Aalto-yliopisto

Gripenberg, Potka, Pöllänen, Tuhkanen, Ääri

MS-A0401 Diskreetin matematiikan perusteet
2. välikoe 22.10.2015

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

1. U ja V käyttävät RSA-algoritmia keskinäisessä viestinnässään. U:n julkinen avain on (n_U, k_U) ja yksityinen avain (n_U, d_U). V:n julkinen avain on (n_V, k_V) ja yksityinen avain (n_V, d_V) ja molemmat pitävät tietenkin yksityiset avaimensa salassa muilta. Lisäksi he käyttävät allekirjoituksia varten hajautusfunktiota h. Jos nyt U saa V:ltä viestin, joka salattuna on x ja lisäksi allekirjoituksen, joka on s, niin mitä U:n pitää laskea, jotta hän voisi olla varma siitä, että V on viestin lähettäjä?

2. Alla olevan kuvion rotaatioilla ja peilauksilla saadaan permutaatiot $p_1 = (1)$, $p_2 = (1\ 6)(2\ 5)(3\ 4)$, $p_3 = (1\ 2)(5\ 6)$ ja $p_4 = (1\ 5)(2\ 6)(3\ 4)$.

(a) Mitä pitäisi osoittaa, jotta tulisi todistetuksi, että yllä mainitut permutaatiot muodostavat ryhmän? (Sinun ei tarvitse suorittaa näitä laskuja!)
(b) Määritä tämän ryhmän sykli-indeksi.
(c) Määritä Pólyan lauseen avulla monellako, ryhmän toiminnnan suhteen ei-ekvivalentilla, tavalla kuvion ruudut voidaan värittää kahdella värillä.

3.

(a) Osoita, että jos kahdella yksinkertaisella ja suuntaamattomalla verkolla ei ole sama kromaattinen luku niin ne eivät ole isomorfiset.
(b) Määritä lukujen 38 ja 48 suurin yhteinen tekijä Eukleideen algoritmin avulla.

Käännä!!

4.

(a) Piirrä kuvat kaikista yksinkertaisista suuntaamattomista ei-isomorfisista verkoista, joissa on 4 solmua ja jotka ovat metsiä (eli jokaisesta solmusta on korkeintaan yksi yksinkertainen polku jokaiseen toiseen solmuun).

(b) Määritä alla olevassa verkossa Hamilton-polku tai selitä mistä nähdään ettei sellaista löydy.