Faculdade de Ciências da Universidade de Lisboa

Dynamics of the Arnold Cat Map

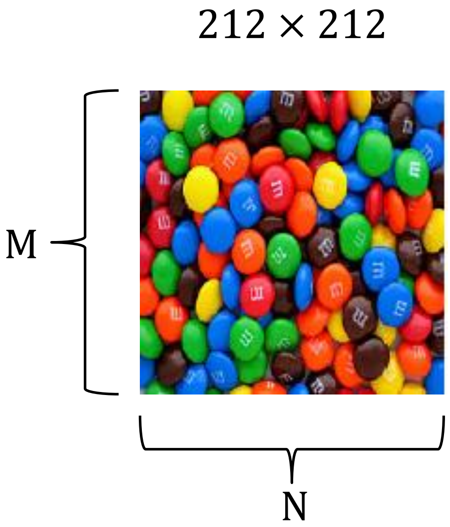
AUTHOR: CLÁUDIO SANTOS, 42208

SISTEMAS DINÂMICOS

JUNE 2017

1. Introduction: What is an image?

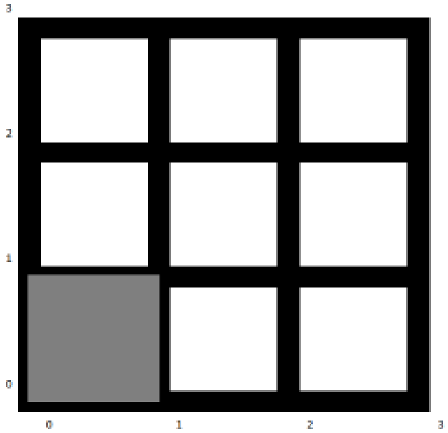
- An image is made of little squares called pixels.
- An image is an $M \times N$ matrix where each numeric value represents a colour code.

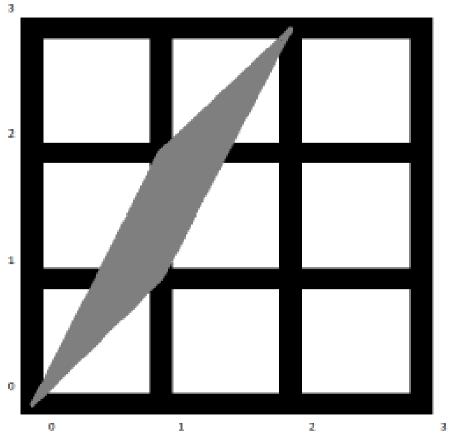


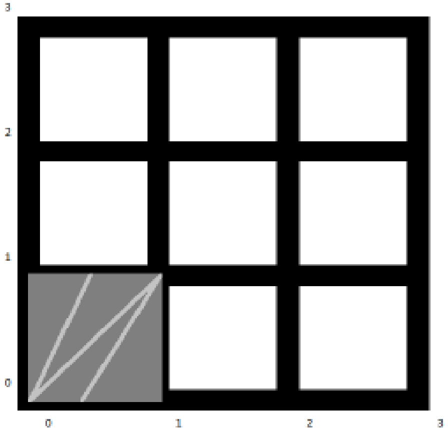
$$X = \begin{bmatrix} 139 & 70 & 77 & \cdots & 255 & 245 & 239 \\ 100 & 74 & 74 & \cdots & 254 & 253 & 251 \\ 98 & 159 & 156 & \cdots & 253 & 255 & 255 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 193 & 175 & 161 & \cdots & 220 & 220 & 220 \\ 219 & 181 & 156 & \cdots & 220 & 219 & 220 \\ 219 & 176 & 156 & \cdots & 218 & 219 & 219 \end{bmatrix}$$

1. Introduction: Geometric Idea

- An iteration of the Arnold cat map is the multiplication of all pixels coordinates by the matrix $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$, taking modulus equal to the side of the image.







- If iterated enough times, like some kind of magic, the original image reappers.

2. Arnold Cat Map Definition: Torus

- The Arnold cat map works on a two dimensional torus $\mathbb{T}^2$.
- However the torus can also be defined as $\mathbb{R}^2/\mathbb{Z}^2 := \{x+\mathbb{Z}^2 : x \in \mathbb{R}^2\}$.
- The cat map is a mapping $\Gamma_{cat} : \mathbb{T}^2 \to \mathbb{T}^2$ defined by $x \mapsto Ax(\mod \mathbb{Z}^2)$ where

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \qquad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

such that $a, b, c, d \in \mathbb{Z}^2$ are chosen with the following properties:

1. $|\det(A)| = 1$;
2. A tenha valores próprios $|\lambda_{\pm}| \neq 1$

2. Arnold Cat Map Definition: Discrete System

- The A matrix studied on this project is $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ and the dynamical system induced is

$$\Gamma_{cat}\left(\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod 1$$

- To use an image, we need to make a transition from the rational coordinates on $[0,1[$ to the integer coordinates $(0,1,2, \ldots, N-1)$ using the following commutative diagram

$$\Gamma_A\left(\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod N$$

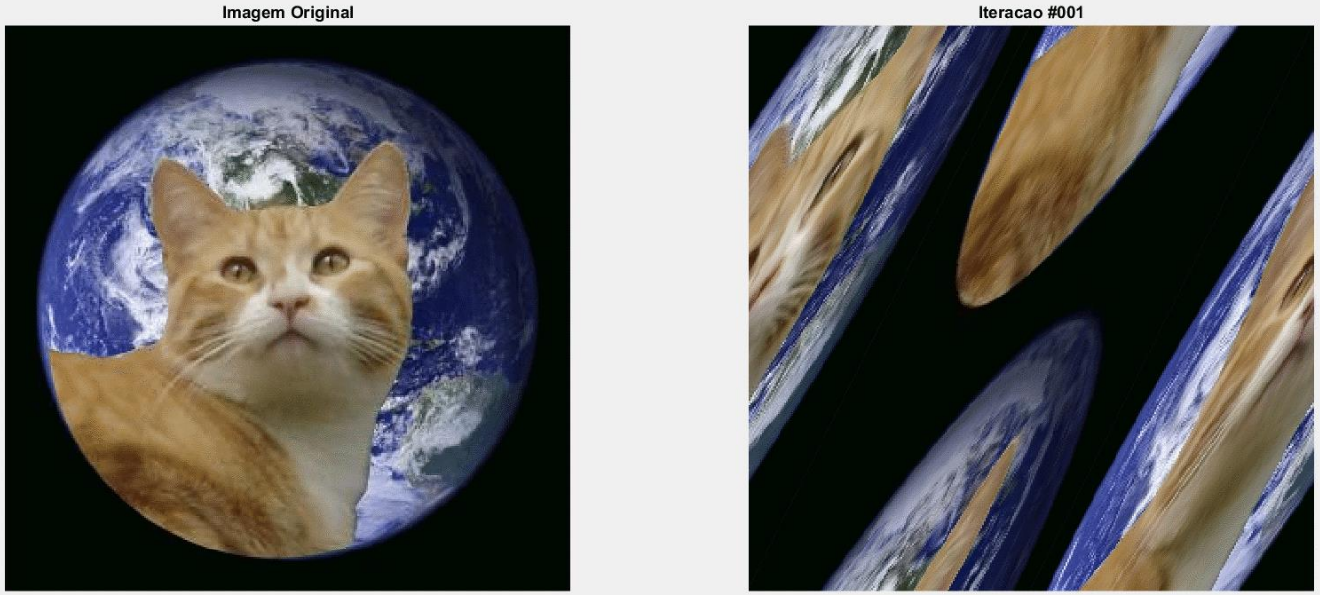
$$\begin{tikzcd} \mathbb{T}^2 \arrow[r, "\Gamma_{cat}"] \arrow[d, "\Phi"'] & \mathbb{T}^2 \arrow[d, "\Phi"] \\ \mathbb{Z}_N \times \mathbb{Z}_N \arrow[r, "\Gamma_A"] & \mathbb{Z}_N \times \mathbb{Z}_N \end{tikzcd}$$

2. Arnold Cat Map Definition: Minimal Period

- The characteristic polynomial is $\lambda^2 - \mathrm{Tr}(A)\lambda + \det(A) = \lambda^2 - 3\lambda + 1$ and the eigenvalues are $\lambda_1 = \frac{3+\sqrt{5}}{2} \approx 2,61803$ and $\lambda_2 = \frac{3-\sqrt{5}}{2} \approx 0,38167$.

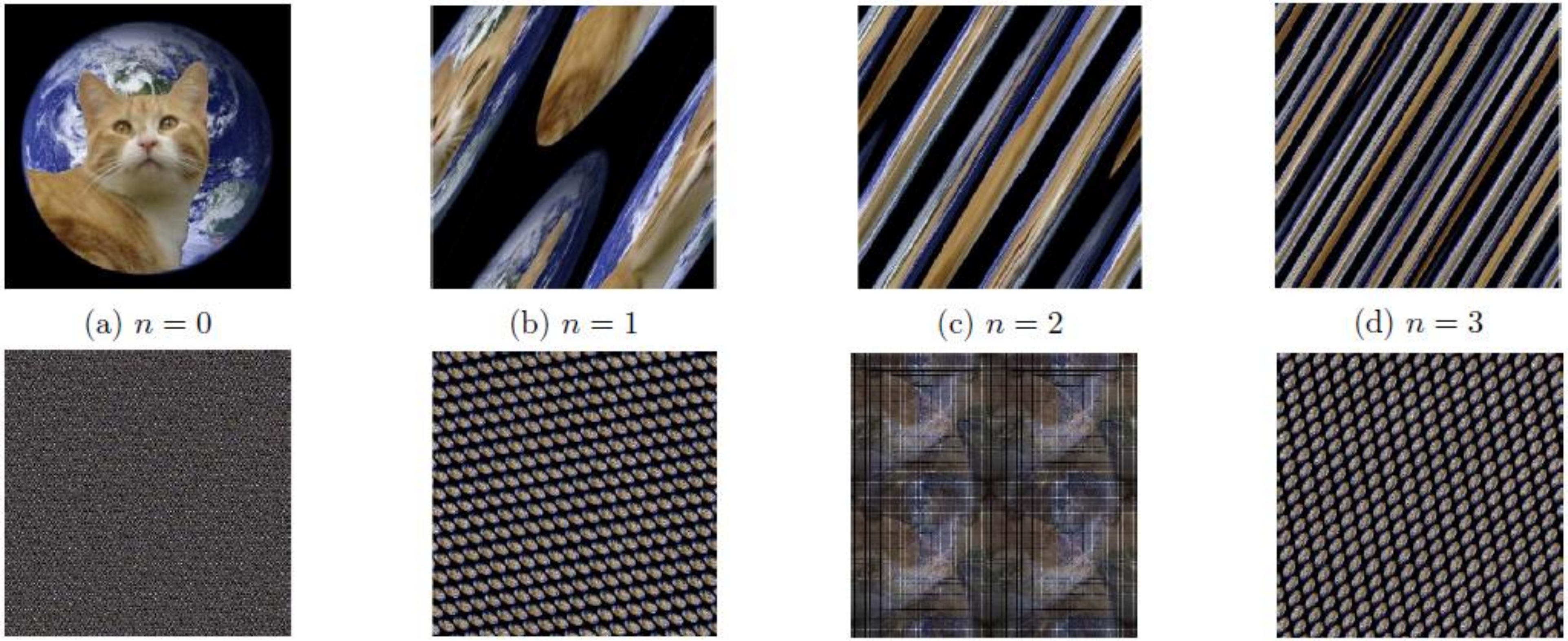
- **Definition 2.1.** The minimal period of the Arnold cat map is the smallest positive integer n such that $A^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ (mod\ N)$. It is defined by $\Pi_A(N)$ the minimal period of the discrete Arnold cat map.

2. Arnold Cat Map Definition: Animation



332×332

2. Arnold Cat Map Definition: Iterations

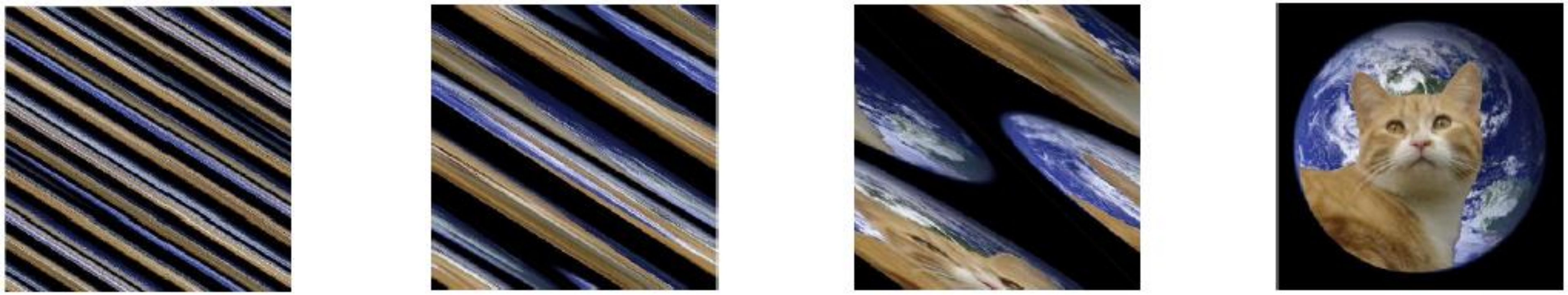


(a) $n = 0$ (b) $n = 1$ (c) $n = 2$ (d) $n = 3$

(e) $n = 6$ (f) $n = 23$ (g) $n = 42$ (h) $n = 61$

332×332

2. Arnold Cat Map Definition: Iterations



(i) $n = 81$ (j) $n = 82$ (k) $n = 83$ (l) $n = 84$

332×332

3. Connection between Arnold Cat Map and Fibonacci sequence

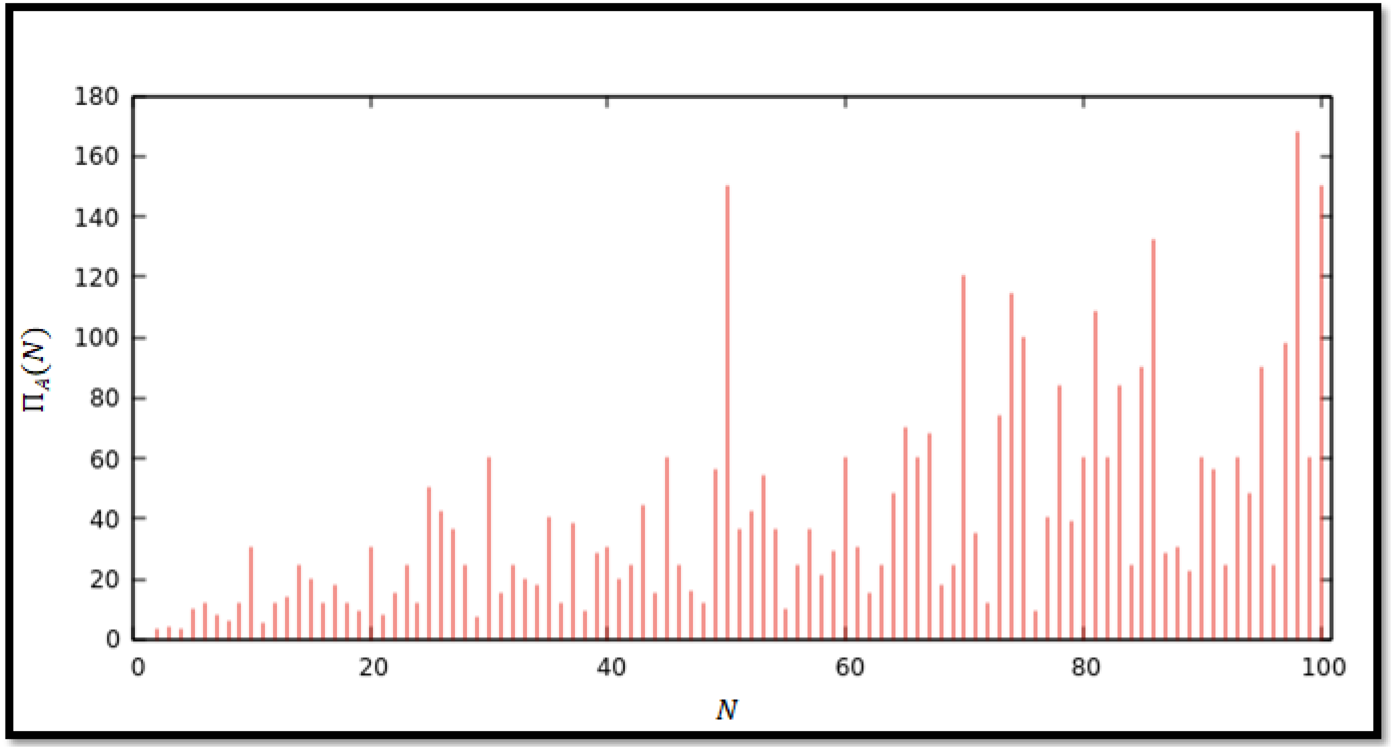
- **Definition 3.1.** Let n be the number of Fibonacci sequence defined by the recurring relation $F_n = F_{n-1} - F_{n-2}$ with $F_1 = 1$ and $F_0 = 0$.
- The first Fibonacci numbers are $0,1,1,2,3,5,8,13,21,34,55,89, \ldots$
- Power of the matrix $\mathrm{F} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} F_0 & F_1 \\ F_1 & F_2 \end{bmatrix}$ generate numbers Fibonacci sequence $F^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}$
- Since A and F have the relation

$$F^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = A$$

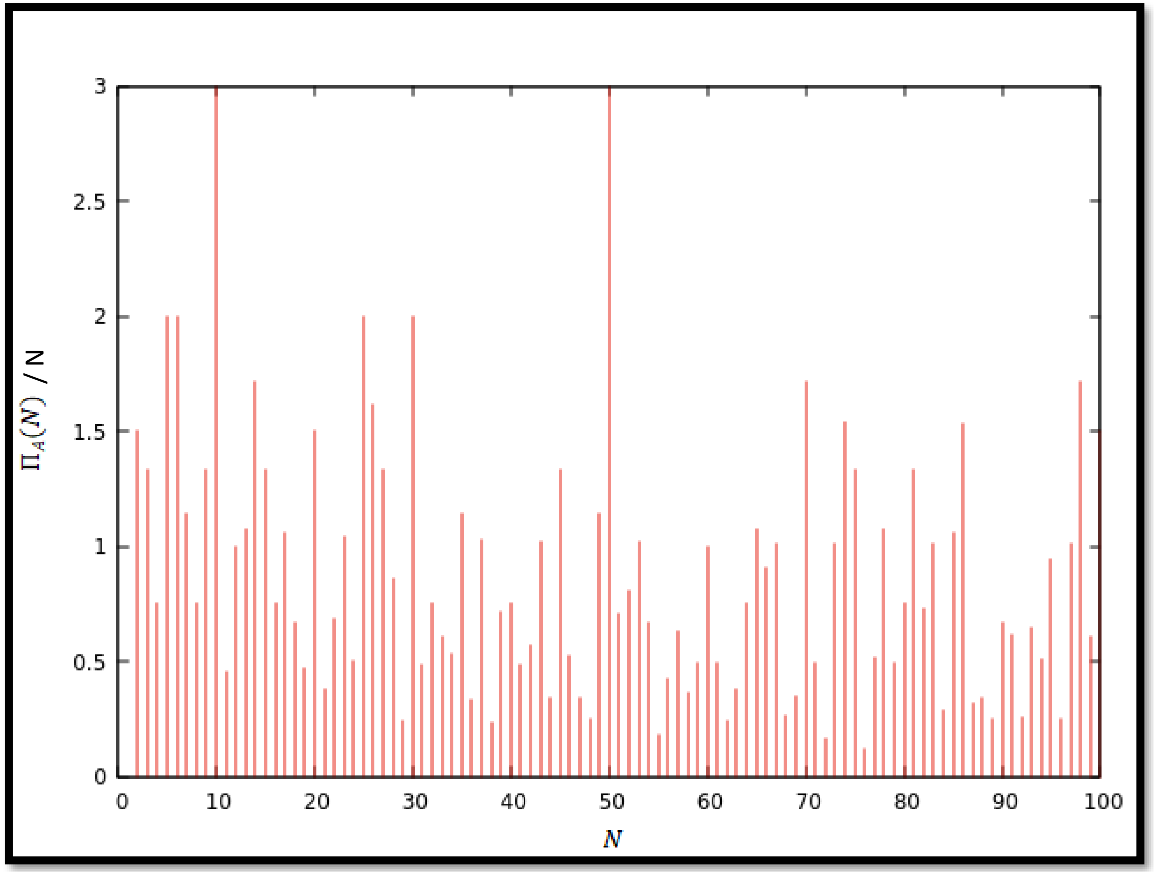
$$A^n = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^n = \begin{bmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 5 & 8 \\ 8 & 13 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 13 & 21 \\ 21 & 34 \end{bmatrix}, \quad A^5 = \begin{bmatrix} 34 & 55 \\ 55 & 89 \end{bmatrix}$$

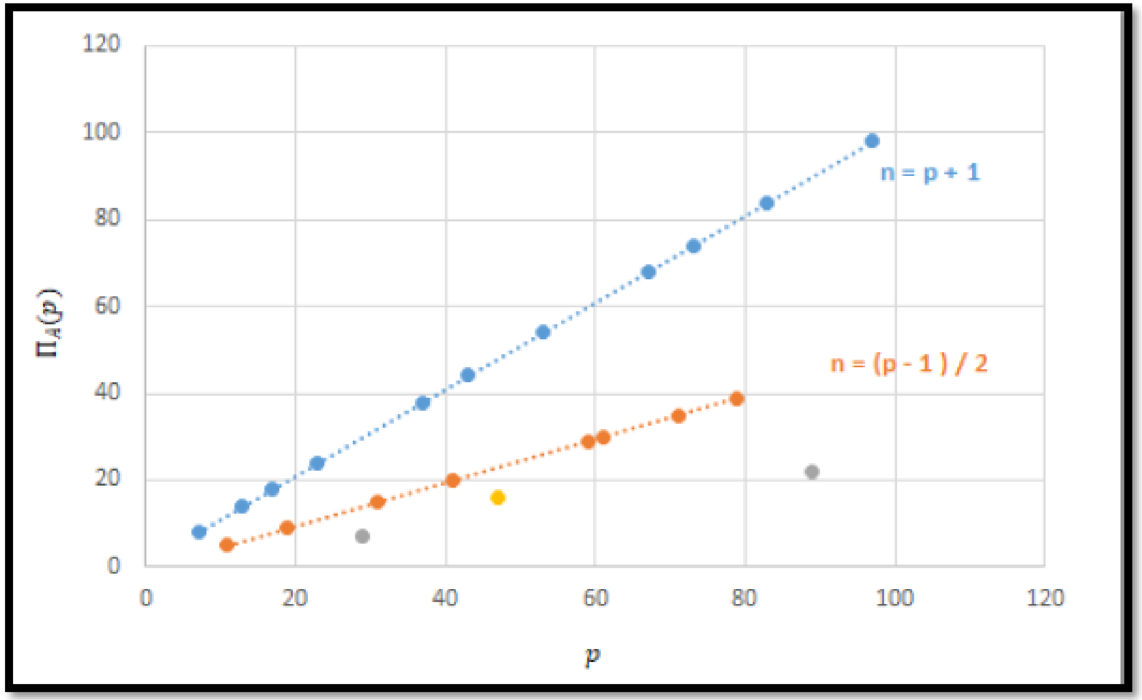
4. Properties of the Arnold Cat Map: Minimal Periods



4. Properties of the Arnold Cat Map: Minimal Periods



4. Properties of the Arnold Cat Map: Period Lenght



4. Properties of the Arnold Cat Map: Period Lenght

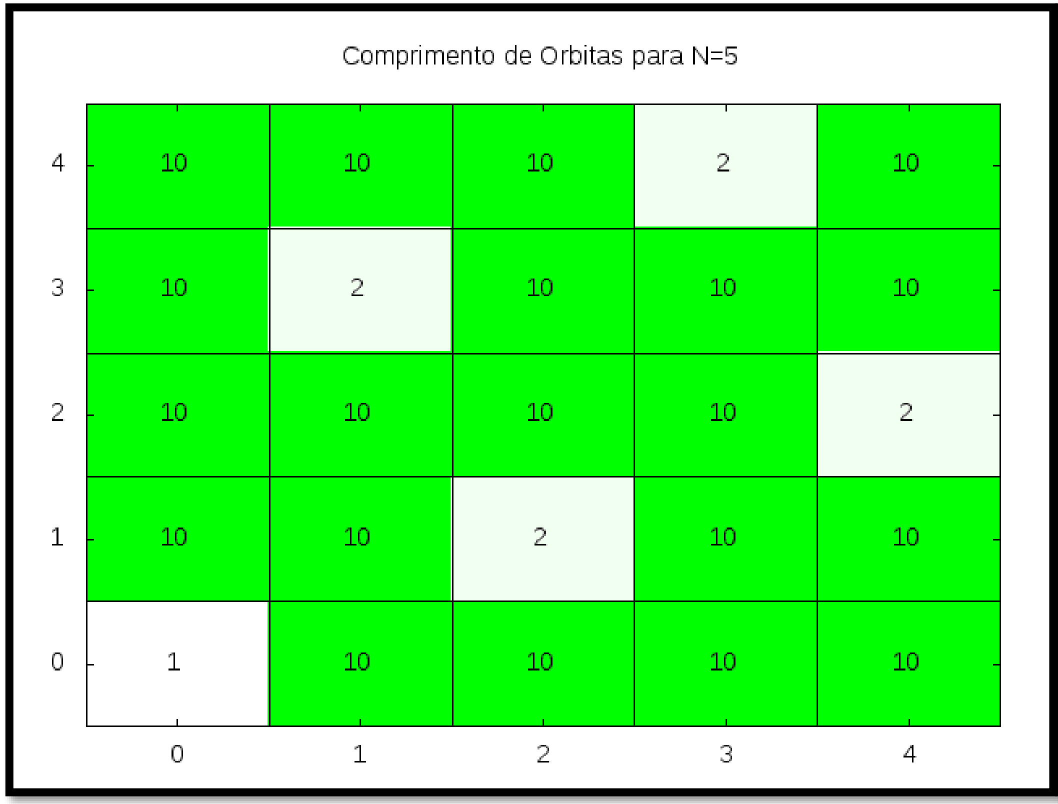
- **Theorem 4.1** If N has prime factorization $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ then $\Pi_A(N) = mmc\,(\Pi_A(p_1^{\alpha_1}), \Pi_A(p_2^{\alpha_2}), \dots, \Pi_A(p_k^{\alpha_k}))$
- **Example 4.2** $\Pi_A(21) = mmc\,(\Pi_A(3), \Pi_A(7)) = mmc\,(4, 8) = 8$
- **Example 4.3** $\Pi_A(N^2) = \Pi_A(N)$, $\Pi_A(6) = \Pi_A(36) = 12$
- The upper limit for the minimal Arnold cat map is $3N$. In particular, for $k = 1,2, \dots,$

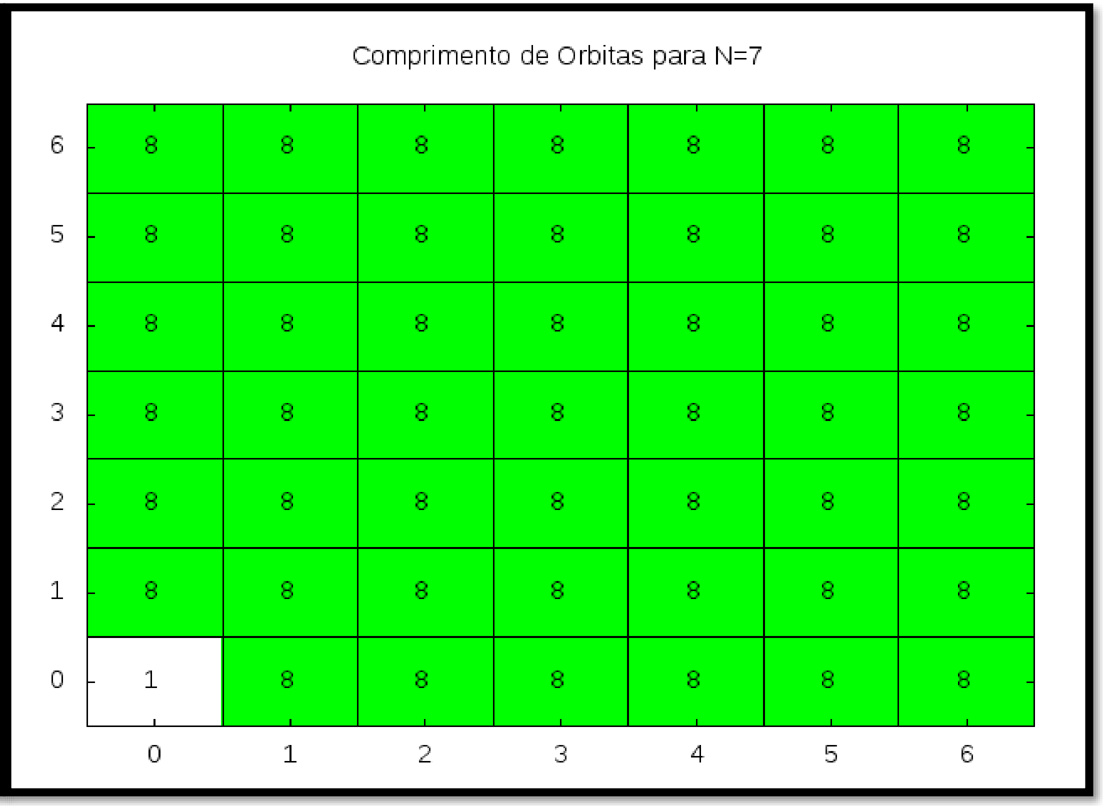
$$\begin{cases} \Pi_A(N) = 3N, & \text{if } N = 2 \cdot 5^k \\ \Pi_A(N) = 2N, & \text{if } N = 5^k \text{ or } N = 6 \cdot 5^k \\ \Pi_A(N) \lneq \frac{12}{7} N & \text{for any other } N \end{cases}$$

4. Properties of the Arnold Cat Map: Disjoint Orbits

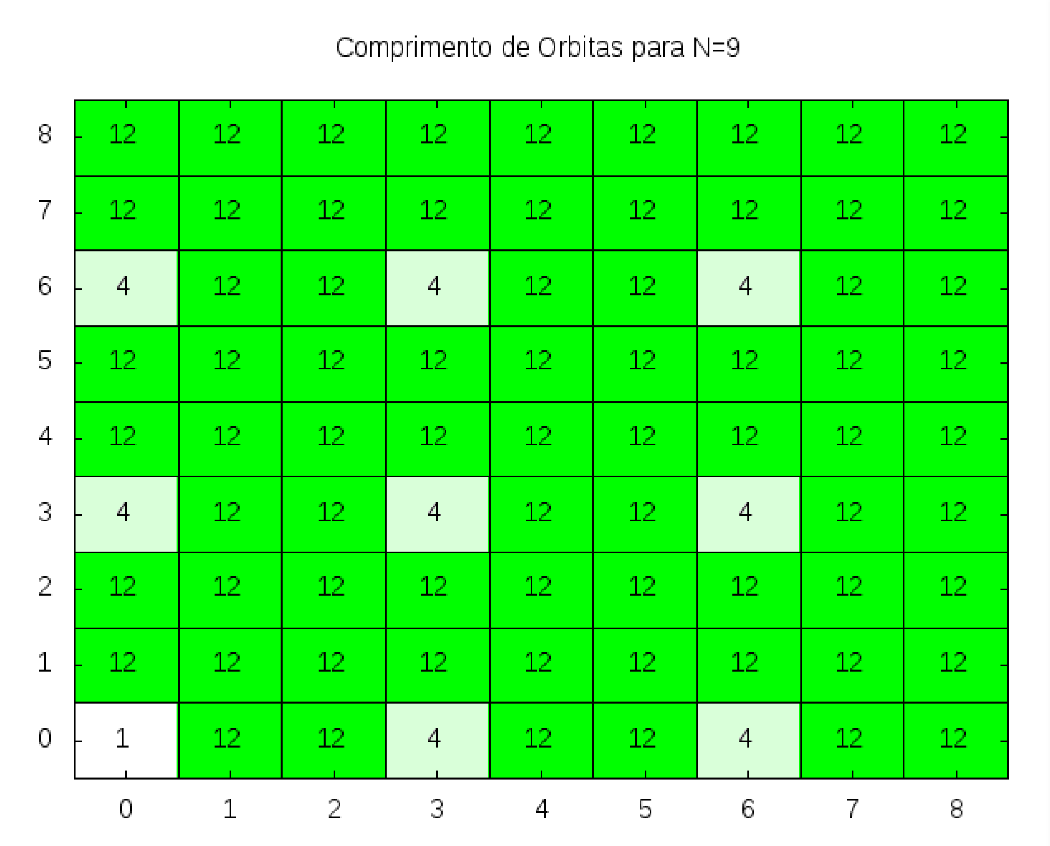
- **Definition 4.4** Let the orbit of a point defined as the pair of coordinates that na individual point assumes under iterations of the Arnold cat map until it returns to its original value. The number of unique points on this orbit gets the name of period lenght.
- Points with orbit lenght 1 are called fixed points. The origin $(0,0)$ is a fixed point.
- All the others are periodic with period lenght equal to the minimal period or a divisor of this.
- Na image is not dense over itself under the Arnold cat map!

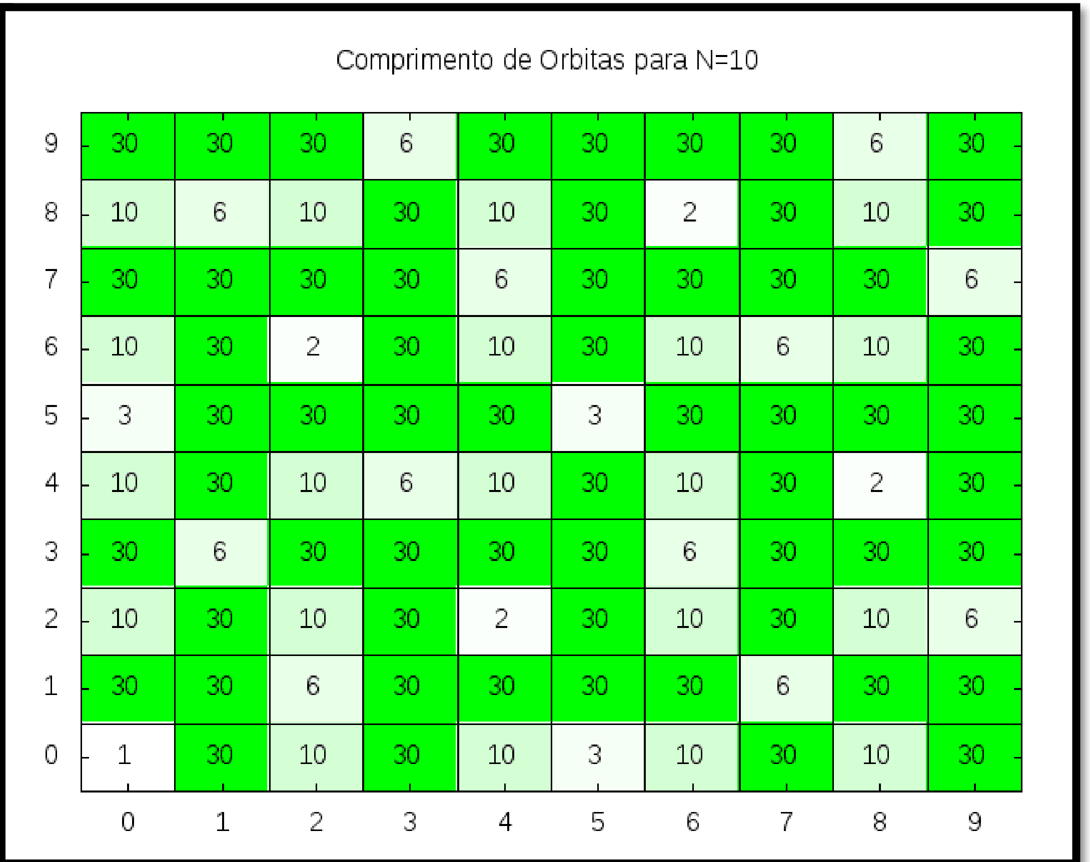
4. Properties of the Arnold Cat Map: Disjoint Orbits of Prime Numbers



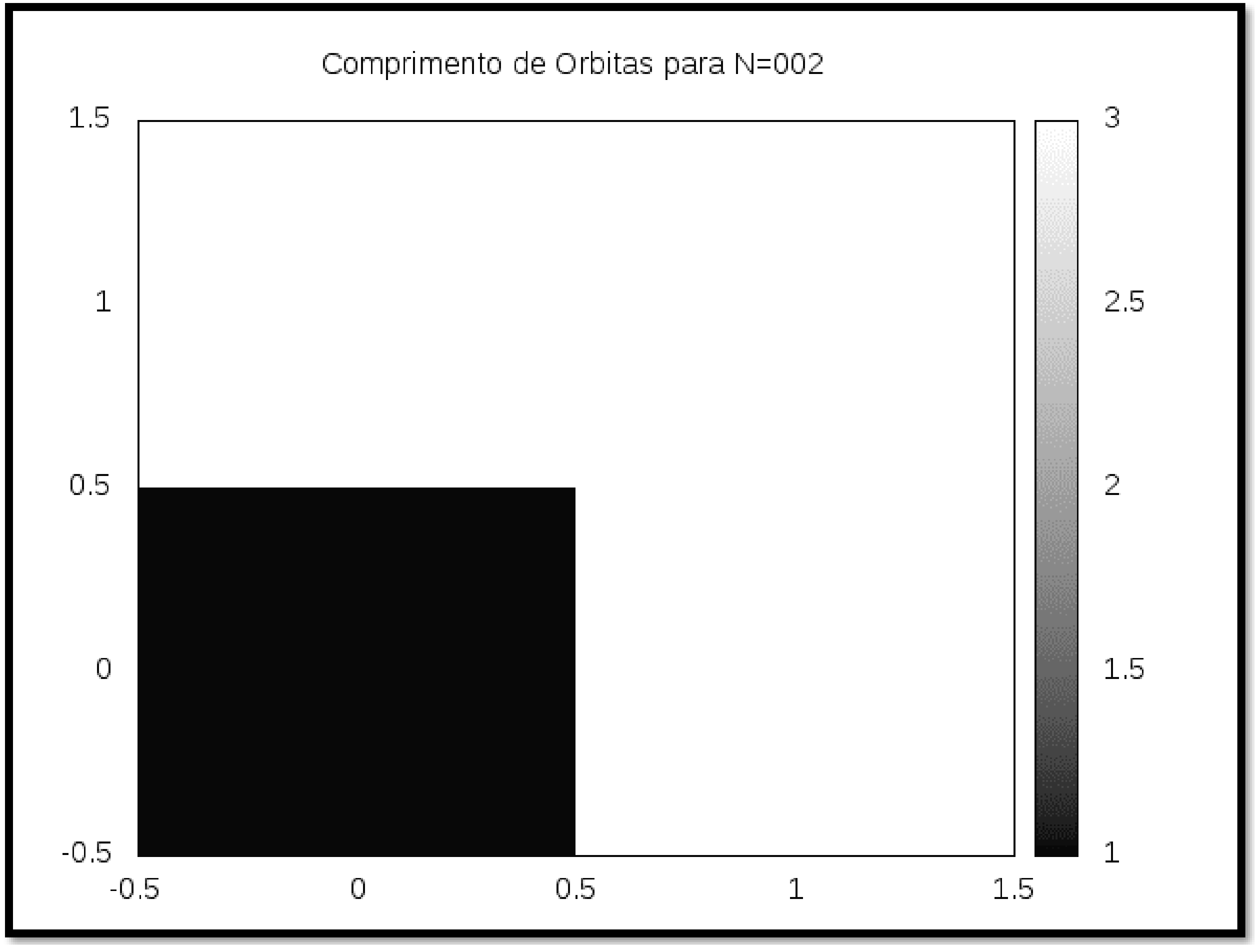


4. Properties of the Arnold Cat Map: Disjoint Orbits of Composite Numbers





4. Properties of the Arnold Cat Map: Disjoint Orbits Animation



4. Properties of the Arnold Cat Map: Extension to Higher Dimensions

- It's possible to extend the cat map to higher dimensions, fixating each coordinate and multiplying the results to get a three dimensional matrix of the cat map

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 4 & 4 \end{bmatrix} = A_{3D}$$

- The higher the dimension, the higher $|\lambda_{max}|$ is and more caotic the map gets.

4. Properties of the Arnold Cat Map: Unitary Positive Determinant

$$\Gamma_{G_1}\left(\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix}\right) = \begin{bmatrix} 1 & a \\ a & a^2+1 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod{N}$$

$$\Gamma_{A_2}\left(\begin{bmatrix} x_{t+1} \\ y_{t+1} \end{bmatrix}\right) = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_t \\ y_t \end{bmatrix} \pmod{N}$$

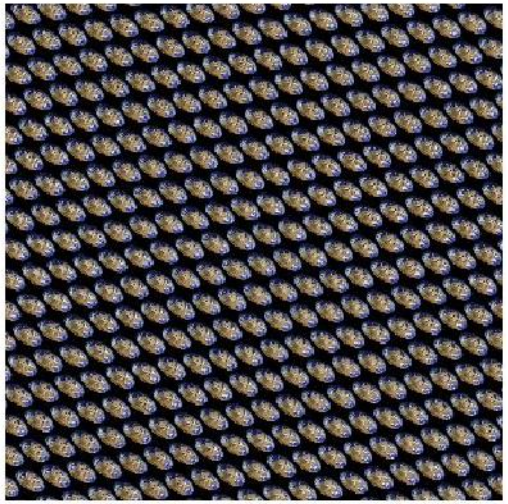
4. Properties of the Arnold Cat Map: Ghost and Miniatures

- Sometimes before we get to the minimal period, we observe some images less chaotic than expected. They are called miniatures and ghosts and have the following propertys
  - Miniatures can happen when the absolutes values of all elements $A^t \pmod{N}$ are small when compared to N. Orientation depens on the columm vectors.

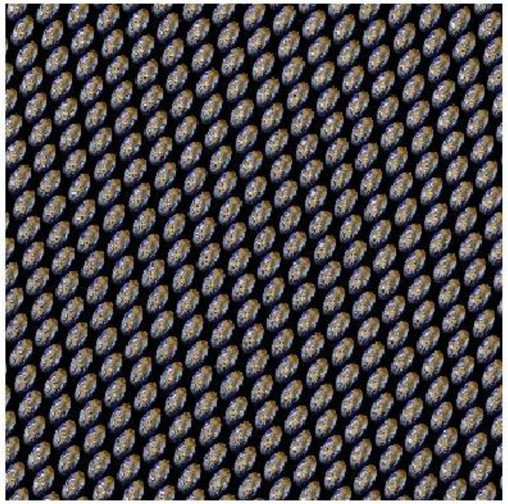
Original

332×332

$t = 23$



$t = 61$



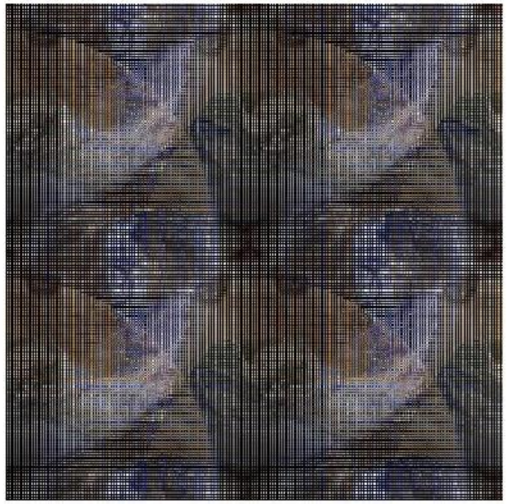
332×332

4. Properties of the Arnold Cat Map: Ghost and Miniatures

- Ghosts and their respective slope depend on vectors with the smallest absolute value that are mapped into themselves by $A^t \pmod{N}$.

Original

$t = 42$



332×332

5. Applications of the Arnold Cat Map: Encryption of text and images

- In cryptography, the color information of a pixel can be changed to letters from the alphabet.
- After a certain number of iterations the text becomes encrypted where the letters is no apparently desorganized have a subjacente order.

Original

S	I	S	T	E
M	A	S		D
I	N	A	M	I
C	O	S		É
	F	I	X	E

SISTEMAS DINÂMICOS É FIXE

After 2 iterations

	X	M	T	
O	A	F	N	I
E	É	D	E	I
A	S	S	S	I
	S	S	C	M

XMT OAFNIEÉDEIASSSI SSCM

5. Applications of the Arnold Cat Map: Steganography and Watermarks

- Steganography is the art of hide a message within another message.
- Can be used to insert a watermark or detect if an image or text was changed in an unauthorized way.

- The method consists on taking a small neighbourhood of pixels after aplying the Arnold cat map k iterations. They are used to insert the watermark on the image.
- The detection algorithm then consists on iterating the image $\Pi(n) - k$. The image should appear chaotic but the watermark is intact if the image wasn't changed.

6. Conclusion

- This project consisted on investigating some properties, and specially the period modulus N, of two dimensional hyperbolic toral automorphismsm, with a strong connection with the Fibonacci sequence, that get the name of Arnold cat map.
- We got numerical results on the minimal periods and period lenght of orbits.
- At the end some applications of the Arnold cat map are shown such as encryption and steganography.

7. References

[1] Fredrik Svanström, *Properties of a generalized Arnold's discrete cat map*, 2014,
http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A725545&dswid=-2366

[2] Jens Marklof, *Cat Map*,
https://people.maths.bris.ac.uk/~majm/bib/catmap.ps

[3] Geon Ho Choe, *Computational ergodic theory*, 2005,
http://www.ams.org/journals/bull/2007-44-01/S0273-0979-06-01120-7/S0273-0979-06-01120-7.pdf

[4] Freeman J. Dyson and Harold Falk, *Period of a Discrete Cat Mapping*, 1992,
http://www.jstor.org/stable/2324989

[5] Gabriel Peterson, *Arnold's Cat Map*, 1997,
https://pdfs.semanticscholar.org/edf4/23832801f51bdf3170cf64033913bac7ae2a.pdf

[6] Joe Nance, *Periods of the discretized Arnold's Cat Mapping andits extension to n-dimensions*, 2011,
https://arxiv.org/abs/1111.2984v1

8. The End

Questions?

Thank you for the attention!