UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

Verjetnostni algoritmi za testiranje praštevilskosti

(Algorithms for testing primality)

Ime in priimek: Tjaša Jogan
Študijski program: Matematika
Mentor: izr. prof. dr. Štefko Miklavič

Koper, avgust 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Tjaša JOGAN

Naslov zaključne naloge: Verjetnostni algoritmi za testiranje praštevilskosti

Kraj: Koper

Leto: 2014

Število listov: 40 Število slik: 1 Število referenc: 9

Mentor: izr. prof. dr. Štefko Miklavič

Ključne besede: praštevila, aritmetične funkcije, kongruence, Fermatov algoritem, Miller-Rabinov algoritem, Lucasov algoritem.

Math. Subj. Class. (2010): 11A05, 11A07, 11A25, 11A41, 11A51.

Izvleček:
V zaključni nalogi z naslovom Verjetnostni algoritmi za testiranje praštevilskosti si bomo ogledali princip delovanja a verjetnostnih algoritmov. Pomembni so pri odkrivanju velikih praštevil, saj do dokaj hitri in natančni.
Najprej se bomo posvetili pravilom o deljivosti števil ter Evklidovemu algoritmu, s katerim običajno poiščemo največji skupni delitelj. Preusmerili bomo pozornost na praštevila in osnovni izrek aritmetike. Pokazali bomo tudi dva enostavna algoritma za preverjanje praštevilskosti pri majhnih številih. Nadaljevali bomo z aritmetičnimi funkcijami in sicer bomo opisali Funkciji σ in τ ter Eulerjevo funkcijo. Omenimo še lastnosti kongruence števil in dokažemo Wilsonov izrek, Eulerjev izrek ter Fermatov izrek, kateri so potrebni za obravnavo verjetnostnih algoritmov. Obravnavali bomo delovanje Fermatovega algoritma, Miller-Rabinovega algoritma ter Lucasovega algoritma. Obogateni so s številnimi primeri za lažje razumevanje.

Key words documentation

Name and SURNAME: Tjaša JOGAN

Title of final project paper:

Place: Koper

Year: 2014

Number of pages: 40 Number of figures: 1 Number of references: 9

Mentor: Assoc. Prof. Štefko Miklavič, PhD

Keywords: prime numbers, aritmetic functions, kongruence, Fermat primality test, Miller-Rabin primality test, Lucas primality test.

Math. Subj. Class. (2010): 11A05, 11A07, 11A25, 11A41, 11A51.

Abstract:
In this thesis we will focus on some probabilistic algorithms for testing primality. They have a primary role in the discovery of large prime numbers, due to their strong efficiency and relatively rapid calculation. In the introduction we present some basic concepts of number theory: the divisibility of numbers, the greatest common factor, the Euclidean algorithm, the prime numbers, the fundamental theorem of arithmetic and the congruences. Further on we present two elementary algorithms for testing primality, which are timely efficient only for relatively small numbers. We introduce the arithmetic functions, namely the functions σ and τ, and the Euler function. We discuss and prove the Wilson theorem, the Euler theorem and the Fermat theorem, which will be of great importance in the definition of the probabilistic algorithms. In the main part of the thesis we present and analyze the Fermat algorithm, the Miller-Rabin algorithm and the Lucas algorithm. In the thesis we use a lot of examples in order to facilitate the understanding of the topics.

Zahvala

Zahvaljujem se mentorju izr. prof. dr. Štefku Miklaviču za strokovno svetovanje in usmerjanje pri nastajanju zaključne naloge.

Hvala Marini in Sanji za skupno učenje, tolaženje ob neuspehih in veselje ob uspešno opravljenih izpitih ter vsem ostalim sošolcem, ki so mi kadarkoli priskočili na pomoč.

Zahvala gre tudi staršema, ki sta mi omogočila študij, me vzpodbujala in podpirala tudi, ko sem bila na robu obupa.

Posebna zahvala pa gre sošolcu in fantu Eriku, s katerim sva se s skupnimi močmi prebijala skozi vsa leta študija in prišla do želenega cilja. Diplomirala sva.

Hvala!

Kazalo vsebine

Kazalo slik

1 Uvod

"Noben drug del teorije števil ni tako nasičen s skrivnostmi in eleganco kot preučevanje praštevil, teh neukrotljivih števil, ki nas tako razburjajo in se nočejo brez ostanka deliti z nobenim celim številom, razen s samim seboj in z enko."

(M. Gardner)

Čeprav je definicija praštevila enostavna in vsakomur razumljiva, je presenetljivo veliko vprašanj v zvezi z njimi še vedno odprtih. Uporaba praštevil je zelo raznolika. Prvotno so jih preučevali, ker se veliko matematičnih problemov nanaša na faktorizacijo števil. Danes so praštevila ključnega pomena na področju kriptografije. Uporabljajo se za različne metode šifriranja, da transakcije varno tečejo.

Praštevila so pritegnila pozornost številnih matematikov skozi več stoletij. Spraševali so se, koliko jih je? Ali obstaja formula, s katerimi jih lahko generiramo?

Že antični Grki so vedeli, da je praštevil neskončno mnogo. Kljub temu pa prav velikih praštevil niso poznali. Ukvarjali so se s preprosto nalogo, kot je ugotoviti, ali je dano naravno število praštevilo. Najstarejši in najbolj preprost poznan algoritem je Eratostenovo rešeto iz leta 240 p.n.š. Naslednji preprost praštevilski test je ta, da število n po vrsti delimo s praštevili od 2 do p, kjer je p največje praštevilo, ki ne presega $\sqrt{n}$. Oba algoritma sta primerna za majhna števila, saj sta zelo zamudna in pri velikih številih praktično neuporabna.

Po letu 1960, zaradi prihoda računalnikov, ni več poudarka na iskanju matematične formule, ki bi dajala praštevila, ampak na iskanju učinkovitega algoritma za razpoznavanje praštevil. Težavo predstavlja prepoznavanje velikih praštevil, ki jih potrebujemo pri asimetričnem šifriranju sporočil. Najbolj znan asimetrični sistem je RSA [8], ki pri šifriranju sporočil temelji na zasebnem in javnem ključu. Za kreiranje ključev pa potrebujemo velika praštevila, ki jih ni enostavno dobiti. Zato potrebujemo učinkovit algoritem, s katerim preverimo ali je dano število praštevilo ali ne.

V praksi se največ uporablja verjetnostne algoritme, saj so do sedaj najhitrejši pri iskanju velikih praštevil. Verjetnostni algoritmi se lahko včasih tudi zmotijo in kakšno število razglasijo za praštevilo, čeprav je v resnici sestavljeno. Ker pa je verjetnost napake izredno majhna (veliko manjša od verjetnosti glavnega dobitka na loteriji), so ti algoritmi za potrebe kriptografije zaenkrat povsem ustrezni.

2 Osnovni pojmi teorije števil

Najprej si bomo pogledali nekaj osnovnih pojmov teorije števil, praštevila in najosnovnejše praštevilske algoritme, ki jih lahko najdemo v literaturi [1].

2.1 O deljivosti števil

Definicija 2.1. Naj bosta a in b poljubni celi števili. Število a je deljivo s številom b, če lahko a enolično zapišemo kot produkt števila b s celim številom k, torej v obliki

$$a = k \cdot b.$$

V tem primeru je b delitelj števila a in a večkratnik števila b. Seveda je tudi k delitelj a-ja in a večkratnik od k. Dejstvo, da je število a deljivo z b ali da b deli a, zapišemo $b|a$. Če b ne deli a, pa zapišemo $a \nmid b$.

Opomba 2.2. Število 0 je deljivo z vsakim od 0 različnim celim številom b ($0 = 0 \cdot b$). Število 0 ne deli nobenega neničelnega celega števila.

Izrek 2.3. *Naj bodo a, b in c poljubna cela števila. Potem velja:*

1. $a|a$
2. *če* $b|a$ *in* $a|b$, *potem je* $b = a$ *ali* $b = -a$
3. *če* $c|b$ *in* $b|a$, *potem* $c|a$
4. *če* $c|a$ *in* $c|b$, *potem* $c|ma + nb$ *; za poljubne* $m, n \in \mathbb{Z}$

Dokaz.

1. Ker je $a = 1 \cdot a$ sledi, da $a|a$.
2. Iz definicije deljivosti sledi, da obstajata taka $k, k_1 \in \mathbb{Z}$, za katera je $a = kb$ in $b = k_1 a$. Iz enakosti $a = bk = kk_1 a$ sledi, da je $a = kk_1 a$. Torej je $kk_1 = 1$. Ker sta $k, k_1 \in \mathbb{Z}$, obstajata dve možnosti: ali je $k = 1$ in $k_1 = 1$ ali $k = -1$ in $k_1 = -1$.

3. Iz definicije deljivosti izpeljemo dve posledici. Ker $b|a$ obstaja tak $k \in \mathbb{Z}$, da $a = kb$ in ker $c|b$ obstaja tak $k_1 \in \mathbb{Z}$, da $b = k_1 c$.
   Dokažimo, da $c|a$. Ker je

$$a = kb = k(k_1 c) = (kk_1)c$$

   sledi, da je število a izraženo s produktom $kk_1 \in \mathbb{Z}$ in c, torej $c|a$.

4. Denimo, da $c|a$ in $c|b$. Zato obstajata taka $k, k_1 \in \mathbb{Z}$, da je $a = kc$ in $b = k_1 c$. Potem za $\forall m, n \in \mathbb{Z}$ velja: $ma + nb = mkc + nk_1 c = (mk + nk_1)c$. Ker je $(mk + nk_1) \in \mathbb{Z}$ sledi, da $c|ma + nb$.

   Opomba 2.4. Celemu številu $ma + nb$ pravimo *cela linearna kombinacija* števil a, b.

□

Izrek 2.5. ***(Lema o deljenju)*** *Naj bosta $a, b \in \mathbb{Z}$ in $b \neq 0$. Potem obstajata enolično določena $q, r \in \mathbb{Z}$ tako, da velja*

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Dokaz. Najprej bomo dokazali, da q in r sploh obstajata in nato, da sta q in r enolično določena. Naj bo množica $A = \{a - bk; k \in \mathbb{Z} \text{ in } a - bk \geq 0\}$. Dokažimo, da je množica A neprazna, to bo natanko tedaj, ko bo obstajal vsaj en element v tej množici. Pokažimo torej, da obstaja tak $k \in \mathbb{Z}$, da velja: $-bk \geq -a$ in pri tem ločimo dve možnosti:

1. Če $-b \in \mathbb{N}$, potem obstaja tak $k \in \mathbb{N}$, da velja $-bk \geq |a| \geq -a$.

2. Če $b \in \mathbb{N}$, potem obstaja tak $k \in \mathbb{N}$, da velja: $bk \geq |a| \geq -a$. Od tod sledi, da $(-b)(-k) \geq -a$.

Torej množica A ni prazna in $A \subseteq \{0, 1, 2, \ldots\}$. Po principu dobre urejenosti sledi, da A vsebuje najmanjši element $r = min(A)$. Ker je $r \in A$, obstaja tak $q \in \mathbb{Z}$, da je $r = a - bq$, oziroma $a = bq + r$. Iz tega sledi, da je $r \geq 0$. Pokažimo še, da je $r < |b|$. Dokaz bomo naredili za primer, ko je $b > 0$. Recimo, da je $r \geq |b|$, $b \in \mathbb{N}$. Potem je $a - (q + 1)b = a - qb - b = r - b \geq 0$.Vidimo, da je $a - (q + 1)b \in A$. Ker je $a - (q + 1)b = r - b < r$, pridemo v protislovje, saj smo zgoraj definirali, da je $r = min(A)$. Podobno velja za $b < 0$. Torej je $r < |b|$.
Sedaj dokažimo še, da velja enoličnost izraza $a = qb + r, 0 \leq r < |b|$. Enoličnost tega izraza pomeni, da imamo pri danih a, b en sam tak par q, r da velja
$a = qb + r, 0 \leq r < |b|$.

Recimo, da obstaja tak par k_1, r_1, da je $a = k_1 b + r_1$ in $0 \leq r_1 < |b|$. Tedaj je $kb + r = k_1 b + r_1$ ali $(k - k_1)b = r_1 - r$ in je torej $r_1 - r$ večkratnik b-ja. Ker je $0 \leq r_1 < |b|, -|b| < -r \leq 0$, sledi da $-|b| < r_1 - r < |b|$. Edini večkratnik b-ja med $-|b|$ in $|b|$ je 0. Zato je $r_1 - r = 0$ in $r_1 = r$. Tako smo dobili $(k - k_1)b = r_1 - r = 0$ in zaradi $b \neq 0$ je $k - k_1 = 0$, torej $k_1 = k$. Dokazali smo enoličnost izraza. □

Definicija 2.6. Naj bosta a in b poljubni celi števili. Tedaj največje naravno število, ki deli tako a kot b, označimo z $D(a, b)$ in ga imenujemo **največji skupni delitelj** števil a in b.

Primer 2.7. Poiščimo največji skupni delitelj števil 20 in 24.

- število 20 ima delitelje: $1, 2, 4, 5, 10, 20$;
- število 24 ima delitelje: $1, 2, 3, 4, 6, 8, 12, 24$;
- skupni delitelji so $1, 2, 4$;
- največji skupni delitelj je 4, kar zapišemo kot $D(20, 24) = 4$

Definicija 2.8. Celi števili a in b sta **tuji**, če velja $D(a, b) = 1$.

Največji skupni delitelj dveh števil običajno poiščemo s pomočjo **Evklidovega algoritma**, ki ga bomo sedaj opisali.

Vzemimo dve neničelni celi števili a in b, denimo da $|a| > |b|$. Zaradi Izreka 2.4. lahko pišemo $a = kb + r, 0 \leq r < b$. Po 5. točki v Izreku 2.3 velja, da vsak skupni delitelj števil b, r deli a in skupni delitelj para a, b je delitelj za r, saj je $r = a - kb$. Par a, b ima iste delitelje kot par b, r. Zato je tudi njun največji skupni delitelj enak $D(a, b) = D(b, r)$.

- če je $r = 0$, je $D(a, b) = D(b, 0) = b$ in je največji skupni delitelj dobljen,
- če je $r \neq 0$, velja $0 < r < b$ in dobimo

$$b = k_1 r + r_1, \qquad 0 \leq r_1 < r.$$

  Kot prej dokažemo, da se skupni delitelji para b, r ujemajo s skupnimi delitelji para r, r_1 zato

$$D(b, r) = D(r, r_1).$$

  Torej velja: $D(a, b) = D(b, r) = D(r, r_1)$

- če je $r_1 = 0$, je $D(a, b) = D(r, 0) = r$,

- če je $r \neq 0$, velja $0 < r_1 < r$ in ravnanje ponovimo z r in r_1. Za novi ostanek r_2 sledi po Izreku 2.4 ocena $0 \leq r_2 < r_1$. Ker se po ocenah $0 \leq r_2 < r_1 < r < b$ ostanki manjšajo in so nenegativna cela števila, moramo po nekaj ponovitvah priti do ostanka 0. Manjka nam še nekaj podobnih enačb in dobimo

$$\begin{aligned} a &= kb + r, & 0 < r < b \\ b &= k_1 r + r_2, & 0 < r_1 < r \\ r &= k_2 r_1 + r_2, & 0 < r_2 < r_1 \\ &\vdots & \vdots \\ r_{n-2} &= k_n r_n - 1 + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= k_n + 1 r_n + 0 \end{aligned}$$

Od tod vidimo, da imajo pari a, b; b, r; r, r_1; $\ldots$; r_{n-1}, r_n; $r_n, 0$ iste skupne delitelje, zato se njihovi največji skupni delitelji ujemajo:

$$D(a, b) = D(b, r) = \ldots = D(r_{n-1}, r_n) = D(r_n, 0) = r_n.$$

$D(a, b)$ je torej kar zadnji od 0 različen ostanek, ki ga dobimo po reševanju zgornjih enačb. Tako z Evklidovim algoritmom določimo največji skupni delitelj dveh števil.

Opomba 2.9. Izrek velja, ko nobeno od obeh števil ni enako 0. Če je eno število 0, drugo ne, je $(a, 0) = |a|$ pri $a \neq 0$. Če sta obe števili enaki 0, $D(a, b)$ ne obstaja.

Primer 2.10. Z Evklidovim algoritmom poiščimo največji skupni delitelj števil 754 in 312.

$$\begin{aligned} 754 &= 2 \cdot 312 + 130 \\ 312 &= 2 \cdot 130 + 52 \\ 130 &= 2 \cdot 52 + 26 \\ 52 &= 2 \cdot 26 + 0 \\ D(754, 312) &= 26 \end{aligned}$$

Izrek 2.11. *Če je $d = D(a, b)$, potem obstajata celi števili m in n tako, da je $d = ma + nb$.*

Dokaz. Zapišemo enačbe iz prejšnjega dokaza v obliki:

$$\begin{aligned} r &= a - kb \\ r_1 &= b - k_1 r \\ &\vdots \\ r_n &= r_{n-2} - k_n r_{n-1}. \end{aligned}$$

Prva enačba pove, da je r cela linearna kombinacija števil a, b. Če vnesemo izraz za r v drugo enačbo dobimo:

$$r_1 = -k_1 a + (1 + kk_1)b.$$

Torej je tudi r_1 cela linearna kombinacija števil a, b. Vnesemo izraz za r in r_1 v tretjo enačbo in dobimo:

$$r_2 = (1 + k_1k_2)a + (-k - k_2 - kk_1k_2)b.$$

Tudi r_2 je cela linearna kombinacija števil a, b. Če nadaljujemo pridemo do zadnje enačbe, kjer bo tudi r_n dobljen kot cela linearna kombinacija števil a, b, to je

$$r_n = ma + nb.$$

□

Posledica 2.12. *$D(a, b) = 1$ natanko tedaj, ko obstajata taka $m, n \in \mathbb{Z}$, da velja $1 = ma + nb$.*

Posledica 2.13. ***(Evklidova lema)*** *Če $a|bc$ in $D(a, b) = 1$, potem $a|c$.*

Dokaz. Ker $a|bc$, obstaja tak $k \in \mathbb{Z}$, da je $bc = ak$. Po Izreku 2.11. je $1 = ma + nb$ za neka $m, n \in \mathbb{Z}$. To enačbo pomnožimo s c in dobimo:

$$c = cma + cnb = a(cm + kn).$$

Od tod sledi, da $a|c$. □

Definicija 2.14. Naj bosta a in b celi števili. Najmanjše naravno število, ki je deljivo tako z a kot z b, imenujemo **najmanjši skupni večkratnik** števil a in b. 0značimo ga z $v(a, b)$.

Primer 2.15. Poišči najmanjši skupni večkratnik števil 5 in 6.

- večkratniki števila 5: $5, 10, 15, 20, 30, 35, 40, 45,$ ...
- večkratniki števila 6: $6, 12, 16, 24, 30, 36, 42,$ ...
- najmanjši skupni večkratnik je 30: $v(6, 5) = 30$.

2.2 Praštevila in osnovni izrek aritmetike

Definicija 2.16. Naravno število $p > 1$ je **praštevilo**, če ima število p natanko dva pozitivna delitelja, število 1 in p.

Primer 2.17. Do števila 23 je devet praštevil in sicer

$$2, 3, 5, 7, 11, 13, 17, 19, 23.$$

Definicija 2.18. Naravno število, ki ni praštevilo in je večje od 1, imenujemo **sestavljeno število**.

Primer 2.19. Števila $6 = 2 \cdot 3$, $10 = 2 \cdot 5$, $25 = 5 \cdot 5$ so sestavljena števila.
Tudi 0 je sestavljeno število, saj je npr. $0 = 0 \cdot 3 \cdot 4$.

Izrek 2.20. *Če je p praštevilo in $p|ab$, potem $p|a$ ali $p|b$.*

Dokaz. Recimo, da $p|ab$.
Predpostavimo, da $p \nmid a$. Potem moremo dokazati, da $p|b$.
Ker $p \nmid a$, je $D(p, a) = 1$ in po Evklidovi lemi sledi, da $p|b$. □

Izrek 2.21. *Vsako naravno število, ki je večje od 1, je deljivo vsaj z enim preštevilom.*

Dokaz. Naj bo a poljubno naravno število. Če je a praštevilo, potem izrek velja, saj $a|a$.
Če pa je a sestavljeno število, ima poleg 1 in a še druge delitelje. Pokažimo, da je vsaj eden izmed teh deliteljev praštevilo. Naj bo q najmanjši med temi drugimi delitelji tako, da je $1 < q < a$. Trdimo, da je q praštevilo. Če q ni praštevilo, ga lahko zapišemo kot $q = km$, kjer $k, m \in \mathbb{N}$ in $k > 1$ in $m > 1$. Sledi, da je $1 < k < km = q$. Število k leži med 1 in q in deli q, zato deli tudi a. Tako pridemo v protislovje, saj smo rekli, da je q najmanjši od 1 različni delitelj a. Vidimo, da je q praštevilo. □

Izrek 2.22. ***(Osnovni izrek aritmetike)*** *Vsako naravno število, ki je večje od 1, je razcepljivo v produkt praštevil. Če se na vrstni red faktorjev ne oziramo, je razcepitev ena sama.*

Dokaz. Najprej dokažimo prvi del izreka.
Naj bo a naravno število, $a > 1$. Po Izreku 2.21 obstaja vsaj eno praštevilo p_1, ki deli a, zato lahko pišemo $a = p_1 n_1$. Če je $n_1 = 1$, je $a = p_1$ iskana razcepitev. Če $n_1 \neq 1$, po Izreku 2.21 obstaja praštevilo p_2, ki deli n_1 in je $n_1 = n_2 p_2$. Pri $n_2 = 1$, je $a = p_1 p_2$ iskana razcepitev. Če $n_2 \neq 1$ spet sledi obstoj praštevila p_3, ki je delitelj za n_2. Vrednosti števila a, n_1, n_2 padajo $a > n_1 > n_2$. Ko tako nadaljujemo, moramo priti do števila n_k, za katero je $n_{k+1} = 1$ in njegova razcepitev je $n_k = p_k$, kjer je p_k praštevilo. Če upoštevamo vse zgornje korake dobimo a v obliki

$$a = p_1 p_2 \cdots p_k.$$

Dobili smo razcepitev števila a v produkt praštevil.
Dokazati moramo še enoličnost faktorizacije.

Naj bo $n \in \mathbb{N}$ in $n > 1$. Recimo, da $n = p_1 p_2 \cdots p_k = q_1 \cdots q_m$, kjer so $p_1, \ldots, p_k$, $q_1, \ldots, q_m$ praštevila in velja $p_1 \leq p_2 \leq \ldots \leq p_k$ in $q_1 \leq q_2 \leq \ldots \leq q_m$. Recimo, da $k \leq m$. Ker $p_1 | q_1 q_2 \ldots q_m$, obstaja tak $1 \leq i \leq m$, da velja: $p_1 = q_i$. Sledi, da $p_1 \geq q_1$. Tako lahko ugotovimo, da tudi $q_1 \geq p_1$. Torej $p_1 = q_1$ in velja $p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m$. Postopek ponavljamo. Če bi bil $k > m$, bi po k-korakih dobili: $1 = q_{k+1} q_{k+2} \cdots q_m > 1$, kar je protislovje. Torej če je $k = m$ sledi, da $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_m$. □

Posledica 2.23. *Če so $p_1, p_2 \ldots, p_j$ vsa različna praštevila iz razcepitve in povedo naravna števila $n_1, n_2, \ldots, n_j$, kolikokrat so praštevila $p_1, p_2, \ldots, p_j$ v razcepitvi kot faktorji, lahko vsako naravno število $a > 1$ zapišemo kot $a = p_1^{n_1} \cdot p_2^{n_2} \cdots p_j^{n_j}$,*
$p_1 < p_2 < \ldots < p_j$.

Temu zapisu pravimo **kanonična izrazitev** števila a na prafaktorje.

Trditev 2.24. *(Evklid) Praštevil je neskončno.*

Dokaz. Predpostavimo, da je praštevil končno mnogo. Lahko jih zapišemo v zaporedju $2, 3, 5, \ldots, p$, kjer je p največje praštevilo. Če ta praštevila zmnožimo, dobimo produkt $2 \cdot 3 \cdot 5 \cdots p$, ki je deljiv s praštevili $2, 3, 5, \ldots, p$. Število $n = (2 \cdot 3 \cdots p) + 1$ je celo in večje od p, ki ni deljivo z nobenim od praštevil $2, 3, 5, \ldots, p$, saj nam pušča pri deljenju z vsakim od praštevil $2, 3, \ldots, p$ ostanek 1. Pri deljenju z vsakim praštevilom med 2 in p imamo dve možnosti: ali je n deljiv s katerim drugim praštevilom, ali je n praštevilo. Praštevilo, s katerim je n deljiv, je torej večje od p in tako p ni največje praštevilo. Če pa je n praštevilo, zaradi $n > p$ pa spet p ni največje praštevilo. Tako vidimo, da največjega praštevila ni. □

Ugotovili smo, da je praštevil neskončno, kako pa ugotovimo ali je neko naravno število n praštevilo ali sestavljeno število? Z uporabo praštevilskih testov lahko pridemo do rezultata. Najosnovnejši praštevilski test za preverjanje, ali je neko naravno število n praštevilo je ta, da preverimo deljivost s praštevili, ki so manjši ali enaki $\sqrt{n}$, saj velja:

Trditev 2.25. *Če je n sestavljeno število, potem obstaja tako praštevilo p, da $p|n$ in $p \leq \sqrt{n}$.*

Dokaz. Ker je n sestavljeno število, lahko pišemo $n = ab$, kjer za a in b velja $1 < a \leq b < n$. Če $a \leq b$ pomnožimo z a in dobimo $a^2 \leq ba$, sledi $a \leq \sqrt{n}$. Po osnovnem izreku aritmetike obstaja tako praštevilo p, da $p|a$. Ker $p|a$ in $a|n$, po 3. točki v Izreku 3.2 velja, da $p|n$. Ker je $p \leq a$ in $a \leq \sqrt{n}$ je tudi $p \leq \sqrt{n}$. □

Primer 2.26. Preverimo, ali je število 89 praštevilo ali sestavljeno število.
$\sqrt{89} = 9,433 \ldots$

$9 < \sqrt{89} < 10$
Če je število 89 deljivo s katerim od praštevil $2, 3, 5, 7$, je to število sestavljeno. Ker pa opazimo, da ni deljivo z nobenim od števil $2, 3, 5, 7$, je število 89 praštevilo.

Imamo še en preprost algoritem za iskanje praštevil in sicer Eretostenovo rešeto. Ta algoritem uporablja Trditev 2.25 za osnovno metodo, ki poišče vsa praštevila, manjša od izbranega števila.

Primer 2.27. Poiščimo vsa praštevila, ki so manjša od 100.
$n = 100$
$\sqrt{100} = 10$

- zapišemo vsa števila od 1 do n
- prečrtamo število 1
- vzamemo prvo neprečrtano število in prečrtamo vse njegove večkratnike. Postopek ponavljamo, dokler ne pridemo do števila $\sqrt{n}$
- vsa neprečrtana števila so praštevila

~~1~~	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~~

Slika 1: Eratostenovo rešeto.

3 Aritmetične funkcije

V tem poglavju bomo navedli nekaj definicij o aritmetičnih funkcijah ter tri aritmetične funkcije podrobneje opisali in predstavili na primerih. Naslednje definicije in izreke najdemo v [1–3].

Definicija 3.1. Aritmetična funkcija je funkcija f, ki slika iz množice naravnih števil v množico kompleksnih števil:

$$f : \mathbb{N} \to \mathbb{C}.$$

Definicija 3.2. Aritmetična funkcija $f : \mathbb{N} \to \mathbb{C}$ je multiplikativna, če za poljubni tuji naravni števili m in n velja:

$$f(m \cdot n) = f(m) \cdot f(n),$$

ter popolnoma multiplikativna, če za poljubni naravni števili m in n velja

$$f(m \cdot n) = f(m) \cdot f(n).$$

Primer 3.3. Funkcija $f(n) = 1$, za $\forall n \in \mathbb{N}$, je popolnoma multiplikativna, saj $f(mn) = 1 \cdot 1 = f(m)f(n)$. Podobno velja za funkcijo $g(n) = n$: je popolnoma multiplikativna, saj $g(mn) = m \cdot n = g(m)g(n)$.

Izrek 3.4. *Naj bo f multiplikativna funkcija. Če je $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ kanonična izrazitev naravnega števila n, kjer so $p_1, p_2, \ldots, p_k$ različna praštevila in $a_1, a_2, \ldots, a_k$ naravna števila, potem velja:*

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \ldots f(p_k^{a_k}).$$

Dokaz. Izrek bomo dokazali z uporabo matematične indukcije po številu k v kanonični izrazitvi števila n. Vzemimo, da je $k = 2$. Ker je $D(p_1^{a_1}, p_2^{a_2}) = 1$ in ker je f multiplikativna je $f(n) = f(p_1^{a_1} p_2^{a_2}) = f(p_1^{a_1}) f(p_2^{a_2})$. Predpostavimo, da izrek drži za vsa naravna števila manjša ali enaka k.
Naj bo sedaj n poljubno naravno število, ki ima $k+1$ različnih praštevil v svojem kanonični izrazitvi. Recimo, da $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}}$. Ker je funkcija f multiplikativna in $D(p_1^{a_1} \cdots p_k^{a_k}, p_{k+1}^{a_{k+1}}) = 1$ je $f(n) = f(p_1^{a_1} \cdots p_k^{a_k}) f(p_{k+1}^{a_{k+1}})$. Po indukcijski predpostavki vemo, da $f(p_1^{a_1} \cdots p_k^{a_k}) = f(p_1^{a_1}) \cdots f(p_k^{a_k})$, zato lahko zapišemo, da tudi $f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k}) f(p_{k+1}^{a_{k+1}})$. □

3.1 Funkciji σ in τ

Definicija 3.5. Naj bo n poljubno naravno število. Funkcijo $\sigma : \mathbb{N} \to \mathbb{N}$ definiramo takole:

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

$\sigma(n)$ je torej vsota vseh pozitivnih deliteljev števila n.

Primer 3.6. Vrednosti $\sigma(n)$ za prvih dvanajst naravnih števil.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28

Definicija 3.7. Naj bo n poljubno naravno število. Funkcijo $\tau : \mathbb{N} \to \mathbb{N}$ definiramo takole:

$$\tau(n) = \sum_{d|n} 1.$$

$\tau(n)$ je torej število vseh pozitivnih deliteljev števila n.

Primer 3.8. Vrednosti $\tau(n)$ za prvih dvanajst naravnih števil.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

Če želimo dokazati, da sta funkciji σ in τ multiplikativni, potrebujemo naslednji izrek:

Izrek 3.9. *Če je f multiplikativna funkcija, potem je multiplikativna tudi funkcija F podana s predpisom*

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

Poglejmo si najprej idejo, da bomo lažje dokazali izrek.
IDEJA: Naj bo f multiplikativna funkcija in $F(n) = \sum_{d|n} f(d)$. Pokazali bomo, da $F(60) = F(4)F(15)$. Delitelje števila 60 lahko zapišemo kot produkt delitelja števila 4 in delitelja števila 15: $1 = 1 \cdot 1, 2 = 2 \cdot 1, 3 = 1 \cdot 3, 4 = 4 \cdot 1, 5 = 1 \cdot 5, 6 = 2 \cdot 3, 10 = 2 \cdot 5, 12 = 4 \cdot 3, 15 = 1 \cdot 15, 20 = 4 \cdot 5, 30 = 2 \cdot 15, 60 = 4 \cdot 15$.
Torej:

$$\begin{aligned} F(60) = {} & f(1) + f(2) + f(3) + f(4) + f(5) + f(6) + f(10) + f(12) + f(15) + \\ & f(20) + f(30) + f(60) = \\ = {} & f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(1 \cdot 5) + f(2 \cdot 3) + f(2 \cdot 5) + \\ & f(2 \cdot 3) + f(1 \cdot 15) + f(4 \cdot 5) + f(2 \cdot 15) + f(4 \cdot 15) = \end{aligned}$$

$$= f(1)f(2)+f(2)f(1)+f(1)f(3)+f(4)f(1)+\ldots+f(2)f(15)+f(4)f(15) =$$
$$= (f(1)+f(2)+f(4))(f(1)+f(3)+f(5)+f(15)) =$$
$$= F(4)F(15).$$

Dokaz. Če želimo pokazati, da je F multiplikativna funkcija, moramo pokazati, da za poljubni tuji naravni števili m in n velja $F(mn) = F(m)F(n)$.
Predpostavimo, da $D(m,n) = 1$. Sledi

$$F(mn) = \sum_{d|mn} f(d).$$

Ker je $D(m,n) = 1$, $d|mn$ natanko tedaj, ko obstajata naravni števili d_1, d_2 in velja: $d = d_1 \cdot d_2$, $d_1|m, d_2|n$ in $D(d_1,d_2) = 1$. Lahko pišemo:

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

Ker je f multiplikativna funkcija in $D(d_1,d_2) = 1$, vidimo da

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

□

Posledica 3.10. *Funkciji σ in τ sta multiplikativni funkciji.*

Dokaz. Naj bo $f(n) = n$ in $g(n) = 1$. Funkciji f in g sta multiplikativni, zato po Izreku 3.9 vidimo, da sta $\sigma(n) = \sum_{d|n} f(d)$ in $\tau(n) = \sum_{d|n} g(d)$ multiplikativni. □

Sedaj ko vemo, da sta σ in τ multiplikativni, lahko izpeljemo formuli za njune vrednosti na podlagi kanonične izrazitve. Najprej bomo zapisali formuli za $\sigma(n)$ in $\tau(n)$, ko je n potenca praštevila.

Lema 3.11. *Naj bo p praštevilo in a naravno število. Potem je*

$$\sigma(p^a) = 1 + p + p^2 + \ldots + p^a = \frac{p^{a+1}-1}{p-1}$$

in

$$\tau(p^a) = a + 1.$$

Dokaz. Delitelji praštevila p^a so: $1, p, p^2, \ldots, p^{a-1}, p^a$. Takoj lahko vidimo, da ima p^a točno $a+1$ deliteljev, zato je $\tau(p^a) = a+1$.
Opazimo tudi, da je $\sigma(p^a) = 1 + p + p^2 + \ldots + p^a = \frac{p^{a+1}-1}{p-1}$.

□

Primer 3.12. Vzemimo $p = 5$ in $a = 3$.

$$\sigma(5^3) = 1 + 5 + 5^2 + 5^3 = \tfrac{5^4-1}{5-1} = 156$$
$$\tau(5^3) = 1 + 3 = 4$$

Izrek 3.13. *Naj bo n naravno število s kanonično izrazitvijo $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. Potem je*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_s^{a_s+1} - 1}{p_s - 1} = \prod_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

in

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_s + 1) = \prod_{j=1}^{s} (a_j + 1).$$

Dokaz. Ker sta funkciji σ in τ multiplikativni, velja
$\sigma(n) = \sigma(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = \sigma(p_1^{a_1})\sigma(p_2^{a_2}) \cdots \sigma(p_s^{a_s})$ in
$\tau(n) = \tau(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = \tau(p_1^{a_1})\tau(p_2^{a_2}) \cdots \tau(p_s^{a_s})$.
Ko vstavimo vrednosti iz Leme 3.11 dobimo željene formule. □

Primer 3.14. Vzemimo za $n = 200$. $200 = 2^3 \cdot 5^2$, torej

$$\sigma(200) = \sigma(2^3 \cdot 5^2) = \tfrac{2^4-1}{2-1} \cdot \tfrac{5^3-1}{5-1} = 15 \cdot 31 = 465$$
$$\tau(200) = \tau(2^3 \cdot 5^2) = (3 + 1) \cdot (2 + 1) = 12$$

3.2 Eulerjeva funkcija

Definicija 3.15. Naj bo n poljubno naravno število. Funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ naj bo enaka številu vseh naravnih števil, ki so tuja z n in niso večja od n. Funkcijo φ imenujemo Eulerjeva funkcija in jo označimo z $\varphi(n)$.

Primer 3.16. Vrednosti $\varphi(n)$ za prvih dvanajst naravnih števil.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Izrek 3.17. *Naravno število p je praštevilo natanko tedaj, ko je $\varphi(p) = p - 1$.*

Dokaz. ($\Rightarrow$): Vzemimo, da je p praštevilo. Vsa števila $1, 2, 3, \ldots, p - 1$ so tuja številu p, zato je $\varphi(p) = p - 1$.
($\Leftarrow$): Vzemimo, da je p naravno število in $\varphi(p) = p - 1$.
Recimo, da p ni praštevilo. Potem je lahko $p = 1$ ali p je sestavljeno število. Če je $p = 1$, potem $\varphi(p) \neq p - 1$, ker $\varphi(1) = 1$. Če je p sestavljeno število, potem obstaja tak $d \in \mathbb{N}$, da $d|p$. Ker p in d nista tuji števili, obstaja med števili $1, 2, \ldots, p-1$ število d in $\varphi(p) < p - 1$. Zato, če je $\varphi(p) = p - 1$ je p praštevilo. □

Izrek 3.18. *Za potenco p^n praštevila p in naravnega števila n je*

$$\varphi(p^n) = p^n(1 - \frac{1}{p}).$$

Dokaz. Vsa naravna števila $p, 2p, 3p, \ldots, p^{n-1}p$ niso tuja s p. Teh je p^{n-1}. Vsa druga števila, ki jih je $p^n - p^{n-1}$, so tuja s p. Torej je $\varphi(p^n) = p^n(1 - \frac{1}{p})$. □

Primer 3.19. $\varphi(81) = \varphi(3^4) = 3^4(1 - \frac{1}{3}) = 3^3 \cdot 2 = 54$.

Izrek 3.20. *Funkcija φ je multiplikativna:*

$$\varphi(mn) = \varphi(m)\varphi(n),$$

kjer sta m in n tuji naravni števili.

Dokaz. Naj bo x produkt med sabo tujih naravnih števil m, n, torej $x = m \cdot n$. Denimo, da poznamo $\varphi(m)$ in $\varphi(n)$. Izračunati želimo $\varphi(x)$. Število $\varphi(x)$ pove koliko je v zaporedju $0, 1, 2, \ldots, x - 1$ proti x tujih števil. Zaporedje zapišimo v n vrstic tako, da pride v vsako vrstico m zaporednih števil

$$\begin{array}{rrrcr}
0 & 1 & 2 & \ldots & m-1 \\
m & m+1 & m+2 & \ldots & 2m-1 \\
2m & 2m+1 & 2m+2 & \ldots & 3m-1 \\
 & & & \vdots & \\
(n-1)m & (n-1)m+1 & (n-1)m+2 & \ldots & mn-1
\end{array}$$

V zgornji shemi so zaradi Evklidove leme tuja proti x tista števila, ki so tuja m in n. Opazimo tudi, če je kako število iz prve vrstice v shemi tuje m, so tuja proti m vsa tista števila, ki so z njim v istem stoplcu. Če pa je kako število iz prve vrstice v tej shemi netuje m, so vsa števila, ki so z njim v istem stolpcu, netuja m. Naj bo k število iz prve vrste, potem so z njim v istem stolpcu števila $tm + k$, kjer je t celo število. Če ima k skupen delitelj z m, ta delitelj po 4. točki v Izreku 2.3 deli tudi $tm+k$. Če pa je k tuj m, noben delitelj m-ja ne deli $tm+k$. Stolpci v shemi se torej glede tujosti nasproti številu m obnašajo tako kot njihova števila iz prve vrstice. Od tod lahko sklepamo, da je število stolpcev, ki vsebujejo vsa proti m tuja števila iz sheme natanko $\varphi(m)$.

Sedaj moramo še preveriti, koliko je v najdenih $\varphi(m)$ stolpcih tujih števil proti n. Vzemimo kakšnega teh $\varphi(m)$ stolpcev. Poljubni števili v tem stolpcu sta $tm + k$, $sm + k$, kjer sta t, s nenegativni celi števili, ne večji od $n - 1$. Če je $t \neq s$, $tm + k$ in $sm + k$ ne dasta pri delitvi z n istega ostanka. Če bi bil ostanek isti, bi bila razlika $(t - s)m$ deljiva z n. Ker je m tuj proti n, bi moral biti po Evklidovi lemi faktor $t - s$

deljiv z n. Toda zaradi $0 < |t - s| \leq n - 1$ je to nemogoče. Ko delimo števila našega stolpca z n, dobimo same različne ostanke. Ker je v stolpcu n števil, so ti ostanki enaki $0, 1, 2, \ldots, n - 1$. Med njimi je $\varphi(n)$ proti n tujih števil. Ker velja to za vsakega od $\varphi(n)$ stolpcev, je v shemi $\varphi(m)\varphi(n)$ števil, ki so tuja obenem proti m in proti n. Torej je $\varphi(x) = \varphi(m)\varphi(n)$ oziroma $\varphi(mn) = \varphi(m)\varphi(n)$. □

Izrek 3.21. *Če je $m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ kanonična izrazitev naravnega števila, kjer so $p_1, p_2, \ldots, p_k$ različna praštevila, potem*

$$\varphi(m) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Dokaz. Ker je φ multiplikativna in $m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ lahko pišemo $\varphi(m) = \varphi(p_1^{n_1})\varphi(p_2^{n_2}) \cdots \varphi(p_k^{n_k})$. Če upoštevamo Izrek 3.18 vemo, da $\varphi(p_j^{n_j}) = p_j^{n_j} - p_j^{n_j - 1} = p_j^{n_j}(1 - \frac{1}{p_j})$ za $j = 1, 2, \ldots, k$. Zato velja

$$\begin{aligned}\varphi(m) &= p_1^{n_1}(1 - \tfrac{1}{p_1}) p_2^{n_2}(1 - \tfrac{1}{p_2}) \cdots p_k^{n_k}(1 - \tfrac{1}{p_k}) = \\ &= p_1^{n_1} \cdots p_k^{n_k}(1 - \tfrac{1}{p_1}) \cdots (1 - \tfrac{1}{p_k}) = \\ &= m(1 - \tfrac{1}{p_1}) \cdots (1 - \tfrac{1}{p_k}).\end{aligned}$$

□

Primer 3.22. $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$

$$\varphi(2100) = 2100(1 - \tfrac{1}{2})(1 - \tfrac{1}{3})(1 - \tfrac{1}{5})(1 - \tfrac{1}{7}) = 480$$

Izrek 3.23. *Za naravno število m je vsota vrednosti, ki jih zavzame Eulerjeva funkcija pri vseh pozitivnih deliteljih d števila m enaka m in sicer:*

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

Dokaz. Najprej izpeljimo dokaz za primer, ko je m potenca praštevila p, torej $m = p^n$. Delitelji števila p^n so $1, p, p^2, \ldots, p^n$. Če upoštevamo Izreka 3.17 in 3.18 dobimo:

$$\begin{aligned}\sum_{d|p^n} \varphi(d) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^n) = \\ &= 1 + (p - 1) + (p^2 - p) + \ldots + (p^n - p^{n-1}) = \\ &= p^n.\end{aligned}$$

Za $m = p^n$ je izrek dokazan.
Obravnavati moramo še splošen primer. Število m naj ima razcepitev $m = p_1^{n_1} \cdots p_k^{n_k}$, kjer so $p_1, \ldots, p_k$ različna praštevila. Ker so delitelji števila m natanko vsa števila oblike $p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, pri čemer velja: $0 \leq r_i \leq n_i$ za vse $i = 1, 2, \ldots, k$, sledi

$$\begin{aligned}
\sum_{d|n} f(d) &= \sum_{r_1=0}^{n_1} \cdots \sum_{r_k=0}^{n_k} \varphi(p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}) = \\
&= \sum_{r_1=0}^{n_1} \cdots \sum_{r_k=0}^{n_k} \varphi(p_1^{r_1}) \cdots \varphi(p_k^{r_k}) = \\
&= \prod_{i=1}^{k} \sum_{r_i=0}^{n_i} \varphi(p_i^{r_i}) = \\
&= \prod_{i=1}^{k} p^{n_i} = \\
&= n.
\end{aligned}$$

□

4 Kongruence

Pogledali si bomo nekaj lastnosti kongruence števil in posebne kongruence: Wilsonov izrek, Eulerjev izrek in Fermatov izrek. Omenjeno najdemo v literaturi [2, 3].

4.1 Kongruenca števil

Definicija 4.1. Naj bodo a in b celi števili in m naravno število. Če $m|a-b$ potem pravimo, da sta a, b kongruentni po modulu m in pišemo

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

Opomba 4.2. Če $m \nmid a-b$ sta a, b nekongruentni po modulu m in pišemo $a \not\equiv b \pmod{m}$.

Primer 4.3. Primer kongruence števil.
$19 \equiv 7 \pmod{6}$, ker $6|19-7=12$
oziroma
$14 \not\equiv 4 \pmod{7}$, ker $7 \nmid 14-4=10$.

Izrek 4.4. *Naj bosta a in b poljubni celi števili. Potem je $a \equiv b \pmod{m}$ natanko tedaj, ko imata a in b enaka nenegativna ostanka pri deljenju z m.*

Dokaz. ($\Rightarrow$): Predpostavimo, da $a \equiv b \pmod{m}$ in $a = b + mk$ za nek $k \in \mathbb{Z}$. Pri deljenju z m naj ima b ostanek r: $b = qm + r$, kjer je $0 \leq r < m$. Zato je

$$a = b + km = (qm + r) + km = (q + k)m + r,$$

kar pomeni, da ima a pri deljenju z m enak ostanek kot b.
($\Leftarrow$): Sedaj predpostavimo, da sta $a = q_1 m + r$ in $b = q_2 m + r$ z enakima ostankoma r ($0 \leq r < m$). Potem

$$a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2)m.$$

Od tod sledi, da $m|a-b$ in lahko pišemo $a \equiv b \pmod{m}$. □

Izrek 4.5. *Naj bodo a, b, c, d poljubna cela števila in $m \in \mathbb{N}$.*
Potem veljajo naslednje lastnosti:

1. $a \equiv a \pmod{m}$.
2. *Če je* $a \equiv b \pmod{m}$, *potem je* $b \equiv a \pmod{m}$.
3. *Če je* $a \equiv b \pmod{m}$ *in* $b \equiv c \pmod{m}$, *potem je* $a \equiv c \pmod{m}$.
4. *Če je* $a \equiv b \pmod{m}$ *in* $c \equiv d \pmod{m}$, *potem je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ *in* $ac \equiv bd \pmod{m}$.
5. *Če je* $ad \equiv bd \pmod{m}$ *in je* $D(d, m) = 1$, *potem je* $a \equiv b \pmod{m}$.

Dokaz.

1. Ker $m|(a - a) = 0$ sledi, da je $a \equiv a \pmod{m}$.
2. Če $a \equiv b \pmod{m}$ potem $m|(a - b)$ in velja, da $a - b = km$ za $k \in \mathbb{Z}$. Torej $b - a = -(km) = (-k)m$ in zato $m|(b - a)$. Posledično $b \equiv a \pmod{m}$.
3. Če $a \equiv b \pmod{m}$ in $b \equiv c \pmod{m}$, potem $m|(a - b)$ in $m|(b - c)$. Vemo, da $m|(a - b) + (b - c) = a - c$. Iz tega sledi, da je $a \equiv c \pmod{m}$.
4. Če $a \equiv b \pmod{m}$ in $b \equiv d \pmod{m}$, potem $m|(a-b)$ in $m|(b-d)$. To pomeni, da $a - b = km$ in $c - d = hm$ za $k, h \in \mathbb{Z}$.
   Če naredimo vsoto, dobimo $(a + c) - (b + d) = (a - b) + (c - d) = (k + h)m$ ali $a + c \equiv b + d \pmod{m}$.
   Če enačbi odštejemo, dobimo $(a - c) - (b - d) = (a - b) - (c - d) = (k - h)m$ ali $a - c \equiv b - d \pmod{m}$.
   Podobno najdemo za produkt $ac = (b + km)(d + hm) = bd + (kd + hb + khm)m$ ali $ac \equiv bd \mod m$.
5. Če $ad \equiv bd \pmod{m}$ potem $m|ad-bd$ in lahko pišemo, da $m|d(a-b)$. Ker vemo, da je $D(d, m) = 1$, potem $m|a - b$. Iz tega sledi, da je $a \equiv b \pmod{m}$.

□

Prve tri točke iz zgornjega izreka nam povedo, da je kongruenca po modulu m ekvivalenčna relacija, saj velja refleksivnost, simetričnost in tranzitivnost.Cela števila se zato razdelijo v m ekvivalenčnih razredov glede na ostanek pri deljenju z modulom m. Ekvivalenčnemu razredu celega števila a pravimo **kongruenčni razred** števila a po modulu m.
Oznaka:

$$[a]_m = \{b \in \mathbb{Z} | a \equiv b \pmod{m}\}.$$

Množico vseh kongruenčnih razredov po modulu m označujemo z $\mathbb{Z}_m$.

Definicija 4.6. Množico m števil, ki so izbrana tako, da je iz vsakega kongruenčnega razreda po modulu m vzeto natančno eno število, imenujemo **popoln sestav ostankov** po modulu m.

Definicija 4.7. Če iz popolnega sestava ostankov po modulu m obdržimo le tista števila, ki so tuja modulu m, dobimo **reducirani sestav ostankov** po modulu m.
Ta sestav vsebuje $\varphi(m)$ števil.

Primer 4.8. Vzemimo število 6.
Popoln sestav ostankov po modulu 6 je npr. množica $\{0, 1, 2, 3, 4, 5\}$. Reduciran sestav ostankov po modulu 6 pa je npr. 1,5. V kongruenčnih razredih $[1]_6$ in $[5]_6$ so sama proti 6 tuja števila.

4.2 Wilsonov izrek

Izrek 4.9. ***(Wilsonov izrek)*** *Če je p praštevilo, potem je $(p-1)! \equiv -1 \pmod{p}$.*

Dokaz. Če je $p = 2$, potem je $(2-1)! = 1 \equiv -1 \pmod 2$. Če je $p = 3$, potem je $(3-1)! = 2 \equiv -1 \pmod 3$.
Privzemimo, da je p praštevilo, večje od 3.
Ker je $\mathbb{Z}_p$ obseg za opreaciji seštevanja in množenja, za vsak $a \in \{1, 2, \ldots, p-1\}$ obstaja tako naravno število $b \in \{1, 2, \ldots, p-1\}$, da velja $ab \equiv 1 \pmod p$.
Recimo, da je $a = b$. To pomeni, da je $a^2 \equiv 1 \pmod p$ oziroma $p|(a^2 - 1) = (a-1)(a+1)$. Po Izreku 2.20 bodisi $p|a-1$ bodisi $p|a+1$. Ker je $a \in \{1, 2, \ldots, p-1\}$, je $a - 1 \in \{0, 1, \ldots, p-2\}$, $a + 1 \in \{2, 3, \ldots, p\}$.
Če $p|a-1$, je $a - 1 = 0$, oziroma $a = 1$.
Če $p|a+1$, je $a + 1 = p$, oziroma $a = p - 1$.
Vidimo, da za vsak $a \in \{2, \ldots, p-2\}$ obstaja tako število b, kjer $a \neq b$ in $b \in \{2, \ldots, p-2\}$ in $ab \equiv 1 \pmod p$. Zmnožek $(p-1)!$ je zato kongruenten $p-1$ po modulu p; $p-1$ pa je kongruenten -1 po modulu p.
Za vsako praštevilo $p > 3$ potem velja, da je $(p-1)! \equiv -1 \pmod p$. □

Primer 4.10. Vzemimo za $p = 7$.
Imamo $(7-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdot 5 \cdot 6$. Združili bomo faktorje v produktu tako, da dobimo nek produkt kongruenten 1 po modulu 7. Opazimo, da $2 \cdot 4 \equiv 1 \pmod 7$ in $3 \cdot 5 \equiv 1 \pmod 7$. Tedaj lahko zapišemo: $6! \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 6 \equiv -1 \pmod 7$.

Pokazali bomo tudi, da velja obrat Wilsonovega izreka [**?**] in sicer:

Izrek 4.11. *Če je $p \in \mathbb{N}$ in $(p-1)! \equiv -1 \pmod p$, potem je p praštevilo.*

Dokaz. Predpostavimo, da p ni praštevilo. Potem je p sestavljeno število in ima vsaj enega delitelja a, tako da $1 < a < p$. Ker je $(p-1)! \equiv -1 \pmod{p}$ lahko pišemo, da $p|(p-1)!+1$. Ker je a delitelj števila p velja tudi, da $a|(p-1)!+1$. Ker je $a < p$, $a|(p-1)!$. Ker pa $a|(p-1)!+1$, od tod dobimo, da $a|1$. Sledi, da je $a = 1$, kar je v nasprotju z izjavo $1 < a < p$. Tako smo prišli v protislovje in lahko rečemo, da mora biti p praštevilo. □

4.3 Eulerjev izrek

Izrek 4.12. ***(Eulerjev izrek)*** *Naj bo $a \in \mathbb{Z}$ in $m \in \mathbb{N}$. Če je $D(a,m) = 1$ potem velja kongruenca*

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

Dokaz. Naj bo $a_1, a_2, \ldots, a_{\varphi(m)}$ reduciran sestav ostankov po modulu m. Ker je število a tuje proti m, je po Definiciji 4.7 tudi množica $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ reduciran sestav ostankov po modulu m. Vsako število iz $a_1, a_2, \ldots, a_{\varphi(m)}$ je kongruentno po modulu m natančno enemu številu iz $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ in obratno. Zato velja po 4. točki v Izreku 4.5 kongruenca

$$aa_1 aa_2 \cdots aa_{\varphi(m)} \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

Tako

$$a^{\varphi(m)} a_1 a_2 \cdots a_{\varphi(m)} \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

Ker so števila iz reduciranega sestava $a_1, a_2, \ldots, a_{\varphi(m)}$ tuja proti m, smemo dobljeni kongruenci na obeh straneh krajšati z $a_1, a_2, \ldots, a_{\varphi(m)}$. Tako dobimo $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Primer 4.13. Vzemimo dve tuji si števili, $a = 41$ in $m = 15$.
$\varphi(15) = \varphi(3 \cdot 5) = 2 \cdot 4 = 8$.
Tako je $41^8 \equiv 1 \pmod{15}$.
Iz tega sledi, da $15|7.984.925.229.121 - 1 = 7.984.925.229.120$.
$7.984.925.229.120 : 15 = 532.328.348.608$.

4.4 Fermatov izrek

Izrek 4.14. ***(Mali Fermatov izrek)*** *Če je p praštevilo in $a \in \mathbb{N}$ tako, da $p \nmid a$, potem je*

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

Dokaz. Če $p \nmid a$, potem je $D(p, a) = 1$. Po Izreku 4.12 velja:

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

V tem primeru je $\varphi(p) = p - 1$ in zato je $a^{p-1} \equiv 1 \pmod{p}$. □

Posledica 4.15. *Za vsako praštevilo p in vsako celo število a velja, da je*

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

Dokaz. Če $p|a$, potem je $a^p \equiv 0 \pmod{p}$ in $a \equiv 0 \pmod{p}$, torej je $a^p \equiv a \pmod{p}$. Če $p \nmid a$, potem je po Malem Fermatovem izreku $a^{p-1} \equiv 1 \pmod{p}$. Ko pomnožimo kongruenco z a, dobimo $a^p \equiv a \pmod{p}$. □

5 Verjetnosti algoritmi

Že od nekdaj so se matematiki ukvarjali s problemom izdelave učinkovitega algoritma za testiranje praštevilskosti. Ko imamo opraviti z velikimi števili, so najbolj pogosti in učinkoviti verjetnostni algoritmi. Poleg števila n, ki ga testiramo, se v teh algoritmih pojavi tudi število a, ki je izbrano naključno. Ponavadi verjetnostni algoritmi nikoli ne proglasijo praštevila za sestavljeno število, toda možno je, da sestavljeno število proglasijo za praštevilo. Če test ponavljamo pri neodvisno izbranih vrednosti a, se verjetnost napake manjša. Osnovna struktura za testiranje praštevil je naslednja:

- Izberemo število n, za katerega bomo preverjali ali je praštevilo ter naključno izberemo število a.
- Preverimo nekatere enakosti (odvisno od algoritma), ki vključujejo števili a in n. Če enakost ne drži, potem je n sestavljeno število, število a pa je priča za sestavljenost števila n in algoritem se ustavi.
- Če enakost drži, ponavljamo od prvega koraka dalje, dokler ni dosežena potrebna gotovost.

V nadaljevanju si bomo ogledali naslednje verjetnostne algoritme: Fermatov algoritem, Miller-Rabinov algoritem ter Lucasov algoritem. Omenjeni algoritmi so povzeti po literaturi [4].

5.1 Fermatov algoritem

Najbolj enostaven algoritem za testiranje praštevilskosti je Fermatov algoritem. Ta algoritem temelji na Fermatovem malem izreku. Če želimo preveriti, ali je neko naravno število n praštevilo, potem izberemo naključno naravno število a, tako, da $D(n, a) = 1$. Po Fermatovem malem izreku testiramo:

- Če je $a^{n-1} \not\equiv 1 \pmod{n}$, potem je n sestavljeno število in a je priča za sestavljenost števila n.
- Če je $a^{n-1} \equiv 1 \pmod{n}$, potem je število n verjetno praštevilo.

Ker ne vemo zagotovo, ali je n praštevilo ali ne, postopek nadaljujemo. Spet izberemo naključno število $a_1 \neq a$ in $D(n, a_1)$:

- Če je $a_1^{n-1} \not\equiv 1 \pmod{n}$, potem je n sestavljeno število in a_1 je priča za sestavljenost števila n.
- Če je $a_1^{n-1} \equiv 1 \pmod{n}$, potem je število n verjetno praštevilo.

Ker ne vemo zagotovo, ali je n praštevilo ali ne, postopek ponovno nadaljujemo. Izberemo naključno število $a_2 \neq a_1$, $a_2 \neq a$ in $D(n, a_2)$:

- Če je $a_2^{n-1} \not\equiv 1 \pmod{n}$, potem je n sestavljeno število in a_2 je priča za sestavljenost števila n.
- Če je $a_2^{n-1} \equiv 1 \pmod{n}$, potem je spet število n verjetno praštevilo.

Postopek lahko nadaljujemo. Od tega, na koliko naključno izbranih številih testiramo veljavnost enakosti, je odvisna natančnost odgovora ali je število n praštevilo ali ne.

Definicija 5.1. Naj bo n sestavljeno število in a poljubno število, tako da $D(n, a) = 1$. Če je $a^{n-1} \equiv 1 \pmod{n}$, potem številu n pravimo *psevdopraštevilo glede na število a*.

Definicija 5.2. Naj bo n sestavljeno število. Če je $a^{n-1} \equiv 1 \pmod{n}$, za vsa števila a, za katera je $D(n, a) = 1$, potem število n imenujemo **Carmichaelovo število**.

Carmichaelova števila [6] so zelo podobna praštevilom. Pomembna so, ker vedno prestanejo Fermatov algoritem za testiranje praštevilskosti, pa čeprav sama niso praštevila. Ravno zaradi njih se težko zanesemo na ta algoritem za dokazovanje praštevilskosti.
Tako kot je neskončno praštevil, obstaja tudi neskončno mnogo Carmichaelovih števil, vendar so zelo redka. Do 1000 je samo 1 Carmichaelovo število in sicer število 561, praštevil pa je 168. Do 10^{16} je 246.683 Carmichaelovih števil, praštevil pa je 279.238.341.033.925. Vidimo lahko, da je manj kot en bilijon možnosti, da izberemo Charmichaelovo število. Charmichaelova števila so vedno liha.

Primer 5.3. Najprej si bomo pogledali primer na Carmichaelovem številu. Izberimo si najmanjše tako število 561.
Izberemo si naključna števila $a, a_1, a_2 \in \mathbb{N}$, tako da $D(a, n) = 1$, $D(a_1, n) = 1$, $d(a_2, n) = 1$, $a \neq a_1 \neq a_2$ in testiramo:

- $a = 7$
  Zanima nas kongruenca števila 7^{560} po modulu 561?
  $7^7 = 823.543 \equiv -5 \pmod{561}$
  $(7^7)^5 \equiv (-5)^5 = -3.125 \equiv -320 \pmod{561}$
  $(7^{35})^2 \equiv (-320)^2 = 102.400 \equiv 298 \pmod{651}$
  $(7^{70})^2 \equiv 298^2 = 88.804 \equiv 166 \pmod{561}$

$(7^{140})^2 \equiv 166^2 = 27.556 \equiv 67 \pmod{561}$
$(7^{280})^2 \equiv 67^2 = 4.489 \equiv 1 \pmod{561}$
$7^{560} \equiv 1 \pmod{561}$

- $a_1 = 8$
  $8^{560} \equiv 1 \pmod{561}$

- $a_2 = 67$
  $67^{560} \equiv 1 \pmod{561}$

Če bi preverili na vseh naključno izbranih številih a, tako da $D(a, n) = 1$, bi se prepričali, da kongruenca $a^{n-1} \equiv 1 \pmod{n}$ velja za vsak tak izbran a. S pomočjo Evklidovega algoritma lahko ugotovimo, da je število 561 razcepljivo na praštevila in sicer:

$$561 = 3 \cdot 11 \cdot 17.$$

Zato število 561 ni praštevilo, je pa Carmichaelovo število.

Primer 5.4. Poglejmo si ali je število 87 praštevilo?
Izberemo si naključni $a = 59$ in izračunamo

$$59^{86} \equiv 1 \pmod{87}.$$

Dobili smo kongruenco enako 1, ali imamo res praštevilo?
Izberemo še en naključni $a_1 = 23$ in računamo naprej

$$23^{86} \equiv 7 \pmod{87}.$$

Sedaj pa nismo dobili kongruence enake 1, torej je 87 sestavljeno število in 23 njegova priča sestavljenosti.
Vidimo tudi, da je število 87 je psevdopraštevilo glede na število 59.

Primer 5.5. Poglejmo si še ali je 223 praštevilo?
Izberemo si pet naključnih števil $a_1 = 5$, $a_2 = 40$, $a_3 = 134$, $a_4 = 204$, $a_5 = 198$ in izračunamo kolikšne so njune kongruence po modulu 223.

$5^{222} \equiv 1 \pmod{223}$
$40^{222} \equiv 1 \pmod{223}$
$134^{222} \equiv 1 \pmod{223}$
$204^{222} \equiv 1 \pmod{223}$
$198^{222} \equiv 1 \pmod{223}$

Po petih poskusih nismo našli priče sestavljenosti števila 223, torej je število verjetno praštevilo. Če bi postopek nadaljevali za naključno izbrana števila a, bi dobili vedno kongruenco enako 1. Tako bi se nam verjetnost, da je to število praštevilo, povečevala. Zaradi Carmichaelovih števil, pa nebi mogli zagotoviti, da je to število res praštevilo.

5.2 Miller-Rabinov algoritem

Poglejmo si nekoliko hitrejši in boljši algoritem od Fermatovega in sicer Miller-Rabinov algoritem [7]. Če želimo pokazati delovanje tega algoritma, potrebujemo naslednji izrek:

Izrek 5.6. *Naj bo n praštevilo. Praštevilo n zapišemo v obliki $1 + 2^s d$, kjer je d liho število. Za vsa števila a, za katera velja, da $1 \leq a < n$ in $D(a, n) = 1$, ima zaporedje*

$$a^d, a^{2d}, a^{4d}, \ldots, a^{2^{s-1}d}, a^{2^s d} \pmod{n} \tag{5.1}$$

obliko

$$(1, 1, 1, \ldots, 1, 1, 1)$$

ali

$$(*, *, *, \ldots, n-1, 1, 1, 1),$$

kjer $*$ predstavlja poljubno število med 0 in $n - 1$.

Dokaz. Naj bo n praštevilo. Pokažimo najprej, da je $a^{2^s d} \equiv 1 \pmod{n}$.
Po Malem Fermatovem izreku je $a^{n-1} \equiv 1 \pmod{n}$. Ker je $n = 1 + 2^s d$ sledi, da je $n - 1 = 2^s d$. Torej lahko zapišemo $a^{2^s d} \equiv 1 \pmod{n}$. Prvi del smo dokazali.
Predpostavimo sedaj, da zaporedje (5.1) ni oblike $(1, 1, 1, \ldots, 1, 1, 1)$. Naj bo x prvi indeks zaporedja (5.1), ki je enak 1. Zanima nas kolikšna je vrednost kongruence člena pred tem izbranim. Torej:

$$\begin{aligned} a^{2^x d} &\equiv 1 \pmod{n} \\ a^{2^{x-1} d} &\equiv y \pmod{n}, \qquad y \neq 1, (0 \leq y \leq n-1). \end{aligned}$$

Izračunati moramo vrednost neznanke y.

$$\begin{aligned} (a^{2^{x-1} d})^2 &\equiv y^2 \pmod{n} \\ a^{2^{x-1} \cdot d \cdot 2} &\equiv y^2 \pmod{n} \\ 1 \equiv a^{2^x d} &\equiv y^2 \pmod{n} \\ y^2 &\equiv 1 \pmod{n} \end{aligned}$$

Iz tega sledi, da $n | y^2 - 1 = (y - 1)(y + 1)$. Ker je n praštevilo, iz Izreka 2.19 sledi, da $n | y - 1$ ali $n | y + 1$:

- Če $n | y - 1$ sledi, da je $y = 1$. Prišli smo v protislovje, saj smo rekli, da $y \neq 1$.
- Če pa $n | y + 1$ sledi, da je $y = n - 1$.

S tem smo dokazali tudi, da je $a^{2^{x-1} d} \equiv n - 1 \pmod{n}$. □

Poglejmo si, kako deluje Miller-Rabinov algoritem.
Najprej si izberimo liho število n za katerega preverjamo ali je praštevilo in n zapišemo v obliki $n = 1 + 2^s d$, kjer je d liho število. Izberemo si naključen a, tako da je $1 \leq a < n$ in $D(a, n) = 1$ ter po zgornejm izreku testiramo:

- Če je zaporedje
$$a^d, a^{2d}, a^{4d}, \ldots, a^{2^{s-1}d}, a^{2^s d} \pmod{n}$$
enako
$$(1, 1, 1, \ldots, 1, 1, 1) \qquad ali \qquad (*, *, *, \ldots, n-1, 1, 1, 1)$$
je n verjetno praštevilo in postopek nadaljujemo za naslednji a_1.

- Sicer je število n sigurno sestavljeno število.

Recimo, da je n verjetno praštevilo in postopek nadaljujemo za naključni $a_1 \neq a$ in $D(a_1, n) = 1$:

- Če je zaporedje
$$a_1^d, a_1^{2d}, a_1^{4d}, \ldots, a_1^{2^{s-1}d}, a_1^{2^s d} \pmod{n}$$
enako
$$(1, 1, 1, \ldots, 1, 1, 1) \qquad ali \qquad (*, *, *, \ldots, n-1, 1, 1, 1)$$
je n verjetno praštevilo in postopek nadaljujemo za naslednji a_2.

- Sicer je število n sigurno sestavljeno število.

Tako postopek nadaljujemo. Natančnost algoritma je odvisna od tega, na koliko naključno izbranih številih testiramo veljavnost enakosti.

Pri Miller-Rabinovem algoritmu moramo torej preveriti, da je

$$a^d \equiv 1 \pmod{n}$$
$$ali$$
$$a^{2^x d} \equiv n-1 \pmod{n}, \qquad \text{za } 0 \leq x \leq s-1.$$

Če ena od zgornjih enakosti velja, potem je n po veliki verjetnosti praštevilo.

Definicija 5.7. Naj bo n sestavljeno število. Če ima n značilnosti, ki so opisane v Izreku 5.6 za nek naključno izbran a, potem število n imenujemo *krepko psevdopraštevilo glede na število a.*

Naj bo n sestavljeno liho število. Potem n prestane Miller-Rabinov algoritem za največ $(n-1)/4$ naključno izbranih števil a, ki so med 1 in n.

Algoritem proglasi sestavljeno število za praštevilo z verjetnostjo največ 4^{-k}, kjer je k število ponovitev algortima.

Primer 5.8. Poglejmo si najprej delovanje algoritma na številu, za katerega vemo, da je praštevilo.
Izberimo si število $n = 29 = 1 + 28 = 1 + 2^2 \cdot 7$, $s = 2$, $d = 7$.
Izberimo si naključno število a, tako da $1 \leq a \leq n-1$ in $D(a, n) = 1$ in testiramo:

- $a = 10$
  $10^7 \equiv 17 \pmod{29} \neq 1$ ali $n-1$
  $(10^7)^2 \equiv -1 \pmod{29} = n-1$
  Dobili smo kongruenco enako $n-1$, torej je število 29 verjetno praštevilo.

- Poskusimo še za $a_1 = 19$.
  $19^7 \equiv 12 \pmod{29} \neq 1$ ali $n-1$
  $(19^7)^2 \equiv -1 \pmod{29} = n-1$
  Spet smo dobili kongruenco enako $n-1$, torej je število 29 verjetno praštevilo.

Podobne odgovore bi dobili za vsa naključno izbrana števila a, tako da $1 \leq a \leq n-1$ in $D(a, n) = 1$. Z gotovostjo bi lahko trdili, da je 29 praštevilo.

Primer 5.9. Sedaj si poglejmo, ali je število $n = 221$ praštevilo ter kolikšna je vertjetnost, da je to število praštevilo, pri k naključno izbranih številih a.
Izbrali si bomo 10 naključnih števil a, kjer je $1 \leq a \leq n-1$, $D(a, n) = 1$, ter izračunali kongruence glede na število 221.
Število 221 zapišemo kot $221 = 1 + 220 = 1 + 2^2 \cdot 55$, $s = 2$, $d = 55$ in pričnemo s testiranjem:

- $a = 4$
  $a^d = 4^{55} \equiv 30 \pmod{221} \neq 1$
  $a^{2d} = 4^{110} \equiv 16 \pmod{221} \neq n-1$

- $a = 25$
  $a^d = 25^{55} \equiv 168 \pmod{221} \neq 1$
  $a^{2d} = 25^{110} \equiv 157 \pmod{221} \neq n-1$

- $a = 77$
  $a^d = 77^{55} \equiv 55 \pmod{221} \neq 1$
  $a^{2d} = 77^{110} \equiv 152 \pmod{221} \neq n-1$

- $a = 84$
  $a^d = 84^{55} \equiv 33 \pmod{221} \neq 1$
  $a^{2d} = 84^{110} \equiv 205 \pmod{221} \neq n-1$

- $a = 86$
  $a^d = 86^{55} \equiv 18 \pmod{221} \neq 1$
  $a^{2d} = 86^{110} \equiv 103 \pmod{221} \neq n - 1$

- $a = 103$
  $a^d = 103^{55} \equiv 103 \pmod{221} \neq 1$
  $a^{2d} = 103^{110} \equiv 1 \pmod{221} \neq n - 1$

- $a = 137$
  $a^d = 137^{55} \equiv 188 \pmod{221} \neq 1$
  $a^{2d} = 137^{110} \equiv 205 \pmod{221} \neq n - 1$

- $a = 174$
  $a^d = 174^{55} \equiv 47 \pmod{221} \neq 1$
  $a^{2d} = 174^{110} \equiv 220 \pmod{221} = n - 1$
  $a^{4d} = 174^{220} \equiv 1 \pmod{221} = 1$

- $a = 185$
  $a^d = 185^{55} \equiv 42 \pmod{221} \neq 1$
  $a^{2d} = 185^{110} \equiv 217 \pmod{221} \neq n - 1$

- $a = 214$
  $a^d = 214^{55} \equiv 124 \pmod{221} \neq 1$
  $a^{2d} = 214^{110} \equiv 127 \pmod{221} \neq n - 1$

Že pri prvem $a = 4$ vidimo, da je število 221 sestavljeno in ne praštevilo, saj je 4 priča njegove sestavljenosti. To velja tudi za vsa druga naključno izbrana števila a, razen za število 174. Število 221 z naključno izbranim številom 174 prestane Miller-Rabinov test, zato lahko rečemo, da je 221 krepko psevdopraštevilo glede na število 174.
Prej smo omenili, da je največ $(n-1)/4$ naključnih števil a, da n prestane ta algoritem. V našem primeru je torej največ $220/4 = 55$ a-jev, za katera število 221 prestane algoritem.
Pri 10 naključno izbranih številih smo našli le eno tako število a, za katerega 221 prestane algoritem.
Za vsak a, ki ga izberemo naključno, je verjetnost, da smo izbrali tak a, da število 221 prestane algoritem, manjša od $1/4$. Torej je pri 10 naključno izbranih številih a verjetnost, da proglasimo sestavljeno število za praštevilo, največ 4^{-10}.

5.3 Lucasov algoritem

Poglejmo si še zadnji izbrani verjetnostni algoritem in sicer Lucasov algoritem. Ta je izmed vseh treh najbolj zapleten za razlago in razumevanje delovanja algoritma. Izhodišče tega algoritma je Lucasovo zaporedje, katerega bomo v nadaljevanju podrobneje predstavili, saj ga bomo potrebovali za delovanje Lucasovega algoritma.

Imejmo kvadratno enačbo $x^2 - ax + b = 0$, diskriminanto $D = a^2 - 4b$ ter naj bosta α in β ničli te enačbe. Potem je

$$\alpha = (a + \sqrt{D})/2 \qquad \text{and} \qquad \beta = (a - \sqrt{D}/2.$$

Pridobili smo naslednje tri relacije med a, b, D, α in β:

$$\alpha + \beta = a, \qquad \alpha - \beta = \sqrt{D}, \qquad \alpha\beta = b.$$

Sedaj lahko definiramo Lucasovi zaporedji $U(a, b)$ in $V(a, b)$ z uporabo teh relacij, kjer so a, b in D neničelna cela števila.

Definicija 5.10. Za vsak $k \geq 0$, velja

$$U_k(a, b) = \tfrac{\alpha^k - \beta^k}{\alpha - \beta} \qquad \text{in} \qquad V_k(a, b) = \alpha^k + \beta^k.$$

To sta eksplicitno podani formuli Lucasovega zaporedja.

Lucasovi zaporedji para (a, b) sta definirani takole:

$$\begin{aligned} U(a, b) &= (U_0(a, b), U_1(a, b), U_2(a, b), \ldots) \qquad \text{in} \\ V(a, b) &= (V_0(a, b), V_1(a, b), V_2(a, b), \ldots). \end{aligned}$$

Omenimo lahko primer Lucasovega zaporedja, to je Fibonaccijevo zaporedje, pri $a = 1$ in $b = -1$. Tako kot Fibonaccijevo, lahko tudi Lucasovo zaporedje definiramo rekurzivno: če je $k \geq 2$, potem imamo

$$U_k(a, b) = aU_{k-1} - bU_{k-2} \qquad \text{in} \qquad V_k(a, b) = aV_{k-1} - bV_{k-2}.$$

Sedaj navedimo še Lucasov algoritem za testiranje praštevil.
V ta namen definiramo Jacobijev simbol. Naj bo a poljubno celo število in p praštevilo. Potem definirajmo

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{če je kongruenca } x^2 \equiv a \pmod{p} \text{ rešljiva;} \\ -1, & \text{če kongruenca } x^2 \equiv a \pmod{p} \text{ ni rešljiva.} \end{cases}$$

Če je n sestavljeno število, ga izrazimo s produktom na praštevila $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ in definiramo

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Izrek 5.11. *Naj bodo a, b, D in U_k kot že zgoraj definirani. Če je p liho praštevilo, $D(b,p) = 1$ in $(\frac{D}{p}) = -1$, potem p deli U_{p+1}.*

Opomba 5.12. Če je $(\frac{D}{p}) = 1$, potem p deli U_{p-1}.

Ta izrek potrebujemo za Lucasov algoritem, ki deluje takole:

Izberemo si liho število n za katerega preverjamo ali je praštevilo. Naj bodo a, b, D in U_k kot so navedeni zgoraj in naj bo $(\frac{D}{n}) = -1$. Potem preverjamo:

- Če n ne deli U_{n+1}, potem je n sestavljeno število.
- Če pa n deli U_{n+1}, potem je n verjetno praštevilo.

Postopek ponavljamo kot pri prej opisanih algoritmih (Fermatovem algoritmu in Miller-Rabinovem algoritmu). Verjetnost, da je število n praštevilo se nam povečuje pri vsakem naslednjem naključno izbranem parametru a in b.

Če je $(\frac{D}{n}) = 1$, potem je Lucasov algoritem ekvivalenten Fermatovem algoritmu. Zato pri Lucasovem algoritmu preverjamo, ali je neko število n praštevilo ali ne, samo pri $(\frac{D}{n}) = -1$.

Definicija 5.13. Naj bo n sestavljeno število, $D(b,n) = 1$ in $(\frac{D}{n}) = -1$. Če n deli U_{n+1}, potem n imenujemo *Lucasovo psevdopraštevilo glede na parametra a in b.*

Pokazali bomo dve metodi, kako izbrati parametra a in b, da pridemo najlažje do rezultata.

1.metoda: Naj bo D prvo od števil $5, -7, 9, -11, 13, -15, \ldots$ za katero je $(\frac{D}{n}) = -1$, $a = 1$ in $b = \frac{1-D}{4}$.

2.metoda: Naj bo D prvo od števil $5, 9, 13, 17, 21, \ldots$ za katero je $(\frac{D}{n}) = -1$. Število a je prvo liho število, ki je večje od $\sqrt{D}$ in $b = \frac{a^2-D}{4}$.

Primer 5.14. Preverimo ali je število $n = 66$ praštevilo ali sestavljeno?
Računali bomo po prvi metodi za izbiro parametra a in b.
Naj bo D prvo od števil $5, -7, 9, -11, \ldots$ in izračunajmo ali je enačba $x^2 \equiv D \pmod{n}$ rešljiva.
$D = 5$
$x = 0, 1, 2, 3, \ldots, 65$
Ali ima enčba $x^2 \equiv 5 \pmod{66}$ rešitev za kateri x?
Enačba nima rešitve, torej je $(\frac{5}{66}) = -1$, $a = 1$ in $b = -1$.
Sedaj moramo izračunati še U_{67}, da vidimo ali n deli U_{67}. V rekurzivno podano formulo $U_k(a, b) = aU_{k-1} - bUk - 2$ vstavimo parametra $a = 1$ in $b = -1$ ter dobimo $U_k = U_{k-1} + U_{k-2}$.
Izračunamo zaporedje števil do U_{67}:
$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, \ldots,$
$27777890035288, 44945570212853$
$U_{67} = 44945570212853$
$66 \nmid 44945570212853$, torej je število 66 sestavljeno.

Primer 5.15. Ali je število $n = 31$ praštevilo?
Najprej poglejmo po prvi metodi:

- $D = 5$
  $x = 0, 1, 2, 3, \ldots, 30$
  Ali je enačba $x^2 \equiv 5 \pmod{31}$ rešljiva?
  Za $x = 6$ je enačba rešljiva.
  $36 \equiv 5 \pmod{31}$, torej je $(\frac{5}{31}) = 1$.
  Zgoraj smo omenili, če je $(\frac{5}{31}) = 1$ lahko računamo po Fermatovem algoritmu, zato si izberemo naslednji D, da dobimo $(\frac{D}{31}) = -1$.

- $D = -7$
  $x = 0, 1, 2, \ldots, 30$
  Enačba $x^2 \equiv -7 \pmod{31}$ nima rešitve, zato je $(\frac{-7}{31}) = -1$, $a = 1$ in $b = 2$.
  $U_k = U_{k-1} - 2U_{k-2}$
  Zaporedje števil do U_{32}:
  $0, 1, 1, -1, -3, -1, 5, 7, -3, -17, -11, 23, 45, -1, -91, -89, 93, 271, 85, -457, -627,$
  $287, 1541, 967, -2115, -4049, 181, 8279, 7917, -8641, -24475, -7193, 41757$
  $U_{32} = 41757$
  $31|41757$, torej je 31 verjetno praštevilo, zato si izberimo naslednji D.

- $D = 9$
  $x = 0, 1, 2, \ldots, 30$
  Za $x = 3$ je enačba rešljiva: $3^2 \equiv 9 \pmod{31}$.

- $D = -11$
  $x = 0, 1, 2, \ldots, 30$
  Za $x = 12$ je enačba rešljiva: $12^2 \equiv -11 \pmod{31}$.

- $D = 13$
  $x = 0, 1, 2, \ldots, 30$
  Enačba $x^2 \equiv 13 \pmod{31}$ nima rešitve, zato je $(\frac{13}{31}) = -1$, $a = 1$, $b = -3$ in $U_k = U_{k-1} + 3U_{k-2}$.
  Zaporedje števil do U_{32}:
  $0, 1, 1, 4, 7, 19, 40, 97, 217, 508, 1159, 2683, 6160, \ldots, 108412748857$
  $31|108412748867$, torej je 31 verjetno praštevilo.

Tako lahko nadaljujemo in verjetnost, da je število 31 praštevilo, se veča z vsakim naslednjim izbranim številom D.

Poglejmo si še po drugi metodi:

- $D = 5$
  Isto kot pri prvi metodi.

- $D = 9$
  Isto kot pri prvi metodi.

- $D = 13$
  $x = 0, 1, 2, \ldots, 30$
  Enačba $x^2 \equiv 13 \pmod{31}$ nima rešitve, zato je $(\frac{13}{31}) = -1$, $a = 5$ in $b = 3$
  $U_k = 5U_{k-1} - 3U_{k-2}$, zaporedje pa si sledi takole:
  $0, 1, 5, 22, 95, 409, 1760, 7573, 32585, 140206, 603275, 2595757, \ldots,$
  $12281122251031033093, 52842913625744643065$
  $31|52842913625744643065$, zato je 31 verjetno praštevilo.

Isto kot pri prvi metodi nadaljejemo z naslednjimi števili D in verjetnost, da je število 31 praštevilo se veča.

6 Zaključek

Algoritmi za testiranje praštevilskosti so še vedno aktualno področje na presečišču matematike in računalništva. Raziskovalci stremijo k temu, da bi našli čim bolj enostaven deterministični algoritem, pri katerem bi bil enostaven tako dokaz pravilnosti, kot tudi samo delovanje algoritma.

Leta 2002 so indijski računalniški znanstveniki Agrawal, Kayal in Saxena razvili deterministični algoritem, poznan z imenom algoritem AKS [9]. Gre za pomembno odkritje, vendar le na področju teoretičnega računalništva.

Ne glede na to pa se v praksi še vedno najbolj uporabljajo verjetnostni algoritmi. Najbolj pogost med njimi je Miller-Rabinov algoritem. Čeprav verjetnostni algoritmi niso 100% zanesljivi, raje večkrat poženemo tak algoritem na naključnih podatkih in potem primerjamo odgovore. Tako poljubno zmanjšujemo verjetnost napake. In čeprav niso zanesljivi, so še vedo hitrejši kot deterministični algoritmi.

7 Literatura

[1] J. Grasselli, *Elementarna teorija števil*, DMFA, Ljubljana, 2009. *(Citirano na straneh 2 in 10.)*

[2] K. H. Rosen, *Elementary number theory and its applications*, 5th edition, Pearson/Addison Wesley, Boston, 2005. *(Citirano na straneh 10 in 17.)*

[3] D. M. Burton, *Elementary number theory*, 7th edition, McGraw-Hill, New York, 2011. *(Citirano na straneh 10 in 17.)*

[4] Z. S. McGregor-Dorsey, Methods of Primality Testing, *MIT Undergraduate Journal of Mathematics, Volume* 1 (1999), 133–142. *(Citirano na strani 22.)*

[5] *The Converse of Wilson's Theorem*, The Oxford Math Center. http://www.oxfordmathcenter.com/drupal7/node/382. (Datum ogleda: 25. 4. 2014.) *(Citirano na strani 19.)*

[6] A. Granville, *Primality testing and Carmichael number*, http://www.dms.umontreal.ca/∼andrew/PDF/Notices1.pdf. (Datum ogleda: 15. 5. 2014.) *(Citirano na strani 23.)*

[7] *Miller–Rabin primality test*, http://en.wikipedia.org/wiki/Miller/%E2%80%93Rabin_primality_test. (Datum ogleda: 30. 5. 2014.) *(Citirano na strani 25.)*

[8] R. Petek, *RSA kriptosistem, diplomsko delo*, http://valjhun.fmf.uni-lj.si/∼ajurisic/diplome/petek_dip.pdf. (Datum ogleda: 15. 6. 2014.) *(Citirano na strani 1.)*

[9] A. Slosu, *Testiranje praštevilskosti, diplomsko delo*, http://eprints.fri.uni-lj.si/2208/1/Slosu_A-1.pdf. (Datum ogleda: 15. 6. 2014.) *(Citirano na strani 33.)*