Nonlinear Dyn (2012) 70:1365–1375
DOI 10.1007/s11071-012-0539-3

ORIGINAL PAPER

Period of the discrete Arnold cat map and general cat map

Jianghong Bao · Qigui Yang

Received: 19 May 2012 / Accepted: 13 July 2012 / Published online: 1 August 2012

Abstract The paper first studies the period of the discrete Arnold cat map. When the modulo is composite, the formulae are developed to calculate the minimal period. When the modulo is prime, the formulae calculating the period are given and an algorithm is proposed in order to determine the minimal period. Then the paper explores the relationship between the period of the discrete general cat map and its modulo for different parameters a and b. Some period formulae are given and some properties about the period are obtained. In addition, the paper also expands the period formulae of the corresponding a-Fibonacci sequence taken the modulo for more new parameters.

Keywords Discrete Arnold cat map · Discrete general cat map · Period · Minimal period

1 Introduction

With the rapid development of the Internet, the communication requirement of images has been greatly increased. More and more attention has been paid to how images can be safely transmitted over the Internet. Compared with text data, there exist some intrinsic features of images such as bulk data capacity and high correlation among pixels. The image encryption schemes based on chaotic map are proposed to work out the problem, because they are sensitive to the initial conditions and parameters and can be processed at high speed [1–3].

Chaos and chaos-based image encryption have been researched in the past decades [1–12], and the cat map is also extensively applied in image encryption. Zhu et al. [1] proposed an image cryptosystem employing Arnold cat map for bit-level permutation. Ye and Wong [2] applied the generalized Arnold map to proposed an efficient image encryption algorithm. Guan et al. [12] applied Arnold cat map to shuffle the position of pixels. It is also well known that a continuous chaotic map must be discretized before it is used for image encryption. However, the discretized cat map has bad effect on image encryption because it is always periodic. Much literature has paid attention to the problem, but only Dyson and Falk [13] discussed the period of the discretized Arnold cat map for some special cases.

If we know the period of the discretized cat map, we can choose a longer period and design a better image encryption scheme. The period of the discrete cat map does not always become greater with an increasing modulo. For the discrete general cat map, its period does not always increase with the increasing parameters. So it is very necessary for us to discuss the relationships of the period, its modulo and the parameters.

Arnold cat map is proposed by Russian mathematician V.I. Arnold [14]. Arnold cat map is a two-

J. Bao (✉) · Q. Yang
Department of Mathematics, South China University of Technology, Guangzhou, Guangdong 510641, P.R. China
e-mail: majhbao@yahoo.com

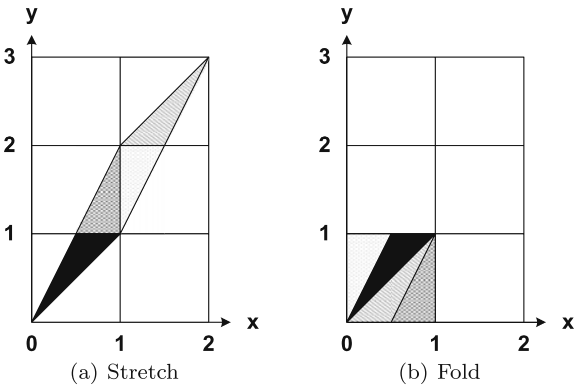

Fig. 1 Geometrical explanation of Arnold cat map

dimensional invertible chaotic map described by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \qquad (1.1)_N$$

where N is the modulo of the map $(1.1)_N$ and mod is the modulo of

$$\begin{bmatrix} x_n + y_n \\ x_n + 2y_n \end{bmatrix}$$

and N [15]. The geometrical explanation of the map $(1.1)_N$ is shown in Fig. 1.

When $x_n, y_n \in \{0, 1, \dots, N-1\}$, the map $(1.1)_N$ is discretized. Here, we assume $N > 1$.

Dyson and Falk [13] gave the relationship between the minimal period $\Pi(N)$ of the discrete Arnold cat map and its modulo N as follows:

(i) $\Pi(N) = 3N$ if and only if $N = 2 \times 5^k$ for $k = 1, 2, \dots$.
(ii) $\Pi(N) = 2N$ if and only if $N = 5^k$ or $N = 6 \times 5^k$ for $k = 1, 2, \dots$.
(iii) $\Pi(N) \le \frac{12N}{7}$ for all other N.

Arnold cat map $(1.1)_N$ is now generalized by introducing two parameters a and b as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \qquad (1.2)_N$$

where a and b are positive integers. N is the modulo of the map $(1.2)_N$.

In the paper, for the discrete Arnold cat map, the minimal period formulae are obtained for a composite N, and the period formulae are given for a prime N, while an algorithm is proposed to determine the minimal period. In addition, we also study the relationship between the period of the discrete general cat map and its modulo N for the parameters $a = b$ and any a and b. Some formulae and properties about the period are obtained. At the same time, we also expand the period formulae of the corresponding a-Fibonacci sequence modulo N for more new parameters.

The paper is organized as follows. Section 2 discusses how to determine the period of the discrete Arnold cat map. Section 3 investigates the period of the discrete general cat map at $a = b$. Section 4 explores the period of the discrete general cat map for any a and b. The final section concludes the paper.

2 Period of the discrete Arnold cat map

The discrete map of the map $(1.1)_N$ is described as [3]

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \qquad (2.1)_N$$

where

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix},$$

and $x_0, y_0 \in \{0, 1, \dots, N-1\}$. For a given N, $\Pi(N)$ denotes the minimal period and $P(N)$ denotes the period.

$(2.1)_N$ can be expressed as [13]

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

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} u_{2n-1}x + u_{2n}y \\ u_{2n}x + u_{2n+1}y \end{bmatrix} \bmod N,$$

where $\{u_n\}$ is Fibonacci number. T is the period of the map $(2.1)_N$ if and only if either of the following conditions satisfies:

(1) $u_{2T-1} \equiv 1 \pmod N$ and $N | u_{2T}$.
(2) $u_{2T+1} \equiv 1 \pmod N$ and $N | u_{2T}$.

On the basis of the result, we can prove the following proposition.

Proposition 2.1 *For the map $(2.1)_N$, the following conclusions hold.*

(1) *T is the period of the map $(2.1)_N$ if and only if $2T$ is the period of $\{u_n \bmod N\}$.*

(2) *T is the minimal period of the map* $(2.1)_N$ *if and only if* $2T$ *is the minimal period of* $\{u_n \bmod N\}$.

Proof From $u_{2T+1} \equiv 1 \pmod N$ and $u_{2T} \equiv 0 \pmod N$, it follows:

$$A^T = \begin{bmatrix} u_{2T-1} & u_{2T} \\ u_{2T} & u_{2T+1} \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N. \quad (2.2)$$

On the other hand, from (2.2), we have

$$u_{2T+1} \equiv 1 \pmod N, \qquad u_{2T} \equiv 0 \pmod N.$$

If T is the minimal period of $(2.1)_N$, but $2T$ is not the minimal period of $\{u_n \bmod N\}$, then there exists the period $2T_1$ of $\{u_n \bmod N\}$ less than $2T$. So, T_1 is the period of $(2.1)_N$. This leads to a contradiction and vice versa. □

According to Proposition 2.1 given above and the conclusions in [16], we have the following two theorems.

Theorem 2.2 *Suppose N is a prime more than 5. Then the following results hold for the map* $(2.1)_N$.

(1) *If N has the form $10m \pm 3$, then $P(N) = N + 1$.*
(2) *If N has the form $10m \pm 1$, then $P(N) = \frac{N-1}{2}$.*

Theorem 2.3 *Suppose N is a composite number. Then the following results hold for the map* $(2.1)_N$.

(1) *If $N = p^M$ and $\Pi(p^2) \neq \Pi(p)$, then $\Pi(N) = p^{M-1}\Pi(p)$. Also, k is the largest integer with $\Pi(p^k) = \Pi(p)$, then $\Pi(N) = p^{M-k}\Pi(p)$ for $M > k$.*
(2) *If N has the prime factorization $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $\Pi(N) = lcm(\Pi(p_i^{\alpha_i}))$, the least common multiple of the $\Pi(p_i^{\alpha_i})$.*

Remark 2.1 If $\Pi(p^2) \neq \Pi(p)$ for $p \neq 2$ is true, then the first case in Theorem 2.3 is equivalent to the following:

(1) If N has the prime factorization $N = p^M$, where $p > 2$ and $M \geq 2$, then $\Pi(N) = p^{M-1}\Pi(p)$.
(2) If $N = 2^M$, where $M \geq 2$, then $\Pi(N) = 2^{M-2}\Pi(4)$.

Applying Theorem 2.3, we only obtain the period when N is prime. In order to determine the minimal period $\Pi(N)$ of the map $(2.1)_N$ for a prime N, we need apply the following proposition, which can be proved by contradiction.

Proposition 2.4 *If s is not a period of the map* $(2.1)_N$, *then any factor of s is not a period of* $(2.1)_N$ *either.*

Applying Proposition 2.4, we propose a computer algorithm to determine the minimal period $\Pi(N)$ in virtue of the period $P(N)$ of $(2.1)_N$. The steps are described as follows:

Step 1. When the period $P(N)$ is prime, there does not exist other factors except 1 and itself. Therefore, $\Pi(N) = P(N)$.

Step 2. When $P(N)$ is composite, we can find out all factors of $P(N)$ except 1, on the basis of the prime factorization of $P(N)$. Suppose that there are n factors in all.

Step 3. Rearrange these factors in ascending order. A sequence $k_1, k_2, \ldots, k_n$ is obtained, where $k_n = P(N)$.

Step 4. When n is odd, we take the middle term of the sequence as k. When n is even, we take either of the middle two terms as k. If k is not a period, then any factor of k is not a period either, according to Proposition 2.4. So, all the factors of k should be removed. If k is a period, because we only consider the minimal period, all the multiples of k should be removed. This step is continued till only one factor is remained. Because $P(N)$ is in the sequence, there must exist one factor remained finally.

Step 5. The factor remained in the sequence is the minimal period $\Pi(N)$.

Example 2.1 When $N = 181$, we obtain $P(N) = 90$ by Theorem 2.2. Try to determine $\Pi(N)$ according to the above algorithm.

$P(N) = 90$ is composite. According to Step 2, we find out all factors of $P(N)$ except 1 on the basis of the prime factorization $90 = 2 \times 3^2 \times 5$. There are 11 factors in all. After rearranged, they are 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, and 90.

(1) Check the factor 10. Because $u_{2\times10-1} \not\equiv 1 \pmod N$ and $u_{2\times10} \not\equiv 0 \pmod N$, 10 is not the period of $(2.1)_N$. After 10, 2, and 5 are removed, only 3, 6, 9, 15, 18, 30, 45, and 90 are remained.

(2) Check the factor 18. We find it is not the period of $(2.1)_N$. After 3, 6, 9, and 18 are removed, only 15, 30, 45, and 90 are remained.

(3) Check the factor 45. We find it is a period. After 90 is removed, only 15, 30, and 45 are remained.

(4) Check the factor 30. We find it is not a period. After 15 and 30 removed, only 45 are remained.

Hence, $\Pi(181) = 45$. Although there are 11 factors, only 4 times are required. In fact, the more factors there are, the more efficient the algorithm is.

We obtain the minimal period from $N = 2$ to $N = 200$, shown in Fig. 2. The first half are given in Table 1. As seen in Fig. 2, with the increase of N, the minimal period does not always tend to increase. For example, $\Pi(125) = 250$, whereas $\Pi(144) = 12$. The relationship between the period and its modulo N is complex.

3 Period of the general cat map when $a = b$

The general cat map $(1.2)_N$ at $a = b$ is discretized according to the following formula:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N, \tag{$3.1)_N$}$$

where

$$A = \begin{bmatrix} 1 & a \\ a & 1+a^2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}^2,$$

and $x_0, y_0 \in \{0, 1, \dots, N-1\}$. For a given N, $\Pi(N)$ denotes the minimal period and $P(N)$ denotes the period.

Because

$$\begin{bmatrix} 1 & k_1N + a \\ k_1N + a & 1 + (k_1N + a)^2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N$$
$$= \begin{bmatrix} 1 & a \\ a & 1+a^2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod N,$$

we only consider a is a positive integer and $a \le N$.

We define the sequence $\{f_n\}$ of a-Fibonacci numbers for any positive integer a as follows:

$$f_0 = 0, \qquad f_1 = 1, \qquad f_{n+1} = a f_n + f_{n-1} \quad \text{for } n \ge 1. \tag{3.2}$$

By induction on n, we have

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = A \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} x_0 + a y_0 \\ a x_0 + (1+a^2) y_0 \end{bmatrix},$$

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = A^2 \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} (1+a^2)x_0 + (a^3+2a)y_0 \\ (a^3+2a)x_0 + (a^4+3a^2+1)y_0 \end{bmatrix},$$

$$\vdots$$

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} f_{2n-1} & f_{2n} \\ f_{2n} & f_{2n+1} \end{bmatrix} \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} f_{2n-1}x_0 + f_{2n} y_0 \\ f_{2n}x_0 + f_{2n+1} y_0 \end{bmatrix}.$$

Therefore, $(3.1)_N$ is reduced to

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} f_{2n-1}x_0 + f_{2n} y_0 \\ f_{2n}x_0 + f_{2n+1} y_0 \end{bmatrix} \pmod N. \tag{3.3}$$

By (3.3), it is easy to see that the following proposition is true.

Proposition 3.1 *T is the period of the map $(3.1)_N$ if and only if either of the following conditions satisfies.*

(1) $f_{2T-1} \equiv 1 \pmod N$ *and* $N | f_{2T}$.
(2) $f_{2T+1} \equiv 1 \pmod N$ *and* $N | f_{2T}$.

From Proposition 3.1, it follows Proposition 3.2, whose proof is similar to Proposition 2.1.

Proposition 3.2 *For the map $(3.1)_N$, the following conclusions hold.*

(1) *T is the period of the map $(3.1)_N$ if and only if $2T$ is the period of $\{f_n \bmod N\}$.*
(2) *T is the minimal period of the map $(3.1)_N$ if and only if $2T$ is the minimal period of $\{f_n \bmod N\}$.*

By Proposition 3.2 given above and Theorem 4 in [17], we have the following Theorem 3.3.

Theorem 3.3 *If N has the prime factorization $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $\Pi(N) = lcm(\Pi(p_i^{\alpha_i}))$.*

Falcon and Plaza [17] prove when $N = a^2 + 4$ and a is an odd number, the minimal period of $\{f_n \bmod N\}$ is $2N$. Next, we will discuss its minimal periods for more N.

Let

$$F_n = f_n \bmod N. \tag{3.4}$$

Proposition 3.4 *For the sequence $\{F_n\}$, the following conclusions hold.*

Table 1 The minimal period of the discrete Arnold cat map from $N = 2$ to $N = 100$

$\Pi(N)$	the units digit of N									
	0	1	2	3	4	5	6	7	8	9
the tens digit of N										
0	–	–	3	4	3	10	12	8	6	12
1	30	5	12	14	24	20	12	18	12	9
2	30	8	15	24	12	50	42	36	24	7
3	60	15	24	20	18	40	12	38	9	28
4	30	20	24	44	15	60	24	16	12	56
5	150	36	42	54	36	10	24	36	21	29
6	60	30	15	24	48	70	60	68	18	24
7	120	35	12	74	114	100	9	40	84	39
8	60	108	60	84	24	90	132	28	30	22
9	60	56	24	60	48	90	24	98	168	60

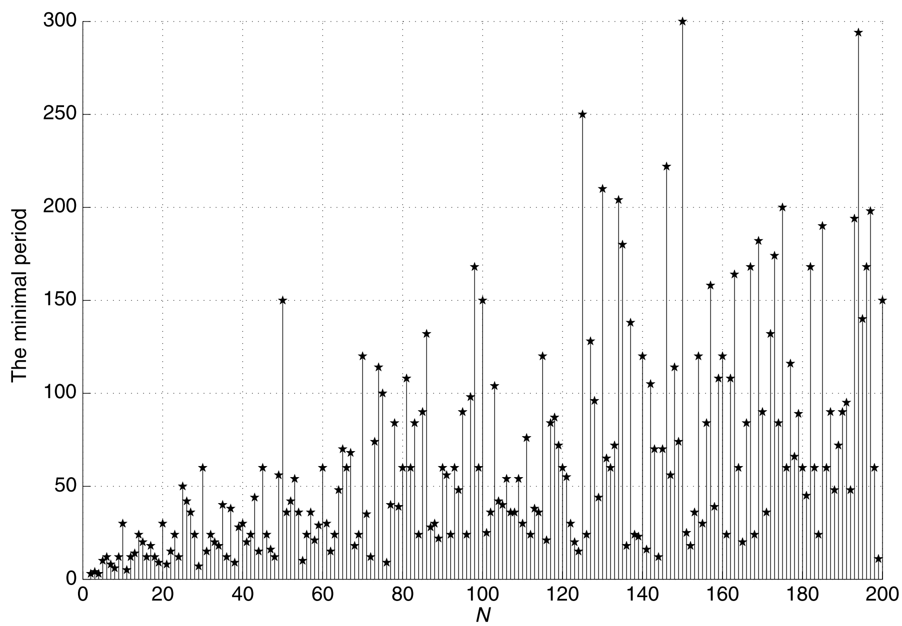

Fig. 2 The minimal period versus N

(1) *If* $N = a^2 + 4$ *and* a *is an even number, then*

$$\begin{cases} F_n \equiv (-1)^{\frac{n}{2}+1}\frac{n}{2}a \pmod N & \textit{for } n \textit{ even;} \\ F_n \equiv (-1)^{\frac{n-1}{2}} n \pmod N & \textit{for } n \textit{ odd.} \end{cases} \tag{3.5}$$

where $n = 0, 1, 2, \ldots$.

(2) *If* $N = a^2$, *then*

$$\begin{cases} F_n \equiv \frac{n}{2}a \pmod N & \textit{for } n \textit{ even;} \\ F_n \equiv 1 \pmod N & \textit{for } n \textit{ odd,} \end{cases} \quad (n = 0, 1, 2, \ldots). \tag{3.6}$$

Proof We prove the conclusions by mathematical induction.

(1) When $n = 0$ or 1, the results is true. Suppose that (3.5) holds for $n = k$. Then we consider the case $n = k + 1$.

Case 1: k is an even number.

$$F_{k+1} = aF_k + F_{k-1}$$
$$\equiv a \times (-1)^{\frac{k}{2}+1}\frac{k}{2}a + (-1)^{\frac{k}{2}-1}(k-1)$$

$$= (-1)^{\frac{k}{2}-1}\left[\frac{k}{2}(a^2+4) - (k+1)\right]$$
$$\equiv (-1)^{\frac{k}{2}}(k+1) \pmod N.$$

Case 2: k is an odd number.

$$\begin{aligned} F_{k+1} &= aF_k + F_{k-1} \\ &\equiv a \times (-1)^{\frac{k-1}{2}}k + (-1)^{\frac{k-1}{2}+1}\frac{k-1}{2}a \\ &= (-1)^{\frac{k+1}{2}+1}\frac{k+1}{2}a. \end{aligned}$$

Hence, (3.5) holds for $n = k+1$.

(2) When $n = 0$ or 1, the results are true. Suppose that (3.6) holds for $n = k$. Then we consider the case $n = k+1$.

Case 1: k is an even number.

$$\begin{aligned} F_{k+1} &= aF_k + F_{k-1} \\ &\equiv a \times \frac{k}{2}a + 1 \\ &\equiv 1 \pmod N. \end{aligned}$$

Case 2: k is an odd number.

$$\begin{aligned} F_{k+1} &= aF_k + F_{k-1} \\ &\equiv a + \frac{k-1}{2}a \\ &= \frac{k+1}{2}a. \end{aligned}$$

Hence, (3.6) holds for $n = k+1$. □

Theorem 3.5 *For the sequence* $\{f_n \bmod N\}$, $\Phi(N)$ *denotes its minimal period. The following results hold.*

(1) *If* $N = a^2 + 4$ *and* a *is even, then* $\Phi(N) = N$.
(2) *If* $N = a^2$ *and* $a > 1$, *then* $\Phi(N) = 2a$.

Proof (1) First, we prove the period is N. From a even, we have

$$F_N \equiv (-1)^{\frac{N}{2}+1}\frac{a}{2}N \equiv 0 \pmod N),$$

$$F_{N+1} \equiv N + 1 \equiv 1 \pmod N).$$

Hence, $F_N = F_0$ and $F_{N+1} = F_1$. It follows that the period of $\{F_n\}$ is N.

Second, we further prove that N is the minimal period of $\{F_n\}$ by contradiction.

Assume that there exists a smaller period k. The terms of a period in $\{F_n\}$ with $n \geq 0$ are as follows:

$$0, 1, a, -3, -2a, 5, 3a, -7, \ldots, -(N-1). \tag{3.7}$$

The subsequence formed by the odd terms of (3.7) is

$$1, -3, 5, -7, \ldots, -(N-1). \tag{3.8}$$

Since the first term of the sequence $\{F_n\}$ is 0 and the remainders of any terms in (3.8) modulo N are not 0, the following term 1 must be in (3.8). Noting that

$$-(N-1) \equiv 1 \pmod N)$$

and k is the factor of the period N, we can conclude that $k = 2$. Namely the period of $\{F_n\}$ is 2. Hence, $a = 0$, contradicting with the fact that a is a positive number.

(2) First, we prove the period is $2a$. By means of Proposition 3.4, we have

$$F_{2a} \equiv a^2 \equiv 0 \pmod N),$$
$$F_{2a+1} \equiv 1 \pmod N).$$

Hence, $F_{2a} = F_0$ and $F_{2a+1} = F_1$. It follows that the period of $\{F_n\}$ is $2a$.

Second, we further prove that $2a$ is the minimal period of $\{F_n\}$. The terms of a period in $\{F_n\}$ with $n \geq 0$ are as follows:

$$0, 1, a, 1, 2a, 1, 3a, 1, \ldots, a(a-1), 1. \tag{3.9}$$

The subsequence formed by the even terms of (3.9) is

$$0, a, 2a, 3a, \ldots, a(a-1). \tag{3.10}$$

Because the first term of the sequence $\{F_n\}$ is 0 and $a > 1$, if there exists a smaller period, then 0 must be among the odd terms. But the odd terms are always 1. Hence, it is impossible. □

We can prove the following theorems by means of the matrix in $(3.1)_N$.

Theorem 3.6 *For the map* $(3.1)_N$, *the following conclusions hold, where* k *is a positive integer.*

(1) *If* $N = a$, *then* $\Pi(N) = 1$.
(2) *For* $N = 2a$,
   (i) *if* a *is an even number, then* $\Pi(N) = 2$;

(ii) *if a is an odd number, then $\Pi(N)=3$.*
(3) *For $N=3a$,*
(i) *if $a=3k$, then $\Pi(N)=3$;*
(ii) *if $a=3k+1$ or $3k+2$, then $\Pi(N)=4$.*
(4) *For $N=4a$,*
(i) *if $a=2k$, then $\Pi(N)=4$;*
(ii) *if $a=2k+1$, then $\Pi(N)=3$.*
(5) *For $N=5a$,*
(i) *if $a=5k$, then $\Pi(N)=5$;*
(ii) *if $a=5k+1$ or $5k+4$, then $\Pi(N)=10$;*
(iii) *if $a=5k+2$ or $5k+3$, then $\Pi(N)=6$.*
(6) *For $N=6a$,*
(i) *if $a=6k$, then $\Pi(N)=6$;*
(ii) *if $a=6k+1$ or $6k+5$, then $\Pi(N)=12$;*
(iii) *if $a=6k+2$ or $6k+4$, then $\Pi(N)=4$;*
(iv) *if $a=6k+3$, then $\Pi(N)=3$.*

Proof If there exists n satisfying

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} x \\ y \end{bmatrix} \pmod N,$$

namely

$$A^n - I \equiv \mathbf{0} \pmod N,$$

where I denotes the identity matrix and $\mathbf{0}$ denotes the zero matrix, then n is the period of the map $(3.1)_N$, and vice versa. When n is prime, n is also the minimal period. When n is composite, only one of the factors of n is possibly the minimal period.

Next, we will prove the results are true for $N=3a$. The rest can be proved similarly.

(3) (i) When $a=3k$, we have

$$\frac{A^3-E}{N} = \begin{bmatrix} 3k(3k^2+1) & (9k^2+1)(3k^2+1) \\ (9k^2+1)(3k^2+1) & 3k(27k^4+15k^2+2) \end{bmatrix}.$$

Hence, $\Pi(N)=3$.

(ii) $a=3k+1$, we have

$$\frac{A^4-E}{N} = \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{bmatrix},$$

where

$$a_{11} = (3k+1)\big(33k^2+14k+4+27k^4+36k^3\big),$$
$$a_{12} = \big(1+3k^2+2k\big)\big(90k^2+36k+7 + 81k^4+108k^3\big),$$
$$a_{22} = (3k+1)\big(11+216k^2+64k+594k^4+432k^3 + 243k^6+486k^5\big),$$

and

$$\frac{A^2-E}{N} = \begin{bmatrix} k+\frac{1}{3} & 1+3k^2+2k \\ 1+3k^2+2k & \frac{1}{3}(3k+1)(4+9k^2+6k) \end{bmatrix}.$$

Hence, $\Pi(N)=4$.

The case $a=3k+2$ can be proved similarly. □

Theorem 3.7 *For the map $(3.1)_N$, the following conclusions hold*:

(1) *If $N=a^2$, then $\Pi(N)=a$.*
(2) *If $N=a^2+1$, then $\Pi(N)=6$ for $a>1$ and $\Pi(N)=3$ for $a=1$.*
(3) *If $N=a^2+2$, then $\Pi(N)=4$.*
(4) *If $N=a^2+3$, then $\Pi(N)=3$.*
(5) *For $N=a^2+4$,*
(i) *if a is an even number, then $\Pi(N)=\frac{N}{2}$;*
(ii) *if a is an odd number, then $\Pi(N)=2N$ and $\Pi(2N^r)=6N^r$, where r is a positive integer.*

Proof We only prove Case 2. Cases 1, 3, 4 can be proved similarly.

(2) From $N=a^2+1$, it follows that

$$\frac{A^6-I}{N} = \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{bmatrix},$$

where

$$a_{11} = a^2\big(a^6+8a^4+20a^2+15\big),$$
$$a_{12} = a\big(2+9a^2+6a^4+a^6\big)\big(3+a^2\big),$$
$$a_{22} = a^2\big(a^8+10a^6+35a^4+49a^2+21\big),$$

and

$$\frac{A^2-I}{1+a^2} = \begin{bmatrix} \frac{a^2}{a^2+1} & \frac{a(2+a^2)}{a^2+1} \\ \frac{a(2+a^2)}{a^2+1} & \frac{a^2(3+a^2)}{a^2+1} \end{bmatrix},$$

$$\frac{A^3-I}{1+a^2} = \begin{bmatrix} \frac{a^2(3+a^2)}{a^2+1} & a(3+a^2) \\ a(3+a^2) & \frac{a^2(6+5a^2+a^4)}{a^2+1} \end{bmatrix}.$$

Therefore, when $a \neq 1$, $\Pi(N) = 6$. When $a = 1$, $\Pi(N) = 3$.

(5) When a is an even number, it is proved by Proposition 3.2 and Theorem 3.5 given above. When a is an odd number, it is proved by Proposition 3.2 and the theorems in [17]. □

In fact, by means of its matrix, we can determine the periods for more parameters.

Corollary 3.8 *For the map* $(3.1)_N$, *the following conclusions hold.*

(1) *If* $N = f_k$ *and* k *is an even number greater than* 3, *then* $\Pi(N) = k$.
(2) *If* $N = f_k$ *and* k *is an odd number greater than* 3, *then* $\Pi(N) = 2k$.

It is a direct consequence of Proposition 3.2 and the theorem in [18].

Applying Proposition 3.2 and Theorems 3.6 and 3.7, we can obtain the period of the a-Fibonacci sequence modulo N for some new parameters as follows.

Corollary 3.9 *For the a-Fibonacci sequence modulo* N, *the following conclusions hold, where* $\Phi(N)$ *denotes its minimal period.*

(1) *If* $N = a^2 + 2$, *then* $\Phi(N) = 8$.
(2) *If* $N = a^2 + 3$, *then* $\Phi(N) = 6$.
(3) *For* $N = 3a$,
   (i) *if* $a = 3k$, *then* $\Pi(N) = 6$;
   (ii) *if* $a = 3k + 1$ *or* $3k + 2$, *then* $\Pi(N) = 8$.
(4) *For* $N = 4a$,
   (i) *if* $a = 2k$, *then* $\Pi(N) = 8$;
   (ii) *if* $a = 2k + 1$, *then* $\Pi(N) = 6$.
(5) *For* $N = 5a$,
   (i) *if* $a = 5k$, *then* $\Pi(N) = 10$;
   (ii) *if* $a = 5k + 1$ *or* $5k + 4$, *then* $\Pi(N) = 20$;
   (iii) *if* $a = 5k + 2$ *or* $5k + 3$, *then* $\Pi(N) = 12$.
(6) *For* $N = 6a$,
   (i) *if* $a = 6k$, *then* $\Pi(N) = 12$;
   (ii) *if* $a = 6k + 1$ *or* $6k + 5$, *then* $\Pi(N) = 24$;
   (iii) *if* $a = 6k + 2$ *or* $6k + 4$, *then* $\Pi(N) = 8$;
   (iv) *if* $a = 6k + 3$, *then* $\Pi(N) = 6$.

Falcon and Plaza [17] discussed the period of the a-Fibonacci sequence modulo N when $N = a^2 + 4$ for a odd, $N = a$ and $N = 2a$. Stanley [18] discussed the period of this sequence when $N = f_3 = a^2 + 1$. Here, we expand the period of this sequence which can be determined not only from $N = a^2$ to $N = a^2 + 4$ but also from $N = a$ to $N = 6a$. In fact, by means of matrix method, though we cannot find the general term of the period for any N, we can obtain the periods for more parameters.

4 Period of the discrete general cat map for any *a* and *b*

The general cat map $(1.2)_N$ is discretized as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}, \qquad (4.1)_N$$

where

$$A = \begin{bmatrix} 1 & a \\ b & 1 + ab \end{bmatrix},$$

and $x_0, y_0 \in \{0, 1, \dots, N - 1\}$. For a given N, $\Pi(N)$ denotes the minimal period and $P(N)$ denotes the period.

Because

$$\begin{bmatrix} 1 & k_1 N + a \\ k_2 N + b & 1 + (k_1 N + a)(k_2 N + b) \end{bmatrix} \times \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N}$$
$$= \begin{bmatrix} 1 & a \\ b & 1 + ab \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \pmod{N},$$

we only consider a and b are positive integers and $a \leq N, b \leq N$.

By $(4.1)_N$ and induction on n, we have

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = A \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \pmod{N},$$
$$\vdots$$
$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \pmod{N}.$$

For the map $(4.1)_N$, the following conclusions are true.

Theorem 4.1 *Let*

$$A^n - I = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

and $d = gcd(a_{11}, a_{12}, a_{21}, a_{22})$, the greatest common divisor of the a_{ij}. For any positive integer N satisfying $N|d$, n is the period of the map $(4.1)_N$.

Proof Obviously,

$$\left(A^n - I\right)\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}.$$

From $d = gcd(a_{11}, a_{12}, a_{21}, a_{22})$ and $N|d$, it follows that $N|a_{ij}$. Then

$$A^n - I \equiv \mathbf{0} \pmod N.$$

Hence, $P(N) = n$. Clearly, when n is a prime, n is also the minimal period of $(4.1)_N$. □

Example 4.1 When $a = 2$ and $b = 3$, one derives

$$A^5 - I = \begin{bmatrix} 3408 & 7810 \\ 11715 & 26838 \end{bmatrix}.$$

Since $gcd(3408, 7810, 11715, 26838) = 71$, it follows that $\Pi(71) = 5$.

The eigenvalues of A are

$$\lambda_1 = 1 + \frac{1}{2}ba + \frac{1}{2}\sqrt{ba(4 + ba)},$$
$$\lambda_2 = 1 + \frac{1}{2}ba - \frac{1}{2}\sqrt{ba(4 + ba)}.$$

Let

$$P = \begin{bmatrix} \frac{a}{\lambda_1 - 1} & \frac{a}{\lambda_2 - 1} \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

We have $A = PBP^{-1}$ and $A^n - I = P(B^n - I)P^{-1}$. There does not exist an integer n, which makes $B^n = I$.

In fact, suppose that there exists an integer n, which satisfies $B^n = I$. Then $\lambda_1^n = 1$ and $\lambda_2^n = 1$. From $\lambda_1\lambda_2 = 1$, it follows that $\lambda_1 = e^{i\frac{2k\pi}{n}}$ and $\lambda_2 = e^{-i\frac{2k\pi}{n}}$, where k is an integer. Thus, $ab = -4(\sin\frac{k\pi}{n})^2$. When a and b are positive integers, the equality $B^n = I$ can't hold.

Theorem 4.2 *If $r|m$, then $\Pi(r)|\Pi(m)$.*

Proof Assume

$$A^{\Pi(m)} - I = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Clearly, $m|a_{ij}$. From $r|m$, it follows $r|a_{ij}$. Thus, $\Pi(m)$ is the period of $(4.1)_r$. Consequently, we have $\Pi(r)|\Pi(m)$. □

Theorem 4.3 *If N has the prime factorization $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $\Pi(N) = lcm(\Pi(p_i^{\alpha_i}))$.*

Proof Let $N_i = p_i^{\alpha_i}$, $(i = 1, \ldots, k)$ and

$$A^{\Pi(N)} - I = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Then $N = N_1 N_2 \cdots N_k$.

According to Theorem 4.2 and $N_i|N$, it follows $\Pi(N_i)|\Pi(N)$. Thus,

$$lcm\big(\Pi(N_i)\big)|\Pi(N). \tag{4.2}$$

On the other hand, it follows from $N|a_{ij}$ that

$$N_1|a_{ij}, N_2|a_{ij}, \ldots, N_k|a_{ij}.$$

Hence

$$\Pi(N)|\Pi(N_i) \quad (i = 1, \ldots, k).$$

Thus, one derives that

$$\Pi(N)|lcm\big(\Pi(N_i)\big). \tag{4.3}$$

From (4.2) and (4.3), it follows that

$$\Pi(N) = lcm\big(\Pi(N_i)\big).$$ □

From

$$A^n - I = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

the greatest common divisors of a_{ij} for some values of n are presented in Table 2. In virtue of Table 2, we obtain Theorem 4.4 as follows.

Theorem 4.4 *For the map $(4.1)_N$, the following conclusions hold*:

(1) *If $N = ab + 1$ with $a \neq 1$ and $b \neq 1$, then $\Pi(N) = 6$.*
(2) *If $N = ab + 2$, then $\Pi(N) = 4$.*
(3) *If $N = ab + 3$, then $\Pi(N) = 3$.*
(4) *If $N = a^2b^2 + 5ab + 5$, then $\Pi(N) = 5$.*
(5) *If $N = a^3b^3 + 7a^2b^2 + 14ab + 7$, then $\Pi(N) = 7$.*
(6) *If $N = a^2b^2 + 4ab + 2$, then $\Pi(N) = 8$.*

Table 2 The greatest common divisors of the elements of $A^n - E$

n	$gcd(a_{11}, a_{12}, a_{21}, a_{22})$
3	$ab+3$
4	$ab+2$
5	$a^2b^2+5ab+5$
6	$(ab+1)(ab+3)$
7	$a^3b^3+7a^2b^2+14ab+7$
8	$(ab+2)(a^2b^2+4ab+2)$
9	$(ab+3)(a^3b^3+6a^2b^2+9ab+3)$
10	$(a^2b^2+3ab+1)(a^2b^2+5ab+5)$
11	$a^5b^5+11a^4b^4+44a^3b^3+77a^2b^2+55ab+11$
12	$(ab+1)(ab+2)(ab+3)(a^2b^2+4ab+1)$
13	$a^6b^6+13a^5b^5+65a^4b^4+156a^3b^3+182a^2b^2+91ab+13$
14	$(a^3b^3+5a^2b^2+6ab+1)(a^3b^3+7a^2b^2+14ab+7)$
15	$(ab+3)(a^2b^2+5ab+5)(a^4b^4+7a^3b^3+14a^2b^2+8ab+1)$

Proof (1) A straightforward computation shows that

$$\frac{A^6-I}{ab+1} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

where

$$a_{11} = ab\big(a^3b^3+8a^2b^2+20ab+15\big),$$

$$a_{12} = a\big(a^3b^3+6a^2b^2+9ab+2\big)(3+ab),$$

$$a_{21} = b\big(a^3b^3+6a^2b^2+9ab+2\big)(3+ab),$$

$$a_{22} = ab\big(a^4b^4+10a^3b^3+35a^2b^2+49ab+21\big),$$

and

$$\frac{A^2-I}{ab+1} = \begin{bmatrix} \frac{ab}{ab+1} & \frac{a(2+ab)}{ab+1} \\ \frac{b(2+ab)}{ab+1} & \frac{ab(3+ab)}{ab+1} \end{bmatrix},$$

$$\frac{A^3-I}{ab+1} = \begin{bmatrix} \frac{ab(3+ab)}{ab+1} & a(3+ab) \\ b(3+ab) & \frac{ab(6+5ab+a^2b^2)}{ab+1} \end{bmatrix}.$$

Thus, when $a \neq 1$ and $b \neq 1$, we have $\Pi(N) = 6$.

This rest can be proved similarly. □

5 Conclusions

In the paper, we study the relationship between the period of the discrete Arnold cat map and its modulo N. For any N, we can determine the minimal period. In addition, we also study the period of the discrete general cat map for $a = b$ and any a, b. By the matrix method, we not only obtain some period formulae for the general cat map, but also greatly widen the range of parameters for the period of the a-Fibonacci sequence modulo N.

Acknowledgements The research is supported by the Fundamental Research Funds for the Central Universities (No. 2011ZM0081) and the National Natural Science Foundation of China (No. 10871074).

References

1. Zhu, Z., Zhang, W., Wong, K., Yu, H.: A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf. Sci. **181**(6), 1171–1186 (2011)
2. Ye, G., Wong, K.-W.: An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn. **69**(4), 2079–2087 (2012)
3. Chen, G., Mao, Y., Chui, C.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals **21**(3), 749–761 (2004)
4. Zhou, T., Chen, G., Čelikovský, S.: :Šilnikov chaos in the generalized Lorenz canonical form of dynamical systems. Nonlinear Dyn. **39**(4), 319–334 (2005)
5. Liu, Y., Pang, W.: Dynamics of the general Lorenz family. Nonlinear Dyn. **67**(2), 1595–1611 (2012)
6. Wei, Z., Yang, Q.: Dynamical analysis of the generalized Sprott C system with only two stable equilibria. Nonlinear Dyn. **68**(4), 543–554 (2012)
7. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurc. Chaos Appl. Sci. Eng. **8**, 1259–1284 (1998)
8. Scharinger, J.: Fast encryption of image data using chaotic Kolmogorov Flows. J. Electron. Imaging **7**, 318 (1998)
9. Mirzaei, O., Yaghoobi, M., Irani, H.: A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn. **67**(1), 557–566 (2012)

10. Wang, X.-Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **62**(3), 615–621 (2010)
11. Huang, X.: Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dyn. **67**(4), 2411–2417 (2012)
12. Guan, Z., Huang, F., Guan, W.: Chaos-based image encryption algorithm. Phys. Lett. A **346**(1–3), 153–157 (2005)
13. Dyson, F., Falk, H.: Period of a discrete cat mapping. Am. Math. Mon. **99**(7), 603–614 (1992)
14. Arnold, V., Avez, A.: Ergodic Problems of Classical Mechanics, vol. 564. Benjamin, New York (1968)
15. Peterson, G.: Arnold's cat map. http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf (1997)
16. Wall, D.: Fibonacci series modulo m. Am. Math. Mon. **67**(6), 525–532 (1960)
17. Falcón, S., Plaza, Á.: k-Fibonacci sequences modulo m. Chaos Solitons Fractals **41**(1), 497–504 (2009)
18. Stanley, T.: A note on the sequence of Fibonacci numbers. Math. Mag. **44**(1), 19–22 (1971)