Fermatov test prostosti prirodnih brojeva (1. dio seminara)

Ivona Raguž

travanj, 2020.

1 Frematov test prostosti

Diskusiju o Frematovom testu prostosti prirodnih brojeva započinjemo sljedećim teoremom koji čini okosnicu ovog testa, kao i mnogih drugih.

Teorem 1 (Mali Frematov teorem) *Ako je n prost broj i a relativno prost s n, tada vrijedi $a^{n-1} \equiv 1 \pmod{n}$.*

1.1 Opis algoritma

Opišimo Frematov test prostosti za proizvoljan ulaz n. Algoritam započinje nasumičnim odabirom prirodnog broja a td. $1 \leq a \leq n-1$, a potom provjerimo jesu li brojevi a i n relativno prosti ($gcd(a, n) = 1$). Ako a i n nisu relativno prosti, tada je jasno da je n složen broj. U slučaju da su a i n relativno prosti, provjerimo vrijedi li kongruencija

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

Ako ne vrijedi (1), n je sigurno složen broj (pozivajući se na teorem (1)). U slučaju da vrijedi kongruencija (1), ne možemo sa sigurnošću reći da je n prost. Mogli bismo ponoviti isti postupak (test) za neke druge vrijednosti a u cilju poboljšanja točnosti testa.

Primjer 1 *Frematovim testom prostosti provjerimo je li broj 2553 prost. Prvo slučajno odaberimo broj a, $1 \leq a \leq 2552$. Neka je $a = 158$. Kako je $158^{2552} \equiv 2209 \not\equiv 1 \pmod{2553}$, zaključujemo da je 2553 složen broj.*

Primjer 2 *Frematovim testom prostosti provjerimo je li broj 2557 prost. Neka je nasumično odabrani $a = 158$. Računajući se uvjerimo da vrijedi $158^{2556} \equiv 1 \pmod{2557}$. Frematov test možemo ponovno provesti za neki drugi, slučajno odabrani a. Neka je sada $a = 1375$. Provjerom kongruencije, vrijedi da je $1375^{2556} \equiv 1 \pmod{2557}$. Zbog ispunjenosti uvjeta (1), za sada ne možemo zaključiti da je broj složen. Daljnjim ponavljanjem testa povećava se vjerojatnost da je ispitivani broj prost.*

Slijedi pseudokod Fermatovog testa prostosti.

Algorithm 1: Fermatov test prostosti

```
Input: n
nasumično odaberi a, 1 ≤ a ≤ n − 1;
for i = 1, . . . , k do
    if gcd(a, n) > 1 then
        return broj je složen;
    end
    if gcd(a, n) = 1 then
        izračunaj x = a^{n−1} (mod n);
        if x ≠ 1 then
            return broj je složen;
        else
            return broj je vjerojatno prost;
        end
    end
end
```

Parametar k iz pseudokoda (1) označava broj a-ova za koje provodimo test. Možemo uočiti da će algoritam u slučaju zadovoljenosti kriterija iz teorema (1) klasificirati broj kao *vjerojatno prost*, tj. ne možemo biti u potpunosti sigurni da je ulaz n prost. Ovim algoritmom prost broj ne može biti klasificiran kao složen, no može se dogoditi da je složen broj klasificiran kao prost. Naime, postoji parovi brojeva a i n takvi da zadovoljavaju kriterij iz teorema (1), ali je n složen. Sukladno tome, definiramo sljedeći pojam.

Definicija 1 *Za neparan složen broj n kažemo da je (Fermat)* ***pseudoprost*** *u bazi a ako vrijedi $a^{n-1} \equiv 1 \pmod{n}$.*

Promotrimo sljedeći primjer koji demonstrira postojanje pseudoprostog broja u nekoj bazi.

Primjer 3 *Fermatovim testom želimo odrediti je li broj $n = 299$ prost. Za početak, slučajnim odabirom uzmimo neki $a \in \{1, \ldots, 298\}$. Neka je, primjerice, $a = 116$. Provjerimo relativnu prostost brojeva a i n. Lako je uvjerimo da je $gcd(116, 299) = 1$. Potom provjerimo vrijedi li izraz (1). Zaista vrijedi $116^{298} \equiv 1 \pmod{299}$, iz čega zaključujemo da je 299 prost ili (Fermat) pseudoprost u bazi 116. Ponovimo li isti postupak za odabrani $a = 155$, dobijemo sljedeće: $gcd(155, 299) = 1$ i $155^{298} \equiv 144 \not\equiv 1 \pmod{299}$. Iz dobivenog zaključujemo da je 299 složen.*

Motivirani brojem 116 iz prethodnog primjera i njegovom ulogom u dokazivanju (pseudo)prostosti prirodnog broja, definiramo pojmove svjedoka složenosti.

Definicija 2 *Za broj a kažemo da je* ***Frematov svjedok složenosti*** *broja n ako vrijedi $gcd(a,n) > 1$ ili $a^{n-1} \not\equiv 1 \pmod{n}$. U suprotnom, ako je n složen i za neki a vrijedi $gcd(a,n) = 1$ i $a^{n-1} \equiv 1 \pmod{n}$, za a kažemo da je* ***Frematov lažov*** *za n.*

Za većinu brojeva dovoljno je svega par puta provesti Fermatov test kako bi utvrdili njihovu složenost. No, postoje i brojevi za koje test ne daje odlučiv odgovor. Nećemo moći utvrditi složenost ovih brojeva i nakon provođenja Fermatova testa za sve baze a.

1.2 Carmichaelovi brojevi

Definicija 3 *Složeni broj n koji za svaki broj a relativno prost s n zadovoljava $a^{n-1} \equiv 1 \pmod{n}$ nazivamo* ***Carmichaelovim brojem.***

Primjer 4 *Najmanji Carmichaelov broj je* 561 *($561 = 3 \cdot 11 \cdot 17$).*

Carmichaelovi brojevi su relativno rijetki u odnosu na ostale brojeve, no ima ih dovoljno da ih se ne može zanemariti pri testiranju Fermatovim testom. Carmichaelovih brojeva manjih od 10^6 ima 43, dok je onih koji su manji od 10^{16} manje od 2.5×10^5. Prostih brojeva manjih od 10^{16} ima više od 2.5×10^{14}, pa je vjerojatnost da je Fermatov pseudoprost broj upravo Carmichaelov broj vrlo mala.

Napomena 1 *Ako je broj a Frematov lažov za broj n, tada je broj $n - a$ također Frematov lažov za broj n.*

Napomenu (1) je vrlo lako dokazati. Uz pretpostavku da je a Frematov lažov za n, znamo da vrijedi:

$$gcd(n-a, n) = gcd(a, n) = 1$$

$$n \mid (n-a)^{n-1} - a^{n-1} \xrightarrow[\text{lažov}]{\text{a Frematov}} (n-a)^{n-1} \equiv a^{n-1} \equiv 1 \pmod{n}.$$

Sada je jasno da je i broj $n - a$ Frematov lažov za n.
Iz primjera (3) i napomene (1) sada možemo zaključiti da je i $183 = 299 - 116$ Frematov lažov za broj 299.

1.3 Uspješnost algoritma

Ono što nas sljedeće zanima jest uspješnost Fermatovog testa prostosti. Kolika je vjerojatnost da će složen broj po završetku testa biti klasificiran kao složen? Zaključak ćemo izvesti iz sljedeće napomene.

Napomena 2 *Nije teško dokazati činjenicu da za složen broj n koji nije Carmichaelov postoji Fermatovih svjedoka složenosti barem onoliko koliko ima Fermatovih lažova za n.*

- *Ako ne postoji niti jedan Fermatov lažov za n, tada je svaki a ($1 \leq a \leq n-1$) Fermatov svjedok za n, pa je jasno da je Fermatovih svjedoka više.*

- *Ako postoji Fermatov lažov za n (b), iz definicije (2) znamo da vrijedi: $gcd(b,n) = 1$ i $b^{n-1} \equiv 1 \pmod{n}$. Kako je n složen i nije Carmichaelov, postoji barem jedan Fermatov svjedok složenosti za n (a) takav da je $gcd(a,n) = 1$ i $a^{n-1} \not\equiv 1 \pmod{n}$. Promotrimo sljedeće:*

$$(ab)^{n-1} \equiv a^{n-1}b^{n-1} \equiv a^{n-1} \cdot 1 \not\equiv 1 \pmod{n} \tag{2}$$

  Kako su a i b relativno prosti s n, tada je i njihov umnožak ab relativno prost s n. Koristeći tu činjenicu i (2), zaključujemo da je ab Fermatov svjedok složenosti broja n. Sada je očito da Fermatovih svjedoka složenosti broja n ima barem onoliko koliko ima Fermatovih lažova od n.

Neka Fermatov test prostosti za ulaz ima složeni broj n koji nije Carmichaelov. Kako Fermatovih svjedoka složenosti za n, sukladno napomeni (2), ima barem onoliko koliko ima Fermatovih lažova za n, jasno je da je vjerojatnost da će Fermatov test prostosti broj n proglasiti složenim barem $\frac{1}{2}$. Ako Fermatov test ponovimo k puta (k različitih vrijednosti baze a), vjerojatnost da će algoritam dati ispravan odgovor je barem $\frac{1}{2^k}$.
Napomenu (2) možemo izreći i na sljedeći način: ako Fermatov test prostosti ne daje pozitivan odgovor za neku bazu b, tada testirani broj ne prolazi test za najmanje polovicu mogućih baza.

Literatura

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

[2] Shreejit Bandyopadhyay. *PRIMALITY TESTING A Journey from Fermat to AKS*