

Számelmélet 2005/2006 ősz

13. gyakorlat: Prímtesztek

Legyen n egész összetett és $(a, n) = 1$. Ekkor a szám n összetettségének *Fermat-tanúja*, ha $a^{n-1} \not\equiv 1 \pmod{n}$ és a az n *Fermat-cinkosa*, ha $a^{n-1} \equiv 1 \pmod{n}$.

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-tanúja*, ha $a^s \not\equiv 1 \pmod{n}$, továbbá $a^{2^i s} \not\equiv -1 \pmod{n}$ minden $0 \leq i < r$ esetén. Egyébként a *Rabin–Miller-cinkos*.

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

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

1. Keressünk egy-egy Fermat-tanút 21 és 143 összetettségének bizonyítására.
2. Igazoljuk, hogy 561 álprím (tehát a Fermat-teszten átmegy). Mutassunk Rabin–Miller-tanút, amely viszont lebuktatja. Oldjuk meg a feladatot 1729-re is.
3. Mutassuk meg, a fenti tétel felhasználásával, hogy ha n páratlan összetett szám, akkor legalább annyi Rabin–Miller tanúja van, mint cinkosa.
4. Az előző feladat alapján hogyan lehet eldönteni legalább 99%-os biztonsággal, hogy 1601 prím-e? És ha 90%-os biztonsággal is beérjük? (Egyébként valóban prím.)
5. Igazoljuk, hogy amennyiben m páratlan szám összetettségének a Fermat-tanúja, akkor a egyben Rabin–Miller-tanú is.
6. Mutassuk meg, hogy az álprímek négyzetmentesek.
7. Bizonyítsuk be, hogy egy álprímnek legalább három prímosztója van.