愛知工業大学研究報告
第38号 A 平成15年

On the Discrete Dynamical Systems in $\mathbf{Z}_n$

$\mathbf{Z}_n$における離散力学系について

Kazuki Wakazono† and Yuji Hashimoto

若園和規　　橋本有司

Abstract. In the RSA cryptosystem, the factorization of a composite integer n , which is the product of two primes, is essential for the decryption of the ciphertext. And the factorization of the integer is very difficult when the integer becomes so large. Therefore, many methods for factorization are developed in recent years. Among them, Pollard ρ method is sometimes very usefull, although there are some cases the method does not work so well. In this paper, we consider the dynamical systems of the mapping in $\mathbf{Z}_n$ and, by investigating the cycles of this mapping, we give a theorem on factorization along the same line of Pollard's.

1. Let $n > 2$ be a positive integer and $\mathbf{Z}_n$ the ring of residue classes modulo n. We consider the mapping $f(x)$ in $\mathbf{Z}_n$. The iteration of f with a initial value x_1 is defined by

$$x_{k+1} = f(x_k) \quad (k = 1, 2, 3, \cdots) .$$

As the sequence $\{x_1, x_2, \cdots\}$ is a finite set, there exist positive integers ℓ and m such that $x_{\ell+1} \neq x_\ell, \cdots, x_{m-1} \neq x_\ell$ and $x_m = x_\ell$. We call $\{x_\ell, x_{\ell+1}, \cdots, x_{m-1}\}$ the cycle of f in $\mathbf{Z}_n$ with the period $\ell - m$.

As for the RSA cryptosystem, the factorization of the integer n which is the product of two primes p and q is important. And the Pollard ρ algorithm is one of the effective methods for factorization. Usually, this algorithm is stated from the viewpoint of probability. In the following, we consider the theoretical side of this algorithm. Therefore, we assume $n = pq$. We first give some examples.

Example 1. We consider the case $n = 15$ and $f(x) = x^2 + 1$ in $\mathbf{Z}_{15}$. We calculate the iteration of f with the initial value 0 in $\mathbf{Z}_{15}$, then, we find the cycle $\{2, 5, 11\}$ of f. We take the greatest common divisor of the difference of the two points in the cycle and the integer n, for example,

$$\gcd(5 - 2, 15) = 3,$$

and we find the factor 3 of 15.

Example 2. We consider the case $n = 295$ and $f(x) = x^2 + 1$ in $\mathbf{Z}_{295}$. We calculate the iteration of f with the initial value 0 in $\mathbf{Z}_{295}$, then, we find the cycle $\{252, 80, 206\}$ of f. We take the greatest common divisor of the difference of the two points in the cycle and the integer n,

†Department of Information Network Engineering

$$\gcd(80-252,295)=1,\ \gcd(206-80,295)=1,\ \gcd(252-206,295)=1,$$

therefore, in this case, we cannot find the factor of 295.

Next, we consider the iteration of f with the initial value 3 in $\mathbf{Z}_{295}$, then, we find another cycle $\{257,265,16\}$ of f. We take the greatest common divisor of the difference of the two points in the cycle and the integer n,

$$\gcd(265-257,295)=1,\ \gcd(16-265,295)=1,\ \gcd(257-16,295)=1,$$

therefore, we cannot also find the factor of 295.

But, we take the greatest common divisor of the difference of the points in these cycles and the integer n,

$$\gcd(252-257,295)=5,\ \gcd(80-265,295)=5,\ \gcd(206-16,295)=5,$$

therefore, we can find the factor 5 of 295.

Example 3. We consider the case $n=21$ and $f(x)=x^2+1$ in $\mathbf{Z}_{21}$. We calculate the iteration of f with the initial value 0 in $\mathbf{Z}_{21}$ and we find the cycle $\{5\}$ of f, the fixed point. This time, the cycle consists of one point, therefore, we cannot find the factor of 21.

Next, we consider the iteration of f with the initial value 3 in $\mathbf{Z}_{21}$, then, we find another cycle $\{17\}$ of f. We take the greatest common divisor of the difference of the two points in these cycles and the integer n,

$$\gcd(5-17,21)=3,$$

therefore, we can find the factor 3 of 21.

According to the above examples, whether we can find the factor of n in a cycle is not certain. This is the reason why the Pollard ρ algorithm is called the Monte Carlo method. But, as the above examples show, by using other cycles, we can possibly find the factor of n . We investigate the situation for the 276 integers each of which is the product of two odd primes p and q $(p\neq q)$ less than 100. The result is the following. That is, there exist

244 cases of Example 1,
17 cases of Example 2,
15 cases of Example 3,

in these 276 cases.

2. According to the result in **1**, we may anticipate that any integer can be factorized by the above algorithm. We state the theorem.

Theorem. Let $n=pq$, where p and q are odd prime integers. We consider the mapping $f(x)=x^2+1$ in $\mathbf{Z}_n$. Then, the factor of n can be found in either of the following cases.

(1) There exists a cycle of f and the greatest common divisor of the difference of two points in the cycle and n gives the factor of n.

(2) There exist at least two cycles of f and the greatest common divisor of the difference of a point in one cycle and a point in the other cycle and n gives the factor of n.

Proof. Let $\{\xi_1,\cdots,\xi_r\}$ be the cycle of f with the period r. We define the two projection mappings

$$\begin{cases}\pi_p(x)=x\ (\mathrm{mod}\ p)\\ \pi_q(x)=x\ (\mathrm{mod}\ q)\end{cases}$$

for $x \in \mathbf{Z}_n$. Then, the set $\{\pi_p(\xi_1), \cdots, \pi_p(\xi_r)\}$ contains the cycle $\{\eta_1, \cdots, \eta_s\}$ in $\mathbf{Z}_p$ and the set $\{\pi_q(\xi_1), \cdots, \pi_q(\xi_r)\}$ contains the cycle $\{\zeta_1, \cdots, \zeta_t\}$ in $\mathbf{Z}_q$.

(1) If the cycle $\{\xi_1, \cdots, \xi_r\}$ contains at least two points and $r > s$ holds for the cycle $\{\eta_1, \cdots, \eta_s\}$, then, there exist the points for which $\pi_p(\xi_i) = \pi_p(\xi_j)$ $(\xi_i \neq \xi_j)$. Therefore, we have $\xi_i - \xi_j = 0 \pmod p$. So that, $\gcd(\xi_i - \xi_j, n) = p$. In this case, s is a divisor of r and the projection π_p is a r/s to 1 mapping.

(2) If the cycle $\{\xi_1, \cdots, \xi_r\}$ contains at least twe points but $r = s$ holds for the cycle $\{\eta_1, \cdots, \eta_s\}$, then, we cannot find the points as in (1). In this case, we may assume $r = t$ also holds for the cycle $\{\zeta_1, \cdots, \zeta_t\}$, for, if $r > t$ holds, we can find the points as in (1). We now construct another cycle in $\mathbf{Z}_n$. By using the Chinese remainder theorem, we solve the following equations,

$$\begin{cases} x = \eta_1 \pmod p \\ x = \zeta_2 \pmod q \end{cases}, \quad \begin{cases} x = \eta_2 \pmod p \\ x = \zeta_3 \pmod q \end{cases}, \quad \cdots, \quad \begin{cases} x = \eta_r \pmod p \\ x = \zeta_1 \pmod q \end{cases}.$$

We set the solutions to be $\chi_1, \cdots, \chi_r$. Then,

$$\begin{cases} \chi_1^2 + 1 = \eta_1^2 + 1 = \eta_2 \pmod p \\ \chi_1^2 + 1 = \zeta_2^2 + 1 = \zeta_3 \pmod q \end{cases},$$

therefore, $\chi_1^2 + 1 = \chi_2$. In a similar way, we have $\chi_2^2 + 1 = \chi_3, \cdots, \chi_r^2 + 1 = \chi_1$ and we obtain another cycle $\{\chi_1, \cdots, \chi_r\}$ of f in $\mathbf{Z}_n$. Therefore, we have $\xi_1 - \chi_1 = 0 \pmod p$. So that, $\gcd(\xi_1 - \chi_1, n) = p$.

The rest of the proof is the case $r = 1$ and the cycle consists of only one point.

Let the cycle in $\mathbf{Z}_n$ be $\{\xi\}$. We shall find another cycle. Setting $\chi = -\xi + 1$, then

$$\chi^2 + 1 = (-\xi + 1)^2 + 1 = -\xi + 1 = \chi \pmod n$$

and we see $\{\chi\}$ is the cycle in $\mathbf{Z}_n$. If $\xi \neq \chi$ and $\pi_p(\xi) = \pi_p(\chi)$, as in the case of (1), we obtain $\gcd(\xi - \chi, n) = p$. If $\xi \neq \chi$ and $\pi_p(\xi) \neq \pi_p(\chi)$, $\pi_q(\xi) \neq \pi_q(\chi)$, as in the above case of (2), by using the Chinese remainder theorem, we obtain another cycle $\{\tau\}$ for which $\gcd(\xi - \tau, n) = p$. If $\xi = \chi$, then, $\xi = -\xi + 1 \pmod n$ so that $\xi = \frac{n+1}{2}$. We consider the projection $\eta = \pi_p(\xi)$, then $\eta^2 + 1 = \eta$ in $\mathbf{Z}_p$ and $x^2 - x + 1 = 0$ has no other solution in $\mathbf{Z}_p$. Therefore, η is the multiple root of $x^2 - x + 1 = 0$ in $\mathbf{Z}_p$. This occurs only in the case $p = 3$. If $p = 3$, then $q \neq 3$ and considering $\zeta = \pi_q(\xi)$, we can find another cycle in $\mathbf{Z}_q$. Using η, ζ and this cycle, we can construct the cycle $\{\tau\}$ in $\mathbf{Z}_n$ for which $\gcd(\xi - \tau, n) = q$.

Remarks. As for Example 2, we have

$$\{\pi_5(252), \pi_5(80), \pi_5(206)\} = \{2, 0, 1\}, \quad \{\pi_{59}(252), \pi_{59}(80), \pi_{59}(206)\} = \{16, 21, 29\}.$$

Solving

$$\begin{cases} x = 2 \pmod 5 \\ x = 21 \pmod{59} \end{cases}, \quad \begin{cases} x = 0 \pmod 5 \\ x = 29 \pmod{59} \end{cases}, \quad \cdots, \quad \begin{cases} x = 1 \pmod 5 \\ x = 16 \pmod{59} \end{cases},$$

we have $\chi_1 = 257, \chi_2 = 265, \chi_3 = 16$ and the cycle $\{257, 265, 16\}$, which is obtained by the iteration with the initial value 3. Further, solving

$$\begin{cases} x = 2 \pmod 5 \\ x = 29 \pmod{59} \end{cases}, \quad \begin{cases} x = 0 \pmod 5 \\ x = 16 \pmod{59} \end{cases}, \quad \cdots, \quad \begin{cases} x = 1 \pmod 5 \\ x = 21 \pmod{59} \end{cases},$$

we have $\chi_1 = 147, \chi_2 = 75, \chi_3 = 21$ and the cycle $\{147, 75, 21\}$, which is the cycle obtained by the iteration with the initial value 7. We can also find the factor 5 of 295 by the cycles $\{252, 80, 206\}$ and $\{147, 75, 21\}$.

As for Example 3, setting $\chi = -5 + 1 = 17 \pmod{21}$, we have another cycle $\{17\}$.

Finally, we remark that it may be an interesting problem whether the theorem is satisfied for any n and any polynomial $f(x)$.

References

[1] J.A.Buchmann, Introduction to cryptography, Springer-Verlag, 2000.

[2] N.Koblitz, A course in number theory and cryptography, Springer-Verlag, 1987.

[3] J.M.Pollard, A Monte Carlo method for factorization, BIT 15, 1975, 331-334.

(受理　平成15年 3 月19日)