Prímtesztek

A cél, hogy minél gyorsabban döntsük el egy (jó nagy) n számról, hogy összetett-e.

Fermat-teszt Tanultuk, hogy ha n prím, akkor minden n-hoz relatív prím a egészre $a^{n-1} \equiv 1 \ (n)$. A Fermat-teszt ezt az egyszerű tény használja ki n prímségének tesztelésére.

Fermat-teszt:
1. Válasszunk egy $0 < a < n$ egész számot.
2. $(a,n) \stackrel{?}{=} 1$ Ha nem $\Rightarrow$ n összetett. Ha igen $\Rightarrow$
3. $a^{n-1} \stackrel{?}{\equiv} 1 \ (n)$ Ha nem $\Rightarrow$ n összetett. Ha igen $\Rightarrow$ bármi lehet.

Természetesen $a^{n-1} \equiv 1 \ (n)$-ből nem következik, hogy n prím volna, tehát ebben az esetben a teszt nem hozott eredményt. Vizsgáljuk meg, hogy mit lehet ilyenkor tenni.

1. Definíció. Legyen n egész összetett és $(a,n) = 1$. Ekkor a az n összetettségének *Fermat-tanú*ja, ha $a^{n-1} \not\equiv 1 \ (n)$ és a az n *Fermat-cinkos*a egyébként.

Ha a Fermat-tesztet egy összetett számra végezzük el, akkor célunk, hogy találjunk egy tanút. Kérdés, hogy mindig le lehet-e buktatatni az összetett számokat így, azaz nem túl sok a választásával lehet-e Fermat-tanút találni. A válasz sajnos nem.

2. Definíció. Ha n összetett számhoz nem létezik Fermat-tanú, akkor n *Carmichael-szám*, más néven *álprím*.

3. Példa. Az 561 Carmichael-szám (ez a legkisebb).
Bizonyítás. $561 = 3 \cdot 11 \cdot 17$. A kínai maradéktétel és a Fermat tétele szerint:

$$\begin{aligned} a^2 \equiv 1 \quad (3) \quad &\Longrightarrow \quad a^{560} \equiv (a^2)^{280} \equiv 1 \quad (3) \\ a^{10} \equiv 1 \quad (11) \quad &\Longrightarrow \quad a^{560} \equiv (a^{10})^{56} \equiv 1 \quad (11) \\ a^{16} \equiv 1 \quad (17) \quad &\Longrightarrow \quad a^{560} \equiv (a^{16})^{35} \equiv 1 \quad (17) \end{aligned}$$

Így $a^{560} \equiv 1 \ (561)$ minden a-ra, melyre $(a, 561) = 1$. □

A következő tétel biztosítja, hogy amennyiben n összetett szám, de nem álprím, akkor a Fermat teszt „nagy valószínűséggel" lebuktatja.

4. Tétel. *Ha n-hez van Fermat-tanú, akkor van legalább $\frac{\varphi(n)}{2}$.*

Bizonyítás. Legyen $\mathbb{Z}_n^* = \{a \in \mathbb{Z} : (a,n) = 1 \text{ és } 0 \le a < n\}$, továbbá jelölje $C = \{a \in \mathbb{Z}_n^* : a^{n-1} \equiv 1 \ (n)\}$ a cinkosok halmazát. A feltétel szerint van Fermat-tanú n-hez, tehát $C \subsetneq \mathbb{Z}_n^*$. Legyen $t \in \mathbb{Z}_n^*$ egy tanú. Ekkor minden $a \in C$ esetén ta is tanú, ugyanis $(ta)^{n-1} \equiv t^{n-1}a^{n-1} \equiv t^{n-1} \not\equiv 1 \ (n)$, hiszen t tanú. Továbbá ha $a \neq a'$ két C-beli elem, akkor $ta \not\equiv ta' \ (n)$, hiszen $t \in \mathbb{Z}_n^*$ invertálható. Ezek szerint a ta alakú elemek adnak legalább $|C|$ Fermat-tanút, tehát az n-hez relatív prím maradékosztályok közül legalább annyi tanú van, ahány cinkos. Az állítást ezzel beláttuk.

A bizonyítást elegánsabb az algebra nyelvén megfogalmazni. Könnyű látni, hogy $\mathbb{Z}_n^*$ a modulo n szorzásra nézve csoport, aminek C részcsoportja. Lagrange tétele szerint (aminek a bizonyítása egyébként nagyjából a fenti érvelés általánosítása) egy csoport részcsoportjának elemszáma osztója a csoport elemszámának, azaz itt $|C|$ osztja $|\mathbb{Z}_n^*|$-ot. Miután $C \neq \mathbb{Z}_n^*$, az állítás ebből már látszik. □

Legyen n összetett szám nem álprím. Válasszuk a Fermat-tesztben szereplő a egészet véletlenszerűen (egyenletes eloszlással) az $[1, n-1]$ intervallumból. Az előbbi tétel alapján annak a valószínűsége, hogy cinkost választottunk legfeljebb $\frac{\varphi(n)}{2n} < \frac{1}{2}$. Ismételjük meg ezt az eljárást k-szor, így annak a valószínűsége, hogy mindannyiszor épp egy cinkost fogunk ki, kisebb, mint $\frac{1}{2^k}$. Más szóval aránylag kevés a kipróbálásával igen nagy eséllyel találunk tanút, amely lebuktatja n-et. Az egyetlen probléma ezzel a módszerrel, hogy álprímekre és prímekre is ugyanazt az eredményt adja.

A prímtesztelési eljárás szempontjából rossz hír, hogy 1992-ben sikerült bebizonyítani, hogy végtelen sok Carmichael-szám létezik (Alford, Granville, Pomerance). A következő részben tárgyalt Rabin–Miller-teszt – amely tekinthető a Fermat-teszt javított változatának – viszont az álprímeket is ki tudja szűrni.

Bár a prímtesztelésen nem segít, az alábbi két tétel igaz álprímekre.

5. Tétel. *Egy n összetett szám pontosan akkor álprím, ha négyzetmentes és minden p prímosztójára $p-1 \mid n-1$.*

Bizonyítás. Tegyük fel először, hogy n álprím. Ha $p^2 \mid n$ volna, akkor legyen g egy primitív gyök modulo p^2. Megmutatjuk, hogy g Fermat-tanúja n összetettségének, ami ellentmondt annak, hogy n Carmichael-szám. Valóban: g modulo p^2 rendje $\varphi(p^2) = p(p-1)$ osztható p-vel, de $n-1$ nem osztható p-vel (mivel $p \mid n$), ezért g rendjével sem, így $g^{n-1} \not\equiv 1 \ (p^2)$, tehát nem teljesülhet a kongruencia modulo n sem. Ezek szerint az álprímek négyzetmentesek. Hasonló érvelés mutatja, hogy n minden p prímosztójára $p-1 \mid n-1$. Legyen ugyanis most g primitív gyök modulo p. Ekkor $1 \equiv g^{n-1} \ (n)$ miatt $1 \equiv g^{n-1} \ (p)$ is igaz, tehát g rendje (ami $p-1$) osztója $n-1$-nek.

Megfordítva: legyen n négyzetmentes szám, amelyre teljesül, hogy $p \mid n$, p prím esetén $p-1 \mid n-1$. Ekkor minden n-hez relatív prím a esetén $a^{n-1} \equiv \left(a^{p-1}\right)^{\frac{n-1}{p-1}} \equiv 1^{\frac{n-1}{p-1}} = 1 \ (p)$, tehát a kínai maradéktétel szerint $a^{n-1} \equiv 1$ igaz modulo n is. □

6. Tétel. *Ha n álprím, akkor legalább három prímosztója van.*

Bizonyítás. Az előző állítást felhasználva tudjuk, hogy n négyzetmentes, tehát ha nem prím és háromnál kevesebb prímosztója van, akkor csak $n = pq$ fordulhat elő valamely p és q különböző prímekre. Feltehető, hogy $p > q$. Ha g primitív gyök modulo p, akkor $1 \equiv g^{n-1} \equiv g^{pq-1} \equiv (g^p)^q \cdot g^{-1} \equiv g^q \cdot g^{-1} \equiv g^{q-1} \ (p)$. Ezek szerint $q-1$ osztható g rendjével, azaz $p-1$-gyel, ami lehetetlen, mert $p > q$. □

Rabin–Miller-teszt Legyen n páratlan egész, $n-1 = 2^r s$ és a egy n-hez relatív prím szám. Ekkor

$$a^{n-1} - 1 = a^{2^r s} - 1 = (a^s - 1) \cdot (a^s + 1) \cdot \left(a^{2s} + 1\right) \cdot \left(a^{2^2 s} + 1\right) \ldots \left(a^{2^{r-2} s} + 1\right) \cdot \left(a^{2^{r-1} s} + 1\right)$$

Ha n prím, akkor $a^{n-1} - 1 \equiv 0 \ (n)$ és így az előbbi szorzat valamelyik tényezője osztható n-nel. Másképpen megfogalmazva, ha az $a^s \equiv 1 \ (n)$, $a^{2^i s} \equiv -1 \ (n)$ $(i = 0, 1, \ldots, r-1)$ kongruenciák közül egyik sem teljesül, akkor n összetett. A Rabin–Miller-teszt ezen az összefüggésen alapul.

Rabin–Miller-teszt:
1. Válasszunk egy $0 < a < n$ egész számot.
2. $(a, n) \stackrel{?}{=} 1$ Ha nem $\Rightarrow$ n összetett. Ha igen $\Rightarrow$
3. $a^s \stackrel{?}{\equiv} 1 \ (n)$, $a^{2^i s} \stackrel{?}{\equiv} -1 \ (n)$ $(i = 0, 1, \ldots, r-1)$.

Ha semelyik sem teljesül $\Rightarrow$ n összetett. Ha valamelyik teljesül $\Rightarrow$ n *valószínűleg* prím.

7. Definíció. Legyen n páratlan összetett szám, $n-1 = 2^r s$, ahol s páratlan és $(a, n) = 1$. Ekkor az a az n összetettségének *Rabin–Miller-tanú*ja, ha $a^s \not\equiv 1 \ (n)$, továbbá $a^{2^i s} \not\equiv -1 \ (n)$ minden $0 \le i \le r-1$ esetén. Egyébként a *Rabin–Miller-cinkos.*

A következő tételek biztosítják, hogy a Rabin–Miller-teszt minden számra nagy valószínűséggel helyes eredményt ad. Az elsőt nem bizonyítjuk, bár nem volna túlságosan bonyolult.

8. Tétel. *Minden páratlan összetett számhoz létezik Rabin–Miller-tanú.*

9. Tétel. *Minden páratlan összetett számhoz van legalább $\frac{\varphi(n)}{2}$ Rabin–Miller-tanú.*

Bizonyítás. Az állítás teljesen igazolható, mint a Fermat-tesztre vonatkozó hasonló tétel, felhasználva, hogy most az előző állítás biztosítja legalább egy Rabin–Miller-tanú létezését. □

A prímtesztelési eljárásból a Fermat-tesztnél látott módon kaphatunk olyan módszert, ami nagy valószínűséggel helyes erdményt ad. Legyen tehát n páratlan egész szám. Válasszunk a egészet ismét véletlenszerűen az $[1, n-1]$ intervallumból. Az imént igazolt tétel szerint ha n összetett, akkor több, mint $\frac{1}{2}$ valószínűséggel máris találtunk egy Rabin–Miller-tanút, tehát az eljárást k-szor ismételve kevesebb, mint $\frac{1}{2^k}$ a valószínűsége, hogy csupa cinkost választottunk. Ha tehát ezek után azt állítjuk, hogy n prím, akkor a tévedés valószínűsége kisebb, mint $\frac{1}{2^k}$. Természetesen ha az eljárás során azt derül ki, hogy n összetett, akkor ezt viszont egészen biztosan (tehát nem csupán nagy valószínűséggel) állíthatjuk.