Obsah

Kapitola 1

Úvod

Verzia: 8. decembra 2007

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: Deliteľnosť v obore $\mathbb{Z}$, prvočísla. Prvočíselná veta. Základné aritmetické funkcie. Dokonalé čísla. Kongruencie. Eulerova veta. Pytagorovské trojuholníky.

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], [KPW], [KLS], [Kos], [Lem2], [Lem1], [Lev1], [Lo], [MSC], [ME], [Nat], [NZM], [Po], [Pr], [Ri] [Ro], [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. Višňovskú.

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
$\mathbb{N} = \{1, 2, \dots\}$ = 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 $z \leq x < z+1$. Označujeme ju $\lfloor x \rfloor$.

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

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

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

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

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

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

Ak $0 \leq \{x\} < \frac{1}{2}$, 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 $\frac{1}{2} \leq \{x\} < 1$, tak $1 \leq 2\{x\} < 1$, z čoho dostaneme $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$ a $\lfloor 2x \rfloor - 2\lfloor x \rfloor = 1$. $\square$

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

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.

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

Navyše, n a r sú týmito podmienkami jednoznačne určené.

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

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

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

Jednoznačnosť: Predpokladajme, že $p = n.q + r = n'.q + r'$, kde $0 \leq r, r' < q$. Potom
$$(n - n').q = r' - r.$$

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

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 $\mid$.

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* $a \leq b$.

(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.

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. $\square$

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.

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.

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 $m \mid b$. $\square$

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 $c \mid ua + vb = (a, b)$. $\square$

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 $\mid$ 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.

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 $a \mid c$. $\square$

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

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 $ab \mid ka = c$. $\square$

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.*

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

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

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

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

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

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 $(\frac{a}{d}, \frac{b}{d}) = 1$. $\square$

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 $7(n^2 + n + 1)$.

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.

Lema 2.1.13. *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. □

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 celé 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 $(a_1, \dots, a_n)$ a $[a_1, \dots, a_n]$.

Cvičenia

1. Je relácia $\mid$ 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 $n!$.
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: Prirodzené číslo N je zložené práve vtedy, keď existujú prirodzené čísla $n, m \in \mathbb{N}$ 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 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots$

2.2.1 Základné vlastnosti prvočísel

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

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 $a_1, \dots, a_n \in \mathbb{Z}$. Ak $p \mid a_1 \dots a_n$, tak $p \mid a_k$ pre niektoré $k = 1, \dots, n$.*

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?

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

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.)

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 [Ni], 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 $\lim\limits_{n\to\infty} S_n = S < +\infty$ (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 $\sum\limits_{n=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}$ (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 $\sum\limits_{n=1}^{\infty} \frac{1}{p_k}$ konverguje. Potom existuje $k \in \mathbb{N}$ také, že

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

Pre každé prirodzené číslo N máme potom nerovnosť

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

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

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

Na odhad čísla N_s opäť použijeme fakt, že každé $n \leq N$ 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 $b_n^2 \leq n \leq N$ máme odhad $b_n \leq \sqrt{N}$, preto máme najviac $\sqrt{N}$ možností pre číslo b_n. Celkovo teda máme

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

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

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

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

Dôkaz. Označme $R_n = \sum\limits_{p\le n, p\in\mathbb{P}} \frac{1}{p}$. 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 $\lim\limits_{n\to\infty} \frac{\pi(n)}{n} = 0$. □

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 π slúžia ako prostriedky na popis rozloženia prvočísel.

Dôkaz vety 2.3.3. Predpokladajme, že rad $\sum\limits_{p\in\mathbb{P}} \frac{1}{p}$ 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 $\sum\limits_{k=1}^{\infty} \frac{1}{n_k}$ 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 π sa nazýva *prvočíselná funkcia.*

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

Funkcia π 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:

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 $0 \leq a < b$, sa nachádza nejaký prvok množiny M. Napríklad $\mathbb{Q} \cap \langle 0, +\infty)$ je hustá podmnožina $\langle 0, +\infty)$.

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

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 $\lim\limits_{n\to\infty} \pi(an) = +\infty$, máme $\lim\limits_{n\to\infty}(\pi(bn) - \pi(an)) = +\infty$. □

[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 $\lim\limits_{n\to\infty}(\pi(bn)-\pi(an)) = +\infty$. 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 $a < \frac{p}{q} \leq b$. $\square$

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

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

$\square$

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.

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.)

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

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

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

$\square$

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

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 $d_n \ge d_{n-1} \ge 2^{n-2}$. $\square$

Veta 2.3.13. *Pre každé kladné číslo n platí*

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

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

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

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

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

(cvičenie 9 v časti 2.1).

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

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 $n \geq 2$.

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

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

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

Súčasne $n = \pi(p_n) > c_1 \frac{p_n}{\ln p_n}$. Pretože $\lim\limits_{x\to\infty} \frac{\ln x}{\sqrt{x}} = 0$, 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 $n \geq 2$. □

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 $n \geq 6$.

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

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

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 $\vartheta(x)$.

Veta 2.3.15.

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

Dôkaz. Zrejme $\vartheta(x) = \sum\limits_{p \leq x} \ln p \leq \sum\limits_{p \leq x} \ln x = \pi(x) \ln x$. Z toho dostaneme, že

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

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

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

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 ε môžeme zvoliť ľubovoľne malé, platí potom

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

□

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

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

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

Podľa predchádzajúcej vety je

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

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

$$
\begin{aligned}
(2n)^{\sqrt{2n}} 4^{\frac{2}{3}n} &\geq \frac{4^n}{2n} \\
(2n)^{\sqrt{2n}+1} &\geq 4^{\frac{n}{3}} \qquad (2.3)
\end{aligned}
$$

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

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

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. $\square$

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 $\lim\limits_{k\to\infty} \prod\limits_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = 0$.

6. Dokážte, že ak $\lim\limits_{n\to\infty} x_n = L$ a $y_n = \frac{x_1+\ldots+x_n}{n}$ je postupnosť aritmetických priemerov čísel x_n, tak $\lim\limits_{n\to\infty} y_n = L$.

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 $\prod\limits_{p \leq n} p \geq n$ 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 $N = 4p_3 \dots p_n + 3$, kde p_k označuje k-te prvočíslo, t.j. $p_1 = 2$, $p_2 = 3$, atď.

Zrejme $N > p_n$ a $(N, p_k) = (4p_3 \dots p_n + 3, p_k) = (3, p_k) = 1$ pre $k > 2$, $k \leq n$. Súčasne $(N, 3) = (4p_3 \dots p_n, 3) = 1$ 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. $\square$

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

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

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 $(F_n, F_{n+k}) = (F_n, 2) = 1$. $\square$

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.* Ani o nich sa nevie, či ich existuje nekonečne veľa. Mersennove prvočísla spomenieme v nasledujúcej kapitole v súvislosti s dokonalými číslami.

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

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 $2^n - 1 = (2^m)^k - 1 = (2^m - 1)(1 + 2^m + \ldots + 2^{m(k-1)})$. $\square$

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.

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.[2]

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 $m \in \mathbb{N}$.

[2] 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.

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 $\overline{k}$.

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 $\cdot$ sú kompatibilné s reláciou $\equiv$. 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*

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

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*

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

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.)

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.

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.*

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 $a \equiv b \pmod{\frac{n}{d}}$.*

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 $a \equiv b \pmod{mn}$.

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, $i = 1, 2, \dots, n$, sú po dvoch nesúdeliteľné, tak platí aj $a \equiv b \pmod{m}$, kde $m = m_1 \dots m_n$.*

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 $p \mid q - 1$.*

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*

$$ax \equiv b \pmod{n} \tag{3.1}$$

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 $x_0, x_0 + \frac{n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$ 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.

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

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 kongruenciám. Druhý dôkaz pekným spôsobom využíva princíp superpozície.

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 $0,1,\dots,m_1m_2-1$. 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 $x_0\in\{0,1,\dots,m_1m_2\dots m_{n-1}-1\}$ 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. $\square$

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 $x_1 \equiv x_0 \pmod{m}$. $\square$

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 kongruenciou 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 $m_1, \dots, m_n$ sú po dvoch nesúdeliteľné čísla. Nech $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}$ a pre každé $k = 1, 2, \dots, n$ 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 $m_1 \dots m_n$.

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 $m_1 \dots m_n$. □

Ako aplikáciu Čínskej vety o zvyškoch môžeme uviesť nasledujúci výsledok:

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

$$f(x) \equiv 0 \pmod M \tag{3.2}$$

má riešenie práve vtedy, keď každá z kongruencií

$$f(x) \equiv 0 \pmod{m_k}, \qquad k = 1, \dots, r \tag{3.3}$$

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

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

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 $k = 1, 2, \dots, r$ 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 $(a_1, \dots, a_r)$ 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 $p^5q - pq^5$ 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 mod 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.

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

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 $f(d) = f(d_1 d_2) = f(d_1)f(d_2)$. 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 σ 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 σ je multiplikatívna funkcia. □

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

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

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^α 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 σ 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. $\square$

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

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

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

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

Súčasne platí $4 \nmid 1 + p_1 + \ldots + p_1^{l_1}$ a $2 \nmid 1 + p_i + \ldots + p_i^{l_i}$ 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 $1 + p + \ldots + p^l$ je párne, l je nepárne, $l = 2t + 1$ pre nejaké t. Z toho $1 + p + \ldots + p^{2t+1} = (1 + p)(1 + p^2 + \ldots + p^{2t})$. Ak by $p = 4b + 3$, tak $4 \mid p + 1 \mid 1 + p + \ldots + p^{2t+1}$, 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 $1+p+\ldots+p^l = 1+p+\ldots+p^{4k+3} = (1+p+p^2+p^3)(1+p^4+\ldots+p^{4k})$. 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 $4 \mid 1+p+\ldots+p^l$. Zostáva teda druhá možnosť, $l = 4k + 1$. $\square$

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 $\sigma(n_k) > k! + \frac{k!}{2} + \frac{k!}{3} + \ldots + \frac{k!}{k}$, čiže

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

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.

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 $d(k!) \geq k$. □

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

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

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

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

Uvažujme jednotlivé činitele p^α.

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 $\lim\limits_{n\to\infty} \frac{d(n)}{n^{\varepsilon}} = 0$. □

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 $n = p_1p_2$, 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.

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 $g(n) = \sum\limits_{d|n, d \text{ nepárne}} f(d)$, 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

3.3.1 Eulerova funkcia, Malá Fermatova veta

Definícia 3.3.1. Nech $m \in \mathbb{N}$. Ako $\varphi(m)$ označíme počet čísel z množiny $\{1, 2, \ldots, m\}$ nesúdeliteľných s m. Funkciu φ 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 $1, 2, \ldots, p - 1$ 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 $\{1, 2, \ldots, p^k\}$ práve p^{k-1}.

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

Veta 3.3.3. *Eulerova funkcia φ je multiplikatívna.*

Dôkaz. Pre ľubovoľné $k \in \mathbb{N}$ označme $M_k = \{a \in \{1, 2, \ldots, k\}; (a, k) = 1\}$. 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 $x \in \{0, 1, \ldots, mn-1\}$ také, že

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

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 $a = x \bmod m$, $b = x \bmod n$. 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

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

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

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.

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 $p \mid \binom{p}{i}$. $\square$

Lema 3.3.6. *Nech p je prvočíslo. Potom*

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

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 $(a+1)^p = \sum\limits_{i=0}^{p} \binom{p}{i} a^i$. Použitím lemy 3.3.5 dostaneme

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

$\square$

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

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

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

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

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

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

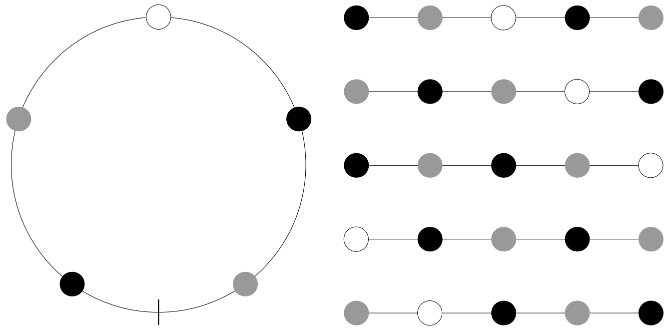
[1] Iný spôsob ako dokázať, že $\binom{n}{k}$ je celé číslo pre ľubovoľné prípustné n a k je indukciou pomocou známeho vzťahu $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.

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

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^α. Pri overovaní Eulerovej vety pre mocniny prvočísel bude užitočná nasledujúca lema.

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 $k = 0, 1, \ldots, p-1$. (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 $k = 0, 1, \ldots, p-1$ 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. □

Veta 3.3.10. *Pre ľubovoľné prirodzené číslo n platí*

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

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

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

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

$\square$

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

Dôkaz. Označme $A := \{1, 2, \dots n\}$ 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 $|A| = \sum\limits_{d|n} |A_d|$.

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

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

$\square$

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

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. $\square$

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.

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

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

(ii) *Ku každému $s \in \mathbb{N}$ existuje $r \in \{1, 2, \dots, k-1\}$ 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

Kongruenciu tvaru $f(x) \equiv b \pmod{m}$, kde f je polynóm n-tého stupňa s celočíselnými koeficientami, nazývame kongruenciou n-tého stupňa. Už sme sa zaoberali kongruenciami prvého stupňa – lineárnymi kongruenciami. 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.

Veta 3.3.14 (Lagrangeova veta). *Ak $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ 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)]).

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 $b_i = a_i \bmod p$, $i = 0, 1, \ldots, n$.

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

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

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 $p \mid a_i$. □

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

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

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 $H_1,\dots,H_r$ spĺňajúcich tieto podmienky:
(a) Pre všetky $i=1,\dots,r$ je $H_i\neq\emptyset$ a $H_i\subseteq\{1,2,\dots,n\}$.
(b) $\bigcup\limits_{i=1}^{r} H_i=\{1,2,\dots,n\}$.
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 $H_1,\dots,H_r$; 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.

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

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

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 $H_2,\dots,H_r$ 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 $H_2,\dots,H_r$ práve $B(n-k,r-1)$ spôsobmi.

Pomocou (3.9) a (3.10) môžeme ukázať nasledujúcu lemu.

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

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

$\square$

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 $1 \equiv -1 \pmod{p}$.) $\square$

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

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

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

Dôkaz. Podľa Wilsonovej vety máme

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

$\square$

Cvičenia

1. Nájdite všetky n také, že a) $\varphi(n) = \frac{n}{2}$; b) $\varphi(n) = \varphi(2n)$; c) $\varphi(n) = 12$.
2. Dokážte vzťah (3.5) pomocou princípu zapojenia a vypojenia.
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 $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$ a $1^p + 2^p + \dots + (p-1)^p \equiv 0 \pmod{p}$.
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 $1^2.3^2 \dots (p-2)^2 \equiv 2^2.4^2 \dots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

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

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.)

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* μ 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 μ 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 $g(n) = \mu(1)f(1) + \mu(p)f(p) + \ldots + \mu(p^k)f(p^k) = 1 - f(p) + 0 + \ldots + 0 = 1 - f(p)$. $\square$

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

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

Dôsledok 3.4.4.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{ak } n = 1, \\ 0, & \textit{inak.} \end{cases}$$

$$\sum_{d|n} \frac{\mu(d)}{d} = \begin{cases} 1, & \textit{ak } n = 1, \\ \prod_{k=1}^{n} \left(1 - \frac{1}{p_k}\right), & \textit{inak.} \end{cases}$$

Z vety 3.3.4 potom máme

Dôsledok 3.4.5.

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

Už vieme, že ak f je multiplikatívna funkcia, tak aj funkcia $g(n) = \sum_{d|n} f(d)$ 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

$$f * g(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

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 $\sum\limits_{d|n} f(n)$, 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 $f * I = f$.

Veta 3.4.7 (Möbiova inverzia). *Ak* $g(n) = \sum\limits_{m|n} f(m)$ *pre ľubovoľné* n, *tak*

$$f(n) = \sum_{m|n} \mu(m) g\left(\frac{n}{m}\right) = \sum_{m|n} \mu\left(\frac{n}{m}\right) g(m).$$

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.) □

Veta 3.4.8 (Möbiova inverzia). *Ak* $f(n) = \sum\limits_{m|n} \mu\left(\frac{n}{m}\right) g(m)$, *tak* $g(n) = \sum\limits_{m|n} f(m) = \sum\limits_{m|n} f\left(\frac{n}{m}\right)$.

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:

$$\begin{aligned} g &= f * u & &\Rightarrow & f &= \mu * g, \\ f &= \mu * g & &\Rightarrow & g &= f * u. \end{aligned}$$

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:

$$\begin{aligned} g &= f * u & &\Rightarrow & g * \mu &= (f * u) * \mu = f * (u * \mu) = f * I = f \\ f &= g * \mu & &\Rightarrow & f * u &= (g * \mu) * u = g * (\mu * u) = g * I = g \end{aligned}$$

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 $g(n) = \prod\limits_{d|n} f(d)$. Dokážte, že $f(n) = \prod\limits_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)} = \prod\limits_{d|n} g(d)^{\mu(n/d)}$.

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

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 $n_1, \dots, n_{\varphi(n)}$ 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.

Veta 4.1.4. *Nech $p > 2$ prvočíslo. Ľubovoľný redukovaný zvyškový systém $\{a_1, \dots, a_{p-1}\}$ 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 $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$.

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 $a_1, \dots, a_{p-1}$ 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.

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:

Lema 4.2.5. *Nech p je nepárne prvočíslo a $a, b \in \mathbb{Z}$. Potom*

(i) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) $\left(\frac{1}{p}\right) = 1$

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

(iv) $\left(\frac{a^2}{p}\right) = 1$

(v) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

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.

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 $q_1, \dots, q_n$ boli všetky prvočísla, ktoré majú po delení 4 zvyšok 1. Položme $N = 4q_1^2 q_2^2 \dots q_n^2 + 1$. Potom N je nepárne zložené číslo a $q_i \nmid N$ pre $i = 1, 2, \dots, n$. Teda N nemá žiadny prvočiniteľ tvaru $4k+1$.

Na druhej strane, ak p je prvočíslo také, že $p \mid N$, tak $(2q_1 \dots q_n)^2 \equiv -1 \pmod p$. 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.

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

$$2.4.6\dots(p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\dots+(p-1)/2} \pmod{p}.$$

Platí $1 + 2 + \dots + \frac{p-1}{2} = \frac{1}{2}\frac{p-1}{2}(\frac{p-1}{2} + 1) = \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = \frac{p^2-1}{8}$. 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 $p = 8k\pm1$, tak číslo $\frac{p^2-1}{8} = \frac{64k^2\pm16k}{8} = 8k^2\pm2k$ je párne a ak $p = 8k\pm3$, tak $\frac{p^2-1}{8} = \frac{64k^2\pm16k+8}{8} = 8k^2 \pm 2k + 1$ 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 $q_1, \dots, q_n$ sú všetky prvočísla tvaru $8k+7$. Položme $N = (4q_1q_2\dots q_n)^2 + 2$. 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 $i = 1, \dots, n$, 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).

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 $\{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$, 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 $S = a.2a.3a \dots \frac{p-1}{2}a$ modulo p dvoma rôznymi spôsobmi. Zrejme

$$S = a^{(p-1)/2}\left(\frac{p-1}{2}\right)!$$

Na druhej strane každé a čísel ka, $k = 1, 2, \dots, \frac{p-1}{2}$ sa dá vyjadriť v tvare $sp + z$, kde z je niektorý z prvkov množiny $\{\pm1, \pm2, \dots, \pm\frac{p-1}{2}\}$. (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 $k_1a \equiv -k_2a \pmod p$. V takomto prípade by totiž platilo $p \mid k_1 + k_2$, čo je v spore s tým, že $k_1, k_2 \in \{1, 2, \dots, \frac{p-1}{2}\}$.

To znamená, že medzi najmenšími zvyškami čísel ka sa vyskytnú všetky čísla $1, 2, \dots, \frac{p-1}{2}$, 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 $\{\pm1, \pm2, \dots, \pm\frac{p-1}{2}\}$ použitá v predchádzajúcom dôkaze tvorí redukovaný zvyškový systém.

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

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor}.$$

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

$$\left\lfloor \frac{2ak}{p} \right\rfloor = \begin{cases} 2\lfloor \frac{ak}{p} \rfloor, & \text{ak } 0 \leq \{\frac{ak}{p}\} < \frac{1}{2}; \\ 2\lfloor \frac{ak}{p} \rfloor + 1, & \text{ak } \frac{1}{2} \leq \{\frac{ak}{p}\}. \end{cases}$$

Z toho vyplýva, že číslo $\lfloor \frac{2ak}{p} \rfloor$ je párne ak $0 \leq \{\frac{ak}{p}\} < \frac{1}{2}$ 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 $\frac{r_k}{p} \geq \frac{1}{2}$ práve vtedy, keď $r_k \geq \frac{p}{2}$. 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

$$(-1)^{\sum\limits_{k=1}^{(p-1)/2} \lfloor \frac{(a+p)}{k} \rfloor}.$$

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

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor} (-1)^{(p^2-1)/8} = (-1)^{\sum\limits_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor} \left(\frac{2}{p}\right),$$

a teda

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{(p-1)/2} \lfloor \frac{ak}{p} \rfloor}.$$

□

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

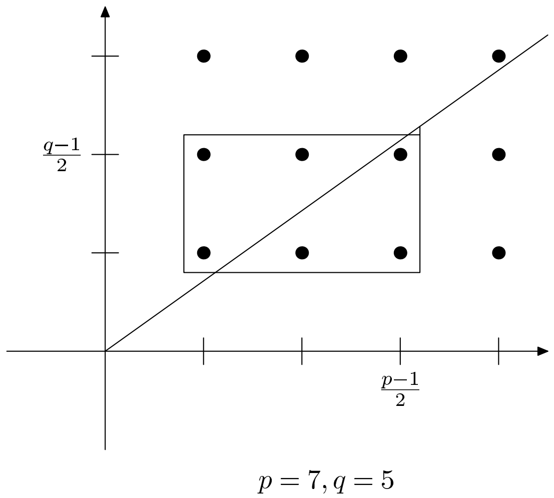
Nasledujúca veta je dosť dôležitá. Ako zaujímavosť môžeme spomenúť, že je známych cez 200 dôkazov tejto vety – pozri `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html` alebo [Lem2].

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 $1 \le x \le \frac{p-1}{2}$ a $1 \le y \le \frac{q-1}{2}$. 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 $p = 7$, $q = 5$

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

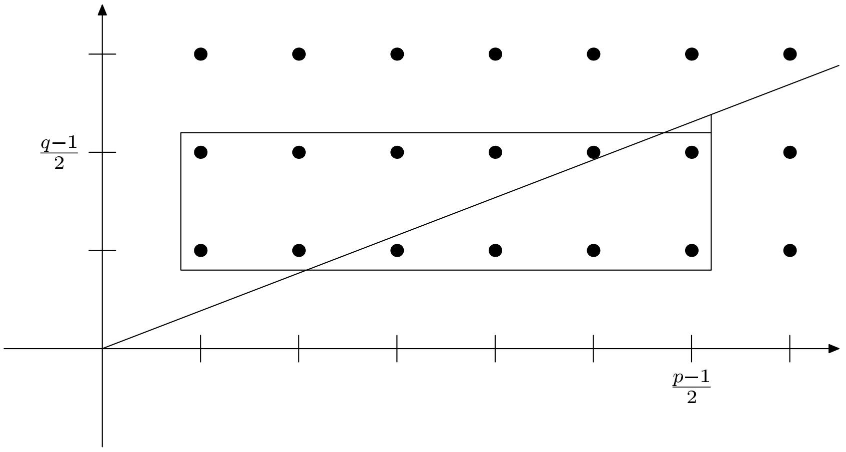
$$q\left(\frac{p-1}{2}\right) - p\left(\frac{q-1}{2}\right) = \frac{p-q}{2} > 0.$$

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. $\square$

Obr. 4.2: Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 13$, $q = 5$



$p = 13, q = 5$

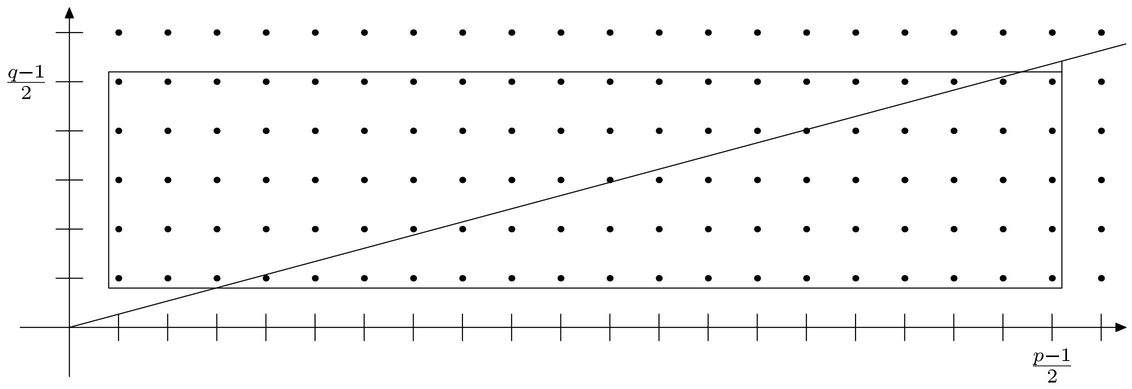
Ľahko vidno, že zákon kvadratickej reciprocity môžeme ekvivalentne preformulovať takto:

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].



$p = 41, q = 7$

Obr. 4.3: Ilustrácia dôkazu zákona kvadratickej reciprocity, prípad $p = 41$, $q = 7$

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 $\{1, 2, \dots, n\}$, v nasledujúcom dôkaze však začneme od nuly, pre nás teda $M = \{0, 1, 2, \dots, n\}$.

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

$$(a_1, \dots, a_n) = (a_1a_2)(a_1a_3)\dots(a_1a_n),$$

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 τ 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 τ.

Z toho, ako sa parita dá vyjadriť pomocou počtu transpozícií, okamžite vidíme užitočnú rovnosť

$$\epsilon(\tau \circ \psi) = \epsilon(\tau).\epsilon(\psi).$$

Lema 4.3.4 (Zolotarevova lema). *Nech p je prvočíslo a $m \in \mathbb{Z}_p \setminus \{0\}$. Ako τ_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 τ_m evidentne ponecháva prvok 0 na mieste, stačí si teda všímať, ako poprehadzuje ostatné prvky.

Vieme, že pre cyklus σ dĺžky k je $\epsilon(\sigma) = (-1)^{k-1}$. Nech rád prvku m v grupe $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ je i. Potom permutácia τ_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 ± 1, tak akonáhle sú kongruentné modulo p, musia sa už rovnať. $\square$

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 τ 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 $0 \leq r < p$ a $0 \leq k < q$.

Najprv si ozrejmime, že takto definované τ je skutočne permutácia M. Predpokladajme, že

$$kp + rq \equiv k'p + r'q \pmod{pq}$$

pre nejaké $0 \leq r, r' < p$ a $0 \leq k, k' < q$. Potom

$$\begin{aligned} kp &\equiv k'p \pmod q, \\ rq &\equiv r'q \pmod p. \end{aligned}$$

a podľa vety 3.1.9

$$\begin{aligned} k &\equiv k' \pmod q, \\ r &\equiv r' \pmod p. \end{aligned}$$

Zistili sme, že r a r' sú také čísla $0 \leq r, r' < p$, 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 τ 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 α permutáciu, ktorej zodpovedá takéto preusporiadanie stĺpcov. Znamená to, že v každom riadku sme urobili permutáciu zodpovedajúcu inverznej k permutácii τ_q z lemy 4.3.4. Táto permutácia jedného riadku pozostáva z rovnakého počtu transpozícií ako τ_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 β. 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 τ:

$$\begin{array}{ccccc}
0 & q & 2q & \dots & (p-1)q \\
p & p+q & p+2q & \dots & p+(p-1)q \\
2p & 2p+q & 2p+2q & \dots & 2p+(p-1)q \\
\dots & \dots & \dots & \dots & \dots \\
(q-1)p & (q-1)p+q & (q-1)p+2q & \dots & (q-1)p+(p-1)q
\end{array}$$

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 τ_p vieme preusporiadať tieto zvyšky do správneho poradia. Podobnú permutáciu použijeme pre všetky stĺpce. Dostaneme takto permutáciu γ, ktorej znamienko je $\epsilon(\gamma) = \left(\frac{p}{q}\right)^p = \left(\frac{p}{q}\right)$. Keď ju zložíme s τ, 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 $\mod pq$.)

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 δ.)

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 τ je potom

0	3	6	9	12
5	8	11	14	2
10	13	1	4	7

Zvyšky v jednotlivých stĺpcoch po delení 5 sú 0, 3, 1, 4, 2 = permutácia τ_3 množiny $\{0,1,2,3,4\}$. Čiže preusporiadaním stĺpcov použitím inverznej permutácie k τ_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 τ_2 množiny $\{0,1,2\}$, τ_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).

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

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right)(-1)^{382.2/4} = \left(\frac{2}{3}\right)(-1)^{191} = 1$$
$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)(-1)^{382.72/4} = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) \stackrel{(*)}{=} 1.1 = 1$$

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 ± 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.

Lema 4.4.3. *Nech P, Q sú nepárne prirodzené čísla a $a, b \in \mathbb{Z}$. Potom*

(i) $a \equiv b \pmod P \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$

(ii) $\left(\frac{1}{P}\right) = 1$

(iii) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$

(iv) $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$

(v) *Ak* $(b, P) = 1$, *tak* $\left(\frac{b^2}{P}\right) = 1$.

(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). □

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

$$P - 1 \equiv \sum_{i=1}^{r}(p_i - 1) \pmod 4, \tag{4.1}$$

$$\frac{P-1}{2} \equiv \sum_{i=1}^{r}\frac{p_i - 1}{2} \pmod 2. \tag{4.2}$$

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

$$P^2 - 1 \equiv \sum_{i=1}^{r}(p_i^2 - 1) \pmod{64},$$

$$\frac{P^2-1}{8} \equiv \sum_{i=1}^{r}\frac{p_i^2 - 1}{8} \pmod 8,$$

$$\left(\frac{2}{P}\right) = \prod_{i=1}^{r}(-1)^{(p_i^2-1)/8} = (-1)^{(P^2-1)/8}$$

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

□

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

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^r \tag{4.3}$$

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 rozklad čísla b sa nevyskytne žiadne z prvočísel $l_1 \dots l_t$.

Pre Jacobiho symbol $\left(\frac{a}{b}\right)$ dostaneme

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{q_1}{b}\right) \cdots \left(\frac{q_n}{b}\right).$$

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 $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$.

$$\left(\frac{a}{b}\right) = \left(\frac{b}{q_1}\right) \cdots \left(\frac{b}{q_n}\right) = \left(\frac{1}{q_1}\right) \cdots \left(\frac{1}{q_{n-1}}\right) \left(\frac{s}{q_n}\right) = -1.$$

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

$$b = 8 l_1 \dots l_t + 3,$$

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 ± 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 $\sum\limits_{a=1}^{p-1} a \left(\frac{a}{p}\right) = 0$ a $\sum\limits_{\substack{a=1 \\ (a|p)=1}}^{p-1} a = \frac{p(p-1)}{2}$.

Dodatok A

Euklidov algoritmus

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.0.4. 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 násjť $u, v \in \mathbb{N}$ 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.0.5. 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.0.6. 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

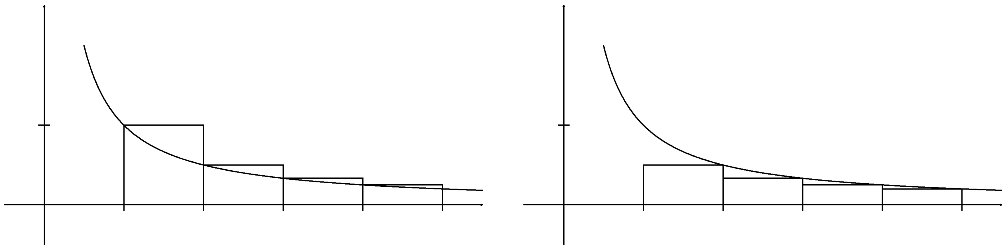
Harmonický rad je rad
$$\sum_{k=1}^{\infty} \frac{1}{k}. \tag{B.1}$$
Ľahko si všimneme, že tento rad diverguje – stačí si všimnúť, že rad (B.1) môžeme rozdeliť na časti, ktorých súčet je vždy aspoň $\frac{1}{2}$
$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \left[\frac{1}{2}\right] + \left[\frac{1}{3} + \frac{1}{4}\right] + \left[\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right] + \dots$$

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
$$\frac{1}{n+1} \leq \frac{1}{x} \leq \frac{1}{n},$$
z čoho máme (sčítaním od 1 po $n-1$)
$$\sum_{k=2}^{n} \frac{1}{k} = \sum_{k=1}^{n} \frac{1}{k} - 1 \leq \int_1^n \frac{1}{x} dx = \ln n \leq \sum_{k=1}^{n} \frac{1}{k},$$
$$\ln n \leq \sum_{k=1}^{n} \frac{1}{k} \leq \ln n + 1.$$
(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
$$\lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n \right) = \gamma. \tag{B.2}$$
Táto limita sa nazýva *Eulerova konštanta* (niekedy aj Eulerova-Mascheroniho konštanta).

Jej hodnota je približne $0,577$. Dodnes nie je známe, či Eulerova konštanta γ 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 $\frac{1}{x}$

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 $0 \le a_n - a_{n-1} = f(n) - \int\limits_n^{n+1} f(x)dx \le f(n) - \int\limits_n^{n+1} f(n+1)dx = f(n) - f(n+1)$.

Postupnosť a_n je je postupnosť čiastočných súčtov radu s kladnými členmi $f(n) - \int\limits_n^{n+1} f(x)dx$. Preto a_n je kladná rastúca postupnosť. Navyše je ohraničená, pretože $a_n \le f(1) - f(2) + f(2) - f(3) + \ldots - f(n) = f(1) - f(n+1) \le f(1)$. Každá rastúca ohraničená postupnosť má limitu. □

B.2 Rad prevrátených hodnôt druhých mocnín

V tejto časti budeme uvažovať o rade

$$\sum_{k=1}^{\infty} \frac{1}{k^2}. \tag{B.3}$$

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

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 [Kn] alebo v knihe [S], 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.

[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.

[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.

[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.

[Kl] M. Klazar. Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti. *Pokroky matematiky, fyziky a astronomie*, 49(3):177–188, 2004.

[Kn] 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.

[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.

[M] 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.

[Ni] 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.

[S] V. Shoup. *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press, Cambridge, 2005. available at http://shoup.net/ntb/.

[ŠHHK] T. Šalát, A. Haviar, T. Hecht, and T. Katriňák. *Algebra a teoretická aritmetika 2.* Alfa, Bratislava, 1986.

[ŠŠN] M. Švec, T. Šalát, and T. Neubrunn. *Matematická analýza funkcií reálnej premennej.* Alfa, Bratislava, 1987.

[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

Zoznam symbolov