IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ser. 2 (Jan. – Feb. 2024), PP 48-70
www.iosrjournals.org

Reproof of the 3x+1 problem

Ming Xian[1] Xunwei Zhou[2] Zi Xian[3]
Fushun Geographical Information Bureau, Fushun, Liaoning province 113008, China
Beijing Key Laboratory of Information Service Engineering, Beijing Union University, Beijing 100101, China
Fushun Library, Fushun, Liaoning province 113006, China

Abstract:
We remedy the defect of our previous paper with respect to the insufficient argument of the necessary premises. To this end, based on the leftward extendedness of the px+q sequences, px+q infinite trees are built; based on the properties of the px+q infinite trees, the unprovability of the px+q sequences being noncircular sequences is revealed. Consequently, the proof of the 3x+1 problem in this paper is rigorous. Since the 3x+1 problem is equivalent to 3x+1 sequences, 3x+1 sequences are one kind of px+q sequences, and px+q sequences are one kind of mapping recurrent sequences. In this paper, we start with mapping recurrent sequences.

Keywords: *3x+1 problem; 3x+1 sequence; px+q sequence; mapping recurrent sequence; px+q infinite tree*

Date of Submission: 24-01-2024 Date of Acceptance: 04-02-2024

I. Introduction

In resolving the 3x+1 problem, we need to prove that "all 3x+1 sequences have equal terms". To obtain the result, we need to solve the equations of the equal terms of the 3x+1 sequences. We all know that to solve an equation, we need to establish the equation first. For this reason, we establish the equations of the equal terms of the 3x+1 sequences based on the supposition "the 3x+1 sequences have the equal terms". However, based on the principle of supposition to make such an assumption, we must take "any 3x+1 sequence does not necessarily not have an equal term" as premise. In our previous paper <<The proof of 3x+1 problem>>[1], we did not prove this premise stringently. Therefore, the aim of this paper is to remedy the defect of the previous paper.

To prove the premise "any 3x+1 sequence does not necessarily not have an equal term", we must resort to the properties of 3x+1 infinite trees. To reveal the properties of 3x+1 infinite trees, we need to expand them into px+q infinite trees. The generation of the px+q infinite trees is determined by the leftward extendedness of the px+q sequences. The in-depth discussion of the leftward extendedness of the px+q sequences in this paper lays the solid foundation for establishing px+q infinite trees. In the discussion of the leftward extendedness of the px+q sequences, we need such preliminary knowledge as the solution of $a^x \equiv b \pmod{m}$ and the equiratio residual sequences. In this paper, we provide the relevant results of this preliminary knowledge.

Because the px+q sequence is one kind of mapping recurrent sequence, some properties of the px+q sequence come from the more fundamental properties of the mapping recurrent sequence. Thus, we also discuss the fundamental properties of the mapping recurrent sequence.

Besides, Example 5 in this paper reveals an unthinkable fact: when $n\to\infty$, $c_n\to\infty$, sequence C is yet a circular sequence.

The rest of this paper is organized as follows: Section 2 introduces the mapping recurrent sequences and their circularity. Section 3 introduces the solution of $a^x \equiv b$ (mod m) and the equiratio residual sequences. Section 4 introduces the leftward extendedness of the px+q sequences. Section 5 introduces the relevant properties of the px+q infinite trees. Section 6 introduces the equations of the equal terms of the 5x+1 sequences. Section 7 is the reproof of the 3x+1 problem. Note 1 introduces the principle of supposition. Note 2 introduces the discussion of the listing of the equations and the solution of the application problems.

We make the following stipulations for the terminologies and symbols used in this paper:

1. The phrase "sequence" refers to an infinite sequence, unless otherwise specified.
2. The lowercase italic Latin letters used as variables denote positive integers, unless otherwise specified.
3. The uppercase italic Latin letters (or with primes or with subscribes) denote the sequences, and their corresponding lower case italic Latin letters denote the general terms of these sequences. For example, the general terms of the two sequences A, B' are a_n, b'_n respectively. Sometimes, $\{a_n\}$ is used to denote the sequence A, and $\{b'_n\}$ is used to denote the sequence B'.
4. N and N_O are two special symbols; N denotes the set of positive integers, and N_O denotes the set of positive odd numbers.

We define two operators frequently used in this paper.
Definition 1: Let us suppose that $0\le a<m$. Then, we denote $a\equiv b \pmod m$ as $a=(b)\bmod m$. We call $()\bmod m$ the minimal nonnegative residual operator modulus m.
From Definition 1, we know that if a is a minimal nonnegative residue of b modulus m, then $a=(b)\bmod m$.
For example, $(9)\bmod 7=2$, $(78)\bmod 63=15$.
The following are the properties of the minimal nonnegative residual operator that are used in this paper:
Property 1. If $a=(b)\bmod m$ or $(a)\bmod m=(b)\bmod m$, then $a\equiv b \pmod m$;
Property 2..$(a+b)\bmod m=((a)\bmod m+b)\bmod m$; (Changing "+" to "×", this property also holds).)
Property 3..$(a^n)\bmod m=(((a)\bmod m)^n)\bmod m$; Property 4. When $n\mid m$, $((a)\bmod m)\bmod n=(a)\bmod n$;
Property 5. $(a)\bmod m\equiv a \pmod m$;
Property 6. There necessarily exists $k\ge 0$ such that $a=km+(a)\bmod m$.
Definition 2: We denote b/a^n satisfying the relations $a^n\mid b$, $a^{n+1}\nmid b$ as $\beta(b)_a$ (i.e., $\beta(b)_a= b/a^n$). We call $\beta()_a$ the de-a factor operator. $\beta(\ )_2$ is simplified as $\beta()$. $\beta()$ is also called the deeven operator (Deeven is a new word coined by the authors).
From Definition 2, we know that $\beta(b)_a$ is the result of b eliminating factor a. Obviously, $\beta(b)_a$ is an integer without factor a.
For example, $\beta(45)_3=45/3^2=5$, $\beta(40)=40/2^3=5$.
Now, let us investigate the sequence $\{a_n\}$: 1,2,3,4,5,… and the sequence $\{b_n\}$: 2,4,6,8,10,…. Obviously, the terms of the two sequences have the following relationship: $b_1=2a_1,\ldots$, $b_n=2a_n$, …. Hence, we have:

Definition 3: Let us suppose that there is a function f such that sequences $\{a_n\}$ and $\{b_n\}$ have the following relationship: $b_1=f(a_1),\ldots$, $b_n=f(a_n)$, …. Then, we call $\{b_n\}$ the parasitic sequence of $\{a_n\}$ and denote $\{b_n\}$ as 〖$b_n=f(a_n)$〗.
People usually call the sequence $\{a_n\}$: 8,10, 1,2,3,1,2,3, … a circular sequence with the circular length being 3, for in sequence $\{a_n\}$ there are $a_3=a_{3+3n}=1$, $a_4=a_{4+3n}=2$, $a_5=a_{5+3n}=3$, …($n=1,2,\ldots$), or, for every l ($3\le l$), there is, $a_l=a_{l+3n}$, $n=1,2,\ldots$.
Now, we give the definition of a circular sequence.
Definition 4: Let us suppose that from the *ith* term of the sequence $\{a_n\}$ onward, every term satisfies $a_i=a_{i+hn}$, $a_{i+1}=a_{i+hn+1}$, …($n=1,2,\ldots$), i.e., for every l ($i\le l$), there is $a_l=a_{l+hn}$ in the sequence $\{a_n\}$. Then, we call $\{a_n\}$ a circular sequence, call h the circular length of $\{a_n\}$, and call a_l($i\le l$) the circular terms of $\{a_n\}$.
From Definition 4, we know that when h is a circular length of the circular sequence $\{a_n\}$, d ($h\mid d$) is also a circular length of $\{a_n\}$. For example, 3 is a circular length of sequence $\{a_n\}$: 8,10, 1,2,3,1,2,3,1,2,3, …, and 6,9, … are also circular lengths of $\{a_n\}$. We call the minimum of the circular lengths the minimal circular length of $\{a_n\}$.
It is not hard to see that, when the third term of $\{a_n\}$ is a circular term of $\{a_n\}$, the terms after the third term are all circular terms of $\{a_n\}$. Thus there is,,
Property 7. If a_l is a circular term of $\{a_n\}$, then a_j ($l<j$) are all circular terms of $\{a_n\}$.
From Definition 4, we know that, when a_k is a circular term of the circular sequence $\{a_n\}$, if the circular length of $\{a_n\}$ is h, then $a_k=a_{k+h}$. Conversely,
Property 8. When a_k is a circular term of the circular sequence $\{a_n\}$, if $a_k\ne a_{k+h}$, then h is not a circular length of $\{a_n\}$.
Definition 5: Let us suppose that a_k is the first circular term of the circular sequence $\{a_n\}$. If $k=1$, then we call $\{a_n\}$ a pure circular sequence ; if $k>1$, then we call $\{a_n\}$ a mixed circular sequence, and we call $a_1,\ldots,a_{k-1}$ noncircular terms of circular sequence A.
From Definition 5, we know that, in $\{a_n\}$: 8,10,1,2,3,1,2,3,1,2,3, … , a_1, a_2 are the noncircular terms, a_l($3\le l$) are the circular terms. $\{a_n\}$ is a mixed circular sequence.
Basic theorem 1: Let us suppose that sequence B is a parasitic sequence of sequence A (i.e., B is 〖$b_n=f(a_n)$〗). Thus, if A is a circular sequence, then B is also a circular sequence.
Proof: According *to* 〖$b_n=f(a_n)$〗,

$$b_l=f(a_l) \tag{1}$$

$$b_{l+nh}=f(a_{l+nh}). \tag{2}$$

Let us suppose that a_i is the first circular term of the circular sequence A, and h is its circular length.
From Definition 4, we know that for every l ($i \le l$),
$a_l = a_{l+nh}$ (3)
If the arguments are equal, then the function values are equal. Therefore, from (3), we know,
$f(a_l) = f(a_{l+nh})$ (4)
From (1) and (4), we know,
$b_l = f(a_{l+nh})$ (5)
From (5) and (2), we know that $b_l = b_{l+nh}$. From Definition 4, we know that $\{b_n\}$ is a circular sequence.
Q.E.D.
For example, the parasitic sequence of circular sequence A: 8,10, 1,2,3,1,2,3,1,2,3,… is 〖$b_n = 2a_n$〗: 16,20, 2,4,6,2,4,6,2,4,6,…, which is also a circular sequence.

It is not hard to see that the equidifference sequence A with the first term being 1 and the common difference being 3 is A: 1,4,7,10,…, which can be denoted as
$a_1 = 1$, $a_2 = a_1 + 3$, $a_3 = a_2 + 3$, …, $a_{n+1} = a_n + 3$, ….
When we use $f(x)$ to denote $x+3$, sequence A can also be denoted as
$a_1 = 1$, $a_2 = f(a_1)$, $a_3 = f(a_2)$, …, $a_{n+1} = f(a_n)$, ….
Obviously, here f is a mapping.
Definition 6: Let us suppose that the first term of the sequence A is $a_1 = a$. If there is a mapping f such that $a_2 = f(a_1)$, …, $a_{n+1} = f(a_n)$, … then we call A a mapping recurrent sequence and denote A as $\{a_1 = a, a_{n+1} = f(a_n)\}$.
The mapping recurrent sequences this paper mainly discusses include: $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$, $\{a_1 = a, a_{n+1} = \beta(pa_n + q)\}$, $\{a_1 = a, a_{n+1} = 2^{\delta p(2)} a_n + b\}$, $\{a_1 = a, a_{n+1} = (a_n + b) \bmod m\}$, etc.
Basic theorem 2: Let us suppose that A is $\{a_1 = a, a_{n+1} = f(a_n)\}$. If $a_i = a_j$, $1 \le j - i = h$, then A is a circular sequence with a circular length of h.
Proof: From $\{a_1 = a, a_{n+1} = f(a_n)\}$ we know,
$a_{i+1} = f(a_i)$ (6)
$a_{i+h+1} = f(a_{i+h})$. (7)
From $a_i = a_j$ and $j - i = h$, we know that $a_i = a_{i+h}$.
Since a_i and a_{i+h} are the arguments, $f(a_i)$ and $f(a_{i+h})$ are their function values. If the arguments are equal, then the function values are equal. Therefore,
$f(a_i) = f(a_{i+h})$ (8)
From (6) and (8), we know,
$a_{i+1} = f(a_{i+h})$ (9)
From (7) and (9), we know that $a_{i+1} = a_{i+h+1}$.
The above process shows that, from $a_i = a_{i+h}$, we can obtain $a_{i+1} = a_{i+h+1}$. Likewise, from $a_{i+1} = a_{i+h+1}$, we can obtain $a_{i+2} = a_{i+h+2}$,…; from $a_{i+h-1} = a_{i+2h-1}$, we can obtain $a_{i+h} = a_{i+2h}$.
Thus, from $a_i = a_{i+h}$ and $a_{i+h} = a_{i+2h}$, we can obtain $a_i = a_{i+2h}$. Similarly, we can obtain $a_i = a_{i+nh}$.
Similar to the above process, we can prove that $a_{i+1} = a_{i+nh+1}$. Similarly, we know that for every l ($i \le l$), $a_l = a_{l+nh}$.
According to Definition 4, A is a circular sequence with a circular length of h.
Q.E.D.
Basic theorem 2 tells us that, as long as in mapping recurrent sequence A, two terms a_i and a_j equal to each other ("Terms equal to each other" are also called equal terms), A is a circular sequence. Basic theorem 2 also tells us,
Property 9. The equal terms in mapping recurrent sequence A are necessarily the circular terms of A and vice versa.
For example, $\{a_1 = 2, a_{n+1} = (10a_n) \bmod 14\}$: 2,6,4,12,8,10,2,6,4,12,8,10,…
The sequence in question is calculated as follows: It is known that $a_1 = 2$. From $a_1 = 2$ and $a_2 = (10a_1) \bmod 14$, we obtain $a_2 = (20) \bmod 14 = 6$
From $a_2 = 6$ and $a_3 = (10a_2) \bmod 14$, we obtain $a_3 = (60) \bmod 14 = 4$
……
There are $a_1 = a_7 = 2$ in the sequence. Thus, $\{a_1 = 2, a_{n+1} = (10a_n) \bmod\}$ is a circular sequence. In addition, a_1 and a_7 are the circular terms of $\{a_1 = 2, a_{n+1} = (10a_n) \bmod\}$. As a_1 is a circular term,

{a_1=2，a_{n+1}＝$(10a_n)\text{mod}$} is a pure circular sequence.
For convenience, we call the sequence *A* that is both a mapping recurrent sequence and a

circular sequence a mapping recurrent circular sequence below.

Property 10. Let us suppose that A is a mapping recurrent circular sequence. I. If h is the minimal circular length of A, then the consecutive h terms of A do not equal one another. II. If h is the circular length of A and circular terms $a_k \neq a_i (k < i < k+h)$, then h is the minimal circular length of mapping recurrent circular sequence A.

Proof: Prove I. Let us suppose that in the consecutive h terms $a_k, a_{k+1}, \ldots, a_{k+h-1}$ of A there is $a_i = a_j$, $k \leq i < j < k+h$.

Let $j - i = n$. Then, $n < h$, $a_j = a_{i+n} = a_i$.

From $a_{i+n} = a_i$ and basic theorem 2, we know that $n (< h)$ is a circular length of mapping recurrent circular sequence A, which contradicts h being the minimal circular length of A. Therefore, I holds.

Prove II. From h being a circular length of A and a_k being a circular term, we know that $a_k = a_{k+h}$. From $a_k \neq a_i$ $(k < i < k+h)$, we know that in the consecutive $h+1$ terms $a_k, a_{k+1}, \ldots, a_{k+h}$ of A, only a_{k+h} and a_k equal each other. That is, when $h' < h$, $a_k \neq a_{k+h'}$.

From this and Property 8, we know that when $h' < h$, h' is not a circular length of A. That is, the circular length of A cannot be less than h. Q.E.D.

II. The solution of $a^x \equiv b \pmod m$ and equiratio residual sequences

Since the solution of the exponential congruence equation $a^x \equiv b \pmod m$ and the relevant properties of the equiratio residual sequences are the prerequisite knowledge for the leftward extendedness of the $px+q$ sequences discussed in the next section, we discuss them specifically.

Definition 7. If $a^x \equiv b \pmod m$ has a solution, then we say that b is a genuine residue of a^x modulus m; otherwise, we say that b is a pseudoresidue of a^x modulus m.

For example, $4^x \equiv 9 \pmod{13}$ has a solution $x=4$. Thus, 9 is a genuine residue of 4^x modulus 13.

$4^x \equiv 8 \pmod{13}$ has no solution. Thus, 8 is a pseudoresidue of 4^x modulus 13.

Definition 8. Let us suppose that A is $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$, $0 < a < m$. Then, we call A a residual sequence of common ratio a modulus m, equiratio residual sequence for short. If $(a, m) = 1$, then we call A the common ratio a and modulus m mutually prime residual sequence, mutually prime residual sequence for short.

From Definition 8, we know that every term in A is less than modulus m. From the pigeonhole principle, we know that A has equal terms. From basic theorem 2, we know that A is a circular sequence.

For example, the equiratio residual sequence $\{a_1 = 4, a_{n+1} = (4a_n) \bmod 13\}$: 4,3,12,9,10,1,4,… is a circular sequence with every term being less than 13. $\{a_1 = 10, a_{n+1} = (10a_n) \bmod 56\}$: 10,44,48,32,40,8,24,16,48,… is a circular sequence with every term being less than 56.

Property 11. Equiratio residual sequences are circular sequences.

Theorem 1. The *nth* term in $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$ is $a_n = (a^n) \bmod m$, $n = 1, 2, \ldots$.

Proof: We use mathematical induction.

Step 1: The case of $n=1$. From Definition 8, we know that $a_1 = a < m$. From Definition 1, we know that $a_1 = (a^1) \bmod m$. In this case, the theorem holds.

Step 2: Let us suppose that when $n=k$, $a_k = (a^k) \bmod m$. Step 3: We prove when $n=k+1$, $a_{k+1} = (a^{k+1}) \bmod m$.

From the induction supposition and Property 5, we know that $a_k = (a^k) \bmod m \equiv a^k \pmod m$. From $a_k \equiv a^k \pmod m$, we obtain $a \cdot a_k \equiv a^{k+1} \pmod m$.

From $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$ we know, $a_{k+1} = (a \cdot a_k) \bmod m \equiv a \cdot a_k \equiv a^{k+1} \pmod m$. From $a_{k+1} = (a \cdot a_k) \bmod m$ and Definition 1, we know $a_{k+1} < m$.

From $a_{k+1} \equiv a^{k+1} \pmod m$, $a_{k+1} < m$, $(a^{k+1}) \bmod m < m$ we know, $a_{k+1} = (a^{k+1}) \bmod m$. Q.E.D. For example, the 4th term a_4 in $\{a_1 = 2, a_{n+1} = (2a_n) \bmod 9\}$: 2,4,8,7,5, 1,2,… is $a_4 = 7 = (2^4) \bmod 9$.

From Theorem 1, we know that various terms in $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$ are the minimal nonnegative residue moduli m of their corresponding terms $a, a^2, \ldots, a^n$ in the equiratio sequence. This is the origin of the name "equiratio residual sequences". We also know that

Conclusion 1. $x = k$ is a solution of $a^x \equiv b \pmod m$ if and only if $(b) \bmod m$ is the *kth* term of $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$ Or $a_k \equiv b \pmod m$.

(Note: $\{a_1 = a, a_{n+1} = (a \cdot a_n) \bmod m\}$ has no 0th term. Hence, when $a^x \equiv 1 \pmod m$ has solutions, we should add the solution "$x=0$".)

For example, we know that $\{a_1 = 6, a_{n+1} = (6a_n) \bmod 56\}$: 6,36,48,8,48,8,… is a mixed circular sequence with a circular length of 2. 6 is the first term of the sequence in question; thus, $x=1$ is a solution of $6^x \equiv 6 \pmod{56}$; 36 is the second term of the sequence in question; thus, $x=2$ is a solution of $6^x \equiv 36 \pmod{56}$; 48

is the $(3+2n)$th (n=0,1,2,…) term of the sequence in question; thus, $x=3+2n$ are solutions of $6^x\equiv 48 \pmod{56}$; 8 is the $(4+2n)$*th* term of the sequence in question; thus, $x=4+2n$ are solutions of $6^x\equiv 8 \pmod{56}$.

We also know that in the minimal nonnegative residual system modulus 56, only 6, 36, 48,8 are the genuine residues of 6^x modulus 56, and the others are all pseudoresidues of 6^x modulus 56.

Another example: When solving $2^x\equiv 1 \pmod{63}$, first, we can calculate $\{a_1=2,\ a_{n+1}=(2a_n) \bmod 63\}$: 2,4,8,16,32,1, 2,…, from which we can obtain that the solutions of $2^x\equiv 1 \pmod{63}$ are $x=6n$ (n=0,1,2,…). (Note that $x=0$ is a solution of $2^x\equiv 1 \pmod{63}$.)

$\{a_1=2,\ a_{n+1}=(2a_n) \bmod 63\}$: 2,4,8,16,32,1, 2,…. Therefore, in the minimal nonnegative residual system modulus 63, only 2, 4, 8, 16, 32, and 1 are the genuine residues of 2^x modulus 63, and the others are all pseudoresidues of 2^x modulus 63.

Now, we discuss the relationship between mutually prime residual sequences $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ and $\delta_a(m)$ (i.e., the order of a modulus m).

From the properties of order, we know that when $(a, m)=1$, there necessarily exists h such that $a^h\equiv 1 \pmod m$ (i.e., $(a^h) \bmod m=1$). This means that for a mutually prime residual sequence $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$, there necessarily exists the term $a_h=1$ ($h\in N$). Thus, we have:

Conclusion 2. Let us suppose that A is a mutually prime residual sequence $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$. If a_h is the first term in A that equals 1, then $h=\delta_m(a)$.

For example, the sequence is $\{a_1=2,\ a_{n+1}=(2a_n) \bmod 9\}$: 2,4, 8,7, 5,1,2,…, in which $a_6=(2^6) \bmod 9=1$ is the first term equaling 1 in the sequence in question; thus, $\delta_9(2)=6$.

In addition, when $h=\delta_m(a)$, the term a_{h+1} in $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ is $a_{h+1}=(a\cdot a_h) \bmod m=a=a_1$. Therefore, from basic theorem 2 and Definition 5, we can also obtain:

Conclusion 3. The mutually prime residual sequence $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ is necessarily a pure circular sequence, and its minimal circular length is $\delta_m(a)$.

Conclusions 2 and 3 tell us that the set formed by the first $\delta_m(a)$ terms in the mutually prime residual sequence $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ is one formed by all of the terms in the sequence in question.

For this reason, we call the sequence formed by the first $\delta_m(a)$ terms in the mutually prime residual sequence $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ the simplest sequence of $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ "simplest $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$" for short.

All of the simplest sequences modulus 11 are shown below: Simplest $\{a_1=1,\ a_{n+1}=(a_n) \bmod 11\}$: 1.

Simplest $\{a_1=2,\ a_{n+1}=(2a_n) \bmod 11\}$: 2,4, 8,5, 10,9,7, 3,6, 1.

Simplest $\{a_1=3,\ a_{n+1}=(3a_n) \bmod 11\}$: 3, 9, 5, 4, 1.

Simplest $\{b_1=4,\ b_{n+1}=(4b_n) \bmod 11\}$: 4, 5, 9, 3, 1.

Simplest $\{a_1=5,\ a_{n+1}=(5a_n) \bmod 11\}$: 5, 3, 4, 9, 1.

Simplest $\{a_1=6,\ a_{n+1}=(6a_n) \bmod 11\}$: 6,3, 7,9, 10, 5,8, 4,2, 1.

Simplest $\{a_1=7,\ a_{n+1}=(7a_n) \bmod 11\}$: 7,5, 2,3, 10, 4,6, 9,8, 1.

Simplest $\{a_1=8,\ a_{n+1}=(8a_n) \bmod 11\}$: 8,9, 6,4, 10,3,2, 5,7, 1.

Simplest $\{a_1=9,\ a_{n+1}=(9a_n) \bmod 11\}$: 9,4, 3,5, 1. Simplest $\{a_1=10,\ a_{n+1}=(10a_n) \bmod 11\}$: 10, 1.

Conclusion 4. Every simplest $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ terminates at "1", or $a_{\delta_m(a)}=1$.

That is,

Conclusion 5. The number of terms in the simplest $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ equals $\delta_m(a)$. The above two conclusions provide a simple iterative algorithm for the calculation of order. Now, we continue the investigation of simplest $\{a_1=6,\ a_{n+1}=(6a_n) \bmod 11\}$: 6,3, 7,9, 10, 5,8, 4,2, 1.

The sequence has 10 terms; therefore, $\delta_{11}(6)=10$. We also discover that the inverse of $a_1=6$ modulus 11 is $a_1^{-1}=a_9=2$ (Please note that the sum of the subscripts of a_1^{-1} and a_9 equals 10); the inverse of $a_2=3$ is $a_2^{-1}=a_8=4$; …; the inverse of $a_5=10$ is $a_5^{-1}=a_5=10$.

Theorem 2. Let us suppose that a_k^{-1} ($a_k^{-1}<m$) in the mutually prime residual sequence $\{a_1=a,\ a_{n+1}=(a\cdot a_n) \bmod m\}$ is the inverse of term a_k modulus m. Then, $a_k^{-1}=a_i$, $k+i=n\delta_m(a)$, n=1,2,…, or $(a^k)^{-1}\equiv a^{n\delta_m(a)-k} \pmod m$.

Proof: There are necessarily positive integers i, k such that,

$$k+i=n\delta_m(a),\ n=1,2,\ldots. \tag{10}$$

From Theorem 1, we know that $a_k=(a^k) \bmod m$, $a_i=(a^i) \bmod m$. From Property 5, we know that,

$$a_k\equiv a^k \pmod m,\ a_i\equiv a^i \pmod m \tag{11}$$

From (10) and

(11), we know that

$a_k a_i \equiv a^{k+i} \equiv a^{n\delta m(a)}$ (mod m) (12)

From $a^{n\delta m(a)} \equiv 1$ (mod m) and (12), we know that

$a_k a_i \equiv 1$ (mod m) (13)

$a^{k+i} \equiv 1$ (mod m) (14)

From (13), we know that

$a^{-1} \equiv a$ (mod m) (15)

From the terms in $\{a_1 = a,\ a_{n+1} = (a \cdot a_n) \bmod m\}$ are less than m, we know that

$a_k^{-1} < m$ and $a_i < m$ (16)

From (15), (16) and (10), we know that $a_k^{-1} = a_i$, $k+i = n\delta m(a)$.

Alternatively, from (14) and (10), we obtain $(a^k)^{-1} \equiv a^i \equiv a^{n\delta m(a)-k}$ (mod m).Q.E.D. Let $i = n\delta m(a) - k$. From $(a^k)^{-1} \equiv a^{n\delta m(a)-k}$ (mod m) in Theorem 2, we know that

Conclusion 6. If $(a, m)=1$, then there are necessarily positive integers k, i such that $(a^k)^{-1} \equiv a^i$ (mod m).

Let n, $k=1$. From $a_k^{-1} = a_i$, $i = n\delta_m(a) - k$ in Theorem 2, we know that $a_1^{-1} = a_{\delta m(a)-1}$. Thus, Conclusion 7. a^{-1} is the term second from the right in simplest $\{a_1 = a,\ a_{n+1} = (a \cdot a_n) \bmod m\}$.

Conclusions 5 and 7 tell us that by calculating the simplest $\{a_1 = a,\ a_{n+1} = (a \cdot a_n) \bmod m\}$, we can obtain two results $\delta m(a)$ and a^{-1} at the same time. The former is the number of terms in the sequence in question, and the latter is the term second from the right in the sequence in question.

III. The leftward extendedness of the *px+q* sequences

The definition of the $px+q$ sequences is shown below.

Definition 9. Let us suppose that $a, p, q \in N_O$, $p > 1$. We call the mapping recurrent sequence $\{a_1 = a,\ a_{n+1} = \beta(pa_n + q)\}$ the $px+q$ sequence. (Here, $\beta(pa_n+q) = (pa_n+q)/2^i$, i is the number of factor 2 in pa_n+q, see Definition 2)

Example 1. $\{a_1=11,\ a_{n+1}=\beta(3a_n+1)\}$: 11,17,13,5,1,1,… is a $3x+1$ sequence with the first term being 11. The sequence in question is shown below:

From $a_1=11$ we can obtain:

$a_2 = \beta(3a_1+1) = \beta(3\times11+1) = \beta(2\times17) = (2\times17)/2^1 = 17$ $a_3 = \beta(3a_2+1) = \beta(3\times17+1) = \beta(2^2\times13) = (2^2\times13)/2^2 = 13$ $a_4 = \beta(3a_3+1) = \beta(3\times13+1) = \beta(2^3\times5) = (2^3\times5)/2^3 = 5$

$a_5 = \beta(3a_4+1) = \beta(3\times5+1) = \beta(2^4\times1) = (2^4\times1)/2^4 = 1$

$a_6 = \beta(3a_5+1) = \beta(3\times1+1) = \beta(2^2\times1) = (2^2\times1)/2^2 = 1$

……

Thus, we see that the $px+q$ sequences are special kinds of sequences formed by the iterative processes by using odd number a as the starting point and by using p and q as the parameters.

We know that when $p=5$ and $q=3$, the $px+q$ sequence formed is called the $5x+3$ sequence. That is, only if p and q are definite odd numbers, "the $px+q$ sequence" is a definite sequence.

$\{a_1=11,\ a_{n+1}=\beta(3a_n+1)\}$ is a mapping recurrent sequence and has equal terms $a_5=a_6=1$, therefore, from basic theorem 2, we know that it is a circular sequence with a circular length of 1.

$\{a_1=3,\ a_{n+1}=\beta(5a_n+1)\}$: 3,1,3,… is a circular sequence with a circular length of 2.

$\{a_1=1,\ a_{n+1}=\beta(5a_n+11)\}$: 1,1,1,… is a circular sequence with a circular length of 1.

From Definition 9, we know that, $\{a_1=11,\ a_{n+1}=\beta(3a_n+1)\}$ is a $3x+1$ sequence with the first term being 11. However, for the readers who read this paper for the first time, it is difficult to realize that the sequence is "$3x+1$ sequence with the first term being 11" from "$\{a_1=11,\ a_{n+1}=\beta(3a_n+1)\}$". Here, we provide a tip. The first term, 11, is given by a_1, which is obvious. We change "a_n" in "$3a_n+1$" to "x", and then we obtain the "$3x+1$" sequence we want.

Thus, we know that, $\{a_1=3,\ a_{n+1}=\beta(5a_n+1)\}$ is a $5x+1$ sequence with the first term being 3;

$\{a_1=1,\ a_{n+1}=\beta(5a_n+11)\}$ is a $5x+11$ sequence with the first term being 1. We expound the leftward extendedness of the $px+q$ sequences below. Sequence 1: $\{a_1=13,\ a_{n+1}=\beta(5a_n+1)\}$ 13,33,83,13, …

Sequence 2: $\{a_1=1331,\ a_{n+1}=\beta(5a_n+1)\}$ 1331,13,33,83,13, …

Sequence 3: $\{a_1=4259,\ a_{n+1}=\beta(5a_n+1)\}$ 4259,1331,13,33,83,13, … Sequence 4: $\{a_1=54515,\ a_{n+1}=\beta(5a_n+1)\}$ 54515,4259,1331,13,33,83,13, …

The above are four $5x+1$ sequences. It is not hard to see that the sequence 2 is formed by adding one term "1331" on the left of the first term 13 in the sequence 1; the sequence 3 is formed by adding two terms "4259, 1331" on the left of the first term in the sequence 1; and the sequence 4 is formed by adding three terms "54515, 4259, 1331" on the left of the first term in the sequence

1. For convenience, we call the sequence 2, sequence 3, and sequence 4 the level 1 leftward extension sequence, level 2 leftward extension sequence, and level 3 leftward extension sequence of sequence 1, respectively.

This section mainly discusses how to obtain the level n leftward extension sequences through the "sequence 1".

Since a in Definition 9 can be any odd number and odd number a is necessarily a term in $\{a_1=a, a_{n+1}=\beta(pa_n+q)\}$, any odd number is a term in the $px+q$ sequences. Thus, we have Definition 10. Let us suppose that $s, r\in N_O$, $r=\beta(ps+q)$. We call s the level 1 predecessor of r and call r the level 1 successor of s. If s_1 is the level 1 predecessor of s_2 and s_2 is the level 1 predecessor of s_3, then we call s_1 the level 2 predecessor of s_3. If s_1 is the level $n-1$ predecessor of $s_n(n>1)$ and s_n is the level 1 predecessor of s_{n+1}, then we call s_1 the level n predecessor (predecessor for short) of s_{n+1}. If s_1 is the level n predecessor of s_{n+1}, then we call s_{n+1} the level n successor (successor for short) of s_1.

According to Definition 10, from Example 1, we know that in $3x+1$ sequence $\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$ 11,17,13,5,1,1,…, the first term "11" is the level 1 predecessor of the second term "17", the level 2 predecessor of the third term "13",…. Thus, we know that Property 12. In any $px+q$ sequence, from the second term onward, any term has a predecessor.

Definition 11. Let us suppose that a is a level n predecessor of b. We call $\{a_1= a, a_{n+1}=\beta(pa_n+q)\}$ the level n leftward extension sequence (leftward extension sequence for short) of

$\{b_1=b, b_{n+1}=\beta(pb_n+q)\}$.

Property 13. If A is a level n leftward extension sequence of B, then the *kth* term in B equals the $(k+n)$*th* term in A.

For example, $\{a_1=54515, a_{n+1}=\beta(5a_n+1)\}$ 54515,4259,1331,13,33,83,… is a level 3 leftward extension sequence of $\{a_1=13, a_{n+1}=\beta(5a_n+1)\}$ 13,33,83,…. Therefore, the first term, second term, … in $\{a_1=13, a_{n+1}=\beta(5a_n+1)\}$ are the fourth (4=1+3) term, fifth (5=2+3) term, of $\{a_1=54515, a_{n+1}=\beta(5a_n+1)\}$ respectively.

In addition, from the sequence 2, we can see that odd number 13 necessarily has predecessor 1331. However, the first term, 54515, in the sequence 4, has no predecessor (below, we discuss the reason). That is, as a term in the $5x+1$ sequence, odd number 13 has a predecessor, and we call 13 a term implying left terms (we give its definition later); 54515 has no predecessor, and we call it a term without a left term (we give its definition later).

Below, we discuss the calculation method of the predecessors.

Let $r=\beta(ps+q)$. From Definition 10, we know that s is a predecessor of r. From Definition 9, we know that $r=(ps+q)/2^i$. Thus,

$$s=(2^i r-q)/p. \quad (17)$$

We call (17) the formula of the leftward extension relationship of $px+q$ sequences.

In (17), p, q, and r are known, and we need to determine only parameter i. For example, when finding level 1 predecessor 1331 of the second term 13 in the sequence 2, we have already known $p=5$, $q=1$, and $r=13$. Let $i=5$, we can obtain the predecessor

$s=(2^5\cdot 13-1)/5=1331$.

How to assign a value to i or what value can be assigned to i is what we discuss next.

Definition 12. Let us suppose that $r\in N_O$, $s=(2^i r-q)/p$. If there exists i such that $s\in N_O$, then we call r *a* term implying left terms in the $px+q$ sequences; otherwise, we call r a term without a left term in the $px+q$ sequences.

"$s\in N_O$" in Definition 12 means that at this time, r has predecessors. Therefore, from Property 12, we know that from the second term onward, any term in any $px+q$ sequence is a term implying left terms; a term without left terms can only be a first term appearing in certain $px+q$ sequences.

Please see the sequence 5: 7,25,11,39,137,15,…i.e., $\{a_1=7, a_{n+1}=\beta(7a_n+1)\}$.

Sequence 6: 5,7,35,17,133,119,…i.e., $\{a_1=5, a_{n+1}=\beta(7a_n+21)\}$. Sequence 7: 7,35,17,133,119,…i.e., $\{a_1=7, a_{n+1}=\beta(7a_n+21)\}$.

First, let us investigate the first term 7 in the sequence 5. From $r=7$, $p=7$, $q=1$ and $s=(2^i r-q)/p$, we know that $s=(2^i\times 7-1)/7\notin N_O$. (because $2^i\times 7-1$ cannot be divided by 7 evenly). Thus, 7 is a term without a left term of the $7x+1$ sequence. (However, later we see that 7 is a term implying left terms of the

$7x+21$ sequence.)

Second, let us investigate the first term 5 in the sequence 6. From $r=5$, $p=7$, $q=21$ and $s=(2^i\times 5-21)/7\notin N_O$, we know that 5 is a term without a left term in the $7x+21$ sequence.

Third, let us investigate the first term 7 in the sequence 7. From $r=7$, $p=7$, $q=21$ and $s=(2^i\times 7-21)/7=(2^i-3)$ we know that, now there is i such that $s=(2^i-3)\in N_O$. Thus, 7 is a term implying left terms in the $7x+21$ sequence.

Let $i=2,3,4,\ldots$, we obtain the predecessors of 7 being $s=1,5,13,\ldots$.

In addition, when we know that $1,5,13,\ldots$ are the predecessors of the first term 7 in the sequence 7, we also know that, the following sequences

$\{a_1=1, a_{n+1}=\beta(7a_n+21)\}$: 1,7,35, 133,119,…

$\{a_1=5, a_{n+1}=\beta(7a_n+21)\}$: 5,7,35, 133,119,…

$\{a_1=13, a_{n+1}=\beta(7a_n+21)\}$: 13,7,35, 133,119,…

…

are all level 1 leftward extension sequences of the sequence 7. Theorem 3. Let us suppose that $r\in N_O$, $(p,q)=c$. Then,

(1) When $c=1$, if $p\mid r$ then r is a term without a left term in the $px+q$ sequences;

(2) When $c>1$, if $c\nmid r$, then r is a term without a left term in the $px+q$ sequences.

Proof: Prove (1). As $p\mid r$, let us suppose that $r=pr'$. From $s=(2^ir-q)/p$, we know that $s=(2^ipr'-q)/p$.

From $(p,q)=c=1$, we know that $p\nmid q$, $p\nmid 2^ipr'-q$. Then, $s=(2^ipr'-q)/p\notin N_O$.

That is, there is no i such that $s\in N_O$. From Definition 12, we know that r is a term without a left term in the $px+q$ sequences.

Proof (2). Let us suppose that $p=cp'$, $q=cq'$. From $s=(2^ir-q)/p$, we obtain $s=(2^ir-cq')/cp'$. From Definition 9, we know that $p,q\in N_O$. Hence, $(p,q)=c\in N_O$. There is a supposition $c\nmid r$; therefore, $c\nmid 2^ir$, $c\nmid 2^ir-cq'$, $cp'\nmid 2^ir-cq'$.

From this, we know that $s=(2^ir-cq')/cp'\notin N_O$. That is, r is a term without a left term in the $px+q$ sequences. Q.E.D.

From (1) of Theorem 3, we know that 7 is a term without a left term in the $7x+1$ sequence, for $c=(p,q)=(7,1)=1$ and $p=7\mid r=7$.

From (2) of Theorem 3, we know that 5 is a term without a left term in the $7x+21$ sequence, for $c=(7,21)=3>1$ and $c=3\nmid r=5$.

Definition 13. If the first term in a $px+q$ sequence is a term implying left terms, then we call the sequence a leftward extendable sequence in the $px+q$ sequences; otherwise, we call the sequence a nonleftward extendable sequence in the $px+q$ sequences.

From Definition 13, we know that the sequence 5 is a nonleftward extendable sequence in the $7x+1$ sequences; the sequence 6 is a nonleftward extendable sequence in the $7x+21$ sequences; and the sequence 7 is a leftward extendable sequence in the $7x+21$ sequences.

Now, let us discuss the sufficient and necessary condition for odd number r to be a term implying left terms in the $px+q$ sequence.

Theorem 4. Let us suppose that $(p, q)=1$, $r\in N_O$. Then, I. The sufficient and necessary condition for r being a term implying left terms in the $px+q$ sequence is $rq^{-1}\equiv 2^k \pmod p$. When r has predecessor s,

$$s=(2^{n\delta p(2)-k}r-q)/p. \tag{18}$$

II. Let us suppose that $p'=cp$, $q'=cq$, $r'=cr$, $c\in N_O$. Then, r' is a term implying left terms in the $p'x+q'$ sequence, if and only if r is a term implying left terms in the $px+q$ sequence. When r' has predecessor s', $s'=s=(2^{n\delta p(2)-k}r-q)/p$.

Proof: Prove I. First, let us prove the necessary condition. That is, let us prove that if $s=(2^ir-q)/p\in N_O$, then $rq^{-1}\equiv 2^k \pmod p$.

From $(2^ir-q)/p\in N_O$ we know that, $2^ir-q\equiv 0 \pmod p$,

$$2^ir\equiv q \pmod p. \tag{19}$$

From $(p, q)=1$ and (19), we know that

$$2^irq^{-1}\equiv 1 \pmod p \tag{20}$$

From $p\in N_O$ (see Definition 9), we know that $(2^i, p)=1$. Thus, 2^i has inverse $(2^i)^{-1}$ modulus p. From this and (20), we know that

$$rq^{-1}\equiv (2^i)^{-1} \pmod p \tag{21}$$

In addition, from Conclusion 6, we know that there necessarily exists a positive integer k such that

$(2^i)^{-1}\equiv 2^k \pmod p$ (22)

From (21) and (22), we obtain $rq^{-1}\equiv 2^k \pmod p$.

Then, let us prove the sufficient condition. That is, let us prove that if $rq^{-1}\equiv 2^k \pmod p$, then $s=(2^i r-q)/p\in N_O$.

There necessarily exist positive integers i, k such that $i+k=n\delta_p(2)$. Therefore, $2^i 2^k=2^{i+k}\equiv 2^{n\delta p(2)}\equiv 1 \pmod p$. That is,

$2^i 2^k\equiv 1 \pmod p$ (23)

According to condition $2^k\equiv rq^{-1} \pmod p$, changing 2^k in (23) into rq^{-1}, we obtain $2^i(rq^{-1})\equiv 1 \pmod p$; that is,

$2^i r\equiv q \pmod p$ (24)

From (24), we know that $2^i r-q\equiv 0 \pmod p$. Thus,

$p \mid 2^i r-q$ (25)

From $q\in N_O$ (see Definition 9), we know that $2^i r-q\in N_O$

From $p\in N_O$, $2^i r-q\in N_O$ and (25), we know that $(2^i r-q)/p\in N_O$. Let $s=(2^i r-q)/p$. Then, $s=(2^i r-q)/p\in N_O$.

From Definition 12 and $s=(2^i r-q)/p\in N_O$, we know that r is a term implying left terms in the $px+q$ sequence.

From $s=(2^i r-q)/p$ and $i+k=n\delta_p(2)$, we know that $s=(2^{n\delta p(2)-k}r-q)/p$. Prove II.

First, let us prove that if r' is a term implying left terms in the $p'x+q'$ sequence, then r is a term implying left terms in the $px+q$ sequence, and $s'=s$.

From r' is a term implying left terms in the $p'x+q'$ sequence, we know that the predecessor of r' is $s'=(2^i r'-q')/p'\in N_O$. Then,

$s'=(2^i cr-cq)/cp=(2^i r-q)/p=s\in N_O$.

From Definition 12, we know that r is a term implying left terms in the $px+q$ sequence. From I, we know that $s=(2^{n\delta p(2)-k}r-q)/p$.

Likewise, we can prove that if r is a term implying left terms in the $px+q$ sequence, then r' is a term implying left terms in the $p'x+q'$ sequence, and $s=s'$.

Q.E.D.

"The sufficient and necessary condition for r being a term implying left terms in the $px+q$ sequence is $rq^{-1}\equiv 2^k \pmod p$" means that if congruence equation $2^k\equiv rq^{-1} \pmod p$ regarding k has solutions, then r is a term implying left terms in the $px+q$ sequence; otherwise, r is a term without a left term in the $px+q$ sequence. From this and Conclusion 1, we have （Note：We stipulate $(p, q)=1$，$r\in N_O$ in Corollaries 1, 2, and 3），

Corollary 1. If $(rq^{-1}) \bmod p$ is the kth term in ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod p$｝, then r is a term implying left terms in the $px+q$ sequence, and the predecessor of r is $s=(2^{n\delta p(2)-k}r-q)/p$. Otherwise, r is a term without a left term in the $px+q$ sequence.

Corollary 1 can also be stated as follows:

Corollary 2. r is a term implying left terms in the $px+q$ sequence, if and only if, $(rq^{-1}) \bmod p$ is a term in simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod p$｝.

Simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod p$｝ has $\delta_p(2)$ terms in total, which means that in a residual system of p with all numbers being odd numbers r has $\delta_p(2)$ values such that $(rq^{-1}) \bmod p$ are the terms in simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod p$｝. Thus,

Corollary 3. Let us suppose that odd numbers $a_1, \ldots, a_p$ are a residual system of p. Then, in $a_1, \ldots, a_p$, there are $\delta_p(2)$ odd numbers that are the terms implying left terms in the $px+q$ sequence. For example, 3,5,7,9,11,13,15 are a residual system of 7 with all numbers being odd numbers.

From Corollary 3, we know that in the residual system, three ($=\delta_7(2)$) numbers 3, 5, 13 are the terms implying left terms in the $7x+3$ sequence. Now $p=7$, $q=3$, $q^{-1}=5$. Thus, r is assigned 3, 5, 13 such that $(3\times 5) \bmod 7=1$, $(5\times 5) \bmod 7=4$, and $(13\times 5) \bmod 7=2$ are the terms in simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod 7$｝ 2,4,1.

We call (18) the predecessor calculation formula of r—a term implying left terms—in the $px+q$ sequences.

Example 2. To decide which of 15,17,119 are the terms implying left terms in the $9x+1$ sequence and to calculate the predecessors of the terms implying left terms.

Solution: Let us decide which of 15,17,119 are the terms implying left terms in the $9x+1$ sequence and calculate the predecessors of the terms implying left terms.

Now, $p=9$, $q=1$, $q^{-1}\equiv 1 \pmod 9$. Simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod 9$｝ 2,4,8,7,5,1.$\delta_9(2)=6$.

When $r=15$, $(15\times1) \bmod 9=6$. 6 is not a term in simplest $\{a_1=2, a_{n+1}=(2a_n) \bmod 9\}$. Therefore, 15 is a term without a left term in the $9x+1$ sequence.

When $r=17$, $(17\times1) \bmod 9=8$. 8 is the third term in simplest $\{a_1=2, a_{n+1}=(2a_n) \bmod 9\}$. Therefore, 17 is a term implying left terms in the $9x+1$ sequence. Thus, the predecessor calculation formula of 17 is $s=(2^{6n-3}17-1)/9$. Let $n=1,2,3,\ldots$, we obtain the predecessors of 17--a term implying left terms--being 15,967,61895,….

When $r=119$, $(119\times1) \bmod 9=2$. 2 is the first term in simplest $\{a_1=2, a_{n+1}=(2a_n) \bmod 9\}$. Therefore, 119 is a term implying left terms in the $9x+1$ sequence. The predecessor calculation formula of 119 is $s=(2^{6n-1}119-1)/9$. Let $n=1,2,3,\ldots$, we obtain the predecessors of 119--a term implying left terms--being 423,27079,1733063,….

In (18), n can be $n=1,2,\ldots$, thus, r—a term implying left terms—in $px+q$ sequences necessarily has infinitely many predecessors s. Now, let us discuss the property of these infinitely many predecessors s.

In Example 2, we obtain infinitely many predecessors of 17—a term implying left terms—in the $9x+1$ sequence, they can be arranged, from small to large, as the sequence $\{a_n\}$: 15,967,61895,….

It is interesting that $967=2^6\times15+7$, $61895=2^6\times967+7$,…, i.e., $a_2=2^6a_1+7$, $a_3=2^6a_2+7$, ….

That is, the sequence $\{a_n\}$ is just the sequence $\{a_1=15, a_{n+1}=2^6a_n+7\}$.

Please see the theorem:

Theorem 5. Let us suppose that the sequence A is $a_1=(2^{\delta p(2)-k}r-q)/p$, $a_2=(2^{2\delta p(2)-k}r-q)/p,\ldots$, $a_n=(2^{n\delta p(2)-k}r-q)/p,\ldots$. Then, A and $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$ (where $a=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$) are the same sequence.

Proof: From the supposition, we know that $a_1=(2^{\delta p(2)-k}r-q)/p$, $a_n=(2^{n\delta p(2)-k}r-q)/p$,

$$a_{n+1}=(2^{(n+1)\delta p(2)-k}r-q)/p$$
$$=(2^{n\delta p(2)+\delta p(2)-k}r-q)/p$$
$$=(2^{\delta p(2)}2^{n\delta p(2)-k}r-q)/p$$
$$=(2^{\delta p(2)}2^{n\delta p(2)-k}r-2^{\delta p(2)}q+2^{\delta p(2)}q-q)/p$$
$$=2^{\delta p(2)}(2^{n\delta p(2)-k}r-q)/p+q(2^{\delta p(2)}-1))/p$$
$$=2^{\delta p(2)}a_n+q(2^{\delta p(2)}-1))/p.$$

Thus, we have proved that A is the mapping recurrent sequence $\{a_1=(2^{\delta p(2)-k}r-q)/p, a_{n+1}=2^{\delta p(2)}a_n+q(2^{\delta p(2)}-1)/p\}$.

Let $a=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$, we obtain $\{a_1=(a, a_{n+1}=2^{\delta p(2)}a_n+b\}$. Q.E.D.

We call $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$ with $a=(2^{\delta p(2)-k}r-q)/p$ and $b=q(2^{\delta p(2)}-1)/p$ the predecessor sequence of r--a term implying left terms--in the $px+q$ sequence.

It is more efficient to calculate the predecessors of r--a term implying left terms—by using the predecessor sequence $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$. Because once we calculate $a=(2^{\delta p(2)-k}r-q)/p$ and $b=q(2^{\delta p(2)}-1)/p$, we calculate all of the predecessors of r. However, calculating the predecessors of r—a term implying left terms—is still a complicated problem. To this end, we give a general method for the decision of r—a term implying left terms—in the $px+q$ sequence and the calculation of its predecessor sequence.

The method for the decision of the term implying left terms and the calculation of its predecessor sequence

1. We calculate simplest $\{a_1=2, a_{n+1}=(2a_n) \bmod p\}$, obtaining that the number of terms in the sequence is $\delta p(2)$ (See Conclusion 5).
2. We find q^{-1}. If $q=1$ then $q^{-1}=1$; if $1<q$ then we calculate simplest $\{a_1=q, a_{n+1}=(qa_n) \bmod p\}$ and q^{-1} is the term second from the right in the sequence (See Conclusion 7).
3. We calculate $(rq^{-1}) \bmod p$.
4. If $(rq^{-1}) \bmod p$ is not a term in simplest $\{a_1=2, a_{n+1}=(2a_n) \bmod p\}$ then r is a term without a left term and terminate. Otherwise, we assign the position value of $(rq^{-1}) \bmod p$ in simplest $\{a_1=2, a_{n+1}=(2a_n) \bmod p\}$ to k (Note: when $(rq^{-1}) \bmod p=1$, $k=0$). (See Conclusion 1).
5. We calculate $a=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$, obtaining the predecessor sequence for r to be $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$ and terminating.

Example 3. To decide whether 7 is a term implying left terms in $31x+25$ sequence or not; if it is, then we calculate its predecessor sequence.

Solution. According to the method for the decision of the term implying left terms and the calculation of its predecessor sequence,

1. We calculate simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod 31$｝：2,4,8,16,1, obtaining $\delta_{31}(2)=5$.
2. Since $1<q=25$，we calculate simplest ｛$a_1=25$, $a_{n+1}=(25a_n) \bmod 31$｝：25,5,1. Because the term second from the right in the sequence is 5, $q^{-1}=25^{-1}=5$.
3. We calculate $(rq^{-1}) \bmod p$. From $r=7$ and $25^{-1}=5$, we obtain $(rq^{-1}) \bmod p=(7\times25^{-1}) \bmod 31=4$.
4. "4" is the second term in simplest ｛$a_1=2$, $a_{n+1}=(2a_n) \bmod 31$｝：2,4,8,16,1 (Thus, we know that, 7 is a term implying left terms in the $31x+25$ sequence) Let $k=2$.
5. We calculate $a=(2^{\delta_p(2)-k}r-q)/p$，$b=q(2^{\delta_p(2)}-1)/p$. From $r=7$，$p=31$，$q=25$，$\delta_{31}(2)=5$，$k=2$ we obtain, $a=(2^{5-2}7-25)/31=1$，$b=25(2^5-1)/31=25$. Finally, we obtain that the predecessor sequence of 7—a term implying left terms—in the $31x+25$ sequence is ｛$a_1=1$，$a_{n+1}=2^5a_n+25$｝：1,57,1849,…. And terminate.

(It is not hard to calculate $\beta(1\times31+25)=\beta(57\times31+25)=\beta(1849\times31+25)=7$, which verifies that 1,57,1849 are predecessors of 7).

Theorem 6. Let us suppose that A is ｛$a_1=a$, $a_{n+1}=2^{\delta_p(2)}a_n+b$｝，$B$ is 〖$b_n=(a_n) \bmod p$〗. Then, B and ｛$b_1=(a) \bmod p$, $b_{n+1}=(b_n+b) \bmod p$｝ are the same sequence.

Proof: From $a_1=a$ and 〖$b_n=(a_n) \bmod p$〗 we obtain $b_1=(a) \bmod p$. Now, we prove $b_{n+1}=(b_n+b) \bmod p$.

From ｛$a_1=a$, $a_{n+1}=2^{\delta_p(2)}a_n+b$｝ we know that

$$a_{n+1}=2^{\delta_p(2)}a_n+b \tag{26}$$

From 〖$b_n=(a_n) \bmod p$〗 we know that,

$$b_{n+1}=(a_{n+1}) \bmod p \tag{27}$$

Substituting (26) into (27), we obtain

$$b_{n+1}=(2^{\delta_p(2)}a_n+b) \bmod p \tag{28}$$

From (28) and Property 2, we know that

$$b_{n+1}=((2^{\delta_p(2)}) \bmod p(a_n) \bmod p+b) \bmod p \tag{29}$$

From $(2^{\delta_p(2)}) \bmod p=1$ and (29), we know that

$$b_{n+1}=((a_n) \bmod p+b) \bmod p. \tag{30}$$

In addition, from 〖$b_n=(a_n) \bmod p$〗, we obtain

$$(a_n) \bmod p=b_n \tag{31}$$

Substituting (31) into (30), we obtain that $b_{n+1}=(b_n+b) \bmod p$. Q.E.D.

Because ｛$b_1=(a) \bmod p$, $b_{n+1}=((b_n+b) \bmod p$｝ is a mapping recurrent sequence and all terms in it are less than p, from the pigeonhole principle and basic theorem 2, we know that the sequence is a circular sequence.

It is not hard to see that when $a=(2^{\delta_p(2)-k}r-q)/p$ and $b=q(2^{\delta_p(2)}-1)/p$, A：｛$a_1=a$, $a_{n+1}=2^{\delta_p(2)}a_n+b$｝ in Theorem 6 is just the predecessor sequence of r—the term implying left terms—in the $px+q$ sequence. Various terms in ｛$b_1=(a) \bmod p$, $b_{n+1}=((b_n+b) \bmod p$｝ of Theorem 6 are the minimal nonnegative residues of their corresponding terms modulus p in ｛$a_1=a$, $a_{n+1}=2^{\delta_p(2)}a_n+b$｝.

Definition 14. We call ｛$b_1=(a) \bmod p$, $b_{n+1}=((b_n+b) \bmod p$｝ with $a=(2^{\delta_p(2)-k}r-q)/p$ and $b=q(2^{\delta_p(2)}-1)/p$ the predecessor residue sequence of r--the term implying left terms--in the $px+q$ sequence.

Corollary 4: Let us suppose that A is ｛$a_1=a$, $a_{n+1}=2^{\delta_p(2)}a_n+b$｝，$B$ is ｛$b_1=(a) \bmod p$, $b_{n+1}=((b_n+b) \bmod p$｝.Then, $a_n\equiv b_n \pmod p$，$n=1,2,\ldots$, or, various terms in the predecessor sequence of r --the term implying left terms--in the $px+q$ sequence are congruent with their corresponding terms modulus p in the predecessor residue sequence.

According to the method for the decision of the term implying left terms and the calculation of its predecessor sequence, we can find the predecessor sequence of 65—a term implying left terms—in the $21x+1$ sequence: ｛$a_1=99$，$a_{n+1}=2^6a_n+3$｝：99,6339,405699,…

From Theorem 6, we can find the predecessor residue sequence of 65—the term implying left terms—in the $21x+1$ sequence:

｛$b_1=(99) \bmod 21$, $b_{n+1}=((b_n+3) \bmod 21$｝：15,18,0,3,6,9,12,15,….

Obviously, $99\equiv15 \pmod{21}$, $6339\equiv18 \pmod{21}$, $405699\equiv0 \pmod{21}$,….

However, it is unexpected that 99,6339,405699,… are all of the terms without a left term in the $21x+1$ sequence (The readers please verify themselves).

Below, we investigate the reason for this. This is a rather complicated problem. We need to prove the following lemmas first.
In the proofs of these lemmas, we need the following properties of noncongruence equation $a\not\equiv b$ (mod m):
When $a\not\equiv b$ (mod m), I. $a+c\not\equiv b+c$ (mod m); II. If $(c, m)=1$ then $ac\not\equiv bc$ (mod m). （The above two properties can be proved by mathematical induction）
Lemma 1. If every consecutive m term in the sequence $\{b_n\}$ is a residual system of m, then
$b_i\equiv b_{nm+i}$(mod m), $i\in N, 0\le n$.
Proof: First, we prove that among the consecutive $m+1$ terms $b_k, b_{k+1}, \ldots, b_{k+m}-1, b_{k+m}$ in $\{b_n\}$
there is $b_k\equiv b_{k+m}$ (mod m).
We use the indirect proof. Let us suppose that $b_k\not\equiv b_{k+m}$ (mod m).

The consecutive m terms $b_k, b_{k+1}, \ldots, b_{k+m}-1$ in $\{b_n\}$ is a residual system of m. Therefore, b_{k+m} is necessarily congruent modulus m with one of the m terms $b_k, b_{k+1}, \ldots, b_{k+m}-1$. Hence, when $b_{k+m}\not\equiv b_k$ (mod m), b_{k+m} is necessarily congruent modulus m with one of the m-1 terms $b_{k+1}, \ldots, b_{k+m}-1$.
Thus, the consecutive m terms $b_{k+1}, \ldots, b_{k+m}-1, b_{k+m}$ are not pairwise noncongruent modulus m, which contradict with that every consecutive m terms in $\{b_n\}$ is a residual system of m. Thus, the supposition does not hold, i.e., $b_k\equiv b_{k+m}$ (mod m).
Likewise, $b_{k+1}\equiv b_{k+m+1}$ (mod m), …
The rest can be inferred by analogy. Thus, we have proved that Lemma 1 holds Q.E.D.
Lemma 2. Let us suppose that A is $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$, $a<m$. Then, I. $a_n=(a+(n-1)b) \bmod m$; II. A is a pure circular sequence with the minimal circular length being $m/(b, m)$.
Proof: Prove I. We use mathematical induction.
Step 1: When $n=1$, $a_1=(a+(1-1)b) \bmod m=(a) \bmod m$. From $a<m$ we know that, $a_1=a$. That is I holds.
Step 2: Let us suppose that when $n=k$, $a_k=(a+(k-1)b) \bmod m$. Step 3: We prove that, when $n=k+1$, $a_{k+1}=(a+kb) \bmod m$.
From $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ we know that, $a_{k+1}=(a_k+b) \bmod m$.
From the induction supposition we know that, $a_{k+1}=((a+(k-1)b) \bmod m+b) \bmod m$. From Property 2 we know that, $a_{k+1}=((a+(k-1)b)+b) \bmod m=(a+kb) \bmod m$.
Prove II. Let us suppose that $(b, m)=c$, $b'=b/c$, $m'=m/c$. Then, $(b', m')=1$, $m'=m/(b, m)$, $b=b'c$, $m=m'c$.
First, we prove that A is a pure circular sequence with a circular length of m'. Let $n=m'+1$. From I, we know that $a_{m'+1}=(a+(m'+1-1)b) \bmod m$. That is,
$a_{m'+1}=(a+m'b) \bmod m=(a+m'b'c) \bmod m=(a+m'cb') \bmod m=(a+mb') \bmod m=a=a_1$.
Because $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ is a mapping recurrent sequence, from $a_{m'+1}=a_1$ and basic theorem 2, we know that A is a pure circular sequence with the circular length being m'.
Then, we prove that m' is the minimal circular length of A.
Obviously, if $m'=1$, then m' is the minimum of the circular lengths. Now, we discuss the case of $1<m$.
As A is a pure circular sequence with a circular length of m', a_1 is a circular term.
Let $1<k\le m'$, we obtain, $m' \nmid (k-1)$. From $(b', m')=1$, we know that
$$m' \nmid (k-1)b' \tag{32}$$
From $(b, m)=c$, we know that $c\neq 0$. From (32), we know that $m'c \nmid (k-1)b'c$, $m \nmid (k-1)b$.
Thus, $(k-1)b\not\equiv 0$ (mod m). Adding a on both sides of "$\not\equiv$", we obtain
$$a+(k-1)b\not\equiv a \pmod m \tag{33}$$
From I and Property 5, we know that $a_k=(a+(k-1)b) \bmod m\equiv a+(k-1)b$ (mod m).
From $a_k\equiv a+(k-1)b$ (mod m) and (33), we know that $a_k\not\equiv a$ (mod m). Thus, $a_k\neq a$, i.e., $a_k\neq a_1$.
From $1<k\le m'$ and $a_k\neq a_1$, we know that $a_2, a_3, \ldots, a_{m'}-1\neq a_1$. From a_1 being a circular term in A and II of Property 10, we know that m' is the minimal circular length of A. Q.E.D.
Please see the following two sequences.
Sequence 8: $\{a_1=1, a_{n+1}=(a_n+3) \bmod 12\}$ 1,4,7,10,1,…
Sequence 9: $\{a_1=1, a_{n+1}=(a_n+3) \bmod 36\}$ 1,4,7,10,13,16,19,22,25,28,31,34,1,…
As to sequence 8, $m/(b, m)=12/3=4$. The minimal circular length of sequence 8:1,4,7,10,1,… is 4. Meanwhile, we notice that, the consecutive four terms in the sequence in question is a residual system of 4.
As to sequence 9, $m/(b, m)=36/3=12$. The minimal circular length of the sequence is 12. However, we notice that, every 12 consecutive terms in the sequence are not a residual system of

12. However, every two or four terms in the sequence are residual systems of 2 or 4.

Lemma 3. Let us suppose that $\{a_n\}$ be $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$. Then, every consecutive d terms in $\{a_n\}$ is a residual system of d if and only if $d \mid m$ and $(d, b)=1$.

Proof: We prove the sufficient condition. That is, we prove that if $d \mid m$ and $(d, b)=1$ then every consecutive d terms in $\{a_n\}$ is a residual system of d.

When $d=1$, the conclusion holds. Now, we prove the case of $d>1$.

Let us suppose that the consecutive d terms in $\{a_n\}$ are $a_j, a_{j+1},\ldots,a_{j+d-1}$. In addition, let us suppose that $j\le k<i<j+d$. Thus, $1\le i-k<d$.

From $1\le i-k<d$ we obtain that, $i-k\not\equiv 0 \pmod d$, $i\not\equiv k \pmod d$, $i-1\not\equiv k-1 \pmod d$.

From $(b, d)=1$ we know that, $(i-1)b\not\equiv (k-1)b \pmod d$,

$a+(i-1)b\not\equiv a+(k-1)b \pmod d$. (34)

From Property 6, we know that there exist integers $k_1\ge 0$ and $k_2\ge 0$ such that

$a+(i-1)b=k_1m+(a+(i-1)b) \bmod m$ and $a+(k-1)b=k_2m+(a+(k-1)b) \bmod m$. (35)

From I in Lemma 2, we know that $a_i=(a+(i-1)b) \bmod m$, $a_k=(a+(k-1)b) \bmod m$. From this and (35), we know that,

$a+(i-1)b=k_1m+a_i$ and $a+(k-1)b=k_2m+a_k$. (36)

From (34) and (36), we know that $k_1m+a_i\not\equiv k_2m+a_k \pmod d$.

From $d \mid m$, we know that $k_1m\equiv k_2m\equiv 0 \pmod d$. Therefore, $a_i\not\equiv a_k \pmod d$.

From $1\le i-k<d$ $(j\le k<i<j+d)$ and $a_i\not\equiv a_k \pmod d$, we know that the consecutive d terms $a_j, a_{j+1},\ldots,a_{j+d-1}$ in $\{a_n\}$ are pairwise noncongruent moduli d. Because for $j=1,2,\ldots$ the result holds, every consecutive d term in $\{a_n\}$ is a residual system of d.

We prove the necessary condition. There are two cases.

Case 1. If $d \nmid m$, then it does not hold that every consecutive d term in $\{a_n\}$ is a residual system of d.

Case 2. If $(d, b)>1$, then it does not hold that every consecutive d terms in $\{a_n\}$ is a residual system of d.

Prove case 1. $d \nmid m$, therefore, $d\ne m$. Thus, $d>m$ or $d<m$.

From II of Lemma 2, we know that $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ is a pure circular sequence with the circular length being less than or equal to m. Thus, when $d>m$, the consecutive d terms in $\{a_n\}$ have necessarily equal terms. Therefore, it does not hold that the consecutive d terms in $\{a_n\}$ are a residual system of d.

When $d<m$, from this and $d \nmid m$ we know that, there is necessarily k such that $1\le kd-m<d$.

Let $kd-m=c$. Thus, $1\le c<d$ and $m=kd-c$,

$m+1=(k-1)d+d-c+1$. (37)

From $c<d$ we know that, $1\le d-c<d$,

$2\le d-c+1\le d$. (38)

Let us suppose that every consecutive d terms in $\{a_n\}$ is a residual system of d. Thus, the first d terms in $\{a_n\}$ is a residual system of d. Hence, we know that,

$a_t\not\equiv a_1 \pmod d$, $2\le t\le d$. (39)

Let $t=d-c+1$, from (38) and (39) we know that,

$a_{d-c+1}\not\equiv a_1 \pmod d$ (40)

Meanwhile, from the supposition that every consecutive d term in $\{a_n\}$ is a residual system of d and Lemma 1 we know that,

$a_{d-c+1}\equiv a_{(k-1)d+d-c+1} \pmod d$ (41)

From (40) and (41), we know that $a_{(k-1)d+d-c+1}\not\equiv a_1 \pmod d$. From this and (37), we know that

$a_{m+1}\not\equiv a_1 \pmod d$ (42)

In addition, from II of Lemma 2, we know that $m/(b, m)$ is the minimal circular length of $\{a_n\}$. From $m/(b, m) \mid m$, we know that m is a circular length of $\{a_n\}$. Thus, $a_{m+1}=a_1$,

$a_{m+1}\equiv a_1 \pmod d$. (43)

Obviously, (42) and (43) are contradictory. Hence, we know that the supposition does not hold, i.e., it does not hold that every consecutive d terms in $\{a_n\}$ are a residual system of d.

Proof of case 2. In case 1, we have proved that it does not hold that when $d \nmid m$ and $(d, b)>1$, every consecutive term of d in $\{a_n\}$ is a residual system of d.

Therefore, here, we only need to prove that, it does not hold that if $d \mid m$ and $(d, b)>1$, then every consecutive term of d in $\{a_n\}$ is a residual system of d.

Let $(d, b)=k$, $b'=b/k$, $t=d/k$. Thus, $b=b'k$, $d=kt$, $k\,t \mid m$. From $(d, b)>1$, we know that $k>1$. From I of Lemma 2, we know that the first d $(=kt)$ terms in $\{a_n\}$, in their proper order, are:

a, $(a+b'k) \bmod m$, …, $(a+(t-1)b'k) \bmod m$,

$(a+tb'k) \bmod m$, $(a+(t+1)b'k) \bmod m$, …, $(a+(2t-1)b'k) \bmod m$,

……

$(a+(k-1)tb'k) \bmod m$, $(a+((k-1)t+1)b'k) \bmod m$, …, $(a+(kt-1)b'k) \bmod m$.

The above $d(=kt)$ terms form a matrix with k rows and t columns. Now, we investigate the second column of the matrix (the other columns can be similarly investigated).

We prove that $(a+b'k) \bmod m \equiv (a+((n-1)t+1)b'k) \bmod m \pmod{kt}$, $n=1,2,\ldots k$ (That is, we prove that all of the terms in the second column are congruent modulus d.).

From $kt=d \mid m$ and Property 4, we know that $((a+((n-1)t+1)b'k) \bmod m) \bmod kt = (a+((n-1)t+1)b'k) \bmod kt$

$=(a+(n-1)tb'k+b'k) \bmod kt$

$=(a+(n-1)ktb'+b'k) \bmod kt$

$=(a+(n-1)ktb') \bmod kt+b'k) \bmod kt$ (Note: $((n-1)ktb') \bmod kt=0$)

$=(a+b'k) \bmod kt$.

From $((a+((n-1)t+1)b'k) \bmod m) \bmod kt=(a+b'k) \bmod kt$ and Property 1, we know that $(a+((n-1)t+1)b'k) \bmod m \equiv a+b'k \pmod{kt}$ (44)

Likewise, from Property 4, we also know that $((a+b'k) \bmod m) \bmod kt=(a+b'k) \bmod kt$. Thus,

$(a+b'k) \bmod m \equiv a+b'k \pmod{kt}$ (45)

From (44) and (45), we know that $(a+((n-1)t+1)b'k) \bmod m \equiv (a+b'k) \bmod m \pmod{kt}$, where $n=1,2,\ldots,k$.

Now, we have proved that various terms on the second column of the above matrix are congruent modulus $d(=kt)$. That is, the consecutive d terms in $\{a_n\}$ are not pairwise noncongruent modulus d, or it does not hold that every consecutive d term in $\{a_n\}$ is a residual system of d.

Q.E.D.

As a special case of Lemma 3, we have,

Corollary 5. Every consecutive m terms in $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ form a residual system of m, if and only if, $(m, b)=1$.

Proof: We prove the sufficient condition. Let $d=m$. Thus, $d \mid m$, and from $(m, b)=1$ we know that, $(d, b)=1$.

From Lemma 3 we know that, every consecutive d $(=m)$ terms in $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ are a residual system of d.

We prove the necessary condition.

From II of Lemma 2 we know that $m/(b, m)$ is the minimal circular length of $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$.

When $(m, b)>1$, the minimal circular length of $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ is less than m. Thus, there are equal terms in the consecutive m terms. Hence, the consecutive m terms are not a residual system of m.

Q.E.D.

For example, sequence $\{a_1=1, a_{n+1}=(a_n+5) \bmod 12\}$ 1,6,11,4,9,2,7,0,5,10,3,8,1,…

Now, $(m, b)=(12, 5)=1$. Thus, every consecutive $(m=)12$ terms in $\{a_1=1, a_{n+1}=(a_n+5) \bmod 12\}$ are a residual system of 12.

(It worth mentioning that $\{a_1=a, a_{n+1}=(a_n+b) \bmod m\}$ in Lemma 3 should be called an equidifference residual sequence, which is similar to the equiratio sequence.)

Now, we prove Theorem 7.

Theorem 7. Let us suppose that $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$ is the predecessor sequence of r--a term implying left terms--in $px+q$ sequence. Then, the sufficient and necessary condition for every consecutive p term in $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$ to be a residual system of p is $(p, q(2^{\delta p(2)}-1)/p)=1$. Proof: First, we prove that the sufficient and necessary condition for every consecutive p term in *r's* predecessor residual sequence $\{b_1=(a) \bmod p, b_{n+1}=((b_n+b) \bmod p\}$ to be a residual system of p is $(p, q(2^{\delta p(2)}-1)/p)=1$.

From Definition 14, we know that in the predecessor residual sequence $\{b_1=(a) \bmod p, b_{n+1}=((b_n+b) \bmod p\}$ of r--a term implying left terms--there is $b=q(2^{\delta p(2)}-1)/p$.

From $b=q(2^{\delta p(2)}-1)/p$, we know that $(p, b)=1$ if and only if $(p, q(2^{\delta p(2)}-1)/p)=1$.

From Corollary 5, we know that $(p, b)=1$ (i.e., $(p, q(2^{\delta p(2)}-1)/p)=1$) is the sufficient and necessary condition for

every consecutive p term in $\{b_1=(a) \bmod p,\ b_{n+1}=((b_n+b) \bmod p\}$ to be a residual system of p.
From Corollary 4, we know that every consecutive p term in $\{a_1=a,\ a_{n+1}=2^{\delta p(2)}a_n+b\}$ is a residual system of p if and only if every consecutive p term in $\{b_1=(a) \bmod p,\ b_{n+1}=((b_n+b) \bmod p\}$ is a residual system of p.
Thus, because $(p,\ q(2^{\delta p(2)}-1)/p)=1$) is a sufficient and necessary condition for every consecutive p term in $\{b_1=(a) \bmod p,\ b_{n+1}=((b_n+b) \bmod p\}$ to be a residual system of p, we know that, $(p,\ q(2^{\delta p(2)}-1)/p)=1$ is the sufficient and necessary condition for every consecutive p term in
$\{a_1=a,\ a_{n+1}=2^{\delta p(2)}a_n+b\}$ to be a residual system of p. Q.E.D.
We call the $px+q$ sequences satisfying $(p,\ q(2^{\delta p(2)}-1)/p)=1$ the first type $px+q$ sequences Obviously, the $21x+1$ sequence is not a first type $px+q$ sequence, for $(21,\ (2^{\delta 21(2)}-1)/21)=(21,$
$(2^6-1)/21)=3$.
Subsequently, we discuss the first type $px+q$ sequences only. We stipulate that in the rest of this paper, "$px+q$ sequences" refer to "the first type $px+q$ sequences".
From Theorem 7 and Corollary 3, we can obtain:

Corollary 6. Of every consecutive p terms in the predecessor sequence of r--a term implying left terms--there are $\delta p(2)$ terms, which are the terms implying left terms in the $px+q$ sequences. Alternatively, in the predecessor sequence of r--a term implying left terms--in the $px+q$ sequence, the ratio of the terms implying left terms to all terms is $\delta p(2)/p$..

Since each term in the predecessor sequence of r—a term implying left terms—is a level 1 predecessor of r. According to Corollary 6, the ratio of the terms implying left terms to all level 1 predecessors of r is $\delta p(2)/p$. The terms implying left terms of the level 1 predecessors of r also have level 1 predecessors (they are the level 2 predecessors of r). The ratio of the terms implying left terms to all of the level 2 predecessors of r is also $\delta p(2)/p$. The terms implying left terms of the level 2 predecessors of r also have level 1 predecessors {They are the level 3 predecessors of r). Thus, we have
Corollary 7. If the sequence A is a leftward extendable sequence in the $px+q$ sequences, then A necessarily has level n ($n=1,2,\dots$) leftward extendable sequence B, and B and A are the same kind of $px+q$ sequences.
Example 4. $\{a_1=13,\ a_{n+1}=\beta(5a_n+1)\}$: 13,33,83,13,… is a leftward extendable sequence of the $5x+1$ sequences. The level 1 leftward extension sequence of the sequence in question includes
$\{a_1=1331,\ a_{n+1}=\beta(5a_n+1)\}$: 1331,13,33,83, 13,…, the level 2 leftward extension sequence includes $\{a_1=4259,\ a_{n+1}=\beta(5a_n+1)\}$: 4259,1331,13,33,83, 13,…, etc. They are all $5x+1$ sequences. Definition 15. If the $px+q$ sequence A is a (level n) leftward extension sequence B, then we call B a subsequence of A.
Corollary 8. Let us suppose that B is a subsequence of A; then, A is a circular sequence if and only if B is a circular sequence. Their circular terms are the same.
In Example 4, the sequence 1331,13,33,83, 13,… is a level 1 leftward extension sequence of sequence 13,33,83,13,…. Therefore, the former is a circular sequence, as is the latter. Terms 13,33,83 are the circular terms of both the former and the latter.

IV. Relevant properties of *px+q* infinite trees

Definition 16. Let us suppose that r is a term implying left terms in the $px+q$ sequence. Step 1. We connect r to every level 1 predecessor of r using lines. Step 2. We connect every predecessor r', which is a term implying left terms, to every level 1 predecessor of r' using lines. We repeat Step 2. The graphic we obtain at last is called the (r) $px+q$ infinite tree, see Fig. 1. $\{a_1=r,\ a_{n+1}=\beta(pa_n+q)\}$ is called the root sequence of (r) $px+q$ infinite tree.

Fig. 1 gives (7) $3x+1$ infinite tree. It is formed as follows. Step 1: We connect 7 to every level 1 predecessor 9,37,149,597,… directly. 37,149,… of the level 1 predecessors of 7 are the terms implying left terms in the $3x+1$ sequence. Step 2: We connect 37 to every level 1 predecessor 49,197,789, … directly; connect 149 to every predecessor 99,397,1589, … directly; …; and so on. Then, we obtain Fig. 1.

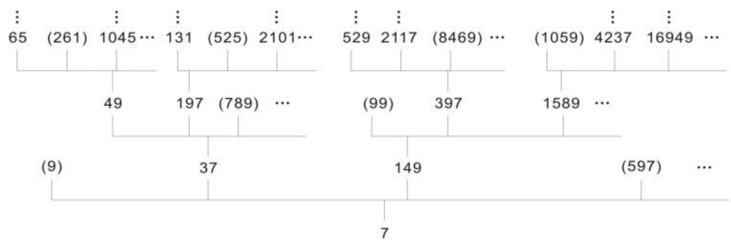

Fig. 1 (7) 3x+1 infinite tree

The root sequence of （7）$3x+1$ infinite tree is $\{a_1=7, a_{n+1}=\beta(3a_n+1)\}$：7,11,17,13,…

The numbers bracketed in Fig. 1 are the terms without a left term in the $3x+1$ sequence. For example, 9 and 99 in Fig. 1 are bracketed, and they are the terms without a left term in the $3x+1$ sequence.

From the formation of Fig. 1, we know that one layer up of 7 (the first layer) contains all of the level 1 predecessors of 7; the second layer contains all of the level 2 predecessors of 7;… . There are infinitely many layers in Fig. 1, and each layer has infinitely many odd numbers.

Fig. 1 gives not only all of the predecessors of 7—a term implying left terms—in a $3x+1$ sequence but also the arrangement of these predecessors.

Definition 17. Let us suppose that $a(\neq r)$ is a number in （r）$px+q$ infinite tree. We call $\{a_1=a, a_{n+1}=\beta(pa_n+q)\}$ the sequence of the （r）$px+q$ infinite tree. We call the set composed of all of the sequences of the （r）$px+q$ infinite tree the set of the sequences of the （r）$px+q$ infinite tree, S（r）$px+q$ for short.

The a in Definition 17 can be any predecessor of r; therefore, from Fig. 1 we can obtain all of the leftward extension sequences of $\{a_1=7, a_{n+1}=\beta(3a_n+1)\}$.

Property 14. Sequence A is a leftward extension sequence of $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$, if and only if, $A\in S$（r）$px+q$.

Property 15. If a is a number in the *nth* layer （$n\geq 1$） of （r）$px+q$ infinite tree, then $\{a_1=a, a_{n+1}=\beta(pa_n+q)\}$ is a level n leftward extension sequence of $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$.

For example, 65 is a number in the third layer of Fig. 1. 65 is connected to 49 downward, 49 is connected to 37 downward, and 37 is connected to 7 downward. The sequence obtained: 65,49,37,7,… is just $\{a_1=65, a_{n+1}=\beta(3a_n+1)$. Obviously, $\{a_1=65, a_{n+1}=\beta(3a_n+1)\}$ is a level 3 leftward extension sequence of $\{a_1=7, a_{n+1}=\beta(3a_n+1)\}$: 7,…

We call a_n with n approaching infinity the ultimate term of A.

Because 7 is a term implying left terms in the $3x+1$ sequence, according to the method for the decision of the term implying left terms and the calculation of its predecessor sequence, we can obtain the predecessor sequence of 7: $\{a_1=9, a_{n+1}=4a_n+1\}$. Various numbers in the first layer of Fig. 1 (i.e., （7）$3x+1$ infinite tree) are given by the sequence in question.

The ultimate term in $\{a_1=9, a_{n+1}=4a_n+1\}$ is necessarily a infinity. We call this infinity the level 1 predecessor infinity of 7.

For every consecutive three terms in $\{a_1=9, a_{n+1}=4a_n+1\}$ 9,37,149,597,…there are two terms which are the terms implying left terms in the $3x+1$ sequence. For example, in the first three terms, 37 and 149 are the terms implying left terms in the $3x+1$ sequence.

By the method for the decision of the term implying left terms and the calculation of its predecessor sequence we can obtain, the predecessor sequence of 37 being $\{a_1=49, a_{n+1}=4a_n+1\}$ 49,197,789,… and the predecessor sequence of 149 being $\{a_1=99, a_{n+1}=4a_n+1\}$ 99,397,1589,….

The ultimate terms in $\{a_1=49, a_{n+1}=4a_n+1\}$, $\{a_1=99, a_{n+1}=4a_n+1\}$,… are all infinity and they are situated at the second layer of Fig. 1. We call this infinity the level 2 predecessor infinity of 7. Obviously, there are infinitely many level 2 predecessors of infinity of 7.

Similarly, in the （7）$3x+1$ infinite tree, except there is only one level 1 predecessor infinity of 7, there are infinitely many level n(n=2,3,…) predecessor infinity of 7.

According to the above discussion, we have

Property 16. In the （r）$px+q$ infinite tree, except there is only one level 1 predecessor infinity of r, there are infinitely many level n (n=2,3,…) predecessor infinity of r.

Property 17. Let us suppose that $A\in S$（r）$px+q$. If A is a circular sequence, then all of the sequences in S（r）$px+q$ (plus the root sequence $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$) are circular sequences.

Proof: From $A\in S$（r）$px+q$ and Property 14, we know that A is a leftward extension sequence of $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$. Thus, from Definition 15, we know that $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a subsequence of A.

From A being a circular sequence and Corollary 8, we know that $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a circular sequence.

Because $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a subsequence of all of the sequences in S（r）$px+q$,

according to Corollary 8, all of the sequences in $S(r)px+q$ are circular sequences. Q.E.D.
Property 17 tells us that, of the sequences in the set $S(r)px+q$, either they are all circular sequences, or none is a circular sequence.
Fig. 2 is given below, which is the (43) $5x+1$ infinite tree.

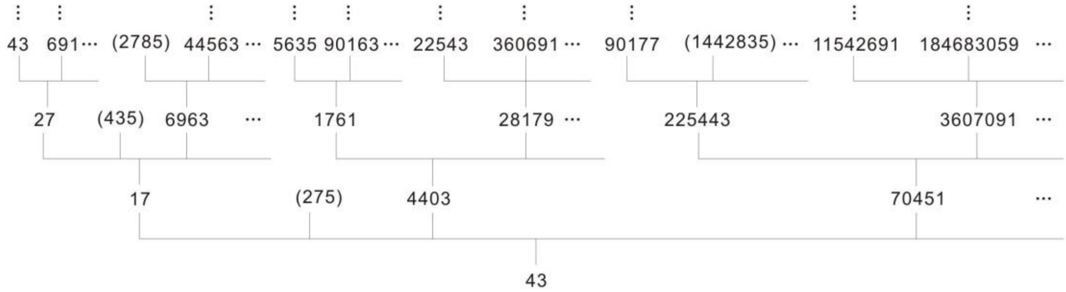

Fig. 2 (43) 5x+1 infinite tree

In the second layer of Fig. 2, there is number 27. The second term in the root sequence $\{a_1=43, a_{n+1}=\beta(5a_n+1)\}$: 43,27,… of the (43) $5x+1$ infinite tree is also 27. Now, $\{a_1=27, a_{n+1}=\beta(5a_n+1)\}$: 27,17,43, 27,… is a circular sequence.

Property 18. Let us suppose that c is a number in the nth layer ($n\geq 1$) of the $(r)px+q$ infinite tree. If the kth term a_k in $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is $a_k=c$ then all of the sequences in $S(r)px+q$ (plus $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$) are circular sequences.

Proof: From the supposition and Property 15, we know that $\{b_1=c, b_{n+1}=\beta(pb_n+q)\}$ is a level n leftward extension sequence of $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ (46)

From phrase (46) and Property 14, we know that $\{b_1=c, b_{n+1}=\beta(pb_n+q)\}\in S(r)px+q$. (47) From phrase (46) and Property 13, we know that $a_k=b_{k+n}=c$.

From $\{b_1=c, b_{n+1}=\beta(pb_n+q)\}$, we know that $b_1=c$. Thus, $b_1=b_{k+n}$. From Basic theorem 2, we know that $\{b_1=c, b_{n+1}=\beta(pb_n+q)\}$ is a circular sequence (48)

From (47), phrase (48) and Property 17, we know that all of the sequences in $S(r)px+q$ (plus $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$) are circular sequences. Q.E.D.

Property 18 tells us that, so long as certain number in the $(r)px+q$ infinite tree equals certain number in the root sequence $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$, all sequences in $S(r)px+q$ are circular sequences.

Property 19. Let us suppose that A is a $px+q$ sequence. Then, A being a noncircular sequence is unprovable.

Proof: Let the second term of A be r. We know that r is necessarily a term implying left terms in the $px+q$ sequence. From Definition 16, we can obtain the $(r)px+q$ infinite tree.

From r being the second term of A and Definition 15, we know that $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a subsequence of A. From this and Corollary 8, we know that A is a circular sequence if and only if $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a circular sequence.

To this end, we prove that $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ being a noncircular sequence is unprovable. There are two cases for term a_n in $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$.

Case 1. When n is any positive integer, a_n is not larger than odd number M, which means that there are necessarily equal terms in $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$. Thus, $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a circular sequence. That is, $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is not a noncircular sequence.
Case 2. When n approaches infinity, a_n is infinity (denoted as a_∞).

The predecessor infinity of r is a term in the $(r)px+q$ infinite tree, and a_∞ is a term in $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$. From Property 18 we know that, if certain predecessor infinity of r equals to a_∞ then $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a circular sequence. Therefore, if we want to prove $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a noncircular sequence, then we must prove that a_∞ is unequal to every predecessor infinity of r.

From Property 16, we know that there are infinitely many predecessor infinity of r, and it is impossible to prove that a_∞ is unequal to the infinitely many predecessor infinity.
Thus, $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ being a noncircular sequence is unprovable.
Q.E.D.
The significance of Property 19 lies in that it topples people's common sense. To general sequence A, when

$n\to\infty$, $a_n\to\infty$, A is necessarily a noncircular sequence. However, it is not the case for $px+q$ sequences. Please see the example:

Example 5. Let us suppose A being $\{a_1=27, a_{n+1}=\beta(5a_n+1)\}$: 27,17,43, 27,… (i.e., A is a circular sequence). Let us suppose B being $\{b_1=b, b_{n+1}=\beta(pb_n+q)\}$ and b being a level 1 predecessor infinity of 27 (Now, B is the level 1 leftward extension sequence of A, the first term of B is $b\to\infty$). Let us suppose C being $\{c_1=c, c_{n+1}=\beta(pc_n+q)\}$ and c being the *kth* predecessor of b with $k\to\infty$ (Now, C is the level k leftward extension sequence of B. Considering $k+1\to\infty$, the $k+1th$ term of C is $c_{k+1}=b\to\infty$). Let $k+1=n$. From the above suppositions we know that $n\to\infty$ and $c_n\to\infty$. However, C is a circular sequence, because circular sequence A is a subsequence of C.

Property 19 can also be stated as

Property 20. Any $px+q$ sequence A does not necessarily not have equal terms. From Property 20 we know that Corollary 9. Any $3x+1$ sequence A does not necessarily not have equal terms.

V. Equations of equal terms of 5x+1 sequences

The reason for us to discuss the equations of equal terms of $5x+1$ sequences is that they have similar properties to those of the equations of equal terms of the $3x+1$ sequences.

Definition 18. Let us suppose that $a_1,\ldots, a_{k+1}\in N_o$, and $a_2=(pa_1+q)/2^{i_1}$, $a_3=(pa_2+q)/2^{i_2},\ldots, a_{k+1}=(pa_k+q)/2^{i_k}$. Then, we call $i_1, i_2,\ldots, i_k$ the p-q iterative k successive exponents of a_1.

It is not hard to discover that $a_1,\ldots, a_{k+1}$ in Definition 18 are the first $k+1$ terms of the $px+q$ sequence $\{a_1= a_1, a_{n+1}=\beta(pa_n+ q)\}$.

For example, find the 3-1 iterative 3 successive exponents of 11 and the 5-3 iterative k successive exponents of 1.

When finding the 3-1 iterative 3 successive exponents of 11, $p=3, q=1, a_1=11$. $a_2=(11\times3+1)/2^{i_1}=(17\times2^1)/2^1=17$, we obtain $i_1=1$. $a_3=(17\times3+1)/2^{i_2}=(13\times2^2)/2^2=13$, we obtain $i_2=2$. $a_4=(13\times3+1)/2^{i_2}=(5\times2^3)/2^3=5$, we obtain $i_3=3$.

Thus, the 3-1 iterative 3 successive exponents of 11 are $i_1=1$, $i_2=2$, and $i_3=3$. It is not hard to discover that a_1, a_2, a_3, and a_4 are the first four terms in the $3x+1$ sequence $\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$ 11,17,13,5,….

When finding the 5-3 iterative k successive exponents of 1, $p=5$, $q=3$, and $a_1=1$. $a_2=(1\times5+3)/2^{i_1}=(2^3)/2^3=1$, we obtain $i_1=3$; …; $a_{k+1}=(1\times5+3)/2^{i_1}=(2^3)/2^3=1$, $i_k=3$.

Thus, the 5-3 iterative k successive exponents of 1 are $i_1=i_2=\ldots=i_k=3$. Obviously, $a_1,a_2,\ldots a_{k+1}$ are the first $k+1$ terms in the $5x+3$ sequence $\{a_1=1, a_{n+1}=\beta(5a_n+3)\}$ 1,1,….

Lemma 4. Let us suppose that the 5-1 iterative k successive exponents of the *ith* term a_i in the $5x+1$ sequence A are $i_1, i_2, \ldots, i_k$. If $a_i=a_{i+k}$, then

$$a_i=(5^{k-1}+5^{k-2}\cdot2^{i_1}+\ldots+5\cdot2^{i_1+i_2+\ldots+i_{k-2}}+2^{i_1+i_2+\ldots+i_{k-1}})/(2^{i_1+i_2+\ldots+i_k}-5^k). \quad (49)$$

Proof: From the definition of k successive exponents, we know that

$$a_{i+1}=(5a_i+1)/2^{i_1} \quad (50)$$

$$a_{i+2}=(5a_{i+1}+1)/2^{i_2} \quad (51)$$

……

$a_{i+k}=(5a_{i+k-1}+1)/2^{i_k}$ Substituting (50) into (51), we obtain $a_{i+2}=(5^2a_i+5+2^{i_1})/2^{i_1+i_2}$ Likewise,

$a_{i+3}=(5^3a_i+5^2+5\cdot2^{i_1}+2^{i_1+i_2})/2^{i_1+i_2+i_3}$

……

$a_{i+k}=(5^ka_i+5^{k-1}+5^{k-2}\cdot2^{i_1}+\ldots+5\cdot2^{i_1+i_2+\ldots+i_{k-2}}+2^{i_1+i_2+\ldots+i_{k-1}})/2^{i_1+i_2+\ldots+i_k}$.

From $a_i=a_{i+k}$, we know that

$a_i=(5^ka_i+5^{k-1}+5^{k-2}\cdot2^{i_1}+\ldots+5\cdot2^{i_1+i_2+\ldots+i_{k-2}}+2^{i_1+i_2+\ldots+i_{k-1}})/2^{i_1+i_2+\ldots+i_k}$. $2^{i_1+i_2+\ldots+i_k}a_i=5^ka_i+5^{k-1}+5^{k-2}\cdot2^{i_1}+\ldots+5\cdot2^{i_1+i_2+\ldots+i_{k-2}}+2^{i_1+i_2+\ldots+i_{k-1}}$. $2^{i_1+i_2+\ldots+i_k}a_i-5^ka_i=5^{k-1}+5^{k-2}\cdot2^{i_1}+\ldots+5\cdot2^{i_1+i_2+\ldots+i_{k-2}}+2^{i_1+i_2+\ldots+i_{k-1}}$.

$a_i=(5^{k-1}+5^{k-2}\cdot2^{i_1}+\ldots+5\cdot2^{i_1+i_2+\ldots+i_{k-2}}+2^{i_1+i_2+\ldots+i_{k-1}})/(2^{i_1+i_2+\ldots+i_k}-5^k)$. Q.E.D. Now, we use symbol x to replace a_i. Thus, (49) becomes (52):

$x=(5^{k-1}+5^{k-2}\cdot 2^{i_1}+\ldots+5\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-5^k)$ (52)

Since (52) is an equality, we can view it as an equation with x and $i_1, i_2, \ldots, i_k$ as its variables (called the equation of equal terms of 5x+1 sequences). We call the solution $x \in N_o$, and $i_1, i_2, \ldots, i_k$ being the 5-1 iterative k successive exponents of x the characteristic solution of the equation of equal terms of the 5x+1 sequences.

Obviously, the characteristic solution of the equation of equal terms is its effective solution (see Note 2). That is, if the equation of equal terms of the 5x+1 sequence has the characteristic solution, then the 5x+1 sequence A have equal terms; otherwise, A has no equal term. Thus, Conclusion 8. The 5x+1 sequence A has equal terms if and only if the equation of equal terms of the 5x+1 sequence has a characteristic solution.

A more important fact is that when we assume any 5x+1 sequence to have equal terms x and the 5-1 iterative k successive exponents of x to be $i_1, i_2, \ldots, i_k$, we can all obtain the equation of equal terms. That is, every 5x+1 sequence can be a "sequence A". Thus, from Conclusion 8, we know that

Conclusion 9. Any 5x+1 sequence has equal terms if and only if the equation of equal terms of the 5x+1 sequence has a characteristic solution.

We have to say that the above feature of the equation of equal terms and the ratio of the circumference of a circle to its diameter $\pi=c/d$ (c is the circumference, d is the diameter) are strikingly similar. We know that the most important parameter for describing a circle is its radius r, but π is irrelevant to r. Thus, π—the ratio of circumference to diameter—that would have been the ratio of one circle becomes the ratio of all circles. Similarly, the most important parameter for describing a sequence is its terms, but the equation of equal terms is irrelevant to the terms of any 5x+1 sequence. Thus, the equation of equal terms having a characteristic solution that would have been the sufficient and necessary condition of a certain 5x+1 sequence A being a circular sequence becomes the sufficient and necessary condition of any 5x+1 sequence being a circular sequence.

We know that, $\{a_1=3, a_{n+1}=\beta(5a_n+1)\}$ 3,1,3,1,… is a 5x+1 sequence with the circular length being 2.

Let k=2, from (52) we can obtain,

Characteristic solution 1: $x=3, i_1=4, i_2=1$. Characteristic solution 2: $x=1, i_1=1, i_2=4$.

$\{a_1=275, a_{n+1}=\beta(5a_n+1)\}$ 275,43,27,17,43,… and $\{a_1=83, a_{n+1}=\beta(5a_n+1)\}$ 83,13,33,83,… are the 5x+1 sequences with the circular length being 3. Let k=3, from (52) wecan obtain, Characteristic solution 3: $x=43, i_1=3, i_2=3, i_3=1$.

Characteristic solution 4: $x=27, i_1=3, i_2=1, i_3=3$. Characteristic solution 5: $x=17, i_1=1, i_2=3, i_3=3$. Characteristic solution 6: $x=83, i_1=5, i_2=1, i_3=1$. Characteristic solution 7: $x=13, i_1=1, i_2=1, i_3=5$. Characteristic solution 8: $x=33, i_1=1, i_2=5, i_3=1$.

From the above result we can see that, x in the characteristic solution is a circular term of the 5x+1 sequence (i.e., the equal term of the 5x+1 sequence). In addition, from (52) we can find all of the equal terms in all 5x+1 sequences. Therefore,

Conclusion 10. x in the characteristic solution of the equation of equal terms of the 5x+1 sequence is the equal term in the 5x+1 sequence. All of the equal terms in all of the 5x+1 sequences can be found by the equation of equal terms of the 5x+1 sequence.

It is worth mentioning that, until now, we have been unable to prove that the above equation of equal terms of the 5x+1 sequence has only the above eight characteristic solutions.

VI. Reproof of the 3x+1 problem

According to the deeven concept (See Definition 2), 3x+1 problem can be stated as: Starting from positive odd numbers a, multiplying by 3, adding 1, and then using deeven process repeatedly, we necessarily arrive at odd number 1 in finite steps. Obviously, the 3x+1 problem is an iterative process.

When we denote positive odd number a as a_1, denote the result of multiplying 3, adding 1, and deeven to a_1 as a_2, now $a_2=\beta(3a_1+1)$; we denote the result of multiplying 3, adding 1, and deeven to a_2 as a_3, now $a_3=\beta(3a_2+1)$.

Analogously, we can obtain sequence A: $a_1=a$, $a_2=\beta(3a_1+1)$, …, $a_{n+1}=\beta(3a_n+1)$, …. Obviously, sequence A is a mapping recurrent sequence $\{a_1=a, a_{n+1}=\beta(3a_n+1)\}$, i.e., sequence A is a 3x+1 sequence.

Thus, if we want to verify that the 3x+1 problem is true, then we only need to prove that any 3x+1 sequence has the terms equal to 1. Now, let us perform the work.

Similar to the proof of Lemma 4, we can prove that, Lemma 5. Let us suppose that the 3-1 iterative k successive exponents of the ith term a_i in 3x+1 sequence A is $i_1, i_2, \ldots, i_k$. If $a_i=a_{i+k}$, then $a_i=(3^{k-1}+3^{k-}$

$2\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-3^k)$.

We use x to replace a_i. Thus, we have $x=(3^{k-1}+3^{k-2}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-3^k)$ (53)

We call (53) the equation of equal terms of the $3x+1$ sequence and call the solution $x\in N_O$, and $i_1, i_2, \ldots, i_k$ being the 3-1 iterative k successive exponents of x the characteristic solution of the equation of equal terms of the $3x+1$ sequence.

We must note that " if $a_i = a_{i+k}$ " in Lemma 5 (in the equation of equal terms a_i is x) demonstrates that in Lemma 5, we suppose a $3x+1$ sequence A "if it has equal terms". The principle of supposition (see Note 1) tells us that to make such a supposition, we must assume that the "$3x+1$ sequence does not necessarily not have equal terms" as its premise (Note: The premise has been given in Corollary 9). In our previous proof (See [1] in the Reference), the premise was not proven rigorously. Therefore, we present this paper to remedy this defect.

Similar to Conclusion 9, we can obtain

Conclusion 11. Any $3x+1$ sequence has equal terms if and only if the equation of equal terms of the $3x+1$ sequence has the characteristic solution.

Similar to Conclusion 10, we can obtain

Conclusion 12. x in the characteristic solution of the equation of equal terms of the $3x+1$ sequence is an equal term of the $3x+1$ sequence. All equal terms in all $3x+1$ sequences can be found from the equation of equal terms of the $3x+1$ sequence.

We know that the range of function $f(i_1,\ldots, i_n)=(3^{n-1}+3^{n-2}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{n-2}}+2^{i_1+i_2+\cdots+i_{n-1}})/(2^{i_1+i_2+\cdots+i_n}-3^n)$ is infinite. However, we should note that in the range, there is only one number that is a positive integer. That is,

Lemma 6. When $f(i_1,\ldots, i_n)\in N$, $f(i_1,\ldots, i_n)=1$ is unique, or, $f(i_1,\ldots, i_n)=1\in N$ is unique.

Proof: We use mathematical induction.

Step 1: We verify that when $f(i_1)\in N$, $f(i_1)=1$ is unique. Because $f(i_1)=1/(2^{i_1}-3)$, there exists and only exists $i_1=2$ such that $f(i_1)=1$, i.e., $f(i_1)=1\in N$ is unique. Hence, when $n=1$, Lemma 6 holds.

To avoid the confusion of the result inferred by Step 3, here, we note the relevance between $f(i_1,\ldots, i_{k+1})$ and $f(i_1,\ldots, i_k)$.

$f(i_1,\ldots, i_k)=(3^{k-1}+3^{k-2}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-3^k)$ (54) Therefore,

$3^{k-1}+3^{k-2}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}}=(2^{i_1+i_2+\cdots+i_k}-3^k)\cdot f(i_1,\ldots, i_k)$ (55) In addition,

$f(i_1,\ldots, i_{k+1})=(3^k+3^{k-1}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{k-1}}+2^{i_1+i_2+\cdots+i_k})/(2^{i_1+i_2+\cdots+i_{k+1}}-3^{k+1})$. Thus, $f(i_1,\ldots, i_{k+1}) =(3(3^{k-1}+3^{k-2}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})+2^{i_1+i_2+\cdots+i_k})/(2^{i_1+i_2+\cdots+i_{k+1}}-3^{k+1})$ (56)

Substituting (55) into (56), we obtain

$f(i_1,\ldots, i_{k+1})=(3(2^{i_1+i_2+\cdots+i_k}-3^k)\cdot f(i_1,\ldots, i_k)+2^{i_1+i_2+\cdots+i_k})/(2^{i_1+i_2+\cdots+i_{k+1}}-3^{k+1})$ (57)

(The above process demonstrates that when $f(i_1,\ldots, i_k)$ is given by (54), $f(i_1,\ldots, i_{k+1})$ in (56) and (57) are the same function. It is worth noting that (57) shows that $f(i_1,\ldots, i_k)$ is a "constituent" of $f(i_1,\ldots, i_{k+1})$. The relationship between $f(i_1,\ldots, i_{k+1})$ and $f(i_1,\ldots, i_k)$ provides the basis for Step 3. Therefore, the existence of (57) is the fundamental reason for Lemma 6 being able to be proved by mathematical induction.)

Step 2: Let us suppose that $f(i_1,\ldots, i_k)=1\in N$ is unique.

Step 3: We prove $f(i_1,\ldots, i_{k+1})=1\in N$ is unique.

From the inductive supposition and (57), we know that

$f(i_1,\ldots, i_{k+1})=(3(2^{i_1+i_2+\cdots+i_k}-3^k)+2^{i_1+i_2+\cdots+i_k})/(2^{i_1+i_2+\cdots+i_{k+1}}-3^{k+1})$ $f(i_1,\ldots, i_{k+1})=(4\cdot 2^{i_1+i_2+\cdots+i_k}-3^{k+1})/(2^{i_1+i_2+\cdots+i_{k+1}}-3^{k+1})$

$f(i_1,\ldots, i_{k+1})=(2^{i_1+i_2+\cdots+i_k+2}-3^{k+1})/(2^{i_1+i_2+\cdots+i_{k+1}}-3^{k+1})$ (58)

From (58), we know that when $i_{k+1}>2$, $f(i_1,\ldots, i_{k+1})<1$. When $i_{k+1}=1$, $f(i_1,\ldots, i_{k+1})=(2^{i_1+i_2+\cdots+i_k+2}-3^{k+1})/(2^{i_1+i_2+\cdots+i_k+1}-3^{k+1})$

$=(2\cdot 2^{i_1+i_2+\cdots+i_k+1}-3^{k+1})/(2^{i_1+i_2+\cdots+i_k+1}-3^{k+1})$

$=((2^{i_1+i_2+\cdots+i_k+1}-3^{k+1})+2^{i_1+i_2+\cdots+i_k+1})/(2^{i_1+i_2+\cdots+i_k+1}-3^{k+1})$

$=1+2^{i_1+i_2+\cdots+i_k+1}/(2^{i_1+i_2+\cdots+i_k+1}-3^{k+1})\notin N$。

Thus, there is and only is $i_{k+1}=2$ such that $f(i_1,\ldots,i_{k+1})=1\in N$, i.e., $f(i_1,\ldots,i_{k+1})=1\in N$ is unique.
Therefore, we have proved that when $f(i_1,\ldots,i_k)=1\in N$ is unique, $f(i_1,\ldots,i_{k+1})=1\in N$ is unique.
Q.E.D.
From Lemma 6, we can prove,
Conclusion 13. The equation of equal terms of the $3x+1$ sequence
$x = (3^{n-1}+3^{n-2}\cdot 2^{i_1}+\ldots+3\cdot 2^{i_1+i_2+\ldots+i_{n-2}}+2^{i_1+i_2+\ldots+i_{n-1}})/(2^{i_1+i_2+\ldots+i_n}-3^n)$ has the following characteristic solution only:
$x=1$, and $i_1=i_2=\ldots=i_n=2$. (59) Conclusion 14. Any $3x+1$ sequence has the term equal to 1.

Proof: From Conclusion 13, we know that (1). The equation of equal terms of the $3x+1$ sequence has a characteristic solution: $x=1, i_1=i_2=\ldots=i_n=2$.(2). The solution is unique. From

(1) and Conclusion 11, we know that any $3x+1$ sequence has equal terms. From (2) and Conclusion 12, we know that all equal terms of the $3x+1$ sequence are equal to 1. Therefore, any $3x+1$ sequence has the term equal to 1. Q.E.D.

That Conclusion 14 holds means that the $3x+1$ problem is true.

Note 1. Principle of supposition
Here, we give an important logical principle that must be abided by in mathematical proofs.

Principle of supposition: If proposition *A* is necessarily true, then we cannot suppose *A* to be false; if proposition *A* is necessarily false, then we cannot suppose *A* to be true.

When proposition *A* being true (false) is the result of logical (or factual) proof, we say *A* being necessarily true (false). *A* that is necessarily true (false) is called a conclusion or theorem. The fundamental difference between a proposition and a conclusion lies in that the former is a judgment whose truth or falsity is unknown, while the latter is a judgment whose truth or falsity is known. Therefore, for the former, we can suppose it being true and we can also suppose it being false. For the latter, we cannot make the opposite supposition (in fact, this is another way of stating the principle of supposition).

(Note: Because there are fundamental differences between propositions and conclusions,

their statements should be differentiated. For example, conclusion I corresponding to proposition I " 6 can be divided evenly by 3" should be " it is true that 6 can be divided evenly by 3"; conclusion II corresponding to proposition II "5 can be divided evenly by 3" should be "it is false that 5 can be divided evenly by 3". However, people are accustomed to omitting "it is true" and "it is false". They usually mention conclusion I as "6 can be divided evenly by 3", mention conclusion II as "5 cannot be divided by 3 evenly". Although the omissions do not result in misunderstanding generally, we must not confuse propositions with conclusions.)

The correctness of the principle of supposition is self-evident. For example, in the axiomatic system of number theory, we must not suppose "3+2–5=1" or"3+2–5≠0". Were we to make such suppositions, there would be 0=1, 0=*n* and 0≠0, *n*≠*n*, etc. Therefore, the axiomatic system of number theory runs into unbearable chaos. Likewise, in the Euclidean geometric axiomatic system, we cannot suppose that the sum of the internal angles is not equal to 180°; in non-Euclidean geometric axiomatic systems, we cannot suppose that the sum of the internal angles is equal to 180°, etc..

Note 2. Discussion on the list of equations to solve the application problems

Application problems in middle school textbooks have a common feature: One or more equations can be listed that correspond to the problem.

When we list the equations corresponding to the application problem, we face two objects. One is the application problem (called the original problem) given. Another is the equation listed. Thus, two questions need to be answered: 1. Why can the solution of the original problem be implemented through the solution of the equation listed? 2. Which solutions of the equation listed are the solutions of the original problem? To answer these questions, let us first investigate an example.

Problem 1. The sum of the square of an integer and a positive integer is equal to 3. Find the two numbers.

Solution: Let us suppose that the integer to be found is x, and the positive integer to be found is *y*. From the problem, we obtain

$$x^2+y=3 \quad (60)$$

Here, Problem 1 is the original problem, and equation (60) is the equation listed. At first glance, they are quite different, with no commonality. However, they have quite identical elements. Because x is set as an integer, x^2 can be read as"the square of an integer." Likewise, y can be read as "a positive integer". Thus, equation (60) can be read as "the sum of the square of an integer and a positive integer is equal to 3 ". Hence, the object given by the original problem and that given by the equation listed are the same, i.e., the equation listed is a restatement of the original problem. Thus, we say that the original problem and the equation listed are "identical" and call this phenomenon "the principle of identity". The principle of identity tells us that finding the solution of the original problem can be implemented by finding the solution of the equation listed. This is the reason for the listing of an equation to solve the application problem to be a classical mathematical method.

In addition, from the pure equation perspective, x and y in (60) can be any real number or complex number. However, for (60) and Problem 1 to be identical, x must be an integer, and y must be a positive integer. Here, x and y are called variables, and the conditions set for variables x and y are called the constraint condition. Therefore, more precisely, only all of the variables satisfy the constraint condition, the equation listed and the original problem are identical. Since in this circumstance the two are identical, the solutions of the two are necessarily the same. The remaining task is to determine what kind of solutions are one of the equations listed in this circumstance.

The so-called solution of an equation, formally speaking, is an assignment to the relevant variables. For the equation listed, if the assignment to each variable satisfies its constraint condition, then the solution (called the effective solution) is one whose variables in the equation listed satisfy the constraint condition. Hence, we know that all of the effective solutions of the equation listed are one of the original problems.

It is not hard to verify that these effective solutions are all solutions of Problem 1. Here, we first know that Problem 1 has solutions, and then we know what the solutions are.

Problem 2. The sum of the square of an integer and a positive integer is equal to -3. Find the two numbers.

Solution: Let us suppose that the integer to be found is x, and the positive integer to be found is y. From the problem, we obtain

$$x^2+y=-3 \tag{61}$$

Obviously, equation (61) has no effective solution. Thus, Problem 2 has no solution. We have,

Conclusion 15. The original problem has solutions if and only if the equation listed has effective solutions.

References

[1]. Ming Xian, Xunwei Zhou, Zi Xian, The Proof Of 3x+1 Problem, IOSR Journal Of Mathematics, Volume 17, Issue 2, Series 3, 05-12, 2021