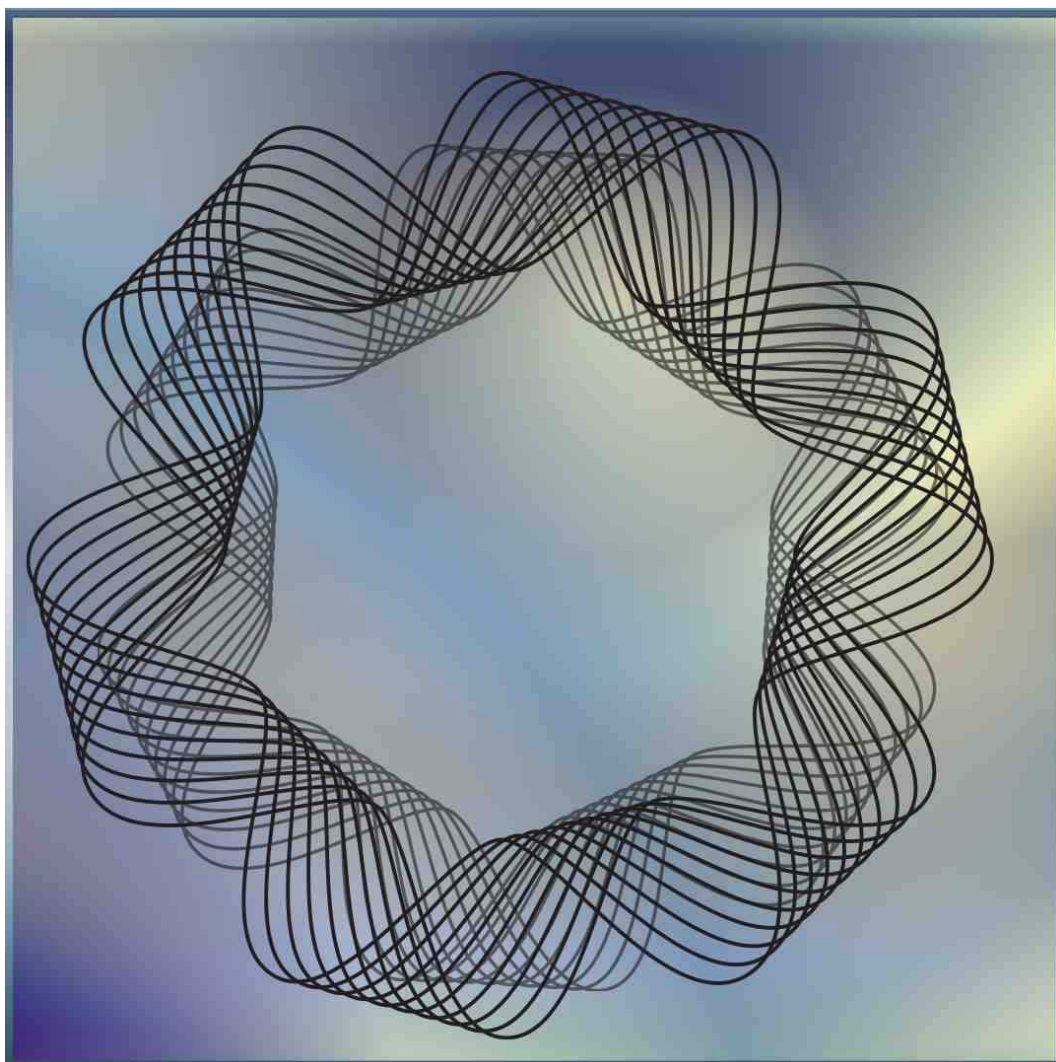


Solmu

Matematiikkalehti
3/2007

<http://solmu.math.helsinki.fi/>



Solmu 3/2007

ISSN 1458-8048 (Verkkolehti)

ISSN 1459-0395 (Painettu)

Matematiikan ja tilastotieteen laitos

PL 68 (Gustaf Hällströmin katu 2b)

00014 Helsingin yliopisto

<http://solmu.math.helsinki.fi/>

Päätoimittaja:

Matti Lehtinen, dosentti, Maanpuolustuskorkeakoulu

Toimitussihteeri:

Juha Ruokolainen, FT, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Sähköposti: *toimitus@solmu.math.helsinki.fi*

Toimituskunta:

Pekka Alestalo, dosentti, Matematiikan laitos, Teknillinen korkeakoulu

Heikki Apiola, dosentti, Matematiikan laitos, Teknillinen korkeakoulu

Aapo Halko, FT, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Ari Koistinen, FM, Helsingin ammattikorkeakoulu Stadia

Marjatta Näätänen, dosentti, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Hilkka Taavitsainen, lehtori, Ressun lukio

Graafinen avustaja *Marjaana Beddard*

Yliopistojen ja korkeakoulujen yhteyshenkilöt:

Virpi Kauko, FT, matemaatikko, *virpi@kauko.org*, Jyväskylä

Jorma K. Mattila, professori, *jorma.mattila@lut.fi*

Sovelletun matematiikan laitos, Lappeenrannan teknillinen yliopisto

Jorma Merikoski, professori, *jorma.merikoski@uta.fi*

Matematiikan, tilastotieteen ja filosofian laitos, Tampereen yliopisto

Kalle Ranto, assistentti, *kalle.ranto@utu.fi*

Matematiikan laitos, Turun yliopisto

Matti Nuortio, opiskelija, *mnuortio@paju.oulu.fi*

Matemaattisten tieteiden laitos, Oulun yliopisto

Timo Tossavainen, lehtori, *timo.tossavainen@joensuu.fi*

Savonlinnan opettajankoulutuslaitos, Joensuun yliopisto

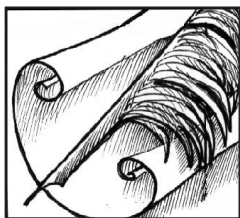
Numeroon 1/2008 tarkoitetut kirjoitukset pyydämme lähettämään 31.1.2008 mennessä.

Kiitämme taloudellisesta tuesta Jenny ja Antti Wihurin rahastoa.

Huom! Solmun paperiversio postitetaan vain niihin kouluihin, jotka ovat sitä erikseen pyytäneet. Toivomme, että lehteä kopioidaan kouluissa kaikille halukkaille.

Sisällys

Pääkirjoitus: Fysiikka, kemia, laskento ja matematiikka: neljä eri lajia (Matti Lehtinen)	4
Uusista opetussuunnitelmista (Marjatta Näätänen)	6
Kalle Väisälän algebran oppikirja Solmuun (Marjatta Näätänen)	6
Lukuteoriaa ja salakirjoitusta, osa 1 (Heikki Apiola)	7
Matematiikkaa Venäjällä (Eemeli Blåsten)	14
Geometrian pähkinä (Tauno Tukkinen)	18
Gauss romaanihenkilönä (Matti Lehtinen)	19
Matematiikkakilpailu opettajillekin? (Matti Lehtinen)	21
Kuusi vaikeaa tehtävää – matematiikkaolympialaiset Hanoissa (Matti Lehtinen)	22
Klikkimenetelmä kombinatoristen ongelmien ratkaisemisessa (Mikko Malinen)	27



Fysiikka, kemia, laskento ja matematiikka: neljä eri lajia

Otsikko luettelee aakkosjärjestyksessä neljä tiedon ja taidon alaa. Kaksi ensimmäistä ovat eksakteja luonnontieteitä, fyysisen maailmamme olemusta selvittäviä, maailmankuvaa rakentavia tietokokonaisuuksia, tekniikan moninaisten saavutusten kulmakiviä. Kolmas on arkipäivämme kannalta olennainen taito, jota tarvitaan kaikenlaisen kvantitatiivisen informaation käsittelyssä, leivontaresepteistä supertietokoneilla tehtäviin monivaiheisiin simulaatiosovelluksiin asti. Matematiikka on abstrakti määrän ja muodon tiede, looginen ja deduktiivinen rakennelma, kuitenkin todellisuuteen ankuroitunut ja maailman ymmärtämiseksi olennaisen tärkeitä työkaluja tarjoava, myös fysiikan, kemian ja laskennon tukitiede, muttei suinkaan vain näiden.

Fysiikka, kemia, laskento ja matematiikka ovat ihmisen eri tiedon- ja taidonalojen joukossa sikäli poikkeuksellisia, että niitä kaikkia opetetaan yleissivistävässä koulussa, eri määriä ja eri aikoina. Laskennon perusteita opetetaan rinnan toisen viestinnän perustaidon, lukemisen kanssa koulun ensimmäisinä vuosina. Näin on ollut kauan, eikä asia ole siitä muuttunut, että oppiaineen nimi on käsitteiden sekaannuksessa ja hienostelutarpeiden vuoksi muutettu matematiikaksi. Oppiainenimen matematiikka alla laskennon opetusta jatketaan peruskoulussa ja lukiossa; lukiossa laskennon nimeksi tulee lyhyt matematiikka. Peruskoulun loppupuolella ja lukiossa on tarkoitus opettaa myös fysiikkaa, kemiaa ja matematiikkaa. Lukiossa matematiikka-aineen nimi on pitkä matematiikka. Myös pitkä matematiikka on konstruktiivinen, johon sisältyy vahva laskentokomponentti.

Fysiikkaa, kemiaa, laskentoa ja matematiikkaa yh-

distää yläkäsiete matemaattiset aineet. Maahamme on juurtunut kansainvälisesti melko ainutlaatuinen käytäntö, jonka mukaan näiden syvästi toisistaan eroavien tiedon- ja taidonalojen opetus yhdistyy samaan opettajaan.

Opettamisen professiosta eli ammattikuvasta on viime vuosina paljon kirjoitettu ja puhuttu. Erityisesti opettajan työn ihmissuhdeaspektien tärkeyttä on korostettu. Ei kuitenkaan voi muuksi muuttaa sitä tosiasiaa, että opettaja voi olla tietojen tai taitojen opettaja vain, jos hän itse osaa. Tanssinopettajan on osattava tanssia, mielellään hyvin. Tanssi tarvitsee tuekseen musiikin, mutta musiikinopettaja ei automaattisesti ole pätevä tanssinopettaja sen enempää kuin tanssinopettaja on musiikinopettaja. Laskennonopettajan on osattava laskea, fysiikan opettajan on osattava fysiikkaa, kemian opettajan kemiaa. Hyvä laskennonopettaja ei välttämättä tiedä matematiikasta tai kemiasta mitään. Haitaksi ei ole, jos laskennon opettaja pitää laskemisesta, fysiikan opettaja fysiikasta ja kemian opettaja kemiasta. Ja välttämätöntä on, että opettajalla on kokonaisnäkemys opetettavasta aineestaan, kyky nähdä ja asettaa kulloinkin opetettavana oleva asia tai taito laajempaankin yhteyteen kuin kulloisenkin opetus-tilanteen mikromaastoon.

Miten huolehditaan siitä, että opettaja osaa? Antaako kunnan sivistyslautakunta tai kaupungin opetusvirasto laskennon opettajaksi pyrkiville laskutehtäviä, kemian opettajaksi pyrkiville analyysitehtäviä, kysytäänkö fysiikan opettajaksi haluavalta sähkömagneettisen säteilyn perusominaisuuksia, jotta varmistuttaisiin opetta-

Pääkirjoitus

jien osaamisen laadusta? Näin ei tehdä, vaan laadun katsotaan näkyvän opettajan tehtäviin hakeutuvan opintosuorituksista. ”Matemaattisten aineiden opettaja” on kuitenkin periaatteessa pätevä opettamaan esimerkiksi matematiikkaa, oppia ja tietoa, jolla ei välttämättä ole mitään tekemistä luonnontieteiden kanssa (vaikka sillä toki usein on!), kunhan hän on suorittanut syventäviä opintoja kemiassa tai fysiikassa ja aineopintoja matematiikassa.

Matemaattisten aineiden opettajia tavatessaan ja esimerkiksi ylioppilastutkinnon matematiikan koetta lähes varmuudella seuraavia kokeen vaikeuden kauhisteluja kuunnellessaan ei voi välttyä saamasta käsitystä, että matemaattisten aineiden opettajien matemaattinen ammattitaito on joskus vähäinen. Ja matematiikan aineopintojen sisällöstä ja suoritustasosta hiukan perillä ollen ei tätä tarvitse ollenkaan ihmetellä.

Matematiikkaa ei tarvitse opettaa kaikille, eikä sitä kaikille opetetakaan - laskentoa kylläkin, ja sitä tarpeeseen. Mutta maa tarvitsee jonkin verran ihan oikeaa matematiikkaa ymmärtäviä, siitä kiinnostuneita, sitä rakastavia. Ja matematiikan tärkeäksi aineekseen lukiossa valinnut opiskelija tarvitsee johdattelijakseen

opettajan, joka itse osaa matematiikkaa, on siitä kiinnostunut, rakastaa sitä. Matematiikan osajaksi ei tulla opinnoita, matematiikan opettajaa eivät kasvata kirjankustantajien markkinoimat oppikirjojen tehtävien mallivastauskokoelmat. Ei ole kovin todennäköistä, että kemiaa tai fysiikkaa pääaineenaan opiskelleet olisivat ehtineet ja jaksaneet kehittää itsestään aidosti ammattitaitoista oikean matematiikan opettajaa. Tätä yksinkertaiselta kuulostavaa faktaa ei monikaan sivistyslautakunta, opetusvirasto tai kasvatusopillisin ansioin tehtäviinsä edennyt rehtori tiedosta tai tunnusta.

Miksi emme osaa irrottaa eri tiedonalojen erityisosaamista toisistaan? Miksei nuorten välttämättä kivistä tietä itse kunkin tiedonalan osaamiseen tasoiteta järjestelmällä, jossa kunkin oppiaineen opetus olisi säännönmukaisesti kyseisen aineen erityisosaajan käsissä?

Ettei syntyisi väärinkäsitystä: en ehdota fakki-idiotismin lisäämistä. Aidosti oman asiansa osaava opettaja, ja juuri hän, ymmärtää tietonsa sekä niiden rajoitukset ja arvostaa toisten erilaisia tietoja ja taitoja.

Matti Lehtinen

**Marjatta Näättänen**

Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

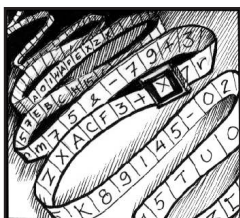
Uusista opetussuunnitelmista

Uusista opetussuunnitelmista on tullut keskusteltua ohimennen joidenkin matemaatikkojen kanssa. Tällaisia mielipiteitä on tullut esille: pahimpia ongelmia uusien opetussuunnitelmien suhteen on, että polynomialgebra on rajoitettu polynomien kertomiseen. Jakoalgoritmi esiintyy vain numeerisena ja erikoiskursilla. Polynomien käsittely on kuitenkin perusosaamista, jota tarvitaan luonnontieteellisillä ja teknisillä aloilla perusopinnoissa. Matematiikasta innostuneet ja sitä harrastavat oppilaat onnistuvat paikkaamaan aukon vaikka itsekseen, mutta muille olisi syytä opettaa jo koulussa nämä asiat — tasa-arvonkin takia olisi tärkeää, että kaikille annettaisiin mahdollisuus oppia nämä asiat, jotta heidän jatkomahdollisuutensa eivät kaatuisi tällaiseen perusosaamisen aukkoon.

Olisi hyvä saada opetussuunnitelmista kokemuksia ja mielipiteitä, osallistukaa keskusteluun!

Kalle Väisälän algebran oppikirja Solmuun

Edellisessä numerossa kerrottiin, että Väisälän algebran oppikirjan tehtäviä julkaistaan Solmussa. Lähiaikoina ilmestyy koko kirja Solmun verkkosoitteessa. Kiitämme julkaisuluvista Väisälän perikuntaa ja WSOY:tä. Kirjan tekstin on kirjoittanut Solmulle Mirjana Mirolovic ja tehtävät Juha Ruokolainen.



Lukuteoriaa ja salakirjoitusta, osa 1

Heikki Apiola

Dosentti

Matematiikan laitos, Teknillinen korkeakoulu

Johdanto

Lukuteoriaa on joskus pidetty esteettisesti kauniina, mutta käytännössä aika hyödyttömänä matematiikan alana. Kukaan ei asettane nykyäänkään tuota esteettistä puolta kyseenalaiseksi, mutta miten on sen käytännön hyödyn laita?

Nykyinen sähköiseen tiedonvälitykseen perustuva asioiden hoitaminen ei olisi mahdollista ilman tehokkaita salausmenetelmiä. Niiden kehittämisessä puolestaan on ollut ratkaisevan tärkeä osa juuri tuolla lukuteorian tarjoamalla ”hyödyttömällä” estetiikalla.

Tässä kirjoituksessa esitetään lukuteorian perusasiat, joita tarvitaan osassa 2 esiteltävän ns. julkisen RSA-salakirjoitusmenetelmän johtamiseen, päteväksi osoittamiseen ja ohjelmoimiseen.

Lukuteoria on sikäli poikkeava matematiikan ala, että siitä voi kirjoittaa lukijalle, jolla on minimaaliset perustiedot matematiikassa. Itse asiassa tarvitaan vain ymmärrys kokonaislukujen perusominaisuuksista ja laskutoimituksista niillä. Näillä eväillä päästään aika nopeasti kiinnostaviin tuloksiin ja sovelluksiin käsiksi.

Kirjoitus toimii testinä yllä olevalle väitteelle. Toki on hyödyksi, jos lukijalla on oheislukemistona vaikkapa lukion lukuteorian syventävän kurssin 11 oppikirja, kuten [Lukio1] tai [Lukio2].

Kirjoitus ei ole lukuteorian alkeiden oppikirjan osa, keskityn välttämättömän (ja toivottavasti riittävän) osuuden esittelyyn päämääränä yllä mainitun julkisen salakirjoituksen RSA-salakirjoitusalgoritmina tunnetun menetelmän ymmärtäminen. Esitän asiat perusteellisesti, niin että yksityiskohtienkin ymmärtäminen olisi mahdollista. Jotta kirjoitus ei paisuisi liian laajaksi, esitän sen kahdessa osassa. Tässä ensimmäisessä keskityn lukuteorian perusteisiin ja toisessa tuohon salakirjoitussovellukseen.

Kokonaisluvut, jaollisuus

Merkintöjä: Käytän joukko-opin ja logiikan standardimerkintöjä:

$x \in A$ tarkoittaa: x kuuluu joukkoon A , eli x on A :n alkio.

Kokonaisluvut: $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

Luonnolliset luvut: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Käsitlemme pelkästään kokonaislukuja, usein viitaamme kokonaislukuun lyhyesti sanalla *luku*.

Pienin ja suurin luku

Kokonaislukujen osajoukoilla on ominaisuus, jota ei ole rationaali- eikä reaaliluvuilla. Kyseessä on mahdollisuus valita osajoukosta pienin ja suurin luku.

Luonnollisten lukujen minimi- ja maksimi-ominaisuus: Jokaisessa $\mathbb{N}$:n epätyhjässä osajoukossa on **pienin luku**.

Tästä seuraa:

Kokonaislukujen minimi- ja maksimi-ominaisuus: Jokaisessa $\mathbb{Z}$:n **ylhäältä rajoitetussa** epätyhjässä osajoukossa on **suurin luku** ja **alhaalta rajoitetussa** on **pienin luku**

Jakoyhtälö

Jos vaikkapa luku $a = 55$ jaetaan luvulla $b = 8$ kokonaislukujakona, saadaan osamäärä $q = 6$ ja jakojäännös $r = 7$, sillä $55 = 6 \cdot 8 + 7$. Osamäärä q löydetään hakemalla suurin luku q , jolle $q \cdot 8 \leq 55$, jakojäännös on se, mitä jää yli. Jakojäännös r on jakajaa ($b = 8$) pienempi, muutenhan osamäärä $q = 6$ ei olisikaan suurin mahdollinen.

Yllä oleva esimerkki noudattaa sitä periaatetta, jolla olemme oppineet jakolaskun suorittamaan jo peruskoulussa. Sama periaate voidaan kirjoittaa yleisesti pelkillä kirjainsymboleilla:

Lause 1. *Olko a ja b luonnollisia lukuja, $a > 0$. Tällöin on olemassa yksikäsitteiset q ja r , $0 \leq r < b$ siten, että $a = qb + r$*

Tod. Toistamme siis vain yllä esimerkissä esitetyn juonen. Voidaan olettaa, että $a > b$, muutenhan voidaan ottaa $q = 0, r = a$.

No, ei muuta kuin valitaan maksimiominaisuuden perusteella suurin luku q niin, että $qb \leq a$. (Epäyhtälön $pb \leq a$ toteuttavia lukuja p varmasti on, ainakin $p = 0$, ja $p = 1$, joten puheena on epätyhjä joukko. Lisäksi kaikki tällaiset luvut p toteuttavat varmasti epäyhtälön $p \leq a$, joten niiden joukko on ylhäältä rajoitettu.)

Merkitään r :llä erotusta $r = a - bq$, jolloin $r \geq 0$. Jos olisi $r \geq b$, niin voitaisiin kirjoittaa $r = b + c$, missä $c \geq 0$.

Tällöin olisi $a = qb + b + c = (q + 1)b + c$, joten q ei olisikaan yllä olevan joukon suurin luku.

Yksikäsitteisyys: Olkoon kaksi esitystä: $a = q_1 b + r_1$, ja $a = q_2 b + r_2$, missä $0 \leq r_i < b$, $i = 1, 2$.

Tällöin $|r_2 - r_1| < b$, joten $|q_1 - q_2| b < b$.

Koska $b > 0$, sillä voidaan jakaa ja saadaan $|q_1 - q_2| < 1$. Kokonaisluvuille tämä on mahdollista vain siten, että $q_1 = q_2$. Siitäpä heti seuraa, että myös $r_1 = r_2$. $\square$

Määritelmä 1 (Jaollisuus). *Luku a on jaollinen luvulla b , jos on olemassa luku n siten, että $a = nb$. Tällöin*

sanotaan, että b on a :n tekijä ja a on b :n moniker- ta. Merkitään: $b | a$, joka voidaan lukea: ” b on tekijänä a :ssa” tai ” b jakaa a :n”

Huomautus 1. *Jos $b | a$, niin $-b | a$. Jokaisella luvulla a on triviaalit tekijät ± 1 ja $\pm a$.*

Luku 0 on jaollinen kaikilla luvuilla b , koska $0 = 0 \cdot b$, toisaalta 0 on tekijänä 0:ssa, mutta ei missään luvussa $a \neq 0$.

Esimerkki 1. *Jaollisuusesimerkkejä*

1) $7 | 56$, $-3 | 12$.

2) Luvun 12 ei-triviaalit tekijät: $\pm 2, \pm 3, \pm 4, \pm 6$

3) Luvulla 6 jaollisten lukujen joukko:

$\{n \cdot 6 | n \in \mathbb{Z}\} = \{0, \pm 6, \pm 12, \pm 18 \dots\}$

Kootaanpa yhteen yleiset jaollisuuden perusominaisuudet.

Lause 2. *Yleiset jaollisuusominaisuudet*

1) *Jos $x | a$ ja $x | b$, niin $x | (a \pm b)$*

Yleisemmin:

1') *Jos $x | a$ ja $x | b$, niin $x | (am + bn)$ mielivaltaisille (kokonais)luvuille m, n*

2) *Jos $x | a$ tai $x | b$, niin $x | (ab)$*

3) *Jos $a | b$, $b \neq 0$, niin $|a| \leq |b|$,*

Tod. Todistetaan malliksi kohta 1). Yleistys 1') on aivan vastaavanlainen. Kohdat 2) ja 3) ovat suorastaan itsestäänselvyyksiä. Mieti kuitenkin.

Kohta 1): Oletuksen mukaan on olemassa (kokonais)luvut s ja t siten, että $a = sx$ ja $b = tx$. Niinpä $a + b = sx + tx = \underbrace{(s + t)}_{\in \mathbb{Z}} x$, joten $x | (a + b)$.

$\square$

Kannattaa huomata, että käänteinen suunta kohdalle 2) ei päde yleisesti.

Esim: $12 = 3 \cdot 4$. Luku 6 on tekijänä luvussa 12, mutta 6 ei ole tekijänä kummassakaan tulontekijässä 3 tai 4.

No, kysehän on siitä, että 6 :lla on yhteinen tekijä sekä 3 :n että 4 :n kanssa. Tähän tärkeään havaintoon palataan, ja muotoillaan lisäehto, jolla käänteinen johdopäätös on voimassa.

Kun puhutaan positiivisten kokonaislukujen a jaollisuudesta, voidaan rajoittaa puhumaan positiivisista tekijöistä b , sillä jos b on tekijä, niin $-b$ on aina myös tekijä, joten sen mainitseminen erikseen on turhaa sanahelinää. (Matemaatikon hyveisiin kuuluu sanojen säästäminen.)

Alkuluvut

Määritelmä 2. Kokonaisluku $a > 1$ on **alkuluku**, jos se on jaollinen vain 1:llä ja itsellään. Muuten puhutaan **yhdistetystä luvusta**.

Jokainen luku a on jaollinen myös -1 :llä ja $-a$:lla. Noudatamme edellä mainittua "turhan sanahelinän välttämisperiaatetta" ja pitäydymme positiivisissa tekijöissä.

Alkulukujen alkupää näyttää tältä: 2, 3, 5, 7, 11, 13, 17. Yksinkertainen algoritmi alkulukujen laskemiseen on jo antiikin Kreikassa tunnettu *Eratostheneen seula*. Lukujoukosta $1, \dots, n$ seulotaan pois kaikki yhdistetyt luvut poistamalla ensin 2:n monikerrat (parilliset luvut), sitten 3:n monikerrat (3:lla jaolliset luvut), jne. Kts. [Lukio1]

Symbolilaskentaohjelmissa on valmiita alkulukualgoritmeja ohjelmoituna. MAPLE:lla voitaisiin 100 ensimmäistä alkulukua laskea näin:

```
> N := [$(2 .. 100)]
[2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 ...
... 99, 100]
> map(ithprime, N)
[3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 ..
... 523, 541]
```

Eratostheneen seula on helppo ymmärtää ja ohjelmoida, mutta se on varsin tehoton. Tehokkaiden alkulukualgoritmien kehittäminen on tärkeä osa mm. kryptologiasta (salakirjoitusmenetelmiin liittyvää) tutkimusta.

Lause 3 (Alkulukuhajotelma). *Jokainen luonnollinen luku $a > 1$ voidaan esittää alkulukujen tulona.*

Tod. Jos a on alkuluku, se on (yksiterminen) alkulukutulo. Jos taas a on yhdistetty luku, se on muotoa $a = a_1 a_2$, $a_i > 1$, $i = 1, 2$. Jos kumpikin on alkuluku, olemme perillä. Ellei, niin ainakin toinen on yhdistetty luku. Esitetään kaikki (toinen tai molemmat) tekijät kahden luvun tulona. Näin jatketaan, kunnes päädytään tuloon, jonka mitään tekijää ei voida jakaa. Tämä tapahtuu viimeistään $\log_2(a)$ askeleen jälkeen, koska yhdistetyn luvun kumpikin tekijä ≥ 2 . $\square$

Tuntuu uskomattomalta, jos alkuluvut loppuisivat jostain alkaen, ts. niitä olisi vain äärellinen määrä. *Eukleides* todisti jo v. 300 eKr. kirjassaan *Elementa* (Kirja IX, propositio 20), että niitä todella on äärettömän paljon. Tämä 2300 vuotta vanha todistus on edelleenkin voimissaan. Näin se menee:

Lause 4 (Eukleides). *Alkulukuja on ääretön määrä.*

Tod. Olkoon p mielivaltainen alkuluku. Osoitetaan, että on olemassa sitä suurempi alkuluku. Tällöinhän äärellinen alkulukujen määrä johtaisi heti ristiriitaan.

Olkoot $p_1, p_2, \dots, p_n = p$ kaikki alkuluvut, jotka ovat $\leq p$. Olkoon $P = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$. Jos P jaetaan millä tahansa luvuista p_j , $j = 1, \dots, n$, niin jakojäännös $= 1$ (ajattele $P : n$ kaavaa jakoyhtälönä). Jako ei siis mene tasan, eli mikään p :tä pienempi alkuluku ei ole tekijänä P :ssä. Mutta alkulukuhajotelmalauseen 3 mukaan P :llä on tekijänä alkuluku (P itse, jos se sattuu olemaan alkuluku). Tämä tekijä ei ole mikään p :tä pienempi tai sen suuruinen (alku)luku, joten sen on oltava p :tä suurempi. $\square$

Myöhemmin on esitetty monia muitakin todistuksia, kts. esim.

http://en.wikipedia.org/wiki/Prime_numbers

Suurin yhteinen tekijä

Lukujen a ja b **suurin yhteinen tekijä**, $\text{syt}(a, b)$ on nimensä mukaisesti suurin luku s , joka on tekijänä sekä a :ssa että b :ssä.

Esimerkiksi $\text{syt}(24, 30) = 6$, $\text{syt}(5, 7) = 1$. Systemaattinen tapa $\text{syt}(a, b)$:n määrittämiseksi on muodostaa alkulukuhajotelmat ja poimia kummastakin yhteiset alkutekijät. Edellisessä esimerkissä: $24 = 2 \cdot 2 \cdot 2 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$. Yksi kakkonen ja yksi kolmonen voidaan poimia kummastakin, eikä mitään muuta, joten todellakin saadaan 6.

Tehokkaampi menetelmä on ns. *Eukleideen algoritmi*, joka esitellään kohta.

Sitä ennen johdetaan suurimmalle yhteiselle tekijälle kaava, josta saadaan kätevästi koko joukko ominaisuuksia. Sitä voidaan pitää tämän kirjoituksen yhtenä tärkeimpänä työkaluna.

Lause 5 (SYTlause). *Olkoot a ja b positiivisia kokonaislukuja.*

$$\text{syt}(a, b) = \min\{s > 0 \mid s = ax + by, \ x, y \in \mathbb{Z}\}$$

Tod. Oikealla puolella oleva joukko koostuu positiivisista kokonaisluvusta. Luonnollisten lukujen minimiominaisuuden mukaan tässä joukossa on pienin luku

$$s_0 = ax_0 + by_0,$$

missä x_0 ja y_0 ovat sellaiset kokonaisluvut, joilla tuo minimi saavutetaan.

Todistuksen juoni on osoittaa, että

$$\begin{cases} (1) \text{ syt}(a, b) \leq s_0, \\ (2) \text{ syt}(a, b) \geq s_0. \end{cases}$$

Epäyhtälö (1) : Koska $\text{syt}(a, b)$ on tekijänä sekä a :ssa että b :ssä, niin se on tekijänä jokaisessa muotoa $ax + by$ olevassa lausekkeessa, siis myös s_0 :ssa. Niinpä on oltava $\text{syt}(a, b) \leq s_0$.

Epäyhtälö (2) : Jos onnistumme osoittamaan, että $s_0 \mid a$ ja $s_0 \mid b$, niin tiedämme, että s_0 on a :n ja b :n yhteinen tekijä ja siten pienempi tai yhtäsuuri kuin suurin yhteinen tekijä $\text{syt}(a, b)$.

Aloitetaan a :sta. Jakoyhtälön mukaan $a = qs_0 + r$, missä $0 \leq r < s_0$. Osoitetaan, että $r = 0$, jolloin väitteemme on a :n osalta todistettu.

Kirjoitetaan $r = a - qs_0 = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$.

Siis r on ”muotoa s_0 ”. Lisäksi $0 \leq r < s_0$. Koska s_0 on pienin positiivinen tuota muotoa oleva luku, on oltava $r = 0$. Siten $a = qs_0$, ts. $s_0 \mid a$.

Aivan samoin voimme menetellä b :n suhteen, ja päätellä, että $s_0 \mid b$. (Suoritapa tämä lasku ja päättely!) Siispä s_0 on a :n ja b :n yhteinen tekijä, ja niin ollen $s_0 \leq \text{syt}(a, b)$.

Niin olemme todistaneet epäyhtälöt (1) ja (2), joten todellakin $\text{syt}(a, b) = s_0$. □

Ennenkuin ryhdymme nautiskelemaan tämän lauseen seurauksista, otamme käyttöön merkinnän ja nimityksen:

Keskenään jaottomat luvut: Luvut a ja b ovat keskenään jaottomat, jos $\text{syt}(a, b) = 1$. Käytämme myös sanontaa *yhteistekijättömät* ja puhetapaa: ” a :lla ja b :llä ei ole yhteisiä tekijöitä” tarkoittaen: ei *yhteisiä epätriviaaleja tekijöitä*.

Aloitetaan edellä luvutulla käänteisellä puolella tulon jaollisuusominaisuuteen (Lause 2)

Lause 6. Oletetaan, että $\text{syt}(a, n) = 1$. Jos $n \mid ab$, niin $n \mid b$

Tod. Koska $\text{syt}(a, n) = 1$, on $1 = x_1a + y_1b$ joillakin kokonaisluvuilla x_1 ja y_1 (SYTlause (Lause 5)). Kun tämä kerrotaan puolittain b :llä, saadaan

$$b = x_1ab + y_1bn.$$

Koska $n \mid ab$, on $ab = kn$ jollain $k \in \mathbb{Z}$. Kun yllä b :n lausekkeessa sijoitetaan ab :n paikalle kn , saadaan:

$$b = x_1kn + y_1bn = n \underbrace{(x_1k + y_1b)}_{\in \mathbb{Z}}.$$

Siispä todellakin n on tekijänä b :ssä. □

Erityisesti saadaan nyt:

Seuraus 7. Olkoon p alkuluku ja a ja b mielivaltaisia kokonaislukuja. Jos p on tekijänä tulossa ab , niin p on tekijänä a :ssa tai p on tekijänä b :ssä. Loogisena lauseena ilmaistuna:

$$p \text{ alkuluku}, p \mid ab \implies p \mid a \vee p \mid b.$$

Tod. Oletetaan siis, että p on tekijänä ab :ssä. Jos p ei ole tekijänä a :ssa, niin $\text{syt}(p, a) = 1$, koska p on alkuluku. Edellisen mukaan p :n täytyy siten olla tekijänä b :ssä. □

Tehtävä 1. Osoita esimerkillä, että edellinen ei päde yleisesti, jos p ei ole alkuluku.

Eukleideen algoritmi

Kyseessä on menettely, jolla voidaan rekursiivisesti määrittää $\text{syt}(a, b)$ annetuille kokonaisluvuille a ja b . Se on peräisin samasta Elementa-teoksesta n. 300 v. eKr kuin lause 4.

Algoritmi pohjautuu havainnolle:

Lause 8. Olkoot a ja b luonnollisia lukuja, $a > b$. Jos r on jakojäännös jakolaskussa a/b , niin $\text{syt}(a, b) = \text{syt}(b, r)$.

Tod. Kirjoitetaan jakoyhtälön mukaan $a = qb + r$. Jos s on a :n ja b :n yhteinen tekijä, niin s on tekijänä r :ssä, koska $r = a - qb$ (Lause 2, kohta 1). Siispä s on b :n ja r :n yhteinen tekijä. Kääntäen, jos s on b :n ja r :n yhteinen tekijä, niin se on a :n tekijä, koska $a = qb + r$. Kaikki yhteiset tekijät ovat samat, joten erityisesti suurin yhteinen tekijä on sama. □

Esimerkki 2. Määrittävä $\text{syt}(576, 168)$.

$$576 = 3 \cdot 168 + 72.$$

Lause 8: $\text{syt}(576, 168) = \text{syt}(168, 72)$.

Jakoyhtälö: $168 = 2 \cdot 72 + 24$.

Lause 8: $\text{syt}(168, 72) = \text{syt}(72, 24)$.

Jakoyhtälö: $72 = 3 \cdot 24 + 0$.

Lause 8: $\text{syt}(72, 24) = \text{syt}(24, 0) = 24$.

Alkuperäisen tehtävän ratkaisu: $\text{syt}(576, 168) = 24$.

Kirjoitetaan algoritmi rekursiiviseksi (itseään kutsuvaksi) ohjelmaksi symbolilaskentaohjelman MAPLE ohjelmointikielellä. Kyseessä on varmasti kaikkien rekursiivisten algoritmien äiti!

(Solmukirjoitus Maplen-käytöstä:

<http://solmu.math.helsinki.fi/1999/5/apiola/>, rekursiota käsitellään kirjoituksessa:

<http://solmu.math.helsinki.fi/1998/2/seppanen/>.

Eräs kuulemani tietosanakirjamääritelmä: *Rekursio*, kts. *rekursio*)

```
Eukleides := proc (a, b)
print(a, b); # seurantaa varten
if b = 0 then a else
  Eukleides(b, a mod b) end if
# a mod b on jakoj\ "a\"ann\"os.
end proc;
```

Suoritetaan esimerkkiajo vaikkapa määrittämällä $\text{sy}(145, 75)$. Oikean sarakkeen b siirtyä seuraavalla rivillä vasemmalle jakajaksi ja saman rivin oikean puolen luku on vastaava jakojäännös.

```
> Eukleides(145, 75)
145, 75
75, 70 ( 145 = 1x75 + 70 )
70, 5 ( 75 = 1x70 + 5 )
5, 0 ( 70 = 14x5 + 0 )
5 ( sy(5,0) = 5 )
```

Siis $\text{sy}(145, 75) = 5$.

Aritmetiikkaa jakojäännöksillä

Meihin on ”sisäänrakennettu” laskenta jakojäännöksillä erityisesti tapauksissa $n = 12$ ja 24 . Jokainen tietää, että kellonajat 5 (i.p.) ja 17 tarkoittavat samaa, ja jos yöjuna lähtee klo 20 ja on perillä klo 9, niin matkaan on kulunut aikaa 13 tuntia. Matemaattisesti nämä voidaan ilmaista kaavoilla:

$$5 \equiv 17 \pmod{12} \text{ ja } 20 + 13 \equiv 9 \pmod{24}$$

Yleisesti määritellään käsite *kongruenssi modulo n* :

Määritelmä 3. *Olko $n > 1$. Luvut a ja b ovat kongruentteja modulo n , jos $n \mid (a-b)$. Tällöin merkitään*

$$a \equiv b \pmod{n}.$$

Määritelmä tarkoittaa sitä, että a ja b saadaan toisistaan lisäämällä sopiva ”modulin” n monikerta: $a - b = kn$ jollain kokonaisluvulla k . Tämä merkitsee, että jakolaskuissa a/n ja b/n on sama jakojäännös.

Tehtävä 2. *Jos tänään on maanantai, niin mikä viikkopäivä on 100:n päivän kuluttua?*

Ratkaisu. Numeroidaan viikkopäivät $0, \dots, 6$ antaen arvo 0 vaikka sunnuntaille. Tehtävänä on selvittää jakojäännös jakolaskussa $100/7$. Jakoyhtälö on $100 = 7 \cdot 14 + 2$. Kun siis kierrämme ”viikkokellotaulua” 14 kertaa (= 98 päivää), tulemme samaan, mistä lähdimme, mennään vielä kahdella yli, joten päivä on $1 + 2 = 3$, eli keskiviikko.

Voidaan ajatella, että $1 + 100$:sta vähennetään sellainen $7:n$ monikerta, että päästään välille $0, \dots, 6$. Sanonta: *Redusoidaan luku 101 modulo 7*. Tämä juhlalliselta kalskahtava sanonta tarkoittaa siis arkikielellä vain sitä, että määritämme jakojäännöksen jakolaskussa $101/7$. Kaiken aikaa vaan siis pyörittelemme samaa jakoyhtälöä.

Modulaariaritmetiikkaa

Havainnollisesti ajatellen modulaariaritmetiikka, eli ”jakojäännöslaskenta” voidaan ajatella niin, että lukusuoran sijasta kuljetaan pitkin ympyrän kehää. Kellotaulu on tästä havainnollinen esimerkki, siinä jakovälejä on 12 ja kyseessä siis laskenta modulo 12.

Voidaan ajatella, että kokonaislukusuora on kierretty rullalle, joka kiertää samaa kehää äärettömän monta kertaa. Kehä on jaettu 12:een osaan, yleisesti modulin eli jakajan ilmaisemaan määrään osia. Useimmiten emme ole kiinnostuneita siitä, montako täyttä kierrosta kehän ympäri tehdään, vaan siitä, mille kohdalle ”onnenpyörää” lopulta pysähdytään.

Käytännön laskutoimitukset $(+ - \cdot)$, kun modulina on n , suoritetaan niin, että lasketaan luvuilla $0, \dots, n-1$. Lopputulos ”redusoidaan modulo n ”, ts. lisätään tai vähennetään $n:n$ monikertoja niin, että päästään välille $0, \dots, n-1$, eli kerran vielä: lasketaan jakojäännös, kun jakajana on n .

Formaalimpi ja matemaattisesti kauemmas kantava tapaa on tarkastella ns. jäännösluokkia modulo n , jolloin ”samaistetaan” kaikki luvut, joilla on sama jakojäännös jaettaessa luvulla n . Viittaaoulukirjoihin [Lukio2] Kongruenssi, s. 126, tai [Lukio1] Kappale 5 s. 82. Koska pyrin pitämään koneiston minimaalisena salakirjoitustavoitteitamme ajatellen, vältän ylimääräisiä uusia abstraktioita, niin elegantteja ja keskeisiä matemaattisen käsitteenrakennuksen välineitä kuin ovatkin.

Kongruensseilla laskeminen

Kongruenssi näyttää yhtälöltä ja monessa suhteessa käyttäytyy samoin.

Lause 9.

$$\text{Jos } a \equiv b \pmod{n} \text{ ja } c \equiv d \pmod{n}, \text{ niin}$$

$$a \pm c \equiv b \pm d \pmod{n} \text{ ja } ac \equiv bd \pmod{n}.$$

Tod. Tyydytään todistamaan vain summan tapaus. Erotus on aivan samanlainen. Tulo on hiukan pitempi, mutta periaate on sama, eikä siinä voi mitenkään johtua harhateille (eihän!). (Yritä itse, mutta voit myös katsoa [Lukio1] s. 85).

No niin, olkoon siis $n \mid (a - b)$ ja $n \mid (c - d)$, ts.

$a - b = jn$ ja $c - d = kn$ joillakin luvuilla j, k . Nyt

$(a + c) - (b + d) = jn - kn = (j - k)n$, joten todellakin

$a + c = (b + d) + Kn$, missä $K = j - k \in \mathbb{Z}$, eli väite on tosi. $\square$

Erityisesti valitsemalla $c = d (= m)$ nähdään, että kongruenssiin voidaan lisätä puolittain luku, se voidaan kertoa puolittain luvulla ja korottaa potenssiin:

Lause 10. Jos $a \equiv b \pmod{n}$ ja $k \in \mathbb{Z}$, $m \in \mathbb{N}$, niin

$$(1.) a + k \equiv b + k \pmod{n},$$

$$(2.) ak \equiv bk \pmod{n},$$

$$(3.) a^m \equiv b^m \pmod{n}.$$

Kongruenssiyhtälön supistaminen

Kyseessä on oikeastaan vain lauseen 6 yhteydessä esitettyjen asioiden pukeminen modulaariaritmetiikan kielelle.

Esimerkki 3.

$$2 \cdot 2 \equiv 2 \cdot 5 \pmod{6}.$$

Voidaanko tekijällä 2 supistaa? Ts, päteekö $2 \equiv 5 \pmod{6}$? No eipä tietenkään, sillä $5 - 2 = 3$, joka ei taatusti ole 6:n kokonaismonikerta.

Ehto, jolla supistaminen on sallittua, ei yllättäne ketään.

Lause 11 (Modsupistus). Jos $\text{sytk}(k, n) = 1$, niin $ak \equiv bk \pmod{n} \implies a \equiv b \pmod{n}$.

Sanallisesti: Kongruenssiyhtälö voidaan supistaa yhteisellä kertoimella k , mikäli kerroin k ja moduuli n ovat yhteistekijättömät.

Tod. Oletetaan siis, että $\text{sytk}(k, n) = 1$ ja $ak \equiv bk \pmod{n}$. Tällöin $(a - b)k \equiv 0 \pmod{n}$, joten $n \mid (a - b)k$. Koska $\text{sytk}(k, n) = 1$, niin lauseen 6 mukaan $n \mid (a - b)$, ts. $a \equiv b \pmod{n}$. $\square$

Kongruenssiyhtälö, käänteisalkio

Tarkastelemme yksinomaan muotoa $ax \equiv b \pmod{n}$ olevia yhtälöitä. Yleisesti kokonaislukukertoimisia yhtälöitä sanotaan *Diofantoksen yhtälöiksi* ja niihin liittyvä teoria on osa lukuteorian perusoppia. Salakirjoituksen kannalta tarvitaan vain yllä olevaa muotoa, vieläpä sillä lisärajoituksella, että $b = 1$.

Lause 12. Olkoon $n > 1$ ja $\text{sytk}(a, n) = 1$. Tällöin yhtälöllä $ax \equiv 1 \pmod{n}$ on yksikäsitteinen ratkaisu x .

Tod. 1. Ratkaisun olemassaolo: Todistus seuraa suoraan Lauseesta 5 näin: Koska $\text{sytk}(a, n) = 1$, on olemassa kokonaisluvut x ja y siten, että $ax + ny = 1$, ts. $ax = 1 - ny$. Mutta tähän tarkoittaa, että $ax \equiv 1 \pmod{n}$.

2. Ratkaisun yksikäsitteisyys seuraa suoraan Modsupistus-lauseesta 11. (Mieti kuitenkin!) $\square$

Yllä olevan yhtälön ratkaisu voidaan ajatella käänteisalkion etsimistehtäväksi annetulle a :lle. Tyydyttävämmän sanottuna kyse on a :n määräämän ”jäänösluokan” modulo n käänteisalkiosta, josta kuitenkin lupasimme olla puhumatta enempää tällä kertaa. Ratkaisua x merkitään usein symbolilla $x = a^{-1} \pmod{n}$. Yksikäsitteinen käänteisalkio $\pmod{n}$ on siis olemassa jokaiselle a :lle, joka on yhteistekijätön modulin n kanssa.

Käänteisalkion määrittämiseen tarvitaan menetelmä lauseen 5 kertoimen x (siellä merkittiin x_0) laskemiseksi. Se voidaan tehdä ns. laajennetulla Eukleideen algoritmilla. Palataan tähän kirjoituksen osassa 2.

Fermat’n pieni lause

Kaikkihan ovat kuulleet legendaarisia tarinoita Fermat’n suuresta lauseesta ”Fermat’s last theorem”. Kuinka ”olen löytänyt ihmeellisen todistuksen, joka ei mahdu muistikirjani marginaaliin”, ja kuinka englantilainen Andrew Wiles, 7 vuotta yksinäisessä vinttikamarissa työskenneltään todisti tuon vuodesta 1630 matemaattista maailmaa kiusanneen lauseen. Kuinka siitä löytyi puutteita, jotka Wiles myöhemmin onnistui paikkaamaan. Ja kuinka tuo todistus ei mahtuisi sataankaan marginaaliin.

No, nyt emme puhu siitä enempää, vaan ”pienestä” lauseesta, joka on yksi keskeinen osa salakirjoitusmenetelmän oikeellisuuden todistusta.

Lause 13 (Fermat’n pieni lause). Jos p on alkuluku ja a ei ole jaollinen p :llä, niin

$$a^{p-1} \equiv 1 \pmod{p}.$$

Tod. Lauseen 10 kohdan (3.) perusteella a voidaan redusoida välille $[0, p - 1]$. Koska p ei ole tekijänä a :ssa, ei a ole kongruentti 0:n kanssa modulo p . Niinpä riittää osoittaa väite oletuksella $0 < a \leq p - 1$.

Muodostetaan jono

$$(A) : a, 2a, 3a, \dots, (p - 1)a \pmod{p}.$$

Nämä ovat siis jakojäännöksiä, kun jakajana on p , siis lukuja välillä $[0, p-1]$.

Osoitetaan, että luvut ovat > 0 , ja että tässä on jokainen luku välillä $1, \dots, p-1$ täsmälleen kerran. Toisin sanoen jono (A) antaa luvut $1, \dots, p-1$ jossain järjestyksessä.

Jotta juonen seuraaminen olisi miellyttävämpää, jätämme tämän yksityiskohdan erikseen osoitettavaksi.

Kun se on tehty, tiedetään siis, että

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot \dots \cdot (p-1) = (p-1)! \pmod{p}.$$

$$\text{Toisin sanoen } a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Palamme halusta jakaa yhtälö puolittain $(p-1)!$:lla, mutta onko lupa? No eipä muuta kuin sydämen kyllyydestä sovellamme lausetta 11, jonka oletus on voimassa, sillä mikään luvuista $2, \dots, p-1$ ei voi olla alkuluvun p tekijä.

Lause on todistettu, kunhan selvitämme tuon edellä mainitun puuttuvan yksityiskohdan.

Tiedämme jo, että $a \neq 0$. Voisiko olla $ka \equiv 0 \pmod{p}$ jollain $k = 1, \dots, p-1$? No tähän merkitsisi, että p olisi tekijänä ka :ssa.

Seuraus 7 vaatisi, että p on tekijänä k :ssa tai a :ssa, mutta kumpikaan ei päde. Tiedämmehän, että $\text{sy}(p, a) = 1$ ja $\text{sy}(p, k) = 1$, kun $k = 1, \dots, p-1$, koska kerran p on alkuluku. Jonon (A) luvut ovat siis joukossa $\{1, \dots, p-1\}$.

Lisäksi ne ovat kaikki erillisiä, sillä jos j ja k ovat joukossa $\{1, \dots, p-1\}$ ja $ja \equiv ka \pmod{p}$, niin modsu-pistulauseen 11 mukaan $j = k$.

Siinä kaikki. $\square$

Huomaamme, että oikeastaan ainoa työkalu oli Modsuspistulause 11. Todistuksen juonen keksiminen on siten aivan toinen juttu.

Pierre de Fermat esitti väitteen ystäväilleen 18.10.1640 päivätyssä kirjeessään. Kuten miehen tapoihin kuului, hän ei tällekkään väitteelle esittänyt todistusta. ("Lähettaisän myös todistuksen, ellen pelkäisi sen olevan liian pitkän.") Ensimmäinen tunnettu todistus on

Leibniz'n julkaisemattomassa käsikirjoituksessa vuodelta 1683 ja ensimmäinen julkaistu on peräisin *Eulerilta* vuodelta 1736. Nämä ovat keskenään periaatteessa samanlaisia, binomikaavaan perustuvia, kokonaan toisenlaisia kuin yllä annettu.

Lauseelle on myöhemmin keksitty useita kiintoisia todistuksia. Kts. http://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem. Uusimpien joukkoon kuuluu hollantilaisen tietojenkäsittelytieteen gurun ja vuoden 1972 *Turingin palkinnon* saajan *Edsger Dijkstra'n* vuonna 1980 keksimä kombinatorinen todistus. Sekin on yllä mainitussa viitteessä esitettyä.

Salakirjoitus tulee

Näillä pohjatiedoilla päästään käsiksi johdannossa mainittuun salakirjoitusmenetelmään, joka on aiheena seuraavassa Solmun numerossa ilmestyvässä osassa 2, toistaiseksi vain omien arkistojeni uumenissa piileskelevänä ja muotoaan hakevana salakirjoituksena.

Viitteet

[Algo] T.H. Cormen, C.E. Leiserson, R.L. Rivest: *Introduction to Algorithms*, The MIT Press, McGraw-Hill, 1998.

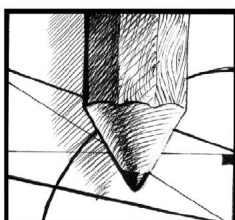
[Lukio1] Halmetoja, Häkkinen, Merikoski, Pippola, Silfverberg, Tossavainen, Laurinolli, Väänänen: *Lukuteoria ja logiikka, Matematiikan taito, syventävä kurssi 11*, WSOY

[Lukio2] Kangasaho, Mäkinen, Oikkonen, Paasonen, Salmela: *Logiikka ja lukuteoria*, Pitkä matematiikka, syventävä kurssi, WSOY

[NumberTH] Humphreys, Prest: *Numbers, groups and codes*, Cambridge U.P. 1989.

[Wiki] http://en.wikipedia.org/wiki/Fermat's_little_theorem

Kirjat [Lukio1] ja [Lukio2] ovat saman syventävän kurssin 11 keskenään vaihtoehtoisia kirjoja. Edellinen käsittelee tätä aihetta hiukan laajemmin.



Matematiikkaa Venäjällä

Eemeli Blåsten

Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

Kesäkuun viidentenä päivänä minulle soitettiin Suomen Matemaattisesta Yhdistyksestä ja kysyttiin kiinnostaisiko minua lähteä Venäjälle. Kyseessä oli Venäjällä jo kuuden vuoden ajan järjestetty kesäkoulu. Tämä oli ensimmäinen kerta, kun sinne kutsuttiin ulkomaalaisia. Sain pari tuntia myöhemmin sähköpostiviestin, jossa kerrottiin yksityiskohdat.

Kesäkoulu järjestetään Dubna-nimisessä ydintutkimuslaitoskaupungissa ja se kestää kymmenen päivää. Luennoitsijoiksi mainitaan Venäjän parhaita matemaatikoi- ta, muun muassa Anosov, Arnold ja Novikov. Viimeksimainittu on saanut Fieldsin Mitalin, mutta en silti tuntenut ketään heistä. Kesäkoulun tarkoituksena on herättää mielenkiinto matematiikan opiskelusta yliopistotasolla ja ketkä sopisivatkaan paremmin tähän tehtävään kuin ison maan huippumatemaatikot? Päätin lähteä matkaan.

Hankin viisumin ja varasin junamatkan Helsingistä Moskovaan ja takaisin. Kesäkoulun järjestäjät sanoivat hoitavansa matkan Moskovasta Dubnaan. Niinpä 18. heinäkuuta lähdin Moskovaan. Olin kolmen muun suomalaisen kanssa samassa hytissä. Matka kesti kolmesta tuntia, joten oli paljon aikaa keskustella kaikesta. Mieleeni jäi lause ”Venäjällä mikään ei toimi, mutta kaikki järjestyy.”

Seuraavana aamuna olin Moskovassa. Tuntui kuin olisin menettänyt lukutaitoni, sillä kaikki oli kirjoitettu kyrillisin aakkosin eikä missään ollut käännöksiä

englanniksi tai miksikään muuksi kieleksi. Olin jo katsonut Google Earthista reitin valmiiksi ja kirjoittanut paperille metroasemien nimet. Toisin kuin Helsingissä, Moskovassa metroverkosto kattaa melkein koko kaupungin. Siellä on kymmenen koko kaupungin läpi kulkevaa linjaa ja yksi kehälinja, jota muut leikkaavat. Onnekseni reitti oli helppo eikä tarvinnut vaihtaa linjaa. Metroasemat olivat hienoja patsaineen ja marmorikäytävineen. Tunnin harhailun jälkeen saavuin Moskovan Matematiikan Jatkuvan Opetuksen Keskukseen, josta bussin oli määrä lähteä kohti Dubnaa. Loppumatka oli kuuma, sillä bussissa ei ollut ilmastointia. Yhdessä vaiheessa juutuimme risteykseen, koska joku oli pysäköinyt autonsa kulmaan eikä bussi mahtunut kääntymään. Illalla saavuin Dubnan rajalla olevaan konferenssikeskukseen ja tapasin Knutin Norjasta sekä Istvanin ja Plaulinin Unkarista.

Aamiainen oli jonkinlaista ravitsevaa siemensoppaa, leipää ja teetä. Ruokailun jälkeen Viktor Kleptsyn tuli esittäytymään. Hän oli eräs kesäkoulun järjestäjistä ja toimisi tulkkina, sillä melkein kaikki luennot olivat venäjäksi. Aluksi oli Uspenskin johdantoluento Gödelin epätäydellisyyslauseesta. Hän määritteli mitä tarkoitetaan logiikan kielellä, mitä ovat kaavat, lauseet, todistukset ja mitä eroa on totuudella ja todistettavuudella. Gödelin epätäydellisyyslause sanoo, että jos jonkin aksioomasysteemin ilmaisuvoima on tarpeeksi tehokas ilmaisemaan luonnollisten lukujen käsitteen, niin tässä systeemissä on lause, joka on tosi, mutta jota ei voi-

da todistaa. Uspenski todisti tuloksen neljällä eri tavalla luentosarjan aikana. Seuraavaksi oli neljä pientä rinnakkaisluentoa, mutta missään ei mainittu asiasta mitään englanniksi, joten oli hyvä hetki ottaa kiinni junamatkan aikana kertyneitä univelkoja. Lounaan jälkeen oli kaksi isoa luentoä peräkkäin. Illalla ihmiset menivät ulos pelaamaan jalkapalloa ja lentopalloa.

Aamulla oli puuroa, leipää ja teetä. Tässä vaiheessa olin jo huomannut, että Venäjällä teellä on samanlainen asema kuin kahvilla Suomessa. Tapasin viidennen ja viimeisen ulkomaalaisen, Michaelin Luxembourgistä. Seuraavaksi oli kaksi luentoä, lounas, kaksi luentoä, illallinen ja frisbeen heittoa Knutin ja Michaelin kanssa. Tästä muodostui kesäkoulun rutiini: aamiainen, kaksi tai kolme luentoä, lounas, kaksi luentoä, illallinen ja mahdollinen iltaohjelma, kuten elokuva, Tsaikovskia, muistelmapuhe Neuvostoliiton hajoamisesta ja niin edelleen. Koulun mielenkiintoisin anti oli kyllä luennot.

Kymmenen päivän aikana osallistuin 42:lle luennot, jotka olivat 23:sta eri aiheesta. Aiheet olivat usealta eri matematiikan haaralta ja esitystapa oli jotakin yliopistoluentojen ja seminaarien väliltä. Laskuharjoituksia ei ollut. Tärkein havainto oli se, että oppilaat ja muut kuuntelijat kommentoivat, korjailivat ja kyselivät paljon enemmän kuin mitä olen nähnyt Suomessa. Mielenkiintoisia olivat Anisovin luennot eri huutokauppatyypeistä ja äänestysistä, Paninin luennot Pythagoraan kolmikoiden luettelemisesta, Kirilovin fraktaaleja koskeva esitelmä, Yaschenkon pitkä luentosarja kryptografiasta, ketjumurtoluvuista ja elliptisistä käyristä, Kleptsynin todistus siitä, että vain muotoa $4k+1$ olevat alkuluvut voidaan esittää kahden neliön summana ja lopuksi Fieldsmitalisti Novikovin esitelmä diskreetistä kompleksianalyysistä kolmiohilalla. Eniten minuun vaikutti kuitenkin kolme eri luentosarjaa, joita kuvailen tarkemmin.

Uspensyn esitelmä neljästä tavasta todistaa Gödelin epätäydellisyyslause oli järäsyttävä ottaen huomioon, että Helsingin Yliopistolla käytetään kahden periodin pituinen kurssi vain yhden tavan esittämiseen. Ensimmäinen Uspensyn esittämä todistus oli oleellisesti ottaen sama kuin mikä matematiikan laitoksen kursilla käydään läpi. Siinä oli ajatuksena, että muodostetaan luonnollisten lukujen aksiomasysteemin avulla täsmällinen lause, joka sanoo "minua ei voi todistaa." Tämä lause on tosi, koska jos se olisi epätosi, niin se voitaisiin todistaa, jolloin se olisi tosi. Miksei sitten tehty lausetta, joka sanoo "minä olen epätosi", vanhaa valehtelijan paradoksia matkien? Sen takia, että todistuvuuden ja totuuden määritelmät eroavat. Todistuvuuden määritelmä on jossain määrin yksinkertaisempi, joten tästä ominaisuudesta voidaan puhua annetussa formaalissa kielessä. Jos haluttaisiin puhua totuudesta, pitäisi käyttää äärettömän pitkiä lauseita, mutta tämä aiheuttaisi ongelmia todistuvuuden määritelmään.

Toinen todistus perustui algoritmiteorian erääseen

kiintopistelauseeseen: "Jos A on algoritmi, joka on määritelty mille tahansa rekursiivista funktiota kuvaavalle ohjelmankoodille ja joka antaa tuloksena rekursiivista funktiota kuvaavan ohjelmakoodin, niin A :lla on kiintopiste. Siis on olemassa ohjelma, jonka A muuntaa ohjelmaksi, joka tekee täsmälleen saman kuin alkuperäinen ohjelma." Gödelin epätäydellisyyslause saadaan numeroimalla kaikki ohjelmat $P_0, P_1, P_2, \dots$ ja tarkastelemalla algoritmia a , joka antaa tulokseksi ensimmäisen ohjelman $a(P)$, jolle voidaan todistaa annetussa formaalissa kielessä, että se ei ole ekvivalentti P :n kanssa. Jos a olisi määritelty kaikille ohjelmille, niin kiintopistelauseen nojalla olisi ohjelma P , joka olisi ekvivalentti tuloksen $a(P)$ kanssa, mutta a :n määritelmän nojalla tämä on mahdotonta. Siispä on olemassa rekursiivista funktiota kuvaava ohjelma Q , jolle ei voida todistaa sen epäekvivalenssia minkään muun ohjelman kanssa. Otetaan nyt jokin ohjelma P , joka ei ole ekvivalentti Q :n kanssa. Rekursiivisten funktioiden määritelmä on sellainen, että on mahdollista muodostaa kyseisessä formaalissa kielessä lause " Q ei ole ekvivalentti P :n kanssa." Tätä lausetta ei siis voida todistaa, vaikka se on tosi.

Kolmas todistus perustuu erääseen paradoksiin. Ensimmäisessä todistuksessa ikään kuin käytettiin hyödyksi vanhaa valehtelijan paradoksia "minä valehtelen", ja tässä käytetään seuraavaa paradoksaalista määritelmää: "olkoon n pienin luonnollinen luku, jota ei voida määritellä alle kahdellakymmenellä sanalla." Edellisessä lauseessa on alle kaksikymmentä sanaa, ja se määrittelee luvun n . Seuraavaksi alettiin määrittelemään tarkemmin erilaisia käsitteitä, jotta saataisiin paradoksia vastaava ristiriita mikäli kaikki todet lauseet voitaisiin todistaa. En muista tarkemmin tätä enkä viimeistäkään todistusta, joka perustuu siihen, ettei voida tehdä algoritmia, joka tarkistaa kaikkien ohjelmien pysähtyvyyttä ne kaikilla syötteillä.

Toiseksi mielenkiintoisin luento oli ehdottomasti Gusein-Zaden, ja sen aihe oli Brownin liike. Aihe on hyvin vaikea jos keskittyy teknisiin yksityiskohhtiin. Ajatuksena oli tarkastella kaksi- ja kolmiulotteisella ruudukolla tapahtuvaa satunnaiskulkua, jossa jokaisella ajanhetkellä kulkijalla on yhtä suuri todennäköisyys siirtyä mihin tahansa viereiseen ruutuun. Seuraavaksi annettiin ruutujen koon pienentyä ja rajaprosessin jälkeen siirryttiin tarkastelemaan jatkuvaa satunnaishäiriötä kaksi- ja kolmiulotteisessa avaruudessa. Tässä ei siis kiinnitetty huomiota rajaprosessin yksityiskohtiin. Tarkoituksena oli etsiä vastaus kysymykseen: "millä todennäköisyydellä kulkija palaa jossakin vaiheessa takaisin aloituspisteeseen?" Oikeastaan, koska piste on nollamittainen joukko avaruudessa, on todennäköisyys nolla. Siispä siirryttiin kysymään millä todennäköisyydellä kulkija palaa takaisin origokeskiseen r -säteeseen palloon.

Ongelman täsmälliseksi muotoilemiseksi määrittelimme

funktion $P(x, y, z)$, joka kertoo millä todennäköisyydellä pisteestä (x, y, z) päästään r -säteiseen origokeskiseen palloon. Tälle on kohtuullista olettaa, että $0 \leq P \leq 1$ kaikkialla ja $P = 1$ r -säteisessä origokeskisessä pallossa. Lisäksi tuntui järkevältä olettaa, että P riippuu vain etäisyydestä origoon, eikä napakulmasta. Itse asiassa tämä ominaisuus todistettiin oikeaksi ruudukolla, joten rajaprosessin myötä se siirtyisi P :lle. Kolmas ominaisuus oli tärkein. Tarkastelimme mielivaltaista pistettä a_0 avaruudessa, ja se keskipisteenä olevaa r_0 säteistä palloa. Symmetrian perusteella oletettiin, että todennäköisyys päästä keskipisteestä ympyrän kehän mielivaltaiselle pisteelle on vakio. Kokonaistodennäköisyyden kaavan perusteella saatiin siis, että $P(a_0)$ on yhtä suuri kuin keskiarvo luvuista $P(x, y, z)$, missä (x, y, z) käy läpi annetun pallon. Tämä on analyysissä hyvin tunnettu ominaisuus. Sitä kutsutaan funktion P harmonisuudeksi. Tarkastelemalla P :n Taylor-kehitysmää saimme, että P :n toisen kertaluvun osittaisderivaattojen summa on aina nolla. Muodostunut yhtälö, eli $\Delta P = 0$, on nimeltään Laplacen yhtälö. Tässä merkitsimme $\Delta = \partial_1^2 + \partial_2^2 + \partial_3^2$, missä viimeistä termiä ei ole kaksiulotteisessa tapauksessa. Koska P riippui vain etäisyydestä R origoon, niin määrittelimme $P(x, y, z) = G(R)$. Tämän jälkeen Laplacen yhtälö sai muodon $G''(R) + (n-1)/R \cdot G'(R) = 0$, missä n on ulottuvuus. Tasossa siis $G'' + G'/R = 0$. Tämän yhtälön ainoa alkuehdot toteuttava ratkaisu on vakiofunktio $G \equiv 1$. Kolmiulotteisessa avaruudessa saatiin ratkaisuksi $G(R) = C_1/R + C_2$ joten piti analysoida lisää ruudukkomallia, jotta nähtäisiin, että $G \rightarrow 0$, kun R kasvaa rajatta. Muiden alkuehtojen kanssa saimme, että $G(R) = r/R$, missä r on alkuperäisen origokeskisen pallon säde. Siis tasossa aina päädytään alkupisteeseen, kun taas kolmiulotteisessa avaruudessa todennäköisyys pienenee etäisyyden kasvaessa.

Viimeisin luento, jonka kuvailen, oli pedagogisesti tärkein. Tihomirovin esitelmän nimi oli ”lyhyt matematiikan kurssi.” Sen aiheena oli Venäjän yliopiston kahden ensimmäisen vuoden opintojen ne tärkeimmät asiat, joita tarvitaan melkein joka tutkimusosalalla. Nämä olivat lineaariset yhtälöt, toisen asteen pinnat, epälineaaristen yhtälöiden ratkaiseminen ja differentiaalilaskenta. Lisäksi näitä käsiteltiin eri ulottuvuuksissa: suoralla, tasossa, mielivaltaisen moniulotteisessa avaruudessa ja ääretönulotteisessa avaruudessa. Esimerkkinä ääretönulotteisesta avaruudesta mainittiin ℓ_2 , jonka pisteet ovat muotoa $\mathbf{x} = (x_1, x_2, x_3, \dots)$, missä ajatuksena on, että $\mathbf{x}$:n ”etäisyys” origoon on äärellinen. Tavallisessa n -ulotteisessa avaruudessa etäisyys origoon, *normi*, on $\sqrt{x_1^2 + x_2^2 + \dots + x_n^2}$. Vastaavalla ajatuksella ääretönulotteisen avaruuden normi on $\sqrt{x_1^2 + x_2^2 + x_3^2 + \dots}$, eli ℓ_2 sisältää ne pisteet, joilla $x_1^2 + x_2^2 + x_3^2 + \dots < \infty$.

Lineaarisista yhtälöistä Tihomirov antoi esimerkin $Ax = b$, missä A ja b olivat reaali-lukuja. Tässä on kolme

tapausta. Jos A ei ole nolla, niin on tasan yksi ratkaisu. Jos $A = b = 0$, niin on äärettömän monta ratkaisua ja jos $A = 0$, $b \neq 0$, niin ei ole yhtäkään ratkaisua. Tasossa ja n -ulotteisessa avaruudessa näimme vastaavan ilmiön, kun tulkitsimme, että A on $n \times n$ -matriisi ja b on $n \times 1$ -sarakematriisi, eli vektori. Äärellisulotteisissa tapauksissa olisimme yhtä hyvin voineet sanoa, että A on lineaarikuvaus, eli $A(\alpha\mathbf{x} + \beta\mathbf{y}) = \alpha A(\mathbf{x}) + \beta A(\mathbf{y})$ kaikilla reaali-luvuilla α, β ja n -ulotteisen avaruuden pisteillä $\mathbf{x}$ ja $\mathbf{y}$. Ääretönulotteisessa tapauksessa Tihomirov kertoi vastaavan tuloksen olevan totta, mikäli A :lle oletettaisiin yksi lisäominaisuus. Tämä tulos tunnetaan nimellä Fredholmin vaihtoehdot (Fredholm alternative), ja se sanoo, että mikäli $A = I + C$, missä I on identtinen operaattori ja C on kompakti lineaarinen operaattori, niin yhtälöllä $A(\mathbf{x}) = \mathbf{b}$ on joko ratkaisu kaikilla $\mathbf{b}$ tai yhtälöllä $A(\mathbf{x}) = 0$ on epätriviaali ratkaisu.

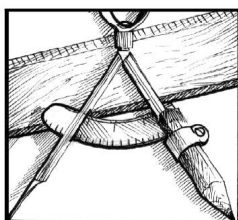
Toisesta aiheesta, toisen asteen pinnoista, emme puhuneet suoraan, vaan tarkastelimme useamman muuttujan toisen asteen polynomeja. Yksiulotteisessa tapauksessa polynomi oli muotoa $Q(x) = ax^2 + bx + c$. Siirryimme uuteen muuttujaan $y = xb/(2a)$, jolloin saimme $Q = ay^2 + c'$, missä c' oli vakio. Toisen ulottuvuuden tapauksessa $Q(x) = a_1x_1^2 + 2a_2x_1x_2 + a_3x_2^2$. Tässä oli jätetty alempiasteiset termit huomioimatta. Tällöinkin oli olemassa kääntyvä lineaarinen muuttujanvaihto $\mathbf{y} = \mathbf{y}(\mathbf{x})$, jolla $Q = \lambda_1y_1^2 + \lambda_2y_2^2$, missä kertoimet λ_1 ja λ_2 olivat vakioita. Vastaavasti n -ulotteisessa avaruudessa saimme $Q = \lambda_1y_1^2 + \lambda_2y_2^2 + \dots + \lambda_ny_n^2$. Ääretönulotteisessa tapauksessa tarkastelimme yllämainitun ℓ_2 :n pisteitä. Määrittelimme Q :n äärettömän summan $Q(\mathbf{x}) = \sum a_{ij}x_ix_j$ avulla, missä $\sum a_{ij}^2$ on äärellinen. Tihomirovin mukaan oli myös totta, että on olemassa muuttujanvaihto, jonka avulla $Q = \sum \lambda_iy_i^2$.

Epälineaaristen yhtälöiden ratkaisemisesta Tihomirov kertoi vain erään numeerisen algoritmin. Perusajatuk-sena oli kysymys: ”mitä jos yhtälöä kuvaava funktio olisikin lineaarinen?” Tihomirov kertoi, että jos nollakohdan alkuarvaus on x_0 , niin funktion arvo ensimmäisessä pisteessä on $f(x_0)$. Jos f olisi lineaarinen ja sen kulmakerroin olisi λ , niin oikea nollakohta olisi $x_0 - \lambda^{-1}f(x_0)$. Tämän toteamiseksi riittää tarkastella kulmakertoimen määritelmää. Edellisestä saimme algoritmin $x_{n+1} = x_n - \lambda^{-1}f(x_n)$. Se muistuttaa Newtonin menetelmää, jossa onkin $\lambda = f'(x_n)$. Tässä tapauksessa λ oli kuitenkin vakio. Seuraavaksi Tihomirov todisti kaikissa äärellisulotteisissa tapauksissa, että eräillä f :n ehdoilla algoritmi suppenee aina johonkin tietyn etäisyyden päässä olevaan nollakohtaan. Ääretönulotteisessa tapauksessa sama on totta, kunhan tulkitaan mitä f , λ ja x ovat. Tihomirov antoi esimerkin, jossa ”pisteinä” tai muuttujina pidettiin välillä $[a, b]$ jatkuvia funktioita. Näiden välinen ”etäisyys” määriteltiin funktioiden erotuksen itseisarvon maksimina, eli $\text{dist}(g, h) = \max |g(x) - h(x)|$. Algoritmis-sa esiintyvä f korvattiin epälineaarilla operaattorilla

$f[y](x) = y(x) - y_a - \int g(t, y(t))dt$ ja λ korvattiin identtisellä kuvauksella. Tässä siis y oli välillä $[a, b]$ jatkuva funktio, kuten myöskin $f[y]$, ja $f[y]$ sai pisteessä x ylläolevan kaavan mukaisen arvon $f[y](x)$. Osoittautui, että tämä operaattori toteuttaa vaaditut ehdot. Tästä seurasi, että alkuarvo-ongelmalla $y'(x) = g(x, y(x))$, $y(a) = y_a$ on aina ratkaisu, joka on määritelty välillä $[a, a + \epsilon]$ jollakin positiivisella ϵ . Kaiken tämän jälkeen Tihomirovilla ei ollut aikaa puhua differentiaalilasken-

nasta.

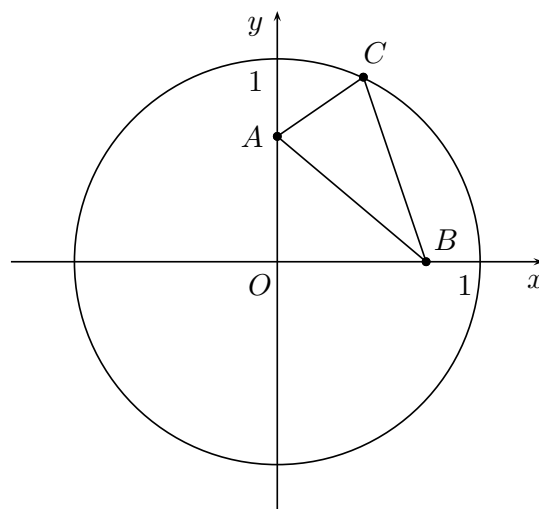
Loppumatka meni yllättävän hyvin. Bussi Dubnasta Moskovaan ei juuttunut mihinkään ja matka kesti vain kolme tai neljä tuntia. Junani lähtöön oli vielä viisi tuntia aikaa, joten kävin parin kesäkoulun järjestäjän kanssa turistikierroksella Kremlin ympäri. Illalla menin junaan ja aamupäivällä olin takaisin Suomessa. Kiitän matkan rahoittajia ja järjestäjiä erinomaisesta kesäkoulusta.



Geometrian pähkinä

Tauno Tukkinen

Yksikköympyrän keskipiste on origossa O . Positiiviselta y -akselilta valitaan yksikköympyrän sisältä jokin piste A , positiiviselta x -akselilta yksikköympyrän sisältä piste B ja yksikköympyrän kehältä ensimmäisestä koordinaattineljänneksestä piste C . Todista, että kolmion ABC piirin pituus on vähintään 2.



Vinkki tehtävään löytyy sivulta 20.

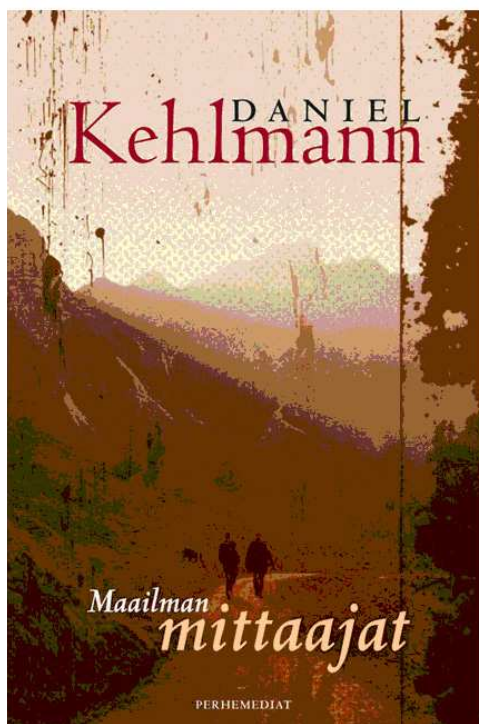


Gauss romaanihenkilönä

Matti Lehtinen

Maanpuolustuskorkeakoulu

Daniel Kehlmann: Maailman mittaajat. Suomentanut Ilona Nykyri. Perhemediat, 2007. 288 s. Ovh. 26 e.



Matemaatikko on yleisen käsityksen mukaan elämälle ja muulle maailmalle vieras norsunluutorninsa asukas.

Tältä kannalta on hiukan yllättävää, että on kuitenkin kohtalaisen useita romaaneja, joissa matemaatikko on pääosassa. Viime aikoina ovat eteen tulleet ainakin Fredrik Långin *Elämäni Pythagoraana* (Tammi) ja Jukka M. Heikkilän kirjat *Arkhimedes Syrakusalainen* sekä *Tyranni*, jossa Arkhimedes myös vahvasti esiintyy (Karisto). Melko vähän kaunokirjallisuudesta tunnettu Perhemediat-kustannusyhtiö on nyt tuonut markkinoille saksalais-itävaltalaisen Daniel Kehlmannin romaanin *Maailman mittaajat*. Siinä on kaksi päähenkilöä, tutkimusmatkailija Alexander von Humboldt ja matemaatikko Carl Friedrich Gauss (1777–1855).

Vuonna 1975 syntynyt Kehlmann on saksalaisella kielialueella varsin tunnettu kirjailija. *Maailman mittaajat* on Saksassa ollut myydyimpien kirjojen listalla ja se on käännetty useille kielille. Romaani seurailee väljästi päähenkilöitään, joiden intohimona on ymmärtää maailmaa. Gaussin ymmärrys syntyy ennen muuta ajattelun kautta, Humboldt, ilmeisesti kirjailijalle helpommin lähestyttävä kohde, kokeilee, matkustaa ja yrittää nähdä. Miehet tapaavat kirjan alussa, mutta kumpikin jo uriensa loppupuolella, vuonna 1828, eivätkä oikeastaan löydä yhteistä pohjaa vaikka yhdistävätkin voimaansa magnetismin tutkimuksessa. Suurin osa romaania jakautuu vuorotteleviin Gaussin ja Humboldtin elämää valottaviin jaksoihin, jotka etenevät paljon toisiinsa sitoutumatta. Kumpikin on omalla tavallaan monomaani ja epäsosiaalinen, kumpikaan ei oikein saa muuta maailmaa oikealla tavalla käsittämään pyrkimyksiään. Kuuluisuuskaan ei tule niistä ansioista, jotka miehet

itse tuntevat tärkeimmikseen.

Kehlmannin Gauss ei aivan vastaa sitä mielikuvaa, jonka saa lukemalla Gaussin elämäkertoja. Niiden kirjoittajat ovat yleensä matemaatikkoja, joita häikäisee Gaussin matemaattinen tuotteliaisuus ja ideoiden runsaus - kaikki se, mikä on saanut jälkimaailman nimittämään Gaussia matemaatikkojen kuninkaaksi. Kehlmann esittää Gaussin hiukan toisessa valossa: pääosin pettyneenä ja kätttyisänä, jonkin verran koomisenakin henkilönä, joka jo kirjoitettuaan suuren lukuteoreettisen teoksensa *Disquisitiones Arithmeticae* parikymppisenä tietää antaneensa tärkeimpänsä ja tietää, että loppuelämä tulee olemaan alamäkeä. Kehlmannin Gauss on ajattelunsa nopeudessa yliverlainen, mutta kärsimätön, kun muut ihmiset eivät ole yhtä nopeita. Vain Gaussin ensimmäinen vaimo Johanna on älyllisesti Gaussin kanssa samoilla tasoilla. Mutta kun tämä kuolee lapsivuoteeseen, Gauss on tyynen rationaalinen. Hänellä on perhe, jota hän ei kykene hoitamaan. Siis on mentävä uudelleen naimisiin, vaikka Johannan ystävä Minna, ilmeinen vaimokandidaatti, onkin Gaussia aina lähinnä ärsyttänyt.

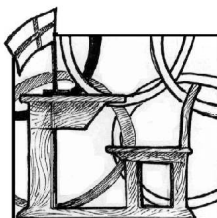
Kehlmann on lukenut Gauss-elämäkertansa. Kirja esittelee suurin piirtein ne Gaussin elämän tapahtumat, jotka historioitsijatkin tapaavat tuoda julki, kuitenkin kaunokirjailijan vapaudella. Niinpä Gaussin lapsuuden ja nuoruuden kuvauksiin liittyy tunnetun lukujen yhdestä sataan yhteenlaskun, Martin Bartelsin tarjoaman matematiikkaan johdatuksen ja Braunschwei-

gin herttuan sponsoritoiminnan ohella myös kuviteltu kuumailmapalloretki Montgolfierin veljesten oppilaan Pilâtre de Rozierin kanssa ja matka jo seniiliin Immanuel Kantin luo Königsbergiin – kytkös Kehlmannin omiin, kesken jääneisiin Kant-tutkimuksiin ja Gaussin myöhemmin ajattelemiin joskin julkaisematta jättämiin euklidista geometriaa korvaaviin rakennelmiin. Kantillehan Eukleideen geometria oli absoluuttinen totuus.

Kirjan lukija saa vahvistusta käsitykselle, että matematiikka olisi erityisesti nuoren miehen työtä, kun Kehlmann antaa ymmärtää, että Gauss koki tehneensä elämäntyönsä *Disquisitiones Arithmeticae* valmistuttua vuonna 1801. Näinhän ei sentään käynyt, ja Gaussin matemaattisten saavutusten lista pitene vielä paljon.

Gaussin yksityiselämän kuvauksissa Kehlmann on voinut pitkälle käyttää mielikuvitustaan. Tuskin tiedämme, seurusteliko Gauss oikeasti pitkään venäläisen prostituoidun kanssa, mutta kun kirjailija antaa henkilönsä näin tehdä, se on osa hänen rakentamaansa maailmaa, johon lukijana on sopeuduttava.

Maailman mittajia ei ole kirjoitettu erityisesti matematiikan harrastajille. Gaussin muissakin yhteyksissä kohdannut lukee toki kirjan erityisen suurella mielenkiinnolla. Ilona Nykyrin suomennos selviytyy hyvin muutamista matemaattisisältöisistä jaksoistakin. Kannattaa lukea!



Matematiikkakilpailu opettajillekin?

Matti Lehtinen

Maanpuolustuskorkeakoulu

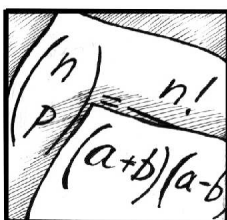
Matematiikkakilpailuja järjestetään kaikkialla maailmassa nuorten innostamiseksi matematiikan pariin. Yksi tärkeä lenkki kilpailujen tavoitteen saavuttamisessa on matematiikan opettaja. Jos opettaja ei tiedota kilpailumahdollisuudesta eikä osaa opastaa oppilaitaan kilpailumatematiikan pariin, ei kilpailujärjestelmä toimi. Suomessa ei ole aivan harvinaista, että tieto esimerkiksi lukion valtakunnallisista matematiikkakilpailuista pysähtyy opettajaan.

Mikä avuksi? Opettaja, joka on itse innostunut tehtävänratkaisu-urheilusta, on varmasti omiaan kannustamaan oppilaitaan ja tasoittamaan heidän tietään matematiikkakilpailun alkuun kivisentuntuisella saralla. Mutta opettajille ei ole omia kilpailuja. Opettajat kilpailevat monissa lajeissa: Opettaja-lehdestä voi lukea niin opettajien šakki- kuin sulkapalloturnauksistakin. Mutta otetaanpa kerran esimerkkiä Mongoliasta, maasta, joka johdonmukaisesti menestyy Kansainvälisissä matematiikkaolympialaisissa Suomea paremmin.

Mongolian kansallisissa matematiikkaolympialaisissa on kaksi kilpailua: oppilaiden ja opettajien. Opettajien kilpailussa palkintoina on kunnian lisäksi rahaa. Seuraavassa 43. Mongolian kansallisten matematiikkaolympialaisten, joita pidettiin Ulan Bataarissa 5. – 11. toukokuuta 2007, opettajien sarjan tehtävät. Opettajat ja oppilaat, lähettäkää ratkaisuehdotuksenne Solmuun. Entä kuka on aktiivinen ja organisoi ensimmäiset Suo-

men opettajien matematiikkakilpailut?

1. Kuinka monen joukon $\{1, 2, 3, \dots, 5n\}$ osajoukon alkoiden summa on jaollinen viidellä?
2. On annettu 101 saman suoran janaa. Todista, että janojen joukossa on 11 sellaista, joilla on yhteinen piste tai 11 sellaista, joista millään kahdella ei ole yhteisiä pisteitä.
3. Olkoon p pariton alkuluku. Olkoon g primitiivijuuri mod p [pienin x , jolle $x^q \not\equiv 1 \pmod{p}$, kun $q < p - 1$]. Määritä kaikki sellaiset p :n arvot, joille joukkojen $A = \{k^2 + 1 \mid 1 \leq k \leq \frac{p-1}{2}\}$ ja $B = \{g^m \mid 1 \leq m \leq \frac{p-1}{2}\}$ alkioit ovat samat mod p .
4. Todista: jos x , y ja z ovat luonnollisia lukuja ja $xy = z^2 + 1$, niin on olemassa kokonaisluvut a , b , c ja d niin, että $x = a^2 + b^2$, $y = c^2 + d^2$ ja $z = ac + bd$.
5. Piste P on tasasivuisen kolmion ABC ympäri piirretyn ympyrän piste. Osoita, että janat PA , PB ja PC voivat olla kolmion sivuja. Olkoon R kolmion ympäri piirretyn ympyrän säde ja d pisteen P ja mainitun ympyrän keskipisteen välimatka. Määritä konstruoidun kolmion ala.
6. Olkoon $n = p_1^{\alpha_1} \dots p_s^{\alpha_s} \geq 2$. Oletetaan, että luvulle α ja kaikille i , $1 \leq i \leq s$, pätee $(p_i - 1) \mid \alpha$. Todista, että $n \mid \sum_{a \in \mathbb{Z}_n^*} a^\alpha$, missä $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$. [(a, n) on lukujen a ja n suurin yhteinen tekijä].



Kuusi vaikeaa tehtävää – matematiikkaolympialaiset Hanoissa

Matti Lehtinen

Maanpuolustuskorkeakoulu

48. Kansainväliset matematiikkaolympialaiset pidettiin Hanoissa Vietnamissa 23.–31. heinäkuuta 2007. Ennätyselliset 520 kilpailijaa 93 maasta ratkoi tavan mukaan kahtena päivänä yhteensä yhdeksän tunnin ajan kuutta vaikeaa tehtävää. Kukaan ei saanut kaikkia tehtäviä virheettömästi ratkaistuksi, mutta jokaiselle tehtävälle löytyi ratkaisija. Olympiatehtävien arvosteluasteikko on nollasta seitsemään. Kilpailun tulokset löytyvät sivuilta <http://www.imo2007.edu.vn>.

Esittelen tässä olympialaisten kuusi tehtävää ja niiden ratkaisut.

Tehtävä 1

Kilpailun tehtävistä ensimmäisen tuomaristo valitsi kategoriasta algebra. Tehtävä oli seuraava:

On annettu reaaliluvut $a_1, a_2, \dots, a_n$. Jokaiselle i , $1 \leq i \leq n$, määritellään

$$d_i = \max\{a_j \mid 1 \leq j \leq i\} - \min\{a_j \mid i \leq j \leq n\}.$$

Olkoon

$$d = \max\{d_i \mid 1 \leq i \leq n\}.$$

(a) Osoita, että mielivaltaisille reaaliluvuille $x_1 \leq x_2 \leq \dots \leq x_n$ pätee

$$\max\{|x_i - a_i| \mid 1 \leq i \leq n\} \geq \frac{d}{2}. \quad (*)$$

(b) Osoita, että on olemassa reaaliluvut $x_1 \leq x_2 \leq \dots \leq x_n$, joille epäyhtälössä (*) vallitsee yhtäsuuruus.

Ensimmäinen tehtävä on tavan mukaan helppohko. Niin tämäkin, vaikka se ensilukemalta näyttää aika mutkikkaalta ja yllättävältäkin: siinähan esiintyy kaksi eri lukujonoa tai oikeastaan n :n luvun järjestettyä joukkoa, joilla ei sinänsä ole mitään tekemistä keskenään. Ensimmäisen jonon perusteella muodostetaan lisäksi kolmas, d_i , jonka jäsenet ovat indeksiin i asti suurimman ja samasta indeksistä i loppuun asti laskettuna pienimmän a -luvun erotuksia. Koska a_i on mukana molemmissa joukoissa, kaikki d_i :t ovat ei-negatiivisia. Luvuista d_i suurin on d . Silloin on jokin indeksi k , ei välttämättä yksikäsitteinen, jolle $d_k = d$. Edelleen, kun kerran äärellisistä joukoista on kyse, löytyvät indeksit p ja q , joille $d = d_k = a_p - a_q$. Tässä on tietysti $p < q$. p ja q eivät nekään ole yksikäsitteisiä, mutta riittää, että ainakin jotkin tällaiset luvut ovat olemassa.

Tehtävän (a)-kohdan todistukseksi riittää, jos osoitetaan, että olipa (x_k) mikä nouseva jono hyvänsä, niin x_k :n etäisyys ainakin toisesta luvuista a_p ja a_q on $\geq \frac{d}{2}$. Mutta tämä onkin aika lailla itsestään selvää.

Jos nimittäin $x_p \leq a_p - \frac{d}{2}$, asia on selvä. Jos taas $x_p > a_p - \frac{d}{2}$, niin (x_i) -jonon kasvavuuden vuoksi myös

$x_q > a_p - \frac{d}{2}$. Mutta $a_p - \frac{d}{2} = a_q + \frac{d}{2}$, joten tässä tapauksessa $x_q - a_q > \frac{d}{2}$. Tehtävän (a)-kohdan oikea ratkaisu tuotti kilpailijalle 3 pistettä.

Täysien pisteiden saamiseksi kilpailijan piti vielä keksiä jokin kasvava lukujono (x_i), jolle tehtävän epäyhtälössä vallitsee yhtäsuuruus. Tässä täytyy huomata, että (a_i) on lukujono, joka on annettu, ja jono (x_i) voidaan rakentaa jonon (a_i) varaan. Jonoa (x_i), joka toimisi halutulla tavalla kaikkien mahdollisten (a_i)-jonojen suhteen, ei tietenkään voi löytyä.

Mahdollisia tapoja määrittellä jono (x_i) on useita. Yksi strategia on lähteä mahdollisimman alhaalta: näin voidaan ehkä helpoimmin varmistua siitä, että jonosta on vara tehdä kasvava. Aloitetaan siis asettamalla $x_1 = a_1 - \frac{d}{2}$. Seuraavan luvun on oltava $\geq x_1$, mutta se ei saa erota a_2 :sta enempää kuin $\frac{d}{2}$. Asetetaan siis $x_2 = \max\{x_1, a_2 - \frac{d}{2}\}$. Nythän $a_1 - a_2 \leq d$, joten a_2 :n ja x_2 :n välimatka ei ylitä $\frac{d}{2}$:ta. Havaintomme kannustaa jatkamaan jonon määrittelyä samalla tavalla. Se on syytä tehdä induktiivisesti: jos $x_1, x_2, \dots, x_{k-1}$ on määritetty, asetetaan $x_k = \max\{x_{k-1}, a_k - \frac{d}{2}\}$. Näin saadaan ilman muuta nouseva jono: $x_k \geq x_{k-1}$ kaikilla k . Myös epäyhtälö $x_k - a_k \geq -\frac{d}{2}$ tulee automaattisesti todeksi. Ainoa varmistettava seikka on enää epäyhtälö $x_k - a_k \leq \frac{d}{2}$. Tämän varmistamiseksi täytyy palata jonossa pienimpään indeksiin j , jolle $x_k = x_j$. Tämä j on joko 1 tai sellainen, että $x_{j-1} < x_j$, jolloin myös, koska x_i :t määritellään niin kuin ne määritellään, $x_j = a_j - \frac{d}{2}$. Mutta $a_j - a_k \leq d$. Siispä $x_k - a_k = x_j - a_j + a_j - a_k < -\frac{d}{2} + d = \frac{d}{2}$, niin kuin pitikin.

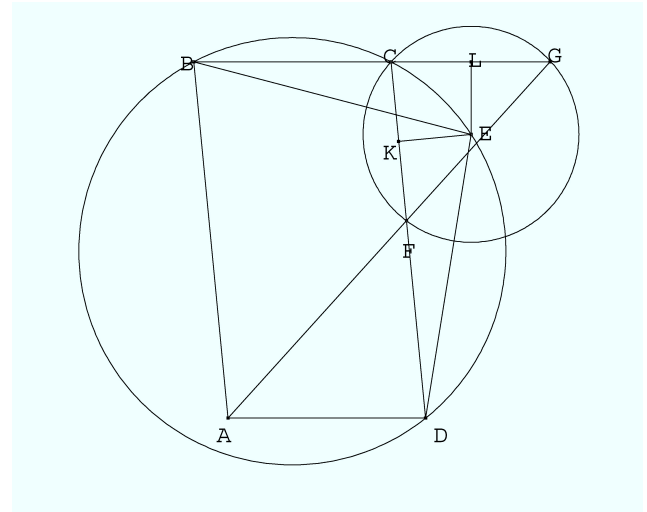
Tehtävään 1 kilpailijat antoivat 161 täysin pistein arvosteltua vastausta. Pistekeskiarvo oli 3,4.

Tehtävä 2

Kansainvälisten matematiikkaolympialaisten tehtävät valitaan neljästä kategoriasta, joista yksi on geometria. Lähes aina geometrian luokasta tulee valituksi kaksi tehtävää, joista toinen on helppo, toinen vaativampi. Tällä kertaa vaativampi tehtävä oli sijoitettu ensimmäisen kilpailupäivän toiseksi tehtäväksi. Se oli tällainen:

Pisteet A, B, C, D ja E sijaitsevat niin, että $ABCD$ on suunnikas ja $BCED$ on jännenelikulmio. Suora ℓ kulkee pisteen A kautta. Oletetaan, että ℓ leikkaa janan DC sen sisäpisteessä F ja suoran BC pisteessä

G . Oletetaan, että $EF = EG = EC$. Todista, että ℓ on kulman DAB puolittaja.



Kun tilanteesta piirtää kuvan, huomaa, että $\angle FAD = \angle FGC$ (koska $GC \parallel AD$) ja $\angle BAF = \angle CFG$ (koska $AB \parallel FC$). Tavoitteeksi voi siis ottaa kulmien CFG ja CGF yhtäsuuruuden osoittamisen, mikä taas seuraisi kolmion CFG tasakylkisyydestä. Jännenelikulmio-oletuksen hyödyllinen seuraus on aika ilmeinen: kulmat CBE ja CDE ovat yhtä suuret. (Jännenelikulmioon tarkoittaa nelikulmiota, jonka ympäri voidaan piirtää ympyrä; kulmien yhtäsuuruus seuraa kehäkulmalauseesta.) Tämä johtaa houkutukseen todistaa kolmiot CBE ja FDE yhteneviksi. Jos tämä saataisiin varmaksi, esitetty tasakylkisyyssuoritus helposti. Kun kolmioista ei kuitenkaan löydy tarvittavaa kolmatta samanlaista osaparia, on edettävä mutkitellen.

Tehdäänpä siis vastaoletus, jonka mukaan olisi $CG > CF$. Koska E on oletuksen mukaan kolmion CFG ympäri piirretyn ympyrän keskipiste, janteen CF tulee nyt olla kauempana E :stä kuin janteen CG .

Piirretään vielä E :n kohtisuorat projektiot K ja L sivuille CF ja CG . Sivujen CF ja CG puolikkaille KF ja CL pätee $KF < CL$. Edellä sanotun perusteella $EK > EL$. Suorakulmaiset kolmiot DEK ja BEL ovat yhdenmuotoisia (kk), joten $KD > BL$. Mutta nyt $AD = BC = BL - CL < DK - KF = FD$. Kolmiot CFG ja DFA ovat yhdenmuotoiset, koska $CG \parallel AD$. Mutta nyt on tultu siihen risitriitatilanteeseen, että kolmiossa ADF on $AD < FD$, mutta kolmiossa CFG vastinsivut ovat toisessa suuruusjärjestyksessä, $CF < CG$. Tämä on mahdotonta, joten vastaoletus $CG > CF$ ei voi olla tosi. Mutta oletuksesta $CG < CF$ seuraa aivan samojen päättelyaskelten jälkeen myös ristiriita. Siis $CG = CF$, ja väite on todistettu.

Tehtävän kaksi ratkaisi oikein 137 kilpailijaa ja pistekeskiarvo oli 2,5.

Tehtävä 3

Ensimmäisen kilpailupäivän kolmas tehtävä oli kombinatorinen. Siinä esiintyy verkkoteorian käsite klikki, mutta tehtävä oli muotoiltu, niin kuin usein tapana on, ihmisjoukossa vallitsevien tai ei-vallitsevien relaatioiden avulla.

Matematiikkakilpailun osallistujista jotkut ovat toistensa ystäviä; ystävyys on aina molemminpuolista. Sanomme, että jokin kilpailijoiden joukko on klikki, jos kaikki sen jäsenet ovat toistensa ystäviä. (Erityisesti joukot, joissa on vähemmän kuin kaksi alkioita, ovat klikkejä.) Sanomme klikin jäsenten lukumäärää klikin kooksi.

Tiedetään, että tässä kilpailussa klikkien suurin koko on parillinen. Todista, että kilpailijat voidaan jakaa kahteen huoneeseen niin, että suurikokoisin toisessa huoneessa oleva klikki on samankokoinen kuin suurikokoisin toisessa huoneessa oleva klikki.

Keskeinen havainto klikin olemuksesta on, että klikin jokainen epätyhjä osajoukko on klikki. Merkitään $|E|$:lla joukon E alkioden lukumäärää. Merkitään huoneissa olevien kilpailijoiden joukkoja symboleilla A ja B ja merkitään vastaavasti huoneessa olevan suurikokoisimman klikin kokoa $c(A)$:lla ja $c(B)$:llä. Olkoon nyt M jokin klikki, jonka koko on suurin mahdollinen. Tällaisiahan voi olla useita, mutta tarkastetaan yhtä sellaista. Olkoon $|M| = 2m$.

Lähdetään rakentamaan vaadittua huoneisiin jakoa niin, että sijoitetaan aluksi kaikki M :n jäsenet huoneeseen A ja kaikki muut kilpailijat huoneeseen B . Silloin $c(A) = |M| \geq c(B)$. Nyt voi olla niin, että $c(A) = c(B)$. Tällöin vaadittu sijoittelu on tehty, ja olemme tyytyväisiä.

Jos onkin $c(A) > c(B)$, siirretään yksi henkilö huoneesta A huoneeseen B . Tällöin $c(A)$ pienenee yhdellä ja $c(B)$ joko säilyy ennallaan tai kasvaa yhdellä, riippuen siitä, kasvattiko siirretty henkilö B -puolen suurinta klikkiä vai ei. Jatketaan siirtoja, kunnes $c(A) \leq c(B) \leq c(A) + 1$. Tällainen tilanne tulee vastaan viimeistään silloin, kun puolet A -huoneessa aluksi olleista on siirretty B :hen. Kuvatussa tilanteessa on siis $c(A) = |A| \geq m$. Merkitään $c(A) = k$. Jos nyt $c(A) = c(B)$, jako on valmis.

Ellei näin ole, on oltava $c(B) = c(A) + 1$. Jos nyt B -huoneessa on kilpailija $x \in M$ ja klikki C , jolle $|C| = k + 1$, mutta $x \notin C$, niin siirretään x huoneeseen A . Silloin $c(A) = k + 1 = |C| = c(B)$, ja jako on suoritettu. Ellei tällaista kilpailijaa ole, niin jokainen $x \in B \cap M$ kuuluu joihinkin sellaiseen klikkiin $C \subset B$, jolle $|C| = k + 1$. Valitaan nyt jokin tällainen klikki C ja siirretään siitä yksi kilpailija, joka ei kuulu M :ään, A -huoneeseen. Tällainen kilpailija on olemassa, koska jos kaikki C :n jäsenet olisivat myös M :n jäseniä,

M :ssä olisi $k + k + 1$ eli pariton määrä jäseniä, toisin kuin tehtävässä oletettiin. Toistetaan askel niin monta kertaa kuin se on mahdollista. Joka siirrossa $c(B)$ pienenee enintään yhdellä. Viimeisen mahdollisen siirron jälkeen $c(B) = k$.

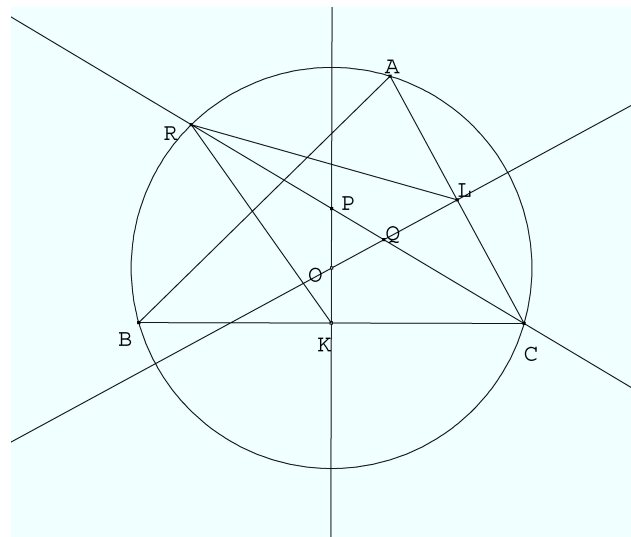
Tarkastellaan nyt tilannetta. A :ssa on yhä klikki $A \cap M$, joten $c(A) \geq k$. Olkoon Q mielivaltainen A :n klikki. Jos $x \in Q$, niin joko $x \in A \cap M$, jolloin x on jokaisen $B \cap M$:n jäsenen ystävä, tai x on siirretty sellaisesta B :n klikistä, joka sisälsi $B \cap M$:n, jolloin x myös on jokaisen $B \cap M$:n jäsenen ystävä. Siis $Q \cup (B \cap M)$ on klikki. Mutta M on suurikokoisin klikki, joten $|M| \geq |Q \cup (B \cap M)| = |Q| + |B \cap M| = |Q| + |M| - |A \cap M|$. Siis $|Q| \leq |A \cap M| = k$. Siis $c(A) \leq k$. Siis $c(A) = k$, ja haluttu jako on suoritettu.

Päätely ei ollut helppo. Kilpailussa sen osasi vain kaksi kilpailijaa. Pistekeskiaarvokaan ei noussut korkeaksi: se oli 0,3.

Tehtävä 4

Kilpailun toinen geometriatehtävä oli sijoitettu toisen kilpailupäivän ensimmäiseksi tehtäväksi. Olettama oli siis, että tehtävä olisi helpohko. Se oli tällainen:

Kolmion ABC kulman BCA puolittaja leikkaa kolmion ympäri piirretyn ympyrän myös pisteessä R , kolmion sivun BC keskinormaalin pisteessä P ja sivun AC keskinormaalin pisteessä Q . Sivun BC keskipiste on K ja sivun AC keskipiste on L . Osoita, että kolmioilla RPK ja RQL on sama ala.



Tehtävä voidaan ratkaista monin tavoin. Tässä yksi: Kolmion RPK sivua RP vastaan piirretyn korkeusjanan pituus on $KP \cdot \sin(\angle CPK)$ ja kolmion RQL sivua RQ vastaan piirretyn korkeusjanan pituus on $LQ \cdot \sin(\angle LQC)$. Koska kulmat KCP ja LCQ ovat yhtä suuret, niin suorakulmaisten kolmioiden CPK ja

CQL kolmannet kulmat KPC ja LQC ovat yhtä suuret. Väite tulee todistetuksi, jos saadaan osoitettua $RP \cdot KP = RQ \cdot LQ$.

Olkoon O kolmion ympäri piirretyn ympyrän keskipiste eli keskinormaalien leikkauspiste. Edellä tehdyn kulmahavainnon perusteella OQP on tasakylkinen kolmio. (Jos $Q = P = O$, tehtävän väite pätee triviaalisti.) Koska P ja Q ovat yhtä etäällä kolmion ABC ympäri piirretyn ympyrän keskipisteestä, niillä on tämänympyrän suhteen sama potenssi. Mutta se merkitsee, että $RP \cdot PC = RQ \cdot QC$. (palautetaan mieleen, että pisteen X potenssi ympyrän Γ suhteen on tulo $XY \cdot XZ$, missä Y ja Z ovat mielivaltaisen X :n kautta kulkevan suoran ja ympyrän Γ leikkauspisteet; tulon arvo on valitusta suorasta riippumaton.) Yhdenmuotoisten suorakulmaisten kolmioiden CPK ja CQL perusteella saadaan heti $PC : KP = QC : LQ$. Siis todellakin $RP \cdot KP = RQ \cdot LQ$.

Tämä tehtävä osoittautui kilpailun helpoimmaksi. Täydet 7 pistettä sai 363 kilpailijaa, ja pistekeskivokin oli 5,7.

Tehtävä 5

Lukuteorian osuudesta kilpailutehtäviin valikoitui vain yksi. Se oli tällainen:

Olkoot a ja b positiivisia kokonaislukuja. Todista, että jos luku $4ab - 1$ on luvun $(4a^2 - 1)^2$ tekijä, niin $a = b$.

Tehtävän ratkaisu on klassisen, Pierre de Fermat'han palautuvan "äärellisen laskeutumisen" menetelmän mukainen. Perusidea on tehdä vastaoletus ja päätellä siitä, että löytyy yhä pienempiä vastaoletukseksi kelpaavia lukuja.

Tehdään siis vastaoletus: oletetaan, että on olemassa vastaesimerkkipari (a, b) , niin että $a \neq b$ mutta $4ab - 1$ on luvun $(4a^2 - 1)^2$ tekijä. Koska $4ab \equiv 1 \pmod{(4ab - 1)}$, niin $(4ab)^2 \equiv 1 \pmod{(4ab - 1)}$ ja $(4b^2 - 1)^2 \equiv (4b^2 - (4ab)^2) = 16b^2(4a^2 - 1) \equiv 0 \pmod{(4ab - 1)}$. Tämä merkitsee, että myös pari (b, a) on vastaesimerkkipari. Voidaan siis olettaa, että on olemassa vastaesimerkkipari (a, b) niin, että $a < b$. Olkoon nyt

$$r = \frac{(4a^2 - 1)^2}{4ab - 1}.$$

Silloin

$$\begin{aligned} r &\equiv (-r)(-1) \equiv (-r)(4ab - 1) \\ &\equiv -(4a^2 - 1)^2 \equiv -1 \pmod{(4a)}. \end{aligned}$$

Siis $r = 4ac - 1$ jollain positiivisella kokonaisluvulla c . Siis $(4ac - 1)(4ab - 1) = (4a^2 - 1)^2$. Oletuksen mukaan $4ab - 1 > 4a^2 - 1$. Siis $4ac - 1 < 4a^2 - 1$ eli $c < a$.

Tarkastellaan nyt kaikkia vastaesimerkkipareja. Jollakin parilla (a, b) lauseke $2a + b$ saa pienimmän mahdollisen arvonsa. Jos $a > b$, niin $2b + a < 2a + b$. Kuitenkin myös (b, a) on vastaesimerkkipari. Jos $a < b$, on olemassa vastaesimerkkipari (a, c) , jolle $c < a$. Selvästi $2a + c < 2a + b$. Kummassakin tapauksessa tullaan ristiriitaan $2a + b$:n minimaalisuuden kanssa. Vastaesimerkkipareja ei siis voi olla olemassa.

Tehtävän ratkaisi oikein 94 kilpailijaa. Pistekeskivaro oli 1,9.

Tehtävä 6

Kilpailun viimeinen tehtävä sisälsi geometrisia ja kombinatorisia aineksia. Ratkaisu oli kuitenkin algebrallinen. Tehtävän alan voisi luonnehtia algebralliseksi geometriaksi. Tehtäviä valittaessa esitettiin arvioita, joiden mukaan tehtävä tulisi osoittautumaan kilpailijoille ylivoimaiseksi.

Olkoon n positiivinen kokonaisluku. Tarkastellaan kolmiulotteisen avaruuden $(n + 1)^3 - 1$ pistettä sisältävää joukkoa

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \dots, n\}, x + y + z > 0\}.$$

Mikä on pienin määrä tasoja, joiden yhdiste sisältää joukon S pisteet, muttei pistettä $(0, 0, 0)$?

Tasot, joiden yhtälöt ovat $x + y + z = k$, $k = 1, \dots, 3n$, sisältävät kaikki S :n pisteet. Näitä tasoja on $3n$ kappaletta. Tästä sinänsä ratkaisun kannalta tarpeellisesta havainnosta ei vielä annettu pisteitä ollenkaan.

Osoitetaan, että vähemmällä kuin $3n$:llä tasolla peitto ei onnistu. Jos peittävien tasoja on m kappaletta ja niiden yhtälöt ovat $T_k(x, y, z) = a_k x + b_k y + c_k z - 1 = 0$, $k = 1, \dots, m$, niin polynomi

$$P(x, y, z) = \prod_{k=1}^m T_k(x, y, z)$$

saa arvon 0 aina kun $(x, y, z) \in S$, mutta $P(0, 0, 0) = (-1)^m \neq 0$. Polynomin aste on m . Osoitetaan, että $m \geq 3n$.

Ratkaisun ymmärtämiseksi kannattaa aluksi käydä läpi tasotapaus. Tarkastellaan siis ensin kahden muuttujan polynomia $P(x, y)$, jolle $P(x, y) = 0$, kun x tai y on jokin luvuista $0, 1, \dots, n$, mutta $(x, y) \neq (0, 0)$, ja jolle $P(0, 0) \neq 0$. Olkoon $S(y) = y(y - 1)(y - 2) \cdots (y - n)$ ja olkoon $R(x, y)$ polynomi, joka saadaan jakojäännökseksi, kun $P(x, y)$ jaetaan $S(y)$:llä: $P(x, y) = Q(x, y)S(y) + R(x, y)$. Nyt $R(x, y)$:n aste y :n suhteen on $< S(y)$:n aste, eikä $R(x, y)$ kaikkiaan ole korkeampaa astetta kuin $P(x, y)$. Lisäksi $R(x, y) = P(x, y)$, kun $x, y \in \{0, 1, \dots, n\}$. Siis

$R(x, y) = R_n(x)y^n + R_{n-1}(x)y^{n-1} + \dots + R_0(x)$. Polynomi $R(0, y)$ saa arvon 0, kun $y = 1, \dots, n$, mutta $R(0, 0) \neq 0$. Siis $R(0, y)$:n aste on $\geq n$. Tästä seuraa, että $R_n(0) \neq 0$. Olkoon sitten $x \in \{1, \dots, n\}$. y :n n :nnen asteen polynomi $R(x, y) = 0$, kun $y = 0, 1, \dots, n$, joten polynomi on identtisesti 0. Siis myös $R_n(x) = 0$, kun $x \in \{1, \dots, n\}$. Koska $R_n(x)$ ei ole nollapolynomi, sen asteen on oltava $\geq n$. Mutta tämä merkitsee, että $R(x, y)$:n ja siis myös $P(x, y)$:n aste kahden muuttujan polynomina on $\geq 2n$.

Nyt todistetun perusteella voidaan osoittaa, että kolmen muuttujan polynomien $P(x, y, z)$, jolle $P(x, y, z) = 0$, kun $(x, y, z) \in S$, mutta $P(0, 0, 0) \neq 0$, aste on $\geq 3n$. Päättely on aivan sama kuin edellä (ja voitaisiin kiteyttää induktioaskeleeksi). Muodostetaan $P(x, y, z)$:n jakojäännös $R(x, y, z)$ modulo $S(z) = z(z-1)\dots(z-n)$. R :n aste z :n suhteen on $\leq n$ ja R saa saman arvon kuin P kaikissa niissä pisteissä (x, y, z) , joissa $x, y, z \in \{0, 1, \dots, n\}$. Jos kirjoitetaan $R(x, y, z) = R_n(x, y)z^n + \dots + R_0(x, y)$, niin $R(0, 0, z)$ ei ole nollapolynomi, mutta kuitenkin polynomi, jolla on ainakin n nollakohtaa; siis $R_n(0, 0) \neq 0$. Jos $(x, y) \neq (0, 0)$, mutta $x, y \in \{0, 1, \dots, n\}$, niin $R(x, y, z)$ on z :n n :nnen asteen polynomi, jolla on $n+1$ nollakohtaa. Se on siis identtisesti nolla, joten

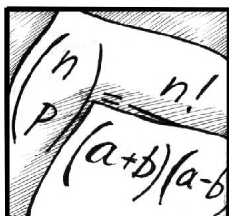
$R_n(x, y) = 0$. Mutta aikaisemmin todistetun perusteella $R_n(x, y)$:n on oltava ainakin astetta $2n$. Siis $R(x, y, z)$ ja myös $P(x, y, z)$ on kolmen muuttujan polynomina ainakin astetta $3n$. Ratkaisu on valmis.

Vastoin ennako-oletuksia tämäkin tehtävä löysi kilpailijoista ratkaisijansa. Heitä oli kaikkiaan 5. Mutta tehtävästä jaettujen pisteiden keskiarvoksi jäi 0,15.

Lopuksi

Kukaan kilpailijoista ei onnistunut ratkaisemaan molempia vaikeita tehtäviä. Siispä täysiin pisteisiin ei yltänyt kukaan. Parhaaseen pistemäärään, 37:ään, ylsi Venäjän **Konstantin Matvejev**. Sääntöjen mukaisesti kultamitalleja sai osapuilleen paras kahdestoistaosa kilpailijoista. Pisterajaksi muodostui 29, ja kultamitalleja jaettiin 39. Hopeamitali annetaan seuraavalle kuu-dennekselle; näitä oli 83 ja pisteraja 21; pronssimitalin saa seuraava neljännes. Pisteraja oli 14 ja kilpailijoita 131.

Seuraavat matematiikkaolympialaiset järjestää Espanja Madridissa heinäkuussa 2008. Sitten ovat järjestyksessä Saksa, Kazakstan ja Hollanti.



Klikkimenetelmä kombinatoristen ongelmien ratkaisemisessa

Mikko Malinen

TkK, opiskelija

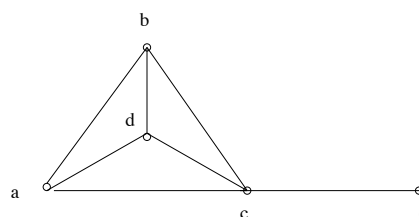
Teknillinen korkeakoulu

Johdanto

Ratkaistaessa tietyn tyyppisiä kombinatorisia yhteensopivuusongelmia tietokoneella voidaan käyttää klikkimenetelmää. Menetelmässä muodostetaan ensin *graafi* ja sitten etsitään siitä tietyn kokoinen *klikki*. Tämän tyyppiset ongelmat voitaisiin periaatteessa ratkaista myös järjestelmällisellä eri tapausten läpikäynnillä (brute force) tai peräytyvällä haulla (backtrack search). Ratkaiseminen näillä on usein käytännössä mahdotonta vaadittavan liian suuren laskenta-ajan takia. Menetelmä soveltuu seuraavanlaisten ongelmien ratkaisuun: Olkoon äärellinen määrä alkioita. Jokainen alkio voi saada arvokseen jonkin arvon annetusta äärellisestä arvojoukosta. Jonkin tai joidenkin alkioiden arvo rajoittaa jonkun toisen tai joidenkin toisten alkioiden mahdollisia arvoja. On löydettävä kaikille alkiolle arvot, jotka ovat yhteensopivia kaikkien muiden alkioiden arvojen kanssa. Voidaan olla myös vähemmän kiinnostuneita alkioiden arvoista, mutta halutaan tietää ratkaisujen kokonaismäärä. Edellisen ongelman esimerkkeinä esitetään erään yksinkertaisen kombinatorisen ongelman ratkaiseminen, Einsteinin ongelman ratkaiseminen sekä sudoku-tehtävän ratkaiseminen. Jälkimmäisen ongelman esimerkkinä esitetään virheenkorjaavien koodien määrän laskeminen.

Hieman graafiteoriaa

Graafi on pari $G = (V, E)$, missä V on solmujen joukko ja E on solmuja yhdistävien kaarien joukko (ks. kuva 1). Yksi kaari yhdistää kaksi solmua toisiinsa.



Kuva 1. Eräs graafi. Solmujen joukko $V = \{a, b, c, d, e\}$. Solmuja yhdistää joukko kaaria.

Klikki on sellainen V :n osajoukko, jossa jokainen solmu on yhdistetty jokaiseen toiseen solmuun kaarella. Kuvan 3 graafin maksimiklikki on $C_1 = \{a, b, c, d\}$. Myös esim. $C_2 = \{b, c, d\}$ on klikki.

Menetelmä

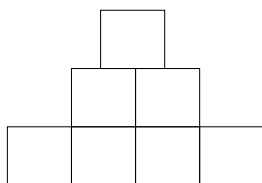
Tarkastellaan graafia, jonka solmuina on ongelman alkioit kaikkine mahdollisista arvoineen. Jos ongelmas-

sa on n alkioita ja kullakin niistä on k mahdollista arvoa, tulee graafiin $n \cdot k$ solmua. Olkoon graafin kahden solmun välillä kaari jos ja vain jos niiden arvot ovat keskenään yhteensopivat. Ratkaisun löytämiseksi eli alkioiden arvojen määräämiseksi graafista etsitään n :n suuruinen klikki. Mikäli halutaan tietää ratkaisujen lukumäärä, etsitään n :n suuruisten klikkien lukumäärä. Algoritmeja klikin etsimiseksi on esitetty [1]:ssä ja [2]:ssa. Yksi mahdollisuus on käyttää valmista aliohjelmatyökalua, jollainen on esimerkiksi [3].

Esimerkkejä

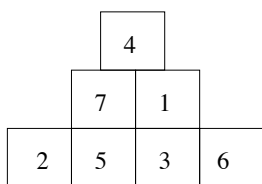
Yksinkertainen tehtävä

Tämä tehtävä on melko helppo ratkaista kynällä ja paperilla, mutta esimerkin yksinkertaisuuden vuoksi esitetään tässä. Tämä on myös esimerkkinä siitä, minkä tyyppisiin tehtäviin menetelmää voidaan käyttää. Tehtävänä on täyttää ruudukkoon numerot 1-7, yksi kutakin, niin, että toisiaan koskettavat ruudut eivät sisällä peräkkäisiä numeroita (ks. kuva 2).



Kuva 2. Täytettävä ruudukko

Graafiin tulee solmuja $n \cdot k = 7 \cdot 7$ kappaletta. Kunkin ruutuun assosioidaan 7 solmua, joihin assosioidaan myös numerot 1-7, yksi kuhunkin. Kahden solmun välille asetetaan kaari jos ja vain jos niitä vastaavat ruudut ja numerot ovat yhteensopivia. Esimerkiksi kahden vierekkäisen ruudun numeroiden ollessa peräkkäiset solmujen välillä ei ole kaarta. Ratkaisu löytyy etsimällä seitsemän kokoinen klikki graafista. Ratkaisujen lukumäärä saadaan laskemalla seitsemän kokoisten klikkien lukumäärä graafissa. Eräs ratkaisu on esitetty kuvassa 3.



Kuva 3. Eräs ratkaisu tehtävään

Sudokutehtävän ratkaiseminen klikkimenetelmällä

Latinalaiset neliöt

Astetta n oleva *latinalainen neliö* on $n \times n$ taulukko, joka koostuu n symbolista niin että jokainen symboli esiintyy tasan kerran jokaisella rivillä ja jokaisessa sarakkeessa (ks. kuva 4). Jatkossa oletetaan, että symbolit ovat $1, 2, \dots, n$.

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Kuva 4. Eräs latinalainen neliö

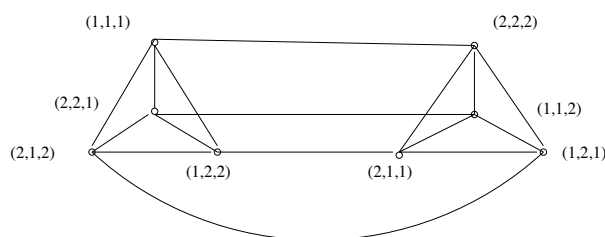
Osittaisessa latinalaisessa neliössä osa alkioista on määrittelemättä. Osittaisen latinalaisen neliön *täydentäminen* on määrittelemättömien alkioiden määrääminen niin, että osittainen neliö täydentyy salitukseksi latinalaiseksi neliöksi.

1	2	3	4	5
2	3	.	.	.
3	.	4	.	.
4	.	.	5	.
5	.	.	.	2

Kuva 5. Eräs osittainen latinalainen neliö

Algoritmi

Graafien kielellä osittaisen latinalaisen neliön täydennys voidaan suorittaa seuraavalla tavalla: Tarastellaan graafin, jonka solmuina on n^3 kpl muotoa (i, j, k) olevaa kolmikkoa; $i, j, k \in \{1, 2, \dots, n\}$. Mitkä tahansa kaksi erillistä kolmikkoa on yhdistetty kaarella jos ja vain jos kolmikot ovat yhtäsuuria korkeintaan yhdessä koordinaateista. Kuvassa 6 on arvolla $n = 2$ syntyvä graafi.



Kuva 6. Graafi arvolla $n = 2$

Intuitio on se, että jokainen kolmikko (i, j, k) kertoo, että annamme arvon k alkiolle rivillä i , sarakkeessa j $n \times n$ taulukossa. Huomaa, että $n:n$ asteen latinalaiset neliöt vastaavat n^2 kokoisia graafin klikkejä. Myöskin, osittainen latinalainen neliö voidaan täydentää jos ja vain jos vastaavat kolmikot ilmenevät kokoa n^2 olevassa klikissä.

Algoritmin muokkaaminen sudokun ratkaisemiseksi tapahtuu niin, että sudokun lisärajoitus, luvut 1-9 laatikossa, huomioidaan siten, että kussakin laatikossa alkioden välillä on kaari jos ja vain jos kyseiset kaksi alkioita eivät ole arvoltaan samat. Ja sudokussahan $n = 9$.

Einsteinin ongelman ratkaiseminen klikkimenetelmällä

Tästä ongelmasta on olemassa erilaisia versioita. Tässä niistä yksi: Pienellä kadulla on viisi eri väristä taloa. Viisi eri kansallisuutta olevaa ihmistä asuu näissä viidessä talossa. Joskaisella asukkaalla on eri ammatti, jokainen pitää eri juomasta ja jokaisella on eri kotieläin. On annettu seuraavat tiedot:

Englantilainen asuu punaisessa talossa.
 Espanjalaisella on koira.
 Japanilainen on maalari.
 Italialainen juo teetä.
 Norjalainen asuu vasemmanpuoleisimmassa talossa.
 Vihreän talon omistaja juo kahvia.
 Vihreä talo on valkoisen talon oikealla puolella.
 Kuvanveistäjä kasvattaa etanoita.
 Diplomaatti asuu keltaisessa talossa.
 Keskimmaisessä talossa joudaan maitoa.
 Norjalainen asuu sinisen talon vieressä.
 Viulunsoittaja juo hedelmämehua.
 Kettu on talossa, joka on lääkärin talon vieressä.
 Hevonen on talossa, joka on diplomaatin talon vieressä.

Kysymys kuuluu, kenellä on seepra ja kuka juo vettä? Tämän ongelman ratkaisemiseksi riittää määrittää jokaiselle talolle sen viisi ominaisuutta:

- väri
- omistajan kansallisuus
- omistajan kotieläin
- omistajan ammatti
- omistajan mieluinen juoma

Taloja on viisi, kullakin talolla on viisi ominaisuutta ja kullakin ominaisuudella on viisi mahdollista arvoa. Muodostetaan graafi, jossa on $5 \cdot 5 \cdot 5 = 125$ solmua. Yhdestä solmusta tiedetään mikä talo on kyseessä, mikä

ominaisuus on kyseessä ja mikä on ominaisuuden arvo. Sitten solmujen välille vedetään kaaria niin, että vain yhteensopivien solmujen välille tulee kaari. Ratkaisu saadaan, kun näin muodostuvasta graafista etsitään 25:n kokoinen klikki. Tämä klikki kertoo, mitkä arvot kunkin talon ominaisuudet saavat. Kerrottakoon, että ratkaisu on: Japanilaisella on seepra ja norjalainen juo vettä.

Koodien lukumäärän laskeminen klikkimenetelmällä

Tässä ongelmassa olemme kiinnostuneita ratkaisujen lukumäärästä. $l:n$ pituinen binäärinen koodisana on $l:n$ pituinen jono nollia ja ykkösiä. 01001 voisi olla viiden pituinen koodisana. $s:n$ kokoinen koodi on $s:n$ kokoinen joukko koodisanoja. Kahden binäärisen koodisanan välinen Hamming-etäisyys on se bittien lukumäärä, jolla koodisanat eroavat toisistaan. Esimerkiksi koodisanojen 01001 ja 01010 Hamming-etäisyys on kaksi, koska ne eroavat toisistaan kahden bitin osalta. Hamming-etäisyydellä on merkitystä virheen havaitsevissa ja -korjaavissa koodeissa. Tässä ongelmassa olemme kiinnostuneita laskemaan l -pituisten, s -kokoisten ja minimi Hamming-etäisyyden h omaavien eri koodien lukumäärän. Graafin solmut muodostetaan kaikista erilaisista l -pituisista bittijonoista. Graafissa on siten $2^l - 1$ solmua. Kahden solmun välille muodostetaan kaari, mikäli niiden Hamming-etäisyys on suurempi tai yhtäsuuri kuin h . Koodien lukumäärä saadaan nyt s -kokoisten klikkien lukumääränä.

Johtopäätökset

Tässä artikkelissa esitettiin, kuinka klikkimenetelmää voidaan käyttää tietäntyyppisten kombinatoristen ongelmien ratkaisujen etsimiseen sekä ratkaisujen lukumäärien laskemiseen. Menetelmää voidaan käyttää usein silloinkin, kun kaikkien vaihtoehtojen läpikäynti tai peräytyvä haku ovat laskenta-ajaltaan liian suuria. Menetelmä edellyttää klikinetsintäalgoritmin käyttöä osana menetelmää.

Viitteet

- [1] P. Kaski ja P.R.J. Östergård, *Classification Algorithms for Codes and Designs*, Springer, Berlin, 2006
- [2] D.L. Kreher ja D.R. Stinson, *Combinatorial algorithms: generation, enumeration and search*, CRC Press, Boca Raton, Florida, 1999
- [3] Ohjelmistotyökalu Cliquer, <http://users.tkk.fi/pat/cliquer.html>

MATEMATIIKAN PÄIVÄT 2008

Teknillinen korkeakoulu 3.1.-4.1.



<http://math.tkk.fi/conferences/matpaivat08/>

Pääesitelmiä pitävät:

Kaisa Nyberg (Teknillinen korkeakoulu)

Paavo Salminen (Åbo Akademi)

Karl Sigmund (University of Vienna, Itävalta)

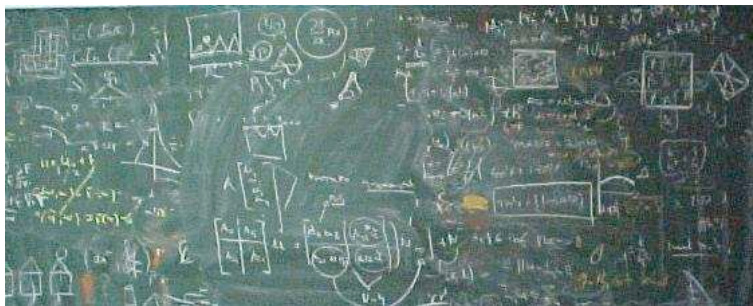
Stanislav Smirnov (Université de Genève, Sveitsi)

Sessiot:

Matematiikan opetuksen sessio

Tietokoneavusteisen opetuksen sessio

Muut sessiot verkkosivulla.



Tervetuloa matematiikan päville!