Aalto-yliopisto

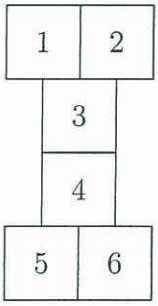
Gripenberg, Potka, Pöllänen, Tuhkanen, Ääri

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.

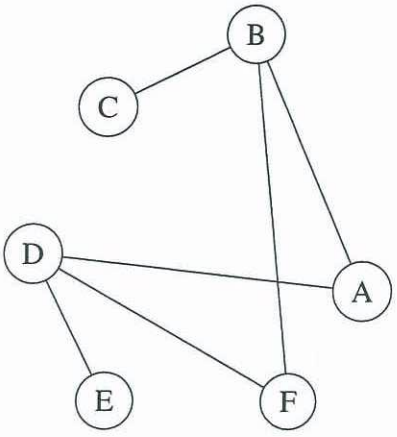
(a) Osoita, että jos kahdella yksinkertaisella ja suuntaamattomalla verkolla ei ole sama kromaattinen luku niin ne eivät ole isomorfiset.
(b) Määritä lukujen 38 ja 48 suurin yhteinen tekijä Eukleideen algoritmin avulla.

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.



Aalto University

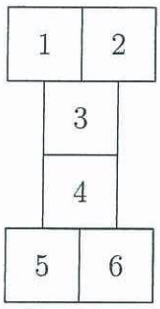
Gripenberg, Potka, Pöllänen, Tuhkanen, Ääri

MS-A0401 Foundations of discrete mathematics
Second midterm exam 22.10.2015

Write your name, student number, and other information on every paper!
Calculators or tables are not allowed in this examination!

1. U and V use the RSA-algorithm to communicate with each other. U has the public key (n_U, k_U) and the private key (n_U, d_U). V has the public key (n_V, k_V) and the private key (n_V, d_V) and both do, of course, keep their private keys secret. In addition they use the hash function h for signing. If now U receives a message, which in encrypted form is x from V and in addition the signature s then what caculations should U do in order to be convinced that V is the sender of the message?

2. With rotations and reflections of the figure below one gets the permutations $p_1 = (1)$, $p_2 = (1\ 6)(2\ 5)(3\ 4)$, $p_3 = (1\ 2)(5\ 6)$, and $p_4 = (1\ 5)(2\ 6)(3\ 4)$.



(a) What should one show in order to prove that these permutations form a group? (You don't have to do these calculations!)
(b) Determine the cycle index of this group.
(c) Determine with the aid of Pólya's theorem in how many, non-equivalent with respect to the action of the group, ways one can colour the squares in the figure using two colours.

3.

(a) Show that if two simple undirected graphs do not have the same chromatic number, then they are not isomorphic.
(b) Determine the greatest common divisor of the numbers 38 and 48 using the Euclidean algroithm.

Turn over!!

4.

(a) Draw pictures of all simple undirected non-isomorhic graphs in which there are 4 nodes and which are forests (that is, there is at most one simpe path from each node to each other node).

(b) Determine a Hamilton path in the graph below or explain why one cannot find such a path.