Linnæus University
Sweden

Degree project

Tribonacci Cat Map

A discrete chaotic mapping with Tribonacci matrix

Author: Linnea Fransson
Supervisor: Per-Anders Svensson
Examiner: Karl-Olof Lindahl
Date: 2021-05-26
Course code: 5MA41E
Subject: Mathematics
Level: Master

Department Of Mathematics

Acknowledgements

First of all, I would like to thank my friend and co-founder of Växjö MathsJam, Maria Ulan, whose encouragement made me take the first step of the long journey that became this thesis. Then, I would like to pass on my thanks to my supervisor, Per-Anders Svensson, for his guidance and immense patience during the whole process. Without his help, there would have not been a thesis today. I would also like to send my appreciation to my examiner, Karl-Olof Lindahl, for his wise words that helped improve my work even further. In fact, I would like to express my deepest gratitude to all teachers from the Department of Mathematics for believing in me and never giving up on me. Lastly, I would like to thank my mother for standing by me through all times, and the rest of my family and friends for their support.

Abstract

Based on the generating matrix to the Tribonacci sequence, the Tribonacci cat map is a discrete chaotic dynamical system, similar to Arnold's discrete cat map, but on three dimensional space. In this thesis, this new mapping is introduced and the properties of its matrix are presented. The main results of the investigation prove how the size of the domain of the map affects its period and explore the orbit lengths of non-trivial points. Different upper bounds to the map are studied and proved, and a conjecture based on numerical calculations is proposed. The Tribonacci cat map is used for applications such as 3D image encryption and colour encryption. In the latter case, the results provided by the mapping are compared to those from a generalised form of the map.

Keywords: Arnold's cat map, Tribonacci matrix, chaotic map, discrete dynamical system, linear recurrence sequence, Trisano period, 3D image encryption, colour encryption.

Contents

1 Introduction

When studying ergodic theory in the 1960s, the Russian mathematician, Vladimir Arnold, introduced the world to a new chaotic dynamical system [8]. By using the picture of a cat, Arnold showed how his newfound mapping rearranged the pixels into chaotic patterns before recreating the original image. This mapping has ever since been known as *Arnold's cat map*.

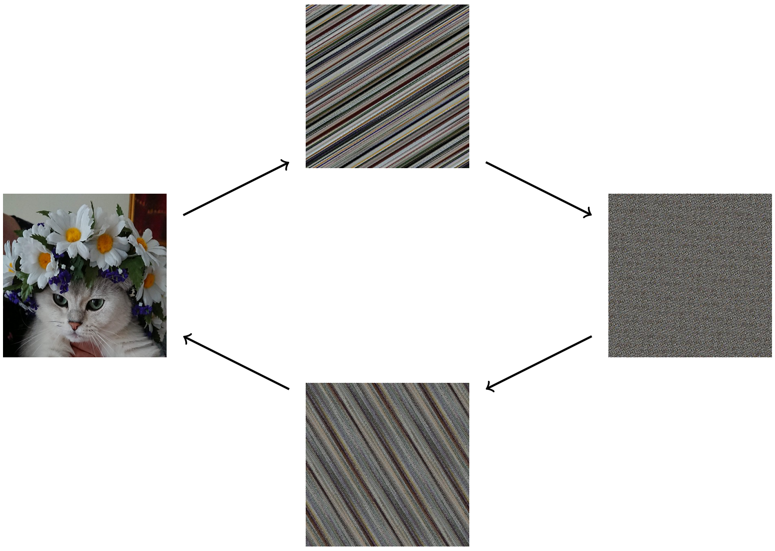


Figure 1: The image becomes unrecognisable for a number of iterations before returning to its original state.

From the very beginning, Arnold's cat map managed to catch the attention of mathematicians and cryptographers around the world due to its simple and yet powerful properties. Until today, there are articles being published regarding its mathematical structure and its computational usage (for a selected list on the subject, see References). Since it was first introduced, Arnold's cat map has been modified to more generalised forms (see section 2.5) and adapted to higher dimensions (see section 2.6).

The key to this mapping's chaotic attributes lies on its connection to the *Fibonacci sequence* (see section 2.2). This fact itself raises the question of whether the *Tribonacci sequence* could create an equally powerful map in three dimensions. Such map, the **Tribonacci cat map**, would be expected to have a mathematical structure worth being studied. Likewise, it could become an effective alternative to the three dimensional adaptation of Arnold's cat map in applications such as encryption and watermarking.

1.1 Purpose of the thesis

The main purpose of this thesis is to study the properties of the discrete three dimensional cat map based on the Tribonacci matrix, i.e. the Tribonacci cat map. In other words, we will examine the outcomes of a 3D image once it has been exposed to the mapping. In order to achieve this purpose, the investigations and analysis will focus on the questions:

1. How does the size of a 3D image affect the number of iterations of the whole image?

2. To what extent does the image size have an impact on the iterations of single pixels?

Besides answering these questions, this thesis will also look at possible applications of the Tribonacci cat map, presenting examples of 3D image encryption and colour encryption.

1.2 Methods

Much of the work presented here is based on empirical investigations and numerical calculations performed by the software Wolfram Mathematica™. The codes used for the purposes of this thesis can be found in the appendix (see A Mathematica code), guaranteeing the replicability of the results. Alongside with the empirical investigations, this thesis also presents work based on theoretical results.

The first result consists in proving the strong relation between the *period*[1] of the Tribonacci cat map and the period of the Tribonacci sequence in Theorem 4.2 by using matrix and divisibility properties. Due to such relation, it has been deemed sufficient to prove the periods of the Tribonacci sequence and simply adapt them to the Tribonacci cat map. These periods have then been grouped based on the factorisation of the size of the 3D image. Theorems 4.5 and 4.8 use results from Wadill's paper [23] in their proofs. The main result of this thesis, Theorem 4.9, proves the properties of the periods of 3D images with prime sizes. The proof relies on results from Number Theory, such as the Legendre symbol and its properties, and concepts from Abstract Algebra, such as kernel, norm map, extension fields and multiplicative groups. The proof is also built on two propositions from previous works, namely Propositions 4.10 and 4.11. The former is about the relation between the discriminant of a polynomial and the number of its factors modulo a prime. It was originally introduced by Stickelberger and can be found in Carlitz's article [5]. The latter is taken from Adams & Shanks in [1] and presents the relation between the period of a third order linear recurrence and the roots of its minimal polynomial.

When studying the upper bounds of the Tribonacci cat map, Corollaries 4.13 and 4.14 are based on an adaptation of Theorem 4.9 and use straightforward modular calculations to prove the upper bounds of two sets of primes. In order to make a conjecture on a possible upper bound for all periods of the mapping, the first 10,000 periods are calculated. Thereafter, numerical calculations of ratios and least common multiples of periods are taken into consideration in order to produce Conjecture 4.15. Even the study of *orbit lengths*[2] relies on both inductive and deductive analysis. Concepts like divisibility from Number Theory and multiplicative order from Abstract Algebra play a major role in the presentation of the orbit lengths for different sizes of the 3D image. Theorem 4.16 and Corollary 4.17 use modular system of equations to prove the number of disjoint orbits with length 1 in even and odd sized images respectively.

For the image encryptions, two pictures were used. The first one was taken from the author's private album and depicts the author's family cat. It was used in its original quadratic format for the colour encryption and, for the 3D image encryption, copies of the picture were placed on top of each other in order to give it depth. The number of copies was the same as the side of the picture. The second image was already cubic to begin with and it was taken from the software

[1] A period is the minimum number of iterations that takes the whole image back to its original state. A proper definition can be found on page 5.

[2] An orbit length is the mininum number of iterations that takes a single pixel back to its original position. A proper definition can be found on page 5.

Wolfram Mathematica$^{\text{TM}}$'s own collection of example images. The picture can be found in the *TestImage3D* collection under the name "MRKnee". In the 3D image encryption, the two images were compared to each other after being encrypted using the Tribonacci cat map. Meanwhile, in the colour encryption, the results from the original Tribonacci cat map were compared to those achieved by a generalised form of the mapping presented in section 4.5. The analysis of all encryptions performed for this thesis is entirely based on empirical observations.

1.3 Limitations

The calculations performed for this thesis were dependent on the computer where the software Wolfram Mathematica$^{\text{TM}}$ was installed. This explains the number of calculated periods being limited to 10,000, as the process of retrieving the periods becomes more demanding and time consuming for greater numbers. Conjecture 4.15 is built upon the values achieved in the interval and might be refuted with further period calculations. Likewise, the encryptions realised in this investigation had to obey the limitations of the hardware and could not be carried out with images over a certain size or with large periods.

1.4 Thesis overview

Sections 2 and 3 contain the necessary theoretical background for the results presented in sections 4 and 5. In section 2, we present the original two dimensional chaotic map, Arnold's cat map, and introduce its discrete version used in image encryption. We look into the properties of the map and its matrix, and focus on the results regarding its periods and orbits. We also mention two forms of generalised cat maps and conclude the section with examples of discrete cat maps in higher dimensions. Section 3 is dedicated to the results in Abstract Algebra and Number Theory that are used in the proofs in section 4.

The Tribonacci cat map, along with its general properties, is proposed in section 4. We study its matrix and its connection to the Tribonacci sequence. The main results of the thesis, already mentioned in subsection 1.2, are contained in this section. We prove the properties of the periods for different domain sizes based on the content in section 3 and examine the upper bounds of the mapping. We also investigate the orbit lengths and analyse them using empirical results and theoretical concepts from section 3. At the end of the section, we suggest a generalised Tribonacci cat map.

In section 5, we use the proposed Tribonacci cat map for 3D image encryption and relate the choices of image sizes to the results on periods and orbit lengths in section 4. The outcomes are compared to those obtained using the discrete version of Arnold's cat map. We also perform colour encryption and compare the results attained by the original Tribonacci cat map and a generalised form of the map. There is a short discussion on the advantages of the generalised map over the original for colour encryption.

Lastly, in section 6, we summarise the results from sections 4 and 5, and discuss them even further. At the end of the section, we propose future investigations on the subject. The codes used for data gathering and image encryption are listed in appendix A. The sets of prime numbers mentioned in the analysis of upper bounds and orbit lengths in section 4 can be found in appendix B.

2 Preliminaries

In this section, we focus on the original Arnold's cat map. We start by introducing the properties of the map in subsection 2.1, and defining a couple of concepts, like *period* and *orbit*, that are vital for the understanding of the main results in section 4. In subsection 2.2, we study the matrix used in the map, also known as *the cat matrix*, and present its connection to the generating matrix of the Fibonacci sequence. In subsection 2.3, we analyse the periods of the Fibonacci sequence and transfer them to the discrete version of Arnold's cat map. The connection between the periods is proved in Theorem 2.4. At the end of the subsection, we state the upper bounds of the map. The orbits, more precisely the orbit lengths, are displayed with the help of colourful matrices in subsection 2.4. A couple of examples of generalised cat maps are demonstrated in subsection 2.5, while a couple of examples of discrete cat maps in higher dimensions are suggested in subsection 2.6.

2.1 Arnold's cat map

Let (x, y) be the coordinates of a point in the unit square, such that $0 \leq x, y < 1$. *Arnold's cat map* (ACM) takes (x, y) to the new point (x', y'), where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1.$$

ACM is a dynamical system that works in discrete time and generates a chaotic mapping inside a two-dimensional torus, a *toral automorphism.* This means that, after a finite number of iterations, all points in the domain return to their original positions at the same time.

Mathematicians and computer scientists have shown a particular interest in the discrete version of ACM, the so-called *Arnold's discrete cat map* (DCM) (e.g. [2, 6, 8, 15]). Instead of working within the unit square, the domain of the mapping is expanded to an $N \times N$ plane, i.e. a plane of size N^2, and the coordinates of the points in the domain are scaled to the integer coordinates $0 \leq x, y \leq N - 1$. For every discrete time $t, t \geq 1$, the new mapping becomes

$$\begin{pmatrix} x_t \\ y_t \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_{t-1} \\ y_{t-1} \end{pmatrix} \pmod N.$$

Example 2.1. Consider the 4×4-matrix and the (x, y)-coordinates of its elements modulo 4:

$$\begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{pmatrix} \equiv \begin{pmatrix} (0,3) & (1,3) & (2,3) & (3,3) \\ (0,2) & (1,2) & (2,2) & (3,2) \\ (0,1) & (1,1) & (2,1) & (3,1) \\ (0,0) & (1,0) & (2,0) & (3,0) \end{pmatrix} \pmod 4$$

This is what happens to the matrix when DCM is applied to it:

$$\begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{pmatrix} \mapsto \begin{pmatrix} B & H & J & P \\ G & I & O & A \\ L & N & D & F \\ M & C & E & K \end{pmatrix} \mapsto \begin{pmatrix} H & A & N & K \\ O & L & E & B \\ F & C & P & I \\ M & J & G & D \end{pmatrix} \mapsto \begin{pmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{pmatrix}.$$

Here is what happens to the coordinates of four arbitrary elements in the matrix:

$$\begin{array}{rcccccc} D:(3,3) & \mapsto & (2,1) & \mapsto & (3,0) & \mapsto & (3,3); \\ K:(2,1) & \mapsto & (3,0) & \mapsto & (3,3) & \mapsto & (2,1); \\ P:(3,0) & \mapsto & (3,3) & \mapsto & (2,1) & \mapsto & (3,0); \\ J:(1,1) & \mapsto & (2,3) & \mapsto & (1,0) & \mapsto & (1,1). \end{array}$$

It takes three iterations of the DCM to return the matrix to its original state. The coordinates of the elements D, K and P are mapped to each other, while the coordinates of the element J are mapped to other elements in the matrix. After a closer look, one can see that J is mapped to the coordinates of the elements C and N. The 4×4 plane in the example has *period* 3 and the coordinates of the elements D, K and P belong to one *orbit*, while the coordinates of the elements J, C and N belong to another orbit.

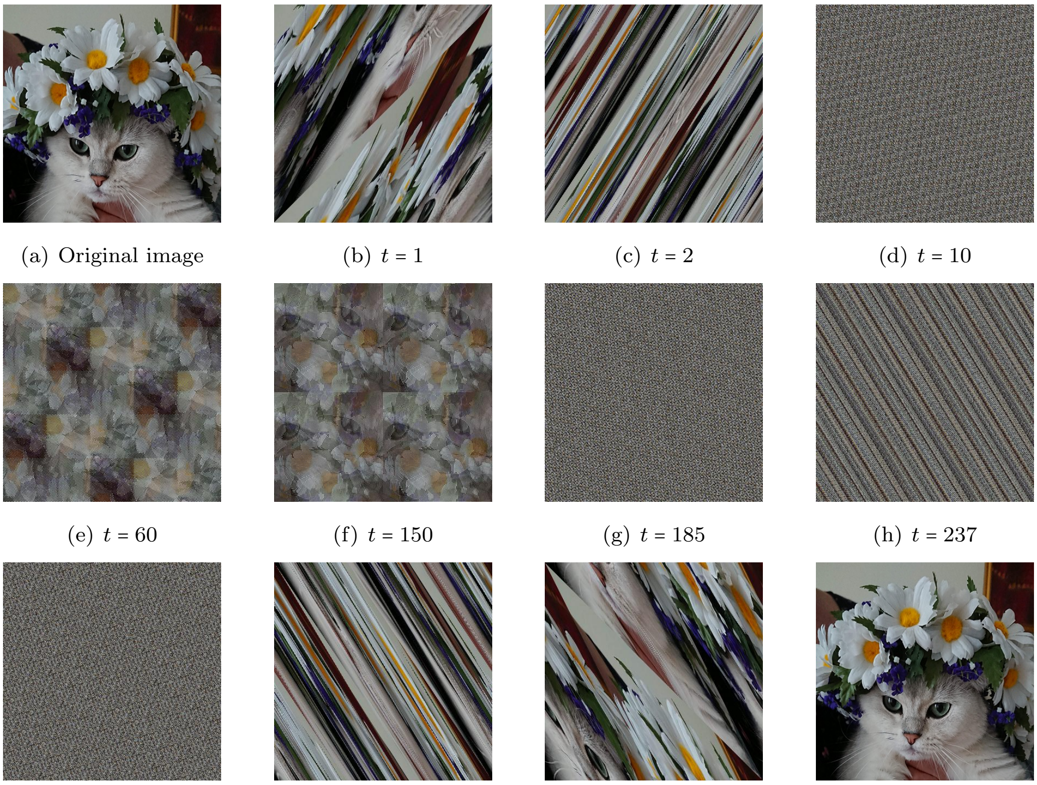
Definition 2.1. The *period* of the DCM is the smallest positive integer t such that

$$\begin{pmatrix} x_t \\ y_t \end{pmatrix} \equiv \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \pmod{N},$$

for all points (x, y) in the domain. In other words, it is the minimum number of iterations that maps the whole plane back to its original state. In this thesis, the period of a DCM on a plane of size N^2 will be denoted by $\rho(N)$.

Definition 2.2. The *orbit* of a point is the set of all coordinates that the point is mapped to under the iterations of the DCM, until being mapped back to itself. The *orbit length* is the number of distinct coordinates in the set. In Example 2.1, all points except for M have orbit length 3. As it only maps to itself, M is called a *fixed point* and has orbit length 1. The origin is always a fixed point so it is known as *trivial point.*

Due to its chaotic nature, DCM has been studied and used in image encryption and watermarking over the recent years (e.g. [4, 7, 14]). On the next page, there is an example to illustrate the behaviour of DCM on a picture of size 400×400 pixels after t iterations.


(a) Original image (b) $t = 1$ (c) $t = 2$ (d) $t = 10$

(e) $t = 60$ (f) $t = 150$ (g) $t = 185$ (h) $t = 237$

(i) $t = 286$ (j) $t = 298$ (k) $t = 299$ (l) $t = 300$

Figure 2: The original image is successfully retrieved after 300 iterations.

Since it takes 300 iterations to recover the original image for the first time, the period in this case is $\rho(400) = 300$. After one iteration, the picture is relatively chaotic yet not unrecognisable. On the second iteration, however, the cat is no longer visible even though the original colours are still distinguishable. For most of the iterations, the result is similar to the one at $t = 10$. When $t = 150$, and for a few other values of t, there are ghosts of the original picture covering the plane. This phenomenon, along with the occurrence of miniatures of the mapped image, is investigated and discussed in Behrends' article [3].

2.2 Properties of the matrix

The chaotic properties of Arnold's cat map derive from its matrix[3]

$$\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Its determinant is equal to 1, which results in the mapping being area preserving. This means that, apart from shuffling the points inside the unit square in the ACM (or inside the $N \times N$-image in the DCM), there is neither any loss nor changes made to the points in the domain.

The entries of A are in fact Fibonacci numbers. Recall that the *Fibonacci sequence* $(F_n)_{n=0}^{\infty}$ is defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The numbers in the sequence can

[3] In some literature, such as in [3], the matrix is given by $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ instead.

be generated by the matrix

$$\mathbf{F} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \text{where} \quad \mathbf{F}^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

When $\mathbf{F}$ is multiplied by itself, the result becomes the cat matrix. Thus the powers of $\mathbf{A}$ are also powers of the generating Fibonacci matrix.

$$\mathbf{F}^2 = \begin{pmatrix} F_1 & F_2 \\ F_2 & F_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \mathbf{A} \quad \text{and}$$

$$\mathbf{A}^n = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^n = \begin{pmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{pmatrix}.$$

The minimal polynomial of $\mathbf{A}$ is $P_A(x) = x^2 - 3x + 1$, with discriminant 5 and roots

$$x_1 = \frac{3+\sqrt{5}}{2} \quad \text{and} \quad x_2 = \frac{3-\sqrt{5}}{2}.$$

The connection to the Fibonacci sequence, together with the discriminant of the minimal polynomial, has a major impact on the periods of DCM.

2.3 Periods

Since the matrix in the DCM is derived from the Fibonacci generating matrix, its period modulo N is strongly related to the period of the recurrence relation modulo N.

Definition 2.3. In the Fibonacci sequence, the smallest positive integer k such that $F_k \equiv F_0 \pmod{N}$ and $F_{k+1} \equiv F_1 \pmod{N}$ is called the *Pisano period*. It will be denoted by $\pi(N)$.

In other words, a Fibonacci sequence with Pisano period $\pi(N) = k$ looks like this:

F_0	F_1	F_2	F_3	$\cdots$	F_{k-2}	F_{k-1}	F_k	F_{k+1}	F_{k+2}	F_{k+3}
0	1	1	2	$\cdots$	$N-1$	1	0	1	1	2

Theorem 2.4. *For every integer $N \geq 3$, the period of DCM modulo N is given by*

$$\rho(N) = \frac{\pi(N)}{2}.$$

Proof. Let $\pi(N) = k$. It means that

$$\mathbf{F}^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}.$$

Since $\mathbf{A} = \mathbf{F}^2$, then $\mathbf{A}^{k/2} = \mathbf{F}^k$ and the theorem follows. □

Remark. The theorem works because $\pi(N)$ is always even for $N > 2$. Further details about the Pisano period can be found in Wall's article [24].

Example 2.2. The Pisano period for $N = 74$ is 228 while its cat map period is 114. Likewise, $\pi(37) = 76$ while $\rho(37) = 38$.

In order to better understand the periods of the cat map for different values of N, it is inevitable to firstly introduce the properties of the Pisano period. Wall presents an extensive study with proofs in [24]. Here are some of the known properties that are relevant for this thesis:

(i) If N is a prime such that $p \equiv \pm 1 \pmod 5$, then $\pi(p) \mid p - 1$.

(ii) If N is a prime such that $p \equiv \pm 2 \pmod 5$, then $\pi(p) \mid 2(p + 1)$.

(iii) If N is a prime power such that $N = p^k$ and if $\pi(p^2) \neq \pi(p)$, then $\pi(p^k) = p^{k-1}\pi(p)$, $k \geq 2$.

(iv) If N is composite and has the prime factorisation $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, then $\pi(N) = \operatorname{lcm}(\pi(p_i^{\alpha_i}))$, where lcm is *the least common multiple.*

Remark. Properties (i) and (ii) provide information for calculating $k\pi(N)$, i.e. a multiple of the period, where k is a positive integer.

Example 2.3. Let $N = 27$. Since $27 = 3^3$ and $3 \equiv -2 \pmod 5$, properties (ii) and (iii) can be used. The former yields $\pi(3) \mid 8$ and, in this case, $\pi(3) = 8$. The latter property gives $\pi(27) = 9 \cdot \pi(3) = 9 \cdot 8 = 72$.

Example 2.4. Let $N = 33 = 3 \cdot 11$. From the previous example it is known that $\pi(3) = 8$. Property (i) states that $\pi(11) \mid 10$, which is the case as $\pi(11) = 10$. Finally, according to property (iv), the period becomes $\pi(33) = \operatorname{lcm}(8, 10) = 40$.

It is noteworthy that even though property (iv) is based on the hypothesis $\pi(p^2) \neq \pi(p)$, there are still no known primes that fulfill $\pi(p^2) = \pi(p)$. These primes are called *Wall-Sun-Sun primes*[4] and the search for them is still ongoing [16]. By 2014, a project held by PrimeGrid could verify that no such prime exists up to $28 \cdot 10^{15}$ [17]. Nonetheless, it has not been proven that Wall-Sun-Sun primes do not exist.

Observe that properties (i) and (ii) depend on the discriminant of the Fibonacci matrix, which is the same as the discriminant of the cat matrix. According to these properties, the period of the cat map for $N = p$, p a prime, is conditioned to whether 5 is a quadratic residue[5] of p, as in property (i), or not, as in (ii).

The periods of the cat map and their properties can be easily derived from the Pisano periods. The results from Theorem 2.4 are clear in (i) and (ii):

(i)* If N is a prime such that $p \equiv \pm 1 \pmod 5$, then $\rho(p) \mid \frac{p-1}{2}$.

(ii)* If N is a prime such that $p \equiv \pm 2 \pmod 5$, then $\rho(p) \mid p + 1$.

(iii)* If N is a prime power such that $N = p^k$, $p > 2$, and if $\rho(p^2) \neq \rho(p)$, then $\rho(p^k) = p^{k-1}\rho(p)$, $k \geq 2$.

(iv)* If N is composite and has the prime factorisation $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, then $\rho(N) = \operatorname{lcm}(\rho(p_i^{\alpha_i}))$.

[4] In Peng's article [16], these primes are called *Fibonacci-Wieferich primes.*

[5] A definition of *quadratic residue* can be found on page 14.

Remark. Unlike with the Pisano period, there is at least one known prime, i.e. $p = 2$, where $\rho(p^2) = \rho(p)$.

Example 2.5. For the composite numbers $N_1 = 27$ and $N_2 = 33$, the cat map periods are $\rho(27) = 36$ and $\rho(33) = 20$. For the prime numbers $p = 41 \equiv 1 \pmod 5$ and $p = 43 \equiv -2$ (mod 5), the periods are $\rho(41) = 20$ and $\rho(43) = 44$.

Authors like Bao and Chen study the properties (i)*-(iv)* and deepen their investigations by analysing the periods of a generalised DCM in [2] and [6] respectively. More on these under subsection 2.5. Dyson and Falk take one step further and examine the lower and upper bounds of the periods of DCM in [8]. In their article, they state and prove the following theorem regarding the upper bounds:

Theorem 2.5. *For a positive integer k,*

$$\begin{aligned}
\rho(N) &= 3N \quad \textit{when } N = 2 \cdot 5^k, \\
\rho(N) &= 2N \quad \textit{when } N = 5^k \textit{ or } N = 6 \cdot 5^k, \\
\rho(N) &\leq \frac{12}{7}N \quad \textit{for all other } N.
\end{aligned}$$

2.4 Orbit lengths

For any value of N, the orbit lengths of the points in the domain are less or equal to $\rho(N)$. Moreover, they are divisors of the period and the origin is the only fixed point with orbit length equal to 1. Consequently, there are a number of disjoint orbits in the DCM, as seen in Example 2.1 on page 4.

When N is a prime number p, where $p \neq 5$, all orbit lengths of the non-trivial points are equal to $\rho(N)$. In the case where $N = 5$, the lengths of the orbits are either equal to $\rho(5) = 10$ or equal to $\rho(5)/5 = 2$. Gaspari presents an extensive investigation on orbits and orbit lengths for prime periods of DCM in [11].

Example 2.6. The orbit lengths of each point in the DCM when $N = 5$ and $N = 7$ are presented as entries in the matrices[6] below.

$$\begin{pmatrix}
10 & 10 & 10 & 2 & 10 \\
10 & 2 & 10 & 10 & 10 \\
10 & 10 & 10 & 10 & 2 \\
10 & 10 & 2 & 10 & 10 \\
\mathbf{1} & 10 & 10 & 10 & 10
\end{pmatrix}
\qquad
\begin{pmatrix}
8 & 8 & 8 & 8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 \\
\mathbf{1} & 8 & 8 & 8 & 8 & 8 & 8
\end{pmatrix}$$

$N = 5$ $\qquad$ $N = 7$

When N is a composite number, except for when $N = 4$, there will be at least three different

[6] The idea of illustrating the orbit lengths in colourful matrices is taken from Svanström's work on a generalised Arnold's cat map [21].

orbit lengths: 1 (the trivial point), $\rho(N)$ and at least one non-trivial divisor of $\rho(N)$. In the special case for $N = 4$, all non-trivial points have orbit length equal to $\rho(4) = 3$.

Example 2.7. The matrices below illustrate the orbit lengths for each point in the DCM when $N = 6$ and $N = 8$.

$$\begin{pmatrix} 12 & 12 & 12 & 12 & 12 & 12 \\ 4 & 12 & 4 & 12 & 4 & 12 \\ 3 & 12 & 12 & 3 & 12 & 12 \\ 4 & 12 & 4 & 12 & 4 & 12 \\ 12 & 12 & 12 & 12 & 12 & 12 \\ \mathbf{1} & 12 & 4 & 3 & 4 & 12 \end{pmatrix} \qquad \begin{pmatrix} 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 3 & 6 & 3 & 6 & 3 & 6 & 3 & 6 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ \mathbf{1} & 6 & 3 & 6 & 3 & 6 & 3 & 6 \end{pmatrix}$$

$N = 6$ $\qquad$ $N = 8$

2.5 Generalised cat map

As mentioned earlier in subsection 2.3, there are generalised forms of DCM. These are preferred over the original mapping for encryption and image validation because of their diversity. The entries in the generalised cat matrices are not uniquely determined as in the original, which leads to different periods for the same modulo N.

On an N^2 plane, a general form of DCM is

$$\begin{pmatrix} x_t \\ y_t \end{pmatrix} \equiv \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \begin{pmatrix} x_{t-1} \\ y_{t-1} \end{pmatrix} \pmod{N}$$

where $p, q \in \{0, 1, \cdots, N-1\}$.

As Chen et al. state in their paper [6], as long as the determinant of the cat matrix is equal to 1, the map is area preserving and periodic for any initial point. They study the properties of the periods and their range for different values of p and q under the same modulo N. One of their examples states that, for $N = 17$, there are 16 different cat maps with the maximum period 34 and 48 mappings with period equal to 18.

Bao & Yang take a different step in [2] and study the generalised form of DCM when $p = q$:

$$\begin{pmatrix} x_t \\ y_t \end{pmatrix} \equiv \begin{pmatrix} 1 & a \\ a & 1+a^2 \end{pmatrix} \begin{pmatrix} x_{t-1} \\ y_{t-1} \end{pmatrix} \pmod{N}.$$

Like in Chen's paper, Bao & Yang present and prove several theorems regarding the generalised mapping's periods. For example, for any value of a, if $N = a^2$, then the period of the cat map is equal to a.

2.6 Higher dimensions

Over the years, extensions of DCM into higher dimensions have also been studied. In his paper, Nance creates a three dimensional cat matrix by fixing each one of the coordinates in the x, y, z-space and keeping the original 2×2 matrix on the remaining coordinates [15]. He presents a similar example for the four-dimensional case, which is based on the 3×3 matrix, and introduces a general formula for the creation of an n-dimensional cat matrix. A three dimensional cat matrix created according to Nance's instructions can be seen below:

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 2\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 1 & 2 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1 & 1\\ 2 & 3 & 2\\ 3 & 4 & 4\end{pmatrix}. \tag{2.1}$$

It is important, however, to highlight that the matrix in (2.1) is not unique due to the non-commutative properties of matrix multiplication. There are as many as 6 possible cat matrices in three dimensions and at most $\prod_{k=3}^{n} k!$ different alternatives in n dimensions. Nevertheless, all versions in any dimension will have the determinant equal to 1, keeping the volume preserving properties of the mapping.

Here is one of the $4! \cdot 3! = 144$ different versions of the four dimensional DCM based on the 3×3 matrix in (2.1):

$$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 1 & 1\\ 0 & 2 & 3 & 2\\ 0 & 3 & 4 & 4\end{pmatrix}\begin{pmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 0 & 0\\ 2 & 0 & 3 & 2\\ 3 & 0 & 4 & 4\end{pmatrix}\begin{pmatrix}1 & 1 & 0 & 1\\ 2 & 3 & 0 & 2\\ 0 & 0 & 1 & 0\\ 3 & 4 & 0 & 4\end{pmatrix}\begin{pmatrix}1 & 1 & 1 & 0\\ 2 & 3 & 3 & 0\\ 3 & 4 & 4 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}17 & 23 & 18 & 5\\ 110 & 149 & 117 & 31\\ 257 & 348 & 274 & 72\\ 432 & 585 & 460 & 122\end{pmatrix}.$$

Since the chaotic properties of the cat map are preserved in higher dimensions, these matrices have also gained their place in image encryption. An example is Ganesan and Murali's proposition of using an 8×8 cat matrix in an encryption algorithm in [10]. The size of the matrix is to match with the number of bits of each pixel in the image. In their article, they use a different but similar approach to Nance's when creating the eight dimensional matrix.

In most cases, the three dimensional extension of the cat map is enough. In [7], Choi et al. create a generalised version of the 3×3 matrix and use it to encrypt colour medical images by shuffling the positions of the colour pixels in the RGB-channels. Meanwhile, in [18], Raj et al. use a three dimensional version of DCM to separately encrypt the vertices and the faces of 3D models.

3 Mathematical background

The main results of the thesis, presented in section 4, rely on previous knowledge from both Abstract Algebra and Number Theory. The purpose of this section is to introduce the reader to the necessary concepts and theorems. The proofs are omitted here but can be found in Hungerford's *Abstract Algebra* [12] and Rosen's *Elementary Number Theory* [19].

3.1 Abstract Algebra

The main result in section 4, namely Theorem 4.9 that proves the properties of the periods for prime values of N, is based on the concept of finite fields and their properties.

Theorem 3.1. *Let F be a finite field. Then, for a specific prime p and any element $\alpha \in F$, it is true that*

$$\underbrace{\alpha + \alpha + \cdots + \alpha}_{p\ times} = p\alpha = 0.$$

Example 3.1. The set of rational numbers, $\mathbb{Q}$, is an infinite field. Meanwhile, the set $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ is a finite field, and any element in $\mathbb{Z}_7$ multiplied by the prime number 7 is equal to 0 modulo 7.

Definition 3.2. Let F and K be fields where F is finite and $F \subseteq K$. Suppose $\alpha \in K$ is algebraic over F. Then the smallest subfield of K that contains α and all elements of F is called a *finite extension field* and will be denoted $F(\alpha)$.

Definition 3.3. The *order* of a finite field F is the number of elements in it. The order of F is denoted $|F|$.

Theorem 3.4. *If F has p elements, where p is prime, then the finite extension field $K = F(\alpha)$ has order equal to a power of p.*

Example 3.2. The finite field $\mathbb{Z}_7$, with size $|\mathbb{Z}_7| = 7$, does not contain the roots of the polynomial $P(x) = x^2 - 3$. The finite field $\mathbb{Z}_7(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_7\}$, on the other hand, contains both the field $\mathbb{Z}_7$ and the roots of $P(x)$. It is therefore an extension field of $\mathbb{Z}_7$ and has size $\left|\mathbb{Z}_7(\sqrt{3})\right| = 7^2 = 49$.

Besides finite fields and their finite extensions, Theorem 4.9 also deals with multiplicative groups and some properties related to them.

Definition 3.5. The *multiplicative group F^** of the finite field F contains all non-zero elements of F.

Theorem 3.6. *If F is a finite field, then the multiplicative group F^* is cyclic, i.e.*

$$F^* = \{\alpha^k \mid k \in \mathbb{Z}\},$$

for some $\alpha \in F^*$.

Example 3.3. Take the subset $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ of the field $\mathbb{Z}_7$. It is cyclic and generated by 3:

$$\begin{aligned} &3^1 \equiv 3 \pmod 7, && 3^2 \equiv 2 \pmod 7, && 3^3 \equiv 6 \pmod 7, \\ &3^4 \equiv 4 \pmod 7, && 3^5 \equiv 5 \pmod 7, && 3^6 \equiv 1 \pmod 7. \end{aligned}$$

Definition 3.7. Let α be an element of the subgroup F^* of the finite field F. The smallest positive integer k such that $\alpha^k = 1$ is called the *multiplicative order of* α. In this thesis, it will be denoted by $\operatorname{ord}(\alpha)$.

The definition of the multiplicative order of an element is important both for the proof of Theorem 4.9 and for the study of orbit lengths. Furthermore, the following theorems and definitions are equally important.

Theorem 3.8. *Let α be an element in F^*. Then $ord(\alpha) \mid |F^*|$.*

Example 3.4. Looking back at Example 3.3, we see that $\operatorname{ord}(3) = 6$ and $|\mathbb{Z}_7^*| = 6$. Clearly, $\operatorname{ord}(3) \mid |\mathbb{Z}_7^*|$. With simple calculations, we can also see that

$$\operatorname{ord}(1) = 1, \qquad \operatorname{ord}(2) = \operatorname{ord}(4) = \operatorname{ord}(5) = 3, \qquad \operatorname{ord}(6) = 2.$$

And they are all divisors of $|\mathbb{Z}_7^*| = 6$.

For the sake of repetition, the remaining definitions and theorems in this subsection will be working with a finite field F and its finite extension $K = F(\alpha)$.

Definition 3.9. Two algebraic elements α_1, α_2 are said to be *conjugates* over F if there is a polynomial $P(x)$ that is irreducible over F such that $P(\alpha_1) = P(\alpha_2) = 0$.

Definition 3.10. The *norm* of an element $\alpha \in K$ is defined as the product of its conjugates. Besides, for any elements $\alpha_1, \alpha_2 \in K$, the *norm map* $N : K^* \to F^*$ fulfils

$$N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2).$$

The map is a surjective homomorphism of the multiplicative groups of K and F respectively. Furthermore, if the polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is irreducible over F and has roots α_i in K, then[7]

$$N(\alpha_i) = (-1)^n a_0. \tag{3.1}$$

Theorem 3.11. *Let $f : G \to H$ be a homomorphism of groups. Then the kernel of f, denoted by $\ker f = \{g \in G \mid f(g) = 1_H\}$, is a subgroup of G. When both G and H are finite, then*

$$|\ker f| = \frac{|G|}{|H|}.$$

[7] This result is actually taken from Vince's article [22].

Example 3.5. Let us once again take the finite field $\mathbb{Z}_7$ and the extension field $\mathbb{Z}_7(\sqrt{3})$. This time, we will look at the element $2+\sqrt{3}$ in $\mathbb{Z}_7(\sqrt{3})$, which is one of the roots of the polynomial $p(x) = x^2 - 4x + 1$. We take the element and calculate its norm:

$$N(2+\sqrt{3}) = (2+\sqrt{3})(2-\sqrt{3}) = 2^2 - (\sqrt{3})^2 = 1.$$

It is clear that the norm of $2+\sqrt{3}$ can be calculated as in (3.1):

$$N(2+\sqrt{3}) = (-1)^2 \cdot 1 = 1.$$

Since 1 is the identity element of the multiplicative group $\mathbb{Z}_7^*$, the element $2+\sqrt{3}$ belongs to the kernel of N, i.e. $\ker N$.

Example 3.6. The norm map N in Example 3.5 is a homomorphism between the multiplicative subgroups $\mathbb{Z}_7(\sqrt{3})^*$ and $\mathbb{Z}_7^*$. Their orders are

$$\left|\mathbb{Z}_7(\sqrt{3})^*\right| = 49 - 1 = 48 \qquad \text{and} \qquad |\mathbb{Z}_7^*| = 7 - 1 = 6.$$

From Theorem 3.11, we have that the order of the kernel is

$$|\ker N| = \frac{48}{6} = 8.$$

3.2 Number Theory

From Number Theory, the concept of the Legendre symbol and its properties are also vital for the proof of Theorem 4.9. Consequently, quadratic residues are equally important.

Definition 3.12. Let a and n be integers, where $n > 0$. If $\gcd(a,n) = 1$ and the congruence $x^2 \equiv a \pmod{n}$ has a solution, then a is a *quadratic residue of n*. If the congruence $x^2 \equiv a \pmod{n}$ has no solution, then a is said to be a *quadratic nonresidue of n*.

Example 3.7. We compute the squares of the integers $1,2,3,4,5,6$ modulo 7. We have

$$1^2 \equiv 6^2 \equiv 1 \pmod{7}, \qquad 2^2 \equiv 5^2 \equiv 4 \pmod{7}, \qquad 3^2 \equiv 4^2 \equiv 2 \pmod{7}.$$

The integers 1, 2, and 4 are quadratic residues of 7, while the integers 3, 5 and 6 are quadratic nonresidues of 7.

Already in section 2, the concept of quadratic residues was used in the classification of periods of the DCM modulo a prime. In the proof of Theorem 4.9 about the periods of prime values of N, this concept is equally inevitable, along with the following definition and its subsequent theorems.

Definition 3.13. Let a be an integer and p be an odd prime. The Legendre symbol is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p; \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p; \\ 0 & \text{if } a \text{ is divisible by } p. \end{cases}$$

Example 3.8. From the previous example, we have the following values:

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \qquad \text{and} \qquad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Theorem 3.14. *Let p be an odd prime and a and b be integers not divisible by p. Then*

(i) if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;

(iii) $\left(\frac{a^2}{p}\right) = 1$.

Example 3.9. We will calculate $\left(\frac{495}{7}\right)$ using the theorem above. We start by factorising 495 into $5 \cdot 11 \cdot 17^2$ and, by part (ii) in Theorem 3.14, we have

$$\left(\frac{495}{7}\right) = \left(\frac{5 \cdot 11 \cdot 17^2}{7}\right) = \left(\frac{5}{7}\right)\left(\frac{11}{7}\right)\left(\frac{17^2}{7}\right).$$

Since $11 \equiv 4 \pmod 7$, we can use part (i) of the theorem and get

$$\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right).$$

Using part (iii), we find that

$$\left(\frac{17^2}{7}\right) = 1.$$

Finally, putting all parts together along with the results from the previous example, we get

$$\left(\frac{495}{7}\right) = 1 \cdot (-1) \cdot 1 = -1.$$

Theorem 3.15 (Euler's Criterion)**.** *Let a be an integer and p be an odd prime that does not divide a. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p.$$

Example 3.10. If we let $a = -1$ and p be any odd prime, then Euler's Criterion gives us

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

When $p \equiv 1 \pmod 4$, i.e. $p = 4k + 1$ for some positive integer k, then

$$(-1)^{(p-1)/2} = (-1)^{2k} = 1.$$

Likewise, when $p \equiv 3 \pmod 4$, i.e. $p = 4k + 3$ for some positive integer k, then

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1.$$

Theorem 3.16 (The Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

In Example 3.10, we saw that $(p-1)/2$ is even when $p \equiv 1 \pmod 4$, and it is odd when $p \equiv 3 \pmod 4$. The same is true when $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ respectively. Hence,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ (mod 4) or } q \equiv 1 \text{ (mod 4) or both;} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

From the Law of Quadratic Reciprocity and the results above, we have that, for two distinct odd primes p and q,

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ (mod 4) or } q \equiv 1 \text{ (mod 4) or both;} \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

We have now the necessary tools to introduce the new discrete chaotic mapping, the Tribonacci cat map, and to analyse its behaviour in form of periods and orbit lenghts.

4 Results

In this section, we introduce the chaotic three dimensional map, the Tribonacci cat map. We start by presenting the map itself in subsection 4.1. In subsection 4.2, we study the matrix used in the map, which can be known as *the Tribonacci cat matrix*, and demonstrate its connection to the generating matrix of the Tribonacci sequence.

In the beginning of subsection 4.3, we prove the connection between the period of the Tribonacci sequence and the period of the Tribonacci cat map in Theorem 4.2. Because of this connection, the remaining of the subsection focus on proving the properties of the periods of the Tribonacci sequence. Theorems 4.5 and 4.8 are adaptations of results taken from Wadill's article [23] and prove the properties of periods of composite N. The proof of Theorem 4.9, which is the main result of the thesis, depends on the mathematical background from section 3 and on Propositions 4.10 and 4.11 to prove the properties of periods of prime N. The results from Theorem 4.9 are then adapted to the Tribonacci cat map in Theorem 4.12. Still in subsection 4.3, we divide the prime numbers into sets according to their periods and analyse the upper bounds for different values of N. We propose Corollaries 4.13 and 4.14 for their respective sets of prime numbers and Conjecture 4.15 for all values of N.

In subsection 4.4, we use the concept of multiplicative order from section 3, together with empirical investigations, and study the orbit lengths of the different sets of prime values of N. We also conduct an inductive analysis on the orbit lengths of composite N. The subsection ends with Theorem 4.16 about the number of fixed points when N is even, and Corollary 4.17, that proves the number of fixed points when N is odd.

Lastly, in subsection 4.5, we propose a generalised Tribonacci cat map and compares a couple of its properties with those of the original Tribonacci cat map. An example of the generalised map is used for colour encryption in section 5.

4.1 Tribonacci cat map

Let (x, y, z) be the coordinates of a point in an $N \times N \times N$ space. For every discrete time t, where $t \geq 1$, the *Tribonacci cat map* is defined by the following mapping:

$$\begin{pmatrix} x_t \\ y_t \\ z_t \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} x_{t-1} \\ y_{t-1} \\ z_{t-1} \end{pmatrix} \pmod{N}.$$

Like the original DCM in three dimensions, this mapping is chaotic. Any three dimensional image will iterate into undistinguishable 3D images until it is eventually recovered after a limited amount of iterations. The period of the Tribonacci cat map modulo N will be denoted by $\rho'(N)$.

4.2 Properties of the matrix

The chaotic properties of the Tribonacci cat mapping derive from its matrix

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 4 \end{pmatrix}.$$

As with the original cat matrix, the determinant of $\mathbf{B}$ is equal to 1, which means that it is volume preserving. The points within the N^3-image are shuffled inside its domain without any loss or gain of information.

While the entries in the 2×2 cat matrix are Fibonacci numbers, the entries in B are numbers of the generalised Fibonacci sequence, also known as the *Tribonacci sequence* $(T_n)_{n=0}^{\infty}$. This sequence is recursively defined by[8] as $T_0 = T_1 = 0$, $T_2 = 1$, and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 3$. The numbers in the sequence can be generated by the matrix[9]

$$\mathbf{T} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \text{where} \quad \mathbf{T}^n = \begin{pmatrix} T_{n-1} & T_{n-2} + T_{n-1} & T_n \\ T_n & T_{n-1} + T_n & T_{n+1} \\ T_{n+1} & T_n + T_{n+1} & T_{n+2} \end{pmatrix}.$$

From matrix multiplication $\mathbf{T}^n \mathbf{T}^k = \mathbf{T}^{n+k}$, the element T_{n+k} can be written as

$$T_{n+k} = T_n T_{k-1} + (T_{n-1} + T_n) T_k + T_{n+1} T_{k+1}. \tag{4.1}$$

Likewise, after some simplification, the determinant of $\mathbf{T}$ is

$$T_n^3 + T_{n-1}^2 T_{n+2} + T_{n+1}^2 T_{n-2} - 2T_{n-1} T_n T_{n+1} - T_{n-2} T_n T_{n+2} = 1. \tag{4.2}$$

When the generating matrix $\mathbf{T}$ is raised to the power of three, the result becomes the Tribonacci cat matrix $\mathbf{B}$. Consequently, any power of $\mathbf{B}$ will also be a power of the Tribonacci matrix.

$$\mathbf{T}^3 = \begin{pmatrix} T_2 & T_1 + T_2 & T_3 \\ T_2 & T_2 + T_3 & T_4 \\ T_4 & T_3 + T_4 & t_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 4 \end{pmatrix} = \mathbf{B} \quad \text{and}$$

$$\mathbf{B}^n = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 4 \end{pmatrix}^n = \begin{pmatrix} T_{3n-1} & T_{3n-2} + T_{3n-1} & T_{3n} \\ T_{3n} & T_{3n-1} + T_{3n} & T_{3n+1} \\ T_{3n+1} & T_{3n} + T_{3n+1} & T_{3n+2} \end{pmatrix}.$$

The minimal polynomial of $\mathbf{B}$ is $P_B(x) = x^3 - 7x^2 + 5x - 1$, where the discriminant is -44 and

[8] For this thesis, the initial values in the recurrence relation are the same as in Klaška's article [13] and in *The On-Line Encyclopedia of Integer Sequences®* (`http://oeis.org`). Meanwhile, authors like Wadill [23] use the initial values $T_0 = 0, T_1 = T_2 = 1$, and authors like Spickerman [20] prefer $T_0 = T_1 = 1, T_2 = 2$.

[9] This generating matrix is taken from Fransson's thesis on generalised Fibonacci series [9].

its roots are[10]

$$\begin{aligned}
x_1 &= \frac{1}{3}(7 + \sigma_1 + \sigma_2) \\
x_2 &= \frac{1}{6}(14 + i(\sqrt{3} + i)\sigma_1 - (1 + \sqrt{3}i)\sigma_2) \\
x_3 &= \frac{1}{6}(14 + i(\sqrt{3} + i)\sigma_2 - (1 + \sqrt{3}i)\sigma_1)
\end{aligned}$$

where

$$\sigma_1 = \sqrt[3]{199 - 3\sqrt{33}} \quad \text{and} \quad \sigma_2 = \sqrt[3]{199 + 3\sqrt{33}}.$$

The prime factors of the discriminant to the minimal polynomial will play an import role in the study of the periods of the Tribonacci cat map. Likewise, the connection to the Tribonacci sequence will be of help when calculating the periods of the mapping.

4.3 Periods

Since the Tribonacci cat map is derived from the third order recurrence relation, the Tribonacci sequence, their periods modulo N are closely related. This relation is similar to the one found between the period of the original cat map and the Pisano period. Before demonstrating their relation in Theorem 4.2, the following definition is required.

Definition 4.1. In the Tribonacci sequence, the smallest positive integer k such that $T_k \equiv T_0 \pmod{N}$, $T_{k+1} \equiv T_1 \pmod{N}$ and $T_{k+2} \equiv T_2 \pmod{N}$ is called the *Trisano period*. It is denoted by $\pi'(N)$.

In other words, a Tribonacci sequence with Trisano period $\pi'(N) = k$ looks like this:

T_0	T_1	T_2	T_3	T_4	$\cdots$	T_{k-2}	T_{k-1}	T_k	T_{k+1}	T_{k+2}	T_{k+3}	T_{k+3}
0	0	1	1	2	$\cdots$	$N-1$	1	0	0	1	1	2

Theorem 4.2. *For every integer $N \geq 2$, the period of the Tribonacci cat map modulo N is*

$$\rho'(N) = \frac{\pi'(N)}{3} \quad \textit{when} \quad 3 \mid \pi'(N),$$

otherwise it is $\rho'(N) = \pi'(N)$.

Proof. Suppose that $\pi'(N) = k$ for some integer $k \geq 2$. Then

$$\mathbf{T}^k = \begin{pmatrix} T_{k-1} & T_{k-2} + T_{k-1} & T_k \\ T_k & T_{k-1} + T_k & T_{k+1} \\ T_{k+1} & T_k + T_{k+1} & T_{k+2} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{N}.$$

Since $\mathbf{B} = \mathbf{T}^3$, it follows that $\mathbf{B}^k = \mathbf{T}^{3k}$.
If $3 \mid k$, then $\mathbf{B}^{k/3} = \mathbf{T}^k$ and $\rho'(N) = \frac{k}{3}$. If $3 \nmid k$, then $\rho'(N) = k$. □

[10] The roots presented here are given in $\mathbb{R}$. If given in a finite field, then $i = \sqrt{-1}$.

Example 4.1. The Trisano period for $N = 48$ is 416, which is not divible by 3, so the period of the Tribonacci cat map is the same. Meanwhile, $\pi'(49) = 336$ is divisible by 3 and therefore $\rho'(49) = 112$.

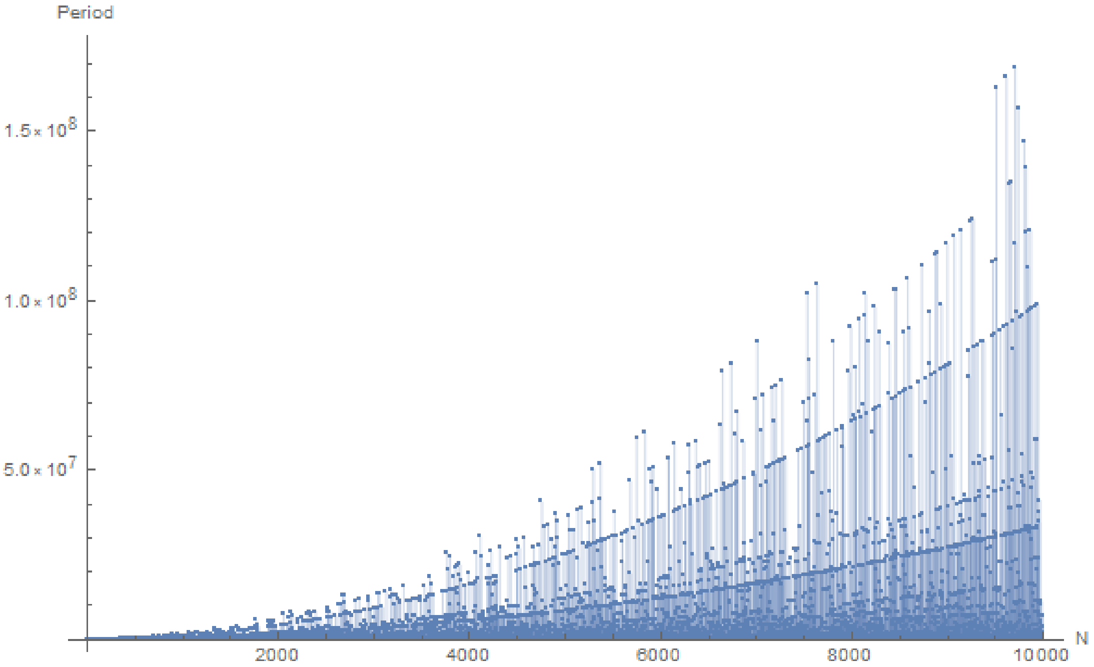


Figure 3: The graph shows the periods of the Tribonacci cat map for the first $10,000$ numbers.

The graphical illustration above has a clear pattern, where most periods seem to lie on invisible parabolas with their symmetry lines somewhere near the y-axis. We will take a closer look at them when discussing the upper bounds. But firstly, we will introduce the properties of the period of the mapping for different values of N.

4.3.1 Periods of composite N

Due to Theorem 4.2, it is sufficient to present and prove the properties regarding the Trisano period. The proofs can be efficiently adapted to the Tribonacci cat map. The results regarding the Trisano period modulo a composite number are mainly taken from Wadill's article [23]. They have been readjusted to fit the initial values and the generating matrix used in this thesis. For the proof of Theorem 4.5, where N has a prime factorisation of two or more powers of primes, we will first need the results from two lemmas.

Lemma 4.3 (Theorem 2 [23]). *If* $T_{k+1} \equiv T_k \equiv 0 \pmod{N}$, *then* $T_{k-1}^3 \equiv T_{k+2}^3 \equiv 1 \pmod{N}$.

Proof. Using the equation of the determinant in (4.2), we have that

$$T_{k-1}^3 + T_{k-2}^2 T_{k+1} + T_k^2 T_{k-3} - 2T_{k-2}T_{k-1}T_k - T_{k-3}T_{k-1}T_{k+1} = 1.$$

From the hypothesis $T_{k+1} \equiv T_k \equiv 0 \pmod{N}$, we have

$$T_{k-2}^2 T_{k+1} \equiv T_k^2 T_{k-3} \equiv 2T_{k-2}T_{k-1}T_k \equiv T_{k-3}T_{k-1}T_{k+1} \equiv 0 \qquad (\text{mod } N),$$

which leads to

$$T_{k-1}^3 \equiv 1 \qquad (\text{mod } N).$$

From the recurrence relation of the Tribonacci sequence, we have that

$$T_{k-1}^3 \equiv T_{k+2}^3 \equiv 1 \qquad (\text{mod } N). \qquad \square$$

Lemma 4.4 (Theorem 3 [23]). *If k is the least positive integer such that $T_{k+1} \equiv T_k \equiv 0$ (mod N), then, for any positive integer n*

(a) $T_{nk+1} \equiv T_{nk} \equiv 0$ (mod N);

(b) if $T_{s+1} \equiv T_s \equiv 0$ (mod N), then $s = nk$.

Proof. We will prove each case separately.

(a) Here, we will use proof by induction.

(i) For $n = 1$, the conclusion is immediate by the hypothesis $T_{k+1} \equiv T_k \equiv 0$ (mod N).

(ii) We assume that $T_{nk+1} \equiv T_{nk} \equiv 0$ (mod N) is true for a positive integer n. By (4.1) we have that $T_{(n+1)k+1}$ can be written as

$$T_{(n+1)k+1} = T_{nk+(k+1)} = T_{nk}T_k + (T_{nk-1} + T_{nk})T_{k+1} + T_{nk+1}T_{k+2}.$$

From the hypothesis $T_{k+1} \equiv T_k \equiv 0$ (mod N), we have

$$T_{nk}T_k \equiv T_{nk}T_{k+1} \equiv T_{nk-1}T_{k+1} \equiv 0 \qquad (\text{mod } N).$$

From the assumption $T_{nk+1} \equiv T_{nk} \equiv 0$ (mod N), we also have $T_{nk+1}T_{k+2} \equiv 0$ (mod N), which implies that

$$T_{nk+1} \equiv 0 \qquad (\text{mod } N).$$

A similar argument can be used to show that $T_{nk} \equiv 0$ (mod N).

(b) Let s be an integer such that $T_{s+1} \equiv T_s \equiv 0$ (mod N). Since k is the least positive integer that fulfils $T_{k+1} \equiv T_k \equiv 0$ (mod N), we have that $s \geq k$. If k does not divide s, then by the division algorithm:

$$s = kt + r, \quad 0 < r < k \quad \text{for some integer } t \geq 0.$$

From (4.1), we have

$$T_s = T_{kt+r} = T_{kt}T_{r-1} + (T_{kt-1} + T_{kt})T_r + T_{kt+1}T_{r+1}.$$

The results from (a) show that

$$T_{kt}T_{r-1} \equiv T_{kt}T_r \equiv T_{kt+1}T_{r+1} \equiv 0 \qquad (\text{mod } N).$$

From Lemma 4.3, together with the results in (a), we have that $T_{kt-1}^3 \equiv 1$ (mod N). This means that, in order to have $T_{kt-1}T_r \equiv 0$ (mod N), we must have $T_r \equiv 0$ (mod N).

But $r < k$ and k is the least positive integer such that $T_{k+1} \equiv T_k \equiv 0$ (mod N). This leads to a contradiction. Hence, $s = nk$ for any positive integer n.

This completes the proof of cases (a) and (b) and, consequently, the proof of the lemma. □

Theorem 4.5 (Theorem 4 [23])**.** *If N has the prime factorisation $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ and k_i denotes the Trisano period modulo $p_i^{\alpha_i}$, then $\pi'(N) = lcm(k_i)$.*

Proof. If $\pi'(p_i^{\alpha_i}) = k_i$ then, from the recurrence relation of the Tribonacci sequence we have

$$\begin{cases} T_{k_i+1} \equiv T_{k_i} \equiv 0 \pmod{p_i^{\alpha_i}} \\ T_{k_i+2} \equiv T_{k_1-1} \equiv 1 \pmod{p_i^{\alpha_i}}. \end{cases}$$

From Lemma 4.4, it is also true that, for any positive integer n,

$$\begin{cases} T_{nk_i+1} \equiv T_{nk_i} \equiv 0 \pmod{p_i^{\alpha_i}} \\ T_{nk_i+2} \equiv T_{nk_1-1} \equiv 1 \pmod{p_i^{\alpha_i}}. \end{cases}$$

Since $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, we can let $s = \mathrm{lcm}(k_i)$ and have

$$\begin{cases} T_{s+1} \equiv T_s \equiv 0 \pmod{N} \\ T_{s+2} \equiv T_{s-1} \equiv 1 \pmod{N}. \end{cases}$$

If $\pi'(N) = k$ it implies that

$$\begin{cases} T_{k+1} \equiv T_k \equiv 0 \pmod{p_i^{\alpha_i}} \\ T_{k+2} \equiv T_{k-1} \equiv 1 \pmod{p_i^{\alpha_i}}. \end{cases}$$

Once again, by Lemma 4.4, $k = n_i k_i$ for all k_i and an appropriate n_i. By the definition of k, it becomes clear that $k = s = \mathrm{lcm}(k_i)$ and $\pi'(N) = \mathrm{lcm}(\pi'(p_i^{\alpha_i}))$. □

The next theorem concerns the Trisano period for a prime power. Like in the previous theorem, the results are equivalent to those for the Pisano period. Even so, in order to prove them, Lemmas 4.6 and 4.7 are necessary.

Lemma 4.6 (Theorem 6 [23])**.** *If $\pi'(N) = k$, then the following identities are true for N^2 and any positive integer n:*

(a) $T_{nk+2} \equiv T_{k+2}^n$ *(mod N^2)*

(b) $T_{nk-1} \equiv T_{k-1}^n$ *(mod N^2)*

(c) $T_{nk} \equiv n T_{k-1}^{n-1} T_k$ *(mod N^2)*

(d) $T_{nk+1} \equiv T_{k+2}^n - n T_{k-1}^{n-1} T_k - T_{k-1}^n$ *(mod N^2).*

Proof. We prove the lemma by considering each case separately.
(a) We will prove this case by induction.

(i) For $n = 1$, the conclusion is immediate.

(ii) Let us assume that $T_{nk+2} \equiv T_{k+2}^n \pmod{N^2}$ is true for a positive integer n. By (4.1) we can write $T_{(n+1)k+2}$ as

$$T_{(n+1)k+2} = T_{(nk+1)+(k+1)} = T_{nk+1} T_k + (T_{nk} + T_{nk+1}) T_{k+1} + T_{nk+2} T_{k+2}.$$

Since $\pi'(N) = k$, we can use the results from Lemma 4.4 where

$$T_{k+1} \equiv T_{nk+1} \equiv T_{nk} \equiv T_k \equiv 0 \pmod{N}.$$

These lead to

$$T_{nk+1}T_k \equiv (T_{nk} + T_{nk+1})T_{k+1} \equiv 0 \pmod{N^2}$$

and to

$$T_{(n+1)k+2} \equiv T_{nk+2}T_{k+2} \pmod{N^2}.$$

From the assumption, we have that $T_{nk+2} \equiv T^n_{k+2} \pmod{N^2}$, giving us

$$T_{(n+1)k+2} \equiv T^n_{k+2}T_{k+2} \equiv T^{n+1}_{k+2} \pmod{N^2}.$$

(b) This case is also proved by induction.

(i) For $n = 1$, the conclusion is immediate.

(ii) Assume that $T_{nk-1} \equiv T^n_{k-1} \pmod{N^2}$ is true for a positive integer n. By (4.1) we have that $T_{(n+1)k-1}$ is

$$\begin{aligned} T_{(n+1)k-1} = T_{nk+(k-1)} &= T_{nk}T_{k-2} + (T_{nk-1} + T_{nk})T_{k-1} + T_{nk+1}T_k \\ &= T_{nk}(T_{k-2} + T_{k-1}) + T_{nk-1}T_{k-1} + T_{nk+1}T_k. \end{aligned}$$

Since $\pi'(N) = k$, we have that $T_{k-2} + T_{k-1} \equiv 0 \pmod{N}$ due to the recurrence relation of the Tribonacci sequence. Along with the results from Lemma 4.4, we have

$$T_{nk}(T_{k-2} + T_{k-1}) \equiv T_{nk+1}T_k \equiv 0 \pmod{N^2},$$

leaving us

$$T_{(n+1)k-1} \equiv T_{nk-1}T_{k-1} \pmod{N^2}.$$

From the assumption, we have $T_{nk-1} \equiv T^n_{k-1} \pmod{N^2}$, which leads to

$$T_{(n+1)k-1} \equiv T^n_{k-1}T_{k-1} \equiv T^{n+1}_{k-1} \pmod{N^2}.$$

(c) Induction will be used here as well.

(i) For $n = 1$, the conclusion is immediate.

(ii) Assume $T_{nk} \equiv nT^{n-1}_{k-1}T_k \pmod{N^2}$ is true for a positive integer n. We use (4.1) to write $T_{(n+1)k}$ as

$$T_{(n+1)k} = T_{nk+k} = T_{nk}T_{k-1} + (T_{nk-1} + T_{nk})T_k + T_{nk+1}T_{k+1}.$$

Once again, we take advantage of the results from Lemma 4.4 and end up with

$$T_{(n+1)k} \equiv T_{nk}T_{k-1} + T_{nk-1}T_k \pmod{N^2}.$$

From the result in (b), we can rewrite the equation above as

$$T_{(n+1)k} \equiv T_{nk}T_{k-1} + T^n_{k-1}T_k \pmod{N^2}.$$

Finally, we use the assumption that $T_{nk} \equiv nT_{k-1}^{n-1}T_k \pmod{N^2}$ in order to get the following:

$$T_{(n+1)k} \equiv nT_{k-1}^{n-1}T_kT_{k-1} + T_{k-1}^{n}T_k \equiv (n+1)T_{k-1}^{n}T_k \qquad (\text{mod } N^2).$$

(d) From the defining recurrence relation of the Tribonacci sequence, we have that

$$T_{nk+1} = T_{nk+2} - T_{nk} - T_{nk-1}.$$

By using the results from the previous cases, (a)-(c), we can rewrite the equation above into

$$T_{nk+1} = T_{k+2}^{n} - nT_{k-1}^{n-1}T_k - T_{k-1}^{n} \qquad (\text{mod } N^2).$$

This proves case (d) and completes the proof of Lemma 4.6. □

Lemma 4.7 (Theorem 7 [23]). *If p is prime and $\pi'(p) = k$, then $T_{k+2}^{p} \equiv T_{k-1}^{p} \equiv 1$ (mod p^2).*

Proof. If $T_{k+2} \equiv 1 \pmod{p^2}$, then the conclusion is immediate. Now, if $T_{k+2} \not\equiv 1 \pmod{p^2}$ then we can factorise $T_{k+2}^{p} - 1$ as the following:

$$T_{k+2}^{p} - 1 = (T_{k+2} - 1)(T_{k+2}^{p-1} + T_{k+2}^{p-2} + \cdots + T_{k+2} + 1).$$

Since $\pi'(p) = k$, it means that

$$T_{k+2} \equiv 1 \qquad (\text{mod } p). \tag{4.3}$$

Therefore, $T_{k+2}^{s} \equiv 1 \pmod{p}$ for any integer s. Hence, we have

$$T_{k+2}^{p-1} + T_{k+2}^{p-2} + \cdots + T_{k+2} + 1 \equiv \underbrace{1 + 1 + \cdots + 1 + 1}_{p \text{ summands}} \equiv 0 \qquad (\text{mod } p). \tag{4.4}$$

Using (4.3) and (4.4), we end up with

$$T_{k+2}^{p} - 1 \equiv 0 \quad \Leftrightarrow \quad T_{k+2}^{p} \equiv 1 \qquad (\text{mod } p^2).$$

The equivalence $T_{k-1}^{p} \equiv 1 \pmod{p^2}$ is proved in a similar manner. □

Theorem 4.8 (Theorem 8 [23]). *If p is prime and $\pi'(p^2) \neq \pi'(p)$, then $\pi'(p^t) = p^{t-1}\pi'(p)$, for any positive integer $t > 1$.*

Proof. We start the proof by showing that the theorem is true for $t = 2$. If we have that $\pi'(p) = k$, then $\mathbf{T}^k \equiv \mathbf{I}$ (mod p), where $\mathbf{T}$ is the generating matrix to the Tribonacci sequence and $\mathbf{I}$ is the identity matrix. By Lemma 4.6 we have the following identities for $n = p$:

(a) $T_{pk+2} \equiv T_{k+2}^{p} \pmod{p^2}$

(b) $T_{pk-1} \equiv T_{k-1}^{p} \pmod{p^2}$

(c) $T_{pk} \equiv pT_{k-1}^{p-1}T_k \pmod{p^2}$

(d) $T_{pk+1} \equiv T_{k+2}^{p} - pT_{k-1}^{p-1}T_k - T_{k-1}^{p} \pmod{p^2}$.

From Lemma 4.7, together with identities (a) and (b), we have $T_{pk+2} \equiv T_{pk-1} \equiv 1 \pmod{p^2}$. Since $\pi'(p) = k$, we have $T_k \equiv 0 \pmod{p}$, which implies that

$$\begin{aligned} T_{pk} &\equiv pT_{k-1}^{p-1}T_k \equiv 0 \pmod{p^2} \quad \text{and by identity (d)} \\ T_{pk+1} &\equiv -pT_{k-1}^{p-1}T_k \equiv 0 \pmod{p^2}. \end{aligned}$$

Thus we end up with

$$\begin{cases} T_{pk+1} \equiv T_{pk} \equiv 0 \pmod{p^2} \\ T_{pk+2} \equiv T_{pk-1} \equiv 1 \pmod{p^2} \end{cases}$$

and we have that $\pi'(p^2) \mid pk$. Now, if $\pi'(p^2) = pk$, there is no s, $s < pk$, that satisfies

$$\begin{cases} T_{s+1} \equiv T_s \equiv 0 \pmod{p^2} \\ T_{s+2} \equiv T_{s-1} \equiv 1 \pmod{p^2}. \end{cases}$$

Let us claim that such s exists. By Lemma 4.4, $s = mk$ for some positive integer m as it is implied that

$$\begin{cases} T_{s+1} \equiv T_s \equiv 0 \pmod{p} \\ T_{s+2} \equiv T_{s-1} \equiv 1 \pmod{p}. \end{cases}$$

Then we have $\mathbf{T}^s \equiv \mathbf{T}^{mk} \equiv (\mathbf{T}^k)^m \equiv \mathbf{I}^m \equiv \mathbf{I} \pmod{p}$. Since $\pi'(p^2) \neq \pi'(p)$, it follows that $\mathbf{T}^k \not\equiv \mathbf{I} \pmod{p^2}$. At the same time we have $(\mathbf{T}^k)^p \equiv (\mathbf{T}^k)^m \equiv \mathbf{I} \pmod{p^2}$. As p is prime, it means that $m \geq p$ and $s \geq pk$, which is a contradiction to our claim.

Hence $\pi'(p^2) = p\pi'(p)$. To show that the theorem is true for $t > 2$, we use induction and follow the same steps as above. The rest is omitted due to redundancy. □

Remark. Similarly to the Pisano period for powers of prime numbers, there is no proof that the hypothesis $\pi'(p^2) \neq \pi'(p)$ is unnecessary. Meanwhile, no prime p that fulfils $\pi'(p^2) = \pi'(p)$ has been found.

4.3.2 Periods of prime N

When N is a prime number p, the Trisano period is strongly related to the minimal polynomial of the recurrence relation and its discriminant. Like with the minimal polynomial of the Tribonacci cat map, the discriminant is -44.

Theorem 4.9. *Assume p is prime and $p \neq 2, 11$. The minimal polynomial of the Tribonacci sequence is*

$$P_T(x) = x^3 - x^2 - x - 1.$$

(a) If $\left(\frac{p}{11}\right) = 1$ and $P_T(x)$ is irreducible over $\mathbb{Z}_p$ then $\pi'(p) \mid p^2 + p + 1$.

(b) If $\left(\frac{p}{11}\right) = 1$ and $P_T(x)$ is reducible over $\mathbb{Z}_p$ then $\pi'(p) \mid p - 1$.

(c) If $\left(\frac{p}{11}\right) = -1$ then $\pi'(p) \mid p^2 - 1$.

In order to prove Theorem 4.9, some specific results are needed. Theorem 4.10 is taken from Carlitz' article [5] and it is originally contained in a theorem of Stickelberger[11] about the relation between the discriminant of a polynomial with rational integer coefficients and the number of irreducible polynomials modulo a prime. For more details regarding Theorem 4.10, the reader is recommended to see [5]. Theorem 4.11 is about a property of the period of a third order linear recurrence. The theorem is taken from Klaška and Skula's article [13] and its proof can be found both in Adams & Shanks' work [1] and in Vince's paper [22].

Proposition 4.10 (Theorem A [5]). *Let D denote the discriminant of the polynomial*

$$P(x) = x^n + a_1x^{n-1} + \cdots + a_n$$

where a_i are rational integers. Let p be an odd prime, $p \nmid D$, and let

$$P(x) = P_1(x)\cdots P_s(x) \qquad (\text{mod } p),$$

where $P_i(x)$ are irreducible polynomials over $\mathbb{Z}_p$. Then the Legendre symbol is

$$\left(\frac{D}{p}\right) = (-1)^{n-s}.$$

Proposition 4.11 (Theorem 1.1(i) [13]). *Let $P(x) = x^3 + a_1x^2 + a_2x + a_3$ be the minimal polynomial of the generating matrix to the third order linear recurrence $X_n = A_1X_{n-1} + A_2X_{n-2} + A_3X_{n-3}$ over the finite field $\mathbb{Z}_p$ where p is prime. Let also $\mathcal{K}$ be the extension field of $\mathbb{Z}_p$ containing the distinct roots $\alpha_1, \alpha_2, \alpha_3$ to $P(x)$. If $\Pi(p)$ is the period of the recurrence relation modulo p and ord(β) is the multiplicative order of the nonzero element $\beta \in \mathcal{K}$ in the multiplicative subgroup $\mathcal{K}^*$ of $\mathcal{K}$, then*

$$\Pi(p) = \textit{lcm}(\textit{ord}(\alpha_1), \textit{ord}(\alpha_2), \textit{ord}(\alpha_3)).$$

With both the results above, we can proceed with proving Theorem 4.9. The proof is inspired by Vince's article on periods of linear recurrences [22].

Proof of Theorem 4.9. According to Theorem 4.10, we have $\left(\frac{D}{p}\right) = (-1)^{3-s}$, where s is the number of factors modulo p, a prime. When applying the properties of the Legendre symbol, we get the following:

$$\left(\frac{D}{p}\right) = \left(\frac{-2^2 \cdot 11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2^2}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{11}{p}\right)$$

(i) Let $p \equiv 1 \pmod 4$, then for some positive integer n

$$\left(\frac{D}{p}\right) = (-1)^{\frac{(4n+1)-1}{2}}\left(\frac{11}{p}\right) = (-1)^{2n}\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right).$$

[11] The original theorem can be found in Stickelberger's article *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, published in "Verhandlungen des ersten internationalen Mathematiker-Kongresses" in Zürich, 1897. However, the article could not be found when this thesis was in progress and it is therefore not a part of the reference list.

(ii) Let $p \equiv 3 \pmod 4$, then for some positive integer n

$$\left(\frac{D}{p}\right) = (-1)^{\frac{(4n+3)-1}{2}}\left(\frac{11}{p}\right) = (-1)^{2n+1}\left[-\left(\frac{p}{11}\right)\right] = \left(\frac{p}{11}\right).$$

So, when calculating the number of factors over $\mathbb{Z}_p$, it suffices to calculate $\left(\frac{p}{11}\right)$ in this case. We complete the proof by considering the three different cases below.

(a) If $\left(\frac{p}{11}\right) = 1$ and $P_T(x)$ is irreducible over $\mathbb{Z}_p$, then let $\mathcal{K} = \mathbb{Z}_p(\alpha_1, \alpha_2, \alpha_3)$ be the extension field of $\mathbb{Z}_p$ containing the roots of $P_T(x)$. The norm map $N : \mathcal{K}^* \to \mathbb{Z}_p^*$ is therefore a surjective homomorphism of the multiplicative subgroup of $\mathcal{K}$ to the multiplicative subgroup of $\mathbb{Z}_p$. Note that both subgroups are cyclic. Since $N(\alpha_i) = (-1)^3(-1) = 1$, where 3 is the degree of $P_T(x)$ and -1 is its constant term, then α_i is an element of the kernel, which is also cyclic. Then, $\operatorname{ord}(\alpha_i) \mid |\ker N|$. The order of the kernel is

$$|\ker N| = \frac{|\mathcal{K}^*|}{|\mathbb{Z}_p^*|} = \frac{p^3-1}{p-1} = p^2+p+1.$$

So we have that

$$\operatorname{ord}(\alpha_i) \mid p^2+p+1 \qquad \text{and also} \qquad \operatorname{lcm}(\operatorname{ord}(\alpha_i)) \mid p^2+p+1.$$

Hence, by Theorem 4.11, we have $\pi'(p) \mid p^2+p+1$.

(b) If $\left(\frac{p}{11}\right) = 1$ and $P_T(x)$ has three factors, then they are all linear and the roots lie in $\mathbb{Z}_p$. Once again, let $\mathbb{Z}_p^*$ be the multiplicative subgroup of $\mathbb{Z}_p$. Since $\mathbb{Z}_p^*$ is cyclic and $\alpha_i \in \mathbb{Z}_p^*$, we have that $\operatorname{ord}(\alpha_i) \mid |\mathbb{Z}_p^*|$. Furthermore

$$\operatorname{lcm}(\operatorname{ord}(\alpha_i)) \mid |\mathbb{Z}_p^*| = p-1.$$

Thus, by Theorem 4.11, we have $\pi'(p) \mid p-1$.

(c) If $\left(\frac{p}{11}\right) = -1$, then $P_T(x)$ has two factors, namely a linear factor and a quadratic factor in $\mathbb{Z}_p$. Let $\mathcal{K} = \mathbb{Z}_p(\alpha_2, \alpha_3)$ be the extension field containing the roots of the quadratic factor. Since the root α_1 of the linear factor lies already in $\mathbb{Z}_p$, it will automatically be an element in $\mathcal{K}$. Following the same reasoning for (b), we have

$$\operatorname{lcm}(\operatorname{ord}(\alpha_i)) \mid |\mathcal{K}^*| = p^2-1.$$

Finally, by Theorem 4.11, we have $\pi'(p) \mid p^2-1$.
This completes the proof of cases (a)-(c) and hence the proof of the theorem. □

The strong relation between the Trisano period and the period of the Tribonacci cat map given by Theorem 4.2, allows us to summarise and adapt all the previous results into one theorem.

Theorem 4.12. *For every integer $N \geq 2$, the period of the Tribonacci cat map modulo N belongs to one of the following statements:*

(i) If N is a prime p such that $p \neq 2, 11$ and $\left(\frac{p}{11}\right) = 1$, then $\rho'(p) \mid p^2+p+1$ or $\rho'(p) \mid p-1$.

(ii) If N is a prime p such that $p \neq 2, 11$ and $\left(\frac{p}{11}\right) = -1$, then $\rho'(p) \mid p^2 - 1$.

(iii) If N is a prime power such that $N = p^k$, and if $\rho'(p^2) \neq \rho'(p)$, then $\rho'(p^k) = p^{k-1}\rho'(p)$.

(iv) If N is composite and has the prime factorisation $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, then $\rho'(N) = lcm(\rho'(p_i^{\alpha_i}))$.

Remark. Since the polynomial $P_T(x)$ shares the same discriminant as the minimal polynomial to the Tribonacci cat map, $P_B(x) = x^3 - 7x^2 + 5x - 1$, properties *(i)* and *(ii)* can be proven in a similar manner as for the Trisano period. Regarding the hypothesis in property *(iii)*, for the first 10,000 numbers, the only prime p with $\rho'(p^2) = \rho'(p)$ is 3, where $\rho'(9) = \rho'(3) = 13$.

Example 4.2. Below are a couple of examples comparing the Trisano period with its respective Tribonacci cat map period modulo a prime.

(i) For $p = 67$, where $\left(\frac{67}{11}\right) = 1$ and $P_T(x)$ is irreducible over $\mathbb{Z}_{67}$. The periods are $\pi'(67) = 1519 = \rho'(67)$.

(ii) For $p = 103$, where $\left(\frac{103}{11}\right) = 1$ and $P_T(x)$ has linear factors in $\mathbb{Z}_{103}$. The periods are $\pi'(103) = 51$ and $\rho'(103) = 17$.

(iii) For $p = 17$, where $\left(\frac{17}{11}\right) = -1$ and $P_T(x)$ has two factors in $\mathbb{Z}_{17}$. The periods are $\pi'(17) = 96$ and $\rho'(17) = 32$.

(iv) For $p = 2$, the periods are $\pi'(2) = 4 = \rho'(2)$.

(v) For $p = 11$, the periods are $\pi'(11) = 110 = \rho'(11)$.

4.3.3 Upper bounds

On the next page, there is a graph illustrating the periods of the Tribonacci cat map for all primes less than 10,000. It is clear that the absolute upper bound for the prime numbers is $\rho'(p) = p^2 + p + 1$. Interestingly, despite that one might first think that there should be periods equal to $\rho'(p) = p^2 - 1$ for primes in group (ii) from Theorem 4.12, the greatest periods in this group are $\rho'(p) = \frac{p^2-1}{3}$. This leads to Corollary 4.13.

Corollary 4.13. *If $N = p$ is a prime p, $p \neq 2, 11$ and $\left(\frac{p}{11}\right) = -1$, then*

$$\rho'(p) \leq \frac{p^2 - 1}{3}.$$

Proof. Due to the strong relation to the Trisano period, it is enough to calculate $\pi'(p)$. By Theorem 4.2, it is true for any value of N that

$$\rho'(N) = \begin{cases} \frac{\pi'(N)}{3} & \text{when} \quad 3 \mid \pi'(N), \\ \pi'(N) & \text{otherwise.} \end{cases}$$

(i) Let $p \equiv 2 \pmod 3$, then for any positive integer n

$$p^2 - 1 = (3n+2)^2 - 1 = 9n^2 + 12n + 3 \quad \text{and} \quad 3 \mid 9n^2 + 12n + 3.$$

(ii) Let $p \equiv 1 \pmod 3$, then for any positive integer n

$$p^2 - 1 = (3n+1)^2 - 1 = 9n^2 + 12n \quad \text{and} \quad 3 \mid 9n^2 + 12n.$$

And the proof is complete. □

We will continue to further develop the results from Theorem 4.12 and introduce the next corollary. This time, it concerns the periods of prime numbers, whose periods lie on the upper curve, neatly visible in Figure 4.

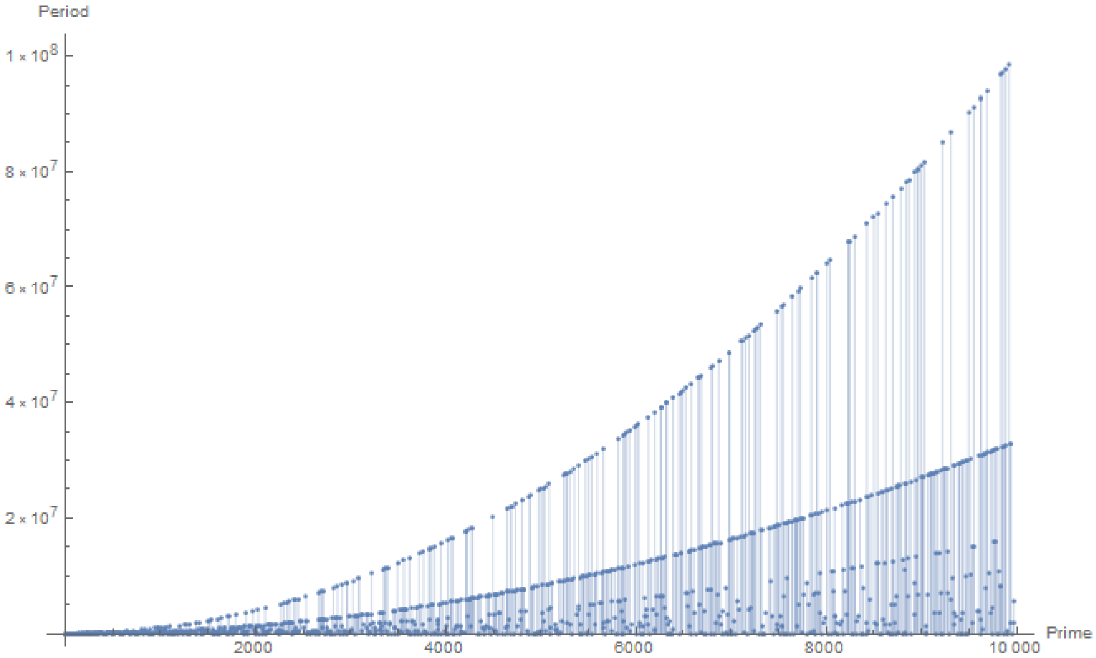


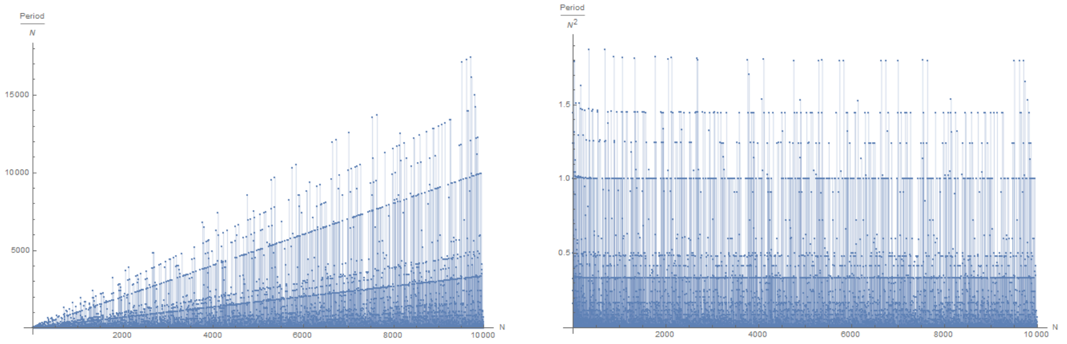
Figure 4: The graph shows the periods of the Tribonacci cat map for all primes p, such that $2 \le p < 10,000$.

Corollary 4.14. *If $\rho'(p) = p^2 + p + 1$ for a prime $p > 3$, then $p \equiv 2 \pmod 3$.*

Proof. Similar calculations to the proof to Corollary 4.13 show that $p \not\equiv 1 \pmod 3$ when $\rho'(p) = p^2 + p + 1$. □

Remark. Observe that the converse of Corollary 4.14 is not true. There are primes $p \equiv 2$ (mod 3) with $\rho'(p) \neq p^2 + p + 1$. Take, for example, $p = 311$ that has period $\rho'(311) = 310$.

When it comes to finding an upper bound for all values of N, it can be interesting to look at the ratios $\rho'(N)/N$ and $\rho'(N)/N^2$ that are presented in their respective diagrams on the next page. In Figure 5 (a), the patterns of the top periods created by the ratios give the false illusion of them lying on perfect straight lines. It is confirmed in Figure 5 (b) that there is not a single slope that fits all top periods. However, for the first 10,000 numbers, there is no ratio in (b) that surpasses or is equal to 2. Furthermore, numerical calculations have showed a negative trend of the ratio for higher numbers.



(a) Plotted graf over $\frac{\rho'(N)}{N}$.

(b) Plotted graf over $\frac{\rho'(N)}{N^2}$.

Figure 5: The ratios of the Tribonacci cat map periods for $2 \le N \le 10,000$.

In Dyson & Falk [8], they calculate the upper bound of the original cat map by analysing the factors of the period for any arbitrary N. In order to factorise the period, we must first consider the factors of N. According to the Fundamental Theorem of Arithmetic, any number N can be written as a product of powers of primes, like

$$N = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5} \cdot 7^{\alpha_7} \cdot 11^{\alpha_{11}} \cdot \dots \ .$$

By Theorem 4.12 (iv), the period of such N is the least common multiple of the periods of the prime powers in the factorisation of N. Before proceding with $\rho'(N)$, we will divide the prime numbers in sets according to their periods:

- $p = 2$, with $\rho'(2) = 4$.
- $p = 11$, with $\rho'(11) = 110$.
- $Q = \left\{q \,\middle|\, \rho'(q) \le q^2 + q + 1\right\}$.
- $R = \{r \mid \rho'(r) \le r - 1\}$.
- $S = \left\{s \,\middle|\, \rho'(s) \le \frac{s^2-1}{3}\right\}$.

Now, N can be rewritten as

$$N = 2^{\alpha_2} \cdot 11^{\alpha_{11}} \left(\prod_{q\in Q} q^{\alpha_q}\right)\left(\prod_{r\in R} r^{\alpha_r}\right)\left(\prod_{s\in S} s^{\alpha_s}\right).$$

Applying all the results from Theorem 4.12, the period of the Tribonacci cat map modulo N becomes

$$\rho'(N) \le \operatorname{lcm}\left(2^{\alpha_2+1}, 11^{\alpha_{11}}(10), \prod_{q\in Q}(q^2+q+1)q^{\alpha_q-1}, \prod_{r\in R}(r-1)r^{\alpha_r-1}, \prod_{s\in S}3^{-\alpha_s}(s^2-1)s^{\alpha_s-1}\right). \tag{4.5}$$

It is apparent in (4.5) that the periods of primes $q \in Q$ are the greatest factors in $\rho'(N)$. In fact, the numerical calculations performed for $2 \le N \le 10,000$ have showed that the greatest periods in the interval (see Figure 3 on page 20) belong to products of primes $q \in Q$, where $q \equiv 2 \pmod 3$, and their multiples. The two top values for $\rho'(N)/N^2$ in Figure 5 (b), for example, belong to 345 and 690, whose prime factorisations are $3 \cdot 5 \cdot 23$ and $2 \cdot 3 \cdot 5 \cdot 23$ respectively.

Nonetheless, it is not true that all products of primes $q_i \in Q$, where $q \equiv 2 \pmod 3$, generate the greatest periods. Take for instance the number 2865 which is a product of 3, 5 and 191, all of them elements in Q. The period of 191 is actually a product of the periods of 3 and 5, resulting in $\rho'(2865) = \rho'(191)$. This means that the periods themselves must be relatively prime.

It is not true either that all multiples of these products produce the greatest periods. Firstly, the multiple cannot yield prime powers in the factorisation of N, i.e. $1725 = 345 \cdot 5 = 3 \cdot 5^2 \cdot 23$. Recall that the period of a prime power q^{α_q} is at most $q^{\alpha_q - 1}$ greater than the period of q. Secondly, after the periods of primes $q_i \in Q$, the greatest factors in (4.5) are the periods of 2 and 11, although not simultaneously as they are not relatively prime. The periods of $r \in R$ and $s \in S$ are comparably low.

The observations above, together with numerical calculations, allow us to come up with a few conditions for the value N. In order for the periods modulo N to lie on the upper bound, all the requirements below must be fulfilled. As noted above,

1. $N = q_1 q_2 \cdots q_n$, or $N = 2 q_1 q_2 \cdots q_n$, or $N = 11 q_1 q_2 \cdots q_n$, for some $q_i \in Q$ and $n \geq 2$;
2. $q_i \equiv 2 \pmod 3$;
3. all $\rho'(q_i)$ are pairwise relatively prime.

Taking into consideration the tendency of the ratios in Figure 5 (b), there is the possibility of the existence of an asymptote as $N \to \infty$. The highest ratios on the graph, for $N = 345$ and $N = 690$, are close to 1.87. As N increases, the top ratios approach 1.79. From this information, we conjecture that no period of the Tribonacci cat map will be equal to or greater than $1.88N^2$.

Conjecture 4.15. *For any value of N,*

$$\rho'(N) < \frac{47}{25} N^2.$$

4.4 Orbit lengths

Similarly to the DCM, for any value of N, the orbit lengths of the points in the N^3-space are divisors of $\rho'(N)$. However, for some values of N, the origin is not the only fixed point. Another remarkable difference between the original discrete mapping and the three dimensional one is that, in the latter, the orbit lengths of the non-trivial points are not always equal to $\rho'(N)$ when N is prime. The results presented in this subsection are based on empirical investigations.

4.4.1 Orbit lengths of prime N

As with periods for prime values of N, the orbit lengths depend on the factorisation of the minimal polynomial $P_B(x) = x^3 - 7x^2 + 5x - 1$ in $\mathbb{Z}_p$. The study of the orbits for prime N can therefore be conducted according to their respective sets:

- $p = 2$ and $p = 11$.

Because both 2 and 11 are present in the discriminant, some of the roots have multiplicity greater than 1. In fact, the polynomial $P_B(x)$ has a triple root in $\mathbb{Z}_2$ while it has a double and a single root in $\mathbb{Z}_{11}$. The orbit lengths consist of the multiplicative orders of the roots and their multiples.

p	Orbit length	Number of disjoint orbits	Roots α_i in $\mathbb{Z}_p$	$\text{ord}_p(\alpha_i)$
2	1	2	$\alpha_{1,2,3} = 1$	$\text{ord}_2(1) = 1$
	2	1		
	4	1		
11	1	1		
	5	2	$\alpha_1 = 3$	$\text{ord}_{11}(3) = 5$
	10	11	$\alpha_{2,3} = 2$	$\text{ord}_{11}(2) = 10$
	110	11		

Table 1: Since the triple root in $\mathbb{Z}_2$ has multiplicative order 1, there is a non-trivial point in the mapping for $N = 2$ with orbit length 1.

- $Q = \{q \mid \rho'(q) \leq q^2 + q + 1\}$.

For primes $q \in Q$, the polynomial $P_B(x)$ is irreducible over $\mathbb{Z}_q$. When this happens, the Tribonacci cat map behaves similarly to the DCM and the orbit length of all non-trivial points is the same as the period of the map. The table below presents the orbits for three prime numbers q.

q	Orbit length	Number of disjoint orbits	Roots α_i in $\mathbb{Z}_q$	$\text{ord}_q(\alpha_i)$
3	1	1	None	-
	13	2		
5	1	1	None	-
	31	4		
67	1	1	None	-
	1519	198		

Table 2: Because the period for $N = q$ is either $\rho'(q) = q^2 + q + 1$ or one of its divisors, it will always be an odd number. There is no restriction as whether the period is a prime number itself or not. While $N = 3$ and $N = 5$ have prime numbers as their periods, $N = 67$ has a composite number, $1519 = 7^2 \cdot 31$.

- $R = \{r \mid \rho'(r) \leq r - 1\}$.

For primes $r \in R$, the polynomial $P_B(x)$ is reducible over $\mathbb{Z}_r$ and has three linear factors. The implication is that the orbit lengths for all non-trivial points are equal to any of the multiplicative orders of the roots of $P_B(x)$ in $\mathbb{Z}_r$. Below follow the orbit lengths of three prime numbers r.

r	Orbit length	Number of disjoint orbits	Roots α_i in $\mathbb{Z}_r$	$\mathrm{ord}_r(\alpha_i)$
	1	1	$\alpha_1 = 31$	$\mathrm{ord}_{47}(31) = 46$
47	23	2	$\alpha_2 = 25$	$\mathrm{ord}_{47}(25) = 23$
	46	2256	$\alpha_3 = 45$	$\mathrm{ord}_{47}(45) = 46$
	1	1	$\alpha_1 = 39$	$\mathrm{ord}_{53}(39) = 52$
53	13	4	$\alpha_2 = 24$	$\mathrm{ord}_{53}(24) = 13$
	52	2862	$\alpha_3 = 50$	$\mathrm{ord}_{53}(50) = 52$
	1	1	$\alpha_1 = 8$	$\mathrm{ord}_{103}(8) = 17$
103	17	64278	$\alpha_2 = 9$	$\mathrm{ord}_{103}(9) = 17$
			$\alpha_3 = 93$	$\mathrm{ord}_{103}(93) = 17$

Table 3: Note that, when all roots have the same multiplicative order, as for $r = 103$, the map exhibits a similar behaviour to when $N = q$.

- $S = \left\{s \;\middle|\; \rho'(s) \leq \frac{s^2-1}{3}\right\}$.

For primes $s \in S$, the polynomial $P_B(x)$ has only one linear factor in $\mathbb{Z}_s$. The result is that the orbit lengths for all non-trivial points are either equal to the multiplicative order of the root, or to a multiple of the root, which is the period of the map. From the calculations realised in this thesis, there is not enough material to predict the period of the mapping once the multiplicative order of the root is known, or vice versa.

s	Orbit length	Number of disjoint orbits	Roots α_i in $\mathbb{Z}_s$	$\mathrm{ord}_s(\alpha_i)$
7	1	1		
	2	3	$\alpha = 6$	$\mathrm{ord}_7(6) = 2$
	16	21		
13	1	1		
	4	3	$\alpha = 5$	$\mathrm{ord}_{13}(5) = 4$
	56	39		
83	1	1		
	41	2	$\alpha = 48$	$\mathrm{ord}_{83}(48) = 41$
	287	1992		

Table 4: For the primes $s = 7$ and $s = 13$, the period of the mapping is equal to the multiplicative order of the root multiplied by $s + 1$, where $16 = 2 \cdot 8$ and $56 = 4 \cdot 14$. This is not true for all primes s, as in the case for $s = 83$, where $287 = 41 \cdot 7$.

4.4.2 Orbit lengths of composite N

When N is composite, the patterns behind the orbit lengths are no longer related to the set in which the prime factors belong. Instead, the behaviour depends on whether N is a prime power or a product of primes. Regardless of which, once the orbit lengths of the prime factors are known, all orbit lengths of N can be predicted.

For instance, the orbit lengths of $N = p^2$ include all orbit lengths of $N = p$ and their respective products with p. This pattern repeats itself for any power $N = p^n$. When the products are already existing lengths in $N = p^n$, then no new orbit lengths related to these are added in $N = p^{n+1}$. To illustrate this, take, for example, $N = 2$ with orbit lengths 1, 2 and 4 (see Table 5). As 2 is already $1 \cdot 2$ and 4 is $2 \cdot 2$, the only new orbit length for $N = 2^2$ is $4 \cdot 2 = 8$. This follows for all powers of 2.

N	Orbit lengths					
2	1	2	4			
2^2	1	2	4	8		
2^3	1	2	4	8	16	
2^4	1	2	4	8	16	32
...	...					

Table 5: Every new power of 2, i.e. 2^{n+1}, has all the orbit lengths of the previous power, i.e. 2^n, together with the product between the greatest orbit length of 2^n and 2.

In the case when $N = 11$ (see Table 6), it is easier to see that the multiples of the orbit lengths in $N = 11$ appear in $N = 11^2$, along with the original orbit lengths. Even in this case, however, the orbit length 110 is already the product of the orbit length 10 and the prime 11. So only the orbit lengths 5 and 110 gain their products with 11 in $N = 11^2$. The procedure is repeated for all powers of 11.

Period	Orbit lengths								
11	5	10		110					
11^2	5	10	55	110		1210			
11^3	5	10	55	110	605	1210		13310	
11^4	5	10	55	110	605	1210	6655	13310	146410
...	...								

Table 6: It is visible that the orbit lengths of 11^{n+1} include all the lengths of 11^n and their respective products with 11.

Examples of primes from the other sets are shown in Table 7. They all follow the same pattern of orbit lengths as presented earlier. The only exception found in the interval $0 < N \leq 10,000$ is $N = 3^2$, which has the same orbit length as $N = 3$. Thereafter, the powers of 3 follow the same patterns as any other prime power.

N	Orbit lengths							
7	2		16					
7^2	2	14	16		112			
7^3	2	14	16	98	112		784	
7^4	2	14	16	98	112	686	784	5488
...	...							
53	13	52						
53^2	13	52	689	2756				
53^3	13	52	689	2756	36517	146068		
...	...							
3	13							
3^2	13							
3^3	13	39						
3^4	13	39	117					
...	...							
5	31							
5^2	31	155						
5^3	31	155	775					
5^4	31	155	775	3875				
...	...							

Table 7: In all cases, it is visible that $N = p^{n+1}$ contains the same orbit lengths as $N = p^n$ plus their respective products with p.

When N is a product of primes, it will inherit all orbit lengths of the non-trivial points from its factors. Furthermore, it will also have all possible least common multiples of the orbit lengths of the different factors. This is similar to the period of N being the least common multiple of the periods of all its factors. Tables 8 and 9 present the orbit lengths of composite numbers where at least one factor is a prime power, while tables 10 and 11 have square-free values of N. Each factor and its orbit lengths are shaded with a specific colour to better illustrate which orbit lengths of N are derived from which factor. When the same orbit length is shared by two factors, it is shaded with both colours when presented for N.

N	Orbit lengths						
5^2		31		155			
19	6		120				
475	6	31	120	155	186	930	3720

Table 8: The shaded orbit lengths in $N = 475$ have the same colour as the factor from which they derive. The non-shaded orbit lengths are the least common multiples of the lengths between the factors. These are $186 = \mathrm{lcm}(6, 31)$, $930 = \mathrm{lcm}(6, 155)$ and $3720 = \mathrm{lcm}(31, 120) = \mathrm{lcm}(120, 155)$.

N	Orbit lengths											
2^3	1	2	4	8		16						
3					13							
17						16		32				
408	1	2	4	8	13	16	26	32	52	104	208	416

Table 9: Note that the orbit length 16 appears in both $N = 2^3$ and $N = 17$. The new orbit lengths of $N = 408$ are $26 = \mathrm{lcm}(2, 13)$; $52 = \mathrm{lcm}(4, 13)$; $104 = \mathrm{lcm}(8, 13)$; $208 = \mathrm{lcm}(13, 16)$; and $416 = \mathrm{lcm}(13, 16, 32)$.

When two or more factors of N share orbit lengths, the number of new lengths in N is less than when all orbit lengths are unique. Similarly, when two or more factors have orbit lengths with *greatest common divisor* (gcd) greater than 1, there are fewer new lengths in N than when the factor's orbit lengths are relatively prime. Take for instance the examples in Tables 10 and 11. The total number of orbit lengths among their factors is the same. However, since no length appears in two or more factors of $N = 66$ and only a few have gcd greater than 1, $N = 66$ ends up having many more orbits than $N = 182$. The latter has two orbit lengths that appear in more than one factor, and almost all lengths have gcd greater than 1.

N	Orbit lengths					
2	1	2	4			
7		2		16		
13			4		56	
182	1	2	4	16	56	112

Table 10: The orbit length 2 appears in both $N = 2$ and $N = 7$, and the orbit length 4 appears in both $N = 2$ and $N = 13$. Besides, apart from the orbit length 1, all the others have greatest common divisor greater than 1. Consequently, there is only one new orbit length in the product $N = 182$, which is the least common multiple of all three periods.

N	Orbits lengths															
2	1	2	4													
3						13										
11				5	10						110					
66	1	2	4	5	10	13	20	26	52	65	110	130	220	260	1430	2860

Table 11: Apart from the even orbit lengths in $N = 2$ and $N = 11$, where their greatest common divisor is 2, all the other lengths have 1 as their greatest common divisor.This results in $N = 66$ having relatively more new orbit lengths than the previous examples.

The three examples where N is even have the orbit length 1 for non-trivial points. This is actually true for all even values of N. In fact, there is only one non-trivial point that is fixed when N is even, and that point is $\left(\frac{N}{2}, \frac{N}{2}, \frac{N}{2}\right)$. This is summarized in the following theorem.

Theorem 4.16. *When N is even, the Tribonacci cat map has exactly two fixed points: the trivial point $(0,0,0)$ and the non-trivial point $\left(\frac{N}{2}, \frac{N}{2}, \frac{N}{2}\right)$.*

Proof. Let $\mathbf{B}$ be the Tribonacci cat matrix and let N be even. The point $X = (x_1, x_2, x_3)$ is fixed when

$$\mathbf{B}X \equiv X \pmod{N}. \tag{4.6}$$

Rearranging (4.6), we get

$$(\mathbf{B} - \mathbf{I})X \equiv 0 \pmod{N}, \tag{4.7}$$

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 2 & 3 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \pmod{N}. \tag{4.8}$$

where $\mathbf{I}$ is the identity matrix. We can rewrite (4.8) as a system of equations modulo N:

$$\begin{cases} \phantom{2x_1 + {}} x_2 + x_3 \equiv 0 & \pmod{N} \\ x_1 + x_2 + 2x_3 \equiv 0 & \pmod{N} \\ 2x_1 + 3x_2 + 3x_3 \equiv 0 & \pmod{N} \end{cases} \tag{4.9}$$

The second equation in (4.9) can be rewritten as

$$x_1 \equiv -x_2 - 2x_3 \pmod{N}$$

and inserted in the third equation of the system in (4.9). We get:

$$x_2 - x_3 \equiv 0 \pmod{N}. \tag{4.10}$$

If we take (4.10) and the first equation in (4.9), we end up with a new and more simplified system of equations modulo N:

$$\begin{cases} x_2 + x_3 \equiv 0 \pmod{N} \\ x_2 - x_3 \equiv 0 \pmod{N}. \end{cases} \tag{4.11}$$

We repeat the same procedure of rewriting the second equation in (4.11) so that x_2 is the only term on the left hand side, and inserting the right hand side into the first equation in (4.11). Finally, we end up with the modular homogeneous equation

$$2x_3 \equiv 0 \pmod{N}. \tag{4.12}$$

Since $\gcd(2, N) = 2$, the equation in (4.12) has exactly two distinct solutions. This implies that the system of equations in (4.9) has two solutions and, consequently, there are two points X_1 and X_2 that fulfil the equation in (4.6).

One of the points is the trivial point $X_1 = (0,0,0)$. The other one is $X_2 = \left(\frac{N}{2}, \frac{N}{2}, \frac{N}{2}\right)$, as

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 2 & 3 & 3 \end{pmatrix} \begin{pmatrix} \frac{N}{2} \\ \frac{N}{2} \\ \frac{N}{2} \end{pmatrix} \equiv \begin{pmatrix} \frac{3N}{2} \\ \frac{5N}{2} \\ \frac{9N}{2} \end{pmatrix} \equiv \begin{pmatrix} \frac{N}{2} \\ \frac{N}{2} \\ \frac{N}{2} \end{pmatrix} \pmod{N}.$$

And the proof is complete. □

The results from Theorem 4.16 lead naturally to Corollary 4.17.

Corollary 4.17. *When N is odd, the Tribonnaci cat map has only one fixed point, the trivial point* $(0,0,0)$.

Proof. If N is composite, then its orbit lengths are derived from the orbit lengths of its prime factors and their least common multiples. For this reason, it suffices to prove for when N is an odd prime.

The procedure is similar to the proof of Theorem 4.16, leading to the same equation as in (4.12):

$$2x_3 \equiv 0 \pmod{N}.$$

Since $\mathrm{gdc}(2, N) = 1$, the equation has only one solution, the trivial point $(0,0,0)$. □

4.5 Generalised Tribonacci cat map

Like with the original DCM, the Tribonacci cat map can also be generalised. For any integers $a, b \in \{0, 1, \cdots, N-2\}$, a general form of the mapping is

$$\begin{pmatrix} x_t \\ y_t \\ z_t \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 1 \\ a & a+1 & a+1 \\ a+1 & b & b+1 \end{pmatrix} \begin{pmatrix} x_{t-1} \\ y_{t-1} \\ z_{t-1} \end{pmatrix} \pmod{N}. \tag{4.13}$$

A simple calculation shows that the determinant of the generalised matrix is always equal to 1, independently of the choices for a and b. As with the original Tribonacci cat map, this mapping is volume preserving and periodic. But even though the determinant remains the same, the minimal polynomial and its discriminant are different from the original. Depending on the choices for a and b, the same value of N can have different periods. Example 4.3 illustrates a couple of these differences.

Example 4.3. In the original Tribonacci cat map, the period modulo $N = 31$ is 331.

(a) For $a = 3$ and $b = 25$, the discriminant is $517712 = 2 \cdot 3 \cdot 21563$ and the period is 960.

(b) For $a = 3$ and $b = 7$, the discriminant is $4064 = 2^5 \cdot 127$ and the period is 192.

(c) For $a = 11$ and $b = 4$, the discriminant is $-10611 = -3^4 \cdot 131$ and the period is 320.

A further investigation in the generalised Tribonacci cat map may reveal how the choices of a and b interfere in the discriminant and, as a consequence, in the periods of the map. Like in Bao's and Chen's studies on the generalised DCM ([2] and [6] respectively), there can be some interesting general properties of the mapping in (4.13). In the next section, we use the generalised Tribonacci cat map to encrypt the RGB-colours of an image.

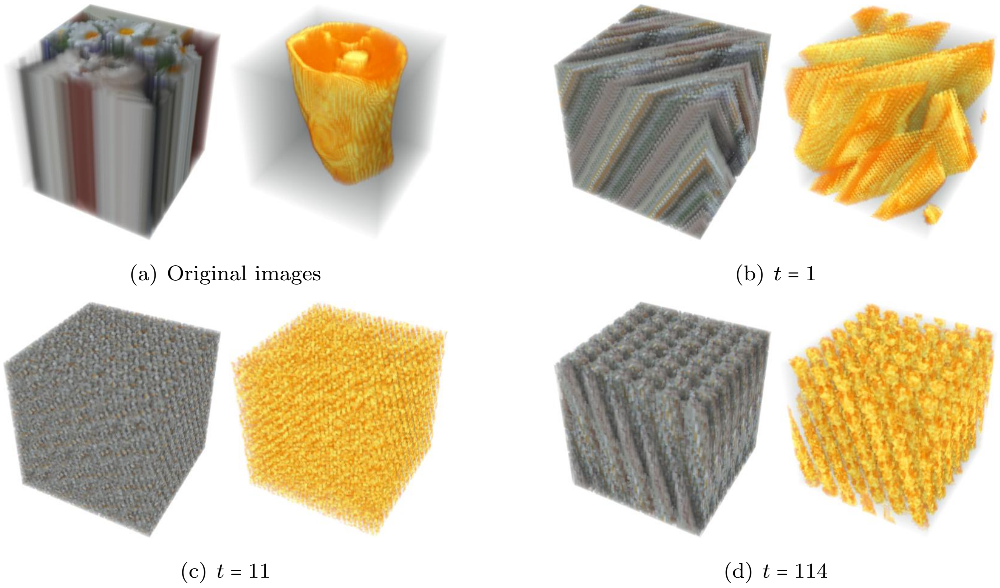
5 Applications

As an alternative to the three dimensional DCM, the Tribonacci cat map can be used for the same purposes, such as encryption and watermarking. The purpose of this section is merely to illustrate and exemplify how this mapping can be used in 3D image encryption and in colour encryption. In subsection 5.1, we use two 3D images and encrypt them using the proposed cat map. We comment on the appearances of ghosts and miniatures, and discuss the impact of the choice of N on the iterations. In subsection 5.2, we try colour encryption on a 2D image using both the original Tribonacci cat map and a generalised form of the map. We compare the outcomes from the two mappings, and discuss briefly on the role of the discriminant in the formation of chaotic colour schemes.

5.1 3D image encryption

From the definition of the Tribonacci cat map, the pixels of the 3D image are shuffled within the domain, creating chaotic patterns, before eventually returning to their original places simultaneously. In the two dimensional DCM, it is known that ghosts and miniatures of the image can appear in the middle of the process for certain values of N. These values have been studied by Behrends and presented in his article [3]. For security reasons, such values are not ideal for 2D image encryption.

After a few experiments with the Tribonacci cat map, it became clear that even this mapping creates ghosts when encrypting 3D images. However, the appearance of miniatures could neither be confirmed nor dismissed based on the experiments performed for this thesis because possible miniatures were difficult to distinguish. While there are studies about these phenomena in the DCM (once again we refer to Behrends' work [3]), there is still much left to learn about them in the Tribonacci cat map.



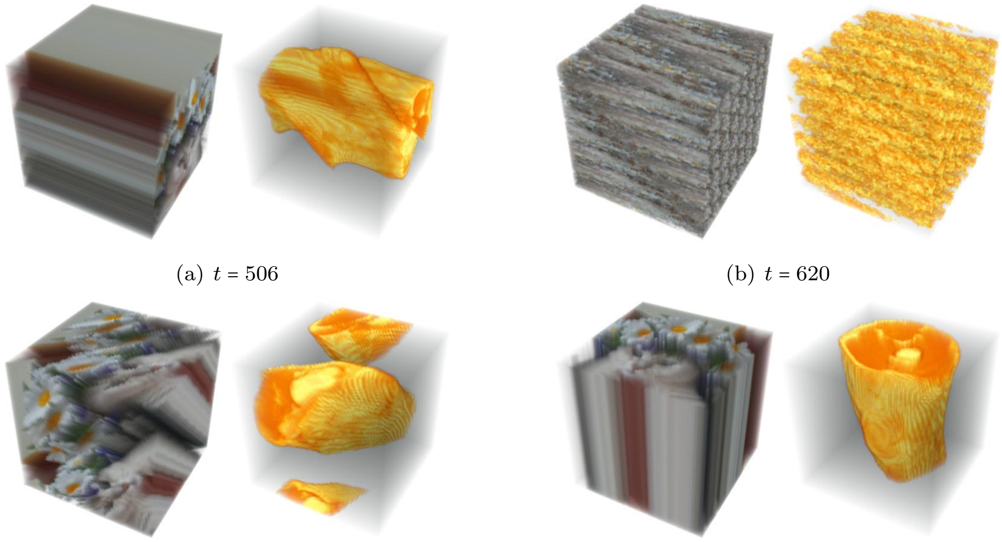
(a) Original images

(b) $t = 1$

(c) $t = 11$

(d) $t = 114$

Figure 6: $N = 67$ and $\rho'(67) = 1519$.



(a) $t = 506$

(b) $t = 620$

(c) $t = 1013$

(d) $t = 1519$

Figure 7: $N = 67$ and $\rho'(67) = 1519$ (cont.).

For a better illustration of the 3D image encryption, two different types of three dimensional images were used in the experiments. One consists of several layers of two dimensional images while the other is an MR-image in three dimensions. When exposed to the mapping, they present similar behaviours at t iterations.

The choice of $N = 67$ lies on the fact that it is a prime number from the set Q, where all orbit lengths of non-trivial points are equal to the period. The expectation, based on results from the original DCM, was that all iterations would present a chaotic image until the very last one. From Figure 7, it is clear that it was not the case. In fact, at approximately one third of the period, the original image was completely retrieved but in a different position. Later, at approximately two thirds of the period, ghosts of the original image appeared. As mentioned earlier, miniatures were difficult to identify in both cases.

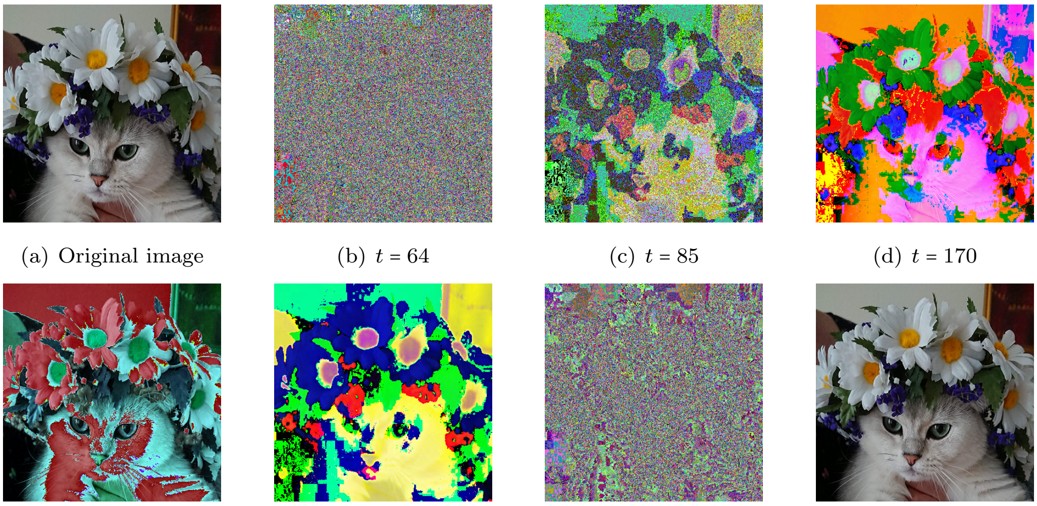
The same behaviour was noted for other prime values of N, not necessarily from the same set. The original image resurfaced in a different position after one third of the period, and then ghosts emerged after two thirds of the period. Even for some composite values of N the map presented the same behaviour. Meanwhile, when the period was a small number, like for $N = 163$ where $\rho'(163) = 54$, none of these phenomena took place. Further investigations are however required before any conclusions can be made.

The Tribonacci cat map is clearly not very secure if used alone. From the size of the image, the period is easily calculated. Even if the period is unknown, just by applying the mapping on the image, the original picture will be eventually retrieved. A solution would be to use a generalised form of the map and keep the values of a and b secret. Nevertheless, in order to increase the security and secrecy of the encrypted image, the Tribonacci cat map should be used as one of several steps in the encryption process.

5.2 Colour encryption

For the colour encryption, we used the RGB-values from 0 to 255. Since each pixel consists of a vector with three entries, (Red, Green, Blue), the Tribonacci cat map could be used to change their values and therefore change the colours inside the picture. For our experiments, a two dimensional image was used for a better visualisation of the changes (see Figures 8 and 9).

When encrypting colours, the size of the picture is no longer relevant. Instead, all calculations are performed modulo 256. This means that the period of the mapping will always be 512, regardless of how big or little the picture is. From a security point of view, this is far from ideal. One way to circumvent this is by using a generalised Tribonacci cat map. By choosing appropriate values of a and b, the period can become greater than 512. By keeping them secret, it increases the difficulty in retrieving the original picture by brute force.



Using the original Tribonacci cat map

(a) Original image

(b) $t = 64$

(c) $t = 85$

(d) $t = 170$

(e) $t = 171$

(f) $t = 341$

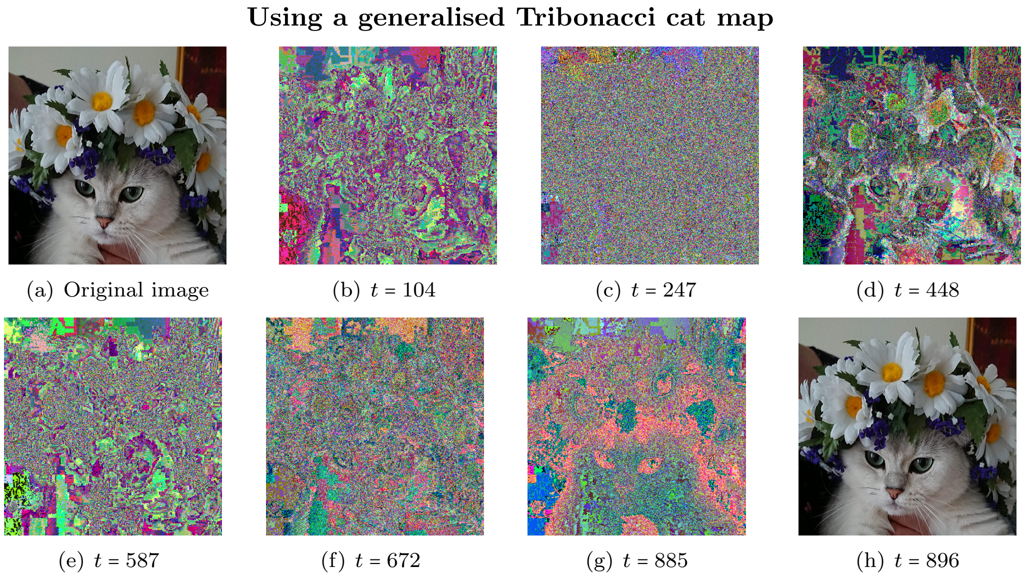
(g) $t = 484$

(h) $t = 512$

Figure 8: After 512 iterations, the colours of the image are restored.

Even though the pixels remain on the same positions all the time, by simply changing the values of their colours, the image becomes chaotic and unrecognisable. When using the Tribonacci cat map, however, the image resurfaces many times during the iterations but with different colour schemes, as illustrated in Figure 8. A hypothesis would be that this is a consequence of $N = 256$ being a power of 2, one of the primes in the discriminant of the minimal polynomial. In order to confirm or reject this hypothesis, as well as to find more information about this pattern, more research is clearly needed.

A few iterations from the encryption process with the generalised Tribonacci cat map are seen in Figure 9. In this investigation, the generalised mapping used for comparison had the parameters $a = 10$ and $b = 5$, and the period 896. The choice of the values for a and b lies on the fact that the period is greater than 512. Unlike with the original Tribonacci cat map, the image does not reappear as often and, when it does, it is not as easily recognisable. In Figure 9, the images (d) and (g) show hints of the original picture, but their colour schemes are not as defined as in Figure 8. Overall, the image becomes more chaotic than in the original



Using a generalised Tribonacci cat map

(a) Original image

(b) $t = 104$

(c) $t = 247$

(d) $t = 448$

(e) $t = 587$

(f) $t = 672$

(g) $t = 885$

(h) $t = 896$

Figure 9: For $a = 10$ and $b = 5$, the period becomes 896.

mapping.

More study on the generalised Tribonacci cat map is evidently needed. Firstly, to clarify how much more secure it is in relation to the original mapping when it comes to colour encryption. Secondly, to identify possible strong and weak relations (from a security point of view) between the parameters a and b. It is equally important to analyse how the values of a and b affect the period.

Colour encryption, as presented here, can also be realised in 3D images as long as their colour values are given in RGB-vectors. Like with the 3D image encryption, using either of the mappings for colour encryption should be but one of several steps in the encryption process in order to increase the security of the information.

6 Discussion

Based on the generating matrix to the Tribonacci sequence, the Tribonacci cat map is a three dimensional discrete chaotic dynamical system defined by the following mapping:

$$\begin{pmatrix} x_t \\ y_t \\ z_t \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} x_{t-1} \\ y_{t-1} \\ z_{t-1} \end{pmatrix} \pmod{N},$$

where $t \geq 1$ and (x, y, z) are the coordinates of a point in an N^3 space. Like its predecessor, Arnold's discrete cat map, it has proved itself of having an interesting mathematical structure and of being quite useful for different kinds of image based encryption. Here, we will discuss the results presented in the previous sections and propose future investigations on the subject.

6.1 Tribonacci cat map

As with the two dimensional discrete mapping, there is a strong relation between the period of the Tribonacci cat map, defined by $\rho'(N)$, and the period of the Tribonacci sequence, defined by $\pi'(N)$ and also known as the Trisano period. This relation was proved in Theorem 4.2, where it was also made clear that the period of the map is either equal to the whole or a third of the Trisano period for the same N. So, in the analysis of the periods of the Tribonacci cat map, we followed the steps from previous studies on the original Arnold's cat map and focused on proving the properties of the Trisano period.

The main result of this thesis is the proof of Theorem 4.9, which states the properties of the Trisano periods for prime values of N. According to the theorem, the period is determined by the factorisation of the minimal polynomial of the generating Tribonacci matrix modulo N. Whether N is a quadratic residue of the discriminant of the polynomial or not is helpful in the determination of the number of irreducible factors modulo N. In fact, the proof of the theorem can be easily adapted to the Tribonacci cat map because of shared properties between the minimal polynomials, like the discriminant.

When N is a prime power, i.e. $N = p^\alpha$ where p is prime and α is a natural number greater than 1, then Theorem 4.8 claims that its Trisano period is equal to $p^{\alpha-1}\pi'(p)$. Meanwhile, when N is a product of primes, the period is, according to Theorem 4.5, the least common multiple of the periods of its prime factors. Both theorems, together with Theorem 4.9, have their results translated to the Tribonacci cat map in Theorem 4.12.

In the study of upper bounds, we divided the prime numbers into sets according to their periods and their appearance in the discriminant, as in the case for $p = 2, 11$. With straightforward modular calculations, we managed to establish upper bounds to the periods of two of these sets in Corollaries 4.13 and 4.14. In order to identify a possible upper bound for all values of N, we analysed the ratios of the periods of the Tribonacci cat map for $2 \leq N \leq 10,000$. From the gathered data, we noticed that the highest ratios belonged to the composite numbers 345 and 690. Apart from these two, it appeared to be an overall negative correlation between the values of N and the ratios $\rho'(N)/N^2$. Based on these observations, Conjecture 4.15 was proposed as a limit to the upper bound. Alongside with these observations, we listed a few requirements that must be fulfilled in order for the period to lie on the upper bound for all values of N.

Besides the connection between the map and the recurrence sequence, there is another resemblance to the original Arnold's cat map. It is the fact that the orbit lengths in the Tribonacci cat map are divisors of the periods. However, the resemblance stops there. The orbit lengths of non-trivial points depend on the factorisation of the minimal polynomial modulo N when N is a prime other than 2 and 11. When the polynomial has linear factors, the orbit lengths are equal to the multiplicative orders of the roots. When the polynomial has a quadratic factor, then the orbit lenghts consist of the multiplicative order of the root in the linear factor and its multiple. Because of the limitations in the investigation, there are inconclusive results regarding the prediction of the multiple. In the case when the polynomial is irreducible modulo N, there is only one orbit length for non-trivial points, and it is the same as the period.

It is easier to predict the orbit lengths for composite values of N once we know the orbit lengths of the factors. Based on empirical investigations, when N is a prime power, i.e. $N = p^{\alpha}$, the orbit lengths are composed of the orbit lengths of $p^{\alpha-1}$ and their respective multiples with p. When N is a product of different primes, i.e. $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, then the orbit lengths consist of the orbit lengths of each prime factor and the least common multiples of the lengths. From the observations, we could see that when N is even, there are two disjoint orbits with length 1. Theorem 4.16 asserts that this is true for all even values of N, and states that the origin and the point $\left(\frac{N}{2}, \frac{N}{2}, \frac{N}{2}\right)$ are the only ones with orbit length equal to 1. As a consequence of the theorem, Corollary 4.17 proves that the origin is the only point with orbit length 1 when N is odd.

6.2 Applications

The main purpose of this thesis was to investigate the Tribonacci cat map and its mathematical properties. Still, a couple of examples in encryption were demonstrated in order to show the mapping's practical applications. Nonetheless, these examples are not enough to generalise the results presented here. The limitations regarding the hardware affected the choice of values of N, as well as hampered any detailed visualization of single iterations. The three dimensional equivalent of ghosts in Arnold's cat map were perceived in the Tribonacci cat map, but we were unable to identify the appearance of miniatures because of the inadequate image quality.

Two 3D images of equal dimensions and different characteristics were used for image encryption. One consisted of multiple layers of 2D images and the other was an original 3D graphic. Inspired by the results on encryption using Arnold's discrete cat map, a prime number from the set where all orbit lengths of non-trivial numbers are equal to the period was chosen. The expectation was to see chaotic images for all iterations before the last one. However, after approximately one third of the period, both images were completely retrieved but in a different position than the one from the beginning. At approximately two thirds of the period, ghosts covered the entire images. The same behaviour was observed for primes from the other sets. Only when the period of a prime N was relatively small did the images become chaotic until the end.

For colour encryption, a 2D image was used. Since the value of N was fixed to 256, the number of RGB-values for every pixel, the results from the Tribonacci cat map were compared with those from a generalised form of the map. By choosing appropriate values to the parameters of the generalised map, its period became greater than $\rho'(256) = 512$. The outcomes of the encryption showed that, besides having a greater period, the iterations of the generalised map turned out to be more chaotic than those from the original Tribonacci cat map. In many iterations of the original map, the image was distinguishable even if with a different colour scheme. A hypothesis is that the chaotic behaviour in colour encryption is strongly related to the connection between the discriminant and the value of N. By changing the parameters of the matrix, the discriminant is also changed, resulting in different properties of the periods and orbit lengths for the same value of N.

6.3 Future investigations

For several decades, researchers have studied Arnold's cat map, fascinated by its mathematical properties and practical applications. The Tribonacci cat map is equally fascinating and may also require many years before being completely understood. More data is needed in order to prove or refute Conjecture 4.15 about the map's upper bound. It can also be of interest to investigate other possible upper bounds for different values of composite N. The limitations in this thesis have also opened the doors to further investigations on orbit lengths. More study is needed on the orbit lengths when N is a prime from the set where the minimal polynomial has only one linear factor modulo N.

In this thesis, there was a short introduction to a generalised Tribonacci cat map and its application in encryption. Clearly, more research is needed on the subject, especially in consideration to its role in cryptography and cryptanalysis. The choice of parameters and their influence over the chaotic behaviour of the map can be relevant for future encryptions and attacks on encrypted images. In general, further investigations on encryption with Tribonacci cat map are essential in a world where more 3D graphics are being used and security of information is as important as ever.

References

[1] Adams W. & Shanks D. (1982). Strong primality tests that are not sufficient. *Mathematics of Computation.* Vol 39.159 pp 255-300. American Mathematica Society.

[2] Bao J. & Yang Q. (2012). Period of the discrete Arnold cat map and general cat map. *Nonlinear Dynamics.* Vol 70.2 pp 1365-1375. Springer Science+Business Media.

[3] Behrends E. (1998). The ghosts of the cat. *Ergodic Theory and Dynamical Systems.* Vol 18 pp 321 - 330. Cambridge University Press.

[4] Brindha M. (2017). Periodicity analysis of Arnold Cat Map and its application to image encryption. *2017 International Conference on Inventive Computing and Informatics (ICICI).* Pp 495 - 498. IEEE.

[5] Carlitz L. (1953). A theorem of Stickelberger. *Mathematica Scandinavica.* Vol 1 pp 82-84. Royal Danish Library.

[6] Chen F. et al. (2014). Period distribution of generalized discrete Arnold cat map. *Theoretical Computer Science.* Vol 552 pp 13 - 25. Elsevier.

[7] Choi U. S. et al. (2019). Color Medical Image Encryption Using 3D Chaotic Cat Map and NCA. *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS).* Pp 1 - 5. IEEE.

[8] Dyson F. J. & Falk H. (1992). Period of a discrete cat mapping. *The American Mathematical Monthly.* Vol 99.7 pp 605 - 614. Mathematical Association of America.

[9] Fransson J. (2013). *Generalized Fibonacci Series Considered Modulo n.* (Bachelor thesis). Linnæus University, Växjö, Sweden.

[10] Ganesan K. & Murali K. (2014). Image encryption using eight dimensional chaotic cat map. *The European Physical Journal: Special Topics.* Vol 223 pp 1611-1622. EDP Sciences, Springer-Verlag.

[11] Gaspari G. (1994). The Arnold cat map on prime lattices. *Physica D.* Vol 73.4 pp 352-372. Elsevier.

[12] Hungerford T. W. (2014). *Abstract Algebra.* Third Edition. Brooks/Cole, Cengage Learning.

[13] Klaška J. & Skula L. (2010). Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$. *Fibonacci Quarterly.* Vol 48.3 pp 228-235. Fibonacci Association.

[14] Mishra M. et al. (2012). High Security Image Steganography with Modified Arnold's Cat Map. *International Journal of Computer Applications.* Vol 37.9 pp 16 - 20. Foundation of Computer Science.

[15] Nance J. (2011). Periods of the discretized Arnold's cat mapping and its extension to n-dimensions. Cornell University Library.
`http://arxiv.org/abs/1111.2984v1` (downloaded 2019-12-08).

[16] Peng W. (2020). ABC implies there are infinitely many non-Fibonacci-Wieferich primes. *Journal of Number Theory.* Vol 212 pp 354-375. Elsevier.

[17] PrimeGrid. (2015). `http://www.primegrid.com/forumthread.php?id=3008&nowrap=true#45946` (visited 2020-07-03).

[18] Raj B. et al. (2019). A new transformation of 3D models using chaotic encryption based on Arnold cat map. In: Barolli L., Xhafa F., Khan Z., Odhabi H. (eds) *Advances in Internet, Data and Web Technologies.* EIDWT 2019. Lecture Notes on Data Engineering and Communications Technologies. Vol 29 pp 1-11. Springer.

[19] Rosen K. H. (2011). *Elementary Number Theory.* Sixth Edition. Pearson.

[20] Spickerman W. R. (1982). Binet's formula for the Tribonacci sequence. *The Fibonacci Quarterly.* Vol 20.2 pp 118-120.

[21] Svanström F. (2014). *Properties of a generalized Arnold's cat map.* (Master thesis). Linnæus University, Växjö, Sweden.

[22] Vince A. (1981). Period of a linear recurrence. *Acta Arithmetica.* Vol 39.4 pp 303-311.

[23] Wadill M. E. (1978). Some properties of a generalized Fibonacci sequence modulo m. *The Fibonacci Quarterly.* Vol 16.4 pp 344-353. Fibonacci Association.

[24] Wall D. D. (1960). Fibonacci series modulo m. *The American Mathematical Monthly.* Vol 67.6 pp 525-532. Mathematical Association of America.

A Mathematica code

Finding the periods for the first 10,000 numbers:

```
Periods = ParallelTable[k = 1;
  A = {{1, 1, 1}, {1, 2, 2}, {2, 3, 4}};
  Ak = A;
  While[Ak != IdentityMatrix[3],
   k++;
   Ak = Mod[A.Ak, n]];
  {n, k}, {n, 2, 10000}]
```

Finding the orbit lengths modulo N:

```
Orbits[n_] := Module[{list, list1, A, v, vk},
  list = {};
  A = {{1, 1, 1}, {1, 2, 2}, {2, 3, 4}};
  For[i = 0, i < n, i++,
   For[j = 0, j < n, j++,
    For[k = 0, k < n, k++,
     v = {{i}, {j}, {k}};
     If[MemberQ[list, v] == False,
      list1 = {};
      AppendTo[list, v];
      AppendTo[list1, v];
      vk = Mod[A.v, n];
      m = 1;
      While[vk != v,
       AppendTo[list, vk];
       AppendTo[list1, vk];
       vk = Mod[A.vk, n];
       m++];
      Print[{v, m}]]]]];
  Print[Length[list]]]
```

Finding the period of a generalised Tribonacci cat map:

```
PeriodGenTriCat[n_, a_, b_]:= Module[{A,At,k},
  A = {{1, 1, 1}, {a, a + 1, a + 1}, {a + 1, b, b + 1}};
  At = A;
  k = 1;
  While[At \neq IdentityMatrix[3],
    k++;
    At = Mod[A.At, n]];
  Print[k]]
```

Encrypting a 3D image with Tribonacci cat map:

```
TribonacciCatMap = Compile[{{pic, _Real, 3}},
  Module[{n},
    n = Dimensions[pic][[1]];
    Table[pic[[
      Mod[x + y + z, n , 1], Mod[x + 2y + 2z, n, 1],
      Mod[2x + 3y + 4z, n , 1]]], {x, n}, {y, n}, {z, n}]]]
```

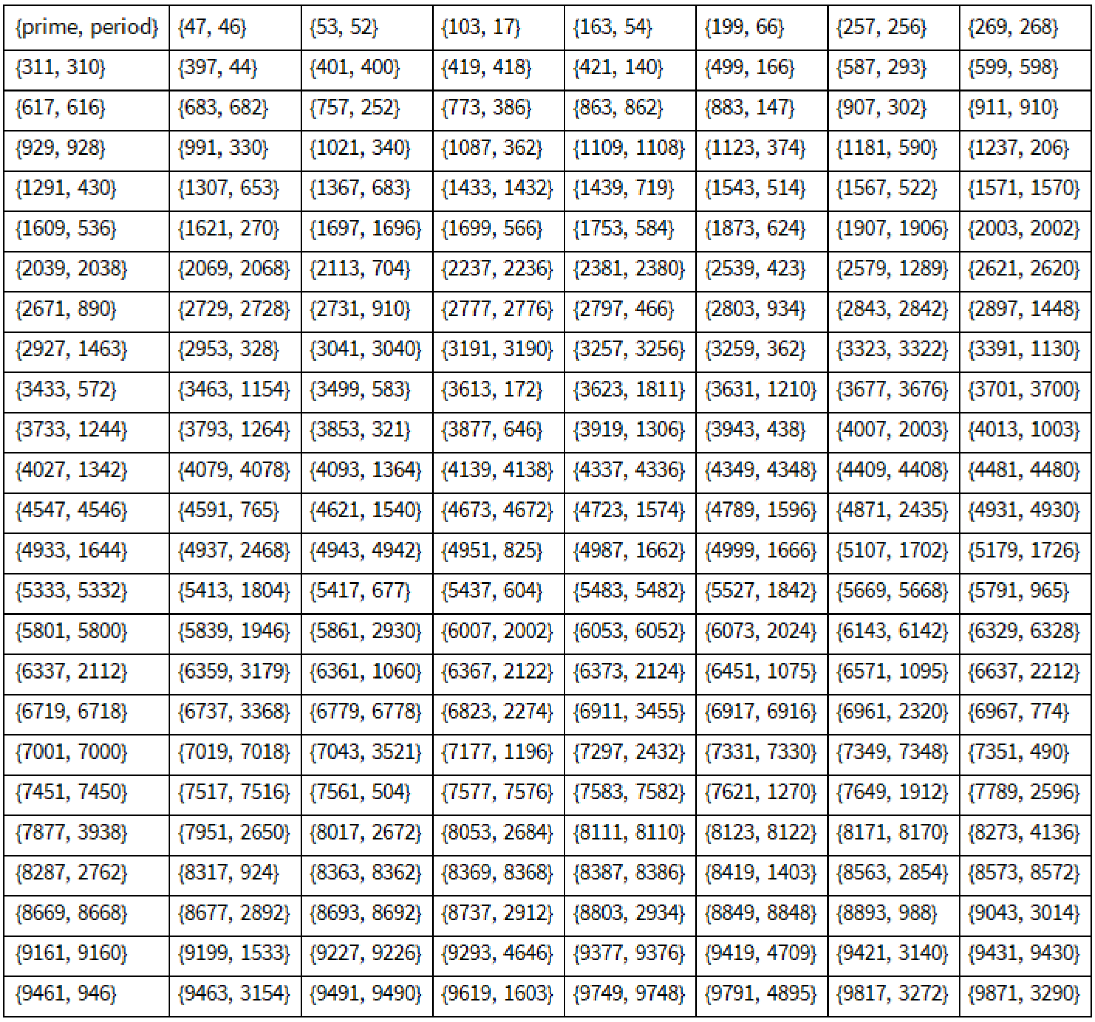
Encrypting colours with Tribonacci cat map:

```
TribonacciCatMap = Compile[{{pic, _Integer, 3}},
  Module[{A},
    A = {{1, 1, 1}, {1, 2, 2}, {2, 3, 4}};
    Table[pic[[
      Mod[x + y + z, n , 1], Mod[x + 2y + 2z, n, 1],
      Mod[2x + 3y + 4z, n , 1]]], {x, n}, {y, n}, {z, n}]]]
```

B Prime number sets

Here we present the primes p under 10,000 divided into the sets presented in section 4. The tables were created directly in Mathematica by using commands such as Partition[] and Grid[], which may have resulted in the removal of the last numbers of the lists.

Table A1: $R = \{r \mid \rho'(r) \leq r - 1\}$



{prime, period}	{47, 46}	{53, 52}	{103, 17}	{163, 54}	{199, 66}	{257, 256}	{269, 268}
{311, 310}	{397, 44}	{401, 400}	{419, 418}	{421, 140}	{499, 166}	{587, 293}	{599, 598}
{617, 616}	{683, 682}	{757, 252}	{773, 386}	{863, 862}	{883, 147}	{907, 302}	{911, 910}
{929, 928}	{991, 330}	{1021, 340}	{1087, 362}	{1109, 1108}	{1123, 374}	{1181, 590}	{1237, 206}
{1291, 430}	{1307, 653}	{1367, 683}	{1433, 1432}	{1439, 719}	{1543, 514}	{1567, 522}	{1571, 1570}
{1609, 536}	{1621, 270}	{1697, 1696}	{1699, 566}	{1753, 584}	{1873, 624}	{1907, 1906}	{2003, 2002}
{2039, 2038}	{2069, 2068}	{2113, 704}	{2237, 2236}	{2381, 2380}	{2539, 423}	{2579, 1289}	{2621, 2620}
{2671, 890}	{2729, 2728}	{2731, 910}	{2777, 2776}	{2797, 466}	{2803, 934}	{2843, 2842}	{2897, 1448}
{2927, 1463}	{2953, 328}	{3041, 3040}	{3191, 3190}	{3257, 3256}	{3259, 362}	{3323, 3322}	{3391, 1130}
{3433, 572}	{3463, 1154}	{3499, 583}	{3613, 172}	{3623, 1811}	{3631, 1210}	{3677, 3676}	{3701, 3700}
{3733, 1244}	{3793, 1264}	{3853, 321}	{3877, 646}	{3919, 1306}	{3943, 438}	{4007, 2003}	{4013, 1003}
{4027, 1342}	{4079, 4078}	{4093, 1364}	{4139, 4138}	{4337, 4336}	{4349, 4348}	{4409, 4408}	{4481, 4480}
{4547, 4546}	{4591, 765}	{4621, 1540}	{4673, 4672}	{4723, 1574}	{4789, 1596}	{4871, 2435}	{4931, 4930}
{4933, 1644}	{4937, 2468}	{4943, 4942}	{4951, 825}	{4987, 1662}	{4999, 1666}	{5107, 1702}	{5179, 1726}
{5333, 5332}	{5413, 1804}	{5417, 677}	{5437, 604}	{5483, 5482}	{5527, 1842}	{5669, 5668}	{5791, 965}
{5801, 5800}	{5839, 1946}	{5861, 2930}	{6007, 2002}	{6053, 6052}	{6073, 2024}	{6143, 6142}	{6329, 6328}
{6337, 2112}	{6359, 3179}	{6361, 1060}	{6367, 2122}	{6373, 2124}	{6451, 1075}	{6571, 1095}	{6637, 2212}
{6719, 6718}	{6737, 3368}	{6779, 6778}	{6823, 2274}	{6911, 3455}	{6917, 6916}	{6961, 2320}	{6967, 774}
{7001, 7000}	{7019, 7018}	{7043, 3521}	{7177, 1196}	{7297, 2432}	{7331, 7330}	{7349, 7348}	{7351, 490}
{7451, 7450}	{7517, 7516}	{7561, 504}	{7577, 7576}	{7583, 7582}	{7621, 1270}	{7649, 1912}	{7789, 2596}
{7877, 3938}	{7951, 2650}	{8017, 2672}	{8053, 2684}	{8111, 8110}	{8123, 8122}	{8171, 8170}	{8273, 4136}
{8287, 2762}	{8317, 924}	{8363, 8362}	{8369, 8368}	{8387, 8386}	{8419, 1403}	{8563, 2854}	{8573, 8572}
{8669, 8668}	{8677, 2892}	{8693, 8692}	{8737, 2912}	{8803, 2934}	{8849, 8848}	{8893, 988}	{9043, 3014}
{9161, 9160}	{9199, 1533}	{9227, 9226}	{9293, 4646}	{9377, 9376}	{9419, 4709}	{9421, 3140}	{9431, 9430}
{9461, 946}	{9463, 3154}	{9491, 9490}	{9619, 1603}	{9749, 9748}	{9791, 4895}	{9817, 3272}	{9871, 3290}

Table A2: $Q = \left\{q \mid \rho'(q) \leq q^2 + q + 1\right\}$

{prime, period}	{3, 13}	{5, 31}	{23, 553}	{31, 331}	{37, 469}	{59, 3541}	{67, 1519}
{71, 5113}	{89, 8011}	{97, 3169}	{113, 12883}	{137, 18907}	{157, 8269}	{179, 32221}	{181, 10981}
{191, 36673}	{223, 16651}	{229, 17557}	{251, 63253}	{313, 32761}	{317, 100807}	{331, 36631}	{353, 124963}
{367, 45019}	{379, 48007}	{383, 147073}	{389, 151711}	{433, 62641}	{443, 196693}	{449, 202051}	{463, 71611}
{467, 218557}	{487, 79219}	{509, 259591}	{521, 271963}	{577, 111169}	{619, 127927}	{631, 132931}	{641, 411523}
{643, 138031}	{647, 419257}	{653, 22477}	{661, 145861}	{691, 159391}	{709, 167797}	{719, 517681}	{727, 176419}
{751, 188251}	{797, 636007}	{823, 226051}	{829, 229357}	{839, 704761}	{859, 246247}	{881, 777043}	{947, 897757}
{971, 943813}	{977, 136501}	{983, 967273}	{1013, 1027 183}	{1039, 360187}	{1049, 1101 451}	{1061, 1126 783}	{1093, 398581}
{1103, 1217 713}	{1153, 443521}	{1171, 457471}	{1193, 1424 443}	{1213, 490861}	{1259, 1586 341}	{1277, 1632 007}	{1279, 545707}
{1301, 1693 903}	{1303, 566371}	{1321, 582121}	{1373, 1886 503}	{1409, 1986 691}	{1423, 675451}	{1453, 704221}	{1483, 733591}
{1489, 739537}	{1499, 2248 501}	{1511, 2284 633}	{1523, 2321 053}	{1549, 800317}	{1607, 2584 057}	{1637, 2681 407}	{1709, 2922 391}
{1721, 2963 563}	{1741, 32611}	{1747, 1017 919}	{1783, 1060 291}	{1787, 3195 157}	{1831, 1118 131}	{1871, 500359}	{1879, 1177 507}
{1901, 3615 703}	{1951, 1269 451}	{1973, 3894 703}	{2011, 1348 711}	{2017, 1356 769}	{2027, 4110 757}	{2029, 1372 957}	{2083, 1446 991}
{2099, 4407 901}	{2137, 1522 969}	{2143, 1531 531}	{2161, 1557 361}	{2179, 1583 407}	{2203, 1618 471}	{2267, 5141 557}	{2269, 1716 877}
{2281, 1735 081}	{2293, 1753 381}	{2297, 5278 507}	{2311, 1781 011}	{2333, 5445 223}	{2341, 1827 541}	{2347, 1836 919}	{2357, 5557 807}
{2377, 1884 169}	{2399, 5757 601}	{2423, 5873 353}	{2447, 5990 257}	{2467, 2029 519}	{2473, 2039 401}	{2531, 6408 493}	{2557, 167713}
{2633, 365017}	{2663, 7094 233}	{2677, 2389 669}	{2687, 7222 657}	{2689, 2411 137}	{2693, 7254 943}	{2699, 1041 043}	{2707, 2443 519}
{2711, 7352 233}	{2753, 1083 109}	{2819, 7949 581}	{2861, 8188 183}	{2887, 2779 219}	{2909, 8465 191}	{2957, 8746 807}	{2963, 8782 333}
{2971, 2943 271}	{3001, 3003 001}	{3019, 434161}	{3023, 9141 553}	{3037, 3075 469}	{3061, 3124 261}	{3067, 3136 519}	{3083, 9507 973}
{3089, 9545 011}	{3169, 3348 577}	{3217, 3450 769}	{3221, 10378 063}	{3271, 509653}	{3301, 3633 301}	{3331, 3699 631}	{3347, 11205 757}
{3359, 11286 241}	{3371, 11367 013}	{3389, 11488 711}	{3413, 1664 569}	{3457, 3984 769}	{3469, 4012 477}	{3491, 12190 573}	{3529, 4152 457}
{3547, 4194 919}	{3557, 12655 807}	{3617, 13086 307}	{3697, 4557 169}	{3719, 13834 681}	{3727, 4631 419}	{3767, 14194 057}	{3821, 14603 863}
{3833, 14695 723}	{3851, 14834 053}	{3881, 15066 043}	{3917, 2192 401}	{3931, 5152 231}	{3947, 15582 757}	{4019, 16156 381}	{4049, 16398 451}
{4051, 5471 551}	{4057, 5487 769}	{4073, 16593 403}	{4129, 5684 257}	{4159, 5767 147}	{4211, 17736 733}	{4217, 17787 307}	{4229, 17888 671}
{4261, 6053 461}	{4271, 18245 713}	{4273, 6087 601}	{4283, 18348 373}	{4327, 6242 419}	{4339, 6277 087}	{4357, 6329 269}	{4423, 6522 451}
{4447, 6593 419}	{4493, 20191 543}	{4513, 6790 561}	{4519, 6808 627}	{4603, 7064 071}	{4643, 21562 093}	{4651, 7212 151}	{4657, 7230 769}
{4679, 21897 721}	{4691, 22010 173}	{4733, 22406 023}	{4783, 7627 291}	{4799, 23035 201}	{4801, 7684 801}	{4877, 23790 007}	{4889, 23907 211}
{4909, 8034 397}	{4973, 24735 703}	{5003, 25035 013}	{5009, 3585 013}	{5021, 25215 463}	{5039, 25396 561}	{5087, 25882 657}	{5113, 8715 961}
{5119, 8736 427}	{5153, 717799}	{5171, 862723}	{5197, 9004 669}	{5237, 27431 407}	{5261, 27683 383}	{5273, 27809 803}	{5281, 9298 081}
{5303, 28127 113}	{5347, 9531 919}	{5351, 28638 553}	{5393, 29089 843}	{5399, 4164 943}	{5443, 9877 231}	{5449, 9899 017}	{5471, 29937 313}
{5479, 10008 307}	{5501, 30266 503}	{5503, 10096 171}	{5531, 30597 493}	{5569, 10339 777}	{5581, 10384 381}	{5591, 31264 873}	{5641, 10608 841}
{5647, 10631 419}	{5657, 32007 307}	{5659, 10676 647}	{5701, 10835 701}	{5743, 10995 931}	{5779, 11134 207}	{5813, 33796 783}	{5857, 11436 769}
{5867, 34427 557}	{5879, 34568 521}	{5897, 34780 507}	{5923, 11695 951}	{5927, 35135 257}	{5987, 35850 157}	{6011, 36138 133}	{6029, 36354 871}
{6037, 12150 469}	{6043, 1739 233}	{6121, 12490 921}	{6131, 37595 293}	{6163, 12662 911}	{6197, 38409 007}	{6229, 12935 557}	{6257, 39156 307}
{6263, 39231 433}	{6271, 13110 571}	{6301, 13236 301}	{6317, 39910 807}	{6323, 39986 653}	{6389, 40825 711}	{6427, 13770 919}	{6449, 41596 051}
{6469, 13951 477}	{6473, 41906 203}	{6491, 42139 573}	{6521, 42529 963}	{6581, 43316 143}	{6653, 44269 063}	{6659, 44348 941}	{6689, 44749 411}
{6691, 14925 391}	{6703, 14978 971}	{6733, 15113 341}	{6763, 15248 311}	{6781, 15329 581}	{6791, 46124 473}	{6803, 46287 613}	{6829, 15547 357}
{6857, 6717 901}	{6869, 47190 031}	{6977, 48685 507}	{6983, 48769 273}	{6997, 16321 669}	{7027, 16461 919}	{7109, 50544 991}	{7121, 50715 763}
{7129, 16943 257}	{7151, 51143 953}	{7159, 17086 147}	{7187, 51660 157}	{7219, 17373 727}	{7243, 17489 431}	{7247, 52526 257}	{7253, 52613 263}
{7283, 53049 373}	{7307, 53399 557}	{7309, 17809 597}	{7393, 18221 281}	{7417, 18339 769}	{7459, 18548 047}	{7481, 55972 843}	{7489, 18697 537}
{7507, 18787 519}	{7529, 56693 371}	{7547, 56964 757}	{7549, 18998 317}	{7573, 19119 301}	{7591, 19210 291}	{7639, 19453 987}	{7643, 58423 093}
{7681, 19668 481}	{7687, 19699 219}	{7703, 59343 913}	{7723, 19884 151}	{7727, 59714 257}	{7753, 20038 921}	{7759, 20069 947}	{7793, 8676 949}
{7841, 61489 123}	{7879, 20695 507}	{7901, 62433 703}	{7907, 62528 557}	{8009, 64152 091}	{8011, 21394 711}	{8039, 64633 561}	{8089, 3116 191}
{8101, 3125 443}	{8167, 22236 019}	{8209, 22465 297}	{8221, 22531 021}	{8231, 67757 593}	{8233, 22596 841}	{8237, 67856 407}	{8243, 67955 293}
{8297, 68848 507}	{8353, 23260 321}	{8429, 71056 471}	{8431, 23696 731}	{8501, 72275 503}	{8537, 72888 907}	{8539, 24307 687}	{8581, 24547 381}
{8627, 74433 757}	{8629, 24822 757}	{8647, 24926 419}	{8699, 75681 301}	{8713, 1946 797}	{8761, 25587 961}	{8779, 25693 207}	{8783, 77149 873}
{8831, 11142 199}	{8837, 78101 407}	{8867, 78632 557}	{8933, 79807 423}	{8941, 26650 141}	{8963, 80344 333}	{8969, 80451 931}	{8999, 80991 001}
{9001, 27009 001}	{9007, 27045 019}	{9013, 27081 061}	{9029, 81531 871}	{9067, 27406 519}	{9091, 27551 791}	{9109, 27660 997}	{9133, 27806 941}
{9157, 27953 269}	{9221, 85036 063}	{9241, 28468 441}	{9277, 28690 669}	{9311, 86704 033}	{9337, 29062 969}	{9343, 29100 331}	{9397, 29437 669}
{9403, 29475 271}	{9439, 29701 387}	{9497, 90202 507}	{9551, 91231 153}	{9601, 30729 601}	{9623, 92611 753}	{9629, 92727 271}	{9661, 31114 861}
{9689, 93886 411}	{9733, 31580 341}	{9739, 31619 287}	{9769, 31814 377}	{9839, 96815 761}	{9857, 97170 307}	{9859, 32403 247}	{9883, 32561 191}

Table A3: $S = \left\{ s \;\middle|\; \rho'(s) \leq \frac{s^2-1}{3} \right\}$

{prime, period}	{7, 16}	{13, 56}	{17, 32}	{19, 120}	{29, 140}	{41, 560}	{43, 308}	{61, 620}
{73, 1776}	{79, 1040}	{83, 287}	{101, 680}	{107, 424}	{109, 330}	{127, 1792}	{131, 5720}	{139, 1288}
{149, 7400}	{151, 950}	{167, 9296}	{173, 2494}	{193, 1552}	{197, 1078}	{211, 1855}	{227, 17176}	{233, 3016}
{239, 4760}	{241, 9680}	{263, 23056}	{271, 24480}	{277, 12788}	{281, 13160}	{283, 13348}	{293, 28616}	{307, 10472}
{337, 5408}	{347, 40136}	{349, 5800}	{359, 14320}	{373, 46376}	{409, 13940}	{431, 20640}	{439, 6424}	{457, 34808}
{461, 35420}	{479, 76480}	{491, 10045}	{503, 14056}	{523, 91176}	{541, 19512}	{547, 49868}	{557, 34472}	{563, 52828}
{569, 53960}	{571, 13585}	{593, 3256}	{601, 24080}	{607, 61408}	{613, 15657}	{659, 72380}	{673, 37744}	{677, 11752}
{701, 18200}	{733, 89548}	{739, 7585}	{743, 46004}	{761, 193040}	{769, 197120}	{787, 103228}	{809, 72720}	{811, 12180}
{821, 28085}	{827, 75992}	{853, 60634}	{857, 61204}	{877, 256376}	{887, 131128}	{919, 15640}	{937, 292656}	{941, 147580}
{953, 100912}	{967, 155848}	{997, 331336}	{1009, 169680}	{1019, 43265}	{1031, 354320}	{1033, 355696}	{1051, 73640}	{1063, 23541}
{1069, 95230}	{1091, 99190}	{1097, 66856}	{1117, 13416}	{1129, 424880}	{1151, 1840}	{1163, 450856}	{1187, 156552}	{1201, 480800}
{1217, 246848}	{1223, 166192}	{1229, 503480}	{1231, 252560}	{1249, 260000}	{1283, 274348}	{1289, 12040}	{1297, 70092}	{1319, 579920}
{1327, 34528}	{1361, 308720}	{1381, 127144}	{1399, 652400}	{1427, 678776}	{1429, 340340}	{1447, 697936}	{1451, 701800}	{1459, 78840}
{1471, 360640}	{1481, 365560}	{1487, 184264}	{1493, 247672}	{1531, 19533}	{1553, 14356}	{1559, 405080}	{1579, 207770}	{1583, 139216}
{1597, 212534}	{1601, 284800}	{1613, 867256}	{1619, 48540}	{1627, 882376}	{1657, 305072}	{1663, 460928}	{1667, 926296}	{1669, 928520}
{1693, 136488}	{1723, 494788}	{1733, 500548}	{1759, 1031 360}	{1777, 150368}	{1789, 533420}	{1801, 360400}	{1811, 1093 240}	{1823, 1107 776}
{1847, 1137 136}	{1861, 30380}	{1867, 580948}	{1877, 1174 376}	{1889, 79296}	{1913, 304964}	{1931, 1242 920}	{1933, 1245 496}	{1949, 1266 200}
{1979, 435160}	{1987, 658028}	{1993, 1324 016}	{1997, 147704}	{1999, 222000}	{2053, 1404 936}	{2063, 709328}	{2081, 360880}	{2087, 120988}
{2089, 96976}	{2111, 67520}	{2129, 302176}	{2131, 1513 720}	{2141, 509320}	{2153, 772568}	{2207, 1623 616}	{2213, 136038}	{2221, 411070}
{2239, 334208}	{2243, 838508}	{2251, 281500}	{2273, 26909}	{2287, 581152}	{2309, 161560}	{2339, 75985}	{2351, 1842 400}	{2371, 1873 880}
{2383, 236612}	{2389, 1902 440}	{2393, 318136}	{2411, 80735}	{2417, 973648}	{2437, 247457}	{2441, 397232}	{2459, 403112}	{2477, 2045 176}
{2503, 1044 168}	{2521, 2118 480}	{2543, 2155 616}	{2549, 166600}	{2551, 108460}	{2591, 49728}	{2593, 560304}	{2609, 378160}	{2617, 134288}
{2647, 333648}	{2657, 2353 216}	{2659, 294595}	{2683, 2399 496}	{2713, 2453 456}	{2719, 2464 320}	{2741, 313045}	{2749, 2519 000}	{2767, 79753}
{2789, 432140}	{2791, 173104}	{2801, 2615 200}	{2833, 1337 648}	{2837, 2682 856}	{2851, 2709 400}	{2857, 2720 816}	{2879, 460480}	{2903, 1404 568}
{2917, 472716}	{2939, 575848}	{2969, 195888}	{2999, 374750}	{3011, 755510}	{3049, 3098 800}	{3079, 3160 080}	{3109, 3221 960}	{3119, 3242 720}
{3121, 463840}	{3137, 1640 128}	{3163, 3334 856}	{3167, 1114 432}	{3181, 421615}	{3187, 3385 656}	{3203, 142489}	{3209, 1716 280}	{3229, 1737 740}
{3251, 352300}	{3253, 881834}	{3299, 725560}	{3307, 1822 708}	{3313, 1829 328}	{3319, 524560}	{3329, 1231 360}	{3343, 3725 216}	{3361, 1882 720}
{3373, 541768}	{3407, 1934 608}	{3449, 3965 200}	{3461, 998210}	{3467, 1001 674}	{3511, 4109 040}	{3517, 515387}	{3527, 49364}	{3533, 2080 348}
{3539, 2087 420}	{3541, 181720}	{3559, 4222 160}	{3571, 4250 680}	{3581, 356210}	{3583, 2139 648}	{3593, 4303 216}	{3607, 542102}	{3637, 2204 628}
{3643, 4423 816}	{3659, 2231 380}	{3671, 1497 360}	{3673, 408816}	{3691, 4541 160}	{3709, 573195}	{3739, 4660 040}	{3761, 1571 680}	{3769, 36424}
{3779, 528920}	{3797, 200239}	{3803, 4820 936}	{3823, 2435 888}	{3847, 4933 136}	{3863, 4974 256}	{3889, 210060}	{3907, 636027}	{3911, 2549 320}
{3923, 1709 992}	{3929, 5145 680}	{3967, 5245 696}	{3989, 530404}	{4001, 1334 000}	{4003, 5341 336}	{4021, 2694 740}	{4091, 697345}	{4099, 1400 150}
{4111, 5633 440}	{4127, 5677 376}	{4133, 1423 474}	{4153, 1437 284}	{4157, 320012}	{4177, 242324}	{4201, 29414}	{4219, 5933 320}	{4231, 2983 560}
{4241, 5995 360}	{4243, 6001 016}	{4253, 6029 336}	{4259, 1209 272}	{4289, 6131 840}	{4297, 6154 736}	{4363, 6345 256}	{4373, 2124 792}	{4391, 1071 160}
{4397, 805567}	{4421, 1303 016}	{4441, 6574 160}	{4451, 3301 900}	{4457, 6621 616}	{4463, 1106 576}	{4483, 837387}	{4507, 3385 508}	{4517, 566758}
{4523, 6819 176}	{4549, 6897 800}	{4561, 3467 120}	{4567, 3476 248}	{4583, 7001 296}	{4597, 7044 136}	{4637, 895907}	{4639, 1434 688}	{4649, 7204 400}
{4663, 2415 952}	{4703, 7372 736}	{4721, 7429 280}	{4729, 7454 480}	{4751, 1254 000}	{4759, 7549 360}	{4787, 2546 152}	{4793, 3828 808}	{4813, 7721 656}
{4817, 7734 496}	{4831, 3889 760}	{4861, 463320}	{4903, 8013 136}	{4919, 8065 520}	{4957, 8190 616}	{4967, 114218}	{4969, 117576}	{4993, 319616}
{5011, 8370 040}	{5023, 2102 544}	{5051, 340168}	{5059, 8531 160}	{5077, 4295 988}	{5081, 8605 520}	{5099, 1083 325}	{5101, 4336 700}	{5147, 1471 756}
{5167, 211888}	{5189, 8975 240}	{5209, 58352}	{5227, 2276 794}	{5231, 9121 120}	{5233, 9128 096}	{5279, 1857 856}	{5297, 9352 736}	{5309, 1565 860}
{5323, 9444 776}	{5381, 3217 240}	{5387, 4836 628}	{5407, 9745 216}	{5419, 1631 420}	{5431, 9831 920}	{5441, 9868 160}	{5477, 113627}	{5507, 3369 672}
{5519, 10153 120}	{5521, 5080 240}	{5557, 5146 708}	{5563, 10315 656}	{5573, 1478 968}	{5623, 5269 688}	{5639, 5299 720}	{5651, 1774 100}	{5653, 887678}
{5683, 10765 496}	{5689, 2157 648}	{5693, 10803 416}	{5711, 2174 368}	{5717, 10894 696}	{5737, 5485 528}	{5741, 332920}	{5749, 11017 000}	{5783, 2786 924}
{5807, 5620 208}	{5821, 11294 680}	{5827, 5658 988}	{5843, 11380 216}	{5849, 3801 200}	{5851, 11411 400}	{5869, 2296 344}	{5881, 5764 360}	{5903, 967928}
{5939, 391908}	{5953, 1476 592}	{5981, 11924 120}	{6047, 1354 304}	{6067, 12269 496}	{6079, 1231 808}	{6089, 3089 660}	{6091, 6183 380}	{6101, 4135 800}
{6113, 3114 064}	{6133, 1567 237}	{6151, 12611 600}	{6173, 4233 992}	{6199, 800575}	{6203, 458062}	{6211, 6429 420}	{6217, 12883 696}	{6221, 3225 070}
{6247, 6504 168}	{6269, 6550 060}	{6277, 6566 788}	{6287, 13175 456}	{6299, 4408 600}	{6311, 2655 248}	{6343, 1676 402}	{6353, 2242 256}	{6379, 678194}
{6397, 13640 536}	{6421, 13743 080}	{6481, 14001 120}	{6529, 7104 640}	{6547, 7143 868}	{6551, 4768 400}	{6553, 14313 936}	{6563, 14357 656}	{6569, 1198 660}
{6577, 14418 976}	{6599, 7257 800}	{6607, 14550 816}	{6619, 3650 930}	{6661, 4929 880}	{6673, 14842 976}	{6679, 177020}	{6701, 14967 800}	{6709, 3750 890}
{6761, 7618 520}	{6793, 7690 808}	{6827, 15535 976}	{6833, 1945 412}	{6841, 15599 760}	{6863, 15700 256}	{6871, 3147 376}	{6883, 15791 896}	{6899, 1586 540}
{6907, 3975 554}	{6947, 116572}	{6949, 8048 100}	{6959, 3228 512}	{6971, 16198 280}	{6991, 354160}	{7013, 16394 056}	{7039, 2064 480}	{7057, 5533 472}
{7069, 16656 920}	{7079, 4176 020}	{7103, 16817 536}	{7127, 256536}	{7193, 4311 604}	{7207, 4328 404}	{7211, 17332 840}	{7213, 17342 456}	{7229, 17419 480}
{7237, 311751}	{7321, 17865 680}	{7333, 1378 792}	{7369, 3620 144}	{7411, 9153 820}	{7433, 3069 416}	{7457, 18535 616}	{7477, 665542}	{7487, 1557 088}
{7499, 18745 000}	{7523, 3144 196}	{7537, 1183 466}	{7541, 1263 704}	{7559, 6348 720}	{7589, 9598 820}	{7603, 19268 536}	{7607, 19288 816}	{7669, 19604 520}
{7673, 19624 976}	{7691, 19717 160}	{7699, 1411 300}	{7717, 4962 674}	{7741, 166453}	{7757, 6685 672}	{7817, 5092 124}	{7823, 20399 776}	{7829, 170259}
{7853, 20556 536}	{7867, 6876 632}	{7873, 503936}	{7883, 6904 632}	{7919, 6967 840}	{7927, 20945 776}	{7933, 10488 748}	{7937, 3499 776}	{7949, 21062 200}
{7963, 1921 496}	{7993, 2662 002}	{8059, 10824 580}	{8069, 10851 460}	{8081, 7255 840}	{8087, 21799 856}	{8093, 164152}	{8117, 1830 158}	{8147, 1580 324}
{8161, 2220 064}	{8179, 11149 340}	{8191, 7454 720}	{8219, 3216 760}	{8263, 22759 056}	{8269, 11396 060}	{8291, 11456 780}	{8293, 22924 616}	{8311, 2302 424}
{8329, 2890 510}	{8377, 11695 688}	{8389, 7819 480}	{8423, 1970 748}	{8443, 424311}	{8447, 23783 936}	{8461, 5965 710}	{8467, 23896 696}	{8513, 2013 088}
{8521, 12101 240}	{8527, 1731 184}	{8543, 12163 808}	{8597, 24636 136}	{8599, 2464 760}	{8609, 12352 480}	{8623, 1549 086}	{8641, 85824}	{8663, 1563 491}
{8681, 5023 984}	{8689, 25166 240}	{8707, 12635 308}	{8719, 5068 064}	{8731, 25410 120}	{8741, 6367 090}	{8747, 118071}	{8753, 25538 336}	{8807, 12927 208}
{8819, 22045}	{8821, 25936 680}	{8839, 26042 640}	{8861, 6543 110}	{8863, 13092 128}	{8887, 26326 256}	{8923, 3317 497}	{8929, 8858 560}	{8951, 13353 400}
{8971, 6706 570}	{9011, 27066 040}	{9041, 1238 480}	{9049, 26245}	{9059, 6838 790}	{9103, 27621 536}	{9127, 27767 376}	{9137, 3478 532}	{9151, 13956 800}
{9173, 28047 976}	{9181, 14048 460}	{9187, 3516 707}	{9203, 7057 934}	{9209, 28268 560}	{9239, 28453 040}	{9257, 28564 016}	{9281, 14356 160}	{9283, 7181 174}
{9319, 5789 584}	{9323, 9657 592}	{9341, 1615 820}	{9349, 3641 825}	{9371, 2927 188}	{9391, 29396 960}	{9413, 2461 238}	{9433, 29660 496}	{9437, 3710 707}
{9467, 9958 232}	{9473, 29912 576}	{9479, 29950 480}	{9511, 30153 040}	{9521, 10072 160}	{9533, 15146 348}	{9539, 2022 056}	{9547, 15190 868}	{9587, 3829 607}
{9613, 3850 407}	{9631, 2576 560}	{9643, 30995 816}	{9649, 646550}	{9677, 7803 694}	{9679, 31227 680}	{9697, 31343 936}	{9719, 10495 440}	{9721, 3499 920}
{9743, 4520 288}	{9767, 15899 048}	{9781, 31889 320}	{9787, 15964 228}	{9803, 32032 936}	{9811, 10695 080}	{9829, 8050 770}	{9833, 8057 324}	{9851, 32347 400}

Lnu.se

Linnæus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0) 772-28 80 00
teknik@lnu.se
Lnu.se/faculty-of-technology?l=en