Article ID: 1005 - 9784(2005)S1 - 0278 - 05

Period of Arnold transformation and its application in image scrambling①

LI Bing(李 兵), XU Jia-wei(徐家伟)
(School of Mathematics and Computing Science,
Changsha University of Science and Technology, Changsha 410076, China)

Abstract: With the security problem of image information as the background, some more properties of the period of Arnold transformation of two-dimension were studied by means of introducing a integer sequence. Some new results are obtained. Two interesting conjectures on the period of Arnold transformation are given. When making digital images scrambling by Arnold transformation, it is important to know the period of the transformation for the image. As the application of the theory, a new method for computing the periods at last are proposed.

Key words: digital image; period; dynamic system; Arnold transformation; scrambling transformation
CLC number: O151; TP391; O415.6 **Document code:** A

1 INTRODUCTION

The security and crypto-guard of image information has emerged as an exciting and important research field as more and more image information has to be spread on the Internet. The scrambling technology is one of the basic means for covering huge image information[1]. There are many transformations that have been studied and used in image hiding or scrambling in recent years. In Ref. [2, 3], Arnold transformation (or Arnold's cat map) was used for covering of image information. Because the periodicity is one of the most important properties, a lot of researches have been made on the periods and applications of Arnold transformation[4-10]. Dyson et al[4] got some upper bounds and some lower bounds of the period m_N of Arnold transformation, and they obtained a formula of m_N for N was of 5^k. In Ref. [10] we got some more veracious upper bounds of the period for prime numbers N.

It is to be noted that the period of Arnold's cat map or the upper bounds and lower bounds of the period were also useful in the study of dynamics of some mechanical system and chaotic dynamics[4, 11-13].

But it is still unclear that how the period m_N changes as N varies. In this paper, we study some properties of the period of Arnold transformation by dint of introducing a integer sequence, and we got some new results. Some of them are generalizations of the results in Ref. [4]. We also give two interesting conjectures on the period of Arnold transformation. When making digital images scrambling by Arnold transformation, it is important to know the period of the transformation for the image. As the application of the theory, a new method for computing the periods at last was proposed.

2 ARNOLD TRANSFORMATION AND ITS PERIOD

The Arnold's cat map was introduced by Arnold, it was associated with a discrete-time flow on torus[5,14]. It is also called the cat map as well as Arnold transformation (two-dimension) by some references. In this paper, we use the definitions of Arnold transformation and its period in Ref. [1]. We denote by $P(N)$ the minimal positive period of Arnold transformation for $N\times N$ digital image (i. e. mod N), sometimes we also denote by $p(N)$ a period of the transformation. Note that here the notation $P(N)$ represents the notation m_N in Ref. [1,5](see Ref. [11]). Then it is clear that $P(N)\mid p(N)$ $(N>1)$. The definitions of the conceptions and notations which are not explained here can be found in Ref. [4,10,14,15].

We define a sequence $\{G_n\}$ as follows:

$$G_1=1, G_2=3; G_{n+2}=3G_{n+1}-G_n, n\geqslant 1 \quad (1)$$

Therefore, $G_n=3G_{n+1}-G_{n+2}$, for any $n\geqslant 1$. (2)

According to Eqn. 2, G_1 and $G_{-n}(n>0)$ can also be defined. There are two results as follows in Ref. [10]:

Theorem 1 Suppose n is a positive integer and an integer $N>1$, then $P(N)\mid n$ if and only if $N\mid (G_n, G_{n+1}-1)$.

Theorem 2 Suppose n is a positive integer and $N>1$ is an integer.

① **Foundation item:** Project (10471020) supported by the National Natural Science Foundation; project (04JJ6028) supported by the Natural Science Foundation of Hunan Province; project (03A002) supported by the Ministry of Education of Hunan Province
Received date: 2005 - 05 - 20; **Accepted date:** 2005 - 07 - 10
Correspondence: LI Bing, PhD, Professor; Tel: +86-13874801545; Email: libcs@263.net

(1) When n is even, then $P(N)\mid n$ if and only if $N\mid G_{n/2}$;

(2) When n is odd, then $P(N)\mid n$ if and only if $N\mid (G_{(n-1)/2}+G_{(n+1)/2})$.

To find the expression of $P(N)$, N should be wrote in terms of power of its prime factors. Thus we must consider the expression of $P(N)$ when N is a power of a prime number. Dyson et al[5] gave a result: $m_N=2N$, when $N=5r$, namely:

$$P(5^k)=10\times 5^{k-1}.$$

In digital image scrambling, we are more interested in the situation with $N=2^k$. We prove a theorem which is obviously a generalization of the above result of Dyson et al.

Theorem 3 Suppose k is a positive integer and $N>1$ is an integer, then $P(N^k)\mid N^{k-1}P(N)$.

Theorem 4 Suppose $k>1$ is a integer, then $P(2^k)=3\times 2^{k-2}$.

Theorem 5 Let $p>2$ be a prime number and k be a positive integer. If $p \parallel G_{P(p)}$, then

$$P(p^k)=P(p)\times p^{k-1}$$

where the notation "$a^i \parallel b$" means "b is divided by a^i but can not be divided by a^{i+1}".

A direct corollary of Theorem 5 is as follows:

Corollary 1 Let k be a positive integer, then

$$P(3^k)=4\times 3^{k-1};$$
$$P(5^k)=10\times 5^{k-1};$$
$$P(7^k)=8\times 7^{k-1}.$$

Proof It follows from some simple calculations that $P(3)=4$, $P(5)=10$, $P(7)=8$ and $G_4=21$, $G_8=987$, $G_{10}=6\,765$. Thus $3 \parallel G_4$, $5 \parallel G_{10}$, $7 \parallel G_8$. Then $P(3^k)=4\times 3^{k-1}$, $P(5^k)=10\times 5^{k-1}$ and $P(7^k)8\times 7^{k-1}$ follow the Theorem 5.

It is evident that much more corollaries can be deduced by Theorem 5.

For example, $P(27)=P(3^3)=P(3)\times 3^2=4\times 9$; $P(49)=P(7^2)=P(7)\times 7=8\times 7$.

3 PROOFS OF THEOREMS

Let λ_1,λ_2 be the two roots of the function $f(x)=x^2-3x+1$ and $\lambda_1>\lambda_2$.

Lemma 1[10] For any integer $n\geqslant 0$, $G_n=\frac{1}{\sqrt{5}}\cdot(\lambda_1^n-\lambda_2^n)$.

Lemma 2[10] For any integer n, we have

$$G_{2n}=G_n(G_{n+1}-G_{n-1});$$
$$G_{2n-1}=(G_n-G_{n-1})(G_n+G_{n-1}). \quad (3)$$

Lemma 3 For any integers k, $n\geqslant 0$, we have $\lambda_1^{2kn}+\lambda_2^{2kn}\equiv 2(\mathrm{mod}G_n^2)$

Proof We prove it by the mathematical induction. It follows from lemma 1 that $\lambda_1^n-\lambda_2^n=\sqrt{5}G_n$. Therefore

$$\lambda_1^{2n}+\lambda_2^{2n}=(\lambda_1^n-\lambda_2^n)^2+2=5G_n^2+2,$$

thus the proposition is valid when $k=1$. Now we assume that $\lambda_1^{2in}+\lambda_2^{2in}\equiv 2(\mathrm{mod}G_n^2)$ for all $i<k$. Because

$$\lambda_1^{2kn}+\lambda_2^{2kn}=(\lambda_1^{2n}+\lambda_2^{2n})(\lambda_1^{2(k-1)n}+\lambda_2^{2(k-1)n})-(\lambda_1^{2(k-2)n}+\lambda_2^{2(k-2)n}),$$

$\lambda_1^{2kn}+\lambda_2^{2kn}\equiv 2\cdot 2-2\equiv(\mathrm{mod}G_n^2)$. It completes the proof.

Lemma 4 Let k, n and a be positive integers. Then

(1) $(2k+1)\mid G_n$ implies

$$\lambda_1^{2kn}+\lambda_2^{2kn}+\lambda_1^{2(k-1)n}+\lambda_2^{2(k-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1\equiv 2k+1(\mathrm{mod}(2k+1)^2);$$

(2) $2\mid G_n$ implies $2\mid(\lambda_1^{kn}+\lambda_2^{kn})$;

(3) $a^k\mid G_n$ implies $a^{k+1}\mid G_{a\cdot n}$.

Proof (1) It follows from the above lemma that $\lambda_1^{2in}+\lambda_2^{2in}\equiv 2(\mathrm{mod}G_n^2)$, where $i=1,\cdots,k$, and it is not difficult to see that $(2k+1)\mid G_n$ implies $\lambda_1^{2in}+\lambda_2^{2in}\equiv 2(\mathrm{mod}(2k+1)^2)$. Hence we have

$$\lambda_1^{2kn}+\lambda_2^{2kn}+\lambda_1^{2(k-1)n}+\lambda_2^{2(k-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1\equiv 2k+1(\mathrm{mod}(2k+1)^2)$$

(2) It can be proved that $\lambda_1^{kn}+\lambda_2^{kn}$ is an integer by induction.

(3) At first we assume the number a is odd, say $a=2i+1$. It follows from lemma 1 that

$$G_{a\cdot n}=G_{(2i+1)n}=\frac{1}{\sqrt{5}}(\lambda_1^{(2i+1)n}-\lambda_2^{(2i+1)n})=\frac{1}{\sqrt{5}}(\lambda_1^n-\lambda_2^n)(\lambda_1^{2in}+\lambda_1^{(2i-1)n}\lambda_2^n+\cdots+\lambda_1^n\lambda_2^{(2i-1)n}+\lambda_2^{2in})=G_n(\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1). \quad (4)$$

Note $a\mid G_n$ because $a^k\mid G_n$. It follows fromula (1) that

$$\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1\equiv a(\mathrm{mod}a^2),$$

therefore

$$\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1\equiv 0(\mathrm{mod}a). \quad (5)$$

Then $a^{k+1}\mid G_{a\cdot n}$ follows from the condition $a^k\mid G_n$ and Eqns. (4) and (5).

Now suppose the number is even, say $a=2^j\cdot(2i+1)$, where $i\geqslant 0$ and $j\geqslant 1$. Then

$$G_{a\cdot n}=G_{2^j\cdot(2i+1)n}=\frac{1}{\sqrt{5}}(\lambda_1^{2^j\cdot(2i+1)n}-\lambda_2^{2^j\cdot(2i+1)n})=\frac{1}{\sqrt{5}}(\lambda_1^{(2i+1)n}-\lambda_2^{(2i+1)n})(\lambda_1^{(2i+1)n}+\lambda_2^{(2i+1)n})\cdots(\lambda_1^{2^{j-1}\cdot(2i+1)n}+\lambda_2^{2^{j-1}(2i+1)n})=\frac{1}{\sqrt{5}}(\lambda_1^n-\lambda_2^n)\cdot(\lambda_1^{2in}+\lambda_1^{(2i-1)n}\lambda_2^n+\cdots+\lambda_1^n\lambda_2^{(2i-1)n}+\lambda_2^{2in})\cdot(\lambda_1^{(2i+1)n}+\lambda_2^{(2i+1)n})\cdots(\lambda_1^{2^{j-1}\cdot(2i+1)n}+\lambda_2^{2^{j-1}\cdot(2i+1)n})=G_n(\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1)(\lambda_1^{(2i+1)n}+\lambda_2^{(2i+1)n})\cdots(\lambda_1^{2^{j-1}\cdot(2i+1)n}+\lambda_2^{2^{j-1}\cdot(2i+1)n}) \quad (6)$$

Note $2\mid a$ and $a^k\mid G_n$, it follows fromula (2) that for any positive integer l we have $2\mid(\lambda_1^{l\cdot n}+\lambda_2^{l\cdot n})$, hence

$$2^j\mid(\lambda_1^{(2i+1)n}+\lambda_2^{(2i+1)n})\cdots(\lambda_1^{2^{j-1}\cdot(2i+1)n}+\lambda_2^{2^{j-1}\cdot(2i+1)n}) \quad (7)$$

In addition, $a^k | G_n$ and formula (1) imply

$$\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1\equiv 2i+1(\mathrm{mod}(2i+1)^2),$$

it follows that

$$\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1\equiv 0(\mathrm{mod}(2i+1)). \quad (8)$$

Then $a^{k+1} | G_{a\cdot n}$ follows from the condition $a^k | G_n$ and Eqns. (6)-(8).

Lemma 5 Let n, i, k be integers. Then

(1) $G_n = G_{i+1}G_{n-i} - G_iG_{n-i-1}$;

(2) $G_n | G_{k\cdot n}$.

(1) We prove it inductively. It is obvious that when $i=1$, the proposition is true by the definition of the sequence $\{G_n\}$. Suppose now $i>1$ and

$$G_n = G_{i+1}G_{n-i} - G_iG_{n-i-1}$$

Then

$$G_{i+2}G_{n-i-1} - G_{i+1}G_{n-i-2} = (3G_{i+1}-G_i)G_{n-i-1} - G_{i+1}(3G_{n-i-1}-G_{n-i}) = G_{i+1}G_{n-i} - G_iG_{n-i-1} = G_n.$$

If $i\leqslant 0$ we can prove formula (1) similarly.

(2) It is not difficult to get the result from the following equalities:

$$G_{k\cdot n} = \frac{1}{\sqrt{5}}(\lambda_1^{kn}-\lambda_2^{kn}) = \frac{1}{\sqrt{5}}(\lambda_1^n-\lambda_2^n)(\lambda_1^{(k-1)n}+\lambda_1^{(k-2)n}\lambda_2^n+\cdots+\lambda_2^{(k-1)n}) = G_n(\lambda_1^{(k-1)n}+\lambda_1^{(k-1)n}\lambda_2^n+\cdots+\lambda_2^{(k-1)n})$$

thus when k is even, then

$$G_{k\cdot n} = G_n(\lambda_1^{(k-1)n}+\lambda_2^{(k-1)n}+\lambda_1^{(k-3)n}+\lambda_2^{(k-3)n}+\cdots+\lambda_1^n+\lambda_2^n)$$

and when k is odd, then

$$G_{k\cdot n} = G_n(\lambda_1^{(k-1)n}+\lambda_2^{(k-1)n}+\lambda_1^{(k-3)n}+\lambda_2^{(k-3)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1).$$

It is easy to prove that $\lambda_1^j+\lambda_2^j$ is an integer for any positive integer j, hence $\lambda_1^{(k-1)n}+\lambda_1^{(k-2)n}\lambda_2^n+\cdots+\lambda_2^{(k-1)n}$ is an integer for any k. The lemma is proved.

Now we prove the theorems stated in the previous section.

Proof of Theorem 3 At first we have

$$N | (G_{P(N)}, G_{P(N)+1}-1) \quad (9)$$

by Theorem 1 for $P(N) | P(N)$. Then it follows that $N | G_{P(N)}$ and by **Lemma 4**(3) we get

$$N^k | G_{N^{k-1}\cdot P(N)} \quad (10)$$

Next we prove $N^k | (G_{N^{k-1}\cdot P(N)+1}-1)$. It is valid obviously when $k=1$. Suppose now

$$N^k | (G_{N^{k-1}\cdot P(N)+1}-1). \quad (11)$$

Then $N | (G_{N^{k-1}\cdot P(N)+1}-1)$, therefore $G^i_{N^{k-1}P(N)+1} \equiv 1 \pmod N$ for $i=1,\cdots,N-1$, where $G^i_{N^{k-1}P(N)+1} = (G_{N^{k-1}P(N)+1})^i$. Thus we have

$$N | (G^{N-1}_{N^{k-1}\cdot P(N)+1}+G^{N-2}_{N^{k-1}\cdot P(N)+1}+\cdots+G_{N^{k-1}\cdot P(N)+1}+1). \quad (12)$$

Since

$$G^N_{N^{k-1}\cdot P(N)+1}-1 = (G_{N^{k-1}\cdot P(N)+1}-1)\cdot(G^{N-1}_{N^{k-1}\cdot P(N)+1}+G^{N-2}_{N^{k-1}\cdot P(N)+1}+\cdots+G_{N^{k-1}\cdot P(N)+1}+1),$$

it follows from Eqns. (11) and (12) that

$$N^{k+1} | (G^N_{N^{k-1}\cdot P(N)+1}-1). \quad (13)$$

Now we are going to prove $N^{k+1} | (G^N_{N^k\cdot P(N)+1}-1)$. For $0\leqslant j<N-1$ **Lemma 5**(1) implies

$$G_{(N-j)\cdot N^{k-1}P(N)+1} = G_{i+1}G_{(N-j)\cdot N^{k-1}P(N)+1-i} - G_iG_{(N-j)\cdot N^{k-1}P(N)-i},$$

where i is an positive integer. Let $i=(N-j-1)\cdot N^{k-1}P(N)$ then

$$G_{(N-j)\cdot N^kP(N)+1} = G_{(N-j-1)\cdot N^{k-1}P(N)+1}G_{N^{k-1}P(N)+1} - G_{(N-j-1)\cdot N^{k-1}P(N)}G_{N^{k-1}P(N)}$$

By **Lemma 5** (2) we have $G_{N^{k-1}P(N)} | G_{(N-j-1)\cdot N^{k-1}P(N)}$, therefore

$$N^k | G_{(N-j-1)\cdot N^{k-1}P(N)} \quad (14)$$

Thus Eqns. (10) and (14) imply $N^{k+1} | G_{(N-j-1)\cdot N^{k-1}P(N)}G_{N^{k-1}P(N)}$. Thus by the above equality we get

$$G_{(N-j)\cdot N^{k-1}P(N)+1} \equiv G_{(N-j-1)\cdot N^{k-1}P(N)+1}G_{N^{k-1}P(N)+1} - G_{(N-j-1)\cdot N^{k-1}P(N)}G_{N^{k-1}P(N)} (\mathrm{mod} N^{k+1})$$
$$\equiv G_{(N-j-1)\cdot N^{k-1}P(N)+1}G_{N^{k-1}P(N+1)} (\mathrm{mod} N^{k+1}).$$

Now let $j=0,1,\cdots,N-2$ then we have

$$G_{N^k\cdot P(N)+1} \equiv G_{(N-1)\cdot N^{k-1}P(N)+1}G_{N^{k-1}P(N)+1}\cdot (\mathrm{mod} N^{k+1})$$
$$G_{(N-1)\cdot N^{k-1}P(N)+1} \equiv G_{(N-2)\cdot N^{k-1}P(N)+1}G_{N^{k-1}P(N)+1} (\mathrm{mod} N^{k+1})\cdots$$
$$G_{2\cdot N^{k-1}P(N)+1} \equiv G^2_{N^{k-1}P(N)+1} (\mathrm{mod} N^{k-1}).$$

Substitute the last equality for the former one, and continue in turn, then we get

$$G_{N^k\cdot P(N)+1} \equiv G^N_{N^{k-1}P(N)+1} (\mathrm{mod} N^{k+1})$$

Thus it follows from Eqn. (13) that $N^{k+1} | (G_{N^k\cdot P(N)+1}-1)$. This complete the proof of

$$N^k | (G_{N^{k-1}\cdot P(N)+1}-1) \quad (15)$$

Finally, by Eqns. (10) and (15) we have $N^k | (G_{N^{k-1}\cdot P(N)}, G_{N^{k-1}\cdot P(N)+1}-1)$, therefore the proof is finished by Theorem 1.

Proof of Theorem 4 We give two facts as follows:

(1) Let $k>2$ be a integer, then $2^k \| G_{3\cdot 2^{k-3}}$;

(2) If $k>1$ be a integer, then $P(2^k) | (3\times 2^{k-2})$.

Proof (1) $2^3 \| G_3$ since $G_3=8$. Suppose $2^k \| G_{3\cdot 2^{k-3}}$ and $k>3$. By Lemma 1 and Lemma 2 it is not difficult to get

$$G_{3\cdot 2^{k-2}} = G_{3\cdot 2^{k-3}}(G_{3\cdot 2^{k-3}+1}-G_{3\cdot 2^{k-3}-1}) = G_{3\cdot 2^{k-3}}(\lambda_1^{3\cdot 2^{k-3}}+\lambda_2^{3\cdot 2^{k-3}}).$$

But by Lemma 3 we have $\lambda_1^{3\cdot 2^{k-3}}+\lambda_2^{3\cdot 2^{k-3}} \equiv 2 \pmod{G_3^2}$, thus it follows that $2^{k+1} \| G_{3\cdot 2^{k-2}}$. Then the first fact is proved by the mathematical induction.

(2) It is easy to see the fact is valid when $k=2$ for $P(4)=3$. By Fact (1) we have $2^k | G_{3\cdot 2^{k-3}}$ for $k>2$. Therefore Theorem 2 (1) implies $P(2^k) | (3\times 2^{k-2})$. The fact (2) is proved.

Next we prove the theorem. It is clear that $P(2^2)=3\times 2^{2-2}$ and $P(2^3)=3\times 2^{3-2}$. Suppose $P(2^k)=3\times 2^{k-2}$ and $k>3$. Then we claim that $P(2^{k+1})>P(2^k)$. In fact, from Theorem 1 we have $2^{k+1} | (G_{P(2^{k+1})}, G_{P(2^{k+1})+1}-1)$ because $P(2^{k+1}) | P(2^{k+1})$, thus $2^k | (G_{P(2^{k+1})}, G_{P(2^{k+1})+1}-1$. Again by Theorem 1 we obtain that

$$P(2^k)\,|\,P(2^{k+1}). \quad (16)$$

Therefore $P(2^{k+1})\geqslant P(2^k)$. If $P(2^{k+1})=P(2^k)$ then $P(2^{k+1})=P(2^k)=3\times 2^{k-2}$. Thus it follows from Theorem 2(1) that $2^k\,|\,G_{3\cdot 2^{k-3}}, 2^{k+1}\,|\,G_{3\cdot 2^{k-3}}$, this is contrary to the Fact (1), the claim is proved. Now the second fact implies $P(2^{k+1})\,|\,(3\times 2^{k-1})$, thus there is a positive integer s such that $2^{k-1}\cdot 3=s\cdot P(2^{k+1})$, and by Eqn. (16) there must be a positive integer t such that $P(2^{k+1})=t\cdot P(2^k)=t\cdot 2^{k-2}\cdot 3$, then it follows that $st=2$. Therefore $s=1$ (otherwise $t=1$ and it contradicts $P(2^{k+1})>P(2^k)$), thus we get $P(2^{k+1})=3\times 2^{k-1}$. This finishes the proof by the mathematical induction.

Proof of Theorem 5 We prove a claim at first as follows:

Claim Let $p>2$ be a prime number, k a positive integer. If $p\parallel G_{P(p)}$, then $p^k\parallel G_{p^{k-1}\cdot P(p)}$.
Proof of the claim. It is trivial when $k=1$. Suppose $p^k\parallel G_{p^{k-1}\cdot P(p)}$ and $k>1$. Let $p=2i+1$ and $n=p^{k-1}P(p)$, where i is a positive integer. It follows from Lemma 1 that

$$G_{p\cdot n}=G_{(2i+1)n}=\frac{1}{\sqrt{5}}(\lambda_1^{(2i+1)n}-\lambda_2^{(2i+1)n})=$$
$$\frac{1}{\sqrt{5}}(\lambda_1^n-\lambda_2^n)(\lambda_1^{2in}+\lambda_1^{(2i-1)n}\lambda_2^n+\cdots+$$
$$\lambda_1^n\lambda_2^{(2i-1)n}+\lambda_2^{2in})=G_n(\lambda_1^{2in}+\lambda_2^{2in}+$$
$$\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+\lambda_1^{2n}+\lambda_2^{2n}+1).$$

By the condition and Lemma 4(3) we have

$$p^k\parallel G_n, \quad (17)$$

therefore $p\,|\,G_n$, thus it follows from Lemma 4(1) that

$$\lambda_1^{2in}+\lambda_2^{2in}+\lambda_1^{2(i-1)n}+\lambda_2^{2(i-1)n}+\cdots+$$
$$\lambda_1^{2n}+\lambda_2^{2n}+1\equiv p(\text{mod } p^2). \quad (18)$$

Then Eqns. (17) and (18) imply that $p^{k+1}\parallel G_{p\cdot n}$, namely $p^{k+1}\parallel G_{p^k\cdot P(p)}$. This completes the proof of the claim by induction.

Next we will prove the theorem by induction. It is trivial when $k=1$. Suppose $P(p^k)=p^{k-1}\cdot P(p)$ and $k>1$. Then we have that $P(p^{k+1})>P(p^k)$. In fact, from Theorem 1 we get $p^{k+1}\,|\,(G_{P(p^{k+1})}, G_{P(p^{k+1})+1}-1)$, thus $p^k\,|\,(G_{P(p^{k+1})}, G_{P(p^{k+1})+1}-1)$. Again by Theorem 1 we obtain that

$$P(p^k)\,|\,P(p^{k+1}). \quad (19)$$

Therefore $P(p^{k+1})\geqslant P(p^k)$. If $P(p^{k+1})=P(p^k)$, then $P(p^{k+1})=P(p^k)=p^{k-1}\cdot P(p)$. It follows from **Theorem 1** that

$$p^k\,|\,G_{p^{k-1}\cdot P(p)}, p^{k+1}\,|\,G_{p^{k-1}\cdot P(p)},$$

This contradicts the claim $p^k\parallel G_{p^{k-1}\cdot P(p)}$ hence

$$P(p^{k+1})>P(p^k). \quad (20)$$

By **Theorem 3**, we have $P(p^{k+1})\,|\,p^k\cdot P(p)$, thus there is a positive integer a such that $p^k\cdot P(p)=a\cdot P(p^{k+1})$, and by Eqn. (19) there must be a positive integer b such that $P(p^{k+1})=b\cdot P(p^k)=b\cdot p^{k-1}P(p)$, then it follows that $ab=p$. Therefore $a=1$, otherwise $b=1$ it contradicts Eqn. (20), thus we get $P(p^{k+1})=p^k\cdot P(p)$. This completes the proof.

4 CONJECTURES AND APPLICATIONS

The following conjecture comes from a lot of numerical experiments. At least, it is valid for the prime numbers which are not very large, i. e. $p<10^4$ or $p<10^5$ ($p>2$), by numerical computation.

Conjecture 1 Let $p>2$ be a prime number and k a positive integer. then $P(p^k)=P(p)\times p^{k-1}$.

It seems that both the proof of the above proposition and the numerical verifying by computation for large prime number p and any positive integer k are not trivial. Therefore, Theorem 1. 5 is significative. By the theorem, we need only to deal with a simpler thing (if it is sure-enough), namely the following conjecture:

Conjecture 2 Let $p>2$ be a prime number, then $P\parallel G_{P(p)}$.

We made the numerical verifying of this proposition for the prime numbers which are not very large (prime numbers $p<10^4$ and $p>2$). It takes about 3 s before our program finishes computation. It should be noticed that $G_P(p)$ may be very large, thus it is useful to consider $G_{P(p)}$ mod p and $G_{P(p)}$ mod p^2.

When making digital images scrambling by Arnold transformation, it is important to know the period of the transformation for the image. As the application of the theory, we propose a new method for computing the periods next. It is obviously suitable for such situations that the values of the pixels of the images are not very large, for example, they are less than 10^8. In the practice of processing of usual images, that may be enough.

For any $N\times N$ image, the positive integer N must be factored to one of the following three forms

1) $N=2^{k_1}p_2^{k_2}\cdots p_n^{k_n}$;
2) $N=2p_2^{k_2}\cdots p_n^{k_n}$;
3) $N=p_2^{k_2}\cdots p_n^{k_n}$;

where $k_i(i=1,\cdots,n)$ are positive integers ($k_1>1$) and $p_i>2$ are prime numbers. Thus $P(N)$ can be calculated respectively as follows:

1) $P(N)=[P(2)\cdot 2^{k_1-2}, P(p_2)\cdot p_2^{k_2-1},\cdots, P(p_n)\cdot p_n^{k_n-1}]$,
2) $P(N)=[P(2),P(p_2)\cdot p_2^{k_2-1},\cdots,P(p_n)\cdot p_n^{k_n-1}]$,
3) $P(N)=[P(p_2)\cdot p_2^{k_2-1},\cdots,P(p_n)\cdot p_n^{k_n-1}]$,

where the symbol $[a, b,\cdots,c]$ denotes the lease common multiple of $a, b, \cdots, c$.

Remark We have proved (in another note) that:

if $(N_1, \cdots, N_n) = 1$, then $P(N_1 \times \cdots \times N_n) = [P(N_1), \cdots, P(N_n)]$.

Example $P(296\,352) = [P(2) \times 8, P(3) \times 9, P(7) \times 49] = [3 \times 8, 4 \times 9, 8 \times 49] = 8 \times 9 \times 49 = 3\,528$.

5 CONCLUSIONS

Some more properties of the period of Arnold transformation by means of introducing a new integer sequence were studied. Some new results are obtained. Some of them are generalizations of the results in Ref. [5]. we also give two interesting conjectures on the period. As the application of the theory, new method for computing the periods are proposed. A simple example is given to explain the method.

REFERENCES

[1] QI Dong-xu, ZOU Jian-cheng, HAN Xiao-you. A new class of scrambling transformation and its application in the image information covering [J]. Science in China (Series E), 2000, 43(3): 304 - 312.

[2] DING Wei, QI Dong-xu. Digital image transformation and information hiding and disguising technology [J]. J Computers, 1998, 21(9): 838. (in Chinese)

[3] QI Dong-xu. Matrix transformation and its application to image hiding [J]. J North China Univ Tech, 1999, 11(1): 24 - 28. (in Chinese)

[4] Dyson F J, Falk H. Period of a discrete cat mapping [J]. The Amer Math Monthly, 1992, 99: 603 - 614.

[5] ZOU Jian-cheng, TIE Xiao-yun. Arnold transformation of digital image with two dimension and its periodicity [J]. J North China Univ Tech, 2000, 12(1): 10 - 14. (in Chinese)

[6] DING Wei, QI Dong-xu. A new kind of digital image transformation in information disguising [A]. Information Sciences and Microelectronic Technology [C]. Beijing: Academic Press, 1998. 309 - 311. (in Chinese)

[7] SUN Wei. The periodicity of Arnold transformation [J]. J North China Univ Tech, 1999, 11(1): 29 - 32. (in Chinese)

[8] ZHAO Hui. Arnold transformation of n dimension and its periodicity [J]. J North China Univ Tech, 2002, 14(1): 21 - 25. (in Chinese)

[9] KONG Tao, ZHANG Dan. A new anti-arnold transformation algorithm [J]. J Software, 2004, 15(10): 1558 - 1564. (in Chinese)

[10] LI Bing, XU Jia-wei. On the periods of Arnold Transformations and some applications [J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(S2): 139 - 142. (in Chinese)

[11] Lakshminarayan A, Balazs N L. On the quantum cat and sawtooth maps-return to generic behaviour [EB/OL]. http://arxiv:org/pdf/chao-dyn/9307005, 1993. 7.

[12] Barash L, Shchur L N. Periodic orbits of the ensemble of cat maps and pseudorandom number generation [EB/OL]. http://arxiv. org/PS_cache/physics/pdf/0409/0409069. pdf, 2004. 9.

[13] Arnold V I, Avez A. Ergodic problems of classical mechanics [A]. Mathematical Physics Monograph Series [C]. New York: W. A. Benjamin, 1968.

[14] ZHOU Chi-zhong. The Fibonacci-Lucas sequences [M]. Changsha: Hunan Science and Tech Press, 1993. (in Chinese)

[15] PAN Cheng-dong, PAN Cheng-biao, An introduction to the theory of numbers [M]. Beijing: Beijing University Press, 1998. (in Chinese)

(Edited by ZHAO Jun)