Számelmélet II.

(Kongruenciák, Euler–Fermat-ttel)

Diszkrét modellek alkalmazásai feladatsor

Gyakorlatvezető: Uray M. János

1. Kimerítő kereséssel oldjuk meg:

$$5x^{10} + 3x^2 - 6x \equiv 7 \pmod{1237}$$

2. Kimerítő kereséssel oldjuk meg a kongruenciarendszert:

$$\begin{aligned} x^2 + 3xy - 2y^2 + 3x + 4 &\equiv 0 \pmod{197} \\ (x^2+1)x + 2y &\equiv 0 \pmod{197} \\ y - 2x &\equiv 3 \pmod{197} \end{aligned}$$

3. Oldjuk meg a tanult módszerrel:
   a) $5170549x \equiv 12345689 \pmod{4195813}$
   b) $5170549x \equiv 12345679 \pmod{4195813}$

4. A kínai maradéktétel segítségével oldjuk meg:
   a) $\begin{aligned} x &\equiv 2 \mod 7 \\ x &\equiv 5 \mod 8; \end{aligned}$ b) $\begin{aligned} 154547x &\equiv 50340 \mod 111111 \\ 48675x &\equiv 16054 \mod 65536; \end{aligned}$

5. a) Generáljuk 2, 3 és 4 hatványait modulo 5. Mit veszünk észre?
   b) Generáljuk $1, 2, 3, \ldots, p-1$ hatványait modulo p különböző p prímszámokra. Mit veszünk észre? Mi a szabály?
   c) Mi a helyzet nem prímszámok esetén?

6. Számítsuk ki a Sage moduláris hatványozás funkciói nélkül, majd ellenőrizzük vele:
   a) $173^{163} \pmod{17}$;
   b) $3^{123456789} \pmod{100}$;
   c) $1948211768^{241243598} \pmod{195427}$;
   d) $128^{123456789} \pmod{1000}$.

7. a) Írjunk függvényt, amely egy bemenő `n`-re kiszámítja az Euler-féle φ-függvény értékét (ne használjuk a beépített függvényt). (Tipp: induljunk ki a prímtényezős felbontásból, `list(factor(n))`-ből.)
   b) Teszteljük a beépített függvény segítségével 1-től 10000-ig minden számra.

8. a) Írjunk két függvényt a következők szerint. Mindkettő két prímszámot vár paraméterként (p és q). Az első visszaadja a szorzatukhoz, mint modulushoz tartozó nyilvános RSA-kulcsot, azaz az (n, e) párt (a nyilvános exponens legyen a szabványos $2^{16} + 1$ érték). A másik függvény a titkos kulcsot, (n, d)-t adja vissza, ahol a titkos exponenst a szabványos nyilvános exponensből számítja ki.

   b) Írjunk egy kódoló függvényt, amely bementként vár egy RSA-kulcsot (akár nyilvános, akár titkos) és egy üzenetet, és visszaadja a kódolt értéket (vagy kódoltból az üzenetet, a kulcstól függően).

   c) Vegyünk két hatjegyű prímszámot, számítsuk ki belülők az RSA-kulcsokat az első két függvény segítségével, majd a harmadik függvénnyel kódoljunk az 123456 üzenetet, és ellenőrzésként dekódoljuk.