

JOHDATUS MATEMATIIKKAAN

JOUNI PARKKONEN

0. LUKIJALLE

Tämä on syksyn 2012 Johdatus matematiikkaan -kurssin teksti. Joitain asioita käsiteltiin luennolla enemmän kuin tässä tekstissä, samoin joistain asioista on tässä tekstissä muutama lisähuomio, joita ei käsitelty luennolla. Tämän tekstin lisäksi suosittelen lukemaan Käenmäen tai Juutisen monisteita, joihin on linkki kurssin kotisivulla. Näissä monisteissa käsitellään matemaattisten väitteiden todistustekniikkaa melko perusteellisesti.

1. MATEMAATTISIA VÄITTEITÄ JA TODISTUKSIA

1.1. **Väitteitä.** Seuraavat ovat matemaattisia väitteitä:

- (1) $\sqrt{2}$ on irrationaaliluku.
- (2) $\sqrt{2}$ on rationaaliluku.
- (3) Olkoon $k \geq 3$ luonnollinen luku. Kaikki yhtälön

$$x^k + y^k = z^k$$

kokonaislukuratkaisut (x, y, z) toteuttavat yhtälön $xyz = 0$

- (4) Jokainen yhdesti yhtenäisen suljettu 3-ulotteinen monisto on homeomorfinen 4-ulotteisen euklidisen avaruuden yksikköpallon pinnan kanssa.
- (5) Jokaisen kokonaisluvun neliö on jaollinen luvulla 4 tai neljällä jaettaessa jakojäännös on 1.
- (6) Jokaiselle luonnolliselle luvulle n pätee

$$\sum_{i=0}^n 2^i = 2^{n+1} - 1.$$

Havaintoja: • Vain toinen väitteistä (1) ja (2) voi olla tosi.

• Väite (3) sanoo, että ainakin yksi kokonaisluvuista x, y, z , jotka toteuttavat väitteen yhtälön, on 0. Jäljelle jääviä ratkaisuja, jotka ovat esimerkiksi muotoa $x = 0$ ja $y = z$ sanotaan *triviaaleiksi* eli itsestäänselviksi ratkaisuiksi. Tämä väite on *Fermat'n suuri lause*. Fermat muotoili väitteen 1600-luvulla ja osasi todistaa sen ilmeisesti vain tapauksessa $k = 4$. Euler, Legendre, Dirichlet jne todistivat 1700-1800-lukujen taitteessa tapaukset 3, 5 ja 7 ja joitain erikoistapauksia, ja 1800-luvulla uuden matematiikan alan *algebrallisen lukuteorian* keinoilla saatiin monia alkulukueksponentteja käsiteltyä. Lopullisesti lauseen todisti Wiles noin vuonna 1995 menetelmillä, jotka ovat jo kaukana väitteen muotoilussa esiintyvistä käsitteistä.

• Väite (4) on niin edistynyttä matematiikkaa, että pelkästään sen ymmärtäminen, mitä väitetään, vaatii monien uusien käsitteiden määrittelemistä. Tämä väite on *Poincarén konjektuuri*, jonka Poincaré muotoili 1900-luvun alussa. Väitteen todisti Perelman noin vuonna 2002-2003.

• Nimitys *konjektuuri* tarkoittaa matemaattista väitettä, jonka *uskotaan* olevan tosi. Koska Perelman todisti Poincarén konjektuurin, väitteen nimityksen voisi vaihtaa

esimerkiksi *Perelmanin lauseeksi*. Alkuperäistä nimitystä käytettiin kuitenkin niin kauan, että se säilynee käytössä. Vastaavasti Fermat'n suurta lausetta olisi ollut parempi sanoa konjektuuriksi. . .

- Väitteessä (6) käytetään summamerkintää

$$\sum_{i=0}^n 2^i = 2^0 + 2^1 + \cdots + 2^{n-1} + 2^n$$

parantamassa luettavuutta ja helpottamassa kirjoittamista.

1.2. Todistuksia. Selvitämme luvussa 2, kumpi väitteistä (1) vai (2) on tosi. Väitteet (3) ja (4) ovat aivan liian haastavia käsiteltäväksi tällä tai monella muullakaan kurssilla. Väitteet (5) ja (6) eivät ole kovin vaikeita mutta ne ovat opettavaisia esimerkkejä väitteistä, jotka koskevat kaikkia luonnollisia lukuja samanaikaisesti. Todistamme seuraavaksi nämä väitteet.

Väitteen (5) todistus. Jokainen kokonaisluku n on joko parillinen tai pariton. Jos n on *parillinen*, on kokonaisluku k , jolle $n = 2k$. Tällöin

$$n^2 = (2k)^2 = 4k^2,$$

joten tässä tapauksessa n^2 on jaollinen luvulla 4. Jos n on *pariton*, niin on kokonaisluku k , jolle $n = 2k + 1$. Tällöin

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1,$$

joten luvun n^2 jakojäännös jaettaessa luvulla 4 on 1. □

Mutta miten perustellaan, että kaikki kokonaisluvut ovat parillisia tai parittomia?

On helppo vakuuttaa itsensä siitä, että väite (6) on tosi kokeilemalla muutamalla luvun k arvolla. Tämä ei kuitenkaan todista väitettä kuin niille arvoille, joilla se on testattu. Koska luonnollisia lukuja on äärettömän monta, vaaditaan kehittyneempi todistusmenetelmä, jota kutsutaan *induktiotodistukseksi*. Induktiotodistus perustuu yksinkertaiseen ideaan:

Kun lukuun 0 lisätään 1 tarpeeksi monta kertaa,
päästään mihin tahansa luonnolliseen lukuun.

Todistetaan väite (6) tällä idealla.

Väitteen (6) todistus. Vaihe 1: Havaitaan, että väite on tosi, kun $n = 0$:

$$\sum_{i=0}^0 2^i = 2^0 = 1 = 2^{0+1} - 1.$$

Vaihe 2: Osoitetaan, että siitä, että väite pätee, kun $n = k - 1$ seuraa, että se pätee, kun $n = k$: Oletetaan siis, että

$$\sum_{i=0}^{k-1} 2^i = 2^k - 1.$$

Tätä kutsutaan *induktio-oletukseksi*. Havaitaan, että

$$\sum_{i=0}^k 2^i = \sum_{i=0}^{k-1} 2^i + 2^k,$$

joten induktio-oletuksen nojalla

$$\sum_{i=0}^k 2^i = 2^k - 1 + 2^k = 2 \times 2^k - 1 = 2^{k+1} - 1,$$

kuten haluttiin. $\square$

Se, että induktioperiaate toimii, on luonnollisten lukujen sisäänrakennettu ominaisuus kuten ennen todistusta todettiin. Todistamme sen avulla kurssin aikana useita eri tuloksia ja loppukokeessa on varmasti induktiotodistus.

Lause 1.1. *Kaikille luonnollisille luvuille $n \geq 1$ pätee*

$$(1) \quad 1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

Todistus. Tapaus $n = 1$ on helppo: $1 = \frac{1 \times 2}{2}$. Oletetaan, että kaava (1) pätee, kun $n = k$. Nyt induktio-oletuksen nojalla pätee

$$\begin{aligned} 1 + 2 + \dots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{((k+1)+1)(k+1)}{2}. \end{aligned} \quad \square$$

Induktiotodistuksella voidaan todistaa myös väitteitä, jotka pätevät kaikille kokonaisluvuille, jotka ovat suurempia tai yhtä suuria kuin $N \in \mathbb{Z}$. Tällöin tarkastetaan väite luvulle N ja tehdään induktioaskel kaikille kokonaisluvuille, jotka ovat vähintään N .

2. LUVUISTA

Lukuteoria on klassinen matematiikan ala, jolla on tämän kurssin kannalta ainakin kaksi hyvää ominaisuutta:

- Pienillä lukuteorian tuloksilla on hyvä harjoitella todistamisen alkeita
- Lukuteoriassa on helppo muotoilla haastavia kysymyksiä, joiden ratkaisemiseen on käytetty satoja vuosia ja sellaisiakin, joita ei vielä kukaan osata ratkaista.

2.1. Merkintöjä. *Luonnollisten lukujen joukko on*

$$\mathbb{N} = \{0, 1, 2, \dots\}.$$

Kokonaislukujen joukko on

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Ajattelemme reaalilukujen joukkoa $\mathbb{R}$ havainnollisesti lukusuorana. *Rationaalilukujen joukko on*

$$\mathbb{Q} = \left\{ \frac{p}{q} \in \mathbb{R} : p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

Merkintä $a \in A$ tarkoittaa, että a on joukon A alkio. Jos kaikki joukon C alkioit ovat myös joukon D alkioita, niin C on joukon D osajoukko, tätä merkitään $C \subset D$. Merkintä

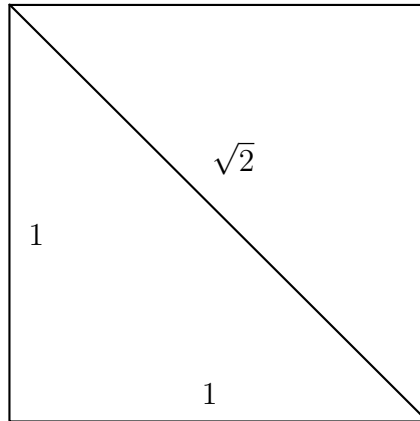
$$B = \{a \in A : \text{alkiolla } a \text{ on ominaisuus } P(a)\}$$

määrittelee joukon A osajoukon. Esimerkiksi rationaalilukujen joukko kuvattiin yllä tällaisella merkinnällä reaalilukujen joukon osajoukkona.

2.2. Rationaali- ja irrationaaliluvuista.

Lause 2.1. $\sqrt{2}$ on irrationaaliluku.

Mitä ylläoleva väite tarkoittaa? Luvun 2 *neliöjuuri* $\sqrt{2}$ on positiivinen reaaliluku, jolle pätee $(\sqrt{2})^2 = 2$. Onko tällainen luku varmasti? Ilmeisesti on, koska *Pythagoraan lauseen* mukaan yksikköneliön halkaisijan pituus on $\sqrt{2}$. Tarkempi perustelu vaatii reaalilukujen olemuksen lähempää pohdiskelua, joka jääköön myöhempiin ajankohtaan.



Todistus. Oletetaan, että $\sqrt{2} = p/q$. Siis $(p/q)^2 = 2$ eli $p^2 = 2q^2$. Tästä voi jatkaa ainakin kahdella tavalla:

(1) Nyt p^2 on parillinen, joten p on parillinen, $p = 2p_1$, $0 < p_1 < p$. Supistetaan ja saadaan yhtälö

$$(2) \quad 2p_1^2 = q^2.$$

Kuten edellä saadaan, että q on parillinen, $q = 2q_1$, jollain kokonaisluvulla q_1 , joka toteuttaa $0 < q_1 < q$. Sijoittamalla $q = 2q_1$ yhtälöön (2) saadaan supistamalla yhtälö $p_1^2 = 2q_1^2$, josta päätellään kuten edellä, että $p_1 = 2p_2$ jollekin luonnolliselle luvulle p_2 . Jatkamalla saadaan aidosti vähenevät jonot luonnollisia lukuja

$$p > p_1 > p_2 > \cdots$$

ja

$$q > q_1 > q_2 > \cdots,$$

mutta tämä on mahdotonta! Siis $\sqrt{2}$ ei ole rationaaliluku.

(2) Oletetaan, että rationaaliluku p/q on supistetussa muodossa, toisin sanoen lukujen p ja q suurin yhteinen tekijä on 1. Kuten edellä saadaan $p^2 = 2q^2$, josta saadaan, että $p = 2p_1$ on parillinen. Supistamalla saadaan $q^2 = 2p_1^2$, joten myös q on parillinen ja lukujen p ja q suurin yhteinen tekijä onkin vähintään 2, mikä on ristiriita sen kanssa, että p/q oli supistetussa muodossa. Siis $\sqrt{2}$ ei ole rationaaliluku. $\square$

Lauseen 2.1 todistus on hyvä esimerkki epäsuorasta todistuksesta: Lauseen 2.1 sisältö voidaan jakaa osiin näin:

Oletus: $x^2 = 2$.

Väite: x ei ole rationaaliluku.

Todistuksessa oletetaan, että väite ei ole voimassa. Käyttämällä tätä *vastaoletusta* eli *antiteesiä* (x on rationaaliluku) ja väitteen oletusta ($x^2 = 2$) osoitetaan, että tästä seuraa jokin ristiriita. Koska ristiriita saadaan aikaan, päätelmä on, että väite on tosi. Tämä johtuu siitä, että reaaliluku $\sqrt{2}$ on joko rationaaliluku tai irrationaaliluku ja olemme pystyneet osoittamaan, että se ei voi olla rationaaliluku. Eri versiot todistuksen loppuosasta johtivat eri ristiriitoihin.

Lauseen 2.1 todistuksessa käytimme päättelyä

$$p^2 \text{ on parillinen, joten } p \text{ on parillinen.}$$

Tämä väite on helppo todistaa: Jos p on pariton, niin sen neliö on pariton, kuten huomasimme Väitteen (5) todistuksessa Luvussa 1.

Huomaa, että väite "Jos p^2 on jaollinen luvulla 4, p on jaollinen luvulla 4" ei ole tosi: Valitaan $p = 2$. Luku 4 jakaa luvun $p^2 = 2^2 = 4$ mutta ei lukua $p = 2$. Tämä johtuu siitä, että 2 on alkuluku ja 4 ei ole. Tarkastelemme tätä aihetta luvussa 2.3.

Yleisemmin pätee tulos, jota emme nyt todista:

Lause 2.2. *Olko $P(x)$ kokonaislukukertoiminen polynomi, jonka korkeimman asteen termin kerroin on 1 ja olko $P(a) = 0$ jollekin reaaliluvulle a . Tällöin a on luonnollinen luku tai irrationaaliluku.*

Seuraus 2.3. *Olko $n, k \in \mathbb{N}$. Tällöin $\sqrt[k]{n}$ on luonnollinen luku tai irrationaaliluku.*

Todistus. Reaaliluku $\sqrt[k]{n}$ on kokonaislukukertoimisen polynomin $P(x) = x^k - n$ nollakohta. Väite seuraa siis Lauseesta 2.2. $\square$

Vetosimme ennen Lauseen 2.1 todistusta Pythagoraan lauseeseen:

Lause 2.4 (Pythagoraan lause). *Euklidisessa tasossa olevan suorakulmaisen kolmion kateettien pituuksien neliöiden summa on sen hypotenuusan pituuden neliö.*

Pythagoraan lauseelle on klassisia geometrisia todistuksia, esimerkiksi seuraava kolmioiden siirtelyyn perustuva todistus:

Todistus. Olko kateettien pituudet a ja b ja hypotenuusan pituus c . Kun $a + b$ -sivuisen neliön kulmiin asetetaan suorakulmaiset kolmiot kuten kuvassa, keskelle jää c -sivuinen neliö. Kun kolmiot siirretään uusiin asemiin, niiden komplementti muodostuu a -sivuisesta ja b -sivuisesta neliöstä. $\square$

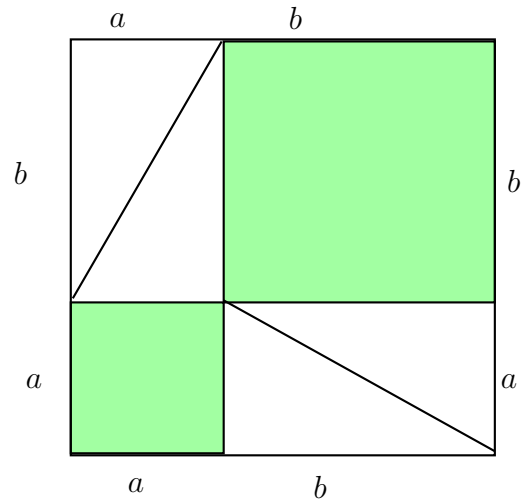
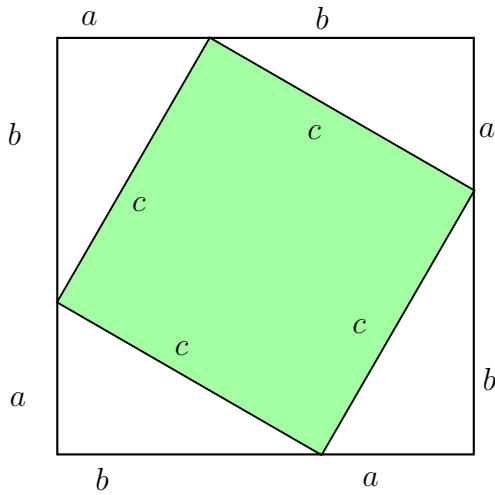
Toisaalta, jos määrittelemme tason pisteiden $a = (a_1, a_2)$ ja $b = (b_1, b_2)$ etäisyydeksi

$$d(a, b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2},$$

niin Pythagoraan lause on selviö, kun tarkastellaan suorakulmaista kolmiota, jonka kärkipisteet ovat $0 = (0, 0)$, $(b, 0)$ ja $(0, a)$.

%Jatkamme vielä irrationaalilukujen parissa. *Kultaisella leikkauksella* tarkoitetaan janan jakamista kahteen osaan siten, että lyhyemmän osan suhde pidempään on sama kuin pidemmän osan suhde koko janan pituuteen. Tätä suhdetta ϕ (ja usein myös sen käänteislukua $\Phi = \frac{1}{\phi}$) kutsutaan *kultaisen leikkauksen luvuksi*. Jos lähdetään yksikköjanasta, joka jaetaan kahteen osaan pisteellä $x > \frac{1}{2}$, kultaisen leikkauksen luku ϕ on yhtälön $\frac{x}{1} = \frac{1-x}{x}$ ratkaisu. Tämä yhtälö on yhtäpitävä toisen asteen polynomiyhtälön

$$(3) \quad x^2 + x - 1 = 0$$



kanssa. Erityisesti siis pätee $\phi(\phi + 1) = 1$ eli

$$\Phi = \frac{1}{\phi} = \phi + 1.$$

Todistamme kultaisen leikkauksen luvun irrationaalisuuden geometrisella argumentilla.

Lause 2.5. *Kultaisen leikkauksen luku ϕ on irrationaaliluku.*

Todistus. Olkoon S_0 suorakulmio, jonka sivut ovat kultaisen leikkauksen suhteessa, *kultainen suorakulmio*. Jaetaan suorakulmion S_0 pitkä sivu kultaisen leikkauksen suhteessa niin, että muodostuu neliö ja suorakulmio S_1 . Kultaisen leikkauksen määritelmän nojalla suorakulmion S_1 sivut ovat kultaisen leikkauksen suhteessa. Toistetaan prosessi suorakulmiolle S_1 ja saadaan pienempi kultainen suorakulmio S_2 . Tätä prosessia voi jatkaa loppumattomiin ja saadaan sisäkkäisten kultaisen suorakulmioiden jono.

Oletetaan, että $\phi = \frac{p}{q}$ on rationaaliluku, $0 < p < q$. Tällöin suorakulmio S_0 , jonka sivujen pituudet ovat p ja q on kultainen suorakulmio. Yllä kuvatun prosessin suorakulmion S_1 sivujen pituudet ovat p ja $0 < q - p < q$, $q - p \in \mathbb{N}$, seuraavan suorakulmion S_2 sivujen pituudet ovat $q - p$ ja $0 < 2p - q < p$, $2p - q \in \mathbb{N}$. Näin saadaan ääretön jono sisäkkäisiä aidosti pieneneviä suorakulmioita, joiden sivujen pituudet ovat luonnollisia lukuja. Tämä ei ole mahdollista, joten ϕ on irrationaaliluku. $\square$

Tunnetusti yhtälön (3) ratkaisut ovat $\frac{-1+\sqrt{5}}{2}$ ja $\frac{-1-\sqrt{5}}{2}$, joista vain ensimmäinen on positiivinen, joten

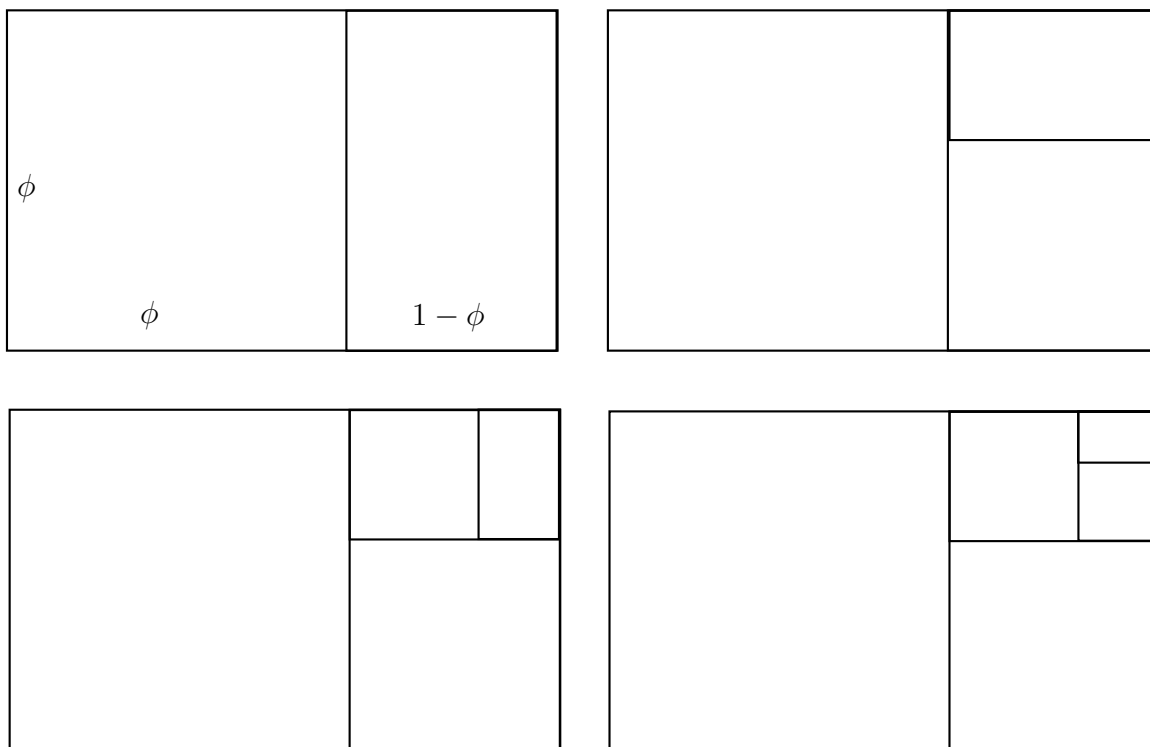
$$\phi = \frac{\sqrt{5} - 1}{2} \approx 0.61803.$$

Ensimmäisissä harjoituksissa osoitetaan toisella tavalla kuin yllä, että ϕ on irrationaaliluku lähtemällä tästä esitysmuodosta.

2.3. Alkuluvuista ja jaollisuudesta.

Määritelmä 2.6. Luonnollinen luku $d \geq 1$ on luonnollisen luvun q *tekijä*, jos on luonnollinen luku q_1 , jolle $q = dq_1$. Luonnollinen luku $p \geq 2$ on *alkuluku*, jos sen ainoat tekijät ovat 1 ja p .

Lause 2.7. *Jokainen luonnollinen luku, joka on vähintään 2 voidaan esittää alkulukujen tulona.*



Todistus. Teemme induktiotodistuksen, joka alkaa luvusta 2. Todistamme induktiolla väitteen

Jokaiselle $N \in \mathbb{N}$, $N \geq 2$ pätee, että
kaikki luonnolliset luvut $2 \leq n \leq N$ voidaan esittää alkulukujen tulona.

(Lauseen väite seuraa tästä väitteestä, joka muotoillaan tällä tavalla teknisestä syystä, joka selviää todistuksen edetessä.) Luku 2 on alkuluku, joten väite pätee sille.

Tehdään induktio-oletus: Oletetaan, että väite pätee luvulle k . Osoitetaan, että väite pätee luvulle $k+1$. Induktio-oletuksen nojalla riittää tarkastaa, että luku $k+1$ voidaan esittää alkulukujen tulona. Tarkastelu jakautuu kahteen tapaukseen:

- (1) Jos $k+1$ on alkuluku, niin väite pätee.
- (2) Jos $k+1$ ei ole alkuluku, niin sillä on jokin tekijä d , jolle pätee $2 \leq d \leq k$. Siis $k+1 = de$ jollekin e , jolle myös pätee $2 \leq d, e \leq k$. Induktio-oletuksen nojalla luvut d ja e voidaan esittää alkulukujen tulona. Kertomalla nämä tulot keskenään saadaan luvun $k+1$ esitys alkulukujen tulona.

Koska väite pätee molemmissa tapauksissa, todistus on valmis. $\square$

Lause 2.8. *Alkulukuja on äärettömän monta.*

Todistus. Oletetaan, että alkulukujen joukko on äärellinen. Olkoot siis $p_1, p_2, \dots, p_N$ kaikki alkuluvut. Luvulla

$$(4) \quad p_1 p_2 \cdots p_N + 1$$

on esitys alkulukujen tulona. Kuitenkaan mikään luvuista $p_1, p_2, \dots, p_N$ ei ole luvun $p_1 p_2 \cdots p_N + 1$ tekijä, joten kaikki alkuluvut eivät ole luettelossa $p_1, p_2, \dots, p_N + 1$. $\square$

Lauseen 2.8 todistuksessa käytettävä luku $p_1 p_2 \cdots p_N + 1$ ei aina ole itse alkuluku vaikka siltä voisi ensin vaikuttaa: Luvut $2+1 = 3$, $2 \times 3 + 1 = 7$, $2 \times 3 \times 5 \times 7 + 1 = 211$, $2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$ ovat alkulukuja mutta $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$. Vastaavanlaisen esimerkin löytää nopeasti aloittamalla luvusta 2 kuten yllä

ja lisäämällä kokoelmaan aina uuden alkuluvun, kun sellainen löydetään lausekkeella (4): $2 \times 3 \times 7 + 1 = 43$ on alkuluku mutta $2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139$.

Seuraava tulos kertoo, että Lauseen 2.1 todistuksessa käytetty päättely n^2 on parillinen, joten n on parillinen yleistyy, kun tarkastellaan jaollisuutta alkuluvuilla:

Lause 2.9 (Eukleideen lemma). *Olko p alkuluku ja olkoot a ja b luonnollisia lukuja. Jos p on luvun ab tekijä, niin se on luvun a tai b tekijä.*

Emme todista tätä tulosta, joka käsitellään lukuteorian ensimmäisellä kurssilla. Jos p on alkuluku ja p on luvun n^2 tekijä, niin Eukleideen lemmän mukaan p on luvun n tekijä.

Eukleideen lemmän avulla voidaan täydentää Lausetta 2.7 ja todistaa, että jokainen luku voidaan esittää alkulukujen tulona täsmälleen yhdellä tavalla.

2.4. Frobeniuksen luvut. Harjoituksissa käsiteltiin seuraavaa "sovelletun matematiikan kysymystä": Suuri ravintolaketju alkoi 1980-luvulla myydä uppopaistettuja kananpaloja kuuden, yhdeksän ja 20 palan annoksina. Tällöin 43 on suurin määrä kananpaloja, jota ei voi tilata. Myöhemmin valikoimaan lisättiin neljän kananpalan annos. Jos sallitaan tämän annoskoon käyttö, niin suurin määrä, jota ei voi tilata on 11 kananpalaa.

Lukuja, jotka voidaan muodostaa lukujen 6, 9 ja 20 positiivisten monikertojen summina kutsutaan tämän vuoksi "Chicken McNugget-luvuiksi". Tämä on esimerkiksi yleisemmästä kysymyksestä, jota Frobenius käsiteli luennoissaan 1800-luvun lopulla:

Lause 2.10 (Schur 1935). *Olkoot $2 \leq a_1 < a_2 < \dots < a_k$ kokonaislukuja, joiden suurin yhteinen tekijä on 1. Jokainen kokonaisluku, joka on suurempi kuin*

$$G(a_1, a_2, \dots, a_k) = (a_1 - 1)(a_k - 1) - 1$$

voidaan esittää summana

$$c_1 a_1 + c_2 a_2 + \dots + c_k a_k,$$

missä $c_1, \dots, c_k \in \mathbb{N}$.

Suurin luku, jota ei voi esittää summana $c_1 a_1 + c_2 a_2 + \dots + c_k a_k$ on *Frobeniuksen luku*. Lauseessa 2.10 annettu luku $G(a_1, a_2, \dots, a_k)$ on siis yläraja lukujen $a_1, a_2, \dots, a_k$ Frobeniuksen luvulle. Sylvester osoitti, että $G(a_1, a_2)$ on lukujen a_1 ja a_2 Frobeniuksen luku. Yleisessä tapauksessa Frobeniuksen luvulle ei tunneta vastaavanlaista kaavaa. Lauseen 2.10 mukaan kaikki lukua $G(6, 9, 20) = 94$ suuremmat luvut ovat Chicken McNugget -lukuja. Harjoituksissa saimme siis tarkemman tuloksen tässä erikoistapauksessa.

3. LUKUJONOJA

Fibonaccin jono $(F_k)_{k=1}^{\infty}$ määritellään seuraavasti: Asetetaan $F_0 = F_1 = 1$ ja määritellään rekursiivisesti $F_k = F_{k-1} + F_{k-2}$ kaikille $k \geq 2$. Fibonaccin jono on siis

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...	30	...
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	...	832040	...

Kahden peräkkäisen Fibonaccin luvun suhde käyttäytyy mielenkiintoisella tavalla: Viiden desimaalin tarkkuudella

$\frac{n}{F_n}$	2	3	4	5	6	7	8	9
$\frac{F_n}{F_{n-1}}$	1	3	3/2	5/3	8/5	1.625	1.615384	1.6190
$\frac{n}{F_{n-1}}$	10	11	12	13	14	15	30	...
$\frac{F_n}{F_{n-1}}$	1.6176	1.61818	1.61797	1.61805	1.61802	1.61803	1.61803	...

Vaikuttaa siltä, että suhteen $\frac{F_n}{F_{n-1}}$ arvot lähenevät jotain lukua, joka on noin 1.61803, joka muuten on kultaisen leikkauksen luvun ϕ käänteisluvun likiarvo $\Phi = \frac{1}{\phi} = \frac{1+\sqrt{5}}{2}$ viiden desimaalin tarkkuudella.

Miten määrittelimme täsmällisesti sen, että jonkin lukujonon luvut lähestyvät jotain reaalityötä ja miten selvitetään, lähestyykö jono $(F_n/F_{n-1})_{n=1}^\infty$ tässä mielessä kultaisen leikkauksen lukua Φ ?

Muistamme, että reaalityön x itseisarvo $|x|$ on x , jos x on positiivinen ja $-x$ muulloin. Havainnollisesti

$$|a - b| \text{ on reaalityön } a \text{ ja } b \text{ etäisyys.}$$

Lukujonolla tarkoitetaan luonnollisilla luvuilla tai positiivisilla kokonaisluvuilla numeroitua eli *indeksoitua* jonoa $a_1, a_2, \dots$ reaalityöjä. Luku $a \in \mathbb{R}$ on lukujonon $(a_k)_{k=1}^\infty$ *raja-arvo*, jos kaikilla positiivisilla reaalityöillä $\epsilon > 0$ on jokin indeksi $N = N(\epsilon)$ siten, että kaikille $i \geq N$ pätee $|a - a_i| < \epsilon$. Luku $a \in \mathbb{R}$ on siis jonon $(a_k)_{k=1}^\infty$ *raja-arvo*, jos voidaan valita mikä tahansa tarkkuus ja riittävän suurilla indekseillä jonon kaikki luvut ovat lähempänä lukua a kuin tuo valittu tarkkuus. Määritelmä kirjoitetaan matemaattisesti täsmällisessä melko tiiviissä muodossa näin

Määritelmä 3.1. Reaalityö a on lukujonon $(a_k)_{k=1}^\infty$ *raja-arvo*, jos kaikilla $\epsilon > 0$ on $N \in \mathbb{N}$ siten, että kaikille $k \geq N$ pätee $|a - a_k| < \epsilon$. Sanotaan, että jono $(a_k)_{k=1}^\infty$ *suppenee* kohti raja-arvoa a .

Tarkastellaan muutamaa esimerkkiä:

Esimerkki 3.2. Jonon $(\frac{1}{k})_{k=1}^\infty$ *raja-arvo* on 0.

Todistus. Olkoon $\epsilon > 0$. Tällöin $\frac{1}{\epsilon}$ on positiivinen. Valitaan luvuksi N pienin kokonaisluku, joka on suurempi kuin $\frac{1}{\epsilon}$. Tällöin $k > \frac{1}{\epsilon}$ kaikilla $k \geq N$, joten $\frac{1}{k} < \epsilon$ kaikilla $k \geq N$. Koska $\frac{1}{k} > 0$ kaikilla $k \geq 1$, saadaan siis

$$|0 - \frac{1}{k}| = \frac{1}{k} < \epsilon$$

kaikilla $k \geq N$. □

Seuraavassa esimerkissä tarvitsemme kolmioepäyhtälöä, joka on tärkeä työväline muunmuassa analyysin kursseilla.

Lause 3.3 (Kolmioepäyhtälö). *Kaikille $x, y \in \mathbb{R}$ pätee*

$$|x + y| \leq |x| + |y|.$$

Todistus. Katso Juutisen moniste Lause 3.3.2. tai Käenmäen moniste Lause 8.5. □

Seuraus 3.4. *Kaikille $x, y, z \in \mathbb{R}$ pätee*

$$|x + y| \leq |x - z| + |z - y|.$$

Todistus. Katso Juutisen moniste Lause 3.3.4. □

Toinen hyödyllinen epäyhtälö, jota emme nyt tarvitse, tunnetaan myös nimellä Kolmioepäyhtälön toinen puoli.

Lause 3.5 (Käänteinen kolmioepäyhtälö). *Kaikille $x, y \in \mathbb{R}$ pätee*

$$||x| - |y|| \leq |x + y|.$$

Todistus. Katso Käenmäen moniste Lause 8.8. □

Esimerkki 3.6. Jonolla $((-1)^k)_{k=1}^\infty$ ei ole raja-arvoa.

Todistus. Jos jonolla olisi raja-arvo, kutsutaan tätä kuvitteellista lukua nimellä a , niin kaikilla $\epsilon > 0$ olisi jokin indeksi N , josta eteenpäin kaikki jonon luvut ovat korkeintaan etäisyydellä ϵ raja-arvosta. Valitaan $\epsilon = \frac{1}{2}$. Koska suurillakin indekseillä jonon luvut ovat vuorotellen -1 ja 1 , saadaan kolmioepäyhtälön nojalla

$$2 = |1 - (-1)| = |(1 - a) + (a - (-1))| \leq |1 - a| + |a - (-1)| < \frac{1}{2} + \frac{1}{2} = 1,$$

mikä on mahdotonta. Siis mikään reaaliluku ei ole jonon $((-1)^k)_{k=1}^\infty$ raja-arvo. □

Määritelmä 3.7. Lukujonon $(a_k)_{k=1}^\infty$ raja-arvo on ∞ , jos kaikilla $M > 0$ on $N \geq 0$ siten, että $a_k > M$, kun $k \geq N$. Tällöin sanotaan, että jono $(a_k)_{k=1}^\infty$ *kasvaa rajatta*.

Esimerkki 3.8. Jono $(a_k)_{k=1}^\infty$, jossa $a_k = k$ kasvaa rajatta. Jos jono $(a_k)_{k=1}^\infty$ *kasvaa rajatta*, niin jonon $(\frac{1}{a_k})_{k=1}^\infty$ raja-arvo on 0 . Tämä todistetaan kuten Esimerkki 3.2.

Esimerkki 3.9. Luvun 3 alussa kuvattujen laskelmien mukaan näyttäisi siltä, että ainakin tarkkuudella $\epsilon = 10^{-5}$ kaikki jonon $(F_n/F_{n-1})_{n=2}^\infty$ luvut indeksistä $n = 15$ tai ainakin indeksistä $n = 30$ toteuttavat $|F_n/F_{n-1} - 1.61803| < 10^{-5}$. Nämä laskut eivät todista mitään mutta ne antavat syytä epäillä, että jonon raja-arvo voisi olla lähellä lukua Φ , joka myös toteuttaa $|\Phi - 1.61803| < 10^{-5}$. Osoitamme seuraavaksi, että Φ on jonon $(F_n/F_{n-1})_{n=2}^\infty$ raja-arvo.

Luku Φ toteuttaa yhtälön

$$(5) \quad x^2 - x - 1 = 0,$$

kuten on helppo nähdä muokkaamalla kultaisen leikkauksen määrittelevää yhtälöä. Tämän yhtälön toinen ratkaisu on $\frac{1-\sqrt{5}}{2} = -\phi$. Yhtälöstä (5) seuraa, että luvut Φ^n ja $(-\phi)^n$ toteuttavat samanlaisen rekursion kuin Fibonaccin luvut: Kaikille $n \geq 3$ pätee

$$\Phi^n = \Phi^{n-1} + \Phi^{n-2}$$

ja

$$(-\phi)^n = (-\phi)^{n-1} + (-\phi)^{n-2}.$$

Yhtälöstä (5) seuraa, että $\Phi^2 = \Phi + 1$ ja $(-\phi)^2 = -\phi + 1$, joten

$$\Phi^2 - (-\phi)^2 = \Phi + \phi = \sqrt{5}.$$

Tästä intoutuneena määrittelemme lukujonon $(H_n)_{n=1}^\infty$ asettamalla

$$H_n = \frac{\Phi^n - (-\phi)^n}{\sqrt{5}}.$$

Lukujonon $(H_n)_{n=1}^\infty$ kaksi ensimmäistä lukua ovat $H_1 = H_2 = 1$ ja jono toteuttaa saman rekursion kuin Fibonaccin jono

$$(6) \quad H_n = H_{n-1} + H_{n-2}$$

kaikille $n \geq 3$. Saadaan

Lause 3.10 (Binet'n kaava). *Kaikille luonnollisille luvuille $n \geq 1$ pätee*

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$

Todistus. Tarkastimme edellä, että Binet'n kaava pätee, kun $n = 1$ tai $n = 2$. Tehdään induktio-oletus, että Binet'n kaava pätee kaikille $n \leq k$. Osoitetaan, että tästä seuraa, että se pätee myös kaikille $n \leq k + 1$.

Induktio-oletuksen nojalla riittää tarkastella tapaus $n = k + 1$. Tällöin rekursiivisen määritelmän mukaan $F_{k+1} = F_k + F_{k-1}$. Induktio-oletuksen mukaan Binet'n kaava pätee indekseille k ja $k - 1$, joten

$$F_{k+1} = F_k + F_{k-1} = H_k + H_{k-1}.$$

Kaavan (6) nojalla siis $F_{k+1} = H_{k+1}$ ja Binet'n kaava pätee myös indeksillä $k + 1$. Induktioperiaatteen nojalla Binet'n kaava pätee kaikille $n \geq 1$. $\square$

Binet'n kaavan etu on siinä, että se ei ole rekursio vaan Fibonaccin jonon termit saadaan kahden luvun potenssien erotuksina. Binet'n kaavan mukaan

$$\begin{aligned} \frac{F_n}{F_{n-1}} &= \frac{\frac{1}{\sqrt{5}}(\Phi^n - (-\phi)^n)}{\frac{1}{\sqrt{5}}(\Phi^{n-1} - (-\phi)^{n-1})} \\ &= \frac{\Phi(\Phi^{n-1} - (-\phi)^{n-1}) + \Phi(-\phi)^{n-1} - (-\phi)^n}{\Phi^{n-1} - (-\phi)^{n-1}} \\ &= \Phi + (-\phi)^{n-1} \frac{\Phi + \phi}{\Phi^{n-1} - (-\phi)^{n-1}}. \end{aligned}$$

Koska $|\phi| < 1$ ja $\Phi > 1$, nähdään, että $(-\phi)^{n-1} \frac{\Phi + \phi}{\Phi^{n-1} - (-\phi)^{n-1}}$ suppenee kohti nollaa, kun n kasvaa rajatta. Peräkkäisten Fibonaccin jonon termien suhteet suppenevat siis kohti lukua Φ . Täsmällisempi perustelu tälle viimeiselle päättelylle tehdään kurssilla Analyysi 1.

4. JOUKOISTA JA KUVAUKSISTA

4.1. Perusasioita joukoista ja kuvauksista. Olkoot A ja B joukon X osajoukkoja. Voimme muodostaa uusia joukkoja: Joukkojen A ja B *leikkaus* on

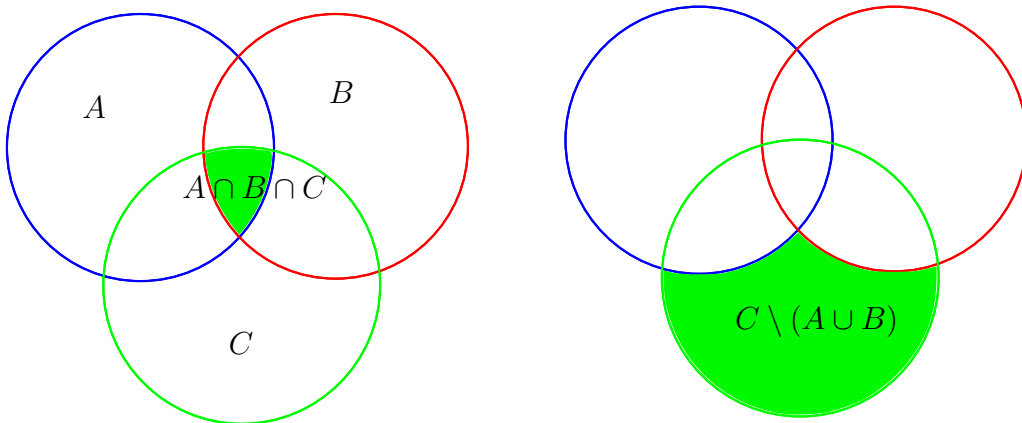
$$A \cap B = \{a \in X : a \in A \text{ ja } a \in B\}$$

ja niiden *yhdiste* on

$$A \cup B = \{a \in X : a \in A \text{ tai } a \in B\}.$$

Joukkojen A ja B *erotus* on

$$A \setminus B = \{a \in X : a \in A \text{ ja } a \notin B\}.$$



Joukko, jolla ei ole yhtään alkioita on *tyhjä joukko* $\emptyset$. Huomaa, että tyhjä joukko on jokaisen joukon osajoukko!

Propositio 4.1. Joukolla $\{1, 2, \dots, n\}$ on 2^n osajoukkoa.

Todistus. Todistetaan väite induktiolla: Joukolla $\{1\}$ on kaksi osajoukkoa $\emptyset$ ja $\{1\}$. Oletetaan, että joukolla $\{1, 2, \dots, k\}$ on 2^k osajoukkoa. Lasketaan sitten joukon $\{1, 2, \dots, k+1\}$ osajoukot: Joukot, joihin $k+1$ ei kuulu ovat joukon $\{1, 2, \dots, k\}$ osajoukkoja. Tällaisia joukkoja on induktio-oletuksen nojalla 2^k . Joukot, joihin $k+1$ kuuluu ovat muotoa $\{k+1\} \cup B$, missä $B \subset \{1, 2, \dots, k\}$. Myös tällaisia joukkoja on induktio-oletuksen nojalla 2^k . Kaikki tapaukset on käsitelty, joten joukolla $\{1, 2, \dots, k+1\}$ on $2^k + 2^k = 2 \times 2^k = 2^{k+1}$ osajoukkoa. Induktioperiaatteen nojalla väite pätee. $\square$

On selvää, että positiivisten kokonaislukujen joukolla on äärettömän monta osajoukkoa. Mutta voimmeko sanoa jotain tarkempaa? Onko niitä yhtä paljon kuin positiivisia kokonaislukuja vai jopa enemmän? Palaamme kysymykseen Lauseessa 4.9

Joukkojen A ja B *karteeminen tulo* on

$$A \times B = \{(a, b) : a \in A \text{ ja } b \in B\}.$$

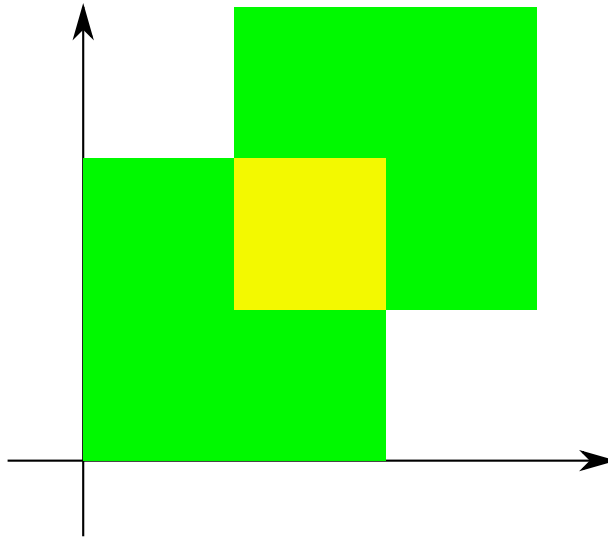
Tässä (a, b) on *järjestetty pari*. Järjestetyille pareille pätee $(a, b) = (c, d)$, jos $a = c$ ja $b = d$. Vastaavasti kaikille $n \in \mathbb{N}$, $n \geq 2$ määritellään järjestetyt n alkion äärelliset jonot eli *n -iköt* $(a_1, a_2, \dots, a_n)$, $a_i \in A_i$ kaikilla $i \in \{1, 2, \dots, n\}$ ja joukkojen $A_1, A_2, \dots, A_n$ karteeminen tulo

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_i \in A_i \text{ kaikilla } i \in \{1, 2, \dots, n\}\}.$$

Jos $A_1 = A_2 = \dots = A_n = A$, käytetään merkintää

$$A^n = A \times A \times \dots \times A = \{(a_1, a_2, \dots, a_n) : a_i \in A \text{ kaikilla } i \in \{1, 2, \dots, n\}\}.$$

Tuttuja esimerkkejä karteesisista tuloista ovat taso $\mathbb{R}^2$ ja yksikkökuutio $[0, 1]^3 \subset \mathbb{R}^3$.



KUVA 1. Joukot $[0, 2]^2 \cap [1, 3]^2$ ja $[0, 2]^2 \cup [1, 3]^2$

Leikkauksen ja yhdisteen käsitteet voidaan yleistää useamman kuin kahden joukon tapaukseen: Jos $A_1, A_2, \dots$ ovat joukon X osajoukkoja, niiden *leikkaus* on

$$\bigcap_{i=1}^{\infty} A_i = \{x \in X : x \in A_i \text{ jokaisella } i \in \{1, 2, \dots\}\}$$

ja niiden *yhdiste* on

$$\bigcup_{i=1}^{\infty} A_i = \{x \in X : x \in A_i \text{ jollakin } i \in \{1, 2, \dots\}\}.$$

Itse asiassa voidaan yleistää vielä pidemmällekin: Olkoon I jokin epätyhjä joukko ja olkoot A_i joukon X osajoukkoja kaikille $i \in I$. Tämän kokoelman $(A_i)_{i \in I}$ *leikkaus* on

$$\bigcap_{i \in I} A_i = \{x \in X : x \in A_i \text{ jokaisella } i \in I\}$$

ja sen *yhdiste* on

$$\bigcup_{i \in I} A_i = \{x \in X : x \in A_i \text{ jollakin } i \in I\}.$$

Jos $A, B \neq \emptyset$, niin *kuvaus* eli *funktio* $f: A \rightarrow B$ on sääntö, joka liittää jokaiseen joukon A alkioon a yhden alkion $f(a) \in B$.

Esimerkki 4.2. (1) Tuttuja esimerkkejä funktioista ovat polynomifunktiot $P: \mathbb{R} \rightarrow \mathbb{R}$,

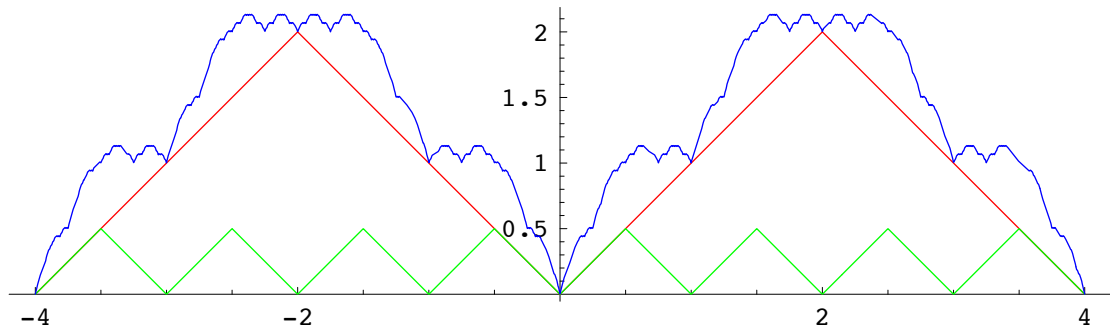
$$P(x) = \sum_{k=0}^N ax^k.$$

(2) Joukon A osajoukon B *karakteristinen funktio* on $\chi_B: A \rightarrow \mathbb{R}$, joka määritellään asettamalla

$$\chi(a) = \begin{cases} 1, & \text{jos } a \in B, \\ 0, & \text{jos } a \notin B \end{cases}$$

(3) Lukujono $(a_k)_{k=0}^{\infty}$ on funktio $a: \mathbb{N} \rightarrow \mathbb{R}$, $a(k) = a_k$.

(4) Monilla funktioilla on yllättäviä ominaisuuksia. Kurssin Analyysi 3 menetelmillä saadaan aikaan jatkuvia funktioita, jotka eivät ole derivoituvia missään. Jatkuvuuden ja derivoituvuuden määritelmät tulevat kursseilla Analyysi 1 ja 2.



KUVA 2. Sininen käyrä on Takagin funktion kuvaaja. Tämä on esimerkki funktioista, joka on jatkuva mutta ei ole derivoituva missään.

Määritelmä 4.3. Olkoon $f: A \rightarrow B$ kuvaus. Joukon $D \subset A$ *kuva* kuvauksessa f on

$$f(D) = \{f(d) : d \in D\}.$$

Kuvauksen f *kuvajoukko* on $f(A)$. Joukon $C \subset B$ *alkukuva* kuvauksessa $f: A \rightarrow B$ on

$$f^{-1}(C) = \{a \in A : f(a) \in C\}.$$

Kuvauksia luokitellaan niiden perusominaisuuksien mukaan seuraavasti:

Määritelmä 4.4. Kuvaus $f: A \rightarrow B$ on

- *surjektio*, jos $f(A) = B$.
- *injektio*, jos $f(x) \neq f(y)$ aina, jos $x \neq y$.
- *bijektio*, jos se on surjektio ja injektio.

Esimerkki 4.5. Tarkastellaan funktiota $F: \mathbb{R} \rightarrow \mathbb{R}$, joka määritellään asettamalla $F(x) = |x|$ kaikille $x \in \mathbb{R}$. Nyt

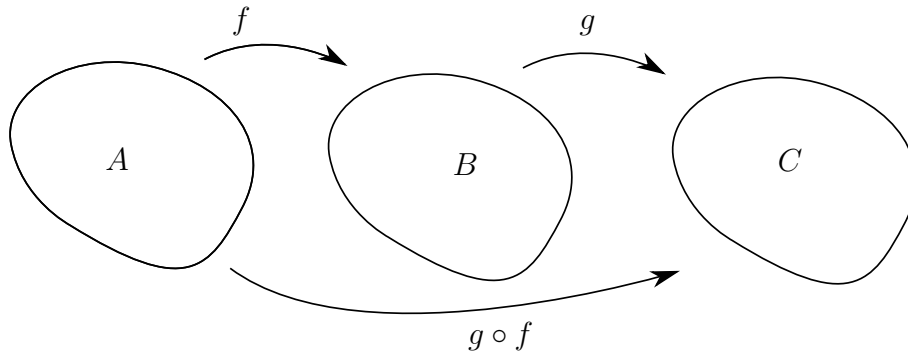
$$F(\mathbb{R}) = \{|x| : x \in \mathbb{R}\} = [0, \infty[,$$

koska kaikki funktion F arvot ovat joukossa $[0, \infty[$ ja jokaiselle $y \in [0, \infty[$ pätee $f(y) = y$. Funktio F

- ei ole surjektio koska mitään negatiivista arvoa ei saavuteta.
- ei ole injektio koska esimerkiksi $f(-1) = f(1) = 1$.

Funktion $g: A \rightarrow B$ rajoittuma joukkoon $C \subset A$ on funktio $g|_C: C \rightarrow B$, joka määritellään asettamalla $g|_C(x) = g(x)$ kaikille $x \in C$. Selvästi funktion F rajoittuma joukkoon $[0, \infty[$ on injektio mutta ei surjektio. Sen sijaan samalla lausekkeella määritelty funktio $F^*: [0, \infty[\rightarrow [0, \infty[$, $F^*(x) = |x| = x$ on bijektio.

Kuvausten $f: A \rightarrow B$ ja $g: B \rightarrow C$ yhdistetty kuvaus on $g \circ f: A \rightarrow C$, joka määritellään asettamalla $g \circ f(a) = g(f(a))$.



Jos $f: A \rightarrow A$ on kuvaus joukolta A itselleen, voidaan muodostaa sen iteroidut yhdistetyt kuvaukset $f^2 = f \circ f$ ja $f^k = f \circ f^{k-1}$ kaikille $k \geq 3$.

Esimerkki 4.6. Olkoon $T_3: \mathbb{R} \rightarrow \mathbb{R}$,

$$T_3(x) = \begin{cases} 3x, & \text{kun } x \leq \frac{1}{2} \\ 3 - 3x, & \text{kun } x > \frac{1}{2}. \end{cases}$$

Funktio T_3 ei ole surjektio koska $T_3(\mathbb{R}) =]-\infty, \frac{3}{2}] \neq \mathbb{R}$. Se ei ole injektio koska $T_3(0) = T_3(1) = 0$.

Miten jono $(T_3^k(x))_{k=1}^\infty$ käyttäytyy muuttujan x eri arvoilla?

- Jos $x < 0$, niin $T_3^k(x) = 3^k x$, ja tällaisen jonon raja-arvo on selvästi $-\infty$.
- Jos $x > 1$, niin $T_3(x) < 0$, joten näilläkin alkuarvoilla jonon raja-arvo on $-\infty$.
- Jos $x \in]\frac{1}{3}, \frac{2}{3}[$, niin $T_3(x) > 1$, joten näilläkin alkuarvoilla jonon raja-arvo on $-\infty$.
- Jos $x \in]\frac{1}{9}, \frac{2}{9}[\cup]\frac{7}{9}, \frac{8}{9}[$, niin $T_3(x) \in]\frac{1}{3}, \frac{2}{3}[$, joten $T_3^2(x) > 1$. Siis näilläkin alkuarvoilla jonon raja-arvo on $-\infty \dots$

Kuitenkin joillakin alkuarvoilla käyttäytyminen on täysin erilaista:

- $T_3(0) = 0$, joten $(T_3)^k(0) = 0$ kaikilla $k \in \mathbb{N} \setminus \{0\}$. Lisäksi $(T_3)^m(\frac{1}{3^m}) = 1$ kaikilla $m \in \mathbb{N}$. Siis $(T_3)^M(\frac{1}{3^m}) = 0$ kaikilla $M \geq m$, joten jonon $(T_3^k(\frac{1}{3^m}))_{k=1}^\infty$

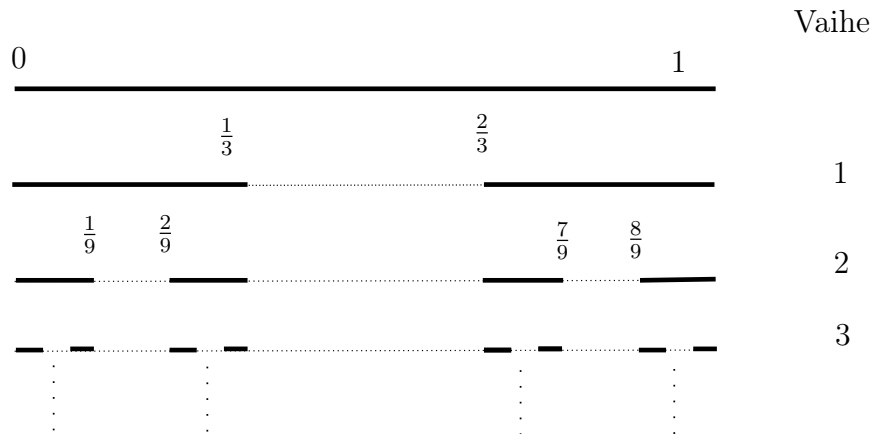
raja-arvo on 0 kaikilla $m \in \mathbb{N}$. Tämä johtuu siitä, että nämä jonot ovat vakiojonoja suurilla indekseillä k .

- $T_3(\frac{3}{4}) = \frac{3}{4}$, $T_3(\frac{1}{4}) = \frac{3}{4}$, $T_3(\frac{1}{12}) = \frac{1}{4}$ ja niin edelleen.

Cantorin joukko

$$C = \bigcap_{k=1}^{\infty} (T_3^k)^{-1}([0, 1]) = \{x \in \mathbb{R} : T_3^k(x) \in [0, 1]\}$$

koostuu niistä pisteistä, joita vastaavat jonot pysyvät välillä $[0, 1]$. Itse asiassa ne pysyvät joukossa C .



Cantorin joukon konstruktiossa yksikkövälistä poistetaan ensimmäisessä vaiheessa väli, jonka pituus on $\frac{1}{3}$, toisessa vaiheessa kaksi väliä, joiden pituudet ovat $\frac{1}{9}$, kolmannessa vaiheessa neljä väliä, joiden pituudet ovat $\frac{1}{27}$ ja niin edelleen. Vaiheessa k on siis poistettu joukko, jonka pituus on yhteensä

$$\frac{1}{3} + \frac{2}{9} + \frac{4}{27} + \cdots + \frac{1}{3} \left(\frac{2}{3}\right)^{k-1} = \frac{1}{3} \frac{1 - \left(\frac{2}{3}\right)^k}{1 - \frac{2}{3}} = 1 - \left(\frac{2}{3}\right)^k.$$

Tämän jonon raja-arvo on 1, joten joukon $[0, 1] \setminus C$ pituus näyttäisi olevan 1. Kuitenkaan Cantorin joukko ei ole tyhjä. Edellä löysimme jo äärettömän monta Cantorin joukon pistettä, nimittäin $\frac{1}{3^m} \in C$ kaikilla $m \in \mathbb{N}$.

Jos valitsemme sisäkkäisen jonon Cantorin joukon konstruktiossa esiintyviä jonoja $I_1 \supset I_2 \supset I_3 \supset \cdots$, niin kurssilla Analyysi 1 käsiteltävän *sisäkkäisten välien periaatteen* nojalla $\bigcap_{i=1}^{\infty} I_i$ on yhden pisteen joukko jokaisella tällaisella välien muodostamalla jonolla. Selvästi kahta eri jonoa vastaa kaksi eri pistettä koska jossain vaiheessa toiseen jonoon on valittu kahdesta mahdollisesta välistä oikeanpuoleinen ja toiseen vasemmanpuoleinen.

Jokaiseen Cantorin joukon pisteeseen voidaan liittää yksikäsitteinen *osoite*, joka on jono $(a_i)_{i=1}^{\infty}$, missä $a_k = 0$, jos k . vaiheessa valitaan vasemmanpuoleinen kahdesta mahdollisesta jonosta ja $a_k = 1$, jos k . vaiheessa valitaan oikeanpuoleinen väli.

Osoitamme, että Cantorin joukossa on paljon enemmän pisteitä kuin luonnollisten lukujen joukossa kunhan ensin sovimme, mitä moinen väite tarkoittaa.

4.2. Joukon mahtavuus.

Määritelmä 4.7. Joukko A on *numeroituvasti ääretön*, jos on bijektio joukolta $\mathbb{N}$ joukolle A . Ääretön joukko, joka ei ole numeroituva on *ylinnumeroituva*.

Esimerkki 4.8. (1) Positiivisten kokonaislukujen joukko on numeroituvasti ääretön: Kuvaus $S: \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$, $S(x) = x + 1$ on bijektio.

- (2) Kokonaislukujen joukko on numeroituvasti ääretön: Määritellään kuvaus $b: \mathbb{N} \rightarrow \mathbb{Z}$ asettamalla $b(k) = k/2$, jos k on parillinen ja $b(k) = -(k+1)/2$, jos k on pariton.
- (3) Rationaalilukujen joukko on numeroituvasti ääretön. Tämä todistus vaatii hie-
man enemmän työtä.

Lause 4.9. *Positiivisten kokonaislukujen joukon potenssijoukko on ylinumeroituva.*

Todistus. Jokaista joukon $\mathbb{N} \setminus \{0\}$ osajoukkoa A vastaa yksikäsitteisesti sen karakteristinen funktio χ_A . Oletetaan, että on bijektio $b: \mathbb{N} \setminus \{0\} \rightarrow \mathcal{P}(\mathbb{N} \setminus \{0\})$. Tällöin $b(k)$ on lukujono $(b_{kj})_{j=1}^\infty$. Lukujono $(1 - b_{ii})_{i=1}^\infty$ ei ole joukossa $b(\mathbb{N})$ sillä jokaisella $k \in \mathbb{N}$ se eroaa jonosta $b(k)$ koska $1 - b_{kk} \neq b_{kk}$. Huomaa, että $1 - b_{kk} = 1$, jos $b_{kk} = 0$ ja $1 - b_{kk} = 0$, jos $b_{kk} = 1$. Tämä on ristiriita, joten oletettua bijektiota ei ole. $\square$

Lauseen 4.9 todistusta kutsutaan Cantorin diagonaalitodistukseksi.

Seuraus 4.10. *Reaalilukujen joukko on ylinumeroituva.*

Todistus. Lauseen 4.9 mukaan desimaalilukuja, jotka ovat muotoa $0.a_1a_2a_3\cdots$, missä $a_i \in \{0, 1\}$ kaikilla $i \in \mathbb{N}$ on ylinumeroituvan monta. Kurssilla Analyysi 1 tarkastetaan, että jokainen tällainen desimaaliluku määrää eri reaaliluvun. Siis reaalilukujen joukko on ylinumeroituva koska sillä on ylinumeroituva osajoukko. $\square$

Seuraus 4.11. *Cantorin joukko on ylinumeroituva.*

Todistus. Cantorin joukolta on bijektio osoitteiden joukolle, joka on sama kuin positiivisten kokonaislukujen joukon osajoukkojen karakterististen funktioiden joukko. Tämä osoitettiin ylinumeroituvaksi Lauseessa 4.9. $\square$

Jos on bijektio $b: A \rightarrow B$, sanotaan, että joukot A ja B ovat *yhtä mahtavia*. Jos on injektio $i: A \rightarrow B$ mutta ei yhtään surjektiota $s: A \rightarrow B$, sanotaan, että joukko B on mahtavampi kuin A . Cantorin diagonaalitodistus osoittaa, että luonnollisten lukujen joukon potenssijoukko on mahtavampi kuin luonnollisten lukujen joukko. Todistuksen yleistetyllä versiolla voidaan osoittaa, että jokaisen joukon potenssijoukko on mahtavampi kuin joukko itse.