

Számelmélet 2004/2005 ősz

12. gyakorlat: Prímtesztek

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. 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.