Properties of a generalized Arnold’s discrete cat map
Abstract

After reviewing some properties of the two dimensional hyperbolic toral automorphism called Arnold’s discrete cat map, including its generalizations with matrices having positive unit determinant, this thesis contains a definition of a novel cat map where the elements of the matrix are found in the sequence of Pell numbers. This mapping is therefore denoted as Pell’s cat map. The main result of this thesis is a theorem determining the upper bound for the minimal period of Pell’s cat map. From numerical results four conjectures regarding properties of Pell’s cat map are also stated. A brief exposition of some applications of Arnold’s discrete cat map is found in the last part of the thesis.

Keywords: Arnold’s discrete cat map, Hyperbolic toral automorphism, Discrete-time dynamical systems, Poincaré recurrence theorem, Number theory, Linear algebra, Fibonacci numbers, Pell numbers, Cryptography.
1 Introduction

Consider mixing two different colors of paint. It appears to be against all common sense that the colors would separate and appear in their original states after a certain amount of mixing. It would also be a bit perplexing if we at some intermediate point in time suddenly had a checkerboard color mix. This is however exactly the consequence of the Poincaré Recurrence Theorem\(^1\) for mathematical objects known as dynamical systems.

The two colors in Figure 1.1 are mixed in discrete-time steps, iterations, of Arnold’s cat map\(^2\). An iteration of Arnold’s cat map is the effect of a matrix multiplication and then the modulo operation on the pixel coordinate values. The image of the two colors are so to speak stretched and then folded back to fit within the original square shaped boundaries.

![Figure 1.1: Two colors and how they are mixed after 1, 25 and 306 iterations of Arnold’s cat map](image)

Even stranger behavior can be observed if we mix the pixels of an actual image rather than just two colors. The original image will sometimes appear upside down and occasionally we will experience how miniatures of the motive are lined up before our eyes.

The certain matrix used in Arnold’s cat map, closely related to the well known Fibonacci sequence, is chosen from the set of invertible 2x2 matrices with integer elements. This guarantees that it preserves the area of the image. By a generalization of Arnold’s cat map we mean choosing another such area preserving matrix. The novel generalized cat map presented in this thesis has a connection to the Pell sequence, so it is therefore called Pell’s cat map.

Since we wish to shed some light on the connection between the number of pixels in the image and the number of iterations needed to recover the original image we initially summarize, without proofs, the relevant material on Arnold’s cat map. It is natural to try to relate the two different mappings, so in the latter part of the thesis we will extend the known results to Pell’s cat map. It is also here we find the main result of the thesis in the form of a theorem for the upper bound of the number of iterations needed to recover the original image. Our observations also motivate some conjectures regarding the behavior of Pell’s cat map. Hereinafter we will primarily be using results and methods from linear algebra and elementary number theory. A brief exposition of some cryptographic applications of Arnold’s cat map is thereto found in the last part of the thesis.

\(^1\)After J.H. Poincaré 1854-1912

\(^2\)After V. I. Arnold 1937-2010. Following the convention, we will preferably be using an image of a cat to illustrate the effects of Arnold’s cat map and its generalizations
2 Arnold’s cat map

Take a square image, consisting of \(N\) by \(N\) pixels, where the coordinates of each pixel is represented by the ordered pair \((X, Y)\) of real numbers in the interval \([0, 1)\). Let an iteration of Arnold’s cat map firstly be the multiplication of all pixel coordinates by the matrix \(A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\). Then all values are taken modulo 1, so that the resulting coordinates are still in \([0, 1)\).

The effect of Arnold’s cat map on an image is shown in Figure 2.1. Even though the image looks chaotic already after a few iterations, the underlying order among the pixels lets us recover the original image after a certain number of additional iterations. We can also observe that, at one time, the image looks to be turned upside down before the original image appears once again.

Arnold’s cat map induces a discrete-time dynamical system in which the evolution is given by iterations of the mapping \(\Gamma_{\text{cat}} : \mathbb{T}^2 \to \mathbb{T}^2\) where

\[
\Gamma_{\text{cat}} \left( \begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} \right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \pmod{1}.
\]

This mapping is also known as a toral automorphism\(^4\) since \(\mathbb{T}^2\) is the 2-dimensional torus defined to be \(\mathbb{T}^2 = \mathbb{R}^2 / \mathbb{Z}^2 = \mathbb{R} / \mathbb{Z} \times \mathbb{R} / \mathbb{Z}\).

Following from the modulo 1 operation we must consider the image to be without edges, as shown in Figure 2.2, hence the torus \(\mathbb{T}^2\).

\(^3\)Some literature, such as [3] and [15], use \(A = \begin{bmatrix} \frac{3}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\), but this is just a mere technicality that does not affect the material presented in this thesis.

\(^4\)From [18] we have that an isomorphism from a group onto itself is an automorphism

---

Figure 2.1: The effect of Arnold’s cat map on a 289x289 pixels image after \(n\) iterations

Arnold’s cat map
In Figure 2.3 we can see the effect of Arnold’s cat map on the unit square, first stretching and then folding it. Since the matrix determinant $\det(A) = 1$, the mapping is area preserving and the point marked in (0,1) helps illustrating the orientation preserving characteristics of Arnold’s cat map.

**Remark 2.1.** Compare the result of the modulo 1 operation in Figure 2.3 to the image of the cat shown in Figure 2.1 after one iteration.

For an image with rational coordinates $0 \leq \frac{x}{N}, \frac{y}{N} < 1$, a scaling of the image makes it possible to work with integer coordinates $0 \leq x, y \leq N - 1$. This clearly forces us to use modulo $N$ instead of modulo 1, hence Arnold’s discrete cat map $\Gamma_A : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$ is

$$\Gamma_A \left( \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}.$$  

With $\pi$ being the transition from rational coordinates in the interval $[0, 1)$ to integer coordinates $(0, 1, 2, \ldots, N - 1)$, we have the following commutative diagram

$$
\begin{array}{ccc}
\mathbb{T}^2 & \xrightarrow{\Gamma_A} & \mathbb{T}^2 \\
\downarrow{\pi} & & \downarrow{\pi} \\
\mathbb{Z}_N \times \mathbb{Z}_N & \xrightarrow{\Gamma_A} & \mathbb{Z}_N \times \mathbb{Z}_N
\end{array}
$$
The characteristic polynomial of the matrix $A$ is
\[ \lambda^2 - \text{trace}(A)\lambda + \det(A) = \lambda^2 - 3\lambda + 1 \]
and the two eigenvalues of the matrix $A$, i.e. the roots of the characteristic polynomial, are $\lambda_1 = (3 + \sqrt{5})/2 \approx 2.618034$ and $\lambda_2 = (3 - \sqrt{5})/2 \approx 0.381866$.

The discriminant of the characteristic polynomial is
\[ D = (\text{trace}(A))^2 - 4 \cdot \det(A) = 5. \]

Since neither of the two eigenvalues of $A$ is of unit length the mapping $\Gamma_{\text{cat}} : T^2 \to T^2$ is said to be a hyperbolic toral automorphism and since $A$ is a symmetric matrix the two eigenvectors are orthogonal.

The fact that the discrete-time dynamical system i.e. the set of rules imposed by Arnold’s cat map, will follow the Poincaré Recurrence Theorem and hence be periodic leads us to make the following definition.

**Definition 2.2.** The minimal period of Arnold’s discrete cat map is the smallest positive integer $n$ such that $A^n \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N}$. We denote by $\Pi_A(N)$ the minimal period of Arnold’s discrete cat map modulo $N$.

**Example 2.3.** From Figure 2.1 we can conclude that $\Pi_A(289) = 306$, since there is no positive integer smaller than $n = 306$ such that the original image reappears.

In this thesis we will be working preferably with integer coordinates and the modulo $N$ operation, so for simplicity of notation we will write Arnold’s cat map instead of Arnold’s discrete cat map when no confusion can arise.

Henceforth $p, q, r$ and $s$ will denote prime numbers while $a, b, i, j, k, m, n$ and $N$ are all integers. Two disjoint sets of prime numbers called $R$ and $S$ will be defined in Subsection 5.3.

Figures and numerical computations used in this thesis are made using MATLAB®.

4
3 The connection between Arnold’s cat and Fibonacci’s rabbits

**Definition 3.1.** Let the \( n \)th number of the Fibonacci sequence be defined by the recurrence relation \( F_n = F_{n-1} + F_{n-2} \) with \( F_0 = 0 \) and \( F_1 = 1 \).

Hence the first Fibonacci numbers are 0, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

The Fibonacci sequence can be found in many varying contexts stretching from Pascal’s triangle\(^5\) to real life objects, such as the shell of a pineapple.

Powers of the matrix 
\[
F = \begin{bmatrix}
0 & 1 \\
1 & 1
\end{bmatrix}
\]
will generate numbers the Fibonacci sequence
\[
F^n = \begin{bmatrix}
F_{n-1} & F_n \\
F_n & F_{n+1}
\end{bmatrix}.
\]

In [1] the matrix \( F \) is called the golden cat map due to the well known connection between two consecutive Fibonacci numbers and the golden ratio\(^6\). Note that the golden ratio is also equal to the largest eigenvalue of \( F \).

Since \( F \) and \( A \) have the relationship
\[
F^2 = \begin{bmatrix}
0 & 1 \\
1 & 1
\end{bmatrix} \begin{bmatrix}
0 & 1 \\
1 & 1
\end{bmatrix} = \begin{bmatrix}
1 & 1 \\
1 & 2
\end{bmatrix} = A,
\]
the Fibonacci numbers will also appear when we take powers of the matrix \( A \) in the following manner
\[
A^n = \begin{bmatrix}
1 & 1 \\
1 & 2
\end{bmatrix}^n = \begin{bmatrix}
F_{2n-1} & F_{2n} \\
F_{2n} & F_{2n+1}
\end{bmatrix},
\]
with the first powers of \( A \) being
\[
A^2 = \begin{bmatrix}
2 & 3 \\
3 & 5
\end{bmatrix},
A^3 = \begin{bmatrix}
5 & 8 \\
8 & 13
\end{bmatrix},
A^4 = \begin{bmatrix}
13 & 21 \\
21 & 34
\end{bmatrix},
A^5 = \begin{bmatrix}
34 & 55 \\
55 & 89
\end{bmatrix}, \ldots
\]

From the definition of the minimal period of Arnold’s cat map we know that we are looking for the smallest integer \( n \) such that \( A^n \equiv \begin{bmatrix}1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \) i.e. we must find the smallest \( n \) such that \( F_{2n-1} \equiv 1 \pmod{N} \) and \( F_{2n} \equiv 0 \pmod{N} \). Hence the period of Arnold’s cat map will have a direct connection to the Pisano period\(^7\) of the Fibonacci sequence. From the above-mentioned relation between the matrices \( F \) and \( A \) follows that the period of Arnold’s cat map will be exactly half the Pisano period for all \( N \geq 3 \).

---

\(^5\)After B. Pascal 1623-1662

\(^6\)(1 + \( \sqrt{5} \))/2 \approx 1.618

\(^7\)The period length of the Fibonacci sequence modulo \( N \), named after Leonardo of Pisa
4 Properties of Arnold’s cat map

As depicted in Figure 4.1 there is no obvious connection between the minimal period of Arnold’s cat map, and hence the Pisano period, and the number $N$. This fact has been the object of many studies and articles where [19] by Wall can be considered as the most prominent.

![Figure 4.1: Minimal periods $\Pi_A(N)$ of Arnold’s cat map and the ratio $\Pi_A(N)/N$ for the interval $2 \leq N \leq 100$](image)

4.1 Period lengths

It is worth pointing out that there exists no known closed form expression for $\Pi_A(N)$ valid for all $N$, so to find the minimal period we are referred to numerical calculations. To formulate a theorem regarding the upper bound for the minimal period length, we must also define the period of Arnold’s cat map. This is not necessarily the minimal period, but we can nevertheless use elementary results stemming from elementary number theory to actually calculate it for all $N$.

**Definition 4.1.** A period $\Psi_A(N)$ of Arnold’s cat map is an integer $k$ such that

$$A^k \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N}.$$ 

Therefore $\Pi_A(N) \leq \Psi_A(N)$ and, more precisely, $\Pi_A(N)$ will always be a divisor of $\Psi_A(N)$. All multiples of $\Psi_A(N)$ will also be congruent to $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (mod $N$).

The reason behind the inequality $\Pi_A(N) \leq \Psi_A(N)$ comes from the phenomena that, for some prime numbers and hence also for composite numbers with such prime factors, the minimal period is a divisor of the period that we get using the expression for $\Psi_A(N)$ found in [15] by Neumärker and [9] by Dyson and Falk.

**Definition 4.2.** Prime numbers with the property that $\Pi_A(p) < \Psi_A(p)$ will be referred to as short prime numbers for Arnold’s cat map.
Example 4.3. We have that $\Pi_A(29) = 7 \neq \Psi_A(29) = 14$, hence 29 is a short prime number for Arnold’s cat map.

Dyson and Falk propose in [9] an expression for the asymptotic behavior of the fraction of integers up to and including $N$ that will have $\Pi_A(N) = \Psi_A(N)$ calling these integers “primitive”. In [2] Bao and Yang present an algorithm to find $\Pi_A(N)$ for a given $\Psi_A(N)$ using stepwise elimination of the factors of $\Psi_A(N)$.

Wall [19] provides a table for the 99 short prime numbers $5 < p < 2000$ (there are 300 prime numbers $5 < p < 2000$ in total). Brother continues this work in [4] with the 38 (out of totally 127) prime numbers $2000 < p < 3000$ for which the minimal period is a divisor of the period $\Psi_A(p)$. Even though these two articles actually precede the introduction of the cat map, made by Arnold in 1967, these results are directly transferable to Arnold’s cat map due to the connection between the matrices $F$ and $A$. A computation for $5 < p < 50000$ yields that about 33% (1716/5130) are short prime number for Arnold’s cat map.

Figure 4.2 shows the minimal periods of Arnold’s cat map for prime numbers $2 \leq p \leq 5000$. Note the scattered presence of short prime numbers below the two prominent lines $p + 1$ and $(p - 1)/2$.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig4_2.png}
\caption{Minimal periods of Arnold’s cat map for the prime numbers $2 \leq p \leq 5000$}
\end{figure}

The discriminant of the characteristic polynomial plays an important role for the periods of Arnold’s cat map modulo $N$. If the discriminant is a square in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ i.e. if 5 is a quadratic residue modulo $p$, then the characteristic polynomial has roots in $\mathbb{F}_p$, and from Fermat’s Little Theorem $\Psi_A(p) = (p - 1)/2$. By the notation that an integer $n$ is a quadratic residue modulo $p$ we mean that there exist an integer $k$ such that $k^2 \equiv n \pmod{p}$.

If 5 is a quadratic nonresidue modulo $p$ and hence $x^2 - 3x + 1$ has no roots in $\mathbb{F}_p$, we follow [18] using Kronecker’s Theorem to extend the field so that it becomes $\mathbb{F}_p[x]/(x^2 - 3x + 1)$, which is the splitting field of $x^2 - 3x + 1$. In this case $\Psi_A(p) = p + 1$.

\footnote{After P. de Fermat 1601-1665}

\footnote{After L. Kronecker 1823-1891}
Considering the two special cases $\Pi_A(2) = 3$ and $\Pi_A(5) = 10$, a period $\Psi_A(N)$ can be calculated for any composite number $N$ using the following theorem proved in [12] by Gaspari.

**Theorem 4.4.** If $N$ has the prime factorization $N = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_k^{a_k}$. Then $\Psi_A(N) = \text{lcm} \left( \Psi_A(p_1^{a_1}), \Psi_A(p_2^{a_2}), \Psi_A(p_3^{a_3}), \ldots, \Psi_A(p_k^{a_k}) \right)$, where lcm is the least common multiple.

**Example 4.5.** We can conclude that $\Psi_A(21) = \text{lcm} \left( \Psi_A(3), \Psi_A(7) \right) = \text{lcm} (4, 8) = 8$.

Note that $p = 2$ is the only known prime number where $\Pi_A(p) = \Pi_A(p^2)$. For all other powers of prime numbers it is believed that $\Pi_A(p^n) = p^{n-1} \Pi_A(p)$. However finding a prime number $p \geq 3$ such that $\Pi_A(p) = \Pi_A(p^2)$ would prove the existence of a Wall-Sun-Sun prime number\(^{10}\) as conjectured by Wall in [19]. No one has yet been able to prove that such a prime number does not exist, but on the other hand no such number has yet been found\(^{11}\) for $p < 3.9 \cdot 10^{16}$ (April 2014).

**Remark 4.6.** For composite $N$ we have cases when $\Pi_A(N) = \Pi_A(N^2)$, for example $\Pi_A(6) = \Pi_A(36) = 12$ and $\Pi_A(12) = \Pi_A(144) = 12$.

**Theorem 4.7.** The upper bound for the minimal period of Arnold’s cat map is $3N$.

The proof of this is omitted here but can be found in [9] by Dyson and Falk, where it in turn is based on theorems from [13] by Hardy and Wright.

Dyson and Falk also prove that for $k = 1, 2, 3, \ldots$

$\Psi_A(N) = 3N$ when $N = 2 \cdot 5^k$,

$\Psi_A(N) = 2N$ when $N = 5^k$ or $N = 6 \cdot 5^k$,

$\Psi_A(N) \leq \frac{12}{7}N$ for all other $N$.

Besides giving an expression for the upper bound, Dyson and Falk also examines the lower bound for the minimal period of Arnold’s cat map.

### 4.2 Disjoint orbits

Besides the periodicity we can also define some other distinct properties valid for discrete-time dynamical systems.

**Definition 4.8.** Let the *orbit* of a point denote the set of coordinates that an individual point will assume under iterations of a dynamical system, for example Arnold’s cat map, until it returns to its initial value. The number of unique coordinates in the orbit is called the *orbit length*. Of course all points belonging to one and the same orbit have the same orbit length.

---

\(^{10}\)These are also known as Fibonacci-Wieferich prime numbers and in [15] by Neumärker $\Pi_A(p) = \Pi_A(p^2)$ is referred to as the plateau phenomenon.

\(^{11}\)It is possible to follow or participate in the search for the first Wall-Sun-Sun prime number on the web page [http://prpnet.primegrid.com:13001/pending_work.html](http://prpnet.primegrid.com:13001/pending_work.html)
Definition 4.9. For a dynamical system any point where the rate of change is zero is called a fixed point or trivial point. For a discrete-time system this will be all points with orbit length 1. Points with an orbit length greater than 1 are called non-trivial.

Example 4.10. So for the discrete mapping $\Gamma_A : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$, the point with coordinates $(0,0)$ is a trivial point. All other points with integer coordinates are non-trivial since they are periodic and have an orbit length greater than 1.

The orbit, with length 12, of the point $(1,1)$ for Arnold’s cat map with $N = 6$, consisting of the coordinates $\{(1, 1), (2, 3), (5, 2), (1, 3), (4, 1), (5, 0), (5, 5), (4, 3), (1, 4), (5, 3), (2, 5), (1, 0)\}$, is depicted in Figure 4.3.

Figure 4.3: The orbit of the point $(1,1)$ for Arnold’s cat map with $N = 6$

Since we know that $(0,0)$ is a trivial point with orbit length 1 and that the upper bound for the period of Arnold’s cat map is $3N$, for all $N > 3$, no point can have an orbit that includes all the $N^2 - 1$ non-trivial points. From this we can conclude that there will be a number of disjoint orbits. The length of these orbits will either be equal to the minimal period or be a divisor of it. The orbit length of the point $(1,1)$ will always be equal to the minimal period $\Pi_A(N)$ for all $N \geq 2$ since the $x$-coordinates of the orbit are equal to odd numbered Fibonacci numbers modulo $N$ and the $y$-coordinate corresponds to even numbered ditto.

When $N$ is a prime number $p$, except for $p = 5$, all of the non-trivial points have one and the same orbit length, as shown by Gaspari in [12]. When $p = 5$ the orbit length of the non-trivial points are either $\Pi_A(5) = 10$ or $\Pi_A(5)/5 = 2$. Figure 4.4 shows the orbit lengths for the prime numbers $p = 5$ and $p = 7$.

Figure 4.4: Orbit lengths for Arnold’s cat map for $p = 5$ and $p = 7$
Composite numbers will have more than one period length for the non-trivial points and investigating \( N \) up to 500 reveals that the highest number of different orbit lengths occurs for \( N = 390 \). The 17 different orbit lengths are then 2, 3, 4, 6, 10, 12, 14, 20, 28, 30, 42, 60, 70, 84, 140, 210 and 420. Figure 4.5 shows the orbit lengths of the points for Arnold’s cat map for the composite numbers \( N = 9 \) and \( N = 10 \).

![Figure 4.5: Orbit lengths for Arnold’s cat map for \( N = 9 \) and \( N = 10 \)](image)

### 4.3 Higher dimensions of the cat map

The cat map can also be extended into higher dimensions as described by Nance in [14] where he, in three steps, fixes each one of the x-, y- and z-coordinate and then multiplies the results to get the matrix of the 3-dimensional cat map \( A_{3D} \).

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 1 \\
0 & 1 & 2
\end{bmatrix} \begin{bmatrix}
1 & 1 & 0 \\
0 & 1 & 0 \\
1 & 0 & 2
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 1 \\
2 & 3 & 2 \\
3 & 4 & 4
\end{bmatrix} = A_{3D}.
\]

The matrix \( A_{3D} \) is not unique due to the non-commutative properties of matrix multiplication, so in [7] we have

\[
A_{3D} = \begin{bmatrix}
2 & 1 & 3 \\
3 & 2 & 5 \\
2 & 1 & 4
\end{bmatrix},
\]

however all \( A_{3D} \) will have the same eigenvalues \( \lambda_1 \approx 7.18, \lambda_2 \approx 0.57 \) and \( \lambda_3 \approx 0.24 \). Interestingly the minimal periods of the 3-dimensional cat map, shown in Figure 4.6, display a totally different pattern than \( \Pi_A(N) \).

The 4-dimensional cat map is calculated using \( A_{3D} \) with yet an additional coordinate, so \( A_{4D} \) is

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 \\
0 & 2 & 3 & 2 \\
0 & 3 & 4 & 4
\end{bmatrix} \begin{bmatrix}
1 & 1 & 0 \\
0 & 1 & 0 \\
2 & 2 & 3 \\
3 & 4 & 4
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 1 & 0 \\
2 & 3 & 2 & 0 \\
0 & 0 & 1 & 0 \\
3 & 4 & 4 & 0
\end{bmatrix} = A_{4D}.
\]

Figure 4.5: Orbit lengths for Arnold’s cat map for \( N = 9 \) and \( N = 10 \)
The reason to choose a cat map of a higher dimension is the behavior of the largest eigenvalue. A cat map of a higher dimension is considered being more chaotic by the topological entropy measure \( \log |\lambda_{\text{max}}| \) as defined in [3]. This a property that is preferred in a cryptographic context. The largest eigenvalue of \( A_{8D} \) is about 1090.

4.4 The generalized cat maps with positive unit determinant

The generalized cat maps, with determinant 1, of type 1 and 2, are defined to be

\[
\Gamma_{G_1}\left( \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \right) = \begin{bmatrix} 1 & a \\ a & a^2 + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}
\]

\( A_{8D} \) is a product of matrices with determinant 1, but when the determinant of \( A_{8D} \) is calculated the result becomes −299, indicating that there is a typographical error in [11].
and

\[ \Gamma_{G_2} \left( \begin{array}{c} x_{n+1} \\ y_{n+1} \end{array} \right) = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}. \]

Periods of the two generalized cat maps are studied in [2]. In [5] and [6] Chen et al. use the Hensel lift method\(^\text{13}\) to study the period distribution. In the latter article Chen et al. states that “Our next step aims to work on the corresponding period distribution for general composite \(N\)’s”, but so far (April 2014) no further work has yet been published.

### 4.5 Miniatures and ghosts

Before reaching the minimal period we can sometimes observe that the image appears to be less chaotic than expected. Behrends [3] gives an explanation to how and when these phenomena that we will call miniatures and ghosts occur, claiming the following

- Miniatures may occur when the absolute values of all of the elements of \(A^n \pmod{N}\), i.e. \(\min |a_{i,j}, N - a_{i,j}| \) for \(i, j = 1, 2\), are small compared to \(N\).
- If miniatures occur, the number of miniatures\(^\text{14}\) is always \(\pm 1 \pmod{N}\).
- The orientation of the miniatures will depend on the column vectors of \(A^n \pmod{N}\).
- Ghosts are more likely to occur when \(N\) is a composite number than when it is a prime number.
- The number of ghosts and their slopes depend on vectors, with small absolute values, that are mapped onto themselves by \(A^n \pmod{N}\).

Figure 4.7 shows miniatures in a 289x289 pixels image using a type 1 generalized cat map and Figure 4.8 shows ghosts occurring after 70 iterations of Arnold’s cat map on a 286x286 pixels image.

Figure 4.7: Miniatures occurring after 34 iterations of a type 1 generalized cat map \(G_1 = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}\) on a 289x289 pixels image

So since

\[
\begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}^{34} \equiv \begin{bmatrix} 277 & 12 \\ 12 & 12 \end{bmatrix} \equiv \begin{bmatrix} -12 & 12 \\ 12 & 12 \end{bmatrix} \pmod{289}
\]

\(^{13}\)After K. Hensel 1861-1941

\(^{14}\)Remember to consider the image as being without edges
there must be $|12 \cdot (-12) - 12 \cdot 12| = 288$ miniatures. The slopes of the miniatures are $-1$ and $1$ following from the column vectors $\begin{bmatrix} -12 \\ 12 \end{bmatrix}$ and $\begin{bmatrix} 12 \\ 12 \end{bmatrix}$.

Figure 4.8: Ghosts occurring after 70 iterations of Arnold’s cat map on a 286x286 pixels image

Here we have that

\[
\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^{70} \equiv \begin{bmatrix} 1 & 143 \\ 143 & 144 \end{bmatrix} \pmod{286}
\]

and since

\[
\begin{bmatrix} 1 & 143 \\ 143 & 144 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 286 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 0 \end{bmatrix} \pmod{286}
\]

the vector $\begin{bmatrix} 2 \\ 0 \end{bmatrix}$ is mapped onto itself. This is also true for the vector $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$, so there will be $|2 \cdot 2 - 0 \cdot 0| = 4$ miniatures orientated horizontally and vertically.

As we saw in Figure 2.1 the 289x289 pixels image appears to be upside down after 153 iterations. This can be considered as a special case of miniatures but with only one miniature occurring whose orientation is determined by the column vectors of $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. Actually, the full image is not rotated, since the pixels with $y$-coordinate 0 will not be mapped to $y = N - 1$. This can be seen in Figure 4.9. The fact that the full image is not rotated is also elementary when considering that $(0,0)$ is a trivial point.

Figure 4.9: A rotated image occurring after 7 iterations of Arnold’s cat map on a 13x13 pixels image
5 Pell’s cat map

As we have seen, Arnold’s cat map with $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ and the two types of generalized cat maps with $G_1 = \begin{bmatrix} 1 & a \\ \frac{1}{a} & 2 \end{bmatrix}$ and $G_2 = \begin{bmatrix} b & a \\ \frac{b}{a} & b+1 \end{bmatrix}$, all have determinant 1. Taking the generalization of the cat map even further we can also allow for matrices with negative unit determinant.

A discrete mapping using the matrix $P = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ with determinant $-1$ is still area preserving but also orientation reversing. As it turns out the matrix $P$ will generate numbers in the Pell\textsuperscript{15} and half-companion Pell sequences, so $P$ together with the modulo $N$ operation will henceforth be denoted Pell’s cat map, $\Gamma_P : \mathbb{Z}_N \times \mathbb{Z}_N \rightarrow \mathbb{Z}_N \times \mathbb{Z}_N$ where

$$\Gamma_P \left( \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \right) = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}.$$

The effect of Pell’s cat map on an image is shown in Figure 5.1. With the corresponding notations so far used for the period and the minimal period of Arnold’s cat map we can conclude that $\Pi_P(289) = 272$, which is notably not the same as $\Pi_A(289) = 306$ from Figure 2.1.

As we can see from the numerical results depicted in Figure 5.2, and comparing this with Figure 4.1, the minimal periods of Pell’s cat map and of Arnold’s cat map are generally not the same.

\textsuperscript{15}After J. Pell 1611-1685
From Theorem 4.7 we know that the upper bound for the period of Arnold’s cat map is \( \Pi_A(N) = 3N \), for Pell’s cat map our numerical results suggest that the upper bound is \( \Pi_P(N) = \frac{8N}{3} \). The remainder of this section will be devoted to proving that this is true for all \( N \geq 2 \). We will also state four conjectures regarding properties of Pell’s cat map at the very end of this section.

### 5.1 Defining Pell’s cat map

**Definition 5.1.** Let the \( n \)th number of the Pell sequence be defined to be \( P_n = 2P_{n-1} + P_{n-2} \) with \( P_0 = 0 \) and \( P_1 = 1 \).

Just like the Fibonacci sequence, the Pell sequence is a linear recurrence relation of order 2. The first numbers of the Pell sequence are 0, 1, 2, 5, 12, 29, 70, 169, 408, 985, . . .

If we also allow negative indices for the Pell numbers we have that \( P_{-1} = 1 \). This condition is essential in the forthcoming proofs.

**Remark 5.2.** The connection between the Pell sequence and Pell’s equations is that \( x_n = P_{2n} + P_{2n-1} \) and \( y_n = P_{2n} \) are solutions to the equation \( x_n^2 - 2y_n^2 = 1 \).

We also have a sequence of numbers denoted \( H_n \) being the half-companion Pell sequence\(^{16}\) defined to be \( H_n = 2H_{n-1} + H_{n-2} \) where \( H_0 = 1 \) and \( H_1 = 1 \), so the first numbers in this sequence are 1, 1, 3, 7, 17, 41, 99, 239, 577, 1393, . . .

Powers of the matrix \( P \) can be expressed using numbers from the Pell and

\(^{16}\) This is half the value of the *companion Pell* or *Pell-Lucas sequence* defined to be \( Q_n = 2Q_{n-1} + Q_{n-2} \) where \( Q_0 = 2 \) and \( Q_1 = 2 \)
half-companion Pell sequences in the following way

\[ P^n = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^n = \begin{bmatrix} H_n & P_n \\ 2P_n & H_n \end{bmatrix}, \]

hence the first powers of the matrix \( P \) are

\[ P^2 = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}, \quad P^3 = \begin{bmatrix} 7 & 5 \\ 10 & 7 \end{bmatrix}, \quad P^4 = \begin{bmatrix} 17 & 12 \\ 24 & 17 \end{bmatrix}, \quad P^5 = \begin{bmatrix} 41 & 29 \\ 58 & 41 \end{bmatrix}, \ldots \]

Moreover, it is also possible to use exclusively Pell numbers, so

\[ P^n = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^n = \begin{bmatrix} H_n & P_n \\ 2P_n & H_n \end{bmatrix} = \begin{bmatrix} P_n + P_{n-1} & P_n \\ 2P_n & P_n + P_{n-1} \end{bmatrix}, \]

this is the form used hereinafter.

The characteristic polynomial of \( P \) is \( \lambda^2 - 2\lambda - 1 \), so the discriminant \( D = 8 \) and the two eigenvalues\(^{17} \) are \( \lambda_1 = 1 + \sqrt{2} \approx 2.414214 \) and \( \lambda_2 = 1 - \sqrt{2} \approx -0.414214 \). Since both of the eigenvalues are different from one, Pell’s cat map is a hyperbolic toral automorphism, just like Arnold’s cat map. Since \( P \) is not a symmetric matrix the eigenvectors are not orthogonal.

The effect of Pell’s cat map on the unit square is shown in Figure 5.3. Compare this to Figure 2.3 and note especially the orientation reversing characteristics of Pell’s cat map.

Besides the fact that the minimal periods of Arnold’s cat map and Pell’s cat map are not generally the same, it is of interest to point out a few other differences between the two.

Unlike Arnold’s cat map, Pell’s cat map has two trivial points whenever \( N \) is even. Besides \((0, 0)\), the point \((N/2, 0)\) is then also trivial since

\[ \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} N/2 \\ 0 \end{bmatrix} = \begin{bmatrix} N/2 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} N/2 \\ 0 \end{bmatrix} \pmod{N}. \]

Studying Arnold’s cat map we saw that, for all prime numbers except \( p = 5 \), all non-trivial points have the same orbit length. This is not the case for Pell’s

\[^{17}1 + \sqrt{2} \text{ is also known as the silver ratio}\]
cat map, where numerical results suggests that, for about half of the prime numbers of the form \(8k \pm 1\), the non-trivial points has more than one orbit length. Figure 5.4 shows the orbit lengths for the prime numbers \(p = 5\) and \(p = 7\).

![Figure 5.4: Orbit lengths of the points for Pell’s cat map for the prime numbers \(p = 5\) and \(p = 7\)](image)

Figure 5.4 shows the orbit lengths of the points for Pell’s cat map for the prime numbers \(p = 5\) and \(p = 7\).

In Figure 5.6 we can see that the orbit of the point \((1, 1)\) under Pell’s cat map is not the same as for Arnold’s cat map depicted earlier in Figure 4.3. The orbit length for \((1, 1)\) is 8, the same value as \(\Pi_P(6)\).

![Figure 5.6: The orbit of the point \((1,1)\) for Pell’s cat map with \(N = 6\)](image)
5.2 Some results from elementary number theory

For the proof of the theorem for the upper bound of the minimal period of Pell’s cat map, and the lemmas leading up to it, we firstly need some results from elementary number theory found in [17] by Rosen and in [16] by Ribenboim.

Definition 5.3. Let $a$ be an integer and $p$ an odd prime number. The Legendre symbol is defined to be

$$\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p} \\
-1 & \text{if } a \text{ is a quadratic nonresidue modulo } p.
\end{cases}$$

We may also adopt the convention that $\left( \frac{a}{p} \right) = 0$ when $p$ divides $a$.

Example 5.4. So $\left( \frac{2}{7} \right) = 1$ since $3 \cdot 3 = 9 \equiv 2 \pmod{7}$.

Note that the congruence $k^2 \equiv 2 \pmod{7}$ has not only the solution given above since we also have that $4 \cdot 4 = 16 \equiv 2 \pmod{7}$. The second solution $k_2$ can always be found by subtracting the first solution $k_1$ from $p$ since then

$$k_2^2 \equiv -k_1^2 \equiv (-1)^2k_1^2 \equiv k_1^2 \equiv a \pmod{p}.$$  

Theorem 5.5. Wilson’s theorem

If $p$ is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. An easy computation shows that if $p = 2$, then $(p-1)! = 1 \equiv -1 \pmod{2}$ and if $p = 3$, then $(p-1)! = 2 \equiv -1 \pmod{2}$. Now let $p$ be a prime number greater than 3. For each integer $a$ in $1 \leq a \leq p-1$ there exist an inverse $a^{-1}$ such that $aa^{-1} \equiv 1 \pmod{p}$.

Since 1 and $p-1$ are their own inverses modulo $p$ we can form pairs of all integers from 2 to $p-2$ such that the product of each pair is congruent to 1 modulo $p$. If we multiply the result of all these pairs with 1 and $p-1$ we will get $1 \cdot 1 \cdot \ldots \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$. \qed

Example 5.6. Take $p = 5$, then $(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 \equiv -1 \pmod{5}$. This can also serve as an example of the forming of pairs congruent to 1 modulo $p$ made in the proof. Consider the pair $2 \cdot 3 = 6 \equiv 1 \pmod{5}$, it easy to see that $1 \cdot (2 \cdot 3) \cdot 4 \equiv 1 \cdot 1 \cdot (5-1) \equiv -1 \pmod{5}$.

The converse of Wilson’s theorem is also true, so it can actually be used to demonstrate that a number is composite.

Example 5.7. Take $p = 4$, then $(p-1)! = 1 \cdot 2 \cdot 3 = 6 \equiv 2 \pmod{4}$.

The proof of this is omitted here.

---

18 After A-M. Legendre 1752-1833. The Legendre symbol is also sometimes called the quadratic residue symbol
19 After J. Wilson 1741-1793
Theorem 5.8. **Euler’s criterion**\(^{20}\) Let \( a \) be an integer and \( p \) an odd prime number, then
\[
\left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p}.
\]

**Proof.** First assume that there exist an integer such that
\[
k^2 \equiv a \pmod{p},
\]
hence \( a \) is a quadratic residue modulo \( p \) and \( \left( \frac{a}{p} \right) = 1 \). Using Fermat’s little theorem we see that
\[
a^{(p-1)/2} = (k^2)^{(p-1)/2} = k^{p-1} \equiv 1 \pmod{p},
\]
so
\[
\left( \frac{a}{p} \right) = 1 \Rightarrow \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p}.
\]

If \( \left( \frac{a}{p} \right) = -1 \) then \( a \) is a quadratic nonresidue modulo \( p \) and the congruence \( k^2 \equiv a \pmod{p} \) has no solutions.

For each integer \( i \) co-prime to \( p \), there exists an integer \( j \) such that \( ij \equiv a \pmod{p} \). Since \( a \) is a quadratic nonresidue there exist no \( i \) such that \( i^2 \equiv a \pmod{p} \). We can now group the residue classes modulo \( p \), i.e. the integers \( 1, 2, 3, \cdots, p-1 \) into \( (p-1)/2 \) pairs where each pair \( (i, j) \) has the product \( a \). Multiplying all these pairs together gives
\[
(p-1)! \equiv a^{(p-1)/2} \pmod{p}.
\]
Here we can use Wilson’s theorem
\[
(p-1)! \equiv -1 \pmod{p}
\]
to conclude that
\[
-1 \equiv a^{(p-1)/2} \pmod{p}.
\]
This completes the proof of Euler’s criterion. \( \square \)

**Example 5.9.** Let \( p = 7 \) and \( a = 3 \) then \( 3^{(7-1)/2} = 3^3 = 27 \equiv -1 \pmod{7} \), so \( \left( \frac{3}{7} \right) = -1 \) which gives that 3 is a quadratic nonresidue modulo 7.

The multiplicative properties of the Legendre symbol
\[
\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right),
\]
follows from Euler’s criterion, since if
\[
\left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p}, \quad \left( \frac{b}{p} \right) \equiv b^{(p-1)/2} \pmod{p}
\]
and
\[
\left( \frac{ab}{p} \right) \equiv ab^{(p-1)/2} \pmod{p},
\]
\(^{20}\)After L. Euler 1707-1783
we can conclude that
\[
\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv ab^{(p-1)/2} \equiv \left( \frac{ab}{p} \right) \pmod{p}.
\]

We will also need an expression for the \(n\)th Pell number, hence we show by induction that the Binet formula\(^{21}\) is valid for the Pell sequence \(P_n = 2P_{n-1} + P_{n-2}\) with \(P_1 = 1\) and \(P_2 = 2\).

**Theorem 5.10.** The \(n\)th Pell number is
\[
P_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} = \frac{\lambda_1^n - \lambda_2^n}{2\sqrt{2}}
\]
where \(\lambda_1 = 1 + \sqrt{2}\) and \(\lambda_2 = 1 - \sqrt{2}\) are the eigenvalues of the matrix \(P = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}\).

**Proof.** For \(n = 1\)
\[
P_1 = \frac{\lambda_1 - \lambda_2}{\lambda_1 - \lambda_2} = \frac{1 + \sqrt{2} - 1 + \sqrt{2}}{1 + \sqrt{2} - 1 + \sqrt{2}} = \frac{2\sqrt{2}}{2\sqrt{2}} = 1.
\]

For \(n = 2\)
\[
P_2 = \frac{\lambda_1^2 - \lambda_2^2}{\lambda_1 - \lambda_2} = \frac{(1 + \sqrt{2})^2 - (1 - \sqrt{2})^2}{1 + \sqrt{2} - 1 + \sqrt{2}} = \frac{3 + 2\sqrt{2} - 3 + 2\sqrt{2}}{2\sqrt{2}} = \frac{4\sqrt{2}}{2\sqrt{2}} = 2.
\]

For the induction assume that
\[
P_{n-1} = \frac{\lambda_1^{n-1} - \lambda_2^{n-1}}{2\sqrt{2}}
\]
and
\[
P_n = \frac{\lambda_1^n - \lambda_2^n}{2\sqrt{2}}.
\]

Then
\[
P_{n+1} = 2P_n + P_{n-1} = 2\left( \frac{\lambda_1^n - \lambda_2^n}{2\sqrt{2}} \right) + \frac{\lambda_1^{n-1} - \lambda_2^{n-1}}{2\sqrt{2}} = \frac{2\lambda_1^n - 2\lambda_2^n + \lambda_1^{n-1} - \lambda_2^{n-1}}{2\sqrt{2}} = \frac{2\lambda_1^n + \lambda_1^{n-1} - 2\lambda_2^n - \lambda_2^{n-1}}{2\sqrt{2}} = \frac{\lambda_1^{n-1}(1 + 2\lambda_1) - \lambda_2^{n-1}(1 + 2\lambda_2)}{2\sqrt{2}} = \frac{\lambda_1^{n-1}(3 + 2\sqrt{2}) - \lambda_2^{n-1}(3 - 2\sqrt{2})}{2\sqrt{2}} = \frac{\lambda_1^{n+1} - \lambda_2^{n+1}}{2\sqrt{2}}.
\]

\(^{21}\)After J. Binet 1786-1856
5.3 A partition of the prime numbers

Using the Legendre symbol we divide the prime numbers into three disjoint sets

i. \( p = 2 \)

ii. The set \( R \) consisting of all prime numbers of the form \( 8k + 1 \)

From [16] we have that 2 is a quadratic residue modulo \( p \) for prime numbers of this form, hence

\[
R = \left\{ p \mid \left( \frac{2}{p} \right) = 1 \right\} \text{ using that } \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}.
\]

In the proof of Lemmas 5.16, 5.17 and Theorem 5.19, any prime number in this set will be denoted by \( r \), so we have that \( r \in R \).

iii. The set \( S \) will be all prime numbers of the form \( 8k + 3 \)

For prime numbers of this form, 2 is a quadratic nonresidue modulo \( p \), so

\[
S = \left\{ p \mid \left( \frac{2}{p} \right) = -1 \right\},
\]

and \( s \in S \). Note that this set will also include \( p = 5 \), that for Arnold’s cat map had to be treated separately.

This division of the prime numbers agrees exactly with the second supplementary law of quadratic reciprocity first proved by Euler.

The law of quadratic reciprocity tells us the connection between the existence of a solution to the congruence \( k^2 \equiv q \pmod{p} \) and the possibility to solve \( k^2 \equiv p \pmod{q} \) where \( p \) and \( q \) are odd prime numbers and \( p \neq q \). It was formulated and proved by Euler, Legendre and Gauss in the study of quadratic Diophantine equations. The second supplementary law of quadratic reciprocity tells us that the congruence \( k^2 \equiv 2 \pmod{p} \) is solvable if and only if \( p \equiv \pm 1 \pmod{8} \).

Remark 5.11. Pell’s equation \( x^2 - ny^2 = 1 \) is a quadratic Diophantine equation, mistakenly named after Pell by Euler.

We say earlier that for Arnold’s cat map we related the prime numbers to the discriminant of the characteristic polynomial of the matrix \( A \). One might ask why we are not doing so here too where the discriminant is 8. However if 8 is a quadratic residue modulo \( p \) then so is 2. This follows from the multiplicative properties of the Legendre symbol

\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right),
\]

so

\[
\left( \frac{8}{p} \right) = 1 \Rightarrow \left( \frac{2}{p} \right) \left( \frac{2}{p} \right) = 1 \Rightarrow \left( \frac{2}{p} \right) = 1.
\]

\[22\text{C. F. Gauss 1777-1855} \]
5.4 The upper bound for the minimal period of Pell’s cat map

Here we will extend results regarding Arnold’s cat map to derive an explicit expression for the upper bound for the minimal period of Pell’s cat map. The first thing that we can conclude about the minimal period of Pell’s cat map is that, due to the orientation reversing properties of the $P$ matrix, it must always be even. This is not the case for Arnold’s cat map where both even and odd minimal periods occur, for example, $\Pi_A(18) = 12$ and $\Pi_A(19) = 9$.

To find the minimal period of Pell’s cat map we are looking for the number of iterations necessary such that the $n$th Pell number is congruent to $0 \pmod{N}$ and the $(n-1)$th Pell number is congruent to $1 \pmod{N}$.

Besides the results from Subsections 5.2 and 5.3 we will also need the two following lemmas from Ribenboim [16].

**Lemma 5.12.** For numbers in the Pell sequence $P_n^2 - P_{n-1}P_{n+1} = (-1)^{n-1}$.

This is also known as Cassini’s identity.

**Lemma 5.13.** The relationship $P_{i+j} = P_iP_{j+1} + P_{i-1}P_j$ is true for numbers in the Pell sequence.

The two lemmas can be proved by induction.

**Lemma 5.14.** For $p = 2$ the minimal period of Pell’s cat map $\Pi_P(2) = 2$.

*Proof.* By direct computation we have that
\[
\begin{bmatrix}
1 & 1 \\
2 & 1
\end{bmatrix}^2 = \begin{bmatrix}
3 & 2 \\
4 & 3
\end{bmatrix} \equiv \begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix} \pmod{2}.
\]

**Remark 5.15.** For Arnold’s cat map we have that $\Pi_A(2) = \Pi_A(2^2) = \Pi_A(4) = 3$. This is not the case for Pell’s cat map since $\Pi_P(2) = 2 \neq \Pi_P(4) = 4$. This fact will be used later on in the proof of Theorem 5.19.

In the following we will use $\Psi_P(N)$ instead of $\Pi_P(N)$ with the same meaning and background as for Arnold’s cat map. If we can prove that $\Psi_P(N) \leq 8N/3$ we will also have proven that $\Pi_P(N) \leq 8N/3$ since $\Pi_P(N) \leq \Psi_P(N)$.

Furthermore we must utilize the division of the prime numbers made in Subsection 5.3. To shorten the notation we will write $r$ and $s$ without indices. Recall that $\lambda_1 = 1 + \sqrt{2}$ and $\lambda_2 = 1 - \sqrt{2}$ are the eigenvalues of the matrix $P = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$.

**Lemma 5.16.** For prime numbers $r$ such that $2$ is a quadratic residue modulo $r$ a period of Pell’s cat map $\Psi_P(r) = r - 1$.

*Proof.* We have $\lambda_1^p = (1 + \sqrt{2})^p$ and from the binomial theorem it follows that
\[
\lambda_1^p = \sum_{i=0}^{p} \binom{p}{i} (1)^{p-i} (\sqrt{2})^i \quad \pmod{p}.
\]

After G. D. Cassini 1625-1712
Except for the first and the last one, $p$ divides all the binomial coefficients, so these are congruent to 0 (mod $p$) and can therefore be dropped.

Repeating this calculation for $\lambda_2$ we have that $\lambda_2^p \equiv 1 - 2^{p/2}$ (mod $p$).

Using the Binet formula yields

$$P_p = \frac{\lambda_1^p - \lambda_2^p}{2\sqrt{2}} \equiv 2^{-1/2} \cdot 2^{p/2} \equiv 2^{(p-1)/2} \text{ (mod } p).$$

Since $r$ is chosen from the set of prime numbers such that 2 is a quadratic residue modulo $p$, it possible to use Euler’s criterion $(a^p)^{p}\equiv a^{(p-1)/2} \text{ (mod } p)$ to get $(2^r)^{r}\equiv 2^{(r-1)/2} \text{ (mod } r)$, and we can conclude that $(2^r)^{r}\equiv 1 \text{ (mod } r)$.

Using Cassini’s identity, $P^2 - P = (-1)^{n-1}$, and in this case, since $r-1$ is always even and $P_r \equiv 1$ (mod $r$), it must follow that $P_{r-1}P_{r+1} \equiv 0$ (mod $r$), so $r$ must divide at least one of $P_{r-1}$ and $P_{r+1}$.

Since it is elementary that $\lambda_1^{p+1} = \lambda_1^p \cdot \lambda_1$ and $\lambda_2^{p+1} = \lambda_2^p \cdot \lambda_2$, we once again use the Binet formula

$$P_{p+1} = \frac{(\lambda_1^p \cdot \lambda_1) - (\lambda_2^p \cdot \lambda_2)}{2\sqrt{2}}.$$

Together with our former results $\lambda_1^p \equiv 1 + 2^{p/2}$ (mod $p$) and $\lambda_2^p \equiv 1 - 2^{p/2}$ (mod $p$), this becomes

$$P_{p+1} \equiv \frac{(1 + 2^{p/2})(1 + \sqrt{2}) - (1 - 2^{p/2})(1 - \sqrt{2})}{2\sqrt{2}} \text{ (mod } p),$$

which after some calculation yields that $P_{p+1} \equiv 1 + 2^{(p-1)/2}$ (mod $p$). Since $2^{(r-1)/2} \equiv 1$ (mod $r$) we have $P_{r+1} \equiv 2$ (mod $r$) and hence we can conclude that $P_{r-1} \equiv 0$ (mod $r$).

We now have

$$P_r \equiv 1 \text{ (mod } r) \text{ and } P_{r-1} \equiv 0 \text{ (mod } r).$$

Inserting this into the relation $P_{i+j} = P_iP_{j+1} + P_{i-1}P_j$ with $i = n$, $j = r - 1$, we have

$$P_{n+r-1} = P_nP_r + P_{r-1}P_n+1 \equiv P_n \text{ (mod } r).$$
Since the definition of Pell sequence yields that \( P_0 = 0 \) and \( P_{-1} = 1 \), we can conclude that
\[
\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^0 = \begin{bmatrix} P_0 + P_{-1} \\ 2P_0 \\ P_0 + P_{-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.
\]
Therefore
\[
\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^{r-1} = \begin{bmatrix} P_0 + r - 1 + P_{-1} + r - 1 \\ 2P_0 + r - 1 \\ P_0 + r - 1 + P_{-1} + r - 1 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \pmod{r}.
\]
Hence \( \Psi_P(r) = r - 1 \) for all prime numbers \( r \) such that 2 is a quadratic residue modulo \( r \). \( \square \)

**Lemma 5.17.** For prime numbers \( s \) such that 2 is a quadratic nonresidue modulo \( s \), a period of Pell’s cat map \( \Psi_P(s) = 2(s + 1) \).

Proof. Let us once again apply the expression \( P_{p+1} \equiv 1 + 2^{(p-1)/2} \pmod{p} \) from the proof of Lemma 5.16. In this case, when \( 2^{(s-1)/2} \equiv -1 \pmod{s} \), we have that \( P_{s+1} \equiv 1 - 1 \equiv 0 \pmod{s} \).

Recalling that \( P_{i+j} = P_iP_{j+1} + P_{-1}P_j \), this time setting \( i = s + 1, j = n \), we can conclude
\[
P_{s+n} = P_{s+1}P_{n+1} + P_{-1}P_n \equiv -P_s \pmod{s},
\]
and setting \( n = 0 \) leads to
\[
\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^{s+1} = \begin{bmatrix} P_{s+1} + P_{-1+s+1} \\ 2P_{s+1} \\ P_{s+1} + P_{-1+s+1} \end{bmatrix} \equiv \begin{bmatrix} -P_0 - P_{-1} \\ -2P_0 \\ -P_0 - P_{-1} \end{bmatrix} \equiv \begin{bmatrix} -1 \\ 0 \\ -1 \end{bmatrix} \pmod{s}.
\]
Obviously
\[
\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^{2(s+1)} \equiv \begin{bmatrix} -1 \\ 0 \\ -1 \end{bmatrix}^2 \equiv \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \pmod{s}.
\]
Hence \( \Psi_P(s) = 2(s + 1) \) for all prime numbers \( s \) such that 2 is a quadratic nonresidue modulo \( s \). \( \square \)

To compute a period for any power of the prime factors of \( N \), we will apply the following lemma from [13] by Hardy and Wright.

**Lemma 5.18.** If \( m \equiv 1 \pmod{p^\sigma} \) and \( \sigma \geq 1 \) then \( m^p \equiv 1 \pmod{p^{\sigma+1}} \).

The proof is omitted here.

**Theorem 5.19.** The upper bound for the minimal period of Pell’s cat map is \( 8N/3 \).
Proof. This proof builds on the proof of Theorem 4.7 given in [9], but here we must apply the aforegoing Lemmas 5.14, 5.16, 5.17, 5.18 and Remark 5.15.

From the Fundamental Theorem of Arithmetic we have that any integer \( N \) can be uniquely factorized as a product of powers of prime numbers, so

\[
N = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot 7^{a_7} \cdot 11^{a_{11}} \cdot \ldots = \prod_{i=1}^{k} p_i^{a_i}.
\]

Using the partition of the prime numbers into the three types \( p = 2 \), \( R = \{ p \mid \left(\frac{2}{p}\right) = 1\} \) and \( S = \{ p \mid \left(\frac{2}{p}\right) = -1\} \) from Subsection 5.3, any integer \( N \) can be written as

\[
N = 2^\gamma \left( \prod_{r \in R} r^{\alpha_r} \right) \left( \prod_{s \in S} s^{\beta_s} \right).
\]

Using lemma 5.18, setting \( m = k^{r-1} \) and \( \sigma = 1 \), we have that if \( k^{r-1} \equiv 1 \pmod{r} \) then \( k^{(r-1)r} \equiv 1 \pmod{r^2} \), repeating this and inserting \( \alpha \geq 2 \) yields that

\[
k^{r-1} \equiv 1 \pmod{r} \Rightarrow k^{(r-1)r^{\alpha_r-1}} \equiv 1 \pmod{r^{\alpha_r}}.
\]

Likewise,

\[
k^{2(s+1)} \equiv 1 \pmod{s} \Rightarrow k^{2(s+1)s^{\beta_s-1}} \equiv 1 \pmod{s^{\beta_s}}.
\]

Just as for Arnold’s cat map in [9] we can now make use of the properties of the least common multiple to get an explicit expression for a period of Pell’s cat map for any composite number \( N \),

\[
\Psi_P(N) = \text{lcm} \left( 2^\gamma, \prod_{r \in R} (1 - r^{-1}), \prod_{s \in S} 2(s+1)s^{\beta_s-1} \right).
\]

Since

\[
\text{lcm} \ (a, b) = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}
\]

for any two integers \( a = \prod_{i=1}^{k} p_i^{a_i} \) and \( b = \prod_{i=1}^{k} p_i^{b_i} \),

we must have that

\[
\frac{\Psi_P(N)}{N} = \left( \prod_{r \in R} (1 - r^{-1}) \right) \left( \prod_{s \in S} 2(1 + s^{-1}) \right) \left( \prod_{p|\Psi_P(N)} p^{-k_p} \right),
\]

where \( k_p \) is the total number of powers of any prime number \( p \) that appear redundantly in the terms of the expression for \( \Psi_P(N) \).

To find the largest possible ratio \( \Psi_P(N)/N \) it is evident that we must choose prime factors \( s \) from the set \( S = \{ p \mid \left(\frac{2}{p}\right) = -1\} \). Note that all factors \( 2(s+1) \) are divisible by 4, so if we choose just one prime factor from the set \( S \) then \( k_2 = 0 \). However choosing two prime factors from \( S \) will result in \( k_2 = 2 \) and so on, which will reduce \( \Psi_P(N)/N \).
To maximize $\Psi_P(N)/N$ we must choose only one prime number $s$ such that the factor $2(1 + s^{-1})$ becomes as large as possible. It is now straightforward that we must choose the smallest possible prime number in $S$ i.e. 3, resulting in $\Psi_P(N)/N = 2(1 + 1/3) = 8/3$. The fact that $\Pi_P(N) \leq \Psi_P(N)$ completes the proof.

Example 5.20. To illustrate the computation of a period of Pell’s cat map we take $N = 49588 = 2^2 \cdot r_1^2 \cdot s_1 \cdot r_2^1$ where $r_1 = 7$, $s_1 = 11$ and $r_2 = 23$, so

$$\Psi_P(49588) = \text{lcm}(2^2 \cdot (7 - 1) \cdot 7, 2(11 + 1), (23 - 1)) = \text{lcm}(2^2, 2 \cdot 3 \cdot 7, 2^3 \cdot 3 \cdot 11) = (2^3 \cdot 3 \cdot 7 \cdot 11) = 1848.$$  

The prime numbers 2 and 3 appear redundantly in the expression $\Psi_P(49588) = \text{lcm}(2^2, 2 \cdot 3 \cdot 7, 2^3 \cdot 3 \cdot 11)$ resulting in $k_2 = 4$ and $k_3 = 1$, so the calculation of $\Psi_P(N)/N$ will be

$$\Psi_P(49588) = \frac{6}{7} \cdot \frac{24}{23} \cdot \frac{22}{11} \cdot \frac{2^{-4} \cdot 3^{-1}}{49588} = \frac{1848}{49588} \approx 0.037.$$  

Calculating the minimal period numerically for $N = 49588$ we have that $\Pi_P(49588) = 1848 = \Psi_P(49588)$. This agrees well with the fact that there are no short prime numbers in the factorization of 49588.

As indicated above we will, in a similar way as for Arnold’s cat map, from time to time encounter short prime numbers, and hence also composite numbers, such that in $\Pi_P(N) < \Psi_P(N)$. For Pell’s cat map we have for example $\Pi_P(29) = 20 \neq \Psi_P(29) = 60$ and $\Pi_P(41) = 10 \neq \Psi_P(41) = 40$. As we saw earlier for Arnold’s cat map we had that $\Pi_A(29) = 7 \neq \Psi_A(29) = 14$ but $\Pi_A(41) = \Psi_A(41) = 20$ so the set of short prime numbers are not the same for Pell’s and Arnold’s cat maps. In Figure 5.7 the presence of short prime numbers can be seen below the two prominent lines $2(p+1)$ and $(p-1)$.

![Figure 5.7: Minimal periods of Pell’s cat map for 2 ≤ p ≤ 5000](image)

For $5 < p < 50000$ we find that approximately 34% (1756/5130) are short prime numbers for Pell’s cat map. With this sample size the short prime numbers are unevenly distributed between the prime numbers, with a more common occurrence in the set $R$, i.e. prime numbers $p$ for which 2 is a is a quadratic residue modulo $p$. This uneven distribution can also be observed for Arnold’s cat map, with a higher frequency of short prime numbers such that the discriminant $D = 5$ is a quadratic residue modulo $p$, in the interval $5 < p < 50000$.  

26
For Pell’s cat map it is also possible to find Wall–Sun–Sun-type prime numbers, e.g. $\Pi_P(13) = \Pi_P(169) = 28$. From [10] $\Pi_P(p) = \Pi_P(p^2)$ is also true for $p = 31$ and $p = 1546463$. This is confirmed by a numerical verification. However, the existence of such prime numbers, does not inflict with the theorem for the upper bound for the minimal period of Pell’s cat map.

Just as for Arnold’s cat map in [9], we can sharpen the upper bound for the minimal period of Pell’s cat map further.\(^\text{24}\)

**Corollary 5.21.** For $k = 1, 2, 3, \ldots$ the minimal period of Pell’s cat map is

\[
\Pi_P(N) = \frac{8}{3}N \quad \text{when } N = 3^k,
\]

\[
\Pi_P(N) = \frac{12}{5}N \quad \text{when } N = 5^k,
\]

\[
\Pi_P(N) \leq \frac{24}{11}N \quad \text{for all other } N.
\]

**Proof.** This follows immediately from the proof of Theorem 5.19, taking the period lengths of the three lowest prime numbers $s = 3$, $s = 5$, and $s = 11$ from the set $S$ of prime numbers such that $2$ is a quadratic nonresidue modulo $p$. \(\square\)

### 5.5 An alternative mapping with the same period as Pell’s cat map

**Theorem 5.22.** The mapping

\[
\Gamma_{\text{AltP}} \left( \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \right) = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}
\]

will have the same minimal period as Pell’s cat map for all $N$.

**Proof.** Since we know that

\[
\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}^2 = \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}
\]

we can use the concept of *topological conjugacy* from [1] by Baake et al. to find a generalized cat map of type 1 or 2 with the same period as a mapping using the matrix $\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$.

To be topologically conjugate, and hence have the same minimal period for all $N$, the matrices must have the same determinant, trace and *matrix greatest common divisor* (mgcd), where the latter is defined to be $\gcd(b, c, d - a)$ for a 2 by 2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. So the generalized cat map of type 1 with $a = 2$, i.e. using the matrix $\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$, with determinant 6 and mgcd 2, will have the same minimal period for all $N$ as a mapping using $\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$.

What is left is to observe that

\[
\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}
\]

\(^{24}\)Compare this result to Figure 5.2
to conclude that the mappings $\Gamma_P$ with $\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$ and $\Gamma_{AltP}$ with $\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$ will have the same minimal period for all $N$.

Note that although the minimal periods are the same, properties such as the orbits will differ since the eigenvectors of the two matrices are not the same.

Assuming that Chen et al. will publish a full theory for the generalized cat map of type 1 and 2, as they claim in [6], their work could be used to give an alternative proof to Theorem 5.19 since Pell’s cat map will have exactly double the period as the type 1 generalized cat map with $a = 2$.

### 5.6 Conjectures regarding Pell’s cat map

Numerical results suggest that the following four conjectures hold.

**Conjecture 5.23.** The average value of the minimal period of Pell’s cat map is higher than that of Arnold’s cat map when $2 \leq N \leq \infty$.

So although the upper bound for the period of Pell’s cat map is lower than that of Arnold’s cat map we have the opposite when looking at the average minimal period. For $2 \leq N \leq 50000$ the average minimal period of Pell’s cat map is $0.371N$ while the corresponding value of Arnold’s cat map is $0.289N$.

**Conjecture 5.24.** For Pell’s cat map only prime numbers of the form $8k \pm 1$ can have more than one orbit length for the non-trivial points when $N$ is a prime number.

Studying Arnold’s cat map we saw that, except for $p = 5$, all non-trivial points have one and the same orbit length when $N$ is a prime number. This is not the case for the Pell’s cat map, where calculations suggests that, for about half of the prime numbers in the set $R = \left\{ p \mid \left( \frac{2}{p} \right) = 1 \right\}$, the non-trivial points have more than one orbit length.

**Conjecture 5.25.** Although the sets of short prime numbers are different for Arnold’s and Pell’s cat maps, the fraction of such numbers are asymptotically the same.

For prime numbers $5 < p < 50000$ we have $33\%$ short prime numbers for Arnold’s cat map and $34\%$ for Pell’s cat map.

**Conjecture 5.26.** There exists infinitely many Wall-Sun-Sun-type prime numbers for Pell’s cat map.

These are prime numbers such that $\Pi_P(p) = \Pi_P(p^2)$. Since we have numerically verified that this is true for the prime numbers $p = 13$, $p = 31$ and $p = 1546463$, we conjecture that there are infinitely many such numbers.
6 Applications

Abstract as the concept of the cat map may seem, several applications of it are not far-fetched. In the following section we shall briefly review some possible applications of Arnold’s cat map and its generalizations.

6.1 Encryption of images and text

One of the simplest possible ways to use Arnold’s cat map in a cryptographic context is to replace the color information of the individual pixel with a letter of the plaintext. A suitable number of iterations act as a transposition cipher producing a ciphertext where the seemingly unordered letters actually have an underlying order, enabling the holder of the key to retrieve the plaintext. Using a generalized cat map where the elements of the matrix are part of the key will complicate a cryptanalysis further. Figure 6.1 illustrates how the plaintext mathematics is not a spectator sport is encrypted as CTTT RAMEHSAO SITOA SOIAPT MCE TRNPS after two iterations of Arnold’s cat map.

![Figure 6.1: The plaintext and the resulting ciphertext after two iterations of Arnold’s cat map](image)

As aforementioned in Subsection 4.3, an image encryption system is proposed in [11], using an 8-dimensional cat map as a pseudo random number generator, where an initial point is part of the key and the output sequence is the chaotic looking orbit of that point.

6.2 Steganography, watermarks and image tampering detection

Steganography is the art of concealing a message within another message. This can also apply to images and be used to insert a watermarking into an image or to detect if an image has been altered in an unauthorized way i.e. image tampering detection.

This method utilize that a collection of neighboring pixels are spread across the surface of the \( N \times N \) pixels image after \( k \) iterations of Arnold’s cat map. The pixels of a relatively small watermark is spread across the larger image surface and, without being noticed, inserted into the image we want to mark. The image tampering detection algorithm iterates the image \( \Pi_{A}(N) - k \) times. The image appears chaotic but the watermark should appear intact if the image is unaffected. In [8] this method is used to detect the unwanted addition of three bananas into a picture of a baboon.
7 Conclusions

This thesis was intended to investigate some properties, and especially the period modulo $N$, of the two dimensional hyperbolic toral automorphism, strongly connected to the Fibonacci sequence, called Arnold’s cat map. This also included its generalizations with positive unit determinant. Doing so a novel mapping with negative unit determinant, called Pell’s cat map, was defined. The name was chosen due to the relationship with the sequence of Pell numbers.

The methods of the proof for the existence of an upper bound for the minimal period of Arnold’s cat map was carried over to this map and the main result of the thesis is hence a theorem stating that the minimal period of Pell’s cat map is always equal to or shorter than $8N/3$. Here $N$ is the number of rows or columns of the object e.g. an image, used to visualize the effects of the discrete-time dynamical system that the mapping induces.

However, the solution falls short of providing a closed form expression for the exact minimal period for all choices of $N$, since we lack a complete theory for the occurrence of what we referred to as short prime numbers. This is also true for Arnold’s cat map although the sets of such numbers are not one and the same.

From numerical results four conjectures regarding properties of Pell’s cat map was also stated. Indeed these conjectures demonstrates some of the differences found when trying to relate Pell’s cat map to Arnold’s cat map. Finding a proof for some or all of them could be the objective of further work concerning Pell’s cat map.

Such work could also include a closer look at the distribution of short prime numbers or an extended search for Wall-Sun-Sun-type prime numbers for Pell’s cat map, i.e. prime numbers for which $\Pi_P(p) = \Pi_P(p^2)$. As it is conjectured that if such number is found for Arnold’s cat map, then there must be infinitely many, so maybe it is likewise possible to find more than the three presented in this thesis for Pell’s cat map.

Some interesting applications of Arnold’s cat map within the cryptographic area were also briefly reviewed in this thesis, showing that the practical relevance of this area of mathematics is not so far-fetched as it may first appear.
References

   http://web.maths.unsw.edu.au/~jagr/BRW08.pdf
   (downloaded 140220)

   (downloaded 140116)

   http://journals.cambridge.org/action/displayAbstract?
   fromPage=online&aid=32347
   (downloaded 140118)

   http://www.fq.math.ca/Scanned/1-1/alfred1.pdf
   (downloaded 140501)

   http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6121983
   (downloaded 140116)

   http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6392276
   (downloaded 140116)

   (downloaded 140127)

   www.mdpi.com/1099-4300/15/8/3170/pdf
   (downloaded 140127)
http://www.jstor.org/stable/2324989
(downloaded 140118)

http://arxiv.org/pdf/1006.0824v1
(downloaded 140427)

http://link.springer.com/content/pdf/10.1140/epjst/e2014-02123-1
(downloaded 140322)

(downloaded 140130)


http://arxiv.org/abs/1111.2984v1
(downloaded 140116)

https://pub.uni-bielefeld.de/download/2508475/2508565
(downloaded 140127)


http://www.jstor.org/stable/2309169
(downloaded 140420)