Mat-1.128 Diskreetin matematiikan perusteet

1. välikoe 19.3.2001, ratkaisut

1. Kuinka monta kokonaislukuratkaisua, joille $0 \le x_j \le 6$, on yhtälöllä $x_1 + x_2 + x_3 + x_4 = 16$?

Ratkaisu. Voidaan ajatella, että ykkösiä jaetaan neljään pinoon, niin että x_i saa arvon, joka on i:nnessä pinossa olevien ykkösten lukumäärä. Jos yleisesti n samanlaista esinettä pitäisi jakaa k:hon eri pinoon, tämän voi tehdä $\binom{n+k-1}{n} = \binom{n+k-1}{k-1}$ eri tavalla (n:n esineen ja $k-1$:n väliseinän permutaatiot).

Inkluusio–ekskluusioperiaatteella saadaan kysytyksi lukumääräksi

$$\binom{16+3}{3} - \binom{4}{1}\binom{16-7+3}{3} + \binom{4}{2}\binom{16-2\cdot 7+3}{3} = \frac{19\cdot 18\cdot 17}{3!} + 4\cdot\frac{12\cdot 11\cdot 10}{3!} + \frac{4\cdot 3}{2}\cdot\frac{5\cdot 4\cdot 3}{3!} = 149.$$

Ensimmäinen termi kuvaa kaikkia tapoja jakaa ykköset pinoihin ilman rajoituksia. Sitten on vähennetty tavat tehdä jako niin, että ainakin yhdessä pinossa (jolle on $\binom{4}{1}$ eri vaihtoehtoa) on vähintään pienin kielletty määrä 7, ja loput $16-7$ ykköstä jaetaan vapaasti. Tämän jälkeen on taas lisätty niiden jakojen lukumäärä, joissa 2 pinossa on vähintään 7 ykköstä. Tätä useampaa kiellettyä pinoa ei voikaan olla, koska $16 < 3\cdot 7$.

Vaihtoehtoisesti voisi muodostaa *tavallisen* emäfunktion $(1+x+\ldots+x^6)^4$, jolloin vastaus olisi x^{16}:n kerroin auki kerrotussa muodossa.

2. Miten monella tavalla voivat n opiskelijaa jakautua osallistumaan samanaikaisiin ruotsinkielen ja fysiikan harjoituksiin, tai mennä kahvilaan, kun kunkin em. vaihtoehdoista tekee ainakin yksi opiskelija? Tarkastellaan a) vain lukumääriä, ja b) henkilökohtaisia valintoja.

Ratkaisu. a) Asetetaan ensin kuhunkin kohteeseen 1 opiskelija; tämän jälkeen loput $n-3$ voidaan jakaa vapaasti kolmeen kohteeseen, eli esine–väliseinäajattelulla saadaan lukumääräksi $\binom{n-3+2}{2} = \frac{1}{2}(n-1)(n-2)$.

b) Inkluusio–eksluusioperiaatteella saadaan $3^n - 3\cdot 2^n + 3\cdot 1^n$, missä 3^n kuvaa tapoja jakaa opiskelijat kolmeen kohteeseen ilman rajoituksia, $3\cdot 2^n$ on niiden tapojen lukumäärä, joissa jokin kohde (3 vaihtoehtoa) jää tyhjäksi, jolloin kullakin on vain 2 vaihtoehtoa, ja $3\cdot 1^n$ kuvaa tapauksia, joissa kaksi kohdetta jää tyhjäksi, eli kaikki menevät samaan paikkaan (3 vaihtoehtoa).

Vaihtoehtoisesti voi käyttää eksponentiaalista emäfunktiota: kuhunkin kolmesta kohteesta voi mennä $1, 2, \ldots$ opiskelijaa, mitä kuvaava eksponentiaalinen emäfuntio on $\sum_{k=1}^{\infty} \frac{x^k}{k!} = e^x - 1$. Kokonaistilannetta kuvaa komen tällaisen funktion tulo, eli

$$(e^x-1)^3 = e^{3x} - 3e^{2x} + 3e^x - 1 = \sum_{k=0}^{\infty}\frac{(3x)^k}{k!} - 3\sum_{k=0}^{\infty}\frac{(2x)^k}{k!} + 3\sum_{k=0}^{\infty}\frac{x^k}{k!} - 1 = \sum_{k=0}^{\infty}(3^k - 3\cdot 2^k + 3)\frac{x^k}{k!} - 1,$$

missä $\frac{x^n}{n!}$:n ($n \ge 1$) kertoimeksi nähdään sama $3^n - 3\cdot 2^n + 3$.

3. Olkoon $(G, \circ)$ äärellinen ryhmä ja H sen aliryhmä. Merkitään $a \circ H = \{a \circ h | h \in H\}$, kun $a \in G$. Katsotaan todistetuksi, että jos $a, b \in G$, niin joko $a \circ H = b \circ H$ tai $a \circ H \cap b \circ H = \emptyset$. Osoita, että a) $|a \circ H| = |H|$, ja b) $|H|$ jakaa $|G|$:n.

Ratkaisu. a) Kuvaus $h \mapsto a \circ h$ joukolta H joukolle $a \circ H$ on selvästi surjektio, sillä määritelmän perusteella jokainen $a \circ H$:n alkio on $a \circ h$ eräälle $h \in H$. Se on myös injektio, sillä jos $a \circ h_1 = a \circ h_2$, saadaan ryhmän supistussäännön nojalla $h_1 = h_2$. Siis joukkojen H ja $a \circ H$ alkioiden välillä on kääntäen yksikäsitteinen vastaavuus (bijektio), joten joukot ovat yhtä suuret.

b) Jokainen $g \in G$ kuuluu joukkoon $g \circ H$, sillä $e \in H$, ja $g \circ e = g$. Toisaalta on selvää, että $g \circ H \subset G$, kun $g \in G$, $H \subset G$, sillä G on suljettu ryhmälaskutoimituksen $\circ$ suhteen. Täten $G = \cup_{g \in G}(g \circ H)$, ja mitkä tahansa kaksi tässä yhdisteessä esiintyvää joukkoa ovat joko samat tai täysin erilliset. Olkoot $g_1 \circ H, \ldots, g_k \circ H$ kaikki *eri* joukot, jotka esiintyvät edellä. Tällöin

$$|G| = \left|\bigcup_{i=1}^{k} g_i \circ H\right| = \sum_{i=1}^{k} |g_i \circ H| = \sum_{i=1}^{k} |H| = k|H|,$$

missä toinen yhtälö seuraa $g_i \circ H$:iden erillisyydestä ja kolmas tehtävän (a)-kohdasta. Edellisestä yhtälöstä nähdään, että $|H|$ jakaa $|G|$:n.

4. Kuution sivutahkot maalataan kermanvärisiksi, oransseiksi tai turkooseiksi. Jokin tai jotkin värit saavat myös puuttua. Montako erilaista väristystä voidaan näin muodostaa, kun kappaletta saa vapaasti käännellä avaruudessa? Sovella Polyan lausetta tai siihen liittyviä tuloksia.

Ratkaisu. Määritetään ensin kuution *liikeryhmä* ja kunkin tähän kuuluvan permutaation syklistruktuuri.

1. Identiteettipermutaatio pitää kaikki kuusi tahkoa paikoillaan, joten sillä on kuusi yksialkioista rataa, siis syklistruktuuri x_1^6.

2. Kuutiota voidaan kääntää kahden vastakkaisen sivutahkon läpi kulkevan akselin (tällainen akseli voidaan valita 3:lla tavalla) ympäri $\pm 90°$. Tällöin akselilla olevat sivutahkot (2 kpl) pysyvät paikallaan, ja loput 4 muodostavat radan. Siis syklistruktuuri on $x_1^2 x_4$, ja näitä on $3 \cdot 2 = 6$ kappaletta.

3. Kierretään vastaavan akselin ympäri, kuin edellisessä kohdassakin, mutta 180°. Akselitahkot pysyvät paikallaan, ja muut vaihtavat pareittain paikkaa, eli syklistruktuuri on $x_1^2 x_2^2$, ja näitä on 3 kappaletta (vain akselin valinta, kiertosuunnalla ei ole väliä).

4. Kierretään kahden vastakkaisen kärjen kautta kulkevan akselin ympäri $\pm 120°$. Tällöin kummankin akselikärjen viereiset kolme sivutahkoa muodostavat radan, eli x_3^2. Kärkipari akselille voidaan valita 4 tavalla. (Kärkiä on yhteensä 8; kun toinen on valittu, toinen määräytyy, mutta valitsemalla jokainen kärki kerran, tulee jokainen vastapari kahdesti.) Lisäksi on 2 eri kiertosuuntaa, eli yhteensä $4 \cdot 2 = 8$.

5. Kierretään kahden vastakkaisen särmän keskipisteiden kautta kulkevan akselin ympäri 180°. Muodostuu kolme kahden alkion rataa, eli x_2^3. Akseli voidaan valita 6 tavalla (Särmiä on yhteensä 12, mutta valitsemalla jokainen särmä, tulee jokainen vastapari kahdesti.)

Löydettiin yhteensä $1 + 6 + 3 + 8 + 6 = 24$ permutaatiota. Se, että tässä täytyy olla kaikki, nähdään esim. seuraavasti: Ajatellaan kuutio asetetuksi pöydälle. Sen asento on tarkkaan määrätty, kun tiedetään, mikä tahko on eteenpäin ja mikä ylöspäin. (Kokeile arpakuutiolla, jos et usko!) Lähtemällä liikkeelle jostakin valitusta perusasennosta, määräytyy kuution liikepermutaatio siitä, mihin uuteen asentoon se kääntyy. Nyt edessä olevalle tahkolle on 6 vaihtoehtoa, ja ylöspäin olevalle tahkolle 4 (kaikki edessä olevan tahkon viereiset tahkot). Yhteensä on siis $6 \cdot 4 = 24$ vaihtoehtoa.

Sykli-indeksi on syklistruktuurien keskiarvo:

$$\frac{1}{24}\left(x_1^6 + 6x_1^2 x_4 + 3x_1^2 x_2^2 + 8x_3^2 + 6x_2^3\right).$$

Nyt erilaisten väritysten lukumäärä saadaan sijoittamalla jokaisen x_i:n paikalle käytettävissä olevien värien lukumäärä eli 3, jolloin saadaan

$$\frac{1}{24}\left(3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2 + 6 \cdot 3^3\right) = 57.$$

Tähän olisi voinut päätyä myös sykli-indeksiä kirjoittamatta käyttämällä Burnsiden lemmaa, jossa yllä oleva lauseke olisi muodostettu laskemalla kuution liikeryhmän kunkin permutaation kiintoväritysten lukumäärät. Edellä olevan kaltainen luettelointi olisi ollut joka tapauksessa tarpeen.

Varsinaista Polyan lausetta ei käytetty. Sen avulla olisi voinut tutkia tietyntyyppisten väritysten lukumääriä vielä tarkemmin tekemällä sykli-indeksiin sijoituksen $x_i = k^i + o^i + t^i$, missä k, o ja t tarkoittavat kermanväristä, oranssia ja turkoosia. Tätä ei kuitenkaan pyydetty.

Mat-1.128 Diskreetin matematiikan perusteet

2. välikoe 8.5.2001, ratkaisut

Tehtävä 1. Ratkaise kongruenssiprobleema $\begin{cases} x \equiv 3 \pmod{12} \\ x \equiv 9 \pmod{15} \\ x \equiv 19 \pmod{20} \end{cases}$

Ratkaisu. Ensimmäisen yhtälön perusteella $x = 3 + 12y$ ja toisen perusteella $x = 9 + 15z$. Siis $3 + 12y = 9 + 15z \Rightarrow 12y - 15z = 6 \Rightarrow$ (jaetaan 3:lla)$4y - 5z = 2$. Tämän Diofanteen yhtälön voi ratkaista Eukleideen algoritmilla, mutta tässä tapauksessa pienellä kokeilullakin löytyy helposti ratkaisu $y = z = -2$. Kaikki ratkaisut ovat muotoa $y = -2 + 5n, z = -2 + 4n \Rightarrow x = 3 + 12y = 3 + 12 \cdot (-2) + 12 \cdot 5n = -21 + 60n$.

Toisaalta kolmannen yhtälön perusteella $x = 19 + 20m' = -1 + 20m$. Siis saadaan uusi Diofanteen yhtälö $-21 + 60n = -1 + 20m \Rightarrow 60n - 20m = 20 \Rightarrow 3n - m = 1$. Nähdään helposti, että $n = 1, m = 2$ on eräs ratkaisu, ja kaikki ratkaisut ovat muotoa $n = 1 + k, m = 2 + 3k \Rightarrow x = -1 + 20 \cdot 2 + 20 \cdot 3k = 39 + 60k$.

Siis $\boxed{x \equiv 39 \pmod{60}}$. Huomaa, että $60 = \text{p.y.j.}(12, 15, 20)$.

Tehtävä 2. Muodosta RSA-salakirjoitusavain, joka toteuttaa ehdot: Modulin $n = pq$ tekijät ovat suurin alkuluku, jolle $p < 95$ ja pienin alkuluku, jolle $q > 140$, ja salakirjoituseksponentti on pienin alkuluku, jolle $e > 15$. Muodosta myös vastaava tulkinta-avain. Salakirjoita viesti OK käyttäen kirjain–lukuvastaavuutta $A \leftrightarrow 00$, $B \leftrightarrow 01, \ldots$.

Ratkaisu. Tutkimalla järjestyksessä mahdollisten lukujen jaollisuutta, nähdään että $p = 89$, $q = 149$ ja $e = 17$ ovat tehtävänannossa tarkoitetut luvut. Siis $n = pq = 89 \cdot 149 = 13261$ ja $\varphi(n) = (p-1)(q-1) = 88 \cdot 148 = 13024$. Salausavaimeksi saadaan suoraan $\boxed{(e, n) = (17, 13261)}$.

Tulkinta-avainta varten tarvitaan $d \equiv e^{-1} \pmod{\varphi(n)}$, eli täytyy ratkaista Diofanteen yhtälö $ex - \varphi(n)y = 1$, jolloin $d \equiv x$ on haluttu salauseksponentti. Eukleideen algoritmilla saadaan

$$13024 = 766 \cdot 17 + 2, \qquad 17 = 8 \cdot 2 + 1 \qquad \Rightarrow$$
$$1 = 17 - 8 \cdot 2 = 17 - 8 \cdot (13024 - 766 \cdot 17) = (1 + 8 \cdot 766) \cdot 17 - 8 \cdot 13024 = 6129 \cdot 17 - 8 \cdot 13024.$$

Siis $d = 6129$, ja tulkinta-avaimeksi käy $\boxed{(d, n) = (6129, 13261)}$.

Annetulla kirjain–lukuvastaavuudella $O \leftrightarrow 14$, $K \leftrightarrow 10$. Siis selväkielinen viesti P (plain text) on $P = 1410$, ja salattu viesti C (code) on $C \equiv P^e \pmod{n} \equiv 1410^{17} \pmod{13261}$.

Potenssin laskemista varten havaitaan, että $17 = 16 + 1 = 2^4 + 1$. Seuraavassa kaikki kongruenssit ovat $\pmod{13261}$:

$$1410^2 \equiv -1050, \qquad 1410^4 \equiv (-1050)^2 \equiv 1837, \qquad 1410^8 \equiv 1837^2 \equiv 6275,$$
$$1410^{16} \equiv 6275^2 \equiv 3716, \qquad 1410^{17} \equiv 3716 \cdot 1410 \equiv 1465.$$

Siis lähetettävä viesti on $\boxed{1465}$.

Tehtävä 3. Olkoon $f(x) = x^4 + x^3 + x + 1$. Jaa tämä polynomi redusoitumattomien tekijöiden tuloksi, kun se kuuluu polynomirenkaaseen a) $GF(2)[x]$, b) $GF(3)[x]$, c) $GF(4)[x]$.

Ratkaisu. Selvästi aina (renkaasta riippumatta) $x^4 + x^3 + x + 1 = x^3(x+1) + (x+1) = (x+1)(x^3+1) = (x+1)(x+1)(x^2 - x + 1)$. Jos polynomin kerroinrengas on $GF(2) = \mathbb{Z}_2$, ei tämä enää jakaannu, sillä $0^2 - 0 + 1 = 1 \neq 0$ ja myös $1^2 - 1 + 1 = 1 \neq 0$. $GF(2)$:ssa voidaan kuitenkin miinusmerkki jättää pois. Siis $GF(2)[x]$:ssä kysytty jako on $\boxed{f(x) = (x+1)^2(x^2 + x + 1)}$.

Renkaassa $GF(3) = \mathbb{Z}_3$ saadaan $(-1)^2 - (-1) + 1 = 1 + 1 + 1 = 3 = 0$, joten polynomi $x^2 - x + 1$ jakaantuu edelleen. Jako voidaan tehdä jakokulmassa, mutta helpommin havaitsemalla suoraan, että $\mathbb{Z}_3$:ssa $x^2 - x + 1 = x^2 + 2x + 1 = (x+1)^2$. Siis $GF(3)[x]$:ssä $\boxed{f(x) = (x+1)^4}$.

Koska $4 = 2^2$ ei ole alkuluku, $GF(4) \neq \mathbb{Z}_4$. Sen sijaan $GF(4)$ muodostetaan renkaasta $GF(2) = \mathbb{Z}_2$ jaottoman 2. asteen polynomin avulla. Tällainen on esim $u^2 + u + 1$, joten $GF(4) = \{a + bu : a, b \in \mathbb{Z}_2, u^2 + u + 1 = 0\} = \{0, 1, u, u+1\}$. Nyt polynomilla $x^2 - x + 1 = x^2 + x + 1$ on juuri u (suoraan u:n määritelmän perusteella). Jakolaskulla saadaan

$$\frac{x^2 + x + 1}{x + u} = x + \frac{(u+1)x + 1}{x + u} = x + (u+1) + \frac{u^2 + u + 1}{x + u} = x + (u+1),$$

sillä $u^2 + u + 1 = 0$. Siis $GF(4)[x]$:ssä $\boxed{f(x) = (x+1)^2(x+u)(x+u+1)}$.

Tehtävä 4. Hammingin $(7,4)$-koodilla on tarkistusmatriisi $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$.

a) Muodosta vastaava generoiva matriisi, ja koodaa viestit 0101 ja 1011.

b) Tulkitse vastaanotetut sanomat 1010010 ja 1110011.

c) Sanomien välityksessä käytetään symmetristä binäärikanavaa, jolla yhden virhebitin todennäköisyys on $p = 0,8\%$. Millä todennäköisyydellä a-kohdassa lähetetyt sanomat tulevat oikein tulkituiksi?

Ratkaisu. a) Kun tarkistusmatriisi on muotoa $H = (A^T \vdots I)$, on generoivamatriisi $G = (I \vdots A)$, missä I on aina sopivan kokoinen yksikkömatriisi. Siis generoiva matriisi on

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \vdots & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & \vdots & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & \vdots & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & \vdots & 0 & 1 & 1 \end{pmatrix}.$$

Annettu viesti p koodataan (matriisi)kertolaskulla pG, joten

$$0101 \mapsto \boxed{0\,1\,0\,1\,1\,0\,1} \qquad 1011 \mapsto \boxed{1\,0\,1\,1\,0\,0\,1}.$$

b) Vastaanotettu viesti r tarkistetaan (matriisi)kertolaskulla Hr^T, jolloin saadaan

$$H\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad H\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Ensimmäisessä tapauksessa tulkitaan, että viestissä ei ole virhettä. Varsinainen sanoma on neljässä ensimmäisessä bitissä, eli viesti on $\boxed{1010}$. Toisessa tapauksessa saatiin tarkistusmatriisin H ensimmäinen sarake, mikä tulkitaan niin, että viestin ensimmäinen bitti on virheellinen. Siis oikea viesti on 0110011 ja varsinainen sanoma $\boxed{0110}$ (taas neljä ensimmäistä bittiä).

c) Yksittäinen neljän bitin sana saadaan tulkittua oikein, jos siinä on korkeintaan yksi virhe (eli joko 0 virhettä tai tasan 1 virhe). Siis tämän todennäköisyys on $(1-p)^7 + \binom{7}{1}(1-p)^6 p = 0,99869141$. Todennäköisyys, että kaksi kappaletta sanoja saadaan oikein, on edellinen luku potenssiin 2 eli $0,9973845 \approx \boxed{99{,}74\%}$.