Pisano-jaksot Fibonaccin lukujonoissa moduleilla m

Iiris Saresma

LuK-tutkielma
Huhtikuu 2026

Tarkastajat:
Dos. Jyrki Lahtonen

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Iiris Saresma: Pisano-jaksot Fibonaccin lukujonoissa moduleilla m
LuK-tutkielma, 39 s., 12 liites.
Matematiikka
Huhtikuu 2026

Tässä tutkielmassa esitellään Fibonaccin lukujonon ominaisuuksia, kun Fibonaccin luvut esitetään modulin $m \in \mathbb{N}$ suhteen. Tutkielman päätavoitteena on ilmaista muodostuvan jaksollisen lukujonon Pisano-jakson pituus luvun m avulla. Ensin tarkastellaan tapauksia, joissa m on alkuluku, ja lopulta palautetaan yleisen modulin tapaukset edelliseen.

Asiasanat: Fibonaccin lukujono, Fibonaccin luvut modulo m, Pisano-jakso.

Sisällys

1 Johdanto

Fibonaccin lukujono

$$1, 1, 2, 3, 5, 8, 13, 21, ...$$

on peräisin Leonardo Pisalaisen eli Fibonaccin (n. 1170-1240) aritmetiikkaa käsittelevästä teoksesta *Liber abaci* (1202). Fibonaccin luvut määrittelevä rekursioyhtälö

$$F_n = F_{n-1} + F_{n-2}$$

ei kuitenkaan todistettavasti ollut käytössä ennen 1600-lukua. [7, Luku 1.]

Fibonaccin lukujonon ominaisuuksia tutkitaan yhä [6, Luku 3.1.2]. Tämä tutkielma perustuu erääseen Fibonaccin lukujen ominaisuuteen: Valittiinpa mikä tahansa luonnollinen luku m, löydetään tällä luvulla jaollinen Fibonaccin luku. Tutkielmassa tullaan osoittamaan, että luvulla m jaollisia Fibonaccin lukuja on äärettömästi, ja ne vieläpä esiintyvät lukujonossa säännöllisesti. Nämä ominaisuudet nähdään helposti sellaisesta lukujonosta, jossa kukin Fibonaccin lukujonon alkio esitetään jakojäännöksenä luvun m suhteen. Tällaisessa lukujonossa jokainen luvulla m jaollinen Fibonaccin alkio kuvautuu luvuksi 0. Näin muodostetun lukujonon huomataan olevan aina jaksollinen, ja lyhyintä mahdollista jaksoa kutsutaan Leonardo Pisalaisen mukaan Pisano-jaksoksi.

Tutkielmassa esitellään luonnollisen luvun m suhteen muodostetun Pisano-jakson ominaisuuksia keskittyen erityisesti jakson pituuteen. Luvun m määrittämän Pisano-jakson pituutta ei voida suoraan ilmaista laskematta Fibonaccin lukujonon alkioita modulo m. Tutkielmassa kuitenkin näytetään, kuinka jakson pituus riippuu luvun m tekijöiden, erityisesti alkulukutekijöiden, Pisano-jaksojen ominaisuuksista.

Ennen Pisano-jaksojen käsittelyä tutkielmassa esitellään Fibonaccin lukujonon ominaisuuksia, kuten yleisiä jäseniä kuvaavat kaava ja matriisiesitys. Näitä voidaan hyödyntää myös modulin m suhteen esitetyn Fibonaccin lukujonon tapauksessa.

2 Fibonaccin lukujono

Määritelmä 1. *Fibonaccin lukujono* $(F_n) = F_0, F_1, F_2...$ muodostetaan määrittelemällä jäsenet $F_0 = 0$ ja $F_1 = 1$, sekä ehto $F_n = F_{n-1} + F_{n-2}$, kun $n \geq 2$.

Fibonaccin lukujono jatkuu loputtomasti, sillä kaksi edellistä jäsentä määräävät aina seuraavan jäsenen rekursiokaavan avulla. Taulukossa 1 luetellaan Fibonaccin lukujonon (F_n) jäsenet $F_0, F_1, ..., F_9$.

n :	0	1	2	3	4	5	6	7	8	9	...
F_n :	0	1	1	2	3	5	8	13	21	34	...

Taulukko 1: Fibonaccin lukujono (F_n).

Määritelmä 2. *Yleistetty Fibonaccin lukujono* (g_n) on lukujono, jonka jäsenet täyttävät ehdon

$$g_n = g_{n-1} + g_{n-2} \tag{1}$$

kaikilla kokonaislukuindekseillä n [10].

Yleistetyn Fibonaccin lukujonon alkiot määräytyvät yksikäsitteisesti kahden annetun alkuarvon perusteella. Fibonaccin lukujono (F_n) kuuluu yleistettyjen Fibonaccin lukujonojen joukkoon, alkuarvoiksi valittuna $F_0 = 0$ ja $F_1 = 1$. Rekursiivisen ehdon (1) ja alkuarvojen avulla lukujonoa voidaan jatkaa myös negatiivisiin kokonaislukuindekseihin:

$$\begin{gathered} \text{Rekursiokaava (1)} \iff \\ g_{n-2} = g_n - g_{n-1}, \end{gathered} \tag{2}$$

joten esimerkiksi $F_{-1} = F_{1-2} = F_1 - F_{1-1} = 1 - 0 = 1$.

2.1 Fibonaccin lukujono modulo m

Määritelmä 3. Lukujonon $(F_n^{(m)})$ alkioina ovat Fibonaccin luvut, jotka on esitetty modulin $m \in \mathbb{N}$ suhteen. Lukujonon $(F_n^{(m)})$ jäsenet kuuluvat jäännösluokkien (mod m) joukkoon $\mathbb{Z}_m$. [10]

Indeksin i Fibonaccin lukua vastaa lukujonon $(F_n^{(m)})$ alkio $F_i^{(m)}$, joka on pienin sellainen ei-negatiivinen kokonaisluku a, että $F_i \equiv a \pmod{m}$. Esimerkiksi

$$(F_n^{(5)}) = 0, 1, 1, 2, 3, 0, 3...,$$

koska $F_5 = 5 \equiv 0 \pmod{5}$ ja $F_6 = 8 \equiv 3 \pmod{5}$.

Lause 1. *Lukujono* $(F_n^{(m)})$ *on yleistetty Fibonaccin lukujono modulin* m *suhteen, eli* $F_n^{(m)} \equiv F_{n-1}^{(m)} + F_{n-2}^{(m)} \pmod{m}$.

Todistus. Fibonaccin lukujono kuuluu yleistettyjen Fibonaccin lukujonojen joukkoon, joten kaikilla $n \in \mathbb{Z}$ on voimassa $F_n = F_{n-1} + F_{n-2}$. Kun tämä esitetään modulin m jakoalgoritmin avulla, saadaan yhtälö

$$(d_n \cdot m + r_n) = (d_{n-1} \cdot m + r_{n-1}) + (d_{n-2} \cdot m + r_{n-2}),\ d_i \in \mathbb{Z},\ 0 \leq r_i < m,$$

joka vastaa kongruenssia

$$r_n \equiv r_{n-1} + r_{n-2} \pmod{m}.$$

Lukujonon $(F_n^{(m)})$ ja jakoalgoritmin jäännöksen r_i määritelmien perusteella $r_i = F_i^{(m)}$, joten rekursiokaava

$$F_n^{(m)} \equiv F_{n-1}^{(m)} + F_{n-2}^{(m)} \pmod{m}$$

on voimassa. □

$n:$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$F_n^{(3)}:$	$\underline{0}$	1	1	2	0	2	2	1	$\underline{0}$	1	1	2	0	2	2	...
$F_n^{(4)}:$	$\underline{0}$	1	1	2	3	1	$\underline{0}$	1	1	2	3	1	$\underline{0}$	1	1	...

Taulukko 2: Fibonaccin lukujonot modulo 3 ja modulo 4.

Taulukossa 2 esitetään lukujonojen $(F_n^{(3)})$ ja $(F_n^{(4)})$ alut. Nähdään, että alleviivatut jäsenet jakavat lukujonon toistuviin jaksoihin, joita kutsutaan *Pisano-jaksoiksi*. Huomio jaksollisuudesta voidaan yleistää:

Lause 2. *Lukujono* $(F_n^{(m)})$ *on jaksollinen jokaisella modulilla* $m \in \mathbb{N}$.

Todistus. Koska on olemassa vain m mahdollista jäännöstä $a \in \mathbb{Z}_m$ ja $(F_n^{(m)})$ koostuu vain näistä jäännöksistä, mahdollisia $(F_i^{(m)}, F_{i+1}^{(m)})$-pareja on $m \cdot m$ kappaletta, erityisesti siis äärellinen määrä. Lukujono on kuitenkin päättymätön, joten ainakin yhden mahdollisista pareista on esiinnyttävä uudelleen.

Lisäksi lauseen 1 mukaan $(F_n^{(m)})$ täyttää yleistetyn Fibonaccin lukujonon ehdon (1), joten mikä tahansa pari $(F_i^{(m)}, F_{i+1}^{(m)})$ määrää lukujonon kaikki seuraavat jäsenet. Lukujono on siis jaksollinen jos ja vain jos ensimmäisenä uudelleen toistuva pari on alkuarvopari $(F_0^{(m)}, F_1^{(m)}) = (0, 1)\ \forall m > 1$.

Oletetaan ettei näin ole, eli ensimmäisenä toistuva pari on (x, y), missä $x = F_j^{(m)} \neq 0$ ja $y = F_{j+1}^{(m)} \neq 1$ jollain $j > 0$. Lukujono on siis muotoa

$$(F_n^{(m)}) = 0, 1, ..., x, y, ..., x, y, ...,$$

missä pari $(0, 1)$ ei esiinny toistuvan parin (x, y) esiintymien välillä. Rekursiokaavasta (2) kuitenkin seuraa, että pari (x, y) määrää lukujonon yksikäsitteisesti myös pieneneville indekseille. Koska pari $(0, 1)$ esiintyy ennen ensimmäistä parin (x, y) esiintymää, sen on esiinnyttävä myös välillä $x, y, ..., x, y$. Muutoin parin (x, y) määräämä lukujono pieneneville indekseille ei olisi yksikäsitteinen. Nyt pari $(x, y) \neq (0, 1)$ ei ole ensimmäinen toistuva pari, mikä on ristiriita oletuksen kanssa. Ensimmäinen toistuva peräkkäisten jäsenten pari on siis $(0, 1)$, joka myös aloittaa aina uuden jakson. Siten $(F_n^{(m)})$ on jaksollinen kaikilla $m > 1$. [7, s. 17]

Jos taas $m = 1$, $(F_0^{(m)}, F_1^{(m)}) = (0, 0)$, jolloin lukujonon $(F_n^{(0)})$ jaksollisuus on selvä. □

Esitettiinpä Fibonaccin lukujonon alkiot minkä tahansa modulin $m \in \mathbb{N}$ suhteen, muodostuva lukujono $(F_n^{(m)})$ on jaksollinen. Oletetaan vastaisuudessa, että $m > 1$, jolloin lukujono $(F_n^{(m)})$ alkaa alkioilla $F_0^{(m)} = 0$ ja $F_1^{(m)} = 1$ ja jokainen Pisano-jakso parilla $(0, 1)$.

2.2 Fibonaccin lukujonon matriisiesitys

Fibonaccin lukujono ja sen ominaisuuksia voidaan esittää myös matriisien avulla. Alaluvun tulokset ovat peräisin Robinsonilta [9].

Fibonaccin lukujonossa on voimassa rekursiokaava $F_{n+1} = F_n + F_{n-1}$. Kun Fibonaccin lukuja ajatellaan pareina (F_{n-1}, F_n) ja (F_n, F_{n+1}) ja määritellään matriisi

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

rekursiokaava täyttyy yhtälössä

$$(F_{n-1}, F_n)U = (0 \cdot F_{n-1} + F_n, F_{n-1} + F_n) = (F_n, F_{n+1}).$$

Induktion avulla voidaan myös näyttää, että

$$(F_n, F_{n+1}) = (0, 1)U^n, \tag{3}$$

missä

$$U^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}, \tag{4}$$

jota kutsutaan Fibonaccin lukua F_n vastaavaksi matriisiksi. Matriisi U^n voidaan esittää muodossa

$$U^n = I + dM, \tag{5}$$

missä I on indentiteettimatriisi $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $d \in \mathbb{Z}$ ja M on jokin sopiva 2×2-matriisi.

Matriisin esitysmuodosta (3) nähdään, että $(F_n, F_{n+1}) \equiv (0, 1) \pmod{m}$ jos ja vain jos matriisi U^n on kongruentti identiteettimatriisin kanssa modulo m. Silloin matriisin U^n alkiolle

$$F_{n-1} \equiv F_{n+1} \equiv 1 \pmod{m} \text{ ja } F_n \equiv 0 \pmod{m},$$

eli pari (F_n, F_{n+1}) aloittaa uuden jakson lukujonossa $(F_n^{(m)})$. Kun $U^n \equiv I \pmod{m}$, yhtälössä (5) on voimassa $d \equiv 0 \pmod{m}$.

2.3 Lukujonon yleinen jäsen

Fibonaccin lukujonon yleiselle jäsenelle F_n voidaan johtaa kaava, jota käytettäessä ei tarvitse tuntea jonon edellisiä alkioita.

Lukujonolle (a_n), joka on muotoa

$$a_0 = c_0, a_1 = c_1 \text{ ja } a_n = Aa_{n-1} + Ba_{n-2} \ \forall n \geq 2,$$

missä $A, B \in \mathbb{R}$ ja $B \neq 0$, voidaan muodostaa lukujonon rekursiokaavaa vastaava *karakteristinen yhtälö*

$$x^2 = Ax + B.$$

Jos karakteristisella yhtälöllä on kaksi juurta, α ja β, yleiselle jäsenelle tunnetaan kaava

$$a_n = K_1\alpha^n + K_2\beta^n, \tag{6}$$

missä K_1 ja K_2 voidaan laskea tunnettujen jäsenten $a_0 = c_0$ ja $a_1 = c_1$ avulla. Tarkemmin aiheesta todistuksineen voi lukea lähteestä [1, luku 10.]

Määritelmästä 1 nähdään, että Fibonaccin lukujonon tapauksessa karakteristinen yhtälö on $x^2 = x + 1$, jolla on juuret $\alpha = \frac{1+\sqrt{5}}{2}$ ja $\beta = \frac{1-\sqrt{5}}{2}$. Nyt tunnettujen jäsenten $F_0 = 0$ ja $F_1 = 1$ avulla saadaan yhtälöryhmä

$$\begin{cases} F_0 = K_1(\frac{1+\sqrt{5}}{2})^0 + K_2(\frac{1-\sqrt{5}}{2})^0 = K_1 + K_2 = 0 \\ F_1 = K_1(\frac{1+\sqrt{5}}{2})^1 + K_2(\frac{1-\sqrt{5}}{2})^1 = K_1(\frac{1+\sqrt{5}}{2}) + K_2(\frac{1-\sqrt{5}}{2}) = 1, \end{cases}$$

josta voidaan ratkaista $K_1 = \frac{1}{\sqrt{5}}$ ja $K_2 = -\frac{1}{\sqrt{5}}$. Nyt kaavan (6) perusteella yleistä jäsentä F_n kuvaava *Binet'n kaava* on

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

Binet'n kaava

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

toimii myös lukujonon $(F_n^{(m)})$ alkioille, jos alkiot $F_n^{(m)}$ kuuluvat sellaiseen kuntaan K, että yhtälöllä

$$x^2 = x + 1 \tag{7}$$

on kunnassa K kaksi toisistaan eroavaa ratkaisua α ja β. Nyt yhtälön (7) ratkaisut

$$\frac{1+\sqrt{5}}{2} \text{ ja } \frac{1-\sqrt{5}}{2}$$

vaativat uuden, kunnasta K riippuvan tulkinnan. Ensinnäkin jakolaskun luvulla $2 \pmod m$ tulee olla määritelty, joten vaaditaan $m \neq 2$. Myös $\sqrt{5}$ on tulkittava uudelleen:

Jos luku 5 on neliönjäännös modulo m, löydetään sellainen lukua $\sqrt{5}$ vastaava kokonaisluku a, että $a^2 \equiv 5 \pmod m$. Muistetaan, että jäännösluokkarengas $\mathbb{Z}_m$ on kunta vain jos moduli m on alkuluku $p \in \mathbb{P}$ [3, Seuraus 3.1.7]. Nyt voidaan merkitä kunnaksi K kunta $\mathbb{Z}_p$ ja juuriksi $\alpha = \frac{1+a}{2}$ ja $\beta = \frac{1-a}{2}$, jotka ovat erisuuria kun $a \not\equiv 0 \pmod p$. Tapauksessa $a \equiv 0 \pmod p$ voimassa on myös $a^2 \equiv 0$, mikä on totta silloin ja vain silloin, kun $p = 5$, koska määriteltiin $a^2 \equiv 5 \pmod p$.

Jos taas luku 5 ei ole neliönjäännös, eli yhtälöllä $x^2 \equiv 5 \pmod m$ ei ole kokonaislukuratkaisua x, käytetään merkintää $\mathbb{Z}_m[\sqrt{5}]$ siitä renkaasta, jonka alkiot ovat

muotoa $a + b\sqrt{5},\ a, b \in \mathbb{Z}_m$. Tämän kanssa isomorfinen rengas saadaan myös polynomirenkaan tekijärenkaana $\mathbb{Z}_m[x]/I$ samaistamalla $\sqrt{5}$ ja sivuluokka $x + I$. Tässä I on renkaassa $\mathbb{Z}_m[x]$ jaottoman polynomin $x^2 - 5$ generoima ihanne. [3, Luvut 3.6 ja 3.7.]

Myös renkaan $\mathbb{Z}_p[\sqrt{5}]$ tiedetään olevan kunta vain kun $m = p \in \mathbb{P}$. Tällöin Binet'n kaavan erisuuret vakiot

$$\alpha = \frac{1+\sqrt{5}}{2} = 2^{-1} + 2^{-1}\sqrt{5} \text{ ja } \beta = \frac{1-\sqrt{5}}{2} = 2^{-1} - 2^{-1}\sqrt{5}$$

kuuluvat kuntaan $K = \mathbb{Z}_p[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}_p\}$.

Seuraavan lauseen ja sen avulla muotoillun seurauksen avulla voidaan helposti määrittää, käsitelläänkö modulin $p \in \mathbb{P} \setminus \{2, 5\}$ tapauksessa kuntaa $\mathbb{Z}_p$ vai kuntaa $\mathbb{Z}_p[\sqrt{5}]$.

Lause 3. *Kun $p > 2$,*

(i) 5 on neliönjäännös modulo p, jos $p \equiv \pm 1 \pmod 5$.

(ii) 5 ei ole neliönjäännös modulo p, jos $p \equiv \pm 2 \pmod 5$.

Todistus.

(i) 5 on neliönjäännös $\pmod p$, jos Legendren symboli $(\frac{5}{p}) = 1$.

Neliönjäännösten resiprookkilain [5, 3.18] mukaan

$$\begin{aligned}(\frac{5}{p})(\frac{p}{5}) &= (-1)^{(\frac{p-1}{2})(\frac{5-1}{2})} \\ &= (-1)^{p-1} = 1,\end{aligned}$$

koska $p > 2$ on pariton. Siis on oltava $(\frac{5}{p}) = (\frac{p}{5})$. Nyt oletuksen muotoa $p = 5r + 1$ ja $p = 5r - 1,\ r \in \mathbb{N}$, oleville alkuluvuille

$$(\frac{5}{p}) = (\frac{5r+1}{5}) = (\frac{1}{5}) = 1,$$

ja

$$(\frac{5}{p}) = (\frac{5r-1}{5}) = (\frac{-1}{5}) = 1,$$

koska $(\frac{a}{p}) = (\frac{b}{p})$ jos $a \equiv b \pmod p$, $1^2 \equiv 1 \pmod p$ ja $2^2 \equiv -1 \pmod 5$. Siis 5 on neliönjäännös modulo $p \equiv \pm 1 \pmod 5$.

(ii) Vastaavasti 5 ei ole neliönjäännös $\pmod p$, jos Legendren symboli $(\frac{5}{p}) = -1$. Jälleen $(\frac{5}{p}) = (\frac{p}{5})$, joten kun $p = 5r \pm 2$, saadaan

$$(\frac{5}{p}) = (\frac{5r+2}{5}) = (\frac{2}{5}) = -1$$

respirookkilain toisella täydennyslauseella [5, 3.16], ja

$$(\frac{5}{p}) = (\frac{5r-2}{5}) = (\frac{-2}{5}) = (\frac{-1}{5}) \cdot (\frac{2}{5}) = 1 \cdot (-1) = -1$$

multiplikatiivisuuden ja aiempien laskujen perusteella. Näin ollen 5 ei ole neliönjäännös modulo $p \equiv \pm 2 \pmod 5$. [7, Lemma 3.9.]

□

Lauseen 3 avulla voidaan koota yhteen, missä alkulukutapauksissa lukujonon $(F_n^{(p)})$ yleinen jäsen voidaan selvittää:

Seuraus 1. *Lukujonon* $(F_n^{(p)})$, $p \in \mathbb{P}$ *ja* $p > 2$, *yleinen jäsen saadaan kaavalla*

$$F_n^{(p)} \equiv \frac{\alpha^n - \beta^n}{\alpha - \beta} \pmod{p}, \tag{8}$$

jos

(i) $p \equiv \pm 1 \pmod 5$, *jolloin yhtälön* (7) *erisuuret juuret* $\alpha = \frac{1+a}{2}$ *ja* $\beta = \frac{1-a}{2}$ *ovat kunnassa* $\mathbb{Z}_p$. *Tässä* $a \neq -a$ *ja* $(\pm a)^2 \equiv 5 \pmod p$.

(ii) $p \equiv \pm 2 \pmod 5$, *jolloin yhtälöllä* (7) *on erisuuret juuret* $\alpha = \frac{1+\sqrt{5}}{2}$ *ja* $\beta = \frac{1-\sqrt{5}}{2}$ *kunnassa* $\mathbb{Z}_p[\sqrt{5}]$.

Binet'n kaava kattaa kaikki alkulukutapaukset lukuja 2 ja 5 lukuun ottamatta. Lukujonosta $(F_n^{(2)}) = 0, 1, 1, 0, 1, ...$ nähdään, että $F_n^{(2)} = 0$, kun $3 \mid n$, ja 1 muulloin. Tapaukseen $p = 5$ liittyen tullaan huomaamaan, että lukujonon $(F_n^{(5)})$ ominaisuudet poikkeavat muiden lukujonojen $(F_n^{(p)})$, $p \in \mathbb{P}$, ominaisuuksista.

Lause 4. *Yhtälöllä* $x^2 \equiv x + 1 \pmod p$ *on yksi kaksinkertainen juuri tarkalleen silloin, kun* $p = 5$.

Todistus. Olkoon r yhtälön kaksinkertainen juuri. Voidaan johtaa seuraava ekvivalenssiketju:

$$\begin{aligned} x^2 - x - 1 \equiv &(x - r)^2 = x^2 - 2xr + r^2 \pmod p \\ &\iff 2r \equiv 1 \text{ ja } r^2 \equiv -1 \pmod p \\ &\iff 4r^2 \equiv 1 \text{ ja } 4r^2 \equiv -4 \pmod p \\ &\iff 0 \equiv 5 \pmod p \iff p = 5, \end{aligned}$$

mistä väite käy ilmi. [12, s.528.] □

Esimerkki 1. Tutkitaan Binet'n kaavaa lukujonojen $(F_n^{(29)})$ ja $(F_n^{(7)})$ tapauksissa.

Alkuluvut 29 ja 7 ovat muotoa $5r-1$ ja $5s+2$, joten seurauksen 1 mukaan yleinen jäsen voidaan selvittää Binet'n kaavalla (8). Selvitetään karakteristisen yhtälön (7) juuret α ja β kummallekin alkuluvulle.

Seurauksen 1 mukaan tapauksessa $p = 29$ juuret kuuluvat kuntaan $\mathbb{Z}_{29}$. Koska $(\pm 11)^2 = 121 \equiv 5 \pmod{29}$, saadaan juuret $\alpha = \frac{1+11}{2} = 6$ ja $\beta = \frac{1-11}{2} = -5 \equiv 24 \pmod{29}$. Kun Binet'n kaava esitetään muodossa

$$F_n^{(p)} \equiv \frac{1}{\alpha - \beta} \cdot (\alpha^n - \beta^n) \pmod{p},$$

voidaan tapauksessa $p = 29$ laskea

$$\frac{1}{\alpha - \beta} = \frac{1}{-18} \equiv 11^{-1} = 8 \pmod{29}.$$

Taulukosta 3 nähdään, että jokaisella indeksin n arvolla $F_n^{(29)} \equiv 8 \cdot (6^n - 24^n) \pmod{29}$, mikä on Binet'n kaava jäsenelle $F_n^{(29)}$.

Tapauksessa $p = 7$ yhtälöllä (7) on kuntaan $\mathbb{Z}_7[\sqrt{5}]$ kuuluvat juuret $\alpha = 2^{-1} + 2^{-1}\sqrt{5} = 4 + 4\sqrt{5}$ ja $\beta = 2^{-1} - 2^{-1}\sqrt{5} = 4 + 3\sqrt{5}$. Nyt kertoimeksi $\frac{1}{\alpha-\beta}$ saadaan $\sqrt{5}^{-1} = 3\sqrt{5}$, ja taulukosta 4 nähdään, että $F_n^{(7)} = 3\sqrt{5}((4 + 4\sqrt{5})^n - (4 + 3\sqrt{5})^n)$ kaikilla indeksin n arvoilla.

Taulukoista nähdään myös, että lukujonot $(\alpha^n \pmod p)$, $(\beta^n \pmod p)$ ja $(\alpha^n - \beta^n \pmod p)$ ovat yleistettyjä Fibonaccin lukujonoja.

n :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$\alpha^n = 6^n \pmod{29}$:	1	6	7	13	20	4	24	28	23	22	16	9	25	5	1	...
$\beta^n = 24^n \pmod{29}$:	1	24	25	20	16	7	23	1	24	25	20	16	7	23	1	...
$\alpha^n - \beta^n \pmod{29}$:	0	11	11	22	4	26	1	27	28	26	25	22	18	11	0	...
$F_n^{(29)}$:	0	1	1	2	3	5	8	13	21	5	26	2	28	1	0	...

Taulukko 3: Lukujonon $(F_n^{(29)})$ yleinen jäsen karakteristisen yhtälön juurien potenssien avulla.

n :	0	1	2	3	4	5	...
$\alpha^n = (4 + 4\sqrt{5})^n \pmod 7$:	1	$4 + 4\sqrt{5}$	$5 + 4\sqrt{5}$	$2 + \sqrt{5}$	$5\sqrt{5}$	$2 + 6\sqrt{5}$	...
$\beta^n = (4 + 3\sqrt{5})^n \pmod 7$:	1	$4 + 3\sqrt{4}$	$5 + 3\sqrt{5}$	$2 + 6\sqrt{5}$	$2\sqrt{5}$	$2 + \sqrt{5}$	...
$\alpha^n - \beta^n \pmod 7$:	0	$\sqrt{5}$	$\sqrt{5}$	$2\sqrt{5}$	$3\sqrt{5}$	$5\sqrt{5}$	...
$F_n^{(7)}$:	0	1	1	2	3	5	...

Taulukko 4: Lukujonon $(F_n^{(7)})$ yleinen jäsen karakteristisen yhtälön juurien potenssien avulla.

Yleistä jäsentä F_n kuvaavan Binet'n kaavan lisäksi Fibonaccin lukujonon jäsenille voidaan esittää myös muita laskemista helpottavia kaavoja. Ne esitetään lemmassa 1, ja niiden todistukset löytyvät lähteestä [7, luku 1.]

Lemma 1. *Fibonaccin lukujonon alkioille F_n ja F_k, $n, k \in \mathbb{Z}$, ovat voimassa seuraavat tulokset:*

(i) $(F_n, F_{n+1}) = 1$, *eli peräkkäiset luvut ovat suhteellisia alkuluja*

(ii) $F_{n+k} = F_{n-1}F_k + F_nF_{k+1}$

(iii) $F_{k-n} = (-1)^n(F_kF_{n+1} - F_{k+1}F_n)$

(iv) $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$

(v) $F_n^2 + F_{n+1}^2 = F_{2n+1}$.

3 Pisano-jakson pituus

Kuten lauseesta 2 kävi ilmi, modulin $m \in \mathbb{N}$ avulla esitetyt Fibonaccin luvut muodostavat jaksollisen lukujonon, ja yhtä tällaista jaksoa kutsutaan Pisano-jaksoksi. Pisano-jaksojen pituudet vaihtelevat: modulilla $m = 29$ jakson pituus on 14, modulilla $m = 30$ vastaava luku on 120 [11]. Tässä luvussa esitetään arvioita Pisano-jakson pituudesta eri moduleilla $m > 1$.

Käytetään modulin $m \in \mathbb{N}$ avulla muodostetusta Pisano-jaksosta merkintää P_m, jakson pituudesta merkintää k_m ja ensimmäisestä positiivisesta indeksistä a, jolla $F_a^{(m)} = 0$, merkintää a_m. Määritelmistä nähdään, että $F_i^{(m)} = F_{i+k_m}^{(m)}$ ja $a_m \leq k_m$. Esimerkiksi taulukon 2 lukujonoissa $a_3 = 4,\ k_3 = 8, a_4 = k_4 = 6$ ja $P_4 = 0, 1, 1, 2, 3, 1$. Alkio F_{a_m} on ensimmäinen luvulla m jaollinen positiivinen Fibonaccin luku. Myös muut nollien esiintymät lukujonossa $(F_n^{(m)})$ kertovat, mitkä Fibonaccin lukujonon alkiot ovat jaollisia luvulla m.

Koska jokainen Pisano-jakso P_m alkaa alkiolla 0, voidaan olettaa, että luvulla m jaolliset Fibonaccin luvut liittyvät pituuteen k_m. Keskitytään siis ensin Pisano-jakson nolla-alkioihin liittyviin ominaisuuksiin.

3.1 Nollat Pisano-jaksossa

Lukujonon $(F_n^{(m)}) = 0, 1, 1, ...$ jaksollisuudesta seuraa, että ainakin Fibonaccin luvut $F_{d \cdot k_m},\ d \in \mathbb{Z}$ ovat jaollisia modulilla m. Jaollisia lukuja voi esiintyä kuitenkin myös useammin, kuten nähdään taulukosta 5.

n :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	...
F_n :	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	...
$F_n^{(5)}$:	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0	2	2	4	1	0	...

Taulukko 5: Lukujono $(F_n^{(5)})$, jolle $a_5 = 5$ ja $k_5 = 20$.

Lause 5. *Lukujonossa $(F_n^{(m)})$ ehdon $F_i^{(m)} = 0$ toteuttavat indeksit i muodostavat aritmeettisen lukujonon. [12, Lause 3.]*

Todistus. Jos $F_i \equiv F_j \equiv 0 \pmod{m}$, lemman 1 kohdan ii mukaan

$$F_{i+j} \equiv F_{i+1} \cdot 0 + 0 \cdot F_{j+1} = 0 \pmod{m}. \tag{9}$$

Kohdan iii mukaan taas

$$F_{j-i} \equiv (-1)^i (0 \cdot F_{i+1} - F_{j+1} \cdot 0) = 0 \pmod{m}. \tag{10}$$

Koska $F_0^{(m)} = F_{a_m}^{(m)} = 0$, kaavojen (9) ja (10) perusteella luku 0 toistuu lukujonossa $(F_n^{(m)})$ ainakin luvun a_m välein. [7, s. 18.] Se ei voi kuitenkaan toistua useammin:

Tehdään vastaoletus, ja oletetaan, että olisi olemassa sellainen indeksi $b_m = d \cdot a_m + r,\ 0 < r < a_m$, jolla $F_{b_m} \equiv 0 \pmod{m}$. Silloin kaavan (10) mukaan

$$F_r = F_{b_m - d \cdot a_m} \equiv 0 \pmod{m},$$

mikä on ristiriita, koska a_m oli määritelty pienimmäksi positiiviseksi indeksiksi i, jolla $F_i \equiv 0 \pmod{m}$. Vastaoletuksen indeksi $b_m \not\equiv 0 \pmod{a_m}$ ei siis ole mahdollinen, joten nolla-alkiot esiintyvät a_m-välein. □

Siitä, että ehdon $F_i^{(m)} = 0$ täyttävät alkiot esiintyvät lukujonossa $(F_n^{(m)})$ säännöllisesti, voidaan johtaa kaksi suoraa seurausta:

Seuraus 2. $F_n^{(m)} = 0 \iff a_m \mid n$.

Seuraus 3. *Lukujonossa $(F_n^{(m)})$ on voimassa ehto $k_m = z_m \cdot a_m$, missä z_m kuvaa nolla-alkioiden määrää jaksossa P_m.*

Seurauksen 3 perusteella Pisano-jakson pituudella ja sen nolla-alkioiden määrällä on suora yhteys. Pitkässäkään Pisano-jaksossa nolla-alkioiden määrä ei kuitenkaan nouse yli tietyn rajan.

Lause 6. *Lukujonon $(F_n^{(m)})$ Pisano-jaksossa on 1, 2 tai 4 nollaa.*

Todistus. Alaluvun 2.2 Fibonaccin lukujen esitysmuoto (3) on voimassa kaikille indeksin arvoille n myös modulo m, joten

$$(F_n, F_{n+1}) \equiv (0,1)U^n \pmod{m} \ \forall n \in \mathbb{N}.$$

Jos merkitään arvolla s sitä alkiota, joka seuraa ensimmäistä positiivisen indeksin nolla-alkiota $F_{a_m}^{(m)}$, saadaan

$$(F_{a_m}, F_{a_m+1}) \equiv (0,s) \equiv (0,1)U^{a_m} \pmod{m},$$

missä $(0,s) = s(0,1)$. Tämän avulla voidaan laskea

$$\begin{aligned}(F_{2a_m}, F_{2a_m+1}) \equiv (0,1)U^{2a_m} &= ((0,1)U^{a_m})U^{a_m} \\ &\equiv (0,s)U^{a_m} \\ &\equiv s(0,1)U^{a_m} \\ &\equiv s(0,s) = (0,s^2) \pmod{m},\end{aligned}$$

ja samoin laskemalla

$$(F_{3a_m}, F_{3a_m+1}) \equiv (0,s^3) \pmod{m},$$

ja edelleen

$$(F_{4a_m}, F_{4a_m+1}) \equiv (0,s^4) \pmod{m}. \tag{11}$$

Lemman 1 kohdasta iv tunnetaan yhtälö

$$F_{a_m-1}F_{a_m+1} - F_{a_m}^2 = (-1)^{a_m}, \tag{12}$$

joka on voimassa myös modulo m. Koska määriteltiin $F_{a_m} \equiv F_{a_m}^{(m)} = 0 \pmod{m}$ ja $F_{a_m+1} \equiv F_{a_m-1} \equiv F_{a_m\pm1}^{(m)} = s \pmod{m}$, yhtälö (12) saadaan muotoon

$$s^2 \equiv (-1)^{a_m} \pmod{m}, \tag{13}$$

josta puolittain toiseen potenssiin korottamalla saadaan $s^4 \equiv 1 \pmod{m}$. Silloin kaavan (11) mukaan

$$(F_{4a_m}, F_{4a_m+1}) \equiv (0, 1) \pmod{m},$$

jolloin $k_m \mid 4 \cdot a_m$. Koska myös $a_m \mid k_m$, saadaan

$$k_m = a_m,\ k_m = 2 \cdot a_m \text{ tai } k_m = 4 \cdot a_m,$$

joten seurauksen 3 mukainen z_m saa arvon $1, 2$ tai 4. □

Olipa m kuinka suuri luonnollinen luku tahansa, Pisano-jaksossa P_m on $1, 2$ tai 4 nolla-alkiota. Jos tunnetaan lukujonon $(F_n^{(m)})$ ensimmäinen positiivinen indeksi a_m, jossa alkio on 0, voidaan jakson nolla-alkioiden määrä z_m ilmaista seuraavan lauseen avulla. Silloin seurauksen 3 perusteella voidaan todeta myös Pisano-jakson pituus k_m.

Lause 7. *Pisano-jakson P_m nolla-alkioiden määrälle on voimassa*

(i) $z_m = 4 \iff a_m$ *on pariton, kun* $m \geq 3$

(ii) $z_m = 1 \iff 4 \nmid k_m$

(iii) $z_m = 2 \iff 4 \mid k_m$ *ja* a_m *on parillinen.*

Todistus. (i) Oletetaan ensin, että $z_m = 4$. Olkoon $s = F_{a_m+1}^{(m)}$, jolle on voimassa lauseen 6 todistuksen yhtälö (13). Yhtälössä

$$s^2 \equiv (-1)^{a_m} \pmod{m} \tag{14}$$

s^2 on alkio toisen positiivisen indeksin nolla-alkion jälkeen. Tällöin on oltava $s^2 \neq 1$, koska muutoin jaksossa olisi alle neljä nollaa. Silloin yhtälön (14) mukaan myös $(-1)^{a_m} \neq 1$, joten a_m on pariton kun $m \geq 3$.

Oletetaan sitten, että a_m on pariton. Koska $m \geq 3$, niin $(-1)^{a_m} = -1$, joten $s^2 \equiv -1 \pmod{m}$. Korottamalla tämä puolittain toiseen saadaan $s^4 \equiv 1 \pmod{m}$, mistä nähdään alkion $s \in (F_n^{(m)})$ kertaluku $\mathrm{ord}_m(s) = 4$. Alkion s kertaluku vastaa jakson nolla-alkioiden määrää [8], joten $z_m = 4$.

(ii) Osoitetaan, että vastaoletus johtaa kummassakin implikaatiossa päinvastaiseen väitteeseen, mikä todistaa halutun implikaation.

Oletetaan ensin, että $z_m \neq 1$, jolloin lauseen 6 perusteella $z_m = 2$ tai $z_m = 4$. Seurauksen 3 mukaan $k_m = z_m \cdot a_m$, joten tapauksessa $z_m = 4$ on voimassa $4 \mid k_m$. Jos taas $z_m = 2$, niin ehto $m \leq 3$ on voimassa. Silloin kohdasta i seuraa, että a_m on parillinen. Erityisesti siis $k_m = z_m \cdot a_m = 2 \cdot (2q),\ q \in \mathbb{Z}$, joten $k_m \mid 4$. Siis $z_m \neq 1 \Rightarrow 4 \mid k_m$, joten myös implikaatio $z_m = 1 \Rightarrow 4 \nmid k_m$ on voimassa.

Oletetaan sitten, että $4 \mid k_m$. Lemman 1 kohta iii saadaan muotoon

$$F_{k_m-j} \equiv F_{0-j} = (-1)^j(F_0F_{j+1} - F_{0+1}F_j) = (-1)^{j+1}F_j \pmod{m}, \tag{15}$$

kun huomioidaan lukujonon $(F_n^{(m)})$ jaksollisuus k_m-välein. Sijoitetaan kaavaan (15) pariton luku $j = \frac{k_m}{2} + 1$:

$$F_{k_m - \frac{k_m}{2} - 1} \equiv 1 \cdot F_{\frac{k_m}{2}+1} \pmod{m}.$$

Alkioiden $F_{\frac{k_m}{2}-1}$ ja $F_{\frac{k_m}{2}+1}$ välissä on yksi alkio, ja sen on täytettävä ehto $F_{\frac{k_m}{2}} \equiv 0 \pmod{m}$, koska lukujono $(F_n^{(m)})$ toteuttaa yleistetyn Fibonaccin lukujonon rekursiivisen ehdon (1). Koska Pisano-jaksossa $P_m = F_0^{(m)}, F_1^{(m)}, ...F_{\frac{k_m}{2}}^{(m)}, ..., F_{k_m-1}^{(m)}$ on nyt ainakin kaksi nollaa, $4 \mid k_m \Rightarrow z_m \neq 1$, eli $4 \nmid k_m \Rightarrow z_m = 1$.

(iii) Kohta seuraa suoraan kahdesta edellisestä.
[7, Lauseet 3.34, 3.35 & 3.36.] □

Yhdistämällä seuraus 3 ja lause 6 saadaan lukujonon $(F_n^{(m)})$ Pisano-jakson pituudelle sen ylärajaa kuvaava epäyhtälö $k_m \leq 4a_m$, mikä kuitenkin edellyttää lukujonon jäsenten laskemista. Etsitään siis edelleen yleisempiä, vain modulista m riippuvia arvioita jakson pituudelle k_m. Keskitytään seuraavaksi vain alkulukumoduleihin: Nimittäin, jos jokin Fibonaccin luku F_n on jaollinen modulilla m, se on jaollinen myös jokaisella luvun m tekijällä. Jos siis m on yhdistetty luku $p_1^{r_i} p_2^{r_2} ... p_s^{r_s}$, $p_i \in \mathbb{P}$ ja $r_i \in \mathbb{N}$ $\forall i = 1, ..., s$, ja $F_n^{(m)} = 0$, myös $F_n^{(p_i)} = 0$ $\forall p_i, i = 1, ..., s$. Silloin seurauksen 2 mukaan $a_{p_i} \mid a_m$, ja koska $a_m \mid k_m$, myös $a_{p_i} \mid k_m$. Voidaan siis olettaa, että luvun m Pisano-jakson pituus voidaan esittää sen alkulukutekijöiden Pisano-jaksojen ominaisuuksien avulla.

3.2 Alkuluvuille

Yleisen alkuluvun p muodostaman Pisano-jakson pituudelle ei voida antaa tarkkaa, vain luvusta p riippuvaa arvoa. Pisano-jaksoon P_p liittyy kuitenkin useita tuloksia, joiden avulla sen pituutta k_p voidaan arvioida. Tuloksissa hyödynnetään seurausta 1, joten oletetaan $p > 2$.

Lemma 2. *Olkoon moduli $p \neq 5$ alkuluku ja α ja β seurauksen 1 mukaiset juuret joko kunnassa $\mathbb{Z}_p$ tai kunnassa $\mathbb{Z}_p[\sqrt{5}]$. Silloin*

$$F_n^{(p)} = 0 \text{ ja } F_{n+1}^{(p)} = 1 \iff \alpha^n = \beta^n = 1. \tag{16}$$

Todistus. Seurauksen 1 perusteella tiedetään, että Binet'n kaava on valitussa kunnassa voimassa. Oletetaan ensin $k_p \mid n$, eli

$$F_n^{(p)} = \frac{\alpha^n - \beta^n}{\alpha - \beta} = 0 \text{ ja } F_{n+1}^{(p)} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} = 1.$$

Edellisestä nähdään, että $\alpha^n = \beta^n$, ja sijoittamalla tämä jälkimmäiseen saadaan

$$\frac{\alpha^n \alpha - \alpha^n \beta}{\alpha - \beta} = \alpha^n (\frac{\alpha - \beta}{\alpha - \beta}) = \alpha^n = 1.$$

Samoin

$$\beta^n(\frac{\alpha-\beta}{\alpha-\beta}) = \beta^n = 1,$$

joten ensimmäinen implikaatio on voimassa. Jos taas oletetaan, että $\alpha^n = \beta^n = 1$, Binet'n kaavan mukaan

$$F_n^{(p)} = \frac{1-1}{\alpha-\beta} = 0 \text{ ja } F_{n+1}^{(p)} = \frac{1\cdot\alpha - 1\cdot\beta}{\alpha-\beta} = 1,$$

joten väitteen ekvivalenssi on todistettu. □

Lause 8. *Olkoot α ja β seurauksen 1 mukaiset juuret joko kunnassa $\mathbb{Z}_p$ tai kunnassa $\mathbb{Z}_p[\sqrt{5}]$. Silloin $k_p = [\mathrm{ord}(\alpha), \mathrm{ord}(\beta)]$, missä kertaluku koskee valittua kuntaa.*

Todistus. Koska k_p on pienin positiivinen indeksi n, jolle lemman 2 ekvivalenssin (16) vasen puoli on voimassa, on se myös pienin luku n, jolla sekä $\alpha^n = 1$ että $\beta^n = 1$. Tästä seuraa, että k_p on lukujen pienin yhteinen jaettava $[\mathrm{ord}(\alpha), \mathrm{ord}(\beta)]$. [10, Lause 2.] □

Lauseen 8 antama Pisano-jakson pituus on tarkka, mutta sitä ei voida ilmaista helposti vain alkuluvun p avulla. Yleisen alkuluvun $p \in \mathbb{P} \setminus \{2, 5\}$ Pisano-jakson pituudelle voidaan antaa yläraja $p-1$ tai $2p+2$, kuten alaluvun lauseiden tulokset osoittavat. Jakson pituus k_p myös jakaa ylärajan, joten sen mahdollisia arvoja on rajallisesti.

Lause 9. *Jos $\alpha \in \mathbb{Z}_p$, eli $p \equiv \pm 1 \pmod 5$, niin $k_p \mid (p-1)$.*

Todistus. Kunnassa $\mathbb{Z}_p$ karakteristisen yhtälön juurille on voimassa yhtälöketju

$$(-\alpha)\cdot\beta = \frac{-1-a}{2}\cdot\frac{1-a}{2} = \frac{-(1-a^2)}{4} = \frac{a^2-1}{4} = \frac{5-1}{4} = 1,$$

joten $\beta = (-\alpha)^{-1}$. Silloin joko $\mathrm{ord}(\beta) = \mathrm{ord}(\alpha)$, $\mathrm{ord}(\alpha) = 2\,\mathrm{ord}(\beta)$ tai $2\,\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$. Nyt lauseesta 8 seuraa, että $k_p = \mathrm{ord}(\alpha)$ tai $k_p = \mathrm{ord}(\beta)$.

Kunta $\mathbb{Z}_p$ on ryhmä, jonka kertaluku on $p-1$. Tämä kertaluku on jaollinen jokaisella ryhmän alkion kertaluvulla [2, Seuraus 2.4.10], joten $\mathrm{ord}(\alpha)|(p-1)$ ja $\mathrm{ord}(\beta)|(p-1)$. Silloin siis $k_p|(p-1)$. [10, Lause 3.] □

Lemma 3. *Jos $p \equiv \pm 2 \pmod 5$, niin $\alpha = \beta^p$ ja $\beta = \alpha^p$ kunnassa $\mathbb{Z}_p[\sqrt{5}]$.*

Todistus. Seurauksesta 1 tiedetään, että kunnassa $\mathbb{Z}_p[\sqrt{5}]$ yhtälön $x^2 \equiv x+1 \pmod p$ ratkaisut ovat $\alpha = \frac{1+\sqrt{5}}{2}$ ja $\beta = \frac{1-\sqrt{5}}{2}$. Osoitetaan, että myös α^p on yhtälön ratkaisu:

$$(\alpha^p)^2 = (\frac{1+\sqrt{5}}{2})^{2p} = (\frac{6+2\sqrt{5}}{4})^p = (1+\frac{1+\sqrt{5}}{2})^p = (\alpha+1)^p,$$

eli $(\alpha^p)^2 = \alpha^p + 1$, koska kunta $\mathbb{Z}_p[\sqrt{5}]$ on kokonaisalue [3, Esimerkki 2.11.17]. Koska toisen asteen karakteristisella yhtälöllä on kuitenkin vain kaksi ratkaisua, on oltava $\alpha^p = \alpha$ tai $\alpha^p = \beta$. Yhtälöllä $x^p = x$ on p ratkaisua, joiden tiedetään Fermat'n pikku lauseen [5, Lause 2.22] mukaan olevan kunnan $\mathbb{Z}_p$ alkiot. Koska $\alpha \notin \mathbb{Z}_p$, on oltava $\alpha^p = \beta$. Samoin $\beta^p = \alpha$. [4, Lause 4.4.] □

Lause 10. *Jos* $p \equiv \pm 2 \pmod 5$, *niin* $a_p \mid (p+1)$.

Todistus. Lemman 3 mukaan $\alpha^p = \beta$ ja $\beta^p = \alpha$. Tällöin $\alpha^{p+1} = \beta\alpha = \beta^{1+p}$. Sijoittamalla tämä jäsenen $F_{p+1}^{(p)}$ Binet'n kaavaan saadaan

$$F_{p+1}^{(p)} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} = 0,$$

joten seurauksen 2 mukaan $a_p \mid (p+1)$. [4, Lause 4.4.] □

Lause 11. *Jos* $\alpha \notin \mathbb{Z}_p$, *eli* $p \equiv \pm 2 \pmod 5$, *niin* $k_p \mid (2p+2)$.

Todistus. Riittää osoittaa, että $F_{2p+2}^{(p)} = 0$ ja $F_{2p+3}^{(p)} = 1$. Lemman 3 mukaan $\alpha^p = \beta$ ja $\beta^p = \alpha$, koska $\alpha \notin \mathbb{Z}_p$. Sijoitetaan nämä Binet'n kaavaan lukujonon jäsenille $F_{2p+2}^{(p)}$ ja $F_{2p+3}^{(p)}$:

$$\begin{aligned} F_{2p+2}^{(p)} &= \frac{\alpha^{2p+2} - \beta^{2p+2}}{\alpha - \beta} = \frac{\beta^2\alpha^2 - \alpha^2\beta^2}{\alpha - \beta} = 0 \text{ ja} \\ F_{2p+3}^{(p)} &= \frac{\alpha^{2p+3} - \beta^{2p+3}}{\alpha - \beta} = \frac{\beta^2\alpha^3 - \alpha^2\beta^3}{\alpha - \beta} = (\alpha^2\beta^2)\frac{\alpha - \beta}{\alpha - \beta} \\ &= (\frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2})^2 \cdot 1 = (\frac{1-5}{4})^2 = 1, \end{aligned}$$

mikä todistaa väitteen. [10, Lause 4.] □

Huomautus 1. Alaluvun lauseet 9, 10 ja 11 koskevat kaikkia alkulukuja $p > 2$. Samat tulokset ovat kuitenkin voimassa myös luvulle $m = 1$ ja alkuluvulle $p = 2$: Tapauksessa $m = 1$ lukujonon $(F_n^{(1)}) = 0, 0, ...$ Pisano-jakson pituudelle selvästi $k_1 = 1 \mid (1-1)$, joten lauseen 9 tulos on voimassa. Kun $p = 2$, lauseiden 10 ja 11 tulokset täyttyvät lukujonossa $(F_n^{(2)}) = 0, 1, 1, 0, ...$, koska $a_2 = 3 \mid 3 = 2+1$ ja $k_2 = 3 \mid 6 = 2 \cdot 2 + 2$.

Modulilla $p = 5$ lukujonolla $(F_n^{(p)})$ on muista alkulukutapauksista poikkeavia ominaisuuksia. Esimerkiksi ehto $p \mid k_p$ täyttyy vain luvulla $p = 5$. Tämä johtuu siitä, että $(F_n^{(5)})$ on ainoa sellainen lukujono $(F_n^{(p)}), p \in \mathbb{P}$, jonka jaksossa kukin jäännösluokkarenkaan $\mathbb{Z}_p$ alkio esiintyy yhtä monta kertaa. [7, Luku 3.2.]

Seuraus 4. *Mielivaltainen alkuluku* p *jakaa Fibonaccin lukujonossa joko jäsenen* F_{p-1}, F_p *tai* F_{p+1}.

Todistus. Jos $p = 5$, niin $5 \mid F_5$, kuten taulukosta 5 nähdään.

Jos $p \equiv \pm 1 \pmod 5$, lauseesta 9 ja huomautuksesta 1 seuraa, että $F_{p-1}^{(p)} = 0$ eli $p \mid F_{p-1}$.

Jos $p \equiv \pm 2 \pmod 5$, lauseen 10, seurauksen 2 ja huomautuksen 1 nojalla $F_{p+1}^{(p)} = 0$ eli $p \mid F_{p+1}$. [4, Lause 4.5.] □

3.3 Yhdistetyille luvuille

Luvussa 3.2 esitettiin Pisano-jakson pituuteen liittyviä tuloksia tapauksessa, jossa moduli m on alkuluku. Aritmetiikan peruslauseen mukaan jokainen luonnollinen luku m voidaan esittää alkulukutekijöidensä avulla [5, Lause 1.27], joten olkoon moduli nyt yhdistetty luku $m = p_1^{r_1}p_2^{r_2}...p_s^{r_s}$. Tässä kanonisessa esitysmuodossa luvut $p_i, i = 1, ..., s$, ovat erisuuria alkulukuja ja r_i kuvaa alkuluvun p_i lukumäärää alkutekijöiden tulossa.

Kanonisesta muodosta nähdään, että yhdistetty luku m on alkulukujen potenssien tulo. Tutkitaan siis ensin modulin $q = p^r,\ p \in \mathbb{P}, r \in \mathbb{N}$, muodostaman Pisano-jakson ominaisuuksia, ja palautetaan sitten mielivaltainen luonnollinen luku m näiden tuloksi.

Lemman 2 ja lauseen 8 tulokset on voimassa myös alkuluvun p potensseille $q = p^r$, kuten Seltzer todistaa lähteessä [10, Lause 2]. Seltzerin käyttämä rengas $\mathbb{Z}_m[\alpha]$ vastaa olennaisilta osin luvussa 2.3 määriteltyä rengasta $\mathbb{Z}_m[\sqrt{5}]$.

Seuraus 5. *Olkoon $q = p^r,\ p \in \mathbb{P} \setminus \{2, 5\}$. Silloin*

(i) $k_q = [\mathrm{ord}(\alpha), \mathrm{ord}(\beta)]$, *missä α ja β kuuluvat renkaaseen $\mathbb{Z}_q$ tai renkaaseen $\mathbb{Z}_q[\alpha]$, joissa $\alpha^2 = \alpha + 1$ ja $\beta^2 = \beta + 1$.*

(ii) $F_n^{(q)} = 0$ *ja* $F_{n+1}^{(q)} = 1 \iff \alpha^n = \beta^n = 1$.

Alkulukujen 2 ja 5 muodostamien lukujonojen $(F_n^{(2)})$ ja $(F_n^{(5)})$ ominaisuuksien on huomattu eroavan muiden alkulukumodulien tapauksista. Käsitellään näiden lukujen potenssit $q = 2^r$ ja $q = 5^r$ erikseen.

Lause 12. *Olkoon $q = 2^r$. Tällöin $k_q = 3 \cdot 2^{r-1}$.*

Todistus. Todistetaan väite induktion avulla. Oletetaan, että $k_{2^r} = 3 \cdot 2^{r-1}$, jolloin $F_{3\cdot 2^{r-1}} \equiv 0$ ja $F_{3\cdot 2^{r-1}+1} \equiv 1 \pmod{2^r}$. Osoitetaan, että $k_{2^{r+1}} = 3 \cdot 2^r$.

Lemman 1 kohdan ii avulla alkio $F_{3\cdot 2^r}$ voidaan esittää seuraavasti:

$$\begin{aligned} F_{3\cdot 2^r} = F_{2\cdot(3\cdot 2^{r-1})} = F_{3\cdot 2^{r-1}+3\cdot 2^{r-1}} &\overset{ii}{=} F_{3\cdot 2^{r-1}-1}F_{3\cdot 2^{r-1}} + F_{3\cdot 2^{r-1}+1}F_{3\cdot 2^{r-1}} \\ &= F_{3\cdot 2^{r-1}}(F_{3\cdot 2^{r-1}-1} + F_{3\cdot 2^{r-1}+1}). \end{aligned} \tag{17}$$

Tulon (17) ensimmäinen tekijä on induktio-oletuksen perusteella kongruentti luvun 0 kanssa modulo 2^r. Kuten alaluvun 2.3 lopulla todettiin, joka kolmas lukujonon (F_n) termi on jaollinen luvulla 2. Silloin tulon toinen tekijä

$$(F_{3\cdot 2^{r-1}-1} + F_{3\cdot 2^{r-1}+1}) \equiv 1 + 1 \equiv 0 \pmod{2}.$$

Yhdistämällä nämä saadaan

$$F_{3\cdot 2^r} \equiv 0 \pmod{2^{r+1}}. \tag{18}$$

Alkio $F_{3\cdot 2^r+1}$ voidaan lemman 1 kohdan v avulla esittää seuraavasti:

$$F_{3\cdot 2^r+1} = F_{2\cdot(3\cdot 2^{r-1})+1} \overset{v}{=} F_{3\cdot 2^{r-1}}^2 + F_{3\cdot 2^{r-1}+1}^2 \equiv 0^2 + 1^2 = 1 \pmod{2^{r+1}}. \tag{19}$$

Kohtien (18) ja (19) perusteella $F_{3\cdot 2^r}$ aloittaa uuden Pisano-jakson modulo 2^{r+1}, joten $k_{2^{r+1}} \mid 3 \cdot 2^r$.

Lisäksi $k_{2^r} \mid k_{2^{r+1}}$, koska jos $F_{2^{r+1}}$ on jaollinen luvulla 2^{r+1}, se on jaollinen myös luvulla 2^r. Jos lisäksi $F_{2^{r+1}+1} \equiv 1 \pmod{2^{r+1}}$, luku $F_{2^{r+1}+1}$ on kongruentti luvun 1 kanssa myös modulo 2^r. Täten uusi Pisano-jakso alkaa myös modulo 2^r, mistä seuraa $k_{2^r} \mid k_{2^{r+1}}$.

Induktio-oletuksen perusteella $k_{2^r} = 3 \cdot 2^{r-1}$. Tiedetään siis, että $3 \cdot 2^{r-1} \mid k_{2^{r+1}}$ ja $k_{2^{r+1}} \mid 3 \cdot 2^r$, joten $k_{2^{r+1}} = 3 \cdot 2^r$ tai $k_{2^{r+1}} = 3 \cdot 2^{r-1}$. Todistetaan seuraavaksi, että näistä jälkimmäinen on mahdoton.

Jos $k_{2^{r+1}} = 3 \cdot 2^{r-1}$, erityisesti $F_{3\cdot 2^{r-1}} \equiv 0$ ja $F_{3\cdot 2^{r-1}+1} \equiv 1 \pmod{2^{r+1}}$. Jälkimmäinen voidaan esittää muodossa

$$F_{3\cdot 2^{r-1}+1} = F_{2\cdot(3\cdot 2^{r-2})+1} = F^2_{3\cdot 2^{r-2}} + F^2_{3\cdot 2^{r-2}+1}$$

lemman 1 kohdan v avulla. Tämä summa saa arvon $2^r + 1 \pmod{2^{r+1}}$, kuten Renaultin todistuksen [7, Lause 3.5] laskuista nähdään. Koska

$$F_{3\cdot 2^{r-1}+1} \equiv 2^r + 1 \not\equiv 1 \pmod{2^{r+1}},$$

oletus $k_{2^{r+1}} = 3 \cdot 2^{r-1}$ ei voi pitää paikkansa. Siispä $k_{2^{r+1}} = 3 \cdot 2^r$.

Koska kaava on voimassa eksponentin arvolla $r = 1$, se on voimassa kaikilla luonnollisilla luvuilla r. [7, Lause 3.5.] □

Samanlainen tulos löydetään modulille $p = 5$. Seuraavan lauseen todistus on peräisin Renautilta lähteestä [7, Lemma 3.6, lause 3.7].

Lause 13. *Olkoon $q = 5^r$. Tällöin $k_q = 4 \cdot 5^r$.*

Todistus. Jos p on pariton alkuluku ja r ja $d, p \nmid d$, luonnollisia lukuja, tunnetaan implikaatio

$$p^r \mid F_n,\ p^{r+1} \nmid F_n \Rightarrow p^{r+1} \mid F_{ndp},\ p^{r+2} \nmid F_{ndp}. \tag{20}$$

Koska $5^1 \mid F_5$, niin $5^2 \mid F_{d_1\cdot 5^2}$, ja näin jatkamalla

$$5^r \mid F_{d_2\cdot 5^r}, \tag{21}$$

kun $5 \nmid d_i$. Siis

$$F_{4\cdot 5^r} \equiv 0 \pmod{5^r}. \tag{22}$$

Lemman 1 kohdan v avulla voidaan muodostaa yhtälö

$$F^2_{2\cdot 5^r} + F^2_{2\cdot 5^r+1} = F_{4\cdot 5^r+1}, \tag{23}$$

josta implikaation (20) seurauksen (21) mukaan $F^2_{2\cdot 5^r} \equiv 0^2 = 0 \pmod{5^r}$. Lemman 1 kohdan iv avulla taas voidaan ratkaista

$$F^2_{2\cdot 5^r+1} = F_{2\cdot 5^2} F_{2\cdot 5^r+2-} - (-1)^{2\cdot 5^r+1} \equiv 0 + 1 = 1 \pmod{5^r}.$$

Yhtälöstä (23) saadaan siis

$$F_{4\cdot 5^r+1} \equiv 1 \pmod{5^r},$$

mikä yhdistettynä kohtaan (22) antaa

$$k_{5^r} \mid 4 \cdot 5^r.$$

Osoitetaan nyt väite

$$k_{5^r} = 4 \cdot 5^r \tag{24}$$

induktion avulla. Kun $r = 1$, taulukosta 5 nähdään väitteen olevan tosi. Oletetaan sitten, että $k_{5^r} = 4 \cdot 5^r$, ja osoitetaan $k_{5^{r+1}} = 4 \cdot 5^{r+1}$:

Induktio-oletuksen nojalla $4 \cdot 5^r = k_{5^r}$, joka jakaa luvun $k_{5^{r+1}}$, kuten lauseen 12 todistuksessa $k_{2^r} \mid k_{2^{r+1}}$. Lisäksi $k_{5^{r+1}} \mid 4 \cdot 5^{r+1}$, joten

$$k_{5^{r+1}} = 4 \cdot 5^r \text{ tai } k_{5^{r+1}} = 4 \cdot 5^{r+1}.$$

Näistä edellinen on ristiriidassa implikaation (20) kanssa, joten

$$k_{5^{r+1}} = 4 \cdot 5^{r+1}.$$

Näin lauseen väite on todistettu. □

Modulien $q = 2^r$ ja $q = 5^r$, $r \in \mathbb{N}$ muodostamien Pisano-jaksojen pituudet voidaan siis ilmaista tarkasti. Oletetaan nyt, että modulissa $q = p^r$ alkuluku $p \notin \{2, 5\}$.

Lause 14. *$a_{p^{r+1}} = a_{p^r}$ tai $a_{p^{r+1}} = p \cdot a_{p^r}$.*

Todistus. Alaluvun 2.2 perusteella lukujonon $(F_n^{(q)})$ indeksin a_q alkion matriisiesitys voidaan laskea seuraavasti:

$$U^{a_q} = \begin{pmatrix} F_{a_q-1} & F_{a_q} \\ F_{a_q} & F_{a_q+1} \end{pmatrix} \equiv \begin{pmatrix} s_q & 0 \\ 0 & s_q \end{pmatrix} = s_q I \pmod{q},$$

missä s_q on ensimmäistä positiivisen indeksin nolla-alkiota seuraava alkio lukujonossa $(F_n^{(q)})$. Saadaan siis Fibonaccin matriisi

$$U^{a_{p^r}} = s_{p^r} I \pmod{p^r},$$

joka voidaan esittää muotoa (5) vastaavassa muodossa

$$U^{a_{p^r}} = s_{p^r} I + p^r M,$$

johon on valittu $d = p^r \equiv 0 \pmod{p^r}$. Korottamalla tämä yhtälö puolittain potenssiin p saadaan

$$U^{p\cdot a_{p^r}} = (s_{p^r} I)^p + \binom{p}{1}(s_{p^r} I)^{p-1}(p^r M) + \binom{p}{2}(s_{p^r} I)^{p-2}(p^r M)^2 + \ldots + \binom{p}{p}(p^r M)^p,$$

jossa binomikaavan summan jokainen termi ensimmäistä lukuunottamatta on jaollinen luvulla p^{r+1}. Saadaan siis

$$U^{p \cdot a_{p^r}} \equiv (s_{p^r} I)^p = (s_{p^r})^p I = \begin{pmatrix} s_{p^r}^p & 0 \\ 0 & s_{p^r}^p \end{pmatrix} \pmod{p^{r+1}},$$

joten Fibonaccin luvun matriisimuodosta (4) nähdään, että $F_{p \cdot a_{p^r}} \equiv 0 \pmod{p^{r+1}}$. Seurauksen 2 perusteella siis $a_{p^{r+1}} \mid p \cdot a_{p^r}$.

Lisäksi $a_{p^r} \mid a_{p^{r+1}}$, koska kun $F_{a_{p^{r+1}}}$ on jaollinen luvulla p^{r+1}, se on jaollinen myös luvulla p^r. Silloin $F^{(p^r)}_{a_{p^{r+1}}} = 0$, ja seurauksen 2 mukaan $a_{p^r} \mid a_{p^{r+1}}$.

Koska $a_{p^r} \mid a_{p^{r+1}}$ ja $a_{p^{r+1}} \mid p \cdot a_{p^r}$, voidaan nämä yhdistää väitteeksi $a_{p^{r+1}} = a_{p^r}$ tai $a_{p^{r+1}} = p \cdot a_{p^r}$. [7, Lause 3.32.] □

Lause 15. *$k_{p^{r+1}} = k_{p^r}$ tai $k_{p^{r+1}} = p \cdot k_{p^r}$.*

Todistus. Käytetään alaluvun 2.2 esitysmuotoa (5) ja arvoa $n = k_{p^r}$, joka selvästi aloittaa uuden jakson. Silloin

$$U^{k_{p^r}} = I + p^r M,$$

koska on oltava $U^{k_{p^r}} \equiv I \pmod{p^r}$.

Korottamalla yhtälö puolittain potenssiin p saadaan yhtälö

$$U^{p \cdot k_{p^r}} = (I + p^r M)^p = I^p + \binom{p}{1} I^{p-1}(p^r M) + \binom{p}{2} I^{p-2}(p^r M)^2 + ... + \binom{p}{p} (p^r M)^p,$$

jossa binomikaavan summan jokainen tekijä ensimmäistä lukuunottamatta on jaollinen luvulla p^{r+1}. Siis

$$U^{p \cdot k_{p^r}} \equiv I^p = I \pmod{p^{r+1}},$$

joten alaluvun 2.2 perusteella $p \cdot k_{p^r}$ aloittaa uuden jakson lukujonossa $(F_n^{(p^{r+1})})$, ja siten $k_{p^{r+1}} \mid p \cdot k_{p^r}$.

Lisäksi $k_{p^r} \mid k_{p^{r+1}}$, koska jos indeksillä $i = k_{p^{r+1}}$ on voimassa

$$F_i \equiv 0 \pmod{p^{r+1}} \text{ ja } F_{i+1} \equiv 1 \pmod{p^{r+1}},$$

niin ensimmäisen kongruenssiyhtälön alkio F_i on jaollinen myös luvulla p^r, joten $F_i^{(p^r)} = 0$. Jälkimmäisestä yhtälöstä taas seuraa, että F_{i+1} voidaan esittää seuraavasti:

$$F_{i+1} = d \cdot p^{r+1} + 1 = dp \cdot p^r + 1 \equiv 1 \pmod{p^r}.$$

Koska F_i siis aloittaa uuden jakson myös modulo p^r, jakson $P_{p^{r+1}}$ pituus on jaollinen jakson P_{p^r} pituudella. Väite $k_{p^r} \mid k_{p^{r+1}}$ seuraa helposti myös myöhemmin todistettavasta lauseesta 19.

Koska nyt $p \cdot k_{p^r}$ on jaollinen luvulla $k_{p^{r+1}}$, joka taas on jaollinen luvulla k_{p^r}, saadaan väite $k_{p^{r+1}} = k_{p^r}$ tai $k_{p^{r+1}} = p \cdot k_{p^r}$. [10, Lause 5], [7, Lause 3.8.] □

Lause 16. *Parittoman alkuluvun p potenssien $q = p^r$ Pisano-jaksoissa nollien määrä on sama kaikilla $r \in \mathbb{N}$.*

Todistus. Lauseiden 14 ja 15 mukaan luvun $q = p^r$ potenssin kasvaessa yhdellä a_q ja k_q pysyvät samana tai kertautuvat luvulla p. Voidaan siis esittää suhteet

$$\frac{a_{p^r}}{a_p} = p^i \text{ ja } \frac{k_{p^r}}{k_p} = p^j \tag{25}$$

joillakin kokonaisluvuilla i ja j. Koska selvästi

$$\frac{k_{p^r}}{a_p} \cdot \frac{a_{p^r}}{a_{p^r}} = \frac{k_{p^r}}{a_p} \cdot \frac{k_p}{k_p},$$

voidaan tämä järjestää uudelleen yhtälöksi

$$\frac{k_{p^r}}{a_{p^r}} \cdot \frac{a_{p^r}}{a_p} = \frac{k_{p^r}}{k_p} \cdot \frac{k_p}{a_p}. \tag{26}$$

Kohdan (25) ja seurauksen 3 perusteella yhtälö (26) saadaan muotoon

$$z_{p^r} \cdot p^i = p^j \cdot z_p. \tag{27}$$

Koska z_q voi saada vain arvot $1, 2$ tai 4, ja parittoman alkuluvun potensseilla p^i ja p^j ei ole parillisia tekijöitä, on oltava $p^i = p^j$. Yhtälöstä (27) seuraa siis väite siitä, että nollia on sama määrä kaikilla potenssin arvoilla r. [7, Lause 3.32.] □

Lause 17. *Jos $k_p \neq k_{p^2}$, niin $k_{p^r} = p^{r-1}k_p$ kaikille $p \in \mathbb{P} \setminus \{2, 5\}$ ja $r \in \mathbb{N}$.*

Todistus. Lauseen 15 mukaan $k_{p^{r+1}} = k_{p^r}$ tai $k_{p^{r+1}} = p \cdot k_{p^r}$. Oletetaan, että jälkimmäinen on voimassa, ja osoitetaan, että $k_{p^{r+2}} = p \cdot k_{p^{r+1}}$.

Käytetään alaluvun 2.2 esitysmuotoa (5), jolloin

$$U^{k_{p^r}} = I + p^r M,$$

ja korotetaan yhtälö puolittain potenssiin p:

$$U^{p \cdot k_{p^r}} = I^p + \binom{p}{1} I^{p-1}(p^r M) + \binom{p}{2} I^{p-2}(p^r M)^2 + ... + \binom{p}{p}(p^r M)^p.$$

Yhtälön binomikaavan summan jokainen termi kahta ensimmäistä lukuun ottamatta on jaollinen luvulla p^{r+2}. Saadaan kongruenssiyhtälö

$$U^{p \cdot k_{p^r}} \equiv I^p + I^{p-1} p \cdot (p^r M) = I + p^{r+1} M \pmod{p^{r+2}}.$$

Nyt

$$U^{k_{p^{r+1}}} = U^{p \cdot k_{p^r}} \equiv I + p^{r+1} M \pmod{p^{r+2}}, \tag{28}$$

koska oletettiin $k_{p^{r+1}} = p \cdot k_{p^r}$. Samasta oletuksesta seuraa, että $k_{p^{r+1}} \neq k_{p^r}$, jolloin $p^{r+1} \nmid p^r$. Myös $p^{r+2} \nmid p^{r+1}$ on siis voimassa, jolloin yhtälöstä (28) saadaan

$$U^{k_{p^{r+1}}} \not\equiv I \pmod{p^{r+2}},$$

eli $k_{p^{r+1}} \neq k_{p^{r+2}}$. Silloin lauseen 15 mukaan on oltava $k_{p^{r+2}} = p \cdot k_{p^{r+1}}$.

Jos siis $k_p \neq k_{p^2}$, niin $k_{p^2} = p \cdot k_p$ on voimassa. Tästä taas seuraa, että $k_{p^3} = p \cdot k_{p^2} = p \cdot p \cdot k_p$, ja yhä edelleen ehto $k_{p^r} = p^{r-1}k_p$ on voimassa mielivaltaiselle potenssille $r \in \mathbb{N}$. [7, Lause 3.8.] □

Yleisesti uskotaan, että ehto $k_p \neq k_{p^2}$ on voimassa kaikille alkuluvuille. Todistusta tälle ei kuitenkaan tunneta. [7, s. 24.] Jos oletetaan, että $k_p \neq k_{p^2}$ on voimassa kaikille luvuille $p \in \mathbb{P} \setminus \{2, 5\}$, niin $k_{p^r} = p^{r-1}k_p$ on voimassa kaikille alkuluvuille. Lauseiden 13 ja 12 väitteet ovat nimittäin myös tätä muotoa. Oletuksen $k_p \neq k_{p^2}$ ollessa voimassa modulin $q = p^r$ Pisano-jakson pituus voidaan siis laskea helposti, jos k_p tunnetaan.

Siirrytään nyt käsittelemään yleistä modulia $m \in \mathbb{N}$, joka voidaan esittää alaluvun alun kanonisessa muodossa.

Lause 18. *Olkoon* $m = p_1^{r_1}p_2^{r_2}...p_s^{r_s},\ p_i \in \mathbb{P}$, *luonnollinen luku. Silloin*

$$a_m = [a_{p_1^{r_1}}, a_{p_2^{r_2}}, .., a_{p_s^{r_s}}].$$

Todistus. Yhdistetty luku m jakaa luvun M silloin ja vain silloin, kun jokainen sen tekijä jakaa kyseisen luvun. Siis

$$m \mid F_M \iff p_i^{r_i} \mid F_M\ \forall i = 1, ..., s.$$

Jälkimmäinen on seurauksen 2 nojalla voimassa silloin ja vain silloin, kun

$$a_{p_i^{r_i}} \mid M\ \forall i = 1, ..., s.$$

Pienin tämän ehdon täyttävä luku M on $[a_{p_1^{r_1}}, a_{p_2^{r_2}}, .., a_{p_s^{r_s}}]$, joka on siis myös pienin alkio, joka täyttää ekvivalentin ehdon $m \mid F_M$. Siis

$$M = a_m = [a_{p_1^{r_1}}, a_{p_2^{r_2}}, .., a_{p_s^{r_s}}].$$

[7, Lause 3.30.] □

Seuraava tulos on tärkeä selvitettäessä Pisano-jakson pituutta yleiselle luonnolliselle luvulle m. Tuloksen seurauksen perusteella voidaan laskea yhdistetyn luvun Pisano-jakson pituus luvun alkulukutekijöiden potenssien $p_i^{r_i}$ Pisano-jaksojen avulla.

Lause 19. *Olkoon* $(F_i^{(n)})$ *ja* $(F_i^{(m)})$ *Fibonaccin lukujonoja modulien* n *ja* m *avulla esitettynä. Silloin, jos* $n \mid m$, *niin* $k_n \mid k_m$.

Todistus. Halutaan osoittaa, että siirryttäessä lukujonossa $(F_i^{(m)})$ eteenpäin k_m alkion verran, myös lukujonossa $(F_i^{(n)})$ ollaan siirrytty kokonaisten Pisano-jaksojen verran. Osoitetaan tämä näyttämällä, että $F_i \equiv F_{i+k_m} \pmod{n}$.

Jakson pituuden määritelmästä seuraa, että $F_i^{(m)} \equiv F_{i+k(m)}^{(m)} \equiv a \pmod{m},\ a \in \mathbb{Z}_m$. Merkitään

$$F_i = a + xm \text{ ja} \tag{29}$$
$$F_{i+k_m} = a + ym,\ x, y \in \mathbb{Z}. \tag{30}$$

Oletuksesta $n \mid m$ seuraa, että $m = dn,\ d \in \mathbb{Z}$. Merkitään $a = a' + zn,\ a' \in \mathbb{Z}_n$. Sijoitetaan nämä kaavoihin (29) ja (30):

$$F_i = a' + zn + xdn = a' + (z + xd)n \text{ ja}$$
$$F_{i+k_m} = a + zn + ydn = a' + (z + yd)n,$$

mistä seuraa väite

$$F_i \equiv F_{i+k_m} \equiv a' \pmod{n}.$$

[7, s.19.] □

Seuraus 6. *Kun $m \in \mathbb{N}$ on muotoa $p_1^{r_1}p_2^{r_2}..p_s^{r_s}$, niin $k_m = [k_{p_1{}^{r_1}}, k_{p_2{}^{r_2}}, ..., k_{p_s{}^{r_s}}]$.* [12, Lause 2.]

Todistus. Koska $p_i^{r_i} \mid m$, lauseen 19 mukaan $k_m = d \cdot k_{p_i^{r_i}}$ jollakin $d \in \mathbb{Z}$. Tämä on voimassa jokaiselle $i = 1, ..., s$, joten k_m on lukujen $k_{p_i^{r_i}}$ pienin yhteinen monikerta. □

Näin minkä tahansa luonnollisen luvun Pisano-jakson pituus voidaan palauttaa alkulukujen potenssien ja siten alkulukujen Pisano-jaksojen pituuksiin. Vaikka yleiselle alkuluvulle $p \in \mathbb{P} \setminus \{2, 5\}$ ei voida laskea tarkkaa alkuluvusta p riippuvaa arvoa, joillekin luvuille voidaan tehdä näin laskematta lukujonon $(F_n^{(m)})$ jäseniä.

Lause 20. *Olkoon moduli m Fibonaccin lukujonon indeksiä n vastaava alkio, eli $m = F_n$. Silloin,*

(i) jos $n \geq 5$ on pariton, niin $k_m = 4n$.

(ii) jos $n \geq 4$ on parillinen, niin $k_m = 2n$.

Todistus. Selvästi $a_m = n$, koska a_m on määritelty ensimmäiseksi positiiviseksi indeksiksi n, jolla F_n on jaollinen modulilla m. Lisäksi kun $n \geq 4$, niin $m = F_n \geq 3$, joten voidaan käyttää lauseen 7 kohtaa i.

(i) Kun $n = a_m$ on pariton, lauseen 7 mukaan $z_m = 4$. Siten $k_m = a_m \cdot z_m = 4n$.

(ii) Kun n on parillinen, $z_m \neq 4$. Jos olisi $z_m = 1$, niin $F_{n\pm1} \equiv 1 \pmod{F_n}$. Saadaan epäyhtälö

$$F_3 \equiv 2 \geq 1 \equiv F_{n-1} \pmod{m},$$

josta syntyy ristiriita, koska (F_n) on kasvava modulo m kun $n = 0, 1, 2, 3, ...n - 1$. Jäljelle jää siis vaihtoehto $z_m = 2$, jolloin $k_m = z_m \cdot a_m = 2n$.

[7, Lause 3.45.] □

4 Yhteenveto

Kun Fibonaccin lukujonot esitetään modulin $m \in \mathbb{N}$ suhteen, muodostuvan lukujonon voidaan näyttää olevan aina jaksollinen. Tämän Pisano-jakson pituudelle ei kuitenkaan voida yleisessä tapauksessa antaa tarkkaa, vain luvusta m riippuvaa arvoa. Arvolle k_m voidaan kuitenkin esittää erilaisia ylärajoja.

Keskeinen tulos tutkielmassa on kaava

$$k_m = z_m \cdot a_m,$$

missä Pisano-jakson nolla-alkioiden määrää kuvaava z_m saa arvon 1, 2 tai 4. Laskemalla lukujonon $(F_n^{(m)})$ alkioita ensimmäiseen ehdon $F_i^{(m)} = 0$, $i > 0$, täyttävään alkioon asti saadaan arvo $a_m = i$ ja pituudelle k_m yläraja $4a_m$. Luvulle k_m voidaan kuitenkin löytää myös yleisempiä ominaisuuksia, jotka voidaan ilmaista vain arvon m avulla.

Eräs hyödyllisimmistä tutkielmassa esitetyistä tuloksista on lause 19, jonka mukaan luvun m tekijän n Pisano-jakson pituus k_n jakaa luvun k_m. Tämän avulla luvun $m \in \mathbb{N}$ Pisano-jakson pituus voidaan esittää sen tekijöiden, eli erityisesti kanonisen esitysmuodon tekijöiden $p_i^{r_i}$, Pisano-jaksojen avulla. Luku k_m on tällöin lukujen $k_{p_i^{r_i}}$ pienin yhteinen jaettava, ja siten laskettavissa.

Myös modulin p^r muodostaman Pisano-jakson pituus k_{p^r} on laskettavissa, kun arvo k_p, $p \in \mathbb{P}$, tunnetaan: Kun p on mielivaltainen alkuluku, modulin p^r, $r \in \mathbb{N}$, Pisano-jakson pituus voidaan ilmaista kaavalla

$$k_{p^r} = k_p \cdot p^{r-1},$$

jos $k_p \neq k_{p^2}$, minkä oletetaan olevan voimassa kaikille alkuluvuille.

Jos siis tunnetaan arvo k_p, $p \in \mathbb{P}$, voidaan helposti laskea k_{p^r} ja edelleen k_m, kun $r \in \mathbb{N}$ ja m on mielivaltainen luonnollinen luku $p_1^{r_1} p_2^{r_2} ... p_s^{r_s}$. Arvolle k_p ei voida antaa yleistä kaavaa, mutta sillä on seuraavat ominaisuudet:

(i) Jos alkuluvulle p on voimassa $p \equiv \pm 1 \pmod 5$, niin

$$k_p \mid (p-1).$$

(ii) Jos alkuluvulle p on voimassa $p \equiv \pm 2 \pmod 5$, niin

$$k_p \mid (2p+2).$$

(iii) Jos $p \equiv 0 \pmod 5$, eli $p = 5$,

$$k_p = 20.$$

Alkuluvun $p \neq 5$ Pisano-jakson pituudelle saadaan siis alkuluvusta riippuva yläraja $p-1$ tai $2p-2$. Yläraja on lisäksi jaollinen luvulla k_p, joten mahdollisten arvojen k_p lukumäärä on rajoitettu. Koska mielivaltaisen luvun m Pisano-jakson pituus palautuu näihin arvoihin, tuloksia i ja ii voidaan pitää tutkielman tärkeimpinä.

Kun $p \notin \{2, 5\}$, tuloksissa hyödynnettiin Fibonaccin lukujonon karakteristisen yhtälön

$$x^2 = x + 1$$

erisuuria ratkaisuja α ja β, jotka löytyivät kunnasta $\mathbb{Z}_p$ tai kunnasta $\mathbb{Z}_p[\sqrt{5}]$. Näiden avulla voitiin esittää yleinen jäsen

$$F_n^{(p)} = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{31}$$

Koska jokainen Pisano-jakso alkaa lukujonon $(F_n^{(p)})$ jäsenillä

$$F_{d \cdot k_p}^{(p)} = 0 \text{ ja } F_{d \cdot k_p + 1}^{(p)} = 1, \ d \in \mathbb{Z},$$

voidaan Pisano-jakson pituus tarkistaa sijoittamalla kaavaan (31) indeksin arvot $n = k_p'$ ja $n = k_p' + 1$. Tässä k_p' on jokin tulosten i ja ii mukainen mahdollinen arvo k_p. Nyt Pisano-jakson pituus k_p saa pienimmän arvon k_p', jolla

$$F_{k_p'}^{(p)} = 0 \text{ ja } F_{k_p' + 1}^{(p)} = 1.$$

Kuten todettua, nyt yleisen modulin m tapaus k_m voidaan laskea alkulukutapausten avulla.

Viitteet

[1] Iiro Honkala. Kombinatoriikka, 2015.

[2] Markku Koppinen. Algebran peruskurssi I. Turun yliopisto, 2006.

[3] Markku Koppinen. Algebran peruskurssi II. Turun yliopisto, 2008.

[4] Brian Lawrence. Fibonacci numbers modulo p, 2014.

[5] Iiro Honkala Matti Jutila. Lukuteoria, 2011.

[6] Vesa Halava Teemu Pirttimäki. Matematiikan historia. Turun yliopisto, 2021.

[7] Marc Renault. The Fibonacci Sequence Under Various Moduli. Master's thesis, Wake Forest University, 1996.

[8] Marc Renault. The Fibonacci Sequence Modulo M. `https://sites.math.rutgers.edu/~zeilberg/essays683/renault.html`, 24.4.2000. Viitattu 17.11.2025.

[9] D. W. Robinson. The Fibonacci Matrix Modulo m. *The Fibonacci Quarterly*, 1:29–36, 1963.

[10] Scott Seltzer. Generalizer Fibonacci sequences modulo powers of a prime. *Brandeis University, Waltham*, 2000.

[11] N. J. A. Sloane The OEIS Community. Pisano periods (or pisano numbers): period of Fibonacci numbers mod n. `https://oeis.org/A001175`, Päivitetty 15.1.2026. Viitattu 15.1.2026.

[12] D. D. Wall. Fibonacci Series Modulo m. *The America Mathematical Monthly*, 67(6):525–532, 1960.