

Lukuteoria

Harjoitus 9/2007

Tehtävissä (ja jatkossa ylipäätään) on suositeltavaa käyttää Maplea apuna numerolaskuissa.

1. Määrää lukujen 5040 ja 36000 positiivisten tekijöiden lukumäärä.
2. Olkoon $n = 2^q$, missä $2^{q+1} - 1$ on alkuluku. Osoita, että $\sigma(\sigma(n)) = 2n$.
3. Olkoon $n = 2^{p-1}(2^p - 1)$, missä $2^p - 1$ on alkuluku. Osoita, että n on täydellinen luku.
4. Tarkastellaan 1-dimensionaalista affinia kryptausmuunnosta

$$C \equiv aP + b \pmod{26}, \quad 0 \leq C \leq 25,$$

missä $a, b \in \{0, 1, \dots, 25\}$ ovat vakioita siten, että $\text{syte}(a, 26) = 1$. Osoita, että dekryptausmuunnos saadaan ehdosta

$$P \equiv \bar{a}(C - b) \pmod{26}, \quad 0 \leq P \leq 25,$$

missä $\bar{a}$ on luvun a käänteisluku modulo 26.

5. Kryptoteksti IVHYXNAJOF on kryptattu käyttäen affinia muunnosta

$$C \equiv 23P + 7 \pmod{26}.$$

Dekryptaa teksti.

6. Määrää matriisin

$$A = \begin{pmatrix} 23 & 3 \\ 10 & 25 \end{pmatrix}$$

käänteismatriisi modulo 26.

7. Dekryptaa teksti UW DM NK QB EK, joka on aikaan saatu 2-dimensionaalisella Hillin kryptausmuunnoksella

$$\begin{aligned} C_1 &\equiv 23P_1 + 3P_2 \pmod{26} \\ C_2 &\equiv 10P_1 + 25P_2 \pmod{26}. \end{aligned}$$