LUKUTEORIA JA RYHMÄT

Loppukoe 19.3.2012

Ei laskimia, ei matkapuhelimia, ei taulukkokirjoja

1. a) Olkoon $a \equiv b(m)$ ja $c \equiv d(m)$. Osoita, että tällöin
$$ac \equiv bd(m).$$
   b) Ratkaise kongruenssiyhtälö
$$6x \equiv 8(20).$$
   Perustele miksi ratkaisu on olemassa.

2. a) Määrää Eukleideen algoritmin avulla lukujen 136 ja 426 suurin yhteinen tekijä syt(136,426) ja etsi sellaiset kokonaisluvut u ja v, että $\text{syt}(136, 426) = 136u + 426v$.
   b) Määritellään joukossa $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ relaatio R seuraavasti: aRb, jos $ab > 0$. Osoita, että R on ekvivalenssirelaatio.

3. a) Määrää ryhmän $(\mathbb{Z}_{14}^*, \cdot)$ alkiot ja esitä ryhmätaulu.
   b) Onko ryhmä $(\mathbb{Z}_{14}^*, \cdot)$ syklinen? Perustele!
   c) Määrää ryhmän $(\mathbb{Z}_{14}^*, \cdot)$ kaikki aliryhmät. Perustele!

4. a) Olkoon G Abelin ryhmä ja määritellään kuvaus $f : G \to G$ s.e
$$f(a) = (a^{-1})^2 \text{ aina, kun } a \in G.$$
   Osoita, että kuvaus f on ryhmähomomorfismi.
   b) Olkoon $G = (\mathbb{Z}_{14}^*, \cdot)$. Määrää a)-kohdan homomorfismin f ydin $\text{Ker}(f)$ ja kuva $\text{Im}(f)$.
   c) Muodosta b)-kohdan ryhmien nojalla tekijäryhmä $G/\text{Ker}(f)$ ja esitä sen ryhmätaulu.

5. a) Olkoon G ryhmä ja $N \trianglelefteq G$. Osoita, että sivuluokkien tulo $aN \cdot bN = abN$ on hyvin määritelty.
   b) Olkoon $(G, \cdot)$ ääretön syklinen ryhmä. Osoita isomorfismin määritelmään perustuen, että
$$(G, \cdot) \cong (\mathbb{Z}, +).$$

Laskut täydellisesti näkyviin, pelkkä vastaus ei riitä.

Perustele ratkaisusi täydellisesti.