Taikaneliöiden konstruointi jakojäännösaritmetiikan avulla

Eveliina Koskela

LuK-tutkielma
Helmikuu 2026

Tarkastajat:
Dos. Jyrki Lahtonen

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

EVELIINA KOSKELA: Taikaneliöiden konstruointi jakojäännösaritmetiikan avulla
LuK-tutkielma, 10 s.
Matematiikka
Helmikuu 2026

Tässä tutkielmassa perehdytään taikaneliöiden konstruoimiseen jakojäännösaritmetiikan pohjalta. Taikaneliöt ovat neliöitä, jotka sisältävät luvut $1, .., n^2$ tai $0, ..., n^2-1$. Lisäksi neliön jokaisen sarakkeen, rivin ja diagonaalin summa on sama. Tätä summaa kutsutaan neliön taikavakioksi.

Oletetaan, että lukija tunteen algebran perusteet.Tutkielmassa perehdytään taikaneliöiden määritelmään, sekä muodostamiseen ortogonaalisten latinalaisten neliöiden pohjalta.

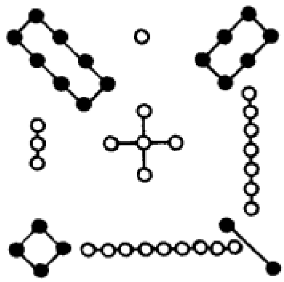
Asiasanat: latinalainen neliö, ortogonaalisuus, taikaneliö

Sisällys

1 Johdanto

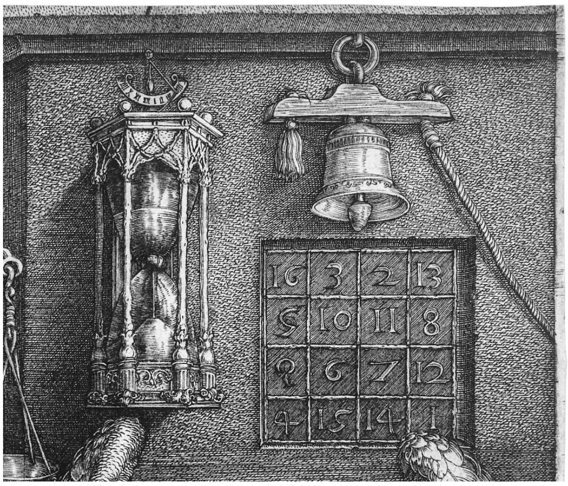
Tutkielmassa perehdytään taikaneliöiden konstruoimiseen jakojäännösaritmetiikan pohjalta. Oletetaan, että lukija tuntee algebran perusteet. Taikaneliö on matemaattinen rakenne, jossa luvut, yleensä $1, 2, 3, ..., n^2$ tai $0, 1, 2, ..., n^2 - 1$, on järjestetty $n \times n$ -ruudukkoon siten, että jokaisen rivin, sarakkeen ja päädiagonaalin summa on sama ja jokainen luku esiintyy ruudukossa vain kerran. Tuota summaa kutsutaan taikavakioksi. Taikaneliöiden historia ulottuu tuhansien vuosien taakse ja siihen liittyy mystiikkaa, astrologiaa ja puhdasta matematiikkaa. Ne ovat kiehtoneet niin matematiikoita kuin muitakin ihmisiä. Näitä neliöitä on pidetty universumin harmonian ja tasapainon symboleina ja ovat siirtyneet mystisistä suojaavista amuleteista aina moderneiksi matemaattisiksi pulmiksi. Johdannossa tutustutaan taikaneliöiden historiaan.

Varhaisin tunnettu taikaneliö esiintyi muinaisessa Kiinassa ennen ajanlaskun alkua. Legendan mukaan keisari Yu näki mystisen kilpikonnan nousevan Lu joesta. Kilpikonnan kilvessä oli kuvio, joka muodostui pisteistä 3x3 ruudukossa. Kyseistä taikaneliötä kutsutaan Lo Shu -neliöksi. Siinä luvut 1-9 on järjestetty siten, että jokaisen rivin, sarakkeen ja diagonaalin summa on yhtäsuuri eli neliön taikavakio on 15. Kiinalaiset tulkitsivat Lo Shu-neliön jumalalliseksi merkiksi, jolla hallittiin Lo joen tulvia. Kiinassa taikaneliöt ovat vahvasti liitetty mytologiaan ja astrologiaan, ja niitä käytettiin amuleteissa suojaamaan pahalta ja tuomaan onnea. Mystisen ajattelutavan takia neliöiden matemaattinen kehitys jäi vähäiseksi.



Kuva 1: Lo Shu taikaneliö

Kiinasta taikaneliöt levisivät Intiaan, missä niitä käytettiin 500 vuotta ennen ajanlaskun alkua lääketieteessä, ennustamisessa ja uskonnollisissa rituaaleissa. 4x4 -neliöitä on löydetty temppeleistä, kuten Khajurahon Parvanathasta noin 1100-luvulla. Arabimaissa oppineet, kuten Geber kehittivät taikaneliöitä alkemian yhteydessä 700-luvulla. Hän yritti taikanelöiden avulla yhdistellä metalleista kultaa. Taikaneliöt liitettiin myös astrologian kautta planeettoihin ja suojelusamuleteiksi. Euroopassa taikaneliöt tulivat tutuiksi renessanssin aikana arabialaisten lähteiden kautta. Yksi tunnetuimmista taikaneliöistä löytyy Albrecht Dürerin kaiverruksesta *Melencolia 1* vuodelta 1514, josta löytyy 4×4 taikaneliö . Myöhemmin 1700-luvulla amerikkalainen Benjamin Franklin loi 8×8 ja 16×16 taikaneliöitä, joissa myös taivutetut rivit ja diagonaali saivat saman taikavakion.



Kuva 2. Vasemmalla Albrecht Dürerin Melankolia 1 -taideteos ja oikealla Dürerin neliö.

Ajan kuluessa taikaneliöt ovat muuttuneet mystisistä symboleista matemaattisimmiksi. 1800-1900 -luvuilla kehitettiin erilaisia luokituksia, kuten pandiagonaaliset ja multimagiset neliöt, sekä laajennuksia kuutoihin ja muihin ulottuvuuksiin. Taikaneliöt ovat olleet pohjana myös sudoku -pelille. Tutkielmassa perehdytään taikaneliöiden luomiseen latinalaisten neliöiden ortogonaalisuuden avulla ja kertaluvulla p muodostettuihin taikaneliöihin, joissa p on alkuluku. Neliöhin sijoitetaan luvut nollasta eteenpäin. Päälähteena on käytetty dosentti Jyrki Lahtosen tekemää opetusmateriaalia [1] ja Anthony B. Evansin kirjaa Orthogonal Latin Squares Based on Groups [2]. Muita lähteitä on käytetty johdannon kirjoittamiseen.

2 Latinalaisista neliöistä

Tässä luvussa käsitellään latinalaisia neliöitä ja niiden muodostamista yhteenlasku- ja kertotaulun avulla. Lisäksi perehdytään latinalaisten neliöiden ortogonaalisuuteen, joka on tärkeä ominaisuus, kun muodostetaan taikaneliöitä.

2.1 Määritelmä ja esimerkkejä

Tässä alaluvussa määritellään latinalainen neliö, sekä havainnoillistetaan esimerkeillä määritelmää.

Määritelmä 1. Olkoon L joukko, jossa on n alkioita. Sanotaan, että $n \times n$ -matriisi on kertaluvun n latinalainen neliö, jossa kaikki joukon L alkiot esiintyvät matriisin jokaisessa rivissä ja sarakkeessa vain kerran.

Esimerkki 1. Tämä 3×3 -matriisi

a	b	c
b	c	a
c	a	b

on esimerkki latinalaisesta neliöstä, sillä jokainen alkio esiintyy jokaisessa sarakkeessa ja rivissä vain kerran. Seuraava taulukko

a	b	c
a	b	c
a	b	c

ei ole latinalainen neliö, sillä sama alkio esiintyy sarakkeessa useamman kerran.

2.2 Kongruessien käyttö latinalaisten neliöiden konstruoinnissa

Tässä alaluvussa käsitellään latinalaisten neliöiden konstruointia käyttäen apuna kongruesseja yhteenlasku- ja kertotaulujen kautta.

2.2.1 Yhteenlaskutaulu

Latinalaisia neliöitä voidaan muodostaa jäännösluokkien yhteenlaskutaulun avulla. Seuraavassa esimerkissä 2 käytetään yhteenlaskutaulua modulo 4. Huomataan, että yhteenlaskutaulu on latinalainen neliö. Yhteenlaskutaulu modulo m on aina latinalainen neliö.

Esimerkki 2.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2.2.2 Kertotaulu

Valitaan jokin moduli m >1. Valitaan $m = 5$ ja luodaan kertotalu modulo 5.

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Nollarivin ja -sarakkeen takia kertotaulu ei ole latinalainen neliö. Huomataan, että nollarivin ja -sarakkeen poistamisen jälkeen jäljelle jää 4×4 latinalaisen neliön määritelmän täyttävä neliö.

Valitaan vielä toinen moduli $m = 6$ ja toistetaan kertotaulu.

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	4	1

Huomataan, että tässä tapauksessa nollarivin ja -sarakkeen poistamisen jälkeen jäljelle jäävä 5×5 -taulukko ei täytä latinalaisen neliön määritelmää. Joten kertotaulu ei aina tuota latinalaista neliötä. Seuraavaksi todistetaan, että kertotaulu on latinalainen neliö vain jos m on alkuluku.

Lause 1. *Todetaan, että p on alkuluku. Jos i on välillä $0 < i < p$, niin jäännösluokkakertotaulun modulo p pysty- tai vaakarivillä i esiintyvät luvut* $0, 1, ..., p-1$.

Todistus. Väitetään, että rivillä olevat tulot $\bar{i} \cdot \bar{j} = a$ ja $\bar{i} \cdot \bar{k} = b$ ovat eri luvut, kun $\bar{j} \neq \bar{k}$. Jos nyt $a \equiv b \pmod p$,niin tällöin

$$i(k-j) = ik - ij \equiv a - b \equiv a - a = 0 \ (mod\ p),$$

josta seuraa, että tulo $i(j-k)$ on jaollinen luvulla p. Koska p on alkuluku, tämä on mahdollista vain, jos ainakin toinen tekijöistä on jaollinen p:llä. Tämä ei kuitenkaan ole mahdollista, koska $0 < i < p$ ja $0 < k - j < p$. Rivillä/sarakkeella ei siten esiinny jäännösluokkien $0, 1, ..., p-1$ toistoja. Siinä on kuitenkin p alkiota, joten jokaisen jäännösluokan on esiinnyttävä siellä tasan yhden kerran. □

Tässä tutkielmassa käytetää yhteenlaskutaulun variaatiota modulo p, jossa rivin i alkio kerrotaan luvulla a.

Lause 2. *Olkoon $p \geq 2$ ja $a \in \mathbb{Z}_p$. Määritellään $p \times p$ -matriisi*

$$L^{(a)} = (L_{ij}^{(a)}), \qquad L_{ij}^{(a)} \equiv ai + j \ (mod \ \ p),$$

missä $i, j \in \{0, 1, ..., p-1\}$. Matriisi on latinalainen neliö, silloin kun p on alkuluku ja $a \not\equiv 0$ (mod p).

Todistus. Tarkastellaan neliön rivejä. Kiinnitetään i. Oletetaan , että samalla rivillä

$$L_{ij}^{(a)} \equiv L_{ik}^{(a)} \ (mod\ p).$$

Nyt

$$ai + j \equiv ai + k \ (mod\ p),$$

josta seuraa

$$j \equiv k \ (mod\ p).$$

Koska $j, k \in \{0, 1, ..., p-1\}$, tästä seuraa $j = k$. Samalla rivillä ei esiinnyt kahta samaa alkiota. Rivillä on kuitenkin p alkiota, joten jokainen jäännösluokka esiintyy rivillä vain kerran.

Tarkastellaan sarakkeiden alkiota ja kiinnitetään j. Oletetaan, että sarakkeella

$$L_{ij}^{(a)} \equiv L_{ik}^{(a)} \ (mod\ p).$$

Nyt

$$ai + j \equiv ak + j \ (mod\ p),$$

josta saadaan

$$a(i-k) \equiv 0 \ (mod\ p).$$

Koska p on alkuluku ja $a \not\equiv 0 \ (mod\ p)$, täytyy olla

$$i - k \equiv 0 \ (mod\ p),$$

joten nyt $i = k$. Joten myöskään sarakkeissa ei esiinnyt toistoa.

Nyt riveillä ja sarakkeilla ei esiinnyt toistoa, joten $L^{(a)} = (L_{ij}^{(a)})$, $L_{ij}^{(a)} \equiv ai + j \ (mod\ \ p)$ on latinalainen neliö. □

2.3 Latinalaisten neliöiden ortogonaalisuus

Tässä alaluvussa käsitellään latinalaisten neliöiden ortogonaalisuutta. Tätä ominaisuutta tarvitaan myöhemmin taikaneliöiden muodostamiseen. Esimerkeissä muodostetaan pareittain ortogonaalisia latinalaisia neliöitä.

Määritelmä 2. Kaksi n-rivistä latinalaista neliötä $L = (L_{ij})$ ja $L' = (L'_{ij})$ ovat *keskenään ortogonaalisia*, jos niiden n^2:n lukuparin (L_{ij}, L'_{ij}) joukossa esiintyvät kaikki mahdolliset parit (k, l) kukin tasan kerran, kun $0 \leq k < n$, ja $0 \leq l < n$.

Lause 3. *Valitaan alkuluku p sekä kertoimet a ja b siten, että 0<a<b<p. Tällöin latinalaiset neliöt L ja L' ovat keskenään ortogonaaliset.*

Todistus. Tehdään vastaoletus, että tällä tavalla tehdyssä neliössä $L^{(a,b)}$ esiintyy sama lukupari kahdesti kohdassa (i, j) ja (k, l). Tällöin on voimassa kongruenssit

$$ai + j \equiv ak + l \ (mod\ p) \text{ ja } bi + j \equiv bk + l.$$

Kun vähennetään ensimmäinen kongruenssi jälkimmäisestä seuraa siitä

$$bi + j - ai - j \equiv bk + l - ak - l \ (mod\ p)$$

$$\Rightarrow (b-a)i \equiv (b-a)k \ \ (mod\ \ p).$$

Kertotaulussa modulo p ei esiinny toistoja rivillä $b - a$. Tästä voidaan päätellä, että $i \equiv k$. Kun tulos sijoitetaan ylempänä olevaan kongruenssipariin kumpikin sievenee kongruenssiksi $j \equiv l$. Tästä seuraa, että taulukon ruutu (i, j) on sama ruutu kuin (k, l) □

Esimerkki 3. Taikaneliöiden muodostamiseen tarvitaan kaksi keskenään ortogonaalista latinalaista neliötä, joiden diagonaaleilla esiintyvät kaikki alkiot vain kerran.

Olkoon $p \geq 3$ ja latinalaisten neliöiden alkiot muodostuvat

$$L_{ij}^{(a)} \equiv ai + j \ (mod\ p).$$

Nyt päädiagonaali saa seuraavat arvot, kun $i = j$

$$L_{ii}^{(a)} \equiv (a+1)i \ (mod\ p).$$

Sivudiagonaaleilla $i + j = p - 1$ saadaan arvot

$$L_{i,p-1-i}^{(a)} \equiv (a-1)i + (p-1) \ (mod\ p).$$

Jotta kaikkien diagonaalien alkiot muodostavat täydellisen jäännösluokkajärjestelmän modulo p, täytyy olla

$$syt(a+1,p) = syt(a-1,p) = 1.$$

Tästä seuraa, että $a \not\equiv \pm 1 \quad (mod\ p)$. Latinalaisen neliön muodostuksessa täytyy valita a, tätä ehtoa noudatten eli $2 \leq a < p - 2$.

Esimerkki 4. Muodostetaan kaksi keskenään ortogonaalista latinalaista neliötä $L_{ij}^{(a)}$, jossa

$$L_{ij}^{(a)} \equiv ai + j (mod\ p) \text{ ja } L_{ij}^{(b)} \equiv bi + j (mod\ p).$$

Jotta neliöt ovat varmasti keskenään ortogonaaliset, valitaan jokin alkuluku p ja luvut a, b väliltä $2 \leq a < b < p-1$. Nyt $p = 5$, $a = 2$ ja $b = 3$, joten saadaan yhtälöt

$$L_{ij}^{(2)} \equiv 2i + j \ (mod\ m) \text{ ja } L_{ij}^{(3)} \equiv 3i + j \ (\text{mod m}).$$

Täytetään luvun p, tässä tapauksessa 5, jäännösluokkataulua kaavojen mukaan, kun i on pystyrivi ja j vaakarivi.

$i \backslash j$	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

$i \backslash j$	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

Seuraavaksi yhdistetään neliöiden alkiot samoihin ruutuihin.

00	11	22	33	44
23	34	40	01	12
41	02	13	24	30
14	20	31	42	03
32	43	04	10	21

Huomataan, että jokainen alkioyhdistelmä esiintyy vain kerran taulukossa, joten latinalaiset neliöt $L^{(1)}$ ja $L^{(3)}$ ovat keskenään ortogonaalisia.

3 Taikaneliöt

Tässä luvussa käsitellään taikaneliön määritelmää. Esimerkeissä konstruoidaan taikaneliöitä ortogonaalisten latinalaisten neliöiden avulla, sekä tutustutaan taikaneliön ominaisuuksiin.

Määritelmä 3. Kertaluvun n taikaneliö on $n \times n$ -matriisi, jonka alkioina esiintyvät kaikki luvut $0, 1, ..., n^2 - 1$. Jokaisen rivin, sarakkeen ja diagonaalin alkioiden yhteen laskettu summa on sama. Tätä summaa kutsutaan taikaneliön taikavakioksi.

Lause 4. *Valitaan $m > 1$. Olkoon L ja L' kaksi m-rivistä latinalaista neliötä. Niistä muodostetaan uusi $m \times m$ neliö M seuraavalla tavalla:*

$$M_{ij} = L_{ij} + mL'_{ij}.$$

Tässä tapauksessa laskutoimitukset ovat yhteen- ja kertolaskuja, eli ei kongruensseja modulo m. Tällöin neliön M jokaisen vaaka- ja pystyrivin summa on sama. Jos lisäksi L ja L' ovat keskenään ortogonaalisia, niin M on taikaneliö.

Todistus. Tiedätään, että neliöillä L j L' jokaisen rivin lukujen summa on $m(m-1)/2$. Jolloin neliön mL' jokaisen rivin lukujen summa on $m^2(m-1)/2$. Tästä seuraa, että neliön M jokaisen rivin summa on

$$= \frac{m(m-1)}{2} + \frac{m^2(m-1)}{2} = \frac{m(m-1)(m+1)}{2}.$$

Neliöiden L ja L' luvut ovat välillä $0, .., m-1$. Ortogonaalisuuden vuoksi kukin mahdollinen lukupari (x, y) esiintyy tarkalleen kerran. Näin ollen neliössä M esiintyy kaikki luvut välillä $[0, m^2 - 1]$. □

Esimerkki 5. Käytetään esimerkissä ortogonaalisista latinalaisista neliöistä luotua yhdistettyä neliötä.

00	11	22	33	44
23	34	40	01	12
41	02	13	24	30
14	20	31	42	03
32	43	04	10	21

Tästä neliöstä voidaan muodostaa taikaneliö M. Sen alkiot saadaan seuraavalla kaavalla

$$M_{ij} = L_{ij} + mL'_{ij}.$$

Koska on valittu m=5, niin

$$M_{ij} = L_{ij}^{(1)} + 5L_{ij}^{(3)}.$$

0	6	12	18	24
17	23	4	5	11
9	10	16	22	3
21	2	8	14	15
13	19	20	1	7

Nyt huomataan, että jokaisen rivin, sarakkeen ja diagonaalin summa on

$$\frac{m(m-1)(m+1)}{2} = \frac{5(5-1)(5+1)}{2} = 60.$$

Esimerkki 6. Muodostetaan taikaneliö tässä tutkielmassa annettujen tietojen avulla. Aloitetaan muodostamalla kaksi keskenään ortogonaalista latinalaista neliötä. Valitaan $m = 11$ ja jotkin luvut a ja b väliltä $2 \leq a, b \leq m-2$,

$$L_{ij}^{(a)} \equiv ai + j \textit{(mod m)} \text{ ja } L_{ij}^{(b)} \equiv bi + j \textit{(mod m)}.$$

Nyt

$$L_{ij}^{(2)} \equiv 2i + j \ \textit{(mod 11)}$$

i/j	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0	1
2	4	5	6	7	8	9	10	0	1	2	3
3	6	7	8	9	10	0	1	2	3	4	5
4	8	9	10	0	1	2	3	4	5	6	7
5	10	0	1	2	3	4	5	6	7	8	9
6	1	2	3	4	5	6	7	8	9	10	0
7	3	4	5	6	7	8	9	10	0	1	2
8	5	6	7	8	9	10	0	1	2	3	4
9	7	8	9	10	0	1	2	3	4	5	6
10	9	10	0	1	2	3	4	5	6	7	8

$$\text{ja } L_{ij}^{(7)} \equiv 7i + j \ \textit{(mod 11)}$$

i/j	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	7	8	9	10	0	1	2	3	4	5	6
2	3	4	5	6	7	8	9	10	0	1	2
3	10	0	1	2	3	4	5	6	7	8	9
4	6	7	8	9	10	0	1	2	3	4	5
5	2	3	4	5	6	7	8	9	10	0	1
6	9	10	0	1	2	3	4	5	6	7	8
7	5	6	7	8	9	10	0	1	2	3	4
8	1	2	3	4	5	6	7	8	9	10	0
9	8	9	10	0	1	2	3	4	5	6	7
10	4	5	6	7	8	9	10	0	1	2	3

Seuraavaksi yhdistetään neliöiden alkiot samoihin ruutuihin.

00	11	22	33	44	55	66	77	88	99	1010
27	38	49	510	60	71	82	93	104	05	16
43	54	65	76	87	98	109	010	10	21	32
610	70	81	92	103	04	15	26	37	48	59
86	97	108	09	110	20	31	42	53	64	75
102	03	14	25	36	47	58	69	710	80	91
19	210	30	41	52	63	74	85	96	107	08
35	46	57	68	79	810	90	101	02	13	24
51	62	73	84	95	106	07	18	29	310	40
78	89	910	100	01	12	23	34	45	56	67
94	105	06	17	28	39	410	50	61	72	83

Jokainen alkioyhdistelmä esiintyy taulukossa vain kerran, joten latinalaiset neliöt $L^{(2)}$ ja $L^{(7)}$ ovat keskenään ortogonaaliset. Tästä neliöstä voidaan muodostaa taikaneliö M. Sen alkiot saadaan seuraavalla kaavalla

$$M_{ij} = L_{ij} + mL'_{ij}.$$

Koska on valittu $m = 11$, niin

$$M_{ij} = L^{(2)}_{i,j} + 11L^{(7)}_{ij}.$$

0	12	24	36	48	60	72	84	96	108	120
79	91	103	115	6	18	30	42	54	55	67
37	49	61	73	85	97	109	110	1	13	25
116	7	19	31	43	44	56	68	80	92	104
74	86	98	99	111	2	14	26	38	50	62
32	33	45	57	69	81	93	105	117	8	20
100	112	3	15	27	39	51	63	75	87	88
58	70	82	94	106	118	9	21	22	34	46
16	28	40	52	64	76	77	89	101	113	4
95	107	119	10	11	23	35	47	59	71	83
53	65	66	78	90	102	114	5	17	29	41

Lasketaan 11×11 -neliön taikavakio kaavan avulla, kun $m = 11$.

$$\frac{m(m-1)(m+1)}{2} = \frac{11(11-1)(11+1)}{2} = 660.$$

Viitteet

[1] Jyrki Lahtonen, Turun yliopisto; Päivölän opisto 4.6.2019

[2] Anthony B. Evans, Orthogonal Latin Squares Based on Groups 17.8.2018

[3] Seymor S Block, Santiago A Tavare, Before Sudoku The World of Magic Squares 24.2.2009

[4] Clifford A Pickover, The Zen of Magic Squares, Circles and Stars 2002