Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Silné Pseudoprvočísla

(bakalárska práca)

Tomáš Váňa

---

vedúci:
RNDr.Martin Mačaj, PhD.

Bratislava, 2007

Čestne prehlasujem, že som túto bakalársku prácu vypracoval samostatne s použitím citovaných zdrojov.

. . . . . .

Obsah

Kapitola 1

Úvod

V práci, ktorú čitateľ berie do rúk, sa budeme zaoberať algoritmami na testovanie prvočíselnosti prirodzených čísel. Týmto problémom sa matematici zaoberajú už od čias starých Grékov, no mimoriadnu zaujímavosť získal nedávno keď našiel praktické využitie. Objavom šifrovacieho systému RSA sa uskutočnila revolúcia v kryptografii smerom k asymetrickému šifrovaniu znamenajúcemu zásadný prevrat. V tomto systéme sú kľúčovými pojmami práve prvočísla, testovanie prvočíselnosti a faktorizácia čísel, ktoré vzniknú ako súčin dvoch prvočísel. Napriek tomu, že od objavu už ubehlo pár rokov a odvtedy boli vymyslené ďalšie asymetrické metódy, zostáva otvorený problém zložitosti faktorizácie a aspekty týkajúce sa RSA rovnako zaujímavý pre matematikov a informatikov. Nielen preto, že na šifre RSA je aj v súčasnosti založené veľké množstvo bezpečnostných systémov, ale aj pre jednoduchosť zadania kontrastnú k zložitému problému, ktorý popisuje, charakteristickú pre mnohé problémy v teórii čísel (za všetky snáď stačí spomenúť Veľkú Fermatovu vetu, ktorá napriek svojmu jednoduchému zneniu pochopiteľnému priemerným stredoškolákom, odolávala snahám o dokázanie stovky rokov).

Práca je tematicky zameraná na skupinu testov, ktoré majú istú jednotiacu líniu a všetky sú viacmenej založené na Malej Fermatovej vete, čo je až prekvapivo jednoduchý výsledok elementárnej teórie čísel. Samozrejme pri skúmaní rôznych aspektov týchto testov budeme potrebovať oveľa viac vedomostí z teórie čísel a algebry. V zásade však chceme predložiť teóriu, ktorú sa budeme snažiť budovať čo najsebestačnejšie a veľa výsledkov budeme dokazovať len zo základných vedomostí a predpokladov na čitateľa. Pri putovaní od najjednoduchších testov prvočíselnosti založených na

jednoduchých vylepšeniach definície až po najsofistikovanejší test si budeme všímať rôzne vlastnosti. Vo všeobecnosti na testy prvočísel kladieme jasne definované nároky - chceme, aby boli rýchle v zmysle výpočtovej zložitosti a presné v zmysle matematickej korektnosti výsledku. Z oboch týchto podmienok mierne upustíme v záujme poskytnutia iného pohľadu na vec pre nezainteresovaného čitateľa. Väčšina testov, ktorými sa budeme zaoberať, majú v skutočnosti pravdepodobnostný charakter a teda nespĺňajú druhú podmienku. Ak o nejakom čísle prehlásia, že je prvočíslom, alebo naopak ho označia za číslo zložené, môžu sa s istou pravdepodobnosťou mýliť. Taký test na prvý pohľad vyzerá pre matematika nezaujímavo, no v skutočnosti tento prístup otvára úžasné možnosti nielen z hľadiska praktickej aplikovateľnosti výsledkov.

Naše rozprávanie vyvrcholí v kapitole o Miller-Rabinovom teste, v ktorej sa po úvodnej analýze (rovnako ako v ostatných prípadoch sa pozrieme na pravdepodobnosť omylu tohto algoritmu a preskúmame existenciu čísel, pre ktoré zlyháva úplne) budeme zaoberať súvislosťou tohoto testu s tzv. Rozšírenou Riemannovou hypotézou. Táto dodnes nedokázaná veta z komplexnej analýzy má prekvapujúce dôsledky v rôznych oblastiach matematiky, teóriu čísel nevynímajúc. Jej platnosť implikuje skutočnosti, ktorých využitím sa nám podarí ukázať, že uvedený Miller-Rabinov test možno jednoduchým spôsobom upraviť na deterministickú polynomiálnu verziu. Ako som spomenul, aj v otázke výpočtovej zložitosti upustíme od presných dôkazov a ostaneme v intuitívnej rovine. Nebude to však na škodu výkladu, nakoľko sa pokúsime, aby z popisu algoritmov bolo zrejmé, ako sa príslušný polynomiálny algoritmus zostrojí a aby čitateľ bol schopný ďalej pokračovať v úvahách smerom ku korektnému zavedeniu ohraničení na výpočtovú zložitosť. Do týchto detailov sa nepúšťame v záujme čo najstručnejšieho vystihnutia podstatných vlastností, ktoré uvedené algoritmy budú mať. Nakoniec, čitateľ si iste všimne, že mnohokrát sú tieto algoritmy tak jednoduché, že ani nepoužívame slovo algoritmus, aby sme veci zbytočne nekomplikovali a ostávame pri statickom opise vlastností. Všetky uvedené vlastnosti sa však na algoritmus dajú pretransformovať a v skutočnosti sa naozaj s menšími úpravami a vylepšeniami používajú.

Zostáva ešte pripomenúť, že si nedávame za cieľ poskytnúť vyčerpávajúci pohľad na testovanie prvočíselnosti. Zaoberáme sa predovšetkým líniou, ktorá využíva Malú Fermatovu vetu a postupným zovšeobecňovaním Fermatovho testu sa dostaneme až k testu Miller-Rabinovmu. Práve táto jednotná línia je veľmi zaujímavá z estetického a pedagogického

hľadiska, nakoľko odkrýva mnohé zaujímavé skutočnosti. Testy, ktorými sa zaoberáme, však nie sú jedinými spôsobmi, ako prvočíselnosť testovať. V súčasnosti je už známy Agrawal-Kayal-Saxena (AKS) test prvočíselnosti, ktorý je deterministický bez závislosti na akejkoľvek nedokázanej hypotéze, a teda z teoretického hľadiska významnejší ako testy, ktorými sa zaoberáme my. Takisto existujú testy využívajúce eliptické krivky a pravdepodobne do zbierky testov ešte nejaké pribudnú aj v budúcnosti. Napriek tomu testy, ktorými sa zaoberáme v práci sú jednoduché na pochopenie a ich implementácie sa používajú v mnohých praktických aplikáciách. Verím, že čitateľa s hlbším záujmom o testy prvočíselnosti inšpirujem k štúdiu literatúry, kde sa o nich dozvie viac.

Kapitola 2

Pseudoprvočísla

Ako sme spomenuli v úvode, budeme sa v tejto práci zaoberať predovšetkým témami súvisiacimi s testovaním prvočíselnosti. V tejto kapitole sa pokúsime naznačiť hlavnú líniu vysvetlením pojmu pseudoprvočísla. Ak chceme zistiť, či je nejaké číslo prvočíslo, máme niekoľko možností. Tou najjednoduchšou a najpriamočiarejšou je nasledovať definíciu, ktorá hovorí o prvočísle ako o čísle $p > 1$, ktoré má v množine $\{1, \ldots, p\}$ práve dva delitele, a to 1 a p. Takže nám stačí jednoducho pre každé číslo z tejto množiny preveriť, či je deliteľom čísla p. Ak také číslo nájdeme a nebude to ani jedno z dvojice 1 a p, potom je číslo p zložené. V opačnom prípade môžeme s istotou prehlásiť (nakoľko sme splnili podmienku z definície), že číslo p je prvočíslo. Samozrejme takýto prístup je pre veľké p časovo náročný, až prakticky nerealizovateľný. Avšak práve to dáva motiváciu zaoberať sa testovaním prvočíselnosti ako pomerne bohatou podmnožinou algoritmickej teórie čísel. Pozrime sa najprv, ako sa dá tento test zjednodušiť triviálnymi priamočiarymi úvahami. Nasledujúcu vetu iste pozná každý stredoškolák :

Veta 2.1 *Prirodzené číslo n je prvočíslom práve vtedy, ak $n \geq 2$ a n nemá žiadneho deliteľa d pre ktorého by platilo $1 < d \leq \sqrt{n}$*

Dôkaz Ukážeme, že ak n je zložené číslo, potom existuje prvočíselný deliteľ p čísla n pre ktorý platí $p \leq \sqrt{n}$. Keďže číslo n je zložené, musia existovať prirodzené čísla $r, s > 1$, pre ktoré je $n = rs$. Nech p je najmenší prvočíselný deliteľ čísla n. Potom určite platí $p \leq r$ a $p \leq s$, odkiaľ už $p \leq \sqrt{n}$. Preto ak nejaké číslo nemá deliteľa $1 < d \leq \sqrt{n}$, nemôže byť zložené a je nutne

prvočíslom. ■

Táto veta nám sformulovala podmienku ekvivalentnú definícii prvočísla, ktorej preverenie však vyžaduje menej času. Navyše z dôkazu ľahko nahliadneme, že vetu možno upraviť : Nielen že stačí aby číslo n nemalo žiadneho deliteľa $1 < d \leq \sqrt{n}$, stačí ak nemá žiadneho prvočíselného deliteľa $1 < p \leq \sqrt{n}$. Ak preveríme deliteľnosť čísla n všetkými prvočíslami z tohto rozsahu, môžeme s istotou určiť, či je n prvočíslo. Známym konštruktívnym zovšeobecnením tohto prístupu je konštrukcia množiny prvočísel pomocou Eratostenovho sita, čo je metóda postupného hľadania prvočísel odstraňovaním násobkov už nájdených prvočísel. Tento algoritmus je vhodný ak chceme zostrojiť tabuľku prvočísel v nejakom rozsahu. Prirodzene, tu už vstupujú do hry nielen nároky na časovú zložitosť, ale aj zložitosť pamäťovú. Pri veľkostiach prvočísel, ktoré sú pre nás zaujímavé z hľadiska aplikácii je prakticky nemožné takúto tabuľku zostrojiť a uložiť. Samozrejme nakoľko zlepšenie v podobe predchádzajúcej vety nie je až tak významné, nie je to v rámci súčasných výpočtových možností realizovateľné ani časovo. Veľmi zaujímavým, nie už tak celkom triviálnym tvrdením je nasledujúca veta :

Veta 2.2 (Wilsonova veta) *Nech p je prirodzené číslo, $p > 1$. Potom p je prvočíslo práve vtedy, ak platí $(p-1)! \equiv -1 \pmod{p}$.*

Dôkaz Prípady $p = 2, 3$ sa ľahko rozoberú samostatne, takže môžeme predpokladať, že platí $p > 3$. Ak p je zložené, potom sa medzi číslami $1, 2, \ldots, p-1$ nachádzajú nejaké jeho delitele, takže celkom určite platí $((p-1)!, p) > 1$ a teda nemôže byť $(p-1)! \equiv -1 \pmod{p}$. Ak je však p prvočíslo, potom p je nesúdeliteľné s každým z týchto čísel. Preto pre každé z nich, povedzme a, existuje číslo b také, že $ab \equiv 1 \pmod{p}$. Všimnime si, že toto b je jednoznačne určené. Keby bolo zároveň $ac \equiv 1 \pmod{p}$, muselo by byť $ab \equiv ac \pmod{p}$, a teda $b \equiv c \pmod{p}$, odkiaľ už (keďže čísla sú z príslušného rozsahu) plynie $b = c$. Teda ku každému z čísel a existuje príslušné b, pričom keďže p je prvočíslo $a = b$ platí len ak a je 1 alebo $p-1$. Z tohoto už dostávame popárovanie, vďaka ktorému máme $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$. Prenásobením kongruencie číslom $p-1$ už dostávame požadovaný vzťah.■

Wilsonova veta poskytuje nutnú a postačujúcu podmienku prvočíselnosti pre ľubovoľné prirodzené číslo. Metóda testovania prvočíselnosti, ktorá ju využíva, pre číslo n overí platnosť kongruencie $(n-1)! \equiv -1 \pmod{n}$ a na základe toho s istotou prehlási, či sa jedná alebo nejedná o prvočíslo. Na mierne zrýchlenie tohto postupu môžeme využiť fakt, že pre čísla i z množiny $1, \ldots, p-1$ platí $i \equiv n - i \pmod{n}$, takže pre nepárne n je $((\frac{(n-1)}{2})!)^2 \equiv (n-1)!$. To nám umožňuje overiť platnosť kongruencie z Wilsonovej vety v polovičnom čase. V skutočnosti napriek tomu táto metóda nie je efektívnejšia ako naivná metóda prehľadávania deliteľov, keďže na výpočet modulárneho faktoriálu zatiaľ nebol vymyslený rýchlejší postup ako postupné násobenie. Vezmime si napríklad číslo 1997 a pokúsme sa zistiť, či podľa Wilsonovej vety je prvočíslom. Na to, aby sme to urobili, potrebujeme zistiť, aký dáva číslo 999! zvyšok po delení 1997. Nakoľko nie je známe žiadne dramatické vylepšenie tohoto výpočtu, de facto musíme na to vykonať približne 1000 modulárnych násobení (pričom ak sa nám pri niektorom podarí zvyšok vynulovať, končíme). Na porovnanie, ak postupujeme podľa stredoškolského algoritmu hľadania deliteľov, musíme vykonať 44 delení, dokonca ak poznáme množinu malých prvočísel a delíme iba nimi, bude ich ešte menej. Napriek tomu je táto veta z teoretického hľadiska zaujímavá, najmä preto, že ide o ekvivalenciu. Ekvivalentné tvrdenia v tvare $Prime(p) \iff S(p)$ majú výhodu v tom, že poskytujú úplnú charakterizáciu pojmu prvočíslo a dávajú metódy ako s istotou určiť prvočíselnosť. V centre nášho záujmu však nebudú takéto tvrdenia, ale tvrdenia v tvare $Prime(p) \implies S(p)$. Tie nám dávajú síce voľnosť v zavedení jednoducho testovateľných podmienok, no nezaručujú nám z teoretického hľadiska prakticky nič o čísle p. To je veľmi nepríjemná skutočnosť, ako však neskôr uvidíme, vhodnou voľbou tvrdenia S možno dosiahnuť, že implikáciu do istej miery otočíme (pri prijatí určitej pravdepodobnosti omylu alebo predpokladu platnosti Rozšírenej Riemannovej hypotézy). Veľmi jednoduchým príkladom tvrdenia $S(p)$ by bolo : Číslo $p > 1$ je 2,3,5 alebo nie je deliteľné 2,3 ani 5. Takéto tvrdenie naozaj spĺňajú všetky prvočísla a tiež ho zrejme spĺňa veľa zložených čísel. Na tomto jednoduchom tvrdení možno ilustrovať, kam bude viesť naše snaženie. Ak o nejakom čísle p platí $S(p)$, potom je to buď preto že p je prvočíslo, alebo je to jedno z čísel, ktoré sú síce zložené, ale napriek tomu tvrdenie pre ne platí. Pre tieto čísla zavedieme špeciálne pomenovanie.

Definícia 2.1 *Nech S je unárny predikátový symbol, pričom $S(p)$ platí pre*

ľubovoľné prvočíslo p. Potom zložené číslo n, pre ktoré platí $S(n)$ nazveme $S-$pseudoprvočíslom.

$S-$pseudoprvočísla sú čísla, ktorých existencia nám bráni otočiť implikáciu $Prime(p) \implies S(p)$ a používať tvrdenie S ako potenciálne jednoduchší test prvočíselnosti. V závislosti od voľby vhodného tvrdenia S dostaneme rôzne množiny takýchto $S-$pseudoprvočísel. Konkrétne v našom jednoduchom príklade je táto množina veľmi veľká. Veľkosť množiny možno zadefinovať rôznymi spôsobmi, každopádne nech už si zavedieme akýkoľvek spôsob posudzovania, našim hlavným cieľom je dosiahnuť, aby $S-$pseudoprvočísel bolo v istom zmysle dostatočne málo. Budeme sa pritom odvolávať na pojem nízkej relatívnej početnosti, čím máme na mysli, že počet $S-$pseudoprvočísel nejakej veľkosti (napr. $l-$bitových) je (výrazne) menší ako počet prvočísel tejto veľkosti. Navyše požadujeme, aby preverenie platnosti predikátu S bolo možné vykonať rýchlo, inak by pre nás nemal nijaký význam. V nasledujúcich troch kapitolách sa budeme venovať práve predikátom s týmito vlastnosťami.

Kapitola 3

Fermatove pseudoprvočísla

Naznačili sme, kam smeruje naša snaha pri zavádzaní pojmu pseudoprvočísla. Chceme nájsť tvrdenie, ktoré platí pre všetky prvočísla, pričom nie je nutne postačujúcou podmienkou prvočíselnosti čísla. Navyše požadujeme, aby bolo efektívne vyhodnotiteľné, či nejaké konkrétne číslo toto tvrdenie spĺňa (t.j. má vlastnosť ním predpísanú). Prvým takým tvrdením, od ktorého sa budú tak trochu odvíjať aj všetky ostatné, o ktorých budeme hovoriť, je Malá Fermatova veta.

Veta 3.1 (Malá Fermatova veta) *Nech p je prvočíslo. Pre ľubovolné celé číslo a platí $a^p \equiv a \pmod{p}$, ak navyše a nie je deliteľné p tak $a^{p-1} \equiv 1 \pmod{p}$.*

Dôkaz Ak a je násobkom p, tvrdenie zrejme platí (a^p rovnako ako a dávajú po delení p zvyšok 0). Predpokladajme teda, že $(a, p) = 1$. Ukážeme, že čísla $0 \cdot a, 1 \cdot a, \cdots, (p-1) \cdot a$ predstavujú úplnú sústavu zvyškov modulo p, teda že z hľadiska zvyškov po delení p sa jedná iba o permutáciu množiny $0, 1, \ldots, p-1$. Keďže uvažovaných čísel je p, stačí nám ukázať, že všetky dávajú po delení p rôzne zvyšky. Vezmime ľubovoľné dve z nich a predpokladajme sporom $i \cdot a \equiv j \cdot a \pmod{p}$. Odtiaľ máme $p \mid (i-j)a$ a keďže $(a, p) = 1$ musí $p \mid (i-j)$. Avšak obe čísla i, j sú menšie ako p, takže tento vzťah nutne implikuje $i = j$. Naozaj teda platí, že čísla $0 \cdot a, 1 \cdot a, \cdots, (p-1) \cdot a$ tvoria úplnú sústavu zvyškov a keď ich medzi sebou (s výnimkou prvého) vynásobíme, musíme dostať ten istý výsledok modulo p ako pri vynásobení čísel $1, \ldots, p-1$. Inými slovami, platí $a \cdot 2a \cdots (p-1)a = a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Pretože číslo $(p-1)!$ nie je deliteľné prvočíslom p, môžeme ním túto kongruenciu krátiť,

čím dostaneme $a^{p-1} \equiv 1 \pmod{p}$.■

Malá Fermatova veta je tvrdenie tvaru $Prime(p) \implies F(p,a)$, kde

$$F(p,a) \iff a^p \equiv a \pmod{p}$$

Voľbou konkrétneho a (ktoré budeme nazývať *bázou*) dostaneme tvrdenie, ktoré môžeme použiť v našom mechanizme. Prakticky to znamená, že budeme testovať prvočíselnosť testovaním platnosti tvrdenia $F(p,a)$. Ak zistíme, že $F(p,a)$ neplatí, potom p celkom iste nie je prvočíslom. Ak však $F(p,a)$ platí, buď budeme mať šťastie a správne ho identifikujeme ako prvočíslo, alebo ho tak označíme mylne. Na prvý pohľad sa síce môže zdať, že umocnenie na $p-$tu nie je o nič jednoduchšie než skúšanie $p-1$ zvyškových tried. Avšak na umocnenie možno použiť metódu, ktorá postupne generuje štvorce získaných zvyškov (teda čísla $a, a^2, a^4, a^8, \ldots$) a zohľadňuje ich podľa cifry v dvojkovom zápise čísla p. Tento postup vedie k algoritmu s logaritmickou časovou náročnosťou, takže preverenie platnosti Fermatovej vety pre konkrétnu bázu je naozaj efektívne.

Definícia 3.1 *Prirodzené číslo p nazývame Fermatovym pseudoprvočíslom v báze a, ak platí $F(p,a)$ a číslo p je zložené.*

Nasledujúca tabuľka obsahuje niektoré z prvých Fermatovych pseudoprvočísel pri malých bázach.

a	Fermatove pseudoprvočísla v báze a
2	341, 561, 645, 1105, 1387, 1729, 1905,...
3	91, 121, 286, 671, 703, 949, 1105, 1541, 1729, ...
4	15, 85, 91, 341, 435, 451, 561, 645, 703, ...
5	4, 124, 217, 561, 781, 1541, 1729, 1891, ...

Názov Fermatove pseudoprvočísla zjednodušíme a budeme ich nazývať jednoducho pseudoprvočísla. Oproti $S-$pseudoprvočíslam (pre naše jednoduché tvrdenie S zavedené vyššie) majú výhodu minimálne v tom, že sú parametrizovateľné číslom a, tzv. bázou. Pre každé a tak dostávame inú množinu pseudoprvočísel, ktoré všetky vyhovujú vyššie uvedenej implikácii. Zaujímavý je na tom fakt, že vhodným výberom báz a a zostrojením prieniku množín pseudoprvočísel v týchto bázach by mohlo byť potenciálne možné obmedziť množinu pseudoprvočísel. Totiž, ak je nejaké číslo pseudoprvočíslom

v niektorej z báz, nemusí byť pseudoprvočíslom v inej. V krajnom prípade by sa nám dokonca mohlo stať, že prienik množín pseudoprvočísel v týchto bázach by bol prázdny, čím by sme získali deterministický test prvočíselnosti (čo je len iný názov pre otočenie našej implikácie). Tento test by spočíval v jednoduchom preverení platnosti $F(p, a)$ postupne pre všetky vybrané bázy. Ak by bol pre všetky úspešný, potom by sme mohli s istotou tvrdiť, že p je prvočíslo. Totiž, ak by p bolo zložené, potom musí byť na základe výsledku pseudoprvočíslom vo všetkých testovaných bázach. Avšak to by znamenalo, že množiny pseudoprvočísel v týchto bázach majú neprázdny prienik, dostávame spor. Také jednoduché to bohužiaľ nie je. Každopádne parametrizácia bázou nám dáva väčšie manipulačné možnosti.

Definícia 3.2 *Nech n je zložené prirodzené číslo. Ak pre všetky prirodzené čísla a platí $a^n \equiv a \pmod{n}$, nazveme n Carmichaelovym číslom.*

Predpokladajme, že existuje nejaké Carmichaelove číslo n podľa predchádzajúcej definície. Potom pre všetky čísla a platí $F(n, a)$, teda číslo n je pseudoprvočíslom pre všetky bázy. Čo to však znamená ? Takéto Carmichaelove číslo leží vo všetkých množinách pseudoprvočísel, a teda určite nevieme vybrať skupinu disjunktných množín. Každá množina pseudoprvočísel obsahuje všetky Carmichaelove čísla. Koľko však takých čísel vôbec existuje ? Pozrime sa najprv na niektoré vlastnosti Carmichaelovych čísel. Skôr než tak urobíme, musíme spomenúť fakt, že v literatúre sa obvykle používa mierne odlišná definícia Carmichaelovych čísel ako sme použili my, viacmenej z technických dôvodov. Preto predtým ako budeme pokračovať, vyslovíme alternatívnu definíciu a ukážeme, že je našej ekvivalentná.

Lema 3.1 (Carmichaelove čísla) *Nech n je zložené prirodzené číslo. Potom n je Carmichaelove číslo práve vtedy, ak pre všetky čísla a nesúdeliteľné s n platí $a^{n-1} \equiv 1 \pmod{n}$.*

Dôkaz Fakt, že Carmichaelovo číslo spĺňa uvedenú podmienku je viacmenej triviálny. Ak totiž pre všetky a platí $a^n \equiv a \pmod{n}$, potom $n \mid a(a^{n-1} - 1)$ a v prípade, že $(a, n) = 1$ zrejme platí $n \mid a^{n-1} - 1$. Zaujímavejšia je druhá implikácia. Predpokladajme, že pre všetky a nesúdeliteľné s n platí $a^{n-1} \equiv 1 \pmod{n}$. Ukážeme, že potom n nemôže byť deliteľné štvorcom žiadneho prvočísla. Predpokladajme sporom, že pre nejaké prvočíslo p platí $p^2 \mid n$. Pretože grupa $Z^*_{p^2}$ je cyklická (tento výsledok algebry niekoľkokrát v tejto

práci použijeme, čitateľ môže jeho dôkaz nájsť napr. v [8]), existuje jej generátor, číslo g, ktoré v nej má rád $p(p-1)$. Označme m súčin všetkých prvočísel, ktoré okrem prvočísla p delia číslo n (ak také neexistujú, bude $m = 1$). Keďže $(p^2, m) = 1$, podľa Čínskej zvyškovej vety má sústava kongruencií $a \equiv g \pmod{p^2}$, $a \equiv 1 \pmod{m}$ riešenie. Toto číslo a je vďaka druhej kongruencii nesúdeliteľné s m, vďaka prvej je nesúdeliteľné s p. Pretože tieto dve čísla obsahujú všetky prvočíselné delitele čísla n, musí platiť $(a, n) = 1$. Odtiaľ podľa predpokladu platí $a^{n-1} \equiv 1 \pmod{n}$, tým skôr aj $a^{n-1} \equiv 1 \pmod{p^2}$. Pretože však rád prvku a v grupe $Z^*_{p^2}$ je $p(p-1)$, musí platiť $p(p-1) \mid n-1$. Avšak $p \mid n$, a teda ani p nemôže deliť $n-1$, čím sme dostali hľadaný spor. Ukázali sme teda, že číslo n je súčinom rôznych prvočísel. Ďalej ukážeme, že pre všetky tieto prvočísla platí $p-1 \mid n-1$. Predpokladajme, že pre nejaký prvočíselný deliteľ p čísla n neplatí $p-1 \mid n-1$. Nech g je generátor cyklickej grupy $(\mathbb{Z}^*_p, \cdot)$. Označme $m = \frac{n}{p}$, podľa Čínskej zvyškovej vety existuje a spĺňajúce kongruencie $a \equiv g \pmod{p}$ a $a \equiv 1 \pmod{m}$. Potom $(a, n) = 1$ a $a^{n-1} \equiv g^{n-1} \pmod{p}$. Ale $g^{n-1} \not\equiv 1 \pmod{p}$, pretože $n-1$ nie je podľa predpokladu deliteľné rádom prvku g, čo je číslo $p-1$. Preto $a^{n-1} \not\equiv 1 \pmod{p}$, a teda nemôže platiť ani $a^{n-1} \equiv 1 \pmod{n}$, čo už je hľadaný spor. Ukážeme teraz, ako z toho, že číslo n je súčinom rôznych prvočísel, pre ktoré platí $p-1 \mid n-1$, plynie, že n je Carmichaelovo číslo. Keďže n nie je deliteľné štvorcom žiadneho z prvočísel, stačí nám ukázať, že platí $a^n \equiv a \pmod{p}$ pre všetky prvočíselné delitele čísla n. Zrejme ak $(a, p) \neq 1$, uvedená kongruencia je triviálne splnená. V opačnom prípade je ekvivalentná kongruencii $a^{n-1} \equiv 1 \pmod{p}$. Podľa Malej Fermatovej vety platí $a^{p-1} \equiv 1 \pmod{p}$ a podľa predpokladu platí $p-1 \mid n-1$. Z týchto dvoch faktov už uvedenú kongruenciu dostávame. ■

Ukázali sme, že definícia Carmichaelovho čísla, ktorá berie do úvahy iba bázy nesúdeliteľné s n je našej definícii ekvivalentná. V skutočnosti sme dokázali oveľa viac, a to platnosť ekvivalentnej podmienky nazývanej Korseltovo kritérium :

Veta 3.2 (Korseltovo kritérium) *Nech n je nepárne zložené číslo. Potom*

a) *Ak n je deliteľné štvorcom nejakého prvočísla, potom n nie je Carmichaelovo číslo.*

b) *Ak n je súčinom rôznych prvočísel, potom je Carmichaelovym číslom*

práve vtedy, ak $p-1 \mid n-1$ *pre všetky prvočíselné delitele* p *čísla* n.

Miernym spresnením získaného výsledku je nasledujúca lema.

Lema 3.2 *Každé Carmichaelovo číslo je súčinom najmenej troch rôznych prvočísel.*

Dôkaz Z Korseltovho kritéria vieme, že Carmichaelovo číslo je súčinom prvočísel, musíme len vylúčiť možnosť, že by bolo súčinom len dvoch rôznych prvočísel. Predpokladajme teda, že $n = pq$, $p < q$. Potom, keby n bolo Carmichaelovo číslo, podľa časti b) Korseltovho kritéria by muselo platiť $n-1 \equiv 0 \pmod{p-1}$. Avšak platí $n-1 = p(q-1+1)-1 = pq-p+p-1 = p(q-1)+p-1 \equiv p-1 \pmod{q-1}$ a $p-1 \not\equiv 0 \pmod{q-1}$, keďže $0 < p-1 < q-1$. To je hľadaný spor, takže tvrdenie platí. ■

Keď Korselt v roku 1899 sformuloval uvedené kritérium, ešte netušil, či v skutočnosti vôbec nejaké Carmichaelove čísla existujú. Presnejšie, sformuloval ho v snahe ich existenciu vyvrátiť. Nielen z úvah naznačených vyššie je totiž jasné, že existencia Carmichaelovych čísel spôsobuje neprekonateľnú prekážku v používaní Fermatovho testu prvočíselnosti. V roku 1910 Robert D. Carmichael našiel prvé takéto číslo, ktorým je 561. Použitím Korseltovho kritéria sa o tom môžeme veľmi jednoducho presvedčiť aj my : platí $561 = 3 \cdot 7 \cdot 11$, pričom $2 \mid 560$, $10 \mid 560$ aj $16 \mid 560$. Jednoduchosť tohoto príkladu pôsobí až prekvapivo keď si uvedomíme, že Korseltovi sa ho nepodarilo nájsť. On sa však zrejme snažil skôr o vyvrátenie jeho existencie. Ďalšie Carmichaelove čísla sú $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, atď. Takmer o storočie neskôr dokázali W.R.Alford, A.Granville a C.Pomerance, že Carmichaelových čísel je nekonečne veľa a našli odhad ich relatívnej početnosti. Pre dostatočne veľké n existuje aspoň $n^{\frac{2}{7}}$ Carmichaelovych čísel nepresahujúcich n. Na druhej strane, pre $x = 10^n$ pre n menšie ako 16 (čo sú možnosti, ktoré boli preverené výpočtom) existuje menej ako $x^{0.337}$ Carmichaelovych čísel menších než n a nezdá sa byť veľmi pravdepodobné, že by ich bolo viac než $x^{\frac{1}{2}}$ pre $x < 10^{100}$. Každopádne tieto fakty znamenajú, že naše úvahy o nemožnosti výberu báz, pre ktoré budú množiny disjunktné sa ukázali opodstatnené. Každá množina pseudoprvočísel určená nejakou bázou obsahuje minimálne všetky Carmichaelove čísla. Avšak možnosť vybrať množinu báz, ktorá určí disjunktné množiny pseudoprvočísel, je veľmi silný

výsledok a Carmichaelove čísla nepredstavujú prekážku iba v jeho dosiahnutí. Najväčším problémom je fakt, že použitím Fermatovho testu ich nemáme šancu odlíšiť od prvočísel, ani keď ho vykonáme pre všetky bázy. V ďalšom si ukážeme, že toto obmedzenie sa dá pri iných testoch prekonať. Pozastavme sa ešte ale na chvíľu pri Fermatovom teste a položme si otázku, ako je to s ostatnými zloženými číslami.

Lema 3.3 *Nech n je prirodzené číslo. Ak existuje číslo a, nesúdeliteľné s n, ktoré nespĺňa kongruenciu $a^{n-1} \equiv 1 \pmod{n}$, potom z čísel nesúdeliteľných s n ju spĺňa najviac polovica.*

Dôkaz Uvažujme grupu $(\mathbb{Z}_n^*, \cdot)$, ukážeme že v rámci nej je množina $F(n) = \{a \mid a^{n-1} \equiv 1 \pmod{n}\}$ podgrupou. Keď si vezmeme ľubovoľné dva prvky $a, b \in F(n)$, platia kongruencie $a^{n-1} \equiv 1 \pmod{n}$ a $b^{n-1} \equiv 1 \pmod{n}$, z ktorých plynie $(ab)^{n-1} = a^{n-1} \cdot b^{n-1} \equiv 1 \pmod{n}$, takže súčin ab patrí do $F(n)$. Ďalej pre ľubovoľné $a \in F(n)$ platí $(a^{-1})^{n-1} = (a^{n-1})^{-1} \equiv 1 \pmod{n}$, takže aj $a^{-1} \in F(n)$. To znamená, že množina $F(n)$ je uzavretá na súčin a inverzné prvky a je teda naozaj podgrupou grupy $\mathbb{Z}_n^*$. Keďže podľa Lagrangeovej vety počet jej prvkov musí deliť počet prvkov grupy, ak nie je táto podgrupa totožná s celou grupou (čo je zaručené existenciou prvku, ktorý do nej nepatrí), má najviac polovičný počet prvkov, čo sme chceli dokázať. ■

Tento výsledok je celkom optimistický a hovorí nám, že ak pri testovaní nenatrafíme na Carmichaelovo číslo, potom šanca, že bude pseudoprvočíslom pri náhodne zvolenej báze je najviac polovičná. Inými slovami, ak zložené číslo nie je Carmichaelovo, potom patrí do najviac polovice z množín pseudoprvočísel vo všetkých bázach. To znamená, že keď vyberieme dostatočný počet báz, bude pomerne veľká šanca, že v niektorej z množín sa toto číslo nebude nachádzať. Nebudeme sa teraz púšťať do presného opisu tohto faktu, lebo situácia v ďalších testoch bude veľmi podobná a navyše nám ju nebudú ďalej komplikovať Carmichaelove čísla. Naše rozprávanie o pseudoprvočíslach zakončíme zaujímavým príkladom, ktorý objavil Lehmer v roku 1950 : Pri definícii, akú sme zvolili, je číslo $161038 = 2 \cdot 73 \cdot 1103$ párnym pseudoprvočíslom v báze 2. V článku [10] sú dokonca spomenuté ďalšie príklady a niektoré pozorovania o párnych pseudoprvočíslach. Ich existencie by sme sa zbavili, ak by sme mierne upravili definíciu pseudoprvočísla, no v podstate ide len o kozmetický problém, ktorý navyše inšpiruje k zaujímavým

úvahám, takže to robiť nebudeme. V ďalšom rozprávaní sa budeme nakoniec aj tak zaoberať inými možnosťami, ako definovať pseudoprvočísla, nakoľko spôsob priamo využívajúci Fermatovu vetu sa ukázal neuspokojivý.

Kapitola 4

Euler - Jacobiho pseudoprvočísla

V snahe zlepšiť naše možnosti otočenia implikácie $Prime(p) \implies S(p)$ a čo najviac ochudobniť množiny pseudoprvočísel, musíme sa pokúsiť nájsť ďalšie netriviálne tvrdenia platné pre prvočísla. Za týmto účelom sa budeme zaoberať pojmom kvadratický zvyšok.

Definícia 4.1 *Nech p je nepárne prvočíslo a a je celé číslo, $(a, p) = 1$. Číslo a nazývame* kvadratickým zvyškom *modulo p ak kongruencia $y^2 \equiv a \pmod{p}$ má riešenie. V opačnom prípade číslo a nazývame kvadratickým nezvyškom modulo p.*

O ľubovoľnom čísle vieme povedať, či je kvadratickým zvyškom, ak vyriešime príslušnú kongruenciu. Keďže sa však vo všeobecnosti nejedná o jednoduchý problém (napríklad skúšanie všetkých zvyškových tried ako najjednoduchší prístup iste nie je pre veľké p prakticky realizovateľné), je na mieste uvažovať o efektívnejšom zisťovaní odpovede na otázku, či je nejaké číslo kvadratickým zvyškom. Skôr než uvedieme tvrdenie, ktoré nám to umožní, zaveďme ešte pojem Legendrovho symbolu.

Definícia 4.2 *Nech p je nepárne prvočíslo. Pre ľubovoľné celé číslo $a \geq 0$ definujeme* Legendrov symbol $\left(\frac{a}{p}\right)$ *nasledujúcim spôsobom:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{ak } a \equiv 0 \pmod{p} \\ 1 & \text{ak } a \text{ je kvadratický zvyšok modulo } p \\ -1 & \text{ak } a \text{ je kvadratický nezvyšok modulo } p \end{cases}$$

Legendrov symbol teda jednoduchým spôsobom vyjadruje skutočnosť, či nejaké číslo je kvadratickým zvyškom podľa príslušného modulu. Nasledujúca veta ukazuje, že hodnoty symbolu nie sú volené náhodne a zároveň poskytuje jednoduchší prístup k nášmu problému.

Veta 4.1 (Eulerovo kritérium) *Nech p je nepárne prvočíslo. Potom*

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

Dôkaz Ak $a \equiv 0 \pmod{p}$, potom zrejme aj $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$, a teda tvrdenie platí. Ak je a kvadratický zvyšok modulo p, potom podľa definície kongruencia $y^2 \equiv a \pmod{p}$ má riešenie. Umocnením tejto kongruencie na $\frac{p-1}{2}$ dostávame $y^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$. Číslo y zjavne nemôže byť deliteľné prvočíslom p, nakoľko by to znamenalo, že a je deliteľné p. Avšak podľa predpokladu a je kvadratický zvyšok, čo je číslo s modulom nesúdeliteľné. To nám umožňuje použiť Malú Fermatovu vetu, podľa ktorej $y^{p-1} \equiv 1 \pmod{p}$. Porovnaním už dostávame $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, čo sme chceli dokázať. Nakoniec predpokladajme, že a je kvadratickým nezvyškom modulo p. Keďže $(a, p) = 1$, opäť podľa Malej Fermatovej vety platí $a^{p-1} \equiv 1 \pmod{p}$, čo možno prepísať na tvar $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$, odkiaľ je zrejmé, že ak neplatí kongruencia $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, potom platí $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Ukážeme teda sporom, že prvá z kongruencií naozaj neplatí. Uvažujme teraz grupu $(\mathbb{Z}_p^*, \cdot)$, keďže sa jedná o multiplikatívnu grupu konečného poľa, je cyklická a teda existuje nejaký jej generátor b. Zrejme môžeme bez ujmy na všeobecnosti predpokladať, že a je prvkom tejto grupy (pričítaním násobku p k nemu sa skúmané vlastnosti nezmenia), preto pre vhodné i platí $a = b^i$. To ďalej znamená, že $(b^i)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Pretože však rád generátora b v grupe je $p - 1$, musí $p - 1$ deliť číslo $i\frac{p-1}{2}$, inými slovami číslo $\frac{i}{2}$ musí byť celé a teda i je párne. Avšak potom číslo $b^{\frac{i}{2}}$ je riešením kongruencie $y^2 \equiv a \pmod{p}$, a teda a je kvadratický zvyšok, čo je hľadaný spor. ■

Vďaka Eulerovmu kritériu získavame pomerne účinný nástroj na vyčíslovanie Legendrovho symbolu. Podobne ako v prípade Fermatovej vety môžeme použiť metódu postupného umocňovania čísla a a zohľadnenia mocnín podľa dvojkového zápisu exponenta, takže tento postup je rovnako

ako použitie Fermatovej vety efektívny. Uvedieme jednoduchý príklad na ilustráciu tohto algoritmu. Majme prvočíslo 643 a zaoberajme sa otázkou, či je číslo 21 kvadratickým zvyškom modulo toto prvočíslo. Zaujíma nás teda hodnota $\left(\frac{21}{643}\right)$. Podľa Eulerovho kritéria nám stačí vypočítať zvyšok čísla 21^{321}. Na to si najprv vyjadríme exponent v dvojkovej sústave $321 = 2^8 + 2^6 + 2^0$ a predpočítame si jednotlivé zvyšky postupným umocňovaním : $21^1 \equiv 21 \pmod{643}$, $21^2 \equiv 441 \pmod{643}$, $21^4 \equiv 295 \pmod{643}$, $21^8 \equiv 220 \pmod{643}$, $21^{16} \equiv 175 \pmod{643}$, $21^{32} \equiv 404 \pmod{643}$, $21^{64} \equiv 537 \pmod{643}$, $21^{128} \equiv 305 \pmod{643}$, $21^{256} \equiv 433 \pmod{643}$. Teraz vyberieme mocniny, ktoré sa nachádzajú v dvojkovom rozklade exponenta a už dostávame $\left(\frac{21}{643}\right) \equiv 21 \cdot 537 \cdot 433 \equiv -1 \pmod{643}$, teda číslo 21 nie je kvadratickým zvyškom modulo 643. Práve Eulerovo kritérium bude pre nás základom ďalšieho typu pseudoprvočísel. Pokúsime sa použiť náš osvedčený postup a pozrieť sa na neho ako na implikáciu $Prime(p) \implies E(p,a)$, kde

$$E(p,a) \iff \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Avšak máme jeden veľký problém - Legendrov symbol nie je definovaný pre $p = 2$ ani pre zložené čísla. Celá implikácia teda má zmysel len ak p je nepárne prvočíslo, a vtedy z pochopiteľných dôvodov nemá pre nás nijaký prínos. Od tohto miesta príjmeme dohodu zaoberať sa výlučne nepárnymi prirodzenými číslami. Na mnohých miestach sa tak naše úvahy technicky zjednodušia a čitateľ iste uzná, že zistiť, či je párne prirodzené číslo prvočíslom, rovnako ako zistiť či je prirodzené číslo párne je problémom, ktorý môžeme s čistým svedomím považovať za triviálny. S faktom, že v definícii sa hovorí iba o nepárnych prvočíslach sa však pokúsime vysporiadať. Jeden z prístupov ako to urobiť by bol nahradiť Legendrov symbol jeho potenciálnymi hodnotami. Takto dostávame nasledujúci pojem.

Definícia 4.3 *Nepárne zložené číslo n nazveme Eulerovym pseudoprvočíslom v báze a, ak platí $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$.*

Takto zavedené Eulerove pseudoprvočísla sú zjavne podmnožinou Fermatových pseudoprvočísel a majú podobné vlastnosti. Existujú tzv. *absolútne Eulerove pseudoprvočísla*, ktoré sú podmnožinou Carmichaelovych čísel a sú Eulerovymi pseudoprvočíslami pre všetky bázy s nimi nesúdeliteľné. Najmenším takýmto Eulerovym pseudoprvočíslom je číslo $1729 = 7 \cdot 13 \cdot 19$. Aj preto tento spôsob riešenia našej komplikácie nie je zrejme najvhodnejší.

Vhodnejším bude zovšeobecniť pojem Legendrovho symbolu na zložené čísla. Na to budeme potrebovať niekoľko pomocných tvrdení.

Veta 4.2 (Gaussova lema) *Nech p je nepárne prvočíslo a $(a,p)=1$. Nech ďalej $\rho_1, \rho_2, \ldots, \rho_{\frac{p-1}{2}}$ sú absolútne najmenšie zvyšky pri delení prvočíslom p utvorené postupne k číslam $1\cdot a, 2\cdot a, \ldots, \frac{p-1}{2}\cdot a$. Nech v je počet záporných čísel v množine $\{\rho_1, \rho_2, \ldots, \rho_{\frac{p-1}{2}}\}$. Potom platí*

$$\left(\frac{a}{p}\right) \equiv (-1)^v \pmod{p}$$

Dôkaz Pre absolútne najmenšie zvyšky platí $-\frac{p}{2} \leq \rho_i < \frac{p}{2}$. Ukážeme, že čísla $|\rho_1|, |\rho_2|, \ldots, |\rho_{\frac{p-1}{2}}|$ sú všetky rôzne. Predpokladajme, že by medzi nimi boli nejaké dve rovnaké, teda nech pre vhodné i, j platí $|\rho_i| = |\rho_j|$. Potom tiež platí $\rho_i^2 = \rho_j^2$ a vzhľadom na to, ako sú definované aj $a^2 \cdot i^2 \equiv a^2 \cdot j^2 \pmod{p}$. Túto kongruenciu možno vzhľadom na podmienku $(a,p)=1$ krátiť číslom a^2, čím dostaneme $i^2 \equiv j^2 \pmod{p}$ alebo $(i-j)\cdot(i+j) \equiv 0 \pmod{p}$. Zrejme $2 < i+j < p-1$, preto musí byť $i \equiv j \pmod{p}$, čo však už znamená $i = j$. Teda čísla $|\rho_1|, |\rho_2|, \ldots, |\rho_{\frac{p-1}{2}}|$ sú všetky rôzne a nadobúdajú $\frac{p-1}{2}$ hodnôt z intervalu $(0, \frac{p}{2})$. Pretože však v tomto intervale je práve $\frac{p-1}{2}$ rôznych celočíselných hodnôt, sú len ich permutáciou. Vynásobme ich teraz medzi sebou a prihliadnime na ich znamienka. Dostaneme rovnosť

$$\rho_1 \cdot \rho_2 \cdots \rho_{\frac{p-1}{2}} = (-1)^v \cdot \left(\frac{p-1}{2}\right)!$$

Avšak z definície jednotlivých zvyškov plynie kongruencia

$$\rho_1 \cdot \rho_2 \cdots \rho_{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$$

Porovnaním máme $a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^v \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$. Vzhľadom na to, že $p \nmid \left(\frac{p-1}{2}\right)!$, môžeme túto kongruenciu krátiť číslom $\left(\frac{p-1}{2}\right)!$, čím dostávame $a^{\frac{p-1}{2}} \equiv (-1)^v \pmod{p}$. Použitím Eulerovho kritéria už odtiaľ plynie dokazovaný vzťah. ■

Teraz nás bude zaujímať, ako sa Legendrov symbol správa v prípade $a = 2$ a niektoré ďalšie, viac menej triviálne identity.

Lema 4.1 *Nech p je nepárne prvočíslo. Potom*

a) *Ak* $a \equiv b \pmod{p}$, *potom* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

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

Dôkaz Vlastnosti a),b) plynú priamo z definície Legendrovho symbolu a vety 4.1. Zaoberajme sa teda vzťahom c). Na výpočet hodnoty $\left(\frac{2}{p}\right)$ použijeme Gaussovu lemu. Aby sme zistili potrebnú hodnotu v, uvažujme, koľko čísel z množiny $S = \{2, 4, \ldots, p-1\}$ sa nachádza v intervale $I = (\frac{p}{2}, p)$. Zrejme tento počet je rovnaký ako počet čísel v prieniku intervalu $\frac{1}{2}I = (\frac{p}{4}, \frac{p}{2})$ s množinou celých čísel. Ak položíme $p = 8c + r$, môžeme písať $|I \cap S| = |\frac{1}{2}I \cap \mathbb{Z}| = |(\frac{p}{4}, \frac{p}{2}) \cap \mathbb{Z}| = |(2c + \frac{r}{4}, 4c + \frac{r}{2}) \cap \mathbb{Z}|$. Túto rovnosť možno ďalej upraviť na kongruenciu ak si uvedomíme, že pričítaním párneho celého čísla k hranici intervalu sa nezmení parita počtu čísel v jeho prieniku s množinou celých čísel. Je teda $|I \cap S| \equiv |(\frac{r}{4}, \frac{r}{2}) \cap \mathbb{Z}| \pmod 2$. Keď teraz použijeme Gaussovu lemu a uvážime, že číslo $\frac{p^2-1}{8}$ je párne pre $r = 1, 7$ a nepárne pre $r = 3, 5$, dostávame už dokazované tvrdenie. ■

Skôr než prejdeme k zovšeobecneniu pojmu Legendrov symbol na zložené čísla, zastavíme sa ešte pri jednej zaujímavej vlastnosti Legendrovho symbolu, nazývanej kvadratická reciprocita. Dokážeme si najprv pomocnú lemu a potom samotné tvrdenie.

Lema 4.2 *Nech p, q sú nepárne prvočísla a $a \in \mathbb{N}$, pričom $p \nmid a, q \nmid a$. Ak platí* $p \equiv q \pmod{4a}$ *alebo* $p \equiv -q \pmod{4a}$, *potom* $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Dôkaz Použijeme Gaussovu lemu na výpočet $\left(\frac{a}{p}\right)$. Na to potrebujeme zistiť paritu počtu čísel z množiny $S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$, ktoré zároveň patria do množiny $I = (\frac{1}{2}p, p) \cup (\frac{3}{2}p, 2p) \cup \ldots \cup ((b - \frac{1}{2})p, bp)$, kde $b = \lfloor \frac{a}{2} \rfloor$. Totiž b je jedno z čísel $\frac{a}{2}$, $\frac{a-1}{2}$, a teda v prvom prípade $bp = \frac{1}{2}ap > \frac{p-1}{2}a$, v druhom prípade $bp + \frac{p}{2} = \frac{1}{2}ap > \frac{p-1}{2}a$, čo znamená, že žiadny prvok množiny S so záporným absolútne najmenším zvyškom modulo p neleží mimo množiny

I (interval $((b-\frac{1}{2})p, bp)$ bol posledný, ktorý mohol obsahovať taký prvok). Navyše žiadne z krajných bodov intervalov v I, ktoré sú celými číslami, nepatria do množiny S, keďže sú všetky deliteľné prvočíslom p, zatiaľ čo prvky množiny S nie sú prvočíslom p deliteľné. Po vydelení číslom a ľahko nahliadneme, že platí $|S \cap I| = |\mathbb{Z} \cap \frac{1}{a}I|$, kde $\frac{1}{a}I = (\frac{p}{2a}, \frac{p}{a}) \cup (\frac{3p}{2a}, \frac{2p}{a}) \cup \ldots \cup (\frac{(2b-1)p}{a}, \frac{bp}{a})$. Položíme teraz $p = 4ac+r$ a označíme $J = (\frac{r}{2a}, \frac{r}{a}) \cup (\frac{3r}{2a}, \frac{2r}{a}) \cup \ldots \cup (\frac{(2b-1)r}{a}, \frac{br}{a})$. Rozdiel medzi množinami $\frac{1}{a}I$ a J je len v tom, že druhá z nich má všetky krajné body intervalov posunuté o číslo $2c$. To však nezmení počet čísel v prieniku s množinou celých čísel, platí teda $|\mathbb{Z} \cap \frac{1}{a}I| = |\mathbb{Z} \cap J|$. Avšak rovnakú konštrukciu možno vykonať aj pre prvočíslo q. Inými slovami, keďže parita čísla $|S \cap I|$, a tým pádom aj výsledok $\left(\frac{a}{p}\right)$, závisela len od zvyšku čísla p po delení $4a$ a teda analogickým postupom by sme zistili že $\left(\frac{a}{q}\right)$ závisí len od zvyšku čísla q po delení $4a$, platí v prípade $p \equiv q \pmod{4a}$ naozaj rovnosť $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Uvažujme teraz prípad $p \equiv -q \pmod{4a}$. Jediná zmena v dôkaze je, že číslo r nahradí číslo $4a - r$. Tým sa množina $\frac{1}{a}I$ zmení na množinu $K = (2-\frac{r}{2a}, 4-\frac{r}{a}) \cup (6-\frac{3r}{2a}, 8-\frac{2r}{a}) \cup \ldots \cup (4b-2-\frac{(2b-1)r}{2a}, 4b-\frac{br}{a})$. Teda K predstavuje množinu, ktorá vznikne z množiny $-\frac{1}{a}I$ pričítaním párnych celých čísel k hraniciam intervalov. Z toho však plynie $|K \cap \mathbb{Z}| \equiv |\frac{1}{a}I \cap \mathbb{Z}| \pmod 2$, odkiaľ už $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, čím je dôkaz ukončený. ■

Veta 4.3 (Zákon kvadratickej reciprocity) *Nech p, q sú rôzne nepárne prvočísla. Potom $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.*

Dôkaz Keďže p, q sú nepárne prvočísla, dávajú po delení štyrmi zvyšky 1 alebo 3. Každopádne platí jeden zo vzťahov $p \equiv q \pmod 4$, $p \equiv -q \pmod 4$. Rozoberme oba prípady. Nech teda najprv $p \equiv q \pmod 4$, potom nech bez ujmy na všeobecnosti $p > q$ a môžeme písať $p - q = 4a$ pre vhodné $a \in \mathbb{N}$, teda $p = 4a + q$. Ďalej platí

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$$

a

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right)$$

Podľa lemy je $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, keďže $p \equiv q \pmod{4a}$. To však znamená že

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

Pritom posledná rovnosť plynie zo skutočnosti, že číslo $\frac{q-1}{2}$ je párne práve vtedy, keď je párne číslo $\frac{p-1}{2}$. Nech teraz $p \equiv -q \pmod{4}$. Položme $p + q = 4a$ pre vhodné a. Dostávame postupne

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right) \text{ a } \left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right)$$

Z lemy však plynie $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, čo znamená že $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Keďže v tomto prípade $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1$, je tým dôkaz ukončený. ■

Na ilustráciu užitočnosti dokázaných tvrdení sa vrátime k príkladu, ktorý sme riešili použitím Eulerovho kritéria. Zaujímala nás vtedy hodnota Legendrovho symbolu $\left(\frac{21}{643}\right)$. Túto môžeme teraz vypočítať inak. Podľa lemy 4.1 môžeme písať $\left(\frac{21}{643}\right) = \left(\frac{7}{643}\right) \cdot \left(\frac{3}{643}\right)$. Obidva symboly na pravej strane môžeme zjednodušiť použitím zákona kvadratickej reciprocity. Dostaneme tak $\left(\frac{21}{643}\right) = -\left(\frac{643}{7}\right) \cdot -\left(\frac{643}{3}\right) = \left(\frac{6}{7}\right)\left(\frac{1}{3}\right)$. Tu už jednoduchým dopočítaním napríklad aj použitím Eulerovho kritéria dostaneme $\left(\frac{6}{7}\right) \cdot \left(\frac{1}{3}\right) = (-1) \cdot 1 = -1$. Dostali sme ten istý výsledok ako priamym použitím Eulerovho kritéria a dostali sme sa k nemu oveľa rýchlejšie.

V tejto chvíli máme teda v rukách všetky nástroje potrebné na efektívnu manipuláciu s Legendrovym symbolom a môžeme pristúpiť k jeho zovšeobecneniu. Legendrov symbol $\left(\frac{a}{p}\right)$ sme definovali len ak p je prvočíslo. Prirodzený spôsob, ako túto definíciu rozšíriť aj na zložené číslo ukazuje nasledujúca definícia.

Definícia 4.4 *Nech n je nepárne prirodzené číslo, ktorého prvočíselný rozklad je $n = p_1^{e_1} \dots p_k^{e_k}$. Nech $a \geq 0$ je celé číslo.* Jacobiho symbol $\left(\frac{a}{n}\right)$ *je definovaný nasledovne:*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

Takto zavedený Jacobiho symbol má bohužiaľ niekoľko nevýhod. Jednou z nich je, že už nám neposkytuje informáciu, ktorú niesol Legendrov symbol, a teda nehovorí, či je príslušné číslo a kvadratickým zvyškom modulo n. Je to tak preto, že Jacobiho symbol je súčinom Legendrových symbolov, a keď párny počet z nich má hodnotu -1, výsledok napriek tomu bude 1. Takéto číslo je kvadratickým nezvyškom modulo niekoľko prvočíselných faktorov a teda nemôže byť kvadratickým zvyškom modulo ich násobok. Veľmi jednoduchý príklad, ktorý to ilustruje, je $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$. Hodnota tohto Jacobiho symbolu je síce 1, no číslo 2 je kvadratickým nezvyškom modulo 3 aj 5, a teda nemôže byť kvadratickým zvyškom modulo 15. Napriek tomu, že Jacobiho symbol nám nenesie informáciu ktorá motivovala vznik Legendrovho symbolu, vďaka jeho definícii teraz máme možnosť zaviesť nový typ pseudoprvočísel na základe zovšeobecneného Eulerovho kritéria. Pretože pre prvočísla sa Legendrov a Jacobiho symbol zhodujú, môžeme ich jednoducho v tomto tvrdení zameniť. Dostaneme tak predikát

$$E(p,a) \iff \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

o ktorom už má zmysel uvažovať pre všetky nepárne čísla, s čím sa uspokojíme a zavedieme nový pojem.

Definícia 4.5 *Nepárne prirodzené zložené číslo n nazývame Euler-Jacobiho pseudoprvočíslom v báze a, ak a a n sú nesúdeliteľné a platí $E(n,a)$.*

V nasledujúcej tabuľke uvádzame niekoľko prvých Euler-Jacobiho pseudoprvočísel v malých bázach :

a	Euler-Jacobiho pseudoprvočísla v báze a
2	561, 1105, 1729, 1905, 2047, 2465, 3277, ...
3	121, 1729, 2821, 7381, 8401, ...
5	781, 1541, 1729, 5461, 5611, 6601, 7449, ...
7	25, 703, 2101, 2353, 2465, 3277, ...

Úspešne sa nám podarilo založiť na Eulerovom kritériu pojem pseudoprvočísel, ktorými sa môžeme ďalej zaoberať, no predsa len sa musíme pri spôsobe, ktorý sme použili, ešte chvíľu pozastaviť. Prirodzená požiadavka na vhodné tvrdenie S do našej šablóny $Prime(p) \implies S(p)$ je aby bolo možné rozhodnúť o platnosti tvrdenia S efektívnejšie ako o tvrdení $Prime(p)$.

Problém je v tom, že Jacobiho symbol je definovaný ako súčin Legendrovych symbolov pre prvočinitele čísla n. Samozrejme keby sme poznali prvočinitele n, asi by otázka či je n prvočíslo bola pomerne bezpredmetná. Naštastie však existuje spôsob, ako Jacobiho symbol počítať efektívne bez nutnej priamej znalosti prvočíselného rozkladu čísla n. Tento spôsob využíva zovšeobecnenie vlastností Legendrovho symbolu, ktoré sme si už dokázali. Nasledujúce tvrdenia nám teda umožnia rýchlu enumeráciu Jacobiho symbolu a potom sa budeme môcť ďalej zaoberať vlastnosťami Euler-Jacobiho pseudoprvočísel.

Lema 4.3 *Nech n je nepárne prirodzené číslo. Potom*

a) *Ak $a \equiv b \pmod{n}$, potom $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*

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

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

Dôkaz Nech $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ je prvočíselný rozklad čísla n. Z definície Jacobiho symbolu máme $\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$, $\left(\frac{b}{n}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i}$. Ak platí $a \equiv b \pmod{n}$, potom pre všetky p_i, keďže delia n, platí tiež $a \equiv b \pmod{p_i}$. Podľa lemy 4.1 však z toho vyplýva aj $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, odkiaľ už plynie tvrdenie a). Takisto pretože podľa lemy 4.1 je $\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right) \cdot \left(\frac{b}{p_i}\right)$, platí aj $\prod_{i=1}^{k} \left(\frac{ab}{p_i}\right)^{e_i} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} \cdot \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i}$, čo implikuje tvrdenie b). Na dôkaz tvrdenia c) si uvedomme, že z lemy 4.1 plynie vzťah $\left(\frac{2}{n}\right) = \prod_{i=1}^{k} \left(\frac{2}{p_i}\right)^{e_i} = \prod_{i=1}^{k} (-1)^{e_i \frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{k} e_i \frac{p_i^2-1}{8}}$. Dokazovaná rovnosť je teda ekvivalentná s kongruenciou $\sum_{i=1}^{k} e_i \frac{p_i^2-1}{8} \equiv \frac{n^2-1}{8} \pmod{2}$, alebo $\sum_{i=1}^{k} e_i (p_i^2 - 1) \equiv n^2 - 1 \pmod{16}$. Štvorec nepárneho čísla p môže dávať po delení 16 iba 2 rôzne zvyšky, a to 1, ak $p \equiv 1, -1 \pmod{8}$ alebo 9, ak $p \equiv 3, 5 \pmod{8}$. Ďalej platí, že ak nejaké nepárne číslo p je súčinom niekoľkých nepárnych čísel, z ktorých ľubovoľný počet dáva po delení 8 zvyšky 1,-1 a párny, resp. nepárny počet dáva zvyšky 3,5, potom p dáva po delení 8 zvyšky 1,-1, resp. 3,5. (Je totiž $3 \cdot 5 \equiv -1 \pmod{8}$ a $3^2 \equiv 5^2 \equiv 1 \pmod{8}$). Tieto fakty aplikujeme na náš problém. Zrejme ak prvočíslo p_i dáva po delení 8 zvyšky 1,-1 alebo má párny exponent e_i, je výraz $e_i(p_i^2 - 1)$ deliteľný 16, ak dáva niektorý zo zvyškov 3,5 a exponent e_i je nepárny, potom dáva tento výraz zvyšok 8 po

delení 16. Inými slovami, platí $\sum_{i=1}^{k} e_i(p_i^2-1) \equiv 8u \pmod{16}$, kde u je počet prvočísel s nepárnym exponentom a jedným zo zvyškov 3,5 v rozklade čísla n. Na druhej strane, ak je tento počet u párny, znamená to podľa vyššie uvedeného, že $n^2 \equiv 1 \pmod{16}$, ak je u nepárne platí $n^2 \equiv 9 \pmod{16}$. Porovnaním pre oba prípady už dostávame dokazovanú kongruenciu. ■

Lema 4.4 *Nech m, n sú nesúdeliteľné nepárne prirodzené čísla. Potom*

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$$

Dôkaz Toto tvrdenie je zovšeobecnením vety o kvadratickej reciprocite a predstavuje najdôležitejší nástroj umožňujúci praktický výpočet Jacobiho symbolu. Nech $m = p_1 \dots p_r$ a $n = q_1 \dots q_s$. S použitím lemy 4.3 a vety 4.3 dostávame $\left(\frac{m}{n}\right) = \prod_{j=1}^{r} \prod_{k=1}^{s} \left(\frac{p_j}{q_k}\right) = \prod_{j=1}^{r} \prod_{k=1}^{s} \epsilon_{j,k} \left(\frac{q_k}{p_j}\right) = (-1)^u \left(\frac{n}{m}\right)$, kde $\epsilon_{j,k}$ je -1 ak $p_j \equiv q_k \equiv 3 \pmod 4$ a 1 v opačnom prípade, a teda u je počet párov (j, k) takých, pre ktoré $\epsilon_{j,k} = -1$. Avšak $u = ab$, kde a je počet prvočísel p_j dávajúcich zvyšok 3 po delení 4 a b je počet prvočísel q_k dávajúcich zvyšok 3 po delení 4. Potom $m \equiv 3^a \equiv (-1)^a \pmod 4$ a $n \equiv 3^b \equiv (-1)^b \pmod 4$. Ak sú obe čísla a,b nepárne, potom $(-1)^u = -1$, v opačnom prípade $(-1)^u = 1$. Platí teda $(-1)^u = -1$ práve vtedy, ak $m \equiv n \equiv 3 \pmod 4$. V tomto prípade je $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$, inak platí $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$. Ľahko nahliadneme, že tento fakt je ekvivalentný s dokazovaným tvrdením. ■

Použitím predchádzajúcich tvrdení vieme v polynomiálnom čase (od veľkosti vstupu) enumerovať Jacobiho symbol, podobne ako sme to robili v prípade Legendrovho symbolu, pričom nepotrebujeme vedieť nič o prvočíselnom rozklade čísla n. Ukázali sme teda, že Euler-Jacobiho pseudoprvočísla spĺňajú všetky predpoklady, ktoré po nich požadujeme. My však samozrejme chceme viac - chceme, aby množiny Euler-Jacobiho pseudoprvočísel boli v istom zmysle chudobnejšie ako množiny Fermatovych. Navyše sa chceme zbaviť ich spoločného prieniku v podobe Carmichaelovych čísel a ukázať, že v tomto prípade žiadne podobné čísla neexistujú. O tom, že to tak naozaj je, hovorí nasledujúca veta.

Veta 4.4 *Nech n je nepárne zložené číslo. Potom existuje aspoň jedno*

prirodzené číslo a, $2 \leq a \leq n-1$, nesúdeliteľné s n, pre ktoré neplatí kongruencia $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.

Dôkaz Predpokladajme, že pre všetky prirodzené čísla a menšie ako n nesúdeliteľné s n platí $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$. Umocnením tejto kongruencie dostávame pre $(a,n)=1$ vzťah $a^{n-1} \equiv \left(\frac{a}{n}\right)^2 \equiv (\pm 1)^2 \equiv 1 \pmod{n}$. Odtiaľ plynie, že n je Carmichaelovo číslo. Preto podľa lemy 3.2 musí byť súčinom rôznych prvočísel a môžeme písať $n = q_1 \dots q_r$, kde $q_1, \dots, q_r$ sú navzájom rôzne nepárne prvočísla. Nech u je kvadratický nezvyšok modulo q_1. Podľa Čínskej zvyškovej vety existuje a, pre ktoré platí $a \equiv u \pmod{q_1}$ a $a \equiv 1 \pmod{q_2 \dots q_r}$. Avšak pre takéto a platí $\left(\frac{a}{n}\right) = \left(\frac{a}{q_1 \dots q_r}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2 \dots q_r}\right) = \left(\frac{u}{q_1}\right)\left(\frac{1}{q_2 \dots q_r}\right) = -1$. Na druhej strane zrejme $a^{\frac{n-1}{2}} \equiv 1 \pmod{q_2 \dots q_r}$, takže nemôže platiť $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Preto neplatí ani $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, a teda existencia čísla a je v spore s predpokladom. Tvrdenie preto platí. ■

Každé zložené číslo teda nepatrí aspoň do jednej z množín Euler-Jacobiho pseudoprvočísel. Uvažujme teraz prvky $a \in \mathbb{Z}_n^*$ a špeciálne označíme $G(n)$ množinu tých, ktoré spĺňajú kongruenciu, napriek tomu že n nie je nutne prvočíslo. Teda $G(n) = \{a \in \mathbb{Z}_n^* | \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}\}$. Ukážeme, že $G(n)$ je podgrupou grupy $(\mathbb{Z}_n^*, \cdot)$. Pre ľubovoľné dva prvky $a_1, a_2 \in G(n)$ totiž platí $\left(\frac{a_1 \cdot a_2}{n}\right) = \left(\frac{a_1}{n}\right) \cdot \left(\frac{a_2}{n}\right) \equiv a_1^{\frac{n-1}{2}} \cdot a_2^{\frac{n-1}{2}} \pmod{n}$, teda $G(n)$ je uzavretá na súčin. Rovnako je uzavretá na inverzné prvky, nakoľko pre ľubovoľné $a \in G(n)$ platí $\left(\frac{a}{n}\right) \cdot \left(\frac{a^{-1}}{n}\right) = 1$, preto $\left(\frac{a^{-1}}{n}\right) \equiv (a^{\frac{n-1}{2}})^{-1} \equiv (a^{-1})^{\frac{n-1}{2}} \pmod{n}$. Podľa Lagrangeovej vety teda stačí, aby existovalo jedno a ktoré do $G(n)$ nepatrí a už ich tam bude patriť najviac polovica zo $\mathbb{Z}_n^*$. My sme v predchádzajúcej vete také a našli, a teda už vieme, že každé zložené číslo patrí najviac do polovice množín pseudoprvočísel vo všetkých bázach. Na tomto fakte je založený tzv. Solovay-Strassenov algoritmus, ktorý testuje prvočíselnosť čísla n tak, že postupne volí rôzne náhodné bázy a a zisťuje platnosť tvrdenia $E(n,a)$. My sme práve ukázali, že pravdepodobnosť, že sa Solovay-Strassenov algoritmus pomýli a o zloženom čísle prehlási po m opakovaniach, že je to prvočíslo, je menšia než 2^{-m}. Ak budeme chcieť použitím tohto algoritmu generovať prvočísla tak, že zvolíme náhodné číslo a otestujeme ho, potom vstupuje do hry otázka rozvrstvenia prvočísel a zaujíma nás trochu zložitejšia otázka, ktorú vyriešime v nasledujúcej vete.

Veta 4.5 *Pravdepodobnosť omylu pri generovaní prvočísel pomocou Solovay-Strassenovho algoritmu, t.j. pravdepodobnosť, že číslo n je zložené, napriek tomu, že algoritmus po m opakovaniach o náhodne zvolenom čísle prehlásil, že sa jedná o prvočíslo, je najviac* $\frac{\ln n-2}{\ln n-2+2^{m+1}}$.

Dôkaz Označme a udalosť *"Náhodné nepárne prirodzené číslo n príslušnej veľkosti je zložené"*, zrejme $\overline{a}$ je potom *"Náhodné nepárne prirodzené číslo n je prvočíslo"*, ďalej nech b je udalosť *"Solovay-Strassenov algoritmus vyhlási o čísle n že je prvočíslo m-krát po sebe"*. Z predchádzajúcich úvah vieme, že platí $P(b \mid a) \leq 2^{-m}$. Na výpočet pravdepodobnosti $P(a \mid b)$, ktorá nás zaujíma, použijeme Bayesovu vetu. Aby sme tak mohli urobiť, potrebujeme najprv poznať pravdepodobnosť udalosti a. Nech $N \leq n \leq 2N$. Podľa prvočíselnej vety je počet prvočísel medzi N a $2N$ približne $\frac{2N}{\ln 2N} - \frac{N}{\ln N} \approx \frac{N}{\ln N} \approx \frac{n}{\ln n}$. Keďže medzi číslami N a $2N$ je približne $\frac{N}{2} \approx \frac{n}{2}$ nepárnych prirodzených čísel, môžeme použiť približnú hodnotu $P(a) \approx 1 - \frac{2}{\ln n}$. Podľa Bayesovej vety teda máme $P(a \mid b) = \frac{P(b|a)P(a)}{P(b)} = \frac{P(b|a)P(a)}{P(b|a)P(a)+P(b|\overline{a})P(\overline{a})} \approx \frac{P(b|a)(1-\frac{2}{\ln n})}{P(b|a)(1-\frac{2}{\ln n})+\frac{2}{\ln n}} = \frac{P(b|a)(\ln n-2)}{P(b|a)(\ln n-2)+2} \leq \frac{2^{-m}(\ln n-2)}{2^{-m}(\ln n-2)+2} = \frac{\ln n-2}{\ln n-2+2^{m+1}}$, čo predstavuje požadované ohraničenie. ■

Predchádzajúce tvrdenie je zavŕšením nášho úsilia v oblasti Euler-Jacobiho pseudoprvočísel. Podarilo sa nám zostrojiť polynomiálny algoritmus na testovanie prvočíselnosti, ktorý má určitú pravdepodobnosť omylu, avšak táto je pre dostatočne veľký počet opakovaní taká malá, že z praktického hľadiska môžeme považovať jeho výsledky za takmer isté. Ukázali sme, že tento algoritmus na rozdiel od algoritmu Fermatovho nemá slabinu v existencii nerozlíšiteľných pseudoprvočísel. Jeho najväčšou slabinou (najmä z teoretického hľadiska) je jeho pravdepodobnostný charakter. Napriek tomuto nedostatku má význam, minimálne kvôli praktických aplikáciám, zaoberať sa pravdepodobnostnými algoritmami. V ďalšej kapitole ukážeme ešte jeden z nich a podarí sa nám tiež neistotu úspechu algoritmu nahradiť neistotou platnosti Riemannovej hypotézy, čo pre ľudí presvedčených o jej platnosti znamená odstránenie nedostatku, pre ostatných aspoň rozšírenie možností. Každopádne už len súvislosti, ktorými sa budeme zaoberať si zasluhujú pozornosť.

Kapitola 5

Silné pseudoprvočísla

V tejto chvíli sa v našom rozprávaní dostávame k najsofistikovanejšej voľbe predikátu S v modeli $S-$pseudoprvočísel, akým sa budeme zaoberať. Predstavuje akýsi vrchol v hierarchii tvrdení a zovšeobecnenie našich predchádzajúcich skúseností. Nebude však opäť založený na žiadnych náročných vlastnostiach prvočísel, dokonca sa vrátime o krok späť a opäť použijeme iba Malú Fermatovu vetu, tentokrát trochu v elegantnejšej podobe.

Lema 5.1 *Nech p je prvočíslo, a nech platí $p = 2^s t$, kde t je nepárne prirodzené číslo (t.j. 2^s je najvyššia mocnina dvojky, ktorá delí číslo p). Potom pre ľubovoľné prirodzené číslo a, ktoré nie je deliteľné prvočíslom p buď platí $a^t \equiv 1 \pmod{p}$, alebo existuje číslo $0 \leq i \leq s-1$, pre ktoré platí $a^{2^i t} \equiv -1 \pmod{p}$.*

Dôkaz Lema je pomerne jednoduchým dôsledkom Malej Fermatovej vety. Stačí si totiž uvedomiť, že podľa nej platí $a^{2^s t} \equiv 1 \pmod{p}$, čo môžeme prepísať ako $(a^{2^{s-1}t} - 1)(a^{2^{s-1}t} + 1) \equiv 0 \pmod{p}$. Pretože p je prvočíslo, ak delí súčin, znamená to, že delí aspoň jedného súčiniteľa. Ak teda neplatí $a^{2^{s-1}t} \equiv -1 \pmod{p}$, potom celkom určite platí $a^{2^{s-1}t} \equiv 1 \pmod{p}$. Avšak tento vzťah opäť možno prepísať na tvar $(a^{2^{s-2}t} - 1)(a^{2^{s-2}t} + 1) \equiv 0 \pmod{p}$ (pre s>1, inak sme skončili už predtým, keďže platilo $a^t \equiv 1 \pmod{p}$). Z neho analogicky buď dôkaz ukončíme alebo pokračujeme ďalej tým istým postupom. Ak sa nám nikde dôkaz nepodarí ukončiť, dostaneme sa až k tomu, že platí $a^t \equiv 1 \pmod{p}$, kde tiež dostávame jednu z dokazovaných možností. Tvrdenie teda platí. ■.

Lema 5.1 nám podobne ako príslušné tvrdenia v predchádzajúcich kapitolách poskytuje možnosť voľby tvrdenia S do modelu $S-$pseudoprvočísel, nakoľko má správnu formu implikácie $Prime(p) \implies R(p,a)$, kde

$$R(p,a) \iff a^t \equiv 1 \pmod{p} \vee (\exists i \in (0, s-1))a^{2^i t} \equiv -1 \pmod{p},$$

ak predpokladáme že $p = 2^s t$ a t je nepárne. Navyše je podobne ako v prípade predikátov F a E parametrizovaná parametrom a, ktorý budeme nazývať, ako inak, bázou. Analogicky si zavedieme definíciu silných pseudoprvočísel (prečo ich tak odvážne nazývame silnými, pokúsime sa opísať v tejto kapitole).

Definícia 5.1 *Nech n je nepárne zložené číslo, a ľubovoľné prirodzené číslo a nech platí $R(n,a)$. Potom n nazývame silným pseudoprvočíslom v báze a.*

V nasledujúcej tabuľke uvádzame niekoľko prvých silných pseudoprvočísel v malých bázach :

a	silné pseudoprvočísla v báze a
2	2047, 3277, 4033, 4681, 8321, ...
3	121, 703, 1891, 3281, 8401, 8911, ...
4	341, 1387, 2047, 3277, 4033, 4371, ...
5	781, 1541, 5461, 5611, 7813, ...

Podobne ako v predchádzajúcich prípadoch nás bude zaujímať, akú váhu má skutočnosť, že číslo n spĺňa predikát $R(n,a)$ pre nejakú bázu a. Inými slovami, ako veľa vlastne silných pseudoprvočísel existuje. Zavedieme si navyše ešte jeden pojem, ktorý bude hrať významnú rolu v našich úvahách.

Definícia 5.2 *Nech n je nepárne zložené číslo. Číslo a nazveme* svedkom, *ak platí $1 \leq a \leq n-1$ a číslo n nie je silným pseudoprvočíslom v báze a.*

Ak sa pozeráme na vec z algoritmického pohľadu postupného preverovania platnosti predikátu $R(n,a)$ pre rôzne bázy a, potom svedok je báza, na ktorej naše skúšanie zlyhá a umožní nám s istotou prehlásiť, že testované číslo je zložené. Existencia pseudoprvočísel by nám až tak nevadila, keby každé konkrétne číslo bolo pseudoprvočíslom len v malom počte báz, zatiaľ čo všetky ostatné bázy by boli svedkami. Potom by sme totiž mali veľkú pravdepodobnosť, že sa nám po malom počte opakovaní preverovania predikátu R podarí číslo "usvedčiť". Na tejto myšlienke, ktorá nakoniec bola použitá aj v predchádzajúcich kapitolách, je založený tzv. Rabin-Millerov

test prvočíselnosti. Tento test nesie pomerne paradoxné meno, nakoľko pôvodným autorom myšlienky silných pseudoprvočísel a využitia lemy 5.1 na testovanie prvočíselnosti bol Artjuhov (v práci [2]), ktorému sa nepodarilo myšlienku presadiť a až o desaťročie neskôr ju spopularizoval Selfridge. Miller je autorom článku [11], z ktorého čerpá táto práca a v ktorom sa zaoberá súvislosťou Riemannovej hypotézy s možným deterministickým rozšírením testu. Rabin sa zaslúžil o pravdepodobnostnú variantu testu (v prácach [13] a [14]), o ktorej práve rozprávame. V skutočnosti nezávisle od neho k rovnakému výsledku prišiel Monier (v práci [12]), no okolnosti spôsobili, že Rabinov výsledok sa podarilo spopularizovať výraznejšie. Nech už história tvrdí čokoľvek, tento test vo všetkých podobách je veľmi poučným využitím mnohých dôsledkov teórie čísel. My sa budeme ďalej zaoberať ohraničením počtu báz, pre ktoré môže byť číslo silným pseudoprvočíslom.

Lema 5.2 *Nech n je nepárne prirodzené číslo a nech 2^s je najvyššia mocnina dvojky, ktorá delí $n-1$ (t.j. platí $n-1 = 2^s t$, kde t je nepárne prirodzené číslo). Nech $\nu(n)$ je najväčšie prirodzené číslo, ktoré spĺňa $2^{\nu(n)} \mid p-1$ pre každé prvočíslo p, ktoré delí n. Ak n je silné pseudoprvočíslo v báze a, potom platí jedna z kongruencií $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$, $a^{2^{\nu(n)-1}t} \equiv -1 \pmod{n}$.*

Dôkaz Fakt, že n je silné pseudoprvočíslo v báze a znamená, že muselo prejsť testom a teda predovšetkým buď platí $a^t \equiv 1 \pmod{n}$, alebo pre nejaké i z množiny $\{0, \ldots, s-1\}$ platí $a^{2^i t} \equiv -1 \pmod{n}$. V prvom prípade je triviálne splnená kongruencia $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$ a nie je čo dokazovať. Zaoberajme sa teda druhým prípadom a predpokladajme, že máme nejaké prirodzené číslo i, ktoré spĺňa uvedenú kongruenciu. Vezmime si navyše ľubovoľné prvočíslo p, ktoré delí číslo n. Keďže p delí n, plati okrem vyššie uvedenej kongruencie aj $a^{2^i t} \equiv -1 \pmod{p}$ a tiež $a^{2^{i+1}t} \equiv 1 \pmod{p}$. Ak označíme r rád prvku a v grupe Z_p^*, potom zrejme z predchádzajúcich dvoch kongruencií dostávame, že $r \mid 2^{i+1}t$ a $r \nmid 2^i t$. Rád je totiž najmenšie číslo s vlastnosťou $a^r \equiv 1 \pmod{p}$, ktoré delí všetky ostatné čísla s touto vlastnosťou. Z posledných dvoch vzťahov vidno, že číslo r nemôže obsahovať vo svojom prvočíselnom rozklade dvojku v inej ako (i+1)-tej mocnine - keby obsahovalo vo vyššej, nemôže platiť $r \mid 2^{i+1}t$ (pripomeňme, že t je nepárne číslo), keby naopak v nižšej, muselo by platiť aj $r \mid 2^i t$. Z Malej Fermatovej vety vieme, že platí $a^{p-1} \equiv 1 \pmod{p}$. Opäť použijeme argument, že číslo r ako rád prvku a musí deliť všetky čísla s touto vlastnosťou, a teda platí $r \mid p-1$. Odtiaľ už podľa vyššie uvedého máme, že $2^{i+1} \mid p-1$. Pretože táto

úvaha nijako nezávisela od výberu konkrétneho prvočíselného deliteľa p čísla n, dá sa urobiť pre každý z nich. To ale znamená, že $2^{i+1} \mid p-1$ pre každé prvočíslo p, ktoré delí n. Podľa zadania $\nu(n)$ je najväčšie číslo s takouto vlastnosťou, a preto $i+1 \leq \nu(n)$. Rozoberme teraz dva prípady - najprv nech $i+1 = \nu(n)$. Vtedy $a^{2^{\nu(n)-1}t} = a^{2^i t} \equiv -1 \pmod{p}$, takže je splnená prvá z kongruencií zo zadania. V druhom prípade, teda ak $i+1 < \nu(n)$, môžeme písať $\nu(n) - 1 = i + d$ pre nejaké vhodné kladné celé číslo d. Vďaka tomu platí $a^{2^{\nu(n)-1}t} = a^{2^{i+d}t} = (a^{2^i t})^{2^d} \equiv (-1)^{2^d} \equiv 1 \pmod{p}$. V tomto prípade je teda splnená druhá kongruencia zo zadania a dôkaz je hotový. ■

Lema 5.3 *Nech n je nepárne prirodzené číslo. Označme $\overline{S}(n)$ nasledovne definovanú množinu čísel :* $\{0 \leq a < n \mid a^{2^{\nu(n)-1}t} \equiv 1 \pmod{p} \vee a^{2^{\nu(n)-1}t} \equiv -1 \pmod{p}\}$*, kde $\nu(n)$ má rovnaký význam ako v predchádzajúcej leme. Ďalej označme $\omega(n)$ počet rôznych prvočísel, ktoré delia číslo n. Potom platí*

$$|\overline{S}(n)| = 2 \cdot 2^{(\nu(n)-1)\omega(n)} \prod_{p|n} (t, p-1)$$

Dôkaz Nech číslo n má prvočíselný rozklad $n = \prod_{i=1}^{\omega(n)} p_i^{\alpha_i}$ (podľa zadania je v ňom práve $\omega(n)$ prvočísel). Rozdelíme si množinu $\overline{S}(n)$ na dve disjunktné časti $\overline{S}(n) = \overline{S_1}(n) \cup \overline{S_2}(n)$, kde $\overline{S_1}(n) = \{0 \leq a < n \mid a^{2^{\nu(n)-1}t} \equiv 1 \pmod{p}\}$ a $\overline{S_2}(n) = \{0 \leq a < n \mid a^{2^{\nu(n)-1}t} \equiv -1 \pmod{p}\}$. Najprv sa budeme zaoberať prvou z nich. Zaujíma nás teda, koľko riešení má kongruencia $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$. Pomocou prvočíselného rozkladu za použitia Čínskej zvyškovej vety môžeme tento problém preformulovať na hľadanie riešení sústavy rovníc tvaru $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{p_i^{\alpha_i}}$ pre všetky i z množiny $1, \ldots, \omega(n)$. Takto získaná sústava má totiž nesúdeliteľné moduly a teda každé jej riešenie je zároveň riešením pôvodnej kongruencie. Navyše počet riešení sústavy je súčinom počtu riešení jednotlivých kongruencií. Zaoberajme sa teda týmito kongruenciami. Využijeme pri tom fakt, že grupa $Z_{p^\alpha}^*$ je pre nepárne prvočíslo p a kladné prirodzené číslo α vždy cyklická, a teda existuje jej generátor, ktorý si označíme g. Všetky prvky grupy, a teda všetky potenciálne riešenia našej kongruencie potom môžeme napísať v tvare $g^1, \ldots, g^{p^{\alpha-1}(p-1)}$. Pritom využívame, že počet prvkov takejto grupy je $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ (ϕ je Eulerova funkcia - počet čísel nesúdeliteľných s argumentom a menších ako argument). Pozrime sa na to, ktoré z nich naozaj riešeniami sú. Rád

prvku g v grupe $Z^*_{p^\alpha}$ je presne $p^{\alpha-1}(p-1)$, takže ak má byť nejaké g^i riešením kongruencie $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{p^\alpha}$, potom číslo $i \cdot 2^{\nu(n)-1}t$ musí byť násobkom rádu, teda čísla $p^{\alpha-1}(p-1)$. Označme si pre jednoduchosť $m = 2^{\nu(n)-1}t$, $q = p^{\alpha-1}(p-1)$ a nech $(m,q) = D$, $m = MD$ a $q = QD$. Potom teda musí platiť, že iMD je násobkom QD, alebo, čo je ekvivalentné s tým, iM je násobkom Q. Keďže však M a Q sú nesúdeliteľné, musí byť číslo i násobkom Q. No a vďaka tomu už sme našli všetky riešenia našej kongruencie - sú to čísla zodpovedajúce mocninám generátora s exponentami $Q, 2Q, \ldots, DQ$. Týchto čísel je presne D, takže aj riešení kongruencie je presne D. Čo je však D ? Pozrime sa naspäť na definíciu a dostávame $D = (2^{\nu(n)-1}t, p^{\alpha-1}(p-1))$. Z definície v predchádzajúcej leme vidno, že $2^{\nu(n)-1}t$ delí číslo $n-1$, čo znamená, že je nesúdeliteľné s n a aj s ľubovoľným prvočíselným deliteľom p čísla n. Preto platí $D = (2^{\nu(n)-1}t, p-1)$. Ďalej rovnako priamo z definície čísla $\nu(n)$ dostávame, že $2^{\nu(n)-1}$ delí $p-1$, takže keďže číslo t je nepárne, môžeme písať $D = 2^{\nu(n)-1}(t, p-1)$. Dostali sme teda už vyjadrenie počtu riešení každej z kongruencií našej sústavy, no a ako sme spomenuli na začiatku počet riešení celej sústavy, a teda počet riešení našej pôvodnej kongruencie, je rovný súčinu týchto počtov. Teda platí $|\overline{S_1}(n)| = \prod_{i=1}^{\omega(n)} 2^{\nu(n)-1}(t, p_i - 1) = 2^{(\nu(n)-1)\omega(n)} \prod_{p|n}(t, p-1)$. Vidíme, že to je presne polovica z dokazovaného počtu prvkov množiny $\overline{S}(n)$, takže už nám stačí dokázať, že množiny $\overline{S_1}(n)$ a $\overline{S_2}(n)$ sú rovnako veľké a budeme hotoví. Chceme ukázať, že kongruencia $a^{2^{\nu(n)-1}t} \equiv -1 \pmod{n}$ má rovnako veľa riešení ako kongruencia $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$. Podobne ako predtým, stačí nám zaoberať sa kongruenciami v tvare $a^m \equiv -1 \pmod{p^\alpha}$, kde p sú prvočíselné delitele čísla n. Ak však máme takúto kongruenciu, dá sa ukázať, že je ekvivalentná so sústavou dvoch kongruencií $a^{2m} \equiv 1 \pmod{p^\alpha}$ a $a^m \not\equiv 1 \pmod{p^\alpha}$. Jedným smerom je implikácia zrejmá, druhým plynie z toho, že kongruenciu $a^{2m} \equiv 1 \pmod{p^\alpha}$ možno prepísať do tvaru $(a^m-1)(a^m+1) \equiv 0 \pmod{p^\alpha}$. Tu využijeme, že p je nepárne prvočíslo, a teda nemôže deliť naraz obe zátvorky, teda p^α musí deliť niektorú z nich. Prvú z nich však podľa predpokladu nedelí, a teda musí druhú a naozaj platí $a^m \equiv -1 \pmod{p^\alpha}$. Z ekvivalentnosti so sústavou už dostávame použitím rovnakého postupu ako v prípade množiny $\overline{S_1}(n)$, že počet riešení každej z kongruencií je $2^{\nu(n)}(t, p-1) - 2^{\nu(n)-1}(t, p-1) = 2^{\nu(n)-1}(t, p-1)$. Riešení každej z kongruencií je rovnako veľa, takže použitím Čínskej zvyškovej vety dostaneme, že aj riešení pôvodnej kongruencie je rovnako veľa a teda množiny $\overline{S_1}(n)$ a $\overline{S_2}(n)$ sú rovnako veľké. Tým je dôkaz ukončený. ■

Predchádzajúce dve lemy nás dôkladne pripravili, môžeme prejsť k dôkazu podstatného výsledku.

Veta 5.1 *Nech $n > 9$ je nepárne zložené číslo. Označme $S(n)$ nasledovne definovanú množinu čísel :* $\{0 \leq a < n \mid n$ *je silné pseudoprvočíslo v báze* $a\}$. *Potom platí* $S(n) \leq \frac{1}{4}\phi(n)$.

Dôkaz Z lemy 5.2 vyplýva, že množina $\overline{S}(n)$ definovaná v leme 5.3 obsahuje všetky bázy, v ktorých je číslo n silným pseudoprvočíslom. Preto $|S(n)| \leq |\overline{S}(n)|$ a ak sa nám podarí ukázať, že platí $|\overline{S}(n)| \leq \frac{1}{4}\phi(n)$, budeme hotoví. Budeme sa zaoberať pomerom $\frac{\phi(n)}{|\overline{S}(n)|}$, o ktorom chceme ukázať, že je najmenej 4. Nech $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ je prvočíselný rozklad čísla n, potom podľa lemy 5.3 platí

$$\frac{\phi(n)}{|\overline{S}(n)|} = \frac{p_1^{\alpha_1 - 1} \dots p_N^{\alpha_N - 1}(p_1 - 1) \dots (p_N - 1)}{2 \cdot 2^{(\nu(n)-1)N} \cdot \prod_{i=1}^{N}(t, p_i - 1)}$$

V čitateli sme pritom použili známy vzorec na výpočet Eulerovej funkcie z prvočíselného rozkladu argumentu. Tento vzťah môžeme ďalej upraviť na tvar

$$\frac{\phi(n)}{|\overline{S}(n)|} = \frac{1}{2} \prod_{i=1}^{N} p_i^{\alpha_i - 1} \frac{p_i - 1}{2^{\nu(n)-1}(t, p_i - 1)}$$

Zaoberajme sa teraz číslami $\frac{p_i - 1}{2^{\nu(n)-1}(t, p_i - 1)}$. Keďže podľa definície čísla $\nu(n)$ platí vždy $2^{\nu(n)} \mid p_i - 1$ a číslo t je nepárne, a teda číslo $(t, p_i - 1)$ je nepárnym deliteľom čísla $p_i - 1$, uvedené členy sú párne celé čísla. Pretože aj súčiniteľ $p_i^{\alpha_i - 1}$ je vždy celým číslom, aj celý pomer bude vždy celým číslom. My potrebujeme ukázať, že toto celé číslo je najmenej 4. Na to rozoberieme viacero možností, ako môže vyzerať prvočíselný rozklad čísla n. Ak $N \geq 3$, t.j. ak číslo n delia aspoň 3 rôzne prvočísla, potom keďže každý súčiniteľ v našom výraze je aspoň 2, spolu s koeficientom $\frac{1}{2}$ to znamená, že $\frac{\phi(n)}{|\overline{S}(n)|} \geq 4$. Takže nám stačí zaoberať sa prípadmi $N = 2$ a $N = 1$. V prvom z nich najprv predpokladajme, že niektoré z dvoch prvočísel, ktoré delia n ho delia vo vyššej ako prvej mocnine. Potom však príslušný člen $p_i^{\alpha_i - 1}$ má hodnotu aspoň 3 (číslo n je nepárne a teda aj prvočíslo p_i musí byť nepárne). Obidva členy $\frac{p_i - 1}{2^{\nu(n)-1}(t, p_i - 1)}$ majú hodnotu aspoň 2, a teda celý súčin spolu s koeficientom $\frac{1}{2}$ je rovný najmenej 6. Môžeme teda ďalej predpokladať, že

číslo n má tvar $n = p \cdot q$, kde $p < q$ sú rôzne prvočísla. Ak by číslo $q-1$ bolo deliteľné číslom $2^{\nu(n)+1}$ (pripomeňme, že podľa definície musí byť deliteľné číslom $2^{\nu(n)}$), potom súčiniteľ $\frac{q-1}{2^{\nu(n)-1}(t,q-1)}$ by mal hodnotu aspoň 4, súčiniteľ $\frac{p-1}{2^{\nu(n)-1}(t,p-1)}$ aspoň 2, a spolu s koeficientom $\frac{1}{2}$ celý súčin aspoň 4, boli by sme teda hotoví. Ďalej teda môžeme predpokladať, že číslo $q-1$ je deliteľné presne $\nu(n)$-tou mocninou dvojky. Platí $n-1 = pq-1 = p(q-1)+(p-1)$, odkiaľ $n-1 \equiv p-1 \pmod{q-1}$, a keďže $p < q$ dostávame $q-1 \nmid n-1$. Pretože $2^{\nu(n)} \mid n$, znamená tento fakt, že musí existovať nepárne prvočíslo, ktoré delí $q-1$ vo vyššej mocnine ako číslo $n-1$. Nech $q-1 = 2^{\nu(n)}q'$, potom $(t, q-1) = (t, q') \leq \frac{q'}{3}$. Teda $2^{\nu(n)-1}(t, q-1) \leq 2^{\nu(n)-1}\frac{q'}{3} = \frac{q-1}{6}$, čo znamená, že člen $\frac{q-1}{2^{\nu(n)-1}(t,q-1)}$ má hodnotu najmenej 6. Keďže opäť člen $\frac{p-1}{2^{\nu(n)-1}(t,p-1)}$ má hodnotu aspoň 2 a koeficient je $\frac{1}{2}$, platí v tomto prípade $\frac{\phi(n)}{|\overline{S}(n)|} \geq 6$. Posledný prípad, pre ktorý sme ešte nedokončili dôkaz je $N = 1$, t.j. ak číslo n je mocninou prvočísla $n = p^{\alpha}$. Pritom zrejme musí platiť $\alpha \geq 2$, nakoľko podľa predpokladu je číslo n zložené. Keďže v tomto prípade máme prvočíslo iba jedno, opäť $2^{\nu(n)}$ je presne mocnina dvojky, ktorá delí $p-1$. Môžeme teda písať $p-1 = 2^{\nu(n)}p'$, kde p' je nepárne prirodzené číslo. Platí $p^{\alpha}-1 = 2^s t$, kde $s \geq \nu(n)$, čo ďalej môžeme rozpísať ako $(p-1)(p^{\alpha-1}+\ldots+1) = 2^s t$ a ďalej $p'(p^{\alpha-1}+\ldots+1) = 2^{s-\nu(n)}t$. Odtiaľ, keďže p' je nepárne číslo, dostávame $p' \mid t$ alebo inými slovami $(t, p-1) = (t, p') = p'$. Dosadením tohoto výsledku už dostávame $\frac{p-1}{2^{\nu(n)-1}(t,p-1)} = 2$, celkovo to znamená $\frac{\phi(n)}{|\overline{S}(n)|} = p^{\alpha-1}$, čo je pre $n > 9$ určite viac ako 4. Tým sme rozobrali aj poslednú možnosť a dôkaz je ukončený. ■

Podobne ako v prípade Solovay-Strassenovho algoritmu nám tento výsledok poskytuje ohraničenia pravdepodobnosti omylu, ktoré nás presvedčia o tom, že pravdepodobnostný charakter pri dostatočnom počte opakovaní vôbec nepredstavuje prekážku v praktickom použití, a že prvočísla, ktoré takýmto spôsobom vygenerujeme (výstižne nazývané ako industrial-grade prvočísla), môžeme bez výčitiek svedomia používať aj v aplikáciách, kde potrebujeme vysokú presnosť a bezpečnosť. Pravdepodobnosť zlyhania ostatných článkov nástroja, ktorý používame (napr. na šifrovanie) môže byť často oveľa väčšia. Aká je teda pravdepodobnosť omylu pri použití Rabin-Millerovho algoritmu na testovanie prvočísla a aká pri generovaní pri prvočísel v nejakej množine ? Tieto otázky sú často zamieňané a nesprávne odpovedané triviálnym spôsobom "menšia než $\frac{1}{4^T}$", pri počte opakovaní T.

Táto odpoveď je správna pre prvú otázku, kde plynie z predchádzajúcej lemy. V druhom prípade však nie je na prvý pohľad zrejmá, keďže tu vstupuje do hry otázka rozvrstvenia prvočísel, podobne ako to bolo v situácii, ktorou sa zaoberá veta 4.5. Dá sa ukázať (napr. v [4]), že aj tu je pravdepodobnosť omylu menšia než $\frac{1}{4^T}$. Každopádne pre dosť veľké T sa jedná naozaj o zanedbateľné čísla, ktoré úplne postačujú pre praktické účely. Nás však bude ďalej zaujímať teoretická otázka, či možno tento nedostatok odstrániť. Ukážeme, že za predpokladu platnosti Rozšírenej Riemannovej hypotézy možno naozaj dosiahnuť deterministickú modifikáciu Rabin-Millerovho testu. Tá spočíva v nasledujúcej myšlienke : Ak je číslo zložené, potom aspoň $\frac{3}{4}$ čísel sú svedkami jeho zloženosti. Nám stačí nájsť jedného z nich a budeme vedieť, že číslo je zložené. Ak by sa nám podarilo vždy nájsť dostatočne malého svedka, nemusíme prechádzať všetky čísla a stále budeme mať istotu správneho výsledku. Presnejšie, ak sa nám podarí ukázať, že existuje ohraničenie na najmenšieho svedka, potom stačí hľadať svedkov menších ako toto ohraničenie. Ak taký neexistuje, potom neexistuje žiadny. Zaveďme si preto označenie $W(n)$ pre najmenšieho svedka čísla n a pozrime sa na to, ako vieme číslo $W(n)$ zhora ohraničiť.

V nasledujúcom dôkaze použijeme výsledok o tzv. *hladkých* (v anglickej literatúre *smooth*) číslach, ktorý dokázali v roku 1997 Konyagin a Pomerance v [9]. Prirodzené číslo sa nazýva $y-$hladké, ak nie je deliteľné žiadnym prvočíslom väčším ako y. Takto definované čísla pri rôznych voľbách parametra y sú medzi prirodzenými číslami často až prekvapivo početne zastúpené. Napríklad viac ako 30 percent čísel z množiny $\{1, \ldots, n\}$ sú pre dostatočne veľké n $\sqrt{n}-$hladké čísla, tzn. majú v prvočíselnom rozklade len "malé" prvočísla. Na vyjadrenie pomerného zastúpenia hladkých čísel sa zavádza funkcia

$$\psi(x, y) = |\{1 \leq n \leq x \mid n \text{ je } y - \text{hladké}\}|$$

Výsledok z [9] hovorí o tom, že pre všetky prirodzené čísla $x \geq 4$, $2 \leq x^{\frac{1}{u}} \leq x$ platí $\psi(x, x^{\frac{1}{u}}) \geq x \ln^{-u} x$. Pozrime sa na to, ako ho možno využiť.

Lema 5.4 *Nech n je nepárne zložené číslo, ktoré je deliteľné štvorcom nejakého prvočísla. Potom platí $W(n) < \ln^2 n$.*

Dôkaz Najprv ukážeme s využitím uvedeného výsledku, že ak p je nepárne prvočíslo, potom existuje prvočíslo $a < 4 \ln^2 p$, pre ktoré neplatí $a^{p-1} \equiv 1$

(mod p^2). Predpokladajme sporom, že každé prvočíslo $a < 4\ln^2 p$ túto kongruenciu spĺňa. Potom ak b je ľubovoľné číslo z množiny $\{1,\ldots,p^2\}$, ktoré sa dá napísať ako súčin prvočísel menších než $4\ln^2 p$ (inými slovami podľa našej terminológie ľubovoľné $4\ln^2 p-$hladké číslo), potom spĺňa kongruenciu $b^{p-1} \equiv 1 \pmod{p^2}$. Takýchto čísel b je v množine $\{1,\ldots,p^2\}$ presne $\psi(p^2, 4\ln^2 p)$. Teraz použijeme horeuvedený výsledok na ohraničenie tohoto počtu. Pre ľubovoľné x, y také, že $x \geq 4$, $2 \leq y \leq x$, platí $\psi(x,y) \geq x^{1-\frac{\ln\ln x}{\ln y}}$ (tento vzťah dostaneme jednoducho prepísaným horeuvedeného výsledku za predpokladu $y = x^{\frac{1}{u}}$). Ak do tohto vzťahu dosadíme konkrétne x, y ktoré nás zaujímajú, dostávame $\psi(p^2, 4\ln^2 p) \geq (p^2)^{1-\frac{\ln\ln p^2}{\ln 4\ln^2 p}} = (p^2)^{\frac{1}{2}} = p$. Čísel b, ktoré spĺňajú kongruenciu $b^{p-1} \equiv 1 \pmod{p^2}$ je teda aspoň p. Skúsme zistiť, koľko ich je presne iným spôsobom. Grupa $Z^*_{p^2}$ je cyklická, obsahuje teda nejaký generátor g. Tento generátor má rád rovný počtu prvkov grupy, t.j. $p(p-1)$. Navyše všetky prvky grupy sa nachádzajú práve raz v postupnosti $g, g^2, \ldots, g^{p(p-1)}$. Ak nejaký prvok $b = g^i$ má spĺňať $b^{p-1} \equiv 1 \pmod{p^2}$, musí platiť $g^{i(p-1)} \equiv 1 \pmod{p^2}$. Pretože rád prvku g je presne $p(p-1)$, musí $i(p-1) \mid p(p-1)$, a teda $i \mid p$. Toto je nutná a zároveň postačujúca podmienka pre číslo i na to, aby $b = g^i$ spĺňala príslušnú kongruenciu. V množine exponentov $\{1,\ldots,p(p-1)\}$ je práve $p-1$ čísel, ktoré ju spĺňajú. To ale znamená, že existuje práve $p-1$ rôznych možností pre číslo b, ktoré vyhovujú našej kongruencii. My sme však dokázali, že ich je najmenej p, čo už znamená spor. Vráťme sa teraz k dôkazu zo zadania. Opäť budeme sporom predpokladať, že neexistuje žiadny svedok, ktorý by bol menší ako $\ln^2 n$. To znamená, že číslo n je silným pseudoprvočíslom vo všetkých bázach menších než $\ln^2 n$. Podľa zadania existuje prvočíslo p také, že $p^2 \mid n$. Keďže n je silným pseudoprvočíslom v bázach $a \in [1, \ln^2 n)$, platí pre všetky tieto a kongruencia $a^{n-1} \equiv 1 \pmod{n}$, a preto aj kongruencia $a^{n-1} \equiv 1 \pmod{p^2}$. Vezmime si ľubovoľné také a a označme v jeho rád v grupe $Z^*_{p^2}$. Keďže podľa Eulerovej vety platí $a^{\phi(n)} = a^{p(p-1)} \equiv 1 \pmod{p^2}$, musí $v \mid p(p-1)$. Pretože však tiež $v \mid n-1$, odkiaľ plynie, že v a p sú nesúdeliteľné, dostávame $v \mid p-1$. To znamená, že $a^{p-1} \equiv 1 \pmod{p^2}$, pričom sme nič nepredpokladali o čísle a, takže táto kongruencia platí pre všetky čísla, a tým skôr pre všetky prvočísla a z rozsahu $a \in [1, \ln^2 n)$. Pretože $4\ln^2 p \leq \ln^2 n$, platí táto kongruencia aj pre všetky prvočísla $a < 4\ln^2 p$. To už je ale spor s výsledkom, ktorý sme dokázali vyššie, a teda naozaj musí existovať svedok menší než $\ln^2 n$, čo znamená, že platí $W(n) < \ln^2 n$. ■

Predchádzajúca lema poskytuje ohraničenie pre špeciálny tvar čísla n, ktoré sme zatiaľ boli schopný dokázať bez použitia nedokázanej Riemannovej hypotézy. Vo všeobecnom prípade si ju však vezmeme na pomoc. Nasledujúce tvrdenie je zavŕšením nášho rozprávania. V dodatku sa spomína dôsledok Rozšírenej Riemannovej hypotézy, aj priamy dôkaz tvrdenia o existencii malého svedka. Na tomto mieste však uvedieme elegantnejší spôsob ako toto tvrdenie dokázať s využitím výsledku z teórie charakterov. Dá sa ukázať, že pre ľubovoľnú nevlastnú podgrupu H grupy Z_n^* existuje prvok menší než $2\ln^2 n$, ktorý do nej nepatrí. Ukážeme, že táto vlastnosť už stačí na odvodenie výsledku, ktorý nás zaujíma.

Veta 5.2 *Nech n je nepárne zložené číslo a platí Rozšírená Riemannova hypotéza, potom platí $W(n) < 2\ln^2 n$.*

Dôkaz Ukázali sme už, že množina $\overline{S}(n)$, o ktorej sa ľahko ukáže, že je podgrupou Z_n^*, je nadmnožinou množiny $S(n)$. Množina $S(n)$ pritom obsahuje všetky bázy, v ktorých je n pseudoprvočíslom. Takže ak nájdeme nejaké číslo, ktoré nepatrí do $\overline{S}(n)$, nebude patriť ani do $S(n)$ a bude svedkom. My chceme ukázať, že vieme nájsť také číslo menšie než $2\ln^2 n$. S použitím dôsledku spomenutého vyššie však máme existenciu takého čísla zaručenú. Preto toto číslo je svedkom a dôkaz je ukončený. ■

Predpokladajme, že platí Rozšírená Riemannova hypotéza. Zhrňme si, čo nám hovorí táto veta. Pre ľubovoľné zložené číslo n existuje svedok menší ako $2\ln^2 n$. Ak vyskúšame všetky bázy v rozsahu 1 až $2\ln^2 n$ a nenájdeme ho tam, môžeme s istotou tvrdiť, že sa jedná o prvočíslo. Ak tam svedka nájdeme, naopak s istotou vieme, že sa jedná o číslo zložené. Máme teda k dispozícii deterministický, a čo je dôležité, polynomiálny test prvočíselnosti (podmienený platnosťou Rozšírenej Riemannovej hypotézy).

Kapitola 6

Záver

Deterministický test využívajúci Rozšírenú Riemannovu hypotézu predložil Miler v článku [11] v roku 1976 (v skutočnosti sa líšila konštanta pred logaritmom, nakoľko toto ohraničenie spravil až Bach v [3] r.1990). Odvtedy bol nájdený deterministický Agrawal-Kayal-Saxena (AKS) test prvočíselnosti, ktorý využíva vlastnosti cyklotomických polynómov a ktorý nezávisí na žiadnej nedokázanej hypotéze a test ECPP založený na eliptických krivkách, ktorý má tú výhodu, že ak prehlási o čísle že je prvočíslom, potom naozaj prvočíslom je (samotný názov obsahujúci *primality proving* naznačuje, že výsledok je o niečo cennejší ako v prípade pravdepodobnostných algoritmov). Napriek tomu sa dodnes používa aj Rabin-Millerov test v nedeterministickej podobe (v praktických aplikáciách sa väčšinou pracuje s nejakou fixne zvolenou množinou testovaných báz), nakoľko je rýchlejší a dostatočne spoľahlivý.

Praktickému použitiu algoritmov a metódami na ich používanie v reálnych aplikáciách sme sa zaoberali iba okrajovo. Určite stojí za zmienku, že Rabin-Millerov test je implementovaný ako prvočíselný test v systémoch ako Mathematica či Matlab, jeho modifikáciu obsahuje aj knižnica NTL (Number theory library), jedna z najrýchlejších knižníc na výpočty v teórii čísel. V týchto systémoch je test implementovaný s pevne danou množinou báz, voči ktorej sa testované číslo skúša, a ktorou je v istom rozsahu prvočíselnosť naozaj zaručená. Vďaka svojej rýchlosti uprednostnili autori týchto systémov Rabin-Millerov test pred deterministickými, ktoré síce dávajú presné výsledky, no pre praktické aplikácie sú nedostatočne rýchle. Aj pri vedeckých výpočtoch je preferovaný spôsob najprv použiť Rabin-Millerov test na úvodnú elimináciu a až potom nasadiť testy typu ECPP alebo AKS.

V práci sme si dali za úlohu predstaviť čitateľovi jednotiaciu líniu prvočíselných testov založených na Malej Fermatovej vete, previesť ho na ceste od Fermatovho testu až k Miller-Rabinovmu a ukázať možnosť deterministického rozšírenia tohto testu, čo zároveň považujeme za najzaujímavejší výsledok, ktorým sme sa zaoberali. V texte bola naznačená línia prechádzajúca od Fermatovych pseudoprvočísel cez Eulerove a Euler-Jacobiho pseudoprvočísla k silným pseudoprvočíslam. Až po poslednú dvojicu sa vždy jednalo o zovšeobecnenie predchádzajúceho pojmu zavedením novej definície. Euler-Jacobiho a silné pseudoprvočísla takýmto spôsobom nesúvisia, v skutočnosti ani jedna z týchto množín nie je podmnožinou druhej, ako môže čitateľ ľahko nahliadnuť z tabuliek uvedených v texte (napr. už číslo 561 je Euler-Jacobiho pseudoprvočíslom v báze 2 a nie je silným pseudoprvočíslom v tejto báze a naopak 703 je silným pseudoprvočíslom v báze 3 a nie je Euler-Jacobiho pseudoprvočíslom v tejto báze).

Napriek tomu, že sme sa nevenovali presnému popisu výpočtovej zložitosti, je z rozprávania zrejmé, že všetky testy, ktorými sme sa zaoberali, sú pri testovaní konkrétnej bázy približne rovnako rýchle a všetky sú polynomiálne od veľkosti vstupu. Pri zovšeobecňovaní testov sme sa nesnažili hľadať spôsoby ako ich urýchliť, ale snažili sme sa odstraňovať niektoré ich nedostatky. Prvým významným nedostatkom bola existencia Carmichaelovych čísel a absolútnych Eulerových pseudoprvočísel, ktorý sa nám podarilo odstrániť zovšeobecnením na Euler-Jacobiho, resp. silné pseudoprvočísla. Nakoniec sme použitím predpokladu Rozšírenej Riemannovej hypotézy získali podmienený výsledok, ktorý môže v prípade dôvery k Riemannovej hypotéze odstrániť aj teoretický nedostatok spočívajúci v pravdepodobnostnom charaktere testov.

Naše rozprávanie skončilo, no problémy v teórii čísel ostávajú otvorené. Rovnako ostáva otvorená otázka platnosti Riemannovej hypotézy. Možno čitateľ za pár rokov pri čítaní tohto textu bude môcť ignorovať všetky poznámky o neistej platnosti našich úvah na konci textu, alebo naopak bude musieť ignorovať všetky výsledky podopreté hypotézou. Určite však vďaka pokroku v matematike nadobudnú naše úvahy iný rozmer v kontexte aktuálnych znalostí. Okrem takto formulovaných tvrdení však moja práca obsahuje veľa konštrukcií a poučení, ktoré budú pre čitateľa užitočné kedykoľvek sa bude chcieť hlbšie zaoberať aspektami algoritmickej teórie čísel. To som si kládol pri písaní za cieľ a verím že sa mi to v čo najuspokojivejšej miere podarilo dosiahnuť.

Dodatok A

Riemannova hypotéza

Riemannova hypotéza je pomerne známym problémom, dokonca sa občas spomína vo filmoch určených pre bežného diváka, ktorý ani netuší, o čom táto veta hovorí. V skutočnosti ide o netriviálny problém, pri ktorom už formulácia a pochopenie vyžaduje isté znalosti komplexnej analýzy. Predstavuje tak kontrast k vetám ako Veľká Fermatova veta, ktoré naopak majú znenie jednoduché, napriek tomu že ide o problém porovnateľnej zložitosti. Veľká Fermatova veta však už v dnešnej dobe dokázaná je, Riemannova hypotéza zatiaľ pokusom o dôkaz alebo vyvrátenie odoláva. Napriek tomu predstavuje kľúčovú vetu, o ktorú sa opiera množstvo teórii, často až prekvapivo vzdialených od pôvodného zamerania samotnej hypotézy. Takou je v podstate aj naša teória, v ktorej sa zaoberáme pseudoprvočíslami. Na prvý pohľad nijako nesúvisí s komplexnou analýzou. V nasledujúcich riadkoch sa pokúsime naznačiť Riemannovu hypotézu a jej súvislosť s teóriou čísel. Pozrieme sa aj na jej zovšeobecnenie, ktoré bude viesť k vete, ktorá bude kľúčová v úvahách v ďalšej kapitole. Začneme definíciou Riemannovej zeta-funkcie (podľa nej sa Riemannova hypotéza zvykne nazývať aj Riemannovou zeta-hypotézou).

Definícia A.1 *Riemannova zeta-funkcia $\zeta(s)$ je funkciou komplexnej premennej s, ktorá je analytickým rozšírením nasledujúcej funkcie definovanej nekonečným radom :*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Už z tejto definície je zrejmé, že Riemannova hypotéza nebude jednoduchou záležitosťou. Nekonečný rad v definícii poznáme z reálnej analýzy

a vieme, že pre reálne $s \leq 1$ diverguje. V skutočnosti konverguje pre všetky komplexné čísla s, ktorých reálna časť je väčšia než 1. Pre ostatné komplexné čísla priamo z tohto predpisu nedostaneme hodnotu Riemannovej funkcie, keďže rad diverguje. Práve preto je v definícii zmienka o analytickom rozšírení na celú množinu komplexných čísel. Pre všetky komplexné funkcie s istými špeciálnymi vlastnosťami vieme nájsť takéto rozšírenie jednoznačne. Konkrétne ak máme na otvorenej podmnožine komplexných čísel definovanú hladkú funkciu, vieme ju jednoznačným spôsobom rozšíriť na hladkú funkciu definovanú na celej množine komplexných čísel. Teda napriek tomu, že uvedený predpis nám nehovorí, aké hodnoty nadobúda funkcia pre čísla s s $Re(s) \leq 1$ (v skutočnosti nám to priamo nehovorí ani pre ostatné s, uzavreté tvary nekonečného radu sú známe len pre niektoré špeciálne s), definuje ju tento predpis pre všetky komplexné čísla jednoznačne. Vďaka tomu má zmysel vôbec zaoberať sa kritickou oblasťou $0 < Re(s) < 1$ a hľadať v nej nuly Riemannovej funkcie, o čom hovorí Riemannova hypotéza. Skôr než prejdeme k jej formulácii, zastavme sa pri vete, ktorá nám naznačí súvislosť Riemannovej hypotézy s prvočíslami a teóriou čísel.

Veta A.1 *Nech s je komplexné číslo, pre ktoré platí $Re(s) > 1$ a nech P je množina všetkých prvočísel. Potom platí*

$$\zeta(s) = \prod_{p \in P} (1 - p^{-s})^{-1}$$

Dôkaz Súčin na pravej strane rovnosti obsahuje činitele tvaru $(1-p^{-s})^{-1} = \frac{1}{1-\frac{1}{p^s}}$, ktoré sú podľa vzorca pre súčet geometrickej postupnosti uzavretým tvarom nekonečných súčtov v tvare $1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots$. Celý súčin teda možno interpretovať ako roznásobené zátvorky obsahujúce uvedený rad pre každé prvočíslo. Pritom pre každé prvočíslo máme práve jednu takúto zátvorku. Ak ich roznásobíme, dostaneme súčet členov v špeciálnom tvare. Podľa toho, ktoré zátvorky sme zohľadnili a ktoré mocniny sme z nich vybrali, dostaneme konkrétne číslo v tvare $(p_1^{-a_1 s} p_2^{-a_2 s} \cdots p_k^{-a_k s})^{-1}$. (Na to, aby sme dostali konečné číslo sme mohli len z konečne veľa zátvoriek vybrať niečo iné ako jednotku, preto má takéto preoznačenie opodstatnenie). Ak teraz označíme $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, vidíme, že člen, ktorý sme dostali má tvar $\frac{1}{n^s}$ pre príslušné komplexné číslo s. To znamená, že sa nachádza aj v súčte, ktorým je definovaná Riemannova funkcia, t.j. $\sum_{n=1}^{\infty} \frac{1}{n^s}$. Na druhej strane, každý člen tohto súčtu sa dá spätne rozpísať v uvedenom tvare a nie je

ťažké si uvedomiť, že správnym výberom zátvoriek vieme dostať akýkoľvek člen. Pretože kanonický rozklad každého prirodzeného čísla na prvočisla je jednoznačný, dostávame už jednoznačnú korešpondenciu medzi členmi na ľavej a pravej strane rovnosti. Platí teda dokazovaná rovnosť. ■

Predchádzajúca veta naznačila v hrubých rysoch súvislosti medzi komplexnou analýzou zaoberajúcou sa spojitými veličinami s rýdzo diskrétnym oborom teórie čísel. Súvislostí oveľa prekvapujúcejších existuje omnoho viac, pre nás je zaujímavý napríklad fakt, že je možné zostrojiť vyjadrenie funkcie $\pi(x)$, ktorá počíta prvočísla menšie ako x, v závislosti od núl Riemannovej zeta-funkcie v kritickom pásme $0 < Re(s) < 1$. Riemannova funkcia nadobúda nulu triviálne v záporných celých číslach, no keď sa obmedzíme na oblasť $0 < Re(s) < 1$, ukazuje sa, že všetky netriviálne nuly nadobúda Riemannova funkcia v argumentoch špeciálneho tvaru. O tom hovorí Riemannova hypotéza.

Hypotéza A.1 (Riemannova hypotéza) *Pre všetky komplexné čísla s, ktoré ležia v oblasti $0 < Re(s) < 1$ platí, že ak $\zeta(s) = 0$, potom $Re(s) = \frac{1}{2}$.*

Inými slovami všetky nuly Riemannovej funkcie v kritickom pásme ležia na priamke $Re(s) = \frac{1}{2}$. Z tohto nenápadného tvrdenia možno odvodiť množstvo netriviálnych dôsledkov z rôznych oblastí matematiky. Pre nás bude zaujímavé predovšetkým tvrdenie, ktoré je dôsledkom jedného zo zovšeobecnení Riemannovej hypotézy. Na jej zovšeobecnenie však potrebujeme nahliadnuť do teórie Dirichletovych charakterov.

Definícia A.2 *Nech D je prirodzené číslo. Funkciu χ definovanú pre všetky prirodzené čísla a nadobúdajúcu hodnoty z množiny komplexných čísel nazývame Dirichletovym charakterom modulo D, ak spĺňa podmienky:*

a) $\chi(mn) = \chi(m)\chi(n)$ *pre všetky* m, n

b) χ *je periodická s periódou* D

c) $\chi(n) = 0$ *práve vtedy ak* $(n, D) > 1$

Dirichletov charakter vznikol ako rozšírenie pojmu charakter v grupe, podstatná vlastnosť ktorú majú spoločnú je multiplikatívnosť. Priamo z tejto vlastnosti máme $\chi(1) = \chi(1 \cdot 1) = \chi^2(1)$, odkiaľ keďže $(1, D) = 1$ pre

ľubovoľný modul D podľa podmienky c) je $\chi(1) \neq 0$ a teda musí byť $\chi(1) = 1$. Tým máme jednoznačne determinovanú hodnotu v bode 1 pre všetky Dirichletove charaktery. Ako možno ľahko preveriť, jedným príkladom Dirichletovho charakteru je aj Legendrov, resp. Jacobiho symbol. Stačí položiť $\chi(a) = \left(\frac{a}{D}\right)$ a všetky podmienky sú triviálne splnené. V tomto konkrétnom prípade nadobúda vo všetkých bodoch jednu z hodnôt 1,-1 a 0. Aké ďalšie hodnoty môže vo všeobecnosti nadobúdať Dirichletov charakter?

Lema A.1 *Nech χ je Dirichletov charakter modulo D. Potom pre všetky prirodzené čísla n nesúdeliteľné s D platí $|\chi(n)| = 1$.*

Dôkaz Podľa Eulerovej vety platí pre ľubovoľné n nesúdeliteľné s modulom D kongruencia $n^{\phi(D)} \equiv 1 \pmod{D}$, kde ϕ je Eulerova funkcia - počet čísel nesúdeliteľných s argumentom. Pretože Dirichletov charakter je periodická funkcia s periódou D, v argumentoch líšiacich sa o násobok D dáva rovnaké hodnoty. To znamená, že platí $\chi(n^{\phi(D)}) = \chi(1) = 1$. Navyše z multiplikatívnosti vieme, že $\chi(n^{\phi(D)}) = \chi(n)^{\phi(D)}$. Odtiaľ už plynie, že $\chi(n)$ je jedna z komplexných odmocnín jednotky a jej absolútna hodnota je rovná jednej. ■

Dirichletove charaktery teda nadobúdajú výlučne hodnoty ležiace na jednotkovej kružnici v komplexnej rovine. Pre konkrétny modul D máme potenciálne $\phi(D)^{\phi(D)}$ možností, ako môže vyzerať Dirichletov charakter. Hodnota v každom bode je totiž podľa predchádzajúceho dôkazu $\phi(D)$-tou odmocninou z jednotky. V skutočnosti je Dirichletovych charakterov oveľa menej a majú niekoľko ďalších zaujímavých vlastností. Napríklad keď si vezmeme ľubovoľné dva Dirichletove charaktery χ_1, χ_2 modulo D_1, D_2, potom môžeme definovať ich súčin $\chi_1\chi_2$ modulo $D = [D_1, D_2]$. Ľahko sa ukáže, že tento tiež spĺňa vlastnosti Dirichletovho charakteru : Z definície a multiplikatívnosti χ_1, χ_2 dostaneme $\chi_1\chi_2(mn) = \chi_1(mn) \cdot \chi_2(mn) = \chi_1(m) \cdot \chi_1(n) \cdot \chi_2(m) \cdot \chi_2(n) = \chi_1\chi_2(m) \cdot \chi_1\chi_2(n)$. Periodickosť modulo D plynie priamo z toho, že D je spoločným násobkom D_1 a D_2, rovnako ako tretia podmienka z definície. Ak položíme $D_1 = D_2$, dostávame priamo z vyššie uvedeného, že Dirichletove charaktery modulo D sú uzavreté na násobenie. V skutočnosti platí viac.

Veta A.2 *Množina Dirichletovych charakterov modulo konkrétne prirodzené číslo D tvorí s operáciou násobenia definovanou ako bežné násobenie funkcií grupu.*

Dôkaz Ukázali sme už, že množina je vzhľadom na operáciu násobenia uzavretá. Asociatívnosť násobenia plynie z asociatívnosti násobenia ľubovoľných funkcií, zaoberať sa preto musíme predovšetkým neutrálnym a inverzným prvkom. Funkciu χ_0 definovanú nasledujúcim spôsobom nazveme *základným* alebo *triviálnym* Dirichletovym charakterom :

$$\chi_0(n) = \begin{cases} 0 & \text{ak } (n, D) > 1 \\ 1 & \text{ak } (n, D) = 1 \end{cases}$$

Ľahko sa overí, že je v rámci našej množiny neutrálnym prvkom, pri prenásobení nezmení žiadny Dirichletov charakter a sama definíciu Dirichletovho charakteru spĺňa. Nech χ je ľubovoľný Dirichletov charakter, potom $\overline{\chi}$ je funkcia, ktorá pre všetky prirodzené čísla n spĺňa rovnosť $\overline{\chi}(n) = \overline{\chi(n)}$, t.j. všetky hodnoty sú komplexne združené čísla k hodnotám pôvodnej funkcie χ. Ukážeme, že platí $\chi\overline{\chi} = \chi_0$. Pre prirodzené čísla n také, že $(n, D) > 1$ platí $\chi\overline{\chi}(n) = \chi(n)\overline{\chi}(n) = 0$. Pre čísla n nesúdeliteľné s D platí $\chi\overline{\chi}(n) = \chi(n)\overline{\chi(n)} = |\chi(n)|^2 = 1$, kde posledná rovnosť plynie z lemy A.1. Odtiaľ už vidíme, že funkcie $\chi\overline{\chi}$ a χ_0 sú identické. Preto $\overline{\chi}$ je inverzným prvkom k prvku χ a uvedená množina je naozaj grupou. ■

Ukázali sme, že Dirichletove charaktery modulo D tvoria multiplikatívnu grupu. Ďalšou prirodzenou otázkou je aká je táto grupa veľká. Už sme spomenuli, že všetkých možností, ako možno definovať Dirichletov charakter modulo D pri obmedzení na hodnoty, ktorými sú $\phi(n)$-te odmocniny z jednotky, je $\phi(n)^{\phi(n)}$. Nie všetky z týchto potenciálnych kandidátov naozaj spĺňajú definíciu. Z dôkazu lemy A.1 navyše vieme, že $\chi^{\phi(D)}$ je vždy triviálnym Dirichletovym charakterom. Rád každého prvku v grupe Dirichletovych charakterov teda delí $\phi(D)$. Dá sa ukázať, že počet prvkov grupy Dirichletovych charakterov modulo konkrétne prirodzené číslo D je práve $\phi(D)$ a navyše táto grupa je izomorfná so Z_D^*. To nám poskytuje pomerne jasnú predstavu o štruktúre Dirichletovych charakterov, pozrime sa teraz na ich využitie.

Definícia A.3 *Nech χ je Dirichletov charakter modulo D. Potom k nemu prislúchajúca Dirichletova L-funkcia má tvar*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Dirichletova L-funkcia je pokusom o zovšeobecnenie Riemannovej zeta-funkcie s využitím Dirichletovych charakterov. V konkrétnom prípade triviálneho Dirichletovho charakteru dostaneme v čitateli funkcie jednotku až na čísla súdeliteľné s modulom D (také členy majú v čitateli nulu, teda zo sumy vypadnú), takže v tomto prípade je L-funkcia takmer totožná so zeta-funkciou. Podobným spôsobom ako v dôkaze vety A.1 vieme dostať vzťah, ktorý ukazuje súvislosť L-funkcií s prvočíslami :

$$L(s,\chi) = \prod_{p \in P} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

P v predchádzajúcom vzorci tradične označuje množinu prvočísel. Analogicky rozšírime aj samotnú Riemannovu hypotézu.

Hypotéza A.2 (Rozšírená Riemannova hypotéza) *Nech χ je ľubovoľný Dirichletov charakter. Pre všetky komplexné čísla s, ktoré ležia v oblasti $0 < Re(s) < 1$ platí, že ak $L(s,\chi) = 0$, potom $Re(s) = \frac{1}{2}$.*

V skutočnosti existuje ďalšie zovšeobecnenie Riemannovej hypotézy, ktoré sa zaoberá tzv. Dedekindovymi zeta-funkciami, no to pre nás nie je až tak podstatné. Navyše zrejme s rastúcou všeobecnosťou narastá aj úsilie, ktoré bude potrebné na to, aby boli tieto hypotézy v budúcnosti dokázané alebo vyvrátené. My však v nasledujúcom rozprávaní podoprieme jeden náš výsledok Rozšírenou Riemannovou hypotézou, presnejšie jej dôsledkom v podobe nasledujúcej vety :

Veta A.3 *Nech platí Rozšírená Riemannova hypotéza. Nech D je prirodzené číslo a χ je netriviálny Dirichletov charakter modulo D. Potom existuje prirodzené číslo n, pre ktoré platí $n < 2\ln^2 D$ a $\chi(n) \neq 1$. Tiež existuje prirodzené číslo m, pre ktoré platí $m < 3\ln^2 D$ a $\chi(m) \neq 0$ a $\chi(m) \neq 1$.*

Tento pomerne silný výsledok (dokázal ho Bach spresnením Ankenyho výsledku v práci [3]) nám hovorí, že ak si vezmeme netriviálny Dirichletov charakter, t.j. funkciu ktorá okrem nuly a jednotky nadobúda aj nejaké iné hodnoty, tak prvú takúto hodnotu nadobúda pre dosť malý argument. V podstate nám to hovorí, že štruktúra funkcie Dirichletovho charakteru nemôže byť úplne ľubovoľná a vykazuje pre nás podstatnú pravidelnosť. My sa zaoberáme veľmi podobným problémom, ktorým je hľadanie svedkov, čo

sú čísla dokazujúce zloženosť testovaného čísla. Máme k dispozícii výsledok, ktorý nám hovorí, že svedkov je dostatočne veľa, no my potrebujeme viac. Chceme ukázať, že vieme nájsť dostatočne malého svedka. Iba v hrubých rysoch som načrtol cieľ snaženia, no istá podobnosť je už zrejmá - chceme ohraničiť výskyt prvkov špeciálnych vlastností v nejakej množine. Vieme, že tam sú, no nevieme, či sú z istého hľadiska dostatočne malé. O tom hovorí predchádzajúca veta aj ňou podopretý hlavný výsledok nášho rozprávania. Ten si v nasledujúcej vete dokážeme použitím výsledku z kapitoly o silných pseudoprvočíslach. V nej sa nachádza aj jednoduchšia verzia dôkazu, ktorá však používa výsledok z teórie charakterov. Ak čitateľa zaujíma priamy dôkaz bez použitia tohto výsledku, v ďalšom texte sa ho dozvie.

Veta A.4 *Nech n je nepárne zložené číslo a platí Rozšírená Riemannova hypotéza, potom platí $W(n) < 2\ln^2 n$.*

Dôkaz Vďaka leme 5.4 môžeme predpokladať, že n nie je deliteľné štvorcom žiadneho prvočísla, a teda je súčinom niekoľkých (určite aspoň dvoch, keďže je zložené) prvočísel. Keby bolo, platilo by totiž ešte silnejšie ohraničenie $W(n) < \ln^2 n$, a to dokonca bez predpokladu platnosti Riemannovej hypotézy a nemali by sme čo dokazovať. Vezmime si teda ľubovoľné prvočíslo p, ktoré delí číslo n a označme $2^{s'}$ najvyššiu mocninu dvojky, ktorá delí číslo $p-1$. Presnejšie nech platí $p-1 = 2^{s'}t'$, kde t' je nepárne číslo. Ukážeme, že ak je n silné pseudoprvočíslo v nejakej báze a, potom nasledujúce dve kongruencie sú ekvivalentné : $a^{2^{s'-1}t} \equiv -1 \pmod{n}$ a $a^{2^{s'-1}t'} \equiv -1 \pmod{p}$. Nech platí prvá z nich. Keďže z Malej Fermatovej vety vieme (nakoľko n je silné pseudoprvočíslo v báze a, určite platí $(a,p) = 1$), že $a^{p-1} \equiv 1 \pmod{p}$, platí $a^{2^{s'}t'} \equiv 1 \pmod{p}$. Túto kongruenciu možno prepísať na tvar $(a^{2^{s'-1}t'} - 1)(a^{2^{s'-1}t'} + 1) \equiv 0 \pmod{p}$. Pretože p je prvočíslo, a teda fakt, že delí súčin znamená, že musí deliť niektorého zo súčiniteľov, stačí nám ukázať, že platí $a^{2^{s'-1}t'} \not\equiv 1 \pmod{p}$ a bude nutne platiť $a^{2^{s'-1}t'} \equiv -1 \pmod{p}$. Predpokladajme sporom, že platí $a^{2^{s'-1}t'} \equiv 1 \pmod{p}$, potom aj $a^{2^{s'-1}t't} \equiv 1 \pmod{p}$. Umocnením kongruencie $a^{2^{s'-1}t} \equiv -1 \pmod{n}$ na t'-tu, keďže t' je nepárne číslo, dostaneme $a^{2^{s'-1}tt'} \equiv -1 \pmod{n}$, čo už implikuje spornú kongruenciu $a^{2^{s'-1}tt'} \equiv -1 \pmod{p}$ (p je totiž deliteľom n). Predpokladajme teraz naopak najprv že platí $a^{2^{s'-1}t'} \equiv -1 \pmod{p}$. Podľa predpokladu n je

silné pseudoprvočíslo v báze a. Prešlo teda testom, čo znamená, že splnilo niektorú z kongruencií. Nech najprv $a^t \equiv 1 \pmod{n}$. Potom umocnením dostávame $a^{2^{s'-1}tt'} \equiv 1 \pmod{n}$, preto aj $a^{2^{s'-1}tt'} \equiv 1 \pmod{p}$. Na druhej strane priamo z predpokladov máme tiež umocnením $a^{2^{s'-1}t't} \equiv -1 \pmod{p}$ (využívame pritom, že t je nepárne), čo je opäť spor. Nech teda pre nejaké $0 \leq i \leq s-1$ platí $a^{2^i t} \equiv -1 \pmod{n}$. Z dôkazu lemy 5.2 plynie, že platí $i+1 \leq \nu(n)$. Z definície čísla $\nu(n)$ navyše priamo dostávame, že $\nu(n) \leq s'$, čo znamená, že platí $i+1 \leq s'$, alebo $i \leq s'-1$. Predpokladajme sporom, že $i < s'-1$, v takom prípade umocnením kongruencie $a^{2^i t} \equiv -1 \pmod{n}$ na $2^{s'-i-1}$−tu dostaneme $a^{2^{s'-1}t} \equiv 1 \pmod{n}$. Ak umocníme ďalej túto kongruenciu na nepárne číslo t' a využijeme, že $p \mid n$, dostávame $a^{2^{s'-1}tt'} \equiv 1 \pmod{p}$. Umocnením predpokladu na nepárne číslo t dostávame spornú kongruenciu $a^{2^{s'-1}t't} \equiv -1 \pmod{p}$. Ukázali sme teda, že platí $i = s'-1$, odkiaľ zároveň $a^{2^{s'-1}t} \equiv -1 \pmod{n}$. Tým sme ukončili dôkaz pomocného tvrdenia a môžeme sa zaoberať tvrdením zo zadania. Ako sme spomenuli, číslo n je deliteľné aspoň dvomi prvočíslami, každým v presne prvej mocnine. Vezmime si ľubovoľné 2 z nich a označme ich p_1, p_2, ďalej podobne ako vyššie píšme $p_1 = 2^{s_1}t_1$, $p_2 = 2^{s_2}t_2$, kde t_1, t_2 sú nepárne a navyše bez ujmy na všeobecnosti nech platí $s_1 \leq s_2$. Budeme sa zaoberať nasledujúcimi Dirichletovymi charaktermi definovanými pomocou Jacobiho symbolu : $\chi_1(a) = \left(\frac{a}{p_1 p_2}\right)$ a $\chi_2(a) = \left(\frac{a}{p_2}\right)$, prvý modulo $p_1 p_2$, druhý modulo p_2. Predpokladajme najprv, že $s_1 = s_2$. Z vety A.3, ktorá je dôsledkom Riemannovej hypotézy dostávame priamo, že existuje také číslo a, pre ktoré platí $a < 2\ln^2 p_1 p_2$ a $\chi_1(a) \neq 1$. Zrejme $a < 2\ln^2 n$, ukážeme, že sa jedná o svedka. Nerovnosť $\chi_1(a) = \left(\frac{a}{p_1 p_2}\right) \neq 1$ implikuje jednu z rovností $\left(\frac{a}{p_1 p_2}\right) = 0$ a $\left(\frac{a}{p_1 p_2}\right) = -1$. Prvá z nich priamo vedie k tomu, že a je deliteľné niektorým z prvočísel p_1, p_2, a teda je svedkom. Druhá znamená, keď použijeme definíciu Jacobiho symbolu, že Legendrove symboly $\left(\frac{a}{p_1}\right)$ a $\left(\frac{a}{p_2}\right)$ majú rôzne hodnoty 1 a -1. Teraz použijeme naše pomocné tvrdenie spolu s vetou 4.1 (Eulerovym kritériom). Tie nám vravia, že tvrdenie $\left(\frac{a}{p_i}\right) = -1$ je ekvivalentné s kongruenciou $a^{2^{s_i-1}t_i} \equiv -1 \pmod{p_i}$, ktorá je zas ekvivalentná kongruencii $a^{2^{s_i-1}t} \equiv -1 \pmod{n}$. Pretože $s_1 = s_2$, táto kongruencia vyzerá pre obidve prvočísla rovnako, a teda aj tvrdenia $\left(\frac{a}{p_1}\right) = -1$ a $\left(\frac{a}{p_2}\right) = -1$ sú navzájom ekvivalentné, čo je ale spor. Rozoberme teda aj druhú možnosť, nech $s_1 < s_2$.

Opäť použitím dôsledku Riemannovej hypotézy, vety A.3, dostávame pre druhý Dirichletov charakter, že musí existovať číslo $a < 2\ln^2 p_2 < 2\ln^2 n$, pre ktoré platí $\chi_2(a) = \left(\frac{a}{p_2}\right) \neq 1$. To znamená, že buď $\left(\frac{a}{p_2}\right) = 0$ alebo $\left(\frac{a}{p_2}\right) = -1$. V prvom prípade je a zrejme svedok, nakoľko je deliteľné číslom p_2. Nech teda $\left(\frac{a}{p_2}\right) = -1$. Použitím vety 4.1 a výsledku z prvej časti dôkazu dostávame, že platí $a^{2^{s_2-1}t} \equiv -1 \pmod{n}$. Ak by sme predpokladali, že n je silné pseudoprvočíslo v báze a, a teda a nie je svedok, potom podľa vety 5.2 musí platiť jedna z kongruencií $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$ a $a^{2^{\nu(n)-1}t} \equiv -1 \pmod{n}$. Každopádne pre všetky $k \geq \nu(n)$ platí $a^{2^k t} \equiv 1 \pmod{n}$ (to zistíme jednoduchým umocnením oboch kongruencií na $2^{k-\nu(n)+1}$−tu). To ale znamená, že musí platiť $s_2 - 1 < \nu(n)$, alebo $s_2 \leq \nu(n)$. To ďalej vzhľadom na definíciu čísla $\nu(n)$ znamená, že platí $2^{s_2} \mid p_1 - 1 = 2^{s_1}t_1$. Z tohto vzťahu ale už dostávame spor, nakoľko implikuje nerovnosť $s_2 \leq s_1$, ktorá je opačnou k predpokladanej $s_2 > s_1$. Tým sme prebrali všetky možnosti a ukončili dôkaz. ■

Literatúra

[1] N. C. Ankeny: *The Least Quadratic Non-Residue.* Annals of mathematics, 55 (1952), s. 65-72

[2] M. Artjuhov: *Certain criteria for the primality of numbers connected with the little Fermat theorem.* Acta Arith., 123 (1966/67), s. 55?364.

[3] E. Bach: *Explicit bounds for primality testing and related problems.* Math. Comp., s. 355-380, 1990.

[4] R. Burthe, Jr.: *Further investigations with the strong probable prime test.* Math. Comp., 65:213 (1996), s. 373-381.

[5] H. Cohn: *Advanced number theory.* Dover Publications, 1980. ISBN 0-486-64023-X

[6] R. Crandall, C. Pomerance: *Prime Numbers - A computational perspective.* Springer-Verlag, New York, 2001

[7] G. H. Hardy, E. M. Wright: *An introduction to the theory of numbers.* Oxford university press, 1975. ISBN 0-19-853310-7

[8] M. Kolibiar a kol.: *Algebra a príbuzné disciplíny.* Alfa, Bratislava, 1992. ISBN 80-05-00721-3.

[9] S. Konyagin, C. Pomerance: *On primes recognizable in deterministic polynomial time, The mathematics of Paul Erdös, R. L. Graham and J. Nesetril.* Springer-Verlag, Berlin, s. 176-198, 1997.

[10] W. L. McDaniel : *Some pseudoprimes and related numbers having special forms.* Mathematics of Computation, 53:187 (1989), s.407-409

[11] G. L. Miller: *Riemann's hypothesis and tests for primality.* Proceedings of seventh annual ACM symposium on Theory of computing, Albuquerque, New Mexico, United States, s. 234-239, 1975.

[12] L. Monier: *Evaluation and comparison of two efficient probabilistic primality testing algorithms.* Theoret. Comput. Sci., 12 (1980), s. 97-108.

[13] M. Rabin: *Probabilistic algorithms.* Algorithms and Complexity (Proc. Sympos., Carnegie-Mellon Univ., Pittsburgh, PA, 1976), Academic Press, s. 21?39, 1976.

[14] M. Rabin: *Probabilistic algorithm for testing primality.* J. Number Theory, 12 (1980), s. 128?138.

[15] B. Schneier: *Applied cryptography.* John Wiley & Sons, 1996. ISBN 0-471-11709-9

[16] D. R. Stinson: *Cryptography theory and practice.* CRC Press, 1995. ISBN 0-8493-8521-0

[17] Š. Znám: *Teória čísel.* Alfa, vydavateľstvo technickej a ekonomickej literatúry, 1986.

Abstrakt

Práca sa zaoberá metódami testovania prvočíselnosti, konkrétne predovšetkým myšlienkovou líniou založenou na dôsledkoch Malej Fermatovej vety. Opisuje pojem pseudoprvočísel ako prekážky efektívneho využitia algoritmov a zaoberá sa ich existenciou a relatívnou početnosťou v množine prirodzených čísel. Podáva prehľad metód, ktoré postupne zlepšujú pravdepodobnosť úspechu a všetky sú z hľadiska výpočtovej zložitosti polynomiálne od veľkosti vstupu. Takisto sa zaoberá Riemannovou hypotézou a jej dôsledkami, ktoré priamo súvisia s Miller-Rabinovym prvočíselným testom a umožnujú upraviť ho do deterministickej podoby. Práca je predovšetkým prehľadom teoretického pozadia metód a nezaoberá sa do podrobností praktickými aplikáciami ani otázkami výpočtovej zložitosti. Mala by však poskytovať ucelený pohľad na teoretické pozadie nutné pri skúmaní testov z hľadiska matematickej korektnosti a pravdepodobnosti ich omylu v nedeterministickej podobe.