sum_{i \ge k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Pre každé prirodzené číslo $N$ máme potom nerovnosť

$$\sum_{i \ge k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Nazvime prvočísla $p_1, \dots, p_k$ malými prvočíslami, ostatné prvočísla budeme volať veľké.

Pre $N \in \mathbb{N}$ označme $N_b$ počet tých čísel z $1, 2, \dots, N$, ktoré obsahujú vo svojom kanonickom rozklade aspoň jedno veľké prvočíslo. Ako $N_s$ označíme počet tých čísel, ktoré obsahujú len malé prvočinitele (sem rátame aj číslo 1). (Indexy $b$ a $s$ sú z anglického big a small.) Týmto sme rozložili množinu $\{1, 2, \dots, N\}$ na dve disjunktné časti, preto platí $N = N_s + N_b$. Pokúsime sa teraz odhadnúť čísla $N_b$ a $N_s$.

Počet čísel nepresahujúcich $N$, ktoré sú deliteľné prvočíslom $p_i$, je $\lfloor \frac{N}{p_i} \rfloor$. Preto

$$N_b \le \sum_{i \ge k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \le \sum_{i \ge k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Na odhad čísla $N_s$ opäť použijeme fakt, že každé $n \le N$ môžeme napísať ako $n = a_n b_n^2$, kde $a_n$ je číslo bez kvadratických deliteľov. Pretože $a_n$ vo svojom prvočíselnom rozklade obsahuje len malé prvočinitele a všetky sú v prvej mocnine, máme $2^k$ možností pre číslo $a_n$. Z toho, že $b_n^2 \le n \le N$ máme odhad $b_n \le \sqrt{N}$, preto máme najviac $\sqrt{N}$ možností pre číslo $b_n$. Celkovo teda máme

$$N_s \le 2^k \sqrt{N}.$$

Ak zvolíme dostatočne veľké $N$, tak $N_s \le 2^k \sqrt{N} < \frac{N}{2}$ a $N_b + N_s < N$, čo je spor. □

Ako ďalšiu možnosť dôkazu vety 2.3.3 spomenieme nasledujúce tvrdenie z článku [Mo].

{rozloz:TVRMOSER}

**Tvrdenie 2.3.4.** *Ak rad* $\sum_{p\in\mathbb{P}} \frac{1}{p}$ *konverguje, tak* $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$, *kde* $\pi(n) = |\{p \in \mathbb{P}; p \le n\}|$ *označuje počet prvočísel neprevyšujúcich* $n$.

*Dôkaz.* Označme $R_n = \sum_{p\le n, p\in\mathbb{P}} \frac{1}{p}$. Všimnime si, že platí

$$\pi(n) = R_1 - R_0 + 2(R_2 - R_1) + \ldots + n(R_n - R_{n-1}) = nR_n - (R_0 + R_1 + \ldots + R_{n-1}).$$

Z toho dostaneme

$$\frac{\pi(n)}{n} = R_n - \frac{R_0 + R_1 + \ldots + R_{n-1}}{n}.$$

Je známe, že ak nejaká postupnosť konverguje, tak aj postupnosť pozostávajúca z jej aritmetických priemerov konverguje k tomu istému číslu (cvičenie 6). Preto

$$\lim_{n\to\infty} R_n = \lim_{n\to\infty} \frac{R_0 + R_1 + \ldots + R_{n-1}}{n}$$

a z predchádzajúcej rovnosti ľahko vyplýva $\lim_{n\to\infty} \frac{\pi(n)}{n} = 0$. □

Teraz si ukážeme, ako sa dá pomocou predchádzajúceho tvrdenia odvodiť veta 2.3.3. Toto tvrdenie však súčasne slúži ako prvý príklad použitia funkcie $\pi(n)$, ktorou sa budeme podrobne zaoberať v nasledujúcej časti. Tvrdenie 2.3.4 ukazuje súvis medzi touto funkciou a divergenciou prevráteného radu prvočísel. Prevrátený rad prvočísel ako aj funkcia $\pi$ slúžia ako prostriedky na popis rozloženia prvočísel.

*Dôkaz vety 2.3.3.* Predpokladajme, že rad $\sum_{p\in\mathbb{P}} \frac{1}{p}$ konverguje. V takom prípade existuje $n$ také, že

$$\sum_{p\in\mathbb{P}, p>n} \frac{1}{p} < \frac{1}{2}.$$

Podľa tvrdenia 2.3.4 k tomuto $n$ existuje $m \in \mathbb{N}$ také, že $\frac{\pi(n!m)}{n!m} < \frac{1}{2n!}$, čiže

$$\frac{\pi(n!m)}{m} < \frac{1}{2}.$$

Uvažujme teraz čísla $T_i = n!i - 1$ pre $i = 1, \ldots, m$. Je zrejmé, že tieto čísla nie sú deliteľné žiadnym z čísel $2, 3, \ldots, n$. Teda ak prvočíslo $p$ delí $T_i$, tak $p > n$. Ďalej si uvedomme, že ak súčasne platí $p \mid T_i$ a $p \mid T_j$ pre nejaké $i \neq j$, tak máme $p \mid T_i - T_j = n!(i-j)$, z čoho dostaneme (pretože $p > n$), že $p \mid i - j$. Teda ak pevne zvolíme prvočíslo $p$, toto prvočíslo môže byť deliteľom najviac $1 + \frac{m}{p}$ čísel spomedzi čísel $T_1, \ldots, T_m$.

Pretože každé z čísel $T_i$ je deliteľné nejakým prvočíslom $p$ spĺňajúcim nerovnosť $n!m > p > n$, dostávame z toho

$$\sum_{n!m>p>n} \left(\frac{m}{p} + 1\right) \ge m,$$

$$\sum_{p>n} \frac{1}{p} + \frac{\pi(n!m)}{m} \ge 1,$$

čo je v spore s odhadmi uvedenými v prvej časti dôkazu. □



V súvislosti s vetou 2.3.3 možno spomenúť hypotézu, ktorú vyslovil P. Erdös. Táto hypotéza tvrdí, že každá množina $A = \{n_1 < n_2 < \ldots\}$ taká, že rad $\sum_{k=1}^{\infty} \frac{1}{n_k}$ diverguje obsahuje ľubovoľne dlhé konečné aritmetické postupnosti. (T.j. pre každé $n$ existujú $a$ a $d$ tak, že $\{a, a+d, \ldots, a+nd\} \subseteq A$.) Táto hypotéza je dodnes nerozriešená.

Veta 2.3.3 hovorí, že množina $\mathbb{P}$ spĺňa predpoklady Erdösovej hypotézy. Ale aj problém, či prvočísla obsahujú ľubovoľne dlhé konečné aritmetické postupnosti bol veľmi dlho otvorený, pomerne nedávno na túto otázku kladne odpovedali B. Green a T. Tao [GT]. Viac sa o ich dôkaze možno dozvedieť napríklad v prehľadovom článku [Kl].[1]

### 2.3.3 Prvočíselná funkcia

**Definícia 2.3.5.** Počet prvočísel nepresahujúcich reálne číslo $x$ označujeme $\pi(x)$. Funkcia $\pi$ sa nazýva *prvočíselná funkcia.*

$$\pi(x) = |\{p \le x; p \in \mathbb{P}\}|$$

Funkcia $\pi$ teda popisuje rozloženie prvočísel medzi prirodzenými číslami.

Jedným z najhlbších výsledkov teórie čísel je *prvočíselná veta,* ktorá vlastne dáva odhad pre rád funkcie $\pi(x)$. Táto veta hovorí, že

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1,$$

t.j. $\pi(x) \sim \frac{x}{\ln x}$.

Prvočíselnú vetu dokázali nezávisle od seba J. Hadamard a Ch. de la Valleé Poussin koncom 19-teho storočia. P. Erdös a A. Selberg v 50-tych rokoch našli dôkaz tejto vety, ktorý nevyužíval komplexnú analýzu. (Viac o tomto dôkaze sa môžete dozvedieť napríklad v [Lev2].) Túto vetu nebudeme dokazovať (dôkaz je pomerne zložitý – napriek tomu, že viacerí matematici zostrojili jednoduchšie dôkazy než bol pôvodný dôkaz tejto vety, pozri napríklad články [Ne], [Za] alebo diplomovú prácu [VR]), v nasledujúcej časti však dokážeme aspoň o niečo slabšie tvrdenia.

Prvočíselná veta vlastne hovorí, že $\pi(x) \sim \frac{x}{\ln x}$. Poznamenajme, takisto bez dôkazu, že pre $n$-té prvočíslo platí asymptotický odhad $p_n \sim n \ln n$ (dôkaz tohto tvrdenia z prvočíselnej vety možno nájsť napríklad v [GKP]).

Z prvočíselnej vety môžeme odvodiť napríklad tento zaujímavý fakt:

{rozloz:TVRHUST}

**Tvrdenie 2.3.6.** *Množina* $\{\frac{p}{q}; p, q \in \mathbb{P}\}$ *je hustá v* $\langle 0, +\infty)$.

Pripomeňme, že podmnožina $M \subseteq \langle 0, +\infty)$ je *hustá* v $\langle 0, +\infty)$, ak v každom otvorenom intervale $(a, b)$, kde $0 \le a < b$, sa nachádza nejaký prvok množiny $M$. Napríklad $\mathbb{Q} \cap \langle 0, +\infty)$ je hustá podmnožina $\langle 0, +\infty)$.

{rozloz:LMHUST}

**Lema 2.3.7.** *Nech* $0 < a < b$ *sú reálne čísla. Potom* $\lim_{n\to\infty} (\pi(bn) - \pi(an)) = +\infty$.

*Dôkaz.* Najprv vypočítame limitu podielu $\frac{\pi(an)}{\pi(bn)}$. Z prvočíselnej vety máme

$$\lim_{n\to\infty} \frac{\pi(an)}{\pi(bn)} = \lim_{n\to\infty} \frac{\frac{bn}{\ln(bn)}}{\frac{an}{\ln(an)}} = \lim_{n\to\infty} \frac{b}{a} \frac{\ln a + \ln n}{\ln b + \ln n} = \frac{b}{a}.$$

Pretože $\pi(bn) - \pi(an) = \pi(an)\left(\frac{\pi(bn)}{\pi(an)} - 1\right)$ a $\lim_{n\to\infty} \pi(an) = +\infty$, máme $\lim_{n\to\infty} (\pi(bn) - \pi(an)) = +\infty$. □

[1] Terence Tao dostal v roku 2006 Fieldsovu medailu. Je zlatý medailista z IMO 1988.

*Dôkaz tvrdenia 2.3.6.* Nech $0 < a < b$ sú reálne čísla. Ukážeme, že existujú $p, q \in \mathbb{P}$ také, že $a < \frac{p}{q} \leq b$.

Podľa lemy 2.3.7 $\lim_{n\to\infty}(\pi(bn)-\pi(an)) = +\infty$. Preto existuje také $n_0$, že pre všetky $n > n_0$ platí $\pi(bn) - \pi(an) > 1$.

Nech $q$ je ľubovoľné prvočíslo väčšie ako $n_0$. Potom $\pi(bq) - \pi(aq) > 1$, teda existuje prvočíslo $p$ také, že $aq < p \leq bq$ a $a < \frac{p}{q} \leq b$. □

Prvočíselná veta sa často zvykne uvádzať aj vo formulácii, kde namiesto $\frac{x}{\ln x}$ vystupuje niektorá z funkcií

$$\mathrm{li}(x) = \int_0^x \frac{dt}{\ln t}, \qquad \mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t} = \mathrm{li}(x) - \mathrm{li}(2).$$

(S integrálom v definícii funkcii $\mathrm{li}(x)$ je trochu problém – ak chceme byť úplne presný, táto funkcia sa definuje pre $x \geq 1$ ako

$$\mathrm{li}(x) = \lim_{\varepsilon\to 0^+} \int_0^{1-\varepsilon} \frac{dt}{\ln t} + \int_{1+\varepsilon}^x \frac{dt}{\ln t}.$$

) Zaujímavé je spomenúť, že funkcia $\mathrm{li}(x)$ dáva pre „malé“ hodnoty $x$ skutočne veľmi presné odhady pre $\pi(x)$.

Je zrejmé, že $\frac{\mathrm{li}(x)}{\mathrm{Li}(x)} \to 1$. Ak ukážeme, že $\frac{Li(x)}{x/\ln x} \to 1$, tak z toho vyplynie, že ekvivalentné formulácie prvočíselnej vety sú

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1 \qquad \text{a} \qquad \lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1.$$

**Tvrdenie 2.3.8.**

$$\lim_{x\to\infty} \frac{\mathrm{Li}(x)}{x/\ln x} = 1$$

*Dôkaz.* Obe funkcie, $\mathrm{Li}(x)$ aj $\frac{x}{\ln x}$ rastú do $+\infty$. Preto môžeme použiť L'Hospitalove pravidlo a dostaneme

$$\lim_{x\to\infty} \frac{\mathrm{Li}(x)}{\frac{x}{\ln x}} = \lim_{x\to\infty} \frac{\mathrm{Li}'(x)}{\left(\frac{x}{\ln x}\right)'} = \lim_{x\to\infty} \frac{\frac{1}{\ln x}}{\frac{\ln x - 1}{\ln^2 x}} = 1.$$

□

Dlho sa verilo (na základe numerických výpočtov), že platí nerovnosť $\mathrm{li}(x) < \pi(x)$. Až v roku 1914 dokázal J. E. Littlewood, že funkcia $\pi(x) - \mathrm{li}(x)$ má nekonečne veľa znamienkových zmien. Neskôr E. Skewes dokázal, že prvá znamienková zmena sa vyskytne najneskôr pri čísel $10^{10^{10^{1000}}}$. Postupne sa podarilo nájsť aj podstatne menšie ohraničenia, stále však ide o obrovské čísla. Zaujímavý je fakt, že aj takéto obrovské čísla sa môžu vyskytnúť s určitým matematickým významom.

### 2.3.4 Čebyševove nerovnosti

Cieľom tejto časti je dokázať Čebyševovu vetu, ktorá je o niečo slabší výsledok, než prvočíselná veta.

{rozloz:VTCEBY}

**Veta 2.3.9 (Čebyševove nerovnosti).** *Existujú také reálne kladné konštanty $c_1, c_2$, že pre všetky $x \geq 2$ platí*

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}.$$



V tejto časti bude platiť dohoda, že vždy keď vytvárame sumu alebo súčin a sčitujeme alebo násobíme všetky $p$ z daného rozsahu, tak $p$ predstavuje iba prvočísla. (Čiže ide o sumu alebo súčin len cez prvočísla patriace do tohto rozsahu.)

{rozloz:SUCINPRIME}

**Lema 2.3.10.** *Pre každé reálne číslo $x \geq 2$ platí*

$$\prod_{p\leq x} p < 4^x,$$

*pričom uvedený súčin berieme cez všetky prvočísla $p$ nepresahujúce $x$.*

*Dôkaz.* Najprv si všimnime, že stačí dokazovať lemu pre prirodzené čísla $n \geq 2$. Ak totiž lema platí pre každé prirodzené číslo, tak pre reálne číslo $x \geq 2$ dostaneme

$$\prod_{p\leq x} p = \prod_{p\leq \lfloor x\rfloor} p < 4^{\lfloor x\rfloor} \leq 4^x.$$

Pre prirodzené čísla $n \geq 2$ dokážeme tvrdenie lemy matematickou indukciou, pričom budeme rozlišovať dva prípady - keď $n$ je párne a keď $n$ je nepárne. Pre $n = 2$ tvrdenie platí. Predpokladajme teraz, že platí pre všetky čísla menšie ako $n$.

Ak $n = 2k$ pre nejaké prirodzené číslo $k > 1$, tak $n$ nie je prvočíslo, čiže platí

$$\prod_{p\leq 2k} p = \prod_{p\leq 2k-1} p < 4^{2k-1} < 4^{2k}.$$

Ak $n = 2k + 1$, tak platí

$$\prod_{p\leq 2k+1} p = \prod_{p\leq k+1} p \prod_{k+1<p\leq 2k+1} p < 4^{k+1} \prod_{k<p\leq 2k+1} p.$$

Kombinačné číslo

$$\binom{2k+1}{k+1} = \frac{(2k+1)\cdot(2k)\cdots(k+2)}{1\cdot 2\cdots k}$$

je deliteľné každým prvočíslom $p$, pre ktoré $k + 1 < p \leq 2k + 1$. (Takéto prvočísla delia čitateľ ale nedelia menovateľ uvedeného zlomku.) Preto platí $\prod_{k+1<p\leq 2k+1} p \leq \binom{2k+1}{k+1}$. Tento binomický koeficient môžeme ľahko odhadnúť na základe nerovnosti

$$2^{2k+1} > \binom{2k+1}{k+1} + \binom{2k+1}{k} = 2\binom{2k+1}{k+1},$$

z ktorej dostaneme

$$\prod_{k+1<p\leq 2k+1} p \leq \binom{2k+1}{k+1} < 2^{2k} = 4^k.$$

Celkovo teda dostávame, že $\prod_{p\leq 2k+1} p < 4^{k+1}\cdot 4^k = 4^{2k+1}$. □

{rozloz:ODHADPI}

**Veta 2.3.11.** *Pre každé dostatočne veľké číslo $n$ platí*

$$\pi(n) \leq \frac{5n}{\lg n}.$$

*Dôkaz.* V dôkaze odhadneme zhora aj zdola výraz $\sum_{p\le n} \lg p$.

$$\sum_{p\le n} \lg p \ge \sum_{\sqrt{n}<p\le n} \lg p \ge \sum_{\sqrt{n}<p\le n} \lg\sqrt{n} = (\pi(n)-\pi(\sqrt{n}))\lg\sqrt{n} = (\pi(n)-\pi(\sqrt{n}))\frac{\lg n}{2}$$

Z lemy 2.3.10 dostaneme

$$\sum_{p\le n} \lg p = \lg\left(\prod_{p\le n} p\right) < 2n.$$

Spojením týchto dvoch nerovností dostaneme $\pi(n) \le \frac{4n}{\lg n} + \pi(\sqrt{n}) \le \frac{4n}{\lg n} + \sqrt{n}$. Pre dostatočne veľké $n$ platí $\sqrt{n} \le \frac{n}{\lg n}$, z čoho vyplýva

$$\pi(n) \le \frac{5n}{\lg n}.$$

□

Pre ľubovoľné kladné číslo $n$ označme $d_n = [1, 2, \ldots, n]$ najmenší spoločný násobok prvých $n$ prirodzených čísel. Nasledujúci dôkaz dolného odhadu pre $\pi(n)$ je z článku [Nai].

{rozloz:LMNSN}

**Lema 2.3.12.** *Pre každé kladné číslo $n$ platí $d_n \ge 2^{n-2}$.*

*Dôkaz.* Označme $I := \int_0^1 x^m(1-x)^m dx$. Pre každé $x \in (0,1)$ platí $0 < x(1-x) = \frac{1}{4} - (x-\frac{1}{2})^2 \le \frac{1}{4}$, z čoho vyplýva $0 < I \le \frac{1}{4^m}$.

Súčasne platí

$$I = \int_0^1 \sum_{k=0}^{m} x^{m+k}\binom{m}{k}(-1)^k dx = \sum_{k=0}^{m}\binom{m}{k}(-1)^k \int_0^1 x^{m+k}dx = \sum_{k=0}^{m}(-1)^k\binom{m}{k}\frac{1}{m+k+1}.$$

Po úprave na spoločného menovateľ dostaneme zlomok, ktorého menovateľ je najviac $d_{2m+1}$, pretože $d_{2m+1}$ je najmenší spoločný násobok všetkých zlomkov, ktoré vystupujú v súčte. Môžeme teda uvedený integrál vyjadriť v tvare $I = \frac{A}{d_{2m+1}}$, kde $A > 0$ je prirodzené číslo. Potom platí pre $n = 2m+1$

$$d_n = d_{2m+1} \ge 4^m = 2^{n-1}.$$

Ak $n$ je párne, tak platí $d_n \ge d_{n-1} \ge 2^{n-2}$. □

{rozloz:VTPIDOLNY}

**Veta 2.3.13.** *Pre každé kladné číslo $n$ platí*

$$\pi(n) \ge \frac{n-2}{\lg n}.$$

*Dôkaz.* Nech $p_1, \ldots, p_k$ sú všetky prvočísla, ktoré sú menšie alebo rovné $n$. Každé číslo $m = 1, \ldots, n$ má rozklad tvaru

$$m = \prod_{i=1}^{k} p_i^{s_{m_i}},$$

kde $s_{m_i} \ge 0$ pre všetky $i = 1, \ldots, k$. Potom najmenší spoločný násobok $d_n$ čísel $1, 2, \ldots, n$ má tvar

$$d_n = \prod_{i=1}^{k} p_i^{\max\{s_{1_i}, \ldots, s_{n_i}\}}$$

(cvičenie 9 v časti 2.1).

Zrejme platí $p_i^{\max\{s_{1_i},\ldots,s_{n_i}\}} \le n$ pre každé $i = 1, \ldots, k$. Z toho vyplýva, že $d_n \le n^k = n^{\pi(n)}$. Z toho dostaneme podľa lemy 2.3.12 $\pi(n) \ge \frac{\lg d_n}{\lg n} \ge \frac{n-2}{\lg n}$. □



Z viet 2.3.11 a 2.3.13 už vyplývajú obe Čebyševove nerovnosti.

**Dôsledok 2.3.14.** *Nech $p_n$ označuje $n$-té prvočíslo. Potom existujú reálne čísla $0 < a < b$ také, že*

$$an\ln n < p_n < bn\ln n$$

*pre každé $n \ge 2$.*

*Dôkaz.* Podľa vety 2.3.9 existujú reálne kladné konštanty $c_1, c_2$, že $c_1\frac{x}{\ln x} \le \pi(x) \le c_2\frac{x}{\ln x}$. Položme $x = p_n$. Potom $\pi(x) = n$ a máme

$$n\ln n < n\ln p_n \le c_2 p_n,$$

pre $a = \frac{1}{c_2}$ teda platí ľavá nerovnosť.

Súčasne $n = \pi(p_n) > c_1\frac{p_n}{\ln p_n}$. Pretože $\lim_{x\to\infty}\frac{\ln x}{\sqrt{x}} = 0$, pre dostatočne veľké $n$ máme

$$\frac{\ln p_n}{\sqrt{p_n}} < c_1.$$

Pre dosť veľké $n$ teda platí $\sqrt{p_n} < n$, z čoho vyplýva $p_n < n^2$ a $\ln p_n < 2\ln n$, a teda

$$p_n < \frac{1}{c_1} n\ln p_n < \frac{2}{c_1} n\ln n.$$

Vhodnou voľbou konštanty $b$ vieme dosiahnuť, aby táto nerovnosť platila pre každé $n \ge 2$. □

Poznamenajme, že je známe, že dokonca platí presnejší odhad

$$n\ln n + n\ln\ln n - n < p_n < n\ln n + n\ln\ln n$$

pre všetky $n \ge 6$.

Ďalšou dôležitou funkciou v teórii čísel je *Čebyševova funkcia* $\vartheta(x)$, ktorá je definovaná ako

$$\vartheta(x) = \sum_{p\le x} \ln p.$$

Podľa dohody na začiatku tejto časti uvedenú sumu berieme len cez prvočísla z daného rozsahu. (Všimnite si, že podobnú funkciu sme použili v dôkaze vety 2.3.11).

Nasledujúca veta zachytáva vzťah medzi funkciami $\pi(x)$ a $\vartheta(x)$.

{rozloz:VTTHEPI}

**Veta 2.3.15.**

$$\pi(x) \sim \frac{\vartheta(x)}{\ln x}$$

*Dôkaz.* Zrejme $\vartheta(x) = \sum_{p\le x} \ln p \le \sum_{p\le x} \ln x = \pi(x)\ln x$. Z toho dostaneme, že

$$\frac{\vartheta(x)}{\pi(x)\ln x} \le 1.$$

Majme teraz $x \ge 2$ a $0 < \varepsilon < 1$. Potom platí

$$\vartheta(x) \ge \sum_{x^{1-\varepsilon}<p\le x} \ln p \ge (1-\varepsilon)\ln x(\pi(x) - \pi(x^{1-\varepsilon})) \ge (1-\varepsilon)\ln x(\pi(x) - x^{1-\varepsilon}).$$

Z toho dostaneme (podľa vety 2.3.9)

$$\frac{\vartheta(x)}{\pi(x)\ln x} \geq (1-\varepsilon)\left(1-\frac{x^{1-\varepsilon}}{\pi(x)}\right) \geq (1-\varepsilon)\left(1-\frac{x^{1-\varepsilon}\ln x}{c_2 x}\right).$$

Ak urobíme limitu pre $x$ idúce do nekonečna, tak máme

$$\liminf_{x\to\infty} \frac{\vartheta(x)}{\pi(x)\ln x} \geq 1-\varepsilon.$$

Pretože $\varepsilon$ môžeme zvoliť ľubovoľne malé, platí potom

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

□ {rozloz:DOSTHETA}

**Dôsledok 2.3.16.** *Existujú také reálne konštanty $A, B > 0$, že pre všetky $x \geq 2$ platí*

$$Ax \leq \vartheta(x) = \sum_{p\leq x} \ln p \leq Bx.$$

Súčasne nám veta 2.3.15 dáva ekvivalentnú formuláciu prvočíselnej vety:

$$\vartheta(x) \sim x.$$

### 2.3.5 Bertrandov postulát

V tejto časti ukážeme nasledujúcu vetu {rozloz:VTBERTRAND}

**Veta 2.3.17 (Bertrandov postulát).** *Pre každé $n \in \mathbb{N}$ existuje prvočíslo $p$ také, že*

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

Túto vetu dokázal P. Čebyšev, nazýva sa však na počet J. Bertranda, ktorý ju overil pre $n < 3\,000\,000$ a vyslovil ju ako hypotézu. Dôkaz, ktorý tu uvádzame, je z knihy M. Aigner, G. M. Ziegler: Proofs from THE BOOK [AZ]. Táto kniha je venovaná pamiatke P. Erdösa, jedného z najväčších matematikov minulého storočia.

P. Erdös zvykol hovorievať, keď sa mu podaril veľmi elegantný dôkaz: „Tento je z Knihy.“ Tvrdil totiž že Boh má pri sebe Knihu – The Book – v ktorej má napísané tie najelegantnejšie dôkazy matematických viet. V súvislosti s ňou je známy aj iný Erdösov výrok: „Nemusíte veriť v Boha, ale mali by ste veriť v Knihu.“

Pred dôkazom Bertrandovho postulátu uvedieme jednu pomocnú vetu.

**Veta 2.3.18.** *Prvočíslo $p$ sa v kanonickom rozklad čísla $n!$ vyskytuje v mocnine rovnej*

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

*Dôkaz.* Z čísel $1, 2, \ldots, n$ sa $p$ vyskytne ako faktor v $\lfloor \frac{n}{p} \rfloor$ číslach, v aspoň druhej mocnine sa vyskytne práve v $\lfloor \frac{n}{p^2} \rfloor$ číslach, atď. Celkove teda dostávame $\sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$ výskytov prvočísla $p$. □



Uvedená suma je v skutočnosti konečná – od istého $k$ budú členy $\lfloor \frac{n}{p^k} \rfloor$ nulové.

Napríklad číslo $n = 10!$ môžeme zapísať v tvare $10! = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}$, kde
$\alpha_1 = \lfloor \frac{10}{2} \rfloor + \lfloor \frac{10}{4} \rfloor + \lfloor \frac{10}{8} \rfloor = 5 + 2 + 1 = 8$,
$\alpha_2 = \lfloor \frac{10}{3} \rfloor + \lfloor \frac{10}{9} \rfloor = 3 + 1 = 4$,
$\alpha_3 = \lfloor \frac{10}{5} \rfloor = 2$ a
$\alpha_4 = \lfloor \frac{10}{7} \rfloor$=1.

*Dôkaz vety 2.3.17.* Dôkaz spočíva v tom, že z predpokladu, že medzi $n$ a $2n$ nie sú prvočísla, dostaneme odhad hodnoty kombinačného čísla $\binom{2n}{n}$. Ukážeme, že od určitého $n$ tento odhad neplatí. Pre menšie $n$ tvrdenie vety overíme priamo.

Predpokladajme teda, že $n$ je také prirodzené číslo, že neexistuje prvočíslo $p$, $n < p \leq 2n$.

Označme ako $r(p, n)$ mocninu v akej sa vyskytuje prvočíslo $r$ v kanonickom rozklade čísla $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. Pretože predpokladáme, že medzi $n$ a $2n$ nie sú žiadne prvočísla, dostávame rovnosť

$$\binom{2n}{n} = \prod_{p\leq n} p^{r(p,n)}. \tag{2.1}$$ {rozloz:EQBINOM}

Podľa predchádzajúcej vety je

$$r(p,n) = \sum_{j=1}^{\infty} \left( \left\lfloor \frac{2n}{p^j} \right\rfloor - 2\left\lfloor \frac{n}{p^j} \right\rfloor \right). \tag{2.2}$$ {rozloz:EQPRN}

Sčítance vystupujúce v tomto súčte môžu nadobúdať iba hodnoty 0 a 1 (lema 1.3.3) a pre $p^j > 2n$ sú nulové.

Z toho vyplýva, že pre $p > \sqrt{2n}$ máme $r(p, n) = \lfloor \frac{2n}{p} \rfloor - 2\lfloor \frac{n}{p} \rfloor$.

Ďalej ak $n > p > \frac{2}{3}n$, čiže $\frac{3}{2} > \frac{n}{p} > 1$, tak $\lfloor \frac{2n}{p} \rfloor - 2\lfloor \frac{n}{p} \rfloor = 0$.

Pre $n > \frac{9}{2}$ máme $\frac{2}{3}n > \sqrt{2n}$.

Vidíme teda, že pre $p > \frac{2}{3}n$ je $r(p, n) = 0$.

Pre prvočísla také, že $\sqrt{2n} \leq p < \frac{2}{3}n$ je $r(p, n) \leq 1$. Podľa lemy 2.3.10 potom dostaneme

$$\prod_{\sqrt{2n}\leq p<\frac{2}{3}n} p^{r(p,n)} \leq \prod_{p<\frac{2}{3}n} p < 4^{\frac{2}{3}n}.$$

Ďalej si uvedomme, že pre všetky prvočísla vystupujúce v kanonickom rozklade $\binom{2n}{n}$ musí platiť $p^{r(p,n)} \leq 2n$. (Stačí si všimnúť, že sčítance v (2.2) sú nulové pre všetky $j$ také, že $p^j > 2n$, čiže $r(p, n) \leq \max\{j; p^j \leq 2n\}$.) Čiže prvočísla veľkosti najviac $\sqrt{2n}$ neprispejú k súčinu (2.1) väčšou hodnotou než $(2n)^{\sqrt{2n}}$. Z (2.1) dostaneme potom horný odhad

$$\binom{2n}{n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}.$$

Teraz sa pokúsime $\binom{2n}{n}$ odhadnúť zdola. Všimnime si, že v binomickom rozvoji $(1+1)^{2n}$ je $\binom{2n}{n}$ najväčší koeficient. Pretože tento rozvoj má $2n+1$ koeficientov, dostaneme $\binom{2n}{n} \geq \frac{4^n}{2n+1}$. Ak si všimneme, že $\binom{2n}{n}$ je pre $n \geq 1$ aspoň tak veľký ako súčet $\binom{2n}{0} + \binom{2n}{1} = 2$ dvoch najmenších koeficientov, môžeme tento odhad o kúsok vylepšiť:

$$\binom{2n}{n} \geq \frac{4^n}{2n}.$$

Dostávame teda nerovnosti

$$(2n)^{\sqrt{2n}} 4^{\frac{2}{3}n} \geq \frac{4^n}{2n}$$
$$(2n)^{\sqrt{2n}+1} \geq 4^{\frac{n}{3}} \tag{2.3}$$ {rozloz:INEQBERT}

Posledná nerovnosť je ekvivalentná s nerovnosťou $(\sqrt{2n}+1)(\lg n + 1) \geq \frac{2n}{3}$. Pretože podiel ľavej a pravej strany konverguje k 0, od istého $n$ táto nerovnosť neplatí. My však potrebujeme ešte nájsť nejaké dostatočne veľké $n$ také, že pre väčšie $n$ už táto nerovnosť neplatí (a pre ne teda dostávame želaný spor) a overiť, že pre menšie $n$ je tiež Bertrandov postulát splnený.

To môžeme urobiť nasledovným spôsobom. Použitím nerovnosti $a + 1 < 2^a$ (ktorá platí pre $a \geq 2$) dostaneme

$$2n = (\sqrt[6]{2n})^6 < (\lfloor \sqrt[6]{2n} \rfloor + 1)^6 \leq 2^{6\lfloor \sqrt[6]{2n} \rfloor}. \tag{2.4}$$ {rozloz:INEQBERT2}

Z nerovností (2.3) a (2.4) dostaneme

$$2^{2n} \leq (2n)^{3(\sqrt{2n}+1)} < 2^{\lfloor \sqrt[6]{2n} \rfloor (18\sqrt{2n}+18)}.$$

Pre $n \geq 50$ máme $\sqrt{2n} \geq 10$, čiže $18\sqrt{2n} + 18 < 20\sqrt{2n}$.

$$2^{2n} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}}$$

Táto nerovnosť môže byť splnená iba ak $(2n)^{\frac{1}{3}} < 20$, $2n < 8000$, $n < 4000$.

Aby sme overili Bertrandov postulát pre $n < 4000$, stačí overiť

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

sú prvočísla také, že nasledujúce je vždy menšie než dvojnásobok predchádzajúceho. □

**Cvičenia**

1. Existuje v každej aritmetickej postupnosti ľubovoľný počet po sebe idúcich zložených čísel?
2. Aká je najväčšia možná dĺžka postupnosti po sebe idúcich čísel bez kvadratických deliteľov? Nájdite príklad takej postupnosti. Riešte podobnú úlohu pre prípad tretích mocnín.
3. Konverguje rad $\sum_{p\in\mathbb{P}} \frac{1}{p^2}$?
4. Zistite, či rad $\sum_{p\in\mathbb{P}} \left(e^{\frac{1}{p}} - 1\right)$ konverguje alebo diverguje.
5. Dokážte, že $\lim_{k\to\infty} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = 0$. {rozlozcvic:CESARO}
6. Dokážte, že ak $\lim_{n\to\infty} x_n = L$ a $y_n = \frac{x_1+\ldots+x_n}{n}$ je postupnosť aritmetických priemerov čísel $x_n$, tak $\lim_{n\to\infty} y_n = L$.
7. Dokážte, že funkcia $\frac{n}{\pi(n)}$ nadobúda všetky celočíselné hodnoty väčšie ako 1.
8. Dokážte, že 5 je jediné prvočíslo, ktoré je súčtom všetkých od neho menších prvočísel.



9. Nech $a$ je maximálny exponent taký, že $p^a \mid n$. Dokážte, že $p \nmid \binom{n}{p^a}$.
10. Dokážte $\prod_{p\leq n} p \geq n$ pre $n \in \mathbb{N}$, $n \neq 1$.
11. Dokážte, že $n!$ nie je štvorec prirodzeného čísla pre žiadne $n > 1$.

## 2.4 Prvočísla špeciálneho tvaru

### 2.4.1 Prvočísla v aritmetických postupnostiach

Najprv si dokážeme jedno veľmi jednoduché tvrdenie, ktorého dôkaz do istej miery pripomína Euklidov dôkaz o nekonečnosti množiny $\mathbb{P}$.

**Tvrdenie 2.4.1.** *Existuje nekonečne veľa prvočísel tvaru $4k+3$.*

*Dôkaz.* Sporom.

Všetky prvočísla väčšie ako 2 sú tvaru $4k+1$ alebo $4k+3$. Predpokladajme, že by existoval iba konečný počet prvočísel tvaru $4k+3$. Nech teda $p_n$ je najväčšie prvočíslo takéhoto tvaru. Položme $N = 4p_3 \ldots p_n + 3$, kde $p_k$ označuje $k$-te prvočíslo, t.j. $p_1 = 2$, $p_2 = 3$, atď.

Zrejme $N > p_n$ a $(N, p_k) = (4p_3 \ldots p_n + 3, p_k) = (3, p_k) = 1$ pre $k > 2$, $k \leq n$. Súčasne $(N, 3) = (4p_3 \ldots p_n, 3) = 1$ a $N$ je nepárne. Teda $N$ nie je deliteľné žiadnym prvočíslom menším ako $p_n$. Ak $N$ je zložené, tak musí byť súčinom prvočísel väčších ako $p_n$, z nich každé má tvar $4k+1$. Všimnime si, že súčin ľubovoľného počtu takýchto čísel dáva po delení 4 opäť zvyšok 1, $(4k+1)(4l+1) = 4(4kl+k+l)+1$. To znamená, že číslo $N$ nemôžeme dostať takýmto spôsobom. □

V predchádzajúcom dôkaze sme využili úvahu, že súčin 2 čísel, ktoré majú po delení 4 zvyšok 1, dáva po delení 4 opäť zvyšok 1. V ďalšej kapitole sa budeme zaoberať kongruenciami, ktoré umožňujú elegantnejší a prehľadnejší zápis podobných úvah.

Bez dôkazu spomenieme nasledujúci výsledok.

**Veta 2.4.2 (Dirichletova veta).** *Nech $a, d \in \mathbb{N}$, $(a, d) = 1$. Potom v aritmetickej postupnosti $a + nd$ existuje nekonečne veľa prvočísel.*

V súvislosti s uvedenou vetou je možné pýtať sa na prvočísla vyjadriteľné pomocou kvadratických, kubických polynómov atď. O tejto problematike je dodnes známe veľmi málo, nevie sa napríklad, či existuje nekonečne veľa prvočísel tvaru $k^2 + 1$ alebo tvaru $k^2 + k + 1$.

Dirichletova veta samozrejme nehovorí o tom, že prvočísla v danej aritmetickej postupnosti nasledujú tesne po sebe. O aritmetických postupnostiach prvočísel sme už hovorili v súvislosti s výsledkom B. Greena a T. Taa [GT].

### 2.4.2 Ďalšie typy prvočísel a niektoré známe otvorené problémy

**Prvočíselné dvojčatá**

Ak $p$ aj $p+2$ sú prvočísla, hovoríme, že sú to *prvočíselné dvojčatá*. Dodnes nie je známe, či ich existuje nekonečne veľa. Je však známe, že aj ak by ich bolo nekonečne veľa, tak ich prevrátený rad konverguje, čiže ich je v istom zmysle podstatne menej ako všetkých prvočísel. Tento fakt dokázal nórsky matematik V. Brun, súčet prevráteného radu prvočíselných dvojčiat

$$B_2 := \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \left(\frac{1}{29} + \frac{1}{31}\right) + \ldots$$

sa nazýva *Brunova konštanta.*

Uvedený rad konverguje veľmi pomaly, preto je ťažké numericky odhadnúť Brunovu konštantu. Dnes je známe iba to, že $1,82 < B_2 < 2,15$. Práve pri snahe numericky vyrátať Brunovu konštantu odhalil T. R. Nicely známu chybu procesora Pentium pri aritmetike s desatinnou čiarkou.

Snáď najväčším priblížením k dokázaniu hypotézy o prvočíselných dvojčatách je výsledok, že existuje nekonečne veľa takých prvočísel $p$, že $p+2$ je súčin najviac 2 prvočísel.

### Fermatove čísla

**Definícia 2.4.3.** *Fermatove čísla* sú čísla tvaru $F_n = 2^{2^n}+1$.

**Veta 2.4.4.** *Ľubovoľné dve Fermatove čísla sú nesúdeliteľné.*

*Dôkaz.* Uvažujme čísla $F_n = 2^{2^n}+1$ a $F_{n+k} = 2^{2^{n+k}} = (2^{2^n})^{2^k}+1$. Všimnime si, že $F_{n+k}-2 = (2^{2^n})^{2^k}-1 = (2^{2^n}+1)((2^{2^n})^{2^k-1}-(2^{2^n})^{2^k-2}+\ldots-1)$, čiže $F_n \mid F_{n+k}-2$.

Z toho vyplýva, že $(F_n, F_{n+k}) = (F_n, 2) = 1$. □

Dokázali sme, že ak $k \leq m$, tak $F_k \mid F_m - 2$. Indukciou sa dá overiť, že platí dokonca viac: $\prod_{k=0}^{m-1} F_k = F_m - 2$.

Predchádzajúcu vetu je možné využiť na iný dôkaz nekonečnosti množiny prvočísel. Každé číslo $F_m$ musí byť deliteľné nejakým prvočíslom $q_m$. Pretože Fermatove čísla sú po 2 nesúdeliteľné, pre rôzne čísla $m$ dostaneme rôzne prvočísla $q_m$. Teda prvočísel je nekonečne veľa.

P. de Fermat sa domnieval, že všetky takéto čísla sú prvočísla. L. Euler vyvrátil jeho hypotézu tým, že sa mu podarilo rozložiť číslo $F_5 = 2^{32}+1 = 4\,294\,967\,297 = 641.6700417$. Dodnes nie je známe, či existuje nekonečne veľa Fermatových prvočísel ani či existuje nekonečne veľa zložených Fermatových čísel.

Vzhľadom k tomu, že pre veľké $n$ je Fermatove číslo $F_n$ zložené je veľmi ťažké overiť túto hypotézu už pre malé $n$. V súčasnosti jediné známe Fermatove prvočísla sú $F_1$ až $F_4$. Je známe, že všetky ďalšie Fermatove čísla až po $F_{32}$ sú zložené.

Číslo $F_5$ je skutočne obrovské – ťažko si predstaviť overenie ručným výpočtom, či ide o prvočíslo. L. Euler však dokázal výsledok, z ktorého vyplývalo, že stačí overovať deliteľnosť číslami tvaru $64k+1$ a tak pomerne ľahko našiel deliteľa $641 = 64.10+1$. (Neskôr – v kapitole o kongruenciách – si ukážeme, ako možno deliteľnosť overovať bez toho, aby sme daným číslom museli deliť.)

Viacerí odborníci na históriu teórie čísel vyjadrili predpoklad, že Fermat poznal tento výsledok, preto je do istej miery prekvapivé, že sám neprišiel na neplatnosť svojej hypotézy.

Konkrétne, Euler ukázal, že ak prvočíslo $p$ je deliteľom čísla $F_m$, tak $p$ musí mať tvar $k2^{m+1}+1$ pre nejaké prirodzené číslo $k$. My tento fakt dokážeme neskôr ako vetu 3.3.11. Eulerov výsledok sa podarilo neskôr zlepšiť F. Lucasovi, ktorý dokázal, že také prvočíslo musí byť tvaru $k2^{m+2}+1$.

V súvislosti s Fermatovými číslami je veľmi zaujímavý výsledok C. F. Gaussa a P. Wantzela, že pravidelný $n$-uholník možno zostrojiť pomocou pravítka a kružidla práve vtedy, keď $n$ je súčin mocniny 2 a niekoľkých Fermatových prvočísel. Teda jediné „prvočíselnouholníky“, o ktorých vieme, že sú skonštruovateľné, sú $n$-uholníky pre $n$ =3, 5, 17, 257 a 65537.

### Mersennove čísla

Prvočísla tvaru $M_n = 2^n - 1$ sa nazývajú *Mersennove prvočísla.*[2] Ani o nich sa nevie, či ich existuje nekonečne veľa. Mersennove prvočísla spomenieme v nasledujúcej kapitole v súvislosti

[2] Marin Mersenne (1588–1648), francúzsky matematik, teológ a hudobný teoretik.



s dokonalými číslami.

Podobným spôsobom ako pre Fermatove čísla sa dá ukázať, že ľubovoľné 2 Mersennove čísla $M_n$ sú nesúdeliteľné.

{prvtvar:LMMERS}

**Lema 2.4.5.** *Ak $2^n-1$ je prvočíslo, tak $n$ je tiež prvočíslo.*

*Dôkaz.* Ak by $n$ bolo zložené číslo, čiže $n = m.k$ pre $1 < m, k < n$, tak $2^n-1 = (2^m)^k - 1 = (2^m-1)(1+2^m+\ldots+2^{m(k-1)})$. □

Nie všetky Mersennove čísla sú prvočísla. Neskôr ukážeme (tvrdenie 3.1.15), že ak $p$, $q$ sú prvočísla a $q \mid M_p = 2^p-1$, tak $p \mid q-1$. Skúsme využiť tento výsledok na hľadanie prvočíselných faktorov prvých Mersennových čísel.

{prvtvar:PRMERS}

**Príklad 2.4.6.** $2^2-1 = 3$, $2^3-1 = 7$, $2^5-1 = 31$ sú prvočísla.

V prípade $M_7 = 2^7-1 = 127$ musí pre prvočíselné faktory platiť $7 \mid q-1$, čiže stačí skúšať čísla tvaru $7k+1$. Čísla 8 a 15 nie sú prvočísla, tie teda ani skúšať nemusíme. Ďalej už nemusíme pokračovať, lebo $15^2 > 127$ (a každé zložené číslo $n$ má prvočíselný faktor veľkosti najviac $\sqrt{n}$).

Teraz preskúmajme $M_{11} = 2^{11}-1 = 2047$. V tomto prípade máme $11 \mid q-1$, čiže nás zaujímajú prvočísla tvaru $11k+1$. Priamym výpočtom zistíme, že už prvé také prvočíslo $23 = 2.11+1$ je deliteľom $M_{11}$ a platí $2^{11}-1 = 2047 = 23.89$.

Bez dôkazu uveďme nasledujúcu vetu, ktorá umožňuje dokázať ešte jednoduchším spôsobom, že niektoré Mersennove čísla sú zložené.

**Veta 2.4.7.** *Ak $p = 4k+3$ je prvočíslo, $k > 1$, tak $2p+1$ je prvočíslo práve vtedy, keď $2p+1 \mid M_p = 2^p-1$.*

Uvedená veta pochádza od L. Eulera. Dokázať ju možno použitím výsledkov o kvadratických zvyškoch. K nim sa dostaneme neskôr; uvedenú vetu dokážeme ako vetu 4.2.11.

### Prvočísla Sophie-Germainovej

V predchádzajúcej vete sa objavila podmienka, že $p$ aj $2p+1$ sú prvočísla. Takéto prvočísla sa vyskytli v súvislosti s viacerými problémami v teórii čísel. Tiež je s nimi spojených viacero otvorených otázok.

**Definícia 2.4.8.** Prvočíslo $p$ sa nazýva prvočíslo *Sophie-Germainovej* ak aj $2p+1$ je prvočíslo.

Nie je známe, či takých prvočísel je nekonečne veľa.[3]

### Cvičenia

1. Dokážte, že existuje nekonečne veľa prvočísel tvaru $6k+5$.
2. Dokážte, že pre prirodzené čísla $m \neq n$ platí $(M_m, M_n) = 1$, kde $M_k = 2^k-1$ je $k$-te Mersennove číslo. Ako z toho vyplýva nekonečnosť množiny všetkých prvočísel?
3. Ak je $2^n+1$ prvočíslo, tak $n = 2^m$ pre nejaké $m \in \mathbb{N}$.

[3] Prvočísla Sophie-Germainovej sa spomínajú vo filme Proof (2005).

# Kapitola 3

# Aritmetické funkcie

## 3.1 Kongruencie

### 3.1.1 Definícia a základné vlastnosti

Kongruencie sú veľmi elegantný prostriedok na zápis a dokazovanie niektorých faktov o deliteľnosti. Zápis pre kongruencie zaviedol C. F. Gauss.

**Definícia 3.1.1.** Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Hovoríme, že $a$ a $b$ sú *kongruentné modulo $n$,* ak $n \mid a - b$. Označenie: $a \equiv b \pmod{n}$.

Inými slovami, to že $a$ a $b$ sú kongruentné modulo $n$ znamená, že majú rovnaký zvyšok po delení číslom $n$. Napríklad $13 \equiv 1 \pmod 4$, $13 \equiv 8 \pmod 5$.

Teraz si ukážeme, že so zvyškami môžeme počítať rovnako ako s číslami – ibaže všetky operácie treba robiť modulo $n$. Inak povedané, s kongruenciami môžeme narábať do určitej miery podobne ako s rovnicami. Najprv však (bez dôkazu) uvedieme niektoré jednoduché vlastnosti kongruencií.

{kong:LMRELEKV}

**Lema 3.1.2.** *Nech $n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$.*

(i) $a \equiv a \pmod n$

(ii) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

(iii) $a \equiv b \pmod n \wedge b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$

Táto veta vlastne hovorí, že kongruencia modulo $n$ je relácia ekvivalencie.

**Definícia 3.1.3.** Triedy ekvivalencie zodpovedajúce relácii $a \equiv b \pmod n$ nazývame *zvyškové triedy modulo $n$.* Zvyškovú triedu čísla $k$ označujeme $\overline{k}$.

{kong:VTKOMPAT}

**Veta 3.1.4.** *Nech $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Nech $a \equiv b \pmod n$, $c \equiv d \pmod n$. Potom*

$$a + c \equiv b + d \pmod n,$$
$$ac \equiv bd \pmod n.$$

*Dôkaz.* Podľa predpokladov $n \mid a - b$ a $n \mid c - d$. Z toho dostaneme $n \mid (a + c) - (b + d) = (a - b) + (c - d)$ a $n \mid ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d)$. □



Predchádzajúca veta ukazuje, že operácie + a · sú kompatibilné s reláciou ≡. Preto súčet a súčin zvyškových tried dané nasledujúcimi vzťahmi sú dobre definované operácie.

$$\overline{a} + \overline{b} = \overline{a + b},$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Všimnime si, že množina zvyškových tried modulo $n$ tvorí grupu aj okruh s jednotkou. Je to vlastne okruh $(\mathbb{Z}_n, \oplus, \odot)$, ktorý dobre poznáte z algebry. Teda výpočty s kongruenciami sú vlastne spôsob zápisu výpočtov v tomto okruhu.

Z vety 3.1.4 môžeme ľahko indukciou odvodiť tieto dôsledky:

**Dôsledok 3.1.5.** *Ak $a_i \equiv b_i \pmod n$ pre všetky $i = 1, \dots k$, tak*

$$a_1 + \cdots + a_k \equiv b_1 + \cdots + b_k \pmod n,$$
$$a_1 \dots a_k \equiv b_1 \dots b_k \pmod n.$$

{kong:DOSPOLYN}

**Dôsledok 3.1.6.** *Ak $a \equiv b \pmod n$ pre nejaké $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, tak platí pre všetky $k \in \mathbb{N}$ aj kongruencia*

$$a^k \equiv b^k \pmod n.$$

*Ak $f$ je polynóm s celočíselnými koeficientmi, tak*

$$f(a) \equiv f(b) \pmod n.$$

{kong:PRIKLEULER}

**Príklad 3.1.7.** Ako sme spomenuli v súvislosti s Fermatovými číslami, L. Euler ukázal, že číslo $F_5 = 2^{32} + 1$ je zložené, konkrétne, ukázal, že $641 \mid F_5$. Práve kongruencie nám poskytujú prostriedok ako môžeme overiť tento fakt bez toho, aby sme museli deliť číslo $2^{32} + 1$ číslom 641. Stačí si uvedomiť, že dokazované tvrdenie je ekvivalentné s kongruenciou $2^{32} \equiv -1 \pmod{641}$.

Jednoduchým výpočtom dostaneme
$2^8 \equiv 256 \pmod{641}$
$2^{16} \equiv 256^2 = 64.4.256 = 1024.64 = 102.640 + 256 \equiv 256 - 102 \equiv 154 \pmod{641}$
$2^{32} \equiv 154^2 = 14^2.11^2 = 196.121 = (3.64 + 4)(2.64 - 7) = 6.64^2 + 8.64 - 21.64 - 28 = (384 + 8 - 21).64 - 28 = 371.64 - 28 = 37.640 + 64 - 28 \equiv -37 + 36 \equiv -1 \pmod{641}$

(Samozrejme, stačilo by v každom kroku umocniť predchádzajúci výsledok na druhú a urobiť zvyšok po delení 641. Výpočty, ktoré sme tu urobili, sú pokusom ukázať, ako by sme si mohli zjednodušiť prácu, keby sme to skutočne počítali ručne – tak ako kedysi Euler.)

{kong:PRMERS}

**Príklad 3.1.8.** V príklade 2.4.6 sme zistili, že $M_{11} = 2^{11} - 1$ je najmenšie zložené Mersennove číslo. Ukázali sme konkrétne, že $23 \mid M_{11}$. Pomocou použitia kongruencií môžeme ten istý fakt overiť nasledovne:
$2^4 = 16 \equiv -7 \pmod{23}$,
$2^8 \equiv (-7)^2 = 49 \equiv 3 \pmod{23}$,
$2^{11} = 2^8.2^3 \equiv 3.8 \equiv 24 \equiv 1 \pmod{23}$.

Videli sme, že kongruencie môžeme sčitovať, násobiť i umocňovať. Naskytá sa otázka, či môžeme krátiť číslom vyskytujúcim sa na oboch stranách kongruencie.

{kong:VTMN}

**Veta 3.1.9.** *Ak $(m, n) = 1$, tak existuje $u \in \mathbb{Z}$ také, že $um \equiv 1 \pmod n$.*

*Ak $(m, n) = 1$, tak pre ľubovoľné celé čísla $k, l$ platí implikácia $km \equiv lm \pmod n \Rightarrow k \equiv l \pmod n$.*

*Dôkaz.* Na základe vety 2.1.7 máme existenciu $u, v \in \mathbb{Z}$ takých, že $um + vn = 1$. To ale znamená, že $um \equiv 1 \pmod{n}$.

Na dôkaz druhej časti tvrdenia stačí kongruenciu $km \equiv lm \pmod{n}$ vynásobiť číslom $u$, ktorého existenciu sme ukázali v prvej časti. □

**Definícia 3.1.10.** Zvyškovú triedu modulo $n$ nazveme *redukovanou,* ak každý jej prvok je nesúdeliteľný s číslom $n$.

Z vety 3.1.9 a z lemy 2.1.11(ii) vyplýva, že

**Veta 3.1.11.** *Množina všetkých redukovaných zvyškových tried modulo $n$ tvorí grupu vzhľadom na násobenie.* {kong:VTREDGRUP}

Ak $n$ je prvočíslo, tak všetky zvyškové triedy sú redukované. V tom prípade je grupa z predchádzajúcej vety grupa $(\mathbb{Z}_n \setminus \{0\}, \odot)$.

Vetu 3.1.9 môžeme zovšeobecniť nasledovne:

**Veta 3.1.12.** *Ak $ac \equiv bc \pmod{n}$ a $d = (n, c)$, tak $a \equiv b \pmod{\frac{n}{d}}$.* {kong:VTMN2}

*Dôkaz.* Z toho, že $n \mid (a-b)c$ ľahko vyplýva $\frac{n}{d} \mid (a-b)\frac{c}{d}$. (Všimnite si, že $\frac{n}{d}$ aj $\frac{c}{d}$ sú celé čísla.)

Podľa lemy 2.1.11(v) máme $(\frac{n}{d}, \frac{c}{d}) = 1$, preto z Euklidovej lemy (lema 2.1.9) dostaneme $\frac{n}{d} \mid a - b$, čo znamená, že $a \equiv b \pmod{\frac{n}{d}}$. □

Uvedieme ešte niektoré jednoduché vlastnosti kongruencií.

**Tvrdenie 3.1.13.** *Ak $a \equiv b \pmod{n}$ a $m \mid n$, tak platí $a \equiv b \pmod{m}$.*

*Ak $a \equiv b \pmod{n}$ a $a \equiv b \pmod{m}$, kde $m$ a $n$ sú nesúdeliteľné, teda $(m, n) = 1$, tak $a \equiv b \pmod{mn}$.* {kong:TVRMMIDN}

*Dôkaz.* Keďže $m \mid n$ a $n \mid a - b$, z tranzitívnosti $m \mid a - b$.

Ak $n \mid a - b$ a $m \mid a - b$ pre nesúdeliteľné $m$, $n$, tak máme $mn \mid a - b$ z lemy 2.1.10. □

**Dôsledok 3.1.14.** *Ak platí $a \equiv b \pmod{m_i}$, pričom $m_i$, $i = 1, 2, \ldots, n$, sú po dvoch nesúdeliteľné, tak platí aj $a \equiv b \pmod{m}$, kde $m = m_1 \ldots m_n$.* {kong:DOSPOMCIN}

Fakt, že redukované zvyškové triedy tvoria grupu, nám často umožní výhodne použiť niektoré poznatky z teórie grúp na dôkaz teoreticko-číselných výsledkov. To budeme vidieť na viacerých miestach v tejto kapitole. Ako prvú ilustráciu môžeme dokázať nasledujúce tvrdenie o Mersennových číslach:

**Tvrdenie 3.1.15.** *Nech $p$, $q$ sú prvočísla a $q \mid M_p = 2^p - 1$. Potom $p \mid q - 1$.* {kong:TVRMERS}

*Dôkaz.* Podľa predpokladu platí $2^p \equiv 1 \pmod{q}$. To znamená, že rád čísla 2 v grupe $(\mathbb{Z}_q \setminus \{0\}, \odot)$ je deliteľ $p$; keďže $p$ je prvočíslo, tak rád čísla 2 je $p$. Podľa Lagrangeovej vety rád ľubovoľného prvku delí počet prvkov grupy, preto $p \mid q - 1$. □

### 3.1.2 Lineárne kongruencie

V tejto časti sa budeme zaoberať riešením *lineárnych kongruencií,* teda kongruencií tvaru

$$ax \equiv b \pmod{n},$$

kde $x$ je neznáma. (Nájsť riešenie znamená nájsť zvyškové triedy, ktorých prvky spĺňajú danú kongruenciu. Samozrejme, stačí nájsť jedného reprezentanta z každej triedy.)



**Veta 3.1.16.** *Kongruencia* {kong:VTLIN}

$$ax \equiv b \pmod{n} \tag{3.1}$$ {kong:LIN}

*má riešenie práve vtedy keď $d \mid b$, kde $d = (a, n)$.*

*Navyše, ak kongruencia* (3.1) *má riešenie, tak počet* (*navzájom nekongruentných*) *riešení je $d$. Ak $x_0$ je ľubovoľné riešenie* (3.1)*, tak všetky riešenia tejto kongruencie sú tvaru $x_0 + \frac{kn}{d}$.*

*Dôkaz.* $\boxed{\Rightarrow}$ Nech existuje riešenie $x$ kongruencie (3.1). Potom platí $b - ax = k.n$ pre nejaké $k \in \mathbb{Z}$, z čoho vyplýva $b = ax + kn$. Pretože $d$ je spoločným deliteľom $a$ a $n$, máme $d \mid ax + kn = b$.

$\boxed{\Leftarrow}$ Nech $d \mid b$, teda $b = cd$ pre vhodné $c \in \mathbb{Z}$. Podľa Bézoutovej identity (veta 2.1.7) existujú $u, v \in \mathbb{Z}$ také, že $d = au + nv$. Potom máme $b = acu + ncv$, čiže $acu \equiv b \pmod{n}$, teda $x = cu$ je riešením kongruencie (3.1).

Zostáva nám ukázať tvrdenie o počte riešení. Nech $x_0$ je nejaké riešenie tejto kongruencie. Tvrdíme, že potom všetky riešenia (3.1) sú tvaru $x_0 + \frac{kn}{d}$ pre nejaké $k \in \mathbb{Z}$. Najprv overíme, že čísla tohto tvaru sú skutočne riešeniami. Na to si stačí všimnúť, že

$$n \mid \frac{akn}{d} = \frac{a}{d}kn$$
$$a\left(x_0 + \frac{kn}{d}\right) = ax_0 + \frac{akn}{d} \equiv ax_0 \equiv b \pmod{n}.$$

Ďalej ukážeme, že každé riešenie musí mať uvedený tvar. Skutočne, ak $x$ je riešenie (3.1), tak platí $ax \equiv ax_0 \pmod{n}$ a podľa vety 3.1.12 $x \equiv x_0 \pmod{\frac{n}{d}}$. To znamená, že $x$ má tvar $x_0 + \frac{kn}{d}$ pre vhodné $k$.

Všimnime si, že čísla $x_0, x_0 + \frac{n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$ sú po dvoch nekongruentné modulo $n$ (pretože rozdiel ľubovoľnej dvojice z nich je menej ako $n$). Teda máme aspoň $d$ riešení.

Takisto však vidno, že každé riešenie je kongruentné s niektorým z uvedených $d$ riešení. Ak totiž $x = x_0 + \frac{kn}{d}$, kde $k = p.d + r$ a $0 \le r < d - 1$, tak rozdiel $x - (x_0 + \frac{rn}{d}) = \frac{pdn}{d} = pn$ je deliteľný číslom $n$, a teda $x \equiv x_0 + \frac{rn}{d} \pmod{n}$. □

Všimnime si, že dôkaz predchádzajúcej vety nám dáva súčasne návod na výpočet riešení. Ak kongruencia (3.1) má riešenie, tak jedno riešenie nájdeme pomocou Euklidovho algoritmu a ostatné pripočítaním vhodného násobku čísla $\frac{n}{d}$.

Uvedený postup ilustrujeme na jednoduchom príklade.

**Príklad 3.1.17.** Riešte kongruenciu $34x \equiv 60 \pmod{98}$.

Pretože $(34, 98) = 2 \mid 60$, podľa vety 3.1.16 má táto kongruencia 2 riešenia. Najprv, použitím Euklidovho algoritmu, vyjadríme 2 ako celočíselnú kombináciu 34 a 98.

$$\begin{aligned} 98 &= 2.34 + 30 & 30 &= 98 - 2.34 \\ 34 &= 1.30 + 4 & 4 &= 34 - 30 = 3.34 - 98 \\ 30 &= 7.4 + 2 & 2 &= 30 - 7.4 = 8.98 - 23.34 \end{aligned}$$

Zistili sme teda, že $34.(-23) \equiv 2 \pmod{98}$. Aby sme získali riešenie pôvodnej kongruencie, musíme túto kongruenciu vynásobiť 30. Použitím pozorovania, že $4.23 \equiv -6 \pmod{98}$ dostaneme $23.30 = 23.2 + 7.4.23 \equiv 46 - 7.6 \equiv 4 \pmod{98}$.

Riešením kongruencie je teda -4. Ďalšie riešenie dostaneme pripočítaním $\frac{98}{2} = 49$.

Riešenia uvedenej kongruencie sú teda $-4$ a 45.

### 3.1.3 Čínska veta o zvyškoch

Nasledujúca veta sa volá Čínska veta o zvyškoch pretože jej prvý známy výskyt je v knihe čínskeho matematika Sun Tzua. Existujú zovšeobecnenia tejto vety na okruhy a obory integrity. Tvrdenie vety, ktorú tu vedieme sa v niektorých učebniciach formuluje nie pomocou kongruencií ale pomocou homomorfizmov grúp (napríklad [HGK, Theorem 7.6.1]) alebo pomocou ideálov v okruhoch ([Ro, Theorem 1.10]). Istú okruhovo-teoretickú verziu tejto vety sa môžete naučiť na predmete počítačová algebra.

Táto veta hovorí o existencii riešenia niektorých systémov kongruencií. Uvedieme 2 dôkazy, oba z nich sú pomerne prirodzené. Jedna z myšlienok, ktorá napadne človeku pri riešení takejto úlohy, je vyskúšať všetky možnosti pre jednotlivé kongruencie. V prvom dôkaze pomocou Dirichletovho princípu ukážeme, že medzi nimi sa vyskytne aj možnosť, ktorá vyhovuje všetkým kongrueniám. Druhý dôkaz pekným spôsobom využíva princíp superpozície.

{kong:VTCHIN}

**Veta 3.1.18 (Čínska veta o zvyškoch).** *Nech $m_1, \dots, m_n$ sú po dvoch nesúdeliteľné čísla. Nech $b_1, \dots, b_n \in \mathbb{Z}$. Potom systém kongruencií*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

*má práve jedno riešenie modulo $m_1 \dots m_n$ (čiže existuje práve jedno $x \in \{0, 1, \dots, m_1 \dots m_n - 1\}$ spĺňajúce všetky uvedené kongruencie.)*

*Dôkaz.* Pre $n = 1$ tvrdenie zrejme platí - stačí položiť $x = b_1 \mod m_1$. Jednoznačnosť je takisto zrejmá.

Ukážeme, že tvrdenie platí pre $n = 2$. Chceme nájsť riešenie kongruencií

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned}$$

medzi číslami $0, 1, \dots, m_1 m_2 - 1$. Prvú z nich spĺňajú práve čísla tvaru $km_1 + b$, $k = 0, 1, \dots, m_2 - 1$.

Všimnime si, že žiadne 2 z týchto čísel nemajú rovnaký zvyšok po delení $m_2$. Ak totiž platí $km_1 + b \equiv lm_1 + b \pmod{m_2}$, tak $km_1 \equiv lm_1 \pmod{m_2}$ a z vety 3.1.9 dostaneme $k \equiv l \pmod{m_2}$. Pretože $k$ aj $l$ sú menšie ako $m_2$, musí už potom platiť $k = l$.

Máme teda $m_2$ riešení prvej kongruencie, ktoré majú rozličné zvyšky po delení $m_2$. Preto sa medzi zvyškami musí vyskytnúť aj číslo $b_2 \mod m_2$ (Dirichletov princíp). Teda daná sústava kongruencií má riešenie. Navyše, toto riešenie je jednoznačné (každý zvyšok sa vyskytne práve raz).

Predpokladajme teraz, že tvrdenie platí pre $n-1$. To znamená, že existuje jediné riešenie $x_0 \in \{0, 1, \dots, m_1 m_2 \dots m_{n-1} - 1\}$ kongruencií

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_{n-1} \pmod{m_{n-1}}. \end{aligned}$$



Inými slovami, uvedená sústava kongruencií je ekvivalentná jedinej kongruencii $x \equiv x_0 \pmod{m_1 \dots m_{n-1}}$.

Pôvodná sústava

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n}. \end{aligned}$$

je teda ekvivalentná sústave

$$\begin{aligned} x &\equiv x_0 \pmod{m_1 \dots m_{n-1}} \\ x &\equiv b_n \pmod{m_n}. \end{aligned}$$

Z predchádzajúcej časti dôkazu (prípad $n = 2$) už vieme, že táto sústava má jednoznačne určené riešenie. □

*Dôkaz. Existencia:* Označme $m := m_1 \dots m_n$ a $M_i := \frac{m}{m_i}$ pre $i = 1, 2, \dots, n$. Inak, položili sme $M_i = m_1 \dots m_{i-1} m_{i+1} \dots m_n$. Potom pre $i \neq j$ platí $m_j \mid M_i$ a $(m_i, M_i) = 1$. Podľa vety 3.1.16 kongruencia

$$M_i y \equiv 1 \pmod{m_i}$$

má riešenie pre každé $i$. Označme toto riešenie $c_i$. Teda $c_i$ je také číslo, že platí $c_i M_i \equiv 1 \pmod{m_i}$, a teda $c_i M_i b_i \equiv b_i \pmod{m_i}$.

Dostali sme zatiaľ

$$\begin{aligned} c_i M_i b_i &\equiv b_i \pmod{m_i} \\ c_i M_i b_i &\equiv 0 \pmod{m_j} \end{aligned}$$

pre všetky $j \neq i$. Teraz už stačí tieto riešenia „pospájať“.

Položme $x_0 := \sum_{i=1}^{n} c_i M_i b_i$. Z toho, že $c_i M_i b_i \equiv b_i \pmod{m_i}$ a $M_j \equiv 0 \pmod{m_i}$ pre $j \neq i$ dostaneme $x_0 \equiv b_i \pmod{m_i}$ pre všetky $i = 1, 2, \dots, n$. Teda takto zvolené $x_0$ je skutočne riešením danej sústavy.

*Jednoznačnosť:* Nech $x_1$ a $x_0$ sú dve riešenia danej sústavy, teda

$$x_1 \equiv x_0 \equiv b_i \pmod{m_i}.$$

Podľa dôsledku 3.1.14 potom platí $x_1 \equiv x_0 \pmod{m}$. □

V nasledujúcom príklade sa dá okamžite uhádnuť, že riešenie daného systému kongruencií je $x \equiv -1 \pmod{210}$. Aj napriek tomu si však, ako ilustráciu, ukážeme výpočet riešenia kongruencie postupom uvedeným v predchádzajúcom dôkaze.

**Príklad 3.1.19.** Riešme sústavu

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

Dostávame $M_1 = 3.5.7 = 105$, $M_2 = 2.5.7 = 70$, $M_3 = 2.3.7 = 42$, $M_4 = 2.3.5 = 30$. Vyriešme teraz kongruencie $M_i c_i \equiv 1 \pmod{m_i}$.
$105y \equiv 1 \pmod 2 \Leftrightarrow y \equiv 1 \pmod 2 \Rightarrow c_1 = 1$
$70y \equiv 1 \pmod 3 \Leftrightarrow y \equiv 1 \pmod 3 \Rightarrow c_2 = 1$
$42y \equiv 1 \pmod 5 \Leftrightarrow 2y \equiv 1 \pmod 5 \Leftrightarrow y \equiv 3 \pmod 5 \Rightarrow c_3 = 3$
$30y \equiv 1 \pmod 7 \Leftrightarrow 2y \equiv 1 \pmod 7 \Leftrightarrow y \equiv 4 \pmod 7 \Rightarrow c_4 = 4$

Riešením kongruencie je potom $x_0 = \sum_{i=1}^{4} c_i M_i b_i = 105 + 2.70 + 4.42.3 + 6.30.4 = 1469 \equiv 209 \pmod{210}$.

Iná možnosť riešenia je začať s prvou kongrueniou a výsledok vždy dosadiť do nasledujúcej. (Tento postup zodpovedá prvému z dôkazov, ktoré sme si uviedli.) Prvá kongruencia $x \equiv 1 \pmod 2$ znamená, že $x = 2k + 1$. Dosadením do nasledujúcej dostaneme:
$2k + 1 \equiv 2 \pmod 3 \Rightarrow 2k \equiv 1 \pmod 3 \Rightarrow k \equiv 2 \pmod 3 \Rightarrow k = 3l + 2 \Rightarrow x = 6l + 5$.
$6l + 5 \equiv 4 \pmod 5 \Rightarrow l \equiv 4 \pmod 5 \Rightarrow l = 5m + 4 \Rightarrow x = 30m + 29$.
$30m + 29 \equiv 6 \pmod 7 \Rightarrow 2m + 1 \equiv 6 \pmod 7 \Rightarrow 2m \equiv 5 \pmod 7 \Rightarrow m \equiv 6 \pmod 7 \Rightarrow m = 7n + 6 \Rightarrow x = 210m + 209$.

(Nepochybujem, že väčšina z vás si hneď po napísaní sústavy kongruencií všimla, že $-1$ je jej riešením. Na ukážku postupu pri riešení však stačí aj takýto očividný príklad.)

Čínska veta o zvyškoch sa vraj používala na počítanie vojakov v čínskej armáde, stačilo ich postupne nechať zoradiť do 5-stupu, 7-stupu atď. a keď sa takto zistili zvyšky po delení dosť veľkým počtom prvočísel, bol určený počet vojakov.

Z Čínskej vety o zvyškoch ľahko dostaneme nasledujúce zovšeobecnenie:

**Veta 3.1.20.** *Nech $m_1, \ldots, m_n$ sú po dvoch nesúdeliteľné čísla. Nech $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ a pre každé $k = 1, 2, \ldots, n$ platí $(a_k, m_k) = 1$. Potom systém kongruencií*

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}$$

*má práve jedno riešenie modulo $m_1 \ldots m_n$.*

*Dôkaz.* Podľa vety 3.1.9 ku každému $a_k$ existuje $a'_k$ tak, že $a_k a'_k \equiv 1 \pmod{m_k}$. Vynásobením každej kongruencie v sústave príslušným $a'_k$ dostaneme systém kongruencií, ktorý je ekvivalentný s pôvodným a má tvar ako systém vo vete 3.1.18, a teda má podľa tejto vety jediné riešenie modulo $m_1 \ldots m_n$. □

Ako aplikáciu Čínskej vety o zvyškoch môžeme uviesť nasledujúci výsledok:

**Veta 3.1.21.** *Nech $f(x)$ je polynóm s celočíselnými koeficientmi. Nech $m_1, \ldots, m_r \in \mathbb{N}$ sú po dvoch nesúdeliteľné a nech $M = m_1 \ldots m_r$. Potom kongruencia*

$$f(x) \equiv 0 \pmod{M} \qquad (3.2) \quad \{\texttt{kong:EQFM}\}$$

*má riešenie práve vtedy, keď každá z kongruencií*

$$f(x) \equiv 0 \pmod{m_k}, \qquad k = 1, \ldots, r \qquad (3.3) \quad \{\texttt{kong:EQFMK}\}$$

*má riešenie. Ak $v(m_k)$ označuje počet riešení kongruencie* (3.3)*, tak*

$$v(M) = v(m_1) v(m_2) \ldots v(m_k)$$

*je počet riešení kongruencie* (3.2)*.*



*Dôkaz.* Ak platí $f(a) \equiv 0 \pmod M$, tak platí aj kongruencia $f(a) \equiv 0 \pmod{m_k}$, lebo $m_k \mid M$ (tvrdenie 3.1.13).

Obrátene, ak pre každé $k = 1, 2, \ldots, r$ máme riešenie $a_k$ kongruencie (3.3), tak podľa Čínskej vety o zvyškoch existuje modulo $M$ jediné $a$ také, že $a \equiv a_k \pmod M$. Pre také $a$ platí $f(a) \equiv f(a_k) \pmod{m_k}$ (dôsledok 3.1.6) a $f(a) \equiv f(a_k) \pmod M$ (druhá časť tvrdenia 3.1.13).

Podľa Čínskej vety o zvyškoch máme jedno-jednoznačnú korešpondenciu medzi $n$-ticami $(a_1, \ldots, a_r)$ riešení kongruencií (3.3) a riešeniami $a$ kongruencie (3.2). Preto počet riešení $v(M)$ je súčinom počtov $v(m_k)$. □

**Cvičenia**

1. Dokážte lemu 3.1.2.
2. Dokážte, že pre ľubovoľné celé čísla $p$, $q$ je $p^5 q - p q^5$ deliteľné 5.
3. Nájdite všetky prirodzené čísla $n$, pre ktoré $2^n - 1$ je deliteľné 7.
4. Dokážte, že prirodzené číslo $n > 1$, ktorého desiatkový zápis pozostáva zo samých jednotiek, nemôže byť štvorcom prirodzeného čísla.
5. Nech $F_n$ označuje $n$-té Fibonacciho číslo (t.j. $F_n$ je určené rekurentným predpisom $F_{n+2} = F_{n+1} + F_n$ a počiatočnými hodnotami $F_0 = 0$, $F_1 = 1$.) Dokážte, že pre každé $m \in \mathbb{N}$ existuje nekonečne veľa čísel $n$ takých, že $F_n \equiv 0 \pmod m$; inak povedané $m \mid F_n$. (Hint: Pokúste sa pomocou Dirichletovho princípu dokázať, že postupnosť $F_n \bmod m$ sa bude cyklicky opakovať.)
6. Dokážte, že ak $a \equiv b \pmod{p^n}$, pre nejaké prvočíslo $p$, $n \in \mathbb{N}$ a $a, b \in \mathbb{Z}$, tak $a^p \equiv b^p \pmod{p^{n+1}}$.
7. Riešte lineárne kongruencie: a) $25x \equiv 4 \pmod{11}$; b) $16x \equiv 4 \pmod{12}$; c) $16x \equiv 4 \pmod{13}$.
8. Riešte sústavu kongruencií

$$\begin{aligned} 3x &\equiv 7 \pmod 5 \\ x &\equiv 1 \pmod 4 \\ 5x &\equiv 2 \pmod{11} \end{aligned}$$

9. Riešte sústavu kongruencií

$$\begin{aligned} 2x &\equiv 5 \pmod 7 \\ 4x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

10. Nájdite 5 po sebe idúcich prirodzených čísel takých, že prvé z nich je párne, ďalšie je deliteľné 3, tretie je deliteľné 5, štvrté je deliteľné 7 a piate je deliteľné 11.

## 3.2 Aritmetické funkcie, multiplikatívne funkcie

**Definícia 3.2.1.** *Aritmetickou funkciou* nazývame akúkoľvek funkciu $f\colon \mathbb{N} \to \mathbb{C}$ ($\mathbb{C}$ označuje množinu všetkých komplexných čísel).

Hovorím, že aritmetická funkcia $f$ je *multiplikatívna,* ak pre ľubovoľné $a, b \in \mathbb{N}$, $(a, b) = 1$ platí rovnosť

$$f(ab) = f(a)f(b)$$

a ak existuje $n \in \mathbb{N}$ také, že $f(n) \neq 0$.

Multiplikatívna funkcia je *úplne multiplikatívna,* ak táto rovnosť platí pre ľubovoľné $a, b \in \mathbb{N}$.

**Lema 3.2.2.** *Ak $f$ je multiplikatívna funkcia tak $f(1) = 1$.*

*Dôkaz.* Podľa definície multiplikatívnej funkcie existuje prirodzené číslo $n$ také, že $f(n) \neq 0$. Potom z rovnosti $f(n) = f(n.1) = f(n).f(1)$ dostaneme $f(1) = 1$. □

Ako najjednoduchšie príklady multiplikatívnych funkcií môžeme spomenúť konštantnú funkciu $f(1) = 1$ a identitu $f(n) = n$. Je zrejmé, že súčin 2 multiplikatívnych funkcií je opäť multiplikatívna funkcia.

Z dôsledku 2.1.14 vyplýva, že pre pevne zvolené $k \in \mathbb{N}$ je funkcia $f(n) = (n, k)$ multiplikatívna.

Nasledujúca lema je zrejmá priamo z definície multiplikatívnej funkcie.

{multip:LMKANON}

**Lema 3.2.3.** *Ak $f$ je multiplikatívna funkcia a $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla $n$, tak*

$$f(n) = f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \dots f(p_k^{\alpha_k}).$$

*Ak je navyše úplne multiplikatívna, tak*

$$f(p^\alpha) = f(p)^\alpha$$

*pre ľubovoľné $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$.*

{multip:LMSUMD}

**Lema 3.2.4.** *Ak $f$ je multiplikatívna funkcia, tak aj funkcia*

$$g(n) = \sum_{d|n} f(d)$$

*je multiplikatívna.*

*Dôkaz.* Platí $g(1) = f(1) \neq 0$, čiže máme zaručenú existenciu prirodzeného čísla, pre ktoré je hodnota $g$ nenulová.

Nech $m, n \in \mathbb{N}$ sú nesúdeliteľné; $(m, n) = 1$. Potom $g(m.n) = \sum_{d|mn} f(d)$. Podľa lemy 2.1.13 sa každé číslo $d$, ktoré delí $mn$, dá jednoznačne zapísať ako súčin $d_1.d_2$, kde $d_1 \mid m$ a $d_2 \mid n$. (Inak povedané, máme jednojednoznačnú korešpondenciu medzi deliteľmi $d$ čísla $mn$ a dvojicami čísel $d_1$, $d_2$ takými, že $d_1 \mid m$ a $d_2 \mid n$.) Zrejme $(d_1, d_2) = 1$, preto $f(d) = f(d_1d_2) = f(d_1)f(d_2)$. Potom ale dostávame

$$g(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1).f(d_2) = \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) = g(m)g(n).$$

□



Iná možnosť ako dokázať predchádzajúcu lemu je využiť cvičenie 3.

V tejto časti sa budeme ďalej zaoberať niektorými jednoduchými multiplikatívnymi funkciami.

**Definícia 3.2.5.** Nech $n \in \mathbb{N}$. Potom označíme ako

*(i)* $d(n)$ počet všetkých kladných deliteľov čísla $n$,

*(ii)* $\sigma(n)$ súčet všetkých kladných deliteľov čísla $n$.

Najprv ukážeme, že funkcie, ktoré sme práve zadefinovali sú multiplikatívne a nájdeme vyjadrenie $d(n)$ a $\sigma(n)$ pomocou kanonického rozkladu čísla $n$.

**Lema 3.2.6.** *Funkcie $d$ a $\sigma$ sú multiplikatívne.*

*Dôkaz.* Všimnime si, že platí $d(n) = \sum_{k|n} 1$. Funkcia $f(n) = 1$ je multiplikatívna, preto podľa lemy 3.2.4 je aj funkcia $d$ multiplikatívna.

Ďalej platí $\sigma(n) = \sum_{k|n} k$ a opäť z lemy 3.2.4 máme, že $\sigma$ je multiplikatívna funkcia. □

{multip:SIGMAKANON}

**Veta 3.2.7.** *Nech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla $n$. Potom*

$$d(n) = (\alpha_1 + 1) \dots (\alpha_k + 1),$$
$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

*Dôkaz.* Podľa lemy 3.2.3 stačí overiť tieto vzorce pre čísla tvaru $n = p^\alpha$, kde $p$ je prvočíslo. Všetky kladné delitele čísla $p^\alpha$ sú $1, p, p^2, \dots, p^\alpha$.

Teda $d(p^\alpha) = \alpha + 1$ a $\sigma(p^\alpha) = 1 + p + \dots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$. □

Môžete si tiež všimnúť, že tieto vzorce takisto vyplývajú z cvičenia 3.

Pomocou funkcie $\sigma$ môžeme definovať pojem dokonalého čísla.

**Definícia 3.2.8.** Hovoríme, že prirodzené číslo $n$ je *dokonalé* (alebo tiež *perfektné*) číslo, ak $\sigma(n) = 2n$.

Inými slovami, $n$ je dokonalé ak sa rovná súčtu svojich vlastných deliteľov.

Dodnes nie je známe, či existuje nepárne dokonalé číslo. Párne dokonalé čísla sa dajú charakterizovať pomocou *Mersennových prvočísel* tvaru $2^p - 1$. Tento výsledok bol známy už starogréckym matematikom. Bohužiaľ, ani táto charakteristika nie je úplne uspokojivá – nie je známe, či existuje nekonečne veľa Mersennových prvočísel. (Pripomeňme, že nutná podmienka na to, aby $M_n = 2^n - 1$ bolo prvočíslo je, že aj $n$ je prvočíslo, pozri lemu 2.4.5.) Nie je známe ani to, či existuje nepárne dokonalé číslo.

**Veta 3.2.9.** *Párne číslo $n$ je dokonalé číslo práve vtedy, keď má tvar $n = 2^{p-1}(2^p - 1)$, kde $p$ aj $2^p - 1$ sú prvočísla.*

*Dôkaz.* $\boxed{\Leftarrow}$ Ak $n$ má uvedený tvar, tak $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1)$. Pretože $2^p - 1$ je prvočíslo, platí $\sigma(2^p - 1) = 2^p$. Z toho dostaneme $\sigma(n) = (2^p - 1)2^p = 2n$.

$\boxed{\Rightarrow}$ Nech $n$ je párne dokonalé číslo. Potom $n$ v tvare $n = 2^k l$, kde $k \geq 1$ a $2 \nmid l$. Z podmienky $\sigma(n) = 2n$ dostaneme rovnosť

$$(2^{k+1} - 1)\sigma(l) = 2^{k+1}l.$$

Z nej vyplýva, že $2^{k+1}-1 \mid l$, čiže $l = r.(2^{k+1}-1)$. Po dosadení dostaneme

$$(2^{k+1}-1)\sigma(l) = 2^{k+1}r.(2^{k+1}-1),$$
$$\sigma(l) = 2^{k+1}r.$$

Súčasne vieme, že $l$ aj $r$ sú deliteľmi čísla $l$ a $l > r$ (lebo $2^{k+1}-1 > 1$), čiže $r$ je vlastný deliteľ čísla $l$, preto $\sigma(l) \geq l + r = 2^{k+1}.r = \sigma(l)$.

Ak by $l$ malo aj nejaké ďalšie delitele, tak by posledná nerovnosť bola ostrá, čo vedie k sporu. Preto $l$ a $r$ sú jediné delitele čísla $l$, čo znamená, že $r = 1$ a $l$ je prvočíslo.

Pretože $l = 2^{k+1}-1$ je prvočíslo, podľa lemy 2.4.5 je aj $k+1$ prvočíslo. □

Pre nepárne dokonalé čísla uvedieme nasledujúcu nutnú podmienku.

**Veta 3.2.10.** *Ak $n > 1$ je nepárne dokonalé číslo, tak $n$ má tvar $p^{4k+1}m^2$, kde $m$ je nepárne, $p$ je prvočíslo tvaru $4b+1$, $p \nmid m$ a $k \geq 0$.*

*Dôkaz.* Predpokladajme, že $n > 1$ je nepárne dokonalé číslo a $n = p_1^{l_1} \dots p_r^{l_r}$ je jeho kanonický rozklad. Pretože $n$ je nepárne, medzi prvočíslami $p_1, \dots, p_r$ sa nevyskytuje 2. Z toho, že $n$ je dokonalé, dostaneme

$$\sigma(n) = \prod_{i=1}^{r}(1 + p_i + \dots + p_i^{l_i}) = 2n.$$

Práve jeden z činiteľov na ľavej strane poslednej rovnosti musí byť deliteľný 2. Bez ujmy na všeobecnosti, nech je to prvý z nich, teda

$$2 \mid 1 + p_1 + \dots + p_1^{l_1}.$$

Súčasne platí $4 \nmid 1 + p_1 + \dots + p_1^{l_1}$ a $2 \nmid 1 + p_i + \dots + p_i^{l_i}$ pre $i = 2, 3, \dots, r$.

Z poslednej podmienky vyplýva, že $l_i$ pre $i = 2, 3, \dots, r$ sú párne, teda $n = p_1^{l_1}.m^2$, kde $m = \prod_{i=2}^{r} p_i^{\frac{l_i}{2}}$ je nepárne celé číslo.

Označme $p := p_1$ a $l := l_1$. Zostáva nám ukázať, že $p$ je tvaru $4b+1$ a $l = 4k+1$ pre nejaké $k \in \mathbb{N}_0$.

Pretože $1 + p + \dots + p^l$ je párne, $l$ je nepárne, $l = 2t+1$ pre nejaké $t$. Z toho $1 + p + \dots + p^{2t+1} = (1+p)(1+p^2+\dots+p^{2t})$. Ak by $p = 4b+3$, tak $4 \mid p+1 \mid 1+p+\dots+p^{2t+1}$, čo však neplatí. Zostáva teda druhá možnosť, že $p$ je tvaru $4b+1$.

Pre nepárne číslo $l$ máme takisto 2 možnosti; $l = 4k+1$ alebo $l = 4k+3$. Ak by platilo $l = 4k+3$, tak $1+p+\dots+p^l = 1+p+\dots+p^{4k+3} = (1+p+p^2+p^3)(1+p^4+\dots+p^{4k})$. Lenže $4 \mid 1+p+p^2+p^3$ (stačí si všimnúť, že $p \equiv 1 \pmod 4$ implikuje $p^t \equiv 1 \pmod 4$ pre všetky prirodzené $t$; čiže $1+p+p^2+p^3 \equiv 1+1+1+1 \pmod 4$), čo by znamenalo $4 \mid 1+p+\dots+p^l$. Zostáva teda druhá možnosť, $l = 4k+1$. □

Podmienka z predchádzajúcej vety je iba nutná, nie však postačujúca. Napríklad $5 = 5^{4.0+1}.1^2$ ale $\sigma(5) = 6 \neq 2.5$.

**Veta 3.2.11.** (i) *Ku každému reálnemu číslu $t > 1$ existuje nekonečne veľa takých čísel $n \in \mathbb{N}$, že $\frac{\sigma(n)}{n} > t$.*

(ii) *Existuje nekonečne veľa takých čísel $n \in \mathbb{N}$, že $\frac{\sigma(n)}{n} < 2$.*



*Dôkaz.* a) Uvažujme čísla $n_k = k!$ Potom $\sigma(n_k) > k! + \frac{k!}{2} + \frac{k!}{3} + \dots + \frac{k!}{k}$, čiže

$$\frac{\sigma(n_k)}{n_k} > 1 + \frac{1}{2} + \dots + \frac{1}{k}.$$

Zvyšok vyplýva z divergencie harmonického radu.

b) Pre každé prvočíslo máme $\sigma(p) = p+1$, čiže $\frac{\sigma(p)}{p} = 1 + \frac{1}{p} < 2$. Prvočísel je nekonečne veľa. □

Ďalej popíšeme správanie funkcií $\sigma(n)$ a $d(n)$ pre veľké $n$. (V istom zmysle ho popisuje aj tvrdenie 5.1.18.)

**Veta 3.2.12.**

$$\lim_{n\to\infty} \sigma(n) = +\infty$$
$$\liminf_{n\to\infty} d(n) = 2$$
$$\limsup_{n\to\infty} d(n) = +\infty$$

*Dôkaz.* Stačí si všimnúť, že platí:
$\sigma(n) > n$,
$d(p) = 2$ ak $p$ je prvočíslo
a $d(k!) \geq k$. □

{multip:VTTAU}

**Veta 3.2.13.** *Pre každé $\varepsilon > 0$ platí $\lim_{n\to\infty} \frac{d(n)}{n^\varepsilon} = 0$.*

**Lema 3.2.14.** *Pre ľubovoľné $\delta > 0$ existuje reálne číslo $k_\delta$ také, že $\frac{d(n)}{n^\delta} \leq k_\delta$ pre všetky $n \in \mathbb{N}$.*

*Dôkaz.* Nech $\delta > 0$ a $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Potom

$$\frac{d(n)}{n^\delta} = \prod_{i=1}^{k} \frac{\alpha_i + 1}{p^{\alpha\delta}}.$$

Uvažujme jednotlivé činitele $p^\alpha$.

Ak $p > 2^{1/\delta}$, tak $p^{\alpha\delta} > 2^\alpha$, a preto

$$\frac{\alpha+1}{p^{\alpha\delta}} < \frac{\alpha+1}{2^\alpha} \leq 1.$$

Zostáva druhá možnosť $p \leq 2^{1/\delta}$. Vtedy

$$\frac{\alpha+1}{p^{\alpha\delta}} \leq 1 + \frac{\alpha}{p^{\alpha\delta}}$$

a súčasne

$$p^{\alpha\delta} \geq 2^{\alpha\delta} = e^{\alpha\delta\ln 2} \geq 1 + \alpha\delta\ln 2 > \alpha\delta\ln 2.$$

Z toho

$$\frac{\alpha+1}{p^{\alpha\delta}} \leq 1 + \frac{1}{\delta\ln 2}.$$

Pretože takýchto činiteľov nemôže byť viac ako $2^{1/\delta}$, dostávame

$$\frac{d(n)}{n^\delta} \leq \left(1 + \frac{1}{\delta\ln 2}\right)^{2^{1/\delta}} =: k_\delta.$$

□

*Dôkaz vety 3.2.13.* Nech $0 < \delta < \varepsilon$. Potom

$$0 \leq \frac{d(n)}{n^\varepsilon} = \frac{d(n)}{n^\delta} \cdot \frac{1}{n^{\varepsilon-\delta}} \leq \frac{k_\delta}{n^{\varepsilon-\delta}}.$$

Pretože pravá strana konverguje k 0, dostávame $\lim_{n\to\infty} \frac{d(n)}{n^\varepsilon} = 0$. □

**Cvičenia**

1. Prirodzené číslo nazvime dokonalým číslom druhého druhu, ak je rovné súčinu svojich vlastných deliteľov. Ukážte, že $n$ je dokonalé číslo druhého druhu práve vtedy, keď $n$ je súčin 2 prvočísel $n = p_1 p_2$, alebo $n$ je treťou mocninou nejakého prvočísla $n = p^3$. Ukážte, že číslo 6 je jediné dokonalé číslo prvého aj druhého druhu. (Pod dokonalým číslom prvého druhu rozumieme číslo rovné súčtu svojich vlastných deliteľov.)

2. Číslo $n$ nazvime vyvážené, ak $\frac{\sigma(n)}{d(n)} = \frac{n}{2}$ (priemerná veľkosť deliteľa je $\frac{n}{2}$). Dokážte, že 6 je jediné vyvážené číslo. {multipcvic:SUMD}

3. Nech $f$ je multiplikatívna funkcia a nech $n = p_1^{l_1} \dots p_k^{l_k}$ je kanonický rozklad čísla $n$. Dokážte, že
$$\sum_{d|n} f(d) = \prod_{i=1}^{k} (1 + f(p_i) + \ldots + f(p_i^{l_i})).$$

4. Dokážte: Ak $f$ je úplne multiplikatívna funkcia a $g(n) = \sum_{d|n, d \text{ nepárne}} f(d)$, tak funkcia $g$ je multiplikatívna, ale nemusí byť úplne multiplikatívna. Môžeme predpoklad, že $f$ je plne multiplikatívna nahradiť predpokladom, že $f$ je multiplikatívna?

5. Označme ako $d^*(n)$ počet nepárnych deliteľov čísla $n$. Ukážte, že $d^*$ je multiplikatívna, ale nie je úplne multiplikatívna. Čo by sa stalo ak by sme uvažovali párne delitele?

6. Dokážte, že $d(n)$ je nepárne práve vtedy, keď $n$ je druhou mocninou celého čísla.

7. Dokážte, že $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ platí pre všetky $n \in \mathbb{N}$. Ak $n$ je dokonalé, tak $\sum_{d|n} \frac{1}{d} = 2$.

8. Dokážte, že $\sum_{t|n} d(t)^3 = (\sum_{t|n} d(t))^2$.

9. Dokážte, že $\prod_{t|n} t = n^{d(n)/2}$.

## 3.3 Eulerova funkcia

{SECTEULER}

### 3.3.1 Eulerova funkcia, Malá Fermatova veta

{SUBSECTEULER}

**Definícia 3.3.1.** Nech $m \in \mathbb{N}$. Ako $\varphi(m)$ označíme počet čísel z množiny $\{1, 2, \dots, m\}$ nesúdeliteľných s $m$. Funkciu $\varphi$ nazývame *Eulerova funkcia.*

**Príklad 3.3.2.** $\varphi(1) = 1$

$\varphi(12) = 4$, pretože čísla neprevyšujúce 12, ktoré sú s číslom 12 nesúdeliteľné sú práve $1, 5, 7, 11$.

Ak $p$ je prvočíslo, tak $\varphi(p) = p - 1$, lebo čísla $1, 2, \dots, p-1$ sú nesúdeliteľné s $p$.

Tiež platí $\varphi(p^k) = p^k - p^{k-1}$, pretože s číslom $p^k$ sú súdeliteľné práve násobky čísla $p$. Tých je medzi číslami $\{1, 2, \dots, p^k\}$ práve $p^{k-1}$.



Pretože poznáme hodnotu $\varphi(p^\alpha)$ pre ľubovoľné prvočíslo $p$, ak je funkcia $\varphi$ multiplikatívna, tak vieme podľa lemy 3.2.3 z kanonického rozkladu čísla $n$ vyrátať hodnotu $\varphi(n)$. Poďme sa preto pokúsiť ukázať, že funkcia $\varphi$ je multiplikatívna.

{euler:VTVPMULT}

**Veta 3.3.3.** *Eulerova funkcia $\varphi$ je multiplikatívna.*

*Dôkaz.* Pre ľubovoľné $k \in \mathbb{N}$ označme $M_k = \{a \in \{1, 2, \dots, k\}; (a, k) = 1\}$. Pri tomto označení platí $\varphi(k) = |M_k|$.

Nech $m, n \in \mathbb{N}$ a $(m, n) = 1$. Chceme ukázať, že $\varphi(m.n) = \varphi(m).\varphi(n)$. Na to stačí nájsť bijekciu $f\colon M_m \times M_n \to M_{mn}$.

Nech $(a, b) \in M_m \times M_n$, t.j. $(a, m) = 1$ a $(b, n) = 1$, pričom $a < m$ a $b < n$ sú z $\mathbb{N}_0$. Podľa čínskej vety o zvyškoch existuje jediné $x \in \{0, 1, \dots, mn - 1\}$ také, že

$$\begin{aligned} x &\equiv a \pmod m, \\ x &\equiv b \pmod n. \end{aligned} \tag{3.4}$$

{euler:EQAB}

To znamená, že $x = km + a = ln + b$ pre nejaké $k, l \in \mathbb{Z}$.

Všimnime si, že

$$\begin{aligned} (x, m) = (km + a, m) = (a, m) = 1, \\ (x, n) = (ln + b, n) = (b, n) = 1. \end{aligned}$$

Máme teda $(x, m) = (x, n) = 1$ (pozri lemu 2.1.11), a teda aj $(x, mn) = 1$. To znamená, že $x \in M_{mn}$ a zobrazenie $f$ môžeme definovať tak, že dvojici $(a, b) \in M_m \times M_n$ priradí riešenie sústavy (3.4).

Podľa čínskej vety o zvyškoch existuje ku každej dvojici $(a, b) \in M_m \times M_n$ práve jedno riešenie, preto $f$ je prosté zobrazenie.

Zobrazenie $f$ je aj surjektívne. Nech $(x, mn) = 1$. Položme $a = x \mod m$, $b = x \mod n$. Pretože $x = km + a$, dostávame $(a, m) = (km + a, m) = (x, a) = 1$. Podobne sa overí, že $(b, n) = 1$. Teda $(a, b) \in M_m \times M_n$ a je zrejmé, že $f(a, b) = x$. □

Z predchádzajúcej vety a z lemy 3.2.3 dostaneme potom

{euler:VTVZOREC}

**Veta 3.3.4.** *Nech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla $n$. Potom*

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \tag{3.5}$$

{euler:EQVZOREC}

Iný spôsob, ako dokázať predchádzajúci výsledok, je použiť princíp zapojenia a vypojenia (cvičenie 2). Ďalší možný dôkaz môžete nájsť v [Č].

Teraz ukážeme Eulerovu vetu, ktorá hovorí o súvise Eulerovej funkcie s niektorými kongruenciami. Na jej dôkaz použijeme jednu pomocnú lemu a Malú Fermatovu vetu. Pre Malú Fermatovu vetu poskytneme 3 dôkazy, jeden z nich je algebraický, druhý by sme mohli nazvať „teoreticko-číselný“ a tretí je kombinatorický.

{euler:LMBINOM}

**Lema 3.3.5.** *Nech $p$ je prvočíslo a nech $1 \leq i \leq p - 1$. Potom $p \mid \binom{p}{i}$, čiže*

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

*Dôkaz.* Z kombinatorického významu čísla $\binom{p}{i}$ (počet $i$-prvkových podmnožín ľubovoľnej $p$-prvkovej množiny) vyplýva, že je to celé číslo.[1] Máme vyjadrenie

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1.2\dots i}.$$

Prvočíslo $p$ delí čitateľ tohto zlomku, ale nedelí jeho menovateľ, lebo všetky čísla v menovateli sú menšie ako $p$. Z toho vyplýva, že $p \mid \binom{p}{i}$. □

{euler:LMFERM}

**Lema 3.3.6.** *Nech $p$ je prvočíslo. Potom*

$$a^p \equiv a \pmod{p} \tag{3.6}$$

{euler:EQFERM1}

*pre každé celé číslo $a$.*

*Dôkaz.* Pre každé prvočíslo $p$ máme $(-a)^p \equiv -a^p \pmod{p}$, čiže stačí overiť platnosť kongruencie pre $a \geq 0$. Uvedená kongruencia zrejme platí pre $a = 0$, $a = 1$. Pre ostatné $a$ ju môžeme dokázať indukciou vzhľadom na $a$.

Predpokladajme, že $a \geq 0$ a platí $a^p \equiv a \pmod{p}$. Z binomickej vety máme $(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^i$. Použitím lemy 3.3.5 dostaneme

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

□

{euler:VTFERM}

**Veta 3.3.7 (Malá Fermatova veta).** *Nech $p$ je prvočíslo a nech $a$ je celé číslo také, že $p \nmid a$. Potom*

$$a^{p-1} \equiv 1 \pmod{p} \tag{3.7}$$

{prelitc:EQFERM}

*Dôkaz.* Tvrdenie malej Fermatovej vety vyplýva z lemy 3.3.6 a z toho, že $(a, p) = 1$. □

*Dôkaz.* Počet prvkov grupy $(\mathbb{Z}_p \setminus \{0\}, \odot)$ je $p-1$. Podľa Lagrangeovej vety rád každého prvku tejto grupy delí $p-1$. Teda $a^t \equiv 1 \pmod{p}$, pre nejaké $t \mid p-1$, a preto aj $a^{p-1} \equiv 1 \pmod{p}$. □

*Kombinatorický dôkaz lemy 3.3.6.* Nech $p$ je prvočíslo. Budeme počítať ofarbenia náhrdelníka pozostávajúceho z $p$ guličiek $a$ farbami. (Farby sa môžu opakovať. Pozri obr. 3.1.)

Najprv majme náhrdelník rozopnutý. Potom máme $a^p$ rôznych ofarbení. Ako uvidíme o chvíľu, budú sa nám hodiť tie ofarbenia, ktoré používajú aspoň dve rôzne farby. Takýchto ofarbení je práve

$$a^p - a.$$

(Vynechali sme $a$ možný ofarbení jedinou farbou.)

Ak uvažujeme zopnutý náhrdelník, je logické považovať za rovnaké tie ofarbenia, ktoré sa líšia iba otočením. Pre dané ofarbenie náhrdelníka máme $p$ možných otočení – inak povedané, ofarbenie zopnutého náhrdelníka zodpovedá $p$ možným ofarbeniam rozopnutého náhrdelníka. Ak by sa nám podarilo dokázať, že ľubovoľné dve ofarbenia vzniknuté otočením sú rôzne, rozdelili by sme takto $a^p - a$ ofarbením do skupín po $p$ (každá skupina je reprezentovaná jedným ofarbením zopnutého náhrdelníka), čiže

$$p \mid a^p - a.$$

[1] Iný spôsob ako dokázať, že $\binom{n}{k}$ je celé číslo pre ľubovoľné prípustné $n$ a $k$ je indukciou pomocou známeho vzťahu $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.

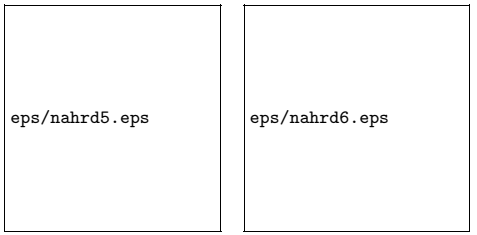


Uvažujme teraz, či otočením niektorého ofarbenia obsahujúceho aspoň 2 farby môžeme dostať opäť rovnaké ofarbenie. Predpokladajme, že otočením o $k$ pozícií dostaneme rovnaké ofarbenie. Pretože niektoré dve susedné gulôčky majú rôznu farbu, nemôže ísť o otočenie o jedinú pozíciu. Ak rovnaký náhrdelník dostaneme otočením o $k$ pozícií, znamená to, prvá gulôčka má rovnakú farbu ako $(k+1)$-vá, druhá rovnakú ako $(k+2)$-há, atď.

Zvoľme najmenšie možné také $k \in \mathbb{N}$. Tvrdíme, že $k \mid p$. Ak by to tak nebolo, mali by sme $p = ak - r$ pre nejaké $a, r \in \mathbb{Z}$ také, že $0 < r < k$. (Použili sme trochu zmenené tvrdenie vety o delení so zvyškom – namiesto zvyšku po delení číslom $k$ berieme rozdiel $p$ a tohoto zvyšku.)

Rovnosť $ak = p + r$ nám však hovorí, že $a$-krát opakovaným pootočením o $k$ pozícií dostaneme presne to isté, čo jediným otočením o $r$ pozícií. Teda ani otočenie o $r$ pozícií nemení ofarbenie. Súčasne však $0 < r < p$, čo je spor s výberom $k$.

Vidíme, že $k \mid p$ a $1 < k < p$, čo nemôže nastať, lebo $p$ je prvočíslo. □




Obr. 3.1: Ofarbenie zopnutého náhrdelníka a 5 ofarbení rozopnutého náhrdelníka, ktoré mu zodpovedajú

{euler:FIGNAH}

Poznamenajme, že obrátenie malej Fermatovej vety neplatí. Existuje nekonečne veľa zložených čísel, ktoré tiež spĺňajú kongruenciu (3.6) pre každé $a$. Tieto čísla sa nazývajú *absolútne pseudoprvočísla* alebo *Carmichaelove čísla* (pozri [AGP, CP, HW, KS, V]). Najmenšie Carmichaelove číslo je $561 = 3 \cdot 11 \cdot 17$.

Pomocou malej Fermatovej vety teraz dokážeme Eulerovu vetu. Pri dôkaze použijeme nasledovný postup: Tvrdenie najprv overíme pre prvočísla, potom pre mocniny prvočísel a nakoniec pre ľubovoľné čísla – tie môžeme dostať ako súčin čísel tvaru $p^\alpha$. Pri overovaní Eulerovej vety pre mocniny prvočísel bude užitočná nasledujúca lema.

{euler:LMROSE}

**Lema 3.3.8.** *Nech $n \in \mathbb{N}$ a $p$ je prvočíslo. Ak $n \equiv 1 \pmod{p^\alpha}$, tak $n^p \equiv 1 \pmod{p^{\alpha+1}}$.*

*Dôkaz.* Chceme ukázať, že $p^{\alpha+1} \mid n^p - 1$. Použijeme rovnosť $n^p - 1 = (n-1)(1+n+\ldots+n^{p-1})$. Podľa predpokladu máme $p^\alpha \mid n - 1$.

Súčasne platí

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

pre všetky $k = 0, 1, \dots, p-1$. (Tieto kongruencie dostaneme jednoducho umocnením kongruencie $n \equiv 1 \pmod{p}$, ktorá vyplýva z $n \equiv 1 \pmod{p^\alpha}$.) Sčítaním týchto kongruencií cez všetky $k = 0, 1, \dots, p-1$ dostaneme

$$1 + n + \ldots + n^{p-1} \equiv 0 \pmod{p},$$

inými slovami $p \mid 1 + n + \ldots + n^{p-1}$.

Celkovo teda dostaneme $p^{\alpha+1} = p^\alpha . p \mid (n-1)(1 + n + \ldots + n^{p-1}) = n^p - 1$. □

**Veta 3.3.9 (Eulerova veta).** *Nech $a, n \in \mathbb{N}$ sú také, že $(a, n) = 1$. Potom*

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

*Dôkaz.* Prípad, že $n = p$ je prvočíslo je už rozriešený vo vete 3.3.7. V tomto prípade totiž platí $\varphi(n) = p - 1$.

Nech teraz $n = p^\alpha$, kde $p$ je prvočíslo. Teraz máme $\varphi(n) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$. Z vety 3.3.7 vieme, že $a^{p-1} \equiv 1 \pmod{p}$. Opakovaným použitím lemy 3.3.8 (resp. indukciou) potom dostaneme $a^{(p-1)p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$.

Nech teraz $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Pre každé $i = 1, 2, \ldots, k$ máme $a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. Z toho vyplýva

$$a^{\varphi(n)} = (a^{\varphi(p_i^{\alpha_i})})^{\varphi(n/p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}.$$

Podľa čínskej vety o zvyškoch existuje jediné $m \in \{0, 1, \ldots, n-1\}$ také, že $m \equiv 1 \pmod{p_i^{\alpha_i}}$ pre každé $i$. Zrejme $m = 1$ spĺňa túto kongruenciu. Ukázali sme však, že ju spĺňa aj $a^{\varphi(n)}$, preto

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

□

Nasledujú dva ďalšie „algebraické“ dôkazy Eulerovej vety, ktoré sú podstatne jednoduchšie.

*Dôkaz.* Nech $a_1, \ldots, a_{\varphi(n)}$ sú všetky čísla z množiny $\{1, 2, \ldots, n\}$ nesúdeliteľné s $n$. Pretože $(a, n) = 1$, platí aj $(aa_k, n) = 1$ pre všetky $k = 1, 2, \ldots, \varphi(n)$. Navyše, podľa vety 3.1.9, žiadne dve z čísel $aa_1, \ldots, aa_{\varphi(n)}$ nie sú kongruentné modulo $n$. Sú to teda tie isté čísla ako $a_1, \ldots, a_{\varphi(n)}$ len inak usporiadané. Preto platí

$$a_1 \ldots a_{\varphi(n)} \equiv aa_1 \ldots aa_{\varphi(n)} \pmod{n}$$
$$a_1 \ldots a_{\varphi(n)} \equiv a^{\varphi(n)} a_1 \ldots a_{\varphi(n)} \pmod{n}$$

Keďže $(a_1 \ldots a_{\varphi(n)}, n) = 1$, môžeme opäť použiť vetu 3.1.9 a dostaneme

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

□

*Dôkaz.* Množina redukovaných zvyškových tried modulo $n$ tvorí grupu (Veta 3.1.11). Počet prvkov tejto grupy je $\varphi(n)$. Preto rád každého prvku tejto grupy musí byť deliteľom čísla $\varphi(n)$, z čoho dostávame, že

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

pre každé $a$ nesúdeliteľné s $n$. □

{euler:VTSUMPHI}

**Veta 3.3.10.** *Pre ľubovoľné prirodzené číslo $n$ platí*

$$\sum_{d \mid n} \varphi(d) = n.$$



*Dôkaz.* Podľa lemy 3.2.4 je funkcia $g(n) = \sum_{d \mid n} \varphi(d)$ multiplikatívna, a teda stačí dokázať uvedenú rovnosť pre mocniny prvočísel.

Ak $n = p^k$, kde $p$ je prvočíslo, tak máme

$$g(n) = \varphi(1) + \varphi(p) + \ldots \varphi(p^k) = 1 + p - 1 + \ldots + p^k - p^{k-1} = p^k = n.$$

□

Ukážeme si ešte jeden dôkaz vety 3.3.10, ktorý nevyužíva lemu 3.2.4.

*Dôkaz.* Označme $A := \{1, 2, \ldots n\}$ a $A_d = \{k \in A; (k, n) = d\}$. Takýmto spôsobom sme rozložili množinu $A$ na viacero podmnožín. Množina $A_k$ je neprázdna iba vtedy, keď $d \mid n$. Preto platí $|A| = \sum_{d \mid n} |A_d|$.

Množina $A_d$ obsahuje také čísla, že $(k, n) = d$, čo je podľa lemy 2.1.11(v) ekvivalentné s tým, že $\left(\frac{k}{d}, \frac{n}{d}\right) = 1$. Navyše existuje bijekcia medzi číslami $k \mid d$ spĺňajúcimi $(k, n) = d$ a číslami $j \mid \frac{n}{d}$ takými, že $(j, \frac{n}{d}) = 1$. Preto $|A_d| = \{j \leq \frac{n}{d}; \left(j, \frac{n}{d}\right) = 1\} = \varphi\left(\frac{n}{d}\right)$. Z toho vyplýva

$$\varphi(n) = |A| = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = \sum_{d \mid n} \varphi(d).$$

□

Teraz dokážeme výsledok L. Eulera, ktorý sme spomínali pri Fermatových číslach.

{euler:VTEULFEM}

**Veta 3.3.11 (Euler).** *Ak $p$ je prvočíslo a $p \mid F_m$, tak $p$ je tvaru $p = k2^{m+1} + 1$ pre nejaké $k \in \mathbb{N}$.*

*Dôkaz.* Nech $p \mid F_m = 2^{2^m} + 1$. Označme $r$ rád čísla 2 v grupe $(\mathbb{Z}_p \setminus \{0\}, \odot)$; t.j. $r$ je najmenšie číslo také, že $2^r \equiv 1 \pmod{p}$ alebo ekvivalentne $p \mid 2^r - 1$.

Podľa Lagrangeovej vety rád každého prvku grupy delí počet jej prvkov. Preto $r \mid p - 1$, čiže $p = k.r + 1$ pre nejaké $k \in \mathbb{N}$.

Ukážeme rovnosť $r = 2^{m+1}$, z čoho už vyplýva tvrdenie vety.

Najprv si všimnime, že

$$p \mid 2^{2^{m+1}} - 1 = (2^{2^m} - 1)(2^{2^m} + 1),$$

z čoho vyplýva, že $r \leq 2^{m+1}$ a $r \mid 2^{m+1}$.

Teda $r$ musí byť mocnina 2. Aby sme ukázali, že číslo $r$ nemôže byť menšie ako $2^{m+1}$ stačí overiť, že $p \nmid 2^{2^m} - 1$.

Ak by platilo $p \mid 2^{2^m} - 1$, tak aj $p \mid 2 = (2^{2^m} + 1) - (2^{2^m} - 1)$, čiže $p = 2$, čo je spor s tým, že $p$ delí nepárne číslo $F_m$. □

**Definícia 3.3.12.** Nech $a, n \in \mathbb{N}$ a $(a, n) = 1$. Potom najmenšie také číslo $k$, že $a^k \equiv 1 \pmod{n}$, sa nazýva *exponent čísla $a$ modulo $n$*.

Existencia čísla $k$ v predchádzajúcej definícii vyplýva priamo z Eulerovej vety. Exponent čísla $a$ modulo $n$ je vlastne rád prvku $\overline{a}$ grupy redukovaných zvyškových tried (Veta 3.1.11). V dôkaze vety 3.3.11 sme vlastne ukázali, že exponent čísla 2 modulo $p$ je $2^{m+1}$.

Základné vlastnosti exponentu sú zhrnuté v nasledujúcej vete.

{euler:VTEXPON}

**Veta 3.3.13.** *Nech $a, n \in \mathbb{N}$ sú nesúdeliteľné a nech $k$ je exponent čísla $a$ modulo $n$. Potom*

(i) *Čísla $1, a, a^2, \ldots, a^{k-1}$ sú nekongruentné modulo $n$.*

(ii) *Ku každému $s \in \mathbb{N}$ existuje $r \in \{1, 2, \ldots, k-1\}$ také, že $a^s \equiv a^r \pmod{n}$.*

(iii) *Ak $a^s \equiv 1 \pmod{n}$ pre nejaké $s \in \mathbb{N}$, tak $k \mid s$. Špeciálne platí $k \mid \varphi(n)$.*

### 3.3.2 Wilsonova a Lagrangeova veta

Kongrunciu tvaru $f(x) \equiv b \pmod m$, kde $f$ je polynóm $n$-tého stupňa s celočíselnými koeficientami, nazývame kongrunciou $n$-tého stupňa. Už sme sa zaoberali kongrunciami prvého stupňa – lineárnymi kongrunciami. Videli sme, že lineárna kongruencia môže mať viac než jedno riešenie. Teda vo všeobecnosti nie je pravda, že kongruencia $n$-tého stupňa má najviac $n$ riešení. Ukážeme však, že ak ide o kongruencie modulo $p$, kde $p$ je prvočíslo, tak toto tvrdenie platí.

{euler:VTLAG}

**Veta 3.3.14 (Lagrangeova veta).** *Ak $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ je polynóm s celočíselnými koeficientami, $p$ je prvočíslo a $p \nmid a_n$, tak kongruencia $f(x) \equiv 0 \pmod p$ má najviac $n$ (navzájom nekongruentných) riešení.*

*Ekvivalentne, ak táto kongruencia má viac ako $n$ (navzájom nekongruentných) riešení, tak $p$ delí všetky koeficienty polynómu $f(x)$.*

*Dôkaz.* Matematickou indukciou.

Pre $n = 1$ sme už tvrdenie dokázali. V tomto prípade máme totiž lineárnu kongruenciu $ax + b \equiv 0 \pmod p$. Ak $p \nmid a$, čiže $(a, p) = 1$, podľa vety 3.1.16 má táto kongruencia jediné riešenie (až na kongruenciu modulo $p$).

Predpokladajme, že tvrdenie platí pre $n-1$. Nech by $x_0, \ldots, x_n$ bolo $n+1$ rôznych riešení kongruencie $f(x) \equiv 0 \pmod p$. Máme

$$f(x)-f(x_0) = \sum_{k=1}^{n} a_k(x^k - x_0^k) = (x-x_0)\sum_{k=1}^{n} a_k(x^{k-1}+x^{k-2}x_0+x^{k-3}x_0^2+\ldots+x_0^{k-1}) = (x-x_0)g(x).$$

kde $g(x)$ je polynóm stupňa $n-1$ s vedúcim koeficientom $a_n$.

Dostávame $(x_i - x_0)g(x_i) \equiv 0 \pmod p$ a $g(x_i) \equiv 0 \pmod p$ pre každé $i = 1, \ldots, n$. Čiže $g(x) \equiv 0 \pmod p$ má $n$ riešení, z ktorých žiadne 2 nie sú kongruentné modulo $p$, čo je spor s indukčným predpokladom. □

Podáme ešte jeden dôkaz Lagrangeovej vety. Pripomeňme najprv jeden výsledok o determinantoch z lineárnej algebry (pozri [Kor, Príklad 6.2.17(2)]).

{euler:TVRVDM}

**Tvrdenie 3.3.15 (Vandermondov determinant).** *Nech $x_1, \ldots, x_n$ sú prvky poľa $F$. Potom*

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

*Špeciálne dostávame, že ak $a_i \neq a_j$ pre všetky $i \neq j$, tak Vandermondov determinant je nenulový.*

*Dôkaz Lagrangeovej vety.* Riešenia kongruencie $f(x) \equiv 0 \pmod p$ jednojednoznačne zodpovedajú riešeniam rovnice $g(x) = 0$ v poli $\mathbb{Z}_p$, kde $g(x)$ má koeficienty $b_i = a_i \mod p$, $i = 0, 1, \ldots, n$.

Predpokladajme, že $x_1, \ldots, x_{n+1}$ sú navzájom rôzne riešenia rovnice $g(x) = 0$ v $\mathbb{Z}_p$. Potom



koeficienty $b_0, b_1, \ldots, b_n$ sú riešením sústavy

$$\begin{aligned} b_n x_1^n + b_{n-1}x_1^{n-1} + \cdots + b_0 &= 0 \\ b_n x_2^n + b_{n-1}x_2^{n-1} + \cdots + b_0 &= 0 \\ &\vdots \\ b_n x_{n+1}^n + b_{n-1}x_{n+1}^{n-1} + \cdots + b_0 &= 0 \end{aligned}$$

Všimnime si, že matica tejto sústavy je práve Vandermondova matica prislúchajúca prvkom $x_1, \ldots, x_{n+1}$. Jej determinant je teda nenulový. Z toho vyplýva, že táto sústava má iba nulové riešenie a $b_i = 0$ v $\mathbb{Z}_p$ pre všetky $i$. Pretože $a_i \mod p = 0$, máme $p \mid a_i$. □

{euler:VTWIL}

**Veta 3.3.16 (Wilsonova veta).** *Číslo $p$ je prvočíslo práve vtedy, keď platí kongruencia*

$$(p-1)! \equiv -1 \pmod p. \tag{3.8}$$

{euler:EQWIL}

Aj pre Wilsonovu vetu uvedieme 3 dôkazy, jeden z nich bude algebraický, druhý bude využívať Lagrangeovu vetu a tretí z nich by sa dal nazvať kombinatorický.

*Dôkaz.* $\boxed{\Rightarrow}$ Vieme, že $\mathbb{Z}_p \setminus \{0\}$ tvorí vzhľadom na násobenie grupu, čiže ku každému prvku existuje inverzný prvok. T.j. ku každému $a \in \{1, \ldots, p-1\}$ existuje $b$ také, že $ab \equiv 1 \pmod p$.

Skúsme najprv zistiť, ktoré prvky sú inverzné sami k sebe (idempotentné). Musí pre ne platiť

$$\begin{aligned} a^2 &\equiv 1 \pmod p \\ a^2 - 1 = (a-1)(a+1) &\equiv 0 \pmod p \end{aligned}$$

To znamená, že súčin $a-1$ a $a+1$ v $\mathbb{Z}_p$ je 0. Pretože $(\mathbb{Z}_p, +, \cdot)$ je pole (a teda nemá delitele nuly), dostaneme $a-1 \equiv 0 \pmod p$ alebo $a+1 \equiv 0 \pmod p$, čiže máme iba 2 idempotentné prvky: $a \equiv 1, p-1 \pmod p$.

Ostatné prvky $\{2, \ldots, p-2\}$ môžeme teda usporiadať do dvojíc tak, že $ab \equiv 1 \pmod p$ pre každú dvojicu. Súčin týchto prvkov modulo $p$ je teda 1. Preto

$$(p-1)! \equiv 1.(p-1) \equiv -1 \pmod p.$$

$\boxed{\Leftarrow}$ Nepriamo. Nech $p$ je zložené číslo, $p = m.n$, $1 < m, n < p$.

Ak by platilo $(p-1)! \equiv -1 \pmod p$, tak platí aj $(p-1)! \equiv -1 \pmod n$, lebo $n \mid p$. Číslo $n$ sa však vyskytne ako jeden z činiteľov v súčine $(p-1)! = 1.2 \ldots (p-1)$, preto $(p-1)! \equiv 0 \pmod n$, čo je spor.

□

*Dôkaz.* $\boxed{\Rightarrow}$ Uvažujme polynóm

$$f(x) = x^{p-1} - 1 - \prod_{m=1}^{p-1} (x - m).$$

Stupeň tohoto polynómu je nanajvýš $p-2$. Podľa malej Fermatovej vety sú všetky čísla $x = 1, 2, \ldots, p-1$ riešeniami kongruencie $f(x) \equiv 0 \pmod p$, preto podľa Lagrangeovej vety $p$ delí všetky koeficienty polynómu $f$. Teraz si stačí všimnúť, že absolútny člen polynómu $f$ je $-1 - (-1)^{p-1}(p-1)!$.

Opačnú implikáciu sme ukázali v predchádzajúcom dôkaze. □

Uvedieme ešte jeden dôkaz pochádzajúci z článku [Gup], môžete ho nájsť aj v [KLŠZ, s.83].

Ako $M(n,r)$ označíme systém všetkých usporiadaných $n$-tíc $H_1,\ldots,H_r$ spĺňajúcich tieto podmienky:

(a) Pre všetky $i=1,\ldots,r$ je $H_i\neq\emptyset$ a $H_i\subseteq\{1,2,\ldots,n\}$.

(b) $\bigcup_{i=1}^{r} H_i=\{1,2,\ldots,n\}$.

Symbolom $B(n,r)$ budeme označovať počet prvkov množiny $M(n,r)$.

Čísla $B(n,r)$ úzko súvisia so *Stirlingovými číslami druhého druhu*. Ako $S(n,r)$ sa označuje počet rozkladov $n$-prvkovej množiny na $r$ (neprázdnych) podmnožín. Vidíme, že jediný rozdiel oproti našej definícii je teda ten, že nezáleží na poradí množín $H_1,\ldots,H_r$; teda $B(n,r)=r!S(n,r)$. Je možné, že so Stirlingovými číslami (a takisto s Bellovými číslami, ktoré vyjadrujú počet všetkých rozkladov $n$-prvkovej množiny), ste sa už stretli na iných prednáškach.

Najprv uvedieme 2 rekurentné vzťahy, ktoré platia pre čísla $B(n,r)$. Podobné vzťahy platia aj pre $S(n,r)$; pozri cvičenie 16 v tejto kapitole.

$$B(n,r)=r(B(n-1,r)+B(n-1,r-1)) \tag{3.9}$$ {euler:EQSTIR1}

$$B(n,r)=\sum_{k=1}^{n-r+1}\binom{n}{k}B(n-k,r-1) \tag{3.10}$$ {euler:EQSTIR2}

Vzťahom (3.9) a okrajovými podmienkami $B(n,n)=n!$, $B(n,1)=1$ sú určené všetky hodnoty $B(n,r)$.

Na overenie vzťahu (3.9) si stačí rozdeliť prvky $M(n,r)$ na také, ktoré obsahujú množinu $\{n\}$ a také, ktoré ju neobsahujú. Máme $r$ možností, do ktorej množiny bude patriť prvok $n$. Ak rozklad obsahuje ako 1 z množín, množinu $\{n\}$, tak ostatné prvky musia byť rozdelené do ostatných $r-1$ množín, takýchto (usporiadaných) rozkladov je $B(n-1,r-1)$. V opačnom prípade je prvok $n$ vo viac než jednoprvkovej množine, preto ostatné prvky rozdeľujeme do $r$ množín (nejaké prvky musíme pridať aj do tej množiny, ktorá obsahuje $n$). To zodpovedá členu $B(n-1,r)$ vystupujúcemu v (3.9).

Pri druhom uvedenom vzťahu sme rozdelili prvky $M(n,r)$ podľa toho, koľkoprvková je množina $H_1$. Táto množina nemôže mať viac ako $n-r+1$ prvkov (pretože množiny $H_2,\ldots,H_r$ sú neprázdne). Ak obsahuje $k$ prvkov, tak máme $\binom{n}{k}$ rôznych spôsobov, ktorými môžeme vybrať týchto $k$ prvkov. Ak sme už vybrali $k$-prvkovú množinu $H_1$, tak zvyšných $n-k$ prvkov môžeme rozdeliť do množín $H_2,\ldots,H_r$ práve $B(n-k,r-1)$ spôsobmi.

Pomocou (3.9) a (3.10) môžeme ukázať nasledujúcu lemu. {euler:LMGUPTA}

**Lema 3.3.17.** *Nech $p$ je prvočíslo. Potom*

(i) *$p\mid B(p,r)$ pre všetky $r\geq 2$,*

(ii) *$p\mid B(p-1,r)+(-1)^r$ pre všetky $r$ také, že $1\leq r\leq p-1$.*

*Dôkaz.* (i) Ak $r\geq 2$, tak v (3.10) sčitujeme len cez $k<p$ Podľa lemy 3.3.5 sú všetky sčítance v (3.10) sú deliteľné číslom $p$.

(ii) Indukciou vzhľadom na $r$. Ak $r=1$, tak máme $B(p-1,r)=1$, čiže uvedené tvrdenie hovorí, že $p\mid 1-1=0$, čo je skutočne pravda.

Predpokladajme teraz, že toto tvrdenie platí pre $r-1$, čiže $p\mid B(p-1,r-1)+(-1)^{r-1}$. Súčasne vieme, že $B(p,r)=r(B(p-1,r)+B(p-1,r-1))$. Podľa časti (i) platí $p\mid B(p,r)$ a, keďže $p\nmid r$, dostaneme $p\mid B(p-1,r)+B(p-1,r-1)$. Z toho dostaneme

$$p\mid [B(p-1,r)+B(p-1,r-1)]-[B(p-1,r-1)+(-1)^{r-1}]=B(p-1,r)+(-1)^r.$$



□

*Dôkaz Wilsonovej vety.* $\boxed{\Rightarrow}$ Vyplýva z lemy 3.3.17 – stačí zobrať $r=p-1$ a dostaneme $p\mid B(p-1,r)+(-1)^r=(p-1)!+(-1)^{p-1}$, z čoho máme $(p-1)!\equiv -1 \pmod p$. (Ak $p$ je nepárne, tak $(-1)^p=-1$; ak $p=2$, tak $1\equiv -1 \pmod p$.) □

Wilsonovu vetu možno použiť na dôkaz jedného známeho výsledku o kvadratických zvyškoch.

**Definícia 3.3.18.** Číslo $q$ sa nazýva kvadratický zvyšok modulo $n$, ak existuje také $x\in\mathbb{Z}$, že

$$x^2\equiv q \pmod n.$$

{euler:VTWILSKVAD}

**Veta 3.3.19.** *Ak $p$ je prvočíslo tvaru $p=4k+1$, tak $-1$ je kvadratický zvyšok modulo $p$.*

*Dôkaz.* Podľa Wilsonovej vety máme

$$1\ldots(p-1)=1\ldots 2k.(2k+1)\ldots 4k\equiv 1\ldots 2k(-2k)\ldots(-1)\equiv$$
$$\left(\prod_{j=1}^{2k} j\right)^2.(-1)^{2k}\equiv\left(\prod_{j=1}^{2k} j\right)^2\equiv -1 \pmod p.$$

□

**Cvičenia**

1. Nájdite všetky $n$ také, že a) $\varphi(n)=\frac{n}{2}$; b) $\varphi(n)=\varphi(2n)$; c) $\varphi(n)=12$. {euler:CVICVYPZAP}
2. Dokážte vzťah (3.5) pomocou princípu zapojenia a vypojenia. {euler:CVIC3}
3. Dokážte, že $343\mid 2^{147}-1$.
4. Dokážte, že ak $p$ je prvočíslo, tak $(a+b)^p\equiv a^p+b^p \pmod p$.
5. Nech $p$ je nepárne prvočíslo. Dokážte, že $1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1}\equiv -1 \pmod p$ a $1^p+2^p+\ldots+(p-1)^p\equiv 0 \pmod p$.
6. Dokážte, že $17\nmid 5n^2+15$ pre ľubovoľné $n\in\mathbb{N}$.
7. Čísla ktoré spĺňajú kongruenciu (3.6) pre nejaké konkrétne číslo $a$ nazývame *pseudoprvočísla pri báze $a$*. Dokážte, že ak $n$ je nepárne pseudoprvočíslo pri báze 2, tak aj $m=2^n-1$ je pseudoprvočíslo pri báze 2. (Teda existuje nekonečne veľa nepárnych pseudoprvočísel pri báze 2.)
8. Dokážte, že ak $p$ je prvočíslo a Mersennove číslo $M_p=2^p-1$ je zložené, tak $M_p$ je pseudoprvočíslo pri báze 2.
9. Ak $p$ je nepárne prvočíslo, dokážte pomocou Malej Fermatovej vety, že $x^2\equiv -1 \pmod p$ má riešenie práve vtedy, keď $p\equiv 1 \pmod 4$. Použitím tohoto výsledku ukážte, že všetky nepárne prvočíselné delitele čísla $n^2+1$ sú tvaru $4k+1$ a že existuje nekonečne veľa prvočísel takéhoto tvaru.
10. Ak $p$ je nepárne prvočíslo, dokážte, že $1^2.3^2\ldots(p-2)^2\equiv 2^2.4^2\ldots(p-1)^2\equiv(-1)^{(p+1)/2} \pmod p$.

11. Dokážte: Ak $p$ je prvočíslo a $h+k=p-1$, tak $h!k! \equiv (-1)^{k+1} \pmod p$. {eulercvic:KVZVYS}

12. Nech $p$ je prvočíslo tvaru $4k+3$ a nech $p \mid a^2+b^2$. Dokážte, že potom $p$ delí čísla $a$ a $b$.

13. Nech $a, n \in \mathbb{N}$ a $a \geq 2$. Dokážte, že $a^k \equiv 1 \pmod{a^n-1}$ práve vtedy, keď $n \mid k$. Ďalej ukážte, že $n \mid \varphi(a^n-1)$.

14. Dokážte vetu 3.3.13.

15. Nech $a(n) = ((n-1)!)^2 \mod n$ a $b(n) = ((n-1)!+1)^2 \mod n$. Dokážte, že $f(n) = na(n)+2b(n)$ je vždy prvočíslo, pričom každé prvočíslo možno získať v takomto tvare. (Hint: Skúste využiť že $((p-1)!)^2 \equiv p \pmod 0$ práve vtedy, keď $p$ je zložené a $((p-1)!)^2 \equiv p \pmod 1$ práve vtedy, keď $p$ je prvočíslo. Tento fakt sa dá ľahko odvodiť z Wilsonovej vety.) {euler:CVICSTIR}

16. Dokážte, že pre Stirlingove čísla druhého druhu platia rovnosti $S(n,k) = kS(n-1,k)+S(n-1,k-1)$ a $S(n,k) = \sum_{m=k}^{n} k^{n-m} S(m-1,k-1)$.

17. Aký je vzťah medzi ofarbeniami $n$-prvkovej množiny použitím $k$ farieb (pričom nemusíme použiť všetky z nich) a jej rozkladmi na $k$ množín. Dokážte, že $k^n = \sum_{r=1}^{k} B(n,r)\binom{k}{r}$. Odvoďte z tohoto vzťahu a z lemy 3.3.17 Malú Fermatovu vetu. Obrátene, použitím postupu z „náhrdelníkového dôkazu“ Malej Fermatovej vety dokážte, že $p \mid B(p,r)$ pre $r \geq 2$.

## 3.4 Möbiova funkcia

**Definícia 3.4.1.** Pre ľubovoľné prirodzené číslo $n$ definujeme *Möbiovu funkciu* $\mu$ predpisom

$$\mu(n) = \begin{cases} 1, & \text{ak } n = 1; \\ (-1)^r, & \text{ak } n = p_1 \dots p_r \text{ je súčin navzájom rôznych prvočísel} \\ 0, & \text{inak.} \end{cases}$$

Vidíme, že $\mu(n) \neq 0$ práve vtedy, keď $n$ je číslo bez kvadratických deliteľov.

**Lema 3.4.2.** *Funkcia $\mu$ je multiplikatívna.*

*Dôkaz.* Nech $a$, $b$ sú prirodzené čísla, $(a,b)=1$. Ak je niektoré z nich násobkom štvorca, tak $\mu(ab) = \mu(a).\mu(b) = 0$.

Ak sú obe čísla bez kvadratických deliteľov, tak ani $ab$ nemá kvadratické delitele. (Kvadratický deliteľ by mohol vzniknúť jedine z prvočísel obsiahnutých v kanonických rozkladoch oboch čísel, čo nie je možné, pretože čísla $a$ a $b$ sú nesúdeliteľné.) Označme $k$ počet prvočíselných deliteľov čísla $a$ a $l$ počet prvočíselných deliteľov čísla $b$. Dostávame $\mu(ab) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(a)\mu(b)$. □

**Veta 3.4.3.** *Nech $f$ je multiplikatívna funkcia a nech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla $n > 1$. Potom*

$$\sum_{d \mid n} \mu(d) f(d) = (1-f(p_1)) \dots (1-f(p_k)).$$

*Dôkaz.* Funkcia $\mu(n)f(n)$ je multiplikatívna (súčin 2 multiplikatívnych funkcií). Potom aj funkcia $g(n) = \sum_{d \mid n} \mu(d) f(d)$ je multiplikatívna (lema 3.2.4), teda je jednoznačne určená svojimi hodnotami pre mocniny prvočísel.



Takisto ľahko vidno, že funkcia na pravej strane rovnosti, ktorú sa snažíme dokázať, je tiež multiplikatívna. Preto na dôkaz rovnosti týchto dvoch funkcií stačí overiť, že sa rovnajú pre mocniny prvočísel.

Ak $n = p^k$, kde $p$ je prvočíslo, tak $g(n) = \mu(1)f(1) + \mu(p)f(p) + \dots + \mu(p^k)f(p^k) = 1 - f(p) + 0 + \dots + 0 = 1 - f(p)$. □

*Iný dôkaz.* Z definície Möbiovej funkcie vyplýva, že v súčte $\sum_{d \mid n} \mu(d)f(d)$ budú nenulové len členy prislúchajúce deliteľom tvaru $d = p_{i_1} \dots p_{i_s}$ (pre ostatné delitele je $\mu(d) = 0$). Každý takýto deliteľ prispeje k celkovej sume hodnotou $(-1)^s f(p_{i_1}) \dots f(p_{i_s})$. Je zrejmé, že rovnakú sumu dostaneme roznásobením pravej strany dokazovanej rovnosti. □

Ak za multiplikatívnu funkciu $f$ zvolíme v predchádzajúcej vete $f(n) = 1$ resp. $f(n) = \frac{1}{n}$, tak dostaneme {mobi:DOSMU}

**Dôsledok 3.4.4.**

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & ak\ n = 1, \\ 0, & inak. \end{cases}$$

$$\sum_{d \mid n} \frac{\mu(d)}{d} = \begin{cases} 1, & ak\ n = 1, \\ \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right), & inak. \end{cases}$$

Z vety 3.3.4 potom máme {mobi:DOSMUPHI}

**Dôsledok 3.4.5.**

$$\varphi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$$

Už vieme, že ak $f$ je multiplikatívna funkcia, tak aj funkcia $g(n) = \sum_{d \mid n} f(d)$ je multiplikatívna. Ukážeme ako pomocou Möbiovej funkcie a tzv. Dirichletovej konvolúcie (Dirichletovho súčinu) môžeme z funkcie $g$ vyjadriť funkciu $f$.

**Definícia 3.4.6.** *Dirichletova konvolúcia* (*Dirichletov súčin*) aritmetických funkcií $f$ a $g$ je funkcia

$$f * g(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right).$$

Túto definíciu môžeme ekvivalentne prepísať aj takto: $f * g(n) = \sum_{ab=n} f(a)g(b)$.

Hoci sme na to explicitne neupozornili, s Dirichletovým súčinom sme sa už stretli. Napríklad Dôsledok 3.4.5 vlastne hovorí, že $\varphi = \mu * \mathrm{id}_{\mathbb{N}}$.

Takisto výraz $\sum\limits_{d \mid n} f(n)$, s ktorým sme sa už viackrát stretli, sa dá zapísať ako $f * u$, kde $u$ je funkcia definovaná ako $u(n) = 1$ pre všetky $n \in \mathbb{N}$.

Dôsledok 3.4.4 nám hovorí, že $\mu * u = I$, kde $I$ označuje multiplikatívnu funkciu definovanú ako $I(1) = 1$ a $I(n) = 0$ pre $n \neq 1$. Je pomerne ľahké zistiť, že platí $f * I = f$. {mobi:VTINV1}

**Veta 3.4.7 (Möbiova inverzia).** *Ak $g(n) = \sum\limits_{m \mid n} f(m)$ pre ľubovoľné $n$, tak*

$$f(n) = \sum_{m \mid n} \mu(m) g\left(\frac{n}{m}\right) = \sum_{m \mid n} \mu\left(\frac{n}{m}\right) g(m).$$

*Dôkaz.* Druhá rovnosť je zrejmá. Počítajme

$$\sum_{m|n}\mu(m)g\left(\frac{n}{m}\right) \;=\; \sum_{m|n}\mu(m)\sum_{k|\frac{n}{m}}f(k) \;=\; \sum_{mk|n}\mu(m)f(k) \;=\; \sum_{k|n}f(k)\sum_{m|\frac{n}{k}}\mu(m) \;=\; f(n)$$

(Pri výpočte sme použili zámenu poradia sumácie a v poslednej rovnosti dôsledok 3.4.4.) □

{mobi:VTINV2}

**Veta 3.4.8 (Möbiova inverzia).** *Ak* $f(n) = \sum_{m|n}\mu\left(\frac{n}{m}\right)g(m)$, *tak* $g(n) = \sum_{m|n}f(m) = \sum_{m|n}f\left(\frac{n}{m}\right)$.

*Dôkaz.* Opäť použijeme podobný výpočet ako v predchádzajúcom dôkaze.

$$\sum_{m|n}f\left(\frac{n}{m}\right)=\sum_{m|n}\sum_{k|\frac{n}{m}}\mu\left(\frac{n}{mk}\right)g(k)=\sum_{k|n}g(k)\sum_{m|\frac{n}{k}}\mu\left(\frac{m/n}{k}\right)=g(n)$$

□

Napríklad z dôsledku 3.4.5 a vety 3.4.7 dostaneme, že $n = \sum_{d|n}\varphi(d)$, čiže dostávame ďalší dôkaz vety 3.3.10.

Tvrdenia viet 3.4.7 a 3.4.8 môžeme pomocou Dirichletovho súčinu zapísať takto:

$$\begin{aligned} g = f*u \quad &\Rightarrow \quad f=\mu*g,\\ f = \mu*g \quad &\Rightarrow \quad g=f*u. \end{aligned}$$

Ak uveríte (prípadne overíte), že Dirichletov súčin je asociatívna operácia, tak s využitím vlastností $\mu*u=I$ a $I*f=f$ môžeme dôkaz týchto viet zapísať veľmi elegantne:

$$\begin{aligned} g = f*u \quad &\Rightarrow \quad g*\mu=(f*u)*\mu=f*(u*\mu)=f*I=f\\ f = g*\mu \quad &\Rightarrow \quad f*u=(g*\mu)*u=g*(\mu*u)=g*I=g \end{aligned}$$

Mnohé ďalšie vlastnosti a aplikácie Dirichletovho súčinu môžete nájsť v kapitole knihy [Ap], ktorá je venovaná aritmetickým funkciám. (V knihe [Ap] zvolil autor taký prístup, že najprv zavedie Möbiovu funkciu a dokáže viaceré vlastnosti Dirichletovho súčinu – medziným vety 3.4.7 a 3.4.8 – a veľa vlastností ostatných aritmetických funkcií dokazuje práve použitím poznatkov o Möbiovej funkcii a Dirichletovom súčine.)

### Cvičenia

1. Dokážte, že ak $f$ a $g$ sú multiplikatívne funkcie, tak aj Dirichletov súčin $f*g$ je multiplikatívna funkcia.
2. Dokážte, že $\frac{n}{\varphi(n)}=\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}$.
3. Dokážte, že $\sum_{d^2|n}\mu(d)=\mu^2(n)$.
4. Nech $g(n)=\prod_{d|n}f(d)$. Dokážte, že $f(n)=\prod_{d|n}g\left(\frac{n}{d}\right)^{\mu(d)}=\prod_{d|n}g(d)^{\mu(n/d)}$.

{mobicvic:SUMKN}

5. Dokážte, že existuje multiplikatívna funkcia $g$ taká, že

$$\sum_{k=1}^{n}f((k,n))=\sum_{d|n}f(d)g\left(\frac{n}{d}\right).$$



6. Pomocou cvičenia 5 dokážte

$$\sum_{k=1}^{n}(k,n)\mu((k,n))=\mu(n).$$

# Kapitola 4

# Kvadratické kongruencie

{chkvadr}

V tejto časti sa budeme zaoberať riešiteľnosťou kongruencií tvaru

$$x^2 \equiv a \pmod{p},$$

kde $p$ je nepárne prvočíslo, $p > 2$. (Prípad $p = 2$ sme vynechali pretože ten je skutočne triviálny.)

Touto témou sa zaoberalo mnoho významných matematikov. L. Eulera priviedol k základným výsledkom o kvadratických kongruenciách výskum Fermatových čísel. Z ďalších známych mien môžeme spomenúť C. F. Gaussa alebo A.-M. Legendra. Do určitej miery môžeme medzi priekopníkov tejto oblasti rátať aj Fermata, hoci pojem kvadratického zvyšku nepoužíval, mnoho z jeho výsledkov sa dá interpretovať ako výsledky o kvadratických zvyškoch.

## 4.1 Kvadratické zvyšky

**Definícia 4.1.1.** Nech $n \nmid q$. Potom sa číslo $q$ sa nazýva *kvadratický zvyšok* modulo $n$, ak existuje také $x \in \mathbb{Z}$, že

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

V opačnom prípade hovoríme, že $q$ je *kvadratický nezvyšok* modulo $n$.

Budeme používať aj stručnejší zápis: $qRn$ znamená, že $q$ je kvadratický zvyšok modulo $n$ a $q\overline{R}n$ znamená, že $q$ je kvadratický nezvyšok modulo $n$.

**Príklad 4.1.2.** Pokúsme sa nájsť všetky kvadratické zvyšky modulo 7. Platí

$$1^2 \equiv 1 \pmod 7 \qquad 2^2 \equiv 4 \pmod 7 \qquad 3^2 \equiv 2 \pmod 7.$$

Ďalšie čísla už v podstate netreba skúšať, pretože

$$4^2 \equiv (-3)^2 \equiv 3^2 \equiv 2 \pmod 7 \qquad 5^2 \equiv (-2)^2 \equiv 2^2 \equiv 4 \pmod 7 \qquad 6^2 \equiv (-1)^2 \equiv 1^2 \equiv 1 \pmod 7.$$

Kvadratické zvyšky modulo 7 sú teda 1, 2 a 4.

**Definícia 4.1.3.** Množina čísel $n_1, \ldots, n_{\varphi(n)}$ sa nazýva *redukovaný zvyškový systém* modulo $n$ ak sú tieto čísla reprezentantmi všetkých redukovaných zvyškových tried modulo $n$.

Ekvivalentne: Je to takých $\varphi(n)$ čísel, že žiadne dve z nich nie sú kongruentné modulo $n$ a navyše každé z nich je nesúdeliteľné s $n$.



{kvadr:VTPOCZVYS}

**Veta 4.1.4.** *Nech $p > 2$ prvočíslo. Ľubovoľný redukovaný zvyškový systém $\{a_1, \ldots, a_{p-1}\}$ modulo $p$ obsahuje $\frac{p-1}{2}$ kvadratických zvyškov a $\frac{p-1}{2}$ kvadratických nezvyškov modulo $p$.*

*Kvadratické zvyšky sú práve tie čísla, ktoré sú kongruentné s číslami $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.*

*Dôkaz.* Všimnime si, že pre ľubovoľné celé čísla platí $a^2 \equiv b^2 \pmod p$ práve vtedy, keď $a \equiv b \pmod p$ alebo $a \equiv -b \pmod p$. Uvedená rovnosť je totiž ekvivalentná s rovnosťou $(a-b)(a+b)$ v $\mathbb{Z}_p$. Pretože $\mathbb{Z}_p$ je pole, platí táto rovnosť iba vtedy, keď niektorý z prvkov $a-b$ je $a+b$ je 0 v $\mathbb{Z}_p$, čo zodpovedá kongruenciám $a - b \equiv 0 \pmod p$ a $a + b \equiv 0 \pmod p$.

Reprezentantov $a_1, \ldots, a_{p-1}$ redukovaných zvyškových tried môžeme rozdeliť na dvojice prvkov, ktoré po umocnení na druhú dávajú rovnaký zvyšok po delení $p$. Keďže sme rozdelili $p-1$ prvkov na dvojice prislúchajúce rovnakému zvyšku štvorca, všetkých možných kvadratických zvyškov je práve $\frac{p-1}{2}$.

Takisto je vidno, že z dvojice čísel, ktorých druhá mocnina dáva rovnaký zvyšok po delení $p$, je jedno nanajvýš $\frac{p-1}{2}$ a druhé je väčšie než $\frac{p-1}{2}$. Z toho vyplýva druhá časť tvrdenia. □

## 4.2 Legendrov symbol

**Definícia 4.2.1.** Ak $p$ je prvočíslo a $a$ je celé číslo, tak *Legendrov symbol* $\left(\frac{a}{p}\right)$ definujeme nasledovne:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ak } aRp, \\ -1 & \text{ak } a\overline{R}p, \\ 0 & \text{ak } p \mid a. \end{cases}$$

Niekedy sa používa aj označenie $(a|p)$.

**Príklad 4.2.2.** $\left(\frac{1}{p}\right) = 1$, $\left(\frac{3}{7}\right) = -1$, $\left(\frac{4}{7}\right) = 1$, $\left(\frac{a^2}{p}\right) = 1$

Vo vete 3.3.19 sme ukázali, že $\left(\frac{-1}{p}\right) = 1$ pre prvočísla tvaru $4k+1$.

V ďalšom uvedieme viacero výsledkov, ktoré sa dajú použiť na výpočet Jacobiho symbolu $\left(\frac{n}{p}\right)$ pre dané $n$ a $p$.

{kvadr:VTEULKRIT}

**Veta 4.2.3 (Eulerovo kritérium).** *Nech $p > 2$ je prvočíslo. Potom pre všetky $n$ platí*

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

*Dôkaz.* Ak $p \mid n$, tvrdenie vety je zrejmé.

Ak $p \nmid n$, tak podľa Malej Fermatovej vety máme

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

Potom $p$ delí niektorý z výrazov $n^{\frac{p-1}{2}} \pm 1$, čiže $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. Teda výraz, o ktorom chceme ukázať, že sa rovná $\left(\frac{n}{p}\right)$ skutočne nadobúda len hodnoty 1 a $-1$. Treba ešte ukázať, že 1 to bude práve vtedy, keď $n$ je kvadratický zvyšok modulo $p$.

Ak $n$ je kvadratický zvyšok, tak existuje $x$ také, že $n \equiv x^2 \pmod p$, z čoho potom dostaneme

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

(opäť sme použili Malú Fermatovu vetu). Teda pre kvadratické zvyšky má tento výraz skutočne hodnotu 1 (modulo $p$). Súčasne vieme z Lagrangeovej vety (veta 3.3.14), že kongruenciu $n^{\frac{p-1}{2}} \equiv 1 \pmod p$ môže spĺňať najviac $\frac{p-1}{2}$ čísel. Keďže kvadratických zvyškov modulo $p$ je $\frac{p-1}{2}$, túto kongruenciu už nespĺňajú žiadne iné čísla. Pre kvadratické nezvyšky teda platí $n^{\frac{p-1}{2}} \equiv -1 \pmod p$. □

**Príklad 4.2.4.** $\left(\frac{4}{7}\right) \equiv 4^3 \equiv 2.4 \equiv 1 \pmod 7$

Základné vlastnosti Legendrovho symbolu sú zhrnuté v nasledujúcej leme: {kvadr:ZAKLJACO}

**Lema 4.2.5.** *Nech $p$ je nepárne prvočíslo a $a, b \in \mathbb{Z}$. Potom*

(i) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ {kvadr:JACit1}

(ii) $\left(\frac{1}{p}\right) = 1$ {kvadr:JACit2}

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ {kvadr:JACit3}

(iv) $\left(\frac{a^2}{p}\right) = 1$ {kvadr:JACit5}

(v) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ {kvadr:JACit4}

*Dôkaz.* (i) Ak $a \equiv b \pmod p$, tak $a$ je kvadratický zvyšok práve vtedy, keď $b$ je kvadratický zvyšok. ($x^2 \equiv a \pmod p \Leftrightarrow x^2 \equiv b \pmod p$)
(ii) Číslo 1 je kvadratický zvyšok pre každé prvočíslo $p$.
(iii) Vyplýva z Eulerovho kritéria.
(iv) $a^2 \equiv a^2 \pmod p$
(v) Vyplýva z (iii) a z (iv). □

Lema 4.2.5(iii) vlastne hovorí, že pre pevné $p$ je funkcia $a \mapsto \left(\frac{a}{p}\right)$ úplne multiplikatívna. Na jej určenie nám stačí poznať prvočíselné hodnoty.

Teraz sa pokúsime zistiť, kedy sú čísla $-1$ a 2 kvadratickými zvyškami.

Nasledujúce tvrdenie vyplýva priamo z Eulerovho kritéria. Jeho prvú časť sme už dokázali vo vete 3.3.19. {kvadr:TVRCHAR-1}

**Tvrdenie 4.2.6.** *Pre každé nepárne prvočíslo platí*

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

*Teda $-1$ je kvadratický zvyšok modulo $p$ ak $p = 4k+1$ a kvadratický nezvyšok modulo $p$ ak $p = 4k+3$.*

Pomocou predchádzajúceho tvrdenia môžeme ukázať, že existuje nekonečne veľa prvočísel tvaru $4k+1$.

**Tvrdenie 4.2.7.** *Existuje nekonečne veľa prvočísel tvaru $4k+1$.*

*Dôkaz.* Sporom. Predpokladajme, že by $q_1, \ldots, q_n$ boli všetky prvočísla, ktoré majú po delení 4 zvyšok 1. Položme $N = 4q_1^2 q_2^2 \ldots q_n^2 + 1$. Potom $N$ je nepárne zložené číslo a $q_i \nmid N$ pre $i = 1, 2, \ldots, n$. Teda $N$ nemá žiadny prvočiniteľ tvaru $4k+1$.

Na druhej strane, ak $p$ je prvočíslo také, že $p \mid N$, tak $(2q_1 \ldots q_n)^2 \equiv -1 \pmod p$. Teda $-1$ je kvadratický zvyšok modulo $p$ a podľa tvrdenia 4.2.6 má $p$ tvar $4k+1$. Spor. □



Takisto zistiť, kedy je 2 kvadratický zvyšok, nie je príliš zložité. {kvadr:TVRJAC2P}

**Tvrdenie 4.2.8.** *Nech $p > 2$ je prvočíslo. Potom*

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

*Teda 2 je kvadratický zvyšok pre prvočísla tvaru $8k \pm 1$ a kvadratický nezvyšok pre prvočísla tvaru $8k \pm 3$.*

*Dôkaz.* Uvažujme nasledujúcich $\frac{p-1}{2}$ kongruencií:

$$\begin{aligned} p - 1 &\equiv 1(-1)^1 \pmod p \\ 2 &\equiv 2(-1)^2 \pmod p \\ p - 3 &\equiv 3(-1)^3 \pmod p \\ 4 &\equiv 4(-1)^4 \pmod p \\ &\vdots \\ r &\equiv \frac{p-1}{2}(-1)^{(p-1)/2} \pmod p \end{aligned}$$

pričom $r$ je (v závislosti od parity $\frac{p-1}{2}$) buď $p - \frac{p-1}{2}$ alebo $\frac{p-1}{2}$.

Vynásobením týchto kongruencií dostaneme

$$2.4.6 \ldots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\ldots+(p-1)/2} \pmod p.$$

Platí $1 + 2 + \ldots + \frac{p-1}{2} = \frac{1}{2}\frac{p-1}{2}(\frac{p-1}{2} + 1) = \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = \frac{p^2-1}{8}$. Dostávame teda

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8} \pmod p.$$

Pretože $p \nmid (\frac{p-1}{2})!$, vyplýva z toho

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

Ľahko overíme, že ak $p = 8k \pm 1$, tak číslo $\frac{p^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$ je párne a ak $p = 8k \pm 3$, tak $\frac{p^2-1}{8} = \frac{64k^2 \pm 16k + 8}{8} = 8k^2 \pm 2k + 1$ je nepárne. □

**Príklad 4.2.9.** Prvočíslo 7 spĺňa predpoklady predchádzajúceho tvrdenia – je tvaru $8k-1$. Skutočne 2 je kvadratický zvyšok modulo 7, pretože $3^2 \equiv 2 \pmod 7$.

Opäť môžeme tento výsledok použiť na dôkaz existencie nekonečne veľa prvočísel v istej aritmetickej postupnosti.

**Tvrdenie 4.2.10.** *Existuje nekonečne veľa prvočísel tvaru $8k+7$.*

*Dôkaz.* Sporom. Nech $q_1, \ldots, q_n$ sú všetky prvočísla tvaru $8k+7$. Položme $N = (4q_1q_2 \ldots q_n)^2 + 2$. Vidíme, že 2 je kvadratický zvyšok modulo $N$, teda každý prvočíselný deliteľ čísla $N$ musí byť tvaru $8k+7$.

Súčasne však $N \equiv q_i \pmod 2$ pre $i = 1, \ldots, n$, čiže žiadne z prvočísel tvaru $8k+7$ nedelí $N$. Dostali sme hľadaný spor. □

Nasledujúcu vetu sme spomínali v súvislosti s Mersennovými číslami. Pred jej dôkazom pripomeňme, že všetky prvočíselné delitele $M_p = 2^p - 1$, kde $p$ je prvočíslo, sú tvaru $kp + 1$ (tvrdenie 3.1.15).

{kvadr:VTEULMERS}

**Veta 4.2.11.** *Ak $p = 4k + 3$ je prvočíslo, $k > 1$, tak $q = 2p + 1$ je prvočíslo práve vtedy, keď $2p + 1 \mid M_p = 2^p - 1$.*

*Dôkaz.* $\boxed{\Rightarrow}$ Nech $q = 2p+1$ je prvočíslo. Pretože $2p+1 = 8k+7$, číslo 2 je kvadratický zvyšok modulo $2p + 1$. Existuje teda $x$ také, že $x^2 \equiv 2 \pmod{2p + 1}$ z čoho dostaneme na základe Malej Fermatovej vety $2^p \equiv x^{2p} \equiv x^{q-1} \equiv 1 \pmod{q}$, čo znamená, že $q \mid 2^p - 1 = M_p$.

$\boxed{\Leftarrow}$ Ak $2p+1 \mid M_p$, tak všetky delitele $2p+1$ sú súčasne deliteľmi $M_p$, čiže podľa tvrdenia 3.1.15 sú tvaru $kp + 1$. Jediné možnosti sú $2p + 1$ a $p + 1$, pričom párne číslo $p + 1$ nemôže deliť nepárne číslo $2p + 1$. Teda $2p + 1$ skutočne nemá vlastné delitele. □

Užitočným prostriedkom pri výpočte $\left(\frac{a}{p}\right)$ je aj Gaussova lema. Jej dôkaz do istej miery pripomína postup z dôkazu tvrdenia 4.2.8.

**Veta 4.2.12 (Gaussova lema).** *Nech $p > 2$ je prvočíslo a $p \nmid a$. Nech $m$ je počet tých čísel z množiny $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, ktorých zvyšok po delení $p$ je väčší než $\frac{p}{2}$. Potom*

$$\left(\frac{a}{p}\right) = (-1)^m.$$

*Dôkaz.* Dôkaz spočíva vo vyjadrení súčinu $S = a.2a.3a \ldots \frac{p-1}{2}a$ modulo $p$ dvoma rôznymi spôsobmi. Zrejme

$$S = a^{(p-1)/2} \left(\frac{p-1}{2}\right)!$$

Na druhej strane každé a číslo $ka$, $k = 1, 2, \ldots, \frac{p-1}{2}$ sa dá vyjadriť v tvare $sp + z$, kde $z$ je niektorý z prvkov množiny $\{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$. (Prvky tejto množiny sa niekedy zvyknú nazývať najmenšie zvyšky modulo $p$.) Zvyšok $z$ bude záporný práve pre tie čísla, ktorých zvyšok po delení $p$ je väčší ako $\frac{p}{2}$, čiže práve pre $m$ čísel. Pritom žiadne dve z čísel $ka$ nie sú kongruentné modulo $p$ a takisto nemôže nastať situácia $k_1 a \equiv -k_2 a \pmod{p}$. V takomto prípade by totiž platilo $p \mid k_1 + k_2$, čo je v spore s tým, že $k_1, k_2 \in \{1, 2, \ldots, \frac{p-1}{2}\}$.

To znamená, že medzi najmenšími zvyškami čísel $ka$ sa vyskytnú všetky čísla $1, 2, \ldots, \frac{p-1}{2}$, z nich $m$ so záporným a ostatné s kladným znamienkom. Z toho dostaneme

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

z čoho vyplýva $a^{(p-1)/2} \equiv (-1)^m \pmod{p}$. □

Všimnime si, že množina $\{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ použitá v predchádzajúcom dôkaze tvorí redukovaný zvyškový systém.

{kvadr:VTMGAUSS}

**Veta 4.2.13.** *Pre číslo $m$ z Gaussovej lemy platí*

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ak}{p} \right\rfloor \pmod{2}.$$

*Teda*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{2ak}{p} \rfloor}.$$



*Pre nepárne $a$ platí*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor}.$$

*Dôkaz.* Zaujímajú nás zvyšky čísel $ka$, kde $k = 1, 2, \ldots, \frac{p-1}{2}$, po delení prvočíslom $p$.

Podľa lemy 1.3.3 platí

$$\left\lfloor \frac{2ak}{p} \right\rfloor = \begin{cases} 2\lfloor \frac{ak}{p} \rfloor, & \text{ak } 0 \le \{\frac{ak}{p}\} < \frac{1}{2}; \\ 2\lfloor \frac{ak}{p} \rfloor + 1, & \text{ak } \frac{1}{2} \le \{\frac{ak}{p}\}. \end{cases}$$

Z toho vyplýva, že číslo $\lfloor \frac{2ak}{p} \rfloor$ je párne ak $0 \le \{\frac{ak}{p}\} < \frac{1}{2}$ a nepárne v opačnom prípade.

Podľa vety o delení so zvyškom platí $ak = q_k.p + r_k$, z čoho $\{\frac{ak}{p}\} = \{q_k + \frac{r_k}{p}\} = \{\frac{r_k}{p}\} = \frac{r_k}{p}$. Teda $\frac{r_k}{p} \ge \frac{1}{2}$ práve vtedy, keď $r_k \ge \frac{p}{2}$. Číslo $m$ z Gaussovej lemy je teda práve počet tých čísel, pre ktoré je $\lfloor \frac{2ak}{p} \rfloor$ nepárne, z čoho už vyplýva tvrdenie vety.

Pre nepárne $a$ máme

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right).$$

(Pre nepárne $a$ je číslo $\frac{a+p}{2}$ celé.) Už sme ukázali, že Legendrov symbol na pravej strane tejto rovnosti sa rovná

$$(-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{(a+p)}{k} \rfloor}.$$

Sumu v exponente tohto výrazu môžeme upraviť ako

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{(a+p)k}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} \left( \left\lfloor \frac{ak}{p} \right\rfloor + k \right) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ak}{p} \right\rfloor + \frac{p^2-1}{8}.$$

Z toho dostaneme

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor} (-1)^{(p^2-1)/8} = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor} \left(\frac{2}{p}\right),$$

a teda

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor}.$$

□

**Príklad 4.2.14.** Zvyšky čísel 4, 4.2 a 4.3 po delení 7 sú po rade 4, 1 a 5. Z nich $\frac{7}{2}$ presahujú len čísla 4 a 5. Dostávame $m = 2$, teda $\left(\frac{4}{7}\right) = (-1)^2 = 1$.

Keď sa ten istý výraz pokúsime vyjadriť pomocou vety 4.2.13, tak dostaneme $\lfloor \frac{8}{7} \rfloor + \lfloor \frac{16}{7} \rfloor + \lfloor \frac{24}{7} \rfloor = 1 + 2 + 3 = 6$ a $\left(\frac{4}{7}\right) = (-1)^6 = 1$.

## 4.3 Zákon kvadratickej reciprocity

Nasledujúca veta je dosť dôležitá. Ako zaujímavosť môžeme spomenúť, že je známych cez 200 dôkazov tejto vety – pozri `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html` alebo [Lem2].

{kvadr:VTRECIP}

**Veta 4.3.1 (Gaussov zákon kvadratickej reciprocity).** *Ak $p$ a $q$ sú rôzne nepárne prvočísla, tak*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

*Dôkaz.* Skúsme vyrátať počet všetkých dvojíc $(x, y) \in \mathbb{N} \times \mathbb{N}$ takých, že $1 \leq x \leq \frac{p-1}{2}$ a $1 \leq y \leq \frac{q-1}{2}$. Množinu týchto dvojíc označme $S$. Ich počet je samozrejme $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Môžeme ho však vyjadriť aj iným spôsobom.

Tieto dvojice rozdelíme na dve časti. Nech $S_1 = \{(x, y); qx > py\}$ a $S_2 = \{(x, y); qx < py\}$. Skutočne platí $S_1 \cup S_2 = S$, pretože neexistuje dvojica $(x, y) \in S$ taká, že $qx = py$ (ak platí táto rovnosť, tak $q \mid y$ a $p \mid x$). Uvedená situácia je znázornená na obrázkoch 4.1, 4.2 a 4.3.

Obr. 4.1: Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 7$, $q = 5$

{kvadr:FIGREC75}

Ľahko zistíme, že

$$|S_1| = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor,$$

$$|S_2| = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Preto

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{p-1}{2}\frac{q-1}{2},$$

$$(-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor} (-1)^{\sum_{k=1}^{(q-1)/2} \lfloor \frac{kp}{q} \rfloor} = (-1)^{(p-1)/2.(q-1)/2},$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$



Tým je už dôkaz skoro hotový, až na jednu drobnosť – v skutočnosti sme počítali počet mrežových bodov v o čosi väčšom útvare než je náš obdĺžnik - pribudne k nemu ešte maličký trojuholník. (V prípade, že $p > q$ je tento trojuholník nad obdĺžnikom, pozri obrázky.) Poďme sa teda presvedčiť, že tento trojuholník je skutočne natoľko malý, že neobsahuje žiadne mrežové body.

Predpokladajme, že $p > q$. (Zostávajúci prípad je symetrický.) Potom bod $((p-1)/2, (q-1)/2)$ leží pod priamkou $qx = py$, pretože

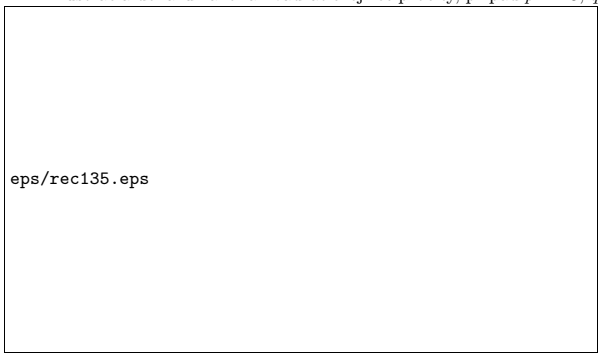
$$q\left(\frac{p-1}{2}\right) - p\left(\frac{q-1}{2}\right) = \frac{p-q}{2} > 0.$$

Nám stačí ukázať, že body s väčšou $y$-vou súradnicou už pod touto priamkou neležia. Očividne to stačí ukázať pre bod $((p-1)/2, (q-1)/2+1)$ s $y$-ouvou súradnicou o jedna vyššou. Skutočne

$$q\left(\frac{p-1}{2}\right) - p\left(\frac{q-1}{2}+1\right) = \frac{q-p}{2} < 0,$$

a teda v trojuholníku, ktorý sme pridali, nie sú žiadne mrežové body. □

Obr. 4.2: Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 13$, $q = 5$




{kvadr:FIGREC135}

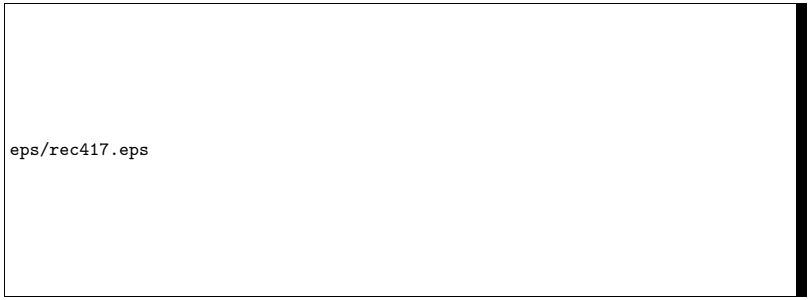
Ľahko vidno, že zákon kvadratickej reciprocity môžeme ekvivalentne preformulovať takto:

**Dôsledok 4.3.2.** *Ak $p \neq q$ sú nepárne prvočísla, tak*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

*s výnimkou prípadu, že $p \equiv q \equiv 3 \pmod 4$. (V tomto prípade $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.)*

Keď existuje také veľké množstvo dôkazov predchádzajúcej vety, bola by hanba, keby sme nespomenuli aspoň jeden ďalší. Základná myšlienka tohoto dôkazu pochádza od E. I. Zolotareva, možno ho nájsť (s rôznymi drobnými obmenami) napríklad v [Lem2, Exercise 1.36], [B] alebo tiež na na [PLA, WIK].




Obr. 4.3: Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 41$, $q = 7$ {kvadr:FIGREC417}

Najprv potrebujeme pripomenúť niektoré základné pojmy súvisiace s permutáciami a ich vlastnosti.

Ak $M$ je konečná množina, ľubovoľná bijekcia $\varphi\colon M \to M$ sa nazýva *permutácia*. Zvyčajne sa pracuje s množinou $\{1, 2, \ldots, n\}$, v nasledujúcom dôkaze však začneme od nuly, pre nás teda $M = \{0, 1, 2, \ldots, n\}$.

Permutácie zapisujeme v takomto tvare: $\left(\begin{smallmatrix}0&1&2&3&4\\0&4&3&2&1\end{smallmatrix}\right)$, kde horné číslo vždy predstavuje prvok z $M$ a dolné číslo jeho obraz.

Špeciálny význam majú *cykly* – permutácie, ktoré cyklicky zobrazujú nejaké prvky z $M$ vždy na nasledujúci. Používame zápis $\varphi = (134)$, ktorý znamená $\varphi(1) = 3$, $\varphi(3) = 4$, $\varphi(4) = 1$ (a ostatné prvky táto permutácia nemení).

Každá permutácia sa dá napísať ako zloženie disjunktných cyklov, napríklad $\left(\begin{smallmatrix}0&1&2&3&4\\0&4&3&2&1\end{smallmatrix}\right) = (14)(23)$.

Cykly dĺžky 2 nazývame *transpozície*. Pretože každý cyklus sa dá rozložiť na transpozície

$$(a_1, \ldots, a_n) = (a_1 a_2)(a_1 a_3) \ldots (a_1 a_n),$$

každú permutáciu možno rozložiť na súčin transpozícií. Pre nás budú dôležité pojmy parita permutácie a znamienko permutácie.

**Definícia 4.3.3.** *Parita permutácie* – podľa toho, či je počet týchto transpozícií párny alebo nepárny, hovoríme o *párnej* alebo *nepárnej* permutácii. (Parita permutácie je určená jednoznačne.)

*Znamienko permutácie* $\epsilon(\tau)$ je 1 pre párnu a -1 pre nepárnu permutáciu.

Platí teda $\epsilon(\tau) = (-1)^k$, kde $k$ je počet transpozícií, na ktoré sa $\tau$ dá rozložiť.

Paritu a znamienko permutácie môžeme počítať aj pomocou inverzií. *Inverzia* permutácie je taká dvojica $(\varphi(i), \varphi(j))$ pre ktorú platí $i < j$ a $\varphi(i) > \varphi(j)$ (čiže tieto prvky majú „nesprávne“ poradie.)

Permutácia je párna práve vtedy, keď má párny počet inverzií, preto $\epsilon(\tau) = (-1)^i$, kde $i$ je počet inverzií permutácie $\tau$.

Z toho, ako sa parita dá vyjadriť pomocou počtu transpozícií, okamžite vidíme užitočnú rovnosť

$$\epsilon(\tau \circ \psi) = \epsilon(\tau).\epsilon(\psi).$$



{kvadr:LMZOLOT}

**Lema 4.3.4 (Zolotarevova lema).** *Nech $p$ je prvočíslo a $m \in \mathbb{Z}_p \setminus \{0\}$. Ako $\tau_m$ označme permutáciu $k \mapsto mk$ množiny $\{0, 1, 2, \ldots, p-1\}$ (pričom $mk$ znamená násobenie v $\mathbb{Z}_p \setminus \{0\}$). Potom platí*

$$\left(\frac{m}{p}\right) = \epsilon(\tau_m).$$

*Dôkaz.* Permutácia $\tau_m$ evidentne ponecháva prvok 0 na mieste, stačí si teda všímať, ako poprehadzuje ostatné prvky.

Vieme, že pre cyklus $\sigma$ dĺžky $k$ je $\epsilon(\sigma) = (-1)^{k-1}$. Nech rád prvku $m$ v grupe $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ je $i$. Potom permutácia $\tau_m$ pozostáva z $\frac{p-1}{i}$ disjunktných cyklov dĺžky $i$, a teda platí $\epsilon(\tau_m) = (-1)^{\frac{(p-1)(i-1)}{i}}$.

Ak $i$ je párne, tak $m^{\frac{i}{2}} = -1$ v $\mathbb{Z}_p$ (čiže $m^{\frac{i}{2}} \equiv -1 \pmod p$), z čoho dostaneme

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \equiv (m^{\frac{i}{2}})^{\frac{p-1}{i}} \equiv (-1)^{\frac{p-1}{i}} \equiv \epsilon(\tau_m) \pmod p.$$

Ak $i$ je nepárne, tak $2i$ delí $p-1$, čiže môžeme písať

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \equiv (m^i)^{\frac{p-1}{2i}} \equiv 1 \equiv \epsilon(\tau_m) \pmod p.$$

Keďže obe čísla, $\left(\frac{m}{p}\right)$ aj $\epsilon(\tau_m)$, môžu nadobúdať iba hodnoty $\pm 1$, tak akonáhle sú kongruentné modulo $p$, musia sa už rovnať. □

**Príklad 4.3.5.** $p = 5$, $m = 3$, $\tau_m = \left(\begin{smallmatrix}0&1&2&3&4\\0&3&1&4&2\end{smallmatrix}\right) = (1342) = (13)(14)(12)$, $\epsilon(\tau_m) = -1 = \left(\frac{3}{5}\right)$
$p = 5$, $m = 2$, $\tau_m = \left(\begin{smallmatrix}0&1&2&3&4\\0&2&4&1&3\end{smallmatrix}\right) = (1243) = (12)(14)(13)$, $\epsilon(\tau_m) = -1 = \left(\frac{2}{5}\right)$
$p = 5$, $m = 4$, $\tau_m = \left(\begin{smallmatrix}0&1&2&3&4\\0&4&3&2&1\end{smallmatrix}\right) = (14)(23)$, $\epsilon(\tau_m) = 1 = \left(\frac{4}{5}\right)$
$p = 3$, $m = 2$, $\tau_m = \left(\begin{smallmatrix}0&1&2\\0&2&1\end{smallmatrix}\right) = (12)$, $\epsilon(\tau_m) = -1 = \left(\frac{2}{3}\right)$

*Dôkaz zákonu reciprocity pomocou Zolotarevovej lemy.* Budeme uvažovať permutáciu $\tau$ množiny $M = \{0, 1, 2, \ldots, pq-1\}$ určenú predpisom

$$\tau(kp + r) = (kp + rq) \mod pq,$$

kde $kp + r$ je vyjadrenie ľubovoľného čísla z $M$ pomocou vety o delení so zvyškom, čiže také vyjadrenie, že $0 \le r < p$ a $0 \le k < q$.

Najprv si ozrejmime, že takto definované $\tau$ je skutočne permutácia $M$. Predpokladajme, že

$$kp + rq \equiv k'p + r'q \pmod{pq}$$

pre nejaké $0 \le r, r' < p$ a $0 \le k, k' < q$. Potom

$$kp \equiv k'p \pmod q,$$
$$rq \equiv r'q \pmod p.$$

a podľa vety 3.1.9

$$k \equiv k' \pmod q,$$
$$r \equiv r' \pmod p.$$

Zistili sme, že $r$ a $r'$ sú také čísla $0 \le r, r' < p$, že $p \mid r - r'$. To je možné jedine pre $r = r'$. Zdôvodnenie, že $k = k'$ je úplne analogické.

Vidíme, že $\tau\colon M \to M$ je injekcia, pretože $M$ je konečná, je to aj bijekcia.

Dôkaz bude spočívať v tom, že dvoma rôznymi spôsobmi vyjadríme znamienko tejto permutácie.

Skúsme zapísať permutáciu $\tau$ trochu inak. Je to vlastne preusporiadanie $pq$ prvkov množiny $M$ v poradí

$$\begin{array}{ccccc} 0 & q & 2q & \dots & (p-1)q \\ p & p+q & p+2q & \dots & p+(p-1)q \\ 2p & 2p+q & 2p+2q & \dots & 2p+(p-1)q \\ \dots & \dots & \dots & \dots & \dots \\ (q-1)p & (q-1)p+q & (q-1)p+2q & \dots & (q-1)p+(p-1)q \end{array}$$

(Uvedené prvky čítame v poradí zľava doprava; v každom riadku by mal byť zvyšok daného čísla po delení $pq$, pre stručnosť ho však vynechávame. Možno to brať tak, že všetky výpočty robíme v $\mathbb{Z}_{pq}$.)

Prvky v jednom stĺpci majú rovnaký zvyšok modulo $p$. V ľubovoľnom riadku máme všetky možné zvyšky po delení $p$. Môžeme poprehadzovať stĺpce tak, aby zvyšky po delení číslom $p$ išli v poradí $0, 1, 2, \dots, p-1$. Označme ako $\alpha$ permutáciu, ktorej zodpovedá takéto preusporiadanie stĺpcov. Znamená to, že v každom riadku sme urobili permutáciu zodpovedajúcu inverznej k permutácii $\tau_q$ z lemy 4.3.4. Táto permutácia jedného riadku pozostáva z rovnakého počtu transpozícií ako $\tau_q$, teda má aj rovnaké znamienko. Pretože sme urobili $w$ takýchto permutácií, máme $\epsilon(\alpha) = \epsilon(\tau_q)^q = \left(\frac{q}{p}\right)^q = \left(\frac{q}{p}\right)$. (Posledná rovnosť vyplýva z toho, že $q$ je nepárne.)

Permutácia $\alpha \circ \tau$ má tvar

$$\begin{array}{ccccc} 0 & pk_1+1 & pk_2+2 & \dots & pk_{p-1}+p-1 \\ p & p(k_1+1)+1 & (pk_2+1)+2 & \dots & p(k_{p-1}+1)+p-1 \\ 2p & p(k_1+2)+1 & (pk_2+2)+2 & \dots & p(k_{p-1}+2)+p-1 \\ \dots & \dots & \dots & \dots & \dots \\ (q-1)p & p(k_1+(q-1))+1 & (pk_2+(q-1))+2 & \dots & p(k_{p-1}+(q-1))+p-1 \end{array}$$

(Presnejšie, v tabuľke by sme mali na každom mieste ešte urobiť zvyšok po delení $pq$, kvôli stručnosti sme ho však vynechali.)

Všimnime si druhý stĺpec. Máme v ňom všetky čísla so zvyškom jedna po delení $p$ v poradí $1, p+1, 2p+1, \dots, (q-1)p+1$, ibaže cyklicky posunuté. Čiže do správneho poradia ich vieme dostať pomocou cyklu dĺžky $q$. Podobne pre ostatné stĺpce. Permutáciu skladajúcu sa z týchto cyklov označme $\beta$. Pretože cyklus nepárnej dĺžky je párna permutácia, máme $\epsilon(\beta) = 1$.

Dostali sme teda $\beta \circ \alpha \circ \tau = id_M$, preto $\epsilon(\alpha).\epsilon(\tau) = 1$, čiže

$$\epsilon(\tau) = \epsilon(\alpha) = \left(\frac{q}{p}\right).$$

Teraz sa pokúsime vyjadriť $\epsilon(\tau)$ iným spôsobom. Opäť začneme takýmto zápisom permutácie $\tau$:

$$\begin{array}{ccccc} 0 & q & 2q & \dots & (p-1)q \\ p & p+q & p+2q & \dots & p+(p-1)q \\ 2p & 2p+q & 2p+2q & \dots & 2p+(p-1)q \\ \dots & \dots & \dots & \dots & \dots \\ (q-1)p & (q-1)p+q & (q-1)p+2q & \dots & (q-1)p+(p-1)q \end{array}$$



Tentokrát však nebudeme vymieňať riadky, ale stĺpce. Všimnime si, že čísla v každom riadku majú rovnaký zvyšok po delení $q$ a že sa vyskytujú všetky možné zvyšky. Zvyšok v $i$-tom riadku, je rovnaký ako zvyšok čísla $p.i$. Použitím permutácie inverznej k $\tau_p$ vieme preusporiadať tieto zvyšky do správneho poradia. Podobnú permutáciu použijeme pre všetky stĺpce. Dostaneme takto permutáciu $\gamma$, ktorej znamienko je $\epsilon(\gamma) = \left(\frac{p}{q}\right)^p = \left(\frac{p}{q}\right)$. Keď ju zložíme s $\tau$, máme

$$\begin{array}{ccccc} 0 & q & 2q & \dots & (p-1)q \\ qk_1+1 & q(k_1+1)+1 & q(k_1+2)+1 & \dots & q(k_1+p-1)+1 \\ qk_2+2 & q(k_2+1)+2 & q(k_2+2)+2 & \dots & q(k_2+p-1)+2 \\ \dots & \dots & \dots & \dots & \dots \\ qk_{q-1}+q-1 & q(k_{q-1}+1)+2 & q(k_{q-1}+2)+2 & \dots & q(k_{q-1}+p-1)+2 \end{array}$$

(V predchádzajúcej tabuľke sme opäť všade vynechali $\bmod pq$.)

Opäť použitím niekoľkých cyklov dĺžky $q$ dostaneme

$$\begin{array}{ccccc} 0 & q & 2q & \dots & (p-1)q \\ 1 & q+1 & 2q+1 & \dots & (p-1)q+1 \\ 2 & q+2 & 2q+2 & \dots & (p-1)q+2 \\ \dots & \dots & \dots & \dots & \dots \\ q-1 & 2q-1 & 3q-1 & \dots & pq-1 \end{array}$$

(Zloženie použitých cyklov označme $\delta$.)

Aké je znamienko permutácie, ktorú sme takto dostali? Všimnime si, že ľubovoľný prvok tvorí inverzie s prvkami, ktoré sú od neho v tabuľke napravo a nahor. Prvok v $i$-tom riadku a $j$-tom stĺpci prispeje k počtu inverzií číslo $(i-1)(j-1)$. Počet inverzií je teda

$$\sum_{i=1}^{q}\sum_{j=1}^{p}(i-1)(j-1) = \sum_{i=0}^{q-1}\sum_{j=0}^{p-1} ij = \left(\sum_{i=0}^{q-1} i\right)\left(\sum_{j=0}^{p-1} j\right) = \frac{q(q-1)}{2}\frac{p(p-1)}{2}.$$

Z toho máme rovnosť

$$\epsilon(\delta \circ \gamma \circ \tau) = \left(\frac{p}{q}\right)\epsilon(\tau) = (-1)^{q(q-1)p(p-1)/4}.$$

Keď použijeme prvé vyjadrenie pre $\epsilon(\tau)$ a fakt, že $p$ a $q$ sú nepárne (a $(p-1)/2$, $(q-1)/2$ sú celé) dostávame

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(q-1)(p-1)/4}.$$

□

Možno predchádzajúci dôkaz bude trochu jasnejší, ak si ukážeme v ňom vystupujúce permutácie na konkrétnom príklade. Skúsme $p = 5$ a $q = 3$ (najmenší možný zmysluplný príklad). Permutácia $\tau$ je potom

$$\begin{array}{ccccc} 0 & 3 & 6 & 9 & 12 \\ 5 & 8 & 11 & 14 & 2 \\ 10 & 13 & 1 & 4 & 7 \end{array}$$

Zvyšky v jednotlivých stĺpcoch po delení 5 sú 0, 3, 1, 4, 2 = permutácia $\tau_3$ množiny $\{0, 1, 2, 3, 4\}$. Čiže preusporiadaním stĺpcov použitím inverznej permutácie k $\tau_3$ dostaneme

$$\begin{array}{ccccc} 0 & 6 & 12 & 3 & 9 \\ 5 & 11 & 2 & 8 & 14 \\ 10 & 1 & 7 & 13 & 4 \end{array}$$

Aby sme dostali identickú permutáciu, ešte treba prehodiť prvky v prvom, druhom a štvrtom stĺpci, čo zodpovedá cyklom $(1, 11, 6)$, $(2, 7, 12)$ a $(4, 14, 9)$. (Sú to cykly dĺžky 3, čiže párne permutácie.)

Pri druhom vyjadrení sme si všimli, že zvyšky v riadkoch po delení 3 sú 0, 2, 1, čiže ich prehodením dostaneme

$$\begin{array}{ccccc} 0 & 3 & 6 & 9 & 12 \\ 10 & 13 & 1 & 4 & 7 \\ 5 & 8 & 11 & 14 & 2 \end{array}$$

(Riadky sme vymenili permutáciou $\tau_2$ množiny $\{0, 1, 2\}$, $\tau_2$ preto, že $5 \mod 3 = 2$.)

Potom ešte treba „zrotovať“ riadky:

$$\begin{array}{ccccc} 0 & 3 & 6 & 9 & 12 \\ 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \end{array}$$

a dostaneme permutáciu, v ktorej vieme zrátať počet inverzií spôsobom uvedeným v dôkaze (všetky inverzie sú také, že jedno z čísel je od druhého napravo a nahor).

{kvadr:PRIKL383}

**Príklad 4.3.6.** Pokúsme sa vypočítať $\left(\frac{219}{383}\right)$ (a tým pádom zistiť, či 219 je kvadratický zvyšok modulo 383.)

Ľahko zistíme, že 383 je prvočíslo a $219 = 3.73$. Máme teda

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

Teraz použijeme zákon kvadratickej reciprocity

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right)(-1)^{382.2/4} = \left(\frac{2}{3}\right)(-1)^{191} = 1$$
$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)(-1)^{382.72/4} = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) \overset{(*)}{=} 1.1 = 1$$

V rovnosti $(*)$ sme využili to, že 73 je tvaru $8k+1$, čiže podľa tvrdenia 4.2.8 je 2 kvadratický zvyšok modulo 73. To, že $9 = 3^2$ je kvadratický zvyšok modulo 73 je zrejmé.

**Príklad 4.3.7.** Nájdite všetky nepárne prvočísla $p$, pre ktoré je 3 kvadratickým zvyškom.

Podľa zákona reciprocity máme

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{(p-1)/2}.$$

Pritom $\left(\frac{p}{3}\right) = 1$ práve vtedy, keď $p = 3k+1$. Podobne $(-1)^{(p-1)/2} = 1$ práve vtedy, keď $p = 4l+1$. Ich súčin bude 1, ak sú obidve 1 alebo obidve $-1$. Teda $\left(\frac{p}{3}\right)$ je 1 práve vtedy, keď $p = 3k+1 = 4l+1$ alebo $p = 3k-1 = 4l-1$ pre nejaké $k$ a $l$. Celkovo teda dostávame, že 3 je kvadratickým zvyškom práve pre prvočísla tvaru $p = 12k \pm 1$. (Kvadratickým nezvyškom bude pre $p = 12k \pm 5$. Pre ostatné zvyšky po delení 12 dostaneme vždy zložené číslo.)

(V predchádzajúcom príklade sme ako jeden z medzivýsledkov dostali $\left(\frac{3}{383}\right) = 1$. Skutočne $383 = 12.32 - 1$.)



## 4.4 Jacobiho symbol

**Definícia 4.4.1.** Nech $P$ je nepárne číslo a $P = p_1 \dots p_r$, kde $p_1, \dots, p_r$ sú (nepárne) prvočísla. Potom *Jacobiho symbol* $\left(\frac{m}{P}\right)$ je definovaný ako

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\dots\left(\frac{m}{p_r}\right).$$

Všimnite si, že prvočísla $p_1, \dots, p_r$ nemusia byť rôzne – ak sa vyskytne nejaké prvočíslo viackrát, viackrát ho zarátame. V prípade, že $n$ je prvočíslo, tak Jacobiho symbol je to isté ako Legendrov symbol.

Z definície vyplýva, že Jacobiho symbol $\left(\frac{m}{P}\right)$ je 0 pre $m$ také, že $(m, P) > 1$. Pre ostatné čísla $m$ môže nadobúdať hodnoty $\pm 1$.

Ak $(m, P) \neq 1$ a kongruencia $x^2 \equiv m \pmod P$ má riešenie, tak $\left(\frac{m}{p_i}\right) = 1$ pre všetky $i = 1, 2, \dots, k$, a teda $\left(\frac{m}{P}\right) = 1$. (Číslo $x$ je totiž riešením všetkých kongruencií $x^2 \equiv m \pmod{p_i}$.) Opačná implikácia však neplatí, ako ukazuje nasledujúci príklad:

**Príklad 4.4.2.** Platí rovnosť $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, ale 2 nie je kvadratický zvyšok modulo 15. (Kvadratické zvyšky modulo 15 sú 1,4,9,10,6.)

Ukážeme niektoré základné vlastnosti Jacobiho symbolu. Ako uvidíme, veľa vlastností, ktoré sme odvodili pre Legendrov symbol, platí aj pre Jacobiho symbol.

{kvadr:LMZAKLJAC}

**Lema 4.4.3.** *Nech $P, Q$ sú nepárne prirodzené čísla a $a, b \in \mathbb{Z}$. Potom*

{kvadr:JAit1}
(i) $a \equiv b \pmod P \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$

{kvadr:JAit2}
(ii) $\left(\frac{1}{P}\right) = 1$

{kvadr:JAit3}
(iii) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$

{kvadr:JAit4}
(iv) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$

{kvadr:JAit6}
(v) *Ak $(b, P) = 1$, tak* $\left(\frac{b^2}{P}\right) = 1$.

{kvadr:JAit5}
(vi) *Ak $(b, P) = 1$, tak* $\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right)$.

*Dôkaz.* Nech $P = p_1 \dots p_m$ a $Q = q_1 \dots q_n$, kde $p_i, q_i \in \mathbb{P}$.

(i) $a \equiv b \pmod P \Rightarrow a \equiv b \pmod{p_i} \Rightarrow \left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$

(ii) $\left(\frac{1}{P}\right) = \prod_{i=1}^m \left(\frac{1}{p_i}\right) = \prod_{i=1}^m 1 = 1$

(iii) $\left(\frac{ab}{P}\right) = \prod_{i=1}^m \left(\frac{ab}{p_i}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right) \prod_{i=1}^m \left(\frac{b}{p_i}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$

(iv) $\left(\frac{a}{PQ}\right) = \prod_{i=1}^m \left(\frac{a}{p_i}\right) \prod_{j=1}^n \left(\frac{a}{q_j}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$

(v) $\left(\frac{b^2}{P}\right) = \prod_{i=1}^m \left(\frac{b^2}{p_i}\right) = \prod_{i=1}^n 1 = 1$

(v) vyplýva (vi) a (iii). □

{kvadr:TVRJACO12P}

**Tvrdenie 4.4.4.** *Nech $P$ je nepárne prirodzené číslo. Potom*

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

*Dôkaz.* Máme $P = p_1 \dots p_r$. Túto rovnosť môžeme prepísať ako

$$P = \prod_{i=1}^{r}(1 + p_i - 1) = 1 + \sum_{i=1}^{r}(p_i - 1) + \sum_{i \neq j}(p_i - 1)(p_j - 1) + \dots$$

Pretože každé $p_i - 1$ je párne, bude každý súčin 2 a viac takýchto čísel deliteľný 4. Preto

$$P - 1 \equiv \sum_{i=1}^{r}(p_i - 1) \pmod 4, \tag{4.1}$$ {kvadr:EQKONG1}

$$\frac{P-1}{2} \equiv \sum_{i=1}^{r}\frac{p_i - 1}{2} \pmod 2. \tag{4.2}$$ {kvadr:EQKONG2}

a

$$\left(\frac{-1}{P}\right) = \prod_{i=1}^{r}(-1)^{(p_i-1)/2} = (-1)^{(P-1)/2}.$$

Na dôkaz druhej rovnosti môžeme použiť podobný postup.

$$P^2 = \prod_{i=1}^{r}(1 + p_i^2 - 1) = 1 + \sum_{i=1}^{r}(p_i^2 - 1) + \sum_{i \neq j}(p_i^2 - 1)(p_j^2 - 1) + \dots$$

Pretože $p_i$ sú nepárne, platí $p_i^2 - 1 \equiv 0 \pmod 8$, preto všetky členy obsahujúce súčin aspoň 2 takýchto výrazov sú deliteľné 64. Z toho dostaneme

$$P^2 - 1 \equiv \sum_{i=1}^{r}(p_i^2 - 1) \pmod{64},$$

$$\frac{P^2-1}{8} \equiv \sum_{i=1}^{r}\frac{p_i^2 - 1}{8} \pmod 8,$$

$$\left(\frac{2}{P}\right) = \prod_{i=1}^{r}(-1)^{(p_i^2-1)/8} = (-1)^{(P^2-1)/8}$$

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

□ {kvadr:VTRECIPJAC}

**Veta 4.4.5 (Zákon reciprocity pre Jacobiho symbol).** *Pre ľubovoľné nepárne prirodzené čísla $P$ a $Q$ platí*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(P-1)(Q-1)/4}.$$

*Dôkaz.* Bez ujmy na všeobecnosti môžeme predpokladať, že $(P, Q) = 1$. (V opačnom prípade sú obe strany rovnosti nulové.)

Nech $P = p_1 \dots p_m$ a $Q = q_1 \dots q_n$, kde $p_i, q_i \in \mathbb{P}$ (prvočísla $p_i$ resp. $q_i$ nemusia byť nutne rôzne). Potom

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i=1}^{m}\prod_{j=1}^{n}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right).$$



Teraz použijeme zákon kvadratickej reciprocity na činitele vystupujúce v súčine na pravej stane poslednej rovnosti. Máme

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{(p_i-1)(q_i-1)/4},$$

z čoho dostaneme

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^r \tag{4.3}$$ {kvadr:EQREJA1}

pre

$$r = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{p_i - 1}{2}\frac{q_i - 1}{2} = \left(\sum_{i=1}^{m}\frac{p_i - 1}{2}\right)\left(\sum_{j=1}^{n}\frac{q_i - 1}{2}\right).$$

V dôkaze tvrdenia 4.4.4 sme ukázali (pozri rovnosť (4.2))

$$\frac{P-1}{2} \equiv \sum_{i=1}^{m}\frac{p_i - 1}{2} \pmod 2$$

a takisto platí aj

$$\frac{Q-1}{2} \equiv \sum_{j=1}^{m}\frac{q_j - 1}{2} \pmod 2.$$

Z toho dostaneme

$$r \equiv \frac{P-1}{2}\frac{Q-1}{2} \pmod 2$$

a z tejto kongruencie spolu s rovnosťou (4.3) už ľahko vyplýva tvrdenie vety. □

Jacobiho symbol často umožňuje zjednodušiť výpočet Legendrovho symbolu.

**Príklad 4.4.6.** S použitím Legendrovho symbolu môžeme trochu zjednodušiť výpočty použité v príklade 4.3.6, kde sme počítali $\left(\frac{219}{383}\right)$ (všimnime si, že 383 je prvočíslo ale $219 = 73.3$).

$$\left(\frac{219}{383}\right) = \left(\frac{383}{219}\right)(-1)^{109.191} = -\left(\frac{383}{219}\right) = -\left(\frac{383-219}{219}\right) =$$
$$-\left(\frac{164}{219}\right) = -\left(\frac{4.41}{219}\right) = -\left(\frac{41}{219}\right) = -\left(\frac{41}{3}\right)\left(\frac{41}{73}\right)$$

Pritom $\left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1$ a opätovným použitím reciprocity dostaneme

$$\left(\frac{41}{73}\right) = \left(\frac{73}{41}\right) = \left(\frac{32}{41}\right) = \left(\frac{2.16}{41}\right) = \left(\frac{2}{41}\right) = 1,$$

lebo 41 má tvar $8k + 1$, teda 2 je kvadratický zvyšok modulo 41.

Celkovo teda dostávame

$$\left(\frac{219}{383}\right) = 1.$$

Uvedeieme ešte jednu aplikáciu Jacobiho symbolu.

**Tvrdenie 4.4.7.** *Nech $a$ je celé číslo, ktoré nie je druhou mocninou celého čísla. Potom existuje nekonečne veľa prvočísel $p$, pre ktoré je $a$ kvadratický nezvyšok.*

*Dôkaz.* Bez ujmy na všeobecnosti môžeme predpokladať, že $a$ nemá kvadratické delitele (pozri lema 4.2.5(v)). Nech teda $a = 2^e q_1 \dots q_n$, pričom $e \in \{0,1\}$ a $n \geq 1$. (Prípad $a = 2$ ošetríme zvlášť.)

Nech $l_1, \dots, l_t$ sú nejaké nepárne prvočísla rôzne od $q_1 \dots q_n$ a $s$ je kvadratický nezvyšok modulo $q_n$. Uvažujme kongruencie

$$\begin{aligned} x &\equiv 1 \pmod{l_i} \qquad \text{pre } i = 1, 2, \dots, t \\ x &\equiv 1 \pmod 8 \\ x &\equiv 1 \pmod{q_j} \qquad \text{pre } j = 1, 2, \dots, n-1 \\ x &\equiv s \pmod{q_n} \end{aligned}$$

Podľa čínskej vety o zvyškoch existuje riešenie tejto sústavy, označme niektoré jej ako $b$.

Zrejme $b$ je nepárne. Z kongruencií $b \equiv 1 \pmod{l_i}$ vyplýva, že v rozklade čísla $b$ sa nevyskytne žiadne z prvočísel $l_1 \dots l_t$.

Pre Jacobiho symbol $\left(\frac{a}{b}\right)$ dostaneme

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{q_1}{b}\right) \dots \left(\frac{q_n}{b}\right).$$

Pritom $b$ je tvaru $8k+1$, takže $\left(\frac{2}{b}\right) = 1$. Súčasne $(b-1)/4$ je párne, teda zo zákona kvadratickej reciprocity máme $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$.

$$\left(\frac{a}{b}\right) = \left(\frac{b}{q_1}\right) \dots \left(\frac{b}{q_n}\right) = \left(\frac{1}{q_1}\right) \dots \left(\frac{1}{q_{n-1}}\right) \left(\frac{s}{q_n}\right) = -1.$$

Teda $a$ je kvadratický nezvyšok modulo $b$, čiže aj modulo každé prvočíslo $p$ vystupujúce v rozklade $b$. Pretože $p \notin \{l_1 \dots l_t\}$, pre každú danú konečnú množinu prvočísel vieme takýmto spôsobom nájsť nejaké ďalšie prvočíslo, modulo ktoré je $a$ kvadratický nezvyšok. To znamená, že takýchto prvočísel je skutočne nekonečne veľa.

Zostáva nám teda doriešiť prípad $a = 2$. Opäť uvažujme ľubovoľnú konečnú množinu prvočísel $\{l_1, \dots, l_t\}$, tentokrát však navyše predpokladajme, že sa medzi nimi nevyskytne 3. Ak položíme

$$b = 8l_1 \dots l_t + 3,$$

tak 2 je kvadratický nezvyšok modulo $b$ a prvočíselné delitele čísla $b$ sú rôzne od $l_1, \dots, l_t$. □

## 4.5 Kvadratické kongruencie modulo zložené čísla

Najprv vyriešime, aká je situácia s mocninami prvočísel. Iný dôkaz nasledujúcej vety môžete nájsť napríklad v [An, Theorem 9-6] alebo [Lev1, Theorem 5-1].

**Veta 4.5.1.** *Nech $p$ je nepárne prvočíslo a $n \geq 1$. Potom $a$ je kvadratický zvyšok modulo $p^n$ práve vtedy, keď $\left(\frac{a}{p}\right) = 1$.*

*Dôkaz.* Ak $x^2 \equiv a \pmod{p^n}$, tak aj $x^2 \equiv a \pmod p$, netriviálna je iba opačná implikácia. Tú dokážeme indukciou vzhľadom na $n$, pričom pre $n = 1$ zrejme platí. Treba teda ukázať, že ak $aRp^n$, tak aj $aRp^{n+1}$.

Majme teda nejaké $x$ také, že

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



a $(x, p) = 1$. Potom platí

$$x^2 \equiv a + bp^n \pmod{p^{n+1}}$$

pre nejaké $b \in \mathbb{Z}$. Zvoľme si $c$ tak, aby platilo $2c \equiv -b \pmod{p^{n+1}}$. Pretože $(2c, p) = 1$, také $c$ existuje podľa vety 3.1.16. Potom máme

$$(x + cp^n)^2 \equiv x^2 + 2cp^n \equiv a + bp^n - bp^n \equiv a \pmod{p^{n+1}}.$$

□

O tom, ako pri riešení polynomiálnych kongruencií prejsť od prvočísel k ich mocninám hovorí Henselova lema, pozri napríklad [Ap, Theorem 5.30] alebo [Nat, Theorem 3.19]. Môžete sa s ňou stretnúť aj na predmete Počítačová algebra 2 [Gur].

Teraz sa pokúsme vyjasniť si situáciu s kvadratickými zvyškami modulo $2^n$.

**Tvrdenie 4.5.2.** *Modulo 2, 4 alebo 8 je jediným nepárnym kvadratickým zvyškom číslo 1.*

*Ak $n \geq 3$, tak existuje $2^{n-3}$ nepárnych kvadratických zvyškov modulo $2^n$ a sú to práve čísla tvaru $8k + 1$.*

*Dôkaz.* Prvú časť tvrdenia môžeme overiť priamym výpočtom.

Aby sme ukázali druhú časť tvrdenia, skúsme najprv určiť počet kvadratických zvyškov modulo $2^n$. Pri tom nám pomôže, ak budeme poznať počet rôznych riešení kongruencie

$$x^2 \equiv 1 \pmod{2^n}.$$

Ak platí $2^n \mid x^2 - 1 = (x+1)(x-1)$, tak máme 2 možnosti. Buď je jedno z čísel $x \pm 1$ kongruentné s 1 a druhé s $2^n$ – takto dostaneme riešenia $\pm 1$. Druhá možnosť je, že sú obe čísla párne. Pretože ich rozdiel je 2, nemôžu byť obidve súčasne násobkom vyššej mocniny dvojky než prvej. Teda jedno z nich musí byť deliteľné $2^{n-1}$, čiže dostaneme ďalšie 2 riešenia $2^{n-1} \pm 1$. Zistili sme teda, že všetky možné riešenia sú $\pm 1, 2^{n-1} \pm 1$, pre $n \geq 3$ sú tieto čísla navzájom rôzne.

Ak teraz $a$ je nepárny kvadratický zvyšok modulo $2^n$, počet riešení kongruencie

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

je opäť 4. Skutočne, ak máme dané jedno riešenie $x$, tak pre všetky ostatné riešenia musí platiť $x^2 \equiv y^2 \pmod{2^n}$, a teda aj

$$(yx^{-1})^2 \equiv 1 \pmod{2^n},$$

kde $x^{-1}$ označuje inverzný prvok k $y$ v grupe redukovaných zvyškových tried modulo $2^n$ (veta 3.1.11). Teda máme 4 rôzne možnosti pre $yx^{-1}$, ktoré nám dajú 4 rôzne riešenia kongruencie $x^2 \equiv a \pmod{2^n}$.

Všetky nepárne kvadratické zvyšky modulo $2^n$ dostaneme tak, že umocníme na druhú všetky nepárne čísla menšie ako $2^n$ (a urobíme zvyšok). Keďže vždy 4 z nich zodpovedajú rovnakému zvyšku, dostaneme celkovo $2^{n-1}/4 = 2^{n-3}$ kvadratických zvyškov. Keďže už vieme, že každý kvadratický zvyšok musí dávať po delení 8 zvyšok 1 a čísel tvaru $8k+1$ menších ako $2^n$ je práve $2^{n-3}$, vidíme, že všetky z nich musia byť kvadratickými zvyškami. □

**Príklad 4.5.3.** Zistite, či 5 je kvadratický zvyšok modulo 44.

Vidíme, že $n = 44 = 2^2.11$, číslo 5 je s týmto číslom nesúdeliteľné. Podľa Čínskej vety o zvyškoch stačí overiť, či 5 je kvadratický zvyšok modulo $2^2$ a 11 . Máme $5 \equiv 1 \pmod 4$, čiže ide o kvadratický zvyšok modulo 4 a

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Teda 5 je kvadratický zvyšok modulo 44. (V tomto jednoduchom prípade by sme to zamozrejme vedeli aj uhádnuť, lebo $7^2 \equiv 5 \pmod{49}$.)

**Cvičenia**

1. Zistite, pre ktoré prvočísla platí $\left(\frac{-3}{p}\right) = 1$ a pre ktoré $\left(\frac{-3}{p}\right) = -1$.
2. Dokážte, že 5 je kvadratický zvyšok pre prvočísla tvaru $10k \pm 1$ a kvadratický nezvyšok pre prvočísla tvaru $10k \pm 3$.
3. Zistite, či sú riešiteľné kongruencie a) $x^2 \equiv 3 \pmod{31}$, b) $x^2 \equiv 5 \pmod{31}$, c) $x^2 \equiv 631 \pmod{1093}$.
4. Zistite, či sú riešiteľné kongruencie a) $x^2 \equiv 17 \pmod{29}$, b) $3x^2 \equiv 12 \pmod{23}$, c) $2x^2 \equiv 27 \pmod{41}$.
5. Zistite, či sú riešiteľné kongruencie a) $x^2 + 5x \equiv 12 \pmod{31}$, b) $x^2 \equiv 19 \pmod{30}$.
6. Zistite, či sú riešiteľné kongruencie a) $x^2 \equiv 3 \pmod{31}$, b) $x^2 \equiv 5 \pmod{31}$, c) $x^2 \equiv 631 \pmod{1093}$.
7. Aký je počet riešení kongruencií a) $x^2 \equiv 5 \pmod{73}$, b) $x^2 \equiv 3 \pmod{73}$?
8. Aký je počet riešení kongruencií a) $x^2 \equiv 226 \pmod{563}$, b) $x^2 \equiv 429 \pmod{563}$?
9. Dokážte, že ak $p = 4k + 1$, tak $\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = 0$ a $\sum_{\substack{a=1 \\ (a|p)=1}}^{p-1} a = \frac{p(p-1)}{2}$.



# Kapitola 5

# Hustoty podmnožín prirodzených čísel

V úvahách o prvočíslach sme už hovorili o tom, že to či je podmnožina prirodzených čísel „veľká“ alebo „malá“ môžeme posudzovať podľa rozličných kritérií. Jednou z možností je použiť niektorú z definícii hustoty – hustota je jednoducho funkcia, ktorá priradí ľubovoľnej podmnožine $\mathbb{N}$ reálne číslo z intervalu $\langle 0, 1\rangle$, pričom väčšie číslo znamená v istom zmysle väčšiu množinu.

Existuje viacero rôznych druhov hustôt, my spomenieme tie najpoužívanejšie.

## 5.1 Asymptotická hustota

Ak máme danú konečnú množinu $B \subset \mathbb{N}$ a podmnožinu $A \subseteq B$, tak pravdepodobnosť, že pri náhodnom výbere jedného prvku z množiny $B$ bude tento prvok patriť do $A$, je $\frac{|A|}{|B|}$ (kde $|M|$ značí počet prvkov množiny $M$). V prípade, že $B = \{1, 2, \ldots, n\}$, tak tento výraz môžeme prepísať v tvare $\frac{A(n)}{n}$, kde $A(n) := |A \cap \{1, 2, \ldots, n\}|$.

V prípade, že existuje limita tohoto podielu pre $n$ idúce do nekonečna, mohla by táto limita v istom zmysle vyjdarovať pravdepodobnosť, že náhodne vybraté prirodzené číslo patrí do $A$. (Hoci táto analógia je dosť nepresná, oblasť teórie čísel, v ktorej sa skúmajú rôzne druhy hustôt, sa skutočne nazýva pravdepodobnostná teória čísel [St], [T].)

{hust:DEFASYMP}

**Definícia 5.1.1.** Pre $A \subseteq \mathbb{N}$ budeme používať označenie $A(n) := |A \cap \{1, 2, \ldots, n\}|$.

Potom hodnota

$$\underline{d}(A) := \liminf_{n\to\infty} \frac{A(n)}{n}$$

sa nazýva *dolná asymptotická hustota* množiny $A$ a

$$\overline{d}(A) := \limsup_{n\to\infty} \frac{A(n)}{n}$$

sa nazýva *horná asymptotická hustota* množiny $A$.

Ak $\underline{d}(A) = \overline{d}(A)$, tak túto hodnotu nazývame *asymptotická hustota množiny* $A$ a označujeme $d(A)$. (V opačnom prípade hovoríme, že $A$ nemá asymptotickú hustotu.)

Ekvivalentne môžeme definíciu asymptotickej hustoty formulovať tak, že

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n},$$

ak táto limita existuje.

Je zrejmé, že $\underline{d}(A), \overline{d}(A) \in \langle 0,1\rangle$ a ak existuje $d(A)$, tak platí aj $d(A) \in \langle 0,1\rangle$. Priamo z definície vidíme, že $d(\emptyset) = 0$ a $d(\mathbb{N}) = 1$.

So špeciálnym prípadom označenia $A(n)$ sme sa už stretli – prvočíselná funkcia $\pi(n)$ je pri takomto značení vlastne $\mathbb{P}(n)$.

Priamo z definície asymptotickej hustoty vyplývajú nasledujúce jednoduché pozorovania.

{asymp:LMDIN01}

**Lema 5.1.2.** *Pre každú podmnožinu $A \subseteq \mathbb{N}$ platí*

$$0 \leq \underline{d}(A) \leq \overline{d}(A) \leq 1.$$

*Ak $A \subseteq B \subseteq \mathbb{N}$, tak*

$$\underline{d}(A) \leq \underline{d}(B) \qquad a \qquad \overline{d}(A) \leq \overline{d}(B).$$

Často je na výpočet hodnoty asymptotickej hustoty výhodné zapísať prvky množiny do rastúcej postupnosti.

{hust:LMDANN}

**Lema 5.1.3.** *Ak $A = \{a_1 < a_2 < \ldots < a_k < \ldots\} \subseteq \mathbb{N}$, tak*

$$\underline{d}(A) = \liminf_{k\to\infty} \frac{k}{a_k}$$
$$\overline{d}(A) = \limsup_{k\to\infty} \frac{k}{a_k}$$
$$d(A) = \lim_{k\to\infty} \frac{k}{a_k}$$

(*Poslednou rovnosťou sa myslí, že limita existuje práve vtedy, keď $A$ má asymptotickú hustotu a v takomto prípade sa tieto dve hodnoty rovnajú.*)

*Dôkaz.* Pre každé $n \geq a_1$ existuje $k \in \mathbb{N}$ také, že $a_k \leq n < a_{k+1}$. Pre také $n$ a $k$ vždy platí $A(n) = k$. Z toho dostávame

$$\frac{k}{a_k} \geq \frac{A(n)}{n} = \frac{k}{n} > \frac{k}{a_{k+1}} = \frac{k+1}{a_{k+1}} - \frac{1}{a_{k+1}}.$$

Pretože $\lim_{k\to\infty} \frac{1}{a_{k+1}} = 0$, dostávame platnosť rovností uvedených vo vete. □

Ako príklad uvedieme hustoty niektorých množín.

**Príklad 5.1.4.** Hustota množiny párnych čísel $d(2\mathbb{N}) = \frac{1}{2}$. Všeobecnejšie, pre ľubovoľnú aritmetickú postupnosť platí $d(a\mathbb{N} + b) = \frac{1}{a}$ (predpokladáme, že $a$ a $b$ sú prirodzené čísla). Skutočne, použitím lemy 5.1.3 pre $A = \{ak + b; n \in \mathbb{N}\}$ dostaneme $d(A) = \lim_{k\to\infty} \frac{k}{ak+b} = \frac{1}{a}$.

Ak $A$ je konečná množina, tak $d(A) = 0$.

Ak $A = \{k^2; k \in \mathbb{N}\}$ je množina všetkých štvorcov, tak máme $d(A) = \lim_{k\to\infty} \frac{k}{k^2} = 0$.

Pre množinu všetkých prvočísel dostávame (z prvočíselnej vety) $d(\mathbb{P}) = \lim_{n\to\infty} \frac{\pi(n)}{n} = \lim_{n\to\infty} \frac{1}{\ln n} = 0$.

V prípade, že chceme zistiť asymptotickú hustotu množiny, ktorá pozostáva z viacerých úsekov po sebe idúcich čísel, bude sa nám hodiť nasledujúca lema.



{asymp:LMUSEKY}

**Lema 5.1.5.** *Nech $a_n$, $b_n$ sú rastúce postupnosti prirodzených čísel také, že $a_n < b_n$ pre každé $n \in \mathbb{N}$. Potom pre množinu $A = \mathbb{N} \cap \bigcup_{n=1}^{\infty} (a_n, b_n\rangle$ platí*

$$\overline{d}(A) := \limsup_{n\to\infty} \frac{A(b_n)}{b_n}$$
$$\underline{d}(A) := \liminf_{n\to\infty} \frac{A(a_n)}{a_n}$$

*Dôkaz.* Nerovnosť $\overline{d}(A) \geq \limsup_{n\to\infty} \frac{A(b_n)}{b_n}$ vyplýva z toho, že ide o limes superior z podpostupnosti postupnosti $\frac{A(n)}{n}$ vystupujúcej v definícii hornej asymptotickej hustoty.

Na druhej strane, pre $b_{n-1} < k \leq a_n$ platí $A(k) = A(b_{n-1})$, a teda

$$\frac{A(k)}{k} \leq \frac{A(b_{n-1})}{b_{n-1}}$$

zatiaľčo pre $a_n < k \leq b_n$ máme

$$\frac{A(k)}{k} = \frac{A(b_n) - (b_n - k)}{b_n - (b_n - k)} \leq \frac{A(b_n)}{b_n}$$

(posledná nerovnosť vyplýva z toho, že $A(b_n) \leq b_n$.) Dostávame teda skutočne

$$\overline{d}(A) := \limsup_{n\to\infty} \frac{A(b_n)}{b_n}.$$

Analogická nerovnosť pre dolnú asymptotickú hustotu sa dokáže podobne (alebo prechodom k množine $\mathbb{N} \setminus A$). □

Ďalej uvedieme príklad množiny, ktorá nemá asymptotickú hustotu. Postup, ako skonštruovať také príklady je zrejmý – stačí množinu vytvoriť tak, že zoberieme dostatočne dlhé súvislé úseky prirodzených čísel, ktoré zabezpečia, že na ich konci bude podiel $\frac{A(n)}{n}$ veľký a za každým takým úsekom zasa dosť veľa prirodzených čísel vynecháme, aby sme dosiahli, že na konci vynechaného úseku bude hodnota tohoto podielu malá.

{asymp:PRDIGIT}

**Príklad 5.1.6.** Nech $A = \bigcup_{n=0}^{\infty} \{3^{2n}, \ldots, 3^{2n+1} - 1\}$, čiže $A$ je množina všetkých čísel, ktorých zápis v trojkovej sústave má nepárny počet cifier.

Použijeme lemu 5.1.5 pre $a_n = 3^{2n} - 1$, $b_n = 3^{2n+1} - 1$. Dostávame

$$A(b_n) = \sum_{k=0}^{\infty} 3^{2n+1} - 3^{2n} = \sum_{k=0}^{\infty} 2.3^{2n} = 2 \cdot \frac{3^{2(n+1)} - 1}{8} = \frac{3 \cdot 3^{2n+1} - 1}{4} = \frac{3b_n - 1}{4}$$

z čoho

$$\overline{d}(A) = \lim_{n\to\infty} \frac{3b_n - 1}{4b_n} = \frac{3}{4}.$$

Z rovnosti $A(a_n) = a_{b_{n-1}}$ dostaneme podobným spôsobom $\underline{d}(A) = \frac{1}{4}$.

Zo známych vlastností lim sup a lim inf a z jednoduchého pozorovania, že ak $A \cap B = \emptyset$, tak $(A \cup B)(n) = A(n) + B(n)$, možno odvodiť nasledujúce vlastnosti hornej a dolnej asymptotickej hustoty.

{asymp:LMCUP}

**Lema 5.1.7.** *Nech $A, B \subseteq \mathbb{N}$, $A \cap B = \emptyset$. Potom platí*

$$\underline{d}(A) + \underline{d}(B) \leq \underline{d}(A \cup B) \leq \underline{d}(A) + \overline{d}(B) \leq \overline{d}(A \cup B) \leq \overline{d}(A) + \overline{d}(B).$$

Ako dôsledok dostávame, že asymptotická hustota je konečne-aditívna na systémy tých podmnožín $\mathbb{N}$, ktoré majú hustotu a tiež vzťah medzi asymptotickou hustotou nejakej podmnožiny $\mathbb{N}$ a jej doplnku.

{asymp:DOSFINADD}

**Dôsledok 5.1.8.** *Ak množiny $A, B \subseteq \mathbb{N}$ majú asymptotickú hustotu a $A \cap B = \emptyset$, tak*

$$d(A \cup B) = d(A) + d(B).$$

*Podobne, ak $A_1, \ldots, A_n$ sú disjunktné podmnožiny $\mathbb{N}$, ktoré majú asymptotickú hustotu, tak*

$$d\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} d(A_i).$$

{asymp:DOSKOMPL}

**Dôsledok 5.1.9.** *Nech $A \subseteq \mathbb{N}$. Potom $\overline{d}(\mathbb{N} \setminus A) = 1 - \underline{d}(A)$, $\underline{d}(\mathbb{N} \setminus A) = 1 - \overline{d}(A)$. Ak existuje $d(A)$ tak existuje aj $d(\mathbb{N} \setminus A)$ a platí $d(\mathbb{N} \setminus A) = 1 - d(A)$.*

Ako jedno z kritérií na posúdenie, či je množina veľká alebo malá sme používali vlastnosť, či rad prevrátených hodnôt prvkov tejto množiny konverguje alebo diverguje. Nasledujúce tvrdenie ukazuje ako táto vlastnosť súvisí s asymptotickou hustotou. Tento výsledok sme už dokázali (iným spôsobom) v tvrdení 2.3.4. (Hoci spomínané tvrdenie hovorí iba o množine prvočísel, jeho dôkaz prejde pre ľubovoľnú podmnožinu $\mathbb{N}$.)

{asymp:TVRPREVR}

**Tvrdenie 5.1.10.** *Ak $A = \{a_1 < a_2 < \ldots < a_n < \ldots\} \subseteq \mathbb{N}$ a rad $\sum_{k=1}^{\infty} \frac{1}{a_k}$ konverguje, tak množina $A$ má asymptotickú hustotu a $d(A) = 0$.*

*Dôkaz.* Ak rad $\sum_{k=1}^{\infty} \frac{1}{a_k}$ konverguje, tak podľa Cauchy-Bolzanovho kritéria existuje pre každé $\varepsilon$ také $n_0$, že pre $n > n_0$ a ľubovoľné $p \in \mathbb{N}$ platí

$$\sum_{k=n}^{n+p} \frac{1}{a_k} < \varepsilon.$$

Z toho dostávame

$$\varepsilon > \sum_{k=n}^{2n} \frac{1}{a_k} \geq n \frac{1}{a_{2n}},$$

$$2\varepsilon > \frac{2n}{a_{2n}}.$$

Teda pre všetky $m \geq 2n_0$ platí $\frac{m}{a_m} < 2\varepsilon$ a teda $d(A) = \lim_{m \to \infty} \frac{m}{a_m} = 0$. □

Príkladom ukazujúcim, že uvedená implikácia sa nedá obrátiť, je množina všetkých prvočísel $\mathbb{P}$.

Ďalej sa budeme zaoberať asymptotickými hustotami množiny hodnôt danej aritmetickej funkcie $f$. Najprv však uvedieme niektoré tvrdenia, ktoré budú pri tom užitočné.

Pre ľubovoľné $p \in \mathbb{N}$ a $A \subset \mathbb{N}$ označme ako $A_p$ podmnožinu

$$A_p := \{k \in A; p \mid k \wedge p^2 \nmid k\}.$$

Pri odhade asymptotickej hustoty niektorých množín bude pre nás užitočné nasledujúce tvrdenie pochádzajúce z [Niv1] (pozri tiež [KLŠZ, Veta 1.3.8]).



{asymp:TVRHUSTPRVRA

**Tvrdenie 5.1.11.** *Nech $(q_n)_{n=1}^{\infty}$ je postupnosť prvočísel taká, že rad ich prevrátených hodnôt diverguje, t.j.,*

$$\sum_{k=1}^{\infty} \frac{1}{q_k} = +\infty.$$

*Nech pre každé $k \in \mathbb{N}$ platí $d(A_{q_k}) = 0$. Potom aj*

$$d(A) = 0.$$

Dôkaz o niečo slabšieho tvrdenia – ak predpoklad vety nahradíme tým, že pre každé prvočíslo $q_k$ je $d(\{n \in A; q_k \mid n\}) = 0$ – je uvedený v [PS, Věta 20].

Z predchádzajúceho tvrdenia dostávame, že asymptotická hustota množiny všetkých prvočísel je nulová – tentokrát bez použitia prvočíselnej vety.

**Dôsledok 5.1.12.** *Množina všetkých prvočísel má nulovú asymptotickú hustotu 0, t.j.*

$$d(\mathbb{P}) = 0.$$

Pekný dôkaz toho, že $d(\mathbb{P}) = 0$, bez použitia prvočíselnej vety možno nájsť v [ŠHHK, Lema 3.5.1] a v [Ma].

V dôkaze tvrdenia 5.1.11 budeme potrebovať 2 pomocné lemy.

Najprv uvedieme jeden výsledok hovoriaci o nekonečných súčinoch. Nekonečné súčiny môžeme definovať podobne ako nekonečné rady, pomocou limity čiastočných súčinov – pričom treba ale byť trochu opatrný ak sa v danom rade vyskytujú nuly. Prehľad základných poznatkov o nekonečných súčinoch sa dá nájsť napríklad v [Š1] alebo tiež v [Kno].

{asymp:LMRADPROD}

**Lema 5.1.13.** *Nech $(a_n)_{n=1}^{\infty}$ je postupnosť čísel takých, že $0 < a_k < 1$ a*

$$\sum_{k=1}^{\infty} a_k = +\infty.$$

*Potom*

$$\prod_{k=1}^{\infty} (1 - a_k) = 0.$$

*Dôkaz.*

$$\prod_{k=1}^{n} (1 - a_k) \leq \frac{1}{\prod_{k=1}^{n} (1 + a_k)} \leq \frac{1}{1 + \sum_{k=1}^{n} a_k}.$$

□

{asympt:LMBRN}

**Lema 5.1.14.** *Nech $q_1 < q_2 < \ldots < q_n$ sú prvočísla. Nech*

$$B^{(r)} = \mathbb{N} \setminus \left(\bigcup_{j=1}^{r} \mathbb{N}_{q_j}\right).$$

*Potom*

$$B^{(r)}(m) = \sum (-1)^{\alpha_1 + \ldots + \alpha_r} \left\lfloor \frac{m}{q_1^{\alpha_1} \ldots q_r^{\alpha_r}} \right\rfloor, \tag{5.1}$$

{asymp:EQBRN}

*kde posledná suma sa berie cez všetky $\alpha_i \in \{0, 1, 2\}$.*

*Dôkaz.* Dôkaz tejto lemy spočíva v princípe len v použití princípu inklúzie a exklúzie. Všimnime si napríklad, že množina $\mathbb{N}_{q_1}$ obsahuje práve

$$\left\lfloor \frac{m}{q_1} \right\rfloor - \left\lfloor \frac{m}{q_1^2} \right\rfloor$$

čísel menších alebo rovných $m$. (Od počtu čísel deliteľných $q_1$ sme odrátali počet tých, ktoré sú deliteľné číslom $q_1^2$.)

Podobne

$$(\mathbb{N}_{q_1} \cap \mathbb{N}_{q_2})(m) = \left\lfloor \frac{m}{q_1 q_2} \right\rfloor - \left\lfloor \frac{m}{q_1^2 q_2} \right\rfloor - \left\lfloor \frac{m}{q_1 q_2^2} \right\rfloor + \left\lfloor \frac{m}{q_1^2 q_2^2} \right\rfloor.$$

(Opäť sme spočítali čísla deliteľné $q_1 q_2$ a odrátali tie, ktoré z nich sú deliteľné $q_1^2$ alebo $q_2^2$.)

Analogicky sa dá postupovať aj pre ostatné čísla. (Dôkaz je podrobne uvedený v [KLŠZ, s. 24, Lema 1.3.9].) □

*Dôkaz tvrdenia 5.1.11.* Všimnime si, že pre ľubovoľné $r \in \mathbb{N}$ a $j \in \{1, 2, \ldots, r\}$ máme

$$A_{q_j} = A \cap \mathbb{N}_{q_j}$$

$$A = \left( A \setminus \bigcup_{j=1}^{r} A_{q_j} \right) \cup (A_{q_1} \cup \ldots \cup A_{q_r})$$

Pritom

$$A \setminus \bigcup_{j=1}^{r} A_{q_j} \subseteq B^{(r)},$$

z čoho dostaneme odhad

$$\frac{A(n)}{n} \leq \frac{B^{(r)}(n)}{n} + \sum_{j=1}^{r} \frac{A_{q_j}(n)}{n}.$$

Z rovnice (5.1) dostaneme

$$\frac{B^{(r)}(n)}{n} = \frac{\sum (-1)^{\alpha_1+\ldots+\alpha_r} \left\lfloor \frac{n}{q_1^{\alpha_1} \ldots q_r^{\alpha_r}} \right\rfloor}{n} \leq \frac{\sum \left( (-1)^{\alpha_1+\ldots+\alpha_r} \frac{n}{q_1^{\alpha_1} \ldots q_r^{\alpha_r}} + 1 \right)}{n} \overset{(*)}{=}$$

$$\frac{3^r}{n} + \sum \frac{(-1)^{\alpha_1+\ldots+\alpha_r}}{q_1^{\alpha_1} \ldots q_r^{\alpha_r}} = \frac{3^r}{n} + \prod_{j=1}^{r} \left( 1 - \frac{1}{q_j} + \frac{1}{q_j^2} \right)$$

(Rovnosť $(*)$ platí vďaka tomu, že počet sčítancov v sume je $3^r$.) Pretože diverguje rad $\sum_{j=1}^{\infty} \frac{1}{q_j}$, diverguje aj rad $\sum_{j=1}^{\infty} \left( \frac{1}{q_j} - \frac{1}{q_j^2} \right)$. (Od divergentného radu sme odčítali konvergentný.) Podľa lemy 5.1.13 potom platí $\prod_{j=1}^{\infty} \left( 1 - \frac{1}{q_j} + \frac{1}{q_j^2} \right) = 0$. Vďaka tomu môžeme zvoliť dostatočne veľké $r$ tak, aby platilo

$$\prod_{j=1}^{r} \left( 1 - \frac{1}{q_j} + \frac{1}{q_j^2} \right) < \frac{\varepsilon}{4}.$$

(Všetky doterajšie úvahy sme robili pre ľubovoľné $r$, odteraz budeme mať pevne zvolené $r$ s touto vlastnosťou.)



Pre takto zvolené $r$ existuje $n_0$ také, že pre $n > n_0$ platí $\frac{3^r}{n} < \frac{\varepsilon}{4}$.

Súčasne vieme, že $d(A_{q_j}) = 0$. Teda opäť existuje $n_j$ tak, že pre $n > n_1$ je $\frac{A_{q_j}(n)}{n} < \frac{\varepsilon}{2r}$ (pre $j = 1, 2, \ldots, r$), preto

$$\sum_{j=1}^{r} \frac{A_{q_j}(n)}{n} < \frac{\varepsilon}{2}.$$

Celkove v súčte dostaneme

$$\frac{A(n)}{n} < \frac{3^r}{n} + \prod_{j=1}^{r} \left( 1 - \frac{1}{q_j} + \frac{1}{q_j^2} \right) + \sum_{j=1}^{r} \frac{A_{q_j}(n)}{n} < \frac{\varepsilon}{4} + \frac{\varepsilon}{4} + \frac{\varepsilon}{2} = \varepsilon$$

pre všetky $n > \max\{n_0, n_1, \ldots, n_r\}$. □

Z práve uvedenej vety môžeme odvodiť viaceré vcelku zaujímavé dôsledky.

{asymp:VTDMK}

**Veta 5.1.15.** *Nech $M(k)$ označuje množinu všetkých prirodzených čísel, ktoré majú najviac $k$ prvočíselných deliteľov. Potom*

$$d(M(k)) = 0.$$

*Dôkaz.* Uvažujme teraz množinu všetkých prvočísel. O nej vieme, že rad prevrátených hodnôt diverguje (veta 2.3.3), preto môžeme použiť tvrdenie 5.1.11.

Najprv ukážeme tvrdenie vety pre $M(1)$, čiže pre množinu všetkých čísel, ktoré obsahujú vo svojom kanonickom rozklade práve jedno prvočíslo (inými slovami práve mocniny prvočísel). Pre túto množinu platí $M(1)_{p_j} = \{p_j\}$, teda $d(M(1)_{p_j}) = 0$. Z tvrdenia 5.1.11 máme potom $d(M(1)) = 0$.

Predpokladajme, že tvrdenie platí pre $M(k-1)$. Ak $m \in M(k)_p$ pre nejaké prvočíslo, tak prvočíslo $p$ sa v rozklade čísla $m$ vyskytuje v prvej mocnine. Potom $\frac{m}{p} \in M(k-1)$. Pretože $d(M(k-1)) = 0$ a nerovnosť $m \leq n$ je ekvivalentná s nerovnosťou $\frac{m}{p} \leq \frac{n}{p}$, máme

$$\frac{M(k)_p(n)}{n} \leq \frac{M(k-1)\left(\frac{n}{p}\right)}{n} \leq \frac{M(k-1)(n)}{n} \longrightarrow 0.$$

Opäť podľa tvrdenia 5.1.11 máme $d(M(k)) = 0$. □

Teraz ukážeme, že množina hodnôt Eulerovej funkcie má nulovú asymptotickú hustotu. Pripomeňme (veta 3.3.4), že

$$\varphi(n) = n \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right),$$

kde $p_1, \ldots, p_k$ sú všetky prvočinitele čísla $n$.

**Veta 5.1.16.** *Nech $E = \{\varphi(n); n \in \mathbb{N}\}$ je množina hodnôt Eulerovej funkcie $\varphi$. Potom $d(E) = 0$.*

*Dôkaz.* Zvoľme si $k \in \mathbb{N}$. Označme ako $B$ množinu tých prvkov z $E$, ktoré sú deliteľné $2^k$ a $C$ množinu tých, ktoré nie sú deliteľné $2^k$. Zrejme

$$B(n) \leq \frac{n}{2^k},$$

preto $\overline{d}(B) \leq \frac{1}{2^k}$.

Pokúsime sa ešte odhadnúť čísla z druhej množiny. Ak $m = p_1^{a_1} \dots p_s^{a_s}$ je kanonický rozklad čísla $m$, tak

$$\varphi(m) = (p_1^{a_1} - p_1^{a_1-1}) \dots (p_s^{a_s} - p_s^{a_s-1}).$$

Pre prvočíslo $p > 2$ je $p^a - p^{a-1}$ párne číslo, $2^{s-1} \mid \varphi(m)$. To znamená, že $m \in C$ má najviac $k-1$ nepárnych prvočiniteľov, čiže celkový počet prvočiniteľov je najviac $k$. Označme

$$C^* = \{n; \varphi(n) \in C\}.$$

Práve sme dokázali, že $C^* \subseteq M(k)$, čiže $d(C^*) = 0$. Súčasne pre $n \in C^*$ platí $\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s}) \geq \frac{n}{2^k}$. Teda $C(n) \leq C^*(2^k n)$, čiže

$$\lim_{n\to\infty} \frac{C^*(n)}{n} \leq \lim_{n\to\infty} \frac{C(2^k n)}{n} = 2^k d(C) = 0,$$

z čoho vyplýva $d(C) = 0$.

Celkovo dostávame

$$\overline{d}(E) \leq \overline{d}(B) + d(C) \leq \frac{1}{2^k}.$$

Pretože to platí pre ľubovoľné $k$, máme $\overline{d}(E) = 0$. □

Budeme sa zaoberať asymptotickou hustotou množiny hodnôt ešte jednej aritmetickej funkcie – funkcie $\sigma$. [1]

{asymp:LMDMK}

**Lema 5.1.17.** *Majme dané nejaké (pevne zvolené) $k \in \mathbb{N}$. Nech*

$$M^{(k)} = \{p_1 p_2 \dots p_k n^2; n \in \mathbb{N}, p_1, \dots, p_k \text{ sú rôzne prvočísla a } p_i \nmid n\}.$$

*Potom*

$$d(M^{(k)}) = 0.$$

Inými slovami, vyšetrujeme asymptotickú hustotu množiny takých čísel, ktoré sú súčinom nejakého štvorca a čísla obsahujúceho najviac $k$ prvočiniteľov. Pokúsime sa ju vypočítať podobným postupom, ako sme dokázali vetu 5.1.15.

*Dôkaz.* Budeme využívať tvrdenie 5.1.11 a takisto označenie $A_p$ kde $A \subseteq \mathbb{N}$ a $p \in \mathbb{P}$ má rovnaký význam ako v spomínanom tvrdení.

Indukciou na $k$. Začneme s množinou $M^{(1)} = \{pn^2; p \in \mathbb{P}, n \in \mathbb{N}, p \nmid n\}$. Máme

$$M_p^{(1)} = \{pn^2; n \in \mathbb{N}, p \nmid n\}.$$

Pre ľubovoľné $p \in \mathbb{P}$ teda platí $d(M_p^{(1)}) = 0$, a teda podľa tvrdenia 5.1.11 aj $d(M^{(1)}) = 0$.

Predpokladajme, že $d(M^{(k-1)})$. Opäť by sme potrebovali odhadnúť $d(M_p^{(k)})$. Táto množina obsahuje prvky tvaru $p.p_2 p_3 \dots p_k n^2$, kde $n \in \mathbb{N}$ a $p_2, \dots, p_k$ sú ľubovoľné prvočísla. Inak povedané, jej prvky sú tvaru $p.l$ kde $l \in M^{(k-1)}$.

Preto opäť máme

$$\frac{M^{(k)}(n)}{n} \leq \frac{M^{(k-1)}\left(\frac{n}{p}\right)}{n} \to 0.$$

□

[1] Ako si všimli napríklad aj autori článku [RM]; dôkaz, že množina hodnôt pre funkciu $\sigma$ ako aj pre jej zovšeobecnenie – súčet $k$-tych mocnít deliteľov daného čísla – má nulovú asymptotickú hustotu, ktorý je uvedený v [Niv1] a opiera sa o vetu 5.1.15, obsahuje chybu. Istá modifikácia tohoto dôkazu je uvedená v [KLŠZ, Príklad 1.3.14]. Z toho dôvodu sme tu zvolili iný dôkaz.



Zaujíma nás asymptotická hustota množiny

$$F = \{\sigma(n); n \in \mathbb{N}\}.$$

{asymp:TVRDSN}

**Tvrdenie 5.1.18.** *Nech*

$$F = \{\sigma(n); n \in \mathbb{N}\},$$

*kde $\sigma$ označuje súčet deliteľov čísla $n$. Potom*

$$d(F) = 0.$$

*Dôkaz.* Nech $\varepsilon > 0$. Zvoľme $k$ tak, aby $2^{-k} \leq \varepsilon$. Ukážeme, že $\overline{d}(F) \leq \varepsilon$.

Rozdeľme množinu $F$ na dve disjunktné časti.

$$F_1 = \{\sigma(n); n \notin M^{(k)}\} \qquad \text{a} \qquad F_2 = \{\sigma(n); n \in M^{(k)}\},$$

pričom označenie $M^{(k)}$ znamená množinu z lemy 5.1.17.

Ak $n \notin M^{(k)}$, tak v prvočíselnom rozklade čísla $n = p_1^{a_1} \dots p_s^{a_s}$ je aspoň $k+1$ prvočísel s nepárnym exponentom, z týchto prvočísel je aspoň $k$ nepárnych. Pre ne samozrejme platí $2 \mid \sigma(p^a) = 1 + p + \dots + p^a$, a teda

$$2^k \mid \sigma(n).$$

Preto $\overline{d}(F_1) \leq \frac{1}{2^k} \leq \varepsilon$.

Pretože $F_2 = \{\sigma(n); n \in M^{(k)}\}$ a $\sigma(n) \geq n$, máme

$$F_2(m) \leq M^{(k)}(m)$$

a vďaka tomu, že $d(M^{(k)}) = 0$ dostaneme $d(F_2) = 0$.

Celkovo teda dostávame

$$\overline{d}(F) \leq \overline{d}(F_1) + d(F_2) \leq \varepsilon.$$

Pretože za $\varepsilon$ môžeme zvoliť ľubovoľné nezáporné číslo, znamená to, že

$$d(F) = 0.$$

□

**Cvičenia**

1. Nech $A \subseteq \mathbb{N}$ a $0 < a < b$ sú reálne čísla. Ak platí $\liminf_{n\to\infty} \frac{A(bn)}{A(an)} > 1$, tak množina $Q(A)$ všetkých čísel tvaru $\frac{p}{q}$, $p, q \in A$, je hustá v intervale $\langle 0, +\infty)$.
2. Nech $\alpha \in \langle 0, 1\rangle$. Dokážte, že existuje podmnožina $A \subseteq \mathbb{N}$ taká, že $d(A) = \alpha$.
3. Označme ako $T_\alpha$ (kde $\alpha \in \langle 0, 1\rangle$) systém všetkých podmnožín množiny $\mathbb{N}$ takých, že $d(A) = \alpha$. Ukážte, že množina $T_\alpha$ je nespočítateľná.
4. Nech $0 \leq a \leq b \leq 1$. Ukážte, že existuje podmnožina $A \subseteq \mathbb{N}$ taká, že $\underline{d}(A) = a$ a $\overline{d}(A) = b$.
5. Množina všetkých párnych dokonalých čísel má asymptotickú hustotu 0.
6. Aká je asymptotická hustota množiny všetkých mocnín prvočísel?
7. Dokážte, že množiny $\{2^k; k \in \mathbb{N} \cup \{0\}\}$ a $\{2^k 3^l; k, l \in \mathbb{N} \cup \{0\}\}$ majú asymptotickú hustotu 0.

8. Majme množiny $A = \{a_1 < a_2 < \ldots < a_n < \ldots\}$ a $B = \{b_1 < b_2 < \ldots < b_n < \ldots\}$, ktoré majú asymptotickú hustotu. Nech $A_B := \{a_{b_n}; n \in \mathbb{N}\}$. Dokážte, že $d(A_B) = d(A).d(B)$.

9. Nech $A = \{a_1 < a_2 < \ldots < a_n < \ldots\} \subseteq \mathbb{N}$. Ak $A$ má asumptotickú hustotu a $d(A) > 0$, tak $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 1$.

10. Nech $A = \{a_1 < a_2 < \ldots < a_n < \ldots\} \subseteq \mathbb{N}$. Ak existuje limita $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} > 1$, tak $d(A) = 0$.

11. Nájdite príklad množiny takej, že $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 1$ a súčasne $d(A) = 0$.

12. Pre $q \in \mathbb{N}$ definujeme $\mathbb{N}^q$ ako množinu všetkých prirodzených čísel nesúdeliteľných s $q$. Dokážte, že $d(\mathbb{N}^q) = \frac{\varphi(q)}{q}$.

## 5.2 Schnireľmannova hustota

**Definícia 5.2.1.** Pre $A \subseteq \mathbb{N}$ je

$$\sigma(A) = \inf_{n\in\mathbb{N}} \frac{A(n)}{n}$$

*Schnireľmannova hustota* množiny $A$.

Oproti asymptotickej hustote má Schnireľmanova hustota výhodu, že je definovaná pre ľubovoľnú podmnožinu množiny $\mathbb{N}$. Má však aj nevýhody – je veľmi citlivá na zmeny najmenších čísel v množine $A$, čo je v istom zmysle nevýhodné.

Nasledujúce vlastnosti Schnireľmanovej hustoty sú zrejmé:

{schnir:LM1}

**Lema 5.2.2.** *Nech $A \subseteq \mathbb{N}$.*

(i) $0 \le \sigma(A) \le 1$

(ii) *Ak $1 \notin A$ alebo ak $A$ je konečná množina, tak $\sigma(A) = 0$.*

{schnir:LM1it4}

(iii) *Rovnosť $\sigma(A) = 1$ platí práve vtedy, keď $A = \mathbb{N}$.*

(iv) *Pre každé $n \in \mathbb{N}$ platí $A(n) \ge n\sigma(A)$.*

(v) *Ak $A \subseteq B$, tak $\sigma(A) \le \sigma(B)$.*

Vzťah medzi asymptotickou a Schnireľmanovou hustotou je popísaný v nasledujúcom tvrdení.

**Tvrdenie 5.2.3.** *Nech $A \subseteq \mathbb{N}$ a $1 \in A$. Potom $\underline{d}(A) = 0$ práve vtedy, keď $\sigma(A) = 0$.*

*Dôkaz.* Je zrejmé, že ak $\liminf_{n\to\infty} \frac{A(n)}{n} = 0$, tak aj $\inf \frac{A(n)}{n} = 0$.

Obrátene, ak $1 \in A$, tak množina $\{\frac{A(n)}{n}\}$ neobsahuje nulu. Aby teda infimum tejto množiny bolo 0, musí platiť $\liminf_{n\to\infty} \frac{A(n)}{n} = 0$. □

Teraz vypočítame Schnireľmanovu hustotu pre niektoré množiny.

**Dôsledok 5.2.4.** $\sigma(\{1\} \cup \{\mathbb{P}\}) = 0$



Takisto z predchádzajúceho tvrdenia vyplýva, že $\sigma(\{n^2; n \in \mathbb{N}\}) = 0$.

Podobne ako pri asymptotickej hustote môže byť niekedy výhodné usporiadať si danú množinu do rastúcej postupnosti.

**Lema 5.2.5.** *Ak $a_1 = 1$ a*

$$A = \{a_1 < a_2 < \ldots < a_n < \ldots\}$$

*tak*

$$\sigma(A) = \inf_{k>1} \frac{k-1}{a_k - 1}.$$

*Dôkaz.* Stačí si uvedomiť, že podiel $A(n)/n$ spomedzi čísel $n \in \{a_{k-1}, a_{k-1}+1, \ldots, a_k - 1\}$ nadobúda najmenšiu hodnotu práve pre $n = a_k - 1$ a hodnota tohoto podielu sa vtedy rovná

$$\frac{A(n)}{n} = \frac{k-1}{a_k - 1}.$$

□

**Príklad 5.2.6.** Nech $A = a\mathbb{N} + 1$ je množina členov aritmetickej postupnosti. (Ako prvý člen sme zvolili 1, pretože inak by platilo $\sigma(A) = 0$.) Pretože $n$-tý člen tejto postupnosti je $a(n-1)+1$ dostávame (na základe predchádzajúcej lemy) $\sigma(A) = \inf \frac{n-1}{a(n-1)} = \frac{1}{a}$.

Schnireľmannova hustota má aplikácie hlavne v aditívnej teórii čísel – v tejto oblasti sa skúmajú rôzne výsledky týkajúce sa rozkladov čísla na súčet čísel z nejakej vopred danej množiny.

**Definícia 5.2.7.** Ak $A_1, \ldots, A_k \subseteq \mathbb{N}$, tak ako $A_1 + \ldots + A_k$ označujeme množinu všetkých čísel tvaru $a_1 + \ldots + a_k$, kde $a_i \in A_i \cup \{0\}$ pre všetky $i = 1, 2, \ldots, k$.

Ďalej definujeme $nA$ pre $n \in \mathbb{N}$ induktívne ako: $1A = A$ a

$$(n+1)A = nA + A.$$

Ekvivalentne by sme mohli definovať súčet dvoch množín tak, že $A + B = \{a, b, a+b; a \in A, b \in B\}$ a indukciou túto definíciu rozšíriť na ľubovoľný konečný počet množín.

{schnir:VTSCHNIR}

**Veta 5.2.8 (Schnireľmann).** *Nech $A, B \subseteq \mathbb{N}$ a $C = A + B$. Potom*

$$\sigma(C) \ge \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

*Dôkaz.* Ak $\sigma(A) = 0$, tak tvrdenie vety platí, pretože $B \subseteq C$, a teda $\sigma(B) \le \sigma(C)$. Môžeme teda predpokladať, že $\sigma(A) > 0$, z čoho $1 \in A \subseteq C$.

Pokúsime sa nájsť dolný odhad pre $C(n)$. Množina $C \cap \langle 1, n\rangle$ určite obsahuje $A(n)$ prvkov $a_1, a_2, \ldots, a_{A(n)}$. Medzi dvoma prvkami $a_i$, $a_{i+1}$ sa ešte určite vyskytnú súčty tvaru $a_i + b$, kde $b \in B$ je také číslo, že $b < a_{i+1} - a_i$. Takých prvkov je $B(a_{i+1} - a_i - 1)$. Ak $a_{A(n)} < n$, tak ešte bude $C$ obsahovať aspoň $B(n - a_{A(n)})$ prvkov medzi týmito číslami. Dostávame teda

$$C(n) \ge A(n) + \sum_{i=1}^{A(n)-1} B(a_{i+1} - a_i - 1) + B(n - a_{A(n)}).$$

Keďže pre každé $k \in \mathbb{N}$ platí $B(n) > k\sigma(B)$, tak máme

$$C(n) \ge A(n) + \sigma(B)[(a_2 - 1 - 1) + (a_3 - a_2 - 1) + \ldots + (a_{A(n)} - a_{A(n)-1} - 1) + n - a_{A(n)}] \ge A(n) + \sigma(B)(n - A(n)) = n\sigma(B) + A(n)(1 - \sigma(B)).$$

Z toho vyplýva

$$\frac{C(n)}{n} \geq \sigma(B) + \frac{A(n)}{n}(1 - \sigma(B))$$

a z tejto nerovnosti už je zrejmé tvrdenie vety. □

Tvrdenie predchádzajúcej vety môžeme ekvivalentne prepísať ako $1 - \sigma(C) \leq (1 - \sigma(A))(1 - \sigma(B))$. Tento zápis je výhodný z toho dôvodu, že vedie k priamočiaremu zovšeobecneniu na viacero množín (dokáže sa jednoducho matematickou indukciou).

{schnir:DOSSCHNIR}

**Dôsledok 5.2.9.** *Nech $A_1, \ldots, A_n \subseteq \mathbb{N}$ a $C := A_1 + \cdots + A_n$. Potom*

$$1 - \sigma(C) \leq \prod_{i=1}^{n} (1 - \sigma(A_i)) .$$

V dôkaze vety 5.2.8 sme používali skutočne jednoduché odhady – vždy sme použili len niekoľko najmenších prvkov z množiny $B$. Napriek tomu sa ukázalo, že vylepšiť tento odhad je pomerne ťažké. Tvrdenie nasledovnú vetu vyslovil ako hypotézu E. Landau okolo roku 1930, bola dokázaná až v roku 1942 H. B. Mannom.

{schnir:VTMAN}

**Veta 5.2.10 (Mannova veta).** *Nech $A, B \subseteq \mathbb{N}$ a $C = A + B$. Potom*

$$\sigma(C) \geq \min(1, \sigma(A) + \sigma(B)).$$

Schnireľmannovou hustotou sa ešte budeme zaoberať neskôr v súvislosti s aditívnymi bázami množiny prirodzených čísel.

**Cvičenia**

1. Nech $A = \{a_1 < a_2 < \ldots < a_n < \ldots\}$. Dokážte, že ak $\limsup_{n\to\infty}(a_{n+1} - a_n) < \infty$, tak $\sigma(A) > 0$.
2. Majme množiny $A = \{a_1 < a_2 < \ldots < a_n < \ldots\}$ a $B = \{b_1 < b_2 < \ldots < b_n < \ldots\}$. Nech $A_B := \{a_{b_n}; n \in \mathbb{N}\}$. Dokážte, že $\sigma(A_B) \geq \sigma(A).\sigma(B)$ a $\underline{d}(A_B) \geq \underline{d}(A).\underline{d}(B)$.

## 5.3 Logaritmická hustota

Ako príklad množiny, ktorá nemá asymptotickú hustotu sme uviedli množinu čísel, ktoré (v nejakej číselnej sústave) majú nepárny počet cifier (príklad 5.1.6). Teraz si ukážeme príklad hustoty, ktorá tejto množine čísel vie priradiť hustotu.

**Definícia 5.3.1.** Pre ľubovoľné $n \in \mathbb{N}$ označme $S(n) := \sum_{k=1}^{n} \frac{1}{k}$. Nech $A \subseteq \mathbb{N}$. Potom hodnoty

$$\underline{\delta}(A) = \liminf_{n\to\infty} \frac{\sum_{k\in A; k\leq n} \frac{1}{k}}{S(n)} \qquad \overline{\delta}(A) = \limsup_{n\to\infty} \frac{\sum_{k\in A; k\leq n} \frac{1}{k}}{S(n)}$$

nazývame *dolná* a *horná logaritmická hustota* množiny $A$. Ak $\overline{\delta}(A) = \underline{\delta}(A)$, tak túto spoločnú hodnotu označujeme $\delta(A)$ a nazývame ju *logaritmická hustota* množiny $A$.



Logaritmickú hustotu by sme ekvivalentne mohli definovať nasledovne: Ak existuje limita

$$\delta(A) = \lim_{n\to\infty} \frac{\sum_{k\in A; k\leq n} \frac{1}{k}}{S(n)},$$

tak túto limitu nazývame logaritmickou hustotou množiny $A$.

Vďaka tomu, že $S(n) \sim \ln n$ (pozri (B.2)) môžeme menovateľ vo výraze vystupujúcom v definícii logaritmickej hustoty nahradiť $\ln n$. Teda logaritmickú hustotu by sme ekvivalentne mohli definovať takto:

$$\underline{\delta}(A) = \liminf_{n\to\infty} \frac{\sum_{k\in A; k\leq n} \frac{1}{k}}{\ln n},$$
$$\overline{\delta}(A) = \limsup_{n\to\infty} \frac{\sum_{k\in A; k\leq n} \frac{1}{k}}{\ln n},$$
$$\delta(A) = \lim_{n\to\infty} \frac{\sum_{k\in A; k\leq n} \frac{1}{k}}{\ln n}.$$

Priamo z definície by sme vedeli, podobným spôsobom ako pre asymptotickú hustotu, dokázať vlastnosti uvedené v lemách 5.1.2, 5.1.7 a dôsledkoch 5.1.8, 5.1.9. Nebudeme uvádzať dôkazy zodpovedajúcich tvrdení pre logaritmickú hustotu, keďže sú jednoduché a takmer totožné s dôkazmi pre logaritmickú hustotu. Budeme však tieto vlastnosti v tejto časti používať.

Teraz sa pozrieme na vzťah medzi asymptotickou a logaritmickou hustotou. V dôkaze nasledujúcej vety budeme používať tzv. Iversonovu notáciu, ktorá je zavedená napríklad v [GKP, p.24]. Pomocou tejto notácie možno zapísať sumu vystupujúcu v definícii logaritmickej hustoty ako

$$\sum_{k=1}^{n} \frac{1}{k}[k \in A],$$

pričom týmto zápisom sa myslí to, že sčitujeme len cez čísla majúce vlastnosť uvedenú v hranatých zátvorkách. (Teda je to vlastne len iné označenie pre charakteristickú funkciu množiny prirodzených čísel určenú touto vlastnosťou.)

{logar:VTNEROV}

**Veta 5.3.2 (Nerovnosť asymptotickej a logaritmickej hustoty).** *Pre ľubovoľnú podmnožinu $A \subseteq \mathbb{N}$ platí*

$$\underline{d}(A) \leq \underline{\delta}(A) \leq \overline{\delta}(A) \leq \overline{d}(A). \tag{5.2}$$

{logar:INEQ}

*Dôkaz.* Všimnime si najprv, že

$$\frac{1}{k}[k \in A] = \frac{A(k) - A(k-1)}{k},$$
$$D(n) := \sum_{k=1}^{n} \frac{1}{k}[k \in A] = \frac{A(n)}{n} + \sum_{k=1}^{n-1} \frac{A(k)}{k(k+1)}$$

Existuje $n_0 \in \mathbb{N}$ také, že pre každé $n \geq n_0$ platí $\underline{d}(A) - \varepsilon \leq \frac{A(n)}{n} \leq \overline{d}(A) + \varepsilon$.

Označme $C := 1 + D(n_0)$. Pre $n \geq n_0$ dostaneme

$$D(n) \leq C + \sum_{k=n_0}^{n-1} \frac{A(k)}{k} \cdot \frac{1}{k+1} + \frac{A(n)}{n} \leq C + (\overline{d}(A) + \varepsilon) \left(1 + \sum_{k=n_0}^{n-1} \frac{1}{k+1}\right) \sim (\overline{d}(A) + \varepsilon) \ln n,$$

$$\overline{\delta}(A) = \limsup_{n\to\infty} \frac{D(n)}{\ln n} \leq \overline{d}(A) + \varepsilon.$$

Táto nerovnosť platí pre ľubovoľné $\varepsilon > 0$, preto $\overline{\delta}(A) \leq \overline{d}(A)$.

Na dôkaz nerovnosti pre dolné hustoty si stačí uvedomiť, že pre ľubovoľnú podmnožinu $A \subseteq \mathbb{N}$ platí $\underline{d}(\mathbb{N} \setminus A) = 1 - \overline{d}(A)$ a $\underline{\delta}(\mathbb{N} \setminus A) = 1 - \overline{\delta}(A)$. □

Iný dôkaz (hoci do istej miery podobný) možno nájsť v [KLŠZ], [St], [T].

{logar:DOSNEROV}

**Dôsledok 5.3.3.** *Ak množina $A$ má asymptotickú hustotu, tak má aj logaritmickú hustotu.*

Môžeme ešte pre zaujímavosť spomenúť, že pre ľubovoľné „zmysluplné“ čísla (teda také aby vyhovovali nerovnosti 5.2, čiže $0 \leq \underline{\alpha} \leq \underline{\beta} \leq \overline{\beta} \leq \overline{\alpha} \leq 1$) existuje množina $A$ taká, že $\underline{d}(A) = \underline{\alpha}$, $\underline{\delta}(A) = \underline{\beta}$, $\overline{\delta}(A) = \overline{\beta}$ and $\overline{d}(A) = \overline{\alpha}$ (pozri [Mi] a [H]).

Už sme spomenuli, že príkladom množiny, ktoré nemá asymptotickú hustotu ale má logaritmickú hustotu je množina z príkladu 5.1.6. (Teda táto množina ukazuje, že dôsledok 5.3.3 nemožno obrátiť.)

Predtým, ako vypočítame hodnotu logaritmickej hustoty pre túto množinu, uvedieme jednu pomocnú vetu. Vedeli by sme ju síce ľahko vypočítať aj bez použitia tejto vety, je to však vcelku užitočná veta, ktorá sa dá často použiť – preto nezaškodí si ju dokázať.

Táto veta sa zvykne volať Stolzova alebo Stolzova-Cesarova veta ([KN, 2.3.11], [PLA]).

{logar:VTSTOLZ}

**Veta 5.3.4 (Stolzova-Cesarova veta).** *Nech $(x_n)$ a $(y_n)$ sú postupnosti reálnych čísel. Nech $(y_n)$ je kladná, ostro rastúca a $\lim\limits_{n\to\infty} y_n = +\infty$. Ak existuje limita*

$$\lim_{n\to\infty} \frac{x_{n+1} - x_n}{y_{n+1} - y_n} = L,$$

*tak potom aj*

$$\lim_{n\to\infty} \frac{x_n}{y_n} = L.$$

Táto veta do istej miery pripomína L'Hospitalovo pravidlo – ibaže derivácia je nahradená diferenciou po sebe idúcich členou postupnosti.

Stolzovu vetu môžeme preformulovať aj takýmto spôsobom:

**Dôsledok 5.3.5.** *Nech $(a_n)$ a $(b_n)$ sú postupnosti reálnych čísel, pričom $b_n > 0$ pre všetky $n \in \mathbb{N}$ a $\sum b_n = +\infty$. Ak existuje limita*

$$\lim_{n\to\infty} \frac{a_n}{b_n} = L,$$

*tak*

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{n} a_k}{\sum_{k=1}^{n} b_k} = L.$$

Je zrejmé, že obidve formulácie sú ekvivalentné. My budeme túto vetu dokazovať v druhej formulácii.



*Dôkaz.* Podľa predpokladu pre ľubovoľné $\varepsilon > 0$ existuje $n_0$ také, že pre $n > n_0$ platí

$$L - \varepsilon \leq \frac{a_n}{b_n} \leq L + \varepsilon,$$

z čoho máme

$$(L - \varepsilon)b_n \leq a_n \leq (L + \varepsilon)b_n.$$

(Keďže $b_n > 0$, nemení sa znamienko nerovnosti.)

Označme čiastočné súčty $t_n = \sum_{k=1}^{n} a_k$ a $s_n = \sum_{k=1}^{n} b_k$. Pre $n > n_0$ máme

$$t_n - t_{n_0} = \sum_{k=n_0+1}^{n} a_k$$

$$(L - \varepsilon) \sum_{k=n_0+1}^{n} b_k \leq \sum_{k=n_0+1}^{n} a_k \leq (L + \varepsilon) \sum_{k=n_0+1}^{n} b_k$$

$$(L - \varepsilon)(s_n - s_{n_0}) \leq t_n - t_{n_0} \leq (L + \varepsilon)(s_n - s_{n_0})$$

$$t_{n_0} + (L - \varepsilon)(s_n - s_{n_0}) \leq t_n \leq t_{n_0} + (L + \varepsilon)(s_n - s_{n_0})$$

$$\frac{t_{n_0} + (L - \varepsilon)(s_n - s_{n_0})}{s_n} \leq \frac{t_n}{s_n} \leq \frac{t_{n_0} + (L + \varepsilon)(s_n - s_{n_0})}{s_n}$$

Pre $n$ konvergujúce do nekonečna zlomok na ľavej strane konverguje k $L - \varepsilon$ a zlomok na pravej strane k $L + \varepsilon$. Preto

$$L - \varepsilon \leq \liminf_{n\to\infty} \frac{t_n}{s_n} \leq \limsup_{n\to\infty} \frac{t_n}{s_n} \leq L + \varepsilon.$$

Pretože táto nerovnosť platí pre ľubovoľné $\varepsilon$ dostávame nakoniec

$$\lim_{n\to\infty} \frac{\sum_{k=1}^{n} a_k}{\sum_{k=1}^{n} b_k} = \lim_{n\to\infty} \frac{t_n}{s_n} = L.$$

□

Ako dôsledok Stolzovej vety (keď vezmeme $b_n = 1$) dostaneme implikáciu

$$\lim_{n\to\infty} a_n = L \;\Rightarrow\; \lim_{n\to\infty} \frac{a_1 + \cdots + a_n}{n} = L.$$

Tento výsledok sme použili v dôkaze tvrdenia 2.3.4.

Keď si podrobnejšie pozrieme predchádzajúci dôkaz, vidíme, že sme v skutočnosti dokázali o niečo silnejšie tvrdenie, ktoré občas tiež môže byť užitočné. Sformulujeme ho pre postupnosti, formulácia pre súčty radov by bola analogická.

**Tvrdenie 5.3.6.** *Nech $(x_n)$ a $(y_n)$ sú postupnosti reálnych čísel. Nech $(y_n)$ je kladná, ostro rastúca a $\lim\limits_{n\to\infty} y_n = +\infty$. Potom*

$$\liminf \frac{x_{n+1} - x_n}{y_{n+1} - y_n} \leq \liminf \frac{x_n}{y_n} \leq \limsup \frac{x_n}{y_n} \leq \limsup \frac{x_{n+1} - x_n}{y_{n+1} - y_n}.$$

{logar:PRDIGIT}

**Príklad 5.3.7.** Pre $k = 0, 1, 2, \ldots$ označíme $B_k = \{3^k, 3^k+1, 3^k+2, \ldots, 3^{k+1}-1\}$. Množina, s ktorou budeme pracovať je $A := \bigcup_{k=0}^{\infty} B_{2k}$. Aby sme mohli odhadnúť logaritmickú hustotu tejto množiny, pokúsme sa odhadnúť najprv súčet prevrátených hodnôt čísel z množiny $B_k$.

Podobne ako v dôkaze vety B.1.1 môžeme sumu porovnať s obsahom plochy pod hyperbolou, teda

$$\int_{3^k}^{3^{k+1}} \frac{1}{x}dx \le \sum_{n\in B_k} \frac{1}{n} \le \int_{3^k-1}^{3^{k+1}-1} \frac{1}{x}dx$$

$$\ln 3 \le \sum_{n\in B_k} \frac{1}{n} \le \ln\frac{3^{k+1}-1}{3^k-1} = \ln 3 + \ln\left(1+\frac{2}{3^k-1}\right) \le \ln 3 + \frac{2}{3^k-1} \qquad (5.3)$$

{logar:ODHADLN3}

Označme

$$S_k := \sum_{n\in B_k} \frac{1}{n}$$

Z toho, že množina $A$ je zložená zo súvislých úsekov po sebe idúcich čísel, je zrejmé, že stačí zisťovať limitu podielu vystupujúceho v definícii logaritmickej hustoty vždy na začiatku a na konci takéhoto úseku (podobne ako pre asymptotickú hustotu v leme 5.1.5, pozri úlohu 4). To znamená, že nás zaujímajú limity

$$\underline{\delta}(A) = \lim_{n\to\infty} \frac{\sum_{k=0}^{n} S_{2k}}{\sum_{k=0}^{n}(S_{2k}+S_{2k+1})} \qquad \text{a} \qquad \overline{\delta}(A) = \lim_{n\to\infty} \frac{\sum_{k=0}^{n} S_{2k}}{S_0+\sum_{k=1}^{n}(S_{2k-1}+S_{2k})}.$$

Na základe nerovnosti (5.3) vidíme, že platí

$$\lim_{n\to\infty} \frac{S_{2k}}{S_{2k}+S_{2k+1}} = \lim_{n\to\infty} \frac{S_{2k}}{S_{2k-1}+S_{2k}} = \frac{1}{2},$$

vďaka čomu zo Stolzovej vety 5.3.4 dostaneme

$$\underline{\delta}(A) = \overline{\delta}(A) = \frac{1}{2}.$$

Na základe množín, pre ktoré sme doteraz rátali logaritmickú a asymptotickú hustotu, nie je ťažké vymyslieť príklad množiny, ktorá nemá logaritmickú hustotu.

{logar:PRNEMAHUST}

**Príklad 5.3.8.** Pre $k = 0, 1, 2, \ldots$ označíme $B_k = \{3^{3^k}, 3^{3^k}+1, 3^{3^k}+2, \ldots, 3^{3^{k+1}}-1\}$. Potom množina $A := \bigcup_{k=1}^{\infty} B_{2k}$ nemá logaritmickú hustotu.

### 5.3.1 Ďalšie zovšeobecnenia

Podobným spôsobom, ako sme definovali logaritmickú hustotu, by sa dala definovať celá trieda hustôt podmnožín prirodzených čísel.

Pre ľubovoľnú funkciu $f\colon \mathbb{N} \to (0, +\infty)$ môžeme položiť

$$d_f(A) = \lim_{n\to\infty} \frac{\sum\limits_{k\le n, k\in A} f(k)}{\sum\limits_{k\le n} f(k)}$$

a analogicky definovať aj dolnú a hornú hustotu.



Používa sa napríklad funkcia $f(n) = n^\alpha$, kde $\alpha \ge -1$. Hustotu zodpovedajúcu tejto funkcii označme $d_\alpha$. Je napríklad známe, že pre takéto hustoty platí nerovnosť, ktorá je zovšeobecnením nerovnosti (5.2). (Všimnite si, že pre $\alpha = -1$ dostaneme práve logaritmickú hustotu a pre $\alpha = 0$ asymptotickú hustotu.)

**Veta 5.3.9.** *Nech $-1 \le \alpha < \beta$ a $A \subseteq \mathbb{N}$. Potom*

$$\underline{d}_\beta(A) \le \underline{d}_\alpha(A) \le \overline{d}_\alpha(A) \le \overline{d}_\beta(A).$$

Viac o takýchto ale aj iných hustotách používaných v teórii čísel sa môžete dozvedieť napríklad v článku [Gr].

**Cvičenia**

1. Ak $(a_n)$ je postupnosť prirodzených čísel a $\lim_{n\to\infty}(a_{n+1}-a_n) = a$ (kde $a$ je pevne zvolené reálne číslo), tak pre množinu $A = \{a_n; n \in \mathbb{N}\}$ platí $d(A) = \frac{1}{a}$.
2. Ak $(a_n)$ je postupnosť prirodzených čísel a $\lim_{n\to\infty}\left(\frac{a_{n+1}}{a_n}\right)^{a_n} = C$ (kde $C$ je pevne zvolené reálne číslo), tak pre množinu $A = \{a_n; n \in \mathbb{N}\}$ platí $\delta(A) = \frac{1}{\ln C}$.
3. Dokážte, že pre $\alpha > -1$ platí $\lim_{n\to\infty} \frac{n^{\alpha+1}}{\sum_{k=1}^{n} k^\alpha} = \frac{1}{\alpha+1}$. (Z toho vyplýva, že sumu vystupujúcu v menovateli pri definícii hustoty $d_\alpha$ možno nahradiť číslom $\frac{n^{\alpha+1}}{\alpha+1}$. Poznámka: Dá sa to dokazovať porovnaním integrálu a sumy, ale aj pomocou Stolzovej vety.)

{logarcvic:USEKY}

4. Dokážte analógiu lemy 5.1.5 pre logaritmickú hustotu.
5. Dokážte, že množina z príkladu 5.3.8 skutočne nemá logaritmickú hustotu.

## 5.4 Štatistická konvergencia

S pojmom asymptotickej hustoty súvisí štatistická konvergencia postupností prirodzených čísel. Okrem nej tu spomenieme aj niektoré iné zovšeobecnenia pojmu limity postupnosti.

Dôvod, prečo ich chcem spomenúť, nie je ten, že by nevyhnutne museli patriť do základného kurzu teórie čísel. (Asi by to patrilo skôr do analýzy, prípadne niektoré z nich – ako aplikácie pojmu ultrafilter – do teórie množín.) Skôr sú tu z dôvodu, že ich považujem za zaujímavé a tiež preto, že som sa týmito témami trochu zaoberal a som (aspoň dúfam) o nich schopný aj niečo zaujímavé povedať.

Pomocou asymptotickej hustoty môžeme zaviesť štatistickú konvergenciu.

**Definícia 5.4.1.** Hovoríme, že postupnosť $(x_n)$ reálnych čísel *štatisticky konverguje* k $L \in \mathbb{R}$, ak pre každé $\varepsilon > 0$ platí $d(A(\varepsilon)) = 0$, kde

$$A(\varepsilon) = \{n \in \mathbb{N}; |x_n - L| \ge \varepsilon\}.$$

Označujeme

$$\operatorname{limstat} x_n = L.$$

Štatistická konvergencia bola definovaná v článku [Fa].

Ak porovnáme túto definíciu z obvyklou konvergenciou postupností, tak pri obvyklej definícii konvergencie vyžadujeme, aby bola množina bodov, ktoré sú ďaleko od $L$ (teda

množina $A(\varepsilon)$) konečná. Pri štatistickej konvergencii tiež požadujeme, aby táto množina bola malá – ale v inom zmysle, namiesto konečnosti žiadame len asymptotickú hustotu rovnú 0.

Je zrejmé, že ak postupnosť konverguje v obvyklom zmysle, tak konverguje aj štatisticky. Obrátene to neplatí – stačí za postupnosť $(x_n)$ zobrať charakteristickú postupnosť ľubovoľnej podmnožiny $\mathbb{N}$, ktorá je nekonečná a súčasne má nulovú asymptotickú hustotu.

Úplne analogicky by sme boli schopní definovať štatistickú limitu v ľubovoľnom metrickom alebo topologickom priestore, tu sa však budeme zaoberať len reálnymi číslami.

Nasledujúce vlastnosti štatistickej konvergencie sa dokážu pomerne ľahko (dôkazy vynechávame):

**Tvrdenie 5.4.2.**

(i) *Ak* $\lim\limits_{n\to\infty} x_n = L$, *tak* $\operatorname{limstat} x_n = L$.

(ii) *Ak existuje* $\operatorname{limstat} x_n = L$, *tak* $L$ *je hromadný bod postupnosti* $(x_n)$ *a* $\liminf x_n \le \operatorname{limstat} x_n \le \limsup x_n$.

(iii) *Postupnosť* $(x_n)$ *má najviac jednu limitu.*

(iv) $\operatorname{limstat}(ax_n + by_n) = a \operatorname{limstat} x_n + b \operatorname{limstat} y_n$ (*ak postupnosti* $(x_n)$ *a* $(y_n)$ *majú štatistickú limitu*).

(v) $\operatorname{limstat}(x_n.y_n) = \operatorname{limstat} x_n . \operatorname{limstat} y_n$ (*ak postupnosti* $(x_n)$ *a* $(y_n)$ *majú štatistickú limitu*).

**Príklad 5.4.3.** Jednoduchým príkladom postupnosti, ktorá nekonverguje v obvyklom zmysle ale konverguje štatisticky je postupnosť

$$x_n = \begin{cases} 1, & \text{ak } n = k^2 \text{ pre nejaké } k, \\ 0, & \text{inak.} \end{cases}$$

Štatistickú konvergenciu postupnosti možno ekvivalentne popísať nasledovne. (Táto charakterizácia je dokázaná v [Š2] pre postupnosti reálnych čísel a v [Fr] pre postupnosti v metrických priestoroch.)

**Veta 5.4.4.** *Postupnosť reálnych čísel* $(x_n)_{n=1}^{\infty}$ *konverguje štatisticky k číslu* $L$ *práve vtedy, keď existuje podmnožina* $M = \{m_1 < m_2 < \ldots\}$ *taká, že* $d(M) = 1$ *a* $\lim\limits_{k\to\infty} x_{m_k} = L$.

Štatistická konvergencia má niektoré vlastnosti, ktoré chýbajú obvyklej konvergencii. Ako príklad uveďme nasledujúce tvrdenia.

**Tvrdenie 5.4.5.** *Nech* $(x_n)_{n=1}^{\infty}$ *je ohraničená postupnosť reálnych čísel. Ak* $\operatorname{limstat} x_n = L$, *tak* $\lim\limits_{n\to\infty} \frac{x_1+\cdots+x_n}{n} = L$

*Dôkaz.* Pokúsme sa odhadnúť výraz $|\frac{x_1+\cdots+x_n}{n} - L|$. Máme

$$\left|\frac{x_1+\cdots+x_n}{n} - L\right| = \left|\frac{x_1+\cdots+x_n - nL}{n}\right| = \left|\frac{(x_1-L)+\ldots+(x_n-L)}{n}\right|.$$

Použitím trojuholníkovej nerovnosti dostaneme

$$\left|\frac{x_1+\cdots+x_n}{n} - L\right| \le \frac{|x_1-L|+\ldots+|x_n-L|}{n}.$$



Aj postupnosť $x_n - L$ je ohraničená, teda existuje reálne číslo $K$ také, že $|x_k - L| \le K$ (pre ľubovoľné $k$). Súčasne však, pre $k \notin A(\varepsilon)$, máme nerovnosť $|x_k - L| < \varepsilon$. Teda

$$\left|\frac{x_1+\cdots+x_n}{n} - L\right| \le K\frac{A(\varepsilon)(n)}{n} + \varepsilon\frac{B(\varepsilon)(n)}{n},$$

pričom sme označili $B = \mathbb{N} \setminus A$.

Podľa predpokladu máme $d(A) = 0$ a $d(B) = 1$, preto

$$\lim_{n\to\infty} \left|\frac{x_1+\cdots+x_n}{n} - L\right| = 0.$$

□

Predchádzajúcu vetu nemožno obrátiť. Stačí si všimnúť, že pre postupnosť $x_n = (-1)^n$ platí $\frac{x_1+\cdots+x_n}{n} = 0$, ale neexistuje štatistická limita.

Pre obvyklú konvergenciu platí nasledujúce tvrdenie.

**Tvrdenie 5.4.6 (Olivierova veta).** *Nech* $(a_n)_{n=1}^{\infty}$ *je postupnosť reálnych čísel taká, že* $a_{n+1} \ge a_n > 0$ *pre ľubovoľné* $n \in \mathbb{N}$. *Ak* $\sum_{n=1}^{\infty} a_n < +\infty$, *tak platí*

$$\lim_{n\to\infty} na_n = 0.$$

*Dôkaz.* Ak $\sum_{n=1}^{\infty} a_n < +\infty$, tak existuje $n_0$ také, že pre $n \ge n_0$ a ľubovoľné $p \in \mathbb{N}$ platí

$$\sum_{i=1}^{p} a_{n+i} < \varepsilon.$$

Z monotónnosti dostaneme

$$pa_{n+p} \le \sum_{i=1}^{p} a_{n+i} < \frac{\varepsilon}{2}.$$

Pretože $a_n \to 0$, pre existuje $n_1$ tak, že pre $k \ge n_1$ platí $a_k \le \frac{\varepsilon}{2n_0}$.

Potom ľubovoľné $n$, ktoré je väčšie ako $n_0$ aj $n_1$ môžeme zapísať v tvare $n = n_0 + p$ a dostaneme

$$na_n = (n_0+p)a_{n_0+p} \le n_0 a_n + pa_{n_0+p} < \varepsilon.$$

□

Ľahko sa dá nájsť príklad, že bez predpokladu monotónnosti už tvrdenie Olivierovej vety neplatí.

**Príklad 5.4.7.** Nech $a_n = \frac{1}{n}$ pre $n = k^2$ (čiže pre všetky štvorce prirodzených čísel) a $a_n = 0$ inak. Potom $\sum_{n=1}^{\infty} a_n = \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$, ale $na_n = 1$ pre nekonečne veľa čísel $n$ (konkrétne pre všetky štvorce), čiže postupnosť $(na_n)_{n=1}^{\infty}$ nemôže konvergovať k 0.

Pre štatistickú konvergenciu však už analógia Olivierovej vety platí aj po vynechaní predpokladu monotónnosti.

**Tvrdenie 5.4.8.** *Nech* $(a_n)_{n=1}^{\infty}$ *je postupnosť reálnych čísel taká, že* $a_n > 0$ *pre ľubovoľné* $n \in \mathbb{N}$. *Ak* $\sum_{n=1}^{\infty} a_n < +\infty$, *tak platí*

$$\operatorname{limstat} na_n = 0.$$

*Dôkaz.* Potrebujeme dokázať, že množina

$$A(\varepsilon) = \{n \in \mathbb{N}; na_n \geq \varepsilon\}$$

má asymptotickú hustotu 0.

Číslo $n$ patrí do $A(\varepsilon)$ práve vtedy, keď $\frac{\varepsilon}{n} \leq a_n$. Z toho dostaneme

$$\varepsilon \sum_{n\in A(\varepsilon)} \frac{1}{n} = \sum_{n\in A(\varepsilon)} \frac{\varepsilon}{n} \leq \sum_{n\in A(\varepsilon)} a_n \leq \sum_{i=1}^{\infty} a_n < +\infty$$

a podľa tvrdenia 5.1.10 potom $d(A(\varepsilon)) = 0$. □

O podobných zovšeobecneniach Olivierovej vety (súvisiacich s $\mathcal{I}$-konvergenciou, o ktorej hovoríme v nasledujúcej časti) sa možno dozvedieť viac v [ŠT].

Uveďme ešte jednu ilustráciu toho, že štatistická konvergencia môže pomôcť popísať správanie niektorých aritmetických funkcií pričom podobná charakterizácia pomocou obvyklej konvergencie neplatí.

**Definícia 5.4.9.** Pre $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ zadefinujme aritmetické funkcie

$$h(n) = \min\{\alpha_i; i = 1, 2, \dots, r\} \qquad H(n) = \max\{\alpha_i; i = 1, 2, \dots, r\}.$$

Tieto funkcie sa nazývajú *Nivenove funkcie.*

V článku [SŠ] je dokázané, že

$$\operatorname{limstat} \frac{H(n)}{\ln n} = \operatorname{limstat} \frac{h(n)}{\ln n} = 0,$$

hoci množina hodnôt oboch týchto postupností je hustá v $\left(0, \frac{1}{\ln 2}\right)$. (Čiže na základe hromadných bodov týchto postupností by sa zdalo, že sa tieto podiely správajú pomerne nepravidelne, keď sa však na ne pozrieme z hľadiska štatistickej konvergencie, objavíme aspoň nejakú zákonitosť.)

## 5.5 $\mathcal{I}$-konvergencia

TODO Ak nám zvýši čas a chuť, niekedy koncom semestra by sme sa ešte pozreli na túto tému. V prípade záujmu si môžete niečo o nej prečítať v [Sl].



# Kapitola 6

# Diofantické rovnice

*Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*
Pierre de Fermat

*Diofantickými rovnicami* nazývame rovnice s celočíselnými koeficientami, pričom hľadané riešenia sú tiež celé (alebo prirodzené) čísla. V tejto časti spomenieme niektoré špeciálne typy diofantických rovníc.

## 6.1 Lineárne diofantické rovnice

*Lineárne diofantické rovnice* sú rovnice tvaru $\sum_{i=1}^{n} a_i x_i = r$, kde $a_i, r \in \mathbb{Z}$. My sa budeme zaoberať len lineárnymi diofantickými rovnicami s dvoma neznámymi

$$ax + by = r. \tag{6.1}$$ {lind:LIN}

Ich riešenie úzko súvisí s riešením lineárnych kongruencií, ktorými sme sa už zaoberali. Skutočne, ak $ax + by = r$, tak platí $ax \equiv r \pmod{b}$. Podľa vety 3.1.16 má táto kongruencia riešenie práve vtedy, keď $d \mid r$, kde $d := (a, b)$. Ďalej sme v dôkaze vety 3.1.16 ukázali, že všetky riešenia danej kongruencie (ak táto kongruencia má riešenie) sú tvaru

$$x_k = x_0 + \frac{kb}{d},$$

kde $x_0$ je ľubovoľné riešenie. Riešenie $x_0$ vieme nájsť pomocou Euklidovho algoritmu.

Z rovnice (6.1) dostaneme $y = \frac{r-ax}{b}$. Z toho vyplýva, že ku každému riešeniu $x_k$ zodpovedá

$$y_k = \frac{r - ax_k}{b} = \frac{r - ax_0}{b} - \frac{ka}{d} = y_0 - \frac{ka}{d},$$

kde ako $y_0 := \frac{r-ax_0}{b}$ sme označili $y$ zodpovedajúce $x_0$. Dostávame teda nasledujúci výsledok

**Veta 6.1.1.** *Lineárna diofantická rovnica $ax + by = r$ má celočíselné riešenie práve vtedy, keď $d \mid r$, kde $d = (a, b)$. Ak $x_0$, $y_0$ je ľubovoľné riešenie tejto rovnice, tak všetky jej riešenia sú tvaru*

$$x_k = x_0 + \frac{kb}{d}, \qquad y_k = y_0 - \frac{ka}{d}.$$

**Cvičenia**

1. Nájdite riešenia lineárnych diofantických rovníc:
   a) $2x + 3y = 4$,
   b) $17x + 19y = 23$,
   c) $15x + 51y = 41$,
   d) $23x + 29y = 25$,
   e) $10x - 8y = 42$,
   f) $121x - 88y = 572$.

2. Celé čísla $x$, $y$ spĺňajú rovnosť $ax - by = \pm 1$ práve vtedy, keď obsah trojuholníka s vrchomi $(b, a)$, $(x, y)$ a $(0, 0)$ je $\frac{1}{2}$.

3. Aká je minimálna možná vzdialenosť medzi dvoma rôznymi bodmi $(x_0, y_0)$, $(x_1, y_1)$, ktoré predstavujú celočíselné riešenia lineárnej diofantickej rovnice $ax + by = r$. (Čísla $a$, $b$, $r$ sú celé.)

4. Dokážte, že pre ľubovoľné $a, b \in \mathbb{Z}$ má nasledujúci systém nejaké celočíselné riešenie. Nájdite všetky celočíselné riešenia.

$$x + y + 2z + 2t = a$$
$$2x - 2y + z - t = b$$

## 6.2 Pytagorovské trojuholníky

**Definícia 6.2.1.** *Pytagorovskou trojicou* nazývame trojicu prirodzených čísel $x$, $y$, $z$ takú, že

$$x^2 + y^2 = z^2. \tag{6.2}$$ {pytag:PYT}

Motivácia pre toto pomenovanie je zrejmá – pytagorovské trojice zodpovedajú pravouhlým trojuholníkom s celočíselnými stranami. Rovnica (6.2) vyplýva z Pytagorovej vety.

Ukážeme si popis všetkých pytagorovských trojíc. Veta, ktorú dokážeme, sa objavila už v Euklidových Základoch. Všimnime si, že ak $x$, $y$, $z$ spĺňa (6.2), tak to isté platí aj pre ľubovoľný násobok $cx$, $cy$, $cz$, kde $c \in \mathbb{N}$.

**Definícia 6.2.2.** Pytagorovská trojica $x$, $y$, $z$ sa nazýva *primitívna,* ak čísla $x$, $y$, $z$ sú nesúdeliteľné; $(x, y, z) = 1$.

Všimnime si, že na to, aby bola pytagorovská $(x, y, z)$ trojica primitívna, stačí, aby niektorá dvojica z týchto 3 čísel bola nesúdeliteľná. Napríklad, ak by $(x, y) = d > 1$, tak dostaneme, že $d^2 \mid x^2 + y^2 = z^2$, čiže $d \mid z$ a $d = (x, y, z)$. Podobným spôsobom môžeme overiť tento fakt aj pre ostatné dvojice.

{pytag:LMPARITA}

**Lema 6.2.3.** *Ak $x$, $y$, $z$ je primitívna pytagorovská trojica, tak práve 1 z čísel $x$, $y$ je párne a číslo $z$ je nepárne.*

*Dôkaz.* Ak by boli $x$ aj $y$ párne, tak $z^2$ je párne, teda aj $z$ je párne. V takom prípade by čísla $x$, $y$, $z$ boli súdeliteľné.

Nech by boli $x$ aj $y$ nepárne. Potom $x^2 \equiv y^2 \equiv 1 \pmod 4$, a teda $z^2 \equiv 2 \pmod 4$, čo je spor. (Všimnime si, že pre ľubovoľné $z$ platí $z^2 \equiv 0 \pmod 4$ alebo $z^2 \equiv 1 \pmod 4$). Overiť to môžeme jednoducho rozborom všetkých možností.)

Zostáva teda možnosť, že práve jedno z čísel $x$ a $y$ je nepárne. Potom aj $z^2 = x^2 + y^2$ je nepárne, teda aj $z$ je nepárne. □



Nasledujúcu jednoduchú úvahu budeme často používať v tomto a aj v ďalších dôkazoch. Preto ju uvedieme ako samostatnú lemu.

**Lema 6.2.4.** *Ak $(a, b) = 1$ tak, $(a + b, a - b)$ je 1 alebo 2.*

*Z toho vyplýva, že ak $a$, $b$ sú nesúdeliteľné a majú rôznu paritu, tak $(a + b, a - b) = 1$.*

**Veta 6.2.5.** *Prirodzené čísla $x$, $y$, $z$, kde $x$ je párne, tvoria primitívnu pytagorovskú trojicu práve vtedy, keď*

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2 \tag{6.3}$$ {pytag:GEN}

*pre nejaké prirodzené čísla $m$, $n$, také, že $(m, n) = 1$, $m > n$ a $m$, $n$ sú rôznej parity.*

*Dôkaz.* ⇒ Uvažujme rovnosť $x^2 = (z - y)(z + y)$. Pretože $y$ aj $z$ sú nepárne čísla, ich súčet aj rozdiel je párny. Preto existujú také $k, l \in \mathbb{N}$, že $z - y = 2k$, $z + y = 2l$. Z týchto vzťahov môžeme $y$ a $z$ vyjadriť ako $y = l - k$, $z = l + k$.

Pretože $(2k, 2l) = 2$ (predchádzajúca lema), platí $(k, l) = 1$.

Súčasne $kl = \frac{x^2}{4}$ je štvorec prirodzeného čísla. Pretože ide o nesúdeliteľné čísla, musia byť $k$ aj $l$ štvorce. Čiže $k = n^2$, $l = m^2$ pre nejaké prirodzené čísla $m$, $n$. Aby sme dostali $(k, l) = 1$, musí platiť $(m, n) = 1$. Na to, aby platilo $(y, z) = 1$, je nutné, aby čísla $m$, $n$ mali rôznu paritu.

Z týchto vzťahov už dostávame $y = m^2 - n^2$, $z = (m^2 + n^2)$ a $x^2 = 4m^2n^2$. Posledná rovnica implikuje $x = 2mn$. Aby číslo $y$ bolo kladné, musí platiť podmienka $m > n$.

⇐ Ľahko sa overí, že $x^2 + y^2 = (m^2 - n^2)^2 + (2mn)^2 = m^4 + 4m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2$. Teda tieto čísla naozaj tvoria pytagorovskú trojicu.

Pretože $(m^2, n^2) = 1$ a tieto čísla sú rôznej parity, máme aj $(y, z) = (m^2 - n^2, m^2 + n^2) = 1$. □

Dostali sme vlastne úplné riešenie rovnice (6.2) – presne sme popísali všetky riešenia. Podáme ešte jednu podobnú charaktreizáciu všetkých riešení tejto rovnice.

**Veta 6.2.6.** *Prirodzené čísla $x$, $y$, $z$, kde $x$ je párne, tvoria primitívnu pytagorovskú trojicu práve vtedy, keď*

$$x = \frac{k^2 - l^2}{2}, \qquad y = kl, \qquad z = \frac{k^2 + l^2}{2} \tag{6.4}$$ {pytag:GEN2}

*pre nejaké nepárne prirodzené čísla $k$, $l$, také, že $(k, l) = 1$ a $k > l$.*

*Dôkaz.* ⇒ V tomto prípade máme

$$y^2 = (z - x)(z + x)$$

pričom čísla $u := z - x$ a $v := z + x$ sú nepárne. Z lemy 6.2.3 vyplýva, že $(u, v) = 1$. Pretože štvorec $y^2 = uv$ je súčin 2 nesúdeliteľných čísel, obe z nich musia byť štvorce. Položme teda $v = k^2$, $u = l^2$, z čoho hneď dostávame rovnosti

$$x = \frac{k^2 - l^2}{2}, \qquad y = kl, \qquad z = \frac{k^2 + l^2}{2}.$$

⇐ Z toho, že $(k, l = 1)$ máme (opäť na základe lemy 6.2.3) $(k^2 + l^2, k^2 - l^2) = (2z, 2x) = 2$, čiže $(z, x) = 1$. □

Na základe predchádzajúcich viet vieme vygenerovať nekonečne veľa (primitívnych) pytagorovských trojíc.

| $m$ | $n$ | $(x,y,z)$ |
|---|---|---|
| 2 | 1 | (4,3,5) |
| 3 | 2 | (12,5,13) |
| 4 | 1 | (8,15,17) |
| 4 | 3 | (24,7,25) |
| 5 | 2 | (20,21,29) |

Najmenšia (a aj najznámejšia) z nich je trojica $(3,4,5)$. pre zaujímavosť môžeme spomenúť výsledok W. Sierpińskeho [Sie2], [Sie3, s.42], že diofantická rovnica

$$3^x + 4^y = 5^z$$

nemá iné riešenie ako $(x,y,z) = (2,2,2)$. Neskôr bolo toto tvrdenie zovšeobecnené na viaceré pytagorovské trojice. Nie je však známe, či analogické tvrdenie platí pre všetky pytagorovské trojice.

Je zaujímavé si všimnúť, že pre ľubovoľný pravouhlý trojuholník s celočíselnými dĺžkami strán je aj polomer vpísanej kružnice celé číslo. Skutočne

$$r = \frac{2S}{o} = \frac{xy}{x+y+z} = \frac{2mn(m^2-n^2)}{2mn+2m^2} = \frac{2mn(m-n)(m+n)}{2m(m+n)} = n(m-n). \qquad (6.5) \quad \{\texttt{pytag:EQPOLOMER}\}$$

Takisto obrátene, ak si zvolíme ľubovoľné celé číslo $r$, tak z rovnice (6.5) vieme nájsť príslušnú pytagorovskú trojicu: Stačí položiť $n = 1$ a $m = r+1$.

**Cvičenia**

1. Nech $x$, $y$, $z$ je primitívna pytagorovská trojica. Dokážte, že $(x,z) = (y,z) = 1$
2. Nájdite všetky pytagorovské trojice, ktoré súčasne tvoria aritmetickú postupnosť.
3. Nájdite všetky pytagorovské trojice, ktoré súčasne tvoria geometrickú postupnosť.
4. Označme $H = \{\frac{x}{y}; (x,y,z)$ je pytagorovská trojica$\}$. Dokážte, že množina $H$ je hustá v intervale $\langle 0, +\infty)$.
5. Ak $x$, $y$, $z$ je pytagorovská trojica, tak aspoň jedno z čísel $x$, $y$ je deliteľné 3.
6. Ak $x$, $y$, $z$ je primitívna pytagorovská trojica, tak práve jedno z čísel $x$, $y$, $z$ je deliteľné 5.
7. Ak $x$, $y$, $z$ je pytagorovská trojica, tak aspoň jedno z čísel $x$, $y$, $z$ je deliteľné 4.
8. Ak $x$, $y$, $z$ je primitívna pytagorovská trojica, tak $60 \mid xyz$.
9. Ukážte, že neexistuje pytagorovská trojica $a$, $b$, $c$ taká, že $c = 2b$. (Hint 1: $\sqrt{3}$ je iracionálne. Hint 2: Nekonečná regresia.[1])
10. Nájdite všetky pytagorovské trojice také, že jedna z odvesien je o 1 menšia než prepona. Z výsledku by malo byť vidieť, že trojice $(21,220,221), (201,20200,20201), (2001,2002000,2002001), \ldots$ tvoria pytagorovské trojuholníky. ∎

[1] Metóda nekonečnej regresie je zavedená v ďalšej podkapitole.



## 6.3 Diofantická rovnica $x^4 + y^4 = z^4$

P. de Fermat vyslovil hypotézu, že rovnica

$$x^n + y^n = z^n \qquad (6.6) \quad \{\texttt{fermat:EQFERM}\}$$

nemá nenulové riešenie v celých číslach pre žiadne prirodzené číslo $n \geq 3$. História vzniku tejto hypotézy je veľmi známa – Fermat si poznačil toto tvrdenie na okraj Diofantovej Aritmetiky, pričom napísal „našiel som veľmi pekný dôkaz, je tu naň však príliš málo miesta.“ (Citát uvedený na začiatku tejto kapitoly.)

Tento problém, nazvaný Veľká Fermatova veta alebo Posledná Fermatova veta, bol dlho otvorený. O jeho riešenie sa pokúšali mnohí matematici, objavilo sa veľa nesprávnych dôkazov, a aj čiastočných výsledkov – pre niektoré exponenty. (My ju ukážeme pre exponenty 3 a 4.) Veľkú Fermatovu vetu sa nakoniec podarilo dokázať v roku 1994 A. Wilesovi a R. Taylorovi.

Riešenie tohoto problému je veľmi náročné, pre niektoré konkrétne $n$ sa však tento problém dá rozriešiť aj so základnými poznatkami z teórie čísel.

Ľahko si možno všimnúť, že ak rovnica (6.6) nemá riešenie pre nejaké $n = k.l$, tak nemá riešenie ani pre číslo $l$; stačí túto rovnicu prepísať do tvaru $(x^k)^l + (y^k)^l = (z^k)^l$. Z toho vyplýva, že na dôkaz Fermatovej vety stačí uvažovať prípady $n = 4$ a $n$ je nepárne prvočíslo.

Ukážeme, že pre $n = 4$ rovnica (6.6) skutočne nemá riešenie. Dokážeme dokonca o čosi silnejší výsledok.

**Veta 6.3.1.** *Rovnica*

$$x^4 + y^4 = z^2 \qquad (6.7) \quad \{\texttt{fermat:EQFERM4}\}$$

*nemá riešenie v* $\mathbb{Z} \setminus \{0\}$.

*Dôkaz.* Je zrejmé, že pri riešení rovnice (6.7) sa môžeme obmedziť na prirodzené čísla. Nech $u$ je najmenšie prirodzené číslo, pre ktoré existujú $x$ a $y$ také, že $x^4 + y^4 = u^2$. Zrejme $(x,y,u) = 1$, inak by sme vedeli zostrojiť ešte menšie riešenie. Bez ujmy na všeobecnosti, nech $x$ je párne a $y$ je nepárne. Čísla $x^2$, $y^2$, $u$ tvoria primitívnu pytagorovskú trojicu, preto existujú nesúdeliteľné čísla $a$ a $b$ také, že

$$x^2 = 2ab, \qquad y^2 = a^2 - b^2, \qquad u = a^2 + b^2.$$

Práve jedno z čísel $a$ a $b$ je párne (inak by $2ab$ nebol štvorec). Ak by $a$ bolo párne a $b$ nepárne, tak by sme dostali $y^2 \equiv 3 \pmod 4$, čo nemôže nastať. Preto $b$ je párne.

Môžeme ho teda zapísať v tvare $b = 2c$, z čoho dostaneme

$$\left(\frac{x}{2}\right)^2 = ac,$$

kde $(a,c) = 1$.

Z toho vyplýva, že $a$ aj $c$ sú druhé mocniny nesúdeliteľných čísel

$$a = d^2, \qquad c = f^2, \qquad (d,f) = 1.$$

Z toho dostaneme pre $y$ vzťah $y^2 = a^2 - b^2 = d^4 - 4f^4$. Teda platí

$$(2f^2)^2 + y^2 = (d^2)^2.$$

Čísla vystupujúce v predchádzajúcej rovnici sú nesúdeliteľné, preto tvoria primitívnu pytagorovskú trojicu a pre vhodné $l$ a $m$ máme

$$2f^2 = 2lm, \qquad d^2 = l^2 + m^2, \qquad f^2 = lm,$$

pričom $(l, m) = 1$.

Z rovnosti $f^2 = lm$ vyplýva, že musí platiť $l = r^2$, $m = s^2$, čiže dostávame

$$r^4 + s^4 = d^2.$$

Súčasne však $d \leq d^2 = a \leq a^2 < a^2 + b^2 = u$, čo je v spore s tým, že $u$ sme vybrali ako najmenšie možné číslo vyjadriteľné v tomto tvare. □

Základná myšlienka dôkazu predchádzajúcej vety je v tom, že z ľubovoľného riešenia dokážeme dostať riešenie od neho menšie. Takýto postup sa dá použiť na dôkaz neexistencie riešenia v prirodzených číslach. (Keďže prirodzené čísla sú dobre usporiadané, ak je množina riešení neprázdna, musí mať najmenší prvok.) Táto metóda sa nazýva *metóda nekonečnej regresie* (anglicky: infinite descent). Túto metódu často používal vo svojich úvahách práve P. de Fermat.

Podobným spôsobom môžeme dokázať aj:

**Veta 6.3.2.** *Neexistuje riešenie rovnice*

$$x^4 + y^2 = z^4 \tag{6.8}$$ {fermat:EQFERMMINUS}

*v* $\mathbb{Z} \setminus \{0\}$.

*Dôkaz.* Opäť môžeme predpokladať, že máme riešenie, pre ktoré má $z$ najmenšiu možnú nenulovú hodnotu. V takom prípade sú čísla $x$, $y$, $z$ nesúdeliteľné a $(x^2, y, z^2)$ je primitívna pytagorovská trojica.

Preto práve jedno z čísel $x^2$ a $y$ je párne.

Uvažujme najprv možnosť, že $y$ je párne. To znamená, že pre nejaké (nesúdeliteľné) čísla $a$, $b$ platí

$$x^2 = a^2 - b^2 \qquad y = 2ab \qquad z^2 = a^2 + b^2.$$

Z toho dostaneme

$$(xz)^2 = x^2 z^2 = (a^2 - b^2)(a^2 + b^2) = a^4 - b^4.$$

Teda čísla $a$, $b$ a $xz$ spĺňajú rovnosť

$$a^4 = b^4 + (xz)^2,$$

pričom $b^2 < a^2$, teda $0 < b < a < z$, čo je v spore s predpokladom, že sme zobrali trojicu s najmenšou možnou hodnotou pravej strany.

Zostáva teda možnosť, že $y$ je nepárne. (A teda $z$ je nepárne, $x$ je párne.) V tomto prípade máme $x^2 = 2mn$, $z^2 = m^2 + n^2$ pre nejaké nesúdeliteľné čísla $m$, $n$ rôznej parity.

Predpokladajme, že $m$ je párne, $n$ nepárne. Potom $(2m, n) = 1$ a z rovnosti $x^2 = 2mn$ máme $n = s^2$ a $2m = r^2$. Z druhej rovnosti dostaneme, že $r$ je párne, a teda $m = 2t^2$ a $(t, s) = 1$. Z toho

$$z^2 = m^2 + n^2 = 4t^4 + s^4.$$

Opäť sme dostali primitívny pytagorovský trojuholník $s^2$, $2t^2$, $z$. Preto $2t^2 = 2uv$, z čoho máme, že $u$ aj $v$ sú druhé mocniny prirodzených čísel $u = a^2$, $v = b^2$. Potom

$$s^2 = u^2 - v^2 = a^4 - b^4,$$

teda $b^4 + s^2 = a^4$ a $a < a^4 < s^2 < z$. Dostali sme menšie riešenie.

Prípad, že $m$ je nepárne a $n$ je párne je symetrický. (Použili sme len rovnosti $z^2 = m^2 + n^2$ a $x^2 = 2mn$, v ktorých $m$ a $n$ vystupujú rovnocenne.)

□



**Dôsledok 6.3.3.** *Neexistuje pytagorovský trojuholník s celočíselnými dĺžkami strán, ktorého dve strany by boli druhými mocninami prirodzených čísel.*

**Dôsledok 6.3.4.** *Plocha pravouhlého trojuholníka s celočíselnými dĺžkami strán nemôže byť druhou mocninou prirodzeného čísla.*

*Dôkaz.* Ak by sme mali $x^2 + y^2 = z^2$ a $\frac{xy}{2} = s^2$, tak z toho dostaneme

$$(x + y)^2 = z^2 + 4s^2$$
$$(x - y)^2 = z^2 - 4s^2$$
$$(x^2 - y^2)^2 = z^4 - (2s)^4,$$

čiže trojica $2s$, $x^2 - y^2$ a $z$ by tvorila celočíselné riešenie rovnice (6.8). □

**Cvičenia**

1. Metódou nekonečnej regresie ukážte, že rovnica $x^2 + y^2 = 3(z^2 + w^2)$ nemá riešenie v prirodzených číslach.
2. Dokážte, že neexistujú prirodzené čísla $x$, $y$, $z$ a $w$ také, že $x$, $y$, $z$ aj $y$, $z$, $w$ by boli pytagorovské trojice.
3. Riešte diofantickú rovnicu $x^2 + y^2 = 2z^2$.
4. Môže mať riešenie rovnica $x^n + y^n = z^n$; $x, y, z$ sú prvočísla, $n \geq 2$?

## 6.4 Diofantické rovnice a deliteľnosť

Na dôkaz toho, že nejaká diofantická rovnica nemá riešenie môžeme v niektorých jednoduchých prípadoch použiť zvyškové triedy a kongruencie.

**Príklad 6.4.1.** Jediné riešenie rovnice

$$2^m - 3^n = 1$$

v prirodzených číslach je $m = 2$, $n = 1$.

Má platiť $2^m - 1 = 3^n$. Ak $m \geq 3$, tak $8 \mid 2^m$ a $2^m - 1 \equiv 7 \pmod 8$. Ľahko zistíme, že zvyšky $3^n$ po delení 8 sú striedavo 1 (pre párne $n$) a 3 (pre nepárne). Teda $3^n$ je kongruentné s 1 alebo 3, čo znamená, že riešenie s $m \geq 3$ neexistuje. Jediné riešenie je teda $m = 2$, $n = 1$.

Na okraj poznamenajme, že dokonca rovnica

$$x^a - y^b = 1$$

nemá v prirodzených číslach takých, že $x, a, y, b > 1$, iné riešenie ako $x = 3$, $a = 2$, $y = 2$, $b = 3$. Tento výsledok formuloval ako hypotézu Charles Catalan v 19. storočí a v r. 2002 ho dokázal Preda Mihailescu. (Čiastočný výsledok dosiahol holandský matematiky Robert Tijdeman, ktorý dokázal v r. 1976, že táto rovnica môže mať len konečne veľa riešení.)

Nasledujúca veta ukazuje, že niekedy môžu byť pri dôkaze neriešiteľnosti diofantickej rovnické byť užitočné aj zákony kvadratickej reciprocity.

**Veta 6.4.2.** *Diofantická rovnica*

$$y^2 = x^3 + k \tag{6.9}$$ {diofdelit:EQAP1}

*nemá riešenie, ak* $k$ *je tvaru*

$$k = (4n - 1)^3 - 4m^2 \tag{6.10}$$ {diofdelit:EQAP2}

*kde* $m, n \in \mathbb{N}$ *a* $m$ *nie je deliteľné žiadnym prvočíslom tvaru* $p = 4k + 3$.

## 6.5 Gaussovské a eisensteinovské celé čísla

{diof:SECTGCC}

Predtým, ako si ukážeme riešenie niektorých ďalších diofantických rovníc, na chvíľu odbočíme a povieme si niečo o dvoch rozšíreniach celých čísel, ktoré bývajú v teórii čísel často užitočné.

### Euklidovské okruhy

Začneme s o niečo všeobecnejším pojmom Euklidovského okruhu. Najpodstatnejším výsledkom tejto časti je fakt (ktorý už možno poznáte z iných prednášok), že každý Euklidovský okruh je okruhom hlavných ideálov a každý okruh hlavných ideálov je okruhom s jednoznačným rozkladom. Dobrý úvod do teórie Euklidovských okruhov a okruhov s jednoznačným rozkladom možno nájsť napríklad v [DF] alebo [KGGS].

**Definícia 6.5.1.** Obor integrity $R$ sa nazýva *Euklidovský okruh,* ak existuje funkcia $N\colon R \to \mathbb{N}_0$ taká, že pre ľubovoľné $a, b \in R$, $b \neq 0$ existujú $c, d \in R$ také, že $a = bc + d$ a buď $d = 0$ alebo $N(d) < N(b)$.

Funkciu $N$ budeme nazývať *norma.*

Okamžite ste si určite všimli podobnosť s vetou o delení so zvyškom. Názov Euklidovský okruh skutočne pochádza z toho, že v takomto okruhu sa dá používať Euklidov algoritmus.

Pripomeňme, že obor integrity $R$ sa nazýva *okruhom hlavných ideálov,* (skrátene OHI) ak každý ideál $I$ v $R$ je hlavný (vygenerovaný jediným prvkom), čiže je tvaru $I = (a) = \{ar; r \in R\}$ pre nejaké $a \in R$. (Nie vždy sa požaduje, aby okruh hlavných ideálov bol obor integrity – vyskytujú sa obe možné definície. My budeme vždy predpokladať, že OHI je obor integrity.)

**Definícia 6.5.2.** Prvok $u$ okruhu $R$ s jednotkou sa nazýva *invertibilný* alebo tiež *deliteľ jednotky* v okruhu $R$, ak existuje prvok $a$ taký, že $au = 1$. Množinu všetkých deliteľov jednotky v okruhu $R$ budeme označovať $U(R)$.

Ak pre prvky $x, y \in R$ platí $x = ru$ pre nejaký invertibilný prvok $u$, hovoríme, že $x$ a $y$ sú *asociované,* označujeme $x \sim y$.

Invertibilné prvky daného okruhu s jednotkou tvoria grupu vzhľadom na násobenie a relácia $\sim$ je reláciou ekvivalencie na $R$.

Ľahko si môžeme všimnúť, že

**Lema 6.5.3.** *Ak $R$ je euklidovský okruh, $u \neq 0$ a $N(u) = 0$, tak $u$ je invertibilný.*

*Dôkaz.* Priamo z definície máme, že $1 = u.c + d$, pričom $N(d) < 0$ alebo $d = 0$. Pretože prípad $N(d) < 0$ nemôže nastať, máme $d = 0$. □

**Tvrdenie 6.5.4.** *Každý Euklidovský okruh je okruh hlavných ideálov.*

*Dôkaz.* Nech $R$ je Euklidovský okruh, $I \neq \emptyset$ je vlastný ideál v $R$ a $b$ je prvok z $I$ s najmenšou nenulovou normou. (Ideál $I$ je vlastný, preto neobsahuje žiadne invertibilné prvky. Preto musí obsahovať aspoň jeden prvok s nenulovou normou.)

Tvrdíme, že $I = (b)$. Pre každý prvok $a \in I$ máme $a = b.c + d$. Pritom $d = b.c - a \in I$, čiže opäť nemôže nastať možnosť $N(d) < N(b)$. Teda $d = 0$ a $a = b.c$. □

### Deliteľnosť v okruhoch hlavných ideálov

V ľubovoľnom okruhu môžeme definovať reláciu deliteľnosti presne rovnako ako sme ju zaviedli pre prirodzené čísla:



**Definícia 6.5.5.** Nech $a, b \in R$, kde $R$ je okruh. Hovoríme, že $a$ *delí* $b$, značíme $a \mid b$, ak existuje $k \in R$ také, že $b = k.a$.

*Najväčší spoločný deliteľ* prvkov $a, b \in R$ je taký prvok $c \in R$, že

*(i)* $c \mid a$, $c \mid b$,

*(ii)* pre ľubovoľný prvok $d \in R$ taký, že $d \mid a$ a $d \mid b$ platí aj $d \mid c$.

Označujeme ho $(a, b)$.

Ľahko vidíme vzťah medzi deliteľnosťou v okruhu a hlavnými ideálmi:

$$a \mid b \qquad \Leftrightarrow \qquad (b) \subseteq (a).$$

Z toho je zrejmé, že ak existuje $c = (a, b)$ v okruhu hlavných ideálov $R$, tak $c$ je práve generátor ideálu $\{ax + by; x, y \in \mathbb{R}\}$ (čo je najmenší ideál obsahujúci $a$ aj $b$.) Teda v každom OHI platí Bézoutova identita

$$c = au + bv.$$

Vzťah asociovanosti možno vyjadriť pomocou deliteľnosti: $x$ a $y$ sú asociované práve vtedy, keď $x \mid y$ aj $y \mid x$. Z toho sa dá odvodiť, že n.s.d. 2 prvkov je určený jednoznačne až na asociovanosť.

Pripomeňme nasledujúce definície:

**Definícia 6.5.6.** Ideál $I$ v okruhu $R$ voláme *prvoideál,* ak $a.b \in I$ implikuje $a \in I$ alebo $b \in I$.

Ideál $I$ v okruhu $R$ je *maximálny,* ak $I \subseteq J \subseteq R$, kde $J$ je ideál, implikuje $J = I$ alebo $J = R$.

Ideál $I$ je maximálny práve vtedy, keď faktorový okruh $R/I$ je pole. Ideál $I$ je prvoideál práve vtedy, keď faktorový okruh $R/I$ je obor integrity. Každý maximálny ideál je prvoideál. V nasledujúcom tvrdení ukážeme, že v OHI platí aj opačná implikácia. Pripomeňme ešte jeden užitočný fakt, ktorý sa dá dokázať pomocou axiómy výberu: každý ideál v $R$ je obsiahnutý v nejakom maximálnom ideále.

**Tvrdenie 6.5.7.** *Ak $I = (m)$ je prvoideál v OHI $R$, tak $I$ je maximálny.*

*Dôkaz.* Nech $I \subseteq J \subseteq R$. Pretože $R$ je OHI existuje prvok $a \in R$ taký, že $J = (a)$. Máme teda $(m) \subseteq (a)$, čiže $m = a.c$ pre nejaké $c \in R$. Potom buď $a \in I$ a $I = (a)$ alebo $c \in I$, čiže $c = m.d$ a $m = a.c = m(ad)$. Z toho máme $ad = 1$ (pretože $R$ je OI), čiže $a$ je invertibilný a $(a) = R$. □

Pojem analogický k pojmu prvočísla je v okruhu pojem ireducibilného prvku.

**Definícia 6.5.8.** Prvok $a$ okruhu $R$ sa nazýva *ireducibilný,* ak z rovnosti $a = b.c$ vyplýva, že niektorý z prvkov $b$, $c$ je invertovateľný v $R$.

Inými slovami, ireducibilný prvok sa (až na asociovanosť) nedá zapísať ako súčin dvoch prvkov z $R$ inak ako $1.a$.

**Tvrdenie 6.5.9.** *Ak ideál $(p)$ v OI $R$ je prvoideál, tak $p$ je ireducibilný v $R$.*

*Dôkaz.* Ak $(p)$ je prvoideál a $ab = p$, tak jeden prvok z dvojice $a$, $b$ musí byť násobkom $p$. Bez ujmy na všeobecnosti, nech $a = kp$. Potom $p = ab = (kb)p$, z čoho $kb = 1$, čiže $b$ je invertibilný. □

V OHI platí aj obrátená implikácia.

**Tvrdenie 6.5.10.** *Ak $p$ je ireducibilný prvok v OHI $R$, tak $(p)$ je prvoideál.*

*Dôkaz.* Nech $p$ je ireducibilný. Ukážeme, že ideál $p$ je maximálny (a teda je to prvoideál). Nech by $(p) \subseteq (m)$. Z toho vyplýva $p = m.c$. Potom buď $m$ je asociovaný s $p$ a $(p) = (m)$, alebo $m$ je invertibilný a $(m) = R$. □

Z toho dostávame nasledujúci vzťah, ktorý bol kľúčový v dôkaze základnej vety aritmetiky. {gcc:DOSPRVOC}

**Dôsledok 6.5.11.** *V OHI pre ľubovoľný ireducibilný prvok $p$ platí implikácia $p \mid ab \Rightarrow p \mid a \vee p \mid b$.*

### Okruhy s jednoznačným rozkladom

**Definícia 6.5.12.** *Okruh s jednoznačným rozkladom* je obor integrity, v ktorom pre každý prvok $x \in R$, ktorý je nenulový a nie je invertibilný, existuje rozklad

$$x = p_1 \dots p_k$$

na súčin ireducibilných prvkov a navyše je tento rozklad jednoznačný až na asociovanosť a poradie.

**Tvrdenie 6.5.13.** *Obor integrity, ktorý je okruhom hlavných ideálov, je okruh s jednoznačným rozkladom.*

*Dôkaz.* Chceme dokázať existenciu a jednoznačnosť rozkladu na súčin ireducibilných prvkov. Jednoznačnosť vyplýva z dôsledku 6.5.11.

*Existencia.* Sporom. Nech by $x$ bol taký prvok, ktorý sa nedá v $R$ rozložiť na súčin ireducibilných prvkov. Pretože $x$ nie je ireducibilný, vieme ho zapísať ako $x = r_1.q_1$. Keby obidva prvky $r_1$ aj $q_1$ boli ireducibilné, máme rozklad $x$. Teda jeden z nich nie je ireducibilný, bez ujmy na všeobecnosti nech je to $q_1$. Potom $q_1 = r_2.q_2$ pre nejaké $r_2, q_2 \in R$. Takýmto spôsobom indukciou zostrojíme nekonečnú postupnosť prvkov $r_n \in R$ takú, že nasledujúci vždy delí predchádzajúci, teda $r_{n+1} \mid r_n$. To je ekvivalentné s tým, že $(r_n) \subseteq (r_{n+1})$ a takto dostávame nekonečnú postupnosť ideálov $I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n \subsetneq \dots$, kde $I_k$ označuje ideál $(r_k)$. Ukážeme, že v OHI takáto postupnosť nemôže existovať, čím dostaneme požadovaný spor.

Skutočne, ak by sme mali takýto rastúci reťazec ideálov. Potom aj $I = \bigcup_{n=1}^{\infty} I_n$ je ideál. Pretože $R$ je OHI, existuje $a \in R$ také, že $(a) = I$. Lenže z toho, že $a \in \bigcup_{n=1}^{\infty} I_n$ vyplýva existencia čísla $n_0$ s vlastnosťou $a \in I_{n_0}$. Potom pre všetky $n > n_0$ máme $(a) \subseteq I_{n_0} \subseteq I_n \subseteq I$, čiže od $n_0$ počnúc sa už všetky ideály $I_n$ rovnajú. □

Poznamenajme, že okruhy, ktoré spĺňajú podmienku, že v nich neexistuje nekonečný rastúci reťazec ideálov, sa nazývajú *noetherovské.*

### Okruhy $\mathbb{Z}[i]$ a $\mathbb{Z}[\omega]$

**Definícia 6.5.14.** Komplexné číslo $a + bi$ nazývame *gaussovským celým číslom,* ak $a, b \in \mathbb{Z}$. Okruh gaussovských celých čísel označujeme $\mathbb{Z}[i]$.

Očividne $\mathbb{Z}[i]$ je podokruh $\mathbb{C}$.

Veľmi podobne sa definujú eisensteinovské celé čísla. V ďalšom budem $\omega$ označovať číslo

$$\omega = \frac{-1 + i\sqrt{3}}{2},$$

čo je jedna z tretích odmocnín z 1 v komplexných číslach.



**Definícia 6.5.15.** *Eisensteinovské celé čísla* sú čísla tvaru $a + b\omega$, kde $a, b \in \mathbb{Z}$.

Pre počítanie s takýmito číslami je užitočné si uvedomiť, že

$$1 + \omega + \omega^2 = 0.$$

Pomocou tejto rovnosti sa už vcelku jednoducho dá overiť, že aj eisensteinovské celé čísla tvoria podokruh $\mathbb{C}$. Tento okruh označujeme $\mathbb{Z}[\omega]$.

Naším cieľom je ukázať, že oba okruhy, ktoré sme práve zadefinovali, sú euklidovské. Najprv zadefinujeme normu pre tieto okruhy.

**Definícia 6.5.16.** *Normou* gaussovského (eisensteinovského) celého čísla $z = a+bi$ nazývame číslo

$$N(z) = |z|^2 = z.\overline{z}.$$

To znamená, že pre gaussovské celé číslo $z = a + bi$ je norma daná predpisom

$$N(z) = a^2 + b^2. \tag{6.11}$$ {gcc:NORMGAUS}

Pre eisensteinovské celé číslo $z = a + b\omega$ máme

$$N(z) = a^2 + b^2 - ab. \tag{6.12}$$ {gcc:NORMEIS}

Z rovnosti $N(z) = |z|^2$ je zrejmé, že

$$N(z).N(z') = N(zz'). \tag{6.13}$$ {gcc:NORMPROD}

**Tvrdenie 6.5.17.** *Gaussovské celé čísla tvoria euklidovský okruh.*

*Dôkaz.* Nech $z = a + bi$, $w = c + di$ sú dva prvky zo $\mathbb{Z}[i]$. Chceme nájsť $q, r \in \mathbb{Z}[i]$ také, že $z = q.w + r$ a $N(r) < N(w)$.

Potom $\frac{z}{w} = g + hi$, kde $g, h \in \mathbb{Q}$. Zvoľme $m, n \in \mathbb{Z}$ tak, že $|g - m| \leq \frac{1}{2}$ a $|h - n| \leq \frac{1}{2}$. Položme

$$q = m + ni.$$

Potom $r$ musí mať hodnotu

$$r = z - qw = \left(\frac{z}{w} - q\right) w = w.\left((g - m) + (h - n)i\right).$$

Vidíme, že pri takejto voľbe čísla $r$ platí $r \in \mathbb{Z}[i]$ a

$$N(r) = N(w).[(g - m)^2 + (h - n)^2] \leq N(w)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{N(w)}{2} < N(w).$$

□

**Tvrdenie 6.5.18.** *Eisensteinovské celé čísla tvoria Euklidovský okruh.*

*Dôkaz.* Dôkaz bude veľmi podobný ako pre gaussovské celé čísla. Využijeme to, že vzťah (6.13) nám hovorí, ako môžeme deliť čísla tvaru $a + b\omega$.

Označme $z = a + b\omega$, $w = c + d\omega$. Potom

$$\frac{z}{w} = \frac{z\overline{w}}{w\overline{w}} = \frac{(a + b\omega)(c + d\omega^2)}{N(w)} = g + h\omega,$$

kde $g = \frac{ac+bc-d}{N(w)}$ a $h = \frac{bc-ad}{N(w)}$.

Opäť si zvolíme celé čísla $m$, $n$ s vlastnosťou $|g-m| \le \frac{1}{2}$ a $|h-n| \le \frac{1}{2}$ a

$$q = m + n\omega.$$

Potom pre $r$ dostaneme

$$r = z - qw = \left(\frac{z}{w} - q\right) w = w.\left((g-m) + (h-n)\omega\right),$$
$$N(r) = N(w).[(g-m)^2 + (h-n)^2 - (g-m)(h-n)] \le N(w)\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) < N(w).$$

□ {gcc:TVREISENUNITS}

**Tvrdenie 6.5.19.** *Delitele jednotky v $\mathbb{Z}[\omega]$ sú práve čísla*

$$\{\pm 1, \pm\omega, \pm\omega^2\}.$$

*Dôkaz.* Zrejme ak $u$ je deliteľ jednotky, tak musí platiť $N(u) = 1$ (vďaka tomu, že norma v $\mathbb{Z}[\omega]$ je multiplikatívna). Skúsme teda nájsť všetky $a, b \in \mathbb{Z}$ pre ktoré

$$N(a + b\omega) = a^2 + b^2 - ab = (a-b)^2 + ab = 1.$$

Ak si navyše uvedomíme, že $z$ je deliteľ jednotky práve vtedy, keď $\overline{z}$ je deliteľ jednotky, stačí nám uvažovať prípad $ab \ge 0$. (Pre $z = a + b\omega$ máme $\overline{z} = a + b\omega^2 = a - b(1+\omega) = (a-b) - b\omega$. Teda ak $ab < 0$, tak $(a-b)(-b) = -ab + b^2 \ge 0$, čiže prechodom k $\overline{z}$ zmeníme znamienko $ab$ na kladné.)

Ak teda máme 1 dostať ako súčet 2 celých čísel, musí byť jedno z nich 1 a druhé 0, teda máme možnosti
$|a-b| = 1 \wedge ab = 0$, čiže $a = \pm 1$, $b = 0$ alebo $a = 0$, $b = \pm 1$
$|a-b| = 0 \wedge ab = 1$, čiže $a = b = \pm 1$.

Dostali sme takto čísla $\pm 1$, $\pm\omega$ a $\pm(-1-\omega) = \pm\omega^2$. Pridaním komplexne združených čísel nám už nič nepribudne, takže toto sú jediní možní kandidáti na deliteľov jednotky. Ľahko vidno, že tieto čísla aj skutočne deliteľmi jednotky sú.

□

Jednoducho sa dá overiť, že delitele jednotky v $\mathbb{Z}[i]$ sú práve $\{\pm 1, \pm i\}$. V oboch okruhoch teda platí $N(u) = |u|^2 = 1 \Leftrightarrow u$ je deliteľ jednotky.

### Cvičenia

1. Nech $\mathbb{Z}[\sqrt{-2}] = \{a + bi\sqrt{2}; a, b \in \mathbb{Z}\}$. Dokážte, že $\mathbb{Z}[\sqrt{-2}]$ s normou $N(a + bi\sqrt{2}) = a^2 + 2b^2$ je Euklidovský okruh.
2. Ak $r$ je prvok $\mathbb{Z}[i]$ (prvok $\mathbb{Z}[\omega]$) taký, že $N(r)$ je prvočíslo, tak $r$ je ireducibilný prvok v $\mathbb{Z}[i]$ (v $\mathbb{Z}[\omega]$).
3. Overte, že $4\mathbb{Z} + 1$ nie je okruh s jednoznačným rozkladom. {gcccvic:IREDZI}
4. Ak $z$ je prvok okruhu $\mathbb{Z}[i]$ (alebo $\mathbb{Z}[\omega]$) taký, že $N(z)$ je prvočíslo, tak $z$ je ireducibilný.



## 6.6 Diofantická rovnica $x^3 + y^3 = z^3$

V tejto časti využijeme okruh $\mathbb{Z}[\omega]$ na dôkaz toho, že Veľká Fermatova veta platí aj pre exponent 3. {fermat2:VTX3Y3Z3}

**Veta 6.6.1.** *Nech $u \in \mathbb{Z}[\omega]$ je nejaký (pevne zvolený) deliteľ jednotky. Rovnica*

$$x^3 + y^3 = uz^3 \tag{6.14}$$ {fermat2:EQEXP3UNIT

*nemá riešenie v okruhu $\mathbb{Z}[\omega]$ také, že $xyz = 0$. (A teda nemá ani celočíselné riešenie s vlastnosťou $xyz = 0$.)*

Dôkaz, ako ho uvedieme tu, v podstate sleduje knihu [Ri, Chapter III.3]. Nájsť sa dá napríklad aj v [HW] a [IR, Chapter 17.8].

V dôkaze budeme často využívať číslo

$$\lambda = 1 - \omega = \frac{3 - \sqrt{3}i}{2}, \tag{6.15}$$ {fermat2:EQLAMBDA}

preto si najprv ukážeme niektoré jeho vlastnosti.

Priamym výpočtom sa možno presvedčiť, že platí

$$\lambda^2 = 1 - 2\omega + \omega^2 = -3\omega \tag{6.16}$$ {fermat2:EQLAMBSQ}

**Lema 6.6.2.** *Číslo $\lambda$ má v $\mathbb{Z}[\omega]$ normu $N(\lambda) = 3$, je teda ireducibilným prvkom $\mathbb{Z}[\omega]$.*

*Dôkaz.* Priamo dosadením do (6.12) dostaneme $N(\lambda) = N(1-\omega) = 1 + 1 + 1 = 3$. □ {fermat2:LMMODLAMBD

**Lema 6.6.3.** *Pre každé $a \in \mathbb{Z}[\omega]$ platí práve jedna z kongruencií*

$$a \equiv 0, \pm 1 \pmod{\lambda}. \tag{6.17}$$ {fermat2:EQKONGLAMB

*Konkrétne platí*

$$\omega \equiv 1 \pmod{\lambda},$$
$$\omega^2 \equiv 1 \pmod{\lambda}.$$

*Dôkaz.* Stačí si všimnúť, že $\omega \equiv 1 \pmod{\lambda}$ a $\lambda \mid 3$ (pozri (6.16)). Z toho máme $x + y\omega \equiv x + y \pmod{\lambda}$, a pretože $x + y$ je kongruentné s niektorým z čísel $0, \pm 1$ modulo 3, to isté platí aj modulo $\lambda$.

Pretože $\lambda$ nie je invertibilný prvok v $\mathbb{Z}[\omega]$ máme $\lambda \nmid 1$ a $\pm 1 \not\equiv 0 \pmod{\lambda}$, čiže uvedené kongruencie nemôžu platiť súčasne. □ {fermat2:LMLAMB4}

**Lema 6.6.4.** *Ak $a \in \mathbb{Z}[\omega]$ a $\lambda \nmid a$, tak*

$$a^3 \equiv \pm 1 \pmod{\lambda^4}. \tag{6.18}$$ {fermat2:EQLAMB4}

(*Presnejšie $a \equiv 1 \pmod{\lambda} \Rightarrow a^3 \equiv 1 \pmod{\lambda^4}$ a $a \equiv -1 \pmod{\lambda} \Rightarrow a^3 \equiv -1 \pmod{\lambda^4}$.*)

*Dôkaz.* Predpokladajme najprv, že $a \equiv 1 \pmod{\lambda}$, čiže $a = 1 + k\lambda$ pre nejaké $k \in \mathbb{Z}[\omega]$. Potom

$$a^3 - 1 = (a-1)(a-\omega)(a-\omega^2) = k\lambda(1 - \omega + k\lambda)(1 - \omega^2 + k\lambda) =$$
$$k\lambda(\lambda + k\lambda)((1+\omega)\lambda + k\lambda) = \lambda^3 k(1+k)(k - \omega^2)$$

Podľa lemy 6.6.3 buď $\lambda \mid k$, alebo $\lambda \mid 1+k$ alebo $\lambda \mid 1-k$. V poslednom prípade máme $\omega^2 \equiv 1 \equiv k \pmod{\lambda}$, čiže $\lambda \mid k-\omega^2$. Vo všetkých 3 prípadoch teda máme $\lambda \mid k(1+k)(k-\omega^2)$, a teda

$$\lambda^4 \mid a^3 - 1,$$

čiže $a^3 \equiv 1 \pmod{\lambda^4}$.

Zostáva ešte prípad $a \equiv -1 \pmod{\lambda}$. Táto možnosť sa však dá previesť na prípad, ktorý sme riešili v prvej časti dôkazu. Platí totiž $a^3 \equiv -(-a)^3 \equiv -1 \pmod{\lambda}$. □

{fermat2:DOS5}

**Dôsledok 6.6.5.** *Rovnica* (6.14) *nemá riešenie také, že $\lambda$ nedelí žiadne z čísel $x, y, z$.*

*Dôkaz.* Ak by sme mali také riešenie, tak podľa lemy 6.6.4 dostaneme

$$\pm 1 \pm 1 \equiv \pm u \pmod{\lambda^4}.$$

Na ľavej strane môžeme dostať 0 alebo $\pm 2$. Na pravej strane dostaneme $\pm 1$, pretože invertibilné prvky môžu mať len zvyšok $\pm 1$. □

{fermat2:LM6}

**Lema 6.6.6.** *Nech $\lambda \nmid xy$. Ak*

$$x^3 + y^3 = uz^3,$$

*kde $u$ je invertibilný prvok v $\mathbb{Z}[\omega]$ a $x, y \in \mathbb{Z}[\omega]$, tak $\lambda^2 \mid z$.*

*Dôkaz.* Podľa lemy 6.6.4 máme

$$\pm 1 \pm 1 \equiv uz^3 \pmod{\lambda^4}.$$

To môže byť splnené jedine ak $\lambda^4 \mid z^3$, z čoho (vďaka ireducibilnosti $\lambda$) už vyplýva $\lambda^2 \mid z$. □

{fermat2:LMINDKROK}

**Lema 6.6.7.** *Nech $u$ je invertibilný prvok v $\mathbb{Z}[\omega]$, $n \in \mathbb{N}$, $n \geq 2$. Nech existujú $x, y, z$ také, že*

$$x^3 + y^3 = u\lambda^{3n} z^3, \tag{6.19}$$

{fermat2:EQSUCLAM}

*pričom $\lambda \nmid xyz$. Potom existujú $x_1$, $y_1$, $z_1$, $u_1$ také, že*

$$x_1^3 + y_1^3 = u_1 \lambda^{3(n-1)} z_1^3, \tag{6.20}$$

{fermat2:EQSUCLAM2}

*pričom opäť $u_1$ je invertibilný prvok v $\mathbb{Z}[\omega]$ a $\lambda \nmid z_1$.*

*Dôkaz.* Opäť bez ujmy na všeobecnosti môžeme predpokladať $(x, y) = 1$. (Vydelíme prípadným spoločným deliteľom alebo vezmeme riešenie s najmenšou možnou normou $x$.)

Máme

$$(x+y)(x+y\omega)(x+y\omega^2) = u\lambda^{3n} z^3. \tag{6.21}$$

{fermat2:EQSUCIN3}

Pretože $\lambda^4$ delí pravú stranu, aspoň jedno z čísel na ľavej strane musí byť deliteľné $\lambda^2$. Bez ujmy na všeobecnosti môžeme predpokladať, že je to $x+y$. (V opačnom prípade stačí zaviesť substitúciu $y' = \omega y$ prípadne $y' = \omega^2 y$. Toto nové $y$ vyhovuje tej istej rovnici.)

Máme teda $\lambda^2 \mid x + y$. Pretože

$$x + y\omega = x + y - y(1-\omega) = x + y - \lambda,$$

dostávame $\lambda^2 \nmid x + y\omega$. Podobne

$$x + y\omega^2 = x + y - y(1-\omega^2) = x + y - y(1+\omega)\lambda$$



a $y(1+\omega) = -\omega^2 y \not\equiv 0 \pmod{\lambda}$, teda opäť $\lambda^2 \nmid x + y\omega^2$. Z toho dostaneme

$$\lambda^{3n-2} \mid x + y.$$

Súčasne máme $(x+y, x+y\omega) = (x+y, x+y-(x+y\omega)) = (x+y, y\lambda) = \lambda(x+y, y) = \lambda(x, y) = \lambda$. Podobne $(x+y, x+y\omega^2) = (x+y, y(1+\omega)\lambda) = \lambda(x+y, 1+\omega) = \lambda$. (Treba si uvedomiť, že $1+\omega = -\omega^2$ deliteľom jednotky v $\mathbb{Z}[\omega]$.)

Takisto dostaneme $(x+y\omega, x+y\omega^2) = (x+y\omega, y\omega(1-\omega)) = (x+y\omega, y\omega\lambda) = \lambda$.

Dostali sme teda, že čísla $\frac{x+y}{\lambda}$, $\frac{x+y\omega}{\lambda}$ a $\frac{x+y\omega^2}{\lambda}$ sú po dvoch nesúdeliteľné.

$$\left(\frac{x+y}{\lambda}, \frac{x+y\omega}{\lambda}\right) = \left(\frac{x+y}{\lambda}, \frac{x+y\omega^2}{\lambda}\right) = \left(\frac{x+y\omega}{\lambda}, \frac{x+y\omega^2}{\lambda}\right) = 1.$$

Z (6.21) (s využitím toho, že pracujeme v okruhu s jednoznačným rozkladom) máme

$$x + y = \lambda^{3n-2} u_1 a^3,$$
$$x + y\omega = \lambda u_2 b^3,$$
$$x + y\omega^2 = \lambda u_3 c^3,$$

kde $u_{1,2,3}$ sú invertibilné v $\mathbb{Z}[\omega]$ a $a$, $b$, $c$ sú (po dvoch) nesúdeliteľné.

Použitím rovnosti $1 + \omega + \omega^2 = 0$ z toho dostaneme

$$0 = (x+y) + \omega(x+y\omega) + \omega^2(x+y\omega^2) = \lambda^{3n-2} u_1 a^3 + \omega\lambda u_2 b^3 + \omega^2 \lambda u_3 c^3.$$

Túto rovnosť môžeme vydeliť číslom $\lambda$ a dostaneme rovnosť tvaru

$$t' \lambda^{3(n-1)} a^3 = b^3 + tc^3, \tag{6.22}$$

{fermat2:EQTT}

kde $t$ a $t'$ sú opäť nejaké invertibilné prvky, $\lambda \nmid bc$ a $(b, c) = 1$.

V prípade, že $t = \pm 1$ máme riešenie $b$, $tc$, $a$ rovnice (6.20). Stačí teda už len ukázať, že nemôže nastať prípad $t = \pm\omega, \pm\omega^2$.

Pretože $n \geq 2$, rovnosť (6.22) implikuje

$$b^3 + tc^3 \equiv 0 \pmod{\lambda^2}.$$

Súčasne podľa lemy 6.6.4 máme $b^3 \equiv \pm 1 \pmod{\lambda^2}$, $c^3 \equiv \pm 1 \pmod{\lambda^2}$, a teda

$$\pm 1 \pm t \equiv 0 \pmod{\lambda^2},$$

čiže $t \equiv \pm 1 \pmod{\lambda^2}$.

Vieme, že $\lambda^2 = -3\omega$. V jednotlivých prípadoch dostávame $\lambda^2 \nmid 1 - \omega = \lambda$, $\lambda^2 \nmid 1 + \omega$ (lebo $1 + \omega$ je invertibilný prvok), $\lambda^2 \nmid 1 - \omega^2 = (1-\omega)(1+\omega) \sim \lambda$ a $\lambda \nmid 1 + \omega^2 = -\omega$ (opäť z dôvodu, že ide o invertibilný prvok). □

*Dôkaz vety 6.6.1.* BUNV môžeme predpokladať, že riešenia rovnice (6.14) sú nesúdeliteľné v $\mathbb{Z}[\omega]$ (v opačnom prípade predelíme spoločným deliteľom). Číslo $\lambda$ teda nedelí aspoň dve z čísel $x$, $y$, $z$. Súčasne vieme z dôsledku 6.6.5, že $\lambda$ delí aspoň jedno číslo z tejto trojice.

Pomocou nekonečnej regresie vieme dokázať, že neexistuje riešenie také, že $\lambda \mid z$. Vyplýva to z liem 6.6.7 a 6.6.6 – vždy vieme znížiť stupeň „prvočísla“ $\lambda$ v roklade čísla $z$. (Hľadáme riešenie, kde v rozklade $z$ vystupuje $\lambda$ v najmenšom exponente.)

Zostáva teda možnosť, že $\lambda \nmid z$ a $\lambda \mid xy$. Bez ujmy na všeobecnosti nech $\lambda \mid x$. Dostávame potom $\pm 1 \equiv u \pmod{\lambda^3}$, z čoho vyplýva, že $u = \pm 1$ (podobne ako v dôkaze lemy 6.6.7). Potom ale máme $x^3 + y^3 = \pm z^3 \Rightarrow (\pm z)^3 + (-y)^3 = x^3$, čiže sme sa opäť dostali do situácie, že $\lambda$ delí pravú stranu rovnice. □

# Kapitola 7

# Aditívne vlastnosti prirodzených čísel

Táto kapitola je venovaná niektorým problémom patriacim do aditívnej teórie čísel – budeme sa zaoberať otázkou, či sa všetky/niektoré prirodzené čísla dajú vyjadriť ako súčet čísel z nejakej množiny, pričom použijeme najviac/práve $k$ sčítancov ($k$ je nejaké dané číslo.)

## 7.1 Bázy množiny $\mathbb{N}$

**Definícia 7.1.1.** Ak $A_1, \ldots, A_k \subseteq \mathbb{N}$, tak ako $A_1 + \ldots + A_k$ označujeme množinu všetkých čísel tvaru $a_1 + \ldots + a_k$, kde $a_i \in A_i \cup \{0\}$ pre všetky $i = 1, 2, \ldots, k$.

Ďalej definujeme $nA$ pre $n \in \mathbb{N}$ induktívne ako: $1A = A$ a

$$(n+1)A = nA + A.$$

Dôležité je si všimnúť, že v predchádzajúcej definícii povoľujeme ako sčítanec aj 0, preto $A_i \subseteqq A_1 + \ldots A_k$ pre $i = 1, \ldots, k$.

{bazy:DEFBAZA}

**Definícia 7.1.2.** Hovoríme, že $A \subseteq \mathbb{N}$ je *aditívna báza* množiny $\mathbb{N}$, ak existuje $k \in \mathbb{N}$ také, že

$$\mathbb{N} = kA.$$

Najmenšie také $k$ nazývame *rádom* aditívnej bázy $A$.

Ukážeme, ako sa dá použiť pojem Schnireľmanovej hustoty na dôkaz, že nejaká množina je aditívna báza. Dokážeme, že platí:

{bazy:VTSCHNBAZA}

**Veta 7.1.3.** *Ak $A \subseteq \mathbb{N}$ a $\sigma(A) > 0$, tak $A$ je aditívna báza množiny $\mathbb{N}$.*

Dôkaz sa bude opierať o nasledujúce lemy:

{bazy:LMSB1}

**Lema 7.1.4.** *Ak $A, B \subseteq \mathbb{N}$ a pre číslo $n \in \mathbb{N}$, $n \geq 2$ platí*

$$A(n) + B(n) \geq n,$$

*tak $n \in A + B$.*

*Dôkaz.* □



{bazy:LMSB2}

**Lema 7.1.5.** *Nech $A, B \subseteq \mathbb{N}$ a $\sigma(A) + \sigma(B) \geq 1$. Potom $A + B = \mathbb{N}$.*

*Dôkaz.* Musí platiť $1 \in A$ alebo $1 \in B$, inak by obe množiny mali nulovú Schnireľmanovu hustotu. Vďaka tomu $1 \in A + B$.

Nech $n > 1$. Z lemy 5.2.2 (iv) máme

$$A(n) + B(n) \geq n(\sigma(A) + \sigma(B)) \geq n.$$

Z lemy 7.1.4 potom vyplýva $n \in A + B$. □

*Dôkaz vety 7.1.3.* Podľa dôsledku 5.2.9 platí pre $m \in \mathbb{N}$

$$1 - \sigma(mA) \leq (1 - \sigma(A))^m,$$

čiže

$$\sigma(mA) \geq 1 - (1 - \sigma(A))^m.$$

Pre $m \to \infty$ pravá strana tejto nerovnosti konverguje k 1. Preto existuje $m_0$ také, že

$$\sigma(m_0 A) > \frac{1}{2}.$$

Potom platí $\sigma(m_0 A) + \sigma(m_0 A) > 1$ a z lemy 7.1.5 máme $2m_0 A = \mathbb{N}$. □

Bez dôkazu uvedieme nasledujúcu vetu, ktorá je riešením známeho Waringovho problému.

{bazy:VTWARING}

**Veta 7.1.6.** *Pre každé $k \in \mathbb{N}$ je množina $\{n^k; n \in \mathbb{N}\}$ všetkých $k$-tych mocnín aditívnou bázou množiny $\mathbb{N}$ (t.j. existuje prirodzené číslo $g(k)$ také, že každé prirodzené číslo sa dá napísať ako súčet nanajvýš $g(k)$ $k$-tych mocnín).*

Tento problém bol rozriešený Davidom Hilbertom v roku 1909. (Hilbertov dôkaz bol komplikovaný – pôvodný dôkaz využíval 25-násobný integrál, neskôr bol dôkaz založený na rovnakej myšlienke zjednodušený – v zjednodušenej verzii sa vyskytuje 5-násobný integrál.) Ďalšie výsledky, ako aj alternatívne dôkazy, podali Hardy, Littlewood a Vinogradov. (V ich výsledkoch sa už existujú aj odhady na počet $k$-tych mocnín, ktoré stačia na vyjadrenie čísla $n$ pre všetky dostatočne veľké $n$.) Neskôr sa podarilo J. V. Linnikovi výrazne zjednodušiť dôkaz vety 7.1.6 (jeho dôkaz, publikovaný v roku 1943, je elementárny v tom zmysle, že nepoužíva metódy komplexnej analýzy). Tento dôkaz využíva Schnireľmanovu hustotu.

My neskôr ukážeme toto tvrdenie aspoň pre $n = 2$, t.j. dokážeme, že množina všetkých štvorcov tvorí aditívnu bázu množiny $\mathbb{N}$ (v tomto prípade bázu rádu 4). Iný zaujímavý výsledok v tejto oblasti je, že aj prvočísla tvoria aditívnu bázu množiny $\mathbb{N}$. (Všimnime si, že v žiadnom z týchto 2 prípadov nemôžeme priamo použiť vetu 7.1.3.)

### Cvičenia

1. Každé prirodzené číslo väčšie ako 11 sa je súčtom 2 zložených čísel.

## 7.2 Súčty druhých mocnín prirodzených čísel

Cieľom tejto časti je ukázať známe výsledky o súčtoch druhých mocnín prirodzených čísel. Dokážeme Lagrangeov výsledok hovoriaci, že každé číslo sa dá napísať ako súčet štyroch druhých mocnín (veta 7.2.14). Takisto ukážeme tvrdenie pochádzajúce od Fermata, ktoré hovorí, že všetky nepárne prvočísla tvaru 4k+1 sa dajú zapísať ako súčet dvoch druhých mocnín prirodzených čísel (veta 7.2.6).

### 7.2.1 Súčty dvoch štvorcov

V tejto časti sa budeme zaoberať tým, ako možno nejaké čísla rozložiť na súčet 2 druhých mocnín celých čísel, t.j. ako $n = a^2 + b^2$. Samozrejme, keďže $(-a)^2 = a^2$, stačí nám uvažovať $a, b \in \mathbb{N}_0$.

**Príklad 7.2.1.** Skúsme nájsť všetky rozklady prirodzených čísel od 1 po 20. (Z rozkladov, ktoré sa líšia len výmenov sčítancov, vyberieme vždy iba jeden.)
$1 = 1^2 + 0^2$,
$2 = 1^2 + 1^2$,
$4 = 2^2 + 0^2$,
$5 = 2^2 + 1^2$,
$8 = 2^2 + 2^2$,
$9 = 3^2 + 0^2$,
$10 = 3^2 + 1^2$,
$13 = 3^2 + 2^2$,
$16 = 4^2 + 0^2$,
$17 = 4^2 + 1^2$,
$18 = 3^2 + 3^2$,
$20 = 4^2 + 2^2$.

Všimnime si, že pre čísla 3, 6, 7, 11, 12, 14, 15, 19 žiadny taký rozklad neexistuje. Ľahko si môžeme všimnúť, že čísla tvaru $4k+3$ sa nedajú napísať ako súčet 2 štvorcov – lebo druhé mocniny po delení štyrmi dávajú buď zvyšok 0, alebo 1.

Medzi uvedenými príkladmi sme zatiaľ nenašli, žiadny príklad čísla, ktoré by malo (ak neuvažujeme výmenu sčítancov a zmenu znamienka) viac než jeden rozklad. Taký príklad nám však poskytne ktorákoľvek pytagorovská trojica.
$c^2 = a^2 + b^2 = c^2 + 0^2$
$25 = 5^2 + 0^2 = 4^2 + 3^2$

Najprv ukážeme rovnosť (7.1) z ktorej vyplýva, že množina čísel vyjadriteľných ako súčet dvoch štvorcov je multiplikatívna (uzavretá na súčiny). Pretože tento vzťah budeme používať dosť často, sformulujeme ho ako samostatnú lemu.

Tento vzťah sa nachádza v knihe Leonarda Fibonacciho Liber Quadratorum (kniha o štvorcoch). Bol však objavený indickým matematikom Brahmaguptom v 7. storočí, preto sa zvykne volať aj Brahmaguptova-Fibonacciho identita.

{sumsq:LMKOMPL}

**Lema 7.2.2 (Fibonacciho identita).** *Pre ľubovoľné $a, b, c, d \in \mathbb{R}$ platí*

$$(a^2 + b^2).(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \tag{7.1}$$

{sumsq:EQKOMPL}

*Dôkaz.* Pre komplexné čísla $x = a + bi$ a $y = c + di$ platí

$$(ac + bd)^2 + (ad - bc)^2 = |x.y|^2 = |x|^2.|y|^2 = (a^2 + b^2)(c^2 + d^2).$$

□

{sumsq:DOSMULT}

**Dôsledok 7.2.3.** *Ak $m, n \in \mathbb{N}$ sú vyjadriteľné ako súčet dvoch druhých mocnín, tak sa takto dá vyjadriť aj ich súčin $mn$.*

Iný dôkaz vôbec, nevyužívajúci komplexné čísla, spočíva v jenoduchom roznásobení uvedených výrazov.

{sumsq:LMKOMPL2}

**Lema 7.2.4 (Fibonacciho identita).** *Nech $R$ je komutatívny okruh. Pre ľubovoľné $a, b, c, d \in R$ platí*

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



*Dôkaz.*

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

□

Keď sa nad tým zamyslíme, prvok $i$ môžeme pridať k ľubovoľnému komutatívnemu okruhu s jednotkou, pričom vzťah $i^2 = -1$ jednoznačne definuje násobenie. (Navyše, ak by okruh nemal jednotku, tak ju tiež vieme pridať.) Takisto v tomto okruhu $R[i]$ môžeme definovať „komplexne združené“ číslo a bude platiť $\overline{x}.\overline{y} = \overline{xy}$, z čoho dostaneme $\|x.y\| = \|x\|.\|y\|$, kde $\|x\| = x.\overline{x}$. Teda „komplexnejší“ (čiže jednoduchší) dôkaz prejde aj v prípade ľubovoľného okruhu.

{sumsq:LMPRVMIDSUM}

**Lema 7.2.5.** *Ak $p$ je prvočíslo a $p \mid a^2 + b^2$ pre nejaké $a, b \in \mathbb{Z}$, tak buď $p$ delí obe čísla $a$ aj $b$, alebo $-1$ je kvadratický zvyšok modulo $p$.*

*Dôkaz.* Zrejme ak $p \mid a$, tak aj $p \mid b$. Stačí nám teda ukázať, že pre $p \nmid a$ platí $(-1)Rp$. Máme

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

Pretože $p \nmid a$, existuje $c$ také, že $ac \equiv 1 \pmod{p}$ (za $c$ môžeme zobrať inverzný prvok k $a$ mod $p$ v $\mathbb{Z}_p$). Ak túto kongruenciu vynásobíme číslom $c$, dostaneme

$$1 + (cb)^2 \equiv 0 \pmod{p},$$
$$(cb)^2 \equiv -1 \pmod{p},$$

teda $-1$ je skutočne kvadratický zvyšok modulo $p$. □

{sumsq:VTPRVSQ}

**Veta 7.2.6 (Fermat).** *Nech $p$ je nepárne prvočíslo. Nasledujúce podmienky sú ekvivalentné*

{sumsq:it1}

(i) *Prvočíslo $p$ je súčtom dvoch druhých mocnín nezáporných celých čísel.*

{sumsq:it2}

(ii) $(-1)Rp$

(iii) *Prvočíslo $p$ je tvaru $4k + 1$.*

*Navyše, rozklad prvočísla $p$ tvaru $4k + 1$ na súčet druhých mocnín je určený jednoznačne (až na poradie sčítancov).*

*Dôkaz.* Ekvivalenciu druhej a tretej podmienky sme už dokázali v tvrdení 4.2.6.

Implikácia (i) $\Rightarrow$ (ii) vyplýva z lemy 7.2.5 (alebo – ešte jednoduchšie – stačí si všimnúť, že číslo tvaru $4k + 3$ nemôžeme dostať ako súčet 2 štvorcov).

Ak vieme, že $x^2 \equiv -1 \pmod{p}$ pre nejaké celé číslo $x$, znamená to, že $p \mid x^2 + 1$ v $\mathbb{Z}$. Potom aj $p \mid x^2 + 1 = (x + i)(x - i)$ v $\mathbb{Z}$. Pretože násobky čísla $p$ v $\mathbb{Z}[i]$ sú práve čísla tvaru $ap + bpi$, máme $p \nmid x \pm i$. Podľa dôsledku 6.5.11 to znamená, že $p$ nie je ireducibilný prvok v $\mathbb{Z}[i]$, čiže $p = z_1.z_2$ pre nejaké prvky $z_1, z_2 \in \mathbb{Z}[i]$, z ktorých ani jeden nie je deliteľ jednotky.

Potom dostaneme $N(p) = p^2 = N(z_1).N(z_2)$. Teraz už ide o súčin prirodzených čísel, a keďže $p$ je prvočíslo a $z_1, z_2$ nie sú delitele jednotky, je to možné iba ak $p = N(z_1) = N(z_2)$. Teda $p = a_1^2 + b_1^2$, kde $a_1$, $b_1$ sú nenulové celé čísla také, že $z_1 = a_1 + ib_1$. Potom platí aj $p = |a_1|^2 + |b_1|^2$, čiže $p$ vieme dostať ako súčet druhých mocnín 2 prirodzených čísel.

Pretože $N(z_1) = N(z_2) = p$, čísla $z_1$, $z_2$ sú ireducibilné v $\mathbb{Z}[i]$ (cvičenie 4 v časti 6.5). Z jednoznačnosti rozkladu v $\mathbb{Z}[i]$ vyplýva, že $z_1$ a $z_2$ sú určené jednoznačne až na asociovanosť.

Ak máme rozklad $p = a^2 + b^2 = (a + bi)(a - bi)$, tak všetky ostatné rozklady dostaneme prenásobením činiteľov v rozklade vhodnými deliteľmi jednotky. Vieme, že delitele jednotky v $\mathbb{Z}[i]$ sú práve čísla $\pm 1$, $\pm i$. Takto dostaneme napríklad z prvého činiteľa $a + bi$ postupne $-a - bi$, $-b + ai$, $b - ai$, z $a + bi$ dostaneme $-a + bi$, $b + ai$, $-b - ai$. Vidíme, že všetky tieto možnosti zodpovedajú iba zmene znamienka čísel $a$, $b$ (čo je nepodstatné, keď sa obmedzíme na nezáporné čísla) a ich vzájomnej výmene.

Čiže rozklad prvočísla na súčet 2 štvorcov nezáporných čísel je skutočne, až na poradie sčítancov, jednoznačný. □

{sumsq:DOS2SQ}

**Dôsledok 7.2.7.** *Prirodzené číslo $n > 1$ je súčet štvorcov dvoch prirodzených čísel práve vtedy, keď $n$ nemá vo svojom prvočíselnom rozklade žiadne prvočíslo tvaru $p = 4k + 3$ v nepárnom exponente.*

*Dôkaz.* Každé takéto číslo sa dá zapísať ako súčet dvoch štvorcov – vyplýva to z vety 7.2.6 a z multiplikatívnosti takýchto čísel (dôsledok 7.2.3).

Ak $p$ je prvočíslo také, že $p \mid n = a^2 + b^2$ tak podľa lemy 7.2.5 je buď $(-1)Rp$ (a teda $p$ je tvaru $4k + 1$), alebo $p \mid a$, $p \mid b$ a v tomto druhom prípade máme $p^2 \mid a^2$, $p^2 \mid b^2$, z čoho dostaneme $p^2 \mid n = a^2 + b^2$. Zopakovaním rovnakej úvahy pre $\frac{n}{p^2}$ dostaneme, že $p$ sa vyskytuje v rozklad $n$ s párnym exponentom. □

Pripomeňme, že ireducibilné prvky v $\mathbb{Z}[i]$ sa zvyknú volať *gaussovské prvočísla.*

**Veta 7.2.8.** *Prvok $x \in \mathbb{Z}[i]$ je ireducibilný práve vtedy, keď nastane niektorý z nasledujúcich prípadov*

(i) $N(x) = 2$ (*dostávame Gaussovské prvočísla* $1 \pm i$, $-1 \pm i$);

(ii) $N(x) = p$, *kde* $p \in \mathbb{P}$ *a* $p \equiv 1 \pmod 4$;

(iii) $x \sim q$ *pre nejaké prvočíslo* $q \in \mathbb{P}$ *také, že* $q \equiv 3 \pmod 4$.

*Dôkaz.* Ľahko vieme zdôvodniť, že uvedené prvky sú skutočne ireducibilné. V prvých dvoch prípadoch to vyplýva z toho, že majú prvočíselnú normu.

V treťom prípade zopakujeme úvahu, ktorú sme už raz použili. Ak $q = z_1 z_2$, tak $N(q) = q^2 = N(z_1)N(z_2)$. Pretože $q$ je prvočíslo, buď sú obe prirodzené prvočísla $N(z_1)$, $N(z_2)$ rovné $q$, alebo jedno z nich je 1. Ak by bolo $N(z_1) = N(z_2) = q$, tak, tak $q = N(z_1) = a_1^2 + b_1^2$ je súčet 2 štvorcov, čo je spor. V druhom prípade je jeden z činiteľov deliteľ jednotky, preto ide o triviálny rozklad.

Obrátene, predpokladajme, že $x = a + bi$ je ireducibilný v $\mathbb{Z}[i]$. Uvažujme ľubovoľné prvočíslo $r$ také, že $r \mid N(x) = a^2 + b^2$. Ak $r = 2$, tak čísla $a$ a $b$ majú rovnaký zvyšok po delení 2. Ak by boli obe párne, tak $2 = (1 + i)(1 - i) \mid a + bi$, čiže sme našli 2 netriviálnych deliteľov čísla $x$, čo je spor s tým, že $x$ je ireducibilný. Zostáva teda možnosť, že sú obe nepárne. Potom $x - (1 + i) = (a - 1) + (b - 1)i$ je násobkom čísla $2 = (1 + i)(1 - i)$, čiže $1 + i \mid x - (1 + i)$. Potom samozrejme aj $1 + i \mid x$ a z ireducibility $x$ dostaneme $x \sim 1 + i$.

Ak $r \equiv 3 \pmod 4$, tak podľa lemy 7.2.5 $r$ delí $a$ aj $b$, čiže $r \mid a + bi$. To znamená, že $r \sim x$ (opäť z ireducibility).

Ako posledná možnosť nám zostal prípad $r \equiv 1 \pmod 4$. Vtedy existujú $a, b \in \mathbb{Z}$ také, že $r = a^2 + b^2 = (a + bi)(a - bi)$, a keďže čísla $a \pm bi$ majú prvočíselnú normu, musia byť ireducibilné v $\mathbb{Z}[i]$. Pretože $(a + bi)(a - bi) \mid N(x) = x\overline{x}$, niektoré z týchto 2 čísel delí $x$, a teda $x = a \pm bi$, $N(x) = p$. □



{sumsq:VTPOCET2SQ}

**Veta 7.2.9.** *Ak číslo $n$ má kanonický rozklad $n = 2^e p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_l^{f_l}$, kde $p_i$ sú prvočísla tvaru $4k + 1$ a $q_j$ sú prvočísla tvaru $4k + 3$, pričom všetky $f_j$ sú párne, tak počet rozkladov čísla $n$ na súčet 2 druhých mocnín celých čísel je*

$$r_2(n) = 4 \prod_{i=1}^{k} (e_i + 1) \tag{7.2}$$

{sussq:EQR2A}

*Dôkaz.* Ak $n = a^2 + b^2$ pre nejaké $a, b \in \mathbb{Z}$, tak máme rozklad v $\mathbb{Z}[i]$ $n = (a + bi)(a - bi)$. Obrátene, každý rozklad $n$ na súčin dvoch komplexne združených prvkov okruhu $\mathbb{Z}[i]$ nám dáva rozklad $n$ ako súčtu 2 štvorcov celých čísel. Máme teda vlastne zistiť počet možných zápisov čísla $n$ ako $z\overline{z}$ pre $z \in \mathbb{Z}[i]$.

V $\mathbb{Z}[i]$ máme rozklad na súčin (deliteľa jednotky) a ireducibilných prvkov

$$n = (1 + i)^e (1 - i)^e \pi_1^{e_1} \dots \pi_k^{e_k} \overline{\pi}_1^{e_1} \dots \overline{\pi}_k^{e_k} q_1^{f_1} \dots q_l^{f_l} = i(1 - i)^{2e} \pi_1^{e_1} \dots \pi_k^{e_k} \overline{\pi}_1^{e_1} \dots \overline{\pi}_k^{e_k} q_1^{f_1} \dots q_l^{f_l},$$

kde $\pi\overline{\pi} = p$ (tieto prvky sú ireducibilné v $\mathbb{Z}[i]$ a sú – až na výmenu – jednoznačne určené).

Pretože $z$ je deliteľ $n$ v $\mathbb{Z}[i]$, musí preň platiť:

$$z = u(1 - i)^a \pi_1^{a_1} \dots \pi_k^{a_k} \overline{\pi}_1^{b_1} \dots \overline{\pi}_k^{b_k} q_1^{c_1} \dots q_l^{c_l},$$

pričom $u \in U(\mathbb{Z}[i])$ a $0 \le a \le 2e$, $0 \le a_i, b_i \le e_i$, $0 \le c_i \le f_i$.

Potom komplexne združené číslo vyzerá takto

$$\overline{z} = \overline{u}(1 + i)^a \overline{\pi}_1^{a_1} \dots \overline{\pi}_k^{a_k} \pi_1^{b_1} \dots \pi_k^{b_k} q_1^{c_1} \dots q_l^{c_l}.$$

Z toho vidíme, že $z\overline{z} = n$ bude platiť, ak

$$\begin{aligned} a &= e, \\ a_i + b_i &= e_i, \\ 2c_j &= f_j. \end{aligned}$$

Čísla $a$ a $c_j$ sú teda jednoznačne určené, voľnosť máme iba vo voľbe deliteľa jednotky $u$ (4 možnosti) a vo číslo $a_i$ môžeme zvoliť ľubovoľne spomedzi čísel $\{0, 1, \dots, e_i\}$ (tým je číslo $b_i$ jednoznačne určené).

Celkove máme teda skutočne

$$4 \prod_{i=1}^{k} (e_i + 1)$$

možností. □

**Príklad 7.2.10.** Uvažujme $n = 50 = 2.5^2$. Podľa predchádzajúcej vety by malo existovať 12 možných zápisov čísla 50 v tvare súčtu 2 štvorcov celých čísel. (A dôkaz vety nám súčasne poskytuje návod ako ich hľadať, pomocou rozkladu v $\mathbb{Z}[i]$.)

Skutočne máme:
$50 = 5^2 + 5^2$ (spolu s možnými zmenami znamienok dostaneme 4 možnosti; výmena sčítancov tu žiadne možnosti nepridá);
$50 = 7^2 + 1^2$ (všetky zmeny znamienok a výmeny sčítancov nám dajú spolu 8 možností);
čiže spolu máme naozaj 12 možností.

### 7.2.2 Súčty štyroch štvorcov

Teraz dokážeme Lagrangeovu vetu, ktorá hovorí, že každé prirodzené číslo je súčtom 4 štvorcov celých čísel. Dôkaz použije identitu podobnú Fibonacciho identite (ale pre 4 štvorce) a metódu nekonečnej regresie.

Začnime teda najprv s dôkazom identity (7.3), ktorá ukazuje, že čísla vyjadriteľné ako súčet 4 štvorcov sú uzavreté na súčin. {sumsq:LMKVATER}

**Lema 7.2.11 (Eulerova identita).** *Pre ľubovoľné $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{R}$ platí*

$$(a_1^2+a_2^2+a_3^2+a_4^2).(b_1^2+b_2^2+b_3^2+b_4^2) = (a_1b_1-a_2b_2-a_3b_3-a_4b_4)^2+$$
$$(a_1b_2+a_2b_1+a_3b_4-a_4b_3)^2+(a_1b_3-a_2b_4+a_3b_1+a_4b_2)^2+(a_1b_4+a_2b_3-a_3b_2+a_4b_1)^2. \tag{7.3}$$ {sumsq:EQKVATER}

*Dôkaz. Roznásobením.* (Pracné, ale prejde to v ľubovoľnom okruhu.) □

*Kvaternióny.* Využijeme to, že norma (absolútna hodnota) kvaterniónov[1]

$$|a+bi+cj+dk| = \sqrt{a^2+b^2+c^2+d^2}$$

je multiplikatívna. (Stačí si všimnúť, že $|x| = \sqrt{x\overline{x}}$ a z toho, že $ab = \overline{ba}$ platí pre ľubovoľné kvaternióny dostaneme $xy\overline{xy} = xy\overline{y}\overline{x} = x\overline{x}y\overline{y}$. V poslednej rovnosti sme využili to, že kvaternióny komutujú s reálnymi číslami, čo vyplýva priamo z pravidiel pre počítanie s kvaterniónmi alebo tiež zo spomenutej rovnosti $ab = \overline{ba}$; vďaka tomu sme mohli vymeniť $\overline{x}$ s reálnym číslom $y\overline{y}$.)

Ak označíme $x = a_1 + a_2i + a_3j + a_4k$, $y = b_1 + b_2i + b_2j + b_3k$, tak máme

$$xy = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4) + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i$$
$$(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k$$

a rovnosť (7.3) dostaneme prepísaním rovnosti $|xy|^2 = |x|^2|y|^2$. □

*Determinanty.* Uvažujme matice tvaru

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

kde $\alpha$, $\beta$ môžu byť ľubovoľné komplexné čísla. Všimnime si dve veci – súčin matíc takéhoto tvaru je opäť matica uvedeného tvaru

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}\begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma-\beta\overline{\delta} & \alpha\delta+\beta\overline{\gamma} \\ -\overline{\beta}\gamma-\overline{\alpha}\overline{\delta} & \overline{\beta}\overline{\delta}+\overline{\alpha}\overline{\gamma} \end{pmatrix} \tag{7.4}$$ {sumsq:EQSUCINMAT}

Ďalšia vlastnosť, ktorá sa nám hodí, je to, aký tvar má determinant takejto matice

$$\begin{pmatrix} a+bi & c+di \\ di-c & a-bi \end{pmatrix} = a^2+b^2+c^2+d^2.$$

Teraz nám už stačí zvoliť $\alpha = a_1 + a_2i$, $\beta = \alpha = a_3 + a_4i$, $\gamma = b_1 + b_2i$, $\delta = \alpha = b_3 + b_4i$ a rovnosť (7.4) spolu s multiplikatívnosťou determinantu ($|AB| = |A||B|$) nám dajú rovnosť (7.3). □

[1] Pozri napríklad [KGGS, Kapitola 4.7]



Druhý a tretí dôkaz je v podstate ten istý dôkaz – ide o to, že zobrazenie

$$a+bi+cj+dk \mapsto \begin{pmatrix} a+bi & c+di \\ di-c & a-bi \end{pmatrix}$$

je izomorfizmus medzi telesom kvaterniónov a maticami takéhoto tvaru. (Inak povedané, tento maticový okruh je maticovou reprezentáciou kvaterniónov.) {sumsq:LM14SQ}

**Lema 7.2.12.** *Pre každé prvočíslo $p$ má kongruencia*

$$x^2+y^2+1 \equiv 0 \pmod{p} \tag{7.5}$$ {sumsq:EQ4SQKON}

*riešenie.*

*Dôkaz.* Uvažujme množinu $S = \{x^2 \bmod p; x \in \mathbb{Z}\}$. Množina $S$ má $\frac{p+1}{2}$ prvkov. (Nenulové čísla z tejto množiny sú kvadratické zvyšky modulo $p$ – pozri tiež vetu 4.1.4.)

Zoberme ďalej množinu $S' = \{(-1-x^2) \bmod p; x \in \mathbb{Z}\}$. Táto množina má takisto $\frac{p+1}{2}$ prvkov. Pritom $S \cup S' \subseteq \{0, 1, \ldots, p-1\}$, preto z Dirichletovho princípu vyplýva, že existuje aspoň jeden prvok, ktorý patrí do $S$ aj $S'$. Teda máme $x, y \in \mathbb{Z}$ také, že $x^2 \bmod p = (-1-x^2) \bmod p$, čo znamená

$$x^2+y^2+1 \equiv 0 \pmod{p}.$$

□ {sumsq:LM24SQ}

**Lema 7.2.13.** *Ak $p$ je prvočíslo, $1 < m < p$ a*

$$mp = x_1^2+x_2^2+x_3^2+x_4^2$$

*pre nejaké celé čísla $x_1 \ldots x_4$, tak existuje $r$ také, že $0 < r < m$ a*

$$rp = z_1^2+z_2^2+z_3^2+{z_4}^2$$

*pre nejaké celé čísla $z_1 \ldots z_4$.*

*Dôkaz.* Ak platí rovnosť $mp = x_1^2+x_2^2+x_3^2+x_4^2$, tak platí aj

$$x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod{m}.$$

Zvoľme teraz pre $i = 1, 2, 3, 4$ čísla $y_i$ tak, že $x_i \equiv y_i \pmod{m}$ a súčasne $-\frac{m}{2} < y_i \leq \frac{m}{2}$ (najmenšie zvyšky modulo $m$). Potom platí $y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 \pmod{m}$, teda

$$y_1^2+y_2^2+y_3^2+y_4^2 = rm$$

pre nejaké $r \in \mathbb{Z}$.

Z toho, ako sme zvolili $y_i$ vieme, že

$$rm = y_1^2+y_2^2+y_3^2+y_4^2 \leq 4\left(\frac{m}{2}\right)^2 = m^2, \tag{7.6}$$ {sumsq:INEQLM2}

preto $r \leq m$. Je zrejmé, že $r \geq 0$ (súčet štvorcov je nezáporný.)

Ak by platilo $r = 0$, tak $y_1 = y_2 = y_3 = y_4 = 0$, čo ale znamená, že $m$ delí každé z čísel $x_i$, čiže $m^2 \mid x_i^2$, a teda

$$m^2 \mid mp.$$

Z toho vyplýva $m \mid p$, čo je v spore s predpokladmi lemy.

Ak by platilo $r = m$, tak v (7.6) nastane rovnosť. Potom ale

$$pm = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv y_1^2 + y_2^2 + y_3^2 + y_4^2 = m^2 \equiv 0 \pmod{m^2},$$

čiže $m^2 \mid pm$, z čoho opäť dostaneme $m \mid p$, čiže spor.

Zistili sme teda, že $0 < r < m$. Ďalej vieme $rm$ aj $mp$ vyjadriť ako súčet 4 štvorcov, teda použitím (7.3) pre $a_i = x_i$, $b_1 = y_1$, $b_i = -y_i$ pre $i = 2, 3, 4$, máme

$$m^2 rp = (x_1^2 + x_2^2 + x_3^2 + x_4^2).(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 +$$
$$(-x_1y_2 + x_2y_1 - x_3y_4 + x_4y_3)^2 + (-x_1y_3 + x_2y_4 + x_3y_1 - x_4y_2)^2 + (-x_1y_4 - x_2y_3 + x_3y_2 + x_4y_1)^2.$$

Ďalej z toho, že $x_i \equiv y_i \pmod{m}$ vidíme, že každá zo zátvoriek na pravej strane je deliteľná $m$. Po vydelení celej rovnice číslom $m^2$ dostaneme

$$rp = z_1^2 + z_2^2 + z_3^2 + {z_4}^2,$$

kde čísla $z_i$, $i = 1, \ldots, 4$, sú celé. □

{sumsq:VTLAGR}

**Veta 7.2.14 (Lagrange).** *Každé prirodzené číslo je súčtom 4 štvorcov celých čísel.*

*Dôkaz.* Na základe Eulerovej identity je zrejmé, že stačí tvrdenie dokázať pre prvočísla.

Ak máme ľubovoľné prvočíslo $p$ tak podľa lemy 7.2.12 existuje $m \in \mathbb{N}$ také, že $mp = x_1^2 + x_2^2 + 1^2 + 0^2$. Podľa lemy 7.2.13 vieme toto číslo $m$ postupne znižovať, tak aby po znížení bol príslušný násobok čísla $p$ opäť súčtom 4 štvorcov. Po konečnom počte krokov ho takto znížime na jednotku. □

Vzhľadom k tomu, že pri otázke vyjadrenia čísla ako súčtu 2 štvorcov sme využili fakt, že okruh $\mathbb{Z}[i]$ je okruh s jednoznačným rozkladom, je na mieste sa spýtať, či by sa nedalo niečo podobné urobiť pre okruh kvaterniónov s celočíselnými súradnicami. Tento okruh však nie je komutatívny, preto budovanie teórie deliteľnosti v tomto okruhu naráža na viaceré problémy. Ak by Vás zaujímal tento prístup a chceli by ste sa o ňom dozvedieť viac, nájdete ho v [HW, Chapter XX] alebo tiež v [DSV, Section 2.6].

### 7.2.3 Súčet troch štvorcov

**Veta 7.2.15 (Gauss).** *Prirodzené číslo $n > 1$ je vyjadriteľné ako súčet troch druhých mocnín prirodzených čísel práve vtedy, keď $n$ nemá tvar $4^l(8k + 7)$.*

Dôkaz toho, že čísla tvaru $4^l(8k + 7)$ sa nedajú napísať ako súčet 3 štvorcov môžete nájsť napríklad v [Š3]. Dôkaz opačnej implikácie je podstatne náročnejší.

#### Cvičenia

1. Dokážte, že existuje nekonečne veľa celých čísel $n$ takých, že $n$, $n + 1$ aj $n + 2$ sú súčty dvoch druhých mocnín celých čísel. (Úloha z Putnamovej súťaže.[2])

2. Ukážte, že počet rozkladov čísla $n \in \mathbb{N}$ na súčet dvoch druhých mocnín celých čísel (pozri (7.2)) sa dá vyjadriť ako $4(d_1(n) - d_3(n))$, kde $d_i(n)$ znamená počet deliteľov čísla $n$, ktoré sú tvaru $4k + 1$.

[2] Putnamova súťaž je Americká matematická vysokoškolská súťaž.



## 7.3 Goldbachova hypotéza, aditívne vlastnosti prvočísel

*Goldbachova hypotéza:* Každé prirodzené číslo $n \geq 3$ je súčtom najviac 3 prvočísel.

**Veta 7.3.1 (Richert).** *Nech $m_1 < m_2 < \ldots < m_n < \ldots$ je postupnosť prirodzených čísel. Nech existuje $k \in \mathbb{N}$ také, že pre $j > k$ platí $m_{j+1} \leq 2m_j$. Ďalej predpokladajme, že existujú také $a, s_0 \in \mathbb{N}$ , že $s_0 \geq m_{k+1}$ a každé z čísel*

$$a + 1, a + 2, \ldots, a + s_0$$

*je súčtom navzájom rôznych čísel z množiny $\{m_1, \ldots, m_k\}$.*

*Potom každé prirodzené číslo väčšie ako $a$ je súčtom navzájom rôznych čísel z postupnosti $(m_n)$.*

# Dodatok A

# Euklidov algoritmus

{APEUK}

Euklidov algoritmus je algoritmus na určenie nsd prirodzených čísel $a$ a $b$.

Bez ujmy na všeobecnosti, nech $a > b$. Podľa vety o delení so zvyškom $a = kb + b_1$ pre nejaké $k \in \mathbb{N}$ a nejaký zvyšok $0 \leq b_1 < b$. Podľa lemy 2.1.11(i) potom platí $(a, b) = (b, b_1)$. Preto použitím tohto vzťahu môžeme rekurzívne vypočítať $(a, b)$.

Nech $a > b$ sú prirodzené čísla. Euklidovým algoritmom vyrátame ich nsd takto:

1. Položme $a_0 := a$ a $b_0 := b$.
2. V každom kroku algoritmu: vypočítajme $c$ také, že $a_n = k.b_n + c$.
3. Ak $c = 0$, tak výsledkom je číslo $b_n$.
4. V opačnom prípade položme $a_{n+1} := b_n$ a $b_{n+1} := c$.

Všimnime si, že podľa lemy 2.1.11(i) platí $(a_{n+1}, b_{n+1}) = (a_n, b_n)$, preto v každom kroku platí $(a_n, b_n) = (a, b)$. Ak $c = 0$, tak $b_n \mid a_n$, a teda $(a_n, b_n) = b_n$. To znamená, že týmto algoritmom skutočne nájdeme nsd čísel $a$ a $b$.

Pretože $a_{n+1} < a_n$, číslo $a_n$ v priebehu výpočtu klesá a tento algoritmus sa musí zastaviť.

Euklidovým algoritmom vieme nájsť aj čísla $u$ a $v$ z Bézoutovej identity.

Nech $a > b$ sú prirodzené čísla. Euklidovým algoritmom vyrátame ich nsd takto:

1. Položme $a_0 := a$, $b_0 := b$, $u_0 = 0$ a $v_0 = 1$.
2. V každom kroku algoritmu: vypočítajme $c$ také, že $a_n = k.b_n + c$.
3. Ak $c = 0$, tak $b_n$.
4. V opačnom prípade položme $a_{n+1} := b_n$ a $b_{n+1} := c$.
5. Ak $n = 1$, tak $u_1 := 1$ a $v_1 := -k$.
6. Ak $n > 1$, tak $u_{n+1} := u_{n-1} - ku_n$, $v_{n+1} := v_{n-1} - kv_n$.

Čísla $u_n$ a $v_n$ volíme tak, aby v každom kroku platilo $b_n = u_n a_0 + v_n b_0$. Skutočne, ak to platí v $n$-tom kroku, tak v $(n + 1)$-vom kroku skutočne máme $b_{n+1} = c = a_n - kb_n = b_{n-1} - kb_n = (u_{n-1}a + v_{n-1}b) - k(u_n a + v_n b) = (u_{n-1} - ku_n)a + (v_{n-1} - kv_n)b$.

Uvedený postup je ilustrovaný v nasledujúcom príklade.



**Príklad A.0.2.** Vyrátajte $d = (145, 19)$ a nájdite $u, v \in \mathbb{Z}$ také, že $145u + 19v = d$.

$$\begin{aligned} 145 &= 7.19 + 12 & 12 &= 145 - 7.19 \\ 19 &= 1.12 + 7 & 7 &= 19 - 12 = 8.19 - 145 \\ 12 &= 1.7 + 5 & 5 &= 12 - 7 = 2.145 - 15.19 \\ 7 &= 1.5 + 2 & 2 &= 7 - 5 = 23.19 - 3.145 \\ 5 &= 2.2 + 1 & 1 &= 5 - 2.2 = 8.145 - 61.19 \end{aligned}$$

Zistili sme, že $(145, 19) = 1 = 8.145 - 61.19$.

Obor integrity $(R, +, \cdot)$ sa nazýva *euklidovským okruhom,* ak existuje funkcia $v \colon R \setminus \{0\} \to \mathbb{N}$ a pre ľubovoľné $a, b \in R$ existujú $q, r \in R$ také, že

$$a = b.q + r \qquad \text{a} \qquad r = 0 \vee v(r) < v(b).$$

Táto definícia presne zachytáva podmienky potrebné na to, aby mohol fungovať Euklidov algoritmus. Napríklad okruhy polynómov sú euklidovské, v tomto prípade je funkcia $v$ stupeň polynómu.

Euklidov algoritmus môžeme využiť na hľadanie inverzného prvku v multiplikatívnej grupe $\mathbb{Z}_p \setminus \{0\}$. Ak totiž $(a, p) = 1$, vieme Euklidovým algoritmom nájsť $u, v \in \mathbb{N}$ také, že $ua + vp = 1$, čiže

$$ua \equiv 1 \pmod{p}.$$

To znamená, že $u \mod p$ je inverzný prvok k $a$ v $\mathbb{Z}_p \setminus \{0\}$.

**Príklad A.0.3.** Vypočítajte $10^{-1}$ v $\mathbb{Z}_{23}$.

Použijeme Euklidov algoritmus.

$$\begin{aligned} 23 &= 2.10 + 3 & 3 &= 23 - 2.10 \\ 10 &= 3.3 + 1 & 1 &= 10 - 3.3 = 7.10 - 3.23 \end{aligned}$$

Posledná rovnosť znamená, že $7.10 \equiv 1 \pmod{23}$, čiže v $\mathbb{Z}_{23}$ platí $10^{-1} = 7$.

Základnú myšlienku Euklidovho algoritmu môžeme použiť aj v úlohách nasledujúceho typu.

**Príklad A.0.4.** Zistite, čomu sa rovná $(n^3 + 2, n + 1)$ pre $n \in \mathbb{N}$.

Pomocou delenia so zvyškom dostaneme: $(n^3+2) = (n^2-n+1)(n+1)+1$ a $(n^3+2, n+1) = (n + 1, 1) = 1$.

Ďalší príklad tohoto typu je príklad 2.1.12.

# Dodatok B

# Rady

## B.1 Harmonický rad {APRADY}

*Harmonický rad* je rad

$$\sum_{k=1}^{\infty} \frac{1}{k}. \tag{B.1}$$ {rady:EQHAR}

Ľahko si všimneme, že tento rad diverguje – stačí si všimnúť, že rad (B.1) môžeme rozdeliť na časti, ktorých súčet je vždy aspoň $\frac{1}{2}$

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \left[\frac{1}{2}\right] + \left[\frac{1}{3} + \frac{1}{4}\right] + \left[\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right] + \dots$$

Divergenciu radu môžeme overiť aj pomocou integrálneho kritéria. Stačí si všimnúť, že pre ľubovoľné $n \in \mathbb{N}$ a $x \in \langle n, n+1\rangle$ platí

$$\frac{1}{n+1} \le \frac{1}{x} \le \frac{1}{n},$$

z čoho máme (sčítaním od 1 po $n-1$)

$$\sum_{k=2}^{n} \frac{1}{k} = \sum_{k=1}^{n} \frac{1}{k} - 1 \le \int_1^n \frac{1}{x} dx = \ln n \le \sum_{k=1}^{n} \frac{1}{k},$$

$$\ln n \le \sum_{k=1}^{n} \frac{1}{k} \le \ln n + 1.$$

(Pozri obrázok B.1.)

Vidíme teda, že rad (B.1) diverguje relatívne pomaly – zhruba ako funkcia $\ln x$. Posledný odhad možno vylepšiť v tom zmysle, že dokonca existuje limita

$$\lim_{n\to\infty} \left( \sum_{k=1}^{n} \frac{1}{k} - \ln n \right) = \gamma. \tag{B.2}$$ {rady:EQGAMMA}

Táto limita sa nazýva *Eulerova konštanta* (niekedy aj Eulerova-Mascheroniho konštanta).

Jej hodnota je približne $0,577$. Dodnes nie je známe, či Eulerova konštanta $\gamma$ je racionálne alebo iracionálne číslo.

My dokážeme o niečo silnejšie tvrdenie, než je rovnosť (B.2) (tzv. Maclaurin-Cauchyho veta).

Obr. B.1: Harmonický rad a funkcia $\frac{1}{x}$ {rady:FIGHAR}

{rady:VTMACLAURIN}

**Veta B.1.1 (Maclaurin-Cauchy).** *Ak $f(x)$ je kladná reálna funkcia klesajúca k 0, tak existuje limita*

$$\gamma_f := \lim_{n\to\infty} \left[ \sum_{k=1}^{n} f(k) - \int_1^{n+1} f(x)dx \right].$$

*Dôkaz.* Odhadneme rozdiel medzi plochou pod grafom funkcie $f$ (ktorá zodpovedá integrálu) a pod grafom schodovitej funkcie zodpovedajúcej sume. Označme

$$a_n = \sum_{k=1}^{n} f(k) - \int_1^{n+1} f(x)dx.$$

Vidíme, že $0 \le a_n - a_{n-1} = f(n) - \int_n^{n+1} f(x)dx \le f(n) - \int_n^{n+1} f(n+1)dx = f(n) - f(n+1)$.

Postupnosť $a_n$ je je postupnosť čiastočných súčtov radu s kladnými členmi $f(n) - \int_n^{n+1} f(x)dx$.

Preto $a_n$ je kladná rastúca postupnosť. Navyše je ohraničená, pretože $a_n \le f(1) - f(2) + f(2) - f(3) + \dots - f(n) = f(1) - f(n+1) \le f(1)$. Každá rastúca ohraničená postupnosť má limitu. □

## B.2 Rad prevrátených hodnôt druhých mocnín

V tejto časti budeme uvažovať o rade

$$\sum_{k=1}^{\infty} \frac{1}{k^2}. \tag{B.3}$$ {rady:EQSQR}

Z integrálneho kritéria okamžite vidíme, že tento rad konverguje ($\int_1^{\infty} \frac{1}{x^2}dx = 1$). To nám pre mnohé úvahy úplne stačí, jeden z veľmi známych matematických výsledkov (pochádzajúci od L. Eulera) nám však hovorí, že

**Veta B.2.1.**

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

Uvedieme si 2 rôzne dôkazy. Prvý z nich využíva poznatky o Fourierových radoch. Pripomeňme, že trigonometrický Fourierov rad funkcie $f(x)$ je

$$f(x) \sim \frac{1}{2}a_0 + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx),$$

kde

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx dx,$$

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin nx dx,$$

pre $n = 1, 2, \ldots$ a

$$a_0 = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x) dx.$$

Pre každú po častiach spojitú funkciu platí Parsevalova rovnosť

$$\frac{a_0^2}{2} + \sum_{n=1}^{\infty}(a_n^2 + b_n^2) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)^2 dx$$

(pozri [ŠŠN, s.304]). (Z fyzikálneho hladiska možno Parsevalovu rovnosť interpretovať tak, že signál a jeho Fourierova transformácia majú rovnakú energiu. Z matematického hľadiska je zasa dôsledkom faktu, že funkcie $\cos nx$ a $\sin nx$ tvoria úplný ortonormálny systém.) Túto rovnosť použijeme v nasledujúcom dôkaze.

*Dôkaz.* Budeme uvažovať periodické predĺženie funkcie $f(x) = x$ z intervalu $(-\pi, \pi\rangle$ na celú reálnu os. Pretože funkcia $f(x)$ je nepárna, všetky koeficienty $a_n$ sú nulové. Pre ostatné koeficienty dostávame

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} x\sin nx = \frac{1}{\pi}\left[-\frac{x\cos nx}{n} + \frac{\sin nx}{n^2}\right]_{-\pi}^{\pi} = 2\frac{(-1)^{n+1}}{n}.$$

Z Parsevalovej rovnosti potom dostávame $4\sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{1}{\pi}\int_{-\pi}^{\pi} x^2 dx = \frac{2\pi^2}{3}$ a jednoduchou úpravou dostaneme dokazovanú rovnosť. □

Ešte uvedieme pôvodný Eulerov dôkaz – aj keď z dnešného hľadiska ho skôr môžeme považovať za heuristický argument ako za dôkaz.

*Eulerov dôkaz.* Vieme, že

$$p(x) = \frac{\sin x}{x} = 1 - \frac{x^2}{6} + \frac{x^4}{120} - \ldots$$

je „polynóm“, ktorý má korene $\pm\pi, \pm 2\pi, \ldots$ Keď ho zapíšeme pomocou rozkladu na koreňové činitele, dostaneme

$$p(x) = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{(2\pi)^2}\right)\ldots\left(1 - \frac{x^2}{n\pi^2}\right)\ldots$$

Ak vyrátame koeficient tohoto „polynómu“ pri $x^2$, dostávame

$$\frac{1}{6} = \frac{1}{\pi^2} + \frac{1}{4\pi^2} + \ldots = \frac{1}{\pi^2}\sum_{k=1}^{\infty}\frac{1}{k^2},$$

z čoho už vyplýva $\sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{\pi^2}{6}$. □

Viacero dôkazov tohoto výsledku môžete nájsť aj v [AZ, Chapter 7].



# Dodatok C

# Zložitosť niektorých teoreticko-číselných algoritmov

{APZLOZ}

V súvislosti s praktickým použitím teórie čísel sa často objavuje otázka časovej zložitosti teoreticko-číselných algoritmov. Je prirodzené sa pýtať, ako rýchlo viem odpovedať na danú otázku. (Zaujímajú nás otázky typu: Je $p$ prvočíslo? Čomu sa rovná $(a, b)$? Aký je prvočíselný rozklad čísla $n$?) S tým samozrejme aj súvisí to, pre aké veľké vstupy viem vôbec na danú otázku pri výpočtovej sile, ktorú mám k dispozícii, nájsť odpoveď. Takisto

Na túto otázku sa zvyčajne odpovedá spôsobom: zložitosť algoritmu je $O(f(n))$. To znamená, že ak $T(n)$ označíme počet operácií, koľko potrebuje algoritmus vykonať (=procesorový čas), tak platí $T(n) \leq C.f(n)$ pre nejakú konštantu $C$ a všetky dostatočne veľké $n$. Dôvod je ten, že nás zaujíma správanie sa algoritmu, keď ako vstup sú veľké čísla. Tým však aj veľkú časť informácie strácame - pretože v skutočnosti nevieme, aká veľká je konštanta $C$, môže sa stať, že algoritmus, ktorý je asymptoticky rýchlejší, bude v skutočnosti bežať pomalšie.

## C.1 Základné operácie

Aby sme mohli hovoriť o zložitosti komplexnejších algoritmov, musíme najprv vedieť, koľko trvajú (pri vhodnej implementácii) základné operácie, ako násobenie, sčitovanie, delenie so zvyškom.

Hoci táto otázka vyzerá pomerne jednoducho, až taká jednoduchá nie je. Na tieto operácie sa podarilo nájsť veľmi efektívne algoritmy (využívajúce rýchlu Fourierovu transformáciu - fast Fourier transformation, FFT). Bez dôkazu si uvedieme, že čísla veľkosti nanajvýš $n$ vieme sčitovať v čase $O(\lg n)$, násobiť v čase $O(\lg^2 n)$ a delenie so zvyškom vieme urobiť v čase $O(\lg n)$. Ak by ste sa chceli dozvedieť viac napríklad v (dalo by sa povedať legendárnej) knihe [Knu] alebo v knihe [Sh], ktorá je voľne dostupná na internete. O FFT sa môžete niečo dozvedieť aj na iných prednáškach na FMFI (ak sa nemýlim, tak prinajmenšom na predmetoch Počítačová algebra a Tvorba efektívnych algoritmov).

## C.2 Euklidov algoritmus

TODO

### C.3 Výpočet Jacobiho symbolu



# Literatúra


[An] George E. Andrews. *Number Theory.* Saunders, Philadelphia, 1971.

[Ap] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag, Berlin, 1976.

[AGP] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. Math.*, 139:703–722, 1994.

[AKS] M. Agarwal, N. Kayal, and N. Saxena. PRIMES is in P. *Ann. Math.*, 160:781–793, 2004.

[AZ] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK.* Springer, Berlin, 2004.

[B] P. Bachmann. *Niedere Zahlentheorie, 1. Teil.* B. G. Teubner, Leipzig, 1902.

[BD] P. T. Bateman and H. G. Diamond. *Analytic number theory. An introductory course.* World Scientific, New Jersey, 2004.

[C] W. W. L. Chen. Elementary number theory. Lecture notes, `http://www.maths.mq.edu.au/~wchen`.

[Č] Juraj Činčura. Elementárna teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/cvicenia/tc/`.

[CP] R. Crandall and C. Pomerance. *Prime Numbers, a Computational Perspective.* Springer-Verlag, New York, 2001.

[DD] T. P. Dence and J. B. Dence. *Elements of the Theory of Numbers.* Academic Press, San Diego, 1999.

[DF] David S. Dummit and Richard M. Foote. *Abstract Algebra.* Prentice Hall, Englewood Cliffs, 2nd edition, 1999.

[DMR] J. B. Dynkin, S. A. Molčanov, and A. L. Rozental. *Matematické hlavolamy.* Alfa, Bratislava, 1979.

[DSV] G. Davidoff, P. Sarnak, and A. Valette. *Elementary number theory, graph theory and Ramanujan graphs.* Cambridge University Press, Cambridge, 2003.

[E] C. Vanden Eynden. Proofs that $\sum 1/p$ diverges. *Amer. Math. Monthly*, 87(5):394–397, 1980.

[ES] Paul Erdös and János Surányi. *Topics in the Theory of Numbers.* Springer, New York, 2003. Undergraduate Texts in Mathematics.

[Fa] H. Fast. Sur la convergence statistique. *Coll. Math.*, 2:241–244, 1951.

[Fr] J. A. Fridy. On statistical convergence. *Analysis*, 5:301–313, 1985.

[Gr] G. Grekos. On various definitions of density (survey). *Tatra Mt. Math. Publ.*, 31:17–27, 2005.

[Gup] H. N. Gupta. A theorem in combinatorics and Wilson's theorem. *Amer. Math. Monthly*, 92(8):575–576, 1985.

[Gur] Jaroslav Guričan. Faktorizácia polynómov II. *Obzory matematiky, fyziky a informatiky.* `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[GKP] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics.* Addison-Wesley, Massachusetts, 1989.

[GT] B. Green and T. Tao. The primes contain arbitrarily long arithmetic progressions, 2004. arXiv:math.NT/0404188.

[H] F. Hennecart. On the regularity of density sets. *Tatra Mt. Math. Publ.*, 31:113–121, 2005.

[HGK] Michiel Hazewinkel, Nadiya Gubareni, and V.V. Kirichenko. *Algebras, Rings and Modules, Volume 1.* Kluwer, New York, 2004.

[HS] T. Hecht and Z. Sklenáriková. *Metódy riešenia matematických úloh.* SPN, Bratislava, 1992.

[HW] G. H. Hardy and E. M. Wright. *Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 1971.

[IR] K. Ireland and M. Rosen. *A Classical Introduction to Modern Set Theory.* Springer, New York, 1990.

[JJ] Gareth A. Jones and J. Mary Jones. *Elementary Number Theory.* Springer-Verlag, London, 1998. Springer Undergraduate Mathematics Series.

[Kl] M. Klazar. Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti. *Pokroky matematiky, fyziky a astronomie*, 49(3):177–188, 2004.

[Kno] Konrad Knopp. *Theorie und Anwendung der unendlichen Reihen.* Verlag von Julius Springer, Berlin, 1922.

[Knu] D. E. Knuth. *The Art of Computer Programming, volume 2: Seminumerical algorithms.* Addison-Wesley, Massachusetts, 1998.

[Kor] Július Korbaš. *Lineárna algebra a geometria I.* UK, Bratislava, 2003.

[Kos] Thomas Koshy. *Elementary number theory with applications.* Hartcourt Academic Press, San Diego.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[KLS] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers. From number theory to geometry.* Springer, New York, 2001.



[KLŠZ] M. Kolibiar, A. Legéň, T. Šalát, and Š. Znám. *Algebra a príbuzné disciplíny.* Alfa, Bratislava, 1992.

[KN] W. J. Kaczor and M. T. Nowak. *Problems in Mathematical Analysis I. Real numbers, sequences and series.* American Mathematical Society, Providence, 2000.

[KPW] Kiran S. Kedlaya, Bjorn Poonen, and Ravi Wakil. *The William Lowell Putnam Mathematical Competition 1985-2000: Problems, Solutions and Comentary.* The Mathematical Association of America, Washington, 2002. MAA Problem book series.

[KS] M. Křížek and L. Somer. Preudoprvočísla. *Pokroky matematiky, fyziky a astronómie*, 48(2):143–151, 2003.

[Lem1] F. Lemmermeyer. *Numbers and curves.* Springer, Berlin.

[Lem2] F. Lemmermeyer. *Reciprocity laws. From Euler to Eisenstein.* Springer, Berlin, 2000.

[Lev1] William J. Leveque. *Topics in number theory.* Dover, Mineola, 2002.

[Lev2] M. Levinson. A motivated account of an elementary proof of the prime number theorem. *Amer. Math. Monthly*, 76(3):225–245, 1969.

[Lo] C. T. Long. *Elementary introduction to number theory.* Prentice-Hall, Englewood Cliffs, 1987.

[Ma] S. E. Mamangakis. Shorter notes: Remark on $\pi(x) = o(x)$. *Proc. Amer. Math. Soc.*, 13(4):664–665, 1962.

[Mi] L. Mišík. Sets of positive integers with prescribed values of densities. *Math. Slov.*, 52(3):289–296, 2002.

[Mo] L. Moser. On the series $\sum 1/p$. *Amer. Math. Monthly*, 65(2):104–105, 1958.

[ME] M. R. Murty and J. Esmonde. *Problems in Algebraic Number Theory.* Springer, Berlin, 2005.

[MSC] D. S. Mitrinović, J. Sandor, and B. Crstici. *Handbook of Number Theory.* Kluwer Academic Publisher, Dordrecht, 1996.

[Nai] M. Nair. On Chebyshev-type inequalities for primes. *Amer. Math. Monthly*, 89:126–129, 1982.

[Nat] Melvyn Bernard Nathanson. *Elementary methods in number theory.* Springer, New York, 2000. Graduate Texts in Mathematics 195.

[Ne] D. J. Newman. Simple analytic proof of the prime number theorem. *Amer. Math. Monthly*, 87(9):693–696, 1980.

[Niv1] Ivan Niven. The asymptotic density of sequences. *Bull. Amer. Math. Soc.*, 57(6):420–434, 1951.

[Niv2] I. Niven. A proof of the divergence of $\sum 1/p$. *Amer. Math. Monthly*, 78(3):272–273, 1971.

[NZM] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley, New York, 1991.

[Po] Paul Pollack. *Not Always Buried Deep: Selections from Combinatorial and Analytic Number Theory*.

[Pr] V. V. Prasolov. *Zadači po algebre, aritmetike i analizu*.

[PLA] Planetmath. `http://planetmath.org`.

[PS] Milan Paštéka and Renata Smolíková. *Úlohy z teorie čísel*. Ostravská univerzita, Ostrava, 1996.

[Ri] Paulo Ribenboim. *13 Lectures on Fermat's last theorem*. Springer-Verlag, New York, 1979.

[Ro] H. E. Rose. *A Course in Number Theory*. Oxford University Press, Oxford, 1995.

[RM] R. Sita Rama Chandra Rao and G. Sri Rama Chandra Murty. On a theorem of Niven. *Canad. Math. Bull.*, 22(1):113–115, 1979.

[Š1] T. Šalát. *Nekonečné rady*. Academia, Praha, 1974.

[Š2] T. Šalát. On statistically convergent sequences of real numbers. *Math. Slov.*, 30(2):139–150, 1980.

[Š3] T. Šalát. *Vybrané kapitoly z elementárnej teórie čísel*. MFF UK, Bratislava, 1983. Skriptum.

[Sh] V. Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, Cambridge, 2005. available at http://shoup.net/ntb/.

[Sie1] Wacław Sierpiński. *Pythagorean Triangles*. Dover.

[Sie2] W. Sierpiński. O równaniu $3^x + 4^y = 5^z$. *Wiadom. Mat.*, 1:194–195, 1956.

[Sie3] Wacław Sierpiński. *Elementary theory of numbers*. Państwowe Wydawnictwo Naukowe, Warszawa, 1964. available at `http://matwbn.icm.edu.pl/kstresc.php?tom=42&wyd=10&jez=`.

[Sl] Martin Sleziak. I-convergence. `http://thales.doa.fmph.uniba.sk/sleziak/papers/iconvtalk.pdf`.

[St] J. Steuding. Probabilistic number theory. available at `http://www.math.uni-frankfurt.de/~steuding/steuding/prob.pdf`.

[ŠHHK] T. Šalát, A. Haviar, T. Hecht, and T. Katriňák. *Algebra a teoretická aritmetika 2*. Alfa, Bratislava, 1986.

[SŠ] A. Schnizel and T. Šalát. Remarks on maximum and minimum integers in factoring. *Math. Slov.*, 44(5):505–514, 1994.

[ŠŠN] M. Švec, T. Šalát, and T. Neubrunn. *Matematická analýza funkcií reálnej premennej*. Alfa, Bratislava, 1987.

[ŠT] T. Šalát and V. Toma. A classical Olivier's theorem and statistical convergence. *Annales mathématiques Blaise Pascal*, 10(2):305–313, 2003.



[T] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*. Cambridge Univ. Press, Cambridge, 1995.

[V] Tomáš Váňa. Silné pseudoprvočísla, 2007. bakalárska práca.

[VR] A. Valachová-Rusnáková. Prvočísla. Master's thesis, MFF UK, Bratislava, 1981.

[WIK] Wikipedia. `http://en.wikipedia.org`.

[Za] D. Zagier. Newman's short proof of the prime number theorem. *Amer. Math. Monthly*, 104(8):705–708, 1997.

[Zn] Š. Znám. *Teória čísel*. Alfa, Bratislava, 1986.

# Register

absolútne pseudoprvočísla, 44
aditívna báza, 109
asociované prvky, 101

Bertrandov postulát, 23
Bhagmaguptova-Fibonacciho identita, 111
Brunova konštanta, 27
Bézoutova identita, 8

Carmichaelove čísla, 44

deliteľ jednotky, 101
diofantická rovnica, 94
dokonalé číslo, 38
dolná celá časť, 5

eisensteinovské celé číslo, 104
Euklidov algoritmus, 119
Euklidovský okruh, 101
Eulerova identita, 115
exponent čísla $a$ modulo $n$, 46

Fermatove čísla, 27
Fibonacciho identita, 111
Fibonacciho čísla, 11
funkcia
    aritmetická, 37
    multiplikatívna, 37
    úplne multiplikatívna, 37

gaussovské celé číslo, 103

horná celá časť, 5
hustota
    asymptotická, 74
    dolná asymptotická, 74
    dolná logaritmická, 85
    horná asymptotická, 74
    horná logaritmická, 85
    logaritmická, 85
    Schnireľmannova, 83

identita
    Bhagmaguptova-Fibonacciho, 111
    Eulerova, 115
invertibilný prvok, 101
ireducibilný prvok, 102

Jacobiho symbol, 68

kongruencia
    lineárna, 31
kongruencia modulo $n$, 29
kvadratický nezvyšok, 55
kvadratický zvyšok, 55

Legendrov symbol, 56
lema
    Euklidova, 9
lineárna diofantická rovnica, 94

maximálny ideál, 102
Mersennove čísla, 27
metóda nekonečnej regresie, 99

najmenší spoločný násobok, 10
najväčší spoločný deliteľ, 7
    v okruhu, 102
nesúdeliteľné čísla, 7
norma, 101, 104

okruh hlavných ideálov, 101
okruh s jednoznačným rozkladom, 103

perfektné číslo, 38
prvoideál, 102
prvočíselná funkcia, 18
prvočísla Sophie-Germainovej, 28
pseudoprvočíslo pri báze $a$, 50

rad
    harmonický, 121
rád aditívnej bázy, 109

Stirlingove číslo druhého druhu, 49
súdeliteľné čísla, 7

veta
    Dirichletova, 26
    malá Fermatova, 43
    Mannova, 85
    prvočíselná, 18
    Schireľmannova, 84
    Čínska o zvyškoch, 33

zlomková časť, 5
zvyšková trieda
    redukovaná, 31
zvyšková trieda modulo $m$, 29

Čebyševova funkcia, 22
Čebyševove nerovnosti, 19

číslo bez kvadratických deliteľov, 15

## Zoznam symbolov


| | |
|---|---|
| $\mathbb{Z}$ | 4 |
| $\mathbb{N}$ | 4 |
| $\mathbb{N}_0$ | 4 |
| $\mathbb{R}$ | 4 |
| $\mathbb{C}$ | 4 |
| $\ln x$ | 5 |
| $\log x$ | 5 |
| $\lg x$ | 5 |
| $f(x) \sim g(x)$ | 5 |
| $f(x) = O(g(x))$ | 5 |
| $\lfloor x \rfloor$ | 5 |
| $\lceil x \rceil$ | 5 |
| $\{x\}$ | 5 |
| $p \mod q$ | 6 |
| $a \mid b$ | 7 |
| $(a, b)$ | 7 |
| $[a, b]$ | 11 |
| $(a_1, \ldots, a_n)$ | 11 |
| $[a_1, \ldots, a_n]$ | 11 |
| $\pi(x)$ | 18 |
| $\mathrm{li}(x)$ | 19 |
| $\mathrm{Li}(x)$ | 19 |
| $\vartheta(x)$ | 22 |
| $B_2$ | 27 |
| $a \equiv b \pmod{n}$ | 29 |
| $\overline{k}$ | 29 |
| $\mathbb{Z}_n$ | 30 |
| $S(n, r)$ | 49 |
| $qRn$ | 55 |
| $q\overline{R}n$ | 55 |
| $\left(\frac{a}{p}\right)$ | 56 |
| $\left(\frac{m}{P}\right)$ | 68 |
| $\underline{A}(n)$ | 74 |
| $\overline{d}(A)$ | 74 |
| $d(A)$ | 74 |
| $\sigma(A)$ | 83 |
| $A_1 + \ldots + A_k$ | 84 |
| $nA$ | 84 |
| $U(R)$ | 101 |
| $x \sim y$ | 101 |
| $\mathbb{Z}[i]$ | 103 |
| $\omega$ | 103 |
| $\mathbb{Z}[\omega]$ | 104 |
| $N(z)$ | 104 |
| $A_1 + \ldots + A_k$ | 109 |
| $nA$ | 109 |