

MS-A0401 Diskreetin matematiikan perusteet
 Välikoe eli tentti 27.10.2016

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

Vastauksissasi saa numeroiden lisäksi olla potensseja, \cdot , $/$, $+$, $-$, $!$, (ja) mutta ei esimerkiksi binomikertoimia.

1. Osoita induktiopäätelyn avulla (vaikka se olisi mahdollista toisellakin tavalla), että

$$1 + 3 + 5 + \dots + (2 \cdot n - 1) = \sum_{j=1}^n (2 \cdot j - 1) = n^2, \quad n \geq 1.$$

2.

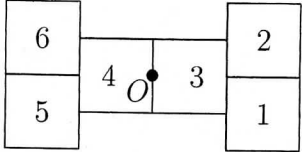
- (a) Yliopiston aulassa on 78 opiskelijaa. Heistä 36 käyvät työsuhdejuridiikan kurssilla, 55 arkkitehtuurigrafiikan kurssilla ja 14 eivät käy kummallakaan kurssilla. Montako opiskelijaa käy sekä työsuhdejuridiikan että arkkitehtuurigrafiikan kurssilla?
- (b) Kokeessa on 14 kysymystä ja niistä on valittava 12 kysymystä, joihin vastataan. Montako vaihtoehtoa on jos lisäksi pitää valita korkeintaan 6 kysymystä kysymyksistä 1 – 7 ja vähintään 5 kysymystä kysymyksistä 8 – 14.

3.

- (a) Selitä määritelmään nojautuen miksi oletuksista $f \in O(n^3)$ ja $g \in O(n^2)$ seuraa, että $f + g \in O(n^4)$.
- (b) Jos RSA-algoritmissa julkinen avain on $(77, 17)$ niin onko yksityinen avain silloin $(77, 3)$? Perustele!

4.

- (a) Alla oleva kuvio pysyy muuttumattomana jos se kierretään 0 tai 180 astetta pisteen O ympäri tai jos kuvio peilataan pisteen O kautta kulkevan joko vaakasuoran tai pystysuoran akselin suhteen. Määritä tällä tavalla saatujen ruutujen 1, 2, 3, 4, 5, 6 permutaatioiden sykliesitykset.



- (b) Joukon $X = \{1, 2, 3, 4, 5\}$ permutaatiot (1) , $(1\ 5)(2\ 4)$, $(1\ 4)(2\ 5)$ ja $(1\ 2)(4\ 5)$ muodostavat ryhmän G (mutta tätä sinun ei tarvitse todistaa). Määritä tämän ryhmän sykli-indeksi.

5.

- (a) Alla olevassa verkossa solmut v_j , $j = 1, 2, \dots, 6$ on "väritetty" väreillä a , b ja c siten, että $\omega(v_1) = b$, $\omega(v_2) = c$, $\omega(v_3) = a$, $\omega(v_4) = b$, $\omega(v_5) = c$ ja $\omega(v_6) = a$. Aseta solmut johonkin järjestykseen siten, että ahne väritysalgoritmi antaa tämän värityksen jos värit ovat aakkosjärjestyksessä.
- (b) Mistä nähdään, ettei tämän verkon solmuja voi värittää kahdella värillä siten, että solmut, joiden välillä on kaari on väritetty eri väreillä.
- (c) Onko alla olevassa verkossa Eulerin polku? Konstruoi sellainen tai selitä miksi se ei ole mahdollista.

