VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Testovanie prvočíselnosti

Primality testing

2014

Erika Straková

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Zadání bakalářské práce

Student: **Erika Straková**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 1103R031 Výpočetní matematika

Téma: Testování prvočíselnosti
Primality testing

Zásady pro vypracování:

Bakalářská práce by měla obsahovat popis nejznámějších deterministických a pravděpodobnostních testů prvočíselnosti. Konkrétně, jejich teoretický základ, algoritmus a popis případných výhod a nevýhod.

Seznam doporučené odborné literatury:

Kolibiar, M., Legéň, A., Šalát, T., Znám, Š.: *Algebra a príbuzné disciplíny*, Bratislava, Alfa, 1992.

Šlát,T.: *Algebra a teoretická aritmetika 2*, Bratislava, Alfa, 1986.

Znám, Š.: *Teória čísel*, Bratislava, Alfa, 1986.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **RNDr. Pavel Jahoda, Ph.D.**

Datum zadání: 01.09.2013
Datum odevzdání: 07.05.2014

doc. RNDr. Jiří Bouchala, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prehlasujem, že som túto bakalársku prácu vypracovala samostatne. Uviedla som všetky literárne pramene a publikácie, z ktorých som čerpala..

V Ostrave 5. mája 2014 ..... Strakova .....

Rada by som sa poďakovala vedúcemu práce RNDr. Pavlovi Jahodovi, Ph.D. za čas venovaný konzultáciám, poskytnuté podklady a za odborné vedenie bakalárskej práce.

Abstrakt

Táto práca popisuje najznámejšie testy prvočíselnosti. Prvé dve kapitoly sú venované základným pojmom, definíciám a dôkazom. Tretia kapitola popisuje Fermatovu-Eulerovu vetu, ktorá sa neskôr využíva pri odvodení Fermatovho a Miller-Rabinovho testu. Zvyšné kapitoly sú venované pravdepodobnostným a deterministickým testom prvočíselnosti, a to konkrétne ich teoretickému základu, odvodeniu a popisu. Tieto kapitoly obsahujú aj algoritmus naimplementovaný v Matlabe aj v Maple

Kľúčové slová: Eratosthenovo sito, Fermatov test prvočíselnosti, Miller-Rabinov test prvočíselnosti, AKS deterministický test prvočíselnosti

Abstract

This thesis describes the most famous primality tests. The first two chapters are about basic terms, definitions and proofs. The third chapter describes Fermat-Euler theorem, which was later used in the derivation of Fermat and Miller-Rabin primality test. The other chapters are about probabilistic and deterministic primality tests, specifically about their theoretical basis, derivation and description. These chapters also contain algorithm, which is deployed in Matlab and Maple.

Keywords: Sieve of Eratosthenes, Fermat primality test, Miller-Rabin primality test, AKS deterministic primality test

Zoznam použitých skratiek a symbolov

$\mathbb{Z}$	–	množina celých čísel
$\mathbb{N}$	–	množina prirodzených čísel
$gcd(a, b)$	–	najväčší spoločný deliteľ čísel a a b
$n(a, b)$	–	najmenší spoločný násobok čísel a a b
$\pi(n)$	–	počet prvočísel menších alebo rovných n
$\bar{r}_m$	–	množina všetkých celých čísel kongruentných s číslom r modulo m
$\varphi(m)$	–	počet prirodzených čísel menších alebo rovných m takých, ktoré sú s m nesúdeliteľné
$\lceil a \rceil$	–	horná celá časť čísla a

Obsah

Zoznam obrázkov

Zoznam výpisov zdrojového kódu

1 Úvod

V tejto práci sa zaoberáme pravdepodobnostnými a deterministickými testami prvočíselnosti. Prvočíslo je číslo, ktoré nemá okrem jednotky a samého seba žiadneho iného deliteľa. Test, ktorý spočíva v tom, že si postupne začneme deliť testované číslo všetkými číslami od dvojky a tak zistíme, či má nejakého deliteľa, nie je pre veľké čísla veľmi praktický. V tejto práci si ukážeme testy, pravdepodobnostné či deterministické, ktoré sú pre veľké testované čísla praktickejšie.

V kapitolách 2 a 3 sa budeme zaoberať základnými pojmami a dôkazmi z problemtiky deliteľnosti a prvočíselnosti.

Kapitola 4 je venovaná odvodeniu, popisu a dôkazu Fermatovej-Eulerovej vety, z ktorej je odvodený Fermatov a Miller-Rabinov test prvočíslenosti.

Zvyšok práce sa zaoberá jednotlivými testami prvočíselnosti a následnou implementáciou v Matlabe a Maple. Najjednoduchší z nich je Eratosthenovo sito, popísaný v kapitole 5. Funguje tak, že prechádza postupne všetky čísla nachádzajúce sa v „site“ a odstraňuje ich násobky až kým nezostanú len prvočísla.

V kapitolách 6 a 7 sa budeme zaoberať Fermatovým a Miller-Rabinovým pravdepodobnostným testom. Tieto testy sú založené na hľadaní svedka zloženosti medzi náhodne vygenerovanými číslami. V prípade, že takéhoto svedka nenájdeme, testované číslo je s určitou pravdepodobnosťou prvočíslo.

Posledná kapitola je venovaná AKS deterministickému testu, ktorý jednoznačne určí, čí testované číslo je prvočíslo alebo číslo zložené, ale je náročnejší na implementáciu a čas.

2 Deliteľnosť a prvočísla

2.1 Základné vlastnosti deliteľnosti

Definícia 2.1.1 Nech $a, d \in \mathbb{Z}$. Hovoríme, že d delí a práve vtedy, keď existuje $q \in \mathbb{Z}$ také, že $a = qd$. Značíme $d \mid a$.

Ak d nedelí a, môžeme to označiť symbolom $d \nmid a$. Keď d delí a, myslíme, že $a = qd$, pričom q je nejaké celé číslo. Požiadavka, že q je celé číslo je rozhodujúca. Napríklad $4 \nmid 6$, pretože $4 = \frac{3}{2} \cdot 6$.

Príklad: Platí: $13 \mid 52$?

Riešenie: Chceme určiť, či existuje celé číslo q také, že $52 = q13$. Takým číslom je číslo 4, pretože $52 = 4 \cdot 13$.

Lemma 2.1.2 Nech $d, m, n, x, y \in \mathbb{Z}$. Ak $d \mid x$ a zároveň $d \mid y$, potom $d \mid (mx + ny)$.

Dôkaz. Ak $d \mid x$, potom existuje $k \in \mathbb{Z}$ také, že

$$x = kd. \tag{2.1}$$

Vynásobením oboch strán rovnice 2.1 číslom m dostávame:

$$mx = mkd.$$

Ak $d \mid y$, potom existuje $l \in \mathbb{Z}$ také, že:

$$y = ld.$$

Vynásobením oboch strán rovnice číslom n dostávame:

$$ny = nld.$$

Sčítaním oboch rovníc dostávame:

$$mx + ny = mkd + nld,$$

$$mx + ny = (mk + nl)d.$$

Keďže $(mk+nl)$ je celé číslo, rovnica ukazuje, že $mx+ny$ je násobok čísla d. Inými slovami $d \mid (mx + ny)$. ∎

Lemma 2.1.3 Nech $a \mid b$, $a, b \in \mathbb{Z}$. Potom platí: $a \mid b \Leftrightarrow a \mid -b$.

Dôkaz.

- Ak $a \mid b$, potom existuje $k \in \mathbb{Z}$ také, že:

$$b = ka. \tag{2.2}$$

  Po prenásobení 2.2 číslom -1 dostaneme $-b = -ka$ a keďže $-k \in \mathbb{Z}$, platí $a \mid -b$.

- Ak $a \mid -b$, potom existuje $k \in \mathbb{Z}$ take, že:

$$-b = ka. \tag{2.3}$$

  Po prenásobení 2.3 číslom -1 dostaneme $b = -ka$ a keďže $-k \in \mathbb{Z}$, platí $a \mid b$.

■

2.2 Spoločné delitele a spoločné násobky

Definícia 2.2.1 *(Najväčší spoločný deliteľ)*
Nech $a_1, a_2, ..., a_n \in \mathbb{Z}$. Každé $d \in \mathbb{Z}$ splňujúce podmienky:

- $d \geq 0$.
- Číslo d je spoločným deliteľom $a_1, a_2, ..., a_n$, to znamená, že $d \mid a_1, d \mid a_2, ..., d \mid a_n$.
- Ak d^* je deliteľom čísel $a_1, a_2, ..., a_n$, potom $d^* \mid d$.

nazveme najväčším spoločným deliteľom čísel $a_1, a_2, ..., a_n$. Fakt, že d je najväčším spoločným deliteľom čísel $a_1, a_2, ..., a_n$, budeme značiť $d = gcd(a_1, a_2, ..., a_n)$.

Poznámka: Na základe uvedenej definície môžeme povedať, že $gcd(a, b) = gcd(b, a)$.

Príklad: $gcd(18, 30) = 6$

- $6 \geq 0$.
- Číslo 6 je spoločným deliteľom čísel 18 a 30, pretože $6 \mid 18$ a zároveň $6 \mid 30$.
- Spoločné nezáporné delitele čísel 18 a 30 sú čísla $1, 2, 3$ a 6. $1 \mid 6$, $2 \mid 6$, $3 \mid 6$ a $6 \mid 6$. To znamená, že všetky spoločne delitele delia číslo 6.

Dokázali sme, že sú splnené všetky podmienky z Definície 2.2.1. Teda $gcd(18, 30) = 6$.

Najväčším spoločným deliteľom $a_1, a_2, ..., a_n$ nazveme teda také nezáporné číslo, ktoré je spoločným deliteľom všetkých týchto čísel a ostatné spoločné delitele týchto čísel to číslo delia.

Definícia 2.2.2 Nech $a, b \in \mathbb{Z}$. Hovoríme, že čísla a a b sú nesúdeliteľné práve vtedy, keď $gcd(a, b) = 1$.

Definícia 2.2.3 Číslo $a \in \mathbb{Z}$ je menšie alebo rovné číslu $b \in \mathbb{Z}$ práve vtedy, keď existuje $d \in \mathbb{N} \cup \{0\}$ také, že $b = a + d$. Označujeme $a \leq b$.

Lemma 2.2.4 Nech $a, b \in \mathbb{N}$. Ak $a \mid b$, potom $a \leq b$.

Dôkaz. Nech $a, b \in \mathbb{N}$. Ak $a \mid b$ podľa Definície 2.1.1 platí, že $b = ka = a + (k-1)a$, kde $k \in \mathbb{N}$. Keďže $(k-1)a \in \mathbb{N} \cup \{0\}$, môžeme označiť $(k-1)a = d$. Dostaneme $b = a + d$, čo podľa Definície 2.2.3 znamená, že $a \leq b$. ∎

Veta 2.2.5 Nech $a, b \in \mathbb{Z}$. Ak existuje najväčší spoločný deliteľ $gcd(a, b)$, potom je jediný.

Dôkaz. Predpokladajme, že $d_1 = gcd(a, b)$ a $d_2 = gcd(a, b)$.
Ak uvažujeme $a, b \neq 0$, potom $d_1, d_2 \geq 1$. Číslo d_1 je najväčším spoločným deliteľom čísel a a b. Podľa Definície 2.2.1, toto číslo musia deliť všetky spoločné delitele čísel a a b, takže aj číslo d_2. Dostávame $d_2 \mid d_1$, čo podľa Lemmy 2.2.4 znamená, že

$$d_2 \leq d_1.$$

Rovnako môžeme uvažovať aj pre číslo d_2. Číslo d_2 je podľa predpokladu najväčším spoločným deliteľom čísel a a b. Podľa Definície 2.2.1 musia toto číslo deliť všetky spoločné delitele čísel a a b, teda aj číslo d_1. Dostávame $d_1 \mid d_2$, takže podľa Lemmy 2.2.4 platí:

$$d_1 \leq d_2.$$

Spojením nerovníc $d_2 \leq d_1$ a $d_1 \leq d_2$ dostávame:

$$d_2 \leq d_1 \leq d_2,$$

čo znamená, že $d_1 = d_2$.

Ak $a \neq 0, b = 0$, potom $gcd(a, 0) = gcd(0, a) = |a|$.
Ak $a = 0, b \neq 0$, potom $gcd(0, b) = gcd(b, 0) = |b|$.
Vieme, že do množiny spoločných deliteľov čísel a a 0 určite patrí aj číslo $|a|$ a musí byť deliteľné všetkými ostatnými číslami z množiny spoločných deliteľov čísel a a 0. Všetky ostatné čísla z množiny spoločných deliteľov čísel a a 0 sú v absolútnej hodnote menšie ako $|a|$ a nerovnajú sa nule, takže môžeme povedať, že nie sú deliteľné číslom a, ktoré patrí do množiny spoločných deliteľov čísel a a 0. Môžeme teda tvrdiť, že žiadne číslo okrem čísla a nemôže byť najväčším spoločným deliteľom čísel a a 0.

Ak $a = 0$ a zároveň $b = 0$, potom $gcd(0, 0) = 0$. Množinou všetkých nezáporných spoločných deliteľov čísel 0 a 0 je množina $M = \mathbb{N} \cup \{0\}$. Všetkými číslami z množiny M je deliteľná len 0. Ktorékoľvek iné číslo z množiny M okrem nuly, nie je deliteľné väčším číslom, ako je ono samo. Takže len číslo 0 spĺňuje podmienky najväčšieho spoločného deliteľa čísel 0 a 0. ∎

Lemma 2.2.6 Nech $a, b, x, y \in \mathbb{Z}, a, b \neq 0, a = xd, b = yd, d = gcd(a, b)$. Potom $gcd(x, y) = 1$.

Dôkaz. Označme $gcd(x, y) = c$.
Keďže $c \mid x$ a zároveň $c \mid y$, existuje $r, s \in \mathbb{Z}$ také, že $x = rc$ a $y = sc$.
Nahradením do rovníc $a = xd$, $b = yd$ dostávame: $a = rcd$, $b = scd$.
Vidíme, že $cd \mid a$ a $cd \mid b$, teda cd je spoločným deliteľom čísel a, b.
Pretože d je najväčším spoločným deliteľom čísel a, b podľa Definície najväčšieho spoločného deliteľa 2.2.1 dostávame $cd \mid d$. Z Lemmy 2.2.4 plynie, že:

$$cd \leq d.$$

Podelením oboch strán nerovnice dostaneme:

$$c \leq 1.$$

Pretože $a \neq 0, b \neq 0$, potom musí platiť, že $x \neq 0, y \neq 0$. Číslo $c = gcd(x, y)$, preto je $c > 0$.
A keďže $c > 0$ a zároveň $c \leq 1$ usúdime, že $c = 1$. ∎

Definícia 2.2.7 Nech $r \in \mathbb{R}$. Celou časťou čísla r nazveme číslo $z \in \mathbb{Z}$, ktoré splňuje:

$$z \leq r < z + 1.$$

Celú časť čísla r označujeme $[r]$.

Lemma 2.2.8 Nech $a, d \in \mathbb{N}$. Potom existuje $k, z \in \mathbb{N} \cup \{0\}$ také, že $a = kd + z$, kde $0 \leq z < d$.

Dôkaz. Označme číslo k ako celú časť čísla $\frac{a}{d}$, teda $k = [\frac{a}{d}], k \in \mathbb{N} \cup \{0\}$. Podľa definície 2.2.7 musí platiť:

$$k \leq \frac{a}{d} < k + 1,$$
$$kd \leq a < kd + d,$$

$$0 \leq a - kd < d. \tag{2.4}$$

Ak označíme $z = a - kd$, potom $a = kd + z, z \in \mathbb{N} \cup \{0\}$ a podľa 2.4 platí $0 \leq z < d$. ∎

Lemma 2.2.9 Nech $a, b \in \mathbb{N}$. Potom $\exists x_0, y_0 \in \mathbb{Z} : gcd(a, b) = x_0 a + y_0 b$.

Dôkaz. Označme množinu $A = \{xa + yb \in \mathbb{N} \mid x, y \in \mathbb{Z}\}$. Do množiny A teda patria prirodzené čísla v tvare $xa + yb$. Označme

$$d = x_0 a + y_0 b \tag{2.5}$$

ako najmenší prvok množiny A. Cieľom je dokázať, že $d = gcd(a, b)$.

- Keďže d patrí do množiny $A \subseteq \mathbb{N}$, $d \geq 0$. Prvý bod z definície 2.2.1 najväčšieho spoločného deliteľa je splnený.
- Keďže $xa + yb, d \in \mathbb{N}$ podľa Lemmy 2.2.8 existujú $k, z \in \mathbb{N} \cup \{0\}$ také, že:

$$xa + yb = kd + z, 0 \leq z < d. \tag{2.6}$$

To znamená, že ktorýkoľvek prvok množiny A môžeme zapísať ako násobok čísla d plus nejaký zvyšok z. Dosadením 2.5 do 2.6 dostaneme:

$$xa + yb = kx_0a + ky_0b + z,$$

$$z = (x - kx_0)a + (y - ky_0)b.$$

Z poslednej rovnosti vyplýva, že v prípade $z > 0$, platí $z \in A$. Vieme, že $z < d$, čo by viedlo k sporu, pretože d je najmenší prvok množiny A. Usudzujeme, že $z = 0$. Keďže $z = 0$, potom $\forall xa + yb \in A : xa + yb = kd$. To ale podľa definície deliteľnosti znamená, že

$$d \mid (xa + yb).$$

Po dosadení $x = 1, y = 0$, dostaneme $d \mid (1a + 0b), (1a + 0b) \in A$, takže

$$d \mid a.$$

Po dosadení $x = 0, y = 1$, dostaneme $d \mid (0a + 1b), (0a + 1b) \in A$, takže

$$d \mid b.$$

Druhý bod z definície najväčšieho spoločného deliteľa je teda splnený.

- Ak $d^* \mid a$, potom $a = k_1d^*$. Ak $d^* \mid b$, potom $b = k_2d^*$. Po dosadení do 2.5 dostaneme:

$$d = x_0k_1d^* + y_0k_2d^*,$$

$$d = (x_0k_1 + y_0k_2)d^*.$$

Z čoho podľa Definície deliteľnosti 2.1.1 vyplýva, že $d^* \mid d$. Týmto máme splnený aj tretí bod Definície 2.2.1.

■

Lemma 2.2.10 Nech $a, b \in \mathbb{Z}$. Potom $gcd(a, b) = gcd(-a, b)$.

Dôkaz. Označme $d = gcd(a, b)$.

- $d \geq 0$.
- Ak $d \mid a$ a zároveň $d \mid b$, potom podľa Lemmy 2.1.3 $d \mid -a$ a $d \mid b$.
- Ak $d^* \mid -a$ a zároveň $d^* \mid b$, potom $d^* \mid a$ a zároveň $d^* \mid b$, takže $d^* \mid d$.

Splnené sú teda všetky podmienky najväčšieho spoločného deliteľa d čísel $-a$ a b, takže $gcd(-a, b) = d = gcd(a, b)$. ∎

Lemma 2.2.11 Nech $a, b \in \mathbb{Z}$. Potom $gcd(a, b) = gcd(a, -b)$.

Dôkaz. $gcd(a, b) = gcd(b, a)$, čo plynie priamo z definície najväčšieho spoločného deliteľa. Podľa Lemmy 2.2.10 $gcd(b, a) = gcd(-b, a)$ a $gcd(-b, a) = gcd(a, -b)$. ∎

Lemma 2.2.12 Nech $a, b \in \mathbb{Z}$. Potom $gcd(a, b) = gcd(-a, -b)$.

Dôkaz. Podľa Lemmy 2.2.10 $gcd(a, b) = gcd(-a, b)$. Z Lemmy 2.2.11 vieme, že $gcd(-a, b) = gcd(-a, -b)$. ∎

Lemma 2.2.13 Nech $a, b \in \mathbb{Z}$. Potom $gcd(a, b) = gcd(|a|, |b|)$.

Dôkaz. Okamžite plynie z Lemmy 2.2.10, 2.2.11 a Lemmy 2.2.12. ∎

Lemma 2.2.14 Nech $a, b \in \mathbb{Z}$. Potom $\exists x, y \in \mathbb{Z} : gcd(a, b) = xa + yb$.

Dôkaz. Ak $b = 0$, potom $gcd(a, b) = gcd(a, 0) = |a|$. Čiže $|a| = ka + 0b$, kde k je 1 alebo -1. Ak $a = 0$, potom $gcd(a, b) = gcd(0, b) = |b|$. Čiže $|b| = 0a + kb$, kde k je 1 alebo -1. Ak $a, b \neq 0$, potom $|a|, |b| \in \mathbb{N}$ a podľa Lemmy 2.2.9 existujú $x_0, y_0 \in \mathbb{Z}$ také, že

$$gcd(|a|, |b|) = x_0|a| + y_0|b|.$$

Existujú však $x, y \in \mathbb{Z}$ také, že $x_0|a| = xa$ a $y_0|b| = yb$. Potom platí:

$$gcd(|a|, |b|) = xa + yb.$$

Podľa Lemmy 2.2.13 platí:

$$gcd(a, b) = gcd(|a|, |b|).$$

Takže $gcd(a, b) = xa + yb$. ∎

Veta 2.2.15 *(Euklidov algoritmus)*
Nech $a, b \in \mathbb{N}, b \geq a$. Ak $b = a$, potom $gcd(a, b) = a$. Ak $b \geq a$, potom existuje $n \in \mathbb{N} \cup \{0\}$ tak, že existujú $r_{-1} = b, r_0 = a, q_j \in \mathbb{N} \cup \{0\}$, pre $j = 1, ..., n + 1$ také, že pre každé $i = -1, ..., n - 1$ platí

$$r_i = q_{i+2}r_{i+1} + r_{i+2}, 0 \leq r_{i+2} < r_{i+1},$$

$$a = r_0 > ... > r_{n+1} = 0.$$

Najväčším spoločným deliteľom čísel a a b je potom číslo r_n, posledný nenulový zvyšok, prípadne $r_n = r_0 = a$), tj. $gcd(a, b) = r_n$.

Dôkaz: Viď literatúra [1].

Poznámka: V prípade $r_n = r_0 = a$ je posledný nenulový zvyšok číslo a. Aby bol posledný nenulový zvyšok číslo a, musí platiť, že $b = aq_1 + 0$, kde $b = r_{-1}, a = r_0, 0 = r_1$. To ale znamená, že b musí byť násobkom a.

Príklad: Určte $gcd(412, 335)$ pomocou Euklidovho algoritmu.

Riešenie:

$$412 = 1.335 + 7$$

$$335 = 4.77 + 27$$

$$77 = 2.27 + 23$$

$$27 = 1.23 + 4$$

$$23 = 5.4 + 2$$

$$4 = 1.3 + \mathbf{1}$$

$$3 = 1.3 + 0,$$

posledný nenulový zvyšok je 1, takže $gcd(412, 335) = 1$.

Definícia 2.2.16 *(Najmenší spoločný násobok)*
Nech $a_1, a_2, ..., a_k \in \mathbb{Z}$. Každé $n \in \mathbb{Z}$ spĺňujúce podmienky:

- $n \geq 0$.
- Číslo n je spoločným násobkom $a_1, a_2, ..., a_k$, to znamená, že $a_1 \mid n, a_2 \mid n, ..., a_k \mid n$.
- Ak $a_1 \mid n^*, a_2 \mid n^*, ..., a_k \mid n^*$, potom $n \mid n^*$. To znamená, že n musí deliť všetky spoločné násobky čísel $a_1, a_2, ..., a_n$.

nazveme najmenším spoločným násobkom čísel $a_1, a_2, ..., a_n$. Značíme $n(a_1, a_2, ..., a_n)$.

Príklad: $n(4, 18) = 36$

- $36 \geq 0$.
- Číslo 36 je spoločným násobkom čísiel 4 a 18, pretože $4 \mid 36$ a zároveň $18 \mid 36$.
- Ak $(4 \mid n^* \wedge 18 \mid n^*) \Rightarrow (4 \mid n^* \wedge 9 \mid n^*) \Rightarrow n^* = 4 \cdot 9 \cdot k \Rightarrow 36 \mid n^*$.

Dokázali sme, že sú splnené všetky podmienky z Definície 2.2.16. Teda $n(4, 18) = 36$.

Najmenším spoločným násobkom čísel $a_1, a_2, ..., a_n$ nazveme teda také nezáporné číslo, ktoré je spoločným násobkom všetkých týchto čísel a delí všetky spoločné násobky týchto čísel.

2.3 Prvočísla a zložené čísla

Definícia 2.3.1 *(Prvočíslo)*
Prvočíslom na množine prirodzených čísel nazveme ľubovoľné číslo $p \in \mathbb{N}, p \geq 2$ práve vtedy, keď $\forall a \in \mathbb{N}$:

$$a \mid p \Leftrightarrow (a = p \vee a = 1).$$

Príklad prvočísla: $p = 17$

Definícia 2.3.2 *(Zložené číslo)*
Číslom zloženým na množine prirodzených čísel nazveme ľubovoľné číslo $n \in \mathbb{N}, n \geq 2$ také, že $\exists a, b \in \mathbb{N} \setminus \{1\}$ a platí:

$$n = ab.$$

Príklad zloženého čísla: $n = 91 = 7 \cdot 13$

Lemma 2.3.3 Číslo $n > 2$ je zložené číslo práve vtedy, keď nie je prvočíslo.

Dôkaz.

- Predpokladajme, že n je zložené číslo. Podľa Definície 2.3.2 musí existovať číslo $a, b \in \mathbb{N} \setminus \{1\}$ také, že $n = ab$. Podľa Definície 2.1.1 to znamená, že $a \mid n$. Číslo a nie je rovné 1, pretože predpokladáme, že $n = ab$ je zložené a podľa definície zloženého čísla $a, b \in \mathbb{N} \setminus \{1\}$. Číslo a taktiež nie je rovné číslu n, pretože potom by platilo, že $n = nb$. Odtiaľ ale vyplýva, že $b = 1$ a to je spor pretože $a, b \in \mathbb{N} \setminus \{1\}$. Preto n nie je prvočíslo.
- Predpokladajme, že n nie je prvočíslo. Ak nie je n prvočíslo, potom musí existovať $a \in \mathbb{N}, a \neq 1 \wedge a \neq n$ také, že $a \mid n$. Podľa Definície 2.1.1 existuje $b \in \mathbb{N}$ (pracujeme s množinou prirodzených čísel) také, že $n = ab$. Číslo b nemôže byť rovné 1, pretože potom by platilo, že $n = a \cdot 1$, čo je spor, pretože $a \neq n$. Dostaneme teda $n = ab$, kde a, b sú prirodzené čísla a zároveň $a, b \neq 1$. Podľa Definície 2.3.2 musí byť n číslom zloženým.

■

Lemma 2.3.4 Nech p, q sú prvočísla. Ak $p \mid q$, potom $p = q$.

Dôkaz. Nech $p, q \in \mathbb{N}$ sú prvočísla také, že $p \mid q$.
Keďže $p \mid q$ a p je prvočíslo, potom p je kladný deliteľ čísla q. Číslo q je prvočíslo a podľa Definície 2.3.1 jediné jeho kladné delitele sú 1 a q. Takže $p = q$ alebo $p = 1$. Číslo p je prvočíslo a podľa Definície 2.3.1 vieme, že $p \geq 2$. Môžeme teda konštatovať, že $p = q$. ■

Dokázaná lemma hovorí o tom, že dané prvočíslo delí z množiny prvočísel len samé seba.

Veta 2.3.5 *(O kanonickom rozklade)*
Nech $n > 1$ je prirodzené číslo. Potom číslo n je prvočíslo, alebo ho môžeme rozložiť na súčin prvočísel.

Dôkaz. Dôkaz vykonáme použitím silnej indukcie.
Nech $n \in \mathbb{N}, n > 1$.

- Pre $n = 2$ je tvrdenie lemmy dokázané, pretože číslo $n = 2$ je prvočíslo.
- Predpokladajme, že každé prirodzené číslo k také, že $2 \leq k < n$ je prvočíslo, alebo ho môžeme rozložiť na súčin prvočísel.
  - n je prvočíslo
    Potom je tvrdenie vety splnené.
  - n je zložené číslo
    Podľa Definície 2.3.2 existujú $a, b \in \mathbb{N}$ také, že $n = ab$, kde $1 < a < n, 1 < b < n$. Keďže a, b sú menšie ako n a väčšie ako 1, indukčný predpoklad zaručuje, že a a b sú prvočísla alebo súčiny prvočísel. Takže existujú prvočísla $p_1, p_2, ..., p_e$ a $q_1, q_2, ..., q_f$ také, že $a = p_1.p_2...p_e$ a $b = q_1.q_2...q_f$. Keďže $n = ab$, prvočíselným rozkladom čísla n je:
    $$n = p_1p_2...p_eq_1q_2...q_f.$$
    Takže číslo n môžeme rozložiť na súčin prvočísel. Z princípu silnej indukcie vyplýva, že každé číslo $n > 1$ je prvočíslo alebo súčin prvočísel.

Príklad: $36 = 2 \cdot 2 \cdot 3 \cdot 3$ ∎

Lemma 2.3.6 Nech p je prvočíslo a $n \in \mathbb{Z}$. Ak $p \nmid n$, potom $gcd(p, n) = 1$.

Dôkaz. Označme $gcd(p, n) = d$.
Z Definície 2.2.1 vieme, že $d \mid p$ a zároveň $d \mid n$.
Z Definície 2.3.1 vieme, že prvočíslo môže byť deliteľné len jednotkou alebo sebou samým: $d = p$ alebo $d = 1$.
Ak $d = p$, potom $p \mid n$. Tu nastáva spor, pretože $p \nmid n$. Z toho vyplýva, že $d = 1$. ∎

Lemma 2.3.7 Nech $k, a, b \in \mathbb{Z}$. Potom platí:

$$(gcd(k, a) = 1 \wedge k \mid ab) \Rightarrow k \mid b.$$

Dôkaz. Z Lemmy 2.2.14 plynie, že $gcd(k, a) = xk + ya = 1$, kde $x, y \in \mathbb{Z}$. Po prenásobení číslom b dostaneme rovnosť

$$xkb + yab = b. \tag{2.7}$$

Ak predpokladáme, že $k \mid ab$, z Definície 2.1.1 plynie, že $ab = k_1k, k_1 \in \mathbb{Z}$. Dosadením do rovnosti 2.7 dostaneme

$$xkb + yk_1k = b,$$

$$k(xb + yk_1) = b.$$

Čo podľa definície deliteľnosti znamená, že $k \mid b$. ∎

Lemma 2.3.8 Nech p je prvočíslo, $s \in \mathbb{N}$. Ak $p \mid (a_1...a_s)$, potom p delí aspoň jedno z čísel $a_1, ..., a_s$, tj.$p \mid a_1 \vee ... \vee p \mid a_s$

Dôkaz. Na vykonanie dôkazu použijeme matematickú indukciu.

- V prípade, že $s = 1$ veta platí.
- Indukčný predpoklad: Ak $p \mid (a_1...a_n)$, potom p delí aspoň jedno z čísel $a_1, ..., a_n$. Úlohou je dokázať, že ak $p \mid (a_1...a_n a_{n+1})$, potom p delí aspoň jedno z čísel $a_1, ..., a_n, a_{n+1}$. Ak $p \mid (a_1...a_n a_{n+1})$ môžu však nastať dve možnosti:
  - $p \mid a_{n+1}$, to však znamená, že p je deliteľom aspoň jedného z čísel $a_1, ..., a_n, a_{n+1}$.
  - Ak $p \nmid a_{n+1}$, potom podľa Lemmy 2.3.6 $gcd(p, a_{n+1}) = 1$. Ak $p \mid (a_1...a_n a_{n+1})$ a zároveň $gcd(p, a_{n+1}) = 1$, potom z Lemmy 2.3.7 plynie, že $p \mid (a_1...a_n)$. Z indukčného predpokladu teda p delí aspoň jedno z čísel $a_1, ..., a_n$.

  Dokázali sme, že buď $p \mid a_{n+1}$ alebo p delí aspoň jedno z čísel $a_1, ..., a_n$. To ale znamená, že p delí aspoň jedno z čísel $a_1, ..., a_n, a_{n+1}$.

■

Veta 2.3.9 *(O jednoznačnosti kanonického rozkladu - Základná veta aritmetiky)*
Pre každé $n \in \mathbb{N}, n \neq 1$ existuje až na poradie činiteľov práve jeden kanonický rozklad na súčin prvočísel. To znamená, že pokiaľ $p_1, p_2, ...p_r, q_1, q_2, ..., q_s$ sú prvočísla a platí:

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_s,$$

potom $r = s$ a pre každé $i \in \{1, ..., r\}$ existuje $j \in \{1, ..., s\}$ také, že $p_i = q_j$.

Dôkaz. Predpokladáme, že $n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$. Z tejto rovnosti dostávame, že $p_1 \mid q_1 q_2 ... q_s$. Podľa Lemmy 2.3.8 je p_1 deliteľom aspoň jedného z čísel $q_1, ..., q_s$. To znamená, že existuje $q_j \in \{q_1, ..., q_s\}$ také, že $p_1 \mid q_j$. Podľa Lemmy 2.3.4 to znamená, že $p_1 = q_j$. Pokiaľ vhodne preindexujeme čísla $q_1, ..., q_s$ dostávame:

$$p_1 p_2 ... p_r = p_1 q_2 ... q_s,$$

$$p_2 ... p_r = q_2 ... q_s.$$

Pokiaľ tento postup zopakujeme $r-$krát, zistíme, že pre každé $i \in \{1, ..., r\}$ existuje $j \in \{1, ..., s\}$ také, že $p_i = q_j$. Nakoniec dostávame rovnosť:

$$1 = q_{s-r} ... q_s,$$

z čoho plynie, že $r = s$. ■

2.4 Vlastnosti množiny prvočísel

Veta 2.4.1 *(Euklidova prvočíselná)*
Prvočísel je nekonečne mnoho.

Dôkaz. Sporom. Predpokladajme, že existuje konečne mnoho prvočísel. Predpokladajme, že

$$p_1, p_2, p_3, ..., p_n \tag{2.8}$$

je kompletný zoznam prvočísel. Nech B je súčin všetkých prvočísel v zozname (2.8):

$$B = p_1 p_2 ... p_n.$$

Uvažujme číslo $B+1$. Z Vety 2.3.5 vieme, že číslo $B+1$ môžeme rozložiť na súčin prvočísel. Nech q je nejaké prvočíslo, ktoré sa vyskytuje v prvočíselnom rozklade čísla $B+1$.

- *Tvrdenie:* Prvočíslo q sa nerovná žiadnemu z prvočísel v zozname (2.8).
- *Dôkaz:* Sporom.
  Predpokladajme, že q sa rovná jednému z prvočísel v zozname (2.8). To znamená, že existuje $k \in \{1, ..., n\} : q = p_k$. Keďže p_k sa vyskytuje v prvočíselnom rozklade B, platí:
  $$q \mid B.$$
  Keďže q sa vyskytuje v prvočíselnom rozklade čísla $B+1$ platí:
  $$q \mid B + 1.$$
  Z Lemmy 2.1.2 plynie, že:
  $$q \mid B + 1 - B.$$
  Zjednodušením dostávame:
  $$q \mid 1.$$
  Žiadne prvočíslo nedelí číslo 1. Keďže sme dosiahli spor, predpoklad, že q je rovné jednému z prvočísel v zozname (2.8) nie je pravdivý. Dokázali sme, že prvočíslo q nie je rovné žiadnemu prvočíslu v zozname (2.8).

Zoznam (2.8) považujeme za kompletný zoznam prvočísel a máme dokázané, že prvočíslo q sa v tomto zozname nevyskytuje, čo je spor. Náš počiatočný predpoklad, že prvočísel existuje konečne mnoho, je nepravdivý. Z toho usudzujeme, že prvočísel je nekonečne mnoho. ∎

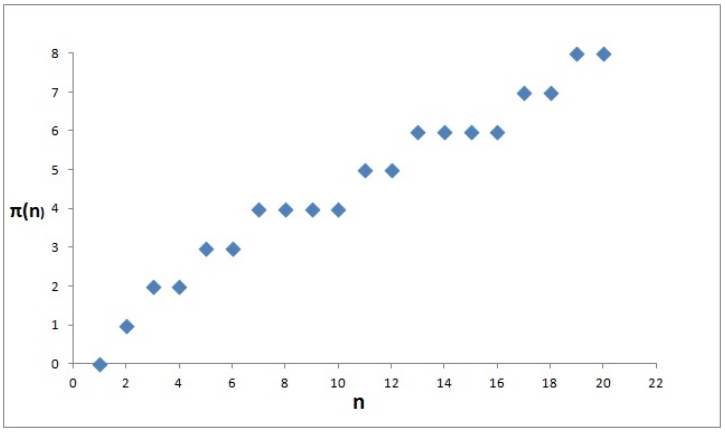
Veta 2.4.2 Nech $\{p_i\}_{i=1}^{\infty}$, je postupnosť všetkých prvočísel. Potom platí:

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

Dôkaz: Viď literatúra [3].

Veta 2.4.2 hovorí o tom, že nekonečný rad prevrátených hodnôt všetkých prvočísel diverguje.

Definícia 2.4.3 Nech $n \in \mathbb{N}$. Hodnotu $\pi(n)$ definujeme ako počet prvočísel, ktoré sú menšie alebo rovné n.



Obr. 2.1: Graf $\pi(n)$ pre malé hodnoty n

Hodnota $\pi(n)$ sa zvyšuje o 1 zakaždým, keď sa vyskytne nové prvočíslo. Napríklad $\pi(7) = \pi(8) = \pi(9) = \pi(10) = 4$. Ale $\pi(11) = 5$, pretože 5 je prvočíslo a počet prvočísel, ktoré sú rovné alebo menšie ako 11, je o 1 väčší ako počet prvočísel menších alebo rovných 10.

Veta 2.4.4 *(Prvočíselná)*

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

Dôkaz: Viď literatúra [3].

Prvočíselná veta popisuje chovanie funkcie $\pi(n)$ pre $n \to \infty$. Pomocou nej môžeme odhadnúť $\pi(n)$. Počet prvočísel nepresahujúcich $n \in \mathbb{R}$ môžeme porovnať s číslom $\frac{n}{\ln n}$.

3 Kongruencie

3.1 Kongruencia modulo m

Definícia 3.1.1 *(Kongruencia na $\mathbb{Z}$)*
Nech $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$. Číslo a sa nazýva kongruentné s číslom b modulo m, práve vtedy, keď $m \mid (a - b)$, to znamená, že existuje $k \in \mathbb{Z}$ také, že $(a - b) = km$. Označujeme: $a \equiv b \pmod{m}$.

Príklad: Platí: $34 \equiv 54 \pmod{10}$?

Riešenie: Podľa Definície 3.1.1 musí platiť $10 \mid (54 - 34)$, teda $10 \mid 20$. Keďže $20 = 2.10$ a $2 \in \mathbb{Z}$, môžeme povedať, že 34 je kongruentné s 54 modulo 10.

Veta 3.1.2 Relácia kongruencie je relácia ekvivalencie na $\mathbb{Z}$. To znamená: $\forall a, b, c \in \mathbb{Z}, m \in \mathbb{N}$ platí:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
- $(a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$

Dôkaz.

- $a - a = 0 = 0m$, takže $a \equiv a \pmod{m}$.
- Ak $a \equiv b \pmod{m}$, potom
$$a - b = km,$$
$k \in \mathbb{Z}$. Po prenásobení rovnice číslom -1 dostávame
$$b - a = -km,$$
$-k \in \mathbb{Z}$. To znamená, že $b \equiv a \pmod{m}$.
- Ak $a \equiv b \pmod{m}$, potom
$$a - b = k_1 m, \tag{3.1}$$
$k_1 \in \mathbb{Z}$. Ak $b \equiv c \pmod{m}$, potom
$$b - c = k_2 m, \tag{3.2}$$
$k_2 \in \mathbb{Z}$. Sčítaním rovníc 3.1 a 3.2 dostávame
$$a - c = (k_1 + k_2)m,$$
$(k_1 + k_2) \in \mathbb{Z}$. To znamená, že $a \equiv c \pmod{m}$.

■

Definícia 3.1.3 Nech $a, r \in \mathbb{Z}, m \in \mathbb{N}$. Redukovať číslo a modulo m znamená nájsť číslo $r \in \{0, 1, ..., m-1\}$ tak, že $a = qm + r, q \in \mathbb{Z}$. Tomuto číslu budeme hovoriť redukcia čísla a modulo m.

Príklad: Redukujte 41 modulo 15.

Riešenie: Keď podelíme číslo 41 číslom 15 dostávame $41 = 2 \cdot 15 + 11$. Takže 11 je redukciou 41 modulo 15.

Lemma 3.1.4 Nech $a \in \mathbb{Z}, m \in \mathbb{N}$. Ak r je redukciou a modulo m, potom platí:

$$a \equiv r \pmod{m}.$$

Dôkaz. Nech $a \in \mathbb{Z}, m \in \mathbb{N}$. Ak r je redukciou a modulo m, potom podľa Definície 3.1.3 $a = qm + r, q \in \mathbb{Z}$, z čoho $a - r = qm, q \in \mathbb{Z}$. Čo podľa definície kongruencie znamená, že $a \equiv r \pmod{m}$. ∎

Definícia 3.1.5 *(Zvyšková trieda)*
Nech $m \in \mathbb{N}$ a $r \in \mathbb{Z}$. Potom zvyšková trieda r modulo m je množina $\bar{r}_m$ všetkých celých čísel kongruentných s číslom r modulo m, tj.

$$\bar{r}_m = \{x \in \mathbb{Z} | x \equiv r \pmod{m}\}.$$

Lemma 3.1.6 Nech $r \in \mathbb{Z}$ a $m \in \mathbb{N}$. Potom platí:

$$\bar{r}_m = \{x \in \mathbb{Z} | x \equiv r \pmod{m}\} = \{km + r | k \in \mathbb{Z}\}.$$

Dôkaz. Dôkaz vyplýva z Definície kongruencie 3.1.1. Vieme, že $x \equiv r \pmod{m}$ práve vtedy, keď $x - r = km$, čiže $x = km + r$. Môžeme usudzovať, že $\{x \in \mathbb{Z} | x \equiv r \pmod{m}\} = \{km + r | k \in \mathbb{Z}\}$. ∎

Definícia 3.1.7 Nech $n \in \mathbb{N}$. Množinu $\mathbb{Z}_n$ definujeme ako

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\},$$

kde $\bar{a}$ je definovaná pre všetky $a \in \mathbb{Z}$ ako zvyšková trieda modulo n:

$$\overline{a} = \{a + kn | k \in \mathbb{Z}\}.$$

3.2 Aritmetické operácie s kongruenciami

Veta 3.2.1 Ak $a \equiv b \pmod{m}$ a zároveň $c \equiv d \pmod{m}$, potom platí:

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

- $ac \equiv bd \pmod{m}$

Dôkaz.

- Ak predpokladáme, že $a \equiv b \pmod{m}$, podľa definície kongruencie platí, že

$$a - b = k_1 m. \tag{3.3}$$

  Ak predpokladáme, že $c \equiv d \pmod{m}$, potom platí:

$$c - d = k_2 m. \tag{3.4}$$

  pričom $k_1, k_2 \in \mathbb{Z}$. Sčítaním rovníc 3.3 a 3.4 dostávame:

$$(a + c) - (b + d) = (k_1 + k_2)m,$$

  kde $k_1 + k_2 \in \mathbb{Z}$. To znamená, že $a + c \equiv b + d \pmod{m}$.

- Odčítanim rovníc 3.3 a 3.4 dostaneme:

$$(a - c) - (b - d) = (k_1 - k_2)m,$$

  kde $k_1 - k_2 \in \mathbb{Z}$. To znamená, že $a - c \equiv b - d \pmod{m}$.

- Vynásobením rovníc 3.3 a 3.4 dostaneme $ac = (b + k_1 m)(d + k_2 m)$. Po roznásobení dostaneme rovnosť:

$$ac - bd = km,$$

  $k \in \mathbb{Z}$. To však znamená, že $ac \equiv bd \pmod{m}$.

■

Veta 3.2.2 Nech $a \equiv b \pmod{m}$, $c \in \mathbb{Z}$. Potom platí:

$$ac \equiv bc \pmod{m}.$$

Dôkaz. Predpokladajme, že $a \equiv b \pmod{m}$. Z Definície 3.1.1 plynie, že $a - b = km$, kde $k \in \mathbb{Z}$. Prenásobením rovnice číslom c dostaneme rovnosť $ac - bc = ckm, ck \in \mathbb{Z}$, z čoho plynie, že $ac \equiv bc \pmod{m}$. ■

Veta 3.2.3 Nech $ac \equiv bc \pmod{m}$ a $gcd(m, c) = 1$. Potom platí:

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

Dôkaz. Predpokladáme, že $ac \equiv bc \pmod{m}$. Z definície kongruencie platí, že $ac - bc = km$. Po úprave dostaneme $c(a - b) = km$, z čoho plynie:

$$m \mid (a - b)c.$$

Keďže predpokladáme, že $gcd(m, c) = 1$ podľa Lemmy 2.3.7 plynie, že $m \mid (a - b)$. Čo podľa definície kongruencie znamená, že $a \equiv b \pmod{m}$. ■

4 Fermatova-Eulerova veta

4.1 Odvodenie a popis

Definícia 4.1.1 *(Eulerova funkcia)*
Funkcia φ priraďuje číslu m počet prirodzených čísel menších alebo rovných m takých, ktoré sú s m nesúdeliteľné. Túto funkciu nazývame *Eulerova funkcia*.

Definícia 4.1.2 *(Redukovaný zvyškový systém)*
Redukovaný zvyškový systém modulo m je systém množín

$$R_m = \{\overline{r}_m | r \in \mathbb{Z}, gcd(r, m) = 1\}.$$

Lemma 4.1.3 Nech $gcd(a, n) = gcd(b, n) = 1$. Potom $gcd(ab, n) = 1$.

Dôkaz. Ak $gcd(a, n) = 1$, potom podľa Lemmy 2.2.9 existuje $x_0, y_0 \in \mathbb{Z}$ také, že

$$ax_0 + ny_0 = 1. \tag{4.1}$$

Ak $gcd(b, n) = 1$, potom existuje $x_1, y_1 \in \mathbb{Z}$ také, že

$$bx_1 + ny_1 = 1. \tag{4.2}$$

Vynásobením rovností 4.1 a 4.2 dostaneme

$$abx_0x_1 + n(ax_0y_1 + y_0bx_1 + ny_0y_1) = 1.$$

Ak označíme $x = x_1x_0$ a $y = ax_0y_1 + y_0bx_1 + ny_0y_1$ dostaneme rovnosť:

$$abx + ny = 1. \tag{4.3}$$

Označme $gcd(ab, n) = d$. Podľa Definície 2.2.1 vieme, že $ab = dk_1$ a $n = dk_2$, kde $k_1, k_2 \in \mathbb{Z}$. Dosadením do rovnosti 4.3 dostaneme:

$$dk_1x + dk_2y = 1,$$

$$d(k_1x + k_2y) = 1.$$

Z čoho vyplýva, že $d \mid 1$, takže $d = 1$. Máme teda dokázané, že $gcd(ab, n) = 1$. ∎

Poznámka: Z Lemmy 4.1.3 plynie, že ak $\overline{r_1}_m$ a $\overline{r_2}_m$ sú také zvyškové triedy, ktoré patria do redukovaného zvyškového systému modulo m, potom aj zvyšková trieda $\overline{r_1r_2}_m$ patrí do redukovaného zvyškového systému modulo m.

Veta 4.1.4 *(Fermatova-Eulerova)*:
Nech $gcd(a, m) = 1$. Potom

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

Dôkaz. Označme zvyškové triedy patriace do redukovaného zvyškového systému modulo m ako $R_m = \{\overline{r_1}, \overline{r_2}, \overline{r_3}, ..., \overline{r_{\varphi(m)}}\}$, kde $1 \leq r_j \leq m, j \in \{1, 2, .., \varphi(m)\}$.
Z predpokladu vieme, že $gcd(a, m) = 1$ a podľa Definície 4.1.2 aj $gcd(r_j, m) = 1$, pre všetky $j \in \{1, 2, .., \varphi(m)\}$. Podľa Lemmy 4.1.3 je potom aj číslo $gcd(ar_j, m) = 1$.
Na základe toho môžeme povedať, že $\overline{ar_j}$ je jednou zo zvyškových tried v redukovanom zvyškovom systéme R_m. Označme ju napríklad $\overline{z_j}$, kde $1 \leq z_j \leq m, j \in \{1, 2, ..., \varphi(m)\}$. Dostaneme tak sústavu kongruencií:

$$\begin{aligned} ar_1 &\equiv z_1 \pmod m \\ ar_2 &\equiv z_2 \pmod m \\ &\vdots \\ ar_{\varphi(m)} &\equiv z_{\varphi(m)} \pmod m \end{aligned}$$

Po vynásobení týchto kongruencií dostaneme:

$$a^{\varphi(m)} r_1 r_2 ... r_{\varphi(m)} \equiv z_1 z_2 ... z_{\varphi(m)} \pmod m. \tag{4.4}$$

Čísla $z_1, z_2, .., z_{\varphi(m)}$ sú navzájom rôzne, pretože zo vzťahu $z_1 \equiv z_j \pmod m$ dostaneme $ar_i \equiv ar_j \pmod m$, čiže

$$r_i \equiv r_j \pmod m.$$

Ak $r_i \neq r_j$, potom $z_i \neq z_j$, preto každé z čísel r_i je rovné niektorému z čísel $z_i, i \in \{1, 2, ..., \varphi(m)\}$. A tak

$$r_1 r_2 .. r_{\varphi(m)} \equiv z_1 z_2 ... z_{\varphi(m)} \pmod m.$$

Dosadením do 4.4 dostaneme

$$a^{\varphi(m)} r_1 r_2 .. r_{\varphi(m)} \equiv r_1 r_2 .. r_{\varphi(m)} \pmod m. \tag{4.5}$$

Keďže $gcd(r_i, m) = 1, i \in \{1, 2, ..., \varphi(m)\}$, potom aj $gcd(r_1 r_2 ... r_{\varphi(m)}, m) = 1$, a preto môžeme kongruenciu 4.5 deliť číslom $r_1 r_2 ... r_{\varphi(m)}$. Dostaneme:

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

■

Veta 4.1.5 *(Malá Fermatova)*:
Nech $gcd(a, p) = 1$ a p je prvočíslo. Potom

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

Dôkaz. Podľa Vety 4.1.4 vieme, že ak $gcd(a, p) = 1$, potom musí platiť $a^{\varphi(p)} \equiv 1 \pmod p$. Vieme, že $\varphi(p)$ je počet čísel z množiny $\{1, 2, ..., p\}$ takých, ktoré sú s p nesúdeliteľné. Keďže p je prvočíslo, počet čísel z množiny $\{1, 2, ..., p\}$ nesúdeliteľných s p je $p - 1$, takže $\varphi(p) = p - 1$. Dostaneme teda

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

■

5 Eratosthenovo sito

5.1 Popis

Lemma 5.1.1 Ak $n = n_1 n_2$, kde $n, n_1, n_2 \in \mathbb{N}$, potom $n_1 \leq \sqrt{n}$ alebo $n_2 \leq \sqrt{n}$.

Dôkaz. Dôkaz vykonáme sporom. Budeme predpokladať, že $n = n_1 n_2$, $n_1 > \sqrt{n}$ a zároveň $n_2 > \sqrt{n}$. Potom bude platiť:

$$n = n_1 n_2 > \sqrt{n}\sqrt{n} = n,$$

kde nastáva spor, pretože neplatí, že $n > n$. Nás predpoklad je teda nepravdivý. A keďže číslo n môžeme určite zapísať v tvare $n = n_1 n_2$, potom musí byť nepravdivý predpoklad, že $n_1 > \sqrt{n}$ a zároveň $n_2 > \sqrt{n}$. Musí platiť, že $n_1 \leq \sqrt{n}$ alebo $n_2 \leq \sqrt{n}$. ∎

Lemma 5.1.2 Nech $n \in \mathbb{N}$ je zložené číslo. Potom existuje prvočíslo $p, p \leq \sqrt{n}$, ktoré je deliteľom čísla n.

Dôkaz. Dôkaz vykonáme sporom. Budeme predpokladať, že číslo n má kanonický rozklad

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n},$$

kde $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{N}$ a zároveň všetky prvočísla v tomto kanonickom rozklade sú väčšie ako $\sqrt{n}$. Môžu nastať dve možnosti:

- $n > 1$, to znamená, že existujú aspoň dva rôzne prvočísla p_1, p_2, ktoré delia číslo n. Potom platí:
$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n} \geq p_1 p_2 > \sqrt{n}\sqrt{n} = n.$$
To je ale spor, pretože neplatí, že $n > n$. Musí teda byť nepravdivý predpoklad.

- $n = 1$, to znamená, že existuje len jedno prvočíslo, ktoré delí číslo n. Potom $n = p_1^{\alpha_1}$, a aby n bolo číslo zložené, musí byť $\alpha_1 \geq 2$. Potom platí:
$$n = p_1^{\alpha_1} \geq p_1^2 > (\sqrt{n})^2 = n.$$
To je spor, pretože neplatí $n > n$. V tomto prípade musí byť tiež nepravdivý predpoklad.

Dokázali sme, že predpoklad, že všetky prvočísla v kanonickom rozklade čísla n sú väčšie ako $\sqrt{n}$, je nepravdivý. Potom ale musí platiť, že aspoň jedno prvočíslo v kanonickom rozklade čísla n je menšie alebo rovné ako $\sqrt{n}$. ∎

Poznámka: Dokázaná lemma nám hovorí o tom, že každé zložené číslo n je násobkom nejakého prvočísla p, ktoré je menšie alebo rovné $\sqrt{n}$.

Na základe dokázanej Lemmy 5.1.2 môžeme povedať, že ak zo zoradeného zoznamu čísel od 2 do n odstránime všetky násobky všetkých takých prvočísel, ktoré sú menšie

alebo rovné ako $\sqrt{n}$ (samotné prvočíslo neodstránime), odstránime tým zo zoznamu vlastne všetky zložené čísla.

Eratosthenovo sito je algoritmus, ktorý hľadá prvočísla menšie ako dané číslo n. Na začiatku máme zoradený zoznam čísel od 2 (keďže 1 sa nepokladá za prvočíslo, preto začíname dvojkou) do n a zoznam prvočísel, ktorý je na začiatku prázdny. V zozname čísel je teda prvým prvkom číslo 2. Dvojku pridáme do zoznamu prvočísel a zo zoznamu čísel odstránime všetky násobky dvojky. Následne ďalším prvkom v zozname čísel bude číslo 3, pridáme ho teda do zoznamu prvočísel a zo zoznamu čísel odstránime všetky násobky trojky. Takto pokračujeme až dovtedy, kým prvý prvok v zozname čísel je menší alebo rovný ako $\sqrt{n}$. Zjednotením čísel, ktoré sa nachádzajú v zozname prvočísel a čísel, ktoré zostali v pôvodnom zozname čísel(neboli vyškrtnuté), dostaneme všetky prvočísla menšie alebo rovné n.

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

Obr. 5.1: Eratosthenovo sito - Číslo 2 je prvočíslo a jeho násobky odstránené.

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

Obr. 5.2: Eratosthenovo sito - Číslo 3 je prvočíslo a jeho násobky odstránené.

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

Obr. 5.3: Eratosthenovo sito - Číslo 5 je prvočíslo a jeho násobky odstránené.

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

Obr. 5.4: Eratosthenovo sito - Číslo 7 je prvočíslo a jeho násobky odstránené.

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

Obr. 5.5: Eratosthenovo sito - Prvočísla menšie ako 100

5.2 Algoritmus

Algoritmus v Maple:

```
> eratosthenovosito:=proc(n)    local  zoznam, zoznamprvocisel;

> zoznam:={seq(i, i = 2 ..  n)};
> zoznamprvocisel:={};

> while (evalf(zoznam[1]) <  evalf(sqrt(n)))   do
>         zoznamprvocisel:={op(zoznamprvocisel), zoznam[1]};
>         zoznam:=select(x->irem(x,zoznam[1]) <> 0, zoznam);
> od;

> zoznamprvocisel:=zoznam union zoznamprvocisel;

> end;
```

Výpis 5.1: Eratosthenovo sito algoritmus v Maple

Algoritmus v Matlabe:

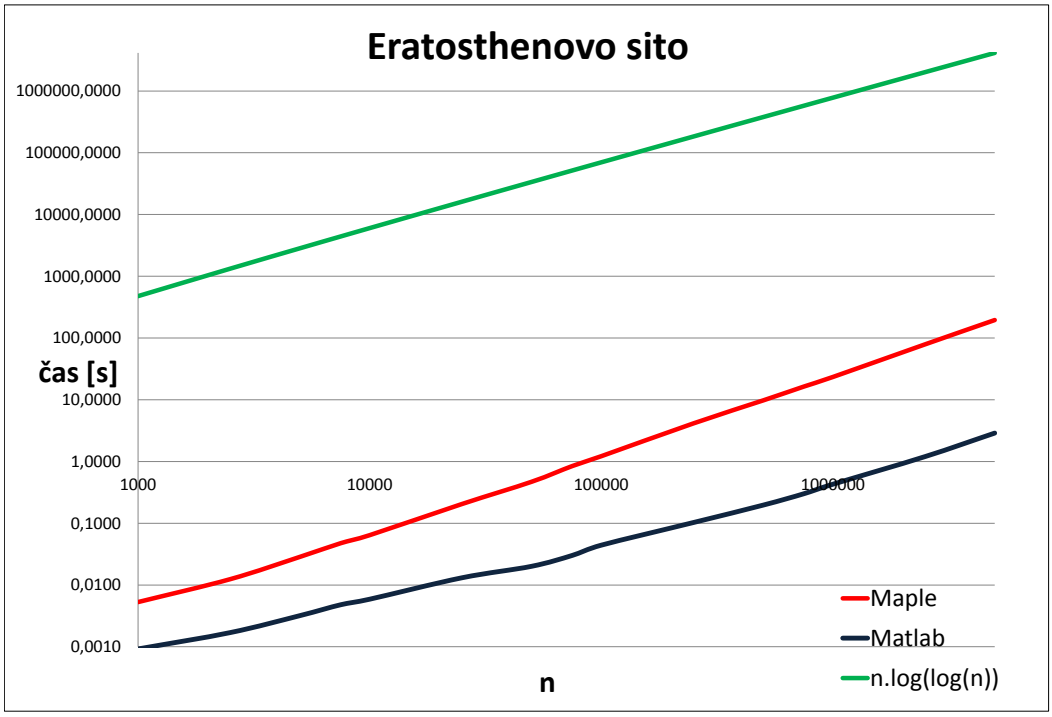
```
function zoznamprvocisel = eratosthenovo_sito(n)

zoznam=[2:1:n];
zoznamprvocisel=[];

while (zoznam(1) < sqrt(n))
    zoznamprvocisel=[zoznamprvocisel zoznam(1)];
    zoznam(mod(zoznam,zoznam(1))==0)=[];
end

zoznamprvocisel=[zoznamprvocisel zoznam];

end
```

Výpis 5.2: Eratosthenovo sito algoritmus v Matlabe

Eratosthenovo sito je algoritmus, ktorý je použiteľný len pri relatívne malých konečných číslach. Pri číslach rádov tisícok a viac je algoritmus náročný a ručne nepoužiteľný.

Časová zložitosť algoritmu je $O(n\log(\log(n))$, kde n je najväčšie číslo z intervalu, na ktorom prvočísla hľadáme.

Algoritmus sme testovali pre n v intervale $(1000, 5000000)$. V grafe 5.6 sú časy výpočtu aritmetickým priemerom $100-$tých nameraných hodnôt. Hodnoty n sú v logaritmickom merítku. Testovanie prebehlo cez vzdialené pripojenie k sieti VŠB.



n:	1000	2500	5000	7500	10000	25000	50000	75000	100000	250000	500000	750000	1000000	2500000	5000000
Maple:	0,00528	0,0124	0,02849	0,04744	0,06396	0,20404	0,46828	0,84256	1,21528	4,1318	9,7328	16,32037	23,30308	78,66512	194,8252
Matlab:	0,000924	0,0017	0,0032	0,0048	0,0059	0,0131	0,0201	0,0302	0,0442	0,1028	0,1967	0,3008	0,4285	1,1995	2,8831

Obr. 5.6: Graf rýchlosti algoritmu Eratosthenovho sita

6 Fermatov test prvočíselnosti

6.1 Popis

Fermatov test prvočíselnosti plynie z Malej Fermatovej Vety 4.1.5. Malá Fermatova Veta hovorí o tom, že ak vyberieme nejaké $a \in \{1, 2, ..., n-1\}$, potom ak je n prvočíslo, musí platiť:

$$a^{n-1} \equiv 1 \pmod{n}.$$

Príklad: $n = 5$
$1^{5-1} \equiv 1 \pmod{5}$
$2^{5-1} = 16 \equiv 1 \pmod{5}$
$3^{5-1} = 81 \equiv 1 \pmod{5}$
$4^{5-1} = 256 \equiv 1 \pmod{5}$
Vieme, že $n = 5$ je prvočíslo, a skutočne pre všetky $a \in \{1, 2, 3, 4\}$ je kongruencia $a^{5-1} \equiv 1 \pmod{5}$ splnená.
Obmenou Malej Fermatovej Vety dostaneme vetu:

Veta 6.1.1 Ak existuje $a \in \{1, 2, ..., n-1\}$ také, že

$$a^{n-1} \not\equiv 1 \pmod{n},$$

potom n nie je prvočíslo, teda je číslom zloženým.

Poznámka: Takému číslu $a \in \{1, 2, ..., n-1\}$ pre ktoré platí $a^{n-1} \not\equiv 1 \pmod{n}$, hovoríme *Fermatov svedok zloženosti čísla* n.

Fermatov test prvočíselnosti daného čísla n spočíva v dvoch krokoch:

- Náhodne vyberieme nejaké číslo a tak, že $1 < a < n$.
- Testujeme či je splnená kongruencia

$$a^{n-1} \equiv 1 \pmod{n}. \tag{6.1}$$

  Môžu teda nastať dve možnosti:

  - Kongruencia 6.1 je splnená. V takomto prípade číslo n môže, ale nemusí byť prvočíslo. Zvolíme iné číslo a, pre ktoré testujeme kongruenciu 6.1 znova.
  - Kongruencia 6.1 nie je splnená. V takomto prípade číslo n určite nie je prvočíslo. Číslo a bude Fermatovým svedkom zloženosti čísla n.

Príklad: Otestujeme, či číslo $n = 15$ môže byť prvočíslo alebo nie. Vyberieme nejaké $a \in \{2, ..., 14\}$ a testujeme či je splnená kongruencia 6.1. Pri voľbe napríklad $a = 2$ dostaneme:

$$2^{14} = 2^{3.4+2} = (2^4)^3.2^2 \equiv 4 \pmod{15}.$$

Kongruencia 6.1 teda nie je splnená. Čo znamená, že číslo 15 nie je prvočíslo, čiže je to číslo zložené. Fermatovým svedkom zloženosti čísla 15 bude napríklad číslo 2.

Definícia 6.1.2 *(Carmichaelovo číslo)*:
Zložené číslo n nazveme Carmichaelovo číslo práve vtedy, keď $\forall a \in \mathbb{Z}$ také, že $gcd(a, n) = 1$ platí

$$a^{n-1} \equiv 1 \pmod{n}.$$

To znamená, že Carmichaelovo číslo je zložené číslo, ktorého jedinými Fermatovými svedkami zloženosti sú čísla s ním súdeliteľné.

Poznámka: Pre Carmichaelove čísla nie je Fermatov test veľmi použiteľný. Fermatov test funguje dobre pre čísla, ktoré nie sú súčinom navzájom rozných prvočísel.

Poznámka: Carmichaelových čísel je nekonečne mnoho. Najmenšie Carmichaelovo číslo je číslo 561.

Veta 6.1.3 *(Korseltovo kritérium)*:
Nech n je zložené číslo. Potom n je Carmichaelovo číslo práve vtedy, keď platia nasledujúce podmienky:

- Pre všetky prvočísla také, že $p \mid n$ platí $(p-1) \mid (n-1)$
- n je súčinom navzájom rôznych prvočísel

Dôkaz: Viď literatúra [2].

Príklad: Číslo 561 je Carmichaelovo číslo, pretože sú splnené podmienky Vety 6.1.3:

- $561 = 3 \cdot 11 \cdot 17$, čiže je súčinom navzájom rôznych prvočísel
- $2 \mid 560$, $10 \mid 560$, $16 \mid 560$, čiže pre všetky prvočísla, ktoré delia číslo n, platí, že $(p-1) \mid (n-1)$

Veta 6.1.4 Nech $n \in \mathbb{N}$ a p je nepárne prvočíslo také, že $p^2 \mid n$. Potom počet prirodzených čísel a, kde $1 \leq a \leq (n-1)$, ktoré spĺňajú kongruenciu

$$a^{n-1} \equiv 1 \pmod{n}.$$

je najviac $\frac{1}{4}(n-1)$.

Dôkaz: Viď literatúra [2].

Poznámka: Táto veta hovorí o tom, že ak testujeme číslo n, ktoré nie je súčinom navzájom rôznych prvočísel (existuje nepárne prvočíslo p také, že $p^2 \mid n$), potom s pravdepodobnosťou najmenej 75% vyberieme medzi číslami $1, 2, ..., n-1$ také číslo, ktoré bude Fermatovým svedkom zloženosti čísla n.

6.2 Algoritmus

Algoritmus má vstupný parameter číslo n, ktorého prvočíselnosť testujeme a číslo $poceta$, ktoré udáva koľko maximálne náhodných čísel a má algoritmus vygenerovať. Algoritmus vygeneruje nejaké náhodné číslo a z intervalu $\langle 2, (n-1)\rangle$ a následne testuje či je splnená kongruencia 6.1. Pokiaľ kongruencia splnená nie je, algoritmus sa ukončí s výsledkom, že zadané číslo n je zložené. Ak kongruencia 6.1 je splnená, algoritmus vygeneruje iné číslo a, pre ktoré otestuje kongruenciu znova. Ak nájde nejaké a, pre ktoré kongruencia nie je splnená, algoritmus je ukončený, pretože našiel Fermatovho svedka zloženosti, takže číslo n je zložené. Ak pre všetky náhodne vygenerované čísla a (čísla sa neopakujú, maximálny počet náhodne vygenerovaných čísel je $poceta$) je kongruencia 6.1 splnená, algoritmus je ukončený s výsledkom, že testované číslo n môže, ale nemusí byť prvočíslo.

Algoritmus v Maple:

```
> fermat := proc (n,pocata) local  a,  zoznam, i;
> zoznam := [];
> i  :=  0;
> while (i<poceta) do
>    a  :=  generuj(n,zoznam);
>    if  (umocnimodulo(a,(n−1),n) <> 1) then
>       print(n  'je zlozene cislo' ) ;
>       print(a  'je Fermatovym svedkom zlozenosti zadaneho cisla');
>    return;
>    fi ;
>    zoznam:=[op(zoznam),a];
>    i  :=  i+1;
> do;
> print(n  'moze ale nemusi byt prvocislo');
> end;

> generuj := proc(n,zoznam) local cislo ,  velkostmnoziny, a,  i ;
> cislo  :=  rand(2..n−1);
> a :=  cislo () ;
> velkostmnoziny := nops(zoznam);
> if  (velkostmnoziny <> 0) then
>    for  i  from 1  to  velkostmnoziny do
>       if  (a = zoznam[i]) then
>          a :=  generuj(n,zoznam);
>          break;
>       fi ;
>    od;
> fi ;
> a := a;
> end;

> umocnimodulo := proc(zaklad,exponent,modulo) local r, a, b, m;  a :=  zaklad;  b :=exponent; m :=
     modulo;
> while (b <> 0) do
>     if  (irem(b,2)=1) then
```

```
>     r := irem(r*a,m);
>     fi;
>     b := floor(b/2);   a := irem(a*a,m);   r;
> od;
> end;
```

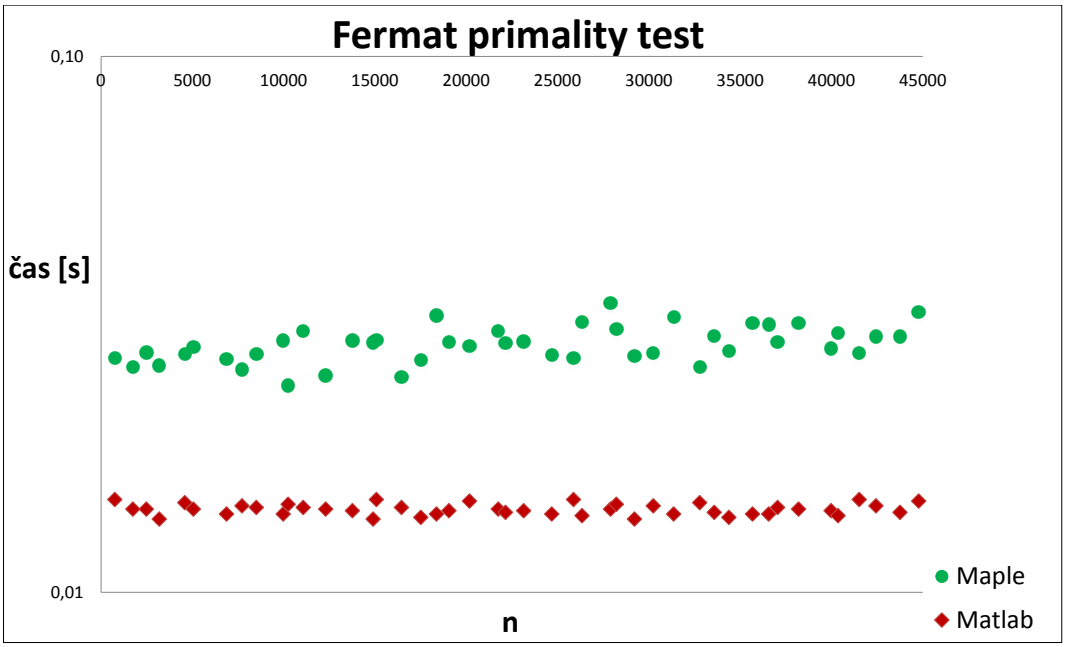
Výpis 6.1: Fermatov test prvočíselnosti v Maple

Algoritmus v Matlabe:

```
function fermat_test(n,poceta)
zoznam=[];
 i=0;

while (i<poceta)
    a=generuj(n,zoznam);
    if (umocnimodulo(a,n-1,n)~=1)
        fprintf('Cislo %i je zlozene cislo! \n',n)
        fprintf('Cislo %i je Frematovym svedkom zlozenosti cisla n= %i \n', [a,n] )
        return
    end
    zoznam(i+1)=a;
    i=i+1;
end

fprintf('Cislo %i moze, ale nemusi byt prvocislo! \n',n)
end

function a = generuj(n,zoznam)
a=1+unique(ceil((n-2)*rand(1,1)));
velkost_mnoziny=size(zoznam);
if (velkost_mnoziny(2)~= 0)
    for i=1:velkost_mnoziny(2)
        if (a==zoznam(i))
            a=generuj(n,zoznam);
            break;
        end;
    end;
end;
end;

function r = umocnimodulo(a,b,m)
exponent=b;
r=1;
while (exponent ~= 0)
    if (mod(exponent,2) == 1)
        r = mod(r.*a,m);
    end
    exponent=floor(exponent/2);
    a = mod(a.*a,m);
end
end
```

Výpis 6.2: Fermatov test prvočíselnosti v Matlabe

Algoritmus bol testovaný pre náhodne vygenerované čísla n v intervale $\langle 1, 45000\rangle$ a to tak, aby v každom intervale $\langle 1, 1000\rangle, \langle 1000, 2000\rangle, ..., \langle 44000, 45000\rangle$ bolo vygenerované jedno číslo. Hodnota $poceta$ bola pri každom teste 100. Čas výpočtu pre testované n a $poceta = 100$ je aritmetickým priemerom $100-$tých nameraných hodnôt.

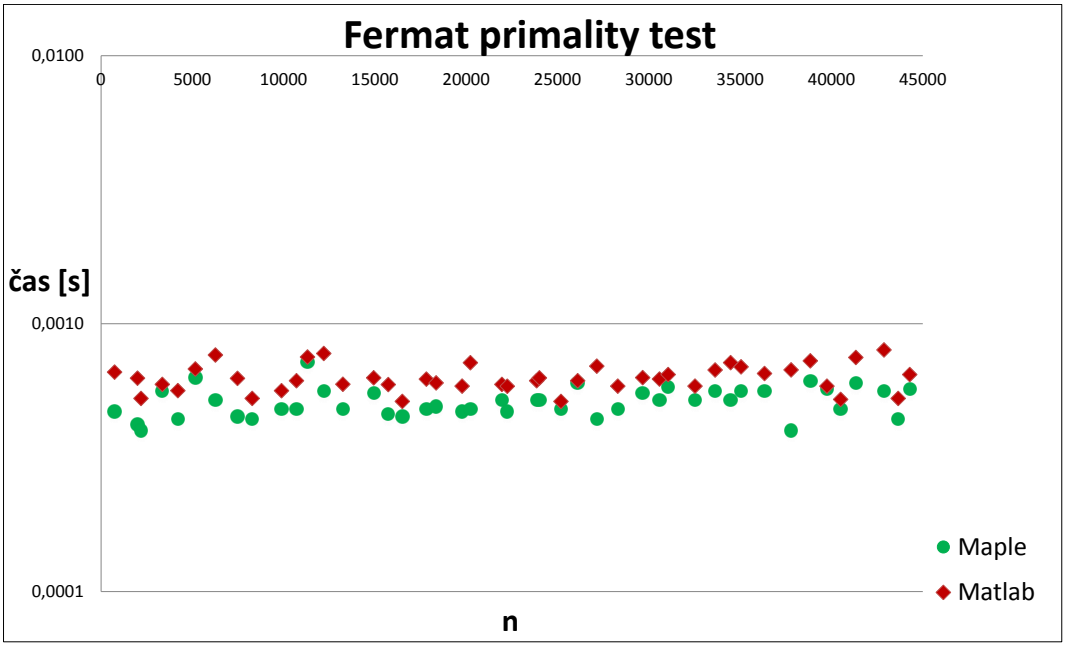


n:	751	1741	2477	3187	4583	5051	6869	7717	8501	9973	10243	11071	12301	13763	14897
Maple:	0,02736	0,02636	0,02804	0,02649	0,02784	0,02872	0,02727	0,02727	0,02788	0,02949	0,02433	0,03073	0,02540	0,02949	0,02928
Matlab:	0,01490	0,01430	0,01430	0,01370	0,01470	0,01430	0,01400	0,01450	0,01440	0,01400	0,01460	0,01440	0,01430	0,01420	0,01370
n:	15077	16451	17509	18367	19051	20177	21751	22147	23143	24683	25873	26339	27901	28219	29209
Maple:	0,02960	0,02524	0,02716	0,01400	0,02932	0,02880	0,03076	0,02920	0,02941	0,02771	0,02736	0,03192	0,03468	0,03096	0,02764
Matlab:	0,01490	0,01440	0,01380	0,01400	0,01420	0,01480	0,01430	0,01410	0,01420	0,01400	0,01490	0,01390	0,01430	0,01460	0,01370
n:	30241	31357	32783	33581	34381	35677	36563	37049	38197	39979	40361	41521	42437	43753	44777
Maple:	0,02796	0,03268	0,02632	0,03008	0,02820	0,03184	0,03160	0,02935	0,03177	0,02852	0,03048	0,02796	0,03001	0,03000	0,03332
Matlab:	0,01450	0,01400	0,01470	0,01410	0,01380	0,01400	0,01400	0,01440	0,01430	0,01420	0,01390	0,01490	0,01450	0,01410	0,01480

Obr. 6.1: Graf rýchlosti Fermatovho algoritmu pre prvočísla

Pokiaľ testujeme len náhodne vygenerované prvočísla, neexistuje žiadny Fermatov svedok zloženosti týchto čísel. Kongruencia 6.1 je splnená pre všetky náhodne vygenerované a. Počet náhodne vygenerovaných čísel a udáva hodnota $poceta$, ktorá je nastavená na číslo 100, teda počet kongruencií 6.1, ktoré algoritmus otestuje je 100. Rýchlosť Fermatovho algoritmu závisí na čísle n a na hodnotách a, ktoré sú náhodne vygenerované, pretože určujú, ako veľmi zložitú kongruenciu algoritmus vyhodnocuje. Z grafu 6.1 vyplýva, že nepatrne rýchlejší na výpočet Fermatovho algoritmu, pokiaľ testujeme prvočíslo, je Matlab.

Pokiaľ testujeme len náhodne vygenerované zložené čísla, tak určite musí existovať nejaký Fermatov svedok zloženosti. V takomto prípade testujeme kongruenciu 6.1 pre náhodne vygenerované a, ktorých maximálny počet udáva hodnota $poceta = 100$, až

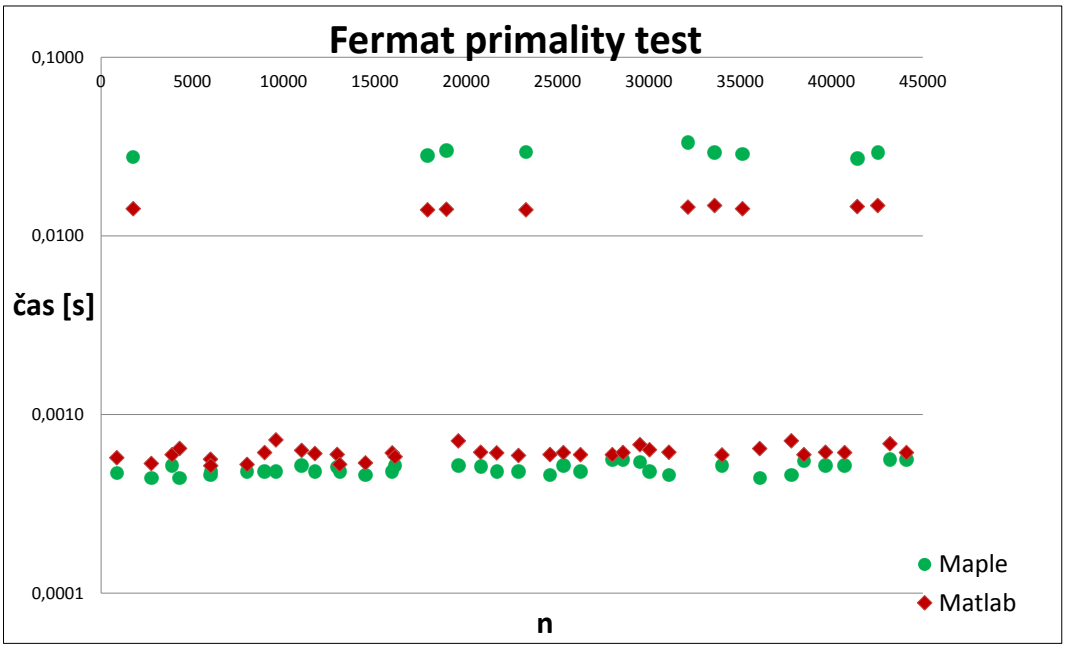


n:	740	1994	2186	3354	4205	5161	6261	7470	8277	9882	10701	11305	12196	13242	14930
Maple:	0,00047	0,00042	0,00040	0,00056	0,00044	0,00063	0,00052	0,00052	0,00044	0,00048	0,00048	0,00072	0,00056	0,00048	0,00055
Matlab:	0,00066	0,00063	0,00053	0,00059	0,00056	0,00068	0,00076	0,00063	0,00053	0,00056	0,00061	0,00075	0,00077	0,00059	0,00063
n:	15728	16498	17814	18348	19772	20225	21951	22246	23854	24003	25186	26101	27149	28298	29661
Maple:	0,00046	0,00045	0,00048	0,00060	0,00047	0,00048	0,00052	0,00047	0,00052	0,00052	0,00048	0,00060	0,00044	0,00048	0,00055
Matlab:	0,00059	0,00051	0,00062	0,00060	0,00058	0,00072	0,00059	0,00058	0,00061	0,00063	0,00051	0,00061	0,00069	0,00058	0,00063
n:	30581	31056	32527	33628	34477	35049	36334	37789	38841	39753	40503	41335	42877	43654	44286
Maple:	0,00052	0,00058	0,00052	0,00056	0,00052	0,00056	0,00056	0,00040	0,00061	0,00057	0,00048	0,00060	0,00056	0,00044	0,00057
Matlab:	0,00062	0,00065	0,00058	0,00067	0,00072	0,00069	0,00065	0,00067	0,00073	0,00058	0,00052	0,00075	0,00080	0,00053	0,00065

Obr. 6.2: Graf rýchlosti Fermatovho algoritmu pre zložené čísla

dovtedy, dokiaľ pre nejaké a kongruencia 6.1 nie je splnená. Rýchlosť algoritmu závisí od čísla n, od hodnôt a a od toho, koľko kongruencií algoritmus otestoval predtým, ako našiel také a, pre ktoré kongruencia 6.1 nie je splnená. V prípade, že také a nenájde (nenájde Fermatovho svedka zloženosti), je počet otestovaných kongruencií 100. Z grafu 6.2 vyplýva, že na výpočet Fermatovho algoritmu, pokiaľ je testované číslo zložené číslo, je nepatrne rýchlejší Maple.

Ak testujeme náhodne vygenerované čísla (prvočísla aj zložené čísla), rýchlosť algoritmu závisí na počte kongruencií, ktoré algoritmus otestuje. Počet otestovaných kongruencií závisí od čísla n a od náhodne vygenerovaných hodnôt a. Viď graf 6.3.



n:	860	1759	2751	3890	4301	5992	6006	7994	8955	9576	10983	11710	12930	13067	14478
Maple:	0,00047	0,02769	0,00044	0,00052	0,00044	0,00046	0,00048	0,00048	0,00048	0,00048	0,00052	0,00048	0,00051	0,00048	0,00046
Matlab:	0,00057	0,01420	0,00053	0,00060	0,00065	0,00056	0,00052	0,00053	0,00061	0,00072	0,00063	0,00061	0,00060	0,00053	0,00054
n:	15944	16102	17881	18913	19565	20788	21668	22860	23269	24587	25319	26255	27999	28583	29511
Maple:	0,00048	0,00052	0,02824	0,01410	0,00052	0,00051	0,00048	0,00048	0,02965	0,00046	0,00052	0,00048	0,00056	0,00056	0,00054
Matlab:	0,00061	0,00058	0,01400	0,01410	0,00071	0,00062	0,00061	0,00059	0,01400	0,00060	0,00061	0,00060	0,00060	0,00061	0,00068
n:	30036	31098	32141	33601	34004	35129	36070	37802	38491	39673	40721	41413	42533	43204	44108
Maple:	0,00048	0,00046	0,03339	0,02940	0,00052	0,02884	0,00044	0,00046	0,00055	0,00052	0,00052	0,02720	0,02932	0,00056	0,00056
Matlab:	0,00064	0,00062	0,01450	0,01480	0,00059	0,01420	0,00065	0,00071	0,00060	0,00062	0,00061	0,01460	0,01480	0,00069	0,00061

Obr. 6.3: Graf rýchlosti Fermatovho algoritmu

7 Miller-Rabinov test prvočíselnosti

7.1 Popis

Z Vety 6.1.4 vyplýva, že Fermatov test prvočíselnosti funguje dobre vtedy, keď sa snažíme preukázať zloženosť čísla, ktoré nie je súčinom navzájom rôznych prvočísel. Napríklad pre Carmichaelove čísla nie je Fermatov test veľmi použiteľný. Nedostatky Fermatovho testu odstraňuje *Miller-Rabinov test* prvočíselnosti.

Miller-Rabinov test prvočíselnosti čísla n spočíva v troch krokoch:

- Náhodne vyberieme nejaké číslo a tak, že $1 < a < n$.
- Číslo $n-1$ rozložíme na tvar $2^k \cdot q$, kde $k \in \mathbb{N}$ a q je nepárne.
- Testujeme, či sú splnené kongruencie:

$$\begin{aligned} a^{2^{(k-1)}\cdot q} &\equiv -1 \pmod{n} \\ a^{2^{(k-2)}\cdot q} &\equiv -1 \pmod{n} \\ &\vdots \\ a^{2\cdot q} &\equiv -1 \pmod{n} \\ a^{q} &\equiv -1 \pmod{n} \\ a^{q} &\equiv 1 \pmod{n}. \end{aligned} \tag{7.1}$$

  Nastanú dva závery:

  - Aspoň jedna z kongruencií 7.1 je splnená. V takomto prípade číslo n môže, ale nemusí byť prvočíslo. Zvolíme iné číslo a, pre ktoré testujeme kongruencie 7.1 znova.
  - Žiadna z kongruencií 7.1 nie je splnená. V takomto prípade číslo n určite nie je prvočíslo. Číslo a bude Miller-Rabinovým svedkom zloženosti čísla n.

Príklad: Číslo $n = 561$ je Carmichaelovo číslo. Podľa definície 6.1.2 pre každé nesúdeliteľné číslo a s číslom n je kongruencia $a^{560} \equiv 1 \pmod{561}$ splnená. Keďže $gcd(2, 561) = 1$, kongruencia $2^{560} \equiv 1 \pmod{561}$ je splnená. Z toho vyplýva, že číslo $a = 2$ nie je Fermatovým svedkom zloženosti čísla $n = 561$. Číslo $n - 1 = 560 = 2^4 \cdot 35$ ($k = 4, q = 35$). Ale ani jedna z kongruencií 7.1 pre $a = 2$ nie je splnená:

$$2^{2^{4-1}\cdot 35} = 2^{280} \equiv 1 \pmod{561}$$

$$2^{2^{4-2}\cdot 35} = 2^{140} \equiv 67 \pmod{561}$$

$$2^{2^{4-3}\cdot 35} = 2^{70} \equiv 166 \pmod{561}$$

$$2^{2^{4-4}\cdot 35} = 2^{35} \equiv 263 \pmod{561}$$

Čo ale znamená, že $n = 561$ nie je prvočíslo. Číslo $a = 2$ nie je Fermatovým svedkom zloženosti, ale Miller-Rabinovým svedkom zloženosti čísla $n = 561$ je.

Lemma 7.1.1 Nech $a, n \in \mathbb{N}$, kde n je liché zložené číslo. Ak číslo a je Fermatovým svedokom zloženosti čísla n, potom je tiež aj Miller-Rabinovým svedkom zloženosti čísla n.

Dôkaz. Ak a je Fermatovým svedkom zloženosti čísla n, potom musí platiť:

$$a^{n-1} \not\equiv 1 \pmod{n},$$

$$a^{n-1} - 1 \not\equiv 0 \pmod{n}.$$

Po dosadení $n - 1 = 2^k \cdot q$ dostaneme:

$$(a^{2^{k-1} \cdot q} + 1)(a^{2^{k-2} \cdot q} + 1)...(a^q + 1)(a^q - 1) \not\equiv 0 \pmod{n}.$$

Čo znamená, že ani jedna z kongruencií overovaných u Miller-Rabinovho testu nemôže platiť. Z čoho vyplýva, že ak je a Fermatovým svedkom zloženosti, tak je potom aj Miller-Rabinovým svedkom zloženosti čísla n. ∎

Poznámka: Dôsledkom Lemmy 7.1.1 je, že použitím Miller-Rabinovho testu prvočíselnosti určite nestratíme informáciu o zloženosti čísla n, ktorú by sme obdržali pri použití Fermatovho testu prvočíselnosti.

Veta 7.1.2 Nech $n \in \mathbb{N}$ je nepárne zložené číslo. Počet Miller-Rabinových svedkov zloženosti čísla n v intervale $\langle 1, n)$ je najmenej $\frac{3}{4}(n-1)$.

Dôkaz: Viď literatúra [2].

Poznámka: Pokiaľ testujeme nepárne zložené číslo n, tak pravdepodobnosť, že náhodne zvolené a ($a \in \langle 1, n)$) nie je Miller-Rabinovým svedkom zloženosti čísla n, je menšia ako $\frac{1}{4}$. Čiže ak $100-$krát náhodne zvolíme číslo a, tak pravdepodobnosť, že ani jedno zo zvolených čísel nebude Miller-Rabinovým svedkom zloženosti čisla n, je menšia ako $(\frac{1}{4})^{100}$.

7.2 Algoritmus

Vstupným parametrom algoritmu je n, čo je testované číslo na prvočíslenosť a hodnota $poceta$, ktorá udáva maximálny počet náhodne vygenerovaných čísel a. Algoritmus vypočíta k a q, tak aby $n - 1 = 2^k \cdot q$. Následne algoritmus náhodne vygeneruje nejaké a z intervalu $\langle 2, (n-1)\rangle$ a testuje, či sú splnené kongruencie 7.1 pre vygenerované a. Ak nie je splnená žiadna z uvedených kongruencií, algoritmus je ukončený, pretože číslo n je určite zložené. Pokiaľ je splnená aspoň jedna z uvedených kongruencií, tak algoritmus vygeneruje iné číslo a, pre ktoré testuje kongruencie 7.1 znova. Ak nájde nejaké a, pre ktoré nie je splnená žiadna z kongruencií 7.1, algoritmus je ukončený, pretože našiel Miller-Rabinovho svedka zloženosti, teda číslo n je zložené. Ak pre všetky náhodne vygenerované čísla a (čísla sa neopakujú, maximálny počet náhodne vygenerovaných čísel je $poceta$) je vždy aspoň jedna z kongruencií 7.1 splnená, algoritmus je ukončený s výsledkom, že testované číslo n môže, ale nemusí byť prvočíslo.

Algoritmus v Maple:

```
> millerrabin := proc (n, poceta)
> local k, q, a, y, x, j, i;
> local zoznam;
> q := n−1;
> k := 0;

> while (umocnimodulo(q,1,2)=0) do
>     q := (1/2)q;
>     k := k+1;
> od;

> zoznam := [];
>  i := 0;

> while (i<poceta) do
>     a := generuj(n,zoznam);
>     if (umocnimodulo(a,q,n) <> 1) then
>         y := 1;
>     else
>         y := 0;
>     fi;

>     for j from 1 to k do
>         if (umocnimodulo(a,(2^(k−j)∗q), n) <> (n−1)) then
>           x := 1;
>         else
>           x := 0;
>         fi;
>         if ((y = 1) and (x = 1)) then
>           y := 1;
>         else
>           y := 0;
>         fi;
>     od;

>     if (y = 1) then
>         print(n 'je␣zlozene␣cislo');
>         print(a 'je␣Miller␣Rabinovym␣svedkom␣zlozenosti␣zadaneho␣cisla');
>     return;
>     fi;

>     zoznam := [op(zoznam),a];
>      i := i+1;
> do;

> print(n 'moze␣ale␣nemusi␣byt␣prvocislo');
> end;
```

Výpis 7.1: Miller-Rabinov test prvočíselnosti v Maple

Algoritmus v Matlabe:

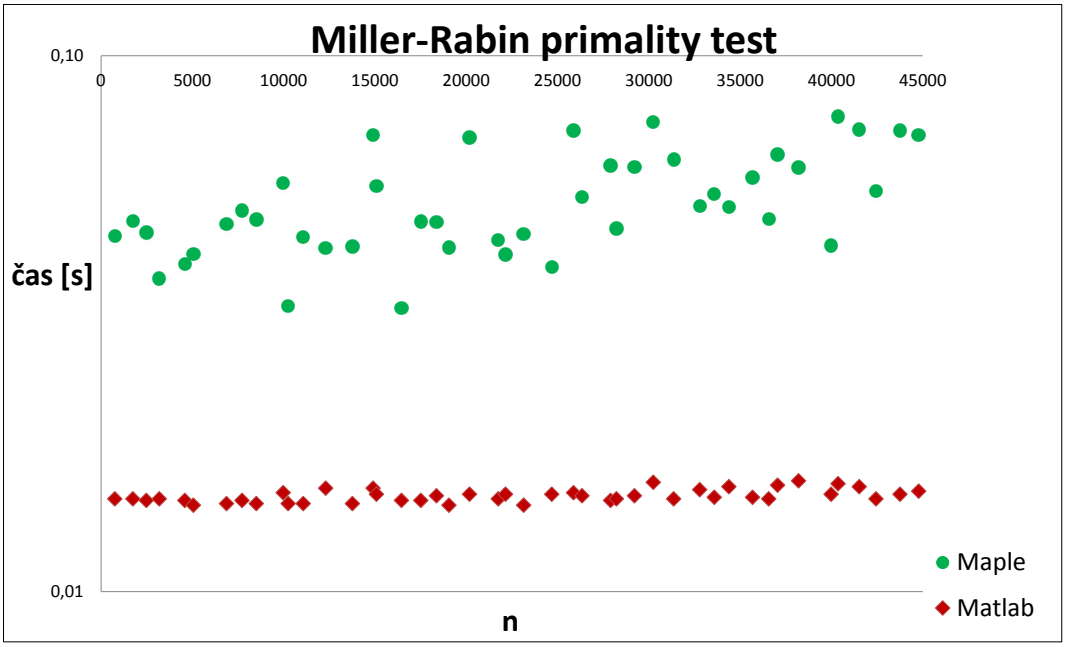
```
function miller_rabin_test (n, poceta)
q=n-1;
k=0;

while (umocnimodulo(q,1,2)==0)
    q=q/2;
    k=k+1;
end

zoznam=[];
i=0;

while (i<poceta)
    a= generuj(n,zoznam);
    y= (umocnimodulo(a,q,n)~=1);

    for j=1:k
        x= (umocnimodulo(a,(2^(k-j)*q),n)~=(n-1));
        y=(y && x);
    end

    if (y==1)
        fprintf('Cislo %i je zlozene cislo!\n',n)
        fprintf('Cislo %i je Miller Rabinovym svedkom zlozenosti cisla n=%i \n',[a,n])
    return
    end

    zoznam(i+1)=a;
    i=i+1;
end

fprintf('Cislo %i moze, ale nemusi byt prvocislo! \n',n)
end
```

Výpis 7.2: Miller-Rabinov test prvočíselnosti v Matlabe

Algoritmus bol testovaný pre náhodne vygenerované čísla n v intervale $\langle 1, 45000\rangle$ a to tak, aby v každom intervale $\langle 1, 1000), \langle 1000, 2000), ..., \langle 44000, 45000\rangle$ bolo vygenerované jedno číslo. Hodnota $poceta$ bola pri každom teste 100. Čas výpočtu pre testované n a $poceta = 100$ je aritmetickým priemerom $100-$tých nameraných hodnôt.

Pravdepodobnosť, že pri testovaní nepárneho zloženého čísla nájdeme svedka zloženosti je $1 - (\frac{1}{4})^{100}$.
Pravdepodobnosť, že náhodne vygenerované nepárne číslo n z intervalu $\langle 1, 45000\rangle$ také, u ktorého pri 100 pokusoch nenájdeme Miller-Rabinovho svedka zloženosti, je prvočíslo, môžeme odvodiť následovne:
Javom P bude, že náhodne vygenerované číslo z intervalu $\langle 1, 45000\rangle$ je prvočíslo.
$P(P) \doteq \frac{\pi(45000)}{45000} = \frac{\frac{45000}{\ln 45000}}{45000} = \frac{1}{\ln 45000}$. Vyplýva v Vety 2.4.4.
Javom LP bude, že náhodne generované nepárne číslo z intervalu $\langle 1, 45000\rangle$ je prvočíslo.

$P(LP) \doteq \frac{2}{\ln 45000}, P(\overline{LP}) \doteq 1 - \frac{2}{\ln 45000}$.
Javom M bude, že ani jedno zo 100 náhodne zvolených čísel $a, a \in \langle 2, n-1 \rangle$ nebude Miller-Rabinovým svedkom zloženosti čísla n.
$P(M|LP) = 1, P(M|\overline{LP}) \leq (\frac{1}{4})^{100}$. Vyplýva v Vety 7.1.2.
Úlohou je zistiť $P(LP|M)$, využijeme Bayesovu vetu:
$P(LP|M) = \frac{P(M|LP).P(LP)}{P(M|LP).P(LP)+P(M|\overline{LP}).P(\overline{LP})} \geq \frac{1.\frac{2}{\ln 45000}}{1.\frac{2}{\ln 45000}+(\frac{1}{4})^{100}.(1-\frac{2}{\ln 45000})} = \frac{1}{1+(\frac{1}{4})^{100}.(\frac{\ln 45000}{2}-1)}$
$\geq \frac{1}{1+8.(\frac{1}{4})^{100}} \geq 1 - 8.(\frac{1}{4})^{100} = 1 - (\frac{1}{2})^{197} \geq 1 - (\frac{1}{10})^{59}$.

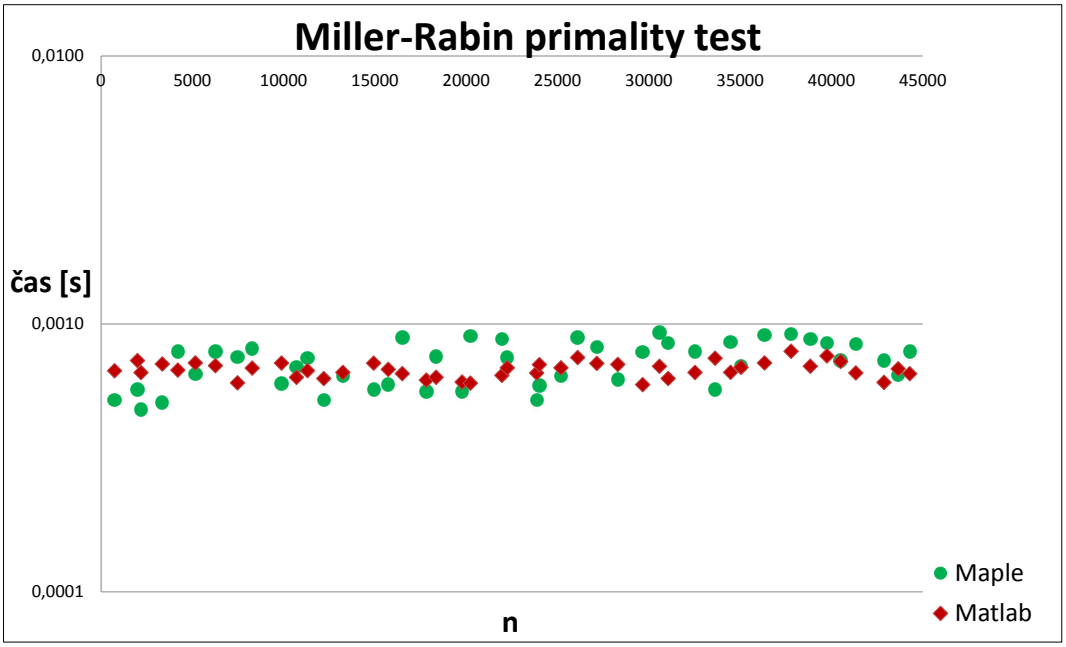


n:	751	1741	2477	3187	4583	5051	6869	7717	8501	9973	10243	11071	12301	13763	14897
Maple:	0,04612	0,04924	0,04680	0,03840	0,04091	0,04268	0,04859	0,04859	0,04944	0,05789	0,03416	0,04588	0,04380	0,04408	0,07120
Matlab:	0,01490	0,01490	0,01480	0,01490	0,01480	0,01450	0,01460	0,01480	0,01460	0,01530	0,01460	0,01460	0,01560	0,01460	0,01560
n:	15077	16451	17509	18367	19051	20177	21751	22147	23143	24683	25873	26339	27901	28219	29209
Maple:	0,05716	0,03384	0,04909	0,01510	0,04388	0,07036	0,04536	0,04260	0,04644	0,04040	0,07252	0,05450	0,06240	0,04764	0,06201
Matlab:	0,01520	0,01480	0,01480	0,01510	0,01450	0,01520	0,01490	0,01520	0,01450	0,01520	0,01530	0,01510	0,01480	0,01490	0,01510
n:	30241	31357	32783	33581	34381	35677	36563	37049	38197	39979	40361	41521	42437	43753	44777
Maple:	0,07528	0,06408	0,05248	0,05516	0,05224	0,05930	0,04963	0,06547	0,06187	0,04424	0,07700	0,07288	0,05588	0,07251	0,07112
Matlab:	0,01600	0,01490	0,01550	0,01500	0,01570	0,01500	0,01490	0,01580	0,01610	0,01520	0,01590	0,01570	0,01490	0,01520	0,01540

Obr. 7.1: Graf rýchlosti Miller-Rabinovho algoritmu pre prvočísla

Ak testujeme len náhodne vygenerované prvočísla, neexistuje žiadny Miller-Rabinov svedok zloženosti týchto čísel. Počet kongruencií 7.1 pre jednotlivé n zavisí od čísla k, kde $(n-1) = 2^k \cdot q$. Kongruencie 7.1 algoritmus otestuje pre náhodne vygenerované a (maximálny počet náhodne vygenerovaných a je $poceta = 100$) a pokiaľ testované n je prvočíslo, tak pre každé náhodne vygenerované číslo a je aspoň jedna z kongruencií 7.1 splnená. To znamená, že počet všetkých kongruencií, ktoré algoritmus otestuje ak testuje prvočíslo, je $100k$. Rýchlosť Miller-Rabinovho algoritmu závisí na testovanom čísle n a na náhodne vygenerovaných hodnotách a. Z grafu 7.1 vidíme, že rýchlejší na výpočet

Miller-Rabinovho algoritmu, pokiaľ je testované číslo prvočíslo, je Matlab.

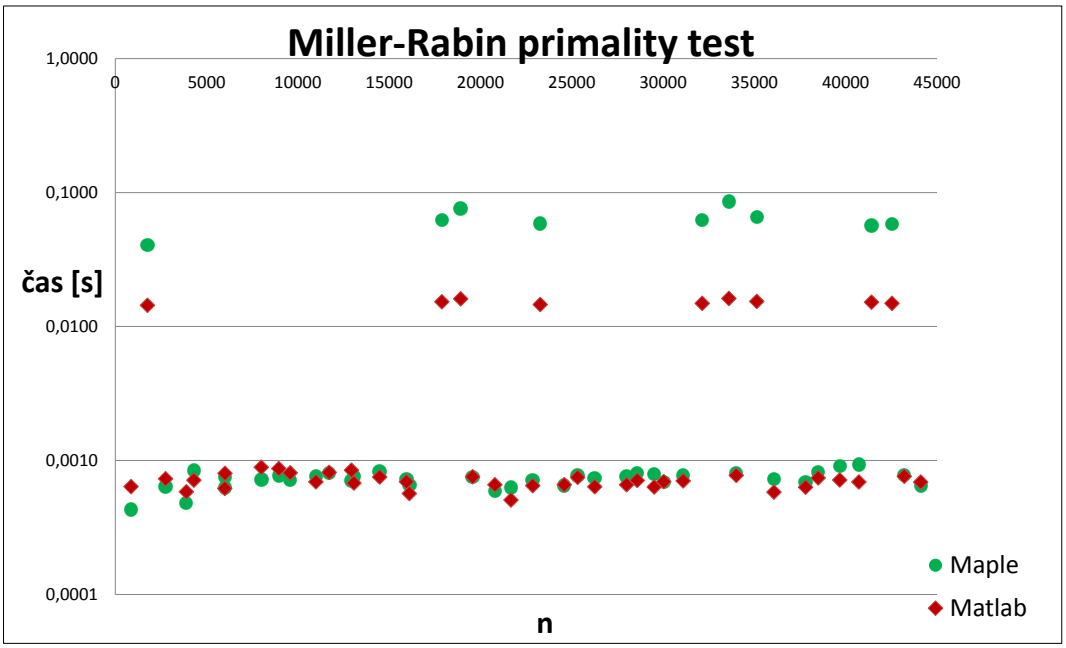


n:	740	1994	2186	3354	4205	5161	6261	7470	8277	9882	10701	11305	12196	13242	14930
Maple:	0,00052	0,00057	0,00048	0,00051	0,00079	0,00065	0,00079	0,00079	0,00081	0,00060	0,00069	0,00075	0,00052	0,00064	0,00057
Matlab:	0,00067	0,00073	0,00066	0,00071	0,00067	0,00072	0,00070	0,00060	0,00068	0,00071	0,00063	0,00067	0,00063	0,00066	0,00071
n:	15728	16498	17814	18348	19772	20225	21951	22246	23854	24003	25186	26101	27149	28298	29661
Maple:	0,00059	0,00089	0,00056	0,00063	0,00056	0,00090	0,00088	0,00075	0,00052	0,00059	0,00064	0,00089	0,00082	0,00062	0,00079
Matlab:	0,00068	0,00065	0,00062	0,00063	0,00061	0,00060	0,00064	0,00069	0,00066	0,00071	0,00069	0,00075	0,00071	0,00071	0,00059
n:	30581	31056	32527	33628	34477	35049	36334	37789	38841	39753	40503	41335	42877	43654	44286
Maple:	0,00093	0,00085	0,00079	0,00057	0,00086	0,00070	0,00091	0,00092	0,00088	0,00085	0,00073	0,00084	0,00073	0,00065	0,00079
Matlab:	0,00070	0,00063	0,00066	0,00075	0,00066	0,00069	0,00072	0,00079	0,00070	0,00076	0,00072	0,00066	0,00061	0,00068	0,00065

Obr. 7.2: Graf rýchlosti Miller-Rabinovho algoritmu pre zložené čísla

Ak testujeme len náhodne vygenerované zložené čísla, tak určite existuje nejaký Miller-Rabinov svedok zloženosti. Počet kongruencií 7.1 je k, $(n-1) = 2^k \cdot q$. Kongruencie 7.1 testujeme pre náhodne vygenerované a (maximálny počet je $poceta = 100$) až dovtedy, dokiaľ pre nejaké a žiadna z uvedených kongruencií nie je splnená. Rýchlosť algoritmu závisí od čísla n, od hodnôt a a od toho, koľko kongruencií algoritmus otestoval predtým, ako našiel také a, pre ktoré žiadna z kongruencií 7.1 nie je splnená. V prípade, že také a nenájde (nenájde Miller-Rabinovho svedka zloženosti), je počet otestovaných kongruencií $100k$. Z grafu 7.2 vyplýva, že rýchlosť Miller-Rabinovho algoritmu, pokiaľ je testované číslo zložené číslo, je približne rovnaká pre Matlab aj Maple.

Ak testujeme náhodne vygenerované čísla (prvočísla aj zložené čísla), rýchlosť algoritmu závisí na počte kongruencií, ktoré algoritmus otestuje. Počet otestovaných kongruencií závisí od čísla n a od náhodne vygenerovaných hodnôt a.Viď graf 7.3.



n:	860	1759	2751	3890	4301	5992	6006	7994	8955	9576	10983	11710	12930	13067	14478
Maple:	0,00043	0,04064	0,00064	0,00048	0,00084	0,00075	0,00063	0,00063	0,00077	0,00072	0,00076	0,00081	0,00071	0,00076	0,00083
Matlab:	0,00064	0,01440	0,00073	0,00058	0,00071	0,00062	0,00080	0,00089	0,00087	0,00081	0,00069	0,00082	0,00085	0,00068	0,00075
n:	15944	16102	17881	18913	19565	20788	21668	22860	23269	24587	25319	26255	27999	28583	29511
Maple:	0,00073	0,00066	0,06277	0,01610	0,00075	0,00059	0,00063	0,00072	0,05876	0,00065	0,00077	0,00074	0,00076	0,00081	0,00079
Matlab:	0,00069	0,00057	0,01530	0,01610	0,00076	0,00066	0,00051	0,00065	0,01460	0,00066	0,00075	0,00064	0,00066	0,00071	0,00063
n:	30036	31098	32141	33601	34004	35129	36070	37802	38491	39673	40721	41413	42533	43204	44108
Maple:	0,00069	0,00077	0,06265	0,08560	0,00081	0,06575	0,00073	0,00069	0,00082	0,00091	0,00093	0,05668	0,05842	0,00078	0,00065
Matlab:	0,00070	0,00070	0,01490	0,01620	0,00077	0,01540	0,00058	0,00063	0,00074	0,00072	0,00069	0,01520	0,01490	0,00076	0,00069

Obr. 7.3: Graf rýchlosti Miller-Rabinovho algoritmu

8 AKS deterministický test prvočíselnosti

8.1 Popis

Definícia 8.1.1 Nech $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ také, že $gcd(a, n) = 1$. Najmenšie kladné celé číslo r také, že $a^r \equiv 1 \pmod{n}$ budeme označovať $ord_n(a)$.

Veta 8.1.2 Nech $n \in \mathbb{Z}, n > 1$, $a \in \mathbb{Z}$ a $gcd(a, n) = 1$. n je prvočíslo práve vtedy, keď v okruhu polynómov $\mathbb{Z}_n$ platí:

$$(x + a)^n \equiv (x^n + a) \pmod{n}.$$

Dôkaz. Z binomickej vety platí:

$$(x + a)^n = \sum_{k=0}^{n} \binom{n}{k} a^k x^{n-k} = x^n + a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^k x^{n-k} \tag{8.1}$$

- $\Rightarrow$: Predpokladajme, že n je prvočíslo. Potom koeficient $\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!}$ je pre všetky $k, 1 \leq k \leq n-1$ deliteľný číslom n, pretože n delí čitateľa a zároveň nedelí menovateľa. Z čoho vyplýva, že $\binom{n}{k} \equiv 0 \pmod{n}$. Preto

  $$(x + a)^n \equiv (x^n + a^n) \pmod{n}.$$

  Z vety 4.1.5 vieme, že $a^{n-1} \equiv 1 \pmod{n}$, čo ale znamená, že $a^n \equiv a \pmod{n}$. Z toho vyplýva, že

  $$(x + a)^n \equiv (x^n + a) \pmod{n}.$$

- $\Leftarrow$: Predpokladajme, že n nie je prvočíslo. Uvažujme prvočíslo $p, p \mid n$ a $s, s \geq 1$ také, že $p^s \mid n, p^{s+1} \nmid n$. Potom $n = p^s k$, pričom $p \nmid k$. Taktiež platí, že $p \nmid (n-1)...(n-p+1)$. Ak vieme, že $gcd(a, n) = 1$, potom určite platí, že $p \nmid a$, lebo pokiaľ by platilo, že $p \mid a$, potom $a = cp, c \in \mathbb{Z}$ a $gcd(cp, p^s k) \neq 1$. V rovnosti 8.1 koeficient pri x^{n-p} je

  $$\binom{n}{p} a^p = \frac{n(n-1)...(n-p+1)}{p!} a^p = \frac{p^s k(n-1)...(n-p+1)}{p!} a^p =$$

  $$= \frac{p^{s-1} k(n-1)...(n-p+1)}{(p-1)!} a^p \tag{8.2}$$

  Koeficient 8.2 nie je deliteľný p^s, pretože pokiaľ by $p^s \mid \frac{p^{s-1}k(n-1)...(n-p+1)}{(p-1)!} a^p$, potom $\frac{p^{s-1}k(n-1)...(n-p+1)}{(p-1)!} a^p = q.p^s, q \in \mathbb{Z}$. Po úprave by sme dostali $\frac{k(n-1)...(n-p+1)}{(p-1)!} a^p = q.p$, a keďže $p \nmid (n-1)...(n-p+1), p \nmid k, p \nmid a, p \nmid (p-1)!$, určite platí, že p^s nedelí koeficient 8.2. Koeficient 8.2 nie je deliteľný p^s, takže nie je deliteľný ani n. To ale znamená, že

  $$(x + a)^n \not\equiv (x^n + a) \pmod{n}.$$

■

Veta 8.1.3 Nech $n, r \in \mathbb{N}$ splňujú podmienky:

- $n \geq 3$
- r je prvočíslo také, že $r < n$
- $a \nmid n$, kde $2 \leq a \leq r$
- $ord_r(n) > 4(\log_2 n)^2$
- $(x + a)^n \equiv (x^n + a) \pmod{(x^r - 1)}$ v $\mathbb{Z}_n$, kde $1 \leq a \leq 2\sqrt{r}\log_2 n$.

Potom n je mocninou prvočísla.

Dôkaz: Viď literatúra [4].

Poznámka: Pokiaľ platí, že $n \neq a^b$, kde $a, b \geq 2$ a zároveň platí, že n je mocninou nejakého prvočísla, potom $n = c^1$, kde c je prvočíslo. To znamená, že n je prvočíslo.

Definícia 8.1.4 Nech $n \in \mathbb{N}$. Pokiaľ existujú čísla $a, b \in \mathbb{N}, a, b \geq 2$ také, že $n = a^b$, potom hovoríme, že n je vlastnou mocninou.

Lemma 8.1.5 Pre všetky $n \geq 2, n \in \mathbb{N}$ existuje prvočíslo $r \leq 20(\lceil \log_2 n \rceil)^5$ také, že $r \mid n$ alebo $r \nmid n$ a súčasne $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$.

Dôkaz: Viď literatúra [4].

AKS test prvočíselnosti čísla n spočíva v krokoch:

- Určíme, či pre dané číslo n platí vzťah $n = a^b$, kde $a, b \geq 2$. Pokiaľ platí, tak n je zložené číslo.
- Hľadáme najmenšie prvočíslo r, tak, že $r < n$, $a \nmid n$, kde $2 \leq a \leq r$(čo znamená, že žiadne číslo menšie alebo rovné r nedelí n - v takom prípade je n určite zložené číslo) a $ord_r(n) > 4(\log_2 n)^2$.
- Pokiaľ také prvočíslo neexistuje, tak $r = n$ a v tom prípade n je prvočíslo.
- Postupne pre a od 1 do $2\lceil\sqrt{r}\rceil\lceil\log_2 n\rceil$ testujeme kongruenciu

$$(x + a)^n \equiv (x^n + a) \pmod{(x^r - 1)}. \tag{8.3}$$

  v $\mathbb{Z}_n$.

  - Pokiaľ nájdeme nejaké a, pre ktoré kongruencia 8.3 neplatí, tak n je zložené číslo.
  - Pokiaľ kongruencia 8.3 platí pre všetky a, tak n je prvočíslo.

8.2 Algoritmus

Algoritmus ma vstupný parameter n, ktorého prvočíselnosť testujeme. Najprv určíme, či n je vlastnou mocninou nejakého čísla, teda $n = a^b, a, b \geq 2$. Pokiaľ je vlastnou mocninou nejakého čísla, tak algoritmus sa ukončí s výsledkom, že zadané číslo n je zložené číslo. Pokiaľ nie je vlastnou mocninou nejakého čísla, hľadáme číslo r v intervale 2 až $n-1$ tak, že začíname od čísla $r = 2$ a skúmame, či $r \mid n$. Pokiaľ áno, algoritmus je ukončený s tým, že n je zložené číslo. Ak $r \nmid n$, skúmame, či r je prvočíslo (použijeme algoritmus Eratosthenovho sita). Ak r je prvočíslo, tak ešte otestujeme, či platí $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$. Ak nerovnosť platí, tak sme našli hľadané r a ukončíme cyklus. Ak nerovnosť neplatí alebo r nie je prvočíslo, tak zvýšime r o jedničku a skúmame spomínané vlastnosti pre takéto r. Cyklus môžeme opakovať až kým $r < n$. Z lemmy 8.1.5 však vyplýva, že určite existuje $r \leq 20(\lceil \log_2 n \rceil)^5$ s požadovanými vlastnosťami. Pri malých testovaných číslach môže však nastať, že $20(\lceil \log_2 n \rceil)^5$ je väčšie ako n. V prípade, že ani pre $r = (n-1)$ neplatí nerovnosť $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$ alebo r nie je prvočíslo, algoritmus je ukončený s výsledkom, že n je prvočíslo. Posledným krokom je testovanie kongruencie 8.3, pre všetky $a, 1 \leq a \leq 2\lceil \sqrt{r} \rceil \lceil \log_2 n \rceil$. Pokiaľ existuje nejaké a, pre ktoré nie je kongruencia 8.3 splnená, výsledkom algoritmu bude, že n je zložené číslo. Ak je kongruencia 8.3 splnená pre všetky a tak výsledkom algoritmu bude, že zadané číslo n je určite prvočíslo.

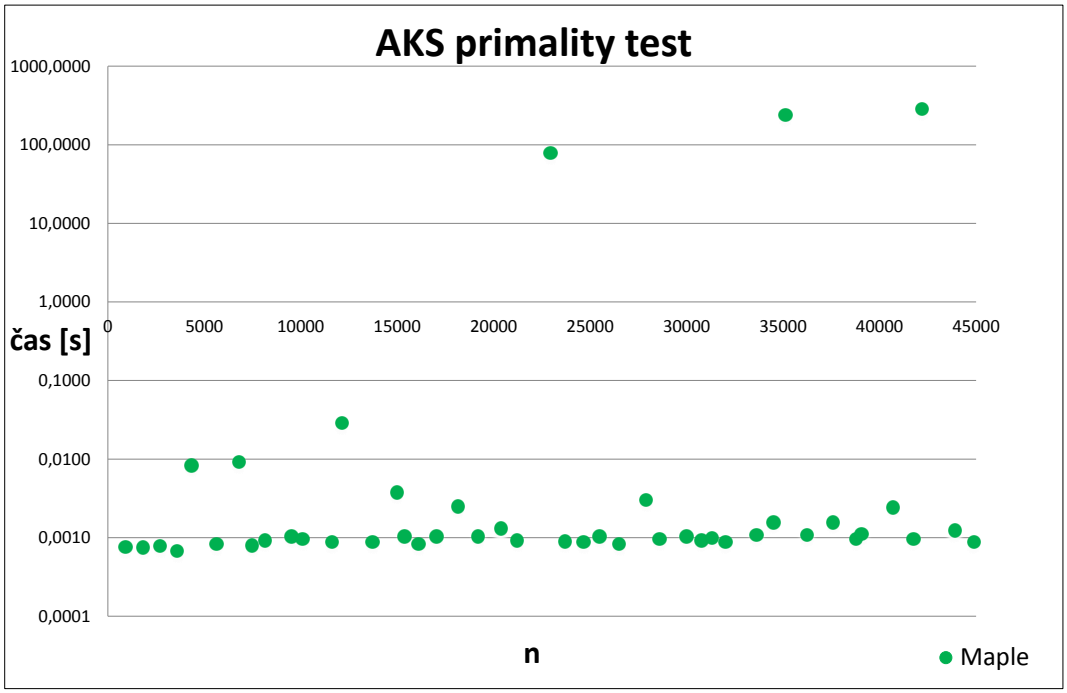
Algoritmus v Maple:

```
>aks:=proc(n) local log2n, j, r, i,a;
>log2n:=floor(evalf(log[2](n)));
> for j from 2 to log2n do
>   if (iroot(n,j)^(j)=n) then
>     print(n 'je zlozene cislo');
>     return;
>   fi;
>od;
>r:=2;
>while (r<n) do
>   if (umocnimodulo(n,1,r)=0) then
>     print(n 'je zlozene cislo');
>     return;
>   fi;
>   if (evalb(r in eratosthenovosito(r))) then
>     i:=1;
>     while (umocnimodulo(n,i,r)<>1) do
>       i:=i+1;
>     od;
>     if (i > (4*(ceil(log[2](n)))^2)) then
>       break;
>     fi;
>   fi;
>   r:=r+1;
>od;
>if (r=n) then
>   print(n 'je prvocislo');
>   return;
```

```
>fi;
>for a from 1 to (2*ceil(sqrt(r))*ceil(log[2](n))) do
>   if ((Powmod(x+a,n,x^(r)-1,x) mod n)<>(Powmod(x^(n)+a,1 ,x^(r)-1,x) mod n)) then
>      print(n 'je zlozene cislo');
>      return;
>   fi;
>od;
>print(n 'je prvocislo');
>end;
```

Výpis 8.1: AKS test prvočíselnosti v Maple

Algoritmus bol testovaný pre náhodne vygenerované čísla n v intervale $\langle 1, 45000\rangle$ a to tak, aby v každom intervale $\langle 1, 1000), \langle 1000, 2000), ..., \langle 44000, 45000\rangle$ bolo vygenerované jedno číslo. Čas výpočtu pre testované n je aritmetickým priemerom $100-$tých nameraných hodnôt.

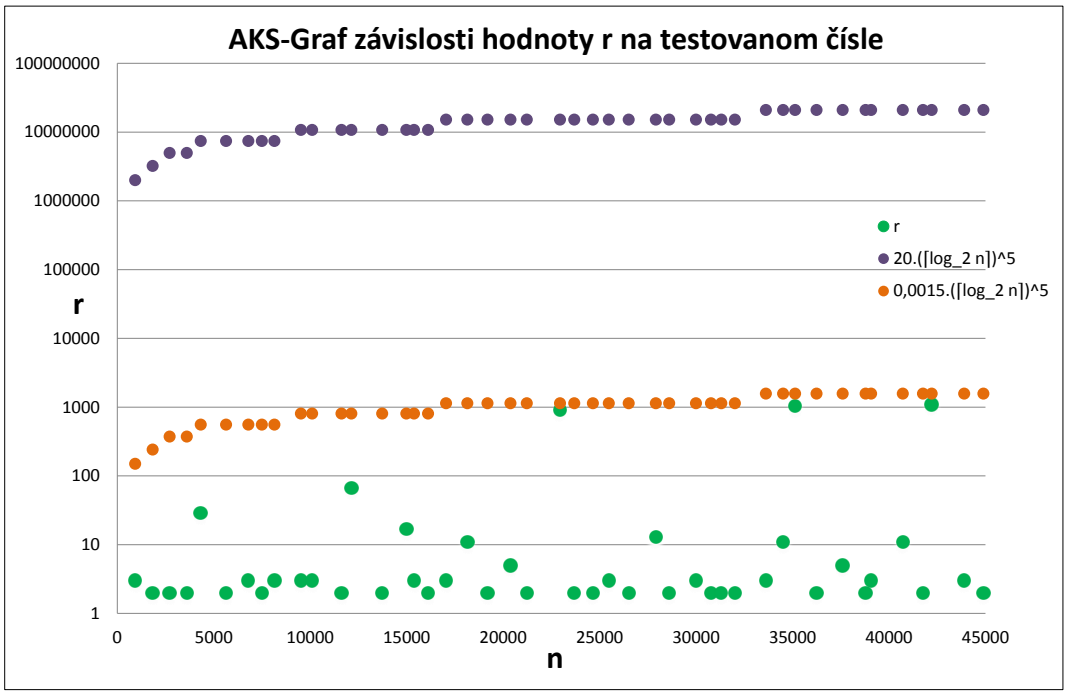


n:	921	1828	2708	3598	4321	5634	6789	7488	8139	9513	10095	11616	12127	13726	14977
Maple:	0,00076	0,00075	0,00079	0,00068	0,00836	0,00084	0,0092	0,0008	0,00092	0,00104	0,00097	0,00088	0,02892	0,00088	0,00376
n:	15375	16104	17037	18139	19184	20375	21222	22943	23682	24648	25473	26504	27911	28602	29991
Maple:	0,00104	0,00084	0,00104	0,00249	0,00104	0,00132	0,00092	78,975	0,0009	0,00088	0,00104	0,00083	0,00303	0,00096	0,00104
n:	30768	31304	32008	33615	34507	35129	36240	37595	38784	39069	40711	41758	42209	43893	44890
Maple:	0,00092	0,001	0,00088	0,00108	0,00156	239,836	0,00108	0,00156	0,00096	0,00112	0,00243	0,00096	286,923	0,00123	0,00088

Obr. 8.1: Graf rýchlosti AKS algoritmu

Rýchlosť AKS algoritmu zavisí od testovaného čísla n. Pokiaľ je n zložené číslo, tak zavisí na tom, či $n = a^b, a, b \geq 2$. Ak áno, algoritmus je ukončený. Ďalej čas výpočtu závisí na tom, či pri hľadaní čísla r (r hľadáme postupne v intervale 2 až $n-1$) nájdeme číslo,

ktoré delí n. V tom prípade je algoritmus ukončený. Pri hľadaní r dôležitú úlohu má aj testovanie či platí $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$, ktorého náročnosť závisí na n. Ak prejdeme všetky r v intervale od 2 do $(n-1)$ a zistíme, že žiadne z nich nie je prvočíslo alebo nesplňuje uvedenú nerovnosť, n je určite prvočíslo. Vieme však, že určite existuje r, ktoré je prvočíslo a splňuje nerovnosť $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$ a platí, že $r \leq 20(\lceil \log_2 n \rceil)^5$. Ak nájdeme r, tak kongruenciu 8.3 testujeme pre $a, 1 \leq a \leq 2\lceil \sqrt{r} \rceil \lceil \log_2 n \rceil$. Ak pri testovaní nejakého a zistíme, že kongruencia 8.3 nie je splnená, tak algoritmus je ukončený s tým, že testované n je zložené číslo. Čas výpočtu bude najdlhší v prípade, keď testujeme kongruenciu pre všetky $a, 1 \leq a \leq 2\lceil \sqrt{r} \rceil \lceil \log_2 n \rceil$, čiže $2\lceil \sqrt{r} \rceil \lceil \log_2 n \rceil -$ krát a kongruencia je splnená pre všetky a. V takom prípade bude n prvočíslo. Rýchlosť AKS algoritmu závisí od testovaného čísla n. Viď graf 8.1.



n:	921	1828	2708	3598	4321	5634	6789	7488	8139	9513	10095	11616	12127	13726	14977
r:	3	2	2	2	29	2	3	2	3	3	3	2	67	2	17
n:	15375	16104	17037	18139	19184	20375	21222	22943	23682	24648	25473	26504	27911	28602	29991
r:	3	2	3	11	2	5	2	907	2	2	3	2	13	2	3
n:	30768	31304	32008	33615	34507	35129	36240	37595	38784	39069	40711	41758	42209	43893	44890
r:	2	2	2	3	11	1039	2	5	2	3	11	2	1097	3	2

Obr. 8.2: Graf závislosti hodnoty r na testovanom čísle pre AKS algoritmus

V grafe 8.2 je závislosť hodnoty r na testovanom čísle. Testované čísla sú náhodne vygenerované z intervalu $\langle 1, 45000 \rangle$ tak, aby v každom intervale $\langle 1, 1000 \rangle, \langle 1000, 2000 \rangle, ..., \langle 44000, 45000 \rangle$ bolo vygenerované jedno číslo. Z grafu vyplýva, že pre každé testované číslo existuje prvočíslo r, ktoré splňuje nerovnosť $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$ a zároveň $r \leq 20(\lceil \log_2 n \rceil)^5$. Z nameraných hodnôt r pre testované čísla z

grafu 8.2 sme zistili, že pre každé testované číslo existuje prvočíslo r, ktoré splňuje nerovnosť $ord_r(n) > 4(\lceil \log_2 n \rceil)^2$ a zároveň $r \leq 0,0015(\lceil \log_2 n \rceil)^5$.

9 Záver

Cieľom tejto práce bolo popísať a naimplementovať pravdepodobnostné a deterministické testy prvočiselnosti a určiť ich prípadné výhody resp. nevýhody.

Eratosthenovo sito je algoritmus, ktorý vyhľadá všetky prvočísla menšie alebo rovné ako zadané n. Funguje tak, že na začiatku je zoradený zoznam čísel, prvé číslo zo zoznamu pridá do zoznamu prvočísel a odstráni v pôvodnom zozname jeho násobky. Časová zložitosť tohoto algoritmu je $O(n\log(\log(n))$, čo odpovedá nameraným hodnotám v Matlabe aj v Maple. Testovanie prebehlo pre $n \in \langle 1000, 5000000\rangle$. Algoritmus je pre čísla rádov tisícok ručne nepoužiteľný.

Fermatov test prvočíselnosti nie je dnes veľmi používaný. Nahradil ho Miller-Rabinov test, ktorý odstránil jeho nedostatky - Miller-Rabinov test funguje dobre aj pre Carmichaelove čísla. Miller-Rabinov test je časom aj zložitosťou náročnejší ako Fermatov test, pretože zatiaľ čo Fermatov algoritmus vyhodnocuje jednu kongruenciu, Miller-Rabinov test ich vyhodnocuje podstatne viac, čo závisí na testovanom čísle.

Nevýhodou Fermatovho a Miller-Rabinovho testu je to, že tieto testy sú pravdepodobnostné. Princíp spočíva v hľadaní svedka zloženosti testovaného čísla, ktorého hľadá medzi náhodne generovanými číslami. Ak ho nenájde, tak výsledkom je, že číslo je prvočíslo s pravdepodobnosťou, ktorá závisí na tom, koľko sme vygenerovali náhodných čísel a hľadali medzi nimi svedka zloženosti. Výhodou týchto testov je, že ak vhodne naimplementujeme funkciu, ktorá vyhodnocuje kongruencie pre veľké čísla, algoritmus je časovo nenáročný.

Výhodou AKS deterministického testu je, že s určitosťou nám dá výsledok o zloženosti testovaného čísla. Časová náročnosť tohoto algoritmu, závisí na testovanom čísle. Algoritmus pozostáva s niekoľkých krokov, a od testovaného čísla závisí, či je po niektorom kroku prerušený alebo sa dostane až k poslednému kroku, čo je testovanie kongruencie v $\mathbb{Z}_n$.

10 Literatúra

[1] JAHODA P., *Základy teorie čísel a jejích aplikací pro nematematiky*, Skripta Vysoká škola Báňská-Technická univerzita Ostrava a Západočeská univerzita v Plzni, 2012.

[2] POMMERSHEIM J.E., MARKS T.K, FLAPAN E.L, *Number theory*, USA: Wiley, 2010, 753 s., ISBN 978-0-470-42413-1.

[3] ŠALÁT T., HAVIAR A., HECHT T., KATRIŇÁK T., *Algebra a teoretická aritmetika 2*, Bratislava, Alfa, 1986.

[4] ŠKARKOVÁ J., *Diplomová práce-Algoritmus AKS*, Brno, 2010.

[5] KOLIBIAR M., LÉGEŇ A., ŠALÁT T., ZNÁM Š., *Algebra a príbuzné disciplíny*, Bratislava, Alfa, 1992.

[6] ZNÁM Š., *Teória čísel*, Bratislava, Alfa, 1986.

A Prílohy na CD

Priložené CD obsahuje tieto matlabovské a mapleovské funkcie:

- `eratosthenovo_sito.m` - implementácia Eratosthenovho sita v Matlabe
- `eratosthenovosito.mw` - implementácia Eratosthenovho sita v Maple
- `fermat_test.m` - implementácia Fermatovho testu prvočíselnosti v Matlabe
- `fermat.mw` - implementácia Fermatovho testu prvočíselnosti v Maple
- `miller_rabin_test.m` - implementácia Miller-Rabinovho testu prvočíselnosti v Matlabe
- `millerrabin.mw` - implementácia Miller-Rabinovho testu prvočíselnosti v Maple
- `aks.mw` - implementácia AKS testu prvočíselnosti v Maple