APPROBATUR 3 (MATP170)
Harjoitus 5
KESKIVIIKKONA **29.4** 10-12 MaD381 ja 12-14 MaD245.
To 30.5 ja Pe 1.5 EI opetusta!

JYVÄSKYLÄN YLIOPISTO

1. Luettele kaikki neljän alkion joukon permutaatiot ts. luettele joukon S_4 alkiot.

2. Olkoot

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \text{ja} \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Etsi sellaiset permutaatiot x, y ja z, että yhtälöt

$$\sigma x = \rho, \quad y\rho = \sigma \quad \text{ja} \quad \rho z \sigma = \mathrm{id}$$

pätevät.

3. Miten monta sellaista permutaatiota, jotka kuvaavat alkion 1 itselleen, on ryhmässä S_5? Entä sellaisia, jotka kuvaavat alkiot 1 ja 3 toisikseen?

4. Anna esimerkit ryhmän S_4 permutaatioista σ ja ρ, joille pätee $\sigma\rho \neq \rho\sigma$. Entä löydätkö sellaiset σ ja ρ, joille edellinen yhtäsuuruus pätee ja kumpikaan permutaatioista ei ole identtinen permutaatio?

5. Onko kuvaus $f(k) \equiv 4k + 3$ joukon $\mathbb{Z}_{24}$ permutaatio? Entä kuvaus $g(k) \equiv 7k$?

6. Jos muutetaan kirjaimet numeroiksi numeroimalla ne aakkosjäjestyksen mukaisesti, niin saadaan englannin kielessä 26 eri numeroa ja suomen kielessä 29 eri numeroa (Muista ÅÄÖ!). Miksi englannin kielisen lauseen salaamisessa EI ole järkevää käyttää funktiota $f(k) \equiv 13k + 5$? Onko tämän funktion käyttö järkevää suomen kielisen tekstin salaamisessa? Keksitkö muita muotoa $ak + b$ olevia funktioita, joita ei kannata käyttää englannin kielisen tekstin salaamiseen?

7. Pura seuraavat funktiolla $f(k) \equiv 5k + 11 \pmod{29}$ salatut viestit:

(a) 5 16 4 4 0 23 16

(b) 28 24 16 23

(c) 27 27 19 27 19 24 27

(d) 8 27 4 4 27 19 !

8. Ilmoita permutaatio

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 5 & 11 & 6 & 1 & 15 & 13 & 2 & 9 & 4 & 16 & 14 & 3 & 12 & 7 & 8 & 10 \end{pmatrix}$$

erillisten kiertojen tulona.

9. Osoita, että jos permutaatiot $\tau_1 \in S_n$ ja $\tau_2 \in S_n$ ovat eri vaihtoja siten, että $\tau_1(k) \neq k$, niin löytyy vaihdot σ_1 ja σ_2 siten, että $\sigma_1(k) = k$, $\sigma_2(k) \neq k$ ja

$$\tau_2\tau_1 = \sigma_2\sigma_1.$$

10. Salakirjoitus 12 0 26 3 3 26 5 20 20 25 5 on salattu säännöllä $f(p) \equiv p + k \pmod{29}$, jollekin $k = 0, 1, 2, 3, \ldots, 28$. Mikä on k ja mitä viestissä lukee, jos salaamattoman tekstin viimeinen kirjain on A?

Ensi viikolla vain YKSI laskuryhmä Ti 18-20 MaD259