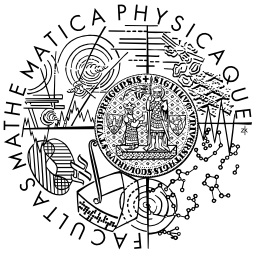

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Sára Vyhnalová

Solovay-Strassenův test prvočíselnosti

Katedra algebry

Vedoucí bakalářské práce: Mgr. Vítězslav Kala, Ph.D.
Studijní program: Matematika
Studijní obor: Matematika pro informační technologie

Praha 2019

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Týmto by som chcela poďakovať vedúcemu práce Mgr. Vítězslavu Kalovi, Ph.D. za mimoriadne ochotný prístup, dobré nápady a dôležité pripomienky. Tiež ďakujem spolužiakovi Samuelovi Staškovi za pomoc s LaTeXom a formátovaním PDF-A a mojej rodine za neustálu podporu.

Název práce: Solovay-Strassenův test prvočíselnosti

Autor: Sára Vyhnalová

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Táto práca sa venuje algoritmu na testovanie prvočíselnosti celého čísla n, založeného na výpočte Jacobiho symbolu, nazývaného Solovay-Strassenov test. Po sformulovaní samotného algoritmu odhadneme pravdepodobnosť, že testované číslo n je skutočne prvočíslo, ak to o ňom vyhlásil Solovay-Strassenov test. Práca ponúka aj vylepšenie výpočtu využívajúce, že n nie je deliteľné konkrétnymi malými prvočíslami, čo môžeme veľmi jednoducho overiť. V záverečnej časti ide o konštrukciu vlastného testu, ako obdoby k Solovay-Strassenovmu testu, založeného na výpočte kvartického symbolu.

Klíčová slova: Jacobiho symbol, Solovay-Strassenov test, kvartický symbol

Title: Solovay-Strassen primality test

Author: Sára Vyhnalová

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: This thesis studies the Solovay-Strassen test for primality of an integer n, which is based on the Jacobi symbol. After formulating the basic algorithm, we compute the probability that the number n being tested is really a prime number if the Solovay-Strassen test declared it so. We further improve the computation of the probability under the assumption that n is not divisible by specific small primes, which can be easily verified. Finally, we construct a new test, as an analogy of the Solovay-Strassen test, based on the quartic residue symbol.

Keywords: Jacobi symbol, Solovay-Strassen test, quartic symbol

Obsah

Úvod

Solovay-Strassenov test prvočíselnosti je algoritmus vytvorený Robertom M. Solovayom a Volkerom Strassenom v roku 1977 ako pravdepodobnostný test na určenie, či je testované číslo prvočíslo alebo nie. Kapitola 1 je venovaná práve tomuto testu. Vychádzali sme v nej z textu amerického matematika Keitha Conrada s názvom „The Solovay-Strassen test“ (Conrad, kapitola 1, 2 a 3). Testovací algoritmus je založený na výpočte Jacobiho symbolu $\left(\frac{a}{n}\right)$ pre rôzne $a \in \mathbb{Z}$ na jednej strane, ten porovnávame s hodnotou $a^{(n-1)/2}$ modulo skúmané číslo n na strane druhej. Pre prvočíslo n táto rovnosť vždy platí, pre zložené číslo, ako uvidíme v prvej kapitole, je celých čísel a, ktoré nespĺňajú túto rovnosť, značný počet. Vďaka zákonu kvadratickej reciprocity je Jacobiho symbol možné spočítať bez znalosti prvočíselného rozkladu čísla n.

V rovnakom texte, ale v odlišnej časti (Conrad, časť Appendix) je spracovaný aj výpočet pravdepodobnosti, že skúmané číslo je prvočíslo, ak ho test označil za prvočíslo. Naším cieľom je výpočet pravdepodobnosti vylepšiť, a to v kapitole 2 tejto práce.

Výpočet z textu (Conrad) ukazuje odhad, že n je prvočíslo, za podmienky, že test ho takto označil a nepredpokladá znalosť ďalších vlastností čísla n. V skutočnosti je však veľmi jednoduché zistiť, či skúmané číslo n nie je deliteľné malými prvočíslami, napríklad 2, 3, 5, a podobne. Do nášho výpočtu pravdepodobnosti teda zahrnieme aj tento fakt. Tým sa odhad pravdepodobnosti, že n je prvočíslo, zväčší.

V kapitole 3 sa pokúsime skonštruovať test obdobný Solovay-Strassenovmu, založený na výpočte kvartického symbolu, pričom vopred uvedieme potrebnú teóriu týkajúcu sa kvartických symbolov. Ako hlavný zdroj pri budovaní základov v teórii kvartických symbolov nám poslúžila kniha autorov Kenneth Ireland a Michael Rosen s názvom „Introduction to Modern Number Theory“ (Ireland a Rosen, 2013, kapitola 9). V sekcii 3.3.2 sformulujeme a dokážeme vlastné tvrdenia, ku ktorým nás inšpirovali Solovay-Strassenove vety, sformulované a dokázané v prvej kapitole.

1. Solovay-Strassenov test prvočíselnosti

1.1 Opakovanie

V nasledujúcej krátkej sekcii zhrnieme definície a tvrdenia, ktoré sú známe z predmetu Teória čísel a RSA a budeme sa na nich odvolávať bez dôkazu. Všetky sa v trochu pozmenenej podobe nachádzajú v skriptách (Drápal). Na začiatok uvedieme niekoľko poznámok k značeniu:

Značenie. Nech R je gaussovský obor. Pre $a, b \in R$ označíme $a \parallel b$, ak $a \mid b$ (a delí b), a súčasne $b \mid a$ (b delí a). V práci sa stretneme najmä s $R = \mathbb{Z}$ a $R = \mathbb{Z}[i]$.

Značenie. Aby sme sa vyhli nezrovnalostiam, v celej práci budeme pre kongruencie využívať nasledujúce značenie: Pre $a, b, n \in \mathbb{Z}$ $a \equiv b \bmod n\mathbb{Z}$ znamená, že $n \mid (a - b)$ v $\mathbb{Z}$. Pre $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ $\alpha \equiv \beta \bmod \gamma\mathbb{Z}[i] \Leftrightarrow \gamma \mid \alpha - \beta$ v $\mathbb{Z}[i]$.

Značenie. Značením $\mathbb{Z}/n\mathbb{Z}$ rozumieme faktorokruh okruhu $\mathbb{Z}$ podľa ideálu $(n) = n\mathbb{Z}$. Z algebry vieme, že $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. V nasledujúcom texte budeme tieto okruhy stotožňovať.

Definícia 1. *Nech $n \in \mathbb{Z}$. Povieme, že n je* bezštvorcové, *ak sa v jeho prvočíselnom rozklade nevyskytuje žiadne prvočíslo vo vyššej ako prvej mocnine.*

1.1.1 Legendrov symbol a jeho vlastnosti

Definícia 2. *Nech p je nepárne prvočíslo, $a \in \mathbb{Z}$. Povieme, že a je* kvadratický zvyšok *modulo p, ak existuje celé číslo x také, že $x^2 \equiv a \bmod p\mathbb{Z}$. V opačnom prípade sa a nazýva* kvadratický nezvyšok.

Definícia 3. *Pre nepárne prvočíslo p definujeme* Legendrov symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ak } a \text{ je kvadratickým zvyškom } \bmod p\mathbb{Z} \text{ a } p \nmid a \\ 0 & \text{ak } p \mid a \\ -1 & \text{inak} \end{cases}$$

Tvrdenie 4. *Nech p je nepárne prvočíslo, $a \in \mathbb{Z}$. Pre Legendrov symbol platí:*

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

Tvrdenie 5. *Presne polovica nenulových čísel modulo prvočíslo p sú štvorce, ekvivalentne $\left(\frac{a}{p}\right) = 1$ pre $(p-1)/2$ čísel $a \in \mathbb{Z}/p\mathbb{Z}$. Ostatné nenulové čísla modulo prvočíslo p nie sú štvorce, ekvivalentne $\left(\frac{a'}{p}\right) = -1$ pre zvyšných $(p-1)/2$ nenulových čísel $a' \in \mathbb{Z}/p\mathbb{Z}$.*

Tvrdenie 6. *Ak je p nepárne prvočíslo, potom $\left(\frac{-1}{p}\right) = 1$ práve vtedy, keď je $p \equiv 1 \bmod 4$, inými slovami -1 je kvadratický zvyšok modulo p práve vtedy, keď $p \equiv 1 \bmod 4$.*

1.1.2 Jacobiho symbol a jeho vlastnosti

Zovšeobecnením Legendrovho symbolu je Jacobiho symbol:

Definícia 7. *Pre nepárne prirodzené číslo n a celé číslo a definujeme* Jacobiho symbol*:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdots \left(\frac{a}{p_r}\right)^{k_r},$$

kde $n \parallel p_1^{k_1} \cdots p_r^{k_r}$ je prvočíselný rozklad čísla n.

Tvrdenie 8 (Tvrdenia pre výpočet Jacobiho symbolu)**.** *Nech a, $b \in \mathbb{Z}$ a n je nepárne prirodzené číslo.*

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
2. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$

Veta 9 (Zákon kvadratickej reciprocity)**.** *Nech sú $m, n \in \mathbb{N}$ nesúdeliteľné čísla. Potom platí:*

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

1.1.3 Fermatov test

Fermatov test prvočíselnosti je jednoduchý test založený na nasledujúcej vete.

Veta 10 (Malá Fermatova)**.** *Nech p je prvočíslo. Potom pre každé $a \in \mathbb{Z}$ také, že $(a,p) = 1$ platí*

$$a^{p-1} \equiv 1 \bmod p\mathbb{Z}.$$

Ak chceme otestovať, či je zadané číslo n prvočíslo, pre rôzne hodnoty $a \in \{1,2,\ldots n-1\}$ overíme, či platí $a^{n-1} \equiv 1 \bmod n\mathbb{Z}$. Problémom sú však tzv. Carmichaelove čísla, u ktorých jediné hodnoty a, pre ktoré neplatí $a^{n-1} \equiv 1 \bmod n\mathbb{Z}$, sú súdeliteľné s n a tých môže byť minimálne množstvo (uvidíme názorný príklad v sekcii 3.3.1.

Definícia 11. Carmichaelovo číslo *je zložené číslo n také, že pre všetky $a \in \mathbb{Z}$ také, že $(a,n) = 1$ platí*

$$a^{n-1} \equiv 1 \bmod n\mathbb{Z}.$$

1.2 Solovay-Strassenove vety

V tejto sekcii sme vychádzali z článku (Conrad). Solovay-Strassenovu vetu aj dôsledok s dôkazmi sme s malými úpravami čerpali práve z tohto zdroja.

Solovay-Strassenov test je algoritmus, ktorý na vstupe dostane nepárne celé číslo n a má za úlohu otestovať, či ide o prvočíslo. Test je založený na fakte, že pre prvočíslo n podľa tvrdenia 4 platí $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\mathbb{Z}$ pre $\forall a \in \mathbb{Z}$, ale pre zložené n to tak nie je.

Ako uvidíme v nasledujúcich tvrdeniach tejto kapitoly, platí dokonca, že čísel $a \in \{1,\ 2,\ \ldots,\ n-1\}$, ktoré túto kongruenciu nespĺňajú, je viac ako polovica. Na ľavej strane kongruencie $\left(\frac{a}{n}\right)$ značí Jacobiho symbol (pre prvočíslo n je Jacobiho symbol zjavne rovný Legendrovmu symbolu).

Definícia 12. *Nech n je nepárne prirodzené číslo,* Eulerovým svedkom pre n *nazveme celé číslo $a \in \{1, \ldots, n\}$ také, že*

$$(a,n) = 1 \ \& \ \left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n\mathbb{Z}$$

Predtým, ako sformulujeme samotný testovací algoritmus, dokážeme dôležitú vetu a jej dôsledok, a to, že pre každé zložené číslo n existuje Eulerov svedok, a že množina Eulerových svedkov pre n má znateľné zastúpenie v množine $\{1, \ldots, n\}$.

Veta 13 (Solovay-Strassen)**.** *Pre každé n zložené nepárne prirodzené číslo existuje celé číslo a také, že $(a,n) = 1$ a*

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n\mathbb{Z}$$

Dôkaz. Rozlíšime 2 prípady: n je bezštvorcové zložené číslo. Nech $n \parallel p_1 \cdots p_r$, kde $p_1, \ldots, p_r$ sú nepárne prvočísla. Keďže je n zložené, $r > 1$ a n je bezštvorcové, čiže $p_i \neq p_j$ pre $i \neq j$. Podľa tvrdenia 5 existuje $b \in \mathbb{Z}, b \neq 0$ také, že $\left(\frac{b}{p_1}\right) = -1$. Čísla p_1 a $p_2 \cdots p_r$ sú nesúdeliteľné. Z čínskej vety o zvyškoch (nájdeme ju sformulovanú aj dokázanú napríklad v skriptách Počítačovej algebry, (Stanovský a Barto, 2017, Věta 6.1)), teda existuje $a \in \{1, 2, \ldots, p_1 p_2 \cdots p_r - 1\}$ také, že

$$a \equiv b \bmod p_1\mathbb{Z}, \text{ a súčasne } a \equiv 1 \bmod p_2 \cdots p_r\mathbb{Z}.$$

Keďže $b \not\equiv 0 \bmod p_1\mathbb{Z}$, máme $(a,p_1) = 1$. Platí tiež $(a,p_2 \cdots p_r) = 1$. Z toho vyplýva, že aj $(a,n) = 1$. Rozpíšeme:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right). \tag{1.1}$$

Z kongruencie $a \equiv b \bmod p_1\mathbb{Z}$ máme $\left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$ a z kongruencie $a \equiv 1 \bmod p_2 \cdots p_r\mathbb{Z}$ zase plynie $\left(\frac{a}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$ pre $i > 1$. Po dosadení do (1.1) dostávame $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) = -1$.

Pre spor predpokladajme, že $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \equiv -1 \bmod n\mathbb{Z}$. Využijeme, že p_2 delí n a prevedieme túto kongruenciu na kongruenciu modulo $p_2\mathbb{Z}$. Keďže $a \equiv 1 \bmod p_2\mathbb{Z}$, dostávame $1 \equiv -1 \bmod p_2\mathbb{Z}$, čo je spor, pretože p_2 je nepárne prvočíslo a $p_2 \nmid 2$. Takže sme ukázali, že $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}$.

Teraz predpokladajme, že n obsahuje faktor p aspoň v druhej mocnine, tj. n je tvaru $n = p^k m$, kde p je nepárne prvočíslo, $k \geq 2$ a $(p, m) = 1$. Podľa čínskej vety o zvyškoch existuje $a \in \mathbb{Z}$ spĺňajúce

$$a \equiv 1 + p \bmod p^2\mathbb{Z}, \text{ a súčasne } a \equiv 1 \bmod m\mathbb{Z}.$$

Keďže $p \nmid a$ a $(a,m) = 1$, platí aj $(a,n) = 1$. Predpokladajme pre spor, že $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\mathbb{Z}$. Umocnením oboch strán na druhú získavame $a^{n-1} \equiv 1 \bmod n\mathbb{Z}$. Keďže $p^2 \mid n$ platí aj $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod p^2\mathbb{Z}$. Celkovo dostávame

$$1 \equiv a^{n-1} \equiv (1+p)^{n-1} \equiv \sum_{i=0}^{n-1} \binom{n-1}{i} 1^{n-1-i} p^i \equiv 1 + (n-1)p \bmod p^2\mathbb{Z}.$$

Odpočítaním jednotky dostávame $(n-1)p \equiv 0 \bmod p^2\mathbb{Z}$, čiže $p \mid n-1$. To je ale spor, pretože $p \mid n$, nemôže deliť aj $n-1$. Opäť sme ukázali, že $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}}$. □

Dôsledok 14. *Nech $n > 1$ je celé nepárne číslo.*

1. *Ak je n prvočíslo, potom*

$$| \{1 \leq a \leq n-1 : (a,n) = 1 \ a \ a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\mathbb{Z}\} | = n-1.$$

2. *Ak je n zložené číslo, potom*

$$| \{1 \leq a \leq n-1 : (a,n) = 1 \ a \ a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\mathbb{Z}\} | < \frac{n-1}{2}.$$

Poznámka. Vo formulácii dôsledku sme v bode *1* napísali, že berieme hodnoty $1 \leq a \leq n-1 : (a,n) = 1$. Pre prvočíslo n je podmienka $(a,n) = 1$ zjavne splnená pre každú voľbu $1 \leq a \leq n-1$. Uviedli sme to však kvôli zdôrazneniu paralely s bodom *2*.

Dôkaz.

1. Vyplýva z tvrdenia 4.
2. Položme množiny

$$\begin{aligned} A &= \{1 \leq a \leq n-1 : (a,n) = 1 \text{ a } a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\mathbb{Z}\}, \\ B &= \{1 \leq a \leq n-1 : (a,n) = 1 \text{ a } a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n\mathbb{Z}\}, \\ C &= \{1 \leq a \leq n-1 : (a,n) > 1\}. \end{aligned}$$

Množiny A, B, C sú disjunktné a ich zjednotenie $A \cup B \cup C = \{1, \ldots, n-1\}$. Platí teda $|A| + |B| + |C| = n-1$.

Vieme, že množina A je neprázdna, pretože $1 \in A$. Tiež vieme, že C nie je prázdna, pretože n je zložené, teda $|C| \geq 1$. Množina B je neprázdna vďaka vete 13.

Ak ukážeme, že $|A| \leq |B|$, dostaneme $n-1 = |A|+|B|+|C| \geq |A|+|A|+1 > 2|A|$ a tým aj požadovaný odhad $|A| < \frac{n-1}{2}$.

Aby sme ukázali $|A| \leq |B|$, skonštruujeme si pomocnú množinu rovnakej veľkosti ako A, ktorá bude podmnožinou B. Vezmime prvok množiny B, nech to je b_0. Označme $Ab_0 = \{ab_0 \bmod n\mathbb{Z} : a \in A\}$. Veľkosť $|A| = |Ab_0|$, pretože $ab_0 \equiv a'b_0 \bmod n\mathbb{Z} \Leftrightarrow a \equiv a' \bmod n\mathbb{Z}$, tj, $a = a'$, lebo v A ležia prvky z množiny $\{1, \ldots, n-1\}$. Stačí teda ukázať, že $Ab_0 \subset B$. Každé $ab_0 \in Ab_0$ a n sú nesúdeliteľné a platí:

$$(ab_0)^{(n-1)/2} \equiv a^{(n-1)/2} b_0^{(n-1)/2} \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \bmod n\mathbb{Z}.$$

Keďže $(ab_0,n) = 1$, každé $ab_0 \bmod n\mathbb{Z}$ patrí buď do množiny A alebo do množiny B. Predpokladajme, že $ab_0 \bmod n\mathbb{Z} \in A$, čiže

$$(ab_0)^{(n-1)/2} \equiv \left(\frac{ab_0}{n}\right) \equiv \left(\frac{a}{n}\right)\left(\frac{b_0}{n}\right) \bmod n\mathbb{Z}.$$

Spolu s predchádzajúcim vyjadrením tak dostávame

$$\left(\frac{a}{n}\right) b_0^{(n-1)/2} \equiv \left(\frac{a}{n}\right)\left(\frac{b_0}{n}\right) \bmod n\mathbb{Z}.$$

Keďže $(a,n) = 1$, platí $\left(\frac{a}{n}\right) = \pm 1$, takže môžeme kongruenciu vykrátiť a obdržíme $\left(\frac{b_0}{n}\right) \equiv b_0^{(n-1)/2} \bmod n\mathbb{Z}$, čo je spor s $b_0 \in B$. Dokázali sme teda, že každé $ab_0 \bmod n\mathbb{Z} \in B$, teda $Ab_0 \subset B$.

Celkovo dostávame $|A| = |Ab_0| \geq |B|$. Takže $n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|$, a teda $|A| < \frac{n-1}{2}$. □

Dôsledok 14 nám hovorí, že zastúpenie Eulerových svedkov pre n v množine $\{1, \ldots, n\}$ je 0 % pre prvočíslo n a ponad 50 % pre zložené číslo n.

Tento fakt poskytuje dobrý dôvod pre vytvorenie Solovay-Strassenovho testu, ktorý slúži na overovanie, či je nepárne číslo $n > 1$ prvočíslo.

1.3 Solovay-Strassenov test

TEST 1.

Vstup: $n \in \mathbb{N}$, nepárne číslo.

1. Zafixujeme celé číslo $t \geq 1$ ako počet pokusov pre test.
2. Vezmeme náhodné číslo $a \in \{1, \ldots, n-1\}$.
3. Overíme, či platí $(a,n) = 1$. Ak odhalíme $(a,n) > 1$, test ukončíme s prehlásením, že „n je zložené“. V opačnom prípade pokračujeme.
4. Ak $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n\mathbb{Z}$, test ukončíme s vyhlásením, že „n je zložené“.
5. Ak $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\mathbb{Z}$, pokračujeme krokom 2.
6. Keď test prebehne t-krát bez nájdenia Eulerovho svedka pre n, vyhlásime, že „n je pravdepodobne prvočíslo.“

Poznámka. V treťom kroku testovacieho algoritmu zisťujeme najväčšieho spoločného deliteľa čísel a a n, na čo môžeme využiť Eukleidov algoritmus. Niekedy sa nám v t pokusoch podarí odhaliť $(a,n) > 1$, rozhodne to ale nenastane vždy. Zastúpenie súdeliteľných čísel s n v množine $\{1, \ldots, n-1\}$ môže byť totiž minimálne.

Poznámka. V Solovay-Strassenovom teste počítame Jacobiho symbol, ktorý sa vďaka zákonu kvadratickej reciprocity (veta 9) dá spočítať bez znalosti prvočíselného rozkladu čísla n, a to nasledujúcim algoritmom.

1.3.1 Algoritmus pre výpočet Jacobiho symbolu

Vstup: a, $n \in \mathbb{Z}$, n nepárne číslo.
Výstup: $\left(\frac{a}{n}\right)$.

1. Overíme, či sú čísla súdeliteľné, ak áno, rovno vyšleme na výstup hodnotu 0.
2. Zredukujeme číslo a modulo $n\mathbb{Z}$.

3. Rozpíšeme $a = 2^k m$, kde m je nesúdeliteľné s 2 a využijeme multiplikativitu Jacobiho symbolu (bod 1 tvrdenia 8). Podľa bodu 2 v tvrdení 8 potom spočítame $A := \left(\frac{2}{n}\right)^k$. Dostaneme tak $\left(\frac{a}{n}\right) = A\left(\frac{m}{n}\right)$.

4. Ak je m rovné 1, vrátime na výstup $\left(\frac{a}{n}\right) = A$. V opačnom prípade pokračujeme.

5. Vďaka zákonu kvadratickej reciprocity (Veta 9) platí nasledujúca rovnosť: $\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right)$. Rekurzívne teda spustíme algoritmus pre hodnoty n a m. Výsledná hodnota jacobiho symbolu $\left(\frac{a}{n}\right)$ bude potom rovná $\left(\frac{a}{n}\right) = A\left(\frac{m}{n}\right)$.

2. Výpočet pravdepodobnosti

V kroku 6 vo formulácii Solovay-Strassenovho testu v sekcii 1.3 sa vyhlásenie, že n je „pravdepodobne“ prvočíslo, spája s pravdepodobnosťou, že skúmané číslo n je prvočíslo za podmienky, že Solovay-Strassenov test prebehol t-krát bez nájdenia Eulerovho svedka. Výpočet tejto pravdepodobnosti sa nachádza v článku (Conrad, Appendix). Našou úlohou je v nasledujúcej sekcii odhad pravdepodobnosti z článku vylepšiť. Spôsob, akým to môžeme dosiahnuť, je heuristicky odhadnúť pravdepodobnosť, že číslo n je prvočíslo, ak Solovay-Strassenov test prebehol bez prerušenia, pričom vieme, že n nie je deliteľné danými malými prvočíslami.

2.1 Zhrnutie faktov pre výpočet pravdepodobnosti

Značenie. Nech Ω je neprázdna množina a $\Im$ značí systém podmnožín Ω. Pripomeňme nasledujúce pojmy z predmetu Pravděpodobnost a statistika, podrobnejšie vysvetlenie nájdeme v texte k predmetu (Hlubinka).

- Zobrazenie $P : \Im \to (0,1)$ sa nazýva *pravdepodobnosť*.
- Prvok $\omega \in \Omega$ sa nazýva *elementárny jav*.
- $A \in \Im$ sa nazýva *náhodný jav*.

V celej kapitole pre 2 náhodné javy A a B značíme $P(A \mid B)$ *podmienenú pravdepodobnosť* javu A za podmienky, že nastal jav B, s definíciou

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}.$$

Označením A' rozumieme *doplnkový jav* k javu A, teda jav, pre ktorý platí, že $P(A) + P(A') = 1$.

Veta 15 (Bayesova veta)**.**

$$P(A \mid B) = \frac{P(B \mid A)\, P(A)}{P(B \mid A)P(A) + P(B \mid A')P(A')},$$

kde A,B sú náhodné javy a $P(B) \neq 0$

Dôkaz.

$$\begin{aligned} P(A \mid B) &= \frac{P(A \cap B)}{P(B)} \\ &= \frac{P(B \mid A)P(A)}{P(B)} \\ &= \frac{P(B \mid A)P(A)}{P(B \mid A)P(A) + P(B \mid A')P(A')}, \end{aligned}$$

kde poslednú rovnosť získame použitím:

$$\begin{aligned} P(B) &= P((B \cap A) \cup (B \cap A')) \\ &= P(B \cap A) + P(B \cap A') \\ &= P(B \mid A)P(A) + P(B \mid A')P(A') \end{aligned}$$

□

Veta 16 (Prvočíselná veta)**.** *Platí:*

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

kde $\pi(x)$ je počet prvočísel menších alebo rovných x.

Dôkaz. Dôkaz nájdeme v článku (Zagier, 1997) . □

2.2 Základný výpočet

Najskôr uvedieme výpočet pravdepodobnosti, že n je prvočíslo, ak Solovay-Strassenov test prebehol t-krát bez prerušenia, ktorý je v trochu odlišnej podobe uvedený aj v (Conrad, Appendix).

Značenie. Symbolom $\approx$ budeme označovať heuristické odhady, napríklad ak X je jav a $m \in (0, 1)$: $P(X) \approx m$ znamená, že $P(X)$ zhruba odpovedá m. Rovnako pre nerovnosti, ktoré nedostaneme priamo, ale pomocou heuristických odhadov zavedieme označenie $\gg$.

Značenie. V celej tejto kapitole budeme označovať javy:

- X: n je prvočíslo
- X': n nie je prvočíslo
- Y_t: Solovay-Strassenov test prebehol t-krát bez nájdenia Eulerovho svedka

Poznámka. Mali by sme písať X_n, X'_n a $Y_{n,t}$ kvôli zdôrazneniu závislosti na n, ale pre zjednodušenie zápisu budeme index závislosti na n vynechávať.

Pozrime sa na to z nasledujúceho pohľadu: predstavme si, že máme množinu čísel $\{1, 2, \ldots, M\}$, $M \in \mathbb{N}$, vyberme z nej náhodné číslo n. Na toto n budeme aplikovať Solovay-Strassenov test a skúmať, aká je pravdepodobnosť, že n je skutočne prvočíslo, ak to prehlásil test. Ak test vyhlásil, že n je zložené, s istotou je n zloženým číslom. Zložitejšie je odhadnúť pravdepodobnosť pre prípad, že n je prvočíslo, značíme $P(X)$.

Výpočet $P(X)$ a $P(X')$

X a X' sú zjavne doplnkové javy. Teda súčet pravdepodobností $P(X) + P(X') = 1$. Potrebujeme odhadnúť $P(X)$, čiže pravdepodobnosť, že n je prvočíslo. $P(X')$ potom spočítame ako $1 - P(X)$. Využijeme prvočíselnú vetu (veta 16) a heuristicky odhadneme $P(X)$ ako pomer počtu prvočísel z množiny $\{1, 2, \ldots n\}$ lomeno počet všetkých čísel tejto množiny (takáto je pravdepodobnosť, že číslo vybraté z tejto množiny je prvočíslo, rovnako to platí pre výber čísla n), čiže

$$P(X) \approx \frac{n/\log n}{n} = \frac{1}{\log n}.$$

Poznámka. Ide len o heuristický odhad, v skutočnosti by sme ho mohli podľa prvočíselnej vety (veta 16) prepísať do precíznych nerovností nasledujúcim spôsobom.

Označme $\pi(x)$ počet prvočísel menších alebo rovných x. Z definície limity potom pre $\forall \epsilon > 0$ $\exists x_0$ také, že pre $\forall x > x_0$ platí

$$(1-\epsilon)\frac{x}{\log x} < \pi(x) < (1+\epsilon)\frac{x}{\log x}. \tag{2.1}$$

Na odhad pomocou dvoch nerovností by sme heuristický odhad mohli previesť takto: zvoľme pevné ϵ, napríklad z intervalu $(0,1)$. V závislosti na ϵ dostaneme hodnotu x_0. Potom pre čísla $x > x_0$ máme odhad počtu prvočísel, ktoré sú menšie než x, značený $\pi(x)$, daný vzťahom (2.1). Pre dostatočne veľké $M > x_0$ potom máme skutočné nerovnosti ohraničujúce počet prvočísel v množine $\{1, 2, \ldots, M\}$, čo využijeme pre výpočet pravdepodobnosti, že n vybraté z tejto množiny je prvočíslo.

Do týchto precíznych nerovností problém prevádzať nebudeme, heuristické odhady dostatočne ilustrujú našu situáciu.

Poznámka k javu Y_t a výpočet $P(Y_t \mid X)$ a $P(Y_t \mid X')$

Skutočnosť, že Solovay-Strassenov test prebehol t-krát bez nájdenia Eulerovho svedka, čiže nastal jav Y_t, znamená, že sa nám t-krát pri výbere náhodného prvku z množiny $\{1, 2, \ldots, n-1\}$ podarilo vybrať číslo a, ktoré nie je Eulerovým svedkom pre n. V prípade, že n je prvočíslo, jav nastane vždy, lebo žiaden Eulerov svedok pre prvočíslo n neexistuje. V prípade, že n je zložené číslo, je počet čísel, ktoré nie sú Eulerovými svedkami, v množine $\{1, 2, \ldots, n-1\}$ podľa dôsledku 14 menší ako polovica. Takže pravdepodobnosť, že Solovay-Strassenov test prebehol t-krát bez nájdenia svedka za podmienky, že n je prvočíslo, je rovná $P(Y_t \mid X) = 1^t = 1$ a za podmienky, že n je zložené číslo, $P(Y_t \mid X') < (1/2)^t = 1/2^t$.

2.2.1 Pravdepodobnosť a úspešnosť Solovay-Strassenovho testu

Chceme spočítať pravdepodobnosť, že číslo n je prvočíslo, ak to prehlásil Solovay-Strassenov test. Pravdepodobnosť, ktorá nás zaujíma, je v skutočnosti $P(X \mid Y_t)$. Odhadli sme $P(Y_t \mid X') < (1/2)^t = 1/2^t$, túto informáciu môžeme zúžitkovať vďaka Bayesovej vete (veta 15). Podľa Bayesovej vety si teda rozpíšeme:

$$P(X \mid Y_t) = \frac{P(Y_t \mid X)\, P(X)}{P(Y_t|X)P(X) + P(Y_t|X')P(X')} > \frac{1 \cdot P(X)}{1 \cdot P(X) + \frac{1}{2^t}P(X')}, \tag{2.2}$$

kde sme využili odhad $P(Y_t|X') < \frac{1}{2^t}$ a tiež sme dosadili $P(Y_t \mid X) = 1$. Môžeme do (2.2) dosadiť aj hodnoty $P(X)$, $P(X')$, ktoré sme heuristicky odhadli. Dostávame

$$P(X \mid Y_t) \gg \frac{1 \cdot 1/\log n}{1 \cdot 1/\log n + \frac{1}{2^t}(1 - 1/\log n)} = \frac{1}{1 + (\log n - 1)/2^t}.$$

Využijeme známy odhad $\dfrac{1}{1+x} > 1 - x$ pre $0 < x < 1$. Takže ak $(\log n - 1)/2^t \in (0,1)$, inými slovami $t > \log_2(\log n - 1)$, dostávame:

$$P(X \mid Y_t) \gg 1 - (\log n - 1)/2^t.$$

Poznámka. Požiadavka $t > \log_2((\log n)/2-1)$ je v skutočnosti nenáročná, pretože $\log_2((\log n)/2-1)$ je pomaly rastúca funkcia. Napríklad pre 101-ciferné číslo 10^{100} je $\log_2((\log n)/2-1) \approx 7.84276$.

Sformulujeme opäť Solovay-Strassenov test, teraz už rozšírený o výpočet pravdepodobnosti.

TEST 2.

Vstup: $n \in \mathbb{N}$, nepárne číslo.

1. Zafixujeme celé číslo $t \geq 1$ ako počet pokusov pre test, $t > \log_2(\log n - 1)$
2. Vezmeme náhodné číslo $a \in \{1, \ldots, n\}$.
3. Overíme, či platí $(a,n) = 1$. Ak odhalíme $(a,n) > 1$, test ukončíme s vyhlásením, že „n je zložené“. V opačnom prípade pokračujeme.
4. Ak $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \mod n$, test ukončíme s vyhlásením, že „n je zložené“.
5. Ak $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n$, pokračujeme krokom 2.
6. Keď test prebehne t-krát bez nájdenia Eulerovho svedka pre n, vyhlásime, že „n je prvočíslo s pravdepodobnosťou väčšou ako $1 - (\log n - 1)/2^t$“

2.3 Nedeliteľnosť n prvočíslom p

Teraz sa pokúsime o vylepšenie odhadu pravdepodobnosti z článku (Conrad, Appendix), s tým, že budeme prihliadať na skutočnosť, že v realite nie je ťažké zistiť, či číslo n, na ktoré budeme aplikovať Solovay-Strassenov test, nie je deliteľné nejakými konkrétnymi, voči n relatívne malými, prvočíslami. Vylepšenie odhadu bude spočívať vo vylepšení heuristického odhadu $P(X)$ a tým pádom aj $P(X') = 1 - P(X)$. Zvyšnými pravdepodobnosťami, konkrétne $P(Y_t \mid X)$, $P(Y_t \mid X')$, nebudeme hýbať.

Značenie. Pre určenie pravdepodobnosti, že n je prvočíslo, vediac, že nie je deliteľné prvočíslom q, zavedieme označenie $P_q(X)$, obdobne $P_q(X')$ a tiež $P_q(X \mid Y_t)$. Týmto značením deklarujeme, že množina čísel, pomocou ktorej heuristicky odhadneme pravdepodobnosť, že n je prvočíslo, sú čísla menšie alebo rovné n, ktoré sú nesúdeliteľné s q. Obdobne pre ľubovoľné číslo $m \in \mathbb{N}$ (aj zložené) $P_m(X)$ bude značiť pravdepodobnosť, že číslo n je prvočíslo za predpokladu, že vieme, že nie je súdeliteľné s m.

Budeme brať do úvahy, že o čísle, na ktoré aplikujeme Solovay-Strassenov test, vieme, že nie je deliteľné prvočíslom q. Počet prvočísel menších ako n nesúdeliteľných s q ostáva približne $(n/\log n) - 1 \approx n/\log n$, ale počet všetkých čísel menších ako n, ktoré nie sú deliteľné q, je zhruba n/q.

Pre $q = 2$ sa teda pravdepodobnosť, že n je prvočíslo, zväčší na

$$P_2(X) \approx \frac{n/\log n}{n/2} = \frac{2}{\log n}.$$

Z toho dostávame aj $P_2(X') = 1 - P_2(X) \approx 1 - 2/\log n$. Dosadíme tieto hodnoty do (2.2) už so zohľadnením faktu, že n je nepárne.

$$P_2(X \mid Y_t) \gg \frac{1 \cdot 2/\log n}{1 \cdot 2/\log n + \frac{1}{2^t}(1 - 2/\log n)} = \frac{1}{1 + ((\log n)/2 - 1)/2^t}$$

Ako v predchádzajúcej sekcii, využijeme známy odhad $\frac{1}{1+x} > 1 - x$ pre $0 < x < 1$. Takže ak $((\log n)/2 - 1)/2^t \in (0,1)$, inými slovami $t > \log_2((\log n)/2 - 1)$, dostávame:

$$P_2(X \mid Y_t) \gg 1 - ((\log n)/2 - 1)/2^t.$$

Teraz uvažujme, že o danom čísle n vieme, že nie je deliteľné číslom 3 (pracujeme s množinou $\{1,2,4,5,7,8, ..., n\}$, dostávame obdobným výpočtom ako pre číslo nedeliteľné 2 odhad (pre $t > \log_2((2\log n)/3 - 1)$)

$$P_3(X \mid Y_t) \gg 1 - ((2\log n)/3 - 1)/2^t.$$

Analogicky pri vylúčení deliteľnosti čísla n piatimi(pre $t > \log_2((4\log n)/5 - 1)$)

$$P_5(X \mid Y_t) \gg 1 - ((4\log n)/5 - 1)/2^t.$$

Obdobne by sme pravdepodobnosť spočítali pre ľubovoľné prvočíslo q. Tieto výpočty zužitkujeme a zovšeobecníme v nasledujúcej sekcii.

2.4 Všeobecná množina prvočísel

V ďalšom odstavci si rozmyslíme, ako sa zmení pravdepodobnosť, že skúmané číslo n je prvočíslo po prejdení Solovay-Strassenovým testom bez prerušenia, ak budeme vedieť, že n nie je deliteľné dvomi a viacerými rôznymi prvočíslami. Najskôr uvedieme príklad, ako sa situácia zmení pre dve konkrétne prvočísla.

Značenie. Pripomeňme, že pre ľubovoľné číslo $m \in \mathbb{N}$ (aj zložené) $P_m(X)$ značí pravdepodobnosť, že číslo n je prvočíslo za predpokladu, že vieme, že nie je súdeliteľné s m.

2.4.1 Názorný príklad

Príklad. Predpokladajme, že n nie je deliteľné 2 ani 3. Najskôr chceme spočítať pravdepodobnosť, že n je prvočíslo, v našom značení teda $P_6(X)$. Na začiatok, máme množinu čísel $\{1, 2, \ldots, n\}$. Teraz odtiaľto vylúčime čísla súdeliteľné s 2 a tiež súdeliteľné s 3. Rovnaký efekt dosiahneme, ak vyhodíme čísla súdeliteľné s číslom 6. Zostane nám teda množina $A = \{1, 5, 7, 11, \ldots, n\}$.

V každej šestici po sebe idúcich čísel v množine $\{1,2 \ldots, n\}$ je nesúdeliteľných čísel so 6 práve $\varphi(6)$ (vyplýva z modulárnej aritmetiky modulo 6 a definície Eulerovej funkcie). Celkový počet čísel nesúdeliteľných so 6 v množine $\{1, 2, \ldots, n\}$ je potom rovný $\lfloor \frac{n}{6} \rfloor \varphi(6) + z$, kde z je počet nesúdeliteľných čísel s 6 v množine $\{\varphi(6)\lfloor \frac{n}{6} \rfloor + 1, \varphi(6)\lfloor \frac{n}{6} \rfloor + 2, \ldots, n\}$, ktorej veľkosť je menšia ako 6. Hodnota z bude zjavne menšia alebo rovná $\varphi(6)$.

Pravdepodobnosť $P_6(X)$, že n je prvočíslo s využitím faktu, že je nesúdeliteľné so 6, budeme takto môcť spočítať ako

$$P_6(X) \approx \frac{n/\log n - 2}{\lfloor \frac{n}{6} \rfloor \varphi(6) + z}.$$

Pre zjednodušenie výpočtov odhadneme

$$P_6(X) \approx \frac{n/\log n}{(n/6)\varphi(6)} = \frac{3}{\log n}.$$

Odchýlky sú v porovnaní s veľkosťou n malé, môžeme ich zanedbať, vo výpočte pravdepodobnosti sa neprejavia.

Tiež môžeme túto pravdepodobnosť podobne ako vo výpočtoch v predchádzajúcej sekcii dosadiť do nerovnosti 2.2 a dostávame:

$$P_6(X \mid Y_t) \gg \frac{1 \cdot \dfrac{3}{\log n}}{1 \cdot \dfrac{3}{\log n} + \dfrac{1}{2^t}\left(1 - \dfrac{3}{\log n}\right)} \gg 1 - \frac{1}{2^t}\left(\frac{\log n}{3} - 1\right),$$

pričom v druhej nerovnosti sme použili odhad $\dfrac{1}{1+x} > 1 - x$ pre $0 < x < 1$, teda odhad je platný pre $t > \log_2\left(\dfrac{\log n}{3} - 1\right)$.

2.4.2 Všeobecný prípad

Pokračujme teraz všeobecným prípadom. Zvolíme si množinu po dvoch rôznych prvočísel $\{p_1, p_2, \ldots, p_r\}$, ktoré sú oproti skúmanému n relatívne malé, tak, aby ich súčin bol značne menší než n. Overíme, že ani jedno z nich nedelí n. Označme $S := \prod_i p_i$. To, že číslo $a \in \mathbb{Z}$ nie je deliteľné ani jedným z čísel $p_1, p_2, \ldots p_r$, je ekvivalentné s faktom, že a nie je súdeliteľné s ich súčinom S. Množinu, s ktorou budeme pri výpočte pravdepodobnosti pracovať, získame vylúčením čísel súdeliteľných s S z pôvodnej množiny $\{1,2,\ldots,n\}$. Pravdepodobnosť, že číslo vybraté z tejto množiny, a teda aj n, je prvočíslo, môžeme heuristicky vyjadriť

$$P_S(X) \approx \frac{n/\log n - r}{\lfloor \frac{n}{S} \rfloor \varphi(S) + z},$$

kde z je počet nesúdeliteľných čísel s S v množine $\{\varphi(S)\lfloor \frac{n}{S} \rfloor + 1, \varphi(S)\lfloor \frac{n}{S} \rfloor + 2, \ldots, n\}$, ktorej veľkosť je menšia ako S.

Pre zjednodušenie výpočtov odhadneme

$$P_S(X) \approx \frac{n/\log n}{(n/S)\varphi(S)} = \frac{S}{\varphi(S)\log n}.$$

Vzhľadom k tomu, že zanedbávané hodnoty sú v pomere k n malé, na výslednom výpočte pravdepodobnosti sa to neprejaví.

Dosaďme túto hodnotu do nerovnosti 2.2 a dostávame:

$$\begin{aligned} P_S(X \mid Y_t) &\gg \frac{1 \cdot \dfrac{S}{\varphi(S)\log n}}{1 \cdot \dfrac{S}{\varphi(S)\log n} + \dfrac{1}{2^t}\left(1 - \dfrac{S}{\varphi(S)\log n}\right)} \\ &= \frac{1}{1 + \dfrac{1}{2^t}\left(\dfrac{\varphi(S)\log n}{S} - 1\right)} \\ &\gg 1 - \frac{1}{2^t}\left(\frac{\varphi(S)\log n}{S} - 1\right), \end{aligned}$$

pričom medzi druhým a tretím riadkom sme použili odhad $\frac{1}{1+x} > 1-x$ pre $0 < x < 1$, takže odhad je platný pre $t > \log_2\left(\frac{\varphi(S)\log n}{S} - 1\right)$.

V tejto chvíli máme všetky výpočty hotové a môžeme sformulovať test s presnejšie spočítanou pravdepodobnosťou.

TEST 3.

Vstup: $n \in \mathbb{N}$, nepárne číslo.

1. Pre ľubovoľné $r \in \mathbb{N}$ si zvolíme množinu r malých rôznych prvočísel (malých vzhľadom k n takých, že ich súčin je tiež menší než n) $\{p_1, p_2, \ldots, p_r\}$ a overíme, že ani jedno z nich nedelí n. Ak nájdeme deliteľa, ukončíme test s vyhlásením, že „n je zložené“.

2. Spočítame $S = \prod_i p_i$ a Eulerovu funkciu $\varphi(S) = \prod_i (p_i - 1)$.

3. Zafixujeme číslo $t \in \mathbb{N}$, $t > \log_2\left(\frac{\varphi(S)\log n}{S} - 1\right)$, ako počet pokusov pre test.

4. Vezmeme náhodné číslo $a \in \{1, \ldots, n\}$.

5. Overíme, či platí $(a,n) = 1$. Ak odhalíme $(a,n) > 1$, test ukončíme s prehlásením, že „n je zložené“. V opačnom prípade pokračujeme.

6. Ak $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n$, test ukončíme s prehlásením, že „n je zložené“.

7. Ak $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$, pokračujeme krokom 4.

8. Keď test prebehne t-krát bez nájdenia Eulerovho svedka pre n, vyhlásime, že „n je prvočíslo s pravdepodobnosťou väčšou ako $1 - \frac{1}{2^t}\left(\frac{\varphi(S)\log n}{S} - 1\right)$.“

Poznámka. Vo formulácii testu sme použili odhad pravdepodobnosti s malou odchýlkou. Vďaka tomu nám nevznikla dolná celá časť $\lfloor \frac{n}{S} \rfloor$ a konštanta z ako počet čísel v množine $\{\lfloor \frac{n}{S} \rfloor, \lfloor \frac{n}{S} \rfloor + 1, \ldots, n\}$ nesúdeliteľných s S, ale dostali sme jediné číslo n/S.

V teste 3 sme zanedbali túto skutočnosť a nerozlišovali sme dolnú celú časť $\lfloor \frac{n}{S} \rfloor$ a konštantu z . Využili sme jednoducho klasické delenie v reálnych číslach. Odchýlka nie je veľká a na výslednej pravdepodobnosti sa neprejaví.

Sformulujeme výpočty tejto kapitoly do nasledujúcej vety.

Veta 17. *Nech je n nepárne celé číslo a $p_1, \ldots, p_r$ sú prvočísla. Označme S súčin prvočísel $p_1 \cdots p_r$. Predpokladajme, že n nie je deliteľné prvočíslami $p_1, \ldots, p_r$ a $S < n$. Ak prebehne Solovay-Strassenov test pre n t-krát bez nájdenia Eulerovho svedka a platí, že $t > \log_2((\varphi(S)\log n)/S - 1)$, potom číslo n je (heuristicky) s pravdepodobnosťou väčšou ako $1 - \frac{1}{2^t}\left(\frac{\varphi(S)\log n}{S} - 1\right)$ prvočíslo a s pravdepodobnosťou menšou ako $\frac{1}{2^t}\left(\frac{\varphi(S)\log n}{S} - 1\right)$ zložené číslo.*

Pre ilustráciu práve sformulovanej vety uvedieme niekoľko ukážkových hodnôt. Porovnáme, ako sa pravdepodobnosť, že n je prvočíslo, ak nie je deliteľné danými prvočíslami a Solovay-Strassenov test ho vyhlásil za prvočíslo, oproti pôvodnému výpočtu pravdepodobnosti z článku (Conrad, Appendix), zmenila.

Podľa (Conrad, Appendix) sa pravdepodobnosť, že n je prvočíslo, za podmienky, že Solovay-Strassenov test prebehol t-krát bez nájdenia svedka, odhadne pre $t > \log_2(\log n - 1)$ ako $P(X \mid Y_t) \gg 1 - (\log n - 1)/2^t$. My sme spočítali, že ak číslo n nie je deliteľné prvočíslami $p_1, p_2, \ldots p_r$, čiže je nesúdeliteľné s ich súčinom S, dostaneme odhad $P_S(X \mid Y_t) \gg 1 - (\varphi(S)\log n/S - 1)/2^t$ pre $t > \log_2\left(\frac{\varphi(S)\log n}{S} - 1\right)$. Pomocou týchto nerovností spočitame:

Príklad.

Máme $n = 3659009$. Zvoľme počet pokusov pre test $t = 7$, máme dostatočnú rezervu, pretože má platiť $t > \log_2(\log n - 1)$ a $t > \log_2\left((\varphi(S)\log n)/S - 1\right)$. Všimnime si, že $\log_2(\log n - 1) \geq \log_2\left((\varphi(S)\log n)/S - 1\right)$ pre hodnoty S uvedené v tabuľke.

Overíme, že n nie je deliteľné prvočíslami v tabuľke a aplikujeme na n Solovay-Strassenov test, ktorým prejde 7-krát bez prerušenia. Spočítame spodný odhad pravdepodobnosti, že n je prvočíslo, zaokruhlený na 6 desatinných miest.

(Conrad) $P(X \mid Y_t) \gg$	S **je rovné**	**(náš výpočet)** $P_S(X \mid Y_t) \gg$
0,889745	2	0,9487785
0,889745	$2 \cdot 3 \cdot 5$	0,976328
0,889745	$2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	0,981392

3. Kvartický symbol a konštrukcia testov prvočíselnosti

3.1 Prehľad základných tvrdení pre obor $\mathbb{Z}[i]$

Pre potreby kvartického symbolu, ktorý je zavedený nad oborom $\mathbb{Z}[i]$, pripomenieme a zhrnieme niekoľko poznatkov, týkajúcich sa tohto oboru.

Tvrdenie 18. *$\mathbb{Z}[i]$ je eukleidovský obor a zobrazenie*

$$N : \mathbb{Z}[i] \to \mathbb{N}_0$$

$$a + bi \mapsto a^2 + b^2$$

je eukleidovská norma na obore $\mathbb{Z}[i]$.

Dôkaz. Dôkaz nájdeme v skriptách Základy algebry (Stanovský, 2010, tvrzení 8.2). □

Poznámka. Z algebry vieme, že ak je nejaký obor R eukleidovský, potom je R gaussovským oborom, (Stanovský, 2010, kapitola Eukleidovské obory). Čiže pre každý neinvertibilný prvok $n \in R$ existuje rozklad $n \parallel p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, kde p_i je ireducibilný prvok a $a_i \geq 1$ pre každé $i \in \{1, \ldots, r\}$. Tento rozklad je jednoznačný až na asociovanosť.

V gaussovskom obore tiež platí, že prvok $p \in R$ je ireducibilný práve vtedy, keď p je prvočiniteľ, (Stanovský, 2010, kapitola Gaussovské obory).

Budeme teda využívať, že $\mathbb{Z}[i]$ je gaussovský obor, existujú v ňom jednoznačné rozklady na súčin prvočiniteľov a pojmy ireducibilný prvok a prvočiniteľ budeme ekvivalentne zamieňať.

Lema 19. *Pre $a, b, n \in \mathbb{Z}$ platí $a \equiv b \bmod n\mathbb{Z} \Leftrightarrow a \equiv b \bmod n\mathbb{Z}[i]$.*

Dôkaz. „⇒“ Z definície kongruencie $a \equiv b \bmod n\mathbb{Z} \Leftrightarrow n \mid (a - b)$ v $\mathbb{Z}$, teda existuje $c \in \mathbb{Z}$, také, že $(a-b)c = n$. Keďže $\mathbb{Z} \subset \mathbb{Z}[i]$, aj $c \in \mathbb{Z}[i]$, a teda $n \mid (a-b)$ aj v $\mathbb{Z}[i]$, ekvivalentne $a \equiv b \bmod n\mathbb{Z}[i]$.

„⇐“ Ak platí, že priamo $a = b$, platnosť tvrdenia je zjavná, vždy $n \mid (a-b) = 0$ v $\mathbb{Z}$. Takže predpokladajme $a \neq b$. Teraz vychádzame z $a \equiv b \bmod n\mathbb{Z}[i]$, čiže existuje $\gamma \in \mathbb{Z}[i]$ taká, že $(a - b)\gamma = n$. γ je prvok tvaru $\gamma = c + di$ pre $c,d \in \mathbb{Z}$, takže po roznásobení $(a - b)(c + di)$ dostávame $n = (a - b)c + (a - b)di$, kde $(a-b)c \in \mathbb{Z}$ aj $(a-b)d \in \mathbb{Z}$. Ale n je celé číslo, takže koeficient u i je nulový, teda $(a-b)d = 0$. Predpokladáme $a \neq b$, takže v obore musí byť $d = 0$. Prvok $\gamma = c+0i$, čiže $\gamma = c \in \mathbb{Z}$, takže platí $(a - b)c = n$, ekvivalentne $a \equiv b \bmod n\mathbb{Z}$. □

Tvrdenie 20. *Nech $\alpha \in \mathbb{Z}[i]$. Ak platí, že $N(\alpha)$ je prvočíslo, potom α je prvočiniteľ.*

Dôkaz. Nech $\alpha = \beta\gamma$ pre $\beta,\gamma \in \mathbb{Z}[i]$. Vezmeme normy oboch strán a dostaneme: $N(\alpha) = N(\beta)N(\gamma)$. Keďže $N(\alpha)$ je prvočíslo, $N(\beta) = 1$ alebo $N(\gamma) = 1$. Potom je β alebo γ invertibilný prvok. Teda rozklad $\beta\gamma$ je nevlastný a α je ireducibilný prvok. □

Tvrdenie 21. *Ak je $p \equiv 3 \bmod 4\mathbb{Z}$ prvočíslom v $\mathbb{Z}$, potom je p prvočiniteľ aj v obore $\mathbb{Z}[i]$.*

Dôkaz. Ak by p nebolo ireducibilné, našli by sme rozklad $p = \alpha\beta$ pre $\alpha,\beta \in \mathbb{Z}[i]$ také, že $N(\alpha) > 1$ aj $N(\beta) > 1$. Prechodom k normám získame: $p^2 = N(\alpha)N(\beta)$. Z tohto plynie,že $p = N(\alpha)$. Keďže prvok α je tvaru $\alpha = a+bi$, potom $p = N(\alpha) = a^2 + b^2$, čo je spor, pretože súčet dvoch druhých mocnín v $\mathbb{Z}$ je kongruentný 0 alebo 1 modulo $4\mathbb{Z}$, ale $p \equiv 3 \bmod 4\mathbb{Z}$. □

Tvrdenie 22. *Všetky prvočinitele v $\mathbb{Z}[i]$ (až na asociovanosť) sú:*

- *prvočísla $p \in \mathbb{N}$, pre ktoré platí $p \equiv 3 \bmod 4\mathbb{Z}$*
- *prvky tvaru $a \pm bi$ také, že $a^2 + b^2 = p$, kde p je prvočíslo, $p \equiv 1 \bmod 4\mathbb{Z}$*
- $1 + i$

Dôkaz. Dôkaz nájdeme v skriptách k predmetu Teória čísel a RSA (Drápal, kapitola 3.1). □

3.2 Zavedenie pojmu kvartického symbolu

V tejto sekcii vychádzame z knihy (Ireland a Rosen, 2013, kapitola 9).

Legendrov symbol rozdeľuje nenulové čísla na tie, ktoré sú štvorcami a tie, ktoré nie sú štvorcami v telese $\mathbb{Z}/p\mathbb{Z}$. Presnejšie, pre nepárne prvočíslo p a $a \in \mathbb{Z}$, také, že $p \nmid a$, je Legendrov symbol $\left(\frac{a}{p}\right) = 1$, práve vtedy, keď má rovnica $x^2 \equiv a \bmod p\mathbb{Z}$ v $\mathbb{Z}$ koreň.

Kvartický symbol je motivovaný riešiteľnosťou rovníc štvrtého stupňa. Aby sme mohli zaviesť pojem kvartického symbolu, potrebujeme sa pohybovať v obore $\mathbb{Z}[i]$. Ako uvidíme v tvrdení 29 v bode 4, pre prvky $\alpha,\pi \in \mathbb{Z}[i]$, kde $\pi \nmid (1 + i)$ je prvočiniteľ a $\pi \nmid a$, máme kvartický symbol $\left(\frac{\alpha}{\pi}\right)_4$ rovný 1, práve vtedy, keď má rovnica $x^4 \equiv \alpha \bmod \pi\mathbb{Z}[i]$ v $\mathbb{Z}[i]$ koreň.

Sformulujeme a dokážeme niekoľko tvrdení, ktoré nám umožnia definovať kvartický symbol.

3.2.1 Tvrdenia potrebné pre definíciu kvartického symbolu

Lema 23. *Nech $\pi \in \mathbb{Z}[i]$ je prvočiniteľ taký, že $\pi \nmid (1 + i)$. Potom: $0, 1, i, -1, -i$ nie sú po dvoch kongruentné $\bmod \pi\mathbb{Z}[i]$.*

Dôkaz. Najskôr vyriešime prípad, že $0 \not\equiv a \bmod \pi\mathbb{Z}[i]$ pre $a \in \{1, -1, i, -i\}$. Ak by $a \equiv 0 \bmod \pi\mathbb{Z}[i]$, z definície kongruencie by platilo, že $\pi \mid a$ v $\mathbb{Z}[i]$, toto ale nastať nemôže, pretože $a \in \{1, -1, i, -i\}$ je invertibilný prvok a π je prvočiniteľ, $\pi \nmid a$.

Teraz ukážeme, že nenulové prvky $1, i, -1, -i$ nie sú po dvoch kongruentné. Pre každú dvojicu ukážeme, že ak by boli tieto 2 prvky kongruentné, potom $\pi \mid (1 + i)$, čo vedie ku sporu s predpokladom $\pi \nmid (1 + i)$, ako nižšie ukážeme.

- Pre spor nech $1 \equiv -i \bmod \pi\mathbb{Z}[i]$. Tento zápis je ekvivalentný $\pi \mid (1 + i)$ v $\mathbb{Z}[i]$.

- Teraz nech $1 \equiv i \bmod \pi\mathbb{Z}[i]$, to je ekvivalentné $\pi \mid (1-i) = -i(1+i)$, ale π je prvočiniteľ, preto $\pi \mid -i$ alebo $\pi \mid (1+i)$. Z definície je ireducibilný prvok neinvertibilný, čiže $\pi \nmid -i$, a preto $\pi \mid (1+i)$.
- Ak uvažujeme $1 \equiv -1 \bmod \pi\mathbb{Z}[i]$, potom $\pi \mid 2 = (1+i)(1-i) = (1+i)^2(-i)$ a podobný argument ako v predchádzajúcom bode nám dá, že prvočiniteľ π musí deliť $(1+i)$.
- $i \equiv -1 \bmod \pi\mathbb{Z}[i] \Leftrightarrow \pi \mid (1+i)$.
- $i \equiv -i \bmod \pi\mathbb{Z}[i] \Leftrightarrow \pi \mid 2i = (1+i)^2$, opäť $\pi \mid (1+i)$.
- $-1 \equiv -i \bmod \pi\mathbb{Z}[i] \Leftrightarrow \pi \mid (i-1) = i(1+i)$, zase $\pi \mid (1+i)$.

Keďže $(1+i)$ je podľa tvrdenia 22 ireducibilný prvok a π je tiež ireducibilný v $\mathbb{Z}[i]$, skutočnosť $\pi \mid (1+i)$ nám hovorí, že $\pi \parallel (1+i)$, čo predpoklad tvrdenia vylučuje, tým dostávame vo všetkých prípadoch spor. □

Nasledujúca veta nám poskytne základy pre ďalšiu teóriu a jej dôsledok umožní jednoznačne definovať kvartický symbol. V knihe (Ireland a Rosen, 2013) bol dôkaz nasledujúcej vety ponechaný na čitateľa s upozornením, že prebieha podobným spôsobom ako dôkaz tvrdenia: $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ je teleso s $N(\pi)$ prvkami pre $\omega = (-1+\sqrt{-3})/2$ a π ireducibilný prvok v $\mathbb{Z}[\omega]$. My sme pre úplnosť dôkaz pre obor $\mathbb{Z}[i]$ doplnili:

Veta 24. *Nech π je prvočiniteľ v $\mathbb{Z}[i]$. Potom $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ je teleso s $N(\pi)$ prvkami.*

Dôkaz. Najskôr ukážeme, že $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ je teleso. Vezmime $\alpha \in \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, $\alpha \not\equiv 0 \bmod \pi\mathbb{Z}[i]$. Potom platí $(\pi, \alpha) = 1$, použijeme rozšírený Eukleidov algoritmus v eukleidovskom obore $\mathbb{Z}[i]$ a pomocou Bézoutovej rovnosti dostaneme $\alpha\beta + \pi\gamma = 1$ pre $\beta, \gamma \in \mathbb{Z}[i]$. Potom platí, že $\alpha\beta \equiv 1 \bmod \pi\mathbb{Z}[i]$, čiže α je invertibilný prvok.

Ďalej overíme, že $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ má $N(\pi)$ prvkov. Podľa popisu prvočiniteľov v tvrdení 22 rozoberieme jednotlivé prípady.

(a) $\pi = p$, kde $p \equiv 3 \bmod 4\mathbb{Z}$ je prvočíslo v $\mathbb{Z}$ a zároveň prvočiniteľ v $\mathbb{Z}[i]$. Označme $M = \{a+bi \mid 0 \leq a,b < p\}$. Ukážeme, že M je množina prvkov, ktorými môžeme reprezentovať všetky rozkladové triedy $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ a každú z nich práve raz. Potom z toho vyplynie veľkosť $|\mathbb{Z}[i]/\pi\mathbb{Z}[i]| = |M| = p^2 = N(p)$.

Zoberme ľubovoľný prvok $\mu = m + ni \in \mathbb{Z}[i]$, kde $m, n \in \mathbb{Z}$. Každé z čísel m, n môžeme využitím delenia so zvyškom napísať v tvare $m = pk_1 + z_1$ a $n = pk_2 + z_2$, kde $k_1, k_2, z_1, z_2 \in \mathbb{Z}$ a $0 \leq z_1, z_2 < p$. Potom je $\mu \equiv z_1 + iz_2 \bmod p\mathbb{Z}[i]$, pričom $z_1 + iz_2 \in M$.

Teraz ukážeme, že žiadne dva prvky M nie sú kongruentné modulo $p\mathbb{Z}[i]$, pokiaľ nenastane rovnosť. Čiže chceme ukázať, že žiadne dva rôzne prvky množiny M neležia v rovnakej rozkladovej triede $\mathbb{Z}[i]/p\mathbb{Z}[i]$.

Vezmeme $z_1 + iz_2, w_1 + iw_2 \in M$ také, že $z_1 + iz_2 \equiv w_1 + iw_2 \bmod p\mathbb{Z}[i]$. Úpravou dostaneme $(z_1 - w_1) + i(z_2 - w_2) \equiv 0 \bmod p\mathbb{Z}[i]$. To je ekvivalentné s faktom, že $p \mid (z_1 - w_1) + i(z_2 - w_2)$, a to nastáva práve vtedy, keď p delí reálnu aj imaginárnu časť, teda $p \mid (z_1 - w_1)$ a tiež $p \mid (z_2 - w_2)$ v $\mathbb{Z}$. To znamená, že $z_1 \equiv w_1 \bmod p\mathbb{Z}$ a $z_2 \equiv w_2 \bmod p$. Ale $0 \leq z_1, w_1, z_2, w_2 < p$, takže kongruencie sú už priamo rovnosťami.

(b) π je prvočiniteľ taký, že $N(\pi) = \pi\bar{\pi} = p$, kde $p \equiv 1 \bmod 4\mathbb{Z}$ je prvočíslo v $\mathbb{Z}$. V tomto prípade označme $M := \{0,1,\ldots,p-1\}$. Ukážeme, že prvky M môžeme zvoliť za reprezentantov rozkladových tried $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ a žiadne dva z týchto prvkov neležia v rovnakej rozkladovej triede. Z tohto potom vyplynie, že $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ má $N(\pi) = p$ prvkov.

Prvok π je tvaru $\pi = a + bi$, kde $a, b \in \mathbb{Z}$. Podľa tvrdenia 22 je norma $N(\pi) = p = a^2 + b^2$. Z toho plynie, že $p > |b|$, a teda $p \nmid b$. Keďže $(p, b) = 1$, môžeme použiť Eukleidov algoritmus v $\mathbb{Z}$ a pomocou Bézoutovej rovnosti dostaneme $u_1 b + u_2 p = 1$ pre nejaké $u_1, u_2 \in \mathbb{Z}$. Takže platí $u_1 b \equiv 1 \bmod p\mathbb{Z}$.

Zoberme ľubovoľný prvok $\mu = m + ni \in \mathbb{Z}[i]$, kde $m, n \in \mathbb{Z}$. Prenásobme kongruenciu $u_1 b \equiv 1 \bmod p\mathbb{Z}$ číslom n. Dostaneme, že $b \cdot u_1 n \equiv n \bmod p\mathbb{Z}$. Označme celé číslo $c := u_1 n \bmod p\mathbb{Z}$, potom platí pre $0 \leq c < p : cb \equiv n \bmod p\mathbb{Z}$. Vezmeme rozdiel $\mu - c\pi \equiv m + ni - c(a + bi) \equiv m - ca \bmod p\mathbb{Z}$, ďalej $m - ca \equiv z \bmod p\mathbb{Z}$, kde $z \in \mathbb{Z}$ a $0 \leq z < p$. Vďaka leme 19 máme teda pre $\mu - c\pi, z \in \mathbb{Z}$, že $\mu - c\pi \equiv z \bmod p\mathbb{Z}[i]$, ale vieme, že $\pi \mid p$ v $\mathbb{Z}[i]$, potom tiež $\mu - c\pi \equiv z \bmod \pi\mathbb{Z}[i]$ a po úprave $\mu \equiv z \bmod \pi\mathbb{Z}[i]$. Ukázali sme, že ľubovoľné $\mu \in \mathbb{Z}[i]$ je kongruentné celému číslu $z \in M$ modulo $\pi\mathbb{Z}[i]$.

Ukážeme teraz, že žiadne dva prvky $m_1, m_2 \in M$ nie sú kongruentné modulo $\pi\mathbb{Z}[i]$, pokiaľ si nie sú rovné. Nech teda $m_1 \equiv m_2 \bmod \pi\mathbb{Z}[i] \Leftrightarrow m_1 - m_2 = \pi\gamma$ pre nejaký prvok $\gamma \in \mathbb{Z}[i]$. Vezmeme normy $(m_1 - m_2)^2 = pN(\gamma)$. V $\mathbb{Z}$ je p prvočiniteľ, a teda p v $\mathbb{Z}$ delí $(m_1 - m_2)$, ale $0 \leq m_1, m_2 < p$, takže nutne $m_1 = m_2$.

(c) $\pi = 1 + i$ V tomto prípade sa dá postupovať podobne ako v dôkaze pre prvočiniteľ tvaru $a + bi$, kde $N(a + bi) = p$, kde $p \equiv 1 \bmod 4\mathbb{Z}$ je prvočíslo v $\mathbb{Z}$.

$N(1+i) = 2$. Ukážeme, že $\{0, 1\}$ je množina reprezentantov rozkladových tried $\mathbb{Z}[i]/(1 + i)\mathbb{Z}[i]$.

Ak máme ľubovoľný prvok $\nu = m + ni \in \mathbb{Z}[i]$ a vezmeme rozdiel $\nu - n(1 + i)$, dostaneme celé číslo $m - n$, čo je modulo $2\mathbb{Z}$ kongruentné jednej z hodnôt $\{0, 1\}$, označme ju z. Podľa lemy 19 je teda $\nu - n(1 + i) \equiv m - n \equiv z \bmod 2\mathbb{Z}[i]$. Keďže $(1 + i)$ je deliteľ dvojky v $\mathbb{Z}[i]$, dostávame:

$$\nu \equiv \nu - n(1 + i) \equiv m - n \equiv z \bmod (1 + i)\mathbb{Z}[i].$$

Ľubovoľné $\nu \in \mathbb{Z}[i]$ je kongruentné z, ktoré je rovné 0 alebo 1 a platí $0 \not\equiv 1 \bmod (1 + i)\mathbb{Z}[i]$. Takže 0,1 sú reprezentanti rôznych rozkladových tried telesa $\mathbb{Z}[i]/(1 + i)\mathbb{Z}[i]$ a každé $\nu \in \mathbb{Z}[i]$ leží v jednej z nich. □

Poznámka. V slovenčine sa niekedy zvykne štruktúra vo vete 24 označovaná ako teleso nazývať poľom.

Tvrdenie 25. *Ak je T konečné teleso, potom je T^* cyklická grupa.*

Dôkaz. Dôkaz nájdeme v skriptách z algebry (Stanovský, 2010, kapitola Cyklické grupy). □

Dôsledok 26. *Nech π je prvočiniteľ v $\mathbb{Z}[i]$, $\alpha \in \mathbb{Z}[i]$. Ak $\pi \nmid \alpha$, potom $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi\mathbb{Z}[i]$.*

Dôkaz. Uvažujme grupu invertibilných prvkov telesa $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ (všetky prvky okrem 0) s násobením pre prvočiniteľ $\pi \in \mathbb{Z}[i]$. Rád grupy je $N(\pi) - 1$ a vieme, že rád každého prvku grupy delí rád grupy. Z tohto plynie tvrdenie. □

Tvrdenie 27. *Nech π je prvočiniteľ v $\mathbb{Z}[i]$, $\alpha \in \mathbb{Z}[i]$. Ak $\pi \nmid \alpha$ a $(\pi) \neq (1+i)$, potom existuje práve jedno nezáporné celé číslo j, $0 \leq j \leq 3$, také, že*

$$\alpha^{(N(\pi)-1)/4} \equiv i^j \bmod \pi\mathbb{Z}[i].$$

Dôkaz. Možnosti, ktoré môžeme dostať na pravej strane kongruencie: $i^0 = 1$, $i^1 = i$,$i^2 = -1$ a $i^3 = -i$. Podľa lemy 23 nie sú $1, i, -1, -i$ po dvoch kongruentné modulo $/\pi\mathbb{Z}[i]$. Sú to teda rôzne korene $x^4 \equiv 1 \bmod \pi\mathbb{Z}[i]$. Podľa dôsledku 26 je aj $\alpha^{(N(\pi)-1)/4}$ koreňom $x^4 \equiv 1 \bmod \pi\mathbb{Z}[i]$. Polynóm stupňa 4 má maximálne 4 rôzne korene v telese $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Z toho plynie, že $\alpha^{(N(\pi)-1)/4} \equiv i^j \bmod \pi\mathbb{Z}[i]$ pre práve jedno j. □

3.2.2 Definícia kvartického symbolu a jeho vlastnosti

Definícia 28. *Nech π je ireducibilný prvok v $\mathbb{Z}[i]$, $N(\pi) \neq 2$ a $\alpha \in \mathbb{Z}[i]$. Definujeme* ***kvartický symbol*** $\left(\frac{\alpha}{\pi}\right)_4$ *ako prvok množiny $\{0, \pm 1, \pm i\}$ taký, že:*

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} \alpha^{(N(\pi)-1)/4} \bmod \pi\mathbb{Z}[i] & \text{ak } \pi \nmid \alpha \\ 0 & \text{ak } \pi \mid \alpha \end{cases}$$

Poznámka. Uvažujme α, π ako v definícii. Podľa tvrdenia 27 vieme, že pre $\pi \nmid \alpha$ platí $\alpha^{(N(\pi)-1)/4} \equiv i^j \bmod \pi\mathbb{Z}[i]$ pre práve jedno j, $0 \leq j \leq 3$, čiže $\left(\frac{\alpha}{\pi}\right)_4$ je rovný práve jednému z prvkov $\{\pm 1, \pm i\}$, ak $\pi \nmid \alpha$ a $\left(\frac{\alpha}{\pi}\right)_4 = 0$ práve vtedy, keď $\pi \mid \alpha$.

Značenie. V knihe, z ktorej vychádzame (Ireland a Rosen, 2013), je pre kvartický symbol použité značenie $\chi_\pi(\alpha)$ namiesto $\left(\frac{\alpha}{\pi}\right)_4$.

V nasledujúcom tvrdení zhrnieme vlastnosti kvartického symbolu, vybrali sme ich z knihy (Ireland a Rosen, 2013, Proposition 9.8.3), pričom dôkazy sme obmenili alebo doplnili o úvahy, ktoré zjednodušujú ich čitateľnosť.

Tvrdenie 29 (Vlastnosti kvartického symbolu)**.** *Nech α,β,π,$\lambda \in \mathbb{Z}[i]$ a π,λ sú ireducibilné prvky také, že $N(\pi), N(\alpha) \neq 2$ Potom platia nasledujúce tvrdenia:*

1. *Ak je $\alpha \equiv \beta \bmod \pi\mathbb{Z}[i]$, potom $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$.*
2. *$\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$.*
3. *Ak $\pi \parallel \lambda$, potom $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\lambda}\right)_4$.*
4. *Ak $\pi \nmid \alpha$, potom:*

$$\left(\frac{\alpha}{\pi}\right)_4 = 1 \Leftrightarrow x^4 \equiv \alpha \bmod \pi\mathbb{Z}[i] \text{ má riešenie v } \mathbb{Z}[i]$$

Dôkaz.

1. Plynie priamo z definície kvartického symbolu: ak platí $\alpha \equiv \beta \bmod \pi\mathbb{Z}[i]$, potom $\pi \mid \alpha \Leftrightarrow \pi \mid \beta$, čiže $\left(\frac{\alpha}{\pi}\right)_4 = 0 \Leftrightarrow \left(\frac{\beta}{\pi}\right)_4 = 0$. Ďalej $\alpha \equiv \beta \bmod \pi\mathbb{Z}[i]$ implikuje $\alpha^{(N(\pi)-1)/4} \equiv \beta^{(N(\pi)-1)/4} \bmod \pi\mathbb{Z}[i]$, takže rovnosť kvartických symbolov dostávame aj v prípade, že $\pi \nmid \alpha$,β.

2. Opäť vychádzame z definície. Najskôr $\pi \mid \alpha\beta$. Potom $\left(\frac{\alpha\beta}{\pi}\right)_4 = 0$. Pre prvočiniteľ π platí, že $\pi \mid \alpha\beta$, práve vtedy, keď π delí aspoň jeden z prvkov α a β, čiže aspoň jeden z kvartických symbolov $\left(\frac{\alpha}{\pi}\right)_4$,$\left(\frac{\beta}{\pi}\right)_4$ je nulový. Na ľavej aj pravej strane máme nulu, rovnosť teda platí.

Teraz prípad $\alpha\beta$ a π sú nesúdeliteľné. Podľa tvrdenia 27 $(\alpha\beta)^{(N(\pi)-1)/4}$ je modulo $\pi\mathbb{Z}[i]$ kongruentné jednému z prvkov $\{\pm 1, \pm i\}$, takto dostaneme $\left(\frac{\alpha\beta}{\pi}\right)_4$. Na pravej strane rovnosti máme súčin dvoch prvkov množiny $\{\pm 1, \pm i\}$, ten tiež leží v tejto množine. Keďže platí $(\alpha\beta)^{(N(\pi)-1)/4} \equiv \alpha^{(N(\pi)-1)/4}\beta^{(N(\pi)-1)/4} \bmod \pi\mathbb{Z}[i]$ a podľa lemy 23 žiadne dva prvky tejto množiny nie sú navzájom kongruentné modulo $\pi\mathbb{Z}[i]$, dostávame, že na oboch stranách kongruencie musí byť rovnaký prvok množiny $\{\pm 1, \pm i\}$, a teda dokazovaná rovnosť platí.

3. To, že sú prvky λ a π asociované v $\mathbb{Z}[i]$, môžeme vyjadriť, že $\lambda = \gamma\pi$ pre γ invertibilný prvok. Vezmeme normy oboch strán, pričom norma invertibilného prvku je 1. Takže $N(\lambda) = N(\gamma)N(\pi) = N(\pi)$ a máme rovnosť noriem λ a π. Ďalej $\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)/4} \bmod \pi\mathbb{Z}[i] \Leftrightarrow \pi \mid \left(\frac{\alpha}{\pi}\right)_4 - \alpha^{(N(\pi)-1)/4}$, ale aj $\lambda \mid \left(\frac{\alpha}{\pi}\right)_4 - \alpha^{(N(\pi)-1)/4}$, lebo $\lambda \mid \pi$. Takže

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)/4} \equiv \alpha^{(N(\lambda)-1)/4} \equiv \left(\frac{\alpha}{\lambda}\right)_4 \bmod \lambda\mathbb{Z}[i].$$

Z asociovanosti aj $\pi \mid \lambda$, čiže $\left(\frac{\alpha}{\pi}\right)_4 \equiv \left(\frac{\alpha}{\lambda}\right)_4 \bmod \pi\mathbb{Z}[i]$. Teda kvartické symboly sa rovnajú podľa lemy 23.

4. Ukážeme postupne platnosť oboch implikácií a tým dostaneme ekvivalenciu. „⇐“ Predpokladáme, že existuje prvok $\beta \in \mathbb{Z}[i]$ taký, že $\beta^4 \equiv \alpha \bmod \pi\mathbb{Z}[i]$. Spočítame kvartický symbol

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)/4} \equiv (\beta^4)^{(N(\pi)-1)/4} \equiv \beta^{(N(\pi)-1)} \equiv 1 \bmod \pi\mathbb{Z}[i],$$

pričom posledná rovnosť plynie z dôsledku 26, ktorý platí pre $\beta \in \mathbb{Z}[i]$ také, že $\pi \nmid \beta$. Ak by však $\pi \mid \beta$, potom by $\pi \mid \alpha$, ale túto možnosť v predpoklade vety vylučujeme.

„⇒“ Teraz predpokladáme, že platí $\left(\frac{\alpha}{\pi}\right)_4 = 1$. Vďaka tvrdeniu 25 vieme, že $F^* := (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ je cyklická grupa. Označme $[\omega]$ jej generátor. $\omega \in \mathbb{Z}[i]$ je reprezentant rozkladovej triedy $[\omega]$. Potom $\alpha \equiv \omega^t \bmod \pi\mathbb{Z}[i]$ pre nejaké $t \in \mathbb{N}_0$. Takto dostávame

$$1 = \left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)/4} \equiv (\omega^t)^{(N(\pi)-1)/4} \equiv \omega^{\frac{t}{4}(N(\pi)-1)} \bmod \pi\mathbb{Z}[i].$$

Ukážeme teraz, že $\frac{t}{4} \in \mathbb{Z}$. Rád ω je rovný $N(\pi)-1$. Ale $\omega^{\frac{t}{4}(N(\pi)-1)} \equiv 1 \bmod \pi\mathbb{Z}[i]$, takže rád prvku ω musí deliť $\frac{t}{4}(N(\pi)-1)$ v $\mathbb{Z}$. Zo skutočnosti, že $(N(\pi)-1) \mid \frac{t}{4}(N(\pi)-1)$ v $\mathbb{Z}$, plynie, že existuje $c \in \mathbb{Z}$ taký, že $c \cdot (N(\pi)-1) = \frac{t}{4}(N(\pi)-1)$, odkiaľ vidíme, že $\frac{t}{4}$ je celé číslo. $\left(\omega^{\frac{t}{4}}\right)^4 \equiv \omega^t = \alpha \bmod \pi\mathbb{Z}[i]$. Našli sme teda riešenie $\omega^{\frac{t}{4}} \in \mathbb{Z}[i]$ kongruencie $x^4 \equiv \alpha \bmod \pi\mathbb{Z}[i]$. □

Vytvoríme a dokážeme obdobu k tvrdeniu 5.

Definícia 30. *Nech $\pi \in \mathbb{Z}[i]$ je prvočiniteľ, $\pi \nmid (1+i)$. Povieme, že $\alpha \in \mathbb{Z}[i]$ je* kvartický zvyšok *modulo $\pi\mathbb{Z}[i]$, ak existuje prvok $\beta \in \mathbb{Z}[i]$ taký, že $\beta^4 \equiv \alpha \bmod \pi\mathbb{Z}[i]$.*

Tvrdenie 31. *Nech $\pi \in \mathbb{Z}[i]$ je prvočiniteľ, $\pi \nmid (1+i)$. Označme teleso $F := \mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Položme pre $k = 0,1,2,3$ množiny $A_k = \{\alpha \in F^* \mid \left(\frac{\alpha}{\pi}\right)_4 = i^k\}$. Potom pre $\forall k \in \{0,1,2,3\}$ platí $|A_k| = \frac{1}{4}|F^*|$.*

Dôkaz. V tvrdení 22 sme popísali, ako vyzerajú prvočinitele v $\mathbb{Z}[i]$. Ďalej vo vete 24 sme si ukázali, že $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ je teleso s $N(\pi)$ prvkami. Rozlíšime 2 prípady prvočiniteľov, tretí prípad $(1+i)$ sme vylúčili v predpoklade vety.

Prípad 1. π je priamo prvočíslo v $\mathbb{Z}$, čiže $\pi = p \equiv 3 \bmod 4\mathbb{Z}$. Potom teleso

$$F = \mathbb{Z}[i]/\pi\mathbb{Z}[i] \simeq (\mathbb{Z}/p\mathbb{Z})[i] \simeq \mathbb{F}_{p^2}.$$

Takže F^* je cyklická grupa rádu $p^2 - 1 = N(\pi) - 1$. Keďže pre prvočíslo $p \equiv 3 \bmod 4\mathbb{Z}$, je $p^2 \equiv 1 \bmod 4\mathbb{Z}$, číslo $N(\pi) - 1$ je deliteľné 4.

Prípad 2. π je prvok tvaru $a+bi$ a $a^2+b^2 = q$, kde q je prvočíslo, $q \equiv 1 \bmod 4\mathbb{Z}$. V tomto prípade je

$$F = \mathbb{Z}[i]/\pi\mathbb{Z}[i] \simeq \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{F}_q.$$

Takže F^* je cyklická grupa rádu $q - 1 = N(\pi) - 1$. Keďže $q \equiv 1 \bmod 4\mathbb{Z}$, číslo $N(\pi) - 1$ je aj v tomto prípade deliteľné 4.

Nasledujúca úvaha platí pre oba prípady. Vieme, že F^* je cyklická grupa (tvrdenie 25). Označme ω jej generátor. Vďaka bodu 2 v tvrdení 29 potom kvartický symbol ľubovoľného prvku grupy F^* spočítame pomocou kvartického symbolu $\left(\frac{\omega}{\pi}\right)_4$, konkrétne, ak $\alpha = \omega^t$, potom $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\omega}{\pi}\right)_4^t$.

Pozorovanie. $\left(\frac{\omega}{\pi}\right)_4 = i$ alebo $\left(\frac{\omega}{\pi}\right)_4 = -i$.

Dôkaz pozorovania. Označme $e := \frac{N(\pi)-1}{4}$. Vezmime prvok $\alpha \in F^*$. Ak je α kvartický zvyšok, inými slovami, ak existuje $\beta \in F$ taká, že $\beta^4 = \alpha$ v F, potom vďaka tvrdeniu 26 je

$$\alpha^e = (\beta^4)^{\frac{N(\pi)-1}{4}} = \beta^{N(\pi)-1} = 1.$$

Čiže α je koreň polynómu $x^e - 1$ nad F. Polynóm $x^e - 1$ má nad telesom F maximálne e koreňov. My ale vieme, že ak $s \in \{0,1,\ldots,(N(\pi)-1)/4\}$, potom ω^{4s} je koreňom $x^e - 1$. Týchto prvkov je e, čo je $\frac{1}{4}(|F^*|)$. Sú to teda presne všetky korene $x^e - 1$.

Ak by $\left(\frac{\omega}{\pi}\right)_4 = 1$, potom by pre ľubovoľný prvok $\alpha = \omega^t$, bolo $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\omega}{\pi}\right)_4^t = 1$. Každá $\alpha \in F$ by bola koreňom $x^e - 1$. To nejde, pretože $x^e - 1$ má presne e koreňov, čo je $\frac{1}{4}|F^*|$.

Ďalej ak by $\left(\frac{\omega}{\pi}\right)_4 = -1$, potom by $\left(\frac{\omega}{\pi}\right)_4^2 = 1$, $\left(\frac{\omega}{\pi}\right)_4^3 = -1$ atď. Čiže koreňov $x^e - 1$ by muselo byť $\frac{1}{2}|F^*|$, to ale neplatí. Čiže $\left(\frac{\omega}{\pi}\right)_4 = i$ alebo $\left(\frac{\omega}{\pi}\right)_4 = -i$. Tým sme dokončili dôkaz pozorovania.

□

Keďže platí $\left(\frac{\omega}{\pi}\right)_4 = \pm i$, dostávame $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\omega}{\pi}\right)_4^t = (\pm i)^t$. Z tohto vidíme:

- $\left(\frac{\alpha}{\pi}\right)_4 = 1 \Leftrightarrow (\pm i)^t = 1$, a to nastáva práve vtedy, keď $4 \mid t$, ekvivalentne $t \equiv 0 \bmod 4\mathbb{Z}$.
- Rovnako $\left(\frac{\alpha}{\pi}\right)_4 = -1 \Leftrightarrow (\pm i)^t = -1$, a to nastane pre $t \equiv 2 \bmod 4\mathbb{Z}$.

- Ďalej $\left(\frac{\alpha}{\pi}\right)_4 = -i \Leftrightarrow (\pm i)^t = -i$. Musíme rozlíšiť hodnoty kvartického symbolu $\left(\frac{\omega}{\pi}\right)_4 = -i$ a $\left(\frac{\omega}{\pi}\right)_4 = i$. V prvom prípade $(-i)^t = -i \Leftrightarrow t \equiv 1 \bmod 4\mathbb{Z}$ a v druhom prípade $i^t = -i \Leftrightarrow t \equiv 3 \bmod 4\mathbb{Z}$.
- Nakoniec úplne analogicky vyriešime prípad $\left(\frac{\alpha}{\pi}\right)_4 = i$. Opäť rozlíšime prípady podľa hodnoty $\left(\frac{\omega}{\pi}\right)_4$. Takže $(-i)^t = i \Leftrightarrow t \equiv 3 \bmod 4\mathbb{Z}$ a v druhom prípade $i^t = i \Leftrightarrow t \equiv 1 \bmod 4\mathbb{Z}$.

Roztriedili sme teda prvky $\alpha \in F^*$ do štyroch rovnako veľkých skupín, v každej z nich je hodnota kvartického symbolu pre každý jej prvok $\left(\frac{\alpha}{\pi}\right)_4$ rovná jednej z hodnôt i^k pre $k = 0,1,2,3$. □

3.2.3 Zovšeobecnený kvartický symbol a zákon bikvadratickej reciprocity

Definícia 32. *Prvok $\alpha \in \mathbb{Z}[i]$ nazveme* primárnym, *ak platí:*

$$\alpha \equiv 1 \bmod (1+i)^3\mathbb{Z}[i].$$

Definícia 33. *Nech $\beta \in \mathbb{Z}[i]$, $\beta \parallel \prod_i \lambda_i$ je rozklad na súčin ireducibilných prvkov, $(1+i) \nmid \beta$ a $\alpha \in \mathbb{Z}[i]$.* ***Zovšeobecnený kvartický symbol*** *definujeme*

$$\left(\frac{\alpha}{\beta}\right)_4 = \prod_i \left(\frac{\alpha}{\lambda_i}\right)_4.$$

Poznámka.

- Zovšeobecnený kvartický symbol je dobre definovaný (vďaka bodu 3 tvrdenia 29).
- Všimnime si, že zovšeobecnený kvartický symbol je rovný nule práve vtedy, keď $(\alpha, \beta) > 1$.
- Pre ireducibilný prvok $\beta \in \mathbb{Z}[i]$ je zovšeobecnený kvartický symbol rovný kvartickému symbolu.
- V ďalšom texte budeme ako pre kvartický symbol, tak aj pre zovšeobecnený kvartický symbol používať rovnaké pomenovanie kvartický symbol.

Zákon bikvadratickej reciprocity je najdôležitejšou vetou teórie kvartických symbolov. Táto veta umožňuje spočítať hodnotu kvartického symbolu $\left(\frac{\alpha}{\beta}\right)_4$ pre ľubovoľné $\alpha, \beta \in \mathbb{Z}[i]$ také, že $(1+i) \nmid \beta$, bez znalosti rozkladu β na súčin prvočiniteľov. Algoritmus pre výpočet kvartického symbolu uvidíme v sekcii 3.3.3.

Dôkaz vety je mimoriadne zdĺhavý a nebudeme sa mu venovať, nachádza sa v knihe (Ireland a Rosen, 2013, Chapter 9, Paragraph 9). V rovnakom zdroji nájdeme aj dôkaz lemy 34.

Lema 34. *Nech je $\alpha \in \mathbb{Z}[i]$ neinvertibilný prvok a $(1+i) \nmid \alpha$. Potom existuje práve jeden invertibilný prvok $u \in \{1, -1, i, -i\}$ taký, že $u\alpha$ je primárny prvok.*

Veta 35 (Zákon bikvadratickej reciprocity)**.** *Nech sú $\alpha, \beta \in \mathbb{Z}[i]$ primárne prvky. Potom:*

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{\frac{N(\alpha)-1}{4}\cdot\frac{N(\beta)-1}{4}} \left(\frac{\beta}{\alpha}\right)_4$$

Tvrdenie 36 (Pravidlá pre výpočet kvartického symbolu)**.** *Ak je $\alpha = a + bi$ primárny prvok, platí:*

1. $\left(\frac{1+i}{\alpha}\right)_4 = i^{\frac{a-b-1-b^2}{4}}$.
2. *(a)* $\left(\frac{1}{\alpha}\right)_4 = 1$
   (b) $\left(\frac{i}{\alpha}\right)_4 = i^{-\frac{a-1}{2}}$
   (c) $\left(\frac{-1}{\alpha}\right)_4 = (-1)^{\frac{a-1}{2}}$
   (d) $\left(\frac{-i}{\alpha}\right)_4 = i^{\frac{a-1}{2}}$

Predchádzajúce tvrdenie použijeme pri výpočte kvartického symbolu na konci tejto práce. Dôkaz jednotlivých bodov poskytuje napríklad článok (Williams, 1976).

3.3 Konštrukcia testov prvočíselnosti

V tejto sekcii sa pokúsime zostrojiť prvočíselný test založený na kvartickom symbole, ktorý bude istou obdobou Solovay-Strassenovho testu, ktorému sme sa venovali v sekcii 1.3. Využijeme pritom teóriu, ktorú sme v predchádzajúcich sekciách vybudovali.

V Solovay-Strassenovom teste sme overili pre t rôznych hodnôt $a \in \mathbb{Z}/n\mathbb{Z}$, či platí kongruencia $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\mathbb{Z}$. V prípade, že sme našli protipríklad, pre ktorý to neplatí, teda Eulerovho svedka, s istotou sme označili číslo n za zložené. Ak test prebehol t-krát a medzitým sme neodhalili, že číslo n je zložené, vyhlásili sme, že ide pravdepodobne o prvočíslo. Celý čas sme sa pohybovali v okruhu $\mathbb{Z}/n\mathbb{Z}$.

Naším zámerom je vytvoriť test, kde na jednej strane bude stáť hodnota kvartického symbolu, ktorú budeme porovnávať s nejakou inou hodnotou na druhej strane, tak ako to je v prípade Solovay-Strassenovho testu. Keďže kvartický symbol máme definovaný v obore $\mathbb{Z}[i]$, pri testovaní potrebujeme skúmať čísla $\alpha \in \mathbb{Z}[i]/n\mathbb{Z}[i]$.

Z tvrdenia 6 vyplýva, že existuje $b \in \mathbb{Z}/p\mathbb{Z}$ také, že $b^2 \equiv -1 \bmod p\mathbb{Z}$, práve vtedy, keď $p \equiv 1 \bmod 4\mathbb{Z}$. To znamená, že prvok i, pre ktorý platí $i^2 = -1$, už v okruhu $\mathbb{Z}/p\mathbb{Z}$ leží pre $p \equiv 1 \bmod 4\mathbb{Z}$. Tento prvok i budeme niekedy označovať $i = \sqrt{-1}$. Je jednoznačne určený až na znamienko. Pre prvočíslo $p \equiv 3 \bmod 4\mathbb{Z}$ naopak prvok $i \notin \mathbb{Z}/p\mathbb{Z}$.

Teraz uvažujme $n \in \mathbb{Z}$ zložené číslo, $n \equiv 3 \bmod 4\mathbb{Z}$.

Lema 37. *Ak máme $n \in \mathbb{Z}$ zložené číslo, $n \equiv 3 \bmod 4\mathbb{Z}$, potom prvok i taký, že $i^2 = -1$, neleží v $\mathbb{Z}/n\mathbb{Z}$.*

Dôkaz. Na dôkaz využijeme nasledujúce pozorovanie:

Pozorovanie. Nech $n \parallel p_1^{a_1} \cdots p_r^{a_r}$ je prvočíselný rozklad n v obore $\mathbb{Z}$. Ak platí $n \equiv 3 \bmod 4\mathbb{Z}$, potom existuje $j \in \{1, \ldots, r\}$ také, že $p_j \equiv 3 \bmod 4\mathbb{Z}$ a exponent a_j je nepárny.

Dôkaz pozorovania. Ak by bolo každé $p_i \equiv 1 \bmod 4\mathbb{Z}$, potom by z vlastností modulárnej aritmetiky vyplývalo, že aj $n \parallel p_1^{a_1} \cdots p_r^{a_r} \equiv 1 \bmod 4\mathbb{Z}$. Označme j index, pre ktorý $p_j \not\equiv 1 \bmod 4\mathbb{Z}$, ide o prvočíslo, čiže $p_j \equiv 3 \bmod 4\mathbb{Z}$. Druhá časť: ak by bol exponent a_j párny, číslo $p_j \equiv 3 \bmod 4\mathbb{Z}$ by po umocnení dávalo výsledok $p_j^{a_j} \equiv 1 \bmod 4\mathbb{Z}$, takže opäť z vlastností modulárnej aritmetiky plynie, že a_j je nepárne číslo. Tým sme dokončili dôkaz pozorovania. □

Označme prvočíselný rozklad n ako v pozorovaní. Čínska veta o zvyškoch (Stanovský a Barto, 2017, Důsledek 6.6) nám dáva izomorfizmus okruhov:

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$$

$$a \mapsto (a \bmod p_1^{a_1}\mathbb{Z}, \ldots,\ a \bmod p_r^{a_r}\mathbb{Z}).$$

Všimneme si, že $\sqrt{-1} \in \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \sqrt{-1} \in \mathbb{Z}/p_i^{a_i}\mathbb{Z}$ pre každé $i \in \{1,2,\ldots,r\}$. Ďalej ak $\sqrt{-1} \in \mathbb{Z}/p_i^{a_i}\mathbb{Z}$, potom $\sqrt{-1} \in \mathbb{Z}/p_i\mathbb{Z}$. Podľa pozorovania existuje $j \in \mathbb{N}$ také, že $p_j \equiv 3 \bmod 4$. Ako sme vyššie uviedli, z teórie čísel vieme, že $p_j \equiv 3 \bmod 4$ je ekvivalentné tomu, že $\sqrt{-1} \notin \mathbb{Z}/p_j\mathbb{Z}$. Prvok $\sqrt{-1}$ neleží v $\mathbb{Z}/p_j\mathbb{Z}$, potom neleží ani v $\mathbb{Z}/p_j^{a_j}\mathbb{Z}$, takže $\sqrt{-1}$ neleží v $\mathbb{Z}/n\mathbb{Z}$. □

Rozšíriť okruh $\mathbb{Z}/n\mathbb{Z}$ o prvok i je rozumné v prípade, že i v pôvodnom okruhu ešte neleží. Obmedzíme sa preto pri vytváraní testu iba na testovanie čísel $n \in \mathbb{Z}$ takých, že $n \equiv 3 \bmod 4\mathbb{Z}$.

3.3.1 Slabší test

Našou úlohou je o čísle $n \equiv 3 \bmod 4\mathbb{Z}$ rozhodnúť, či ide o prvočíslo, alebo je n zložené. Najjednoduchšie by sa mohlo zdať vytvoriť test na základe nasledujúceho tvrdenia, kde by sme porovnávali pre rôzne hodnoty $a \in \mathbb{Z}$, či je hodnota kvartického symbolu $a^{(n^2-1)/4} \equiv 1 \bmod n\mathbb{Z}$. Ide o tvrdenie z knihy (Ireland a Rosen, 2013, Proposition 9.8.4), v dôkaze sme doplnili niektoré medzikroky pre lepšiu čitateľnosť.

Tvrdenie 38. *Nech q je prvočíslo $\in \mathbb{Z}$, $q \equiv 3 \bmod 4\mathbb{Z}$. Potom $\left(\frac{a}{q}\right)_4 = 1$ pre všetky $a \in \mathbb{Z}, q \nmid a$.*

Dôkaz. Pretože $N(q) = q^2$ dostávame:

$$\left(\frac{a}{q}\right)_4 \equiv a^{(q^2-1)/4} \bmod q\mathbb{Z}[i].$$

Keďže $a^{(q^2-1)/4}$ je celé číslo, môžeme uvažovať, čomu je kongruentné modulo $q\mathbb{Z}$. $a^{(q^2-1)/4} \equiv (a^{q-1})^{(q+1)/4} \equiv 1 \bmod q\mathbb{Z}$ podľa malej Fermatovej vety (veta 10). Podľa lemy 19 platí

$$a^{(q^2-1)/4} \equiv 1 \bmod q\mathbb{Z} \Leftrightarrow a^{(q^2-1)/4} \equiv 1 \bmod q\mathbb{Z}[i].$$

Podľa tvrdenia 27 je $a^{(q^2-1)/4} \bmod q\mathbb{Z}[i]$ pre $q \nmid a$ kongruentné práve jednému z prvkov $\{\pm 1, \pm i\}$, takže dostávame $\left(\frac{a}{q}\right)_4 = 1$. □

Testovací algoritmus by vyzeral takto:

TEST 4.

Vstup: $n \in \mathbb{Z}$ také, že $(1+i) \nmid n$.

1. Zafixujeme celé číslo $t \geq 1$ ako počet pokusov pre test.
2. Vezmeme náhodné celé číslo $a \in \{1, \ldots, n-1\}$.
3. Overíme, či platí $(a,n) = 1$. Ak odhalíme $(a,n) > 1$, test ukončíme s prehlásením, že „n je zložené“.
4. Ak $a^{(n^2-1)/4} \not\equiv 1 \bmod n\mathbb{Z}$, test ukončíme s prehlásením, že „n je zložené“.
5. Ak $a^{(n^2-1)/4} \equiv 1 \bmod n\mathbb{Z}$, pokračujeme krokom *2.*
6. Keď test prebehne t-krát bez prerušenia, vyhlásime, že „n je pravdepodobne prvočíslo“.

Vzhľadom k tomu, že v dôkaze tvrdenia 38 využívame malú Fermatovu vetu, jednoducho sa overí, že takto skonštruovaný test bude vyhlasovať chybné výsledky pre Carmichaelove čísla. Pre Carmichaelovo číslo sú jediné protipríklady na kongruenciu $a^{n-1} \equiv 1 \bmod n\mathbb{Z}$ čísla a také, že $(a,n) > 1$. Zastúpenie súdeliteľných čísel v množine $a \in \{1, \ldots, n-1\}$ môže byť minimálne. Často môže nastať situácia, že test prejde t-krát bez prerušenia, hoci číslo je zložené.

Príklad. $n = 8911$ je najmenšie Carmichaelovo číslo také, že $n \equiv 3 \bmod 4$. Jeho rozklad na súčin prvočísel je $8911 = 7 \cdot 19 \cdot 67$. Spočítajme počet súdeliteľných čísel s n v množine $\{1, 2, \ldots, n\}$. Eulerova funkcia $\varphi(n)$ nám dáva počet nesúdeliteľných čísel s n v tejto množine. Počet súdeliteľných teda dostaneme ako $n - \varphi(n)$.

$$n - \varphi(8911) = n - \varphi(7)\varphi(19)\varphi(67) = n - 6 \cdot 18 \cdot 66 = 8911 - 7128 = 1783$$

Takže súdeliteľných čísel s 8911 v množine $\{1, 2, \ldots, 8911\}$ je 1783, čo tvorí len približne 20 %.

Carmichaelove čísla nie sú pre náš testovací algoritmus jediné problematické čísla. Pre každé celé číslo $a \in \{1, \ldots, n\}, (a,n) = 1$ budeme dostávať $a^{(n^2-1)/4} \equiv 1 \bmod n\mathbb{Z}$, hoci n je zložené, aj v prípade, že $\varphi(n) \mid \frac{n^2-1}{4}$ (využitie Eulerovej vety). Toto kritérium je splnené napríklad pre číslo 15.

Príklad. $n = 15$. Spočítame hodnotu $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$.

$$\frac{n^2-1}{4} = \frac{15^2-1}{4} = 56$$

Platí $\varphi(n) = 8 \mid 56 = \dfrac{n^2-1}{4}$. Pre každé číslo nesúdeliteľné s 15, teda pre každé číslo $a \in \{1,2,4,7,8,11,13,14\}$ dostaneme $a^{56} \equiv 1 \bmod n\mathbb{Z}$.

Vidíme, že náš test 4 je vlastne oslabením Fermatovho testu, ktorý sme popisovali v odstavci 1.1.3, a teda jednoduché tvrdenie 38 nie je vhodným základom pre vytvorenie testu.

3.3.2 Test založený na výpočte kvartického symbolu

Pokúsime sa teraz zostrojiť test založený na rovnosti modulo n, kde na jednej strane spočítame hodnotu kvartického symbolu $\left(\frac{\alpha}{n}\right)_4$ a na druhej strane $\alpha^{(n^2-1)/4}$. Keďže prvočíslo $p \equiv 3 \bmod 4$ je prvočiniteľom v $\mathbb{Z}[i]$, budú sa tieto hodnoty modulo p rovnať, a to priamo z definície kvartického symbolu pre prvočiniteľ. Pokúsime sa ukázať, obdobne ako v Solovay-Strassenových vetách, že pre zložené číslo $n \equiv 3 \bmod 4$ existujú svedkovia a odhadneme ich počet.

V tejto kapitole budeme vytvárať a dokazovať tvrdenia analogické k tým, ktoré platia pre Jacobiho symbol. My ich preformulujeme pre kvartický symbol a dôkazy pre Jacobiho symbol prerobíme na dôkazy pre tvrdenia týkajúce sa kvartického symbolu.

Definícia 39. *Nech $n \in \mathbb{Z}[i], n \equiv 3 \bmod 4$ a $\alpha \in \mathbb{Z}[i]$. Povieme, že α je* kvartický svedok*, ak platí*

$$(\alpha,n) = 1 \ a \ \left(\frac{\alpha}{n}\right)_4 \not\equiv \alpha^{\frac{n^2-1}{4}} \bmod n\mathbb{Z}[i]$$

Veta 40 (Existencia kvartických svedkov)**.** *Pre každé prirodzené zložené číslo také, že $n \equiv 3 \bmod 4\mathbb{Z}$, $k \in \mathbb{Z}$, existuje číslo $\alpha \in \mathbb{Z}[i]$ také, že $(\alpha, n) = 1$ a*

$$\left(\frac{\alpha}{n}\right)_4 \not\equiv \alpha^{\frac{n^2-1}{4}} \bmod n\mathbb{Z}[i]$$

Poznámka. Kvartický symbol je definovaný iba pre n také, že $(1+i) \nmid n$. Všimnime si, že predpoklad sme vo vete mohli vynechať, pretože $n \equiv 3 \bmod 4\mathbb{Z}$ implikuje, že $(1+i) \nmid n$.

Dôkaz. Rozlíšime 2 prípady:
v rozklade n sa žiaden prvočiniteľ nevyskytuje vo vyššej ako prvej mocnine.

Nech $n \parallel \pi_1 \cdots \pi_r$, n je zložené, teda $r > 1$ a $\pi_i \nmid\!\!\mid \pi_j$ pre $i \neq j$. Podľa tvrdenia 31 existuje $\beta \in \mathbb{Z}[i], \beta \neq 0$ také, že $\left(\frac{\beta}{\pi_1}\right)_4 = -1$. Keďže platí $(\pi_1, \pi_2 \cdots \pi_r) = 1$, môžeme použiť čínsku vetu o zvyškoch pre eukleidovské obory. Presnú formuláciu aj s dôkazom nájdeme v skriptách Počítačovej algebry, (Stanovský a Barto, 2017, kapitola 6. Zobecněná čínská věta o zbytcích). Tá nám hovorí, že existuje $\alpha \in \mathbb{Z}[i]$ také, že

$$\alpha \equiv \beta \bmod \pi_1\mathbb{Z}[i], \text{a súčasne } \alpha \equiv 1 \bmod \pi_2 \cdots \pi_r\mathbb{Z}[i].$$

Keďže $\beta \not\equiv 0 \bmod \pi_1\mathbb{Z}[i]$, máme $(\alpha,\pi_1) = 1$. Platí tiež $(\alpha, \pi_2 \cdots \pi_r) = 1$. Z toho vyplýva, že aj $(\alpha, n) = 1$. Rozpíšeme:

$$\left(\frac{\alpha}{n}\right)_4 = \left(\frac{\alpha}{\pi_1}\right)_4 \cdots \left(\frac{\alpha}{\pi_r}\right)_4. \tag{3.1}$$

Z kongruencie $\alpha \equiv \beta \bmod \pi_1\mathbb{Z}[i]$ máme vďaka tvrdeniu 1 $\left(\frac{\alpha}{\pi_1}\right)_4 = \left(\frac{\beta}{\pi_1}\right)_4 = -1$ a z kongruencie $\alpha \equiv 1 \bmod \pi_2 \cdots \pi_r\mathbb{Z}[i]$ zase platí $\left(\frac{\alpha}{\pi_i}\right)_4 = \left(\frac{1}{\pi_i}\right)_4 = 1$ pre $i > 1$. Po dosadení do (3.1) dostávame $\left(\frac{\alpha}{n}\right)_4 = \left(\frac{\alpha}{\pi_1}\right)_4 = -1$.

Pre spor predpokladajme, že $\alpha^{\frac{n^2-1}{4}} \equiv \left(\frac{\alpha}{n}\right)_4 \equiv -1 \bmod n\mathbb{Z}[i]$. Využijeme, že π_2 delí n, a teda platí táto kongruencia aj modulo π_2. Keďže $\alpha \equiv 1 \bmod \pi_2\mathbb{Z}[i]$, dostávame $1 \equiv -1 \bmod \pi_2\mathbb{Z}[i]$, čo je ekvivalentné $\pi_2 \mid 2$.

Potom $\pi_2 \mid -i(1+i)^2 = 2$. Ale π_2 je prvočiniteľ, z toho plynie, že $\pi_2 \parallel (1+i)$. π_2 je deliteľ n, ale $(1+i) \nmid n$, ako sme si rozmysleli v poznámke za formuláciou vety, takže dostávame spor, čím sme ukázali $\alpha^{\frac{n^2-1}{4}} \not\equiv \left(\frac{\alpha}{n}\right)_4 \bmod n\mathbb{Z}[i]$.

Teraz predpokladajme, že n obsahuje faktor π aspoň v druhej mocnine, tj. n je tvaru $n = \pi^k\beta$, kde $k \geq 2$, $\beta \in \mathbb{Z}[i]$ a $(\pi,\beta) = 1$. Podľa čínskej vety o zvyškoch pre eukleidovské obory existuje $\alpha \in \mathbb{Z}[i]$ spĺňajúca

$$\alpha \equiv 1 + \pi \bmod \pi^2\mathbb{Z}[i], \text{ a súčasne } \alpha \equiv 1 \bmod \beta\mathbb{Z}[i].$$

Keďže $\pi \nmid \alpha$ a $(\alpha,\beta) = 1$, máme $(\alpha,n) = 1$. Predpokladajme pre spor, že $\alpha^{\frac{n^2-1}{4}} \equiv \left(\frac{\alpha}{n}\right)_4 \bmod \beta\mathbb{Z}[i]$. Umocnením oboch strán na štvrtú máme $\alpha^{n^2-1} \equiv 1 \bmod n\mathbb{Z}[i]$. Keďže $\pi^2 \mid n$, platí aj $\alpha^{n^2-1} \equiv 1 \bmod \pi^2\mathbb{Z}[i]$. Celkovo obdržíme

$$1 \equiv \alpha^{n^2-1} \equiv (1+\pi)^{n^2-1} \equiv \sum_{i=0}^{n^2-1} \binom{n^2-1}{i} 1^{n^2-1-i}\pi^i \equiv 1 + (n^2-1)\pi \bmod \pi^2\mathbb{Z}[i].$$

Odpočítaním jednotky získame $(n^2-1)\pi \equiv 0 \bmod \pi^2\mathbb{Z}[i]$, po vykrátení kongruencie prvkom π dostávame $(n^2-1) \equiv 0 \bmod \pi\mathbb{Z}[i] \Leftrightarrow \pi \mid (n^2-1) = (n-1)(n+1)$. Keďže π je prvočiniteľ, $\pi \mid n-1$ alebo $\pi \mid n+1$.

Najskôr predpokladajme, že $\pi \mid n-1$. Zároveň je π v rozklade n na ireducibilné prvky, $\pi \mid n$. Keďže $\pi \mid n$ a $\pi \mid n-1$, potom $\pi \mid 1$, čo je spor s faktom, že π je ireducibilný prvok v $\mathbb{Z}[i]$. Rovnako dostaneme spor aj v prípade $\pi \mid n+1$.

Opäť sme ukázali, že $\alpha^{\frac{n^2-1}{4}} \not\equiv \left(\frac{\alpha}{n}\right)_4 \bmod \beta\mathbb{Z}[i]$. □

Dôsledok 41 (Veľkosť množiny kvartických svedkov)**.** *Nech n je zložené celé číslo také, že $n \equiv 3 \bmod 4\mathbb{Z}$. Označme*

$$M := \{\alpha = a + bi \in \mathbb{Z}[i], 0 \leq a,b < n : (\alpha,n) = 1 \text{ a } \alpha^{(n^2-1)/4} \equiv \left(\frac{\alpha}{n}\right)_4 \bmod n\mathbb{Z}[i]\}$$

1. *Ak je n prvočíslo, potom $|M| = n^2 - 1$.*
2. *Ak je n zložené číslo, potom $|M| < \frac{n^2-1}{2}$.*

Dôkaz. 1. Vyplýva priamo z definície kvartického symbolu pre ireducibilný prvok a z faktu, že prvočíslo $p \equiv 3 \bmod 4$ je ireducibilný prvok v $\mathbb{Z}[i]$. Pre ľubovoľný prvok $\alpha \in \mathbb{Z}[i]$ taký, že $p \nmid \alpha$ je kvartický symbol $\left(\frac{\alpha}{p}\right)_4$ definovaný ako práve jeden prvok množiny $\{\pm 1, \pm i\}$, ktorý je kongruentný $\alpha^{(N(p)-1)/4}$. Platí $N(p) = p^2$.

Takže pre všetky prvky $\alpha = a + bi \in \mathbb{Z}[i], 0 \leq a,b < p$, okrem prvku $0 + 0i$, ktorý ale nepatrí do M, platí, že $p \nmid \alpha$, takže $\left(\frac{\alpha}{p}\right)_4 \equiv \alpha^{(p^2-1)/4} \bmod p\mathbb{Z}[i]$.

2. Za reprezentantov faktorokruhu $\mathbb{Z}[i]/n\mathbb{Z}[i]$ môžeme zvoliť prvky tvaru $\{a + bi,\ 0 \leq a,b < n\}$, ukázalo by sa to obdobne ako časť dôkazu vety 24, konkrétne časť, v ktorej ukazujeme, akými prvkami môžeme všetky rozkladové triedy reprezentovať a že žiadne dva nereprezentujú rovnakú rozkladovú triedu. Takže veľkosť množiny $|\mathbb{Z}[i]/n\mathbb{Z}[i]| = n^2$. Položme množiny

$$A = \{\alpha = a + bi \in \mathbb{Z}[i], 0 \leq a,b < n : (\alpha,n) = 1 \text{ a } \alpha^{(n^2-1)/4} \equiv \left(\frac{\alpha}{n}\right)_4 \bmod n\mathbb{Z}[i]\},$$

$$B = \{\alpha = a + bi \in \mathbb{Z}[i], 0 \leq a,b < n : (\alpha,n) = 1 \text{ a } \alpha^{(n^2-1)/4} \not\equiv \left(\frac{\alpha}{n}\right)_4 \bmod n\mathbb{Z}[i]\},$$

$$C = \{\alpha = a + bi \in \mathbb{Z}[i], 0 \leq a,b < n,\ \alpha \neq 0 : (\alpha,n) > 1\}.$$

Množiny A, B, C sú disjunktné a ich zjednotenie

$$A \cup B \cup C = (\mathbb{Z}[i]/n\mathbb{Z}[i]) \setminus \{0\}.$$

Platí teda $|A| + |B| + |C| = n^2 - 1$. Vieme, že množina A je neprázdna, pretože $1 \in A$. Tiež vieme, že C nie je prázdna, pretože n je zložené, teda $|C| \geq 1$. Množina B je neprázdna vďaka vete 40.

Ak ukážeme, že $|A| \leq |B|$, dostaneme $n^2 - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|$ a tým aj požadovaný odhad $|A| < \frac{n^2-1}{2}$.

Vezmime prvok množiny B, nech to je β_0. Označme $A\beta_0 = \{\alpha\beta_0 \bmod n\mathbb{Z}[i] : \alpha \in A\}$. Veľkosť $|A| = |A\beta_0|$, vidíme to z nasledujúceho: keďže $\beta_0 \in B$, máme $(\beta_0,n) = 1$ a môžeme teda pomocou krátenia β_0 z kongruencie odstrániť $\alpha\beta_0 \equiv \alpha'\beta_0 \bmod n\mathbb{Z}[i] \Leftrightarrow \alpha \equiv \alpha' \bmod n\mathbb{Z}[i]$, tj, $\alpha = \alpha'$, lebo v A nie sú žiadne dva prvky navzájom kongruentné modulo $n\mathbb{Z}[i]$.

Stačí teda ukázať, že $A\beta_0 \subset B$. Každé $\alpha\beta_0 \in A\beta_0$ a n sú nesúdeliteľné a platí preň:

$$(\alpha\beta_0)^{(n^2-1)/4} \equiv \alpha^{(n^2-1)/4}\beta_0^{(n^2-1)/4} \equiv \left(\frac{\alpha}{n}\right)_4 \beta_0^{(n^2-1)/4} \bmod n\mathbb{Z}[i].$$

Keďže $(\alpha\beta_0,n) = 1$, každé $\alpha\beta_0 \bmod n\mathbb{Z}[i]$ patrí buď do množiny A alebo do množiny B. Predpokladajme, že $\alpha\beta_0 \bmod n\mathbb{Z}[i] \in A$, čiže

$$(\alpha\beta_0)^{(n^2-1)/4} \equiv \left(\frac{\alpha\beta_0}{n}\right)_4 \equiv \left(\frac{\alpha}{n}\right)_4 \left(\frac{\beta_0}{n}\right)_4 \bmod n\mathbb{Z}[i].$$

Spolu s predchádzajúcim vyjadrením tak dostávame

$$\left(\frac{\alpha}{n}\right)_4 \beta_0^{(n^2-1)/4} \equiv \left(\frac{\alpha}{n}\right)_4 \left(\frac{\beta_0}{n}\right)_4 \bmod n\mathbb{Z}[i].$$

Keďže $(\alpha,n) = 1$, potom $\left(\frac{\alpha}{n}\right)_4 \neq 0$ a môžeme kongruenciu vykrátiť. Dostávame

$$\left(\frac{\beta_0}{n}\right)_4 \equiv \beta_0^{(n^2-1)/4} \bmod n\mathbb{Z}[i],$$

čo je spor s $\beta_0 \in B$. Dokázali sme teda, že každé $\alpha\beta_0 \bmod n\mathbb{Z}[i] \in B$, teda $A\beta_0 \subset B$.

Celkovo dostávame $|A| = |A\beta_0| \geq |B|$. Takže $n^2 - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|$, a teda $|A| < \frac{n^2-1}{2}$. □

Tvrdenia, ktoré sme vyššie dokázali, nás nabádajú sformulovať test, ktorý bude založený na výpočte zovšeobecneného kvartického symbolu. Predpokladáme, že $n \in \mathbb{Z}$, $n \equiv 3 \bmod 4\mathbb{Z}$, čo implikuje, že nie je deliteľné $(1 + i)$.

TEST 5.

1. Zafixujeme celé číslo $t \geq 1$ ako počet pokusov pre test.
2. Vezmeme náhodné číslo $\alpha = a + bi \in \mathbb{Z}[i]$, kde $a, b \in \{1, 2, \ldots, n - 1\}$.
3. Overíme, či platí $(\alpha,n) = 1$. Ak odhalíme $(\alpha,n) > 1$, test ukončíme s prehlásením, že „n je zložené“.

4. Ak $\alpha^{(n^2-1)/4} \not\equiv \left(\frac{\alpha}{n}\right)_4 \bmod n\mathbb{Z}[i]$, test ukončíme s prehlásením, že „n je zložené“.

5. Ak $\alpha^{(n^2-1)/4} \equiv 1 \bmod n\mathbb{Z}[i]$, pokračujeme krokom 2.

6. Keď test prebehne t-krát bez prerušenia, vyhlásime, že „n je pravdepodobne prvočíslo“.

Poznámka. Pravdepodobnosť, že n je prvočíslo, ak test prebehol t-krát bez nájdenia kvartického svedka by sa spočítala podobným spôsobom ako v kapitole 2. Potrebovali by sme poznať počty prvočiniteľov v $\mathbb{Z}[i]/n\mathbb{Z}[i]$. Na to by bolo možné použiť známu verziu prvočíselnej vety pre $\mathbb{Z}[i]$, ktorú by sme mohli odvodiť zhruba takto: podľa tvrdenia 22 sú prvočinitele jedného z troch tvarov. Takže počty prvočiniteľov tvaru $\{a + bi \mid a,b \in \mathbb{Z}/n\mathbb{Z}\}$ by sa dali odhadnúť pomocou počtov prvočísel kongruentných 3 modulo $4\mathbb{Z}$ v množine $\{1, 2, \ldots, n\}$, tie zostávajú prvočiniteľmi aj v $\mathbb{Z}[i]$, ďalej pomocou počtu prvočísel kongruentných 1 modulo $4\mathbb{Z}$ v množine $\{1, 2, \ldots, 2n^2\}$, tie sa rozkladajú v $\mathbb{Z}[i]$ na súčin 2 prvočiniteľov a prvočiniteľ $(1+i)$. Tým pádom by sme mohli previesť problém hľadania prvočiniteľov tvaru $\{a + bi \mid a,b \in \mathbb{Z}/n\mathbb{Z}\}$ na problém hľadania prvočísel v $\mathbb{Z}$. Tento problém sa javí menej náročným, ale viaže sa k nemu množstvo výpočtov a odhadovania počtu prvočísel kongruentných 3 modulo $4\mathbb{Z}$ a 1 modulo $4\mathbb{Z}$, nebudeme sa im v tejto práci venovať.

Poznámka. V krokoch 4 a 5 symbol $\left(\frac{\alpha}{n}\right)_4$ značí zovšeobecnený kvartický symbol, ktorý vďaka zákonu bikvadratickej reciprocity spočítame bez znalosti rozkladu n na súčin prvočiniteľov, konkrétne na to využijeme nasledujúci algoritmus.

3.3.3 Výpočet zovšeobecneného kvartického symbolu

Algoritmus

Na vstupe dostaneme prvky $\alpha, \beta \in \mathbb{Z}[i]$, pričom $(1+i) \nmid \beta$ a β je neinvertibilný. Na výstup vydáme hodnotu zovšeobecneného kvartického symbolu $\left(\frac{\alpha}{\beta}\right)_4$. Jednotlivé kroky algoritmu:

0. Overíme, či $(\alpha, \beta) = 1$. Ak odhalíme, že $(\alpha, \beta) > 1$, ukončíme algoritmus s výstupom $\left(\frac{\alpha}{\beta}\right)_4 = 0$. V opačnom prípade pokračujeme.

1. Zredukujeme hodnotu α modulo $\beta\mathbb{Z}[i]$ (využívame bod 1 v tvrdení 29).

2. Prenásobíme β vhodným z prvkov $\{1, -1, i, -i\}$ tak, aby bol prvok β primárnym prvkom v $\mathbb{Z}[i]$ (vďaka leme 34 je takýto prvok jednoznačne určený). Hodnota kvartického symbolu zostane nezmenená $\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\alpha}{\beta'}\right)_4$, lebo $\beta \parallel \beta'$ (viď bod 3 v tvrdení 29).

3. Rozložíme α na súčin $(1+i)^k \cdot \tilde{\alpha}$, kde $(1+i) \nmid \tilde{\alpha}$ a $k \geq 0$. Využijeme vlastnosť 1 tvrdenia 36 a aplikovaním tvrdenia o multiplikativite kvartického symbolu (bod 2 tvrdenia 29) spočítame $A := \left(\frac{1+i}{\beta'}\right)_4^k$. Ostáva $A\left(\frac{\tilde{\alpha}}{\beta'}\right)_4$.

4. Ak je hodnota $\tilde{\alpha}$ z množiny $\{\pm 1, \pm i\}$, spočítame $Q := \left(\frac{\tilde{\alpha}}{\beta'}\right)_4$ pomocou tvrdenia 36 - bod 2. Výstupom v tomto prípade bude AQ. V opačnom prípade pokračujeme.

5. Prenásobíme $\tilde{\alpha}$ vhodným prvkom $\gamma \in \{\pm 1, \pm i\}$, aby sme dostali primárny prvok α' (jednoznačnosť vďaka leme 34). Hodnota kvartického symbolu $\left(\frac{\tilde{\alpha}}{n'}\right)_4 = \left(\frac{\gamma}{\beta'}\right)_4 \left(\frac{\alpha'}{\beta'}\right)_4$. Hodnotu $B := \left(\frac{\gamma}{\beta'}\right)_4$ spočítame pomocou bodu 2 tvrdenia 36. Ostáva $AB\left(\frac{\alpha'}{\beta'}\right)_4$.

6. Oba prvky α' aj β' sú primárne a preto môžeme použiť zákon bikvadratickej reciprocity (veta 35). Dostávame $\left(\frac{\alpha'}{\beta'}\right)_4 = (-1)^{\frac{N(\alpha')-1}{4} \cdot \frac{N(\beta')-1}{4}} \left(\frac{\beta'}{\alpha'}\right)_4$. Označme $C := (-1)^{\frac{N(\alpha')-1}{4} \cdot \frac{N(\beta')-1}{4}}$.

7. Rekurzívne spustíme algoritmus, (od kroku 1) tentokrát pre hodnoty β',α', aby sme spočítali $Q = \left(\frac{\beta'}{\alpha'}\right)_4$. Konečným výstupom bude hodnota $ABCQ$.

Záver

V kapitole 1 sme ponúkli prehľadné zhrnutie algoritmu Solovay-Strassenovho testu spoločne s teóriou, ktorá sa s ním spája.

V kapitole 2 sme sa venovali pravdepodobnosti, s akou je číslo n prvočíslo, ak to o ňom prehlásil Solovay-Strassenov test. Vychádzali sme z článku (Conrad), v ktorom bola táto pravdepodobnosť spočítaná. My sme ju vylepšili, s prihliadnutím na fakt, že pre číslo n je jednoduché skontrolovať, že nie je deliteľné konkrétnym prvočíslom p. Ako sme videli na konci kapitoly 2, v porovnaní s pôvodným výpočtom z (Conrad) sa pravdepodobnosť znateľne zväčšila už aj pre nízky počet prvočísel nedeliacich n.

Kapitola 3 pojednávala o kvartickom symbole a obdobe Solovay-Strassenovho testu, ktorú sme v nej konštruovali. Nepokúsili sme sa skonštruovať validný test pre ľubovoľné nepárne číslo n, vytvorili sme test iba pre $n \equiv 3 \bmod 4\mathbb{Z}$. Dôvod je popísaný v sekcii 3.3.

Možností pre rozšírenie práce sa ponúka hneď niekoľko. Zaujímavý by mohol byť výpočet pravdepodobnosti pre náš skonštruovaný test, obdobný tomu, ktorý sme uviedli v kapitole 2 a porovnať ho s pôvodným Solovay-Strassenovým testom. Ďalšou úlohou by mohol byť pokus rozšíriť test z tretej kapitoly pre čísla $n \equiv 1 \bmod 4\mathbb{Z}$.

Zoznam použitej literatúry

Conrad, K. The Solovay-Strassen test. URL https://kconrad.math.uconn.edu/blurbs/ugradnumthy/solovaystrassen.pdf.

Drápal, A. Teorie čísel a RSA. URL http://www.karlin.mff.cuni.cz/~drapal/teorie_cisel.pdf.

Hlubinka, D. NMAI059 Pravdepodobnost a statistika. Příručka k přednášce. URL http://www.karlin.mff.cuni.cz/~hlubinka/soubory/nmai059_skripta_2018.pdf.

Ireland, K. a Rosen, M. (2013). *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer New York. ISBN 9781475721034.

Stanovský, D. (2010). *Základy algebry*. První vydání. Matfyzpress, Praha. ISBN 978-80-7378-105-7.

Stanovský, D. a Barto, L. (2017). *Počítačová algebra*. Druhé, upravené vydání. Matfyzpress, Praha. ISBN 978-80-7378-340-2.

Williams, K. S. (1976). On the Supplement to the Law of Biquadratic Reciprocity. *Proceedings of the American Mathematical Society*, **59**(1), 19–22.

Zagier, D. (1997). Newman's Short Proof of the Prime Number Theorem. *The American Mathematical Monthly*, **104**(8), 705–708.