Aalto-yliopisto

Gripenberg, Ketola

MS-A0402 Diskreetin matematiikan perusteet
2. välikoe 10.4.2014

Kirjoita jokaiseen koepaperiin nimesi, opiskelijanumerosi ym. tiedot !
Laskimia tai taulukoita ei saa käyttää tässä kokeessa!

1. Lukujen 60 ja 46 suurin yhteinen tekijä on 2 koska Eukleideen algoritmin avulla saadaan

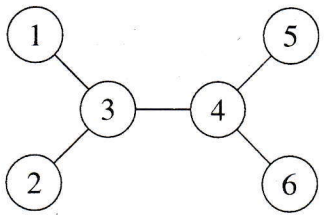
$$\begin{aligned} 60 &= 1 \cdot 46 + 14, \\ 46 &= 3 \cdot 14 + 4, \\ 14 &= 3 \cdot 4 + 2, \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Määritä tämän laskun avulla joitakin kokonaislukuja x ja y siten, että $4 = 60x + 14y$.

2.

(a) Jos RSA-algoritmissa julkinen avain on (n, k) niin miten löydetään yksityinen avain?
(b) Miten nähdään, ettei jäännösluokalla $[12]_{32}$ ole käänteisalkiota joukossa $\mathbb{Z}/32\mathbb{Z}$?
(c) Oletetaan, että $[G, \bullet]$ on ryhmä. Osoita, että neutraalialkio on yksikäsitteinen, eli jos e ja $\hat{e} \in G$, $e \bullet x = x \bullet e = x$ ja $\hat{e} \bullet x = x \bullet \hat{e} = x$ kaikilla $x \in G$ niin $e = \hat{e}$.

3. Määritä kaikki joukon $\{1, 2, 3, 4, 5, 6\}$ permutaatiot, jotka ovat alla olevan verkon isomorfismeja (eli kun solmut permutoidaan, naapurit pysyvät naapureina):



Kirjoita vastauksesi syklimerkinnöillä ja määritä näiden permutaatioiden muodostaman ryhmän sykli-indeksi.

KÄÄNNÄ!!!

4. Määritä alla olevan verkon $[V, E]$ minimaalinen virittävä puu käyttämällä algoritmia, joka takaa optimaalisen tuloksen (mutta sinun ei tarvitse osoittaa, että algoritmi antaa optimaalisen tuloksen). Selitä miten ole menetellyt esimerkiksi kirjoittamalla missä järjestyksessä olet lisännyt solmuja ja/tai kaareja.