Számelmélet 2006/2007 ősz
10. gyakorlat: Prímtesztek

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

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

Ha n összetett számhoz nem létezik Fermat-tanú, akkor n *Carmichael-szám*, másnéven *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.

• 3. Oldjuk meg az előző feladatot 1729-re.

4. Mutassuk meg, hogy ha n összetett szám, de nem álprím, akkor legalább annyi Fermat-tanúja van, mint cinkosa.
5. Bizonyítsuk be a fenti tétel felhasználásával, hogy ha n páratlan összetett szám, akkor legalább annyi Rabin–Miller-tanúja van, mint cinkosa.
6. Hogyan lehet eldönteni legalább 99%-os biztonsággal, hogy 1601 prím-e? És ha 90%-os biztonsággal is beérjük? (Egyébként valóban prím.)

• 7. Igazoljuk, hogy amennyiben m páratlan szám összetettségének a Fermat-tanúja, akkor a egyben Rabin–Miller-tanú is.

8. Mutassuk meg, hogy az álprímek négyzetmentesek.

• 9. Bizonyítsuk be, hogy egy álprímnek legalább három prímosztója van.