

Algebra I (2009)

Harjoitus 4/viikko 47

- (1) (a) Muodosta ryhmän \mathbb{Z}_9^* ryhmätaulu.
(b) Etsi ryhmätaulun avulla luvun 7 käänteisalkio modulo 9.
(c) Onko \mathbb{Z}_9^* syklinen?
- (2) Salasanataulukossa on seuraavat kolme kryptattua salasanaa: $\bar{5}, \bar{7}, \bar{9}$. Anna salasanat, kun salausfunktiona käytettiin kuvausta

$$\{1, \dots, 10\} \rightarrow \mathbb{Z}_{11}^*, m \mapsto \bar{2}^m.$$

- (3) Pertin puolikas Diffien-Hellmanin salausavaimesta on $\bar{6}$ ja Elisan $\bar{3}$. Mikä on heidän yhteinen salausavaimensa, kun $m = 11$ ja ryhmän \mathbb{Z}_{11}^* generoijaksi valitaan $\bar{2}$?
- (4) Olkoon G ryhmä. Todista:
(a) G :n neutraalialkio on yksikäsitteinen.
(b) Jokaisella G :n alkiolla on yksikäsitteinen käänteisalkio.
(c) Jos G on äärellinen, niin sen ryhmätaulussa jokainen alkio esiintyy kullakin rivillä ja sarakeella täsmälleen kerran.

Olkoon (G, \cdot) ryhmä, ja olkoon $\emptyset \neq H \subseteq G$. Jos myös (H, \cdot) on ryhmä, niin se on G :n *aliryhmä*.

- (5) Olkoon (G, \cdot) äärellinen ryhmä ja (H, \cdot) sen aliryhmä. Todista:
(a) on olemassa alkio $a_1, \dots, a_t \in G$, joille pätee

$$G = a_1H \cup a_2H \cup \dots \cup a_tH,$$

missä $a_iH = \{a_ih \mid h \in H\}$ ja $a_iH \neq a_jH$ kaikilla $1 \leq i < j \leq t$.

- (b) $t = |G|/|H|$.
(c) $a^{|G|} = 1 \forall a \in G$.
(d) Todista Fermat'n pieni lause käyttäen kohtaa (c).
- (6) Olkoon G ryhmä, jonka alkioiden lukumäärä on alkuluku. Etsi kaikki G :n aliryhmät.