Miller-Rabinov test prostosti

Ivona Raguž

svibanj, 2020.

1 Uvod

Prije Miller-Rabinova algoritma testiranja prostosti bila su poznata dva načina dokazivanja da je broj n složen:

- naći faktorizaciju broja n: $n = a \cdot b$, $a, b > 1$
- naći broj (bazu) a, td. $1 \leq a \leq n-1$ za koji vrijedi $a^{n-1} \not\equiv 1 \pmod{n}$

Opišimo sada koncept Miller-Rabinova algoritma testiranja prostosti za proizvoljan ulaz n.

1.1 Opis algoritma

Promotrimo na koji način dati odgovor o prostosti za različite ulaze n.
Ako je $n = 2$, zaključujemo da je n prost broj.
Ako imamo slučaj da je $n > 2$ i n paran, jasno je da je n složen.
Preostaje nam razmotriti kako ispitati neparne brojeve.
Neka je n neparan. Tada je $n-1$ paran, pa ga možemo zapisati kao

$$n - 1 = 2^s \cdot r, \quad s > 0, \quad r \geq 0 \text{ neparan.} \tag{1}$$

- Ako je n prost, tada iz Malog Fermatovog teorema za svaki a ($1 \leq a \leq n-1$) relativno prost s n vrijedi

  $$a^{n-1} \equiv 1 \pmod{n}. \tag{2}$$

  Uvrštavajući (1) u (2), dobijemo:

  $$a^{2^s r} \equiv 1 \pmod{n}. \tag{3}$$

  Iz izraza (19), slijedi:

  $$n | a^{2^s r} - 1 \implies n | (a^{2^{s-1} r})^2 - 1 \implies n | (a^{2^{s-1} r} - 1)(a^{2^{s-1} r} + 1). \tag{4}$$

  Iz (4) slijedi:

  $$n | (a^{2^{s-1} r} - 1) \quad \text{ili} \quad n | (a^{2^{s-1} r} + 1), \tag{5}$$

  odnosno

  $$a^{2^{s-1} r} \equiv \pm 1 \pmod{n}. \tag{6}$$

  Ponavljanjem vađenja korijena iz kongruencije mogu se dogoditi dva slučaja:

  - u jednom trenutku za rezultat dobijemo -1, odnosno postoji $j \in \{0, 1, \ldots, s-1\}$ takav da vrijedi $a^{2^j r} \equiv -1 \pmod{n}$
  - ne postoji $j \in \{0, , \ldots, s-1\}$ takav da $a^{2^j r} \equiv 1 \pmod{n}$, odnosno vrijedi $a^r \equiv 1 \pmod{n}$.

- Ako je n složen, tada ne vrijedi ni jedan od dva nabrojana slučaja.

Upravo ova dva slučaja služit će nam kao kriterij određivanja složenosti. Neka je n prirodan broj za kojeg želimo utvrditi je li prost ili nije. Jednostavno i pregledno možemo reći:

- u slučaju da za n i proizvoljnu bazu a ne vrijedi $a^r \equiv 1 \pmod{n}$ te ako ne postoji j, $0 \leq j \leq s-1$, td. $a^{2^j r} \equiv -1 \pmod{n}$, broj n je sigurno složen.

- u slučaju ispunjenosti nekog od uvjeta, ne možemo sa sigurnošću tvrditi da je broj prost. Možemo ponoviti test za drugu bazu a kako bismo eventualno povećali vjerojatnost pozitivnog odgovora na prostost. No, može se dogoditi da broj n ne prođe test za bazu a, pa dobijemo negativan odgovor prostosti.

Ako za ulaz algoritma imamo složen broj, može se dogoditi da za neku bazu a broj prođe test. Tada broj a nazivamo **strogim lažovom** za broj n.
U slučaju da broj n ne prođe test za prozvoljnu bazu a, a nazivamo **svjedokom složenosti** za broj n. U nastavku definiramo pojam koji opisuje neparne složene brojeve koji prolaze Miller-Rabinov test za proizvoljnu bazu a.

Definicija 1. *Neka je n neparan složen broj te neka je $n-1 = 2^s r$, r neparan. Neka je a broj relativno prost s n. Ako vrijedi*

$$a^r \equiv 1 \pmod{n} \quad ili \quad \exists j,\ 0 \leq j < s,\ a^{2^j r} \equiv 1 \pmod{n}, \tag{7}$$

*kažemo da je n **jaki pseudoprosti broj** u bazi a.*

Miller-Rabinovim testom prost broj ne može biti klasificiran kao složen, no može se dogoditi da je složen broj klasificiran kao prost.

Demonstrirajmo primjere testa za neke konkretne uaze.

Primjer 1. *Ispitajmo prostost broja $n = 91$. Faktorizacijom broja 91, $91 = 7 \cdot 13$, zaključujemo da je 91 složen broj.*
Provedimo Miller-Rabinov test za broj 91. Iz rastava broja $91-1 = 90 = 2^1 \cdot 45$, sukladno oznakama iz testa prostosti, označimo $s = 1$, $r = 45$.
Odaberimo prizvoljnu bazu $a \in \{1, \ldots, 90\}$. Neka je nasumično odabrani $a = 9$. Provjerimo vrijedi li kriterij (7) za a. Vrijedi $9^{45} \equiv 1 \pmod{91}$, pa je 91 jaki pseudoprost broj u bazi 9. Broj 9 je strogi lažov za 91.
Provedimo test za još jednu bazu a. Neka je u drugom provođenju testa $a = 5$. Provjerom kriterija, dobijemo $5^{45} \equiv 83 \not\equiv 1 \pmod{91}$, što implicira složenost broja 91.

Primjer 2. *Ispitajmo prostost broja* $n = 6553$.
Provedimo Miller-Rabinov test za broj 6553. *Iz rastava* $6553 - 1 = 6552 = 2^3 \cdot 819$, *označimo* $s = 3$, $r = 819$.
Nasumično odaberimo a. Neka je $a = 123$. *Računamo* 123^{819}. *Kako je*

$$123^{819} \equiv 8 \not\equiv 1 \pmod{6553}, \text{ te}$$

$$123^{819} \equiv 8 \not\equiv -1 \pmod{6553},$$

sljedeći korak je uzastopno kvadriranje kongruencije, najviše $s - 1 = 2$ *puta.*

$$(123^{819})^2 \equiv 123^{2^1 \cdot 819} \equiv 3367 \not\equiv -1 \pmod{6553}$$

$$((123^{819})^2)^2 = 123^{2^2 \cdot 819} \equiv 6552 \equiv -1 \pmod{6553}$$

Zaključujemo da je 6553 *jak pseudoprost broj u bazi* 123.

2 Pseudokod

U nastavku navodimo pseudokod Miller-Rabinova testa prostosti koji će nam poslužiti pri analizi složenosti algoritma.

Ulaz: n
if $n \equiv 0 \pmod 2$ i $n \neq 2$ **then**
  return n je složen
end if
if $n = 2$ **then**
  return n je prost
end if
zapiši $n - 1 = 2^s r$, r neparan
odaberi $a \in \{1, 2, \ldots, n-1\}$
if $gcd(a, n) \neq 1$ **then**
  return n je složen
else
  izračunaj $y = a^r \pmod n$
  if $y \neq 1$ i $y \neq -1$ **then**
    for $j = 1, \ldots, s-1$ **do**
      $y \leftarrow y^2 \pmod n$
      if $y = -1$ **then**
        return n je pseudoprost
      end if
      if $y = 1$ **then**
        return n je složen
      end if
    end for
    if $y \neq -1$ **then**
      return n je složen
    end if

end if
end if
return n je pseudoprost

Ukoliko vrijedi $a^r \equiv 1 \pmod{n}$ ili za $s = 0$, $a^r \equiv -1 \pmod{n}$, n je prošao test za bazu a. Ukoliko ne vrijedi ništa od tog, nastavljamo kvadrirati. Nastavak algoritma temelji se na traženju j-ta za kojeg je $a^{2^j r} \equiv -1 \pmod{n}$. Ukoliko naiđemo na takav s, algoritam se zaustavlja i n je prošao test. Ukoliko u nekom trenutku nađemo j za koji je $a^{2^j r} \equiv 1 \pmod{n}$, daljnjim kvadriranjem nikad nećemo dobiti -1 kao rezultat, pa je n složen.

3 Točnost algoritma

Ukoliko je n neparan složen broj, vjerojatnost da slučajno odabrani broj a nije svjedok složenosti za n je $\leq \frac{1}{4}$. Tvrdnja slijedi iz sljedećeg teorema.

Teorem 1. *Neka je n neparan složen prirodan broj, $n > 9$. Rastavimo $n - 1 = 2^s r$, $s \geq 1$ i r neparan. Neka je*

$$S = \{a : 1 \leq a < n \ \wedge \ (a^r \equiv 1 \pmod{n} \ \vee \ \exists j,\ 0 \leq j < s,\ a^{2^j r} \equiv -1 \pmod{n})\}.$$

Tada je

$$\frac{|S|}{\varphi(n)} \leq \frac{1}{4},$$

gdje je φ Eulerova funkcija ($\varphi(n)$ predstavlja broj elemenata skupa $\{1, \ldots, n\}$ relativno prostih s n).

Dokaz: Faktorizirajmo $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, gdje su p_i-evi međusobno različiti prosti brojevi, α_i odgovarajuće potencije prostih brojeva. Neka je 2^l najveća potencija od 2 koja dijeli svaki $p_i - 1$, gdje je p_i prost faktor broja n. Skup S je sadržan u skupu S' koji je definiran s:

$$S' = \{a : 1 \leq a < n \ \wedge \ a^{2^l r} \equiv \pm 1 \pmod{n}\}.$$

Pokažimo da vrijedi $S \subseteq S'$.

- Neka je $a \in S$ takav da je $a^r \equiv 1 \pmod{n}$. Tada je očito $a^{2^l r} \equiv 1 \pmod{n} \implies a \in S'$.
- Neka je $a \in S$ takav da postoji j, $0 \leq j < s$, $a^{2^j r} \equiv -1 \pmod{n}$. Vrijedi $a^{2^j r} \equiv -1 \pmod{n} \implies n | a^{2^j r} + 1$. Promotrimo li proste faktore p_i broja n, dobijemo:

  $$n | a^{2^j r} + 1 \text{ i } p_i | n \implies p_i | a^{2^j r} + 1 \implies a^{2^j r} \equiv -1 \pmod{p_i}.$$

  Tada je $(a^{2^j r})^2 \equiv a^{2^{j+1} r} \equiv (-1)^2 \equiv 1 \pmod{p_i}$. Odatle slijedi da 2^{j+1} dijeli red elementa $a \bmod p_i$. Kako je p_i prost broj, po Malom Fermatovom

teoremu vrijedi $a^{p_i-1} \equiv 1 \pmod{p_i}$. Sada vrijedi da $2^{j+1} | p_i - 1$. Potenciju 2^l smo izabrali tako da je ona najveća potencija od 2 koja dijeli $p_i - 1$, pa slijedi da je $l \geq j+1$.

$$a^{2^{l-1}r} \equiv a^{2^j r \cdot 2^{l-1-j}} \equiv (a^{2^j r})^{2^{l-1-j}} \equiv (-1)^{2^{l-1-j}} \pmod{n}$$

Rezultat kongruencije je 1 ili -1, ovisno o parnosti potencije. Dobili smo da vrijedi $a^{2^{l-1}r} \equiv \pm 1 \pmod{n}$, pa je $a \in S'$.

Kako je $S \subseteq S'$, vrijedi $|S| \leq |S'|$. Za tvrdnju teorema bit će dovoljno pokazati $\frac{|S'|}{\varphi(n)} \leq \frac{1}{4}$.

Broj rješenja a, $1 \leq a \leq n-1$, kongruencije $a^{2^{l-1}r} \equiv 1 \pmod{n}$ jednak je umnošku broja rješenja kongruencija $x^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}$, gdje su p_i-evi i α_i-evi oni iz rastava $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Kako zaključujemo ovo? Promotrimo sustav kongruencija:

$$\begin{aligned} a^{2^{l-1}r} &\equiv 1 \pmod{p_1^{\alpha_1}} \\ &\vdots \\ a^{2^{l-1}r} &\equiv 1 \pmod{p_k^{\alpha_k}} \end{aligned} \tag{8}$$

Jasno je da je svako rješenje kongruencije

$$a^{2^{l-1}r} \equiv 1 \pmod{n} \tag{9}$$

ujedno i rješenje svake kongruencije iz sustava (8).
Pokažimo: neka je x_0 rješenje kongruencije (9). Tada:

$$ax_0 \equiv 1 \pmod{n} \implies n | ax_0 - 1 \xrightarrow{p_i^{\alpha_i} | n} p_i^{\alpha_i} | ax_0 - 1 \implies ax_0 \equiv 1 \pmod{p_i^{\alpha_i}},$$

za $i = 1, \dots, k$. Neka $a_1, \dots, a_k$ predstavljaju redom po jedno rješenje svake pojedine kongruencija iz sustava (8), tj. a_i je rješenje kongruencije $a^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}$. Promotrimo sustav:

$$\begin{aligned} a &\equiv a_1 \pmod{p_1^{\alpha_1}} \\ &\vdots \\ a &\equiv a_k \pmod{p_k^{\alpha_k}} \end{aligned} \tag{10}$$

Kako su $p_1^{\alpha_i}, \dots, p_k^{\alpha_k}$ u parovima relativno prosti, po Kineskom teoremu o ostacima postoji rješenje $\pmod{p_1^{\alpha_1} \dots p_k^{\alpha_k}}$ sustava (10) i jedinstveno je. Označimo ga s a_0. Pokažimo da je a_0 rješenje kongruencije (9).

$$\begin{aligned} a_0^{2^{l-1}r} \equiv a_i^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}} &\implies p_i^{\alpha_i} | a_0^{2^{l-1}r} - 1, \ i = 1, \dots, k \\ \implies p_1^{\alpha_1} \dots p_k^{\alpha_k} | a_0^{2^{l-1}r} - 1 &\implies n | a_0^{2^{l-1}r} - 1 \implies a_0^{2^{l-1}r} \equiv 1 \pmod{n}. \end{aligned} \tag{11}$$

Sada konačno možemo zaključiti da je različitih a_0 onoliko koliko ima različitih sustava (10), što je jednako $\prod_{i=1}^{k} |\{a : a^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}\}|$ (jasno iz načina na koje smo birali a_i-eve iz sustava (10)). Nakon što smo dokazali prethodno i problem pronalaska broja rješenja kongruencije $a^{2^{l-1}r} \equiv 1 \pmod{n}$ formulirali u drugom obliku, nameće se sljedeće pitanje:

Koliko rješenja ima kongruencija $x^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}$ za fiksirani $i \in \{1, \ldots, k\}$?

Koristimo činjenicu da je $\mathbb{Z}_{p_i^{\alpha_i}}$ ciklička grupa. Generator te grupe označimo s a_0. Ako je a rješenje kongruencije $x^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}$ (za fiksirani i), tada je $a = a_0^y$, za neki y, odnosno vrijedi $a_0^{y2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}$. Kako je red grupe jednak $\varphi(p_i^{\alpha_i})$ i a_0 generator grupe, zaključujemo da je red od a_0 jednak $\varphi(p_i^{\alpha_i})$. Iz prethodno napisane kongruencije i saznanja o redu od a_0, zaključujemo da $\varphi(p_i^{\alpha_i}) | y2^{l-1}r$, tj. $y2^{l-1}r \equiv 0 \pmod{p_i^{\alpha_i - 1}(p_i - 1)}$.

Koliki je broj rješenja kongruencije $y2^{l-1}r \equiv 0 \pmod{p_i^{\alpha_i - 1}(p_i - 1)}$?

Promotrimo općenitu kongruenciju $ax \equiv b \pmod{m}$ i izvedimo zaključaj o broju rješenja te kongruencije.

Zaključak ćemo izvesti iz sljedeće tvrdnje: Neka je $gcd(a, m) = d > 1$. Kongruencija $ax \equiv b \pmod{m}$ ima rješenje ako i samo ako $d|b$. U tom slučaju, kongruencija ima d rješenja danih s

$$x = x_0 + \frac{tm}{d},\ t = 0, 1, \ldots, d-1,$$

gdje je x_0 rješenje kongruencije $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Pokažimo tvrdnju. Neka je x_0 rješenje kongruencije $ax \equiv b \pmod{m}$. Tada vrijedi: $ax_0 \equiv b \pmod{m} \implies ax_0 - b \equiv 0 \pmod{m} \implies ax_0 - b = tm$, za neki $t \in \mathbb{Z} \implies ax_0 - tm = b$. Zapišemo li $a = gcd(a, m)a'$, $m = gcd(a, m)m'$, vrijedi: $gcd(a, m)[a'x_0 - tm'] = b$. Stoga, zaključujemo $\underbrace{gcd(a, m)}_{d} | b$. Ako ne vrijedi $d|b$, kongruencija $ax \equiv b \pmod{m}$ nema rješenja.

U nastavku pretpostavimo da $d|b$. Tada je $gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.

Kongruencija $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ ima jedinstveno rješenje - označimo ga s x_0 $\left(x_0 = \left(\frac{a}{d}\right)^{-1}\frac{b}{d}\right.$, gdje je $\left(\frac{a}{d}\right)^{-1}$ inverz elementa $\frac{a}{d}$ modulo $\left.\frac{m}{d}\right)$. No, x_0 je također rješenje polazne kongruencije $ax \equiv b \pmod{m}$. Pokažimo:

$$\begin{aligned} \frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}} &\implies \frac{a}{d}x_0 - \frac{b}{d} = k\frac{m}{d}, \text{ za neki } k \in \mathbb{Z} \\ &\implies \left(\frac{a}{d}x_0 - \frac{b}{d}\right)d = \left(k\frac{m}{d}\right)d,\ k \in \mathbb{Z} \\ &\implies ax_0 - b = km, k \in \mathbb{Z} \\ &\implies ax_0 \equiv b \pmod{m}. \end{aligned} \tag{12}$$

Također, lako vidimo da je svaki broj $x \equiv x_0 \pmod{\frac{m}{d}}$ rješenje kongruencije $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, a time i polazne kongruencije $ax \equiv b \pmod{m}$ (pokažemo

na sličan način kao (12)).

$$x \equiv x_0 \pmod{\frac{m}{d}} \text{ rješenja kongruencije } ax \equiv b \pmod{m}$$
$$\implies x = x_0 + n\frac{m}{d},\ n \in \mathbb{Z}, \text{ rješenja kongruencije } ax \equiv b \pmod{m},$$

Sva međusobno neekvivalentna rješenja x originalne kongruencije su dana s $x = x_0 + n\frac{m}{d}$, $n = 0, 1, \ldots, d-1$.
Dakle, ako $d|b$, onda kongruencija $ax \equiv b \pmod{m}$ ima točno $d = gcd(a, m)$ rješenja.
Primjenimo sada ovu tvrdnju pri zaključivanju o broju rješenja kongruencije $y2^{l-1}r \equiv 0 \pmod{p_i^{\alpha_i - 1}(p_i - 1)}$.
Kako $gcd(2^{l-1}r, p_i^{\alpha_i-1}(p_i-1))|0$, vrijedi:

$$|\{y : y2^{l-1}r \equiv 0 \pmod{p_i^{\alpha_i-1}(p_i-1))}\}| = gcd(2^{l-1}r, p_i^{\alpha_i-1}(p_i-1)).$$

Kako $2^{l-1}r|(p_i-1)$, $p_i \nmid r$ te $2 \nmid p_i$ (jer je n neparan),

$$gcd((p_i-1)p_i^{\alpha_i-1}, 2^{l-1}r) = gcd(p_i - 1, r)2^{l-1}.$$

Zaključujemo da za fiksirani i vrijedi:

$$\begin{aligned} |\{x : x^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}\}| &= |\{y : y2^{l-1}r \equiv 0 \pmod{p_i^{\alpha_i-1}(p_i-1))}\}| \\ &= gcd(p_i - 1, r)2^{l-1}. \end{aligned} \tag{13}$$

Iz svega gore napisanog, slijedi:

$$|\{a : 1 \le a < n \ \wedge \ a^{2^{l-1}r} \equiv 1 \pmod{n}\}| = \prod_{p_i|n} gcd(p_i - 1, r)2^{l-1}.$$

Na isti način dobijemo da je broj rješenja kongruencije $x^{2^l r} \equiv 1 \pmod{p_i^{\alpha_i}}$ jednak $gcd(p_i - 1, r)2^l$. Broj rješenja te kongruencije dvaput je veći od broja rješenja kongruencije $a^{2^{l-1}r} \equiv 1 \pmod{p_i^{\alpha_i}}$. Odatle slijedi da je broj rješenja kongruencije $a^{2^{l-1}r} \equiv -1 \pmod{n}$ jednak broju rješenja kongruencije $a^{2^{l-1}r} \equiv 1 \pmod{n}$ (sva rješenja kongruencije $a^{2^{l-1}r} \equiv -1 \pmod{n}$ kvadriranjem postaju rješenja kongruencije $a^{2^l r} \equiv 1 \pmod{n}$).

$$|S'| = 2\prod_{p_i|n} gcd(p_i - 1, r)2^{l-1} \tag{14}$$

Podijelimo li jednakost s $\varphi(n)$ te iskoristimo li multiplikativnost funkcije φ, $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$, dobijemo:

$$\frac{|S'|}{\varphi(n)} = 2\prod_{p_i|n} \frac{gcd(p_i - 1, r)2^{l-1}}{p_i^{\alpha_i-1}(p_i-1)} \tag{15}$$

Želimo dobiti da vrijedi: $\frac{|S'|}{\varphi(n)} \leq \frac{1}{4}$.

Pretpostavimo da je $\frac{|S'|}{\varphi(n)} > \frac{1}{4}$, pa ćemo kontadikcijom dobiti traženo. Pretpostavimo da je

$$\frac{1}{4} < \frac{|S'|}{\varphi(n)} = 2 \prod_{p_i|n} \frac{gcd(p_i - 1, r)2^{l-1}}{p_i^{\alpha_i - 1}(p_i - 1)}. \tag{16}$$

Ograničimo desnu stranu jednakosti (15). Koristimo sljedeće: $gcd(p_i - 1, r)|(p_i - 1)$, $2^l|(p_i - 1)$, odnosno $2^{l-1}|\frac{p_i-1}{2}$. Kako je r neparan te $2^l \nmid gcd(p_i - 1, r)$ iz svega navedenog slijedi: $gcd(p_i - 1, r)2^l|(p_i - 1) \underset{l \geq 1}{\Longrightarrow} gcd(p_i - 1, r)2^{l-1}|\frac{p_i-1}{2}$. Za desnu stranu izraza (16) vrijedi:

$$2 \prod_{p_i|n} \frac{gcd(p_i - 1, r)2^{l-1}}{p_i^{\alpha_i - 1}(p_i - 1)} = 2 \prod_{p_i|n} \frac{1}{2} \frac{gcd(p_i - 1, r)2^{l-1}}{p_i^{\alpha_i - 1}(\frac{p_i-1}{2})} \tag{17}$$

$$\leq 2 \prod_{p_i|n} \frac{1}{2} \frac{\frac{p_i-1}{2}}{p_i^{\alpha_i - 1}(\frac{p_i-1}{2})} \leq 2 \prod_{p_i|n} \frac{1}{2} = 2 \cdot 2^{-t} = 2^{1-t}, \tag{18}$$

gdje je t broj p_i-eva (prostih faktora) u rastavu od n. Kako je broj p_i-eva ≥ 1, $2^{1-t} \leq 1$. Promotrimo nejednakosti u ovisnosti o broju prostih faktora broja n.

- Neka je $t = 1$. To znači da je n oblika $n = p^\alpha$, gdje je p neparan prost broj. Jasno je da je $\alpha \geq 2$ jer bi u suprotnom vrijedilo da je $n = p$ prost broj, a pretpostavili smo da je n složen. Uvrstimo li oblik broja n u nejednakost (16), vrijedi:

  $$\frac{1}{4} < 2 \cdot \frac{gcd(p - 1, r)2^{l-1}}{p^{\alpha-1}(p - 1)} = \frac{gcd(p - 1, r)2^{l-1}}{p^{\alpha-1}(\frac{p-1}{2})} \leq \frac{1}{p^{\alpha-1}} \implies p^{\alpha-1} < 4.$$

  Iz gornjeg uvjeta i uvjeta o neparnosti prostog broja p te složenosti broja n ($\alpha \geq 2$), vrijedi $p = 3$ i $\alpha = 2$. Dobijemo da je $n = 3^2$, što je kontadikcija s pretpostavkom teorema da je $n > 9$.

- Promotrimo n oblika $n = p_1^{\alpha_1} p_2^{\alpha_2}$. Promotrimo slučaj kada je barem jedan od eksponenata $\alpha_i \geq 2$. Tada desna strana od (16) izgleda ovako:

  $$2 \cdot \frac{gcd(p_1 - 1, r)2^{l-1}}{p_1^{\alpha_1 - 1}(p_1 - 1)} \cdot \frac{gcd(p_2 - 1, r)2^{l-1}}{p_2^{\alpha_2 - 1}(p_2 - 1)} = (*) \tag{19}$$

  Opet koristimo činjenicu da $gcd(p_i - 1, r)2^{l-1}|\frac{p_i-1}{2}$. Također, znamo da vrijedi $p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \geq 3^{2-1} = 3$. Nastavimo li s raspisom od (19), dobijemo:

  $$(*) = \frac{gcd(p_1 - 1, r)2^{l-1}}{p_1^{\alpha_1 - 1}\frac{p_1-1}{2}} \cdot \frac{gcd(p_2 - 1, r)2^{l-1}}{p_2^{\alpha_2 - 1}\frac{p_2-1}{2}} \cdot \frac{1}{2}$$

  $$\leq \frac{1}{p_1^{\alpha_1 - 1}} \cdot \frac{1}{p_2^{\alpha_2 - 1}} \cdot \frac{1}{2} \leq \frac{1}{3} \cdot \frac{1}{2} = \frac{1}{6}$$

Došli smo do kontradikcije jer $\frac{1}{4} \not< \frac{1}{6}$.
Ova kontradikcija nas navodi da je svaki α_i u rastavu $n = p_1^{\alpha_1} p_2^{\alpha_2}$ jednak 1.
Sukladno tome, $n = p_1 p_2$, $\alpha_1 = \alpha_2 = 1$. Sada izraz (16) izgleda:

$$\frac{1}{4} < 2 \cdot \frac{gcd(p_1 - 1, r)2^{l-1}}{p_1^{\alpha_1 - 1}(p_1 - 1)} \cdot \frac{gcd(p_2 - 1, r)2^{l-1}}{p_2^{\alpha_2 - 1}(p_2 - 1)} = \frac{1}{2} \cdot \frac{gcd(p_1 - 1, r)2^{l}}{p_1 - 1} \cdot \frac{gcd(p_2 - 1, r)2^{l}}{p_2 - 1}$$

Kako su $p_i - 1 > 0$, $gcd(p_i - 1, r)2^l > 0$, izraz možemo transformirati u sljedeći oblik:

$$\frac{p_1 - 1}{gcd(p_1 - 1, r)2^l} \cdot \frac{p_2 - 1}{gcd(p_2 - 1, r)2^l} < 2. \tag{20}$$

Kako vrijedi $gcd(p_i - 1, r) | (p_i - 1)$, $2^l | (p_i - 1)$ te $gcd(gcd(p_i - 1, r), 2^l) = 1$, vrijedi $gcd(p_i - 1, r)2^l | (p_i - 1)$. Sada zaključujemo da su faktori na lijevoj strani u izrazu (20) prirodni brojevi. Sada je jasno da su oba faktora jednaka 1.

$$p_1 - 1 = gcd(p_1 - 1, r)2^l \tag{21}$$
$$p_2 - 1 = gcd(p_2 - 1, r)2^l \tag{22}$$

Znamo da je $p_i - 1$ paran broj, $gcd(p_i - 1, r)$ neparan broj, pa zaključujemo da je 2^l upravo potencija od 2 u rastavu broja $p_i - 1$. Neparni dio broja $p_i - 1$ jednak je $gcd(p_i - 1, r)$, tj. neparni dio broja $p_i - 1$ dijeli r. Prisjetimo se oblika broja n: $n = (n-1) + 1 = 2^s r + 1$, a u ovom slučaju n je oblika $p_1 p_2$, pa $p_1 p_2 = 2^s r + 1$. Želimo vidjeti odnose neparnih dijelova brojeva $p_i - 1$, $i = 1, 2$.
Neparni dio broja $p_i - 1$ jednak je $gcd(p_i - 1, r)$.

$$n = 2^s r + 1 \quad \wedge \quad gcd(p_i - 1, r) | r \implies r | (n - 1) \quad \wedge \quad gcd(p_i - 1, r) | r$$
$$\implies gcd(p_i - 1, r) | (n - 1) \implies n \equiv 1 \pmod{gcd(p_i - 1, r)}$$

Iz te kongruencije slijedi da $gcd(p_1 - 1, r) | gcd(p_2 - 1, r)$ i $gcd(p_2 - 1, r) | gcd(p_1 - 1, r)$. Ta relacija implicira jednakost brojeva $gcd(p_1 - 1, r)$ i $gcd(p_2 - 1, r)$.

$$gcd(p_1 - 1, r) = gcd(p_2 - 1, r) \text{ i jednakost parnih dijelova brojeva}$$
$$p_1 - 1, p_2 - 1 \implies p_1 - 1 = p_2 - 1 \implies p_1 = p_2.$$

Ponovno smo dobili kontradikciju. Gornjim nizom implikacija zaključujemo da su prosti faktori u rastavu od n jednaki, tj. n je oblika $n = p_1^2$. To je kontadikcija s pretpostavkom da je broj različitih prostih prostih faktora broja n jednak 2.

- Promotrimo li slučaj gdje n ima barem 3 različita prosta faktora, tada desna strana izraza (18) nije veća od $2^{1-3} = \frac{1}{4}$, što svakako nije veće od lijeve strane izraza, tj. $\frac{1}{4}$.

Za svaki od ovih slučajeva dobili smo kontradikciju, tj. ne vrijedi $\frac{1}{4} < \frac{|S'|}{\varphi(n)}$. $\square$

Ukoliko test ponavljamo k puta, vjerojatnost da se ni u jednoj iteraciji ne pojavi svjedok složenosti je $\leq \frac{1}{4^k}$. Miller-Rabinov test je sigurniji od Fermatovog testa (manja vjerojatnost pogreške).

4 Složenost

Složenost algoritma provest ćemo direktno analizom pseudokoda.
Promotrimo složenost nekih osnovnih operacija.
Za početak, promotrimo proizvoljan broj n. Binarna reprezentacija broja n bit će duljine $\lfloor \log_2 n \rfloor + 1$ bitova.

- Množenje brojeva a i b modulo n izvršimo jednostavnim množenjem brojeva a i b, a potom uzimanjem ostatka pri dijeljenju s n. Modularno množenje ćemo koristiti u analizi modularnog eksponenciranja.
  Promotrimo množenje brojeva a i b koji su prikazani u binarnom zapisu. Množenje brojeva vršimo na način da svaki bit broja a množimo svakim bitom broja b te potom zbrojimo dobivene produkte. Izvrši se $\mathcal{O}(\log_2 a \cdot \log_2 b)$ množenja. Zbrajanje dobivenih međurezultata ne zahtjeva više od $\mathcal{O}(\log_2 a \cdot \log_2 b)$ operacija, pa je složenost množenja $\mathcal{O}(\log_2 a \cdot \log_2 b)$.
  Nakon završetka običnog množenja, umnožak dijelimo s n. Dijeljenje možemo izvršiti uzastopnim oduzimanjem broja n. Broj oduzimanja broja n je upravo $\lfloor \frac{ab}{n} \rfloor$, a takvih oduzimanja ne može biti više od n. U našem algoritmu, brojevi a i b koji će se množiti modulo n ovisit će o n ($a, b \in \{1, \ldots, n-1\}$, broj bitova a i b je manji ili jednak broju bitova broja n). Operacija modularnog množenja je složenosti $\mathcal{O}(\log_2^2 n)$. U pseudokodu, množenja $y \leftarrow y \cdot y$, tj. $y \leftarrow y^2$ vršimo najviše $s-1$ puta, gdje je s onaj iz rastava broja $n-1$, $n-1 = 2^s r$, pa je $s = \mathcal{O}(\log_2(n))$.

- Modularno potenciranje je sastavni dio pseudokoda u kojem računamo izraz oblika $a^e \pmod n$, za proizvoljne a, e. Trivijalni algoritam kojim bi se a^e računao kao $a \cdot a \cdot \cdots \cdot a$ pomoću $e-1$ množenja bio bi vrlo neefikasan i zauzimao veliku količinu računalne memorije. Najjednostavnija efikasna metoda je metoda uzastopnim kvadriranjem. Temelji se na binarnoj reprezentaciji eksponenta e:

  $$e = \alpha_0 + \alpha_1 \cdot 2^1 + \cdots + \alpha_k \cdot 2^k.$$

  Broj znamenaka broja e u binarnom zapisu je $\lfloor \log_2 e \rfloor + 1 = k+1$. Zapišimo potenciju na sljedeći način:

  $$a^e = a^{\sum_{i=0}^{k} \alpha_i 2^i} = \prod_i a^{\alpha_i 2^i} = \prod_{\alpha_j = 1} a^{2^j}.$$

  Demonstrirajmo algoritam za $a^{32} \pmod n$. Za potrebe ovog modularnog eksponenciranja, računamo samo sljedeće produkte modulo n: $a \cdot a, a^2 \cdot$

$a^2, a^4 \cdot a^4, a^{16} \cdot a^{16}$.
Ovaj postupak je vrlo efikasan, posebice ako ga promatramo na računalu, jer su brojevi već zapisani u binarnom zapisu.
Zapišimo pseudokod algoritma koji bi za proizvoljne ulaze a, e, n računao $a^e \pmod n$.

```
produkt ← 1
a_pot ← a
while e > 0 do
  if e mod 2 == 1 then
    produkt ← (produkt · a_pot) mod n
  end if
  e ← e/2
  a_pot ← (a_pot · a_pot) mod n
end while
```

Broj množenja i dijeljenja modulo n nalazi se između $\lfloor \log_2 e \rfloor$ i $2\lfloor \log_2 e \rfloor$, ovisno o broju jedinica u binarnom zapisu. Složenost modularnog potenciranja $\mathcal{O}(\log_2 e \cdot \log_2^2 n)$ za prizvoljan a, e. U slučaju da je broj e u binarnom zapisu sastavljen samo od jedinica, broj množenja modulo n bit će jednak broju bitova broja e ($\lfloor \log_2 e \rfloor + 1$). U pseudokodu, računamo $a^r \pmod n$, a kako je $r < n$, broja bitova broja r nije veći od $\lfloor \log_2 n \rfloor + 1$ bitova.

Složenost Miller-Rabinova testa je $\mathcal{O}(\log_2^3 n)$, a ako test provodimo k puta (za različite a-ove), složenost algoritma je $\mathcal{O}(k \cdot \log_2^3 n)$.

Literatura

[1] https://www.cs.upc.edu/~diaz/slides4-19.pdf

[2] https://web.math.pmf.unizg.hr/~duje/kript/miller.html

[3] https://shoup.net/ntb/ntb-v2.pdf

[4] https://www.cmi.ac.in/~shreejit/primality.pdf

[5] https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A5409/datastream/PDF/view

[6] http://www.math.leidenuniv.nl/~psh/ANTproc/05rene.pdf

[7] https://cpb-us-w2.wpmucdn.com/blog.nus.edu.sg/dist/2/3912/files/2014/09/Chapter3-2k5sbwd.pdf