Aalto-yliopisto

Gripenberg

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 induktiopäättelyn avulla (vaikka se olisi mahdollista toisellakin tavalla), että

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

Ratkaisu: Kun $n=1$ niin $\sum_{j=1}^{n}(2\cdot j-1)=\sum_{j=1}^{1}(2\cdot j-1)=2\cdot 1-1=1=1^2$ joten väite pätee tässä tapauksessa.

Oletamme seuraavaksi, että väite pätee kun $n=k$, eli $\sum_{j=1}^{k}(2\cdot j-1)=k^2$. Tämän tuloksen avulla saamme

$$\sum_{j=1}^{k+1}(2\cdot j-1)=\sum_{j=1}^{k}(2\cdot j-1)+(2\cdot(k+1)-1)$$
$$=k^2+2\cdot k+2-1=k^2+2\cdot k+1=(k+1)^2.$$

Näin ollen väite pätee myös kun $n=k+1$ ja induktioperiaatteen nojalla se pätee kaikilla $n\geq 1$.

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 $8-14$.

Ratkaisu: (a) Olkoon A aulassa olevien opiskelijoiden muodostama joukko, B niiden opiskelijoiden joukko, jotka käyvät työsuhdejuridiikan kurssilla ja C niiden opiskelijoiden muodostama joukko, jotka käyvät arkkitehtuurigrafiikan kurssilla. Nyt $|A|=78$, $|B|=36$, $|C|=55$, ja $|A\setminus(B\cup C)|=14$. Koska $B\subset A$ ja $C\subset A$ niin

$$14=|A\setminus(B\cup C)|=|A|-|B\cup C|=78-|B\cup C|,$$

joten $|B\cup C|=64$. Seulaperiaatteen nojalla

$$64=|B\cup C|=|B|+|C|-|B\cap C|=36+55-|B\cap C|=91-|B\cap C|,$$

joten $|B\cap C|=91-64=27$.

(b) Jotta saisimme yhteensä 12 kysymystä kokoon siten, että rajoitukset ovat voimassa meidän pitää valita joko 6 kysymystä kysymysten $1-7$ joukosta ja 6 kysymystä kysymysten $8-14$ joukosta tai 5 kysymystä kysymysten $1-7$ joukosta ja kaikki 7 kysymystä $8-14$.

Nämä valinnat johtavat erilaisiin tuloksiin joten vaihtoehtojen lukumääräksi tulee summa- ja tuloperiaatteen nojalla

$$\binom{7}{6} \cdot \binom{7}{6} + \binom{7}{5} \cdot 1 = 7 \cdot 7 + \frac{7 \cdot 6}{2} = 49 + 21 = 70.$$

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!

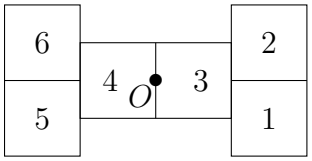
Ratkaisu: (a) Jos $f \in O(n^3)$ niin on olemassa vakiot C_f ja N_f siten, että $|f(n)| \leq C_f \cdot n^3$ kun $n \geq N_f$. Samoin, jos $g \in O(n^2)$ niin on olemassa vakiot C_g ja N_g siten, että $|g(n)| \leq C_g \cdot n^2$ kun $n \geq N_g$. Lisäksi pätee $n^3 \leq n^4$ ja $n^2 \leq n^4$ kun $n \geq 1$ joten oletuksista seuraa, että

$$|f(n) + g(n)| \leq |f(n)| + |g(n)| \leq C_f n^3 + C_g n^2 \leq (C_f + C_g) n^4,$$

kun $n \geq \max(N_f, N_g, 1)$. Määritelmän mukaan pätee siis $f + g \in O(n^4)$.
(b) Koska $n = 77 = 7 \cdot 11$ niin laskemme ensin $m = (7 - 1) \cdot (11 - 1) = 60$. Yksityinen avain (n, d) määräytyy ehdosta $[d]_m = [k]_m^{-1}$ kun julkinen avain on (n, k). Tästä seuraa, että $\operatorname{mod}(d \cdot k, m) = 1$ mutta koska $\operatorname{mod}(3 \cdot 17, 60) = \operatorname{mod}(51, 60) = 51 \neq 1$ niin $(77, 3)$ ei voi olla yksityinen avain.

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 $1, 2, 3, 4, 5, 6$ permutaatioden 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.

Ratkaisu: (a) Permutaatiot ovat

(1)	Kierto 0 astetta,
$(1\ 6)(2\ 5)(3\ 4)$	kierto 180 astetta,
$(1\ 5)(2\ 6)(3\ 4)$	peilaus y-akselin suhteen,
$(1\ 2)(5\ 6)$	peilaus x-akselin suhteen.

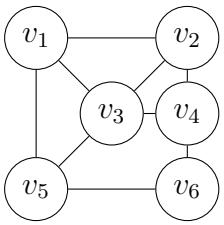
(b) Sykli-indeksi on $\frac{1}{4}\left(t_1^5 + 3t_1 \cdot t_2^2\right)$ koska joukossa X on viisi alkiota joten permutaatiolla (1) in 5 rataa, joniden pituus on 1 ja muilla kolmella permutaatiolla on 2 rataa, joiden pituus on 2 ja 1 rata, jonka pituus on 1

5.

(a) Alla olevassa verkossa solmut v_j, $j = 1, 2, \ldots, 6$ 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.



Ratkaisu: (a) Eräs mahdollinen järjestys on

$$v_6, \quad v_3, \quad v_4, \quad v_1, \quad v_5, \quad v_2$$

(b) Koska esimerkiksi kaikki solmut v_1, v_2 ja v_3 ovat toistensa naapureita niitä ei voi värittää kahdella värillä siten, että jos kahden solmun välillä on kaari niin solmut väritetään eri väreillä joten sama tulos pätee alkuperäiselle verkollekin. Toisella tavalla: $[v_1, v_2, v_3, v_1]$ on yksinkertainen sykli, jonka pituus on pariton ja näin ollen kaksi väriä ei riitä.

(c) Verkossa on 4 solmua. joilla on 3 naapuria ja Eulerin polku on olemassa vain jos on joko 0 tai 2 solmua, joilla on pariton määrä naapureita.