Kokonaislukujen erilaisia esitysmuotoja

Antti Iivari

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2014

Tiivistelmä: A. Iivari, *Kokonaislukujen erilaisia esitysmuotoja* (engl. *Different ways to portray integer numbers*), matematiikan pro gradu -tutkielma, 73 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kevät 2014.

Tämän tutkielman tarkoituksena on perehtyä kokonaislukujen erilaisiin esitysmuotoihin. Tutkielmassa keskeisinä kokonaisuuksina ovat jaollisuuteen ja alkulukuihin perustuvat lukujen esitystavat ja ominaisuudet, mutta myös muulla tavoin muodostettuja lukuja, kuten esimerkiksi Fibonaccin ja kuviolukuja tutkitaan.

Tutkielman alussa tehdään lyhyt katsaus erilaisten lukujärjestelmien historiaan, sekä lasketaan kuten muinaiset roomalaiset. Toisessa luvussa käsitellään jaollisuussääntöjä eri lukujärjestelmissä, sekä määritellään alkuluvut. Kolmannessa luvussa käsitellään monia lukuteorian keskeisiä tuloksia, kuten suurin yhteinen tekijä, Bézout'n yhtälö, Fermat'n pieni lause ja Legendren neljän neliön summa. Samassa luvussa tutustutaan myös Mersennen alkulukuihin, jotka ovat tiettyä muotoa olevia alkulukuja ja joita monet suurimmat tunnetut alkuluvut ovat. Yksi käsiteltävä alkulukuihin liittyvä tulos on Bertrandin postulaatti, jonka mukaan mielivaltaisesta joukosta $\{n, n+1, \ldots, 2n\}$ löytyy vähintään yksi alkuluku p. Alkulukutarkasteluissa kongruenssiyhtälöt ovat myös keskeisessä roolissa.

Neljännessä luvussa lukuja muodostetaan muutenkin kuin suoraan alkuluvuista. Käsiteltävänä ovat muun muassa täydelliset luvut, jotka ovat lukuja joiden itseä pienempien tekijöiden summa on luku itse, kuvioluvut, jotka nimensä mukaisesti perustuvat johonkin kuvioon, Fibonaccin luvut sekä Pascalin kolmio ja häviävät kolmiot. Pascalin kolmio pitää sisällään monta mielenkiintoista ominaisuutta ja siihen on "piilotettu" monet tutkielmassa esitetyt asiat, esimerkiksi binomikertoimet ja kuvioluvut, unohtamatta kolmion alkioiden jaollisuuden ja Sierpinskin maton välistä yhteyttä. Viimeiseen lukuun on vielä lisätty muutamia tuloksia, joita ei kaikkia ole pystytty todistamaan, mutta ne ovat itsessään mielenkiintoisia ja ymmärrettäviä. Lisäksi luvussa on "hajotettu" lukuja muutenkin kuin jaollisuussääntöjen avulla.

Sisältö

Johdanto

Tämän kirjoitelman tarkoituksena on perehdyttää lukija lukujen moninaisiin ilmaisutapoihin ja keinoihin. Kirjoitelmassa tarkastellaan erityisesti alkulukuihin perustuvia esitystapoja, mutta myös muunlaisia ilmaisuja on esitelty. Suuri osa tässä kirjoitelmassa esitetyistä lauseista ja tuloksista ovat 1600-luvulla vaikuttaneiden matemaatikkojen aikaansaannoksia, tuolta vuosisadalta joka on merkittävin sitten Platonin päivien. Varsinaisena matematiikan kulta-aikana pidetään 1800-lukua, jolloin matematiikka kehittyi enemmän kuin koko historiansa aikana yhteensä. [**3**][s.471, 695].

Kirjoitelma aloitetaan tarkastelemalla tunnetuimpia erilaisia numeromerkkejä, sekä lukujärjestelmiä, joita matematiikan historiaan on mahtunut. Muutamien esimerkkien kautta voidaan huomata, miten muut lukujärjestelmät ja lukujen merkintätavat tuntuvat hankalilta, kun johonkin on kerran kunnolla tottunut. Erityisesti tarkastellaan roomalaisilla numeroilla laskemista, sekä verrataan 12-kantaista duodesimaalijärjestelmää "normaaliin" 10-kantaiseen desimaalijärjestelmään.

Toisessa luvussa käsitellään jaollisuussääntöjä eri lukujärjestelmissä, sekä määritellään alkuluvut. Kolmannessa luvussa alkuluvut ovat keskiössä, sillä siinä tutustutaan alkutekijäesitykseen, sekä sen hyödyntämiseen ja soveltamiseen jaollisuutta tutkittaessa. Alkulukuja etsitään tietyt ehdot täyttävien yhtälöiden avulla, joita on esitelty lauseina. Yksi luvun keskeisistä lauseista on Bertrandin postulaatti, jonka mukaan mielivaltaisesta joukosta $\{n, n+1, \ldots, 2n\}$ löytyy vähintään yksi alkuluku p. Kiinnostuneita ollaan erityisesti Mersennen luvuista, jotka ovat tiettyä muotoa olevia alkulukuja ja jota muotoa suurimmat tunnetut alkuluvut ovat. Luvussa tulee tutuksi lukuteorian kannalta keskeisiä tuloksia, kuten esimerkiksi suurin yhteinen tekijä, Bezout'n yhtälö, Fermat'n pieni lause ja Legendren neljän neliön summa.

Neljännessä luvussa tutustutaan hieman erilaisempiin kokonaislukujen ja lukujonojen ilmaisutapoihin muun muassa täydellisten lukujen sekä Fibonaccin lukujen kautta, mutta ei unohdeta myöskään kokonaan alkulukuja. Tietyllä säännöllä muodostetut lukujonot ovat innoittaneet matemaatikkoja myös muodostamaan erilaisia taulukoita ja kuvioita, joihin tässä työssä perehdytään kuviolukujen sekä Pascalin kolmion myötä. Pascalin kolmiota voisi pitää taikakolmiona, sillä siihen on kätketty niin monia tuloksia, joihin osaan tutustutaan myös tässä työssä. Neljännestä luvusta voidaan myös huomata, miten moni puhtaasti matemaattiselta tuntuva asia omaakin vastaavuuksia arkipäivän elämässä, kuten esimerkiksi Fibonaccin luvut luonnossa tai Pascalin kolmion rivien kertoimet todennäköisyyksissä.

Viidenteen ja viimeiseen lukuun on kerätty muutamia mielenkiintoisia tuloksia, joita ei kaikkia ole pystytty vielä todistamaan, mutta jotka itsessään ovat mielenkiintoisia ja helposti ymmärrettäviä. Lisäksi siellä lukuja on "hajotettu" muutenkin kuin jaollisuussääntöjen mukaan.

LUKU 1

Historiaa

Matematiikalla on pitkä historia ja se eroaa muista tieteistä siltä osin, että siinä ei tehdä jatkuvasti merkittäviä korjauksia, ainoastaan laajennuksia. Matematiikan alkeellisia muotoja on ollut maapallolla niin kauan kuin on ollut ihmisiäkin, tai eläimiä, sillä itse asiassa myös eläinkokeissa on havaittu niillä olevan alkeellista matemaattista ymmärrystä muotojen sekä pienten joukkojen tunnistamisessa. [**2**][s.23].

Matematiikan historian suuret kaudet ovat olleet esikreikkalainen antiikki ja erityisesti babylonialainen matematiikka noin 2000 eKr., kreikkalainen ja hellenistinen antiikki 500 eKr.-300 jKr., intialainen varhaiskeskiaika n. 500-1200 jKr., islamin eli arabialaisen matematiikan kulta-aika 500-1200 jKr., renesanssi lähinnä Italiassa 1500-luvulla, uuden matematiikan pääalan eli analyysin synty Euroopassa 1600-luvulla ja sen nopea kehitys 1700-luvulla sekä matematiikan yleinen abstrahoituminen ja laajeneminen 1800-1900 luvulla, joka on kasvattanut matemaattista tietoa yhtä paljon, kuin mikä tahansa aikaisempi periodi ja jonka aikana suurin osa matemaatikoista on elänyt. [**18**][s.6-7].

1.1. Muinaiset lukujärjestelmät

Ennen nykymuotoisen numerojärjestelmän käyttöönottoa, monilla kansoilla on ollut historian varrella omia lukujärjestelmiä. Egyptiläisillä hieroglyyfit, babylonialaisilla 60-kantaiseen lukujärjestelmään perustuva nuolenpääkirjoitus, mayoilla 20-kantainen lukujärjestelmä [**10**][s.21], kreikkalaisilla ja roomalaisilla kirjaimet sekä tietenkin nykypäivää kohti tultaessa intialaisilla kaikkialle levinnyt kymmenjärjestelmä ja numerot. Lukumäärät ja osuudet ovat kehitetty laskennan tarpeisiin, niin paimentamista kuin kaupankäyntiäkin varten.

Egyptiläisillä oli hieroglyfinumerot 3000 eKr., jotka kehittyivät myöhemmin vastaamaan paremmin nykyistä menetelmää hieraattisessa kirjoitustavassa, jossa jokaiselle luvulle on oma merkkinsä [**18**][s.9]. Egyptiläisissä hieroglyfinumeroissa jokaiselle ”kymmenpotenssille” on oma merkkinsä, joita summaamalla muodostettiin lukuja.

$1 =$,
$10 =$,
$100 =$,
$1\ 000 =$,
$10\ 000 =$,
$100\ 000 =$,
$1\ 000\ 000 =$.

Alunperin luvut kirjoitettiin oikealta vasemmalle, esimerkiki luku 341 = 𓍢𓎆𓎆𓏺𓏺𓏺. Koska jokaiselle kymmenpotenssin termille on oma merkkinsä, luku voidaan kirjoittaa yksiselitteisesti myös toisinpäin 𓏺𓏺𓏺𓎆𓎆𓎆𓍢, kuten me olemme luvut tottuneet lukemaan. Jokaiselle kymmenpotenssille oleva oma merkki takaa myös sen, että lukua 0 ei tarvita erikseen, sillä 1209 = 𓆐𓏺𓏺𓆏 ei mene sekaisin 129 = 𓆐𓎆𓎆𓏺 kanssa. Nykymuotoisesta numeroiden esitystavasta egyptiläinen eroaa juuri siksi, että "välistä" puuttuvat nollat eivät muuta lukua, vaikkei niitä kirjoiteta ja että numero voidaan kirjoittaa ikään kuin väärinpäin, ilman että numero muuttuu. [**7**][s.111].

Yksi kirjoitustavasta säilynyt lähde on niin sanottu *Rhindin papyrus*, noin 1650 eKr, jossa on aritmeettisia tehtäviä vastauksineen. Egyptiläiselle artimetiikalle näyttää olleen tyypillisiä piirteitä additiivisuus, kahdennukseen ja osittelulakiin perustuva kerto- ja jakolasku, sekä yksikkömurtolukujen käyttö.

Esimerkki 1.1 (Egyptiläinen kertolasku nykynumeroilla). $67 \cdot 21 = 67 \cdot (16+4+1)$ laskettiin siten, että

$$\begin{aligned} 67 + 67 &= 134 \ (2 \cdot 67) \\ 134 + 134 &= 268 \ (4 \cdot 67) \\ 268 + 268 &= 536 \ (8 \cdot 67) \\ 536 + 536 &= 1072 \ (16 \cdot 67) \end{aligned}$$

Mistä saadaan poimittua, että $67 \cdot (16 + 4 + 1) = 1072 + 268 + 67 = 1407$.

Tai hieman toisella tapaa merkittynä:

1	67
~~2~~	~~134~~
4	268
~~8~~	~~536~~
16	1072
67	1407

Käytännössä ylläoleva kertolasku perustui siis 2-kantaiseen binääriesitykseen.

Babylonialaiset savitaulut sisältävät myös paljon mielenkiintoisia tuloksia, mutta kuten egyptiläisten papyrukset niissä oli pääosin esitelty erikoistapauksia yleisten tulosten sijaan. Yksi esimerkki babylonialaisten savitauluista löytyneistä kaiverruksista on tämän työn Lause 4.14. [**2**][s.69-70].

Keskiajan lammaspaimenet Lincolnshiressä käyttivät kaksikymmenkantaista lukujärjestelmää laskiessaan paimentamiaan eläimiä. Heillä oli olemassa lukusanat luvuille 1-20, joiden avulla he pystyivät laskemaan. Laskiessaan he lisäsivät taskuunsa kiven, piirsivät viivan maahan tai vuolivat paimensauvaansa viivan merkiksi siitä, että 20 on täyttynyt. Mikäli esimerkiksi paimennettavia oli 64, oli paimenella taskussaan kolme kiveä ja laskettuna lukuna 4. [**1**][s.43-44].

Paimenelle tuli kuitenkin ongelma siinä kohtaa, kun taskussa oli jo 20 kiveä ja edelleen piti lisätä, eli lampaita oli yli 400 ($= 20 \cdot 20$). Tällöin paimenen täytyi tehdä jokin muu merkintä tai laittaa esimerkiksi toiseen taskuun kiviä, aina kun 20 oli täynnä. [**1**][s.68-69]. Esimerkiksi jos lampaita oli 1300, paimenella oli ensimmäisessä taskussa 5 kiveä ja toisessa 3, koska $5 \cdot 20 + 3 \cdot 400 = 1300$. Edellä mainitulla tavalla tarvittiin itseasiassa kiviäkin vähemmän, sillä nyt selvittiin yhteensä 8 kivellä, kun muuten olisi tarvittu 65 kiveä.

Hyvin tyypillisiä olivat entisajan lukujärjestelmät, joissa kirjaimilla oli jokin lukuarvo ja tällöin tietty kirjainyhdistelmä vastasi tiettyä lukua. *Lukumystiikka* eli *numerologia* on saanut alkunsa juurikin kirjainten ja numerojen vastaavuuksien tarkastelusta. Lukumystiikassa sanojen ja kirjainten määrittämät tietyt lukuarvot muodostivat osasta sanoista "yliluonnollisen merkityksellisiä". Monissa edellämainitun tyyppisistä järjestelmistä ei ollut ratkaisevaa missä järjestyksessä kirjaimet olivat, sillä luvut saatiin summaamalla kirjaimia yhteen. [**10**][s.20-21].

Nykyisin käytössä olevassa *paikkamerkinnässä* eli *positiojärjestelmässä* numeroiden paikalla ja järjestyksellä on oleellinen merkitys. Pelkkä numero nolla on tuore luku verrattuna muihin numeroihin ja se yleistyikin vasta paikkamerkintään siirryttäessä, koska sitä tarvittiin osoittamaan tyhjää paikkaa. Paikkamerkinnän etu on se, että erilaisa numeromerkkejä tarvitaan vain vähän ja silti niillä voidaan esittää mielivaltaisen suuria lukuja. [**10**][s.20-21]. Intialaiset ottivat 500-luvun lopulla nykyiset numerot käyttöön, mutta eurooppalaiset omaksuivat ne vasta lähes tuhat vuotta myöhemmin [**15**][s.253].

1.1.1. Laskeminen roomalaisilla numeroilla. Meille tutuin kirjaimilla merkittävä numerojärjestelmä lienee roomalaiset numerot, joissa numerot muodostetaan summien avulla.

$$I = 1, \quad II = 2, \quad III = 3, \quad IV = 4, \quad V = 5, \quad VI = 6, \quad \ldots,$$
$$X = 10, \; L = 50, \quad C = 100, \quad D = 500, \quad M = 1000.$$

Alunperin numero 4 merkittiin neljällä ykkösellä eli $IIII$, mutta keskiajalla otettiin käyttöön *"yhtä vailla"*-merkintätapa. Samalla periaatteella merkittiin esimerkiksi $19 = XVIIII (= XIX)$ ja $90 = LXXXX (= XC)$. Suurimpana lukuna, joka voidaan ilmaista tavallisten aakkosten avulla, pidetään

$$MMMCMXCIX (= 3999),$$

mutta se ei itseasiassa ole suurin, sillä koska roomalaisten numeroiden esitys perustuu yhteenlaskuun, voidaan lukuja laittaa peräkkäin vaikka kuinka monia. Summaamisen takia sama luku voidaan myös ilmaista useammalla tavalla, esimerkiksi $MD = DDD = 1500$.

Roomalaislle numeroille ei ole olemassa nollalle omaa merkkiä, joka johtuu ilmeisesti siitä, että roomalaiset numerot ovat ikään kuin kehittynyt tukkimiehen kirjanpitojärjestelmä, eikä silloin tyhjälle ole tarvinnut olla omaa merkkiä. Nykyisin roomalaisia numeroita käytetään muun muassa ilman sijapäätteitä järjestyslukuina, erilaisten tapahtumien yhteyksissä ilmaisemaan kuinka mones tapahtuma on sen historiassa ja lääkeresepteissä. Se että roomalaiset numerot ovat kehitetty lukumäärän ilmaisemista ja yhteenlaskua varten, eikä suinkaan monimutkaista laskemista varten ilman apuvälineitä, kuten helmitaulua, selviää kun tarkastellaan esimerkiksi yhteen-

ja kertolaskua. Seuraavien laskuesimerkkien osalta on käytetty pääasiallisena lähteenä *Matti Lehtisen* Solmussa julkaisemaa artikkelia *Roomalaiset numerot - laskentoa ilman kertotaulua* [**11**].

Esimerkki 1.2 (Roomalaisten numeroiden yhteenlaskua). Lasketaan summa: $CMLIX + DCXXIV + DCCXLVIII \quad (= 959 + 624 + 748)$:

$$\begin{array}{r} CMLIX \\ DCXXIV \\ +\quad DCCXLVIII \\ \hline MMCCCXXXI \end{array}$$

Yhteenlaskussa on laskettu kaikki luvut yhteen ja käytetty supistussääntöä, jossa vajaat ja ylimenevät luvut on supistettu keskenään ja lopuksi kirjoitettu luku 2331 sievemmässä muodossa. Eli

$$\begin{array}{r} CMLIX \\ DCXXIV \\ +\quad DCCXLVIII \\ \hline \underbrace{\not{C}MDD\not{C}CC\not{X}LL\not{X}X\not{I}XV\not{I}V\not{I}\not{I}\not{I}}_{\text{supistetaan vajaat ja ylimenevät luvut summasta}} \\ \underbrace{= MDDCCLLXXVVI}_{\text{sievennetään luku}} \\ = MMCCCXXXI. \end{array}$$

Yhteenlasku sujuu helpommin mikäli käyttää ainoastaan luvuista vanhaa esitysmuotoa, jossa ei ole niin sanottuja ”yhtä vailla” olevia lukuja, sillä silloin kaikki termit vain kirjoitetaan yhteen pötköön, jonka jälkeen sen voi mahdollisesti sieventää nykymuotoiseen esitysmuotoon. Nykymuotoisella kirjoitustavalla harjaantumaton joutuu laskemaan hieman pitempään, joskin merkkimäärä jää monesti lyhyemmäksi. Suurilla luvuilla laskettaessa menetelmä on työläs.

Esimerkki 1.3 (Roomalaisten numeroiden yhteenlaskua). Lasketaan summa: $DCCCCLVIIII + DCXXIIII + DCCXXXXVIII$

$$\begin{array}{r} DCCCCLVIIII \\ DCXXIIII \\ +\quad DCCXXXXVIII \\ \hline \underbrace{DDDCCCCCCCCLXXXXXXXVVIIIIIIIIII}_{\text{sievennetään}} \\ = MMCCCXXXI \end{array}$$

Kertolaskussa käytetään *helmitaulu* -tekniikkaa, joka onnistuu helpoiten silloin, kun luvuissa ei esiinny yhtä aikaa *etruskimerkkejä* D, L tai V, eikä vähennysmerkinnällisiä lukuja. Helpoiten laskeminen onnistuu kun kirjoitetaan kerrottavan ja kertojan ”$MDCLXVI$*-rakenteet”* allekkain, käyttämällä jotain laskumerkkiä. Seuraavassa laskuesimerkissä se on ”x”.

Esimerkki 1.4 (Roomalaisten numeroiden kertolaskua). Lasketaan tulo $CCLXXXVIII \times XIII$ $(= 288 \cdot 13)$:

M	D	C	L	X	V	I
		xx	x	xxx	x	xxx
				x		xxx
		xx	x	xxx	x	xxx
		xx	x	xxx	x	xxx
		xx	x	xxx	x	xxx
xx	x	xxx	x	xxx		
MM	D	CCCCCCCCC	LLLL	XXXXXXXXXXX	VVV	IIIIIIII

Kertominen muistuttaa siis hieman koulussa nykyisinkin opetettavaa menetelmää. Roomalaisilla luvuilla kerrottaessa ei tarvitse varsinaisesti suorittaa mitään kertolaskua, vaan tulo merkitään vastaavalla määrällä laskumerkkejä oikeaan sarakkeeseen. Laskeminen aloitetaan kertomalla ensiksi alemman luvun jokaisella ykkösellä jokainen ylemmän luvun numero ja merkitään joka ykköstä vastaava tulo omalle rivilleen tuloa vastaavaan sarakkeeseen, sitten vitosilla sama, kymmenillä, jne. ... Jokainen luku kerrotaan erikseen, joten laskuun tulee yhtä monta riviä kuin on kertojan luvussa merkkejä. Kun kaikki kertomiset on suoritettu, lasketaan samassa sarakkeessa olevat luvut yhteen ja kirjoitetaan ne numeroin, jonka jälkeen ne voidaan vielä sieventää.

Sievennyksen jälkeen äskeisestä kertolaskusta saadaan vastaukseksi:

$$MMDCCCCCCCCCCLLLLXXXXXXXXXXXXXVVVIIIIIIIII$$
$$= MMMDCCXLIV \ (= 3744).$$

Aina eivät kuitenkaan luvut ole niin yksinkertaisia, että vain toisesta tulontekijästä löytyisi etruskimerkkejä. Tarkastellaan esimerkkiä myös sellaisesta tilanteesta, jossa kummassakin tulontekijässä on etruskimerkkejä. Sitä varten otetaan selvyyden vuoksi toinenkin laskumerkki ja olkoon se tässä ”y”, joka viittaa etruskilukuihin, mutta on arvoltaan kuitenkin yhtä suuri kuin ”x”. Aina silloin kun lasketaan etruskilukuja keskenään, täytyy lisätä kyseiseen sarakkeeseen yksi laskumerkki, mutta sen lisäksi seuraavaan vasemmalla puolella olevaan sarakkeeseen kaksi merkkiä. Muuten laskeminen tapahtuu samalla tavalla kuin edellisessäkin esimerkissä.

Esimerkki 1.5 (Roomalaisten numeroiden kertolaskua). Lasketaan tulo $LXXVIII \times VII$ $(= 78 \cdot 7)$:

D	C	L	X	V	I
		y	xx	y	xxx
				y	xx
		y	xx	y	xxx
		y	xx	y	xxx
	yy	yxx	yy	yxxx	
	CC	LLLLL	XXXXXX	VVVVVV	IIIIII

Edelleen sievennyksen jälkeen saadaan vastaukseksi $DXLVI$ $(= 546)$. Edellisissä laskuissa ei ole ollut mukana ollenkaan ”yhtä vaille” -merkintöjä, joita varten tarvitaan vielä yksi sääntö. Merkitään vähentävien symbolien sarakkeeseen ”*” -merkki

täydentämään laskumerkkiä. Mikäli kertojasarakkeessa on tähtimerkinnällinen merkki, niin kerrottaessa jokainen tähdetön merkki muutetaan tähdelliseksi ja päinvastoin. Lopuksi yhteenlaskettaessa tähdellinen ja tähdetön merkki kumoavat toisensa.

Esimerkki 1.6 (Roomalaisten numeroiden kertolaskua). Lasketaan tulo $XLIV \times XLIV$ $(= 44 \cdot 44 = 44^2)$:

M	D	C	L	X	V	I
			y	x*	y	x*
			y	x*	y	x*
			y*	x	y*	x
		yy	yx*	yy	yx*	
	y*	x	y*	x		
yy	yx*	yy	yx*			
MM	D*	CCCCC	L*L*	XXXX	V*	I

Edellinen tulo voidaan kirjoittaa tähdettömästi $MDMCCCCXXXVI$ (josta $L*$ $L*$ on supistanut yhden C kokonaan ja $V*$ yhden X pelkäksi V) ja sievennyksen jälkeen $MCMXXXVI$ $(= 1936)$.

Edellisistä esimerkeistä huomataan, että kertolaskun suorittaminen onnistuu, vaikkei itse kertotaulua osaisikaan. Mutta miten onnistuukaan jakolasku roomalaisilla numeroilla? Jakolaskussa selvitetään montako kertaa jakaja voidaan vähentää vähennettävästä. Jakolaskusta selviää myös suoraan mahdollinen jakojäännös.

Esimerkki 1.7 (Roomalaisten numeroiden jakolaskua). Lasketaan osamäärä $CCCLXXXVII : XVII$ $(= 387 : 17)$:

	C	L	X	V	I
(1)			x	y	xx
(2)			xx		xx
(3)	xx[x]	(xx)[x]	(xxxxx)xxx	x	xx
(4)	xx	yy	xxxx		
(5)			xxx[x]	(xx)[x]	(xxxxx)xx
(6)			xx	xx	xxxx
(7)			x		xxx

Kaavion riville (1) on merkitty jakaja ja riville (3) jaettava, osamäärä tulee riville (2) ja jakojäännös viimeiselle riville, eli tässä esimerkissä riville (7). Jakolasku aloitetaan ”jakamalla” mahdollisimman suurella luvulla. Tässä siirretään jakajaa kaksi pykälää vasemmalle kaksinkertaisena riville (4), jolloin myös merkitään riville (2) X-sarakkeeseen kaksi laskumerkkiä. Seuraavaksi suoritetaan vähennyslasku rivien (3) ja (4) välillä ja kirjoitetaan erotus riville (5). Koska rivillä (3) X sarakkeessa on vain kolme laskumerkkiä ”lainataan” sarakkeesta L, jolloin vähennyslasku voidaan suorittaa. Esimerkissä on lainattua osaa merkitty kaarisuluilla ja sitä josta on ”lainattu pois” hakasuluilla. Suoritetaan nyt riville (5) lasku kuten tehtiin riville (3). Tässä voidaan kirjoittaa rivin (1) luku kaksinkertaisena vastaaviin sarakkeisiin riville (6), joten merkitään nyt kaksi laskumerkkiä I-sarakkeeseen riville (2). Suoritetaan rivien (5) ja (6) välinen vähennyslasku kuten ylemmillä riveillä, jolloin saadaan jakojäännökseksi $XIII$. Luetaan jakolaskun vastaus riveiltä (2) ja (7), eli osamäärä on $XXII$ ja jakojäännös $XIII$.

Edellisessä esimerkissä ei ollut kummassakaan luvussa, jaettavassa eikä jakajassa, ”vaille” -muotoisia lukuja, joten katsotaan vielä toinen esimerkki tällaisesta tilanteesta. Kuten kertolaskunkin kohdalla, täytyy jakolaskun kohdalla olla tarkkana miten vaillinainen luku vaikuttaa. Mikäli vain vähentävässä luvussa on vaillinainen luku, niin vaillinaista osaa ei vähennetäkkään vaan se lisätään vastaavan sarakkeen lukuun. Mikäli sen sijaan kummassakin vaillinainen luku on samaa muotoa, voidaan vähennyslasku suorittaa.

Esimerkki 1.8 (Roomalaisten numeroiden jakolaskua). Lasketaan osamäärä $CDLXXIV : XXIX$ (eli 474 : 29):

	D	C	L	X	V	I
(1)				xxx		x*
(2)				x	y	x
(3)	[y]	(xxxxx)x*	y	xx	y	x*
(4)		xxx		x*		
(5)		[x]	(xx)y	xxx	y	x*
(6)			xxx		x*	
(7)				xxxx		x*
(8)				xxx		x*
(9)				x		

Jakaja, jaettava ja ratkaisun luvut ovat samoilla riveillä kuten edellisessä esimerkissä (jakojäännös viimeisellä rivillä). Aloitetaan taas laskeminen siirtämällä jakajaa pari pykälää vasemmalle riville (4) ja suoritetaan vähennyslasku riville (5). Aina kun kirjoitetaan jakaja uudelle riville, täytyy muistaa lisätä merkki oikeaan sarakkeeseen riville (2). Nyt koska rivillä (3) joudutaan lainaamaan vähennyslaskua varten, supistavat yksi tähdellinen ja tähdetön lukumerkki samalta riviltä toisensa, lisäksi vähentäjän vaillinainen osa lisätään vähennettävään. Käytännössä siis C-sarakkeessa vähennys suoritetaan supistuksen jälkeen normaalisti, mutta rivillä (4) X-sarakkeessa ei vähennetä, vaan lisätään yksi laskumerkki. Kun riville (5) on lasku suoritettu jatketaan jakamista siirtämällä jakajana oleva luku yhden pykälän vasemmalle riville (6) ja suoritetaan vähennyslasku riville (7) kuten edellä. Nyt huomataan että, V-sarakkeessa täytyisi lukumerkit summata, mutta kun ne summataan tulee X, joten siirretään se suoraan sarakkeeseen X. Jatketaan edelleen jakamista kirjoittamalla jakaja riville (8) ja suoritetaan vähennyslasku riville (9). Vastaus on nyt valmis ja se voidaan lukea riveiltä (2) ja (7), eli osamäärä on XVI ja jakojäännös X.

1.2. Kantaluku ja kantalukujärjestelmä

Määritelmä 1.9. Kantaluku b on ykköstä suurempi luonnollinen luku. Kantalukujärjestelmä sisältää luvut $0, 1, \ldots, b-1$, jotka (yksin tai) peräkkäin aseteltuna muodostavat luvun. Eri järjestelmissä käytettävät numerot ovat aidosti pienempiä kuin kantaluku. Esimerkiksi jos kantalukuna on 2, niin luvun ilmaisuun käytettäviä numeroita ei ole kuin 0 ja 1. Kahdeksankantaisessa järjestelmässä käytössä olevia numeroita ovat 0, 1, 2, 3, 4, 5, 6 ja 7, eli lukumerkkejä on yhtä monta kuin kantaluku ilmoittaa, mutta ne ovat kaikki kuitenkin kantalukua pienempiä. Mikäli kantaluku b on suurempi kuin 10, käytetään yleensä kirjaimia tai muita symboleita numeroina, jotka ylittävät luvun 9.

Tässä työssä käsitellään lukuja kymmenjärjestelmässä, ellei toisin mainita. Kymmenjärjestelmän luvut esiintyvät ”normaaleina” numeroina ilman ala- tai yläindeksejä. Mikäli halutaan esittää lukuja jossain muussa järjestelmässä, esimerkiksi binäärilukuna, on siihen liitetty vastaava alaindeksi eli tässä tapauksessa 2 tai asiasta on muuten mainittu selkeästi. Esimerkiksi kymmenjärjestelmän luku 19 on binäärilukuna 10011_2 tai kahdeksanjärjestelmässä 23_8. Laskeminen muunkantaisissa lukujärjestelmissä onnistuu kuten kymmenkantaisessakin, eikä lukuja tarvitse välttämättä muuttaa kymmenkantaisiksi, täytyy vain muistaa tarvittaessa oikeat muistinumerot [**14**][s.6].

1.2.1. Nykyisin käytössä olevia lukujärjestelmiä. Kuten edellisestä luvusta kävi ilmi, lukujärjestelmiä on ja on ollut historian aikana monia. Nykyään tutuin laskentajärjestelmä on kymmen- tai desimaalijärjestelmä, eli lukujärjestelmä, jonka kantalukuna on luku kymmenen. Mitään tiettyä syytä ei voida sanoa miksi 10-kantainen järjestelmä on valikoitunut yleiseen käyttöön, mutta on arvailtu, että se todennäköisesti juontaa juurensa sormilla laskemisesta. Kymmenkantaisen järjestelmän käyttöön ollaan niin tottuneita, että muiden järjestelmien käyttö tuntuu hankalalta. Oikeastaan ainoana poikkeuksena babylonialaisten lukujärjestelmän yhä tuntuvista vaikutuksista on ajan ja kulmien mittaaminen, sillä kelloissa ja kulmissa käytetään edelleen 60-kantaista järjestelmää. [**10**][s.21].

Ihmisruumiiseen ja ruumiinosiin perustuvia laskutapoja on toki muitakin ja parhaiten numeroiden ja ruumiinosien yhteys selviää numeroiden lukusanoista. Esimerkiksi amerikkalaisen dene-dinje-intiaaniheimon lukusanat yhdestä viiteen viittaavat sormiin [**7**][s.58]:

1	”reunimmainen on taivutettu” (pikkusormi)
2	”taivutettu vielä kerran” (nimetön)
3	”keskimmäinen on taivutettu” (keskisormi)
4	”vain yksi on jäljellä” (peukalo)
5	”käteni on lopussa”

Muun kantaisina järjestelminä mainittakoon tässä tietokoneissa käytettävä kaksikantainen binäärijärjestelmä, sekä DNA-molekyyleihin koodattu tieto elollisten olentojen rakenteesta, joka toimii 4-kantaisen järjestelmän mukaan, sillä niiden pitkä merkkijono sisältää yhden merkin neljästä erilaisesta emäsparista. [**10**][s.21-22].

Esimerkki 1.10. *Luvun arvo a-kantaisessa lukujärjestelmässä.*
Olkoon 10-kantaisen lukujärjestelmän luku 27.
Kaksikantaisen eli binäärijärjestelmän lukuna se on 11011 eli
$1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 8 + 0 + 2 + 1 = 27$.[1]
Nelikantaisen järjestelmän lukuna taas 123, eli
$1 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0 = 16 + 8 + 3 = 27$.
8-kantaisessa eli oktaalijärjestelmässä 33, eli
$3 \cdot 8^1 + 3 \cdot 3^0 = 27$.
12-kantaisessa eli duodesimaalijärjestelmässä 23, eli

[1]Yleisessä muodossahan binäärinen järjestelmä lasketaan $1/0 \cdot 2^n + 1/0 \cdot 2^{n-1} + \ldots 1/0 \cdot 2^2 + 1/0 \cdot 2^1 + 1/0 \cdot 2^0 = 1/0 \cdot 2^n + 1/0 \cdot 2^{n-1} + \ldots 1/0 \cdot 4 + 1/0 \cdot 2 + 1/0 \cdot 1$, mutta kaikki ne ensimmäiset termit joissa kertoimena on 0 jätetään merkitsemättä.

$2 \cdot 12^1 + 3 \cdot 12^0 = 24 + 3 = 27$.
16-kantaisessa eli heksadesimaalijärjestelmässä 1B, eli
$1 \cdot 16^1 + 11 \cdot 16^0$.
a-kantaisessa järjestelmässä, jossa a on jokin tunnettu positiivinen kokonaisluku ($a \in \mathbb{Z}_+$) ja $b, c, \ldots, \beta, \alpha \in \{0, 1, \ldots, a-1\}$
$b \cdot a^n + c \cdot a^{n-1} + \cdots + \beta \cdot a^1 + \alpha \cdot a^0$

Siitä onko 10-kantainen lukujärjestelmä paras, ollaan montaa mieltä, mutta se on juurtunut niin syvään, että tuskin muuhun järjestelmään koskaan vaihdetaan. Kymmenestä tekee hankalan se, että sillä ei ole kuin kaksi tekijää 2 ja 5, kun esimerkiksi potentiaalisimmalla kilpailijallaan 12-kantaisella järjestelmällä kantaluku on jaollinen luvuilla 2,3,4 ja 6. Useammasta jakajasta on hyötyä erityisesti murtoluvuissa. [**10**][s.22].

Kaksitoistajärjestelmän eli dosenaali- tai duodesimaalijärjestelmän luvut ovat järjestyksessä $1, 2, 3, 4, 5, 6, 7, 8, 9, ↊ =$*"dek"*$, ↋ =$*"el"*$, 10 =$*"do"*. Luvuille ↊ ja ↋ on jonkin verran variaatioita riippuen käyttäjistä. Esimerkiksi toisinaan saatetaan merkitä $↊ = * = A$ ja $↋ = \# = B$, mutta vielä muunlaisiakin merkintätapoja löytyy. [**1**][s.50-53, 56].

Esimerkki 1.11. Kymmenkantaisessa lukujärjestelmässä 2:n kertotaulussa kokonaislukujen tulo on aina parillinen luku ja 5:n kertotaulussa tulon viimeinen luku on joko 0 tai 5. Kaksitoistakantaisessa järjestelmässä sen sijaan tällaisia tiettyihin samoihin lukuihin päättyviä tuloja on useampia. Kuten ylempänä todettiin, kantaluku 12 on jaollinen luvuilla 2,3,4 ja 6. Kaksitoistajärjestelmässä 2:n kertotaulussa tulo on niin ikään parillinen, 3:n kertotaulu sen sijaan pättyy aina 0, 3, 6 tai 9, 4:n kertotaulu 4, 8 tai 0 ja 6 kertotaulu numeroihin 6 tai 0. Edellisten lukujen kertotaulut näkyy seuraavista lukujärjestelmien "täydellisistä" kertolaskutaulukoista 1 ja 2.

Taulukko 1. Kaksitoistajärjestelmän kertolaskutaulukko

	1	2	3	4	5	6	7	8	9	↊	↋	10
1	1	2	3	4	5	6	7	8	9	↊	↋	10
2	2	4	6	8	↊	10	12	14	16	18	1↊	20
3	3	6	9	10	13	16	19	20	23	26	29	30
4	4	8	10	14	18	20	24	28	30	34	38	40
5	5	↊	13	18	21	26	2↋	34	39	42	47	50
6	6	10	16	20	26	30	36	40	46	50	56	60
7	7	12	19	24	2↋	36	41	48	53	5↊	65	70
8	8	14	20	28	34	40	48	54	60	68	74	80
9	9	16	23	30	39	46	53	60	69	76	83	90
↊	↊	18	26	34	42	50	5↊	68	76	84	92	↉0
↋	↋	1↊	29	38	47	56	65	74	83	92	↉1	↋0
10	10	20	30	40	50	60	70	80	90	↉0	↋0	100

TAULUKKO 2. Kymmenjärjestelmän kertolaskutaulukko

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

Kuten kertolaskutaulukoista 1 ja 2 voi todeta, kummassakin lukujärjestelmässä luvun 1 ollessa toisena kertoimena luku on suoraan toinen luku ja järjestelmän kantaluvun b ollessa toisena kertoimena kerrottavan luvun perään lisätään luku 0. Lisäksi kuten aiemmin jo todettiin, niin kantaluvun jakajat (sekä niiden monikerrat) käyttäytyvät säännönmukaisesti, niin että lukujen jälkimmäisenä lukuina toistuvat säännöllisesti vain tietyt luvut. Myöskin luvun $b-1$ kertotaulut käyttäytyvät kummassakin järjestelmässä samoin, sillä tulon ensimmäinen luku on taulukon "$y-akselin$" $luku-1$ ja jälkimmäinen luku $b-$"$y-akselin$" $luku$.

Luvut joiden alkulukuesityksessä (vrt. Määritelmä 3.1) ei esiinny kantaluvun tekijöitä, käyttäytyvät "vapaasti" ja niiden tuloissa kummassakin järjestelmässä jälkimmäisenä lukuna esiintyvät kaikki lukujärjestelmän eri luvut. Kymmenjärjestelmässä luvut ovat 3 ja 7, jotka ovat alkulukuja, sekä kaksitoistajärjestelmässä 5 ja 7, jotka ovat niin ikään alkulukuja.

ESIMERKKI 1.12. Kaksitoistajärjestelmän etu kymmenjärjestelmään korostuu vielä paremmin murtolukujen siistimmässä esitystavassa. Tarkastellaan luvun 100 jakamista luvuilla 1-12 sekä 10- että 12-kantaisissa järjestelmissä [2]:

[2]puolipilkku ";" tarkoittaa dosenaalipilkkua

100:n murto-osa	Desimaali	Dosenaali
Yksi	100	100
Puolet	50	60
Kolmasosa	33,333...	40
Neljäsosa	25	30
Viidesosa	20	24;97...
Kuudesosa	16,666...	20
Seitsemäsosa	14,285...	18;6Ƹ35 ...
Kahdeksasosa	12,5	16
Yhdeksäsosa	11,111...	14
Kymmenesosa	10	12;497...
Yhdestoistaosa	9,09...	11;11...
Kahdestoistaosa	8,333...	10

Vaikka kantaluku 12 näyttäisikin menevän monessa kohtaa paremmin tasan ja antavan yksinkertaisempia lukuja, duodesimaalilukuihin tuskin siirrytään niin kauan kun ihmisellä on kymmenen sormea. [**1**][s.50-56].

Esimerkki 1.13 (Binäärijärjestelmä apuna uudella paikkakunnalla). Tunnetuimpia binäärijärjestelmän hyödyntäjiä ovat nykyisin tietokoneet, mutta binäärijärjestelmää pystyy hyödyntämään helposti tilanteissa, joissa pitää muistaa pitkiä sarjoja, mitkä pitävät sisällään vain kaksi vaihtoehtoa. Esimerkkinä tällaisesta tilanteesta voisi olla oikeista risteyksistä oikeaan suuntaan kääntyminen, eli täytyykö kääntyä oikealle vai vasemmalle. [**14**][s.13-14].

Olkoon meillä 7 risteystä, joissa pitää kääntyä seuraavassa järjestyksessä oikea, vasen, vasen, vasen, oikea, vasen, oikea. On sopimus kysymys merkitäänkö kumpaa suuntaa numerolla 1 ja kumpaa numerolla 0, mutta käytetään tässä merkintätapaa, jossa nolla tarkoittaa oikealle kääntymistä, koska 0 muistuttaa o-kirjainta ja täten vasemmalle kääntymistä numerolla 1. Tällöin saadaan risteysten käännösohjeiksi luku $0111010 = 111010$, mikä vastaa 10-järjestelmän lukua $111010_2 = 58$. Nyt koska ensimmäinen käännös on oikealle, mikä vastaa lukua 0, on ohjeistuksessa olennaista mainita että risteyksiä on 7, jolloin luvun eteen täytyy lisätä se 0.

Edellinen risteysmenetelmä vaikuttaa toimivalta ja melko yksinkertaiseltakin toteuttaa, mutta siinä on yksi pieni heikkous, jota järjestelmä ei huomioi. Nimittäin miten toimia jos risteyksestä jatketaankin suoraan? Miten suoraan menemistä merkitään vai täytyykö matkalla tehdä mutka päästäkseen perille? Yksi helppo ratkaisu tähän olisi käyttää 3-kantaista järjestelmää, jolloin jokaiselle vaihtoehdolle; vasemmalle, suoraan ja oikealle olisi oma numeronsa.

LUKU 2

Määritelmiä ja jaollisuusominaisuuksia

Selvennetään sekaannusten välttämiseksi muutamaa merkintää.

Merkintä	*Selitys*
$\mathbb{N}$	Luonnollisten lukujen joukko $\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}_+$	Positiivisten kokonaislukujen joukko $\{1, 2, 3, \dots\}$
$n!$	$1 \cdot 2 \cdot \ldots \cdot n$

MÄÄRITELMÄ 2.1 (Luonnolliset luvut). Määritellään luonnolliset luvut *Peanon aksioomien* avulla [**19**]:

- 0 on luonnollinen luku.
- Jos a on luku, niin myös luvun a seuraaja on luku.
- Nolla ei ole minkään luvun seuraaja.
- Mikäli kahden luvun seuraajat ovat yhtä suuret, ovat luvut itse yhtäsuuret.
- *Induktioaksiooma.* Jos asetetaan että lukujoukko S sisältää nollan ja myös seuraajat kaikille luvuille sisältyvät joukkoon S, niin jokainen luku sisältyy joukkoon S.

Kun luonnolliset luvut on määritelty, saadaan jokainen kokonaisluku luonnollisten lukujen erotusten avulla ja edelleen jokainen rationaaliluku kahden kokonaisluvun suhteena.

LAUSE 2.2. *Olkoon tarkasteltavana kokonaislukujoukon alkiot. Tällöin*

(i) *kahden parillisen luvun tulo on parillinen,*
(ii) *kahden parittoman luvun tulo on pariton,*
(iii) *parillisen ja parittoman luvun tulo on parillinen.*

TODISTUS. Olkoon parilliset mielivaltaiset kokonaisluvut $a = 2n$ ja $b = 2m$ (voivat olla keskenään samoja) sekä parittomat mielivaltaiset kokonaisluvut $c = 2k + 1$ ja $d = 2l + 1$ (voivat olla keskenään samoja). Tällöin

(i) kerrotaan kaksi parillista lukua a ja b keskenään, jolloin saadaan
$$ab = 2n \cdot 2m = 2(2nm),$$
mikä on selvästi parillinen.

(ii) kerrotaan kaksi paritonta lukua c ja d keskenään, jolloin saadaan
$$cd = (2k + 1) \cdot (2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1,$$
mikä on selvästi pariton.

(iii) kerrotaan parillinen luku a ja pariton luku c keskenään, jolloin saadaan
$$ac = (2n) \cdot (2k + 1) = 4nk + 2n = 2(2nk + n),$$
mikä on selvästi parillinen.

□

2.1. Jaollisuus

MÄÄRITELMÄ 2.3. Luku b on jaollinen luvulla a, jos $b = ka$ jollekin luvulle k, missä $a, b, k \in \mathbb{Z}$.

Merkitään lukujen jaollisuutta siten, että jos luku a jakaa luvun b, niin $a|b$ (mikäli luku a ei jaa lukua b, niin merkitään $a \nmid b$). Tällöin siis luku a on luvun b tekijä eli toisin sanottuna luku b on luvun a monikerta. [**4**][s. 83].

Luonnollisten lukujen kertolaskulle pätevät seuraavat ominaisuudet:

$$jos\ ab = ac,\ niin\ b = c, \qquad (supistamislaki) \tag{1}$$

$$ab = ba \quad \forall a, b, \qquad (kommutatiivisuus) \tag{2}$$

$$(ab)c = a(bc) \quad \forall a, b, c, \qquad (assosiatiivisuus) \tag{3}$$

$$1a = a \quad \forall a. \qquad (identtinen\ alkio) \tag{4}$$

Seuraavat ominaisuudet luonnollisille luvuille seuraavat suoraan jaollisuuden määritelmästä 2.3 [**4**][s. 83]:

(i) $a|a\ ja\ 1|a \quad \forall a$,
(ii) $jos\ b|a\ ja\ c|b,\ niin\ c|a$,
(iii) $jos\ b|a,\ niin\ b|ac \quad \forall c$,
(iv) $bc|ac\ jos\ ja\ vain\ jos\ b|a$,
(v) $jos\ b|a\ ja\ a|b,\ niin\ b = a$.

Todistetaan edellisestä kohta (ii).

TODISTUS. Koska luku b jakaa luvun a täytyy luvun a olla luvun b monikerta, eli $kb = a$, missä $k \in \mathbb{N}$. Toisaalta koska myöskin luku c jakaa luvun b, niin luvun b täytyy olla luvun c monikerta, eli $nc = b$, missä $n \in \mathbb{N}$. Nyt edellisten perusteella voidaan todeta että $\frac{a}{c} = \frac{kb}{\frac{b}{n}} = kn$ ja koska luvut k ja n ovat kumpikin luonnollisia lukuja, on niiden tulokin luonnollinen luku, joten luku a on jaollinen luvulla c. □

Jaollisuussännöt ovat riippuvaisia lukujärjestelmästä ja erityisesti kantaluvusta. Jaollisuustarkasteluja varten käydään läpi vielä hyödyllinen menetelmä, jolla selvittely onnistuu helpommin.

2.1.1. Lohkaisuperiaate. Menetelmän lähtökohtana on, että luku esitetään sellaisessa summamuodossa, että luvun ensimmäinen osa, josta käytetään nimitystä lohkaisutermi, on varmasti jaollinen tarkasteltavalla luvulla ja jälkimmäinen osa, jota puolestaan kutsutaan kriittiseksi termiksi, täytyy selvittää erikseen. Mikäli kummatkin osat ovat jaollisia halutulla luvulla, on myös alkuperäinen luku tällä jaollinen.

Merkitään lukua jolla jaetaan muuttujalla n, tutkittavaa lukua muuttujalla t, lohkaisutermiä muuttujalla l ja kriittistä termiä muuttujalla k. Tutkittava luku on siis $t = l + k$ ja missä $n|l$ on kokonaisluku, sillä luku n jakaa luvun l. [**14**][s.39].

Todistetaan vielä ennen jaollisuussääntöihin syventymistä eräs aputulos.

LAUSE 2.4. *Olkoon kokonaisluvut $a, b \in \mathbb{Z}$ ja luonnollinen luku $n \in \mathbb{N}$. Tällöin*

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}), \tag{5}$$

eli $a - b$ jakaa $a^n - b^n$ kaikilla luvun n arvoilla.

TODISTUS. Lasketaan yhtälön oikealla puolella oleva kertolasku

$$\begin{aligned}(a-b)&(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}) \\ &= a^n + a^{n-1}b + a^{n-2}b^2 + \cdots + a^2b^{n-2} + ab^{n-1} \\ &\quad - a^{n-1}b - a^{n-2}b^2 - a^{n-3}b^3 - \cdots - ab^{n-1} - b^n \\ &= a^n - b^n.\end{aligned}$$

Kerrottaessa siis sulut auki, käy niin, että kaikki muut termit supistuvat pois, paitsi a^n ja $-b^n$. □

2.1.2. 10-järjestelmän jaollisuussäännöt. Tarkastellaan aluksi lukujen 2-11 jaollisuutta kymmenjärjestelmässä:

- luku on jaollinen luvulla 2, mikäli luku päättyy parilliseen numeroon (= $0, 2, 4, 6, 8$),
- luku on jaollinen luvulla 3, mikäli luvun numeroiden yhteenlaskettu summa on jaollinen kolmella,
- luku on jaollinen luvulla 4, mikäli luvun kahden viimeisen numeron muodostama luku on jaollinen neljällä,
- luku on jaollinen luvulla 5, mikäli luvun viimeinen numero on 0 tai 5,
- luku on jaollinen luvulla 6, mikäli se on jaollinen kummallakin luvulla 2 ja 3,
- luku on jaollinen luvulla 7, mikäli sen jaksotermien summa on jaollinen seitsemällä,
- luku on jaollinen luvulla 8, mikäli sen kolmen viimeisen numeron muodostama luku on jaollinen kahdeksalla,
- luku on jaollinen luvulla 9, mikäli luvun numeroiden yhteenlaskettu summa on jaollinen yhdeksällä,
- luku on jaollinen luvulla 10, mikäli luvun viimeinen numero on 0,
- luku on jaollinen luvulla 11, mikäli sen vuorotteleva numerosumma on jaollinen yhdellätoista

Tarkastellaan muutamia edellisistä säännöistä hieman tarkemmin. Luvulla 2 jaollisuus on selvä, samoin kuin luvuille 5 ja 10, myös luvulle 4 jaollisuus on helppo todeta lohkaisumenetelmän avulla, sillä 100 on jaollinen luvulla 4 ja täten riittää tarkastella kriittisenä terminä kahta viimeistä numeroa luvusta. Myös kahdeksalla jaollisuutta tarkasteltaessa riittää tarkastella loppupään numeroita, koska luku 1 000 on jaollinen selvästi luvulla 8. Pureudutaan tarkemmin lukujen jaollisuussääntöihin, jotka eivät ole niin selviä suoraan. Aloitetaan luvuista 3 ja 9, joiden taustalla on sama idea.

Kirjoitetaan kasvavia kymmenenpotensseja lohkaisumenetelmän avulla:

$$10 = 9 + 1, 100 = 99 + 1, 1\ 000 = 999 + 1, 10\ 000 = 9\ 999 + 1, \ldots,$$

missä ykkösen lisäystä ennen oleva luku on selvästi jaollinen sekä luvulla 9 ja siten myös luvulla 3. Nyt siis ”jäännösykköset” määrittävät sen onko luku jaollinen luvulla 3 tai 9.

Esimerkki 2.5. Selvitetään onko luku 12 734 jaollinen luvulla 9. Hyödynnetään tarkastelussa lohkaisumenetelmää ja kirjoitetaan luku muodossa

$$\begin{aligned} 12\ 734 &= 1 \cdot 10\ 000 + 2 \cdot 1\ 000 + 7 \cdot 100 + 3 \cdot 10 + 4 \\ &= 1 \cdot (9\ 999 + 1) + 2 \cdot (999 + 1) + 7 \cdot (99 + 1) + 3 \cdot (9 + 1) + 4 \\ &= \underbrace{(1 \cdot 9\ 999 + 2 \cdot 999 + 7 \cdot 99 + 3 \cdot 9)}_{lohkaisutermi} + \underbrace{(1 \cdot 1 + 2 \cdot 1 + 7 \cdot 1 + 3 \cdot 1 + 4)}_{kriittinen\ termi} \end{aligned}$$

Koska lohkaisutermi on jaollinen luvulla 9 riittää tarkastella onko kriittinen termi jaollinen luvulla 9.
$1 + 2 + 7 + 3 + 4 = 17$, mutta $9 \nmid 17$, joten luku 12 734 ei ole jaollinen luvulla 9 (eikä edes jaollinen luvulla 3, koska $3 \nmid 17$).

Esimerkki 2.6 (Ajatuksenlukua osa 1).

- Valitse jokin kolminumeroinen luku, missä ensimmäinen ja viimeinen luku eivät ole samoja (eli luku ei ole palindromi).
- Muodosta luvusta peilikuvaluku kääntämällä numeroiden järjestys, jolloin saat kaksi lukua.
- Vähennä pienempi luku suuremmasta, jolloin saat uuden luvun.
- Muodosta taas peilikuvaluku kääntämällä numeroiden järjestys (HUOM! mikäli käännettävä luku on kaksinumeroinen, lisää ensin eteen 0).
- Laske saadut numerot yhteen (eli erotuksesta saatu luku ja sen peilikuvaluku).
- Mitä saat tulokseksi?

Selitys 2.7. Syy miksi edellisen esimerkin menetelmällä saadaan lopputulokseksi aina 1089 on seuraava:

Olkoon luvut kokonaisluvut x, y, z siten että $x \in \{1, \ldots, 9\}, y, z \in \{0, \ldots, 9\}$.

Tällöin kolminumeroinen luku voidaan kirjoittaa muodossa

$$x \cdot 100 + y \cdot 10 + z \cdot 1 = 100x + 10y + z$$

jolloin peilikuvaluku on muotoa

$$100z + 10y + x$$

oletetaan että ensimmäinen luku on suurempi, eli $x > z$

$$100x + 10y + z - (100z + 10y + x) = 99(x - z).$$

Saatu luku on siis aina luvun 99 moninkerta. Nyt koska $x > z$, niin luku $x - z$ on aina vähintään 1 ja korkeintaan 9. Esimerkiksi jos erotus $x - z$ on 4, niin saatu luku on 396, minkä peilikuva luku on 693 ja näiden summa on $396 + 693 = 1089$.

Vastaavasti mikäli $z > x$. Summa saadaan siis laskemalla kaksi tuloa yhteen, siten että $k \cdot 99 + n \cdot 99$, missä $k + n = 11$, kun $k, n \in \{1, \ldots, 10\}$

Jatketaan vielä 10-järjestelmän jaollisuussääntöjen parissa. Koska luvun 11 jaollisuussäännössä on vastaavia piirteitä kuin luvun 9 jaollisuuden perustelussa, tutkitaan sitä seuraavaksi. Jos tarkastellaan vastaavasti kymmenen eri potensseja huomataan

että $11 = 10 + 1, 99 = 100 - 1, 1\ 001 = 1\ 000 + 1, 9\ 999 = 10\ 000 - 1, \ldots$ jotka ovat selvästi jaollisia luvulla 11. Yleisesti:

$$10^n + 1 \text{ on jaollinen luvulla 11, jos } n \text{ on pariton,}$$
$$10^n - 1 \text{ on jaollinen luvulla 11, jos } n \text{ on parillinen.}$$

Tämä seuraa yhtälöstä (5), mistä on erityisesti huomattava, että

$$a - b | a^n - b^n.$$

Nyt jos sijoitetaan yhtälöön $a = 10, b = -1$, niin

$$11 | 10^n - (-1)^n,$$

missä siis $(-1)^n$ on 1 tai -1 riippuen onko potenssi n parillinen vai pariton. Lohkaisu suoritetaan siten, että kymmenen potenssit korvataan seuraavasti $10 = 11 - 1, 100 = 99 + 1, 1\ 000 = 1\ 001 - 1, 10\ 000 = 9\ 999 + 1, \ldots$, eli yleisesti

$$10^n = [10^n - (-1)^n] + (-1)^n.$$

[**14**][s.43].

Esimerkki 2.8. Selvitetään onko luku 70 653 jaollinen luvulla 11. Aloitetaan selvittäminen kirjoittamallataas luku lohkaistussa muodossa.

$$\begin{aligned} 70\ 653 &= 7 \cdot 10\ 000 + 0 \cdot 1\ 000 + 6 \cdot 100 + 5 \cdot 10 + 3 \\ &= 7 \cdot (9\ 999 + 1) + 0 \cdot (1001 - 1) + 6 \cdot (99 + 1) + 5 \cdot (11 - 1) + 3 \\ &= \underbrace{(7 \cdot 9\ 999 + 0 \cdot 1001 + 6 \cdot 99 + 5 \cdot 11)}_{lohkaisutermi} + \underbrace{(7 \cdot 1 + 0 \cdot (-1) + 6 \cdot 1 + 5 \cdot (-1) + 3)}_{kriittinen\ termi} \end{aligned}$$

Koska lohkaisutermi on jaollinen luvulla 11 riittää tarkastella onko kriittinen termi jaollinen luvulla 11.
$7 - 0 + 6 - 5 + 3 = 11$, joten luku 70 653 on jaollinen luvulla 11. Käytännössa lukujen summaaminen kannattaa aloittaa luvun viimeisestä numerosta, jolloin joka toisen numeron saa lisätä ja joka toisen vähentää. Aloittaessa luvun viimeisestä numerosta, ei tarvitse tietää onko ensimmäinen summattava numero positiivinen vai negatiivinen.

Meillä on vielä käymättä läpi luvut, jotka ovat jaollisia luvulla 7. Tällaisille luvuille sääntö on työläs, mikäli luvut ovat suuria.

Luvulla 7 jaollisuutta tarkasteltaessa aloitetaan myös sillä, että merkitään luku lohkaisumenetelmän avulla. Seitsemällä jaolliset luvut saattavat erota kymmenpotensseista selvästi. Esimerkiksi $10 = 7 + 3, 100 = 98 + 2$ ($1\ 000 = 994 + 6, 10\ 000 = 9\ 996 + 4, 100\ 000 = 99\ 995 + 5, 1\ 000\ 000 = 999\ 999 + 1, 10\ 000\ 000 = 9\ 999\ 997 + 3, \ldots$). Myöskin 7 jaollisuutta selvitettäessä ollaan kiinnostuneita luvun kriittisen termin numeroiden summasta, mutta tietyillä kertoimilla. Luvut ryhmitellään kolmen numeron välein ja mikäli näiden ”jäännösten” summa on jaollinen luvulla 7, niin luku on jaollinen luvulla 7. Jäännökset lasketaan kolmen numeron palasissa, joissa ”kymmenten” paikalla oleva luku kerrotaan luvulla 3 ja ”satojen” paikalla oleva luku kerrotaan luvulla 2 ja nämä summataan ”ykkösten” paikalla olevan luvun kanssa. Toisin sanoen, mikäli kolmen numeron ryhmiin jaoteltujen summien summa on jaollinen luvulla 7, niin itse luku on jaollinen luvulla 7. [**14**][s.45-46].

Esimerkki 2.9. Selvitetään onko luku 9 653 jaollinen luvulla 7. Aloitetaan taas kirjoittamalla luku lohkaisumenetelmän avulla, siten että lohkotaan luvut kolmen numeron välein.

$$\begin{aligned} 9\,653 &= 9 \cdot 1\,000 + 653 = 9 \cdot (1001 - 1) + 6 \cdot (98 + 2) + 5 \cdot (7 + 3) + 3 \\ &= 1001 \cdot 9 + 6 \cdot 98 + 5 \cdot 7 - 9 + 6 \cdot 2 + 5 \cdot 3 + 3 \\ &= \underbrace{(1001 \cdot 9 + 6 \cdot 98 + 5 \cdot 7 - 1 \cdot 7)}_{lohkaisutermi} + \underbrace{(-2 + 6 \cdot 2 + 5 \cdot 3 + 3)}_{kriittinen\ termi} \end{aligned}$$

Nyt kun lasketaan kriittisen termin luvut yhteen saadaan $-2+12+15+3 = 28$, mikä on jaollinen luvulla 7, eli luku 9 653 on jaollinen luvulla 7.

Lause 2.10 (Jakojäännösyhtälö). *Jos $a, b \in \mathbb{Z}$ ja $b \neq 0$, niin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että*

$$a = qb + r, \tag{6}$$

missä $0 \leq r < |b|$. Luku b siis jakaa luvun a q-kertaa ja jakojäännös on r.

Todistus. Tutkitaan muotoa $a - qb$ olevia ei-negatiivisia kokonaislukuja ja etsitään niistä pienin. Olkoon pienin luku $r = a - qb$. Luvun r valinnan nojalla tiedetään että $r \geq 0$. Jos $r \geq b > 0$, niin

$$r - b = a - qb - b = a - (q + 1)b,$$

mikä olisi pienempi kuin r, mikä on ristiriita kun $b > 0$ ja näin ollen $a = qb + r$. Toisaalta jos $r \geq -b > 0$, niin

$$r - (-b) = a - qb + b = a - (q - 1)b,$$

mikä olisi myös pienempää kuin r, mikä on ristiriita kun $b < 0$ ja näin ollen $0 \leq r < |b|$.

Todistetaan vielä yksikäsitteisyys; Olkoon

$$a = gb + r = q'b + r',$$

missä $0 \leq r < b$ ja $0 \leq r' < b$. Yhtälö voitaisiin kirjoittaa myös muotoon

$$r - r' = (q' - q)b, \text{ eli } b | r - r'.$$

Koska $0 \leq r < b$ ja $0 \leq r' < b$, niin $-b < r' - r < b$. Mistä seuraa että $r' - r = 0$ eli $r = r'$ ja koska $b > 0$ niin myös $q = q'$. Vastaavalla päättelyllä voitaisiin käsitellä myös tapaus $0 > b$. □

Esimerkki 2.11 (Ajatustenlukua osa 2). Kerrotaan kaverille, että osataan lukea hänen ajatuksiaan. Annetaan kaverille seuraavat ohjeet: ”Ajattele jotain lukua ja lisää siihen 11, kerro näin saatu luku kahdella ja vähennä tulosta 20. Kerro jäännös viidellä ja vähennä tulosta ajattelemasi luku kymmenkertaisena. Luku jonka saat on 10.” [**9**][s.209]

Selitys 2.12. Tarkastellaan syytä miksi viimeinen luku on 10. Alussa valitulla luvulla ei ole merkitystä lopputuloksen kannalta ja syy selviää kun tarkastellaan luvulle tehtäviä laskutoimituksia. Merkitään valittua lukua muuttujalla x ja kirjoitetaan

operaatiot matemaattisesti:

$$\begin{aligned}&((((x+11)\cdot 2)-20)\cdot 5)-10x\\&=(((2x+22)-20)\cdot 5)-10x\\&=((2x+2)\cdot 5)-10x\\&=(10x+10)-10x\\&=10\end{aligned}$$

2.1.3. Jaollisuus k-kantaisessa järjestelmässä. Seuraavaksi johdetaan yleisiä jaollisuussääntöjä, jotka toimivat k-kantaisessa lukujärjestelmässä. Jaollisuussääntöjä varten tarvitaan seuraavaksi esitettävät yhtälöt, jotka seuraavat suoraan yhtälöstä (5).

Jos valitaan luvut a ja b siten, että luonnollinen luku $a = k$, joka on lisäksi aidosti suurempi kuin luku 1 ja $b = 1$. Tällöin

$$k-1|k^n-1 \text{ jokaisella kokonaisluvulla } n. \tag{7}$$

Jos taas valitaan luvut siten, että $a = k, b = -1$, niin $a^n - b^n = k^n - (-1)^n$, missä jälkimmäinen termi on 1 tai -1 riippuen onko n parillinen vai pariton. Kummassakin edellisessä tapauksessa $a - b = k + 1$, mistä seuraa että

$$\begin{aligned}&k+1|k^n-1, \text{ kun } n \text{ on parillinen,}\\&k+1|k^n+1, \text{ kun } n \text{ on pariton.}\end{aligned} \tag{8}$$

Sitten varsinaisten jaollisuussääntöjen kimppuun. Kantaluvun jakajille sekä jollekin sen potenssin tekijälle jaollisuussäännöt löytyvät helposti kuten kymmenjärjestelmässäkin. Olkoon jakaja luku n ja luku k^r alhaisin kantaluvun potenssi jonka luku n jakaa. Tarkastellaan luvun t jaollisuutta luvulla n.

$$\begin{aligned}t =&a_s a_{s-1}\dots a_r a_{r-1}\dots a_{0_k}\\=&a_s k^s + a_{s-1}k^{s-1}+\dots+a_r k^r + a_{r-1}k^{r-1}+\dots+a_0,\end{aligned}$$

mistä voidaan lohkaisutermiin valita kaikki ne luvut, joissa potenssi on $\geq r$.

$$\underbrace{(a_s k^s + a_{s-1}k^{s-1}+\dots+a_r k^r)}_{lohkaisutermi} + \underbrace{(a_{r-1}k^{r-1}+\dots+a_0)}_{kriittinen\ termi},$$

koska k^r jakaa lohkaisutermin, niin myös luku n jakaa sen. Kriittinen termi merkitään k-järjestelmässä $a_{r-1}\dots a_0$, mikä on luvun viimeiset r numeroa.

Edellisen perusteella saadaan jaollisuussääntö, joka sanoo että:
Mikäli kantaluvun k potenssi k^r on jaollinen luvulla n, niin k-järjestelmässä esitetty luku on jaollinen luvulla n, jos sen r viimeistä numeroa muodostavat luvun joka on jaollinen luvulla n. [**14**][s.47-48].

Esimerkki 2.13. Selvitetään onko luku 8200_{12} jaollinen luvulla 8.
Koska $8200_{12} = 8\cdot 8^3 + 2\cdot 8^2 + 0\cdot 8^1 + 0$, niin voidaan todeta, että pienin 12 potenssi mikä on jaollinen luvulla 8, on $12^2 = 144$, eli tällöin riittää tarkastella kahta viimeistä luvun numeroa ja niiden muodostaman luvun jaollisuutta luvulla 8. Viimeiset kaksi numeroa ovat 00 ja koska mikä tahansa luku jakaa luvun 0, niin luku 8 jakaa kyseisen luvun, joten luku 8200_{12} on jaollinen luvulla 8.

Käydään läpi jaollisuussääntö kantaluvulle k, kun jakajana on $k-1$, joka vastaa kymmenjärjestelmän luvulla 9 (ja 3) jaollisuutta. Olkoon luku t samoin kuin edellisenkin säännön kohdalla ja olkoon luku n luvun $k-1$ tekijä (tai luku itse) eli $n|k-1$. Vähennetään luvun t tekijöistä jokaisesta potenssista k luku 1, eli $k-1, k^2-1, k^3-1, \ldots$, tällöin yhtälön (7) perusteella on erotukset jaollisia luvulla $k-1$ ja siten myös luvulla n. Eli

$$\begin{aligned} t =& a_s a_{s-1} \ldots a_1 \ldots a_{0_k} \\ =& a_s k^s + a_{s-1}k^{s-1} + \ldots a_1 k + a_0 \\ =& \underbrace{[a_s(k^s-1) + a_{s-1}(k^{s-1}-1) + \ldots a_1(k-1)]}_{lohkaisutermi} + \underbrace{(a_s + a_{s-1} + \cdots + a_1 + a_0)}_{kriittinen\ termi}. \end{aligned}$$

Mistä näemme että kriittinen termi on luvun t numerosumma k-järjestelmässä, tällöin saadaan sääntö:
k-järjestelmässä esitetty luku on jaollinen luvulla $k-1$, mikäli sen k-järjestelmässä esitetyn luvun numerosumma on jaollinen myös kyseisessä järjestelmässä. [**14**][s.49].

ESIMERKKI 2.14. Selvitetään onko luku 21310_8 jaollinen luvulla 7.
Koska jakajana oleva luku on kantajärjestelmään verrattuna muotoa $k-1$, riittää tarkastella onko luvun numerosumma luvulla 7 jaollinen 8-järjestelmässä.
2+1+3+1+0=7, joten luku on jaollinen luvulla 7.

Käydään vielä lopuksi jaollisuussääntö kantaluvulle k, kun jakajana on $k+1$. Olkoon edelleen luku t samoin kuin edellistenkin sääntöjen kohdalla ja olkoon luku n luvun $k+1$ tekijä (tai luku itse) eli $n|k+1$. Lohkaisutermin muodostamisessa käytetään hyväksi yhtälöä (8), mikä siis tarkoittaa sitä että jälkimmäisen termin etumerkki on - jos eksponentti n on parillinen ja + jos se on pariton. Toimitaan siis samalla tavalla kun 10-järjestelmässä jaettaessa luvulla 11. Luvulle se tarkoittaa siis, että

$$\begin{aligned} t =& a_s a_{s-1} \ldots a_1 a_{0_k} \\ =& a_0 + a_1 k + a_2 k^2 + \cdots + a_s k^s \\ =& \underbrace{[a_1(k+1) + a_2(k^2-1) + \cdots + a_s(k^s - (-1)^s]}_{lohkaisutermi} + \underbrace{(a_0 - a_1 + a_2 + \cdots + (-1)^s a_s)}_{kriittinen\ termi}. \end{aligned}$$

Kriittinen termi saadaan nyt laskemalla vuorotteleva numerosumma luvusta k-järjestelmässä, tällöin saadaan jaollisuudelle sääntö: *k-järjestelmässä oleva luku on jaollinen luvulla $k+1$ tai sen tekijällä, mikäli luvun vuorotteleva numerosumma on jaollinen samassa järjestelmässä kyseisellä luvulla.* [**14**][s.49-50].

ESIMERKKI 2.15. Selvitetään onko luku 2314_5 jaollinen luvulla 6.
Koska jakajana oleva luku on kantajärjestelmään verrattuna muotoa $k+1$, riittää tarkastella onko luvun vuorotteleva numerosumma luvulla 6 jaollinen 5-järjestelmässä.
$4-1+3-2=4$, joten luku ei ole jaollinen luvulla 6.

2.2. Alkuluvut

MÄÄRITELMÄ 2.16. Alkuluku on luonnollinen luku $n \in \mathbb{N}$, joka on jaollinen vain itsellään ja ykkösellä, kun $2 \leq n$.

Esimerkki 2.17. Alkulukujonon ensimmäiset (ja alle 100 pienemmät luvut) ovat

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Uuspythagoralaiset eivät pitäneet aina lukua 2 aitona alkulukuna, koska heidän mielestään luvut 1 ja 2 olivat parittomien ja parillisten lukujen synnyttäjiä [**2**][s.97].

Lause 2.18. *Alkulukuja on äärettömän monta.*

Todistus. Väite tarkoittaa sitä, että valitaanpa mikä tahansa äärellinen alkulukujoukko, niin silti löytyy joukon ulkopuolelta luku joka on alkuluku, eli ei minkään valitun alkulukujoukon alkion monikerta. Olkoon meillä valittu alkulukujoukko

$$S = p_1, p_2, \ldots, p_n,$$

missä $p_1, \ldots, p_n$ ovat alkulukuja (mutta niiden ei tarvitse välttämättä olla ensimmäisiä alkulukuja). Olkoon luku N, sellainen luku joka saadaan kertomalla kaikki joukon alkiot keskenään ja lisäämällä tuloon 1, eli

$$N = p_1 p_2 \ldots p_n + 1.$$

Tällöin luku N on joko itse alkuluku tai sillä on tekijänä vähintään yksi sellainen alkuluku, joka ei kuulu joukkoon S. Kummassakin tapauksessa on löydetty joukon S ulkopuolelta alkuluku ja näin ollen väite on todistettu. □

[**14**][s.25-26].

Eukleides todisti jo aikoinaan Elementassa että alkulukujen joukko on ääretön. Hänen todistuksensa erosi selvästi edellä esitetystä ja se esitellään seuraavaksi

Todistus. (Vaihtoehtoinen todistus Lauseelle 2.18) [**14**][s.27-28].
Olkoon $p_1, p_2, \ldots, p_k$ muotoa $3n + 2$ olevia alkulukuja ja $2 < p_1, \ldots, p_k$. Halutaan osoittaa että samaa muotoa olevia alkulukuja löytyy joukon $S = \{p_1, p_2, \ldots, p_k\}$ ulkopuolelta, joten tarkastellaan lukua

$$3 \cdot p_1 p_2 \ldots p_k + 2,$$

joka on siis muotoa $3n + 2$, eikä ole jaollinen millään joukon S alkiolla. Se ei ole myöskään jaollinen luvulla 2, koska edellinen termi on $2 < p_1, \ldots, p_k$ perusteella pariton. Jos N on itse alkuluku niin todistus on valmis. Jos taas ei ole, niin voidaan todeta että:

(1) N ei ole jaollinen luvulla kolme, joten myöskään mikään sen alkutekijöistä ei ole jaollinen kolmella.
(2) Jokainen luonnollinen luku, joka ei ole jaollinen luvulla kolme antaa jakojännökseksi luvun 1 tai 2. Tällöin kaikki luvut ovat joko muotoa $3n + 1$ tai $3n + 2$. Mikäli ne ovat jälkimmäistä muotoa, tarkoittaa se suoraan sitä, että on löydetty joukon S ulkopuolinen luku joka on alkuluku.
(3) Olkoon luvut $a = 3n' + 1$ ja $b = 3n'' + 1$, jolloin kumpikin on muotoa $3n + 1$, tällöin tulolle ab saadaan

$$\begin{aligned} ab &= (3n' + 1)(3n'' + 1) = 9n'n'' + 3n' + 3n'' + 1 \\ &= 3(3n'n'' + n' + n'') + 1, \end{aligned}$$

eli tulo on samaa muotoa kuin tulontekijät a ja b.

(4) Jos jokainen luvun N alkutekijä olisi muotoa $3n+1$, niin edellisen kohdan (3) perusteella tuloa toistamalla myös luku N olisi samaa muotoa $3n+1$, mikä ei päde sillä luku N on muotoa $3n+2$.
(5) Kohdan (4) perusteella luvulla N täytyy olla ainakin yksi muotoa $3n+2$ oleva alkutekijä q. Nyt koska joukon S alkiot eivät ole luvun N tekijöitä, niin alkuluku q ei voi olla mikään näistä, joten luvun q on oltava joukon S ulkopuolelta oleva muotoa $3n+2$ oleva alkuluku. Näin ollen väite on todistettu.

□

Vaikka tiedetään että alkulukuja on äärettömän paljon, silti matematiikot vuosien saatossa ovat yrittäneet keksiä ”kaavoja”, jolla pystyttäisiin tuottamaan/etsimään alkulukuja jatkuvasti. Eulerin kehittelemä polynomi oli x^2+x+41, mutta kaava toimii hyvin kun $0 \leq x \leq 39$, mutta kun $x = 40, 41$ ei polynomi tuota alkulukua [**6**][s. 18].

Esimerkki 2.19. Polynomi $P(x) = x^2 + x + 41$ tuottaa seuraavat luvut:
$P(0) = 41, P(1) = 43, P(2) = 47, P(3) = 53, P(4) = 61, P(5) = 71, P(6) = 83, P(7) = 97, P(8) = 113, P(9) = 131, P(10) = 151, P(11) = 173, P(12) = 197, P(13) = 223, P(14) = 251, P(15) = 281, P(16) = 313, P(17) = 347, P(18) = 383, P(19) = 421, P(20) = 461, P(21) = 503, \ldots, P(38) = 1523, P(39) = 1601, P(40) = 1681 = 41^2, P(41) = 1763 = 41 \cdot 43, P(42) = 1847, P(43) = 1933, \ldots$.
Seuraavan polynomin tuottama luku voidaan laskea itse asiassa siten että $P(n+1) = P(n) + 2 \cdot (n+1)$. Kun luvut 40 ja 41 sijoittaa polynomiin, on helppo huomata mikseivät ne tuota alkulukuja.

$$\begin{aligned} P(40) &= 40^2 + 40 + 41 \\ &= 40 \cdot 40 + 40 + 41 \\ &= 41 \cdot 40 + 41 = 41^2 \end{aligned}$$

$$\begin{aligned} P(41) &= 41^2 + 41 + 41 \\ &= 41 \cdot 41 + 41 + 41 \\ &= 43 \cdot 41 \end{aligned}$$

Alkulukuja käytetään hyödyksi muun muassa salausjärjestelmissä viestin salaamisessa. Vaikka alkuluvut sinänsä ovat yksinkertainen asia, niin niihin liittyy vielä ratkaisemattomia ongelmia. Yksi tälläinen on *Goldbachin konjektuuri*[1] , johon palataan tarkemmin myöhemmin kappaleessa 5.2.

[1]konjektuurilla tarkoitetaan matemaattista väitettä, jota ei ole pystytty todistamaan todeksi tai epätodeksi

LUKU 3

Alkulukuja ja alkuluvuilla ilmaisua

Lukuja voidaan ilmaista monin eri tavoin toisten lukujen avulla. Jokainen luonnollinen luku voidaan esimerkiksi esittää alkulukujen tulona, kuten osoitetaan heti tämän luvun alussa. Alkulukuja voidaan puolestaan etsiä erilaisten sääntöjen avulla, joissa nimenomaan tarkastellaan lukujen jaollisuutta. Kongruenssiyhtälöt ovat yksi tässä luvussa käsiteltävä jaollisuuden "apuväline".

3.1. Alkulukuesitys

MÄÄRITELMÄ 3.1 (Alkutekijäesitys). Luonnollisen luvun n alkutekijäesitys on

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k},$$

missä $p_1 < \dots < p_k$ ovat alkulukuja ja $e_1, \dots, e_k \in \mathbb{N}$.

LAUSE 3.2 (Aritmetiikan peruslause). *Jokainen luku on joko alkuluku tai alkulukujen tulo, missä tulo on tulontekijöiden järjestystä vaille yksikäsitteinen.*

TODISTUS. **Oletus:** $B(a)$ tarkoittaa lausetta "a voidaan esittää tekijöiden järjestystä vaille yksikäsitteisesti alkulukujen tulona".

Väite: $\forall\ a \geq 2, a \in \mathbb{N}\ : B(a)$

Todistus: Induktiolla luvun $a > 1$ suhteen.

Perusaskel: $B(2)$ on voimassa, sillä mikä tahansa alkuluku on itsessään yksikäsitteinen alkulukujen tulona.

Induktio-oletus: Oletetaan että $B(a)$ pätee, kun $2 \leq a \leq k-1$.

Induktioväite: $B(k)$ pätee

Induktiotodistus: Luku k on joko alkuluku tai yhdistetty luku.

- Jos k on alkuluku, niin se on itsessään alkulukujen tulo.
- Jos k on yhdistetty luku se voidaan esittää kahden itseään pienemmän luvun a ja b tulona. Induktio-oletuksen mukaan a ja b voidaan esittää alkulukujen tulona, joten koska $k = a * b$, se voidaan esittää alkulukujen tulona.
  Joten induktioperiaatteen nojalla väite pätee. Todistetaan alkulukuesityksen yksikäsitteisyys erikseeen.

□

Todistus. (Alkulukuesityksen yksikäsitteisyys). Väitteen mukaan alkulukuesitys on yksikäsitteinen, joten todistetaan tämä antiteesilla. [**14**][s.23-25].

Antiteesi: On olemassa luku N, jolle on olemassa kaksi eri alkulukuesitystä ja olkoon luku N pienin tällainen luku. Eli

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \tag{1}$$

missä p_j ja q_k ovat alkulukuja. Tällöin $p_j \neq q_k$, koska muuten alkuluku p_j jakaisi toisella puolella olevan luvun, jolloin luvulla p_j olisi voinut supistaa kummankin puolen, eikä näin ollen luku N olisi pienin luku jolla on kaksi eri alkutekijäesitystä.

Olkoon $p_1 < q_1$ sekä luku

$$M = p_1 q_2 \dots q_s. \tag{2}$$

Nyt jos tarkastellaan erotusta $N - M = q_1 q_2 \dots q_s - p_1 q_2 \dots q_s = (q_1 - p_q) q_2 \dots q_s$, mikä on aidosti positiivinen, koska $p_1 < q_1$. Jaetaan myös erotus $q_1 - p_1$ alkutekijöihin, jolloin saadaan $q_1 - p_1 = t_1 t_2 \dots t_l$, missä $t_1, \dots, t_l$ ovat alkulukuja. Todetaan että oikea puoli ei voi olla jaollinen luvulla p_1, koska jos näin olisi, niin olisi myöskin luku $q_1 = p_1 + t_1 \dots t_l$ sillä jaollinen ja näin ei voi olla, koska $p_1 \neq q_1$ ja q_1 on alkuluku. Nyt voimme kirjoittaa siis erotukselle alkutekijäesityksen

$$N - M = t_1 \dots t_l q_2 \dots q_s, \tag{3}$$

missä siis mikään alkulukuesitysten alkuluvuista ei ole p_1. Toisaalta koska p_1 on tekijänä luvulle N (1) ja myös luvulle M (2), niin täytyy sen olla myös luvun $N - M$ tekijä. Merkitään nyt lukua $N - M = p_1 a$, missä luvun a alkulukuesitys on

$$a = u_1 \dots u_v,$$

missä siis $u_1, \dots, u_v$ ovat alkulukuja. Nyt voimme kirjoittaa luvun $N - M$ muodossa

$$N - M = p_1 u_1 \dots u_v. \tag{4}$$

Nyt alkutekijäesitykset (3) ja (4) eroavat toisistaan, sillä jälkimmäinen sisältää luvun p_1, mutta edellinen ei. Näin ollen on löydetty luvulle $N - M$, joka on pienempi kuin luku N, kaksi erilaista alkutekijäesitystä, mikä on ristiriita sen kanssa että luku N olisi pienin tällainen luku jolle löytyy kaksi erilaista alkutekijäesitystä. Näin ollen antiteesi ei voi pitää paikkansa vaan varsinainen väite on tosi. □

Alkuluvut ovat siis (luonnollisten) lukujen rakennuspalikoita [**1**][s.257]. Jokainen kokonaisluku on siis jaollinen vähintään luvulla 1 ja luvulla itse, sekä näiden vastaluvuilla [**13**][s. 5].

Esimerkki 3.3. Luvun 27388 alkulukuesitys on
$27388 = 2^2 \cdot 41 \cdot 167$

Esimerkki 3.4. Luku 1 274 953 680 on mielenkiintoinen luku, sillä se on jaollinen kaikilla luvuilla $1 - 16$ ja sisältää kaikki kymmenjärjestelmän eri numerot [**16**][s.20]. Jaollisuus ei ole niin yllättävä, kun kirjoitetaan luku alkutekijäesityksenä:

$$1\ 274\ 953\ 680 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 61$$

Sille meneekö jonkin kokonaislukujen jako tasan löytyy helppo tapa alkulukuesitystä hyödyntäen, joskin suurilla luvuilla se on työläs, eikä välttämättä järkevinkään.

3.1.1. Bertrandin postulaatti. [6][s. 18-21].

LAUSE 3.5 (Bertrandin postulaatti eli Tšebyšovin lause).
Olkoon $n \in \mathbb{Z}_+$. Tällöin löytyy vähintään yksi alkuluku p, jolle pätee

$$n < p \leq 2n. \tag{5}$$

Todistetaan ennen varsinaista lausetta yksi aputulos.

LEMMA 3.6. *Mille tahansa $n \geq 1$,*

$$\sum_{p \leq n} \log p < 2n \ \log 2. \tag{6}$$

Summataan siis yli kaikkien lukua n pienempien alkulukujen p.

TODISTUS. Olkoon

$$M = \binom{2m+1}{m} = \frac{(2m+1)(2m)\dots(m+2)}{m!}$$

binomikerroin (vrt. Määritelmä 4.33), joka on kokonaisluku. Kerroin M esiintyy kahdesti binomikehitelmässä $2^{2m+1} = (1+1)^{2m+1}$, joten $M < 2^{2m}$. Jos $m+1 < p \leq 2m+1$ jollekin alkuluvulle p, niin p jakaa luvun M osoittajan muttei nimittäjää, joten $\prod_{p \in A(m)} p$ jakaa luvun M, missä $A(m)$ on niiden alkulukujen p joukko, joille $m+1 < p \leq 2m+1$. Tästä seuraa että

$$\sum_{p \leq 2m+1} \log p - \sum_{p \leq m+1} \log p = \sum_{p \in A(m)} \log p \leq \log M < 2m \log \ 2. \tag{7}$$

Todistetaan väite (6) induktiolla.

Perusaskel: Väite pätee kun $n \leq 2$, eli

$$\sum_{p \leq 2} \log p = \log 2 < 2 \cdot 2 \log 2 = 4 \log 2.$$

Induktio-oletus: Väite pätee kaikilla $n \leq k-1$.

Induktioväite: Väite pätee kun $n \leq k$. Jos k on parillinen, niin

$$\sum_{p \leq k} \log p = \sum_{p \leq k-1} \log p \underbrace{<}_{ind.ol} 2(k-1) \log 2 < 2k \log 2.$$

Jos k on pariton, merkitään $k = 2m+1$ ja tällöin

$$\sum_{p \leq 2m+1} \log p = \sum_{p \leq 2m+1} \log p \ - \sum_{p \leq m+1} \log p \ + \sum_{p \leq m+1} \log p$$

$$\underbrace{<}_{(7)} 2m \ \log 2 + 2(m+1) \ \log 2 = 2(2m+1) \log 2 = 2k \ \log 2,$$

silloin kun $m+1 < k$, joten induktio-oletusta voidaan käyttää. Tällöin epyhtälö (6) pätee kaikilla n.

□

Sitten varsinaisen lauseen 3.5 todistus

TODISTUS. Olkoon mille tahansa reaaliluvulle x, lattiafunktio $\lfloor x \rfloor$ [1]. Olkoon lisäksi p mikä tahansa alkuluku. Tällöin

$$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \dots$$

on suurin p:n potenssi, joka jakaa luvun $n!$. Siis lattiafunktio $\lfloor \frac{n}{p} \rfloor$ kertoo montako luvun p monikertaa esiintyy kertomassa $n!$, eli saadaan kertoman $n!$ jakajaksi vastaava määrä luvun p potensseja. Lattiafunktio $\lfloor \frac{n}{p^2} \rfloor$ kertoo montako p^2 monikertaa esiintyy kertomassa $n!$. Nämä ovat tietenkin myös luvun p monikertoja, koska luvulla p on eksponenttina luku 2, mutta saadaan myös jokaista monikertaa kohti uusi luvun p potenssi kertomaan $n!$. Sama pätee edelleen myös seuraaville lattiafunktioille, joille saadaan uusia luvun p potensseja. Jossain vaiheessa käy kuitenkin niin että $p^k > n$, eli lattiafunktio ei palauta mitään lukua ja summa ei enää kasva ja siksi summa on äärellinen. Kiinnitetään $n \geq 1$ ja olkoon

$$N = \prod_{p \leq 2n} p^{k(p)}$$

alkulukuhajotelma luvusta $N = \frac{(2n)!}{(n!)^2}$. Se kuinka monta kertaa annettu alkuluku p jakaa luvun N on ero sen välillä montako kertaa p jakaa luvun $(2n)!$ ja montako kertaa luvun $(n!)^2$, joten

$$k(p) = \sum_{m=1}^{\infty} (\lfloor \frac{2n}{p^m} \rfloor - 2\lfloor \frac{n}{p^m} \rfloor), \tag{8}$$

jossa jokaisen termin summa on joko 0 tai 1 riippuen siitä onko $\lfloor \frac{2n}{p^m} \rfloor$ parillinen $(= 0)$ vai pariton $(= 1)$. Jos $p^m > 2n$ termi on yksinkertaisesti 0, joten

$$k(p) \leq \lfloor \frac{\log\ 2n}{\log\ p} \rfloor. \tag{9}$$

Todistetaan väite käänteisellä päättelyllä. Oletetaan että on joku $n \geq 1$ jolle ei ole alkulukua joka toteuttaisi ehdon (5). Olkoon nyt p alkulukutekijä luvulle $N = \frac{(2n)!}{(n!)^2}$. Tällöin oletuksemme mukaan $p < n$ ja $k(p) \geq 1$. Jos

$$\frac{2}{3}n < p \leq n$$

tällöin

$$2p \leq 2n < 3p \text{ ja } p^2 > \frac{4}{9}n^2 > 2n,$$

kun $n > 5$, joten yhtälöstä (8) saadaan

$$k(p) = \lfloor \frac{2n}{p} \rfloor - 2\lfloor \frac{n}{p} \rfloor = 2 - 2 = 0.$$

[1] Lattiafunktion palauttama luku on suurin mahdollinen kokonaisluku, mikä on pienempi tai yhtä suuri kuin reaaliluku x.

Päätellään että $p \leq \frac{2}{3}n$ kaikilla luvun N alkulukutekijöillä p. Tästä seuraa, että

$$\sum_{p|N} \log\ p \leq \sum_{p \leq \frac{2n}{3}} \log\ p \leq \frac{4}{3} n\ \log\ 2 \tag{Ƶ}$$

Lemman 3.6 perusteella. Jos $k(p) \geq 2$ niin (9) takia

$$2 \log p \leq k(p) \log p \leq \log 2n$$

joten $p \leq \sqrt{2n}$ ja tällöin alkuluvulle p on korkeintaan $\sqrt{2n}$ vaihtoehtoa. Siten

$$\sum_{k(p) \geq 2} k(p) \log p \leq \sqrt{2n} \log 2n.$$

Yhdessä epäyhtälön (Ƶ) kanssa edellinen voidaan kirjoittaa

$$\begin{aligned} \log N &\leq \sum_{k(p)=1} \log p + \sum_{k(p) \geq 2} k(p) \log p \leq \sum_{p|N} \log p + \sqrt{2n} \log 2n \\ &\leq \frac{4}{3} \log 2 + \sqrt{2n} \log 2n. \end{aligned} \tag{Ɛ}$$

Nyt N on suurin kerroin binomille $2^{2n} = (1+1)^{2n}$, siten

$$2^{2n} = 2 + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{2n-1} \leq 2nN.$$

Sijoitetaan estimaatti epäyhtälöön (Ɛ), jolloin saadaan

$$2n \log 2 \leq \frac{4}{3} n \log 2 + \log 2n + \sqrt{2n} \log 2n. \tag{10}$$

On selvää, että epäyhtälö (Ɛ) ei ole voimassa suurilla arvoilla n. Esimerkiksi laskemalla nähdään että epäyhtälö (10) ei päde kun n on suurempi kuin 500.

Tästä seuraa että jos $n > 500$, niin löytyy alkuluku joka toteuttaa epäyhtälön (5). Laskemalla voidaan varmistaa että (5) pätee kaikilla $n \leq 500$. □

3.1.2. Mersennen alkuluvut. [**6**][s. 23-24].

Alkulukuja, jotka ovat muotoa $2^n - 1$, sanotaan *Mersennen alkuluvuiksi* 1600-luvun taitteessa eläneen, luvut ”löytäneen” ranskalaisen munkin Marin Mersennen mukaan. Suurimmat tunnetut alkuluvut ovat kautta historian muutamaa poikkeusta lukuunottamatta olleet Mersennen alkulukuja. [**1**][s.267-269]. Tämän hetkinen suurin alkuluku on tammikuussa 2013 löydetty $2^{57885161} - 1$ [**17**].

Mersennen alkulukujen esittäminen binäärilukuna on helppoa, sillä luku 2^n on binäärilukuna 1 ja n kappaletta nollia, eli esimerkiksi $8 = 2^3$ on binäärilukuna 1000. Täten koska Mersennen alkuluvut ovat muotoa $2^n - 1$ niin luvuissa on n kappaletta ykkösiä peräkkäin, eli esimerkiksi $31 = 2^5 - 1$ eli binäärilukuna 11111. [**1**][s.270].

Lause 3.7. *Jos $2^n - 1$ on alkuluku, niin n on alkuluku.*

Todistus. Todistetaan käänteinen väite siten, että luvun n ollessa yhdistetty luku myöskin luvun $2^n - 1$ täytyy olla yhdistetty luku. Jos $n = ab$, missä $a, b > 1$,

niin silloin

$$2^n - 1 \underbrace{=}_{\text{Lause 2.4}} (2^a - 1)(2^{n-a} + 2^{n-2a} + \cdots + 2^a + 1),$$

joten $2^n - 1$ on yhdistetty luku. □

Kaikki muotoa $2^p - 1$ olevat luvut eivät ole kuitenkaan alkulukuja vaikka p olisikin alkuluku. Esimerkiksi kun $p = 11$ niin $2^{11} - 1 = 2047 = 23 \cdot 89$

LAUSE 3.8. *Olkoon $M_n = 2^n - 1$. Tällöin jokaiselle luonnolliselle luvulle $n \neq 6$, $n > 1$, Mersennen luvulla M_n on primitiivijakaja (=jakajana alkuluku, joka ei ole jakajana missään muussa pienemmässä Mersennen luvussa).*

Ei todisteta lausetta, mutta voidaan todeta seuraavasta taulukosta että väite näyttäisi pätevän.

n	M_n	alkutekijäesitys
2	3	$\mathbf{3}$
3	7	$\mathbf{7}$
4	15	$3 \cdot \mathbf{5}$
5	31	$\mathbf{31}$
6	63	$3^2 \cdot 7$
7	127	$\mathbf{127}$
8	255	$3 \cdot 5 \cdot \mathbf{17}$
9	511	$7 \cdot \mathbf{73}$
10	1023	$3 \cdot \mathbf{11} \cdot 31$
⋮	⋮	⋮

3.2. Suurin yhteinen tekijä

MÄÄRITELMÄ 3.9. Mikäli kokonaisluvuille a ja b löytyy sellainen luku d, joka jakaa kummankin luvun, eli $d|a$ ja $d|b$, niin luku d on näiden *yhteinen tekijä*. Luku d on *suurin yhteinen tekijä* mikäli jokainen lukujen a ja b yhteinen tekijä jakaa luvun d. [**4**][s. 83].

LAUSE 3.10. *Jokaiselle kokonaisluvulle a ja b on olemassa suurin yhteinen tekijä d, eli syt(a,b)=d (eng. gcd(a,b)=d).*

TODISTUS. Sovitaan aluksi että a on suurempi luvuista, eli $a \geq b$. Jos luku b jakaa luvun a, niin $syt(a, b) = b$. Oletetaan että luvuilla a ja b ei ole yhteistä (suurinta) tekijää ja valitaan näistä pareista joku sellainen, missä a on pienin mahdollinen. Tällöin $1 < b < a$, silloin kun luku b ei jaa lukua a. Tällöin myös $1 \leq a - b < a$ ja lukuparin $a - b$ ja b suurin yhteinen tekijä on d. Tällöin mikä tahansa lukujen a ja b yhteinen jakaja jakaa luvun $a-b$ ja siten myös luku d jakaa luvun $(a-b)+b = a$, siitä taas seuraa että luku d on suurin yhteinen tekijä luvuille a ja b. Tämä on kuitenkin ristiriita, joten lause on todistettu. [**4**][s. 84]. □

Suurin yhteinen tekijä voidaan määrittää myös useammalle kuin kahdelle numerolle kerrallaan täysin samalla periaatteella, eli kaksi numeroa kerrallaan. Tällöin aina

yhden lukuparin suurimman tekijän selvittämisen jälkeen otetaan uusi luku, jota verrataan edellä saatuun suurimpaan yhteiseen tekjään ja toistetaan kunnes jokainen luku on käyty läpi.

Suurimmalle yhteiselle tekijälle pätee siis kolme ominaisuutta:

- d on positiivinen kokonaisluku,
- d on lukujen $a_1, a_2, \ldots, a_n$ yhteinen tekijä,
- d on jaollinen jokaisella lukujen $a_1, a_2, \ldots, a_n$ yhteisellä tekijällä.

[**13**][s. 8].

Mikäli $syt(a, b) = 1$, niin luvut a ja b ovat joko alkulukuja tai luvut eivät ole jaollisia samoilla (alku)luvuilla, joten ne ovat keskenään jaottomia [**4**][s. 85].

3.2.1. Pienin yhteinen jaettava.

LAUSE 3.11. *Jokaiselle kokonaisluvulle a ja b on olemassa pienin yhteinen jaettava d, eli pyj(a,b)=m (eng. lcm(a,b)=m).*

TODISTUS. Sovitaan taas aluksi että luku a on suurempi luvuista a ja b. Jos luku b jakaa luvun a, niin $pyj(a, b) = a$. Jos on niin että luku b ei jaa lukua a, niin pienin yhteinen jaettava on sellainen pienemmän luvun b monikerta, jonka alkulukuesitys sisältää suuremman luvun alkulukuesityksen, eli jokaisella lukuparilla tällainen luku on ainakin ab, koska $a|ab$ ja $b|ab$ jaollisuuden määritelmän (2.3) (iii) kohdan perusteella. □

Pienimmälle yhteiselle jaettavalle pätee myöskin kolme ominaisuutta, jotka ovat:

- m on positiivinen kokonaisluku,
- m on lukujen $a_1, a_2, \ldots, a_n$ yhteinen jaettava,
- m on jakaa jokaisen lukujen $a_1, a_2, \ldots, a_n$ yhteisen jaettavan.

[**13**][s. 13].

Helpoiten pienimmän yhteisen jaettavan etsiminen onnistuu alkulukuesityksen avulla, jos kyse on kohtuullisen pienistä luvuista.

LAUSE 3.12. *Jokaiselle $a, b \in \mathbb{N}$, pätee*

$$syt(a, b) \cdot pyj(a, b) = ab \tag{11}$$

TODISTUS. Olkoon lukujen a ja b alkutekijäesitykset $a = p_1 p_2 \ldots p_n$ ja $b = q_1 q_2 \ldots q_m$. Tällöin jos $p_i \neq q_j$ kaikilla $i, j \in \mathbb{N}$, niin $syt(a, b) = 1$ ja $pyj(a, b) = ab$, joten väite pätee selvästi.

Oletetaan että $syt(a, b) = c > 1$, jolloin löytyy $p_1 \ldots p_k = c = q_1 \ldots q_l$, missä $k, l \in \mathbb{N}$ ja alkutekijäesityksen yksikäsitteisyyden perusteella luvuilla a ja b on yksi tai useampi yhteinen tekijä. Olkoon $pyj(a, b) = d$. Koska pienimmän yhteisen jaettavan d on oltava jaollinen kummallakin luvulla a ja b, pitää sen alkutekijäesitys sisällään kummankin luvun a ja b (eri) alkutekijät, jolloin
$p_1 p_2 \ldots p_n q_{l+1} \ldots q_m = d = q_1 q_2 \ldots q_m p_{k+1} \ldots p_n$.
Tällöin siis
$syt(a, b) \cdot pyj(a, b) = (p_1 \ldots p_k) \cdot (q_1 q_2 \ldots q_m p_{k+1} \ldots p_n) = p_1 \ldots p_n q_1 q_2 \ldots q_m = ab$ □

ESIMERKKI 3.13. Olkoon luvut 3150 ja 660. Osoitetaan että edellinen lause pätee näille luvuille. Koska kyseessä pienet luvut, voidaan helposti kirjoittaa niiden alkutekijäesitykset, eli $3150 = 2 \cdot 3^2 \cdot 5^2 \cdot 7$ ja $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$. Alkutekijäesityksistä nähdään

helposti että $syt(3\,150, 660) = 30 = 2{\cdot}3{\cdot}5$ ja $pyj(3\,150, 660) = 69\,300 = 2^2{\cdot}3^2{\cdot}5^2{\cdot}7{\cdot}11$. Sijoitetaan tarvittavat arvot yhtälöön (11), jolloin saadaan

$$syt(3150, 660) \cdot pyj(3150, 660) = 30 \cdot 69\ 300 = 2\ 079\ 000 = 3150 \cdot 660$$

Olemme puhuneet tähän asti, että Määritelmän (2.3) ominaisuudet (i)-(v) pätevät luonnollisille luvuille ja positiivisille kokonaisluvuille, mutta ominaisuudet pätevät kaikille kokonaisluvuille muutamilla lisäehdoilla. Ominaisuuden (iv) osalta vaadimme että $c \neq 0$ ja ominaisuuden (v) osalta sallimme ratkaisuksi $b = \pm a$. Lisäksi kokonaisluvuille on voimassa seuraavat lisäominaisuudet:

(vi) $a|0 \quad \forall a,$
(vii) $jos\ 0|a,\ niin\ a = 0,$
(viii) $jos\ c|a,\ ja\ c|b,\ niin\ c|ax + by \quad \forall x,\ y.$

[**4**][s. 87].

Tähän asti olemme käytännössä tarkastellut lukuja, jotka ovat jaollisia täsmälleen jollain tietyllä luvulla. Laajennetaan tarkastelua siten, että luvut eivät olekaan jaollisia, vaan niihin jää jakojäännös.

3.3. Bézout'n yhtälö

Jos a ja b ovat mielivaltaisia kokonaislukuja siten, että $b < a$ ja $b \neq 0$, niin on olemassa yksikäsitteiset kokonaisluvut q ja r, niin että

$$a = qb + r, \quad 0 \leq r < |b|. \tag{12}$$

Itse asiassa qb on suurin luvun b sisältävä kerroin, joka ei ylitä lukua a. Lukujen a ja b jakolaskussa kokonaisluku q on osamäärä ja r jakojäännös (Vrt. Lause 2.10).

Voidaan myös löytää kokonaisluvuille a ja b, sellaiset luvut että kun $b \neq 0$, niin on olemassa kokonaisluvut q ja r, niin että

$$a = qb + r, \quad |r| \leq \frac{|b|}{2}. \tag{13}$$

Itse asiassa qb on lähin kerroin b:ltä a:lle. Luvut q ja r eivät ole yksikäsitteiset, mikäli luku a on on täsmälleen kahden peräkkäisen luvun b kertoimen puolivälissä.

Kummallekin edelliselle jakoalgoritmille on käyttötarkoituksensa. Ollaan puolueettomia ja käytetään vain tietoa että

$$a = qb + r, \quad |r| < |b|. \tag{14}$$

Eukleideen algoritmillä voidaan selvittää kahden kokonaisluvun suurin yhteinen tekijä.

3.3.1. Eukleideen algoritmi. Olkoon $r_0, r_1 \in \mathbb{N}, r_1 \neq 0$ ja kokonaislukujen jakoyhtälön (2.10) perusteella yksikäsitteiset luvut $q_1, r_2 \in \mathbb{N}$ siten, että on jakoyhtälö

$$r_0 = q_1 r_1 + r_2, \tag{15}$$

missä $0 \leq r_2 < r_1$.

Nyt voidaan jakoyhtälön osamäärä ja jakojäännös ilmaista $q_1 = \lfloor \frac{r_0}{r_1} \rfloor$, kun $r_1 \neq 0$ ja $r_2 = r_0 - q_1 r_1 = r_0 - r_1 \lfloor \frac{r_0}{r_1} \rfloor$. Toistamalla jakoyhtälöä (15) siten, että vaihdetaan aina

jaettavan paikalle jakaja ja jakajan paikalle saatu jakojäännös kunnes jakojäännös on 0, löydetään luvut $l, q_i, r_i \in \mathbb{N}, 1 \leq i \leq l$, siten, että $0 \leq r_{i-1} < r_1$, kun $1 \leq i \leq l$ ja

$$\begin{cases} r_0 &= q_1 r_1 + r_2, \\ r_1 &= q_2 r_2 + r_3, \\ &\vdots \\ r_{l-2} &= q_{l-1} r_{l-1} + r_l, \\ r_{l-1} &= q_l r_l + 0. \end{cases}$$

Eukleideen algoritmilla saatu viimeinen nollasta eroava luku r_l on lukujen r_0 ja r_1 suurin yhteinen tekijä eli $r_l = syt(r_0, r_1)$. Suurin yhteinen tekijä voidaan siis esittää muodossa $sr_0 + tr_1 = r_l$, mikä on itse asiassa *Bézout'n yhtälö*.

LAUSE 3.14 (Bezout'n yhtälö). *Olkoon $r_0, r_1 \in \mathbb{Z}, a \neq 0$. Tällöin on $t, s \in \mathbb{Z}$, joille*

$$syt(r_0, r_1) = sr_0 + tr_1.$$

TODISTUS. Jos $r_0 = r_1$, niin $syt(r_0, r_1) = |r_0|$. Oletetaan, että $r_0 > r_1$ ja lisäksi voidaan olettaa että $r_0, r_1 \in \mathbb{N}$, koska jos jompikumpi on negatiivinen, saadaan se positiiviseksi kertomalla s tai t luvulla (-1).

Jos $r_1 | r_0$, niin $syt(r_0, r_1) = r_1$ ja $r_0 = kr_1$, jollakin $k \in \mathbb{N}$ ja $k \geq 2$. Tällöin

$$r_1 = kr_1 - (k-1)r_1 = r_0 - (k-1)r_1.$$

Jos taas $r_1 \nmid r_0$, niin Eukleideen algoritmilla "peruuttaen" saadaan kertoimet s ja t. □

ESIMERKKI 3.15. Selvitetään Eukleideen algoritmilla $syt(234, 46)$, sekä Bézout'n yhtälön kertoimet luvuille 234 ja 46.

$$\begin{aligned} 234 &= 5 \cdot 46 + 4 \\ 46 &= 11 \cdot 4 + 2 \\ 4 &= 2 \cdot 2. \end{aligned}$$

Joten $syt(234, 46) = 2$. Selvitetään kertoimet s ja t laskemalla "takaperin".

$$\begin{aligned} syt(234, 46) = 2 &= 46 - 11 \cdot 4 \\ &= 46 - 11(234 - 5 \cdot 46) \\ &= 56 \cdot 46 - 11 \cdot 234. \end{aligned}$$

MÄÄRITELMÄ 3.16 (Diofantoksen yhtälö). Olkoon $a, b, c, x, y \in \mathbb{Z}$. Yhtälöä

$$ax + by = c \tag{16}$$

sanotaan Diofantoksen yhtälöksi.

LAUSE 3.17. *Jokaisella kokonaisluvulla a ja b on olemassa suurin yhteinen tekijä $d = syt(a, b)$. Lisäksi mille tahansa kokonaisluvulle c löytyy kokonaisluvut x ja y siten, että*

$$ax + by = c \tag{17}$$

jos ja vain jos luku d jakaa luvun c.

TODISTUS. "⇒"Suurimman yhteisen tekijän määritelmän 3.9 ja Bézout'n yhtälön 3.14 perusteella voidaan todeta että luvuille a, b ja c on olemassa luvut x ja y jos $syt(a, b)|c$.

Olkoon luku $syt(a, b) = d$, mistä seuraa että $a = da_1$ ja $b = db_1$ ja yhtälö voidaan kirjoittaa muotoon

$$da_1x + db_1y = d(a_1x + b_1y) = c,$$

jolloin selvästi $d|c$.

"⇐"Jos taas $d = syt(a, b)|c$, niin $c = dc_1$ ja määritelmän 3.9 ja Lauseen 3.14 perusteella löydetään kokonaisluvut m ja n, siten että $d = am + bn$, mistä seuraa että

$$c = dc_1 = (am + bn)c_1 = amc_1 + bnc_1.$$

Mistä seuraa että väite pätee. □

Diofantoksen yhtälön ratkaisu saadaan ratkaistua nimenomaan Eukleideen algoritmilla.

3.4. Kongruenssit

MÄÄRITELMÄ 3.18. Kokonaisluvut a ja b ovat *kongruentteja* modulo n

$$a \equiv b \mod n, \tag{18}$$

jos erotus $a - b$ kuuluu moduloon (n), eli jos erotus on jaollinen luvulla n, $n|a - b$.

[**13**][s.21].

ESIMERKKI 3.19.

$$21 \equiv 5 \mod 8, \qquad 21 \equiv -3 \mod 4, \qquad 21 \equiv 38 \mod 17.$$

LEMMA 3.20 (Ekvivalenssirelaatio). *Edellisestä määritelmästä seuraa suoraan, että kongruenssi on ekvivalenssirelaatio, jolloin kokonaisluvuille $a, b, c \in \mathbb{Z}$ on voimassa*

(i) $a \equiv a \mod n$ *kaikilla* a, m.
(ii) *Jos* $a \equiv b \mod n$, *niin* $b \equiv a \mod n$.
(iii) *Jos* $a \equiv b \mod n$ *ja* $b \equiv c \mod n$, *niin* $a \equiv c \mod n$.

TODISTUS. Lemman väitteiden todistaminen onnistuu suoraan määritelmän 3.18 perusteella.
(i): $a - a = 0 = n \cdot 0$. OK.
(ii): Jos $n|a - b$, niin pätee myös $n|b - a = -(a - b)$. OK.
(iii): Jos $n|a - b$ ja $n|b - c$, niin tällöin myös $n|a - c = (a - b) + (b - c)$. OK. □

[**4**][s.106].

LEMMA 3.21. *Kongruenttien lukujen summat, erotukset ja tulot ovat kongruentteja.*

(i) *Jos* $a \equiv b \mod n$ *ja* $a' \equiv b' \mod n$, *niin* $a \pm a' \equiv b \pm b' \mod n$.
(ii) *Jos* $a \equiv b \mod n$ *ja* $a' \equiv b' \mod n$, *niin* $aa' \equiv bb' \mod n$.

[**4**][s.106].

TODISTUS. Myös tämän lemman kohtien todistaminen onnistuu määritelmän 3.18 perusteella.

Väitteen mukaan siis modulo n sisältää lukujensa $a-b$ ja $a'-b'$ summan ja erotuksen:

(i): Jos $n|a-b$ ja $n|a'-b'$, niin $n|(a+a')-(b+b') = (a-b)+(a'-b')$ ja toisaalta $n|(a-a')-(b-b') = (a-b)-(a'-b')$. Yhteen yhtälöön kirjoitettuna, kun modulo n niin: $(a-b)\pm(a'-b') = (a\pm a')-(b\pm b')$. OK.

Väitteen mukaan modulo n sisältää lukujensa $a-b$ ja $a'-b'$ monikerrat:

(ii): Jos $n|a-b$ ja $n|a'-b'$, niin $n|aa'-bb' = a'(a-b)+b(a'-b')$. OK. □

Lukukongressiin modulo n kuuluu tietty kokonaislukujen ryhmitys ekvivalenssiluokiksi, jotka ovat keskenään ekvivalentteja. Näitä lukuluokkia sanotaan modulon n *jäännösluokiksi*.

MÄÄRITELMÄ 3.22 (Jäännösluokat). Olkoon a jokin kokonaisluku. Tällöin jakoyhtälön

$$a = qn + r$$

mukaan $a \equiv r \mod n$, jolloin luku r kuuluu samaan ekvivalenssiluokkaan kuin jokin luvuista $\{0, 1, 2, \ldots, n-1\}$.

[**13**][s.26].

Jos siis jäännösluokan luvut eroavat modulon n verran toisistaan, niin ne kuuluvat samaan jäännösluokkaan. Jos $syt(a,n) = 1$ niin luvut ovat keskenään jaottomia, eli luku a on luvun n suhteen jaoton jäännösluokka. [**13**][s.27].

3.4.1. Kongruenssit turvana. Kongruensseja ja alkulukuja käytetään monissa yhteyksissä tarkistamaan virallisten tietojen oikeellisuutta. Esimerkiksi henkilötunnuksen viimeinen merkki eli niin sanottu tarkistusmerkki saadaan muodostamalla 9 ensimmäisestä merkistä luku minkä jaollisuutta tarkastellaan luvulla 31 ja jonka jakojäännös määrittää viimeisen numeron tai merkin.

ESIMERKKI 3.23. Naispuolisen henkilö näyttää ajokorttiaan, mutta henkilötunnuksen viimeinen merkki on hieman epäselvä. Henkilötunnus näyttäisi olevan 230376-172C ja samaa väittää nainen. Tarkistetaan että tarkistusnumero on se mikä sen väitetään olevan.

$$230376172 \equiv 13 \mod 31.$$

Jakojäännöstä vastaava merkki saadaan allaolevasta taulukosta:

1:1,	2:2,	3:3,	4:4,	5:5,	6:6,	7:7,	8:8,	9:9,	10:A,
11:B,	12:C,	13:D,	14:E,	15:F,	16:H,	17:J,	18:K,	19:L,	20:M,
21:N,	22:P,	23:R,	24:S,	25:T,	26:U,	27:V,	28:W,	29:X,	30:Y.

Joten taulukon perusteella saamme varmistuksen asiaan että tarkistusnumero on oikein. Täytyy kuitenkin muistaa että pelkkä tarkistusluvun täsmääminen ei tarkoita sitä, että kyseinen henkilö on se kuka hän väittää olevansa.

Muita edellä mainittuja tarkistusnumeroihin perustuvia jokapäiviäisiä asioita ovat muun muassa tilinumerot, tuotekoodit kuten kirjojen ISBN-tunnisteet ja jotkin sarjanumerot.

3.4.2. Fermat'n pieni lause. Lukuteorian yksi perustuloksista on Fermat'n pieni lause.

LAUSE 3.24. *Fermat'n pieni lause* [**6**]*[s. 24]. Mille tahansa alkuluvulle p ja kokonaisluvulle a,*

$$a^p \equiv a \mod p.$$

TODISTUS. Riittää todistaa väite silloin kun a on positiivinen kokonaisluku, joten todistetaan väite induktiolla.
Perusaskel: Väite pätee kun $a = 1$, sillä silloin molemmat puolet ovat 1.
Induktio-oletus: Väite pätee kun $a = b$, jolloin siis voidaan kirjoittaa

$$(b+1)^p = b^p + pb^{p-1} + \cdots + pb + 1 = \sum_{j=0}^{p} \binom{p}{k} b^j$$

binomilauseen 4.34 mukaan. Kun $0 < j < p$, $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ niin osoittaja on jaollinen luvulla p ja nimittäjä ei ole. Aritmetiikan peruslauseen mukaan $\binom{p}{j}$ on jaollinen luvulla p kun $j = 1, \ldots, p-1$. Joten

$$(b+1)^p \equiv b^p + 1 \equiv b + 1 \mod p$$

induktio-oletuksen mukaan, joten *Fermat'n pieni lause* on todistettu. □

3.4.3. Alkulukuja etsimässä.

LAUSE 3.25 (Wilsonin lause). *Luku p on alkuluku jos ja vain jos*

$$(p-1)! + 1 \equiv 0 \mod p.$$

[**13**][s.33].

TODISTUS. "⇒"Jos $p = 2$ niin

$$(2-1)! + 1 = 2 \equiv 0 \mod 2,$$

eli väite pätee, kun $p = 2$. Muut alkuluvut ovat parittomia, joten osoitetaan että väite pätee myös niille.

Jos p on pariton alkuluku ja joukko $G = \{1, 2, \ldots, p-1\}$, niin tällöin kaikilla G:n alkioilla a on olemassa yksikäsitteinen käänteisalkio b joukosta G, jolle $ab \equiv 1 \mod p$. Jos $a \equiv b \mod p$, niin $a^2 \equiv 1 \mod p$ eli tällöin $a^2 - 1 = (a+1)(a-1) \equiv 0 \mod p$. Nyt koska p on alkuluku, niin täytyy olla että $a \equiv 1 \mod p$ tai $a \equiv -1 \mod p$, tällöin siis $a = 1$ tai $a = p-1$.

Voidaan siis todeta että 1 ja $p-1$ ovat toistensa käänteisalkioita, mutta muilla G:n alkioilla on toinen käänteisalkio. Joten kun alkiot $\{2, \ldots, p-2\}$ kerrotaan keskenään saadaan aina tuloksi lopulta $1 \mod p$ ja kun se kerrotaan alkioiden tulolla $1 \cdot (p-1) \equiv -1 \mod p$, jolloin $(p-1)! + 1 \equiv 0 \mod p$.

Perustellaan hieman tarkemmin vielä käänteisalkion yksikäsitteisyys. Todetaan aluksi että tällainen käänteisalkio ylipäätään on olemassa. Koska $syt(a, p) = 1$, niin

Bézout'n yhtälön (Vrt. Lause 3.14) avulla löytyy luvut b ja k siten, että $ab + kp = 1$, jolloin siis $ab \equiv 1 \mod p$, joten käänteisalkio b on olemassa. Olkoon nyt myös $ab' \equiv 1 \mod p$, joka voidaan Lemman 3.21 (ii) perusteella kertoa puolittain luvulla b, jolloin $b \equiv bab' \mod p$. Vastaavasti saataisiin myös $b' \equiv b'ab \mod p$, joten Lemman 3.20 (iii) perusteella $b \equiv b' \mod p$, mikä tarkoittaa että vain yksi b joukosta G toteuttaa halutun yhtälön $ab \equiv 1 \mod p$ ja näin ollen käänteisalkio on yksikäsitteinen.

"⇐"Väitteen mukaan kongruenssirelaatio pätee vain jos p on alkuluku, joten tehdään antiteesi että p onkin yhdistetty luku. Olkoon d luvun p tekijä, jolloin $1 < d < p$. Tällöin myös $d|(p-1)!$, koska luku d täytyy olla joukossa G. Nyt väitteen perusteella luku d jakaa luvun $(p-1)! + 1$, mikä on ristiriita, sillä tällöin luvun d täytyisi jakaa luku 1, eikä se ole mahdollista voimassa olevilla ehdoilla.

Näin ollen väite on todistettu. □

Esimerkki 3.26. Wieferichin alkuluvut ovat muotoa $2^{p-1} - 1 \equiv 1 \mod p^2$ olevia alkulukuja [**6**][s.25]. Toistaiseksi tunnetaan vain kaksi ehdon toteuttavaa alkulukua ja ne ovat 1093 ja 3511.

Mersennen lukujen n:s jäsen merkitään $M_n = 2^n - 1$. Mersennen luvuilla on erityisominaisuuksia, minkä takia ne soveltuvat hyvin muun muassa alkulukutestaukseen. [**6**][s. 25-26].

Lemma 3.27. *Oletetaan että p on alkuluku ja q on epätriviaali alkulukujakaja luvulle M_p. Tällöin $q \equiv 1 \mod p$.*

Todistus. Ehto että luku q jakaa luvun M_p määrää, että

$$2^p \equiv 1 \mod q$$

Fermat'n pienen lauseen mukaan $2^{q-1} \equiv 1 \mod q$. Olkoon $d = syt(p, q-1)$. Jos $d = p$, niin tällöin myös $p|(q-1)$. Ainut toinen vaihtoehto oli että $d = 1$ silloin kun p on alkuluku. Tällöin Bézout'n lauseen nojalla löytyy kokonaisluvut a ja b siten, että $1 = pa + (q-1)b$. Huomataan että vähintään toisen luvuista a ja b pitää olla negatiivinen. Nyt

$$2 \equiv 2^1 \equiv 2^{pa+(q-1)b} \equiv (2^p)^a (2^{q-1})^b \equiv 1^a 1^b \equiv 1 \mod q, \tag{19}$$

mikä on mahdotonta, kun $q > 1$, joten lemma on todistettu. □

3.4.3.1. *Fermat'n luvut. Fermat'n* luvuiksi sanotaan lukuja, jotka ovat muotoa $F_n = 2^{2^n} + 1$, missä $n \in \mathbb{N}$. Ensimmäiset tällaiset luvut ovat

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537 \; ja \; F_5 = 4294967297.$$

Näistä neljä ensimmäistä ovat myös alkulukuja, mutta viimeiselle pätee $641|4294967297$. Fermat itse luuli että luvut ovat kaikki alkulukuja, mutta Euler osoitti 1732, että viides luku onkin jaollinen. [**6**][s. 29].

3.4.4. Legendren neliösumma. On olemassa tulos, jonka mukaan jokainen positiivinen kokonaisluku n on esitettävissä kahden kokonaisluvun neliön summana, jos n ei ole muotoa $n \equiv 3 \mod 4$. Kolmen kokonaisluvun neliön summalla ei voida esittää jokaista kokonaislukua. Sen sijaan neljällä kokonaisluvun neliön summalla voidaan jokainen positiivinen kokonaisluku esittää ja siihen tutustutaan seuraavaksi.

LEMMA 3.28. *Olkoon p pariton alkuluku. Tällöin on olemassa $a, b \in \mathbb{Z}$, siten että*

$$a^2 + b^2 + 1 \equiv 0 \mod p. \tag{17}$$

TODISTUS. Määritellään joukot A ja B siten, että

$$A = \{a^2\}, \quad \text{missä } 0 \leq a \leq \frac{p-1}{2}$$
$$\text{ja}$$
$$B = \{-b^2 - 1\}, \quad \text{missä } 0 \leq b \leq \frac{p-1}{2}.$$

Nyt ei ole olemassa kummassakaan joukossa A eikä B kahta alkiota, jotka olisivat kongruentteja *modulo p*. Jos olisi niin että A:n alkiot olisivat $a_1^2 \equiv a_2^2 \mod p$, niin joko $a_1 \equiv a_2$ tai $a_1 \equiv -a_2 = p - a_2 \mod p$, mutta näin ei ole mahdollista A:n alkiolle. Vastaavalla päättelyllä voidaan todeta ettei myöskään B:llä voi olla samoja alkioita. Tästä seuraa, että kummassakin joukossa A ja B on $\frac{p+1}{2}$ kappaletta alkioita (modulo p), eli yhteensä $p+1$ alkiota, joten kyyhkyslakkaperiaatteen nojalla täytyy olla joukossa A alkio, joka on yhtä suuri joukon B alkion kanssa *modulo p*, toisin sanoen $x^2 \equiv -y^2 - 1 \mod p$, joillakin $x, y \in 0, 1, \ldots, \frac{p-1}{2}$. Tällöin nämä alkiot toteuttavat kongruenssiyhtälön

$$a^2 + b^2 + 1 \equiv 0 \mod p.$$

[**6**][s.50]. □

LAUSE 3.29 (Lagrangen neljän neliösumman lause). *Jokainen kokonaisluku n on korkeintaan neljän kokonaisluvun neliön summa.*

Ennen lauseen varsinaista todistamista todistetaan yksi aputulos, joka tunnetaan *Eulerin identiteettinä.*

LEMMA 3.30 (Eulerin identiteetti). *Kaikilla $a, b, c, d, \alpha, \beta, \gamma, \delta \in \mathbb{Z}$ pätee*

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = (a\alpha + b\beta + c\gamma + d\delta)^2$$
$$+(a\beta - b\alpha - c\delta + d\gamma)^2 + (a\gamma + b\delta - c\alpha - d\beta)^2 + (a\delta - b\gamma + c\beta - d\alpha)^2$$

[**6**]*[s.50].*

Todistus. Todistetaan kertomalla yhtälö auki ja aloitetaan se yhtälön oikeasta puolesta.

$$
\begin{aligned}
&(a\alpha + b\beta + c\gamma + d\delta)^2 \\
&+ (a\beta - b\alpha - c\delta + d\gamma)^2 \\
&+ (a\gamma + b\delta - c\alpha - d\beta)^2 \\
&+ (a\delta - b\gamma + c\beta - d\alpha)^2 \\
&= a^2\alpha^2 + 2a\alpha b\beta + 2a\alpha c\gamma + 2a\alpha d\delta + b^2\beta^2 + 2b\beta c\gamma + 2b\beta d\delta + c^2\gamma^2 + 2c\gamma d\delta + d^2\delta^2 \\
&+ a^2\beta^2 - 2a\beta b\alpha - 2a\beta c\delta + 2a\beta d\gamma + b^2\alpha^2 + 2b\alpha c\delta - 2b\alpha d\gamma + c^2\delta^2 - 2c\delta d\gamma + d^2\gamma^2 \\
&+ a^2\gamma^2 + 2a\gamma b\delta - 2a\gamma c\alpha - 2a\gamma d\beta + b^2\delta^2 - 2b\delta c\alpha - 2b\delta d\beta + c^2\alpha^2 + 2c\alpha d\beta + d^2\beta^2 \\
&+ a^2\delta^2 - 2a\delta b\gamma + 2a\delta c\beta - 2a\delta d\alpha + b^2\gamma^2 - 2b\gamma c\beta + 2b\gamma d\alpha + c^2\beta^2 - 2c\beta d\alpha + d^2\alpha^2 \\
&= a^2\alpha^2 + b^2\beta^2 + c^2\gamma^2 + d^2\delta^2 \\
&+ a^2\beta^2 + b^2\alpha^2 + c^2\delta^2 + d^2\gamma^2 \\
&+ a^2\gamma^2 + b^2\delta^2 + c^2\alpha^2 + d^2\beta^2 \\
&+ a^2\delta^2 + b^2\gamma^2 + c^2\beta^2 + d^2\alpha^2 \\
&= a^2(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) + b^2(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \\
&+ c^2(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) + d^2(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \\
&= (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)
\end{aligned}
$$

□

Koska $1 = 1^2 + 0^2 + 0^2 + 0^2$ ja $2 = 1^2 + 1^2 + 0^2 + 0^2$, niin edellisen lemman ja aritmetiikan peruslauseen 3.2 perusteella riittää osoittaa että väite pätee kaikille parittomille alkuluville, eli lause voisi kuulua: *Jokainen pariton alkuluku p on neljän kokonaisluvun neliön summa.*

Todistus. (Lause 3.29). Olkoon p pariton alkuluku. Lemman 3.28 mukaan on olemassa $a, b, c, d, m \in \mathbb{Z}$ siten, että

$$mp = a^2 + b^2 + c^2 + d^2. \tag{1Ɛ}$$

Nyt jos $m = 1$, niin väite on selvä, joten oletetaan että $m > 1$. Etsitään pienin tällainen luku $m'p$, joka on neljän neliön summa (1Ɛ) ja $0 < m' < m$. Tällöin kun pienennetään lukua m riittävän usein, niin täytyy lopulta olle $m' = 1$, jolloin itse asiassa etsitään esitystä alkuluvulle p.

Jos $2n$ on kahden neliön summa, eli $2n = x^2 + y^2$, niin x ja y ovat joko kumpikin parillisia tai parittomia, ja tällöin n voidaan kirjoittaa muodossa

$$n = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2. \tag{20}$$

Missä siis sulkeiden sisällä olevat luvut ovat kokonaislukuja, koska luvut x ja y ovat joko kumpikin parillisia tai kumpikin parittomia.

Jos m on parillinen niin erityisesti koko yhtälön (1Ɛ) vasen puoli on parillinen ja tällöin myös oikean puolen summa on parillinen. Oikean puolen summa on parillinen,

jos oikealla puolella on parillinen määrä parittomia (ja siten myös parillisia) termejä ja tällöin termit voidaan järjestää kahdeksi pariksi, joiden kummankin summa on parillinen, sillä kahden parittoman luvun summa on parillinen ja kahden parillisen summa on parillinen. Näihin kahteen pariin voidaan nyt soveltaa kaavaa (20) käyttämällä sitä kahdesti, eli puolitetaan m ja todetaan että $(\frac{m}{2})p$ on edelleen neljän neliön summa.

Jos m on pariton, niin kirjoitetaan että

$$\begin{aligned} \alpha &\equiv a \mod m \\ \beta &\equiv b \mod m \\ \gamma &\equiv c \mod m \\ \delta &\equiv d \mod m \end{aligned}$$

missä $-\frac{m}{2} < \alpha, \beta, \gamma, \delta < \frac{m}{2}$. Tällöin

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 < 4 \cdot \left(\frac{m}{2}\right)^2 = m^2$$

ja

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 \mod m.$$

Mistä seuraa, että

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = km,$$

jollekin $k, 0 < k < m$. Nyt Eulerin identiteetin 3.30

$$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) =& (a\alpha + b\beta + c\gamma + d\delta)^2 \\ &+ (a\beta - b\alpha - c\delta + d\gamma)^2 \\ &+ (a\gamma + b\delta - c\alpha - d\beta)^2 \\ &+ (a\delta - b\gamma + c\beta - d\alpha)^2 \end{aligned}$$

vasen puoli olisi km^2p. Edellä todettiin että $\alpha \equiv a, \beta \equiv b, \gamma \equiv c, \delta \equiv d \mod m$, mistä seuraa että $a\beta \equiv b\alpha \mod m, a\gamma \equiv c\alpha \mod m, \ldots$, joten

$$\begin{aligned} &m^2 | (a\beta - b\alpha - c\delta + d\gamma)^2, \\ &m^2 | (a\gamma + b\delta - c\alpha - d\beta)^2 \qquad \text{ja} \\ &m^2 | (a\delta - b\gamma + c\beta - d\alpha)^2. \end{aligned}$$

Myös ensimmäinen termi on on kongruentti $\alpha \equiv a, \beta \equiv b, \gamma \equiv c, \delta \equiv d \mod m$ perusteella

$$a\alpha + b\beta + c\gamma + d\delta \equiv \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 \mod m.$$

Yhtälön vasen puoli on siis jaollinen luvulla m^2, jolloin voidaan supistaa Eulerin identiteetistä 3.30 saatu yhtälö puolittain luvulla m^2. Luvulle kp saadaan näin ollen esitys neljän neliön summana, kun $0 < k < m$ eli $k = m'$.

Toistamalla siis supistamista äärellisen monta kertaa, supistuu m ykköseksi ja tällöin pariton alkuluku p voidaan esittää neljän neliön summana. □

LUKU 4

Muita lukujen ilmaisutapoja

Lukuja tai lukusarjoja voidaan tuottaa myös erilaisten sääntöjen mukaan muutenkin kuin suoraan alkuluvuista. Monissa säännöissä seuraava luku saadaan aikaisempien lukujen perusteella, kuten huomataan kuvioluvuista, Fibonaccin sekä Pascalin kolmion luvuista. Toisinaan samaan lukusarjaan kuuluvilla luvuilla on jokin yhteinen ominaisuus, vaikkei niitä voisikaan suoraan selvittää edellisten sarjan jäsenten perusteella, kuten esimerkiksi täydellisten lukujen kohdalla on.

4.1. Täydelliset luvut

MÄÄRITELMÄ 4.1. Jos $n \in \mathbb{Z}_+$, niin merkitään että $\sigma(n) = \sum_{d|n} d, \quad d \in \mathbb{Z}_+$, on luvun n positiivisten tekijöiden summa [**5**].

MÄÄRITELMÄ 4.2. Täydellisiksi luvuiksi sanotaan lukuja, joiden lukua pienempien tekijöiden summa on luku itse [**1**][s.265]. Tällaiset luvut ovat siis muotoa $\sigma(n) = 2n$.

Täydellisiä lukuja ovat (esimerkiksi):
6,
28,
496,
8 128,
33 550 336,
8 589 869 056,
137 438 691 328,
2 305 843 008 139 952 128,
2 658 455 991 569 831 744 654 692 615 953 842 176,
191 561 942 608 236 107 294 793 378 084 303 638 130 997 321 548 169 216.

Toistaiseksi ei tiedetä onko täydellisiä lukuja äärellinen vai ääretön määrä. Tällä hetkellä tunnetut täydelliset luvut ovat kaikki parillisia, mutta lukuisista todistusyrityksistä huolimatta ei ole pystytty todistamaan ettei parittomia täydellisiä lukuja ole olemassa. [**5**].

ESIMERKKI 4.3.
$1 + 2 + 3 = 6$
$1 + 2 + 4 + 7 + 14 = 28$
$1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496$
$1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 = 8128$
$\vdots$

4.1.1. Täydelliset luvut alkulukujen avulla. Täydellisiä lukuja pystytään selvittämään kakkosen potenssin ja alkulukujen avulla. Kun kakkosen potenssin termejä lasketaan yhteen järjestyksessä ja mikäli saatu summa on alkuluku, kerrotaan summa suurimmalla summan kakkosenpotenssilla ja näin saadaan täydellinen luku.

Esimerkki 4.4. Kakkosen potensseja ovat: 1, 2, 4, 8, 16, 32, ... tai $2^0, 2^1, 2^2, 2^3, 2^4, 2^5, \ldots$

- $1 + 2 = 3$ (tai $2^0 + 2^1 = 2^2 - 1$). Tässä 3 on alkuluku, joten kerrotaan suurimmalla summattavalla mikä on tässä 2, jolloin saadaan $3 \cdot 2 = 6$, joka on täydellinen luku.
- $1 + 2 + 4 = 7$ (tai $2^0 + 2^1 + 2^2 = 2^3 - 1$). Tässä 7 on myöskin alkuluku, joten kerrotaan taas suurimmalla summattavalla, jolloin saadaan $7 \cdot 4 = 28$, joka on niin ikään täydellinen luku.
- $1 + 2 + 4 + 8 = 15$ (tai $2^0 + 2^1 + 2^2 + 2^3 = 2^4 - 1$). Tässä 15 ei kuitenkaan ole alkuluku, joten ei löydy täydellistä lukua ($15 \cdot 8 = 120$, joka ei ole täydellinen luku)
- $1 + 2 + 4 + 8 + 16 = 31$ (tai $2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 2^5 - 1$). Tässä 31 on alkuluku, joten taas saadaan täydellinen luku $31 \cdot 16 = 496$.
- $1 + 2 + 4 + 8 + 16 + 32 = 63$ (tai $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = 2^6 - 1$). Tässä 63 ei ole alkuluku.
- $1+2+4+8+16+32+64 = 127$ (tai $2^0+2^1+2^2+2^3+2^4+2^5+2^6 = 2^7-1$). Tässä 127 on taas alkuluku, joten seuraava täydellinen luku on $127 \cdot 64 = 8\ 128$.
- ...

[**1**][s.266-267].

Edellistä esimerkkiä olisi voinut jatkaa kokeilemalla niin pitkälle kun intoa riittää, mutta tarkastelemalla asiaa hieman tarkemmin algebran avulla, joihin suluissa oleva versio jo johdattaa, löydetään hieman yksinkertaisempi muoto. Täydellisiä lukuja etsiessä ollaan kiinnostuneita erityisesti siitä, milloin lukujen summa on alkuluku. Summa voidaan kirjoittaa muodossa $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^n - 1$, kuten edellisestä esimerkistäkin käy ilmi. Tämä yksinkertaistaa tarkastelua, sillä nyt riittää tarkastella milloin $2^n - 1$ on alkuluku ja tällöin täydellinen luku on $(2^n - 1) \cdot 2^{n-1}$.

Lause 4.5. *Jos $2^n - 1$ on (Mersennen) alkuluku, niin $2^{n-1}(2^n - 1)$ on (parillinen) täydellinen luku.*

Todistusta varten todistetaan ensin tekijäesitystä koskeva lemma.

Lemma 4.6. *Olkoon $m, n \in \mathbb{Z}_+$ ja $syt(m, n) = 1$. Tällöin niiden tekijäfunktioille pätee*

$$\sigma(mn) = \sigma(m)\sigma(n). \tag{1}$$

TODISTUS. Määritelmästä 4.1 seuraa, että mikäli luku n on alkuluku, niin $\sigma(n) = n + 1$. Nyt koska oletuksen mukaan $syt(m, n) = 1$, niin luvuilla m ja n ei ole yhteisiä tekijöitä. Mikäli kummatkin ovat eri alkulukuja niin väite on selvä, sillä luvun mn ainoat tekijät ovat $1, m, n, mn$. Eli

$$\sigma(mn) = 1 + m + n + mn = (m + 1)(n + 1) = \sigma(m)\sigma(n)$$

Oletetaan että luvut m ja n eivät ole alkulukuja, joten niillä on alkulukuesitys. Olkoon alkulukuesitykset siten, että $m = p_1 p_2 \dots p_k$ ja $n = q_1 q_2 \dots q_l$, missä p_i ja q_j ovat alkulukuja ja joissa erityisesti $p_i \neq q_j$, kaikilla $i, j \in +\mathbb{N}$. Tällöin saadaan lukujen tekijät ja edelleen tekijöiden summat, jotka ovat

$$\begin{aligned}\sigma(m) &= 1 + p_1 + \dots + p_k + p_1p_2 + \dots + p_1p_k + p_2p_3 + \dots + p_2p_k + \dots + p_{k-1}p_k \\ &\quad + p_1p_2p_3 + \dots + p_1p_2p_k + \dots + p_1p_2 \dots p_k \\ \sigma(n) &= 1 + q_1 + \dots + q_l + q_1q_2 + \dots + q_1q_l + q_2q_3 + \dots + q_2q_l + \dots + q_{l-1}q_l \\ &\quad + q_1q_2q_3 + \dots + q_1q_2q_l + \dots + q_1q_2 \dots q_l\end{aligned}$$

Tulon mn tekijöitä ovat kaikki, sekä luvun m että n tekijät, koska mikäli $p_i|m$, niin täytyy myös olla että $p_i|mn$ ja vastaavasti tietenkin myös $q_j|mn$. Tällöin

$$\begin{aligned}\sigma(mn) &= 1 + p_1 + \dots + p_k + q_1 + \dots + q_l + p_1p_2 + \dots + p_1p_k + p_1q_1 + \dots p_1q_l \\ &\quad + p_2p_3 + \dots + p_2p_k + p_2q_1 + \dots + p_2q_l + \dots + p_{k-1}p_k + p_{k-1}q_1 + \dots + p_{k-1}q_l \\ &\quad + p_1p_2p_3 + \dots + p_1p_2p_k + p_1p_2q_1 + \dots + p_1p_2q_l + \dots + p_1p_2 \dots p_k \\ &\quad + p_1p_2 \dots p_kq_1 + p_1p_2 \dots p_kq_l + p_1 \dots p_kq_1q_2 + \dots + p_1 \dots p_kq_1 \dots q_l \\ &\quad + q_1q_2 + \dots + q_1q_l + q_2q_3 + \dots + q_2q_l + \dots + q_{l-1}q_l \\ &\quad + q_1q_2q_3 + \dots + q_1q_2q_l + \dots + q_1q_2 \dots q_l\end{aligned}$$

Nyt edelliset laskemalla auki, voidaan huomata että $\sigma(mn) = \sigma(m)\sigma(n)$, joten väite on todistettu. □

TODISTUS. Lause 4.5. Koska $2^n - 1$ on alkuluku, sen ainoat tekijät ovat luku 1 ja luku itse. Tällöin

$$\sigma(2^{n-1}(2^n-1)) = \sigma(2^{n-1})\sigma(2^n-1) = (2^0+2^1+2^2+\dots+2^{n-1})\cdot(2^n-1+1) = 2^{n-1}\cdot 2^n,$$

joten väite on todistettu □

LAUSE 4.7. *Jos n on parillinen täydellinen luku, niin kaikille parillisille täydellisille luvuille n on olemassa esitysmuoto $2^{p-1}q$, missä $q = 2^p - 1$ on (Mersennen) alkuluku.*

TODISTUS. Olkoon $2^h d$ parillinen täydellinen luku, missä luku d on pariton. Tällöin

$$\sigma(2^h d) = \sigma(2^h)\sigma(d) = (2^{h+1} - 1)\sigma(d).$$

Että luku voisi olla täydellinen, täytyy sille päteä

$$2^{h+1}d = (2^{h+1} - 1)\sigma(d).$$

Tästä seuraa että $2^{h+1} - 1|d$, joka voidaan kirjoittaa muodossa $d = (2^{h+1} - 1)k$ missä $k \in \mathbb{Z}$. Tällöin $\sigma(d) \geq 2^{h+1}k$, missä yhtäsuuruus on voimassa, jos ja vain jos $k = 1$ ja $2^{h+1} - 1$ on alkuluku, eli

$$2^{h+1}(2^{h+1} - 1)k = 2^{h+1}d = (2^{h+1} - 1)\sigma(d) \geq (2^{h+1} - 1)2^{h+1}k.$$

Edelleen yhtäsuuruus pätee vain kun $k = 1$ ja $2^{h+1} - 1$ on alkuluku. Joten väite on todistettu. □

4.1.2. Ystävälliset luvut. Ystävällinen lukupari on sellainen, jossa ensimmäisen luvun lukua itseä pienempien tekijöiden summa on jälkimmäinen luku ja jälkimmäisen luvun lukua itse pienempien tekijöiden summa on ensimmäinen luku. Saattaa kuulostaa harvinaiselta ja niin ne itseasiassa olivatkin, ennen kuin tietokoneet tulivat apuun. Pienin tällainen lukupari on 220 ja 284. [**1**][s.265].

Thabit ibn-Quarra (826-901) julkaisi ystävällisille luvuille kaavan.

LAUSE 4.8. *Olkoon luvut p, q ja r alkulukuja. Jos alkuluvut ovat muotoa $p = 3 \cdot 2^n - 1$, $q = 3 \cdot 2^{n-1} - 1$ ja $9 \cdot 2^{2n-1} - 1$, missä $n \in \mathbb{Z}_+$, niin luvut $2^n pq$ ja $2^n r$ ovat ystävällisiä lukuja.* [**2**]*[s.335-336].*

TODISTUS. Täytyy siis osoittaa että $\sigma(2^n pq) = \sigma(2^n r)$. Nyt koska p, r, q ovat alkulukuja niin niillä ei ole muita tekijöitä kuin luku 1 ja luku itse. Lisäksi koska kumpikin ystävällinen luku sisältää kertoimen 2^n voidaan se jättää tarkastelusta pois, eli itse asiassa väitteen todistamiseksi riittää osoittaa että $\sigma(pq) = \sigma(r)$.

$$\begin{aligned}\sigma(pq) = 1 + p + q + pq =& 1 + 3 \cdot 2^n - 1 + 3 \cdot 2^{n-1} - 1 + (3 \cdot 2^n - 1) \cdot (3 \cdot 2^{n-1} - 1) \\ &= 1 + 3 \cdot 2^n - 1 + 3 \cdot 2^{n-1} - 1 + 9 \cdot 2^{2n-1} - 3 \cdot 2^n - 3 \cdot 2^{n-1} + 1 \\ &= 9 \cdot 2^{2n-1} = 1 + 9 \cdot 2^{2n-1} - 1 = 1 + r = \sigma(r).\end{aligned}$$

Joten väite on todistettu. □

ESIMERKKI 4.9. Ystävällisiä lukupareja:

- luvun **220** tekijöiden summa on: 1+2+4+5+10+11+20+22+44+55+110 = 284,
  luvun **284** tekijöiden summa on: $1 + 2 + 4 + 71 + 142 = 220$.
  Tässä siis luvut ovat Lauseen 4.8 mukaisia, sillä $220 = 2^2 \cdot 5 \cdot 11$ ja $284 = 2^2 \cdot 71$, eli $n = 2, p = 5, q = 11$ ja $r = 71$.

- luvun **17 296** tekijöiden summa on: $1 + 2 + 4 + 8 + 16 + 23 + 46 + 47 + 92 + 94 + 184 + 188 + 368 + 376 + 752 + 1081 + 2162 + 4324 + 8648 = 18\ 416$
  luvun **18 416** tekijöiden summa on: $1 + 2 + 4 + 8 + 16 + 1151 + 2302 + 4604 + 9208 = 17\ 296$
  Myös tässä Lause 4.8 on voimassa, sillä $17\ 296 = 2^4 \cdot 23 \cdot 47$ ja $18\ 416 = 2^4 \cdot 1151$ eli $n = 4, p = 23, q = 47$ ja $r = 1151$.

4.1.3. Seuralliset luvut. Seurallisilla luvuilla tarkoitetaan lukujonoa, jonka seuraava luku saadaan laskemalla luvun kaikki lukua itseä pienemmät tekijät yhteen, seuraava luku saadaan laskemalla tämän summaksi saadun luvun aidot tekijät yhteen ja seuraava taas vastaavasti, kunnes summaksi saadaan ensimmäinen luku. Jonojen pituudelle ei ole mitään tiettyä termien määrää, mutta yleensä ketjut ovat neljän luvun mittaisia. Toistaiseksi ei ole löydetty yhtään lukuketjua, jossa olisi kolme lukua ja pisin löydetty ketju on täydellisen luvun 28 mittainen.

ESIMERKKI 4.10. Viiden luvun lukuketju:
$12\ 496 \to 14\ 288 \to 15\ 472 \to 14\ 536 \to 14\ 264$ [**1**][s.265-266].

Kirjoitetaan malliksi ensimmäinen ja viimeinen kohta auki, eli lukujen $12\ 496 = 2^4 \cdot 11 \cdot 71$ ja $12\ 496 = 2^3 \cdot 1783$ tekijöiden summat:

$$\begin{aligned} 1+2+4+8+11+16+22+44+71+88+142+176+284+568+781 \\ +1\ 136+1\ 562+3\ 124+6\ 248 = 14\ 288 \\ 1+2+4+8+1783+3566+7132 = 12\ 496 \end{aligned}$$

Esimerkki 4.11. Pisin löydetty ketju:
$14\ 316; 1+2+3+4+6+12+1193+2386+3579+4772+7158 = 19\ 116$

$19\ 116; 1+2+3+4+6+9+12+18+27+36+54+59+81+108+118+162+177$
$+236+324+354+531+708+1062+1593+2124+3186+4779+6372+9558 = 31\ 704$

$31\ 704; 1+2+3+4+6+8+12+24+1\ 321+2\ 642+3\ 963+5\ 284+7\ 926$
$+10\ 568+15\ 852 = 47\ 616$

$47\ 616 \to 83\ 328 \to 177\ 792 \to 295\ 488 \to 629\ 072 \to 589\ 786 \to 294\ 896 \to$
$358\ 336 \to 418\ 904 \to 366\ 556 \to 274\ 924 \to 275\ 444 \to 243\ 760 \to 376\ 736 \to$
$381\ 028 \to 285\ 778 \to 152\ 990 \to 122\ 410 \to 97\ 946 \to 48\ 976 \to 45\ 946 \to 22\ 976 \to$
$22\ 744 \to 19\ 916 \to 17\ 716$

4.1.4. Oudot luvut. Oudot luvut ovat lukuja, jotka ovat aidosti pienempiä kuin luvun itseä pienempien tekijöiden summa. Pienin tällainen luku 70 ja seuraavat ovat 836, 4030, ja niin edelleen.

$$\begin{aligned} \sigma(70) &= 1+2+5+7+10+14+35 = 74 > 0 \\ \sigma(836) &= 1+2+4+11+19+22+38+44+76+209+418 = 844 > 836 \\ \sigma(4030) &= 1+2+5+10+13+26+31+62+65+130+155+310+403+806 \\ &\quad +2015 = 4034 > 4030 \\ &\vdots \end{aligned}$$

4.2. Pythagoralaista matematiikkaa

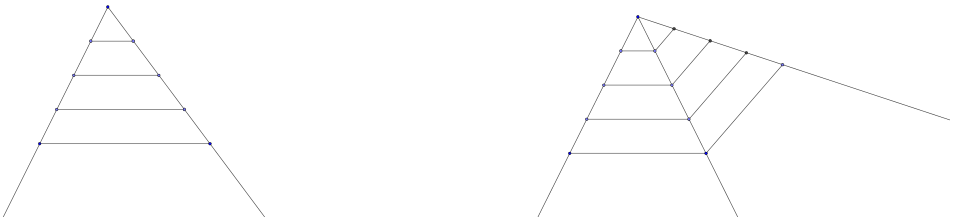
Erilaiset kuvioluvut osoittavat miten numerot olivat pythagoralaisille tärkeitä. Pythagoralaisten mukaan on nimetty lukukolmikot $\frac{m^2-1}{2}$, m, $\frac{m^2+1}{2}$, missä luku m on pariton kokonaisluku. Vaikka luvut on nimetty pythagoralaisten mukaan, niin pidetään todennäköisenä, että he eivät niitä keksineet, sillä jo babylonialaisten esimerkit liittyivät läheisesti vastaaviin lukuihin. [**2**][s.93, 97].

Pythagoralaisten kolmikot toteuttavat *Pythagoraan lauseen;* $a^2 + b^2 = c^2$, silloin kun m on pariton kokonaisluku. Pythagoraan lause toteutuu myös itse asiassa vaikka m ei olisikaan pariton kokonaisluku, tai kokonaisluku ollenkaan, tällöin vain lukukolmikko ei koostu kokonaisluvuista.

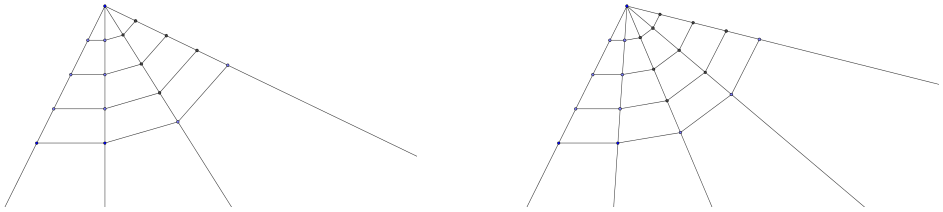
Esimerkki 4.12 (Pythagoraan kolmikot).

$$\left(\frac{m^2-1}{2}\right)^2 + m^2 =$$
$$\frac{m^4}{4} - \frac{2m^2}{4} + \frac{1}{4} + m^2 = \frac{m^4}{4} + \frac{2m^2}{4} + \frac{1}{4}$$
$$= \left(\frac{m^2+1}{2}\right)^2$$

4.2.1. Kolmio, neliö- ja kuutioluvut. Kolmion muodostaminen vaatii vähintään kolme pistettä, mutta niissä voi olla enemmänkin pisteitä. Pistejoukkojen pisteiden lukumäärät saadaan johdettua sarjojen avulla, kuten seuraavien kuvien kuvateksteistä selviää.



Kuva 1. Kolmiolukujen (vasen) pistemäärät saadaan kaavasta $N = 1+2+3+\cdots+n = \frac{n(n+1)}{n}$ ja neliölukujen (oikea) pistemäärät saadaan kaavasta $N = 1+3+5+\cdots+(2n-1) = n^2$, mikä tarkoittaa myöskin sitä, että luvun n neliö n^2 saadaan laskemalla yhteen n ensimmäistä paritonta lukua. Kummassakin kuviossa n on "rivien" määrä.



Kuva 2. Viisikulmiolukujen (vasen) pistemäärät saadaan kaavasta $N = 1+4+7+\cdots+(3n-2) = \frac{n(3n-1)}{2}$ ja kuusikulmiolukujen (oikea) pistemäärät saadaan kaavasta $N = 1+5+9+\cdots+(4n-3) = 2n^2-n$. Kummassakin kuviossa n on "rivien" määrä.

Vastaavalla tavalla saataisiin kaikenlaisia monikulmiolukuja. [**2**][s.93-94].

Nikomakhos Gerasalainen julkaisi teoksensa *Introductio arithmeticae* vuoden 100 jKr tienoilla, jossa hän esittelee huomaamansa tuloksen, jossa peräkkäisten kokonaislukujen summat tuottavat kokonaislukujen kuutioita. Hänen ryhmittelykaavansa vastasi seuraavan esimerkin 4.14 ylintä riviä. [**2**][s.262].

Esimerkki 4.13.

$$\begin{array}{rrrrrl} 1 & 3+5 & 7+9+11 & 13+15+17+19 & 21+23+25+27+29 & \dots \\ =1 & =8 & =27 & =64 & =125 & \dots \\ =1^3 & =2^3 & =3^3 & =4^3 & =5^3 & \dots \end{array}$$

Lause 4.14. *Ensimmäisten kokonaislukujen n kuutioiden summa on yhtä suuri kuin ensimmäisten n kokonaisluvun summan neliö* [**2**]*[s.263].*

Todistus. Kuutioiden summa on

$$\sum_{1\leq n} n^3 = \frac{n^2(n+1)^2}{4}.$$

Todistetaan kuutioiden summakaava induktiolla.

Väite: $\sum_{1\leq n} n^3 = \frac{n^2(n+1)^2}{4}$.

Todistus: Induktiolla luvun n suhteen, missä $n \in \mathbb{N}$.

Perusaskel: Väite pätee kun $n = 1$, koska $1^3 = \frac{1^2(1+1)^2}{4}$

Induktio-oletus: Oletetaan että väite pätee kun $n = k$, eli $\sum_{1\leq k} k^3 = \frac{k^2(k+1)^2}{4}$.

Induktioväite: Väite pätee kun $n = k + 1$, eli $\sum_{1\leq k+1}(k+1)^3 = \frac{k+1^2(k+1+1)^2}{4} = \frac{(k+1)^2(k+2)^2}{4}$.

Induktiotodistus: Erotetaan summasta $k + 1$ viimeinen termi, jolloin voidaan käyttää induktio-oletusta

$$\begin{aligned} \sum_{1\leq k+1}(k+1)^3 &= \sum_{1\leq k} k^3 + (k+1)^3 \\ &\overset{ind.ol}{=} \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\ &= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\ &= \frac{(k+1)^2(k^2+4(k+1))}{4} \\ &= \frac{(k+1)^2(k^2+4k+4)}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4} \end{aligned}$$

Mikä on haluttua muotoa, joten summakaava on esitettyä muotoa induktioperiaatteen nojalla.

Peräkkäisten kokonaislukujen summa puolestaan on

$$\sum_{1\leq n} n = \frac{n(n+1)}{2}.$$

Tällöin selvästi

$$\sum_{1\leq n} n^3 = \frac{n^2(n+1)^2}{4} = \left(\frac{n(n+1)}{2}\right)^2 = \big(\sum_{1\leq n} n\big)^2.$$

□

Esimerkki 4.15. Tarkastellaan edellä esitettyä tulosta kun $n = 5$:
$1^3 + 2^3 + 3^3 + 4^3 + 5^3 = 1 + 8 + 27 + 64 + 125 = 225 = 15^2 = (1 + 2 + 3 + 4 + 5)^2$

4.2.2. Fermat'n suuri lause. Kuuluisa Fermat'n lause, joka tunnetaan myös nimellä *Fermat'n viimeinen teoreema*.

Lause 4.16. *Ei ole olemassa sellaisia positiivisia kokonaislukuja a, b ja c, jotka toteuttaisivat yhtälön $a^n + b^n = c^n$, silloin kun $n \in \mathbb{N}$ ja $n \geq 3$.*

Todistus. Todistus julkaistiin vasta yli 350 vuotta lauseen jälkeen, mutta koska se ei mahdu marginaaliin, jätetään se lukijan oman harrastuneisuuden varaan. □

4.3. Fibonacci

Fibonaccin lukujono alkaa luvuilla 0 ja 1, joiden jälkeen jokainen seuraava termi saadaan summaamalla aina kaksi edellistä lukua yhteen. Lukujono siis alkaa: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, ... [**1**][s.284-285].

Fibonaccin luvuista tekee mielenkiintoisen myös se, että luonto suosii usein fibonaccin lukuja. Esimerkiksi monissa kukissa terälehtien määrä on joku Fibonaccin luku. Myös männynkäpyjen ja ananasten spiraalikuvioista löytyy Fibonaccin lukuja. Eläinmaailman lisääntymistä ja sukupuuta pystytään havainnollistamaan Fibonaccin lukujonon avulla. [**1**][s.285-288].

Esimerkki 4.17. Kanien lisääntyminen kuukausittain, kun alussa on yksi aikuinen kanipari. Kanit ovat sukukypsiä 2 kuukauden ikäisinä ja oletetaan niiden saavan yhden poikasparin kuukaudessa, eikä kanien elämää häiritse ulkopuoliset tekijät.

kuukausi ja populaatio	*pareja*
Kuukausi 1: 1 aikuinen pari	1
Kuukausi 2: 1 aikuinen pari ja 1 poikaspari	2
Kuukausi 3: 2 aikuista paria ja 1 poikaspari	3
Kuukausi 4: 3 aikuista paria ja 2 poikasparia	5
Kuukausi 5: 5 aikuista paria ja 3 poikasparia	8
Kuukausi 6: 8 aikuista paria ja 5 poikasparia	13
Kuukausi 7: 13 aikuista paria ja 8 poikasparia	21
Kuukausi 8: 21 aikuista paria ja 13 poikasparia	34

...

[**1**][s.287].

MÄÄRITELMÄ 4.18. Fibonaccin lukujonon seuraava jäsen saadaan laskemalla aina kahden edellisen termin summa. Fibonaccin lukujonon termejä merkitään F-kirjaimella ja alaindeksillä, joka kertoo monesko jonon termi on kyseessä [**1**][s.288].

$$F_n = \begin{cases} 0 & , \text{ kun } n = 0 \\ 1 & , \text{ kun } n = 1 \\ F_{n-1} + F_{n-2} & , \text{ kun } n > 1. \end{cases}$$

Merkintätapa on siis yleensä sama kuin Fermat'n luvuille, joten asiayhteydestä täytyy päätellä kumpia lukuja tarkoitetaan.

ESIMERKKI 4.19.

F_0	0						
F_1	1	F_6	8	F_{11}	89	F_{16}	987
F_2	1	F_7	13	F_{12}	144	F_{17}	1597
F_3	2	F_8	21	F_{13}	233	F_{18}	2584
F_4	3	F_9	34	F_{14}	377	F_{19}	4181
F_5	5	F_{10}	55	F_{15}	610	F_{20}	6765
							$\vdots$

4.3.1. Fibonaccin lukujen esiintymisiä. Fibonaccin lukujonossa on sellainen mielenkiintoinen ominaisuus, että kun katsotaan joka kolmatta jonon termiä $(F_3, F_6, F_9, F_{12}, \dots)$, ne ovat kaikki jaollisia numerolla 2. Joka neljäs jonon termi $(F_4, F_8, F_{12}, F_{16}, \dots)$ on jaollinen luvulla 3, joka viides jonon termi $(F_5, F_{10}, F_{15}, F_{20}, \dots)$ on puolestaan jaollinen luvulla 5, joka kuudes jonon termi $(F_6, F_{12}, F_{18}, \dots)$ on jaollinen luvulla 8, joka seitsemäs jonon termi $(F_7, F_{14}, \dots)$ on jaollinen luvulla 13 ja niin edelleen. [**1**][s.288-289].

ESIMERKKI 4.20. Fibonaccin lukuja löytyy myös murtoluvusta $\frac{1}{F_{11}} = \frac{1}{89}$, joka saadaan Fibonaccin jonoa noudattavista desimaaliluvuista [**1**][s.289]:

0,0
0,01
0,001
0,0002
0,00003
0,000005
0,0000008
0,00000013
0,000000021
0,0000000034
0,00000000055
0,000000000089
0,0000000000144
0,00000000000233
0,000000000000377
0,0000000000000610
0,00000000000000987
0,000000000000001597
0,0000000000000002584
0,00000000000000004181
0,000000000000000006765
0,0000000000000000010945
0,00000000000000000017711
0,000000000000000000028657
0,0000000000000000000046368
0,00000000000000000000075025
0,000000000000000000000121393
0,0000000000000000000000196418
0,00000000000000000000000317811
0,000000000000000000000000514229
0,0000000000000000000000000832040
0,00000000000000000000000001346269
0,000000000000000000000000002178309
0,0000000000000000000000000003524578
0,00000000000000000000000000005702887
0,000000000000000000000000000009227465
0,0000000000000000000000000000014930352
0,00000000000000000000000000000024157817
0,000000000000000000000000000000039088169
0,0000000000000000000000000000000063245986
0,00000000000000000000000000000000102334155
0,000000000000000000000000000000000165580141
0,0000000000000000000000000000000000267914296
0,00000000000000000000000000000000000433494437
0,000000000000000000000000000000000000701408733
0,0000000000000000000000000000000000001134903170
...

0,01123595505617977528089887640449438202247191011235...

Lienee paikallaan perustella miksi edellisen murtoluvun desimaaliluku on saatu todella Fibonaccin luvuista.

SELITYS 4.21. Merkitään ensinnäkin, että

$$k(x) = \sum_{n=1}^{\infty} F_n \cdot x^n = 0 \cdot x^1 + 1 \cdot x^2 + 1 \cdot x^3 + 2 \cdot x^4 + 3 \cdot x^5 + 5 \cdot x^6 + \dots$$

missä siis F_n on n:s Fibonaccin luku, eli $F_1 = 0, F_2 = 1, F_3 = 1, F_4 = 2, \dots$

Tällöin saadaan että

$$\begin{aligned} k(x) &= 1 \cdot x^2 + 1 \cdot x^3 + 2 \cdot x^4 + 3 \cdot x^5 + 5 \cdot x^6 + \dots \\ xk(x) &= 1 \cdot x^3 + 1 \cdot x^4 + 2 \cdot x^5 + 3 \cdot x^6 + \dots \\ x^2k(x) &= 1 \cdot x^4 + 1 \cdot x^5 + 2 \cdot x^6 + \dots \end{aligned}$$

ja edelleen, että $k(x) - xk(x) - x^2k(x) = x^2 \Leftrightarrow k(x)(1 - x - x^2) = x^2$.

Jos $-x^2 - x + 1 \neq 0$, missä siis $x \neq -\frac{1 \pm \sqrt{5}}{2}$ (vrt. kappale 4.3.2) , niin saadaan tulos

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

mikä voidaan kirjoittaa myös muodossa

$$\frac{1}{x^{-2} - x^{-1} - 1} = \sum_{n=1}^{\infty} F_n \cdot x^n. \tag{2}$$

Nyt jos sijoitetaan ylläolevaan yhtälöön (2) muuttujalle arvo $x = \frac{1}{10}$, niin saadaan yhtälö

$$\frac{1}{89} = \frac{1}{100 - 10 - 1} = \frac{1}{(\frac{1}{10})^{-2} - (\frac{1}{10})^{-1} - 1} = \sum_{n=1}^{\infty} F_n \cdot \left(\frac{1}{10}\right)^n.$$

[**12**][s.17]. Joten selitys murtoluvun desimaaliosalle on löydetty.

Fibonaccin jonon peräkkäisillä termeillä on sellainen ominaisuus, että mikäli valitsee mitkä tahansa kolme peräkkäistä lukujonon termiä ja kerrotaan ensimmäinen viimeisellä, niin tulo poikkeaa aina yhdellä keskimmäisen neliöstä [**1**][s.289]. Poikkeama voi olla kumpaan suuntaan tahansa, riippuen onko kyseessä järjestysluvultaan parillinen vai pariton Fibonaccin lukujonon termi.

ESIMERKKI 4.22. Fibonaccin lukujonon pätkiä:

- F_3, F_4, F_5:
  $F_3 \cdot F_5 = F_4^2 + 1$, koska $2 \cdot 5 = 3^2 + 1$.

- F_{12}, F_{13}, F_{14}:
  $F_{12} \cdot F_{14} = F_{13}^2 - 1$, koska $144 \cdot 377 = 233^2 - 1 \quad (\text{eli } 54\,288 = 54\,289 - 1)$.

- F_{17}, F_{18}, F_{19}:
  $F_{17} \cdot F_{19} = F_{18}^2 + 1$, koska $1\,597 \cdot 4\,181 = 2\,584^2 + 1 \quad (\text{eli } 6\,677\,057 = 6\,677\,056 + 1)$.

Todistetaan edellinen esimerkki yleisessä muodossa.

LAUSE 4.23 (Cassinin lause). *Olkoon Fibonaccin lukujonon luvut* F_{n-1}, F_n, F_{n+1}. *Tällöin*

$$F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^n.$$

TODISTUS. Todistetaan väite induktiolla.

Oletus: Fibonaccin lukujonon luvut F_{n-1}, F_n, F_{n+1}.

Väite: $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^n$.

Perusaskel: Väite pätee kun $n = 1$:
$F_0F_2 - F_1^2 = 0 \cdot 1 - 1^1 = -1 = (-1)^1$.

Induktio-oletus: Oletetaan että väite pätee kun $n = k$ eli
$F_{k-1}F_{k+1} - F_k^2 = (-1)^k$

Induktioväite: Täytyy siis osoittaa että väite pätee kun $n = k + 1$ eli
$F_{(k+1)-1}F_{(k+1)+1} - F_{k+1}^2 = (-1)^{k+1}$

Induktiotodistus: Sievennetään ensin induktioväitteen vasen puoli muotoon
$F_kF_{k+2} - F_{k+1}^2 = (-1)^{k+1}$
Kirjoitetaan lisäksi Fibonaccin lukujen määritelmän 4.18 perusteella
$F_k = F_{k+1} - F_{k-1}$ ja $F_{k+2} = F_k + F_{k+1}$.
Kirjoitetaan nyt väite uudestaan edellisin merkinnöin

$$\begin{aligned} F_kF_{k+2} - F_{k+1}^2 &= (F_{k+1} - F_{k-1})(F_k + F_{k+1}) - F_{k+1}^2 \\ &= F_{k+1}F_k + F_{k+1}^2 - F_{k-1}F_k - F_{k-1}F_{k+1} - F_{k+1}^2 \\ &= F_{k+1}F_k - F_{k-1}F_k - F_{k-1}F_{k+1} \end{aligned}$$

Induktio-oletuksen mukaan $F_{k-1}F_{k+1} - F_k^2 = (-1)^k$, mistä saadaan että $F_{k-1}F_{k+1} = F_k^2 + (-1)^k$ ja sijoitetaan tämä, sekä $F_{k+1} = F_k + F_{k-1}$ väitteeseen, eli

$$\begin{aligned} F_{k+1}F_k - F_{k-1}F_k - F_{k-1}F_{k+1} &= F_{k+1}F_k - F_{k-1}F_k - (F_k^2 + (-1)^k) \\ &= (F_k + F_{k-1})F_k - F_{k-1}F_k - F_k^2 - (-1)^k \\ &= F_k^2 + F_{k-1}F_k - F_{k-1}F_k - F_k^2 - (-1)^k \\ &= -(-1)^k \\ &= -1 \cdot (-1)^k \\ &= (-1)^{k+1}, \end{aligned}$$

mikä on induktioväitteen oikea puoli. Täten induktioperiaatteen mukaan väite on tosi kaikille kokonaisluvuille $n \geq 1$.

□

SEURAUS 4.24. *Millään peräkkäisellä Fibonaccin lukujonon lukuparilla ei ole yhteisiä tekijöitä* [**2**]*[s.364].*

TODISTUS. Olkoon alkuluku p sekä luvun F_n, että F_{n+1} alkulukutekijä. Tällöin p jakaa edellisen lauseen 4.23 kummankin vasemman puoleisen termin, mistä seuraa että $p| \pm 1$, mikä on ristiriita. Siispä $syt(F_n, F_{n+1}) = 1$, eli kahdella peräkkäisellä Fibonaccin lukujonon termillä ei ole yhteisiä tekijöitä. □

4.3.2. Kultainen leikkaus ja Fibonaccin lukujono. Kultaisella suhteella tarkoitetaan täsmällistä suhdelukua, joka saadaan jakamalla jana kahteen osaan siten, että koko janan pituuden suhde suurempaan osaan on sama kuin suuremman janan pituuden suhde pienemmän janan pituuteen. Eli $\frac{A+B}{A} = \frac{A}{B}$, missä jana A on pitempi janoista. Kultaisella suhteella jaettu jana tunnetaan myös kultaisena leikkauksena ja fii eli suuremman ja pienemmän osan välinen suhde, jonka likiarvo voidaan laskea tarkasta arvosta $\varphi = \frac{(1+\sqrt{5})}{2} \approx 1,61803\ 39887\ 49894\ 84820\ldots$. [**1**][s.284]. Tarkka arvo saadaan laskemalla $\frac{A+B}{A} = \frac{A}{B}$ siten, että merkitään täysi mittaista janaa $A + B = 1$, sekä osia $A = x, B = 1-x$ ja ratkaistaan x:lle positiivinen nollakohta (koska kyseessä pituus) kuten allaolevasta kaavan laskemisesta (3) käy ilmi.

$$\begin{aligned} \frac{1}{x} &= \frac{x}{1-x} \\ 1-x &= x^2 \\ x^2 + x - 1 &= 0 \\ x &= \frac{-1\sqrt{1^2 - 4 \cdot 1 \cdot (-1)}}{2 \cdot 1} = \frac{-1+\sqrt{5}}{2} \end{aligned} \tag{3}$$

ESIMERKKI 4.25. Peräkkäisten Fibonaccin lukujen suhde lähestyy kultaistasuhdetta φ [**1**][s.290].

- $\frac{F_2}{F_1}, \frac{F_3}{F_2}, \frac{F_4}{F_3}, \frac{F_5}{F_4}, \frac{F_6}{F_5}, \frac{F_7}{F_6}, \frac{F_8}{F_7}, \frac{F_9}{F_8}, \frac{F_{10}}{F_9}, \frac{F_{11}}{F_{10}}, \frac{F_{12}}{F_{11}} \frac{F_{13}}{F_{12}}, \frac{F_{14}}{F_{13}}, \frac{F_{15}}{F_{14}} \ldots$
- $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \frac{89}{55}, \frac{144}{89}, \frac{233}{144}, \frac{233}{377}, \frac{610}{377}, \ldots$
- 1, 2, 1,5, 1,66667, 1,6 1,625, 1,61538, 1,61905, 1,61765, 1,61818, 1,61798, 1,61806, 1,61803, 1,61804, ... *viiden desimaalin tarkkuudellla*

Itse asiassa jos meillä on Fibonaccin lukujonon kaltainen jono, missä seuraava termi saadaan summaamalla kaksi edellistä termiä, lähestyy kahden peräkkäisen luvun suhde siltikin kultaisen leikkauksen suhdetta [**1**][s.291].

ESIMERKKI 4.26. Olkoon jonon alkuarvot 6 ja 11, jolloin kolmas termi on 17.

- $\frac{11}{6}, \frac{17}{11}, \frac{28}{17}, \frac{45}{28}, \frac{73}{45}, \frac{118}{73}, \frac{191}{118}, \frac{309}{191}, \frac{500}{309}, \frac{809}{500}, \ldots$
- 1,83333, 1,54545, 1,64706, 1,60714, 1,62222, 1,61644, 1,61864, 1,61780, 1,61812, 1,618, ... *viiden desimaalin tarkkuudella*

Sanotaan että kultainen leikkaus miellyttää visuaalisesti katsojan silmää ja itse asiassa monista maalauksista ja vanhoista rakennuksista kultaisen leikkauksen toteuttavia suhteita löytyykin. Leonardo Da Vinci oli eräs tunnetuimmista taiteilijoista, joka käytti töissään hyväksi kultaista leikkausta.

LAUSE 4.27 (Fibonaccin lukujen summa). $\sum_{i=0}^{n} F_i = F_{n+2} - 1$, *kun* $n \in \mathbb{N}$.

TODISTUS. Kirjoitetaan summa auki määritelmän 4.18 perusteella, missä $F_{n-2} = F_n - F_{n-1}$

$$\sum_{i=0}^{n} F_i = F_0 + F_1 + F_2 + \cdots + F_n = (F_2 - F_1) + (F_3 - F_2) + \cdots + (F_{n+2} - F_{n+1})$$

Nyt jos tarkastellaan yhtälön oikeaa puolta, niin huomataan että siellä esiintyy lukuja vastalukuineen ja ilman paria jää ainoastaan $F_{n+2} - F_1 = F_{n+2} - 1$. Todistetaan väite kuitenkin vielä kunnolla induktiolla.

Perusaskel: Väite pätee kun $n = 0$:
$\sum_{i=0}^{0} 0 = F_0 = F_2 - 1 = 1 - 1 = 0$.

Induktio-oletus: Oletetaan että väite pätee kun $n = k$ eli
$\sum_{i=0}^{k} F_i = F_{k+2} - 1$, kun $n \in \mathbb{N}$.

Induktioväite: Täytyy siis osoittaa, että väite pätee kun $n = k + 1$ eli
$\sum_{i=0}^{k+1} F_i = F_{(k+1)+2} - 1$, kun $n \in \mathbb{N}$.

Induktiotodistus: Erotetaan aluksi induktioväitteen summan viimeinen termi, jotta voidaan käyttää induktio-oletusta

$$\begin{aligned}
\sum_{i=0}^{k+1} F_i &= \sum_{i=0}^{k} F_i + F_{k+1} \\
&\overset{ind.ol}{=} F_{k+2} - 1 + F_{k+1} \\
&= \underbrace{F_{k+2} + F_{k+1}}_{=F_{k+3}} - 1 \\
&= F_{k+3} - 1 \\
&= F_{(k+1)+2} - 1,
\end{aligned}$$

mikä on sitä muotoa kuin haluttiinkin.

Induktioperiaatteen nojalla väite on todistettu. □

ESIMERKKI 4.28. Lasketaan esimerkin vuoksi äskeisen lauseen 4.27 kaavalla 18 ensimmäisen (ensimmäiseksi termiksi lasketaan vasta termi F_1) Fibonaccin lukujonon termin summa. Fibonaccin lukujonon 20 ensimmäistä jäsentä on lueteltu esimerkissä

4.19.

$$\begin{aligned}\sum_{k=0}^{18} F_k =& 0+1+1+2+3+5+8+13+21+34\\ &+55+89+144+233+377+610+987+1597+2584\\ =& 6764 = 6765-1\\ =& F_{20}-1 \qquad (= F_{18+2}-1).\end{aligned}$$

Esimerkki 4.29. Fibonaccin lukujonon menetelmällä voidaan muodostaa muitakin kuin Fibonaccin lukujono. Samalla periaatteella muodostettujen lukujonojen kymmenen ensimmäisen luvun summa on sama kuin 7. termi kerrottuna luvulla 11 [**12**][s.18]. Olkoon meillä lukujono

$$55, 87, 142, 229, 371, 600, 971, 1571, 2542, 4113.$$

Tällöin termien summa on $10\,681 = 11 \cdot 971$.

Jälkimmäisen kertolaskun pystyy laskemaan helpohkosti päässäkin, muutenkin kuin $10 \cdot 971 + 971$. Sillä jos esimerkiksi kerrotaan 5 numeroinen luku luvulla 11, niin olkoon ensinnäkin kyseinen luku

$$\begin{aligned}abcde &= a\cdot 10^4 + b\cdot 10^3 + c\cdot 10^2 + d\cdot 10^1 + e\cdot 10^0,\\ 11\cdot abcde &= a\cdot 10^5 + (a+b)\cdot 10^4 + (b+c)\cdot 10^3 + (c+d)\cdot 10^2 + (d+e)\cdot 10^1 + e\cdot 10^0.\end{aligned}$$

[**12**][s.18]. Lasketaan äskeisellä menetelmällä edellä oleva kertolasku $11 \cdot 971$

$$11\cdot 971 = \overbrace{1}^{0+0+1^*}\ \underbrace{0}_{0+9+1^*}\ \overbrace{6}^{9+7}\ \underbrace{8}_{7+1}1,$$

missä 1^* ovat muistinumeroita edellisen luvun summasta.

Selitys 4.30. Tutkitaan vähän tarkemmin miksi edellinen pätee kaikille Fibonaccin menetelmällä luoduille lukujonoille. Merkitään lukujonon kahta ensimmäistä termia luvuilla a ja b, sekä ilmoitetaan loput termit näiden avulla, jolloin saadaan lukujono

$$a, b, a+b, a+2b, 2a+3b, 3a+5b, 5a+8b, 8a+13b, 13a+21b, 21a+34b.$$

Nyt laskemalla kaikki jonon termit yhteen saadaan $55a + 88b$ mikä on täsmälleen $11 \cdot (5a + 8b)$, missä siis $5a + 8b$ on jonon 7. termi.

4.4. Pascalin kolmio

Aritmeettinen kolmio, joka tunnetaan paremmin *Pascalin kolmiona* julkaistiin ensimmäisen kerran painettuna jo vuonna 1527 kaupallisen laskennon lehdessä saksalaisen Peter Apianin toimesta, mutta varsinaisiin kolmion ominaisuuksiin perehtyi ranskalainen Blaise Pascal vasta reilu 100 vuotta myöhemmin [**2**][s.422-424].

Pascalin kolmiossa luvut on helppo laskea ylemmällä rivillä olevien lukujen summana.

										1										
									1		1									
								1		2		1								
							1		3		3		1							
						1		4		6		4		1						
					1		5		10		10		5		1					
				1		6		15		20		15		6		1				
			1		7		21		35		35		21		7		1			
		1		8		28		56		70		56		28		8		1		
	1		9		36		84		126		126		84		36		9		1	
1		10		45		120		210		252		210		120		45		10		1

Pascalin kolmiosta pystytään poimimaan erilaisilla menetelmillä monia tuttuja lukuja ja lukujonoja. Ensinnäkin avaruuslävistäjiltä löytyvät luonnolliset luvut (1, 2, 3, 4, . . .). Kolmioluvut (1, 3, 6, 10, 15, . . .) löytyvät kolmion kolmansilta lävistäjiltä ja tetraediluvut (1, 4, 10, 20, 35, 56, . . .) neljänsiltä lävistäjiltä.

Tarkastelemalla riveittäin lukuja, siten että lasketaan rivin lukujen summa saadaan kakkosen potenssi siten, että rivin n summa on sama kuin 2^{n-1}.

$$\begin{aligned}
1 &= 2^0 \\
1+1 = 2 &= 2^1 \\
1+2+1 = 4 &= 2^2 \\
1+3+3+1 = 8 &= 2^3 \\
1+4+6+4+1 = 16 &= 2^4 \\
&\vdots
\end{aligned}$$

Mersennen luvut ovat myös löydettävissä kolmiosta kun lasketaan aina rivien summat yhteen ja lisätään uuden rivin lukujen summa edelliseen kokonaissummaan. Mersennen lukua $2^n - 1$ vastaa riviin n mennessä kertynyt summa, missä myös rivin n numerot on summattu mukaan.

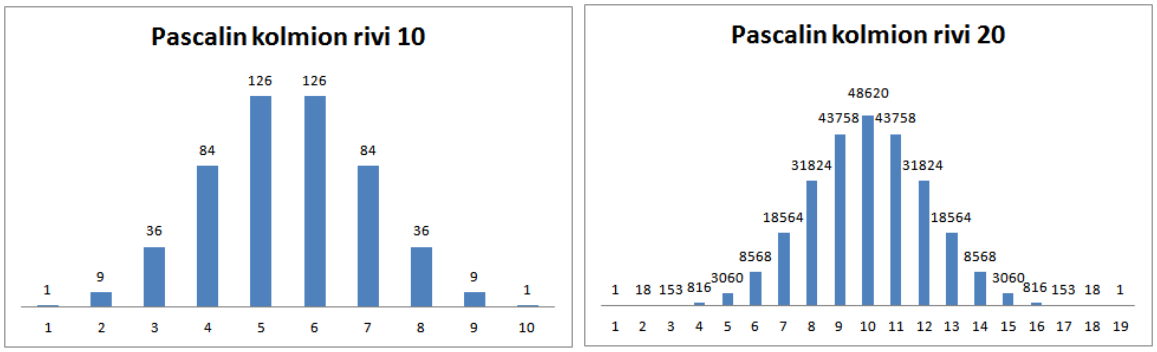
$$\begin{aligned}
1 &= 2^1 - 1 \\
(1)+1+1 = 3 &= 2^2 - 1 \\
(3)+1+2+1 = 7 &= 2^3 - 1 \\
(7)+1+3+3+1 = 15 &= 2^4 - 1 \\
(15)+1+4+6+4+1 = 31 &= 2^5 - 1 \\
&\vdots
\end{aligned}$$

Rivien numeroista muodostettu luku muodostaa yhdentoista potenssit kunhan vain lisää 9 suurempien lukujen ”kymmenet”, ”sadat”, jne. oikeille paikoilleen. Rivin

n muodostama luku vastaa yhdentoista potenssia $n-1$

$$\begin{aligned} 1 &= 11^0 \\ 11 &= 11^1 \\ 121 &= 11^2 \\ 1331 &= 11^3 \\ 14641 &= 11^4 \\ &\vdots \end{aligned}$$

Pascalin kolmiota käytetään paljon todennäköisyyslaskennassa ja sen erilaisissa sovelluksissa, mutta siihen ei tässä työssä ole laajuutensa takia mahdollisuutta pureutua seuraavaa esimerkkiä enempää. Todetaan kuitenkin, että Pascalin kolmiolla on mielenkiintoinen yhteys normaalijakaumaan, sillä kun valitaan kolmiosta jonkin rivin luvut ja tehdään niistä diagrammi, näyttäisi se noudattavan tuttua normaalijakaumaa [**1**][s.362]. Kuvassa 3 on Pascalin kolmion 10. ja 20. rivin lukujonoista muodostetut pylväsdiagrammit.



KUVA 3. Pascalin kolmion 10. ja 20. rivi diagrammina

ESIMERKKI 4.31 (Kombinatoriikkaa). Pascalin lukuja esiintyy kombinatoriikassa. Esimerkiksi jos valittavana on kolme eri väristä palloa ja niiden järjestys jätetään huomioimatta, voidaan pallot valita yhteensä kahdeksalla eri tapaa. Kaikki eri väriset pallot voidaan valita vain yhdellä tapaa, kaksi eriväristä palloa kolmella eri väriyhdistelmävaihtoehdolla, yksi pallo kolmella tapaa ja ei yhtäkään palloa yhdellä tapaa. Nyt jos tarkastelemme vaihtoehtoja kolmelle pallolle niin niitä on 1,3,3,1 eli kertoimet ovat juuri samat kuin *Pascalin kolmion* kolmannen rivin numerot. Tämä pätee muillekin pallomäärille, joten kombinaatiokertoimet pystytään etsimään kolmion avulla. [**1**][s.368-369].

4.4.1. Binomien potenssiin korotus. Jotta nähtäisiin että *Pascalin kolmiosta* on hyötyä muuallakin kuin arkipäiväisissä asioissa, niin tarkastellaan binomin potenssiin korotusta, johon edellinen esimerkki oikeastaan jo vähän johdattelikin.

ESIMERKKI 4.32. Tarkastellaan potenssiin korotusta binomille $(x+y)$

- $(x+y)^1 = x+y$
- $(x+y)^2 = x^2+2xy+y^2$
- $(x+y)^3 = x^3+3x^2y+3xy^2+y^3$
- $(x+y)^4 = x^4+4x^3y+6x^2y^2+4xy^3+y^4$
- ...

Nyt kun tarkastellaan muuttujien edessä olevia kertoimia, voidaan huomata että nekin noudattavat *Pascalin kolmion* lukuja riviltä $n+1$, missä n on potenssi johon binomi korotetaan.

Edellinen esimerkki voidaan kirjoittaa yleisessä muodossa, joka tunnetaan myös *binomilauseena tai -kaavana.*

MÄÄRITELMÄ 4.33. Olkoon $n, k \in \mathbb{N}$, missä $n \leq k$, tällöin binomikerroin

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{4}$$

Tähän määritelmään törmäsimme jo Lemman 3.6 todistuksessa aiemmin.

LAUSE 4.34 (Binomikaava). *Olkoon $a, b \geq 0$ ja $n \in \mathbb{N}$. Tällöin*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k, \tag{5}$$

missä

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Ennen varsinaisen lauseen todistamista todistetaan aputulos, joka tunnetaan *Pascalin identiteettinä.*

LEMMA 4.35 (Pascalin identiteetti). *Olkoon $m, k \in \mathbb{N}$. Tällöin*

$$\binom{m}{k} = \binom{m-1}{k-1} + \binom{m-1}{k} \tag{6}$$

TODISTUS. Todistetaan väite kirjoittamalla summan binomit auki määritelmän 4.33 mukaan.

$$\begin{aligned}
\binom{m-1}{k-1} + \binom{m-1}{k} &= \frac{(m-1)!}{(k-1)!\underbrace{((m-1)-(k-1))!}_{(m-k)!}} + \frac{(m-1)!}{k!(m-1-k)!} \\
\text{\textit{lavennetaan samannimisiksi}} &= \frac{k(m-1)!}{k(k-1)!(m-k)!} + \frac{(m-k)(m-1)!}{k!(m-k)(m-k-1)!} \\
&= \frac{k(m-1)!}{k!(m-k)!} + \frac{(m-k)(m-1)!}{k!(m-k)!} \\
&= \frac{k(m-1)! + (m-k)(m-1)!}{k!(m-k)!} \\
\text{\textit{otetaan yhteinen tekijä }}(m-1)! &= \frac{(m-1)!(k+(m-k))}{k!(m-k)!} \\
&= \frac{m!}{k!(m-k)!} \\
&= \binom{m}{k}
\end{aligned}$$

□

TODISTUS. (Lause 4.34). Todistetaan väite induktiolla.

Perusaskel: Väite pätee kun $n = 1$

$$\begin{aligned}
(a+b)^1 &= \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k \\
a + b &= \binom{1}{0} \underbrace{a^{1-0}b^0}_{=a} + \binom{1}{1} \underbrace{a^{1-1}b^1}_{=b} \\
&= \underbrace{\frac{1!}{0!(1-0)!}}_{=1} a + \underbrace{\frac{1!}{1!(1-1)!}}_{=1} b \\
&= a + b
\end{aligned}$$

Induktio-oletus: Oletetaan että väite (5) pätee kun $n = m$.

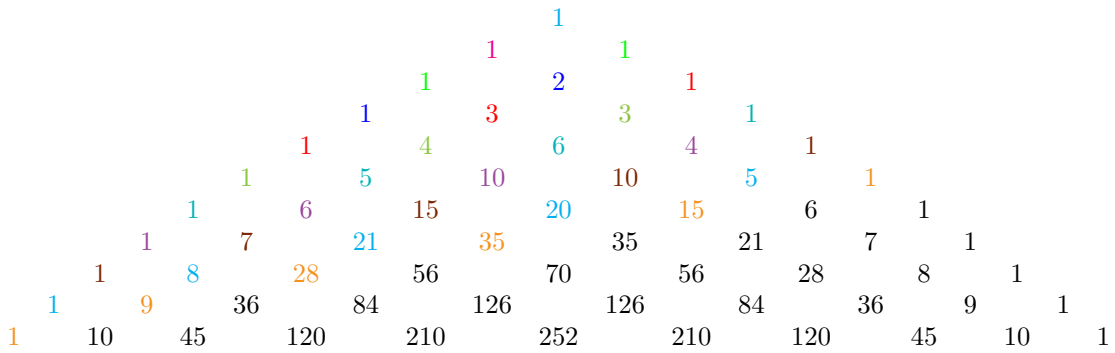
Induktioväite: Väite (5) pätee kun $n = m + 1$

Induktiotodistus: Todistetaan siis väite $(a+b)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k}b^k$

$$
\begin{aligned}
(a+b)^{m+1} &= (a+b)^m(a+b) \\
&\overset{ind.ol}{=} \sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^k(a+b) \\
&= \sum_{k=0}^{m} \binom{m}{k} (a^{m+1-k}b^k + a^{m-k}b^{k+1}) \\
&= \underbrace{\binom{m}{0}}_{=1} a^{m+1-0}b^0 + \underbrace{\sum_{k=1}^{m} \binom{m}{k} a^{m+1-k}b^k}_{\sum_{k=1}^{m+1}\binom{m+1-1}{k}a^{m+1-k}b^k} + \underbrace{\sum_{k=0}^{m} \binom{m}{k} a^{m-k}b^{k+1}}_{\sum_{k=1}^{m+1}\binom{m+1-1}{k-1}a^{m+1-k}b^k} \\
&= a^{m+1-0}b^0 + \sum_{k=1}^{m+1} \Bigg(\underbrace{\binom{m+1-1}{k-1} + \binom{m+1-1}{k}}_{=\binom{m+1}{k}} \Bigg) a^{m+1-k}b^k \\
&= \underbrace{\binom{m+1}{0}}_{=1} a^{m+1-0}b^0 + \sum_{k=1}^{m+1} \binom{m+1}{k} a^{m+1-k}b^k \\
&= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k}b^k
\end{aligned}
$$

□

Esimerkki 4.36. Myöskin Pascalin kolmiosta löytyy Fibonaccin lukujono kun lasketaan kolmion termejä ”vinottain” yhteen, kuten seuraavasta selviää. Luvut lasketaan yhteen siten ”diagonaalilta” että ylemmältä riviltä otetaan toisena oikealla ja alemmalta toisena vasemmalla oleva luku.



$$1 = 1$$
$$1 = 1$$
$$1 + 1 = 2$$
$$1 + 2 = 3$$
$$1 + 3 + 1 = 5$$
$$1 + 4 + 3 = 8$$
$$1 + 5 + 6 + 1 = 13$$
$$1 + 6 + 10 + 4 = 21$$
$$1 + 7 + 15 + 10 + 1 = 34$$
$$1 + 8 + 21 + 20 + 5 = 55$$
$$1 + 9 + 28 + 35 + 15 + 1 = 89$$

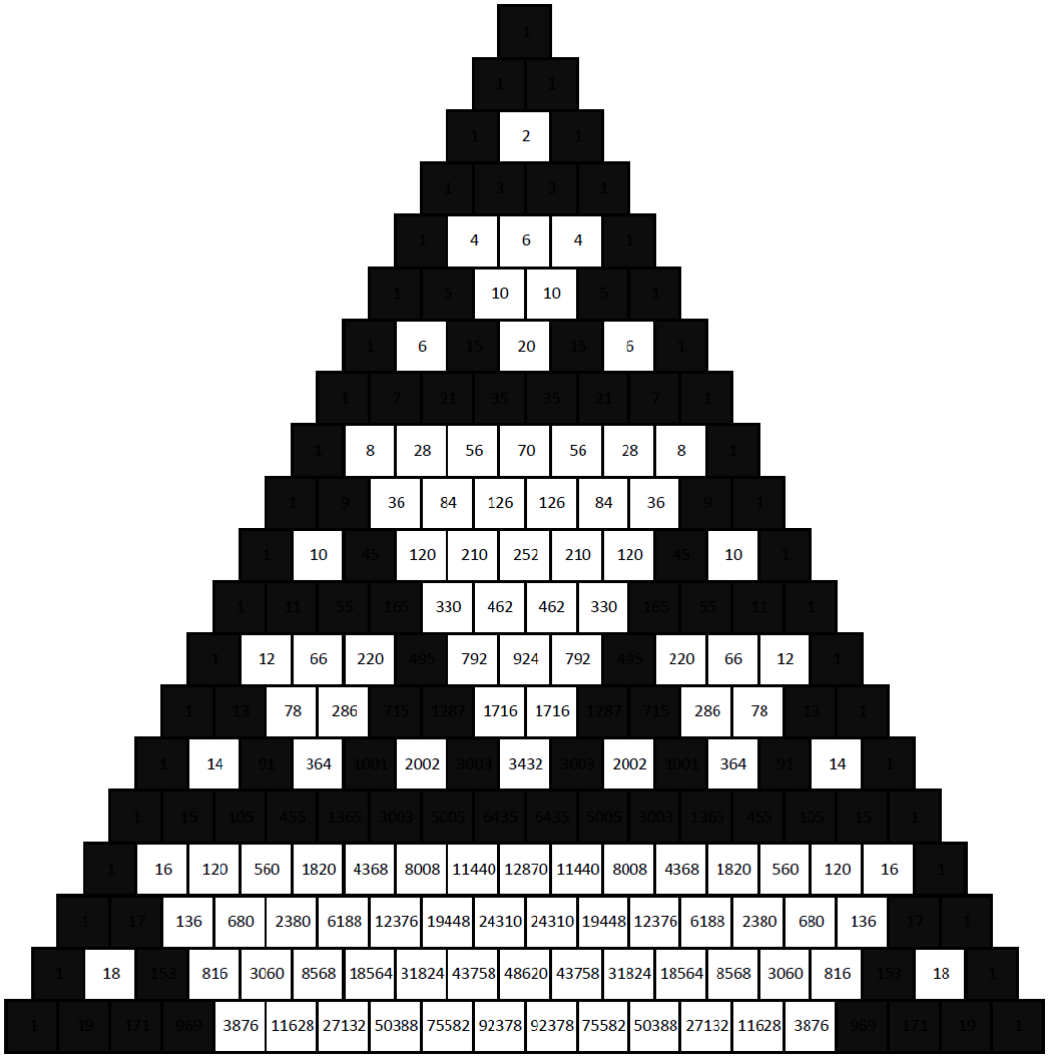
Fibonaccin lukujonon löytyminen kolmiosta ei kuitenkaan ole yllätys lukujen muodostamisen takia.

4.4.2. Pascalin kolmio ja Sierpinskin kolmio. Pascalin kolmion lukujen jaollisuuksista eri luvuilla löytyy mielenkiintoisia visuaalisia säännönmukaisuuksia, mutta muutakin, erityisesti parillisille kolmion luvuille. Tarkastellaan kolmion parillisia lukuja, eli kahdella jaollisia lukuja ja väritetään tällöin kaikki muut luvut ruutuineen mustaksi. Värityksen myötä paljastuu lukukolmiosta tasaisin välein säännöllisiä eri kokoisia kolmioita. Kun kolmion rivimäärä n kasvaa, niin keskelle syntyvän kolmion koko kasvaa myös. Syntyvä kolmio muistuttaa *Sierpinskin kolmiota* mitä enemmän siinä on rivejä ja itse asiassa n:n ollessa äärettömyyden rajalla Pascalin kolmiosta tulee Sierpinskin kolmio. Sierpinskin kolmiolla tarkoitetaan tasasivuista kolmiota, joka on jaettu neljään samanlaiseen osaan ja joista keskimmäinen osa on poistettu, tämän jälkeen jäljelle jääneille kolmioille on toistettu sama ja edelleen syntyville kolmioille ja niin edelleen. [**1**][s.365-366].

Vielä jos tarkastellaan kuvan 4 kolmion huipusta suoraan alaspäin olevia kolmioita ja erityisesti niiden kokoa, voidaan todeta ensimmäisessä olevan 1 ruutu, toisessa 6 ruutua, seuraavassa 28, 496,.... Edellä luetellut luvut ovat meille tuttuja, sillä ne ovat täydellisiä lukuja, jotka voidaan visualisoida tällaisella menetelmällä. [**1**][s.366]. Kuvassa 5 on vastaavat kolmiot, kun jakajana ovat olleet luvut 3, 4, 5, 7, 9, 11.

4.4.3. Häviävät kolmiot. Tutustutaan vielä yhteen lukujen kolmiotyyppiin, eli häviäviin kolmioihin. Kaikki kuvioluvuille johdetut lukusarjat voidaan palauttaa kolmiomuotoon, jossa huipulla on pelkkiä nollia. Häviävissä kolmioissa alin rivi toimii kantana, jossa kyseinen lukusarja on. Ylempi rivi on saatu kahden kantasarjan peräkkäisen luvun erotuksista ja siitä ylöspäin vastaavasti. Syy häviämiseen on siinä, että lukujonot ovat muodostettu samalla tapaa eli kahden peräkkäisen termin summana. [**8**][s.225-226].

Esimerkki 4.37. Tarkastellaan kuusiokulmioluvuille häviävää kolmiota. Alimmalla rivillä on lukujonon ensimmäiset 6 termiä.



KUVA 4. Pascalin kolmion parilliset luvut

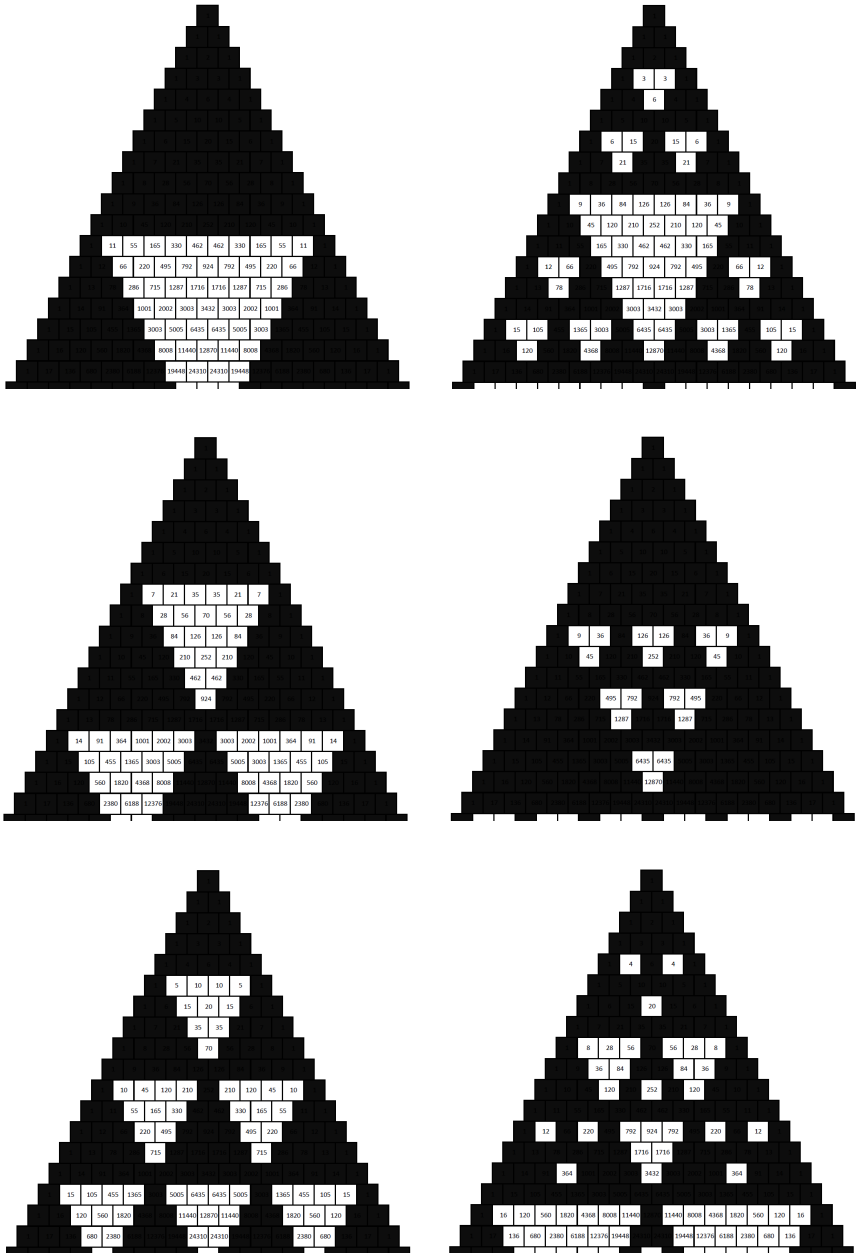
$$
\begin{array}{ccccccccccccccccccc}
 & & & & & & & & 0 & & & & & & & & & & \\
 & & & & & & & 0 & & 0 & & & & & & & & & \\
 & & & & & & 0 & & 0 & & 0 & & & & & & & & \\
 & & & & & 6 & & 6 & & 6 & & 6 & & & & & & & \\
 & & & & 6 & & 12 & & 18 & & 24 & & 30 & & & & & & \\
 & & & 1 & & 7 & & 19 & & 37 & & 61 & & 91 & & & & &
\end{array}
$$

SELITYS 4.38. Tarkastellaan häviävää kolmiota yleisesti. Merkitään kantana olevaa lukusarjaa $x_1, x_2, x_3, \ldots, x_k$, sekä ylempien rivien lukuja D_n^m, missä n kertoo monesko termi se on omalla rivillään ja m monesko rivi se on kannasta lukien.

Aloitetaan kolmirivisestä häviävästä kolmiosta.

$$
\begin{array}{ccccc}
 & & 0 & & \\
 & D_1^1 & & D_2^1 & \\
x_1 & & x_2 & & x_3
\end{array}
$$

$x_2 - x_1 = D_1^1$ ja $x_3 - x_2 = D_2^1$, mutta $D_1^1 - D_2^1 = 0$,
joten täytyy olla $D_2^1 = D_1^1$ ja siten $x_3 = x_1 + 2D_1^1$.



KUVA 5. Vasemmassa sarakkeessa ovat allekkain Pascalin kolmiot, jotka ovat jaollisia 11, 7, 5 (jotka ovat alkulukuja) ja oikeassa sarakkeessa olevat kolmiot ovat jaollisia 3, 9, 4

Laajennetaan tarkastelua neljäriviseen häviävään kolmioon.

$$\begin{array}{ccccccc} & & & 0 & & & \\ & & D_1^2 & & D_2^2 & & \\ & D_1^1 & & D_2^1 & & D_3^1 & \\ x_1 & & x_2 & & x_3 & & x_4 \end{array}$$

Summat voitaisiin kirjoittaa jokaiselle termille kuten kolmirivisessä tapauksessa, mutta kirjoitetaankin nyt luvut suoraan kantajonon termien avulla. Eli

$$\begin{aligned} x_2 =& x_1 + D_1^1, \\ x_3 =& x_2 + D_2^1 = x_2 + D_1^1 + D_1^2, \\ x_4 =& x_3 + D_3^1 = x_3 + D_2^1 + D_2^2 = x_3 + D_1^1 + D_1^2 + D_1^2, \\ \Rightarrow x_4 =& x_1 + 3D_1^1 + 3D_1^2. \end{aligned}$$

Viisirivisen jonon viimeiselle termille muoto olisi

$$x_5 = x_1 + 4D_1^1 + 6D_1^2 + 4D_1^3.$$

Kuusirivisen jonon viimeiselle termille muoto olisi

$$x_6 = x_1 + 5D_1^1 + 10D_1^2 + 10D_1^3 + 5D_1^4.$$

Seitsemänrivisen jonon viimeiselle termille muoto olisi

$$x_7 = x_1 + 6D_1^1 + 15D_1^2 + 20D_1^3 + 15D_1^4 + 6D_1^5.$$

Kantana olevan lukusarjan viimeinen luku on siis ilmoitettavissa ensimmäisen vinorivin lukujen avulla. Tutkitaan vielä hieman vinorivin eri jäsenten kertoimia taulukoimalla ne:

n	x_n	Kerroin					
2	x_2	1					
3	x_3	1	2				
4	x_4	1	3	3			
5	x_5	1	4	6	4		
6	x_6	1	5	10	10	5	
7	x_7	1	6	15	20	15	6
⋮							

Huomataan, että kertoimet ovat itse asiassa binomilausekkeen kertoimia, mutta tämä ei tosiaan liene yllätys, kun mietitään miten kertoimet on saatu laskettua. Kertoimet noudattavat binomilausekkeen $(x+y)^{n-1}$ kertoimia, eli kun häviävän kolmion viimeinen termi on n, niin vinorivin kertoimet saadaan Pascalin kolmion vastaavalta riviltä ylhäältä laskettuna, kunhan jätetään viimeinen termi, eli 1, pois. Yleisessä muodossa viimeinen luku sarjassa on

$$x_n = k_1 x_1 + k_2 D_1^1 + k_3 D_1^2 + k_4 D_1^3 + k_5 D_1^4 + \ldots,$$

joka jatkuu kunnes erotukset D_1^m, missä $m \in \{1, \ldots, n-2\}$ tulevat nolliksi. Kertoimet k_l, missä $l \in \{1, \ldots, n-1\}$ ovat samat, kuin binomilauseen 4.34 kertoimet tilanteessa $(x+y)^{n-1}$ eli

$$1, \frac{(n-1)}{1}, \frac{(n-1)(n-2)}{2 \cdot 1}, \frac{(n-1)(n-2)(n-3)}{3 \cdot 2 \cdot 1}, \ldots, \frac{(n-1)}{1}, 1.$$

Tällöin saadaan n-rivisen häviävän kolmion sääntö siten, että

$$x_n = x_1 + (n-1)D_1^1 + \frac{(n-1)(n-2)}{2 \cdot 1} D_1^2 + \frac{(n-1)(n-2)(n-3)}{3 \cdot 2 \cdot 1} D_1^3 + \cdots + \frac{(n-1)}{1} D_1^{n-2}.$$

Jokainen häviävän kolmion muodostama lukujono on edellisen kaltainen rakenteeltaan. [**8**][s.344-346].

LUKU 5

Mielenkiintoisia löytöjä

Poimitaan tähän kappaleeseen vielä muutamia mielenkiintoisia löytöjä, jotka liittyvät aikaisemmissa luvuissa käsiteltyihin asioihin etäisesti, mutta joita ei todisteta tai niitä ei ole pystytty vielä todistamaan, mutta joita mahdollisesti pystyy käyttämään koulumaailmassa niiden yksinkertaisen ymmärtämisen sekä hämmästyttävyyden takia.

5.1. Laskuvinkkejä

Tässä työssä on perehdytty erilaisiin lukujärjestelmiin ja erilaisiin lukujen esitystapoihin. Tarkastellaan vielä hieman laskemista helpottavia tekniikoita.

5.1.1. Kertolaskua kakkosen potenssilla. Melko hankalannäköisiäkin kertolaskuja pystytään laskemaan helpohkosti pelkästään kahden kertotaulun (tai kakkosen potenssin) ja yhteenlaskun avulla, kun hyödynnetään kakkosen potenssiin korotusta [**1**][s.117-118]. Menetelmässä kahdesta kerrottavasta luvusta ensimmäinen pilkotaan kakkosen potensseihin ja laaditaan taulukko, jossa jälkimmäistä kerrotaan kahden potensseilla ja joista lasketaan yhteen ensimmäisestä pilkottuja potensseja vastaavat luvut. Menetelmän idea on tuttu jo muinaisten egyptiläisten ajoilta, kuten voi todeta esimerkistä 1.1.

Esimerkki 5.1.

$$79 \cdot 62$$

Pilkotaan ensimmäinen tulontekijä kakkosen potensseiksi

$$79 = 1 + 2 + 4 + 8 + 64$$

Kertolaskutaulukko:

$$1 \cdot 62 = 62$$
$$2 \cdot 62 = 124$$
$$4 \cdot 62 = 248$$
$$8 \cdot 62 = 496$$
$$16 \cdot 62 = 992$$
$$32 \cdot 62 = 1984$$
$$64 \cdot 62 = 3968$$

Seuraavaksi poimitaan hajotelmaa vastaavat luvut taulukosta ja lasketaan yhteen. Näin ollen vastaukseksi saadaan

$$62 + 124 + 248 + 496 + 3968 = 4898$$

Tulon laskemisessa ei tarvitse siis osata muuta kuin kakkosella kertominen, sillä loppu on pelkkää yhteenlaskua.

5.1.2. Alkulukujen ominaisuuksia potenssissa. Salamalaskijat ovat taitavia päässälaskijoita, jotka pystyvät laskemaan käsittämättömän suurien lukujen tuloja, erikokoisia juuria ja muita, osaa laskuista jopa nopeammin kuin laskimella, jossa näppäilyyn menee aikaa. He käyttävät laskiessaan hyödyksi lukujen ominaisuuksia ja erilaisia laskemista helpottavia sääntöjä. Eräs tällainen sääntö on se, että vaikka lukua 13 pidetään yleisesti epäonnen lukuna, niin luvun kolmannellatoista juurella on sama viimeinen numero kuin luvussa, josta juuri otetaan ja mikäli juuri on kokonaisluku [**1**][s.147].

Edellä mainittu sääntö ei päde kaikille alkuluvuille, mutta esimerkiksi alkuluvuille 5, 13, 17, 29, ... kyllä.

Esimerkki 5.2. $\frac{1}{19} = 0,0526315789473684210\ldots$. Tässä työssä on keskitytty pääosin kokonaislukuihin, mutta nostetaan esille eräs mielenkiintoinen rationaaliluku, nimittäin $\frac{1}{19}$. Kun luku kirjoitetaan desimaalilukuna, niin luvussa toistuu sama numerosarja tietyn mittaisilla väleillä [**1**][s.157] ja se numerosarja on 18 numeroa pitkä eli 19-1 numeroa. Muitakin tällaisia lukuja löytyy, missä osoittajan ollessa 1 ja nimittäjän alkuluku, niin desimaaliluvussa toistuu jokin tietty numerosarja. Alkulukuja, missä alkuluku on $p < 100$ ja toistuva desimaali on $p - 1$ merkkiä pitkä, ovat 7, 17, 19, 23, 29, 47, 59, 61 ja 97.

Luvussa $\frac{1}{19}$ on muutakin mielenkiintoista, sillä jos tarkastellaan yhteen sarjaan kuuluvia numeroita, noudattavat ne kymmenkantaiseen järjestelmään muunnettujen binäärilukujen yhteenlaskua seuraavalla tavalla:

Aloitetaan yhteenlasku luvusta 0, lisätään aina seuraava luku siten että uuden luvun ykkösten kohdassa oleva luku tulee pykälän verran vasemmalle edelliseen verrattuna. Lasketaan siis edellä mainitulla tavalla luvut 0, 1, 2, 4, 8, 16, 32, ... yhteen, jolloin huomataan, että syntyvä summa noudattaa edellä esitellyn murtoluvun $\frac{1}{19}$

toistuvaa desimaalilukusarjaa.

20	97	15	2									
1	04	85	76									
	5	24	28	8								
		26	21	44								
		1	31	07	2							
			6	55	36							
				32	76	8						
				1	63	84						
					8	19	2					
						40	96					
						2	04	8				
							10	24				
								51	2			
								2	56			
									12	8		
										64		
										3	2	
											16	
												8
												4
												2
												1
				0,	05	26	31	57	89	47	36	84	21	0
	...		84	21	05	26	31	57	89	47	36	84	21	0

5.2. Goldbachin konjektuuri

Goldbachin (vahvan) konjektuurin mukaan, *jokainen lukua 2 suurempi parillinen luku on esitettävissä kahden alkuluvun summana.* Vaikka väite ei ole monimutkainen, sitä ei ole silti pystytty todistamaan todeksi tai epätodeksi, mutta niin pitkälle kun asiaa on voitu tarkastaa (tietokonetutkimuksilla), se pitää paikkansa. [**10**][s.19-20].

Esimerkki 5.3.

$4 = 2 + 2$
$6 = 3 + 3$
$8 = 3 + 5$
$10 = 5 + 5 = 3 + 7$
$\vdots$
$222 = 199 + 23$

$224 = 211 + 13$
$\vdots$

[**1**][s.257-258].

Kuten edeltä voidaan todeta alkulukujen summa ei ole yksikäsitteinen. Toinen merkille pantava seikka on se, että ensimmäinen parillinen luku on numero 2, joka on itsessään alkuluku. Ensimmäisen parillisen numeron puuttuminen ei kuitenkaan välttättä tarkoita sitä että joku muu suurempi parillinen luku olisi mahdoton ilmaista kahden alkuluvun summana.

Goldbachin heikko konjektuuri puolestaan on seuraava: *jokainen viittä suurempi kokonaisluku on kolmen alkuluvun summa*. Tämän konjektuurin todistus on tällä hetkellä tarkistettavana, mutta tähän asti kojektuuria ei ole pystytty todistamaan hyväksytysti kaikille kokonaisluvuille. Kumpikin konjektuuri on peräisin Goldbachin ja Eulerin toisilleen lähettämistä kirjeistä. Ensimmäisenä esitelty konjektuuri on näistä kuitenkin tunnetumpi.

Esimerkki 5.4.
$7 = 2 + 2 + 3$
$9 = 2 + 3 + 3 = 2 + 2 + 5$
$11 = 2 + 2 + 7 = 3 + 3 + 5$
$\vdots$

5.3. Luvun numeroilla laskemista

5.3.1. Persistenssi. Brittimatemaatikko Neil Sloane kerää kokoelmaa erilaisista jonoista. Osa jonoista on puhtaasti matemaattisia, mutta mukaan mahtuu myös muita jonoja, joille löytyy joku hyvä tai vähintään mielenkiintoinen peruste. Sloane päivittää *Encyclopedia* listaansa jatkuvasti ja se löytyy internetistä hakusanalla *"On-Line Encyclopedia of Integer Sequences"*. [**1**][s.255].

Sloane näkee paljon uusia matemaattisia ideoita ja kehittelee niitä itsekin. Vuonna 1973 hän kehitteli luvun *persistenssi* -käsitteen, jolla hän tarkoittaa sitä montako askelta tarvitaan yksinumeroisen luvun tuottamiseen useampilukuisesta numerosta. Askeleet lasketaan siten että ensin kerrotaan annetun luvun numerot keskenään, jolloin saadaan toinen luku ja kerrotaan tämän toisen luvun numerot keskenään, jolloin saadaan kolmas luku ja niin edelleen kunnes tuloksena saatu luku on yksinumeroinen.

Esimerkki 5.5.

- $79 \to 7 \cdot 9 = 63 \to 6 \cdot 3 = 18 \to 1 \cdot 8 = 8$
  Eli Sloanen mukaan luvun 79 persistenssi on 3.
- $71683 \to 1008 \to 0$
  Luvun 71683 persistenssi on siis 2. Olisi saattanut luulla että mitä suurempi luku on sitä suurempi on myös persistenssi, mutta kuten edellinen luku osoitti näin ei kuitenkaan ole.
- $277777788888899 \to 4996238671872 \to 438939648 \to 4478976 \to 338688 \to 27648 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$

Toistaiseksi suurin löydetty persistenssi on 11, vaikka lukuja on tutkittu lukuun 10^{233} asti. Mikäli tulosta saadussa uudessa luvussa esiintyy jossain kohtaa 0, on seuraava tulo aina 0 ja siten yksinumeroinen. Vaikka luku olisi kuinka suuri ja sisältäisi paljon suuria numeroita kuten 7, 8 ja 9, niin silti aina yhdenteentoista iteraatioon mennessä luku viimeistään sisältää nollan, ellei ole aiemmin jo muuttunut yksinumeroiseksi.

[**1**][s.259-260].

Sloane etsi jonon, jossa on mahdollisimman pienet vähintään kaksinumeroiset luvut siten, että askelia tulee n kappaletta. Pienin yhden askeleen luku on 10, kahden askeleen 25, kolmen askeleen 39 ja niin edelleen. Koko jono on:
$10, 25, 39, 77, 679, 6788, 68889, 2677889, 26888999, 3778888999, 277777788888899,$
joka löytyy *Encyclopediasta* jonona (A3001). [**1**][s.260]

Esimerkki 5.6.

- $10 \to 0$, persistenssi 1
- $25 \to 10 \to 0$, persistenssi 2
- $39 \to 27 \to 14 \to 4$, persistenssi 3
- $77 \to 49 \to 36 \to 18 \to 8$, persistenssi 4
- $679 \to 378 \to 168 \to 48 \to 32 \to 6$, persistenssi 5
- $6788 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$, persistenssi 6
- $68889 \to 27648 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$, persistenssi 7
- $2677889 \to 338688 \to 27648 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$, persistenssi 8
- $26888999 \to 4478976 \to 338688 \to 27648 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$, persistenssi 9
- $3778888999 \to 438939648 \to 4478976 \to 338688 \to 27648 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$, persistenssi 10
- $277777788888899 \to 4996238671872 \to 438939648 \to 4478976 \to 338688 \to 27648 \to 2688 \to 768 \to 336 \to 54 \to 20 \to 0$, persistenssi 11

5.3.2. Potenssiketju. Sloanen hyvä ystävä John Horton Conway on myöskin kiinnostunut kehittämään omalaatuisia matemaattisia käsitteitä. Hän keksi vuonna 2007 *potenssiketju*-käsitteen, jolla hän tarkoittaa että luvun $abcd\ldots$ potenssiketju on $a^b c^d \ldots$. Mikäli luvussa on pariton määrä numeroita jätetään viimeinen numero ilman potenssia. Myöskin tässä potenssiketjua toistetaan, kunnes jäljelle jää vain yksi numero.

Esimerkki 5.7.

- $2432 \to 2^4 \cdot 3^2 = 16 \cdot 9 = 144 \to 1^4 \cdot 4 = 4$
  Aina ei tietenkään käy niin että luvut pienenisivät koko ajan vaan saattaa olla että välivaiheessa on lähtöarvoa suurempiakin lukuja tulontekijöinä potenssiin korotuksen seurauksena. Conway halusi tietää onko olemassa sellaisia lukuja, jotka eivät palaudu yksinumeroisiksi potenssiketjukäsittelyssä ja hän löysi seuraavan luvun:
- $2592 \to 2^5 \cdot 9^2 = 32 \cdot 81 = 2592$

5.3.3. Dudeneyn numerot. Henry Ernest Dudeney oli kuuluisa, erinomainen pähkinöiden ratkaisija. Dudeney antoi kuitenkin panoksensa vahingossa myös lukuteorialle, sillä hänen nimeään kantavat numerot ovat lukuja joiden kuutiojuuret ovat yhtä suuria kuin niiden numeroiden summat. Lukuja on yhteensä 6 ja nämä ovat:

$$\begin{aligned} 1 &= (1)^3, \\ 512 &= (5+1+2)^3, \\ 4\,913 &= (4+9+1+3)^3, \\ 5\,832 &= (5+8+3+2)^3, \\ 17\,576 &= (1+7+5+7+6)^3, \\ 19\,683 &= (1+9+6+8+3)^3. \end{aligned}$$

[**1**][s.241].

5.3.4. Recamánin jono. Sloanen Encyclopediasta löytyy jono (A5132), jonka ensimmäiset termit ovat:
$0, 1, 3, 6, 2, 7, 13, 20, 21, 11, 22, 10, 23, 9, 24, 8, 25, 43, 62, 42, 63, 41, 18, 42, 17, 43, 16, 44, \ldots$
Äkkiseltään näyttäisi siltä ettei jonossa ole mitään selkeää johdonmukaisuutta. Sellainen siitä kuitenkin löytyy. Jonon termit määräytyvät yksinkertaisen säännön mukaan ”vähennä jos voit, muussa tapauksessa lisää”. Eli n:s termi saadaan vähentämällä tai lisäämällä edelliseen lukuun luvun n, kuitenkin sillä ehdolla että tulos on positiivinen, eikä se ole esiintynyt jonossa aikaisemmin.
0, 0. termi
$0 + 1 = 1$, ei voida vähentää, koska tulos menisi negatiiviseksi
$1 + 2 = 3$, ei voida vähentää, koska tulos menisi negatiiviseksi
$3 + 3 = 6$, ei voida vähentää, koska 0 esiintyy jo aikaisemmin jonossa
$6 - 4 = 2$,
$2 + 5 = 7$, ei voida vähentää, koska tulos menisi negatiiviseksi
$7 + 6 = 13$, ei voida vähentää, koska 1 esiintyy jo jonossa aikaisemmin
$13 + 7 = 20$, ei voida vähentää, koska 6 esiintyy jo jonossa aikaisemmin
$21 - 8 = 12$,
$12 + 9 = 21$, ei voida vähentää, koska tulos 3 esiintyy jo jonossa aikaisemmin
$\vdots$
Toistaiseksi ei olla pystytty varmistamaan kattaako kyseinen jono koko luonnollisten lukujen joukon, mutta toistaiseksi pienin luku, josta ei ole varmuutta kun 10^{25} numeroa on tutkittu on 852 655. [**1**][s.262-264].

Kirjallisuutta

[1] Alex Bellos: *Kiehtova matematiikka* ensimmäinen laitos, Bookwell Oy, 2011.

[2] Carl Boyer: *Tieteiden kuningatar, Matematiikan historia, osa I* toinen laitos, Art House, 1995.

[3] Carl Boyer: *Tieteiden kuningatar, Matematiikan historia, osa II* toinen laitos, Art House, 1995.

[4] W.A. Coppel: *Number Theory. An Introduction to Mathematics* toinen laitos, Springer, 2009.

[5] Anne-Maria Ernvall-Hytönen: Täydellisyyttä etsimässä *Solmu 1/2011 [s. 6-8] (http://solmu.math.helsinki.fi/2011/1/taydellinen.pdf)* viitattu 8.3.2014

[6] Graham Everest, Thomas Ward: *An Introduction to Number Theory* Springer, 2005.

[7] Graham Flegg: *Lukujen historia* ensimmäinen laitos, Art House, 2002.

[8] Lancelot Hogben: *Matematiikkaa kaikille* neljäs laitos, WSOY, 1955.

[9] Yrjö Karilas: *Antero Vipunen* yhdeksäs laitos, WSOY, 1985.

[10] Hannu Karttunen: *Tiedettä kaikille: Matematiikka* ensimmäinen laitos, Ursa, 2006.

[11] Matti Lehtinen: Roomalaiset numerot - laskentoa ilman kertotaulua *Solmu 1/2000-2001 [s. 16-18] http://solmu.math.helsinki.fi/2000/2/lehtinen/* viitattu 23.3.2014

[12] Kari Mikkola: Kurkistuksia Fibonaccin lukujen maailmaan *EDimensio 2009 http://www.maol.fi/fileadmin/users/EDimensio/2009/Fibonaccin maailma.pdf* viitattu 22.3.2014

[13] Frithiof Nevanlinna: *Johdatus lukuteoriaan ja algebraan* Otava, 1943.

[14] Veikko Nevanlinna: *Lukuteorian alkeet* ensimmäinen laitos, Jyväskylän yliopisto, 1988.

[15] Eirik Newth: *Totuuden jäljillä* ensimmäinen laitos, Tammi, 2002.

[16] Carol Vorderman: *Kiehtova matematiikka* WSOY, 1997.

[17] *http://www.digitoday.fi/tiede-ja-teknologia/2013/02/06/uusi-suurin-alkuluku-tayttaisi-28-romaania/20132017/66* viitattu 8.2.2014

[18] Matematiikan historian luentoja - Matti Lehtinen: *http://cc.oulu.fi/ matleh-ti/histluennot.pdf* viitattu 14.3.2014

[19] Peano's Axioms: *http://mathworld.wolfram.com/PeanosAxioms.html* viitattu 9.2.2014

Lisäksi tätä työtä tehdessä on käytetty hyväksi nettisivua "www.wolframalpha.com"