

### 13. gyakorlat

#### Euklideszi-algo, prímtesztelés, titkosírás

- (a) Határozzuk meg az Euklideszi algoritmussal  $(504, 372)$ -t!  
(b) Írjuk fel  $(504, 372)$ -t  $504x + 372y$  alakban!
- Mutassuk meg, hogy 561 Carmichael-szám, vagyis összetett, de nincsen áruelője.  $(561 = 3 \cdot 11 \cdot 17)$
- Határozzuk meg a dekódoló függvényt a  $C(x) = x^5 \pmod{299}$  nyilvános kulcsú kódoláshoz!

---

4. Legyen  $p$  7-hatvány,  $q$  pedig 5-hatvány. Bizonyítsuk be, hogy léteznek olyan  $k$  és  $l$  pozitív egészek, hogy ha egy  $p$ -fejű sárkány minden fejének  $k$  darab és egy  $q$  fejű sárkány minden fejének  $l$  darab almát adunk, akkor valamelyik sárkánynak épp egy almával jut több!

5. Az (angol) ábécé huszonhat betűjét a  $0, 1, \dots, 25$  számokkal helyettesítem ( $A = 0, B = 1, C = 2, \dots, Z = 25$ ). Nyilvános kódolófüggvényem:

$$x \mapsto x^{43} \pmod{85}.$$

(Ezzel a  $0, 1, \dots, 84$  számokat lehet kódolni, de csak az első huszonhat számnak van valódi jelentése.) Ezzel a függvénnyel kódoltam titkos üzenetemet is:

59 2 59 20 44 52

Törd fel a kódomat, vagyis készíts a fenti kódolófüggvényhez dekódolófüggvényt, majd fejtse meg vele titkos üzenetemet!

---

6. A XV. században is nagy hangsúlyt fektettek a biztonságos adatátvitelre, ezért minden király készítettett magának egy lakatot egyetlen kulccsal. A titkos leveleket, kódexeket egy acél ládába tették, a biztonságos szállítás egyetlen módja a lelakatolt ládában történő továbbítás volt. Milyen eljárással küldhetett Mátyás király Artúr nevű kollégájának titkos üzenetet úgy, hogy saját kulcsát egyik sem adta ki a kezéből?

7. Aliz és Béla telefonon keresztül sakkoznak. Ha a játszma függőben marad, akkor az aki utoljára lépne, borítékolja ezt a lépését (ha nem így tenné, akkor a másiknak egy nap gondolkodási ideje lenne). Hogy lehet ezt telefonon át megtenni? (Például, ha Aliz borítékol, akkor Béla másnapig nem tudhatja, hogy Aliz mit lépett, Aliz viszont nem változtathatja meg lépését később.)