

Algebra I (2009)

Harjoitus 5/viikko 48

- (1) Olkoon $A = \{a, c, \dots, y, z\}$ ja käytetään vastaavuutta $a \leftrightarrow 1, b \leftrightarrow 2, \dots, z \leftrightarrow 26$. Koodataan 2-pituiset merkkijonot 32-järjestelmän luvuiksi; esim. $bc \mapsto 2 \cdot 32 + 3$. Olkoon julkinen salausavain $(e, m) = (11, 10403)$. Murra salattu viesti 1450.
- (2) Laske jakojäännös $x^5 + x^2 + 1 \pmod{3x^2 + 2x + 8}$ renkaassa $\mathbb{Z}_{11}[x]$.
- (3) Etsi kaikki jaottomat astetta neljä olevat \mathbb{Z}_2 -kertoimiset polynomit.
- (4) Olkoon G syklinen ryhmä ja H sen aliryhmä.
 - (a) Osoita, että H on syklinen.
 - (b) Oletetaan, että $G = \langle g \rangle$, $|G| = n$. Todista:
 - (i) $g^i = g^j \Leftrightarrow i \equiv j \pmod{n}$.
 - (ii) Jokaista luvun n tekijää d kohti on täsmälleen yksi kertalukua d oleva G :n aliryhmä H .
 - (a) Etsi kaikki ryhmän (\mathbb{R}^*, \cdot) äärelliset aliryhmät.
 - (b) Etsi kaikki ryhmän $(\mathbb{Z}, +)$ aliryhmät.
- (5) (a) Etsi jokin ryhmän \mathbb{F}_{16}^* generoija, kun $\mathbb{F}_{16} = \mathbb{Z}_2[x]_{(x^4+x^3+x^2+x+1)}$.
(b) Etsi kaikki ryhmän \mathbb{F}_{16}^* aliryhmät.
- (6) Olkoon $(R, +, \cdot)$ rengas, jossa on vähintään kaksi alkioita. Todista:
 - (a) $0 \cdot a = 0$ kaikilla $a \in R$.
 - (b) $1 \neq 0$.
 - (c) $(-1)a = -a$ kaikilla $a \in R$.
 - (d) jos R on kunta ja $a, b \in R$, niin pätee: $ab = 0 \Rightarrow a = 0$ tai $b = 0$.