2次漸化式で与えられる数列の各項を自然数で割った余りの周期性

金森大成

2026年2月20日

要旨

2次漸化式 $a_{n+1}=sa_n{}^2+ta_n+u$ で与えられる数列を自然数で割った余りの周期性について, 具体例を通じて, 周期性の有無やそれに関する性質を証明した.

1　はじめに

先行研究 [1] において, 次の1次の隣接 m 項間漸化式

$$a_{n+m+1}=s_{m-2}a_{n+m-2}+s_{m-3}a_{n+m-3}+\cdots+s_1a_{n+1}+s_0a_n\ \ (n\geq 1)$$

(ただし,$a_1,a_2,\cdots,a_{m-1},s_0,s_1,\cdots,s_{m-2}$ は自然数である.) で与えられた数列の各項を **10** で割った余りの数列を考えている. そのとき, m や s_i の値にかかわらず, 必ずある項から同じ数列が繰りかえされる周期性があることが知られている. 本研究では2次の隣接2項間漸化式で与えられる数列を自然数で割った余りの周期性の有無やその性質について考察する.

2　2次漸化式で与えられる数列の各項の下1桁の周期性

2.1　数列の型の定義

ある数列において, k 項目から初めて長さ d の数列の繰り返しになっているとき, その数列の型を”k-d型”と定義する. また, d を”周期の長さ”とよぶ.

(例)　I-3型　$2,1,6\mid 2,1,6\mid 2,1,6\mid 2,\cdots$

　　Ⅱ-4型　$1\mid 2,3,3,5\mid 2,3,3,5\mid 2,3,3,5\mid 2,\cdots$

　　Ⅲ-2型　$3,8\mid 6,3\mid 6,3\mid 6,3\mid 6,\cdots$

2.2　2次漸化式 $a_{n+1}=sa_n{}^2$

2次漸化式

$$a_{n+1}=sa_n{}^2,a_1=a$$

で与えられる数列の各項を10で割ったときの余りの数列 $\{b_n\}$ を考える. ただし, a , s は0以上9以下の整数である. そこで, a , s の組をかえたときの数列 $\{b_n\}$ の型を調べた. 以下, 合同式の法は10とする.

命題 2.1. すべての $a\,,s$ の組において, 数列 $\{b_n\}$ の型は, I 型, II 型, III 型のいずれかである. また, 周期の長さは必ず 1 である.

Proof.
$n \geq 3$ のとき, $b_{n+1} = b_n$ となることを示す.

(1) $n = 3$ のとき, $b_3 = b_4$ となることを示す.

$$\{a_n\} : a\,,\ sa^2\ , s^3a^4\,, s^7a^8\,, \ldots$$
$$a_4 - a_3 = s^3a^4\,(s^2a^2 + 1)\,(s^2a^2 - 1)$$

このとき, すべての sa の値において,

$$\begin{aligned} sa\,(s^2a^2 + 1)\,(s^2a^2 - 1) \equiv 0 &\iff a_4 - a_3 \equiv 0 \\ &\iff b_3 = b_4 \end{aligned}$$

よって, $b_3 = b_4$ が成り立つ.

(2) $n = k$ のとき, $b_{k+1} = b_k$ が成り立つと仮定すると, $n = k + 1$ のとき, $b_{k+2} = b_{k+1}$ が成り立つことを示す.

$$\begin{aligned} b_{k+1} = b_k &\iff a_{k+1} - a_k \equiv 0 \\ &\iff a_k(sa_k - 1) \equiv b_{k+2} = b_{k+1} \\ &\iff a_{k+2} - a_{k+1} \equiv 0 \\ &\iff a_{k+1}(sa_{k+1} - 1) \equiv 0 \\ &\iff sa_k{}^2(s^2a_k{}^2 - 1) \equiv 0 \\ &\iff sa_k(sa_k + 1)a_k(sa_k - 1) \equiv 0 \end{aligned}$$

よって, $b_{k+1} = b_k$ が成り立つとき, $b_{k+2} = b_{k+1}$ が成り立つ.

(1), (2) より, $b_{n+1} = b_n$ が成り立つ.
したがって, すべての場合は I 型か II 型か III 型のいずれかで, 周期の長さは 1 である.

□

命題 2.2. $a\,,s$ の組を $(a\,,s)$ と表す. $(k\,,l)$ で定まる数列 $\{b_n\}$ の型と $(10-k\,,10-l)$ で定まる数列 $\{b_n\}$ の型は同じである.

Proof.
(k,l) のとき

- $b_1 = k$
- $b_2 = lk^2$
- $b_3 = l^3k^4$

$(10-k,10-l)$ のとき

- $b_1 = 10 - k$
- $b_2 = (10 - l)(10 - k)^2 \equiv 10 - lk^2$
- $b_3 = (10 - l)(10 - lk^2)^2 \equiv 10 - l^3k^4$

よって,$(\,k\,,l\,)$ で定まる数列 $\{b_n\}$ の型と $(\,10-k\,,10-l\,)$ で定まる数列 $\{b_n\}$ の型は同じである. □

3　2 次漸化式 $a_{n+1} = sa_n{}^2 + ta_n$

$$a_{n+1} = sa_n{}^2 + ta_n\,,a_1 = a$$

で与えられる数列の各項を 10 で割った余りの数列 $\{b_n\}$ を考える. ただし,$a\,,s\,,t$ は 0 以上 9 以下の整数である. そのとき,$a\,,s\,,t$ の組をかえたときの数列 $\{b_n\}$ の型を調べた. 以下, 合同式の法は 10 とする.

命題 3.1. すべての $a\,,s\,,t$ の組において, 数列 $\{b_n\}$ の型は, I 型, II 型, III 型のいずれかである.

命題 3.2. $a\,,s\,,t$ の組を $(\,a\,,s\,,t\,)$ と表す. $(\,k\,,l\,,m\,)$ で定まる数列 $\{b_n\}$ の型と $(\,10-k\,,10-l\,,m\,)$ で定まる数列 $\{b_n\}$ の型は同じである.

Proof.
(k,l,m) のとき

- $b_1 = k$
- $b_2 = lk^2 + mk$
- $b_3 = l(lk^2 + mk)^2 + m(lk^2 + mk)$

$(10-k,10-l,m)$ のとき

- $b_1 = 10 - k$
- $b_2 = (10 - l)(10 - k)^2 + m(10 - k) \equiv 10 - (lk^2 + mk)$
- $b_3 = (10 - l)(-lk^2 - mk)^2 + m(-lk^2 - mk) \equiv 10 - (l(lk^2 + mk)^2 + m(lk^2 + mk))$

よって,$(\,k\,,l\,,m\,)$ で定まる数列 $\{b_n\}$ の型と $(\,10-k\,,10-l\,,m\,)$ で定まる数列 $\{b_n\}$ の型は同じである. □

命題 3.3. $s \neq 5\,,t = 1\,,6$ のとき, 周期の長さが 2 の組が存在する. また, $\boldsymbol{t = 1}$ のとき, 周期の長さが 2 になる a の値に対し, $t = 6$ のときも周期の長さが 2 になる.

Proof.
$t = 1$ のとき,

$$a_{n+2} - a_n = sa_n{}^2\{(sa_n + 1)^2 + 1\}$$

より,

$$sa_n \equiv 2\,,6 \iff a_{n+2} - a_n \equiv 0$$

また,

$$a_{n+1} - a_n = sa_n{}^2$$

であり,$s \neq 5$ であるから,

$$a_{n+1} \not\equiv a_n$$

$a_{n+1} \not\equiv a_n$, $a_{n+2} \equiv a_n$ から, $sa \equiv 2\,,6$ のとき, I-2 型となる. また, $sa \equiv 1\,,3\,,7\,,8$ のとき, $sa_2 \equiv 2\,,6$ となるため, Ⅱ-2 型となる.
$t = 6$ のときも同様に示される. □

命題 3.4. $s = 5$ のとき, 周期の長さが 4 の組が存在する.

表 $1(a\,,3\,,t)$ の数列 $\{b_n\}$ の型

a \ t	1	2	3	4	5	6	7	8	9
1	Ⅱ-2	Ⅱ	Ⅱ	Ⅲ	Ⅲ	Ⅱ-2	Ⅱ	Ⅰ	Ⅲ
2	Ⅰ-2	Ⅲ	Ⅲ	Ⅱ	Ⅰ	Ⅰ-2	Ⅲ	Ⅲ	Ⅱ
3	Ⅱ	Ⅰ	Ⅱ	Ⅱ	Ⅱ	Ⅱ	Ⅰ	Ⅱ	Ⅱ
4	Ⅰ-2	Ⅲ	ⅠⅠ	Ⅰ	Ⅲ	Ⅰ-2	Ⅲ	Ⅱ	Ⅰ
5	Ⅱ	Ⅰ	Ⅱ	Ⅰ	Ⅱ	Ⅰ	Ⅱ	Ⅰ	Ⅱ
6	Ⅱ-2	Ⅱ	Ⅰ	Ⅲ	Ⅲ	Ⅱ-2	Ⅱ	Ⅰ	Ⅲ
7	Ⅱ-2	Ⅲ	Ⅲ	Ⅱ	Ⅱ	Ⅰ-2	Ⅲ	Ⅲ	Ⅱ
8	Ⅱ	Ⅰ	Ⅱ	Ⅱ	Ⅱ	Ⅱ	Ⅰ	Ⅱ	Ⅱ
9	Ⅱ-2	Ⅲ	Ⅱ	Ⅰ	Ⅲ	Ⅰ-2	Ⅲ	Ⅱ	Ⅱ

表 2 $(a\,,5\,,t)$ の数列 $\{b_n\}$ の型

$\boldsymbol{a}$ \ $\boldsymbol{t}$	1	2	3	4	5	6	7	8	9
1	Ⅱ	Ⅰ-4	Ⅱ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅱ-4	Ⅰ-4	Ⅱ-2
2	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2
3	Ⅱ	Ⅰ-4	Ⅱ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅱ-4	Ⅰ-4	Ⅱ-2
4	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2
5	Ⅱ	Ⅰ-4	Ⅱ	Ⅰ	Ⅱ	Ⅰ	Ⅱ-4	Ⅰ	Ⅱ
6	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2
7	Ⅱ	Ⅰ-4	Ⅱ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅱ-4	Ⅰ-4	Ⅱ-2
8	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2
9	Ⅱ	Ⅰ-4	Ⅱ-4	Ⅰ-2	Ⅱ	Ⅰ	Ⅰ-4	Ⅰ-4	Ⅰ-2

4 漸化式の部分集合がもつ代数的構造

4.1 合同式の法を 10 としたとき

$A = \{\ 0,1,2,3,4,5,6,7,8,9\ \}$ とする.
写像 $f_{st} : A \to A$ を次のように定義する.

$$f_{st}(a) \equiv sa^2 + ta \quad (a, s, t \in A)$$

また, 二項演算 $\circ$ を次のように定義する.

$$f_{rs} \circ f_{pq} = f_{rs}(f_{pq}(a)) \quad (\ p, q, r, s \in A)$$

命題 4.1. 集合 $G_1 = \{f_{00}, f_{01}, \ldots, f_{09}\}$ に対して $(G_1, \circ)$ はモノイドになる.
また, $G_2 = \{f_{50}, f_{51}, \ldots, f_{59}\}$ とすると, $G_1 = G_2$ となるため, $(G_2, \circ)$ もモノイドである.

また, そのほかの写像 f の集合と演算子 $\circ$ に群やモノイドはみられなかった.

Proof.
以下, $a, s, t, k \in A$ とする.

(1) 閉性
任意の２つの元を演算したときの結果ももとの集合の元であることを示す.
$st \equiv k$ となる s, t, k に対して,

$$sta - ka \equiv a(st - k) \equiv 0 \iff f_{0s} \circ f_{0t} = f_{0k}$$

よって, $f_{0s} \circ f_{0t} \in G_1$ を満たす.

(2) 結合法則
$(f_{0s} \circ f_{0t}) \circ f_{0k} = f_{0s} \circ (f_{0t} \circ f_{0k}) = f_{0k}(f_{0t}(f_{0s}(a)))$
よって, 結合法則が成り立つ.

(3) 単位元の存在
$f_{01}(a) = a$ より,

$$f_{0s} \circ f_{01} = f_{0s}$$

が成り立つ. よって, f_{01} は単位元である.

(1),(2),(3) より, $(G_1, \circ)$ はモノイドになる. □

4.2 合同式の法を 5 としたとき

$B = \{ 0, 1, 2, 3, 4 \}$ とする.
写像 $f_{st} : B \to B$ を次のように定義する.

$$f_{st}(a) \equiv sa^2 + ta \quad (a, s, t \in B)$$

また, 二項演算 $\circ$ を次のように定義する.

$$f_{rs} \circ f_{pq} = f_{rs}(f_{pq}(a)) \quad (p, q, r, s \in B)$$

命題 4.2. 集合 $G_3 = \{f_{00}, f_{01}, \ldots, f_{04}\}$ に対して $(G_3, \circ)$ は群になる.
また, そのほかの写像 f の集合と演算子 $\circ$ に群やモノイドはみられなかった.

Proof.
以下, $a, s, t, k \in B$ とする.

(1) 閉性
任意の２つの元を演算したときの結果ももとの集合の元であることを示す.
$st \equiv k$ となる s, t, k に対して,

$$sta - ka \equiv a(st - k) \equiv 0 \iff f_{0s} \circ f_{0t} = f_{0k}$$

よって, $f_{0s} \circ f_{0t} \in G_3$ を満たす.

(2) 結合法則
$(f_{0s} \circ f_{0t}) \circ f_{0k} = f_{0s} \circ (f_{0t} \circ f_{0k}) = f_{0k}(f_{0t}(f_{0s}(a)))$
よって, 結合法則が成り立つ.

(3) 単位元の存在
任意の s の値において
$f_{0s} \circ f_{0t} = f_{0s}$ となるような t の値が存在することを示す.
$f_{01} \circ f_{01} = f_{01}$, $f_{02} \circ f_{01} = f_{02}$, $f_{03} \circ f_{01} = f_{03}$, $f_{04} \circ f_{01} = f_{04}$.
よって, f_{01} が単位元である.

(4) 逆元の存在
任意の s の値において
$f_{0s} \circ f_{0t} = f_{01}$ となるような t の値が存在することを示す.
$f_{01} \circ f_{01} = f_{01}$, $f_{02} \circ f_{03} = f_{01}$, $f_{03} \circ f_{02} = f_{01}$, $f_{04} \circ f_{04} = f_{01}$,
よって, すべての元に対して逆元が存在する.

(1),(2),(3),(4) より,$(G_3 , \circ)$ は群になる. □

5 2次漸化式 $a_{n+1} = sa_n{}^2 + ta_n + u$ で与えられる数列を自然数で割った余りの周期性

2 次漸化式

$$a_{n+1} = sa_n{}^2 + ta_n + u , a_1 = 1 \quad (s , t , u \in A)$$

で与えられる数列の各項を一般の自然数 m で割ったときの余りの数列 $\{b_n\}$ について考えた。そのとき s , t , u の組をかえたときの数列 $\{b_n\}$ の型を調べた.

命題 5.1. $m = 2k$ のとき, $(s, t, u) = (k, k + 1, 1)$ のとき, $b_n = n$ となる, つまり, 周期の長さが m になる.

Proof.
$(k , k + 1 , 1)$ のとき,
$a_{n+1} = ka_n{}^2 + (k + 1)a_n + 1 = (ka_n + 1)(a_n + 1)$
と表される.
$a_{2l+1} = (ka_{2l} + 1)(a_{2l} + 1) = (2kl + 1)(2l + 1) \equiv 2l + 1 \pmod{2k}$
$a_{2l+2} = (ka_{2l+1} + 1)(a_{2l+1} + 1) = (2kl + k + 1)(2l + 2) \equiv 2l + 2 \pmod{2k}$
よって, $b_n = n$ となる. □

補題 5.2. 素数 q と $1 \leq a \leq q - 1$ をみたす整数 a に対し,

$$at_1 \equiv at_2 \pmod{q} \text{ (ただし, } 1 \leq t_1, t_2 \leq q - 1)$$

をみたす整数 t_1, t_2 は存在しない.

Proof.
t_1, t_2 が存在するには,

$$at_1 - at_2 \equiv 0 \iff a(t_1 - t_2) \equiv 0 \pmod{q}$$

が成り立つ必要があるが, $a, t_1 - t_2 \not\equiv q \pmod{q}$, q は素数であるため, 上の式は成り立たない. □

命題 5.3. 3 以上の相異なる素数 p, q を用いて, $m = pq^2$ とする. (s, t, u) を整数 a, b を用いて, $(pqa, pqb + 1, u)$ と表したとき, $b_n \neq n$ となるような周期の長さが m の組が存在する a, b, u の条件は,

i $q = 6k \pm 1$ のとき, a, b は任意で,u は pq と互いに素

ii $q = 3$ のとき, b は任意で, $2pa + u$ と pq は互いに素, u は 3 の倍数でない.

Proof.
$m = pq^2$ のとき (ただし, p, q は素数),
$(\, s,\, t,\, u\,)$ は $(\, pqa,\, pqb + 1,\, u\,)$ と表される.
よって, 考える式は

$$a_{n+1} = pqa{a_n}^2 + (pqb + 1)a_n + u$$

(1) $u = qk$ のとき (ただし, k は自然数)

$$a_{n+1} \equiv a_n (\bmod q)$$

よって, b_n が m 以下のすべての自然数をとることに矛盾するため, $v = qk$ は不適.

(2) $v = qk + i$ のとき (i は 0 以上 $q - 1$ 以下の整数)
補題 5.3. より i がどんな値でも, a_{qn+1} から $a_{q(n+1)}$ を q で割った余りは全て異なる. よって, $i = 1$ のときを考える.

$$a_{n+1} \equiv a_n + u \equiv a_n + 1 \,(\bmod q\,)$$
$$a_n = 1$$

より,

$$a_{qn+i} \equiv i \,(\bmod q\,)$$

ここで, $q = 2l + 1$ とする.

- $1 \leq i \leq l$ のとき, $a_{qn+i+1} \equiv a_{qn+i} + i^2pqa + ipqb + u \,(\bmod pq^2)$
- $0 \leq i \leq l - 1$ のとき, $a_{qn+q-i} \equiv a_{qn+q-(i+1)} + (i+1)^2pqa + (q - (i+1))pqb + u \,(\bmod pq^2)$
- $i = l + 1$ のとき, $a_{qn+l+1} \equiv a_{qn+q} + u \,(\bmod pq^2)$

よって,

$$\begin{aligned}
a_{q(n+1)} &\equiv a_{qn} + \sum_{i=1}^{l}(i^2pqa + ipqb + u) + \sum_{i=1}^{l-1}((i+1)^2pqa + (q - (i+1))pqb + u) + u \\
&= a_{qn} + \sum_{i=1}^{l}(i^2pqa + ipqb + u) + \sum_{i=1}^{l}(i^2pqa + (q - i)pqb + u) + u \\
&= a_{qn} + \sum_{i=1}^{l}(2i^2pqa + pq^2b + 2u) + u \\
&= a_{qn} + \frac{1}{3}l(l+1)(2l+1)pqa + lpq^2b + (2l+1)u \\
&= a_{qn} + \frac{1}{3}\frac{q-1}{2}\frac{q+1}{2}pq^2a + \frac{q-1}{2}pq^2b + qu \\
&= a_{qn} + pq^2(\frac{(q^2-1)a}{12} + \frac{(q-1)b}{2}) + qu \\
&\equiv a_{qn} + pq^2\frac{(q^2-1)a}{12} + qu \,(\,mod\, pq^2\,)\,(\frac{(q-1)b}{2}\text{は整数より}) \\
&= a_{qn} + q(pq\frac{(q^2-1)a}{2} + u)
\end{aligned}$$

(1), (2) より, $pq\frac{(q^2-1)a}{2}+u$ が pq と互いに素であればよい.

i $q=6k\pm1$ のとき,

$$\begin{aligned}\frac{pq(q^2-1)a}{12}+u&=\frac{((6k\pm1)^2-1)pqa}{12}+u\\&=\frac{36k^2\pm12k}{12}pqa+u\\&=k(3k\pm1)pqa+u\\&\equiv v\,(\,mod\,pq\,)\end{aligned}$$

よって, v は pq と互いに素である.

ii $q=3$ のとき, $a_{qn+q}\equiv a_{qn}+2pa+u\,(\,\mathrm{mod}\,3p\,)$
よって, $2pa+u$ は $3p$ と互いに素である.

□

予想

(1) $m=2k$ としたとき, $b_n=n$ となるような周期の長さ m の組が存在するときの $(s\,,t\,,u)$ の組は,$(k\,,k+1\,,1)$ のみである.

(2) m を素因数分解したとき, すべての素因数が奇数かつ, 少なくとも 1 つの同じ素因数が 2 回以上かけられているとき, $b_n\neq n$ となるような周期の長さが m の組が存在する.

(3) m が $(1)\,,(2)$ 以外のとき, 周期の長さが m の組は存在しない.

謝辞

本研究を行うにあたり, 松本先生, 秋葉先生, 河端先生, 谷島先生や同級生の細木悠音さんから研究の方針や証明の手法など様々なアドバイスをいただきました. ここに感謝申し上げます.

参考文献

[1] 田中義久・上山健太・山上佳男, 隣接 m 項間漸化式の定める数列の下一桁の周期性, 弘前大学教育学部紀要, 127, 57, 66, 2022