Tampereen yliopisto

Niko Satoniitty

FIBONACCIN LUKUJONO JA KONGRUENSSI

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Elokuu 2019

Tiivistelmä

Niko Satoniitty: Fibonaccin lukujono ja kongruenssi
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Elokuu 2019

Kyseessä olevassa työssä käsitellään Fibonaccin lukuja ja niiden sovelluksia. Työn alkuun on koottu muutamia lauseita ja identiteettejä erilliseen kappaleeseen. Varsinainen työ kuitenkin alkaa Fibonaccin luvun taustan ja historian kertomisella. Fibonaccin lukujen käsittelyn edetessä esitellään Fibonaccin lukujonon kaltainen toinen lukujono, Lucas'n lukujono. Lucas'n lukujono on käytännössä samankaltainen kuin Fibonaccin lukujono, mutta niiden rekursiivinen määritelmä eroaa alkuehtojen osalta toisistaan. Työssä esitellään näiden molempien lukujonojen perusominaisuudet lukijalle ja näiden suhteen lukijalta ei vaadita muuta pohjatietoja kuin matemaattisten todistusten ymmärtämistä.

Työn varsinainen pääpaino on kuitenkin näiden lukujonojen sovellusten käsittelyssä. Sovelluksia on valittu kaksi kappaletta ja ne ovat jaollisuus ja kongruenssi. Jaollisuuden ja kongruenssin määritelmät oletetaan ennaltaan lukijalle tutuiksi, mutta muuten kaikki todistuksissa tarvittavat tiedot esitellään teoksessa. Sovelluksista esitellään ensimmäisenä jaollisuus, jonka osana käsitellään myös suurin yhteinen tekijä Fibonaccin lukujen yhteydessä. Toisena sovelluksena käsitellään kongruenssin sovelluksia, jonka käsittelyyn on käytetty suunnilleen kolmannes työn kokonaispituudesta.

Avainsanat: Fibonaccin lukujono, Lucas'n lukujono, kongruenssi ja jaollisuus

Sisältö

1 Johdanto

Työn toteutus on rajoitettu Fibonaccin lukuihin ja yhteen sen kaltaiseen lukujonoon, Lucas'n lukujonoon. Näiden käsittely on toteutettu sovellusten käsittelyn edellyttämin määrin ja työn varsinainen painotus on näiden sovelluksissa. Sovelluksista käsittelyyn on valikoitu kaksi, jotka ovat jaollisuus ja kongruenssi. Työn alussa oleva luku 2 käsittelee pohjatietoja, jotka ovat välttämättömiä myöhempien aiheiden todistuksissa. Tähän osioon on koottu kokoelma erinäisiä lauseita ja identiteettejä, mutta näiden todistukset on sivuutettu, sillä ne eivät ole työn kannalta merkityksellisiä.

Luvun 3 aluksi käsitellään Fibonaccin luvun historiaa ja hieman lukujonon nimen taustaa. Tästä jatketaan varsinaiseen Fibonaccin luvun rekursiiviseen määritelmään, jota seuraa Fibonaccin perusominaisuuksia havainnollistavia lauseita. Tämä luku jatkuu Lucas'n lukujen rekursiivisella määritelmällä, jota seuraa lauseita Lucas'n lukujen perusominaisuuksista.

Tämän työn varsinaisena keskiönä ovat Fibonaccin ja Lucas'n luvun erilaiset sovellukset. Näistä sovelluksista ensimmäisenä esitellään joitakin jaollisuuden ominaisuuksia, jotka on koottu lukuun 4. Tämä luku alkaa esittelemällä lauseina erilaisia Fibonaccin ja Lucas'n lukujen yksinkertaisia jaollisuuden esimerkkejä. Luvun loppupuolella esitellään Fibonaccin ja Lucas'n lukujen yhteyttä suurimpaan yhteiseen tekijään.

Luvussa 5 esitellään Fibonaccin ja Lucas'n lukujen kongruenssien sovelluksia. Luvun aluksi esitellään Fibonaccin ja Lucas'n lukujen kongruenssien ominaisuuksia kokoelman muodossa. Tätä seuraavat todistukset Lucas'n ja Fibonaccin lukujen täydellisten neliöiden esiintymisestä. Luvun lopuksi on esitelty vielä joitain yleisiä Fibonaccin ja Lucas'n lukujen kongruensseja.

Lukijalta pohjatietoina vaaditaan jaollisuuden, kongruenssin ja suurimman yhteisen tekijän käsitteiden tunteminen sekä matemaattisen todistuksen ymmärtäminen niin induktiolla kuin suoralla todistuksella. Työn pääasiallisena pohjateoksena toimii Koshyn teos *Fibonacci and Lucas Numbers with Applications*. Muita lähteitä ovat Vorobievin teos *Fibonacci Numbers*, erinäiset artikkelit The Fibonacci Quarterlystä sekä Koshyn toinen teos *Elementary Number Theory with Applications*.

2 Valmistelevia tarkasteluja

Tähän lukuun on koottu teknisistä syistä myöhemmissä luvuissa esiintyville todistuksille välttämättömiä ja tärkeitä identiteettejä sekä erinäisiä lauseita. Tämän luvun tarkoituksena ei ole siis todistaa mitään, vaan vain listata tarvittavat tiedot myöhempiä lukuja varten. Tästä syystä tämän luvun kaikkien lauseiden todistukset on sivuutettu. Myöskin Fibonaccin lukujen F_n ja Lucas'n lukujen L_n määritelmät tulevat vasta luvussa 3.

Lause 2.1. *Kokoelma joitakin Fibonaccin ja Lucas'n lukujen identiteettejä.*

(2.1) $5F_n^2 = L_n^2 - 4(-1)^n$, vrt. [4, s. 97 kohta 39]

(2.2) $2L_{m+n} = L_m L_n + 5F_n F_m$, vrt. [4, s. 91 kohta 84]

(2.3) $L_{2n} = 5F_n^2 + 2(-1)^n$, vrt. [4, s. 97 kohta 42]

(2.4) $F_{2n} = F_n L_n$, vrt. [4, s. 96 kohta 29]

(2.5) $2F_{m+n} = F_m L_n + F_n L_m$, vrt. [4, s. 91 kohta 83]

(2.6) $F_{-n} = (-1)^{n-1} F_n$, vrt. [4, s. 405 kohta 17]

(2.7) $L_{-n} = (-1)^n L_n$, vrt. [4, s. 84 kohta 19]

(2.8) $L_{2n} = L_n^2 + 2(-1)^{n-1}$,
vrt. [4, s. 404 kohta 7, *Huomio* kirjassa painovirhe]

(2.9) Jos $n \equiv 0 \pmod 2$ ja $n \not\equiv 0 \pmod 3$,
niin $L_n \equiv 3 \pmod 4$, vrt. [4, s. 404 kohta 8]

(2.10) Jos $k \equiv 0 \pmod 2$ ja $k \not\equiv 0 \pmod 3$,
niin $L_{n+2k} \equiv -L_n \pmod{L_k}$, vrt. [4, s. 404 kohta 9]

(2.11) $F_{m+n} = L_n F_m - (-1)^n F_{m-n}$,
missä n ja m ovat kokonaislukuja, vrt. [6, s. 77]

(2.12) $L_{m+n} - L_{m-n} = L_m L_n$, missä n on pariton, vrt. [4, s. 91 kohta 86]

(2.13) $L_{m+n} + L_{m-n} = L_m L_n$, missä n on parillinen, vrt. [4, s. 91 kohta 85]

(2.14) $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$, vrt. [4, s. 363 kohta 3]

(2.15) $F_n = F_{n-m+1} F_m + F_{n-m} F_{m-1}$, vrt. [4, s.197]

(2.16) $F_{mn} = L_m F_{m(n-1)} + (-1)^{m+1} F_{m(n-2)}$, vrt. [4, s. 93 kohta 128]

(2.17) $F_{m+n} = F_{m+1} F_{n+1} - F_{m-1} F_{n-1}$, vrt. [4, s. 89 kohta 44]

(2.18) $L_n = F_{n-1} + F_{n+1}$, vrt. [4, s. 97 kohta 32]

(2.19) $L_{n-m} = (-1)^m(F_{n+1}L_m - F_nL_{m+1})$, vrt. [4, s. 599 kohta 43]

Lause 2.2. (Aritmetiikan peruslause) *Jokainen ykköstä suurempi kokonaisluku n on mahdollista esittää yksikäsitteisesti alkulukujen tulona:*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_m^{a_m},$$

missä $p_1 < p_2 < p_3 < \ldots < p_m$ *ovat alkulukuja ja* a_i *on kokonaisluku,* $i = 1, 2, \ldots, m$.

Todistus. Ks. [5, s. 171]. □

Lause 2.3. (Jakoyhtälö) *Oletetaan, että a on kokonaisluku ja b on positiivinen kokonaisluku. Tällöin on olemassa yksikäsitteiset q ja r siten, että*

$$a = b \cdot q + r,$$

missä $0 \leq r < b$.

Todistus. Ks. [5, s. 66]. □

Lause 2.4. *Olkoot a, b, c,* α *ja* β *kokonaislukuja.*

- *Jos* $a \mid b$ *ja* $b \mid c$, *niin* $a \mid c$.
- *Jos* $a \mid b$ *ja* $a \mid c$, *niin* $a \mid (\alpha b + \beta c)$.
- *Jos* $a \mid b$, *niin* $a \mid bc$.

Todistus. Ks. [5, s. 71]. □

Lause 2.5. Vrt. [4, s. 544]. *Jos* $(a, b) = 1$, *niin* $(b, a + b) = 1$.

Lause 2.6. $a \equiv b \pmod{m}$, *jos ja vain jos* $a = b + km$ *jollakin kokonaisluvulla k.*

Todistus. Ks. [5, s. 211]. □

3 Fibonaccin ja Lucas'n luvut

Tämän luvun käsittelyn taustan osio sekä Binet'n kaavojen esittely mukailee Koshyn teosta [4, s. 78], mutta välissä esitetty Fibonaccin lukujen ominaisuuksien esittely mukailee pääosin Vorobievin teosta. Kolmas osio Lucas'n luvun ominaisuuksista on saanut ideansa Koshyn teoksesta, mutta sisältö on kuitenkin määritelmää lukuunottamatta kirjoittajan omaa.

3.1 Fibonaccin lukujen taustaa

Matematiikan historian kerronta painottuu usein antiikin matematiikkaan. Yleisesti voidaankin sanoa, että antiikin matematiikan nimet, kuten Arkhimedes ja Eukleides, ovat useissa tapauksissa jo ennestään tuttuja. Keskiaikaiset matemaatikot eivät kuitenkaan ole saaneet osakseen samanlaista tunnustusta, koska keskiaikaisen matematiikan kehitys on ollut todella hidasta. Tämä työ painottuu kuitenkin yhden keskiajan suurimman matemaatikon tuottamaan julkaisuun *Liber Abaci (The Book of the Abacus)*. Kyseinen henkilö oli suuri italialainen matemaatikko nimeltään *Leonardo of Pisa* (Leonardo Pisalainen). Hänet tunnetaan paremmin lempinimellään Fibonacci, joka on lyhenne sanoista *filius Bonacci*, joka suomeksi tarkoittaa Bonaccin poikaa.

Fibonacci oli keskiaikaisen Euroopan merkittävin matemaatikko. Hänen elämänsä on kuitenkin jäänyt varsin tuntemattomaksi, sillä hänestä tunnetaan vain tiedot, jotka hän itse antoi osana matemaattisia tekstejään. Hänestä ei ole jäänyt mainintoja edes hänen aikaistensa kollegoiden säilyneisiin teksteihin. Fibonacci syntyi 1170 vuoden tienoilla ja kuoli noin 1240. Fibonacci tuotti useita tärkeitä matemaattisia julkaisuja, joista ensimmäisenä oli edellämainittu *Liber Abaci* (1202), josta hän kirjoitti toisen painoksen kuuden vuoden kuluttua. Tämän ensimmäisen työnsä jälkeen hän kirjoitti vielä kolme muuta merkittävää julkaisua, joista ensimmäisenä *Practica Geometriae (Practice of Geometry)* (1220). Viimeiset kaksi julkaisua hän kirjoitti vuonna 1225 *the Flos (Blossom of Flower)* ja *Liber Quadratorum (The Book of Square Numbers)*.

Fibonaccin ensimmäinen kirja sisältää melkein kaikki aikansa aritmeettiset ja algebralliset tiedot. Se sisälsi myös monia matemaattisia ongelmia, joista tunnetuimpana ongelmana on "kaniongelma". Tässä ongelmassa kysymys on siitä, kuinka monta paria kaneja yksi kanipari voi synnyttää vuodessa.

Oletetaan, että on kaksi juuri syntynyttä kania, yksi uros ja yksi naaras. Selvitetään kanien määrä vuoden lopussa, jos

- jokaisella parilla menee kuukausi saavuttaa sukukypsyys,
- jokainen pari tuottaa sekaparin joka kuukausi toisesta kuukaudesta alkaen,
- yhtään kania ei kuole vuoden aikana.

Havainnollistukseksi oletetaan, että ensimmäinen pari kaneja on syntynyt tammikuun ensimmäinen päivä ja ne ovat sukukypsiä helmikuun ensimmäinen päivä, koska niillä kuluu kuukausi sukukypsyyden saavuttamiseen. Ensimmäinen pari tuottaa siis ensimmäisen sekaparin helmikuun aikana ja näin ensimmäinen maaliskuuta pareja on kaksi, mutta vain alkuperäinen pari on sukukypsä. Huhtikuun alussa pareja on kolme, joista kaksi on sukukypsiä. Tätä samaa kaavaa jatketaan vuoden loppuun. Havainnollistuksen helpottamiseksi tulokset on esitetty alla olevassa taulukossa.

Taulukko 3.1. Kaniongelma

Parien määrä	Tammikuu	Helmikuu	Maaliskuu	Huhtikuu	Toukokuu	Kesäkuu
Aikuisia	0	1	1	2	3	5
Poikasia	1	0	1	1	2	3
Yhteensä	1	1	2	3	5	8
Parien määrä	Heinäkuu	Elokuu	Syyskuu	Lokakuu	Marraskuu	Joulukuu
Aikuisia	8	13	21	34	55	89
Poikasia	5	8	13	21	34	55
Yhteensä	13	21	34	55	89	144

Taulukon yhteensä-riveille muodostuvaa lukusarjaa kutsutaan Fibonaccin luvuiksi. Sarjan nimesi aikansa suuri ranskalainen matemaatikko François Edouard Anatole Lucas, joka oli aiemmin kutsunut sarjaa nimellä Lamén sarja ranskalaisen matemaatikko Gabriel Lamén mukaan. On varsin ironista, että huolimatta Fibonaccin useista matemaattisista saavutuksista hänet muistetaan pääosion hänen nimeään kantavasta lukusarjasta.

3.2 Fibonaccin lukujen yksinkertaisia ominaisuuksia

Edellä esitetyille Fibonaccin luvuille on mahdollista luoda rekursiivinen määritelmä, joka on esitetty seuraavaksi.

Määritelmä 3.1. Vrt. [4, s. 6]. Fibonaccin luvut F_n määritellään rekursiivisesti seuraavalla tavalla:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= F_2 = 1 \\ F_n &= F_{n-1} + F_{n-2}, \quad \text{kun } n \geq 3. \end{aligned}$$

Monet Fibonaccin luvun ominaisuuksista voidaan todistaa yksinkertaisesti matemaattisella induktiolla. Useat työhön kootut todistukset pohjautuvatkin induktioon, mutta joukossa on suoriakin todistuksia.

Lause 3.2. *Lasketaan ensimmäisten n Fibonaccin luvun summa:*

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$$

Todistus. Vrt. [7, s. 5]. Fibonaccin lukujen rekursiivisen määritelmän 3.1 perusteella voidaan esittää Fibonaccin luvut käänteisesti:

$$\begin{aligned} F_1 &= F_3 - F_2 \\ F_2 &= F_4 - F_3 \\ F_3 &= F_5 - F_4 \\ &\vdots \\ F_{n-1} &= F_{n+1} - F_n \\ F_n &= F_{n+2} - F_{n+1}. \end{aligned}$$

Nyt laskettaessa nämä yhtälöt termeittäin yhteen saadaan seuraava summa:

$$F_1 + F_2 + \cdots + F_n = F_{n+2} - F_2.$$

Koska $F_2 = 1$, niin lause $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$ on tosi. □

Seuraavat kaksi lausetta käsittelevät Fibonaccin lukujen summausten erityistapaukset siten, että ensimmäisenä on summa parittomalla järjestysluvulla olevista Fibonaccin luvuista ja toisena summa parillisella järjestysluvulla olevista Fibonaccin luvuista.

Lause 3.3. *Parittoman järjestysluvun Fibonaccin lukujen summa Fibonaccin lukuun F_{2n-1} saakka:*

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}.$$

Todistus. Vrt. [7, s. 5]. Tarkastelemalla Fibonaccin lukujen ominaisuuksia ja nojaten niiden rekursiiviseen määritelmään 3.1 voidaan helposti havaita, että järjestyksessä parittomat Fibonaccin numerot voidaan esittää niitä ympäröivien parillisten Fibonaccin lukujen erotuksena seuraavasti:

$$\begin{aligned} F_1 &= F_2 - F_0 \\ F_3 &= F_4 - F_2 \\ F_5 &= F_6 - F_4 \\ &\vdots \\ F_{2n-1} &= F_{2n} - F_{2n-2}. \end{aligned}$$

Nyt summattaessa edellä esitetyt yhtälöt yhteen saadaan lauseen mukainen summa:

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n} + F_0,$$

joten lause on tosi, koska $F_0 = 0$. □

Lause 3.4. *Parillisen järjestysluvun Fibonaccin lukujen summa Fibonaccin lukuun F_{2n} saakka:*

$$F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1.$$

Todistus. Vrt. [7, s. 6]. Todistetaan lause kahden edellisen lauseen 3.2 ja 3.3 avulla. Ensin lauseesta 3.2 saadaan summa:

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{2n+2} - 1.$$

Nyt tästä summasta vähennetään lauseen 3.3 summa:

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}.$$

Nyt vähennettäessä lauseen 3.2 summasta lauseen 3.3 summa saadaan:

$$\begin{aligned} F_2 + F_4 + \cdots + F_{2n} &= F_{2n+2} - 1 - F_{2n} \\ &= F_{2n} + F_{2n+1} - 1 - F_{2n}, \quad \text{(määritelmän 3.1 perusteella)} \\ &= F_{2n+1} - 1. \end{aligned}$$

□

Seuraava lause osoittaa, että kahden peräkkäisen Fibonaccin luvun suurin yhteinen tekijä on yksi.

Lause 3.5. *Kahden peräkkäisen Fibonaccin luvun suurin yhteinen tekijä*

$$(F_n, F_{n-1}) = 1.$$

Todistus. Vrt. [4, s. 75]. Todistetaan lause käyttäen matemaattista induktiota. Lause on selvästi tosi, kun

$$n = 1 : (F_1, F_{1-1}) = (1, 0) = 1.$$

Oletetaan nyt, että lause on tosi kokonaisluvuilla $n \leq k$ siten, että $k \geq 1$. Asetetaan seuraavaksi induktioväitteeksi, että lause on tosi luvulla $n = k + 1$, kun $k \geq 1$. Silloin

$$\begin{aligned}
(F_{k+1}, F_k) &= (F_k + F_{k-1}, F_k), && \text{(määritelmän 3.1 perusteella)} \\
&= (F_{k-1}, F_k), && \text{(lauseen 2.5 ja induktio-oletuksen perusteella)} \\
&= 1, && \text{(induktio-oletuksen perusteella).}
\end{aligned}$$

□

3.3 Lucas'n lukujen yksinkertaisia ominaisuuksia

Tässä osiossa käsitellään Lucas'n lukujonoa, joka on Fibonaccin lukujonon kaltainen lukujono. Myöhemmin havainnollistetaan, kuinka paljon Fibonaccin ja Lucas'n lukujonoilla on yhdenkaltaisia ominaisuuksia.

Määritelmä 3.6. Vrt. [4, s. 8]. Lucas'n luvut L_n määritellään rekursiivisesti seuraavalla tavalla:

$$\begin{aligned}
L_0 &= 2 \\
L_1 &= 1 \\
L_n &= L_{n-1} + L_{n-2}, \quad \text{kun } n \geq 2.
\end{aligned}$$

Seuraavien kolmen lauseen tulokset Lucas'n luvuista ja niiden todistukset käyttäytyvät samalla tavalla kuin edellä esitettyjen Fibonaccin lukujen vastaavat lauseet. Näiden varsinaiset todistukset ovat kuitenkin kirjoittajan omia, sillä kirjassa vain mainittiin, että samanlaiset ominaisuudet voidaan todistaa myös Lucas'n luvuille.

Lause 3.7. *Lasketaan ensimmäisten n Lucas'n luvun summa:*

$$L_1 + L_2 + L_3 + \cdots + L_n = L_{n+2} - 3.$$

(Vrt. lause 3.2)

Todistus. Lucas'n lukujen rekursiivisen määritelmän 3.6 perusteella voidaan esittää Lucas'n luvut käänteisesti:

$$\begin{aligned} L_1 &= L_3 - L_2 \\ L_2 &= L_4 - L_3 \\ L_3 &= L_5 - L_4 \\ &\vdots \\ L_{n-1} &= L_{n+1} - L_n \\ L_1 &= L_{n+2} - L_{n+1}. \end{aligned}$$

Laskettaessa yhtälöt yhteen termeittäin saadaan seuraava summa:

$$L_1 + L_2 + \cdots + L_n = L_{n+2} - L_2.$$

Koska $L_2 = 3$, niin lause on tosi. □

Lause 3.8. *Parittoman järjestysluvun Lucas'n lukujen summa n:teen Lucas'n lukuun L_{2n-1} saakka:*

$$L_1 + L_3 + L_5 + \cdots + L_{2n-1} = L_{2n} - 2.$$

(Vrt. lause 3.3)

Todistus. Tarkastelemalla Lucas'n lukujen ominaisuuksia ja nojaten niiden rekursiiviseen määritelmään 3.6 voidaan helposti havaita, että järjestyksessä parittomat Lucas'n luvut voidaan esittää niitä ympäröivien parillisten Lucas'n lukujen erotuksena seuraavasti:

$$\begin{aligned} L_1 &= L_2 - L_0 \\ L_3 &= L_4 - L_2 \\ L_5 &= L_6 - L_4 \\ &\vdots \\ L_{2n-1} &= L_{2n} - L_{2n-2}. \end{aligned}$$

Nyt summattaessa edellä esitetyt yhtälöt yhteen saadaan lauseen mukainen summa:

$$L_1 + L_3 + L_5 + \cdots + L_{2n-1} = L_{2n} - L_0.$$

Koska $L_0 = 2$, niin lause on tosi. □

Lause 3.9. *Parillisen järjestysluvun Lucas'n lukujen summa n:teen lukuun L_{2n} saakka :*

$$L_0 + L_2 + L_4 + \cdots + L_{2n} = L_{2n+1} - 1.$$

(Vrt. lause 3.4)

Todistus. Todistetaan lause kahden edellisen lauseen 3.7 ja 3.8 avulla. Ensin lauseesta 3.7 saadaan summa:

$$L_1 + L_2 + L_3 + \cdots + L_n = L_{2n+2} - 3.$$

Nyt edellä esitetystä summasta vähennetään lauseen 3.8 summa:

$$L_1 + L_3 + L_5 + \cdots + L_{2n-1} = L_{2n} - 2.$$

Nyt vähennettäessä lauseen 3.7 summasta lauseen 3.8 summa saadaan:

$$\begin{aligned} L_0 + L_2 + L_4 + \cdots + L_{2n} &= (L_{2n+2} - 3) - (L_{2n} - 2) \\ &= L_{2n+1} + L_{2n} - 3 - L_{2n} + 2, \quad \text{(määritelmän 3.6 perusteella)} \\ &= L_{2n+1} - 1. \end{aligned}$$

□

3.4 Binet'n kaavoja

Tässä luvussa käsitellään kaksi Binet'n kaavaa mukaillen Koshyn teoksen [4, s. 78] esityksen muotoa. Näiden käsittelyssä käytetään lukuja α ja β, jotka ovat muotoa:

$$\alpha = \frac{1 + \sqrt{5}}{2}, \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

Nämä ovat toisen asteen yhtälön $x^2 - x - 1 = 0$ juuria.

Nyt

$$\alpha + \beta = \frac{1 + \sqrt{5}}{2} + \frac{1 - \sqrt{5}}{2} = \frac{1 + \sqrt{5} + 1 - \sqrt{5}}{2} = 1,$$
$$\alpha - \beta = \frac{1 + \sqrt{5}}{2} - \frac{1 - \sqrt{5}}{2} = \frac{1 + \sqrt{5} - 1 + \sqrt{5}}{2} = \sqrt{5}$$

ja

$$\alpha \cdot \beta = \frac{1 + \sqrt{5}}{2} \cdot \frac{1 - \sqrt{5}}{2} = \frac{1^2 - \sqrt{5}^2}{2 \cdot 2} = -1.$$

Seuraavat kaksi Binet'n kaavaa on esitetty lauseina todistusten kanssa, kun kirjassa todistukset on ohitettu.

Lause 3.10. Vrt. [4, s. 79]. *Kaikilla* $n \geq 0$

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Todistus. Merkitään

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{5}},$$

missä $n \geq 0$. Nyt todistettaessa induktiolla luvun n suhteen, niin lause on selvästi tosi, kun

$$n = 0: \quad U_0 = \frac{\alpha^0 - \beta^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = \frac{0}{\sqrt{5}} = 0 = F_0,$$
$$n = 1: \quad U_1 = \frac{\alpha^1 - \beta^1}{\sqrt{5}} = \frac{\alpha - \beta}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1.$$

Nyt voidaan asettaa induktio-oletukseksi, että lause on tosi, kun $n \leq k$, missä $k \geq 1$. Täten induktioväite on $n = k + 1$, kun $k \geq 1$. Nyt

$$\begin{aligned}
F_{k+1} &= F_k + F_{k-1}, && \text{(määritelmän 3.1 perusteella)} \\
&= U_k + U_{k-1}, && \text{(induktio-oletuksen nojalla)} \\
&= \frac{\alpha^k - \beta^k}{\sqrt{5}} + \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}} \\
&= \frac{\alpha^k - \beta^k + \alpha^{k-1} - \beta^{k-1}}{\sqrt{5}} \\
&= \frac{\alpha^{k-1}(\alpha + 1) - \beta^{k-1}(\beta + 1)}{\sqrt{5}} \\
&= \frac{\alpha^{k-1}(\alpha^2) - \beta^{k-1}(\beta^2)}{\sqrt{5}} \\
&= \frac{\alpha^{k+1} - \beta^{k+1}}{\sqrt{5}} \\
&= U_{k+1}.
\end{aligned}$$

□

Lause 3.11. Vrt. [4, s. 79]. *Kaikilla* $n \geq 0$

$$L_n = \alpha^n + \beta^n.$$

Todistus. Merkitään

$$V_n = \alpha^n + \beta^n,$$

missä $n \geq 0$. Nyt todistettaessa induktiolla luvun n suhteen, niin lause on selvästi tosi, kun

$$\begin{aligned} n = 0: &\quad V_0 = \alpha^0 + \beta^0 = (1) + (1) = 2 = L_0, \\ n = 1: &\quad V_1 = \alpha^1 + \beta^1 = \alpha + \beta = 1 = L_1. \end{aligned}$$

Nyt voidaan asettaa induktio-oletukseksi, että lause on tosi, kun $n \leq k$, missä $k \geq 1$. Täten induktioväite on $n = k + 1$, kun $k \geq 1$. Nyt

$$\begin{aligned} L_{k+1} &= L_k + L_{k-1}, && \text{(määritelmän 3.6 mukaan)} \\ &= V_k + V_{k-1}, && \text{(induktio-oletuksen nojalla)} \\ &= \alpha^k + \beta^k + \alpha^{k-1} + \beta^{k-1} \\ &= \alpha^{k-1}(\alpha + 1) + \beta^{k-1}(\beta + 1) \\ &= \alpha^{k-1}(\alpha^2) + \beta^{k-1}(\beta^2) \\ &= \alpha^{k+1} + \beta^{k+1} \\ &= V_{k+1}. \end{aligned}$$

□

4 Fibonaccin ja Lucas'n lukujen jaollisuusominaisuuksia

4.1 Jaollisuus

Fibonaccin ja Lucas'n luvuilla on hyödyllisiä ja mielenkiintoisia jaollisuuden ominaisuuksia, joita esitellään niin myöhempien todistusten tueksi kuin lukijan tietouden laajentamiseksikin.

Lause 4.1. *Kaikilla positiivisilla kokonaisluvuilla m ja n,*

$$F_m \mid F_{mn}.$$

Todistus. Vrt. [4, s. 196].
Todistetaan lause käyttäen matemaattista induktiota. Lause on selvästi tosi, kun $n = 1$, sillä $F_m \mid F_m$. Oletetaan nyt, että lause on tosi luvuilla $n \leq k$ siten, että $k \geq 1$. Asetetaan induktioväitteeksi, että lause on tosi luvulle $n = k + 1$, kun $k \geq 1$. Nyt

$$\begin{aligned} F_{m(k+1)} &= F_{mk+m} \\ &= F_{mk}F_{m+1} + F_{mk-1}F_m, \quad \text{(identiteetin (2.14) perusteella).} \end{aligned}$$

Nyt induktio-oletuksen nojalla $F_m \mid F_{mk}$ ja edelleen $F_m \mid F_{m(k+1)}$, joten lause $F_m \mid F_{mn}$ on tosi. □

Lause 4.2. *$F_m \mid F_n$, jos ja vain jos $m \mid n$.*

Todistus. Vrt. [4, s. 197]. Oletetaan ensin, että $F_m \mid F_n$. Nyt

$$\begin{aligned} &F_m \mid F_n \\ &F_m \mid F_{n-m+1}F_m + F_{n-m}F_{m-1}, && \text{(identiteetin (2.15) perusteella)} \\ &F_m \mid F_{n-m}F_{m-1}, && \text{(lauseen 2.4 perusteella).} \end{aligned}$$

Nyt lauseen 3.5 perusteella, koska $(F_m, F_{m-1}) = 1$, niin $F_m \mid F_{n-m}$. Vastaavasti $F_m \mid F_{n-2m}$ ja edelleen $F_m \mid F_{n-qm}$. Nyt koska jakoyhtälön lauseen 2.3 perusteella $n = qm + r$, missä $0 \leq r < m$, niin voidaan kirjoittaa $F_m \mid F_r$. Tämä on mahdotonta ellei $r = 0$. Tästä seuraa, että $n = qm$. Siis jos $F_m \mid F_n$, niin $m \mid n$.

Vastaavasti oletetaan, että $m \mid n$. Siis $n = qm$ jollakin kokonaisluvulla q. Näin ollen edellisen lauseen nojalla $F_m \mid F_n$. □

Seuraava lause on esitetty alkuperäisessä lähteessä harjoitustehtävänä ilman todistusta.

Lause 4.3. Vrt. [4, s. 208]. *Kaikilla positiivisilla kokonaisluvuilla n,*

$$3 \mid n, \text{ jos ja vain jos } 2 \mid F_n.$$

Todistus. Oletetaan ensin, että $3 \mid n$. Nyt $n = 3m$ jollakin positiivisella kokonaisluvulla m. Siis lauseen 4.1 perusteella $F_3 \mid F_{3m}$ eli $2 \mid F_n$.

Vastaavasti oletetaan, että $2 \mid F_n$. Koska $F_3 = 2$, niin $F_3 \mid F_n$, ja siten lauseen 4.2 perusteella $3 \mid n$. □

Seuraavaksi esitellään apulause, joka on välttämätön seuraavan lauseen todistuksen kannalta. Apulause on esitetty alkuperäisessä lähteessä vain toteamuksella ja siinä esiintyy merkkivirhe. Tässä työssä se on esitetty apulauseena todistuksen kanssa.

Apulause 4.4. Vrt. [1, s. 16]. Aiemmin esitetyillä luvuilla α ja β sekä kaikilla positiivisilla kokonaisluvuilla k ja r, $(r \geq k)$:

$$(\alpha - \beta)F_r = \alpha^{r-k}L_k - \beta^k L_{r-k}.$$

Todistus. Osoitetaan yhtälön molemmat puolet saman suuruisiksi:

$$\begin{aligned}
\alpha^{r-k}L_k - \beta^k L_{r-k} &= \alpha^{r-k}(\alpha^k + \beta^k) - \beta^k(\alpha^{r-k} + \beta^{r-k}), && \text{(lauseen 3.11 perusteella)} \\
&= \alpha^{r-k+k} + \alpha^{r-k}\beta^k - \beta^k\alpha^{r-k} - \beta^{r-k+k} \\
&= \alpha^r - \beta^r \\
&= \frac{(\alpha^r - \beta^r)(\alpha - \beta)}{\alpha - \beta} \\
&= F_r(\alpha - \beta), && \text{(lauseen 3.10 perusteella).}
\end{aligned}$$

□

Lause 4.5. Vrt. [1, s. 15-16]. *Kaikilla positiivisilla kokonaisluvuilla k ja n*

$$L_k \mid F_n, \; jos \; ja \; vain \; jos \; 2k \mid n,$$

missä $k \geq 2$.

Lauseen todistuksen ensimmäinen puoli esitetään käyttäen matemaattista induktiota. Toisesta puolesta esitetty versio hyödyntää Binet'n kaavaa ja algebrallista lukuteoriaa. Työssä ei käsitellä erikseen algebrallista lukuteoriaa vaativaa osiota, mutta on haluttu esitellä kyseinen lause, koska lause on varsin merkityksellinen työn kannalta.

Todistus. Oletetaan, että $2k \mid n$. Siis n on muotoa $n = 2km$, $m \geq 1$.Todistetaan, että $L_k \mid F_{2km}$ käyttämällä matemaattista induktiota luvun m suhteen. Nyt väite on selvästi tosi, kun

$$m = 1: \quad L_k \mid F_{2k\cdot 1},$$

sillä identiteetin (2.4) perusteella

$$F_{2k} = F_k L_k.$$

Myös tapaus $m = 2$ pätee:

$$L_k \mid F_{4k},$$

sillä

$$\begin{aligned} F_{4k} &= F_{2k} L_{2k} \\ &= F_k L_k L_{2k}. \end{aligned}$$

Nyt voidaan asettaa induktio-oletukseksi, että lause on tosi kaikilla $m \leq \ell$ ja $\ell \geq 2$. Täten induktioväitteeksi tulee, että lause on tosi, kun $m = \ell + 1$. Nyt

$$\begin{aligned} F_{2k(\ell+1)} &= L_{2k} F_{2k((\ell+1)-1)} + (-1)^{2k+1} F_{2k((\ell+1)-2)}, \quad \text{(identiteetin (2.16) perusteella)} \\ &= L_{2k} F_{2k\ell} + (-1) F_{2k(\ell-1)}. \end{aligned}$$

Nyt induktio-oletuksen perusteella $L_k \mid F_{2k(\ell+1)}$, joten väite on tosi.

Vastaavasti oletetaan, että $L_k \mid F_n$. Nyt lauseen 2.3 perusteella $n = 2km + r$, kun $0 \leq r < 2k$. Näin ollen

$$\begin{aligned} F_n &= F_{2mk+r} \\ &= \frac{\alpha^{2mk+r} - \beta^{2mk+r}}{\alpha - \beta}, && \text{(lauseen 3.10 perusteella)} \\ &= \frac{\alpha^{2mk}\alpha^r - \beta^{2mk}\beta^r}{\alpha - \beta} \\ &= \frac{\alpha^{2mk}\alpha^r + (-\alpha^r\beta^{2mk} + \alpha^r\beta^{2mk}) - \beta^{2mk}\beta^r}{\alpha - \beta} \\ &= \frac{\alpha^r(\alpha^{2mk} - \beta^{2mk}) + \beta^{2mk}(\alpha^r - \beta^r)}{\alpha - \beta} \\ &= \frac{\alpha^r(\alpha^{2mk} - \beta^{2mk})}{\alpha - \beta} + \frac{\beta^{2mk}(\alpha^r - \beta^r)}{\alpha - \beta} \\ &= \alpha^r F_{2mk} + \beta^{2mk} F_r, && \text{(lauseen 3.10 perusteella).} \end{aligned}$$

Koska α^r on reaaliluku, mutta ei kokonaisluku, niin jakorelaatio tavallisessa mielessä ei ole mielekäs. Siirrytään soveltamaan algebrallista lukuteoriaa (yksityiskohdat sivuuttaen). Täten, koska aiemmin todistetun perusteella $L_k \mid F_{2mk}$, niin $L_k \mid F_r$. Riittää siis osoittaa, että $r = 0$. Tehdään vastaoletus, että $r > 0$. Tällöin $r > k$, koska $L_k \mid F_r$.

Nyt apulauseen 4.4 perusteella

$$(\alpha - \beta)F_r = \alpha^{r-k}L_k - \beta^k L_{r-k}.$$

Nyt $L_k \mid L_{r-k}$, koska $L_k \mid L_k$ ja $L_k \mid F_r$ ja β on yksikkö. Täten $r - k \geq k$, mistä seuraa, että $r \geq 2k$, mikä on ristiriita. □

Lause 4.6. Vrt. [1, s. 15-16]. *Positiivisilla kokonaisluvuilla k, m ja n*

$$L_m \mid L_n, \; jos \; ja \; vain \; jos \; n = (2k-1)m,$$

missä $m \geq 2$.

Tämä todistus koostuu kahdesta osasta, jotka perustuvat päättelyyn ja Fibonaccin ja Lucas'n lukujen identiteetteihin. Todistuksen ensimmäiseen suuntaan sai apua Koshyn teoksen [4, s. 599] harjoitustehtävien vihjeistä, mutta toinen suunta on kirjoittajan oma.

Todistus. Oletetaan ensin, että $n = (2k-1)m$, ja osoitetaan, että $L_m \mid L_{(2k-1)m}$, kun $k \geq 1$. Nyt

$$\begin{aligned} L_{(2k-1)m} &= L_{2kn-m} \\ &= (-1)^m(F_{2km+1}L_m - F_{2km}L_{m+1}), \qquad \text{(identiteetin (2.19) perusteella).} \end{aligned}$$

Nyt selvästi $L_m \mid L_m$ ja edellisen lauseen 4.5 perusteella $L_m \mid F_{2km}$. Täten $L_m \mid L_{(2k-1)m}$.

Vastaavasti oletetaan, että $L_m \mid L_n$. Olkoon r pienin ei-negatiivinen kokonaisluku, jolla $n = (2k-1)m + r$. Nyt jos $r \geq 2m$, niin $r = 2m + s$, kun $0 \leq s$. Joten

$$\begin{aligned} n &= (2k-1)m + 2m + s \\ &= ((2k-1) + 2)m + s \\ &= (2k+1)m + s. \end{aligned}$$

Tämä on ristiriita ja näin $0 \leq r < 2k$. Täten siis

$$\begin{aligned} L_n &= L_{(2k-1)m+r} \\ &= L_{(2km)-(m+r)} \\ &= (-1)^{m+r}(F_{2km+1}L_{m+r} - F_{2km}L_{m+r+1}), \quad \text{(identiteetin (2.19) perusteella).} \end{aligned}$$

Nyt lauseen 4.5 perusteella $L_m \mid F_{2km}$ ja $L_m \nmid F_{2km+1}$. Koska $(F_{2km+1}, F_{2km}) = 1$, niin $L_m \mid L_{m+r}$. Riittää osoittaa, että $r = 0$. Tehdään vastaoletus, että $r > 0$. Nyt identiteettien (2.12) ja (2.13) perusteella

$$L_{m+r} = L_m L_r - (-1)^r L_{m-r}.$$

Nyt selvästi $L_m \mid L_m$ ja näin $L_m \mid L_{m-r}$, joten $|m - r| \geq m$. Jos $m - r \geq 0$, niin $m - r \geq m$ eli $-r \geq 0$, mikä on mahdotonta. Jos taas $m - r < m$, niin $-m + r > m$ eli $r > 2m$, mikä on ristiriita. Täten edellisten perusteella $L_m \mid L_n$, jos ja vain jos $n = (2k - 1)m$. □

4.2 Suurin yhteinen tekijä

Tässä luvussa käsitellään Fibonaccin lukujen välisiä suurimpia yhteisiä tekijöitä. Aluksi esitellään pari apulausetta, jotka ovat välttämättömiä myöhempien lauseiden todistuksille.

Apulause 4.7. Kaikilla positiivisilla kokonaisluvuilla q ja n

$$(F_{qn-1}, F_n) = 1.$$

Todistus. Vrt. [4, s. 198].
Olkoon $d = (F_{qn-1}, F_n)$. Nyt $d \mid F_{qn-1}$ ja $d \mid F_n$. Lauseen 4.1 mukaan $F_n \mid F_{qn}$, joten $d \mid F_{qn}$. Näin ollen $d \mid F_{qn-1}$ ja $d \mid F_{qn}$, mutta lauseen 3.5 perusteella $(F_{qn-1}, F_{qn}) = 1$. Täten $(F_{qn-1}, F_n) = 1$, eli lause on tosi. □

Apulause 4.8. Jos $m = qn + r$, niin $(F_m, F_n) = (F_n, F_r)$.

Todistus. Vrt. [4, s. 198]. Oletetaan, että $m = qn + r$. Nyt

$$\begin{aligned} (F_m, F_n) &= (F_{qn+r}, F_n) \\ &= (F_{qn}F_{r+1} + F_{qn-1}F_r, F_n), && \text{(identiteetin (2.15) perusteella } \textit{Huomautus} \text{ kirjassa virhe)} \\ &= (F_{qn-1}F_r, F_n), && \text{(lauseen 4.1 perusteella)} \\ &= (F_r, F_n), && \text{(apulauseen 4.7 perusteella)} \\ &= (F_n, F_r). \end{aligned}$$

Täten lause, jos $m = qn + r$, niin $(F_m, F_n) = (F_n, F_r)$, on tosi. □

Lause 4.9. *Kaikilla positiivisilla kokonaisluvuilla m ja n*

$$(F_m, F_n) = F_{(m,n)}.$$

Todistus. Vrt. [4, s. 198]. Voidaan yleisyyttä menettämättä olettaa, että $m \geq n$. Nyt Eukleideen algoritmin avulla, kun m on jaettava ja n on jakaja, saamme seuraavan sarjan yhtälöitä:

$$\begin{aligned}
m &= q_0 n + r_1 && 0 \leq r_1 < n \\
n &= q_1 r_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

Nyt apulauseen 4.8 perusteella:

$$(F_m, F_n) = (F_n, F_{r_1}) = (F_{r_1}, F_{r_2}) = \cdots = (F_{r_{n-1}}, F_{r_n}).$$

Kuitenkin, koska $r_n \mid r_{n-1}$, niin lauseen 4.2 perusteella $F_{r_n} \mid F_{r_{n-1}}$. Täten $(F_{r_{n-1}}, F_{r_n}) = F_{r_n}$, joten edelleen $(F_m, F_n) = F_{r_n}$, mutta nyt Eukleideen algoritmin perusteella $r_n = (m, n)$. Täten $(F_m, F_n) = F_{(m,n)}$. □

5 Fibonaccin ja Lucas'n kongruenssi

5.1 Fibonaccin ja Lucas'n lukujen kongruenssiominaisuuksia

Tämä luku esittelee muutamia mielenkiintoisia kongruenssirelaation ominaisuuksia Fibonaccin sekä Lucas'n luvuille.

Lause 5.1. *Muutama Fibonaccin ja Lucas'n lukujen kongruenssi.*

(5.1) $L_n \equiv 0 \pmod 2$, *jos ja vain jos* $n \equiv 0 \pmod 3$.

(5.2) $L_n \equiv 0 \pmod 3$, *jos ja vain jos* $n \equiv 2 \pmod 4$.

(5.3) *Jos* $n \equiv 0 \pmod 2$ *ja* $n \not\equiv 0 \pmod 3$, *niin* $L_n \equiv 3 \pmod 4$.

(5.4) $L_{n+2k} \equiv -L_n \pmod{L_k}$, *kun* $k \equiv 0 \pmod 2$ *ja* $k \not\equiv 0 \pmod 3$.

(5.5) $F_{n+2k} \equiv -F_n \pmod{L_k}$, *kun* $k \equiv 0 \pmod 2$ *ja* $k \not\equiv 0 \pmod 3$.

(5.6) $L_{n+12} \equiv L_n \pmod 8$.

Huomautus. Kohtien (5.1), (5.5) ja (5.6) todistukset mukailevat kirjan todistuksia ja kohtien (5.2), (5.3) ja (5.4) todistukset ovat kirjoittajan omia.

Todistus. Vrt. [4, s. 403].
Kohta (5.1):

Oletetaan, että $L_n \equiv 0 \pmod 2$. Koska identiteetti (2.1) on $5F_n^2 = L_n^2 - 4(-1)^n$, niin $5F_n^2 \equiv 0 \pmod 2$ ja edelleen $F_n^2 \equiv 0 \pmod 2$, mistä seuraa $F_n \equiv 0 \pmod 2$. Siis $F_n \equiv 0 \pmod{F_3}$, joten lauseen 4.3 perusteella $n \equiv 0 \pmod 3$.

Vastaavasti oletetaan $n \equiv 0 \pmod 3$, joten Lauseen 4.3 perusteella $F_n \equiv 0 \pmod{F_3}$. Siis $F_n \equiv 0 \pmod 2$. Täten $5F_n^2 \equiv 0 \pmod 2$, josta seuraa identiteetin (2.1) perusteella, että $L_n^2 - 4(-1)^n \equiv 0 \pmod 2$ ja edelleen $L_n \equiv 0 \pmod 2$.

Kohta (5.2):

Oletetaan $L_n \equiv 0 \pmod 3$. Lauseen 2.6 perusteella oletus voidaan esittää muodossa $3 \mid L_n$. Lauseen 4.6 perusteella $L_m \mid L_n$, jos ja vain jos $n = (2k-1)m$, missä $m \geq 2$ ja $k \geq 1$. Koska $3 \mid L_n$, niin valitaan $m = 2$, sillä $L_2 = 3$. Edelleen lauseen 4.6 perusteella $n = (2k-1) \cdot 2 = 4k - 2$ ja nyt $n \equiv 2 \pmod 4$.

Vastaavasti oletetaan $n \equiv 2 \pmod 4$. Lauseen 2.6 mukaan oletuksen n on muotoa $4 \cdot t - 2$, missä t on kokonaisluku. Nyt lauseen 4.6 perusteella $L_m \mid L_n$, jos ja vain jos $n = (2k-1)m$, missä $m \geq 2$ ja $k \geq 1$. Luvun n ollessa muotoa $4 \cdot t - 2$ se voidaan esittää edellä esitetyn lauseen muodossa, kun asetetaan $m = 2$, eli $n = (2k-1) \cdot 2$. Nyt lauseen 4.6 perusteella seuraa $L_2 \mid L_n$, eli $3 \mid L_n$ ja edelleen $L_n \equiv 0 \pmod 3$.

Kohta (5.3):

Oletus 1: $n \equiv 0 \pmod 2$.
Oletus 2: $n \not\equiv 0 \pmod 3$.
Nyt oletuksen 1 ja lauseen 2.6 perusteella n on muotoa $2k$, missä k on kokonaisluku. Vastaavasti oletuksen 2, lauseen 2.6 ja kohdan (5.1) perusteella L_n on muotoa $2\ell + 1$, missä ℓ on kokonaisluku. Nyt

$$\begin{aligned}
L_n &= L_{2k}, && \text{(oletuksen 1 perusteella)} \\
&= L_k^2 + 2(-1)^{k-1}, && \text{(identiteetin (2.8) perusteella)} \\
&= (2\ell+1)^2 \pm 2, && \text{(oletuksen 2 perusteella)} \\
&= \begin{cases} 4\ell^2 + 4\ell + 1 + 2 \\ 4\ell^2 + 4\ell + 1 - 2 \end{cases} \\
&= \begin{cases} 4\ell^2 + 4\ell + 3 \\ 4\ell^2 + 4\ell - 1 \end{cases} \\
&\equiv \begin{cases} 3 \pmod 4 \\ -1 \pmod 4 \end{cases} \\
&\equiv 3 \pmod 4.
\end{aligned}$$

Kohta (5.4):

Oletetaan, että $k \equiv 0 \pmod 2$ ja $k \not\equiv 0 \pmod 3$. Koska identiteetin (2.2) perusteella $2L_{m+n} = L_m L_n + 5F_n F_m$, niin

$$\begin{aligned}
2L_{2k+n} &= L_{2k}L_n + 5F_n F_{2k}, && \text{(identiteetin (2.2) perusteella)} \\
&= L_n[5F_k^2 + 2(-1)^k] + 5F_n F_{2k}, && \text{(identiteetin (2.3) perusteella)} \\
&= L_n[L_k^2 - 4(-1)^k + 2(-1)^k] + 5F_n F_{2k}, && \text{(identiteetin (2.1) perusteella)} \\
&= L_n L_k^2 - 2(-1)^k L_n + 5F_n F_{2k} \\
&= L_n L_k^2 - 2(-1)^k L_n + 5F_n F_k L_k, && \text{(identiteetin (2.4) perusteella)} \\
&= -2L_n \pmod{L_k}.
\end{aligned}$$

Koska $k \not\equiv 0 \pmod 3$, niin kohdan (5.1) perusteella L_k on pariton. Siis $(2, L_k) = 1$. Joten $L_{n+2k} \equiv -L_n \pmod{L_k}$.

Kohta (5.5):

Oletetaan, että $k \equiv 0 \pmod 2$ ja $k \not\equiv 0 \pmod 3$. Silloin

$$\begin{aligned}
2F_{n+2k} &= F_n L_{2k} + F_{2k} L_n, && \text{(identiteetin (2.5) perusteella)} \\
&= F_n[5F_k^2 + 2(-1)^k] + F_{2k} L_n, && \text{(identiteetin (2.3) perusteella)} \\
&= F_n[L_k^2 - 4(-1)^k + 2(-1)^k] + F_{2k} L_n, && \text{(identiteetin (2.1) perusteella)} \\
&= F_n[L_k^2 - 2(-1)^k] + F_{2k} L_n \\
&= F_n L_k^2 - 2(-1)^k F_n + F_{2k} L_n \\
&= -2(-1)^k F_n + F_n L_k^2 + F_k L_k L_n, && \text{(identiteetin (2.4) perusteella)} \\
&= -2F_n \pmod{L_k}.
\end{aligned}$$

Koska $k \not\equiv 0 \pmod 3$, niin kohdan (5.1) perusteella L_k on pariton. Siis $(2, L_k) = 1$. Joten $F_{n+2k} \equiv -F_n \pmod{L_k}$.

Kohta (5.6):

Nyt

$$\begin{aligned}
2L_{n+12} &= L_n L_{12} + 5F_n F_{12}, && \text{(identiteetin (2.2) perusteella)} \\
&= L_n \cdot 322 + 5F_n \cdot 144 \\
&= 322L_n + 720F_n.
\end{aligned}$$

Joten

$$\begin{aligned}
L_{n+12} &= 161L_n + 360F_n \\
&\equiv 1L_n + 0F_n \pmod 8 \\
&\equiv L_n \pmod 8.
\end{aligned}$$

□

5.2 Lucas'n lukujen neliö

Tutkitaan, onko olemassa Lucas'n lukuja, jotka ovat täydellisiä neliöitä. Selviä esimerkkejä ovat $L_1 = 1$ ja $L_3 = 4$, jotka ovat täydellisiä neliöitä. Nyt kysymys onkin se, että onko tällaisia täydellisien neliön ominaisuuksia täyttäviä Lucas'n lukuja enempää.

Lauseen 5.3 käsittelyssä tarvitaan negatiivisia Lucas'n lukuja. Nyt kertauksena identiteetin (2.7) perusteella

$$L_{-n} = (-1)^n L_n.$$

Lause 5.2. *Jos L_n on täydellinen neliö x^2, niin $L_n = 1$ tai 4 eli $n = 1$ tai 3.*

Todistus. Vrt. [2, s. 110].
1 ja 4 ovat selvästi Lucas'n lukuja ja täydellisiä neliöitä.

Olkoon L_n täydellinen neliö eli $L_n = x^2$ jollakin kokonailuvulla x.

Tapaus 1. Oletetaan, että n on parillinen, joten se voidaan kirjoittaa muodossa $n = 2s$, missä s on kokonaisluku. Nyt identiteetin (2.8) nojalla $L_n = L_{2s} = L_s^2 + 2(-1)^{n-1}$. Koska L_s^2 on neliö, niin $L_s^2 + 2(-1)^{n-1}$ ei voi olla täydellinen neliö. Tämä on ristiriidassa alkuperäisen oletuksen kanssa.

Tapaus 2. Oletetaan, että n on pariton. Olkoon $n \equiv 1 \pmod 4$. Jos $n = 1$, niin $L_n = 1 = 1^2$, joka on täydellinen neliö. Nyt oletetaan, että $n > 1$. Koska $n > 1$ ja $n \equiv 1 \pmod 4$, niin voidaan lauseen 2.6 nojalla kirjoittaa $n = 1 + 4 \cdot p$, missä p on kokonaisluku. Aritmetiikan peruslauseen 2.2 perusteella voidaan $4 \cdot p$ kirjoittaa uudessa muodossa

$$\begin{aligned} 4 \cdot p &= 4 \cdot (2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m}) \\ &= 2 \cdot 2 \cdot (2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m}) \\ &= 2 \cdot 3^{a_2} \cdot (2^{a_1+1} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m}). \end{aligned}$$

Merkitään $k = (2^{a_1+1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m})$ ja $i = a_2$. Nyt saadaan muoto $n = 1 + 2 \cdot 3^i k$, kun $i \geq 0$ ja k on edellä määritellyn mukaan parillinen kokonaisluku, joka ei ole jaollinen luvulla 3. Nyt identiteetin (2.10) ehdot täyttyvät ja $L_n \equiv L_{1+2\cdot 3^i k} \equiv -L_1 \equiv -1 \pmod{L_k}$, koska -1 ei ole neliön jäännös modulo L_k (tarkempi todistus sivuutetaan), niin L_n ei voi olla neliö. Lopuksi, olkoon $n \equiv 3 \pmod 4$. Selvästi, kun $n = 3$, on $L_3 = 4 = 2^2$, mikä on täydellinen neliö. Joten oletetaan, että $n \neq 3$. Koska $n \equiv 3 \pmod 4$, niin $n = 3 + 4 \cdot p$, joten voidaan kirjoittaa samaan tapaan kuin aiemmin $n = 3 + 2 \cdot 3^i k$, kun $i \geq 0$ ja k on parillinen kokonaisluku, joka ei ole jaollinen luvulla 3. Jälleen identiteetin (2.10) ehdot täyttyvät ja $L_n \equiv L_{3+2\cdot 3^i k} \equiv -L_3 \equiv -4 \pmod{L_k}$ ja näin ollen L_n ei voi olla täydellinen neliö.

Edellisten perusteella ainoat Lucas'n luvut, jotka ovat täydellisiä neliöitä, ovat 1 ja 4.

□

Lause 5.3. *Jos L_n on muotoa $2x^2$, niin $n = 0$ tai ± 6.*

Todistus. Vrt. [2, s. 111].
Koska $x^2 \equiv 0, 1$ tai 4 (mod 8), niin $L_n = 2x^2 \equiv 0$ tai 2 (mod 8). Koska L_n on parillinen, niin kohdan (5.1) perusteella $n \equiv 0 \pmod 3$, eli $3 \mid n$.

Tapaus 1. Oletetaan, että n on pariton. Lauseen 2.6 perusteella voidaan olettaa, että n on muotoa $n = 12q + r$, missä q ja r ovat kokonaislukuja ja $0 \leq r < 12$. Koska n on pariton ja jaollinen luvulla 3, niin $r = 3$ tai 9. Täten $n = 12q + 3$ tai $12q + 9$. Jos $n = 12q + 3$, niin kohdan (5.6) nojalla $L_n = L_{12q+3} \equiv L_3 \equiv 4 \pmod 8$. Tämä on ristiriita, sillä alkuperäinen oletus oli, että $L_n = 0$ tai $2 \pmod 8$. Vastaavasti, jos $n = 12q + 9$, niin kohdan (5.6) nojalla $L_n = L_{12q+9} \equiv L_9 \equiv 4 \pmod 8$ ja samoin tämä on ristiriidassa oletuksen kanssa.

Tapaus 2. Oletetaan, että n on parillinen. Tällöin n on mahdollista esittää muodossa $n = 8t$, $8t \pm 2$ tai $8t + 4$ siten, että t on kokonaisluku. Mahdollisia parillisia jakojäännöksiä ovat tällöin 0, ± 2 ja $+4 \pmod 8$ ja huomioitavaa on, että jakojäännöksissä luku 6 vastaa lukua -2. Nyt, jos $n = 8t$ tai $n = 8t + 4$, niin $n \equiv 0 \pmod 4$. Jos $n = 0$, niin Lucas'n lukujen määritelmän perusteella $L_n = L_0 = 2 = 2 \cdot 1^2$. Nyt L_n saa halutun muodon. Jos $n \neq 0$, niin lauseen 2.6 avulla se on mahdollista kirjoittaa muodossa $n = 0 + 4p$, missä p on kokonaisluku. Tätä voidaan edelleen muokata tarkastelemalla erikseen kohtaa $4p$, mikä tapahtuu kuten lauseen 5.2 todistuksessa ja näin se on mahdollista kirjoittaa muodossa $n = 2 \cdot 3^i k$, kun $i \geq 0$ ja k on parillinen kokonaisluku, joka ei ole jaollinen luvulla 3. Nyt identiteetin (2.10) ehdot täyttyvät ja $2L_n \equiv 2L_{2 \cdot 3^i k} \equiv -2L_0 \equiv -4 \pmod{L_k}$. Täten $2L_n$ ei voi olla täydellinen neliö x^2, joten kontrapositiolla saadaan, että L_n ei voi olla muotoa $2x^2$. Oletetaan, että $n \equiv -2 \equiv 6 \pmod 8$. Jos $n = 6$, niin $L_6 = 18 = 2 \cdot 3^2$, mikä on tavoiteltua muotoa. Toisaalta, jos $n \neq 6$, niin n on mahdollista kirjoittaa kuten edellä ensin lauseen 2.6 avulla muotoon $n = 6 + 8h$, missä h on kokonaisluku. Aritmetiikan peruslauseen 2.2 avulla $8h$ on mahdollista kirjoittaa

$$\begin{aligned} 8 \cdot h &= 8 \cdot (2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m}) \\ &= 2 \cdot 2 \cdot 2 \cdot (2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m}) \\ &= 2 \cdot 3^{a_2} \cdot (2^{a_1+2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m}). \end{aligned}$$

Kirjoitetaan $l = (2^{a_1+2} \cdot 5^{a_3} \cdot 7^{a_4} \cdot \ldots \cdot m^{a_m})$ ja $j = a_2$. Nyt voidaan siis kirjoitta, että $n = 6 + 2 \cdot 3^j l$, missä l on jaollinen neljällä, mutta ei kolmella. Nyt $2L_n \equiv 2L_{6+2 \cdot 3^j l} \equiv -2L_6 \equiv -36 \pmod{L_l}$. Nyt kohtien (5.2) ja (5.3) perusteella -36 ei ole

neliönjäännös L_l. Siis kuten aiemmin L_n ei voi olla muotoa $2x^2$. Lopuksi jos $n \equiv 2 \pmod 8$, niin identiteetin (2.7) perusteella $L_{-n} = (-1)^n L_n$. Koska n on parillinen, niin $L_{-n} = L_n$. Joten $-n \equiv 6 \pmod 8$. Tästä seuraa $-n = 6$, joten $n = -6$.

Edellisen perusteella jos L_n on muotoa $2x^2$, niin $n = 0$ tai ± 6.

□

5.3 Fibonaccin lukujen neliö

Historiallisesti yksi vanhimmista oletuksista Fibonaccin lukujen yhteydessä on, että Fibonaccin lukujen ainoat täydelliset neliöt ovat 0, 1 ja 144. Tätä oletusta tutkittiin laajamittaisesti ennen seuraavan todistuksen muodostumista.

Lauseiden 5.4 ja 5.5 käsittelyssä tarvitaan negavisia Fibonaccin lukuja. Nyt kertauksena identiteetin (2.6) perusteella

$$F_{-n} = (-1)^{n-1} F_n.$$

Lause 5.4. *Jos F_n on täydellinen neliö x^2, niin $n = 0, \pm 1, 2$ tai 12.*

Todistus. Vrt. [2, s. 112].
Todistus muodostuu kahdesta osasta: parillisista ja parittomista luvun n arvoista.
Tapaus 1. Oletetaan ensin, että n on pariton eli $n \equiv \pm 1 \pmod 4$. Oletetaan $n \equiv 1 \pmod 4$. Jos $n = 1$, niin $F_n = 1$ ja 1^2 on täydellinen neliö. Jos $n \neq 1$, niin nyt n voidaan kirjoittaa lauseen 2.6 avulla muodossa $n = 1 + 4p$, kun p on kokonaisluku. Luku $4p$ voidaan muokata edelleen lauseen 5.2 todistuksen kanssa samaan tapaan muotoon $n = 1 + 2 \cdot 3^i \cdot k$, missä $i \geq 0$ ja k on parillinen kokonaisluku, joka ei ole jaollinen luvulla 3. Nyt kohdan (5.5) perusteella $F_n \equiv F_{1+2\cdot 3^i \cdot k} \equiv -F_1 = -1 \pmod{L_k}$. Täten F_n ei voi olla täydellinen neliö. Toisaalta jos oletetaan $n \equiv -1 \equiv 3 \pmod 4$, niin identiteetin (2.6) nojalla $-n \equiv 1 \pmod 4$. Joten $F_{-n} = F_n$, siis alkuosan perusteella $-n = 1$ ja täten $n = -1$.

Tapaus 2. Oletetaan kyseessä olevan parillinen n eli $n = 2s$ jollakin kokonaisluvulla s. Nyt identiteetin (2.4) perusteella $F_n = F_{2s} = F_s L_s = x^2$.

Oletetaan $3 \mid n$ ja nyt lauseen 4.3 perusteella $2 \mid F_n$. Joten $F_s = 2y^2$ ja $L_s = 2z^2$, missä y ja z ovat kokonaislukuja. Nyt kohdan (5.3) perusteella $\frac{n}{2} = s = 0$ tai ± 6, joten $n = 0$ tai $n = \pm 12$. Kun $n = 0$, niin $F_s = F_0 = 0 = 2 \cdot 0^2$, ja vastaavasti, kun $n = 12$, niin $F_s = F_6 = 8 = 2 \cdot 2^2$, mutta kun $n = -12$, niin identiteetin (2.6) perusteella $F_s = F_{-6} = (-1)^5 F_6 = -8$, mikä ei ole muotoa $2y^2$, joten n on joko 0 tai 12.

Vastaavasti, jos oletetaan, että $3 \nmid n$, niin lauseen 4.3 perusteella F_n ei ole parillinen. Tällöin $F_s = y^2$ ja $L_s = z^2$, missä y ja z ovat kokonaislukuja. Nyt kohdan (5.2) perusteella $\frac{n}{2} = s = 1$ tai 3, joten $n = 2$ tai 6. Kun $n = 2$, niin $F_s = F_1 = 1^2$, mikä on täydellinen neliö, mutta kun $n = 6$ ja $F_s = F_3 = 2$, niin se ei ole täydellinen neliö.

On siis todistettu, että F_n on täydellinen neliö vain, kun $n = 0, \pm 1, 2$ tai 12. □

Lause 5.5. *Jos F_n on muotoa $2x^2$, niin $n = 0, \pm 3$, tai 6.*

Todistus. Vrt. [2, s. 112].

Tapaus 1. Valitaan ensin, että n on pariton eli $n \equiv \pm 1 \pmod 4$.

Oletetaan $n \equiv -1 \equiv 3 \pmod 4$. Kun $n = 3$, niin $F_n = F_3 = 2 = 2 \cdot 1^2$, mikä on tavoitellussa muodossa. Jos $n \neq 3$, niin lauseen 2.6 avulla voidaan kirjoittaa $n = 3 + 4p$, missä p on kokonaisluku ja $4p$ on mahdollista muokata edelleen kuten lauseen 5.2 todistuksessa. Nyt saatu muoto on $n = 3 + 2 \cdot 3^i \cdot k$, missä $i \geq 0$ ja k on parillinen kokonaisluku, joka ei ole jaollinen luvulla 3. Nyt kohdan (5.5) perusteella $2F_n \equiv 2F_{3+2\cdot 3^i \cdot k} \equiv -2F_3 \equiv -4 \pmod{L_k}$, eli tästä seuraa, että $2F_n$ ei ole täydellinen neliö x^2, joten F_n ei voi olla muotoa $2x^2$ kontraposition perusteella. Oletetaan $n \equiv 1 \equiv -3 \pmod 4$, mikä identiteetin (2.6) nojalla on $-n \equiv 3 \pmod 4$ ja $F_{-n} = F_n$, joten aikaisemman perusteella $-n = 3$. Siis $n = -3$.

Tapaus 2. Valitaan, että n on parillinen, joten se voidaan kirjoittaa $n = 2s$ jollakin kokonaisluvulla s. Nyt identiteetin (2.4) perusteella $F_n = F_{2s} = F_s L_s = 2x^2$. Joten joko ($F_s = y^2$ ja $L_s = 2z^2$) tai ($F_s = 2y^2$ ja $L_s = z^2$), missä y ja z ovat kokonaislukuja. Nyt lauseiden 5.3 ja 5.4 perusteella ainoa muuttujan s arvo, mikä toteuttaa yhtälöt $F_s = y^2$ ja $L_s = 2z^2$ on $s = 0$, joten $n = 0$. Oletetaan, että $F_s = y^2$ ja $L_s = 2z^2$. Nyt lauseen 5.2 mukaan $s = 1$ tai 3, mutta F_1 ei ole muotoa $2y^2$, joten $s \neq 1$. Kuitenkin $F_3 = 2 \cdot 1^2$ on muotoa $F_s = 2y^2$, joten $n = 6$.

Siis F_n on haluttua muotoa muuttujan n arvoilla $0, \pm 3$ ja 6.

□

5.4 Yleisiä Fibonaccin ja Lucas'n kongruensseja

Apulause 5.6. Olkoon p alkuluku. Tällöin

$$L_p \equiv 1 \pmod p.$$

Apulauseen todistus hyödyntää Binet'n kaava sekä Fermat'n pientä lausetta. Varsinainen todistus kuitenkin sivuutetaan, koska se ei ole työn kannalta oleellinen,

mutta sen tulos on kuitenkin välttämätön seuraavien lauseiden kannalta.

Todistus. Ks. [4, s. 410]. □

Lause 5.7. *Olkoon p alkuluku ja $n \geq 0$. Silloin $F_{np} \equiv F_n F_p \pmod{p}$.*

Todistuksen alku eroaa kirjan todistuksesta, mutta loppu mukailee sitä. Todistus on toteutettu käyttäen matemaattista induktiota.

Todistus. Vrt. [3, s. 550]. Lause on selvästi tosi, kun $n = 0$

$$F_{0 \cdot p} = F_0 = 0 = 0 \cdot F_p = F_0 F_p.$$

Vastaavasti, kun $n = 1$, niin

$$F_{1 \cdot p} = F_p = 1 \cdot F_p = F_1 F_p.$$

Nyt tehdään oletus, että lause pätee ei-negatiivisella kokonaisluvulla $n \leq k$. Asetetaan induktioväitteeksi, että lause pätee, kun $n = k + 1$. Nyt

$$\begin{aligned}
F_{(k+1)p} &= F_{kp+p} \\
&= F_{kp} L_p - (-1)^n F_{kp-p}, && \text{(identiteetin (2.11) perusteella)} \\
&= F_{kp} L_p + (-1)^{n+1} F_{kp-p} \\
&\equiv F_{kp} + F_{(k-1)p} \pmod{p}, && \text{(apulauseen 5.6 perusteella)} \\
&= F_k F_p + F_{k-1} F_p, && \text{(induktio-oletuksen nojalla)} \\
&= (F_k + F_{k-1}) F_p \\
&= F_{k+1} F_p, && \text{(määritelmän 3.1 perusteella).}
\end{aligned}$$

Täten $F_{np} \equiv F_n F_p \pmod{p}$ jokaiselle alkuluvulle p ja jokaiselle ei-negatiiviselle kokonaisluvulle n. □

Lause 5.8. *Olkoon p alkuluku ja $n \geq 0$. Silloin*

$$L_{np} \equiv L_n L_p \equiv L_n \pmod{p}.$$

Todistus. Vrt. [3, s. 550]. Todistetaan lause käyttäen matemaattista induktiota. Lause on selvästi tosi, kun $n = 0$:

$$\begin{aligned}
L_{0 \cdot p} &= L_0 \\
&= 2 \\
&= 1 \cdot 2 \\
&\equiv 2 \cdot L_p \pmod{p}, && \text{(apulauseen 5.6 perusteella)} \\
&\equiv L_0 L_p \pmod{p}.
\end{aligned}$$

Vastaavasti, kun $n = 1$:

$$L_{1\cdot p} = L_p = 1 \cdot L_p = L_1 L_p.$$

Nyt tehdään induktio-oletus, että lause pätee kaikilla ei-negatiivisilla kokonaisluvuilla $n \leq k$. Asetetaan induktioväitteeksi, että lause pätee, kun $n = k + 1$. Nyt

$$\begin{aligned}
L_{(k+1)p} &= L_{kp+p} \\
&= L_{kp}L_p - (-1)^n L_{kp-p}, && \text{(identiteettien (2.12) ja (2.13) perusteella)} \\
&= L_{kp}L_p + (-1)^{n+1} L_{kp-p} \\
&\equiv L_{kp} + L_{(k-1)p} \pmod{p}, && \text{(apulauseen 5.6 perusteella)} \\
&\equiv L_k L_p + L_{k-1} L_p \pmod{p}, && \text{(induktio-oletuksen nojalla)} \\
&= (L_k + L_{k-1}) L_p \\
&= L_{k+1} L_p, && \text{(määritelmän 3.6 perusteella).}
\end{aligned}$$

Täten $L_{np} \equiv L_n L_p \pmod{p}$ jokaiselle alkuluvulle p ja jokaiselle ei-negatiiviselle kokonaisluvulle n. □

Lähteet

[1] Carlitz, L. *A Note On Fibonacci Numbers* The Fibonacci Quarterly, 1964, 1:2 (February), 15-28

[2] Cohn, J. H. E. *Square Fibonacci Numbers, Etc.*, The Fibonacci Quarterly, 1964, 2:2 (April), 109-113.

[3] Desmond, J. E. *Elementary Problems and Solutions* The Fibonacci Quarterly, 1970, 8:5 (December), 549-550.

[4] Koshy, T. *Fibonacci and Lucas Numbers with Applications*. New York: Wiley, 2001.

[5] Koshy, T. *Elementary number theory with applications*. San Diego: Harcourt/Academic Press company, 2002.

[6] Ruggles, D. I. *Some Fibonacci Results Using Fibonacci-Type Sequences* The Fibonacci Quarterly, 1963, 1:2 (April), 75 - 80.

[7] Vorobiev, N. N. *Fibonacci Numbers* Berlin: Birkhäuser Verlag, 2002.