IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 18, Issue 2 Ser. III (Mar. – Apr. 2022), PP 01-32
www.iosrjournals.org

Px+q sequences of numbers and *px+q* infinite trees

Ming Xian[1] Xunwei Zhou[2] Zi Xian[3]
[1] *Fushun Geographical Information Bureau, Fushun, Liaoning province 113008, China*
[2] *Beijing key laboratory of information service engineering, Beijing Union University, Beijing 100101, China*
[3] *Fushun Library, Fushun, Liaoning province 113006, China*

Abstract: *3x+1 sequences of numbers are the special cases of px+q sequences of numbers. Px+q sequences of numbers are the mapping recurrent sequences of numbers. The general term a_n in the classical sequences of numbers is a function of n, while the general term a_n of the px+q sequences of numbers is not a function of n. Usually, the classical sequences of numbers are not circular, while circularity is the most important property of the px+q sequences of numbers. The classical sequences of numbers only extend from left to right, while the px+q sequences of numbers can be extended from right to left. The leftward extendedness of the px+q sequences of numbers results in the infinite trees. Because the properties of the equiratio residual sequences of numbers are the basis for studying the leftward extendedness of the px+q sequences of numbers, in this paper, both equiratio residual sequences of numbers and px+q sequences of numbers are studied.*

Keywords: *Mapping recurrent sequences of numbers; px+q sequences of numbers; equiratio residual sequences of numbers; leftward-extendable sequences of numbers; px+q infinite trees*

Date of Submission: 28-03-2022 Date of Acceptance: 09-04-2022

I. Introduction

The authors change 3*x*+1 problem into all-odd *3x*+1 sequences of numbers (in this paper we call them 3*x*+1 sequences of numbers) and prove the problem to be true[1]. We know that, if x_1 is an odd number then $y_1=3x_1+1$ is an even number. When all of the factors 2 of y_1 are eliminated then an odd number x_2 can be obtained. For example, $x_1=9$，$y_1=3x_1+1=28=7 \cdot 2^2$. Eliminating all of the factors of 2 from y_1 we can obtain the odd number $x_2=7$. We call the process from y_1 to x_2 the deeven process of y_1. That is, odd number 9 multiplies 3 and adds 1 and deeven then odd number 7 can be obtained. Odd number 7 multiplies 3 adds 1 and deeven then odd number 11 can be obtained. Odd number 11 multiplies 3 and adds 1 and deeven then odd number 17 can be obtained. ⋯. By the above process the 3*x*+1 sequence of numbers with all the terms are odd numbers can be obtained:

Sequence of number *A*：9,7,11,17，⋯.

From the second term onward, every term of sequence of numbers *A* are obtained by multiplying 3, adding 1 and deeven on the previous term. Because the process of multiplying 3, adding 1, and deeven on the previous term to obtain the new term is a mapping process, from the second term onward, every term of sequence of numbers *A* is a mapping of its previous term, e. g., 7 is the image of original image 9, 11 is the image of original image 7, 17 is the image of original image 11, ….Also because the process of obtaining sequence of numbers *A* is a recurrent process, we call sequence of numbers *A* a (unary) mapping recurrent sequence of numbers. The 3*x*+1 sequences of numbers are the special cases of the *px+q* sequences of numbers, which are only one kind of the mapping recurrent sequences of numbers.

Obviously, the general term a_n of sequence of numbers *A* is not a function of *n*, while the general term a_n of the classical sequences of numbers is a function of *n*. This shows the novelty and uniqueness of the mapping recurrent sequences of numbers. Moreover, the unary mapping recurrent sequences of numbers have a very important property: if a unary mapping recurrent sequence of numbers has two equal terms then the sequence of numbers in question is necessarily a circular sequence. This paves the way for studying the circular sequences of numbers. For several reasons, people have not studied the circular sequences of numbers. Factually, the circular sequences of numbers are the mathematical objects extremely valuable for study. This shows the importance of the mapping recurrent sequences of numbers. The classical sequences of numbers extend from left to right, while the *px+q* sequences of numbers can not only extend from left to right but also from right to left, forming the infinite trees or the complete trees.

Another kind of mapping recurrent sequence of numbers is the equiratio residual sequence of numbers. Its simplest sequence of numbers is convenient to compute, so it has many applications. More importantly, its properties lay a foundation for studying the leftward extendedness of the *px+q* sequences of numbers.

The concept of mapping recurrent sequences of numbers is a new method for constructing sequences of

numbers. It is our original innovation, no previous work can be referred.

The rest of this paper is organized as follows: In Section 2 the mapping recurrent sequences of numbers, the parasitic sequences of numbers and their circularity are introduced. If each term in sequence of numbers *B* is a function of the corresponding term in sequence of number *A*, then *B* is a parasitic sequence of numbers of *A*. For example, sequence of numbers of even numbers *B*：2， 4， 6，... is a parasitic sequence of numbers of natural numbers *A*：1， 2， 3，... . and there is $b_n=2a_n$. In this section, we discuss the sufficient conditions for the mapping recurrent sequences of numbers and the parasitic sequences of numbers to be circular sequences of numbers, based on which we prove that a fraction is necessarily a circular decimal.

In Section 3 the leftward extendedness of the *px+q* sequences of numbers are introduced. *px+q* sequence of numbers is defined as follows: Suppose $a, p, q \in N_o$. If the terms in mapping recurrent sequence of numbers $\{a_n\}$ are $a_1= a$, $a_{n+1}=\beta(pa_n+q)$，then we call $\{a_n\}$ a *px+q* sequence of numbers, denoted as $\{a_1= a, a_{n+1}=\beta(pa_n+q)\}$.（$\beta(\ )$ means to delete all of the factors 2）. Now, we expound what is the leftward extendedness of the *px+q* sequences of numbers.

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

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

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

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

The above are four 5*x*+1 sequences of numbers. It is not hard to see that, sequence of numbers 2 is formed by adding one term “1331” on the left of the first term 13 of sequence of numbers 1; sequence of numbers 3 is formed by adding two terms “4259,1331” on the left of the first term 13 of the sequence of numbers 1; sequence of numbers 4 is formed by adding three terms “54515,4259,1331” on the left of the first term 13 of sequence of numbers 1. For convenience,, we call sequence of numbers 2, sequence of numbers 3 and sequence of numbers 4 as the degree 1 leftward extension sequence of numbers, the degree 2 leftward extension sequence of numbers and the degree 3 leftward extension sequence of numbers respectively.

The main focus of this section is to obtain its degree *n* leftward extension sequences of numbers from “sequence of numbers 1”.

Suppose $a, b \in N_o$， $b = \beta(pa+q)$. We call *a* as the degree 1 predecessor of *b*. Similarly, we can define the degree *n* predecessor.（*a* being a predecessor of *b* means *a* being a left term of *b*）

Besides, from sequence of numbers 2 we see that, odd number 13 has necessarily predecessor 1331. But, the first term 54515 of sequence of numbers 4 has no predecessor. That is to say, as a term in sequence of numbers 2 (i.e., 5*x*+1 sequence of numbers), odd number 13 has a predecessor, we call it a term implying left terms. While 54515 has no predecessor, we call it a term without a left term.

We prove that, as to the *px+q* sequences of numbers, when $(p, (2^{\delta p(2)}-1)/p)=1$， in a residual system of *p* with all terms being odd numbers, there are $\delta_p(2)$ terms implying left terms.

In Section 4 the infinite trees and the complete trees formed by the leftward extendedness of the *px+q* sequences of numbers are introduced. Suppose *r* is a term implying left terms in the *px+q* sequences of numbers. Step 1: We use lines to connect *r* with every degree 1 predecessor of *r*. Step 2: We use lines to connect every predecessor *r′* which is the term implying left terms with every degree 1 predecessor of *r′*. We repeat Step 2, the figure we obtain at last is called a（*r*）*px+q* infinite tree, (See Fig. 1). And we call $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ the root sequence of numbers of the（*r*）*px+q* infinite tree. (The infinite trees are composed from the sequences of numbers, and the sequences of numbers are composed from the numbers. Therefore, the relationship between the infinite trees and the sequences of numbers is similar to one between the sequences of numbers and the numbers. Hence, the infinite trees are a new subject of mathematics.)

Fig. 1 gives the（7）3*x*+1 infinite tree, which is formed as follows: Step 1: Connect 7 with each of its degree 1 predecessors, i.e., 9,37,149,597,⋯. In 7's degree 1 predecessors, 37,149,⋯ are the terms implying left terms in the 3*x*+1 sequence of numbers. Step 2: Connect 37 with each of its degree 1 predecessors, i.e., 49,197,789,⋯, connect 149 with each of its degree 1 predecessors, i.e., 99,397,1589,....Analogously, we obtain Fig. 1.

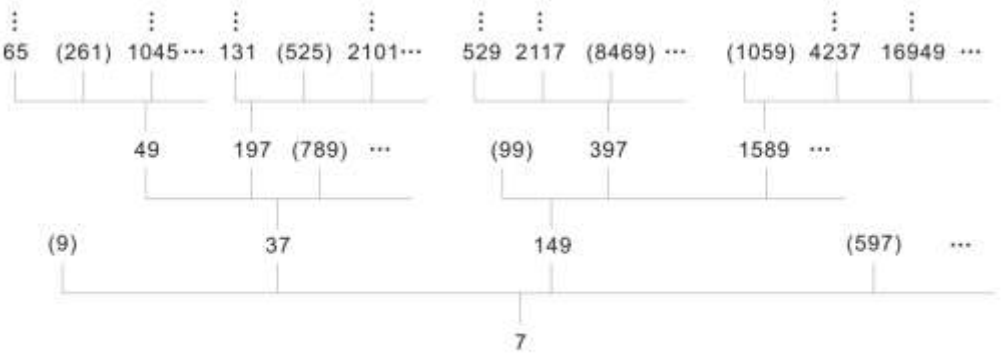


Fig. 1. [7] 3x+1 infinite tree

Similarly, we can obtain complete trees.

In Section 5 the relationship between the characteristic solutions of the equations of equal terms and the $px+q$ circular sequences of numbers and their connection with the complete trees are introduced. The equation of equal terms of the $px+q$ sequences of numbers is:

$$x=q(p^{k-1}+p^{k-2}\cdot 2^{i_1}+\cdots+p\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-p^k)) \quad (8)$$

As its special case, the equation of equal terms of $5x+1$ sequence of numbers is:

$$x=(5^{k-1}+5^{k-2}\cdot 2^{i_1}+\cdots+5\cdot 2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-5^k) \quad (10)$$

From the perspective of the source of formula (10), when we suppose that $5x+1$ sequence of numbers E has an equal term x we can obtain formula (10). This means that when $5x+1$ sequence of numbers E has an equal term then formula (10) has a characteristic solution. From the perspective of the relationship between the solution of an equation and the solution of a problem, when formula (10) has a characteristic solution then $5x+1$ sequence of numbers E has equal term x. Since a $5x+1$ sequence of numbers is a mapping recurrent sequence of numbers, having equal terms means it is a circular sequence of numbers.

Through finding the characteristic solution of formula (10) we can obtain all of the circular terms of the $5x+1$ sequence of numbers, based on which we can obtain the corresponding complete tree.

Note 1. Suppose mapping recurrent sequence of numbers $\{a_n\}$: $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\, m}\}$, $a<m$, then we call $\{a_n\}$ an equiratio residual sequences of numbers. In this section, the properties of the equiratio residual sequences of numbers are introduced, and the computer algorithms for computing order, primitive root, inverse, higher order congruent equations and exponential congruent equations of the elementary number theory[2] are given, and the definitions for the two types of pseudo prime numbers and the proof of sufficient and necessary condition for prime numbers and the big number factorization are given.

Note 2 give an important logical principle that must be abode by in mathematical proofs.

The principle of supposition: If the proposition A is necessarily true, then we cannot suppose it is false; if the proposition A is necessarily false, then we cannot suppose it is true.

Note 3 is a discussion on "list equations to solve application problems". The application problems in middle school mathematics textbook have a common feature: for a given problem, one or more equations can always be listed corresponding to it. When we list an equation corresponding to an application problem, we face two objects. One is the application problem given (called the original problem), the other is the equation listed. This note clearly expounds why the effective solution (or characteristic solution of the equation listed is a solution of the original problem.

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

1. The word "sequences of numbers" in this paper denotes the infinite sequences of numbers, unless otherwise specified.
2. The lower case italic Latin letters used as variables denote the positive integers, unless otherwise specified.
3. The names of the sequences of numbers in this paper are denoted by the upper case italic Latin letters (with prime or subscript), their corresponding lower case italic Latin letters denote the general terms of the sequences of numbers in question. For example, the general terms of the sequences of numbers A, B' are a_n, b'_n. Sometimes, $\{a_n\}$ is used to denote the sequence of numbers A, $\{b_n\}$ is used to denote the sequence of numbers B.
4. N and N_o are two special symbols. N denotes the set of positive integers, N_o denotes the set of positive odd numbers.

II. Mapping recurrent sequences of numbers and their circularity

First, let us define two operators often used in this paper.

Definition 1: Suppose $0\leq a<m$. Then we denote $a\equiv b \pmod m$ as $a=(b)_{\bmod m}$, and we call $()_{\bmod m}$ the minimal non-negative residue operator modulo m.

From Definition 1 we know that, if a is the non-negative residue of b modulo m, then $a=(b)_{\bmod m}$.

For example, $(10)_{\bmod 7}=3$, $(78)_{\bmod 63}=15$.

The following are the properties of the minimal non-negative residue which will be used in this paper:

Property 1: if $(a)_{\bmod m}=(b)_{\bmod m}$ then $a\equiv b \pmod m$;

Property 2: $(a+b)_{\bmod m}=((a)_{\bmod m}+b)_{\bmod m}$; （Transforming "+" into "×", the 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 integer $k\geq 0$ such that $a=km+(a)_{\bmod m}$.

Definition 2: We define b/a^n satisfying $a^n \mid b$, $a^{n+1} \nmid b$ as $\beta(b)_a$（i.e., $\beta(b)_a=b/a^n$）. We call $\beta()_a$ a de-a-factor operator. $\beta()_2$ is abbreviated as $\beta()$, which is called a deeven operator.

From Definition 2 we know that $\beta(b)_a$ is the result of eliminating factor a from b. Obviously, $\beta(b)_a$ is an integer without the factor a.

For example, $\beta(45)_3=45/3^2=5$, $\beta(40)=40/2^3=5$.

Definition 3: Suppose there is a function f such that sequences of numbers $\{a_n\}$ and $\{b_n\}$ satisfying: $b_n=f(a_n)$, $n=1,2,\cdots$. Then, we call $\{b_n\}$ the **parasitic sequence of numbers** of $\{a_n\}$, and denote $\{b_n\}$ as $\{b_n=f(a_n)\}$.

For example, sequence of numbers $\{b_n\}$: 2,4,6,8,10,$\cdots$ with every term being an even number is a parasitic sequence of numbers of $\{a_n\}$: 1,2,3,4,5,$\cdots$ with every term being a natural number. Because now $b_n=2a_n$, $n=1,2,\cdots$, i.e., $\{b_n\}$: $\{b_n=2a_n\}$.

Now, we define circular sequences of numbers.

People usually call sequence of numbers $\{a_n\}$: 8,10, 1,2,3,1,2,3,1,2,3, $\cdots$ as a circular sequence of numbers with the circular length being 3. Because in sequence of numbers $\{a_n\}$ there are $a_3=a_{3+3n}=1$, $a_4=a_{4+3n}=2$, $a_5=a_{5+3n}=3$, $\cdots(n=1,2,\cdots)$. Or, for every l $(3\leqslant l)$, $a_l=a_{l+3n}$, $n=1,2,\cdots$.

However, the authors find out that, up to now, there is no general definition of the circular sequences of numbers. Therefore, we have:

Definition 4: Suppose that from the *ith* term on, every term of sequence of numbers $\{a_n\}$ satisfying $a_i=a_{i+hn}$, $a_{i+1}=a_{i+hn+1}$, $\cdots(n=1,2,\cdots)$, i.e., for every l $(i\leqslant l)$, sequence of numbers $\{a_n\}$'s term $a_l=a_{l+hn}$. Then, we call sequence of numbers $\{a_n\}$ a **circular sequence of numbers**, call h a **circular length** of $\{a_n\}$, call $a_l(i\leqslant l)$ a **circular term** of $\{a_n\}$.

From Definition 4 we know that, when $i<k$, if a_i is a circular term of $\{a_n\}$ then a_k is a circular term of $\{a_n\}$. When $h \mid d$, if h is a circular length of $\{a_n\}$ then d is also a circular length of $\{a_n\}$.we call the minimal length of the circular lengths of $\{a_n\}$ the **minimal circular length**.

For example, 3 is the minimal circular length of sequence of numbers $\{a_n\}$: 8,10, 1,2,3,1,2,3,1,2,3, $\cdots$, and 6,9, $\cdots$ are also the circular length of $\{a_n\}$. At the same time, from the third term on, all of the terms are the circular terms of $\{a_n\}$.

Definition 5: Suppose a_k is the first circular term of circular sequence of numbers $\{a_n\}$. If $k=1$ then $\{a_n\}$ is called a **pure circular sequence of numbers**; if $k>1$ then $\{a_n\}$ is called a **mixed circular sequence of numbers**, and $a_1,\ldots,a_{k-1}$ are called **non-circular terms** of $\{a_n\}$.

From Definition 5 we know that, a_1,a_2 in sequence of numbers $\{a_n\}$: 8,10,1,2,3,1,2,3,1,2,3, $\cdots$ are the non-circular terms, $a_l(3\leqslant l)$ are the circular terms, and $\{a_n\}$ is a mixed circular sequence of numbers.

Basic theorem 1: Suppose sequence of numbers $\{b_n\}$ is a parasitic sequence of numbers of the sequence of numbers $\{a_n\}$, then, if $\{a_n\}$is a circular sequence of numbers then $\{b_n\}$ is also a circular sequence of numbers.

Proof: From Definition 3 we know that, when $\{b_n\}$ is a parasitic sequence of numbers of $\{a_n\}$, then $\{b_n\}$: $\{b_n=f(a_n)\}$.

Thus, , $b_l=f(a_l)$, $b_{l+nh}=f(a_{l+nh})$.

Suppose a_i is the first circular term of circular sequence of numbers $\{a_n\}$, and h is the circular length. From Definition 4 we know that, for every l $(i\leqslant l)$ there is $a_l=a_{l+nh}$..

If the arguments equal each other then the function values equal each other, from which we know $f(a_l)=f(a_{l+nh})$.

From $b_l=f(a_l)$ and $f(a_l)=f(a_{l+nh})$ we know $b_l=f(a_{l+nh})$.

From $b_l=f(a_{l+nh})$ and $b_{l+nh}=f(a_{l+nh})$ we know $b_l=b_{l+nh}$. From Definition 4 we know that $\{b_n\}$ is a circular sequence of numbers. Q.E.D.

For example, parasitic sequence of numbers $\{b_n=2a_n\}$：16,20, 2,4,6,2,4,6,2,4,6,⋯ of circular sequence of numbers $\{a_n\}$：8,10, 1,2,3,1,2,3,1,2,3,⋯ is a circular sequence of numbers.

Now, let's investigate a sequence of numbers.

Fibonacci sequence of numbers is: $a_1=a_2=1$，$a_{n+2}=a_n+a_{n+1}$，$n=1,2,\ldots$.

That is to say, when $a_1=1$，$a_2=1$ are known, then we have $a_3=a_1+a_2$，$a_4=a_2+a_3$，$\ldots a_{n+2}=a_n+a_{n+1}$. At this time, we can regard a_3 as the image of the original images a_1, a_2 ; regard a_4 as the image of the original images a_2, a_3;…; regard a_{n+2} as the image of the original images a_n, a_{n+1}.

Definition 6: Suppose the first k terms $a_1,\ldots,a_k$ of sequence of numbers A are known. Then if there exists a *k-ary* mapping f such that

$a_{k+1}=f(a_1,\ldots,a_k)$,$a_{k+2}=f(a_2,\ldots,a_{k+1})$,…, $a_{k+n}=f(a_n,\ldots,a_{k+n-1})$，$n=1,2,\ldots$

then we call A a ***k-ary* mapping recurrent sequence of numbers.**

(Note: Please do not confuse the mapping recurrent sequences of numbers with the pseudo-random numbers generator. Although Definition 6 is similar to the definition of the pseudo-random numbers generator, the definition of the former is the formation of the sequences of numbers, while that of the latter is the formation of numbers. Although the numbers generated by the pseudo-random numbers generator can be arranged as a sequence of numbers, it does not do so.)

It is not hard to discover that, equidifference sequences of numbers and equiratio sequences of numbers are unary mapping recurrent sequences of numbers, Fibonacci sequence of numbers is a binary mapping recurrent sequence of numbers.

For example, the equidiffference sequence of numbers with the first term being 1, the common difference being 3, that is: 1,4,7,10,… is unary sequence of numbers A：$a_1=1$，$a_{n+1}=a_n+3$，$n=1,2,\ldots$.

The equiratio sequence of numbers with the first term being 1, the common ratio being 3, that is: 1,3,9,27,… is unary sequence of numbers A：$a_1=1$，$a_{n+1}=3a_n$，$n=1,2,\ldots$

The following sequence of numbers A is a 4-ary mapping recurrent sequence of numbers.

It is known that the first 4 terms of sequence of numbers A being $a_1=2$，$a_2=3$，$a_3=5$，$a_4=7$，and $a_{n+4}=a_n$.

Let $n=1,2,\cdots$, we can obtain 4-ary mapping recurrent sequence of numbers A：2,3,5,7,2,3,5,7,⋯. Obviously, A is a pure circular sequence of numbers.

To sum up, the mapping recurrent sequences of numbers have many types. $Px+q$ sequences of numbers we highlight later are the standard mapping recurrent sequences of numbers. As some basic properties of the $px+q$ sequences of numbers come from the mapping recurrent sequences of numbers, we need to discuss the basic properties of the mapping recurrent sequences of numbers before we discuss the $px+q$ sequences of numbers.

Now, we give a simple representation method of the mapping recurrent sequences of numbers.

K-ary mapping recurrent sequences of numbers recur from the k+1th term. When we give the two conditions: (1)$a_1,\cdots,a_k$；(2)$a_{n+k}=f(a_n,\ldots,a_{n+k-1})$ the sequences of numbers in question are defined, no more conditions are needed.

When defining unary mapping recurrent sequences of numbers, we only need to give $a_1=a$ and $a_{n+1}=f(a_n)$. Thus, we abbreviate the unary mapping recurrent sequences of numbers as $\{a_1=a，a_{n+1}=f(a_n)\}$.

In this paper, the relevant properties of the unary mapping recurrent sequences of numbers are mainly discussed. The words "mapping recurrent sequences of numbers" in the rest of this paper all refer to the unary recurrent sequences of numbers.

Basic theorem 2: Suppose A：$\{a_1=a，a_{n+1}=f(a_n)\}$. If $a_i=a_j$，$1\leqslant j-i=h$. Then，A is a circular sequence of numbers with the circular length being h.

Proof: From $a_{n+1}=f(a_n)$ we know，$a_{i+1}=f(a_i)$,$a_{i+h+1}=f(a_{i+h})$.

From $a_i=a_j$ and $j-i=h$ we know，$a_i=a_{i+h}$.

Because a_i and a_{i+h} are the original images of $f(a_i)$ and $f(a_{i+h})$ respectively. From if the original images equaling each other then the images equaling each other, we know，

$f(a_i)=f(a_{i+h})$.

From $a_{i+1}=f(a_i)$ and $f(a_i)=f(a_{i+h})$ we know，$a_{i+1}=f(a_{i+h})$. From $a_{i+1}=f(a_{i+h})$ and $a_{i+h+1}=f(a_{i+h})$ we know，$a_{i+1}=a_{i+h+1}$.

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 proof, we can prove that, $a_{i+1}=a_{i+nh+1}$. Similarly, we know that for every l ($i\leqslant l$)，$a_l=a_{l+nh}$.

According to Definition 4, A is a circular sequence of numbers with the circular length being h. Q.E.D.

Property 7: I. If h is the minimal circular length of mapping recurrent sequence of numbers A then the h consecutive terms of A pairwise non-equal. Ⅱ. Suppose a_k is the first circular term of mapping recurrent sequence of numbers A and $a_k=a_{k+h}$. If $a_k\neq a_i$ ($k<i<k+h$) then h is the minimal circular length of A.

Proof: Prove I. Suppose in A's h consecutive terms $a_k, a_{k+1},\cdots,a_{k+h-1}$ there is $a_i=a_j$, $k\leqslant i<j<k+h$.

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

From $a_{i+n}=a_i$ and the Basic theorem 2 we know that, n ($<h$) is the circular length of A. This contradicts with the fact that h is the minimal circular length of A. Therefore I holds.

Prove Ⅱ. From $a_k\neq a_i$ ($k<i<k+h$) we know that, in A's h+1 consecutive terms $a_k, a_{k+1},\cdots,a_{k+h}$, only a_{k+h} equals a_k. This means that, when $h'<h$, $a_k\neq a_{k+h'}$. From Definition 4 we know that, h' is not a circular length of A. That is, the circular length of A can not be less than h. Q.E.D.

Now, we use the the two Basic theorems to prove that any fraction is a circular decimal.

First, we discuss why fraction 3/14 is a circular decimal. For this reason, we treat the process from fraction 3/14 to decimal c=0.2142857142857… as two sequences of numbers.

Suppose mapping recurrent sequence of numbers A is, $a_1=3$ (3 is the numerator of fraction 3/14), $a_{n+1}=(10a_n)_{\mathrm{mod}\ 14}$. By calculation we can obtain,

A: 3,2,6,4,12,8,10, 2,6,4,12,8,10,…

The calculation process of sequence of numbers A is as follows. $a_1=3$ i.e., the first term of A is 3.

From $a_1=3$ and $a_2=(10a_1)_{\mathrm{mod}\ 14}$ we obtain $a_2=(30)_{\mathrm{mod}\ 14}=2$ (Note: a_2 is the remainder of 30 divided by 14).

From $a_2=2$ and $a_3=(10a_2)_{\mathrm{mod}\ 14}$ we obtain $a_3=(20)_{\mathrm{mod}\ 14}=6$ (Note: a_3 is the remainder of 20 divided by 14).

……

For every term a_n of sequence of numbers A there is $0\leqslant a_n<14$, and A is an infinite sequence of numbers, therefore, according to the pigeonhole principle there necessarily is $a_i=a_j$, $1\leqslant j-i=h$.

From sequence of numbers A we can see that $a_2=a_8=2$ (i.e., the second term equals the 8^{th} term), 8–2=6. From Basic Theorem 2 we know that, A is a circular sequence of numbers with the minimal circular length being 6.

Suppose A's parasitic sequence of numbers B is: $b_n=〔10a_n/14〕$ (Note: $〔x〕$ is the integer part of x). Thus, there is

B: 2,1,4,2,8,5,7,1,4, 2,8,5,7,…

Now we expound that the process of obtaining every term of sequence of numbers B is the process of obtaining every digit on the right of the decimal point of decimal c.

The obtaining of the first term b_1 of sequence of numbers B is: from $b_1=〔10a_1/14〕$ and $a_1=3$ we obtain $b_1=〔10a_1/14〕=2$ (i.e., the quotient of 10×3=30 divided by 14 is 2), while this is the obtaining of the first digit 2 on the right of decimal point of c. The obtaining of the second term b_2 of sequence of numbers B is: from $b_2=〔10a_2/14〕$ and $a_2=2$ we obtain $b_2=〔10a_2/14〕=1$ (i.e., the quotient of 10×2=20 divided by 14 is 1), while this is the obtaining of the second digit 1 on the right of decimal point of c.… (Please perform the process of 3 divided by 14 yourself)

Because A is a circular sequence of numbers, and B is a parasitic sequence of numbers of A, from Basic Theorem 1 we know that B is a circular sequence of numbers. Also because each digits on the right of the decimal point of decimal c equal to their corresponding terms of B, c is a circular decimal.

We call sequence of numbers A the sequence of numbers of the remainders of fraction 3/14, call sequence of numbers B the sequence of numbers of the quotients of fraction 3/14.

Now, we prove that any fraction is a circular decimal.

Proof: We only prove that decimals transformed from proper fraction q/p(i.e., $q<p$) are circular decimals. Based on the above discussion we can suppose that, the sequence of numbers of remainders A of fraction q/p is: $a_1=q$, $a_{n+1}=(10a_n)_{\mathrm{mod}\ p}$; the sequence of numbers of quotients B is: $b_n=〔10\ a_n/p〕$.

Since every term of the sequence of numbers of remainders A is less than p, there necessarily exist two terms in the sequence of numbers in question equal to each other. From A being a mapping recurrent sequence of numbers and Basic Theorem 2 we know that, A is a circular sequence of numbers. While B is a parasitic sequence of numbers of A. From A being a circular sequence of numbers and Basic Theorem 1 we know that, B is a circular sequence of numbers. Because various digits on the right of the decimal point of the decimal obtained from fraction q/p correspond to various terms of the sequence of numbers of B, the decimal obtained from fraction q/p is a circular decimal. Q.E.D.

The above proof fully shows the importance of the two Basic Theorems.

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

We suggest you to read Note 1 before you read this section.

Now, we define *px+q* sequences of numbers.

Definition 7. Suppose $a, p, q \in N_o$. If the terms of mapping recurrent sequence in numbers $\{a_n\}$ are $a_1= a$, $a_{n+1}=\beta(pa_n+q)$, then we call $\{a_n\}$ a ***px+q* sequence of numbers**, denoted as $\{a_1= a, a_{n+1}=\beta(pa_n+q)\}$.（$\beta(\ )$ see Definition 2）

When p=3，q=1，a_1=11，$\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$：11，17，13，5，1，1，…

The following is the calculation process of the sequence of numbers in question. a_1=11 is the first term of $\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$.

$a_2 =\beta(3a_1+1)=\beta(3\times11+1)=\beta(2\times17)=17$

$a_3 =\beta(3a_2+1)=\beta(3\times17+1)=\beta(2^2\times13)=13$

$a_4 =\beta(3a_3+1)=\beta(3\times13+1)=\beta(2^3\times5)=5$

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

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

……

From the above process we see that the *px+q* sequences of numbers are the special sequences of numbers formed by the recurrent processes with odd number a as the starting point and with p and q as the parameters.

We know that, when p=3，q=1， then the *px+q* sequences of numbers are called the 3*x*+1 sequences of numbers（The famous 3*x*+1 problem can be transformed to the 3*x*+1 sequences of numbers to handle）. When p=5，q=3，then the *px+q* sequences of numbers are called the 5*x*+3 sequences of numbers. This is to say, only both p and q are definite odd numbers can “*px+q* sequences of numbers” be a kind of definite sequences of numbers.

As $\{a_1=11, a_{n+1}= \beta(3a_n+1)\}$ is a mapping recurrent sequence of numbers and it has equal terms $a_5=a_6$=1，from Basic Theorem 2 we know that, the sequence of numbers in question is a circular sequence of numbers with the circular length being 1.

Other examples are: $\{a_1=3, a_{n+1}=\beta(5a_n+1)\}$：3,1,3,… is a circular sequence of numbers with the circular length being 2;

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

From Definition 7 we know that, $\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$ is a 3*x*+1 sequence of numbers with the first term being 11. But for the readers who read this paper for the first time, it is difficult to know directly that “$\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$” refer to “the 3*x*+1 sequence of numbers with the first term being 11”. Here we give a tip. The first term 11 is given by a_1, this is obvious. And change “a_n” in “$3a_n+1$” to “x”, obtaining the “3*x*+1” sequence of numbers we want to know.

From the tip we know that, $\{a_1=3, a_{n+1}=\beta(5a_n+1)\}$ is a 5*x*+1 sequence of numbers with the first term being 3; $\{a_1=1, a_{n+1}=\beta(5a_n+11)\}$ is a 5*x*+11 sequence of numbers with the first term being 1.

Once $\{a_1=3, a_{n+1}=\beta(5a_n+1)\}$ is given, we should know that, sequence of numbers $\{a_1=3, a_{n+1}=\beta(5a_n+1)\}$ is sequence of numbers: 3，1，3，….（This should be a tacit agreement between the authors and the readers.）

Now, we expound what is the leftward extendedness of the *px+q* sequences of numbers.

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

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

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

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

The above are four 5*x*+1 sequences of numbers. It is not hard to see that, sequence of numbers 2 is formed by adding one term “1331” on the left of the first term 13 of sequence of numbers 1; sequence of numbers 3 is formed by adding two terms “4259,1331” on the left of the first term 13 of the sequence of numbers 1; sequence of numbers 4 is formed by adding three terms “54515,4259,1331” on the left of the first term 13 of sequence of numbers 1. For convenience,, we call sequence of numbers 2, sequence of numbers 3 and sequence of numbers 4 as the degree 1 leftward extension sequence of numbers, the degree 2 leftward extension sequence of numbers and the degree 3 leftward extension sequence of numbers respectively.

The main focus of this section is to obtain its degree n leftward extension sequences of numbers from “sequence of numbers 1”.

Since a in Definition 7 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 of the *px+q* sequences of numbers. Thus, we have

Definition 8: Suppose $a, b \in N_o$，$b = \beta(pa+q)$. When a, b are the terms of *px+q* sequences of numbers, then we call a as a degree 1 predecessor of b, call b as a degree 1 successor of a. If a_1 is a degree 1 predecessor of a_2 and a_2 is a degree 1 predecessor of a_3, then we call a_1 as a degree 2 predecessor of a_3. If a_1 is an $n-1$ degree

predecessor of $a_n(n>1)$ and a_n is a degree 1 predecessor of a_{n+1}, then we call a_1 as a **degree *n* predecessor** of a_{n+1}. If a_1 is a **degree *n* predecessor** of a_{n+1}, then a_{n+1} is a degree *n* successor of a_1.

Definition 9: If *a* is a degree *n* predecessor of *b* then $\{a_1= a, a_{n+1}= \beta(pa_n+q)\}$ is a **degree *n* leftward extension sequence of numbers** of $\{b_1=b, b_{n+1}= \beta(pb_n+q)\}$.

Besides, from sequence of numbers 2 we see that, odd number 13 has necessarily predecessor 1331. But, the first term 54515 of sequence of numbers 4 has no predecessor.（We will discuss the reason later）. That is to say, as a term in sequence of numbers 2 (i.e., 5*x*+1 sequence of numbers), odd number 13 has a predecessor, we call it a term implying left terms (we will give its definition later); While 54515 has no predecessor, we call it a term without a left term.

From Definition 7 we know that, in *px+q* sequence of numbers $\{a_n\}$ term $a_{k+1}= \beta(pa_k+q)$, and $\beta(pa_k+q) =(pa_k+q)/ 2^i$, in which *i* is the number of factor 2 in pa_k+q. Thus, $a_k=(2^i a_{k+1}-q)/ p$. Let $s=a_k$, $r=a_{k+1,}$ we obtain

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

We call "$s=(2^i r-q)/p$" the **leftward extension relationship formula** of the *px+q* sequences of numbers. "$s =a_k$, $r=a_{k+1}$", therefore, in the leftward extension relationship formula, "*s*" is the predecessor of "*r*". From 13 to obtain 1331（see sequences of numbers 2,3,4） or from 4259 to obtain 54515（see sequence of numbers 4） can all be accomplished by the leftward extension relationship formula.

In the leftward extension relationship formula *p*，*q*，*r* are known, the only parameter need to be determined is *i*. For example, when finding degree 1 predecessor 1331 of term 13 in sequence of numbers 2, we know that, $p =5$, $q=1$, $r=13$. Let $i=5$ we can obtain the predecessor

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

Now, we discuss how *i* is assigned or what values can *i* be assigned.

Definition 10: Suppose $r\in N_o$, $s=(2^i r-q)/p$. If there exists *i* such that $s\in N_o$, then we call *r* a **term implying left terms** of the *px+q* sequences of numbers; otherwise, we call *r* a **term without a left term** of the *px+q* sequences of numbers.

First, we discuss the relevant properties of the predecessors of the class of *x+q* sequences of numbers （i.e., the class of *px+q* sequences of numbers with $p=1$）.

（Note: Generally, "*px+q* sequence of numbers" in this paper refer to one with both *p* and *q* being definite odd numbers. Because only both *p* and *q* are determined can the "*px+q* sequence of numbers" be a kind of definite sequence of numbers. For example, 3*x*+1 sequence of numbers, 5*x*+3 sequence of numbers is a kind of definite *px+q* sequence of numbers respectively. In order to denote certain class of *px+q* sequences of numbers, we add prefix "class" in front of the sequences of numbers in question. For example, the class of *px*+1 sequences of numbers, the class of *x+q* sequences of numbers, etc.）

The leftward extension relationship formula of the class of *x+q* sequences of numbers is $s=2^i r-q$. Because *r*, $q\in N_o$, there necessarily exists *i* such that $s\in N_o$. This means that, in this class of *x+q* sequences of numbers, any odd number *r* is a term implying left terms. That is, the class of *x+q* sequences of numbers have no term without a left term.

For example, $\{a_1=27, a_{n+1}= \beta(a_n+29)\}$：27,7, 9,19, 3,1,15,11, 5,⋯. In this sequence of numbers, the predecessor of the second term 7 is 27. "27" is obtained by $2^3\times 7-29$（Here, $i=3$，$r=7$，$q=29$，$s=27$）. Besides, when $i=3,4,5,6,7,\cdots$, by $2^i\times 7-29$ we can obtain：27,83,195，⋯. This means that, 27,83,195，⋯ are all the predecessors of 7. That is, $\beta(27+29) = \beta(83+29) = \beta(195+29) =\cdots=7$.

But, it is a pity that any kind of *px+q* sequences of numbers with $p>1$ have a lot of terms without a left term.

For convenience, in the following discussion, we stipulate "$p>1$".

Through the above discussion we know that, if *r* is a term of certain *px+q* （Remember $p>1$）sequences of numbers, but not the first term, then *r* is a term implying left terms of these kinds of *px+q* sequences of numbers. For on the left of *r* there is a term which is the predecessor of *r*. Therefore, only *r* is the first term of certain kind of *px+q* sequence of numbers can *r* be the term without a left term of this kind of *px+q* sequence of numbers.

Please see,

Sequence of numbers 5：7,25,11,39,137,15,⋯ i.e., $\{a_1=7, a_{n+1}= \beta(7a_n+1)\}$.

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

Sequence of numbers 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 of sequence of numbers 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 $2^i\times 7-1$ can not be divided by 7 evenly） Thus, 7 is a term without a left term of the 7*x*+1 sequence of numbers.

Then, let us investigate the first term 5 of the sequence of numbers 6. From $r=5$，$p=7$，$q=21$ we know that, s

$=(2^i\times5-21)/7\notin N_o$. Thus, 5 is a term without a left term of the 7x+21 sequence of numbers.

Then, let us investigate the first term 7 of the sequence of numbers 7. From $r=7$, $p=7$, $q=21$ and $s=(2^i\times7-21)/7=(2^i-3)$ we know that, there exists i such that $s=(2^i-3)\in N_o$. Thus, 7 is a term implying left terms of the 7x+21 sequence of numbers.

Let i =2,3,4,… we obtain 7's predecessors $s=1,5,13,\cdots$.

Besides, when we know that 1,5,13,… are the predecessors of the first term 7 of the sequence of numbers 7, we also know that, the following sequences of numbers

$\{a_1=1, a_{n+1}=\beta(7a_n+21)\}$: 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 degree 1 leftward extension sequences of numbers of sequence of numbers 7.

Theorem 1. Suppose $r\in N_o$, $(p,q)=c$. Then,

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

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

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

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

That is to say, there is no i such that $s\in N_o$. From Definition 10 we know that, r is a term without a left term of the $px+q$ sequences of numbers.

Prove (2). Suppose $p=cp'$, $q=cq'$. From $s=(2^ir-q)/p$ we obtain, $s=(2^ir-cq')/cp'$. From Definition 7 we know that, $p,q\in N_o$. Therefore, $(p,q)=c\in N_o$. $c\nmid r$, therefore, $c\nmid 2^ir$, $c\nmid 2^ir-cq'$, $cp'\nmid 2^ir-cq'$.

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

From (1) of Theorem 1 we know that, the first term 7 in the sequence of numbers 5: $\{a_1=7, a_{n+1}=\beta(7a_n+1)\}$ is a term without a left term of the 7x+1 sequence of numbers, for at this time $(p,q)=(7,1)=c=1$ and $p=7\mid r=7$.

From (2) of Theorem 1 we know that, the first term 5 in the sequence of numbers 6: $\{a_1=5, a_{n+1}=\beta(7a_n+21)\}$ is a term without a left term of the 7x+21 sequence of numbers, for at this time $c=(p,q)=(7,21)=3>1$ and $c=3\nmid r=5$.

Definition 11. If the first term of the $px+q$ sequences of numbers is a term implying left terms, then the sequences of numbers in question are the **leftward extendable sequences of numbers** of the $px+q$ sequences of numbers, otherwise, the sequences of numbers in question are the **non-leftward extendable sequences of numbers** of the $px+q$ sequences of numbers.

From Definition 11 we know that, sequence of numbers 5 is a non-leftward extendable sequence of numbers of the 7x+1 sequences of numbers. Sequence of numbers 6 is a non-leftward extendable sequence of numbers of the 7x+21 sequences of numbers. Sequence of numbers 7 is a leftward extendable sequence of numbers of the 7x+21 sequences of numbers.

Now, we discuss the sufficient and necessary condition for odd number r to be a term implying left terms in the $px+q$ sequences of numbers.

Theorem 2. Suppose $(p, q)=1$, $r\in N_o$. Then, Ⅰ. The sufficient and necessary condition for r being a term implying left terms in the $px+q$ sequences of numbers is $rq^{-1}\equiv2^k(\text{mod } p)$. At the same time, s, the predecessor of r, is given by:

$$s=(2^{n\delta p(2)-k}r-q)/p. \qquad (1)$$

Ⅱ. Suppose $p'=cp$, $q'=cq$, $r'=cr$, $c\in N_o$. Then, r' is a term implying left terms in the $p'x+q'$ sequences of numbers if and only if r is a term implying left terms in the $px+q$ sequences of numbers, and s', the predecessor of r', is $s'=s=(2^{n\delta p(2)-k}r-q)/p$.

Proof: prove Ⅰ. First, we prove the necessary condition, i.e., we prove if $s=(2^ir-q)/p\in N_o$ then $rq^{-1}\equiv2^k(\text{mod } p)$.

From $(2^ir-q)/p\in N_o$ we know that, $2^ir-q\equiv0(\text{mod } p)$, $2^ir\equiv q \text{ (mod } p)$.

From $(q, p)=1$ and $2^ir\equiv q(\text{mod } p)$ we know that, $,2^irq^{-1}\equiv1 \text{ (mod } p)$.

From $2^irq^{-1}\equiv1 \text{ (mod } p)$ and $(2^i, p)=1$ we know that, $rq^{-1}\equiv(2^i)^{-1} \text{ (mod } p)$. ($(2^i)^{-1}$ is the inverse of 2^i modulo p)

From Corollary 8 (See Note 1) we know that, there necessarily exists positive integer k such that $(2^i)^{-1}\equiv2^k \text{ (mod } p)$. From $rq^{-1}\equiv(2^i)^{-1} \text{ (mod } p)$ and $(2^i)^{-1}\equiv2^k \text{ (mod } p)$ we obtain, $rq^{-1}\equiv2^k(\text{mod } p)$.

Then we prove sufficient condition, i.e., we prove that, if $rq^{-1}\equiv2^k(\text{mod } p)$ then $s=(2^ir-q)/p\in N_o$.

Because there necessarily exists positive integer i, k such that $i=n\delta_p(2)-k$, $i+k=n\delta_p(2)$.

Thus, $2^{i+k}=2^i2^k\equiv 2^{n\delta p(2)}\equiv 1 \pmod p$.

From $2^i2^k\equiv 1 \pmod p$ and condition $2^k\equiv rq^{-1} \pmod p$ we know that, $2^i (rq^{-1})\equiv 1 \pmod p$， $2^ir\equiv q \pmod p$.

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

Let $s=(2^ir-q)/p$. Then, $s=(2^ir-q)/p\in N_o$. From Definition 10 and $s=(2^ir-q)/p\in N_o$ we know that, r is a term implying left terms of the $px+q$ sequences of numbers.

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

Prove Ⅱ.

First, we prove that, if r' is a term implying left terms in the $p'x+q'$ sequences of numbers then r is a term implying left terms in the $px+q$ sequences of numbers, and $s'=s$.

From r' is a term implying left terms in the $p'x+q'$ sequences of numbers we know that, the predecessor of r' is $s'=(2^ir'-q')/p'\in N_o$. So,

$$s'=(2^icr-cq)/cp=(2^ir-q)/p=s\in N_o.$$

From Definition 10 we know that, r is a term implying left terms in the $px+q$ sequences of numbers. 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 $px+q$ sequences of numbers then r' a term implying left terms in the $p'x+q'$ sequences of numbers, and $s=s'$. Q.E.D.

We call formula (1) the **predecessor calculation formula** of r--the term implying left terms--in the $px+q$ sequences of numbers.

From Theorem 2 we can obtain:

Corollary 1. r is a term implying left terms in the $px+q$ sequences of numbers if and only if $cr(c\in N_o)$ is a term implying left terms in the $cpx+cq$ sequences of numbers. At the same time, the predecessors of cr--the term implying left terms--in the $cpx+cq$ sequences of numbers are the same as those of r--the term implying left terms--in the $px+q$ sequences of numbers.

Theorem 2 is complex. Now, we show an example to expound the meaning of Ⅱ in Theorem 2.

Now, in the leftward extension relationship formula $s=(2^ir-q)/p$, we let $i=1$， $r=143$， $q=1$， $p=3$. $(143\times 2^1-1)/3=95=s$. Thus, 143 is a term implying left terms in the $3x+1$ sequence of numbers（For $p=3,q=1$）and one of its predecessor is 95.

Besides, $5p=15$， $5q=5$， $5r=715$.

What Ⅱ in Theorem 2 refers to is that, when 143 is a term implying left terms in the $3x+1$ sequence of numbers and one of its predecessor is 95, then 715 is a term implying left terms in the $15x+5$ sequence of numbers and one of its predecessor is also 95. Please see the following $15x+5$ sequence of numbers:

$\{a_1=3, a_{n+1}=\beta(15a_n+5)\}$： 3 ,25,95, 715,…

In this sequence of numbers, 95 is a predecessor of 715.

Now, we show an example to expound the meaning of Ⅰ in Theorem 2.

Example 1. Decide which of 15,17,119 are the terms implying left terms in the $9x+1$ sequence of numbers and the $63x+7$ sequence of numbers, and calculate the predecessors of each term implying left terms.

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

At this time, we know that, $p=9$, $q=1$, $q^{-1}\equiv 1 \pmod 9$， $\delta_9(2)=6$.

When $r=15$, $rq^{-1}\equiv 15\times 1\equiv 6 \pmod 9$. Because there exists no k such that $6\equiv 2^k \pmod 9$， 15 is a term without a left term in the $9x+1$ sequence of numbers.

When $r=17$, $rq^{-1}\equiv 17\times 1\equiv 2^3 \pmod 9$， $k=3$. Therefore, 17 is a term implying left terms in the $9x+1$ sequence of numbers Now, we calculate the predecessors of 17:

At this time, the predecessor calculation formula of 17 is: $s=(2^{6n-3}17-1)/9$. When $n=1,2,3, \cdots$， we obtain that, the predecessors of 17--the term implying left terms--in the $9x+1$ sequence of numbers are 15,967, 61895,….

When $r=119$, $rq^{-1}\equiv 119\times 1\equiv 2^1 \pmod 9$ ， $k=1$. Therefore, 119 is a term implying left terms in the $9x+1$ sequence of numbers. Now, we calculate the predecessors of 119.

At this time, the predecessor calculation formula of 119 is: $s=(2^{6n-1}119-1)/9$. When $n=1,2,3, \cdots$， we obtain that, the predecessors of 119--the term implying left terms--in the $9x+1$ sequence of numbers are 423,27079, 1733063,….

Then, we decide which of 15,17,119 are the terms implying left terms in the $63x+7$ sequence of numbers, and calculate the predecessors of the terms in question.

At this time, $c=(63, 7)=7$, $p=63/7=9$, $q=7/7=1$， $q^{-1}\equiv 1 \pmod 9$， $\delta_9(2)=6$.

Since 15,17 cannot be divided evenly by 7, from (2) in Theorem 1, we know that, 15,17 are terms without a left

term in the 63*x*+7 sequence of numbers.

From $cr=119$ and $c=7$ we know that, $r=17$. From 17 being a term implying left terms in the 9*x*+1 sequence of numbers we know that, 119 is a term implying left terms in the 63*x*+7 sequence of numbers, and the predecessor calculation formula of 119: $s=(2^{6n-3}17-1)/9$ is the same as that of 17.

Thus, the predecessors of 119--a term implying left terms--in the 63*x*+7 sequence of numbers are 15,967, 61895,⋯.

Corollary 1 tells us that, so long as we know all *r*--the terms implying left terms--in the class of *px*+*q* sequences of numbers with (*p*, *q*)=1 then we know all *cr*--the terms implying left terms--in the class of *cpx*+*cq* sequences of numbers. Therefore, in the following discussion we stipulate that "(*p*, *q*)=1".

Because *n* in formula (1) can be *n*=1,2,⋯, *r*--the term implying left terms--in the *px*+*q* sequences of numbers has necessarily infinitely many predecessors *s*. Now, let us discuss the properties of the infinitely many predecessors *s*.

In Example 1 we have found the predecessors of 17--term implying left terms--in the 9*x*+1 sequence of numbers are 15,967, 61895,⋯. We should notice that these infinitely many predecessors form a (infinite) sequence of numbers $\{a_n\}$: 15,967, 61895,⋯.

It is interesting that, $967=2^6\times15+7$, $61895=2^6\times967+7$,⋯ i.e., there is $\{a_n\}$:$\{a_1=15, a_{n+1}=2^6a_n+7\}$. Obviously, sequence of numbers $\{a_n\}$ is a mapping recurrent sequence of numbers.

Please see the following theorem:

Theorem 3. Suppose the terms in the sequence of numbers $\{a_n\}$ obtained by letting $n=1,2,\cdots$ respectively of formula (1) of Theorem 2. That is,

$\{a_n\}$: $a_1=(2^{\delta p(2)-k}r-q)/p$, $a_2=(2^{2\delta p(2)-k}r-q)/p$, ⋯, $a_n=(2^{n\delta p(2)-k}r-q)/p$.

Then, sequence of numbers $\{a_n\}$ is the following mapping recurrent sequence of numbers:

$\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$ (2)

Where, $a=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$.

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

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

These prove that sequence of numbers $\{a_n\}$ is a mapping recurrent sequence of numbers: $\{a_1=(2^{\delta p(2)-k}r-q)/p$, $a_{n+1}=2^{\delta p(2)}a_n+q(2^{\delta p(2)}-1)/p\}$.

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

Theorem 3 shows that, sequence of numbers $a_1=(2^{\delta p(2)-k}r-q)/p$, $a_2=(2^{2\delta p(2)-k}r-q)/p,\cdots,a_n=(2^{n\delta p(2)-k}r-q)/p$ is just sequence of numbers $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$, where $a_1=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$.

The former gives all of the predecessors of *r*--the term implying left terms--in the *px*+*q* sequences of numbers, therefore, the latter also gives those of the *px*+*q* sequences of numbers. We call formula (2) the **sequences of numbers of the predecessors** of of *r*--the term implying left terms-- in the *px*+*q* sequences of numbers.

When using formula (2) to obtain the predecessors of *r*, the term implying left terms, we need to calculate $a_1=(2^{\delta p(2)-k}r-q)/p$ and $b=q(2^{\delta p(2)}-1)/p$.

At this time, *p*,*q*,*r* are known, but we need to calculate $\delta_p(2)$, which involves the calculation of order. And at the same time, we need to find *k* according to $rq^{-1}\equiv2^k \pmod p$, which is just a process of solving exponential congruent equation $2^x\equiv a \pmod p$ (Here $x=k$, $a=rq^{-1}$). The calculation of the predecessors of *r*, the term implying left terms, is a difficult task, But it is solved in Note 1. Now, we give a general method for deciding *r*--the term implying left terms--in the *px*+*q* sequences of numbers and calculating its sequences of numbers of predecessors.

Decision and calculation method for the term implying left terms or the term without a left term:

⑴. Find q^{-1}. If $q=1$ then $q^{-1}=1$; if $1<q$ then we calculate the simplest $\{a_1=q, a_{n+1}=(qa_n)_{\bmod p}\}$, q^{-1}=the second term from the right in the sequence of numbers in question.(See Conclusion 19)

⑵. Find $\delta_p(2)$. We calculate the simplest $\{a_1=2, a_{n+1}=(2a_n)_{\bmod p}\}$. $\delta_p(2)$=the number of terms in the sequence of numbers in question.(See Conclusion 18)

⑶. Find *k*. If $(rq^{-1})_{\bmod p}$ is a term in the simplest $\{a_1=2, a_{n+1}=(2a_n)_{\bmod p}\}$ then we know that *r* is a term implying left terms, and *k* is the position value of $(rq^{-1})_{\bmod p}$ at simplest $\{a_1=2, a_{n+1}=(2a_n)_{\bmod p}\}$ (Note: When $(rq^{-1})_{\bmod p}=1$, $k=0$). If $(rq^{-1})_{\bmod p}$ is not a term in the simplest $\{a_1=2, a_{n+1}=(2a_n)_{\bmod p}\}$ then we know that *r* is a term

without a left term. (See Conclusion 20)

⑷.Find the sequences of numbers of the predecessors. Calculate $a=(2^{\delta p(2)-k}r-q)/p$，$b=q(2^{\delta p(2)}-1)/p$，obtaining: $\{a_1=a, a_{n+1}=2^{\delta p(2)}a_n+b\}$.

An example**.** Find the sequence of numbers of the predecessors of 7--the term implying left terms--in the 31*x*+25 sequence of numbers.

Solution: Because $1<q=25$， according to (1) of the decision and calculation method for the term implying left terms or the term without a left term, we need to find q^{-1}（i.e., 25^{-1}）. Because the second term from the right of Simplest $\{a_1=25, a_{n+1}=(25a_n)_{\mathrm{mod}\ 31}\}$： 25,5,1

is 5, $q^{-1}=25^{-1}=5$.

According to (2) of the decision and calculation method for the term implying left terms or the term without a left term, we find

Simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 31}\}$： 2,4,8,16,1.

The number of terms of the sequence of numbers in question is 5, we obtain, $\delta_{31}(2)=5$.

From $r=7$ and $25^{-1}=5$ we obtain，$(rq^{-1})_{\mathrm{mod}\ p}=(7\times25^{-1})_{\mathrm{mod}\ 31}=4$.

"4" is the second term of simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 31}\}$：2,4,8,16,1， according to (3) of the decision and calculation method for the term implying left terms or the term without a left term we know that, 7 is a term implying left terms, and $k=2$.

Then, according to (4) of the decision and calculation method for the term implying left terms or the term without a left term, we calculate *a* and *b*.

From $r=7$，$p=31$，$q=25$，$\delta_{31}(2)=5$，$k=2$ and $a=(2^{\delta p(2)-k}r-q)/p$，$b=q(2^{\delta p(2)}-1)/p$ we obtain,

$a=(2^{5-2}7-25)/31=1$，$b=25(2^5-1)/31=25$.

Thus, we obtain that, the sequence of numbers of the predecessors of 7--the term implying left terms--in the 31*x*+25 sequence of numbers is:

$\{a_1=1, a_{n+1}=2^5a_n+25\}$： 1,57,1849,….

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

(3) of the decision and calculation method for the term implying left terms or the term without a left term also tells us that, the *r* satisfying $(r\times25^{-1})_{\mathrm{mod}\ 31}$=2,4,8,16,1 are all the terms implying left terms in the 31*x*+25 sequence of numbers. And the *r* satisfying $(r\times1^{-1})_{\mathrm{mod}\ 31}$=2,4,8,16,1 are all the terms implying left terms in the 31*x*+1 sequence of numbers.

From $(r\times25^{-1})_{\mathrm{mod}\ 31}$=2,4,8,16,1 we know that, $r\cdot25^{-1}\equiv2,4,8,16,1\ (\mathrm{mod}\ 31)$，$r\equiv19,7,14,28,25(\mathrm{mod}\ 31)$. That is to say, *r* is a term implying left terms in the 31*x*+25 sequence of numbers if and only if $r\equiv19,7,14,28,25(\mathrm{mod}\ 31)$. And *r* is a term implying left terms in the 31*x*+1 sequence of numbers if and only if $r\equiv2,4,8,16,1\ (\mathrm{mod}\ 31)$.

The authors found out earlier that , the terms without a left term in the 3*x*+1 sequence of numbers can only be the odd numbers divided evenly by 3, the terms without a left term in the 5*x*+1 sequence of numbers can only be the odd numbers divided evenly by 5. Therefore, for a long time the authors have considered that"the number of the terms implying left terms is more than that of the terms without a left term". Yet, the number of terms implying left terms in the 31*x*+25 sequence of numbers and the 31*x*+1 sequence of numbers are far less than that of the terms without a left term. Obviously, for both 31*x*+25 sequence of numbers and 31*x*+1 sequence of numbers, in the successive 31 odd numbers there are only $\delta_{31}(2)=5$ terms implying left terms.

The successive *p* odd numbers are a residual system of *p*, which means that in the successive *p* odd numbers only $\delta_p(2)$ odd numbers are the terms implying left terms in the *px+q* sequences of numbers. Therefore, the ratio of the number of the terms implying left terms in the *px+q* sequences of numbers to that of the total odd numbers is $\delta_p(2)/p$. Any odd number can be the first term of the *px+q* sequences of numbers, and the first term of the leftward extendable sequences of numbers is the term implying left terms, therefore, the ratio of the number of the leftward extendable sequences of numbers to the total number of the kind of *px+q* sequences of numbers is $\delta_p(2)/p$.

For example, in the successive 7 odd numbers 1,3,5,7,9,11,13, only 3(=$\delta_7(2)$ odd numbers 1,9,11 are the terms implying left terms in the 7*x*+1 sequence of numbers（The readers please verify yourselves using the decision and calculation method for the term implying left terms or the term without a left term）. Therefore, in the following 7 sequences of numbers,

1. $\{a_1=1, a_{n+1}=\beta(7a_n+1)\}$： 1,1,1,…； 2. $\{a_1=3, a_{n+1}=\beta(7a_n+1)\}$： 3,11,39,…；
3. $\{a_1=5, a_{n+1}=\beta(7a_n+1)\}$： 5,1,1,…； 4. $\{a_1=7, a_{n+1}=\beta(7a_n+1)\}$： 7,25,11,…；
5. $\{a_1=9, a_{n+1}=\beta(7a_n+1)\}$： 9,1, 1,…； 6. $\{a_1=11, a_{n+1}=\beta(7a_n+1)\}$： 11,39, 137,…；
7. $\{a_1=13, a_{n+1}=\beta(7a_n+1)\}$： 13,23, 81,…

only the first, fifth and sixth sequences of numbers (Their first terms are 1, 9, 11 respectively) are the leftward extendable sequences of numbers of the 7*x*+1 sequences of numbers.

However, whether the ratio of the terms implying left terms to all the terms in the sequences of numbers of the predecessors of *r*--the term implying left terms--in the *px+q* sequences of numbers is also $\delta_p(2)/p$? The answer is No.

Please see the sequence of numbers of the predecessors of 65--the term implying left terms--in the 21*x*+1 sequence of numbers: $\{a_1=99,\ a_{n+1}=2^6a_n+3\}$: 99,6339,405699,⋯（From $\beta(99\times21+1)=\beta(6339\times21+1)=\beta(405699\times21+1)=\cdots=65$ we know that, 99,6339,405699,⋯ are the predecessors of 65）. The readers can use Theorem 1 or the decision and calculation method for the term implying left terms or the term without a left term to prove that 99,6339,405699,⋯ are all the terms implying left terms in the 21*x*+1 sequence of numbers.

Subsequently, we discuss the ratio of the terms implying left terms to all the terms in the sequences of numbers of the predecessors of *r*--the term implying left terms--in the *px+q* sequences of numbers. To this end, we need to investigate the residue modulo *p* of the various terms in the sequences of numbers of the predecessors of *r*--the term implying left terms--in the *px+q* sequences of numbers.

Theorem 4. Suppose $\{a_n\}$: $\{a_1=a,\ a_{n+1}=2^{\delta p(2)}a_n+b\}$, $\{b_n\}$: $\{b_n=(a_n)_{\bmod p}\}$. Then,

$\{b_n\}$: $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$.

Proof: From $a_1=a$ and $b_1=(a_1)_{\bmod p}$ we obtain $b_1=(a)_{\bmod p}$. From $b_{n+1}=(a_{n+1})_{\bmod p}$ and $a_{n+1}=2^{\delta p(2)}a_n+b$ we know that,

$b_{n+1}=(2^{\delta p(2)}a_n+b)_{\bmod p}=((2^{\delta p(2)})_{\bmod p}(a_n)_{\bmod p}+b)_{\bmod p}$. （See Property 2）

From $(2^{\delta p(2)})_{\bmod p}=1$ we know that, $b_{n+1}=((a_n)_{\bmod p}+b)_{\bmod p}$.

From the supposition $b_n=(a_n)_{\bmod p}$ we know that,$b_{n+1}=(b_n+b)_{\bmod p}$. Q.E.D.

From Definition 1 we know that, $b_n=(a_n)_{\bmod p}$ is just $b_n\equiv a_n \pmod p$. From Theorem 4 we obtain:

Corollary 2. If $\{a_n\}$: $\{a_1=a,\ a_{n+1}=2^{\delta p(2)}a_n+b\}$ and $\{b_n\}$: $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$, then $a_n\equiv b_n \pmod p$, $n=1,2,\cdots$.

Because $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$ is a mapping recurrent sequence of numbers and all of its terms are less than p, by pigeonhole principle and Basic Theorem 2 we know that the sequence of numbers in question is a circular sequence of numbers.

It is not hard to see that, when $a=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$, $\{a_n\}$: $\{a_1=a,\ a_{n+1}=2^{\delta p(2)}a_n+b\}$ in Theorem 4 is the sequence of numbers of the predecessors of *r*--the term implying left terms--in the *px+q* sequences of numbers given by formula (2). Performing the minimal non-negative residue modulo *p* to each term of it we obtain $\{b_n\}$: $\{b_n=(a_n)_{\bmod p}\}$ i.e., $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$. That is to say, the minimal non-negative residue modulo *p* of the various terms in the sequence of numbers of the predecessors of *r*--the term implying left terms--in the *px+q* sequences of numbers is given by $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$.

For this reason, we call $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$ with $a=(2^{\delta p(2)-k}r-q)/p$, $b=q(2^{\delta p(2)}-1)/p$ as a **sequence of numbers of the residue of the predecessors** of *r*--the term implying left terms--in the *px+q* sequences of numbers.

It worth mentioning that, *a*, *b* in $\{a_1=a,\ a_{n+1}=2^{\delta p(2)}a_n+b\}$ is just *a*, *b* in $\{b_1=(a)_{\bmod p},\ b_{n+1}=((b_n+b)_{\bmod p}\}$. Therefore, if we have the former then we can obtain the latter.

For example, the sequence of numbers of the predecessors of 17--the term implying left terms--in the 9*x*+1 sequence of numbers is:

$\{a_1=15,\ a_{n+1}=2^6a_n+7\}$: 15,967, 61895,⋯.

Thus, the sequence of numbers of the residue of the predecessors of 17--the term implying left terms--in the 9*x*+1 sequence of numbers is:

$\{b_1=(15)_{\bmod 9},\ b_{n+1}=((b_n+7)_{\bmod 9}\}$: 6,4,2,⋯.

Obviously, $15\equiv6 \pmod 9$, $967\equiv4 \pmod 9$, $61895\equiv2 \pmod 9$, ….

Now, we investigate the sufficient condition for the predecessors of the terms implying left terms to be the terms implying left terms. This is a complicated problem, it need to prove the following lemmas first.

In proving the lemmas we will use the following properties of the non-congruent equations $a\not\equiv b \pmod m$:

When $a\not\equiv b \pmod m$, Ⅰ.$a+c\not\equiv b+c \pmod m$; Ⅱ.If $(c, m)=1$ then $ac\not\equiv bc \pmod m$.

（The two properties above can be proved using proof by contradiction）

Lemma 1. Suppose $\{a_n\}$: $\{a_1=a<m,\ a_{n+1}=(a_n+b)_{\bmod m}\}$. Then, Ⅰ. $a_n=(a+(n-1)b)_{\bmod m}$; Ⅱ. $\{a_n\}$ is a pure circular sequence of numbers with the minimal circular length being $m/(b, m)$; Ⅲ. If $m_1 \mid m$ and $(m_1, b)=1$, then, every successive m_1 terms in $\{a_n\}$ are a residual system of m_1. When $(b, m)=1$, then every successive *m* terms in $\{a_n\}$ are a residual system of *m*.

Proof: Similar to the proof of Theorem 9 (in Note 1) we can prove that Ⅰ holds.

Prove Ⅱ. Suppose $(b, m)=c$, $b'=b/c$, $m'=m/c$. Then, $(b', m')=1$, $m'=m/(b, m)$, $b=b'c$, $m=m'c$.

From Ⅰ we know that, $a_{m'+1}=(a+(m'+1-1)b)_{\bmod m}$, i.e.,

$a_{m'+1}=(a+m'b)_{\bmod m}=(a+m'b'c)_{\bmod m}=(a+m'cb')_{\bmod m}=(a+mb')_{\bmod m}=a=a_1$.

From Basic Theorem 2 we know that, $\{a_n\}$ is a pure circular sequence of numbers with the circular length being $m'=m/(b, m)$.

Then, we prove that m' is the minimal circular length of $\{a_n\}$. Since $\{a_n\}$ is a pure circular sequence of numbers, a_1 is a circular term. Thus, we prove that none of the terms $a_2, a_3,\cdots, a_{m'-1}$ in $\{a_n\}$ equals a_1.

When $1<k\leqslant m'$, $m'\nmid(k-1)$.

From $(b', m')=1$ we know that, $m'\nmid(k-1)b'$, $m'c\nmid(k-1)b'c$, $m\nmid(k-1)b$.

Thus, $(k-1)b\not\equiv 0 \pmod m$, $a+(k-1)b\not\equiv a \pmod m$.

From Ⅰ we know that ,$a_k=(a+(k-1)b)_{\bmod m}$. Thus, $a_k\not\equiv a \pmod m$. Then, $a_k\neq a$, i.e., $a_k\neq a_1$.

This proves $a_2, a_3,\cdots, a_{m'-1}\neq a_1$. From Ⅱ of Property 7 we know that, m' is the minimal circular length of $\{a_n\}$.

Prove Ⅲ.

When $m_1=1$, Ⅲ holds. Now, we discuss the case of $m_1>1$.

Suppose $1\leqslant i-k<m_1$. From $m_1>1$ we obtain, $i-k\not\equiv 0 \pmod{m_1}$, $i\not\equiv k \pmod{m_1}$, $i-1\not\equiv k-1 \pmod{m_1}$.

From $(b, m_1)=1$ we know that, $(i-1)b\not\equiv(k-1)b \pmod{m_1}$,

$a+(i-1)b\not\equiv a+(k-1)b \pmod{m_1}$. (3)

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

$a+(i-1)b=k_1m+(a+(i-1)b)_{\bmod m}$ and $a+(k-1)b=k_2m+(a+(k-1)b)_{\bmod m}$, i.e.,

$a+(i-1)b=k_1m+a_i$ and $a+(k-1)b=k_2m+a_k$. (4)

From (3) and (4) we obtain that, $k_1m+a_i\not\equiv k_2m+a_k \pmod{m_1}$.

From $m_1 \mid m$ we know that, $k_1m\equiv k_2m\equiv 0 \pmod{m_1}$. Therefore, $a_i\not\equiv a_k \pmod{m_1}$.

When $1\leqslant i-k<m_1$, $a_i\not\equiv a_k \pmod{m_1}$, this means that the successive m_1 terms of $\{a_n\}$ pairwise non-congruent modulo m_1. Therefore, every successive m_1 terms of $\{a_n\}$ are a residual system of m_1. Especially, when $(b, m)=1$, Let $m_1=m$, at this time, there is $m_1 \mid m$ and $(m_1, b)=1$.Therefore, at this time, every successive $m_1=m$ terms of $\{a_n\}$ are a residual system of $m_1=m$.

Q.E.D.

Let us investigate the following 3 sequences of numbers:

Sequence of numbers 8: $\{a_1=1, a_{n+1}=(a_n+3)_{\bmod 12}\}$ 1,4,7,10,1,⋯

Sequence of numbers 9: $\{a_1=1, a_{n+1}=(a_n+5)_{\bmod 12}\}$ 1,6,11,4,9,2,7,0,5,10,3,8,1,⋯.

Sequence of numbers 10: $\{a_1=1, a_{n+1}=(a_n+3)_{\bmod 36}\}$ 1,4,7,10,13,16,19,22,25,28,31,34,1,⋯

As to sequence of numbers 8, at this time, $b=3$, $m=12$, $(m, b)=(12, 3)=3$, $m/(b, m)=12/3=4$. The minimal circular length of the sequence of numbers 1,4,7,10,1,⋯ is just 4. This verifies Ⅱ in Lemma 1.

Besides, Let $m_1=4$. We have $4 \mid 12$ (i.e., "$m_1 \mid m$") and $(m_1, b)=(4,3)=1$. It is not hard to see that, the successive 4 terms of the sequence of numbers 1,4,7,10,1,⋯ is a residual system of 4. This verifies Ⅲ of Lemma 1.

As to sequence of numbers 9, we have $(m, b)=(12,5)=1$. It is not hard to see that, the minimal circular length of the sequence of numbers 1,6,11,4,9,2,7,0,5,10,3,8,1, ⋯ is 12. Also because $2,3,4,6,12 \mid 12$ and $(2,5)=(3,5)=(4,5)=(6,5)=(12,5)=1$. Every 2, 3, 4, 6, 12 successive terms of the sequence of numbers 9 are the residual systems of 2, 3, 4, 6, 12.

As to sequence of numbers 10, we have $(m, b)=(36,3)=3$, $m/(b, m)=36/3=12$. It is not hard to see that, the minimal circular length of the sequence of numbers 10 is 12. Also because $2, 4 \mid 36$ and $(2,3)=(4,3)=1$. Every successive 2 or 4 terms of the sequence of numbers 10 are the residual systems of 2 or 4.

Please note that, although $6,9 \mid 36$, the successive 6 or 9 terms of the sequence of numbers 10 are not the residual systems of 6 or 9. This will be investigated later in Lemma 3.

First, let us prove Lemma 2.

Lemma 2. If every successive m terms of the sequence of numbers $\{b_n\}$ are a residual system of m then $b_i\equiv b_{nm+i} \pmod m$, $0\leqslant n$.

Proof: First, we prove that in the $m+1$ terms $b_k, b_{k+1},\cdots, b_{k+m-1}, b_{k+m}$ in $\{b_n\}$, we have $b_{k+m}\equiv b_k \pmod m$.

We use proof by contradiction. Suppose $b_k\not\equiv b_{k+m} \pmod m$.

Because $b_k, b_{k+1},\cdots, b_{k+m-1}$ are the successive m terms of $\{b_n\}$, $b_k, b_{k+1},\cdots, b_{k+m-1}$ is a residual system of m. Thus, b_{k+m} is necessarily congruent modulo m with one of $b_k, b_{k+1},\cdots, b_{k+m-1}$.

When $b_{k+m}\not\equiv b_k \pmod m$, b_{k+m} is necessarily congruent modulo m with one of $b_{k+1},\cdots, b_{k+m-1}$.

Thus, the successive m terms $b_{k+1},\cdots, b_{k+m-1}, b_{k+m}$ are not pairwise non-congruent modulo m, which contradicts with the fact that every successive m terms in $\{b_n\}$ are a residual system of m. Therefore the supposition does not hold.

Therefore, $b_{k+m}\equiv b_k \pmod m$.
The rest can be inferred by analogy. Thus, Lemma 2 holds. Q.E.D.
Lemma 3. Every successive m_1 terms in $\{a_n\}$: $\{a_1=a, a_{n+1}=(a_n+b)_{\mathrm{mod}m}\}$ are a residual system of m_1 if and only if $m_1 \mid m$ and $(m_1, b)=1$.
Proof: In Lemma 1 we have proved that, $m_1 \mid m$ and $(m_1, b)=1$ is a sufficient condition of every successive m_1 terms in $\{a_n\}$ being a residual system of m_1. Here we only prove that, $m_1 \mid m$ and $(m_1, b)=1$ is a necessary condition of every successive m_1 terms in $\{a_n\}$ being a residual system of m_1. For this reason, we need to prove the following two cases.
Case 1. If $m_1 \mid m$ and $(m_1, b)>1$ then it does not hold that every successive m_1 terms in $\{a_n\}$ is a residual system of m_1.
Case 2. If $m_1 \nmid m$ then it does not hold that every successive m_1 terms in $\{a_n\}$ is a residual system of m_1.
Prove Case 1.
Suppose $(m_1, b)=k>1$, $b'=b/k$, $m_2= m_1/k$. Thus, $b =b'k$, $m_1=k\,m_2$, $k\,m_2 \mid m$.
From Ⅰ in Lemma 1 we know that, the first $m_1=km_2$ terms of $\{a_n\}$ are:

a, $(a+b'k)_{\mathrm{mod}m}$, …, $(a+(m_2-1)b'k)_{\mathrm{mod}\,m}$,
$(a+(2\,m_2-m_2)b'k)_{\mathrm{mod}\,m}$, $(a+(2m_2-m_2+1)b'k)_{\mathrm{mod}\,m}$, …, $(a+(2m_2-1)b'k)_{\mathrm{mod}\,m}$,
……
$(a+(k\,m_2-m_2)b'k)_{\mathrm{mod}\,m}$, $(a+(km_2-m_2+1)b'k)_{\mathrm{mod}\,m}$, …, $(a+(km_2-1)b'k)_{\mathrm{mod}\,m}$.

The above km_2 terms form a matrix with k rows and m_2 columns. Now, we investigate the second column (The other columns can be treated similarly).
We prove $(a+b'k)_{\mathrm{mod}\,m}\equiv(a+(nm_2-m_2+1)b'k)_{\mathrm{mod}\,m} \pmod{km_2}$, $1\leqslant n\leqslant k$ (i.e., each term in the second column are congruent modulo $m_1=km_2$).
From $km_2 \mid m$ and Property 4 we know that,
$((a+(nm_2-m_2+1)b'k)_{\mathrm{mod}\,m})_{\mathrm{mod}\,km_2}=(a+(nm_2-m_2+1)b'k)_{\mathrm{mod}\,km_2}$
$=(a+(n-1)\,m_2b'k+b'k)_{\mathrm{mod}\,km_2}$
$=(a+(n-1)k\,m_2b'+b'k)_{\mathrm{mod}\,km_2}$
$=(a+b'k)_{\mathrm{mod}\,km_2}$.
From Property 1 we know that, $(a+(nm_2-m_2+1)b'k)_{\mathrm{mod}\,m}\equiv a+b'k \pmod{km_2}$.
Likewise, $(a+b'k)_{\mathrm{mod}\,m}\equiv a+b'k \pmod{km_2}$.
Therefore, $(a+(nm_2-m_2+1)b'k)_{\mathrm{mod}\,m}\equiv(a+b'k)_{\mathrm{mod}\,m} \pmod{km_2}$.
This proves that in $\{a_n\}$ there are successive $m_1=km_2$ terms which are not pairwise non-congruent modulo m_1. Or it does not hold that every successive m_1 terms in $\{a_n\}$ are a residual system modulo m_1.
Prove Case 2. $m_1 \nmid m$, therefore, either $m_1<m$, or $m_1>m$.
First, we prove the case of $m_1 \nmid m$ and $m_1<m$.
From $m_1<m$ and $m_1 \nmid m$ (This means $m_1>1$) we know that, there necessarily exists $1<k$ such that $1\leqslant km_1-m<m_1$.
Let $km_1-m=c$. Thus, $1\leqslant c<m_1$ and $m=km_1-c$, $m+1=(k-1)m_1+m_1-c+1$.
From $c<m_1$ we know that, $1\leqslant m_1-c<m_1$, $2\leqslant m_1-c+1\leqslant m_1$.
Suppose every successive m_1 terms in $\{a_n\}$ are a residual system of m_1. Then, the first m_1 terms of $\{a_n\}$ is a residual system of m_1. Thus we know that, $a_t\not\equiv a_1 \pmod{m_1}$, $2\leqslant t\leqslant m_1$.
Because $2\leqslant m_1-c+1\leqslant m_1$, let $t = m_1-c+1$. Thus, $a_{m_1-c+1}\not\equiv a_1 \pmod{m_1}$.
Besides, from the supposition and Lemma 2 we know that, $a_{m_1-c+1}\equiv a_{(k-1)m_1+m_1-c+1} \pmod{m_1}$.
Thus, $a_{(k-1)m_1+m_1-c+1}\not\equiv a_1 \pmod{m_1}$. From $m+1=(k-1)m_1+m_1-c+1$ we know that,
$a_{m+1}\not\equiv a_1 \pmod{m_1}$.
Besides, from Ⅱ in Lemma 1 we know that, $m/(b, m)$ is the minimal circular length of $\{a_n\}$. Then, m is a circular length of $\{a_n\}$. Thus, $a_{m+1}=a_1$, $a_{m+1}\equiv a_1 \pmod{m_1}$.
Obviously, $a_{m+1}\equiv a_1 \pmod{m_1}$ and $a_{m+1}\not\equiv a_1 \pmod{m_1}$ are contradictory to each other, by which we know that, it does not hold that every successive m_1 terms in $\{a_n\}$ is a residual system of m_1.
Likewise we can prove the case of $m_1 \nmid m$ and $m_1>m$, where it does not hold that every successive m_1 terms in $\{a_n\}$ is a residual system of m_1. Q.E.D.
(It worth mentioning that $\{a_1=a, a_{n+1}=(a_n+b)_{\mathrm{mod}m}\}$ in Lemma 3 should be called a **equidifference residual**

sequence of numbers, which is a sequence of numbers similar to the equiratio residual sequence of numbers)
Now, we prove Theorem 5.

Theorem 5. Suppose $(p, (2^{\delta p(2)}-1)/p)=1$. Then, the successive p terms in the sequence of numbers of the predecessors of r--the term implying left terms--in the $px+q$ sequences of numbers are a residual system of p.

Proof: From Theorem 3 we know that, the sequence of numbers of the predecessors of r--the term implying left terms--in the $px+q$ sequences of numbers is

$\{a_n\}$：$\{a_1= a, a_{n+1}=2^{\delta p(2)}a_n+b\}$，where $a=(2^{\delta p(2)-k}r-q)/p$，$b=q(2^{\delta p(2)}-1)/p$.

According to Corollary 2, we prove that, the successive p terms in $\{b_n\}$：$\{b_1=(a)_{\mod p}, b_{n+1}=((b_n+b)_{\mod p}\}$ is a residual system of p.

From $(p，q)=1$ and $(p, (2^{\delta p(2)}-1)/p)=1$ we know that, $(p, q(2^{\delta p(2)}-1)/p)=1$. From $b=q(2^{\delta p(2)}-1)/p)$ we know that, $(p, b)=1$. From Lemma 3 we know that, the successive p terms in $\{b_n\}$ is a residual system of p. Q.E.D.

The situation of the sequences of numbers of the predecessors of the terms implying left terms in the $px+q$ sequences of numbers with $(p, (2^{\delta p(2)}-1)/p)>1$ is complicated, the authors do not investigate further. The interested readers can investigate themselves.

We stipulate that p in what follows satisfy $(p, (2^{\delta p(2)}-1)/p)=1$.

Theorem 5 tells us that, the successive p terms in the sequences of numbers of the predecessors of r--the term implying left terms--in the $px+q$ sequences of numbers is a residual system of p. From (3) of the decision and calculation method for the term implying left terms or the term without a left term we know that, in the successive p terms in the sequences of numbers of the predecessors of r--the term implying left terms--in the $px+q$ sequences of numbers there are $\delta_p(2)$ terms implying left terms. That is,

Corollary 3. The ratio of the terms implying left terms to all terms in the sequences of numbers of the predecessors of r--the term implying left terms--in the $px+q$ sequences of numbers is $\delta_p(2)/p$.

Various terms in the sequences of numbers of the predecessors of r--the term implying left terms--are degree 1 predecessors of r. According to Corollary 3, the ratio of the terms implying left terms to all the terms of the degree 1 predecessors of r is $\delta_p(2)/p$. The degree 1 predecessors of r also have degree 1 predecessors (They are degree 2 predecessors of r). And the ratio of the terms implying left terms to all terms of the degree 2 predecessors of r is also $\delta_p(2)/p$. And the degree 2 predecessors of r also have degree 1 predecessors (They are degree 3 predecessors of r). Thus,

Corollary 4. If sequence of numbers A：$\{a_1= a, a_{n+1}=\beta(pa_n+q)\}$ is a leftward extendable sequence of numbers, then A has necessarily n degree（n=1,2,…） leftward extension sequences of numbers B. And B and A are the same kind of $px+q$ sequences of numbers.

Definition 12. If B：$\{b_1= b, b_{n+1}=\beta(pb_n+q)\}$ is an n degree ($n\geqslant 1$) leftward extension sequence of numbers of A：$\{a_1= a, a_{n+1}=\beta(pa_n+q)\}$, then we call A as an n degree ($n\geqslant 1$) **sub-sequence of numbers** of B.

Fact 1. Suppose A is a sub-sequence of numbers of B. Then, A is a circular sequence of numbers if and only if B is a circular sequence of numbers. And, a is a circular term in A if and only if a is a circular term in B.

For example, sequence of numbers $\{a_1=33, a_{n+1}=\beta(5a_n+1)\}$：33,83,13,… is a sub-sequence of numbers of $\{a_1=1331, a_{n+1}=\beta(5a_n+1)\}$：1331,13,33,83,13,…. The former is a circular sequence of numbers, the latter is also a circular sequence of numbers.“33,83,13” are the circular terms in the former, they are also the circular terms in the latter.

Theorem 6. Suppose r is a term implying left terms in the $px+q$ sequences of numbers, its 1,…,n degree predecessors are：r_1,…, r_n respectively. If r is a non-circular term in the $px+q$ sequence of numbers R：r_n,…, r_1, r,…, then $r_i\neq r_k$ ($1\leqslant i\leqslant n$, $1\leqslant k\leqslant n$, $i\neq k$), i.e., r_n,…, r_1 are pairwise non-equal.

Proof: Suppose $r_i=r_k$. Since $px+q$ sequence of numbers R is a mapping recurrent sequence of numbers, by Basic Theorem 2 we know that R is a circular sequence of numbers. Thus, r_i, r_k are the circular terms in R. Besides, r_i, r_k in R are the predecessors of r, Thus, from Definition 4 we know that, r is a circular term in R. This contradicts with the condition that r is a non-circular term in $px+q$ sequence of numbers R：r_n,…, r_1, r,…. Thus, $r_i\neq r_k$. Q.E.D.

For example, 5 is a non-circular term in sequence of numbers $\{a_1=7, a_{n+1}=\beta(3a_n+1)\}$ 7,11,17,13,5,1,1,…, its 4 predecessors “7,11,17,13” are pairwise non-equal.

4 Infinite trees and complete trees

Definition 13. Suppose r is a term implying left terms in the $px+q$ sequences of numbers. Step 1. We use lines to connect r with every degree 1 predecessor of r. Step 2. We use lines to connect every predecessor r' which is the term implying left terms with every degree 1 predecessor of r'. We repeat Step 2, the figure we obtain at last is called a **（*r*）*px+q* infinite tree**, (See Fig. 1). And we call $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ the **root sequence of numbers** of the（*r*）$px+q$ infinite tree.

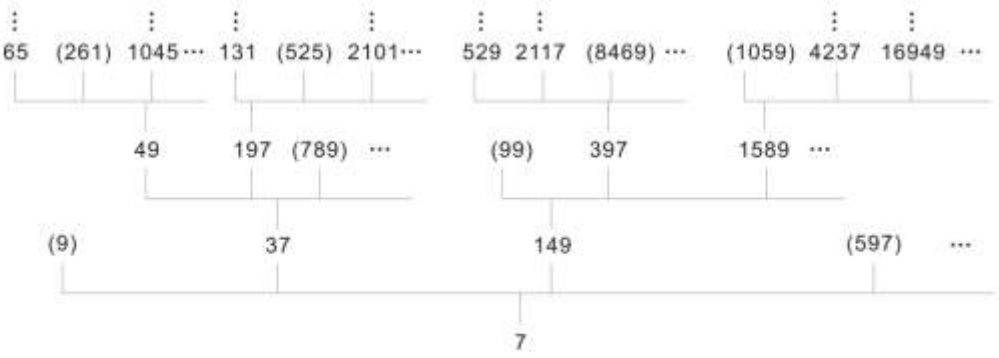


Fig. 1. [7] 3x+1 infinite tree

Fig. 1 gives the（7）3*x*+1 infinite tree, which is formed as follows: Step 1: Connect 7 with each of its degree 1 predecessors, i.e., 9,37,149,597,⋯. In 7's degree 1 predecessors, 37,149,⋯ are the terms implying left terms of the 3*x*+1 sequence of numbers. Step 2: Connect 37 with each of its degree 1 predecessors, i.e., 49,197,789,⋯, connect 149 with each of its degree 1 predecessors, i.e., 99,397,1589,⋯. Analogously, we obtain Fig. 1.

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

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

From the formation of Fig. 1 we know that, the level above 7 (the first level) contains all of the degree 1 predecessors of 7, the second level contains all of the degree 2 predecessors of 7,，⋯. Fig. 1 has infinitely many levels, and each level has infinitely many odd numbers.

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

Definition 14. Suppose $a(a\neq r)$ is a number in a（*r*）*px+q* infinite tree. We call $\{a_1=a, a_{n+1}=\beta(pa_n+q)\}$ as a **sequence of numbers of the（*r*）*px+q* infinite tree**, call the set composed of the sequences of numbers of the（*r*）*px+q* infinite tree as a **set of the sequences of numbers of the（*r*）*px+q* infinite tree**.

In Definition 14, *a* is a predecessor of *r*, therefore we have:

Conclusion 1. Any sequence of numbers of the（*r*）*px+q* infinite tree is a leftward extension sequence of numbers of the root sequence of numbers $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$.

Example 2. 65 is a number on the third level of Fig. 1. 65 connects 49 downward, 49 connects 37 downward, 37 connects 7 downward. The sequence of numbers obtained: 65,49,37, 7,⋯ is $\{a_1=65, a_{n+1}=\beta(3a_n+1)\}$. Obviously, $\{a_1=65, a_{n+1}=\beta(3a_n+1)\}$ is a degree 3 leftward extension sequence of numbers of the root sequence of numbers $\{a_1=7, a_{n+1}=\beta(3a_n+1)\}$：7,11,17,13,⋯.

From Fig. 1 it is not hard to see that $\{a_1=7, a_{n+1}=\beta(3a_n+1)$ has infinitely many degree 1 leftward extension sequences of numbers, infinitely many degree 2 leftward extension sequences of numbers, ⋯, infinitely many degree *n* leftward extension sequences of numbers.

According to Definition 13, when *r* is a term implying left terms in the *px+q* sequence of numbers, $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ has infinitely many degree *n* leftward extension sequences of numbers. Thus, we have

Definition 15. Suppose *A*：a_n,⋯, a_1, *r*,⋯ is the degree *n* leftward extension sequence of numbers of the root sequence of numbers $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$. We call *A* with *n* approaching infinity as a **（*r*）*px+q* extremely leftward extension sequence of numbers**.

（*r*）*px+q* extremely leftward extension sequence of numbers *A* is a sequence of numbers of the（*r*）*px+q* infinite tree, therefore, from Definition 14 we know that,

Conclusion 2. In the set of the sequences of numbers of the（*r*）*px+q* infinite tree there necessarily exist a（*r*）*px+q* extremely leftward extension sequence of numbers.

It should be pointed out that in Definition 15, "*n* approaching infinity" means that *A* is a sequence of numbers extending leftward constantly. The a_n satisfying this requirement can only be the terms implying left terms of the *px+q* sequences of numbers.

Conclusion 3. The first term of the extremely leftward extension sequence of numbers is a term implying left terms of the *px+q* sequences of numbers.

Besides, Suppose *r'* and *r* are the terms in the *px+q* sequence of numbers, when *r'* is a successor of *r*, *r'* is

necessarily a term implying left terms of the $px+q$ sequence of numbers. From Definition 13 we know that, there necessarily exists a $px+q$ infinite tree with r' as its root and r is in the infinite tree in question.

For example, 7 and 9 are the terms of the $3x+1$ sequence of numbers, and 7 is the successor of 9. Thus we see that, 9 is in （7）$3x+1$ infinite tree.

Conclusion 4. Any odd number r is necessarily in certain $px+q$ infinite tree.

Conclusion 5. If there is a circular sequence of numbers in the set of sequences of numbers of the （r）$px+q$ infinite tree, then all of the sequences of numbers in the set in question are circular sequences of numbers.

Proof: Suppose B is a circular sequence of numbers in the set of sequences of numbers of the （r）$px+q$ infinite tree.

From Definition 14 and Conclusion 1 we know that, B is a leftward extension sequence of numbers of $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$.

From Definition 12 we know that, $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is a sub-sequence of numbers of B.

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

Since $\{a_1=r, a_{n+1}=\beta(pa_n+q)\}$ is the sub-sequence of numbers of all of the sequences of numbers in the set of sequences of numbers of the （r）$px+q$ infinite tree, from Fact 1 again we know that, all of the sequences of numbers in the set of sequences of numbers of the （r）$px+q$ infinite tree are circular sequences of numbers. Q.E.D.

Conclusion 5 reveals an important fact that, if there exists a circular sequence of numbers in the $px+q$ sequences of numbers then there exist infinitely many circular sequences of numbers in the kind of $px+q$ sequences of numbers.

Based on Conclusion 5 we have,

Conclusion 6. If there exists a circular sequence of numbers in any set of sequences of numbers of the （r）$px+q$ infinite tree, then the kind of $px+q$ sequences of numbers are circular sequences of numbers (i.e., all sequences of numbers in the kind of $px+q$ sequences of numbers are circular sequences of numbers).

Conclusion 7. Suppose A：$a_m,\cdots, a_1, r,\cdots$ is a （r）$px+q$ extremely leftward extension sequence of numbers. If r is a non-circular term of A, then a_m is infinitely great (and it is an odd number).

Proof: Because r is a non-circular term of A, From Theorem 6 we know that, $a_m,\cdots, a_1$ are pairwise non-equal (odd numbers). From m approaches infinity we know that, a_m is infinitely great (and it is an odd number). Q.E.D.

Definition 16. Suppose A：$a_m,\cdots, a_1, r, b_1,\cdots, b_n$ is a sequence of numbers of the （r）$px+q$ infinite tree. We call A with both m and n approaching infinity as a **（r）$px+q$ double extension sequence of numbers.**

Because any $px+q$ sequence of numbers can extend rightward infinitely, "n approaching infinity" in Definition 16 is a tacit consent. That is to say, the sequences of numbers defined by Definitions 15 and 16 are the same. And the （r）$px+q$ extremely leftward extension sequence of numbers is just the （r）$px+q$ double extension sequence of numbers.

From Conclusion 2 we know,

Conclusion 8. In any set of the sequences of numbers of the （r）$px+q$ infinite tree there necessarily exists a （r）$px+q$ double extension sequence of numbers.

With Conclusion 8, let us discuss two valuable reference results. For this reason, we make such supposition first,

Supposition 1. Suppose a and b are two infinitely great terms implying left terms in the $px+q$ sequences of numbers. Then $a=b$.

Reference result 1. Any （r）$px+q$ double extension sequence of numbers A：$a_m,\cdots, a_1, r, b_1,\cdots, b_n$ is a circular sequence of numbers.

Proof: (1) If r is a circular term of A, then A is a circular sequence of numbers. (2) If r is a non-circular term of A, then from Conclusions 3 and 7 we know that, a_m is infinitely great and is a term implying left terms in the $px+q$ sequences of numbers. Now, there exist two cases for b_n. Ⅰ.b_n is less that certain odd number. Then, from n approaching infinity we know that, there necessarily exist equal terms among $b_1,\cdots, b_n$. Since A is a mapping recurrent sequence of numbers, from Basic Theorem 2 we know that A is a circular sequence of numbers. Ⅱ.b_n is infinitely great. Because b_n is a term implying left terms of the $px+q$ sequences of numbers. From Supposition 1 we know that, $a_m=b_n$. Thus, A is a circular sequence of numbers. Q.E.D.

From Conclusion 8 and Reference result 1 we know that, there exist a circular sequence of numbers in the set of the sequences of numbers of the （r）$px+q$ infinite tree. Thus, from Conclusion 6 we can obtain:

Reference result 2. Any sequence of numbers of the $px+q$ sequences of numbers is a circular sequence of numbers.

References 1 and 2 are based on Supposition 1. They are probable results, only for your reference.

（Note: In the proof of Reference result 1 some interesting mathematical problems are embraced, interested readers can study further.）

Now, let us investigate the relationship among infinite trees.

Definition 17. Suppose *a*--the term implying left terms--in the *px+q* sequences of numbers is a degree *n* predecessor of the odd number *r*. Then we call the（*a*）*px+q* infinite tree as the degree *n* **child tree** of the the（*r*）*px+q* infinite tree, call the（*r*）*px+q* infinite tree as the degree *n* **parent tree** of the （*a*）*px+q* infinite tree.

For example, 37 and 149 are the terms implying left terms in the 3*x*+1 sequence of numbers and are the degree 1 predecessors of 7, therefore, the〔37〕3*x*+1 infinite tree and the〔149〕3*x*+1 infinite tree are the degree 1 child trees of the〔7〕3*x*+1 infinite tree (See Fig. 1).

From Fig. 1 we can also see that, the〔37〕3*x*+1 infinite tree also has degree 1 child trees the〔49〕3*x*+1 infinite tree and the 〔197〕3*x*+1 infinite tree, etc. They are the degree 2 child trees of the〔7〕3*x*+1 infinite tree. Conversely, the〔7〕3*x*+1 infinite tree is their degree 2 parent tree.

Besides, 7 has degree 1 successor 11, and 11 has degree 1 successor 17, ⋯. Thus, the〔7〕3*x*+1 infinite tree has degree 1 parent tree the〔11〕3*x*+1 infinite tree, degree 2 parent tree the〔17〕3*x*+1 infinite tree, ⋯.

From Definition 17 we know that, "infinite trees" are full of "infinity". 1. An infinite tree has infinitely many levels and each level has infinitely many odd numbers. 2. Each infinite tree has infinitely many child trees and each child tree is a infinite tree. 3. Each infinite tree has parent trees, etc.

Yet, what follows is more interesting.

Fig. 2 is the〔43〕5*x*+1 infinite tree, which can be obtained similar to the obtaining of Fig. 1.

Fig. 2. [43] 5x+1 infinite tree

It should be noted that "43" occurred at the third level of Fig. 2. According to Definition 17, the 〔43〕5*x*+1 infinite tree given by this "43" is a child tree of the 〔43〕5*x*+1 infinite tree given by Fig. 2. This means that, a 〔43〕5*x*+1 infinite tree is the child tree of a 〔43〕5*x*+1 infinite tree, a 〔43〕5*x*+1 infinite tree is the parent tree of a 〔43〕5*x*+1 infinite tree. And a 〔43〕5*x*+1 infinite tree has infinitely many child trees and parent trees which are 〔43〕5*x*+1 infinite trees.

The phenomena is amazing that one "embodies" oneself, and one "gives birth" to oneself. But they really exist. What do these phenomena means? We can not answer now. What we want to do now is to prevent the phenomena from happening.

Please see the degree 1 predecessors of 43：17,275,4403,⋯ and various terms of $\{a_1=43, a_{n+1}=\beta(5a_n+1)\}$：43,27,17,43,⋯.

In all of the degree 1 predecessors of 43, only 17 is a circular term of $\{a_1=43, a_{n+1}=\beta(5a_n+1)\}$. Looking at Fig. 2 carefully we can find out that, 17 is the reason of "a 〔43〕5*x*+1 infinite tree is the child tree of a 〔43〕5*x*+1 infinite tree".

For this reason, we delete 17 from the degree 1 predecessors of 43: 17，275，4403，⋯ and take the remaining degree 1 predecessors: 275，4403，⋯ as "the whole" degree 1 predecessors of 43. According to the method given by Definition 13, we regenerate the infinite tree with 43 as the root (See Fig. 3). We call Fig. 3, the newly generated infinite tree, as the〔43〕5*x*+1 pure infinite tree. In fact, Fig. 3 is one obtained by deleting the〔17〕5*x*+1 infinite tree from Fig. 2.

Fig. 3. [43] 5x+1 pure infinite tree

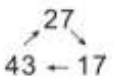
Likewise, we can generate the〔27〕5*x*+1 pure infinite tree and the〔17〕5*x*+1 pure infinite tree.

For convenience, we call the figure by deleting 43 from the〔43〕5*x*+1 pure infinite tree as the pure predecessors figure of 43. Likewise, we call the figure by deleting 27 from the 〔27〕5*x*+1 pure infinite tree as the pure predecessors figure of 27, call the figure by deleting 17 from the 〔17〕5*x*+1 pure infinite tree as the pure predecessors figure of 17. (Similarly, **the pure predecessors figure of *r*** can be defined).

Definition 18. Suppose $a_{i+1}=\beta(pa_i+q)$, $i=1,\cdots n$， and $a_{n+1}=a_1$. We abbreviate the following figure formed by $a_1,\cdots,a_n$

as 《$a_1,\cdots,a_n$》. And we call 《$a_1,\cdots,a_n$》 as a *px+q* directed ring. Usually we use the terminology "***px+q* ring 《$a_1,\cdots,a_n$》**" to denote 《$a_1,\cdots,a_n$》 as thethe *px+q* directed ring.

For example, the first four terms of the sequence of numbers 〔a_1=43, $a_{n+1}=\beta(5a_n+1)$〕: 43,27,17,43… satisfy the condition of Definition 18. At this time, 43,27,17 form the 5*x*+1 ring《43,27,17》, i.e.,



Besides, we view 《43,27,17》，《27,17,43》 and 《17,43,27》 as the same ring, for various numbers in these rings meet the requirement of Definition 18. But "43,17,27" is not a ring.

Now, we define the 5*x*+1 complete tree formed by 5*x*+1 ring 《43,27,17》 first, then we give the general definition of *px+q* complete tree.

We connect 43, 27, 17 in the 5*x*+1 ring 《43,27,17》 with their pure predecessors figures respectively. We call the figure formed (See Fig. 4) as the 5*x*+1 complete tree with 43, 27, 17 as its ring vertexes, or as the《43,27,17》5*x*+1 complete tree, or as the 5*x*+1 complete tree.

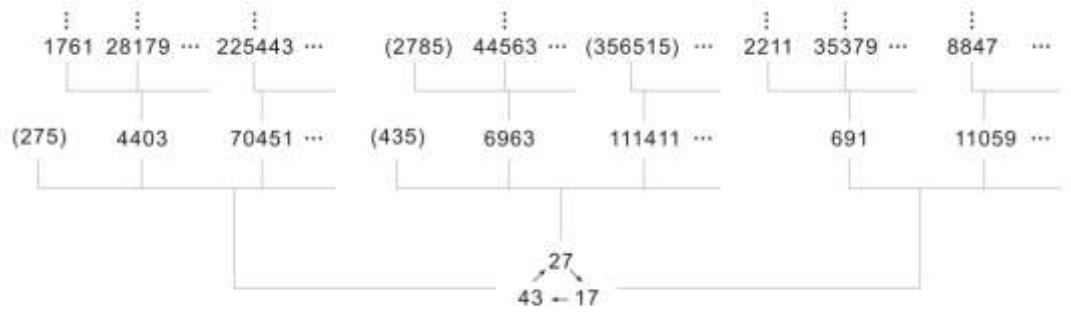


Fig. 4. 《43, 27, 17》5x+1 complete tree

The 《43,27,17》5*x*+1 complete tree has 3 degree 1 child trees, which are the〔43〕5*x*+1 pure infinite tree, the〔27〕5*x*+1 pure infinite tree and the〔17〕5*x*+1 pure infinite tree respectively. It is not hard to imagine that the 《27,17,43》5*x*+1 complete tree and the 《43,27,17》5*x*+1 complete tree are the same complete tree.

（Please note that, the 〔43〕5*x*+1 pure infinite tree in Fig. 4 and that in Fig. 3 looks different, but actually they are the same one）

Definition 19. We connect $a_1,\cdots,a_n$ in the $px+q$ ring《$a_1,\cdots,a_n$》 with their pure predecessors figures respectively, and call the figure obtained as the $px+q$ complete tree with $a_1,\cdots,a_n$ as its ring vertexes, also as the **《$a_1,\cdots,a_n$》 $px+q$ complete tree** or the $px+q$ complete tree.

Conclusion 9. The $px+q$ sequence of numbers obtained by taking any number in the 《$a_1,\cdots,a_n$》 $px+q$ complete tree as the first term is a circular sequence of numbers.

For example, 225443 in Fig. 4 connects downward with 70451, which connects downward with 43→27→17→43⋯. That is, we obtain a circular sequence of numbers: 225443,70451,43,27,17,43,⋯, which is $5x+1$ sequence of numbers $\{a_1=225443,\ a_{n+1}=\beta(5a_n+1)\}$.

Another example is that, from 17→43→27→17⋯ in Fig. 4 we can obtain the circular sequence of numbers: 17,43, 27,17,⋯, which is $5x+1$ sequence of numbers $\{a_1=17,\ a_{n+1}=\beta(5a_n+1)\}$.

Conclusion 10. A $px+q$ complete tree do not has a parent tree and none of its child trees is a complete tree. And a complete tree does not have two numbers equaling to each other.

From 43→27→17→43⋯ in Fig. 4 we can see that, 17 is the degree 1 predecessor of 43. Thus, we can obtain the degree 1 leftward extension sequence of numbers of $\{a_1=43,\ a_{n+1}=\beta(5a_n+1)\}$ i.e., $\{a_1=17,\ a_{n+1}=\beta(5a_n+1)\}$ 17,43, 27,17,⋯. 27 is the degree 1 predecessor of 17. Thus, we can obtain the degree 2 leftward extension sequence of numbers of $\{a_1=43,\ a_{n+1}=\beta(5a_n+1)\}$, i.e., $\{a_1=27,\ a_{n+1}=\beta(5a_n+1)\}$ 27,17, 43, 27,⋯. This is to say that, by "rotating anti-clockwise" the $5x+1$ ring 《43,27,17》 we can obtain a extremely leftward extension sequence of numbers of $\{a_1=43,\ a_{n+1}=\beta(5a_n+1)\}$. The extremely leftward extension sequence of numbers in question is one with all terms are ring vertexes, and it is a "leftward circular sequence of numbers" extending leftward constantly. We call it an **extremely leftward sequence of numbers with ring vertexes**.

Besides, 4403, 70451,⋯ are the degree 1 predecessors of 43,

$\{a_1=4403,\ a_{n+1}=\beta(5a_n+1)\}$ 4403,43, 27,17,⋯。

$\{a_1=70451,\ a_{n+1}=\beta(5a_n+1)\}$ 70451,43, 27,17,⋯。

⋯

From Definition 15 we know that, any leftward extendable sequence of numbers B has degree n leftward extension sequence of numbers, and when n approaches infinity the degree n leftward extension sequence of numbers is the extremely leftward extension sequence of numbers of B. Therefore, all of the above sequences of numbers have corresponding extremely leftward extension sequences of numbers, which are also the extremely leftward extension sequences of numbers of $\{a_1=43,\ a_{n+1}=\beta(5a_n+1)\}$. The common feature of these extremely leftward extension sequences of numbers is that their first terms are infinity. In the extremely leftward extension sequences of numbers of $\{a_1=43,\ a_{n+1}=\beta(5a_n+1)\}$ only the first term of the extremely leftward extension sequences of numbers with ring vertexes is not infinity.

It is not hard to discover that, the 《27,17,43》 $5x+1$ complete tree has the same amount of distinct numbers as that of the〔43〕$5x+1$ infinite tree(or that of the 〔27〕$5x+1$ infinite tree). Therefore, a complete tree is an infinite tree with a stable structure.

Similar to the obtaining of the 《43,27,17》$5x+1$ complete tree, we can also obtain the 《3,1》$5x+1$ complete tree (See Fig. 5), the 《83,13,33》 $5x+1$ complete tree (See Fig. 6), and the 《1》 $3x+1$ complete tree (See Fig. 7).

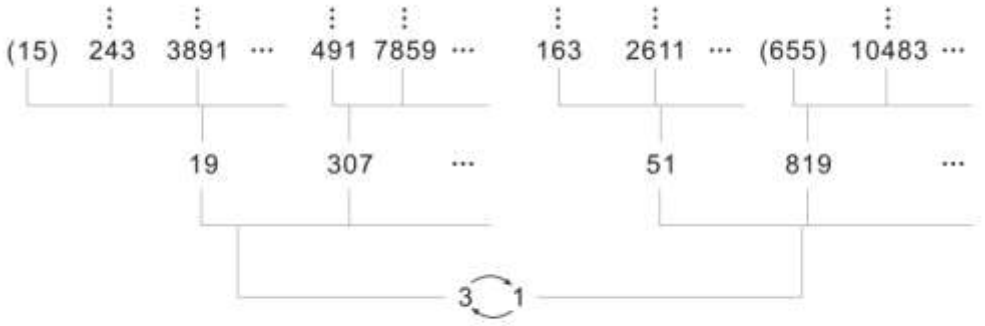


Fig. 5. 《3, 1》5x+1 complete tree

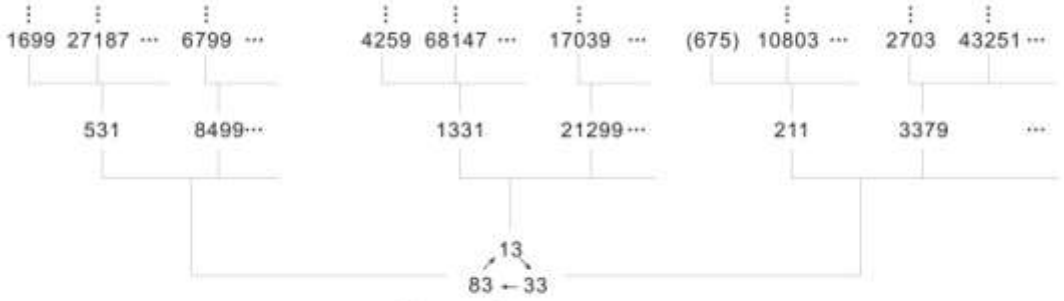


Fig. 6. 《83, 13, 33》5x+1 complete tree

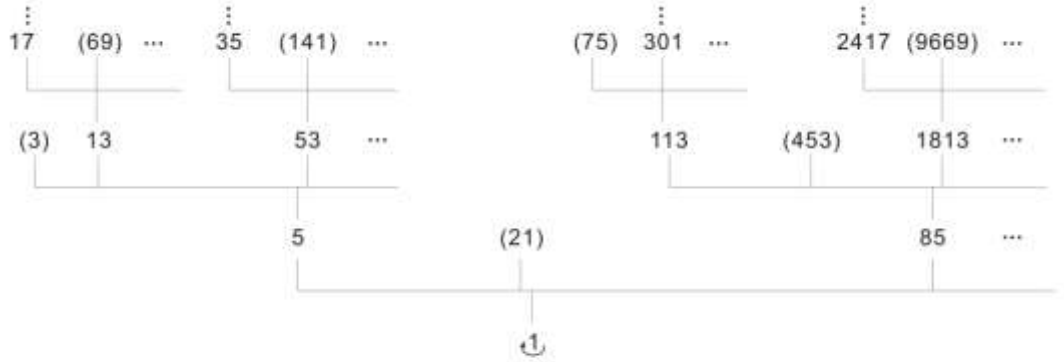


Fig. 7. 《1》3x+1 complete tree

Conclusion 11. Every *px+q* directed ring has its corresponding *px+q* complete tree.

5.The function of the equation of equal terms

Definition 20. Suppose $a_1,\cdots, a_{k+1}\in N_o$, and $a_2=(pa_1+q)/2^{i1}$, $a_3=(pa_2+q)/2^{i2},\cdots, a_{k+1}=(pa_k+q)/2^{ik}$. Then, we call $i_1, i_2,\cdots, i_k$ as **the *k* successive exponents of the *p-q* iteration of a_1**, the *k* successive exponent of a_1 for short.

Definition 20 is not intuitive, we give the following explanation.

We can view $a_1,\cdots, a_{k+1}$ in Definition 20 as the first $k+1$ terms of the *px+q* sequence of numbers: $\{a_1=a_1, a_{n+1}=\beta(pa_n+q)\}$. At this time, a_1 and a_2 satisfy the relation $a_2=\beta(pa_1+q)=(pa_1+q)/2^{i1}$, where i_1 is the number of factor 2 in pa_1+q. The rest can be inferred by analogy.

Example 3. Find the 3 successive exponents of the 3-1 iteration of 11 and the *k* successive exponent of the 5-3 iteration of 1.

First, let us find the 3 successive exponents of the 3-1 iteration of 11.

At this time, $a_1=11, p=3, q=1$. Please see the sequence of numbers: $\{a_1=11, a_{n+1}=\beta(3a_n+1)\}$: 11,17,13,5,⋯

$a_2=(11\times3+1)/2^{i1}=(17\times2^1)/2^1=17$, we obtain $i_1=1$.

$a_3=(17\times3+1)/2^{i2}=(13\times2^2)/2^2=13$, we obtain $i_2=2$.

$a_4=(13\times3+1)/2^{i2}=(5\times2^3)/2^3=5$, we obtain $i_3=3$.

Thus, the 3 successive exponents of the 3-1 iteration of 11 are: $i_1=1$, $i_2=2$, $i_3=3$.

Then, let us find the *k* successive exponents of the 5-3 iteration of 1. At this time, $a_1=1, p=5, q=3$. Please see the sequence of numbers $\{a_1=1, a_{n+1}=\beta(5a_n+3)\}$: 1,1,⋯

$a_2=(1\times5+3)/2^{i1}=(2^3)/2^3=1$, we obtain $i_1=3$. Likewise, $i_1=i_2=\cdots=i_k=3$.

Thus, the *k* successive exponents of the 5-3 iteration of 1 are: $i_1=i_2=\cdots=i_k=3$.

From Example 3 and Definition 20 we know that, when *p* and *q* are given, for any odd number a_1 there necessarily exist unique *k* successive exponents corresponding to it.

Lemma 4. Suppose the *k* successive exponents of the *ith* term e_i in *px+q* sequence of numbers *E* are: $i_1, i_2, \cdots, i_k$, if $e_i=e_{i+k}$, then

$$e_i=(q(p^{k-1}+p^{k-2}\cdot2^{i1}+\cdots+p\cdot2^{i1+i2+\cdots+i_{k-2}}+2^{i1+i2+\cdots+i_{k-1}}))/(2^{i1+i2+\cdots+i_k}-p^k)). \quad (5)$$

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

$$e_{i+1}=(pe_i+q)/2^{i1} \quad (6)$$

$$e_{i+2}=(pe_{i+1}+q)/2^{i2} \quad (7)$$

……

$e_{i+k}=(pe_{i+k-1}+q)/2^{ik}$

Substituting (6) into (7) we obtain:

$e_{i+2}=(p^2e_i+pq+q2^{i1})/2^{i_1+i_2}$

Likewise,

$e_{i+3}=(p^3e_i+p^2q+pq\cdot2^{i1}+q\cdot2^{i_1+i_2})/2^{i_1+i_2+i_3}$

……

$e_{i+k}=(p^ke_i+p^{k-1}q+p^{k-2}q\cdot2^{i1}+\cdots+pq\cdot2^{i_1+i_2+\cdots+i_{k-2}}+q\cdot2^{i_1+i_2+\cdots+i_{k-1}})/2^{i_1+i_2+\cdots+i_k}$.

From $e_i=e_{i+k}$ and the above expression we know that,

$e_i=(p^ke_i+p^{k-1}q+p^{k-2}q\cdot2^{i1}+\cdots+pq\cdot2^{i_1+i_2+\cdots+i_{k-2}}+q\cdot2^{i_1+i_2+\cdots+i_{k-1}})/2^{i_1+i_2+\cdots+i_k}$.

$2^{i_1+i_2+\cdots+i_k}e_i=p^ke_i+p^{k-1}q+p^{k-2}q\cdot2^{i1}+\cdots+pq\cdot2^{i_1+i_2+\cdots+i_{k-2}}+q\cdot2^{i_1+i_2+\cdots+i_{k-1}}$.

$2^{i_1+i_2+\cdots+i_k}e_i-p^ke_i=q(p^{k-1}+p^{k-2}\cdot2^{i1}+\cdots+p\cdot2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})$.

$e_i=q(p^{k-1}+p^{k-2}\cdot2^{i1}+\cdots+p\cdot2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-p^k)$. Q.E.D.

We denote expression (5) as:

$x=q(p^{k-1}+p^{k-2}\cdot2^{i1}+\cdots+p\cdot2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-p^k))$ (8)

Since formula (8) is an equality, we can view it as an equation with x and i_1, i_2, …, i_k as its variables. And we call (8) as the **equation of equal terms** of the $px+q$ sequences of numbers. And we call the solution with $x\in N_o$, and i_1, i_2, …, i_k being the k successive exponents of x as **the characteristic solution** of expression (8).

（Please note that, Lemma 4 is the process of "the listing of the equation" in the process of "the listing of the equation to solve the application problem". Usually, the listing of the equation to solve the application problem is to set the objects we want to find as x,y etc., then we obtain an equation. The setting of the objects we want to find as x,y itself presupposes the existence of the objects. If we know that, the objects we want to find do not exist, then we neither set " the objects" that do not exist as x,y, nor do the useless thing as "the listing of the equation". As to whether the objects we want to find really exist or not, it should be decided by the solution of the equation at last. In Lemma 4, there is condition "if $e_i=e_{i+k}$" . In fact, here we presuppose that any $px+q$ sequence of numbers E has the equal terms （$x=e_i=e_{i+k}$）. While, whether can we make this presupposition or not is an important logical matter. For this reason, the readers must refer to Note 2 at the bottom of this paper.）

We stress again that, formula (8) is meaningful only in the case that both p and q are given. Each $px+q$ sequence of numbers only corresponds its own equation of equal terms. For example, the equation of equal terms to which the $3x+1$ sequence of numbers corresponds is:

$x=(3^{k-1}+3^{k-2}\cdot2^{i1}+\cdots+3\cdot2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-3^k)$ (9)

The equation of equal terms to which the $5x+1$ sequence of numbers corresponds is:

$x=(5^{k-1}+5^{k-2}\cdot2^{i1}+\cdots+5\cdot2^{i_1+i_2+\cdots+i_{k-2}}+2^{i_1+i_2+\cdots+i_{k-1}})/(2^{i_1+i_2+\cdots+i_k}-5^k)$ (10)

In order to draw the readers attention to the correspondence between the equations of equal terms and the $px+q$ sequences of numbers, we discuss the relationship between characteristic solution of formula (10) and the $5x+1$ sequence of numbers.

From the perspective of the source of formula (10), when we suppose that $5x+1$ sequence of numbers E has an equal term x and the k successive exponents of x are i_1, i_2, …, i_k, we can obtain formula (10). This means that when $5x+1$ sequence of numbers E has an equal term then formula (10) has a characteristic solution. From the perspective of the relationship between the solution of an equation and the solution of a problem, when formula (10) has a characteristic solution then $5x+1$ sequence of numbers E has equal term x. Since a $5x+1$ sequence of numbers is a mapping recurrent sequence of numbers, having equal terms means it is a circular sequence of numbers. Thus, we have,

Result 1. $5x+1$ sequence of numbers E is a circular sequence of numbers, if and only if, formula (10) has a characteristic solution x, i_1, i_2, …, i_k, where x is the circular term of E, k is the circular length.

Besides, taking any sequence of numbers in the $5x+1$ sequences of numbers as "sequence of numbers E" we can all obtain formula (10). That is to say, "sequence of numbers E" in Result 1 generally refers to any sequence of numbers in the $5x+1$ sequences of numbers. Thus, we have,

Result 2. Any sequence of numbers of the $5x+1$ sequences of numbers is a circular sequence of numbers, if and only if, formula (10) has a characteristic solution, and x in the characteristic solution is a circular term of the $5x+1$ sequences of numbers.

According to Result 1 we have,

Conclusion 12. *px+q* sequence of numbers *E* is a circular sequence of numbers, if and only if, the equation of equal terms the *px+q* sequence of numbers corresponds has a characteristic solution and *x* in the characteristic solution is a circular term in the *px+q* sequence of numbers *E*.

According to Result 2 we have,

Conclusion 13. Any sequence of numbers of the *px+q* sequences of numbers is a circular sequence of numbers, if and only if, the equation of equal terms the *px+q* sequence of numbers corresponds has a characteristic solution and *x* in the characteristic solution is a circular term of the *px+q* sequence of numbers.

We have to say that, the above feature of the equation of equal terms is very similar to the ratio of the circumference of a circle to its diameter $\pi = c/d$ (*c* is the circumference of the circle, *d* is the diameter of the circle). We know that the most important factor for describing a circle is its radius *r*. But π is irrelevant to *r*. Thus. The ratio of circumference to circle π that would have been one for a circle becomes one for all circles. Similarly, the most important factor for describing a sequence of numbers is its terms. But the equation of equal terms is irrelevant to the terms in any sequence of numbers of the kind of *px+q* sequences of numbers. Thus, the equation of equal terms having the characteristic solution which would have been the sufficient and necessary condition of certain sequence of numbers E of the kind of *px+q* sequences of numbers being a circular sequence of numbers become one of any sequence of numbers of the kind of *px+q* sequences of numbers being circular sequence of numbers.

Now, let us find the characteristic solution of formula (9).

Let k=1. From formula (9) we can obtain characteristic solution: x =1，i_1=2. From Conclusion 13 we know that, any 3*x*+1 sequence of numbers is a circular sequence of numbers and x=1 is the circular term in the 3*x*+1 sequence of numbers in question. From these we can obtain 3*x*+1 ring 《1》， from the ring we can obtain the complete tree given by Fig. 7.

Besides, we can use mathematical induction to prove that formula (9) has a unique characteristic solution: x=1，$i_1 = i_2 = \cdots = i_k = 2$. Therefore, not only any 3*x*+1 sequence of numbers is a circular sequence of numbers, but also any number is in the 《1》3*x*+1 complete tree.

Then, let us find the characteristic solution of formula (10).

Let k=2. From formula (10) 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.

From Conclusion 13 we know that, any 5*x*+1 sequence of numbers is a circular sequence of numbers, and x=3 and x=1 are the circular terms in the 5*x*+1 sequence of numbers. From this we can obtain 5*x*+1 ring 《3, 1》. From the ring we can obtain the complete tree given by Fig. 5.

Let k=3. From formula (10) we can 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; and characteristic solution 5: x =17, i_1=1, i_2=3, i_3=3.

From Conclusion 13 we know that, x =43, 27, 17 are the circular terms in the 5*x*+1 sequence of numbers. From this we can obtain 5*x*+1 ring 《43, 27, 17》. From the ring we can obtain the complete tree given by Fig. 4.

When k=3, formula (10) also has, 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 Conclusion 13 we know that, x =83, 13, 33 are the circular terms in the 5*x*+1 sequence of numbers. From this we can obtain 5*x*+1 ring 《83, 13, 33》. From the ring we can obtain the complete tree given by Fig. 6.

Since we are unable to prove that formula (10) only has the above 8 characteristic solutions, we can not say that, any odd number is necessarily in one of the 《3,1》5*x*+1 complete tree, the 《43,27,17》5*x*+1 complete tree, and the 《83,13,33》5*x*+1 complete tree.

Through the above discussion we know that, from (10) we can find all of the circular terms in the 5*x*+1 sequences of numbers. But we don't know that *x* in each characteristic solution is a circular term of which 5*x*+1 sequence of numbers. There are two reasons for this: One is that when *x* is a circular term of a 5*x*+1 sequence of numbers, *x* is a term implying left terms in the 5*x*+1 sequence of numbers, and there necessarily exists a (x) *px+q* infinite tree, therefore, *x* is necessarily in infinitely many 5*x*+1 sequences of numbers. The other is that, "don't know *x* is a circular term of which 5*x*+1 sequence of numbers" and "don't know π is the ratio of the circumference of which circle to its diameter" has the same logical meaning, the difference is that, all circles has the unique ratio of circumference to diameter π, while formula (10) has many characteristic solutions. Thus, some one may ask: whether Result 2 still holds or not? To this question, we give an affirmative answer in Note 3.

Besides, Conclusion 13 also tells us that, if a kind of *px+q* sequences of numbers has (one) circular sequence of numbers then the equation of equal terms the *px+q* sequences of numbers correspond has a characteristic solution, and when the equation of equal terms the kind of *px+q* sequences correspond has the characteristic solution then any sequence of numbers of the kind of *px+q* sequences of numbers is a circular sequence of

numbers. Thus, we have,

Conclusion 14 If a kind of $px+q$ sequences of numbers have (one) circular sequence of numbers, then any sequence of numbers of the kind of $px+q$ sequences of numbers is a circular sequence of numbers.

Conclusion 14 is a little similar to Conclusion 5. The former is "one" vs. "all", the latter is "one" vs. "infinity". However, their difference is fundamental. The obtaining of Conclusion 5 only depends on the leftward extendedness the $px+q$ sequences of numbers possess. While the obtaining of Conclusion 14 depends on "the listing of the equations to solve application problems", which is a mathematical tool with profound logical meaning. It is not hard to see that, the equation of equal terms contributes a lot to the obtaining of Conclusion 14. Thus, we can see the importance of the equation of equal terms.

Conclusion 14 is very important, now let us see some important conclusions based on it.

For convenience, we call "all sequences of numbers of this kind of $px+q$ sequences of numbers are circular sequences of numbers" as "this kind of $px+q$ sequences of numbers are circular sequences of numbers".

Theorem 7. (I) The class of $x+q$ sequences of numbers （i.e., the class of $px+q$ sequences of numbers with $p=1$） are circular sequences of numbers. (II) The class of $px+q$ sequences of numbers with $p+q=2^m$ are circular sequences of numbers.

Proof: Prove (I).

Because in the $x+1$ sequences of numbers there is $\{a_1=1, a_{n+1}=\beta(a_n+1)\}$：1,1,…. From Conclusion 14 we know that, the $x+1$ sequences of numbers are circular sequences of numbers.

Because in the $x+3$ sequences of numbers there is $\{a_1=3, a_{n+1}=\beta(a_n+3)\}$：3,3,…. From Conclusion 14 we know that, the $x+3$ sequences of numbers are circular sequences of numbers.

……

Because in the $x+q$ sequences of numbers there is $\{a_1=q, a_{n+1}=\beta(a_n+q)\}$：$q, q,\cdots$. From Conclusion 14 we know that, the $x+q$ sequences of numbers are circular sequences of numbers. Thus, (I) holds.

Prove (II). When $p+q=2^m$, in $\{a_1=1, a_{n+1}=\beta(pa_n+q)\}$, there are: $a_2=\beta(pa_1+q)=\beta(p+q)=\beta(2^m)=1$，

$a_3=\beta(pa_2+q)=\beta(p+q)=\beta(2^m)=1$，….

That is, $\{a_1=1, a_{n+1}=\beta(pa_n+q)\}$为：1,1,…. Thus, (II) holds. Q.E.D.

In addition to the above method to prove (I) in Theorem 7, there are other methods to prove the circularity of the class of $x+q$ sequences of numbers. However, it is very hard to find other method to prove (II), i.e., it is very hard to prove the kind of $3x+1$ sequences of numbers, the kind of $7x+1$ sequences of numbers, the kind of $3x+5$ sequences of numbers, etc. are circular sequences of numbers.

Another problem worth thinking is that, although from Theorem 7 we know that, infinitely many kind of $px+q$ sequences of numbers are circular sequences of numbers, it is difficult or even impossible to verify any kind of $px+q$ sequences of numbers are circular sequences of numbers.

For example, it is very difficult to verify $\{a_1=7, a_{n+1}=\beta(7a_n+1)\}$ in the $7x+1$ sequences of numbers is a circular sequence of numbers. But, we can not doubt the correctness of the conclusion in spite of the difficulty in verification.

Lemma 5. Suppose $c\in N_o$, $\{a_1=a, a_{n+1}=\beta(pa_n+q)\}$, $\{b_1=ca, b_{n+1}=\beta(pb_n+cq)\}$. Then, $b_n=ca_n$.

Proof: From $a_1=a$ 和 $b_1=ca$ we know that, $b_1=ca_1$.

From $b_1=ca_1$ and $b_2=\beta(pb_1+cq)$ we obtain that, $b_2=\beta(pca_1+cq)=c\beta(pa_1+q)$. From $b_2=c\beta(pa_1+q)$ and $a_2=\beta(pa_1+q)$ we obtain that, $b_2=ca_2$.

The rest can be inferred by analogy. We know that the Lemma holds. Q.E.D.

Please see the following sequences of numbers.

Sequence of numbers 11： $\{a_1=5, a_{n+1}=\beta(5a_n+1)\}$ 5,13,33,83,13,….

Sequence of numbers 12： $\{a_1=15, a_{n+1}=\beta(5a_n+3)\}$ 15,39,99,249,39,….

Sequence of numbers 13： $\{a_1=45, a_{n+1}=\beta(5a_n+9)\}$ 45,117,297,747,117,….

Each term in sequence of numbers 12 is 3 times the corresponding term in sequence of numbers 11. Each term in sequence of numbers 13 is 9 times the corresponding term in sequence of numbers 11. This is to say that, sequence of numbers 12 and sequence of numbers 13 are all the parasitic sequences of numbers of sequence of numbers 11.

Sequence of numbers 11 is a $5x+1$ sequence of numbers. Sequence of numbers 12 is a $5x+3$ sequence of numbers. Sequence of numbers 13 is a $5x+9$ sequence of numbers. Every sequence of numbers of the $5x+1$ sequences of numbers corresponds to a parasitic sequence of numbers of the $5x+3$ sequences of numbers and $5x+9$ sequences of numbers. Thus we know that, when the $5x+1$ sequences of numbers have circular sequence of numbers, the $5x+q$ sequences of numbers are circular sequences of numbers.

Because from Basic Theorem 1 we know that, when the $5x+1$ sequences of numbers has circular sequence of numbers $\{a_1=a, a_{n+1}=\beta(5a_n+1)\}$, the $5x+q$ sequences of numbers have necessarily circular sequence of numbers $\{b_1=qa, b_{n+1}=\beta(5b_n+q)\}$. From Conclusion 14 we know that, the class of $5x+q$ sequences of numbers are

circular sequences of numbers. Thus, we have,

Conclusion 15. If the $px+1$ sequences of numbers are circular sequences of numbers, then the $px+q$ sequences of numbers are circular sequences of numbers.

Since the class of $px+1$ sequences of numbers with $p=2^m-1$ are circular sequences of numbers, thus

Conclusion 16. The class of $px+q$ sequences of numbers with $p=2^m-1$ are circular sequences of numbers.

For example, $63=2^6-1$. Therefore, the class of $63x+q$ sequences of numbers are circular sequences of numbers.

(Note: For the doubters of Conclusion 13, Conclusion 16 (including (II) in Theorem 7) provides infinitely many "material" for them. So long as they can prove that there exist non-circular sequences of numbers in the classes of $7x+q$, $15x+q$ sequences of numbers and so on, they can disprove Conclusion 13. However, were to Conclusion 13 not holds it is hard for the doubters to achieve their goal. For Reference Result 1 makes it difficult for the doubters to disprove that a $px+q$ sequence of numbers is a circular sequence of numbers.)

In the previous section we have seen 3 $5x+1$ rings, i.e., $5x+1$ ring 《13,33,83》, $5x+1$ ring《43,27,17》, $5x+1$ ring 《3, 1》.

From Lemma 5 we know that, there necessarily exist three $5x+3$ rings, i.e., the $5x+3$ ring 《39,99,249》（See sequence of numbers 12）the, $5x+3$ ring 《129,81,51》, the $5x+3$ ring 《9, 3》.

Likewise, we can obtain three $5x+7$ rings, three $5x+9$ rings,…, three $5x+q$ rings ($1<q\in N_o$).

Besides, $5+3=2^3$. From (II) in Theorem 7 we know that, $\{a_1=1, a_{n+1}=\beta(5a_n+3)\}$为：1,1,…. Therefore, there is a $5x+3$ ring 《1》.

To sum up, there are infinitely many $px+q$ rings. There being one $px+q$ ring means there being one $px+q$ complete tree. Therefore,

Conclusion 17. There are infinitely many $px+q$ complete trees.

Note 1. Equiratio residual sequences of numbers and their applications

The aim of this note is to provide the necessary preliminary knowledge for the study of the $px+q$ sequences of numbers. But, since equiratio residual sequences of numbers are new sequences of numbers, and they are practical, in this note we fully introduce the properties of equiratio residual sequences of numbers.

We use "(x_1, x_2)" to denote the greatest common divisor of x_1 and x_2. And we call a satisfying $a<m$ and $(a, m)=1$ as the **order-existing residue** modulo m.

Definition 21. Suppose mapping recurrent sequence of numbers $\{a_n\}$: $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$, $a<m$. Then we call $\{a_n\}$ as the residual sequence of numbers of equiratio a modulo m, **equiratio residual sequence of numbers** for short. And we call $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ with $(a, m)=1$ as the order-existing residual sequence of numbers of equiratio a modulo m,**order-existing residual sequence of numbers** for short.

From Definition 21 we know that, $\{a_n\}$: $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is a unary mapping recurrent sequence of numbers. Besides, all of the terms in $\{a_n\}$ are less than modulo m. From the pigeon hole principle we know that, there are equal terms in $\{a_n\}$. From Basic Theorem 2 we know that, $\{a_n\}$ is a circular sequence of numbers.

For example, $\{a_1=6, a_{n+1}=(6a_n)_{\mathrm{mod}\ 56}\}$: 6,36,48,8,48,8,… is a mixed circular sequence of numbers with each term being less than modulo 56.

The sequence of numbers is obtained as follows:

$a_1=6$ is the first term,

$a_2=(6a_1)_{\mathrm{mod}\ 56}=(6\times 6)_{\mathrm{mod}\ 56}=36$,

$a_3=(6a_2)_{\mathrm{mod}\ 56}=(6\times 36)_{\mathrm{mod}\ 56}=48$,

…

Once "$\{a_1=6, a_{n+1}=(6a_n)_{\mathrm{mod}\ 56}\}$" is given, we should know that, the sequence of numbers is "6,36,48,8,48,8,…".

Theorem 9. The *nth* term in $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is $a_n=(a^n)_{\mathrm{mod}\ m}$, $n=1,2,$ ….

Proof: We use mathematical induction.

Step 1: The case of $n=1$. From Definition 21 we know that, $a_1=a$, $a<m$. From Definition 1 we know that, $a_1=(a^1)_{\mathrm{mod}\ m}$. For this case the theorem holds.

Step 2: Suppose when $n=k$, $a_k=(a^k)_{\mathrm{mod}\ m}$.

Step 3: Prove when $n=k+1$, $a_{k+1}=(a^{k+1})_{\mathrm{mod}\ m}$.

From induction supposition and Property 5 we know that, $a_k=(a^k)_{\mathrm{mod}\ m}\equiv a^k \pmod m$.

From $a_k\equiv a^k \pmod m$ we obtain that, $a\cdot a_k\equiv a^{k+1} \pmod m$.

From condition $a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}$ we know that, $a_{k+1}=(a\cdot a_k)_{\mathrm{mod}\ m}\equiv a\cdot a_k\equiv a^{k+1} \pmod m$.

From $a_{k+1}=(a\cdot a_k)_{\mathrm{mod}\ m}$ and Definition 1 we know that, $a_{k+1}<m$.

From $a_{k+1}\equiv a^{k+1} \pmod m$ and $a_{k+1}<m$, $(a^{k+1})_{\mathrm{mod}\ m}<m$ we know that, $a_{k+1}=(a^{k+1})_{\mathrm{mod}\ m}$. Q.E.D.

For example, the 4th term in $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 9}\}$: 2,4,8,7,5, 1, 2, … is $a_4=(2^4)_{\mathrm{mod}\ 9}=7$.

From Theorem 9 we know that, various terms in $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ are the minimal non-negative residues modulo m of the corresponding terms in equiratio sequence of numbers : $a, a^2,\cdots,a^n$ respectively. This justifies the name "equiratio residual sequence of numbers".

Now, let us discuss the relationship between order-existing residual sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ and order $\delta_a(m)$ of a modulo m.

The 6th term in sequence of numbers $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 9}\}$ is $a_6=(2^6)_{\mathrm{mod}\ 9}=1$. Besides, the order of 2 modulo 9 is $\delta_9(2)=6$. From the definition of the order we know that, when $(a, m)=1$ there necessarily exists h such that $(a^h)_{\mathrm{mod}\ m}=1$. If h is the minimal positive number for $(a^h)_{\mathrm{mod}\ m}=1$ to hold, then $h=\delta_m(a)$.

Because when $(a, m)=1$, there necessarily exists h such that $a^h\equiv 1(\mathrm{mod}\ m)$. Thus, from Theorem 9 we can obtain,

Corollary 5. Suppose $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is an order-existing residual sequence of numbers. Then, there necessarily exists $h\in N$ such that the *hth* term in the sequence of numbers in question is $a_h=1$. When a_h is the first term in the sequence of numbers in question equaling to 1, then $h=\delta_m(a)$.

When $h=\delta_m(a)$, the term a_{h+1} in order-existing sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is $a_{h+1}=(a\cdot a_h)_{\mathrm{mod}\ m}=a=a_1$. Therefore, from Basic Theorem 2 and Definition 5 we can obtain,

Corollary 6. Order-existing sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is necessarily a pure circular sequence of numbers, and its minimal circular length is $\delta_m(a)$.

Corollaries 5 and 6 tell us that, the set formed by the first $\delta_m(a)$ terms in order-existing sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is one formed by all of the terms in the sequence of numbers in question.

For this reason, we call the sequence of numbers formed by the first $\delta_m(a)$ terms in order-existing sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ **the simplest sequence of numbers** of $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$, "simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$" for short.

Below are all of the simplest sequences of numbers of the order-existing sequences of numbers module 11.

Simplest $\{a_1=1, a_{n+1}=(a_n)_{\mathrm{mod}\ 11}\}$: 1.
Simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 11}\}$: 2,4, 8,5, 10,9,7, 3,6, 1.(The second sequence of numbers)
Simplest $\{a_1=3, a_{n+1}=(3a_n)_{\mathrm{mod}\ 11}\}$: 3, 9, 5, 4, 1.
Simplest $\{b_1=4, b_{n+1}=(4b_n)_{\mathrm{mod}\ 11}\}$: 4, 5, 9, 3, 1. (The fourth sequence of numbers)
Simplest $\{a_1=5, a_{n+1}=(5a_n)_{\mathrm{mod}\ 11}\}$: 5, 3, 4, 9, 1.
Simplest $\{a_1=6, a_{n+1}=(6a_n)_{\mathrm{mod}\ 11}\}$: 6,3, 7,9, 10, 5,8, 4,2, 1.
Simplest $\{a_1=7, a_{n+1}=(7a_n)_{\mathrm{mod}\ 11}\}$: 7,5, 2,3, 10, 4,6, 9,8, 1.
Simplest $\{a_1=8, a_{n+1}=(8a_n)_{\mathrm{mod}\ 11}\}$: 8,9, 6,4, 10,3,2, 5,7, 1.
Simplest $\{a_1=9, a_{n+1}=(9a_n)_{\mathrm{mod}\ 11}\}$: 9,4, 3,5, 1.
Simplest $\{a_1=10, a_{n+1}=(10a_n)_{\mathrm{mod}\ 11}\}$: 10, 1.

From the above simplest sequences of numbers we can observe the following results.

(1). Every order-existing residue a modulo m necessarily corresponds to a simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$.

(2). Every simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ ends with "1".

Conclusion 18. The number of terms in simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is $\delta_m(a)$.

This is convenient for a computer to find order.

Theorem 10. The relationship between $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ and $\{b_1=a_k, b_{n+1}=(a_k\cdot b_n)_{\mathrm{mod}\ m}\}$ is : $b_n=a_{kn}$.

Proof: from Theorem 9 and the supposition we know that, $a_k=(a^k)_{\mathrm{mod}\ m}$, $b_n=(a_k{}^n)_{\mathrm{mod}\ m}$.

Substituting $a_k=(a^k)_{\mathrm{mod}\ m}$ into $b_n=(a_k{}^n)_{\mathrm{mod}\ m}$, we obtain,

$b_n=(((a^k)_{\mathrm{mod}\ m})^n)_{\mathrm{mod}\ m}=((a^{kn})_{\mathrm{mod}\ m}))_{\mathrm{mod}\ m}=(a^{kn})_{\mathrm{mod}\ m}=a_{kn}$. (The transformation of this formula please refer to Property 3) Q.E.D.

Please see the second and the fourth sequences of numbers above.

It is not hard to see that, 1st, 2nd, 3rd, 4th, 5th terms in the fourth sequence of numbers are 2nd, 4th, 6th, 8th, 10th terms in the second sequence of numbers respectively. The reason is that, the first term b_1 in the fourth sequence of numbers is "$b_1=a_2$". Here, "2" is k in Theorem 10. Thus, the number of terms $\delta_{11}(4)$ in the fourth sequence of numbers is only half the number of terms $\delta_{11}(2)$ in the second sequence of numbers. That is, $\delta_{11}(4)=\delta_{11}(2)/2=10/2=5$.

We know that, $\delta_m(a^k)=\delta_m(a)/(\delta_m(a), k)$. From Theorem 9 we know that, in$\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ there is $a_k\equiv a^k(\mathrm{mod}\ m)$. Therefore, $\delta_m(a_k)=\delta_m(a^k)$. Thus, we have,

Corollary 7. The order $\delta_m(a_k)$ of the term a_k modulo m in order-existing sequence of numbers $\{a_1=a, a_{n+1}=$

$(a\cdot a_n)_{\mathrm{mod}\ m}\}$ satisfy I. $\delta_m(a_k)=\delta_m(a)/(\delta_m(a), k)$. II. $\delta_m(a_k)|\delta_m(a)$; III. In simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ there are $\phi(\delta_m(a_k))$ terms whose orders modulo m equal $\delta_m(a_k)$; IV. If $k=\delta_m(a)/d(1<d<\delta_m(a))$ then $\delta_m(a_k)=d$.

From Theorem 10 we can also prove Corollary 7.

Of $\delta_m(a_k)=\delta_m(a)/(\delta_m(a), k)$ and $\delta_m(a^k)=\delta_m(a)/(\delta_m(a), k)$, although they are similar and equivalent, their functions are quite different.

Now, we use $\{a_1=7, a_{n+1}=(7a_n)_{\mathrm{mod}\ 15}\}$ as an example to show the difference between $\delta_m(a_k)$ and $\delta_m(a^k)$.

Because simplest $\{a_1=7, a_{n+1}=(7a_n)_{\mathrm{mod}\ 15}\}$: 7,4, 13,1 has 4 terms, $\delta_{15}(7)=4$（i.e., "$\delta_m(a)=4$"）.

From $\delta_m(a_k)=\delta_m(a)/(\delta_m(a), k)$ we know that,

$\delta_{15}(a_1)=\delta_{15}(7)/(\delta_{15}(7), 1)=4$.（$\delta_{15}(a_1)$ i.e., $\delta_{15}(7)$）

$\delta_{15}(a_2)=\delta_{15}(7)/(\delta_{15}(7), 2)=2$.（$\delta_{15}(a_2)$ i.e., $\delta_{15}(4)$）

$\delta_{15}(a_3)=\delta_{15}(7)/(\delta_{15}(7), 3)=4$.（$\delta_{15}(a_3)$ i.e., $\delta_{15}(13)$）

$\delta_{15}(a_4)=\delta_{15}(7)/(\delta_{15}(7), 4)=1$.（$\delta_{15}(a_4)$ i.e., $\delta_{15}(1)$）.

That is to say, Corollary 7 tells us that, once we find simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$, we can obtain the order modulo m of any term in the sequence of numbers in question. Obviously, $\delta_m(a^k)=\delta_m(a)/(\delta_m(a), k)$ does not have the function.

This fact tells us that, even if the result obtained from the perspective of the equiratio residual sequence of numbers is equivalent to one obtained from number theory, their functions are different. The examples of solving higher order congruent equations and exponential congruent equations given later can expound this point further.

Besides, from $\delta_m(a_k)=\delta_m(a)/(\delta_m(a), k)$ we also know that, the orders modulo m of various terms in order-existing residual sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ are all less than or equal to $\delta_m(a)$, which lay a foundation for the computer algorithm of finding the primitive root.

Now, we discus the computer algorithm for finding the primitive root.（Those readers who do not care the primitive root can skip the following part confined by "〖〗"）

〖Please see sequence of numbers Q: 1, 2, 3, 4, 5, 6, 0, 8, 9, 10, 11, 12, 13, 0,15,16, 17, 18, 19, 20, 0, 22, 23, 24, 25, 26,27,0,29, 30, 31, 32, 33,34, 0, 36, 37, 38, 39, 40, 41, 0, 43, 44, 45, 46, 47, 48, 0.

Sequence of numbers Q has 49 terms, in which the term values of the non-zero terms are the same as their position values, i.e., $q_n=n$. For example, $q_1=1$, $q_{10}=10$ etc.. At the same time, these non-zero terms are just all order-existing residues of 49.

It is impossible for 1 to be a primitive root of 49, therefore, 2 is the minimal number that is possibly a primitive root of 49.

Find the simplest sequence of numbers of 2, i.e., find simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 49}\}$:

2,4,8,16,32,15,30,11,22,44,39,29,9,18,36,23,46,43,37,25,1.

Because the number of terms in the sequence of numbers in question is $\delta_{49}(2)=21<\phi(49)$, 2 is not a primitive root of 49. meanwhile, from Corollary 7 we know that, none of the 21 numbers: 2,4,8,16,32,15,30,11,22,44,39,29,9,18,36,23,46,43,37,25,1 is a primitive root of 49.

We set the terms in sequence of numbers Q whose position values are: 2,4,8,16,32,15,30,11,22,44,39,29,9,18,36,23,46,43,37,25,1 to 0, obtaining sequence of numbers T:

0, 0, 3,0, 5, 6, 0, 0, 0, 10, 0, 12, 13, 0,0,0, 17, 0, 19, 20, 0, 0, 0, 24, 0, 26,

27,0,0, 0, 31, 0, 33,34, 0, 0, 0, 38, 0, 40, 41, 0, 0, 0, 45, 0, 47, 48, 0.

Then, we find the simplest sequence of numbers of the first non-zero term (That is 3) in sequence of numbers T, i.e., simplest $\{a_1=3, a_{n+1}=(3a_n)_{\mathrm{mod}\ 49}\}$:

3,9,27,32,47,43,31,44,34,4,12,36,10,30,41,25,26,29,38,16,48,

46,40,22,17,2,6,18,5,15,45,37,13,39,19,8,24,23,20,11,33,1.

The number of terms in the sequence of numbers in question is $\delta_{49}(3)=42=\phi(49)$. Therefore, 3 is a primitive root of 49, i.e., we have found a primitive root of 49. Termination.

We know that, k satisfying $(k, \phi(49))=1$ are k=1,5,11,13,17,19,23,25,29,31,41. Thus, from Corollary 7 we know that, the first, the 5^{th}, the 11^{th}, the 13^{th}, the 17^{th}, the 19^{th}, the 23^{th}, the 25^{th}, the 29^{th}, the 31^{th}, the 37^{th}, the 41^{th} terms in simplest $\{a_1=3, a_{n+1}=(3a_n)_{\mathrm{mod}\ 49}\}$ are all primitive roots of 49. The first, the 5^{th}, the 11^{th}, the 13^{th}, the 17^{th}, the 19^{th}, the 23th, the 25^{th}, the 29^{th}, the 31^{th}, the 37^{th}, the 41^{th} terms in the sequence of numbers in question are 3,47,12,10,26,38,40,17,5,45,24,33. Therefore, the 12 numbers: 3,47,12,10,26,38,40,17,5,45,24,33 are all primitive roots of 49 (The readers can verify themselves).

Thus we see that, if we have found simplest $\{a_1=3, a_{n+1}=(3a_n)_{\mathrm{mod}\ 49}\}$ then we have found all of the primitive roots of 49.

When we view sequence of numbers Q as an one dimensional array, the process of changing sequence of numbers Q to sequence of numbers T is one that set array Q's terms $q_k=0$ (k adopts the term values of

simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 49}\}$ successively.) This process is one that deletes part of non-primitive roots in array *Q*. We call it the **process of deleting the non-primitive roots**.

If 3 was not a primitive root of 49 then we would perform the process of deleting the non-primitive root again, i.e., we would set array *Q's* terms $q_k=0$ again (At this time, *k* would adopt the term values of simplest $\{a_1=3, a_{n+1}=(3a_n)_{\mathrm{mod}\ 49}\}$ successively). Obviously, the non-zero non-primitive root terms in array *Q* will be reduced further, i.e., the probability of the first non-zero term in array *Q* being a primitive root will be increased. According to this method, we can necessarily find a primitive root modulo *m* that has primitive roots. (Note: "if 3 was not a primitive root of 49" is counterfactual, we only use it as an "explanation", we can not use it to make inference further)

Besides, we know that, 3 is the minimal primitive root of 49. That is to say, the primitive root directly obtained by the above method is the minimal primitive root of 49. Now, we give the general algorithm of finding primitive roots modulo *m* (Here, we tacitly consent that *m* has primitive roots).

Algorithm for finding the minimal primitive root:

Step 1. Initialization. If *m* is an odd number, then let $a=2$, otherwise let $a=3$. And let the one dimensional array Q(*m*) satisfy: If $(k, m)=1$ ($1\leqslant k\leqslant m$) then let $q_k=k$, otherwise let $q_k=0$.

Step 2. Finding simplest $\{a_1=a, a_{n+1}=(aa_n)_{\mathrm{mod}\ m}\}$. If *a* is a primitive root modulo *m* then terminate, otherwise go to Step 3.

Step 3. Performing the process of deleting the non-primitive roots. Let *a* equals the first non-zero term in Q(*m*), and go to Step 2.

Now, we use the algorithm for finding the minimal primitive root to find the primitive roots of 22.

Because 22 is an odd number, according to Step 1, let $a=3$. And let the 22 terms in the one dimensional array Q(22) be: 1,0,3,0,5,0,7,0,9,0,11,0,13,0,15,0,17,0,19,0,21,0, respectively.

According to Step 2,we find simplest $\{a_1=a, a_{n+1}=(aa_n)_{\mathrm{mod}\ m}\}$. Now, it is $\{a_1=3, a_{n+1}=(3a_n)_{\mathrm{mod}\ 17}\}$: 3,9,5,15,1. $\delta_{22}(3)=5<\phi(22)=10$, thus we know that 3 is not a primitive root of 22.

According to the algorithm, go to Step 3. We perform the process of deleting the non-primitive roots, change the 3^{rd}, 9^{th}, 5^{th}, 15^{th}, 1^{st} terms in array Q to 0. Thus, the terms in Q are: 0,0,0,0,0,0,7,0,0,0,11,0,13,0,0,0,17,0,19,0,21,0 respectively. The first non-zero term is the 7^{th} term 7. Let $a=7$.

According to the algorithm, go to Step 2. We find simplest $\{a_1=a, a_{n+1}=(aa_n)_{\mathrm{mod}\ m}\}$. Now, it is $\{a_1=7, a_{n+1}=(7a_n)_{\mathrm{mod}\ 22}\}$: 7,5,13,3,21,15,17,9,19,1. $\delta_{22}(7)=10=\phi(22)$, thus, we know that 7 is the minimal primitive root of 22, terminate.

Besides, 1,3,7,9 are mutually prime with $\phi(22)=10$, therefore, 1^{st}, 3^{rd}, 7^{th}, 9^{th} terms in simplest $\{a_1=7, a_{n+1}=(7a_n)_{\mathrm{mod}\ 22}\}$, that is, 7,13,17,19 are all primitive roots of 22.

Since the computational complexity of the algorithm for finding minimal primitive roots is extremely low and its convergence is better than the sift method for finding the prime numbers, it is an extremely practical computer algorithm. At the same time, if we make proper improvements to it, then it can become a decision algorithm deciding whether *m* has a primitive root or not, and become an algorithm for computing the primitive roots of *m*.〗

Now, we discuss the relationship of the positions between a_k and its inverse a_k^{-1} modulo *m* in simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)\mathrm{mod}\ m\}$.

Simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 11}\}$: 2,4, 8,5, 10,9,7, 3,6, 1 has 10 terms. Its 1^{st} term 2 and the 9^{th} ($9=10-1$) term 6 has the relationship $2\times6\equiv1(\mathrm{mod}\ 11)$; its 2^{nd} term 4 and the 8^{th} ($8=10-2$) 3 has the relationship$4\times3\equiv1(\mathrm{mod}\ 11)$; …; its 5^{th} term 10 and the 5^{th} ($5=10-5$) term 10 has the relationship $10\times10\equiv1(\mathrm{mod}\ 11)$. Thus, we can obtain the following result.:

When any order-existing residue of modulo *m* occurs in order-existing residual sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$, the inverse of the order-existing residue in question necessarily occurs in the sequence of numbers in question.

Any term in order-existing residual sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ is mutually prime with modulo *m*, therefore, any term in the sequence of numbers in question has an inverse. And, we have,

Theorem 11. Suppose a_k^{-1} ($<m$) is the inverse of terms a_k in order-existing residual sequence of numbers $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ to modulo *m*. Then, $a_k^{-1}=a_i$, $i=n\delta_m(a)-k$. Or, $(a^k)^{-1}\equiv a^{n\delta m(a)-k}(\mathrm{mod}\ m)$.

Proof: For *k* given by the Theorem, there necessarily exist positive integers *i*, *n* such that $i=n\delta_m(a)-k$. Thus, $k+i=n\delta_m(a)$.

From $a_k=(a^k)_{\mathrm{mod}\ m}\equiv a^k (\mathrm{mod}\ m)$ and $a_i=(a^i)_{\mathrm{mod}\ m}\equiv a^i (\mathrm{mod}\ m)$ we can obtain, $a_ka_i\equiv a^{k+i}\equiv a^{n\delta m(a)}\equiv1 (\mathrm{mod}\ m)$.

From $a_ka_i\equiv1 (\mathrm{mod}\ m)$ we know, $a_k^{-1}\equiv a_i (\mathrm{mod}\ m)$. From $a_k^{-1}<m$ and $a_i<m$ we know that, $a_k^{-1}=a_i$.

Or, from $a^{k+i}\equiv1 (\mathrm{mod}\ m)$ we obtain, $(a^k)^{-1}\equiv a^i\equiv a^{n\delta m(a)-k}(\mathrm{mod}\ m)$. Q.E.D.

From the proof of Theorem 11 we know that,

Corollary 8. Suppose the inverse of a^k to modulo m is $(a^k)^{-1}$. Then, there necessarily exists positive integer i such that $(a^k)^{-1}\equiv a^i \pmod m$.

As a special case of Theorem 11： Let $k=1$, $n=1$， from $a_k^{-1}=a_i$, $i=n\delta_m(a)-k$ we obtain, $a^{-1}=a_{\delta_m(a)-1}$. Since $a_{\delta_m(a)-1}$ is the second from the right term in simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\text{mod } m}\}$, we have,

Conclusion 19. a^{-1} is the second from the right term in simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\text{mod } m}\}$.

Conclusion 19 is convenient for finding a^{-1} by a computer.

Both finding a^{-1} and finding $\delta_m(a)$ need to find simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\text{mod } m}\}$. The difference is that, the former needs to find the second from the right term in the sequence of numbers in question, while the latter needs to find the number of terms in the sequence of numbers in question.

Now, we use equiratio residual sequence of numbers to solve the higher order congruent equations.

Please see the following 6×6 matrix.

2 4 8 7 5 1
4 7 1 4 7 1
8 1 8 1 8 1
7 4 1 7 4 1
5 7 8 4 2 1
1 1 1 1 1 1

The first to the 6th rows of the matrix are the first 6 terms of ：$\{a_1=2, a_{n+1}=(2a_n)_{\text{mod } 9}\}$, $\{a_1=4, a_{n+1}=(4a_n)_{\text{mod } 9}\}$, $\{a_1=8, a_{n+1}=(8a_n)_{\text{mod } 9}\}$, $\{a_1=7, a_{n+1}=(7a_n)_{\text{mod } 9}\}$, $\{a_1=5, a_{n+1}=(5a_n)_{\text{mod } 9}\}$, $\{a_1=1, a_{n+1}=(a_n)_{\text{mod } 9}\}$ respectively. The first column gives a mutually prime residual system modulo 9, i.e., the first column is a degree 1 order-existing residue of x modulo 9; the second column is a degree 2 order-existing residue of x modulo 9; …; the 6th column is a degree 6 order-existing residue of x modulo 9. We call the above matrix as a matrix of order-existing residue modulo 9.

Using the matrix of order-existing residue modulo 9 we can find mutually prime solutions (i.e., solutions of $(x,9)=1$) of the following congruent equation:

$x^{43}+2x^{38}+3x^{33}+4x^{28}-x^{13}+x^{12}+x+6\equiv 0 \pmod 9$ (11)

$\phi(9)=6$, $x^{6n}\equiv 1 \pmod 9$, therefore, $x^{43}\equiv x \pmod 9$, $x^{38}\equiv x^2 \pmod 9$, …, $x^{12}\equiv 1 \pmod 9$.

That is, the congruent equation (5) is equivalent to

$x+2x^2+3x^3+4x^4+7\equiv 0 \pmod 9$ (12)

$x\equiv(x)_{\text{mod } 9}\pmod 9$, $x^2\equiv(x^2)_{\text{mod } 9}\pmod 9$, $x^3\equiv(x^3)_{\text{mod } 9}\pmod 9$, $x^4\equiv(x^4)_{\text{mod } 9}\pmod 9$, therefore,

$x+2x^2+3x^3+4x^4+7\equiv(x)_{\text{mod } 9}+2(x^2)_{\text{mod } 9}+3(x^3)_{\text{mod } 9}+4(x^4)_{\text{mod } 9}+7 \pmod 9$

Also because the first row of the matrix is the first 6 terms of $\{a_1=2, a_{n+1}=(2a_n)_{\text{mod } 9}\}$, the 1st, 2nd, 3rd, 4th terms of the first row are：$(2)_{\text{mod } 9}$, $(2^2)_{\text{mod } 9}$, $(2^3)_{\text{mod } 9}$, $(2^3)_{\text{mod } 9}$, i.e., 2,4,8,7. At this time, when we let $x=2$（i.e., the first term of the first row）, $(x)_{\text{mod } 9}=2$, $(x^2)_{\text{mod } 9}=4$, $(x^3)_{\text{mod } 9}=8$, $(x^4)_{\text{mod } 9}=7$. Thus,

$(x)_{\text{mod } 9}+2(x^2)_{\text{mod } 9}+3(x^3)_{\text{mod } 9}+4(x^4)_{\text{mod } 9}+7=2+2\times 4+3\times 8+4\times 7+7=69$.

From this we know that, when $x=2$, $x+2x^2+3x^3+4x^4+7\equiv 69 \pmod 9$.

From $69\not\equiv 0 \pmod 9$ we know that, $x\equiv 2 \pmod 9$ is not a solution of congruent equation (12).

From the 1st, 2nd, 3rd, 4th terms of the second row of the matrix we can obtain,

$4+2\times 7+3\times 1+4\times 4+7=54\equiv 0 \pmod 9$

From this we know that, $x\equiv 4 \pmod 9$ is a solution of congruent equation (12).

From the 1st, 2nd, 3rd, 4th terms of the third row of the matrix we can obtain,

$8+2\times 1+3\times 8+4\times 1+7=45\equiv 0 \pmod 9$

From this we know that, $x\equiv 8 \pmod 9$ is a solution of congruent equation (12).

Similar to the above method, we know that, $x\equiv 1,5,7 \pmod 9$ are not solutions of congruent equation (6).

Therefore, the mutually prime solutions of congruent equation (12) are ： $x\equiv 4,8 \pmod 9$.

Because the mutually prime solutions of congruent equation (5) are the same as those of (6), the mutually prime solutions of congruent equation (5) are： $x\equiv 4,8 \pmod 9$.

Now, we find the non-mutually prime solutions of congruent equation (11). Please see the following equiratio residual sequences of numbers:

$\{a_1=0, a_{n+1}=(0a_n)_{\text{mod } 9}\}$ ： 0,0, 0,….

$\{a_1=3, a_{n+1}=(3a_n)_{\text{mod } 9}\}$ ： 3,0, 0,….

$\{a_1=6, a_{n+1}=(6a_n)_{\text{mod } 9}\}$ ： 6,0, 0,….

Since in the minimal non-negative residual system modulo 9, the x satisfying $(x, 9)>1$ can only be 0, 3, 6. From the above 3 sequences of numbers we know that, when $n>1$, $x^n\equiv 0 \pmod 9$. Thus, congruent equation (11) has the same solution as $x+6\equiv 0 \pmod 9$.

Obviously, only $x\equiv 3 \pmod 9$ is the solution of $x+6\equiv 0 \pmod 9$, i.e., the non-mutually prime solution of congruent equation (11). Adding the above mutually prime solutions, we obtain that , the solutions of congruent equation (11) are $x\equiv 3,4,8 \pmod 9$.

It is not hard to prove that, when $m=p^k$ (p is a prime number) and $(m, a)>1$， term a_n in $\{a_1=a, a_{n+1}=(aa_n)_{\mathrm{mod}\ m}\}$ is $a_n=0 (n\geqslant k)$.

According to the above method, we can find the solution of higher order congruent equation $f(x)\equiv 0 \pmod{p^n}$. Furthermore, we can find the general solution of $f(x)\equiv 0 \pmod m$（m is any positive integer）. Since the computation of equiratio residual sequences of numbers can be performed entirely by computers, the solving of the higher order congruent equations can be performed entirely by computers.

Then, we use equiratio residual sequences of numbers to solve the class of exponential congruent equations $a^x\equiv b \pmod m$.

Find the solutions of ⑴$4^x\equiv 10 \pmod{13}$, ⑵$6^x\equiv 48 \pmod{56}$,⑶$6^x\equiv 8 \pmod{56}$,⑷$6^x\equiv 28 \pmod{56}$.

Solving ⑴： Find $\{a_1=4, a_{n+1}=(4a_n)_{\mathrm{mod}\ 13}\}$ ： 4,3,12,9,10,1,4,⋯. The circular length of the sequence of numbers in question is 6.

It is not hard to discover that, $a_{5+6n}=(4^{5+6n})_{\mathrm{mod}\ 13}=10 (0\leq n)$. Therefore, the solutions of $4^x\equiv 10 \pmod{13}$：$x=5+6n$ or $x\equiv 5 \pmod 6$.

（Note： $x=5+6n$ means that, x equals to the position value of 10 in $\{a_1=4, a_{n+1}=(4a_n)_{\mathrm{mod}\ 13}\}$ ）

Solving ⑵⑶⑷： Find $\{a_1=6, a_{n+1}=(6a_n)_{\mathrm{mod}\ 56}\}$ ： 6,36,48,8,48,8,⋯. The sequence of numbers in question is a mixed circular sequence of numbers with the circular length being 2.

From $a_{3+2n}=(6^{3+2n})_{\mathrm{mod}\ 56}=48 (0\leqslant n)$ we know that, the solution of $6^x\equiv 48 \pmod{56}$ is $x=3+2n$.

From $a_{4+2n}=(6^{4+2n})_{\mathrm{mod}\ 56}=8 (0\leqslant n)$ we know that, the solution of $6^x\equiv 8 \pmod{56}$ is $x=4+2n$.

Since 28 does not occur in $\{a_1=6, a_{n+1}=(6a_n)_{\mathrm{mod}\ 56}\}$, which means that, the minimal non-negative residue of 6^x to modulo 56 can not be 28. Therefore, $6^x\equiv 28 \pmod{56}$ has no solution. From this we can obtain,

Conclusion 20. $a^x\equiv b \pmod m$ has solutions if and only if $(b)_{\mathrm{mod}\ m}$ is a term in $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$ and x equals to the position value of $(b)_{\mathrm{mod}\ m}$ in $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\mathrm{mod}\ m}\}$.

This Conclusion is an important foundation in Section 3 in the discussion of the leftward extendeness of the $px+q$ sequences of numbers.

Now, we discuss the relationship between Corollary 7 and the pseudo prime numbers.

People usually call composite number m with $a^m\equiv a \pmod m$ or $\delta_m(a) \mid m-1 (1<a<m-1)$ as a pseudo prime number with base a , a-pseudo prime number for short.

We know that 341 is the minimal 2-pseuso prime number. But there are many a such that 341 is the a-pseudo prime number.

For example, simplest $\{a_1=2, a_{n+1}=(2a_n)_{\mathrm{mod}\ 341}\}$：2,4 ,8,16,32, 64,128,256,171,1. The sequence of numbers in question has 10 terms. Thus, $\delta_{341}(2)=10$.

Let $a\in\{2,4,8,16,32,64,128,256,171\}$， $1<a<341-1$. From II in Corollary 7 we know that, $\delta_{341}(a) \mid \delta_{341}(2)$. From $\delta_{341}(2)=10$ we know that, $\delta_{341}(a) \mid 10 \mid 341-1$.

Therefore, 341 is a pseudo prime number with $a\in\{2,4,8,16,32,64,128,256,171\}$ as the bases.

Another example: simplest $\{a_1=31, a_{n+1}=(31a_n)_{\mathrm{mod}\ 49}\}$ ： 31,30 ,48, 18,19,1 has 6 terms.Thus, $\delta_{49}(31)=6$.

Let $a\in\{31,30, 18,19\}$. $1<a<49-1$. $\delta_{49}(a) \mid 6 \mid 49-1$.

Therefore, $49=7^2$ is a pseudo prime number with $a\in\{31,30,18,19\}$ as the bases. That is, there are 7-3 a such that 7^2 is a a-pseudo prime number.

In order to differentiate another kind of pseudo prime number we will introduce later, we call compose number m with $a (1<a<m-1)$ such that $\delta_m(a) \mid m-1$ holds as type I pseudo prime number. Obviously, when m is a a-pseudo prime number, m is a type I pseudo prime numbers.

Surprisingly, almost all odd composite numbers are type I pseudo prime numbers.

$\delta_{15}(4)=\delta_{15}(11)=2 \mid 15-1$， therefore, 15 is a pseudo prime number with 4 and 11 as its bases. 15 is the minimal type I pseudo prime number.

Lemma 6. Suppose g is a primitive root of odd number m. Then, in simplest $\{a_1=g, a_{n+1}=(g\cdot a_n)_{\mathrm{mod}\ m}\}$, I. There exists and only exists $a_{\phi(m)}=1$. II. If $m>3$ then there exists and only exists term $a_{\phi(m)/2}=m-1$.

Proof: From g being a primitive root of m we know that, the $\phi(m)=\delta_m(g)$ terms of simplest $\{a_1=g, a_{n+1}=(g\cdot a_n)_{\mathrm{mod}\ m}\}$ are a minimal non-negative mutually prime residual system of m, therefore, they are pairwise non-equal. And, if $a_{\phi(m)}=1$ then $a_{\phi(m)}=1$ uniquely； if $a_{\phi(m)/2}=1$ then $a_{\phi(m)/2}=1$ uniquely.

Prove I. Simplest $\{a_1=g, a_{n+1}=(g\cdot a_n)_{\mathrm{mod}\ m}\}$ has $\phi(m)$ terms, therefore, $a_{\phi(m)}$ is the last term of the sequence of numbers in question.

$a_{\phi(m)}=(g^{\phi(m)})_{\mathrm{mod}\ m}=1$. Therefore, I holds.

Prove II. From m being an odd number we know that, $2 \mid \phi(m)$. From $\phi(m)=\delta_m(g)$ we know that, $2 \mid \delta_m(g)$.
From odd number $m>3$ we know that, $\phi(m)>2$, $\delta_m(g)>2$.
Let $c=\delta_m(g)/2$. From $2 \mid \delta_m(g)$ and $\delta_m(g)>2$ we know that, $1<c=\delta_m(g)/2<\delta_m(g)$.
From $c=\delta_m(g)/2(1<c<\delta_m(g))$ and IV in Corollary 7 we know that, $\delta_m(a_c)=2$.
From the definition of order we know that, $(a_c)^2\equiv 1 \pmod m$.
When m has a primitive root, congruent equation $x^2\equiv 1 \pmod m$ only has solution $x\equiv\pm 1 \pmod m$.
From $(a_c)^2\equiv 1 \pmod m$ we know that, $a_c\equiv\pm 1 \pmod m$.
From $a_c\equiv\pm 1 \pmod m$ and a_c being a term in simplest $\{a_1=g, a_{n+1}=(g\cdot a_n)_{\bmod m}\}$we know that, $a_c=1$ or $a_c=m-1$.
However, if $a_c=1$ then $\delta_m(a_c)=1$. Therefore, from $\delta_m(a_c)=2$ we know that, $a_c=m-1$.
From $\phi(m)=\delta_m(g)$ and $c=\delta_m(g)/2$ we know that, $a_{\phi(m)/2}=m-1$. Q.E.D.

Theorem 12. Suppose $m=p^k$(p is a prime number,$1<k$). Then , I. If $\delta_m(a) \mid p-1$ then $\delta_m(a)<m^{1/2}$. II. There necessarily exists $\delta_m(b) \nmid m-1$. III. If $3<p$ then there necessarily exists a such that m is a a-pseudo prime number (i.e., m is a type I pseudo prime number).

Proof: Prove I. From $\delta_m(a) \mid p-1$ we know that, $\delta_m(a)<p$. From $m=p^k(1<k)$ we know that, $p\leqslant m^{1/2}$.
From $\delta_m(a)<p$ and $p\leqslant m^{1/2}$ we know that, $\delta_m(a)<m^{1/2}$. Hence I holds.
Prove II. Suppose g is a primitive root of m. Thus, $\delta_m(g)=\phi(m)=\phi(p^k)=(p-1)p^{k-1}$. $1<p^{k-1}<\delta_m(g)$.
Let $c=p-1$. From $\delta_m(g)=(p-1)p^{k-1}$ we know that, $c=\delta_m(g)/p^{k-1}$.
From $c=\delta_m(g)/p^{k-1}(1<p^{k-1}<\delta_m(g))$ and IV in Corollary 7 we know that, $\delta_m(a_c)=p^{k-1}$.
Let $b=a_c$, $\delta_m(b)=p^{k-1}$. From $1<k$ we know that, $p^{k-1} \nmid p^k-1=m-1$, i.e., $\delta_m(b) \nmid m-1$. Hence II holds.
Prove III. From $\delta_m(g)=(p-1)p^{k-1}$ we know that, there necessarily exists $s=\delta_m(g)/(p-1)$, $1<s<\delta_m(g)$.
From $s=\delta_m(g)/(p-1)$ $(1<s<\delta_m(g))$ and IV in Corollary 7 we know that, $\delta_m(a_s)=p-1$.
From $m-1=p^k-1=(p-1)(p^{k-1}+p^{k-2}+\cdots+1)$ we know that,

$$\delta_m(a_s) \mid m-1 \qquad (13)$$

From $\delta_m(g)=\phi(m)$ and $s=\delta_m(g)/(p-1)$ we know that, $s\neq\phi(m)$. From I in Lemma 6 we know that, $a_s\neq 1$.
From $3<p$ and $s=\delta_m(g)/(p-1)$ we know that, $s\neq\phi(m)/2$. From II in Lemma 6 we know that, $a_s\neq m-1$.
Because 1 and $m-1$ are the minimal term and the maximal terms of the minimal non-negative mutually prime residual system of m (Simplest $\{a_1=g, a_{n+1}=(g\cdot a_n)_{\bmod m}\}$) respectively, from $a_s\neq 1$ and $a_s\neq m-1$ we know that,

$$1<a_s<m-1 \qquad (14)$$

Let $a=a_s$. From formulae (13) and (14) we know that, m is a a-pseudo prime number. That is, III holds. Q.E.D.
From the proof of Theorem 12 we know that,

Corollary 9. If $m=p^k$($3<p$ is a prime number, $1<k$) then there are $p-3$ a's such that $\delta_m(a) \mid m-1(1<a<m-1)$.

Theorem 13. Suppose $m=m_1m_2$, $(m_1,m_2)=1$. Then when $m_1y\equiv -2 \pmod{m_2}$, $x^2\equiv 1 \pmod m$ has solution $x\equiv\pm(m_1y+1) \pmod m$. Or, when $m_1y\equiv 2 \pmod{m_2}$, $x^2\equiv 1 \pmod m$ has solution $x\equiv\pm(m_1y-1) \pmod m$.

Proof: First, we prove that when $x\equiv\pm(m_1y+1) \pmod m$ and $m_1y\equiv -2 \pmod{m_2}$, then $x^2\equiv 1 \pmod m$.
From $x\equiv\pm(m_1y+1) \pmod m$ we know that, $x^2\equiv(m_1y+1)^2 \pmod m$.

$$x^2-1\equiv(m_1y+1)^2-1 \pmod m \qquad (15)$$

From $m_1y\equiv -2 \pmod{m_2}$ we know that, $m_1y+1\equiv -1 \pmod{m_2}$. And there necessarily exists integer q such that $m_1y+1=qm_2-1$.
Thus, $(m_1y+1)^2-1=(qm_2-1)^2-1=qm_2(qm_2-2)$, from which we know that, $m_2 \mid (m_1y+1)^2-1$.
Besides, $(m_1y+1)^2-1=m_1y(m_1y+2)$, from which we know that, $m_1 \mid (m_1y+1)^2-1$.
From $m_1 \mid (m_1y+1)^2-1$ and $m_2 \mid (m_1y+1)^2-1$ we know that, $[m_1, m_2] \mid (m_1y+1)^2-1$.
From $(m_1,m_2)=1$ we know that, $[m_1, m_2]=m_1m_2=m$. Thus, $m \mid (m_1y+1)^2-1$,

$$(m_1y+1)^2-1\equiv 0 \pmod m \qquad (16)$$

From formulae (15) and (16) we know that,$x^2-1\equiv 0 \pmod m$, $x^2\equiv 1 \pmod m$.
Likewise, we can prove that, when $x\equiv\pm(m_1y-1) \pmod m$ and $m_1y\equiv 2 \pmod{m_2}$, $x^2\equiv 1 \pmod m$. Q.E.D.
Now, we solve $x^2\equiv 1 \pmod m$.
I. Decompose modulo m into m_1 and m_2, such that $(m_1, m_2)=1$.
Ⅱ. Solve degree 1 congruent equation $m_1y\equiv -2 \pmod{m_2}$（or $m_1y\equiv 2 \pmod{m_2}$) regarding y.
Ⅲ. Let $y=(y)_{\bmod m_2}$. Finding m_1y+1（or m_1y-1）, we obtain $x\equiv\pm(m_1y+1) \pmod m$（or $x\equiv\pm(m_1y-1) \pmod m$).

Example 4. Solve $x^2\equiv 1 \pmod{105}$.

Solution. At this time $m=105$, which can be decomposed into : 3×35, 5×21, 7×15（satisfying "$(m_1, m_2)=1$"）.

Let m_1=35，m_2=3. From “$m_1y\equiv 2 \pmod{m_2}$” we obtain,

$$35y\equiv 2 \pmod 3$$
$$y \equiv 1 \pmod 3$$

Let y=1. From “m_1y-1” we obtain, $35\times 1-1=34$. Thus, $x^2\equiv 1 \pmod{105}$ has solution $x\equiv\pm 34 \pmod{105}$.

(Note: If we let m_1=3，m_2=35， the result is the same.)

Let m_1=21，m_2=5. From “$m_1y\equiv 2 \pmod{m_2}$” we obtain,

$21y \equiv 2 \pmod 5$

$y \equiv 2 \pmod 4$

Let y=2. From “m_1y-1” we obtain, $21\times 2-1=41$. Thus, $x^2\equiv 1 \pmod{105}$ has solution $x\equiv\pm 41 \pmod{105}$.

Likewise, let m_1=15，m_2=7 we can obtain, $x\equiv\pm 29 \pmod{105}$.

$x^2\equiv 1 \pmod{105}$ has 2^3=8 solutions in total, i.e., $x\equiv\pm 1$，± 34，± 41，$\pm 29 \pmod{105}$.

Obviously, when we let $x\equiv\pm 34$，± 41，$\pm 29 \pmod{105}$, $\delta_{105}(x)=2 \mid 105-1$.

Therefore, 105 is a pseudo prime number with 34,71,41,64,29,76 as its bases. （Note: 71=105-34. 64 and 76 are the same）.

It is not hard to discover that, when $m=p_1^{a1}\cdots p_1^{an}$， $p_1,\cdots,p_n(n>1)$ are distinct odd prime numbers, there are 2^{n-1} distinct $(x)_{\bmod m}$ $(2<(x)_{\bmod m}<m-1)$ such that $x^2\equiv 1 \pmod m$ holds. (Note: Here, $m>3$. Therefore, $(x)_{\bmod m}=2$ can not be a solution of $x^2\equiv 1 \pmod m$)

Conclusion 21. Suppose $m=p_1^{a1}\cdots p_1^{an}$， $p_1,\cdots,p_n(n>1)$ are distinct odd prime numbers. Then,there exist at least 2^n-2 distinct a such that m is an a-pseudo prime number (i.e., m is a type I pseudo prime number).

From Theorem 12 and III in Conclusion 21 we can obtain,

The sufficient condition for type I pseudo prime numbers: Suppose odd number $m>p$(p is a prime number greater than 3). If $p \mid m$ then m is a type I pseudo prime number. That is to say, all odd composite numbers are type I pseudo prime numbers except for $3^k(1<k)$.

Now, we give the sufficient and necessary condition for prime numbers.

Because, when odd number $m=p^k$(p is a prime number，$1<k$)， from II in Theorem 12 we know that, there necessarily exists $\delta_m(a) \nmid m-1$.

Besides, when $m=p_1^{a1}\cdots p_1^{an}$， $p_1,\cdots,p_n(n>1)$ are distinct odd prime numbers, there necessarily exists $1<a<m-1$ such that $\delta_m(a)=2$.

For odd composite numbers only the above tow cases hold. Thus, we have,

Sufficient and necessary condition for prime numbers. The sufficient and necessary condition for odd number m being a prime number is, for any $\delta_m(a)$ we have $\delta_m(a) \mid m-1$， and, if $1<a<m-1$ then $\delta_m(a)\neq 2$.

Definition for type II pseudo prime numbers.

Suppose $2 \mid \delta_m(p)$（p is a prime number）. We call the odd composite number m with $\delta_m(p) \mid m-1$，$p^{\delta m(p)/2}\equiv -1 \pmod m$ as type II pseudo prime number with p as the base, p-II type pseudo prime number for short.

Through verification, almost no 2-pseudo prime number the authors encounter is a 2-II type pseudo prime number except $2^{2^5}+1$. But facts show that there are probably infinitely many p–II type pseudo prime numbers.

Definition 22. Suppose there are 2k terms in simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\bmod m}\}$, we call the kth term a_k as the middle term of the sequence of numbers in question.

Now, we show some examples to expound the function of the middle terms to the factorization of the big numbers.

For example, the middle term a_6 in simplest $\{a_1=2, a_{n+1}=(2a_n)_{\bmod 45}\}$： 2,4 ,8,16,32, 19,38,31,17,34,23,1 is $a_6=19$.

(19-1, 45) = (18,45) =9，there is 9 | 45. At the same time, (19+1, 45) = (20, 45) =5 | 45.

Obviously, there is 45 =9×5.

Another example, the middle term a_{14} in simplest $\{a_1=2, a_{n+1}=(2a_n)_{\bmod 645}\}$： 2,4 ,8,16,32, 64,128,256,512,379,113,226,452,259,

518,391,137,274,548,451,257,514,383,121,242,484,323,1 is $a_{14}=259$.

(259-1,645) = (258,645) =3×43=129 | 645。(259+1,645) = (260,645) =5 | 645.

Obviously, there is 645=129×5.

When simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\bmod m}\}$ has middle term a_k, from Definition 22 we know that, $\delta_m(a)=2k$. From I in Corollary 7 we know that, $\delta_m(a_k)=2$. Therefore, $a_k^2\equiv 1 \pmod m$. From Theorem 13 and Example 4 we know that,

Conclusion 22. Suppose $a_k(1<a_k<m-1)$ is the middle term of simplest $\{a_1=a, a_{n+1}=(a\cdot a_n)_{\bmod m}\}$. Then there necessarily

$1<m_1=(a_k-1, m)$ and $1<m_2=(a_k+1, m)$ such that $m=m_1m_2$，$(m_1,m_2)=1$.

Note 2. The principle of Supposition

Here we give an important logical principle that must be abode by in mathematical proofs.

The principle of supposition: If the proposition *A* is necessarily true, then we cannot suppose it is false; if the proposition *A* is necessarily false, then we cannot suppose it is true.

When the proposition *A* being true (false) is proved logically (or by a fact), then we say that *A* is necessarily true (false), we also say that *A* is a conclusion or a theorem. The difference between a proposition and a conclusion lies in that, the former is a judgement whose truth value is unknown, while the latter is a judgement whose truth value is known. Therefore, to the former we can suppose it being true, we can also suppose it being false, while to the latter we cannot make the opposite supposition. (In fact, this is an alternative expression of the principle of supposition)

(Note: Because there is a fundamental difference between a proposition and a conclusion, their expressions should be different. For example, proposition I "6 can be divided by 3 exactly" corresponds to conclusion I "that 6 can be divided by 3 exactly is true"; proposition II "5 can be divided by 3 exactly" corresponds to conclusion II "that 5 can be divided by 3 exactly is false". But people are accustomed to omit "is true" and "is false". They usually express conclusion I as "6 can be divided by 3 exactly", express conclusion II as "5 cannot be divided by 3 exactly". Although these omissions usually do not result in misunderstanding, but we must not confuse the propositions with the conclusions.)

The correctness of the principle of suppositions is self-evident. For example, in the axiomatic system of number theory, we cannot suppose "3+2–5=1" or "3+2–5≠0". If we made such suppositions, we would obtain 0=1，0=*n* 和 0≠0，*n*≠*n* etc., so as to cause an unbearable chaos in the axiomatic system of number theory. Likewise, in the axiomatic system of Euclidean geometry we cannot suppose the sum of the three internal angles of a triangle not to equal to 180°， while in the axiomatic system of non-Euclidean geometry we cannot suppose the sum of the three internal angles of a triangle to equal to 180° etc.

Because there is no evidence showing that any *px+q* sequence of numbers has no equal terms, the condition "if $a_i=a_{i+k}$" in Lemma 4 does not violate the principle of supposition.

Note 3 Discussion on "list equation to solve application problems"

To answer the question that formula (10) has many characteristic solutions while Result 2 still holds, we need to answer the question why we can solve application problems by listing equations.

Let us investigate the contents of " list equations to solve the application problems" in middle school mathematics textbook. The application problems in middle school mathematics textbook have a common feature: for a given problem, one or more equations can always be listed corresponding to it. Therefore, the problem is called the listable equation problem.

When we list an equation corresponding to an application problem (or a listable equation problem), we face two objects. One is the application problem given (called the original problem), the other is the equation listed. Thus, two questions arise: 1. Why can the solution of the original problem be obtained by solving the equation listed? 2. Which solutions of the equation listed are the solutions of the original problem? In order to answer these questions, let us look at an example first.

Problem 1: The sum of the square of an integer and a positive integer equals 3, find out the two numbers.

Solution: Suppose the integer is x, the positive integer is y. According to the problem we can list

$$x^2+y=3 \qquad (17)$$

Here, Problem 1 is the original problem, equation (17) is the equation listed. At first glance, they are quite different. Yet, they refer to the same thing. Because *x* is supposed to be the integer, x^2 can be read as "the square of the integer". Likewise, *y* can be read as "the positive integer". Thus, equation (17) can be read as "the sum of the square of the integer and the positive integer equals 3". Hence we see that the original problem and the equation listed refer to the same thing, i.e., the equation listed is a re-description of the original problem. Thus we say that, the original problem and the equation listed are "identical" and call this fact "the principle of identity". The principle of identity tells us that, the finding of the solution of the original problem can be realized by finding the solution of the equation listed. This is the fundamental reason for "list equation to solve the application problems" being a classical mathematical method. .

Besides, from the angle of the equation listed, x and y in (17) can be any real number or complex number. But, in order for equation (17) and Problem 1 to refer to the same thing, x must be an integer, y must be a positive integer. Here, x and y are variables. The conditions set to variables x and y are called constraints. Precisely speaking, only all of the variables satisfy the constraints can the equation listed and the original problem refer to the same thing. Since in this case the two refer to the same thing, the solutions of the two are necessarily the same. The remaining thing for us to do is that we should make sure what kind of solutions are the solutions of the equations listed.

The so-called solution of an equation, formally speaking, is an assignment to its relevant variables. As to the equation listed, if the assignment to each variable satisfies the constraints of the variable in question, then the solution (called the effective solution or characteristic solution) is one whose variables of the equation listed satisfy the constraints. Thus, we know that all of the effective solutions of the equation listed are the solutions of the original problem.

Solving equation (17), we can obtain 3 effective solutions of the equation:

$$\begin{cases} x=1 \\ y=2, \end{cases} \quad \begin{cases} x=0 \\ y=3, \end{cases} \quad \begin{cases} x=-1 \\ y=2 . \end{cases}$$

It is not hard to verify that these effective solutions are all the solutions of Problem 1. And we have,

Result 2′. Problem 1 has solutions if and only if formula (17) has effective solutions.

Formula (17) has many effective solutions, while Result 2′ obviously holds. This proves that Result 2 holds. In fact, as to Result 2′ there is the problem of "which of the above 3 effective solutions is the one needed". Yet, this problem is irrelevant to whether Result 2′ holds or not. That is to say, which circular term in the $5x+1$ sequences of numbers does x of the characteristic solutions of formula (10) belongs to is irrelevant to whether Result 2 holds or not.

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, Mar.-Apr. 2021

[2]. Kenneth H. Rosen, Elementary Number Theory and Its Applications, Fifth Edition, Beijing: Pearson Education Asia Limited and China Machine Press, 2005

Ming Xian, et. al. "Px+q sequences of numbers and px+q infinite trees." *IOSR Journal of Mathematics (IOSR-JM)*, 18(2), (2022): pp. 01-35.