

# Diszkrét matematika II. feladatok

5.

## Bemelegítő feladatok

1. Oldja meg az alábbi kongruneciákat az Euler-Fermat tétel segítségével:
  - a)  $2x \equiv 1 \pmod{7}$ ; b)  $3x \equiv 2 \pmod{11}$ ; c)  $5x \equiv 3 \pmod{8}$ ; d)  $3x \equiv 2 \pmod{11}$
  - e)  $6x \equiv 3 \pmod{15}$ ; f)  $14x \equiv 2 \pmod{13}$ ; g)  $5x \equiv 3 \pmod{33}$ ; h)  $15x \equiv 12 \pmod{42}$
2. Oldja meg az alábbi lineáris diofantikus egyenleteket kongruenciák segítségével:
  - a)  $27x + 35y = 3$ ; b)  $33x + 23y = 2$ ; c)  $33x + 15y = 6$ ; d)  $18x + 14y = 16$ .
3. a) Számolja ki a 4 ill. 5 hatványait modulo 7! b) Ellenőrizze, hogy 4 ill. 5 generátor-e modulo 7! c) Legyen  $g$  egy generátor modulo 7, és adja meg a  $\log_g(6)$  értékét!

## Gyakorló feladatok

4. Igazolja, hogy  $g = 2$  generátor modulo 11. Számolja ki továbbá a következő értékeket a diszkrét logaritmus tulajdonságai segítségével. Az eredményt ellenőrizze!
  - a)  $\log_2(2)$ ; b)  $\log_2(4)$ ; c)  $\log_2(5)$ ; d)  $\log_2(10)$  e)  $\log_2(9)$ ; f)  $\log_2(7)$
5. A Diffie-Hellman kulccsere protokollnál legyen  $p = 11$  és  $g = 2$ . Legyen Alice titkos kulcsa  $a = 3$  és Bob titkos kulcs  $b = 4$ . Mi lesz a közös kulcsuk?
6. A Diffie-Hellman kulccsere protokollnál legyen  $p = 13$  és  $g = 2$ . Legyen Alice nyilvános kulcsa 7 és Bob titkos kulcs  $b = 4$ . Mi lesz a közös kulcsuk?

## Érdekes feladatok

7. Felhasználva, hogy  $g = 2$  generátor modulo 13, számolja ki a következő értékeket a diszkrét logaritmus tulajdonságai segítségével. Az eredményt ellenőrizze!
  - a)  $\log_2(2)$ ; b)  $\log_2(4)$ ; c)  $\log_2(3)$ ; d)  $\log_2(6)$  e)  $\log_2(5)$ ; f)  $\log_2(10)$
8. A Diffie-Hellman kulccsere protokollnál legyen  $p = 17$  és  $g = 3$ . Legyen Alice nyilvános kulcsa 7 és Bob nyilvános kulcsa 8. Mi lehet a közös kulcsuk?

---

## Szorgalmi feladatok

9. Emlékeztető Dimat1-ből: „*Egy hotelba 100 fős társaság érkezik, akik közül kezdetben bármely két ember jóban van egymással. Esténként egyetlen nagy kerek asztal köré ül le mindenki. Sajnos egy vacsora alatt az egymás mellé került emberek örökre összevesznek egymással. A társaság minden vacsora előtt úgy ül le, hogy a szomszédjaival jóban legyen. Ha ez lehetetlen, akkor minden résztvevő aznap este hazamegy. Ekkor legalább 25 éjszakát a hotelben tölt a társaság!*”  
Feladat: mutsson módszert (ülésrendet), hogyan tud a társaság  $\varphi(100)/2 = 20$  éjszakát ott eltölteni