ABOUT ODD NUMBERS AGAIN

Witold A. Kossowski

C O N T E N T S

The author is an independent developer in the field of scientific calculation.
His e-mail address is perso@kossowski-witold.eu

Preface

My first idea for a title was “Odd numbers revisited” but I immediately found it risky.
So I chose a less provocative title to try to enter, without any reference, the garden of the number theory.

My goal was to paint a picture of odd numbers just after the act of their creation by **zero** and **the formula 2*i*+1** and to do it as simply as possible.
I think it is exciting and often useful to return to the source of any phenomenon and to observe, with no hurry, what is going on there.

In fact, the paper presents a model of organization of odd numbers with some consequences.
I hope the reader will find this approach interesting.

The model, introducing rather aquatic notions of streams and cascades, brings into relief a periodicity in so organized numbers.

There is defined generating cycle of an odd number and the length of the cycle, which is equal to a fraction of the Euler function and is much easier to determine.

At the occasion, there is also presented an efficient algorithm of calculation of the residue modulo m, another one of calculation of the greatest common divisor, the notions of smooth and sparkling numbers with a formula demonstrating, when a smooth number $2^e + 1$ is a product of a smooth and a sparkling number, etc.

Finally, there is presented the binary number system as a natural environment, in which the proposed model and the relative calculations become especially effective.

All utilized symbols are listed at the end of the paper.

1. Introduction

We will accept without question that every odd number can be written as $q = 2i + 1 = ab = g^2 - h^2$,
where $a,b \in Q$ and g, h do not belong simultaneously to Q or E which are respectively a set of odd positive integers and a set of even positive integers.
We will also accept that zero is an even number.

Definition 1.1
Let $\delta: Z^+ \to Q$ be defined by $\delta a = 2a+1$ and let
$\beta: Q \to Z^+$ be defined by $\beta q = (q - 1) / 2$.
Number βq will be called **a generator of *q*.**
Number δa will be called **a number generated by *a*.**

i successive applications of δ or β will be denoted by β^i and δ^i.
So $\beta^0 q = \delta^0 q = q$, $\beta^1 q = \beta q$ and $\delta^1 q = \delta q$.
We have also $\delta\beta q = \beta\delta q = q$.
As operators, both δ and β have the highest priority.

EXAMPLE
$\beta 39 = 19$ $\quad \delta^3 12 = 103$ $\quad \delta 10 + 1 = 22$

Axiom 1.1
For every odd number q there exist one, and only one even number s such that $q = \delta^i s$ and $s = \beta^i q$, $i \in N$.

Definition 1.2
Let denote $Q_1 = \{q: q = 4m + 1, m \in Z^+\}$
and $Q_3 = \{q: q = 4m + 3, m \in Z^+\}$.
Thus, Q_1 is the set of odd numbers generated by even numbers, while Q_3 is the set of odd numbers generated by odd numbers.
Consequently, $Q = Q_1 \cup Q_3$ and $Q_1 \cap Q_3 = \emptyset$.

Theorem 1.1
Consider $q = g^2 - h^2$.
For any $q \in Q_1$ g is odd and h even, while for any $q \in Q_3$ g is even and h odd.

Proof.
Let $g \in Q$, $h \in E$. Then $q = (2x+1)^2-(2y)^2 = 4x^2 +4x +1 - 4y^2 = 4(x^2 + x- y^2)+1 = 4i+1 \in Q_1$.
Let $g \in E$, $h \in Q$. Then $q = (2x)^2-(2y+1)^2 = 4x^2 - 4y^2 - 4y- 1 = 4(x^2 - y^2 - y- 1)+3 = 4i+3 \in Q_3$.

Theorem 1.2
Consider $q = ab$, where $a, b > 1$.
For any $q \in Q_1$ the generators βa, βb are simultaneously even or odd, while for any $q \in Q_3$ one of the generators βa, βb are even and the other odd.
So, for any $q = ab \in Q_1$ both a and b belong simultaneously to Q_1 or Q_3,
while for any $q = ab \in Q_3$ one of a,b belongs to Q_1 and the other to Q_3

Proof.
Let $\beta a = 2x$, $\beta b = 2y + 1$. Then $q = ab = (2\beta a +1)(2\beta b + 1) = 4(4xy + 3x + y) + 3 \in Q_3$
Let $\beta a = 2x$, $\beta b = 2y$. Then $q = ab = (2\beta a +1)(2\beta b + 1) = 4(4xy + x + y) + 1 \in Q_1$
Let $\beta a = 2x+1$, $\beta b = 2y +1$. Then $q = ab = (2\beta a +1)(2\beta b + 1) = 4(4xy + 3x + 3y+2) + 1 \in Q_1$.

2. About stones and twins

Theorem 2.1
If k can be written $k = i + j + 2ij = i + j\delta i = j + i\,\delta j$, then δk is a product of two numbers generated by i and j.
In the other terms, if $k = i + j + 2ij = i + j\delta i = j + i\,\delta j$, then $\delta k = \delta i \delta j$,
as well as, if $q = ab$, then $\beta q = \beta a + a\beta b = \beta b + b\beta a = \beta a + 2\beta a\beta b + \beta b$.

Proof. $\delta k = 2(i + j + 2ij)+1 = (2i + 1)\,(2j + 1) = \delta i \delta j$.
On the contrary, if $q = ab$, then
$q = (1/2) * (ab - 1) = (1/2) * (\,(2\beta a + 1)\,(2\beta b + 1) - 1) =$
$= \beta a + \beta b + 2\beta a\beta b = \beta a + a\beta b = \beta b + b\beta a$.

EXAMPLE.
147 = 21 * 7. As we can asily verify,
$\beta 147 = 73 = 10 + 21 * 3 = 3 + 7 * 10 = 10 + 2 * 10 * 3 + 3$.
But also 147 = 49 * 3.
Indeed, 73 = 24 + 49 * 1 = 1 + 3 * 24 = 24 + 2 * 24 * 1 + 1.

Definition 2.1
A number k, which cannot be written in the form $k = i + j + 2ij = i + j(2i + 1) = j + i(2j+1)$, where $i, j > 0$, will be called **a stone**.

The set of stones will be denoted by K.

EXAMPLE.
Stones are: 1, 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, …

Axiom 1.2
(a) Stones generate the primes.
(b) Every odd prime number is generated by a stone.
(c) For any stone i and for all successive $n \in Z^+$, we can obtain a sequence $q_n = \delta(i + n\delta i)$, where every term q_n can be divided by a prime number δi and by an odd number δn.
We will say that the numbers q_n are **"touched"** by a stone i.

Let us have a look at a graphic illustration (Fig.1-1) of the distribution of stones. White fields in the line marked by letter g represent the stones. The gray fields represent the generators of composite numbers. The prime twins are marked by the letter B, while every ~~B~~ marks the number that could be a prime twin if there was no the "destructive" touch of one or more stones.

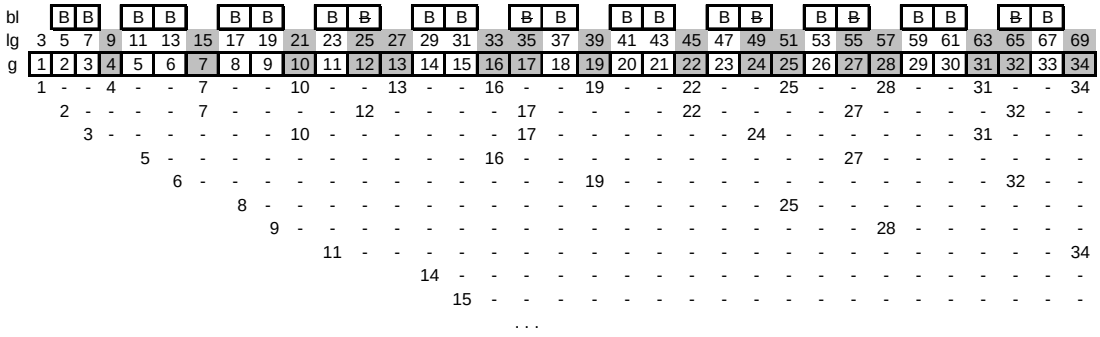

Figure 1-1 Graphic illustration of the distribution of stones
line g – generators
line lg – generated numbers
line bl – virtual twins

We can notice that stones are never touched by other numbers (if "stone" k was touched by stone i, we would have $k_n = i + n\delta i$ and every k_n would generate a number $\delta k_n = \delta i \delta n$ that is not prime).

Fig 1-1 corresponds to condensed Eratosthenes' sieve ("condensed" because there are no even numbers in the line lg), where instead of observing the "behavior" of odd numbers, we can concentrate ourselves on their generators.
There are some advantages in this approach. One of them is the disappearance of traditionally magic problem of prime twins' distribution.

Look at the Fig.1-2, where the actions of two stones, 1 and 2, have been isolated.
We can see that the first generator 1 (a stone) touches successively 4, 7, 10, 13, 16,.
The untouched numbers create the pairs <2,3> <5,6> <8,9> <11, 12> <14, 15> <17, 18> … .
These pairs generate the pairs of virtual prime twins <5,7> <11,13> <17,19> <23,25> <29,31> <35,37> … .
Without action of consecutive stones, as 2, 3, 5, 6, … , all the twin pairs could have a regular, entirely non-magic character.
But stone 2, with its cycle $\delta 2 = 5$, touches successively the terms of the sequence $k_n = 2 + 5n = 7, 12, 17, 22, \ldots$, which, among others, kills 25 in the virtual twin pair <23,~~25~~>, 35 in the virtual twin pair <~~35~~,37>, etc.

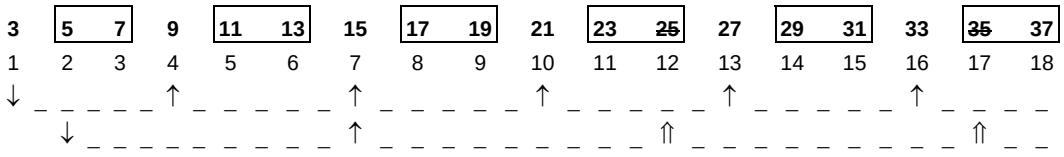

Figure 1-2. "Destruction" of virtual twins 25 and 35 by stone 2

The next stone 3 will touch successively 10, 17, 24, 31, 38, …, and will eliminate 35 in the virtual twin pair <~~35~~,37>, 49 in the virtual twin pair <47,~~49~~>, etc.

Let us look e.g. at twins <59,61> (Fig.1-1). They survive, because it does not exist any stone m such that $m + n\delta m = 29$ or 30. So 29 and 30 are stones and generate the twin pair <59,61>.

Following immediately the above reflection and Axiom 1.2, we can formulate Axiom 1.3, strictly concerning the pairs of twin primes:

Axiom 1.3
The integers q, q+2, form a pair of twin primes if and only if βq and βq+1 are stones, that is,
if there exist no $x \in$ N and $y \in$ N such that $\beta q = x + n\delta x$ and $\beta q+1 = y + m\delta y$, where $n, m \in$ N.
Note, that $\beta q+1 = \beta(q+2)$.

3. About streams

According to Axiom 1.1, for any odd number q there exists one and only one even number s such that $q = \delta^i s$ and $s = \beta^i q$, $i \in$ N.

Now, consider the infinite sequence of numbers, where the first term is generated by some even number s and any other term is generated by a preceding one.

Theorem 3.1
Let $i, j \in$ N and let $s \in$ E.
Let $a_i = \delta a_{i-1}$ be a term of the sequence with $a_1 = \delta s$.
Then
(a) $a_i = \delta^i s = (s+1)2^i - 1$
(b) $a_{i+j} = \delta^j a_i = (a_i + 1)2^j - 1$.

Proof.
(a) The proof is by induction.
Let S(i) denote the statement $a_i = \delta^i s = (s+1)2^i - 1$.
We have $a_1 = \delta s = 2s+1 = 2(s+1) - 1 = (s+1)2^1 - 1$.
Hence, S(1) is true.
Assume that for i>1, S(i) is true that is $a_i = \delta^i s = (s+1)2^i - 1$.
Now S(i+1) denotes $a_{i+1} = \delta(a_i) = (s+1)2^{i+1} - 1$.
Since $a_i = (s+1)2^i - 1$, it follows that $a_{i+1} = \delta((s+1)2^i - 1) = 2((s+1)2^i - 1) + 1 = (s+1)2^{i+1} - 2 + 1 = (s+1)2^{i+1} - 1$.
Therefore S(i+1) is true.
(b) It was required $s \in$ E to accentuate the role of the even source. In fact, according to the proof relative to (a), the state-ment $a_i = \delta^i s = (s+1)2^i - 1$ is true for any s, even or odd.
Let $s = a_i$. Then $a_{i+j} = \delta^j a_i = (a_i + 1)2^j - 1$.

Definition 3.1
We will call **a stream** and denote by T_s the sequence $a_i = \delta a_{i-1}$, where $a_1 = \delta s$ and $i \in$ N.
Number s will be called **a source** of the stream T_s.
The ith term of the stream T_s will be denoted by $T_s(i)$.
Stream T_s with its source will be called **complete stream** and denoted by $\underline{T}_s$.
The source s of the stream T_s will be also called **0th term** of the stream.
Every term $T_s(i)$ can be considered as **local source of substream** L_z.
The first term of the substream L_z equals $L_z(1) = T_s(i+1)$.
The substream L_z with its local source will be called **a complete substream** and denoted by $\underline{L}_z$.
Similar to the case of stream T_s, the local source of the substream L_z will be also called **0th term** of the substream.

EXAMPLE
streams:
T_0 = 1, 3, 7, 15, 31, 63, 127, … T_8 = 17, 35, 71, 143, 287, …

complete streams:
$\underline{T}_0$ = 0, 1, 3, 7, 15, 31, 63, … $\underline{T}_8$ = 8, 17, 35, 71, 143, …

substreams:
L_{15} = 31, 63, 127, 255, … L_{35} = 71, 143, 287, 575,…

complete substreams:
$\underline{L}_{15}$ = 15, 31, 63, 127, 255, … $\underline{L}_{35}$ = 35, 71, 143, 287…

Axiom 3.1
For any $z \in Q$ there is $L_z(i) = T_{m-1}(i+u)$,
where $z+1 = m2^u$, $m \in Q$.
(Yes, $L_z(i)=(z+1)2^i-1 = (m-1+1)*2^{i+u}-1=T_{m-1}(i+u)$.)

EXAMPLE
Consider $L_{23}(5) = 767$.
According to Axiom 3.1, $L_{23}(5) = T_2(8)$,
because if $L_{23}(5) = L_z(i)$, then $z+1 = 23 + 1 = 3*2^3 = m2^u$.
So $L_z(i) = T_{m-1}(i+u) = T_2(8)$.

Axiom 3.2
(a) The sequence $a_i = 2^i - 1$ is identical to the stream T_0, what becomes obvious when assignment $s = 0$ in the expression from Theorem 3.1.a.
(b) Consider an affine transformation
$T(x) = ax + b \pmod n$, $a \geq 1$, $(a, n) = 1$.
If $x_0 = 0$ and $b = 1$, we get a sequence
$0, 1, a + 1, a^2 + a + 1, a^3 + a^2 + a + 1, \ldots$,
called by Marsaglia [1] a "fundamental sequence".
The stream T_0 corresponds to the fundamental sequence with $a = 2$.

Axiom 3.3
(a) Every even number is a source of a stream.
(b) Every number belongs to only one stream.
(c) Every odd number q may be in a unique way determined by
- its generator,
- the source s and the position i in the stream T_s,
- the local source z and the position j in the substream L_z.

EXAMPLE
Consider the number $q = 3583$.
$q = 3583 = \delta 1791 = \delta^2 895 = \delta^3 447 = \delta^4 223 = \delta^5 111 = \delta^6 55 =$
$= \delta^7 27 = \delta^8 13 = \delta^9 6 = T_6(9)$.
But also, for example, $q = L_{111}(5)$ or $q = L_{55}(6)$.

Remarks concerning the notation:

To simplify the notation of a stream, we decided to utilize the sequence. It was, of course, possible to choose the concept of the set of pairs <position, number> as well.
- To note that $T_s(i)$ is a term of the stream T_s, we will simply write $T_s(i) \in T_s$.
- We will accept the convention: $T_s - n$ denotes the sequence T_s after subtracting n from every term, nT_s denotes the sequence T_s after multiplying every term by n, whereas, for example, $p \nmid T_s$ signifies that there are no terms divisible by p in the stream T_s.
- The remainder when q is divided by a, will be called a **residue of *q* modulo *a***, and denoted by $(q)_a$, e.g. $(19)_5$ or $(T_s(i))_a$.

The expression of Theorem 3.1 allows us to formulate immediately the following axiom:

Axiom 3.4
Consider s, $i \in Z^+$.
(a) Every number $T_s(i) + 1$, is divisible by $s+1$ and $T_0(i)+1$.
(b) Every number $T_s(i) - s$, is divisible by $s+1$ and $T_0(i)$.
(c) If $a \mid (s+1)$, then $a \mid (T_s(i) - (a-1))$.
(Yes, if $s + 1 = na$, then $T_s(i) - (a-1) = (s + 1)2^i - a = na2^i - a = a(n2^i - 1)$).
(d) For every $T_s(i)$, we have
$T_s(i) - s - k(s + 1) = (s + 1)(T_0(i) - k)$.
(Yes, $T_s(i) - s - k(s + 1) = (s+1)2^i - 1 - s - k(s+1) = (s+1)2^i - (s+1) - k(s+1) = (s+1)(\underline{T}_0(i) - k)$.)
(e) If a is a non-trivial divisor of $q = T_s(i)$, then, according to (a), $(T_{a-1}(j) + 1 - q)_a = 0$, $j \geq 0$.
Thus when we want to know whether a divides q, it is sufficient to take some $T_{a-1}(j)$, possibly near to q, to calculate $d = T_{a-1}(j) + 1 - q$ and verify whether $(d)_a = 0$.
(f) If $s+1 = p_1^{c1} p_2^{c2} \ldots p_n^{cn} 2^u$, where $p_1, p_2, \ldots, p_n$ are prime numbers, then there are no terms divisible by any of $p_1, p_2, \ldots, p_n$ in the stream $\underline{T}_s$ or in the stream containing the substream $\underline{L}_s$.
(Yes, according to (a), any of $p_1, p_2, \ldots, p_n$ divides $T_s + 1$; so for every p_i from the set $\{ p_1, p_2, \ldots, p_n \}$ we have $T \equiv p_i - 1 \pmod{p_i}$.)

EXAMPLE.
- According to Axiom 3.4.a, all terms of the stream $\underline{T}_6+1$ are divisible by 7.
(Yes, the terms $\underline{T}_6 + 1 = 7, 14, 28, 56, 112, 224, 448, 896, 1792, \ldots$ are divisible by 7.)
- According to Axiom 3.4.b, all terms of the stream $\underline{T}_6-6$ are divisible by 7.
- According to Axiom 3.4.c, all terms of the stream $\underline{T}_{20}-6$ are divisible by 7.
- According to Axiom 3.4.d all terms of the stream $\underline{T}_6-6-2*7$ are divisible by 7.
- Find any divisor of 55, using Axiom 3.4.e.
Let us start with $a = 3$.
Does $a = 3$ divide 55? Let us take $T_{a-1}(j) = T_2(4) = 47$.
$d = \text{abs}(47 + 1 - 55) = 7$ is indivisible by 3, so 3 does not divide 55.
Does $a = 5$ divide 55? Let us take $T_{a-1}(j) = T_3(4) = 39$.
$d = \text{abs}(39 + 1 - 55) = 15$ is divisible by 5, so 5 divides 55.
- Consider the complete stream $\underline{T}_{32} = 32, 65, 131, 263, 527, 1055, 2111, 4223, \ldots$.
According to Axiom 3.4.f, we can immediately say that there are no terms divisible by 3 or 11 in $\underline{T}_{32}$,
i.e. $3 \nmid T_{32}$ as well as $11 \nmid T_{32}$.

On the basis of Axiom 3.4.e, we can construct an elegant algorithm of calculating $(q)_a$, $a < q = T_s(i)$, without any division.
Instead of testing of $(d)_a = 0$, we can determine for eve-ry d_k, the new $T_{a-1}(j)$, as near as possible, calculate d_{k+1}, and repeat the procedure as long as $d_n > a$.

Finally, we obtain $d_n = a$, and then $(q)_a = 0$, or $d_n < a$, and then $(q)_a \neq 0$.
To simplify the presentation of the algorithm, we will search only $T_{a-1}(j) < d_k$..

Algorithm 3.1
Given a number $q = T_s(i)$ and $a \in Q$, $1 < a < q$.
We want to determine $(q)_a$.

0. initialize d:=q.
1. find maximal $T_{a-1}(j) < d$, where $j \geq 0$
2. determine d:= $d - (T_{a-1}(j) + 1)$
3. if $d > a$, then come back to 1
4. if $d = a$, then print "$q \equiv 0$ (mod a)" and terminate
5. if $d < a$, then print "$q \equiv d$ (mod a)" and terminate

Remark 3.1. Obviously, it would be possible to search maximal $a2^j < d$ (by the way, $a2^j = T_{a-1}(j) + 1$), but determining $T_{a-1}(j) < d$ is extremely easy in a binary notation, because, as we will see it in chapter 4, $T_{a-1}(j)$ is a concatenation of a-1 and of j ones.
Remark 3.2. Of course, we can apply the algorithm 3.1 to calculate $(p)_a$, where $p \in E$, $a \in Q$.
In such case we can apply $q = p - 1$ and adapt the points 3, 4, 5.
Remark 3.3. The algorithm 3.1 always provides $d = a$ or $d < a$ in a finite number of steps.
To prove it, let us accept the obvious assumption that for any $q = T_s(i) > 1$ there exist $a \in Q$ and $j \geq 0$ such that $T_{a-1}(j) < d$.
The difference $d = q - (T_{a-1}(j) + 1)$ takes a value from the range $1...T_{a-1}(j)$.
$d = T_{a-1}(j)$ when and only when a-1=s and j=i-1, because
$q - (T_{a-1}(j) + 1) = T_s(i) - (T_s(i\text{-}1) + 1) =$
$= 2T_s(i\text{-}1) + 1 - (T_s(i\text{-}1) + 1) = T_s(i\text{-}1) = T_{a-1}(j)$.
$d = 1$ when and only when $q = T_{a-1}(j) + 2$, because
$q - (T_{a-1}(j) + 1) = T_{a-1}(j) + 2 - (T_{a-1}(j) + 1) = 1$.
This signifies that there exist only one number $T_{a-1}(j)$ and in consequence one a, causing $d = 1$.
From here, or d is not greater than a, what terminates the algorithm, either greater than a but reduced at every step and finally falling to the range $1 \ldots a$.
According to Axiom 3.4.a, for any $T_{a-1}(j)$ there is $(T_{a-1}(j) + 1)_a = 0$ and thus every consecutive d is congruent to q modulo a.

EXAMPLE of application of the algorithm 3.1
Calculate $(536187)_{487}$. So $q = 536187$, $a = 487$

0. $d = 536187$.
1. $T_{a-1}(j) = T_{486}(10) = 498687 < d$
2. d:= $536187 - (498687 + 1) = 37499$
3. $d > a$ ➔ **1**

1. $T_{486}(6) = 31167 < d$
2. d:= $37499 - (31167 + 1) = 6331$
3. $d > a$ ➔ **1**

1. $T_{486}(3) = 3895 < d$
2. d:= $6331 - (3895 + 1) = 2435$
3. $d > a$ ➔ **1**

1. $T_{486}(2) = 1947 < d$
2. d:= $2435 - (1947 + 1) = 487$
3. d is not greater then a
4. $d = a$, print "$536187 \equiv 0$ (mod 487)" and terminate.

The calculating of $(536187)_{487}$ has been reduced here to four searching of the terms $T_{486}(k) < d$, four subtractions and five comparisons. All of that is especially easy in the binary system.

It is easy to transform Algorithm 3.1 to the algorithm of determining the greatest common divisor of two num-bers.

Algorithm 3.2
Given two numbers $n = T_s(i)$ and $m = T_t(j)$, $n > m$.
We want to determine the greatest common divisor (n, m).

0. substitute q:= n, a:= m
1. apply Algorithm 3.1
2. if $d \in E$, that is if $d = w2^u$, $w \in Q$, then d := w
3. if $d = a$, then print "$(n, m) = d$" and terminate
4. if $d = 1$, then print "$(n, m) = 1$" and terminate
5. substitute q:= a, a:= d and come back to 1

EXAMPLE of application of the algorithm 3.2
Calculate (2013, 231). So $n = 2013$, $m = 231$

0. q:= 2013, a := 231
1. Algorithm 3.1 terminated, $d = 66$
2. $d \in E$, that is, if $d = 33*2^1$, then d := 33
3. $d \neq a$
4. $d \neq 1$
5. q:= 231, a:= 33 ➔ **1**

1. Algorithm 3.1 terminated : $d = 33$
2. $d = a$, print "(2013, 231) = 33" and terminate.

EXAMPLE
Calculate (2013, 233). So $n = 2013$, $m = 233$

0. q:= 2013, a := 233
1. Algorithm 3.1 terminated, $d = 149$
2. $d \notin E$
3. $d \neq a$
4. $d \neq 1$
5. q:= 233, a:= 149 ➔ **1**

1. Algorithm 3.1 terminated : $d = 84$
2. $d \in E$, that is, if $d = 21*2^2$, then d := 21
3. $d \neq a$
4. $d \neq 1$
6. q:= 149, a:= 21 ➔ **1**

1. Algorithm 3.1 terminated : $d = 2$
2. $d \in E$, that is, if $d = 1*2^1$, then d := 1
3. $d \neq a$
4. $d = 1$, print "(2013, 233) = 1" and terminate

There was said in the definition 1.2 that all numbers belonging to Q_1 are generated by even numbers, while all numbers generated by odd generators belong to Q_3.
This signifies that $T_s(1)\in Q_1$ and $T_s(i>1)\in Q_3$, for every $s\in E$.

So, every second odd number has a form $T_s(1)$, and in the table, where successive lines correspond to successive streams, as in Fig.3-1, all numbers, belonging to Q_1, find themselves in the column 1.

stream	source	pos. *i*														
		1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	...
T_0	0	1	3	7	15	31	63	127	255	511	1023	2047	4095	8191	16383	...
T_2	2	5	11	23	47	95	191	383	767	1535	3071	6143	12287	24575	49151	...
T_4	4	9	19	39	79	159	319	639	1279	2559	5119	10239	20479	40959	81919	...
T_6	6	13	27	55	111	223	447	895	1791	3583	7167	14335	28671	57343	114687	...
T_8	8	17	35	71	143	287	575	1151	2303	4607	9215	18431	36863	73727	147455	...
T_{10}	10	21	43	87	175	351	703	1407	2815	5631	11263	22527	45055	90111	180223	...
T_{12}	12	25	51	103	207	415	831	1663	3327	6655	13311	26623	53247	106495	212991	...
T_{14}	14	29	59	119	239	479	959	1919	3839	7679	15359	30719	61439	122879	245759	...
T_{16}	16	33	67	135	271	543	1087	2175	4351	8703	17407	34815	69631	139263	278527	...
T_{18}	18	37	75	151	303	607	1215	2431	4863	9727	19455	38911	77823	155647	311295	...
T_{20}	20	41	83	167	335	671	1343	2687	5375	10751	21503	43007	86015	172031	344063	...
T_{22}	22	45	91	183	367	735	1471	2943	5887	11775	23551	47103	94207	188415	376831	...
T_{24}	24	49	99	199	399	799	1599	3199	6399	12799	25599	51199	102399	204799	409599	...
T_{26}	26	53	107	215	431	863	1727	3455	6911	13823	27647	55295	110591	221183	442367	...
T_{28}	28	57	115	231	463	927	1855	3711	7423	14847	29695	59391	118783	237567	475135	...
T_{30}	30	61	123	247	495	991	1983	3967	7935	15871	31743	63487	126975	253951	507903	...
T_{32}	32	65	131	263	527	1055	2111	4223	8447	16895	33791	67583	135167	270335	540671	...
T_{34}	34	69	139	279	559	1119	2239	4479	8959	17919	35839	71679	143359	286719	573439	...
T_{36}	36	73	147	295	591	1183	2367	4735	9471	18943	37887	75775	151551	303103	606207	...
T_{38}	38	77	155	311	623	1247	2495	4991	9983	19967	39935	79871	159743	319487	638975	...
T_{40}	40	81	163	327	655	1311	2623	5247	10495	20991	41983	83967	167935	335871	671743	...
T_{42}	42	85	171	343	687	1375	2751	5503	11007	22015	44031	88063	176127	352255	704511	...
T_{44}	44	89	179	359	719	1439	2879	5759	11519	23039	46079	92159	184319	368639	737279	...
T_{46}	46	93	187	375	751	1503	3007	6015	12031	24063	48127	96255	192511	385023	770047	...
T_{48}	48	97	195	391	783	1567	3135	6271	12543	25087	50175	100351	200703	401407	802815	...
T_{50}	50	101	203	407	815	1631	3263	6527	13055	26111	52223	104447	208895	417791	835583	...
T_{52}	52	105	211	423	847	1695	3391	6783	13567	27135	54271	108543	217087	434175	868351	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Figure.3-1. The table of streams

It can be seen that every stream contains one number belonging to Q_1 and infinite number of numbers belonging to Q_3. Of course, in every even quantity of successive odd numbers, the number of both forms is identical.

Theorem 3.2
Consider $a, b\in Q$.
(a) If a and b belong simultaneously to Q_1 or Q_3, then the product $ab = T_s(1)\in Q_1$, where $s = \beta(ab)$.
(b) If one of a,b belongs to Q_1 and another one to Q_3, then $ab = T_s(i>1)\in Q_3$, where $s = \beta^i(ab)$.
(c) For any $a\in Q$, there is $a^2 = T_s(1)\in Q_1$, where $s = \beta(a^2) = (a+1)(a-1)/2$.

Proof.
According to the definition 1.2, if $a = 4m + 1$ then $a\in Q_1$, while if $a = 4m + 3$ then $a\in Q_3$.
(a) Let $a\in Q_1$ and $b\in Q_1$. So, $a = 4m + 1$ and $b = 4n + 1$.
Then $ab = 16mn + 4m + 4n + 1 = 4w + 1 \in Q_1$.
Let $a\in Q_3$ and $b\in Q_3$. So, $a = 4m + 3$ and $b = 4n + 3$.
Then $ab = 16mn + 12m + 12n + 9 = 4w + 1 \in Q_1$.
(b) Let $a\in Q_1$ and $b\in Q_3$. So, $a = 4m + 1$ and $b = 4n + 3$.
Then $ab = 16mn + 12m + 4n + 3 = 4w + 3 \in Q_3$.
(c) See (a).

Remark 3.4
There exists a hypothesis [2] that there is more prime numbers in Q_3 than in Q_1.
This can be explained, at least partially, by the fact that, according to Theorem 3.2.c, if only $a^2 \in Q$, then $a^2 \in Q_1$.
At the same time, as it was said above, in every even quantity of successive odd numbers, exactly a half of them belongs to Q_1 and another half to Q_3.

We will define now the notion of cascade, as a column in the table from Fig.3-1.

Definition 3.2
We will call **a cascade *i***, and denote by $K(i)$, the sequence composed of $T_s(i)$ for all consecutive sources s.
The s^{th} term of the cascade $K(i)$ will be denoted by $K_s(i)$.
Thus $K_s(i) = T_s(i)$, where $K_s(i) \in K(i)$ and $T_s(i) \in T_s$.

EXAMPLE
Cascade 5 is a sequence
$K(5) = T_0(5), T_2(5), T_4(5), T_6(5), T_8(5), T_{10}(5), T_{12}(5), \ldots$
$= 31, 95, 159, 223, 287, 351, 415, \ldots$
The term $K_4(3) = T_4(3)$.

Axiom 3.5.
Let $j \geq i$.
It is easy to verify that the distance
- between two terms of a stream is
  $h_s(i, j) = T_s(j) - T_s(i) = (s + 1)2^i (2^{j-i} - 1)$
- between two consecutive terms of a stream is
  $h_s(i) = T_s(i+1) - T_s(i) = (s + 1)2^i$
- between two terms of a cascade is
  $v_{t,s}(i) = K_t(i) - K_s(i) = (t - s)2^i$
- between two consecutive terms of a cascade is
  $v_s(i) = K_{s+2}(i) - K_s(i) = 2^{i+1}$.

Axiom 3.6
Let $\underline{T}_s(i) \equiv m_i \pmod q$.
Then, $\underline{T}_s(i+1) \equiv \delta m_i \pmod q$,
as well as, $\underline{T}_s(i+k) \equiv \delta^k m_i \pmod q$.
So, instead of determining all the $(T_s(i))_q$, we can find $(s)_q$ and generate consecutive elements modulo q.

Definition 3.3
Consider $q \in Q$.
Let δ_q: $Z^+ \to Z^+$ be defined by $\delta_q a = (\delta a)_q = (2a+1)_q$.
Number $\delta_q a$ will be called **a number generated by *a* modulo *q*.**
i successive applications of δ_q will be denoted by $\delta_q^{\,i}$.
Let β_q: $Z^+ \to Z^+$ as $\beta_q a = ((a - 1)/2)_q$ for any $a \in Q$ and $\beta_q a = ((a+q-1)/2)_q$ for any $a \in E$.
i successive applications of β_q will be denoted by $\beta_q^{\,i}$.

Theorem 3.3
Let $q \in Q$ and $q > 1$.
Number $q-1$ generates itself modulo q, that is,
$\delta_q(q-1) = q-1$.
Number $q-1$ is the only number smaller than q, possessing this property.

Proof.
Let us assume that there exists a positive number $d < q$ such that $\delta_q(q - d) = q - d$.
Let $q - d < \beta q$, that is, $d > (q+1)/2$.
In such a case, it would be $\delta_q(q - d) = 2q - 2d + 1 = q - d$, then $d = q + 1$, what is impossible, because $d < q$ was assumed.
Let, in turn, $q - d \geq \beta q$, that is, $d \leq (q+1)/2$.
It would be $\delta_q (q - d) = (2q - 2d + 1)_q = q - 2d + 1 = q - d$, then $d = 1$ would be the only solution.
Let us verify: $\delta(q-1) = 2q - 1 \equiv q - 1 \pmod q$.

EXAMPLE
$\delta_5 3 = 2$ because $\delta 3 = 7 \equiv 2 \pmod 5$
$\delta_{21} 5 = 11$
$\delta_{71} 70 = 70$

And, on the contrary, we will note:
$\beta_5 2 = 3$ because $((2 + 5) - 1)/2 = 3$
$\beta_{21} 11 = 5$ because $(11 - 1)/2 = 5$
$\beta_{71} 70 = 70$

Axiom 3.7
Consider $q \in Q$.
(a) Both $\delta_q a$ and $\beta_q a$ are one-to-one functions for all $a \leq q$.
(b) Consider $x < q$.
When $\delta x > q$, then $\delta_q x$ is always even.
So, if $x > \beta q$, then $\delta_q x = 2(x - \beta q)$.
(Indeed, $2(x - \beta q) = 2(x - (q - 1)/2) = 2x + 1 - q \in E$.)
(c) Referring to (a), it is apparent that starting successive generations modulo q from x, we obtain the number x at the latest after q-1 steps, where q-1 is a number of elements in the residue class mod q, reduced by 1, because $\delta_q(q-1) = q-1$.
(d) If we start the generation modulo q from zero, then
- generating sequence is periodically congruent modulo q to the stream T_0, with a period j, that is, $(A)_q \subset\subset (\underline{T}_0)_q$ and $\delta_q^{\,kj} 0 = 0$, $k \in N$,
- consequently, for any odd number q there exist the term $\underline{T}_0(j)$ such that $q \mid \underline{T}_0(kj)$ and that $j \leq q-1$,
- j determines the smallest $\underline{T}_0(j)$ divisible by q,
- terms $T_0(kj)$, $k \in N$ are the only terms of the stream $\underline{T}_0$ divisible by q
- if $T_0(j) = mq$, then, according to Theorem 1.2, if $q \in Q_1$ then $m \in Q_3$, and, on the contrary, if $q \in Q_3$ then $m \in Q_1$.

Definition 3.4
Consider $q \in Q$.
We will call **a stream T_s modulo q** and denote by $(T_s)_q$ the sequence of residues of all consecutive terms $T_s(i)$ modulo q.

EXAMPLE
$(\underline{T_2})_{21} = 2, 5, 11, 2, 5, 11, 2, 5, 11, 2, 5, 11, 2, 5, 11, 2, 5, \ldots$
$(\underline{T_2})_5 = 2, 0, 1, 3, 2, 0, 1, 3, 2, 0, 1, 3, 2\ldots$

Definition 3.5
Consider $a,q \in Q$, $a < q$.
We will call **a loop modulo q of number a** and denote by $\Theta(a)_q$ a finite sequence of numbers, with a as one of terms, where every term is generated modulo q by its predecessor and the first term is generated by the last.
The number of terms of the loop $\Theta(a)_q$ will be called **a length of the loop $\Theta(a)_q$** and denoted by $le\Theta(a)_q$.

Important: One can observe that the position of the number a in the loop is not of importance, under condition of keeping up the order in the circular sense.
So, if any $x \in \Theta(a)_q$, then $\Theta(a)_q = \Theta(x)_q$.

Definition 3.6
Consider $q \in Q$.
We will call **a generating cycle Γ_q of number q** the finite sequence composed of first n terms of the complete stream $(\underline{T_0})_q$, where n is the least number such that $(T_0(n))_q = 0$.
The **i^{th} term of generating cycle** Γ_q will be denoted by $\Gamma_q(i)$.
We will call **a length of generating cycle of number q** and denote by $le\Gamma_q$, the number of terms of the cycle.
We will call **the set of dead sources of number q** and denote by Ψ_q the set of all even numbers less than q and not belonging to the cycle generating Γ_q.

Commentary to definition 3.6
- Note that though the generating cycle Γ_q contains n first terms of $(\underline{T_0})_q$, the term $(T_0(n))_q$ does not belong to the cycle Γ_q. It is so, because the stream $\underline{T_0}$ is a complete one, and the first of n terms is the source $s = 0$, that is, the 0^{th} term of the stream.
- The first term of the cycle Γ_q of any q is zero, and the last is βq.

EXAMPLE
loops modulo q of number a:
$\Theta(2)_{21} = \Theta(5)_{21} = \Theta(11)_{21} = 2, 5, 11 = 5, 11, 2 = 11, 2, 5$
$le\Theta(2)_{21} = 3$

$\Theta(14)_{15} = 14$
$le\Theta(14)_{15} = 1$ (see Theorem 3.3)

cycles Γ_s and sets of dead sources Ψ_q:
$\Gamma_{21} = 0, 1, 3, 7, 15, 10$
$le\Gamma_{21} = 6$
$\Psi_{21} = \{2, 4, 6, 8, 12, 14, 16, 18, 20\}$

$\Gamma_{23} = 0, 1, 3, 7, 15, 8, 17, 12, 2, 5, 11$
$le\Gamma_{23} = 11$
$\Psi_{23} = \{4, 6, 10, 14, 16, 18, 20\}$

$\Gamma_{19} = 0, 1, 3, 7, 15, 12, 6, 13, 8, 17, 16, 14, 10, 2, 5, 11, 4, 9$
$le\Gamma_{19} = 18$
$\Psi_{19} = \{18\}$

Axiom 3.8
Consider $q \in Q$.
(a) There are no two identical terms in one loop.
A number $a < q$ is a term in only one loop modulo q.
(b) Every loop modulo q has a length from the range $1\ldots q\text{-}1$.
The length 1 has exclusively the loop $\Theta(q\text{-}1)_q$.
(c) The set of the terms of the loops modulo q of all dead sources, constitutes the completion of the cycle Γ_q to the set $\{0,.., q-1\}$. In other words, q is a sum of the lengths of all distinct loops modulo q, including the generating cycle Γ_q.
(d) The set of terms of loops modulo q of all dead sources does not contain any term of the stream $\underline{T_0}$. The terms of $\underline{T_0}$ appear exclusively in the generating cycle Γ_q, and the greatest of them, $T_0(j) \le q$, is equal to $[\log_2(q+1)]$.
(e) If in the sequence $(\underline{T_s})_q$ there is at least one term belonging to generating cycle Γ_q, then there are exclusively the terms of generating cycle Γ_q, in the order proper to Γ_q.
There is $\Gamma_q \subset\subset (\underline{T_s})_q$.
On the contrary, if in the sequence $(\underline{T_s})_q$ there is at least one term n belonging to the loop modulo q of any dead source, then there are exclusively the terms of the loop $\Theta(n)_q$ in the order proper to the loop.
There is $\Theta(n)_q \subset\subset (\underline{T_s})_q$.

Definition 3.7
(a) A number $q_{li}(d,j) = 2^{jd} + 2^{(j-1)d} + \ldots + 2^{3d} + 2^{2d} + 2^d + 1$, $j \in N$, will be called **a smooth number**.
(b) A number
$q_{br}(d,j) = 2^{jd} - 2^{(j-1)d} + \ldots + 2^{4d} - 2^{3d} + 2^{2d} - 2^d + 1$,
$j \in E$, will be called **a sparkling number**.

EXAMPLE
$4681 = q_{li}(3,4) = 2^{12} + 2^9 + 2^6 + 2^3 + 1$ is a smooth number.
$3641 = q_{br}(3,4) = 2^{12} - 2^9 + 2^6 - 2^3 + 1$ is a sparkling number.
Every $T_0(i) > 1$ is a smooth number, just because $T_0(i) = 2^i - 1 = 2^{i-1} + 2^{i-2} + \ldots + 1 = q_{li}(i\text{-}1,1)$.

We will show now that for any number $2^e + 1$ there exist the non-trivial divisors if e has an odd non-trivial divisor.

Lemma 3.1
If $j \in E$, then
$2^{(j+1)d}+1=(2^d+1)(2^{jd}-2^{(j-1)d}+\ldots+2^{4d}-2^{3d}+2^{2d}-2^d+1)$.
In other words, the smooth number $q=2^e+1$, where e has an odd non-trivial divisor, is a product of two non-trivial numbers, a smooth one and a sparkling one.

Proof.
Let us multiply the sparkling number $2^{jd}-2^{(j-1)d}+\ldots+2^{2d}-2^d+1$, $j \in E$, by a smooth number 2^d+1.
We get $(2^d+1)(2^{jd}-2^{(j-1)d}+\ldots+2^{4d}-2^{3d}+2^{2d}-2^d+1)=$
$=2^{(j+1)d}+2^{jd}-2^{jd}-2^{(j-1)d}+2^{(j-1)d}+\ldots-2^{3d}+2^{3d}+2^{2d}-2^{2d}-2^d+2^d+1=2^{(j+1)d}+1$.

EXAMPLE
$2^{10}+1=2^{5*2}+1=2^{(4+1)2}+1=(2^2+1)(2^8-2^6+2^4-2^2+1)$.
$2^5+1=2^{(4+1)*1}+1=(2^1+1)(2^4-2^3+2^2-2^1+1)$.

Theorem 3.4
(a) A smooth number $q_{li}(le\Gamma_a, a-1)$ is divisible by a and indivisible by a^2.
A smooth number $q_{li}(kle\Gamma_a, a-1)$, $k \in N$, is divisible by a.
(b) A smooth number $T_0(ale\Gamma_a)$ is divisible by a^2, as well as the smallest term of T_0 divisible by a^2 and indivisible by a^k, $k>2$.
(c) A smooth number $T_0(a^{n-1}le\Gamma_a)$ is divisible by a^n, as well as the smallest term of T_0 divisible by a^n and indivisible by a^k, $k>n$.

Proof.
Let us denote $d=le\Gamma_a$.
We know that $2^{dj}-1=(2^d-1)(2^{(j-1)d}+2^{(j-2)d}+\ldots+2^{2d}+2^d+1)$ and that, according to Axiom 3.7, $T_0(d)=na$ is the smallest term of the stream T_0 divisible by a.
(a) Consider $q_{li}(d,a-1)=2^{(a-1)d}+2^{(a-2)d}+\ldots+2^{2d}+2^d+1$.
We will add and subtract $a-1$ from the right side:
$q_{li}(d,a-1)=$
$=(2^{(a-1)d}-1)+(2^{(a-2)d}-1)+\ldots+(2^{2d}-1)+(2^d-1)+1+a-1=$
$=(2^{(a-1)d}-1)+(2^{(a-2)d}-1)+\ldots+(2^{2d}-1)+(2^d-1)+a$.
We get $(q_{li}(d,a-1))_a=0$.

To show that $q_{li}(d,a-1)$ is indivisible by a^2 we will prove that $q_{li}(d,a-1)/a$ is indivisible by a.
Let us rewrite $q_{li}(d,a-1)=(2^{(a-1)d}-1)+(2^{(a-2)d}-1)+\ldots+(2^{2d}-1)+(2^d-1)+a$ as follows:
$q_{li}(d,a-1)=(2^{(a-2)d}-1)(2^d-1)+(2^{(a-3)d}-1)(2^d-1)+\ldots+(2^d-1)(2^d-1)+(2^d-1)+a$.
Since $T_0(d)=2^d-1=na$, we can denote by v an expression
$v=q_{li}(d,a-1)/a=n(2^{(a-2)d}+\ldots+2^{2d}+2^d+1)+n(2^{(a-3)d}+\ldots+2^{2d}+2^d+1)+\ldots+n(2^d+1)+n+1$.
Now, we will divide both sides by n, keep the brackets and, inside every pair of brackets, we will add and subtract consecutively $a-2$, $a-3$, $a-4$, …, 1:
Thus $v/n=(2^{(a-2)d}+\ldots+2^{2d}+2^d+1)+(2^{(a-3)d}+\ldots+2^{2d}+2^d+1)+\ldots+(2^d+1)+1+1/n=$
$=(2^{(a-2)d}-1+\ldots+2^{2d}-1+2^d-1+1+a-2)+(2^{(a-3)d}-1+\ldots+2^{2d}-1+2^d-1+1+a-3)+\ldots+(2^d-1+1+1)+1+1/n=$
$=(2^{(a-2)d}-1+\ldots+2^{2d}-1+2^d-1)+(2^{(a-3)d}-1+\ldots+2^{2d}-1+2^d-1)+\ldots+(n+1)/n+a-1+a-2+\ldots+2+1+1/n=$
$=1*(2^{(a-2)d}-1)+2*(2^{(a-3)d}-1)+\ldots+(a-2)(2^d-1)+1/n+(1+2+\ldots+(a-1))$.
Note now that for any $x \in Q$, the sum $1+2+\ldots+(x-2)+(x-1)$ is divisible by x.
Hence, all parts of v/n, except for $1/n$, are divisible by a and we get $v/n=ma+1/n$.
We will multiply now the both sides n, what results in $v_a=(mna+1)_a=1$, what proves, in turn, that $q_{li}(d,a-1)$ is indivisible by a^2.

A smooth number $q_{li}(d,a-1)$, $k \in N$ is divisible by a, because it is divisible by $T_0(le\Gamma_a)$ and , according to Axiom3.7, $T_0(le\Gamma_a)$ is the smallest term of T_0 divisible by a.

(b) The truth of (b) immediately follows from (a).
We have $T_0(ad)=2^{ad}-1=T_0(d)*q_{li}(d,,a-1)=$
$=(2^d-1)(2^{(a-1)d}+2^{(a-2)d}+\ldots+2^{2d}+2^d+1)$ and everyone of both factors is divisible by a. At the same time, no one of them is divisible by a^2.
Hence, the number $T_0(ad)$ is the smallest term of the stream T_0 divisible by a^2 and indivisible by a^k, $k>2$.

(c) The proof is by induction
The case $n \le 2$ was proved in (a,b).
Let us assume that $n>2$ and that the theorem is true for $n-1$, that is, that $a^{n-1} \mid T_0(a^{n-2}d)$.
Denote $e=a^{n-2}d$.
We get $T_0(a^{n-1}d)=T_0(ae)=2^{ae}-1=T_0(e)*q_{li}(e,a-1)=$
$=(2^d-1)(2^{(a-1)d}+2^{(a-2)d}+\ldots+2^{2d}+2^d+1)$.
Consider now the smooth number $q_{li}(e,a-1)$.
We showed in (a) that the smooth number $q_{li}(e,a-1)$ is divisible by a and indivisible by a^2.
Consequently, the smooth number
$T_0(a^{n-1}d)=T_0(e)*q_{li}(e,,a-1)=T_0(a^{n-2}d)*q_{li}(a^{n-2}d,a-1)$
is divisible by a^n and indivisible by a^{n+1}.

EXAMPLE
Consider $a=5$. Then $d=le\Gamma_5=4$.
According to Theorem 3.4:
- The smooth number $q=q_{li}(d,a-1)=q_{li}(4,4)=2^{16}+2^{12}+2^8+2^4+1$ is divisible by 5 and indivisible by 5^2.
  Indeed, 5 divides 69905 and 25 does not.
- The smooth number $T_0(ad)=T_0(20)$ is divisible by 5^2 and indivisible by 5^3.
  Indeed, $T_0(20)=1048575$ is divisible by 5^2 and indivisible by $5^3=125$.
- The smooth number $T_0(a^{3-1}*d)=T_0(5^{3-1}*4)=T_0(100)$ is divisible by 5^3 and indivisible by 5^4.
  Indeed, $T_0(100)=1267650600228229401496703205375$ is divisible by $5^3=125$ and indivisible by $5^4=625$.
- The smooth number $T_0(a^{4-1}*d)=T_0(5^{4-1}*4)=T_0(500)$ is divisible by 5^4 and indivisible by 5^5.
  Indeed, $T_0(500)=$
  327339060789614187001318969682759915221664204604306478948329136809613379640467455488327009232590415715088668412756007100921725654588539305332852758 9375 is divisible by $5^4=625$ and indivisible by $5^5=3125$.

We will investigate now some properties of stream T_0.

Lemma 3.2

Consider $q \in Q$.

We know that the generating cycle Γ_q is congruent modulo q to $\underline{T}_0$ periodically, and the period equals $le\Gamma_q$.

(a) Consider a sequence $n\underline{T}_0$.
  (a1) If $(n, q) = 1$, then $(n\Gamma_q)_q \subset\subset (n\underline{T}_0)_q$. The period remains $le\Gamma_q$.
  (a2) If $(n, q) = q$, what means that n is a multiple of q, then all terms of the sequence $(n\underline{T}_0)_q$ are equal to zero.
  (a3) If $(n, q) = m > 1$, $q = xm$, $x \in Q$, what means that n is not a multiple of q and that $q = xm$ is a composite number, then the sequence $(n\underline{T}_0)_q$ is periodical, with a period $le\Gamma_x$.

(b) Consider a sequence $n\underline{T}_0+n-1$.
  (b1) If $(n, q) = 1$, then $(n\Gamma_q+n-1)_q \subset\subset (n\underline{T}_0+n-1)_q$. The period remains $le\Gamma_q$.
  (b2) If $(n, q) = q$, what means that n is a multiple of q, then all terms of the sequence $(n\underline{T}_0+n-1)_q$ are equal to $q-1$,
  (b3) If $(n, q) = m>1$, $q = xm$, $x \in Q$, what means that n is not a multiple of q and that $q = xm$ is a composite number, then the sequence $(n\underline{T}_0+n-1)_q$ is periodical, with a period $le\Gamma_x$.

Proof.

(a1) Assume $(n, q) = 1$.

If $\Gamma_q \subset\subset (\underline{T}_0)_q$, then $(n\Gamma_q)_q \subset\subset (n\underline{T}_0)_q$.

For any i, if $(\underline{T}_0(i))_q = 0$, then $(n\underline{T}_0(i))_q = 0$; if $(\underline{T}_0(i))_q > 0$, then $(n\underline{T}_0(i))_q = ((n)_q * (\underline{T}_0(i))_q)_q > 0$.

Thus the period of the sequence $(n\underline{T}_0)_q$ remains $le\Gamma_q$.

(a2) If $(n, q) = q$, then $n = kq$.

So, for every term of the complete stream $\underline{T}_0$ and for any k, there is $(kq\underline{T}_0)_q = 0$.

(a3) Assume $(n, q) = m > 1$, where $q = xm$, $m,x \in Q$.

So $n = ym$, where $(x,y) = 1$ (x i y are coprimes).

We can see that $(n\underline{T}_0)_q = (ym\underline{T}_0)_q$ equals, of course, zero in the case of the first term of $\underline{T}_0$, but also for every $i = j le\Gamma_x$, what means that x divides $\underline{T}_0(i)$, what means, in turn, that for every $i = j le\Gamma_x$ there is $(n\underline{T}_0(i))_q = (ym\underline{T}_0(i))_q = (yxmz)_q = (yzq)_q = 0$.

Hence, $n\Gamma_x \subset\subset (n\underline{T}_0)_x$, where a period is $le\Gamma_x$.

(b1) It follows from (a1) that if $\Gamma_q \subset\subset (\underline{T}_0)_q$, then $(n\Gamma_q)_q \subset\subset (n\underline{T}_0)_q$, with a period $le\Gamma_q$.

Every term of Γ_q is unique, so after the addition of the constant $(n-1)_q$ to $(n\Gamma_q)_q$ and to $(n\underline{T}_0)_q$, the relation $(n\Gamma_q + n - 1)_q \subset\subset (n\underline{T}_0 + n - 1)_q$ remains true, and the period of the congruence $(n\Gamma_q + n - 1)_q$ do $(n\underline{T}_0 + n - 1)_q$ remains $le\Gamma_q$.

(b2) Similarly to (a2), if $(n, q) = q$, then $n = kq$, and $n\underline{T}_0 + n - 1 = kq\underline{T}_0 + kq - 1$, since immediately follows that for every term of the complete stream $\underline{T}_0$ and for any k, there is $(kq\underline{T}_0+kq-1)_q = q - 1$.

(b3) Assume $(n, q) = m > 1$, $q = xm$, $m,x \in Q$, that is, $n = ym$ and $(x,y) = 1$.

It follows from (a3) that $n\Gamma_x \subset\subset (n\underline{T}_0)_x$, with a period $le\Gamma_x$, and that the addition of the constant $(n-1)_q = (kq-1)_q = q-1$ to the term of sequences $n\Gamma_x$ and $(n\underline{T}_0)_x$ does not change the period of the congruence modulo x of $n\Gamma_x$ to the sequence $(n\underline{T}_0)_x$.

Theorem 3.5

Consider $q \in Q$.

(a) If a divides q, then
- a divides $T_0(le\Gamma_q)$,
- $le\Gamma_a = (le\Gamma_q)/n$, $n \in N$,
- the generating cycle Γ_a is congruent periodically to $(\Gamma_q)_a$, that is, $\Gamma_a \subset\subset (\Gamma_q)_a$,
- the set of dead sources $\Psi_a \subset (\Psi_q)_a$.

(b) Let $q = ab\ldots z$, $a>1$, $b>1$, ..., $z>1$.
There are, in the set of dead source Ψ_q, among others, numbers $a-1$, $b-1$, ... , $z-1$ and all even numbers $p<q$ such that $(p+1)_a = 0$ or $(p+1)_b = 0$ or … or $(p+1)_z = 0$.

(c) Consider $q = ab$, $a \neq q$, $b \neq q$.
Let s be the source of the number q.
  (c1) If $(s)_q = q - 1$, then all terms of the sequence $(\underline{T}_s)_q$ are equal to $q - 1$.
  (c2) If $(s)_b = b - 1$, what means that $(s)_b + 1$ divides q, then the sequence $(\underline{T}_s)_q$ is periodical, with a period $le\Gamma_a$.
  (c3) If $(s)_q \neq q - 1$ and $((s)_q+1, q)=1$, then the sequence $(\underline{T}_s)_q$ is periodical, with a period $le\Gamma_q$.

(d) Let m, n be two different non-trivial divisors of q and let $q = mn$.
The loops $\Theta(m-1)_q$ and $\Theta(n-1)_q$ are disjoint, so the sequences $(T_{m-1})_q$ and $(T_{n-1})_q$ are disjoint.

Proof.

(a) $T_0(le\Gamma_q)$ is the smallest term of T_0 divisible by q; hence, a divides $T_0(le\Gamma_q)$.

If $a \mid T_0(le\Gamma_q)$, then $(T_0(le\Gamma_q - 1))_a = \beta a$, that is, $le\Gamma_q$ equals $le\Gamma_a$ or is divisible by $le\Gamma_a$.

So, we get $le\Gamma_a = (le\Gamma_q)/n$, $n \in N$.

$\Gamma_a \subset\subset (\underline{T}_0)_a$ and $\Gamma_q \subset\subset (\underline{T}_0)_q$. Hence, $\Gamma_a \subset\subset (\Gamma_q)_a$.

There is, as well, $\Psi_a \subset (\Psi_q)_a$, because $(\Gamma_q)_a$ contains exclusively the terms of Γ_a.

(b) According to Theorem 3.3, the number $a-1$ is never present in the generating cycle Γ_a, like the number $q-1$, which is never present in the cycle Γ_q. Consequently, the number $a-1$ must appear in the set of dead sources Ψ_a.

It was proved above that $\Gamma_a \subset\subset (\Gamma_q)_a$. Hence, there are no terms p such that $(p)_a = a - 1$, in Γ_q.

Identical reasoning concerns the number b and all others divisors.

(c1) According to Theorem 3.4.b, $\underline{T}_s = (s+1)\underline{T}_0 + s$.

So, if $s = q - 1 + kq$, $k \in E$, then

$(\underline{T}_s)_q = ((q + kq)\underline{T}_0 + q + kq - 1)_q = q - 1$.

(We require $k \in E$, because the source s is even.)

(c2) It must be $s = b - 1 + kb$, $k \in E$.

According to Theorem 3.4.b, we will write $\underline{T}_s = (b + kb)\underline{T}_0 + b + + kb - 1 = b(k + 1)\underline{T}_0 + b(k + 1) - 1 = n\underline{T}_0 + n - 1$,

where $n = b(k+1)$.

$k + 1$ neither equals a, nor is divisible by a, because we have assumed that $(s)_q \neq q - 1$.

If $k + 1$ equaled ma, $m \in Z^+$, we would have $n = b(k + 1) = mab = mq$, and consequently, $\underline{T}_s = mq\underline{T}_0 + mq - 1$ and $(\underline{T}_s)_q = q - 1$.

Hence, n is not a multiple of q.

For $q = ab$, there is $(n, q) = b > 1$. According to the lemma 3.2.b3, the sequence $(\underline{T}_s)_q$ is periodi-cal with a period equal $le\Gamma_a$ (a,b correspond to x,m from the lemma 3.2).
(c3) If $c = ((s)_q + 1, q) > 1$, then $c \mid q$. Such a case is considered above, in (c2).
We have $((s)_q + 1, q) = 1$, so the case (c2) does not occur.
If $s \neq q - 1 + kq$, $k \in E$, then the case (b2) from the lemma 3.2 neither occurs.
We have here the case (b1) from the lemma 3.2 and so the sequence $(\underline{T}_s)_q$ is periodical with a period $le\Gamma_q$.
(d) According to Axiom 3.4.a, m divides $\underline{T}_{m-1} + 1$, i.e. m divides also $\Theta(m\text{-}1)_q + 1$ and, at the same time, n divides $\underline{T}_{n-1} + 1$, thus n divides $\Theta(n\text{-}1)_q + 1$.
Suppose that there exist in the sequence $\underline{T}_{m-1} + 1$ a term divisible by n.
Such term should have a form $T_{m-1}(i) + 1 = m2^i - 1 + 1 = m2^i$ and should equal wmn, $w \in N$, what means that wn should equal 2^i, what is impossible, because 2^i has no odd divisors.
Hence, if $m \neq n$, the loops $\Theta(m\text{-}1)_q$ and $\Theta(n\text{-}1)_q$, as well as the sequences $(T_{m-1})_q$ and $(T_{n-1})_q$, are disjoint.

EXAMPLE.
concerning Theorem 3.5.a:
Consider 21.
21 divides 105.
There is $le\Gamma_{21} = 6$ and $le\Gamma_{105} = 12$.
As we can see, $le\Gamma_{21}$ divides $le\Gamma_{105}$.
Moreover:
$\Gamma_{21} = 0, 1, 3, 7, 15, 10$
$\Gamma_{105} = 0, 1, 3, 7, 15, 31, 63, 22, 45, 91, 78, 52$
$(\Gamma_{105})_{21} = 0, 1, 3, 7, 15, 10, 0, 1, 3, 7, 15, 10.$
$\Gamma_{21} \subset\subset (\Gamma_{105})_{21}$.
concerning Theorem 3.5.b:
Given $105 = 3 * 5 * 7$.
In the set of dead sources Ψ_{105}, one can find not only 2, 4, 6, 104 but also all $p < 105$ such that $(p)_3 = 2$, $(p)_5 = 4$ and $(p)_7 = 6$, e.g. 20, 24, 14, etc.
concerning Theorem 3.5.c:
Given $q = 55 = 5 * 11$.
(c1) For any i there is
$(T_{54}(i))_{55} = (T_{164}(i))_{55} = (T_{274}(i))_{55} = \ldots = 54$.
(c2) The sequences $(T_{10})_{55}$, $(T_{32})_{55}$, $(T_{76})_{55}$, $(T_{98})_{55}$, etc. are periodical, with a period $le\Gamma_5 = 4$.
(c3) The sequences $(T_2)_{55}$, $(T_6)_{55}$, $(T_8)_{55}$, $(T_{12})_{55}$, etc. are periodical, with $le\Gamma_{55} = 20$.

Axiom 3.9.

(a) It follows from Theorem 3.5 that the length of the loop modulo q of any dead source from the set Ψ_q is equal to q or divide the length of generating cycle Γ_q.
So, the generating cycle Γ_q is the longest or one of the longest loops modulo q.
(b) It follows from Theorem 3.5.c2 that if, for some number q, we can find such s that $le\Theta(s)_q < le\Gamma_q$, then $(s)_q+1$ divides q.
(c) If $q = ab$, that is, if $T_0(le\Gamma_q) = xT_0(le\Gamma_a)$, then x is a smooth number, precisely, $x = q_{li}(a,b-1)$.
(It follows immediately from the well-known formula:
$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)$.)

We will formulate now the theorem, generalizing partly, what was said above about the generating cycles.

Theorem 3.6
(a) Every odd number q has one and unique generating cycle Γ_q, and, at least, one term q-1 in its set of dead sources Ψ_q.
If $q=T_0(i)$, then $le\Gamma_q = i = \log_2(q+1)$.
If $q \notin T_0$, then there is $[\log_2(q+1)]+2 \leq le\Gamma_q \leq q-1$.
(b) If, for any s, $le\Theta(s)_q < le\Gamma_q$, then q is a composite number and $le\Theta(s)_q = le\Gamma_q/n$, $n \in N$.
(c) If q is a prime, then $le\Gamma_q = (q-1)/n$, $n \in N$.
However, $le\Gamma_q = (q-1)/n$ is not enough to recognize q as a prime.
(d) If q is a smooth number, that is,
if $q = q_{li}(d,j) = 2^{jd} + \ldots + 2^{3d} + 2^{2d} + 2^d + 1$,
then $le\Gamma_q = d(j+1)$.
If some number $w = q(2^d - 1) = 2^{d(j+1)} - 1$,
then $le\Gamma_w = le\Gamma_q$.
(e) If q is a sparkling number, that is, if $q = 2^{jd} - 2^{(j-1)d} + \ldots + 2^{4d} - 2^{3d} + 2^{2d} - 2^d + 1$, $j \in E$, then $le\Gamma_q = 2d(j+1)$.
If some number $w = q(2^d + 1) = 2^{d(j+1)} + 1$,
then $le\Gamma_w = le\Gamma_q$.
(f) If $q = a^2$, then $le\Gamma_q = a\, le\Gamma_a$.
If $q = a^i$, then $le\Gamma_q = a^{i-1}\, le\Gamma_a$.
(g) If $q = ab$ and a, b are coprimes,
then $le\Gamma_q = lcm(le\Gamma_a, le\Gamma_b)$, where lcm denotes the least common multiple.
There is, at the same time,
$lcm(le\Gamma_a, le\Gamma_b) \leq (1/2)(\sqrt{q} - 1)^2$.
If a and b are primes,
then $le\Gamma_q * 2kmn = (q-1) - (a-1) - (b-1)$,
where $m = (a-1)/le\Gamma_a$, $n = (b-1)/le\Gamma_b$, $k \in N$.
(h) If $q = a*b*\ldots*z$ and a, b, …, z are coprimes,
then $le\Gamma_q = lcm(le\Gamma_a, le\Gamma_b, \ldots, le\Gamma_z)$.

Proof.
(a) According to Axiom 3.7, there exists a generating cycle Γ_q for every $q \in Q$. It follows from Axiom 3.8 that this cycle is unique.
If $q = T_0(i) = 2^i - 1$, then $\beta q = 2^{i-1} - 1$
and $le\Gamma_q = i - 1 + 1 = i = \log_2(q+1)$.
If $q \notin T_0$, then there exists such i that $T_0(i) < q < T_0(i+1)$.
Hence, $le\Gamma_q \geq [\log_2(q+1)]+1$.
For we accept zero as the first element of the cycle, we add 1 to the length of the cycle. So, $le\Gamma_q \geq [\log_2(q+1)]+2$.
In turn, the length of the generating cycle cannot exceed q-1, as the number of classes of residues modulo q equals q, and finally we get $q - 1$, because, according to Theorem 3.3, there is no the term q-1 in the generating cycle.
Consequently, the term q-1 appears always in the set of dead sources Ψ_q of the number q.
(b) The correctness follows immediately from Theorem 3.5.a and 3.5.c2.
(c) If q is a prime, then, by Fermat's theorem, $(2^{q-1} - 1)_q = 0$.
It follows from (a) that Γ_q is unique.
Since there is $(2^{q-1} - 1)_q = T_0(q-1)_q = 0$, it must be $\Gamma_q = (q - 1)/n$, where $n \in N$.

The fact that $le\Gamma_q = (q\text{-}1)/n$ is not sufficient to say that q is a prime, can be confirmed, among others, by the following example: $le\Gamma_{2047} = 11 = (2047 - 1) / 186$, and, at the same time, $q = 2047 = 89 * 23$.
Note that there is $le\Gamma_{89} = le\Gamma_{23} = 11$.
(d) Given a smooth number $q = 2^{jd} + 2^{(j-1)d} + \ldots + 2^{2d} + 2^d + 1$.
According to the well-known formula:
$T_0(d(j+1)) = 2^{(j+1)d} - 1 = (2^d - 1)(2^{jd} + 2^{(j-1)d} + \ldots + 2^{2d} + 2^d + 1)$.
Thus $w = q(2^d - 1) = qT_0(d) = T_0(d(j+1))$.
It follows immediately from (a) that $le\Gamma_w = d(j+1)$.
It proves the correctness of the second part of (d).

Concerning the first part of (d):
There is $w = T_0(d)q$ and $le\Gamma_w = d(j+1)$.
From (a) follows that $leT_0(d) = d$.
According to Theorem 3.5.a, if q divides w, then $le\Gamma_q$ divides $le\Gamma_w$. Hence, $le\Gamma_w$ equals $j+1$ or $d(j+1)$.
For $q = 2^{jd} + 2^{(j-1)d} + \ldots + 2^{2d} + 2^d + 1$,
then $T_0(jd) < q < T_0(jd + 1) < T_0((j+1)d) = qT_0(d)$.
From above inequality follows that it must be $le\Gamma_w = d(j+1)$.
(e) Let q be a sparkling number. So, $q = q_{br}(d,j) =$
$= 2^{jd} - 2^{(j-1)d} + 2^{(j-2)d} - 2^{(j-3)d} + \ldots + 2^{4d} - 2^{3d} + 2^{2d} - 2^d + 1$, $j \in E$.
According to the lemma 3.1, a product of sparkling number q and smooth number $2^d + 1$ is a smooth number $w = 2^{(j+1)d} + 1$.
So, according to the definition 3.7.a, w is a smooth number $w = q_{li}(x,y) = q_{li}((j+1)d,1)$ and $le\Gamma_w = x(y+1) = (j+1)d(1+1) = 2d(j+1)$.
It proves the correctness of the second part of (e).

Concerning the first part of (e):
Given $w = (2^d + 1)q$ and $le\Gamma_w = 2d(j+1)$.
$v = 2^d + 1$ is a smooth number $q_{li}(x,y) = q_{li}(d,1)$.
Hence, $le\Gamma_v = 2d$.
According to Theorem 3.5.a, if q divides w, then $le\Gamma_q$ divides $le\Gamma_w$. So $le\Gamma_w$ equals $j+1$ or $2(j+1)$ or $2d(j+1)$.

Let us transform the expression q to the form of sum of powers of 2:
$q = 2^{jd} - 2^{(j-1)d} + 2^{(j-2)d} - 2^{(j-3)d} + \ldots + 2^{4d} - 2^{3d} + 2^{2d} - 2^d + 1 =$
$= 2^{(j-1)d}(2^d - 1) + 2^{(j-3)d}(2^d - 1) + \ldots + 2^{3d}(2^d - 1) + 2^d(2^d - 1) + 1 =$
$= 2^{(j-1)d}(2^{d-1} + 2^{d-2} + \ldots + 2^2 + 2^1 + 1) + 2^{(j-3)d}(2^{d-1} + 2^{d-2} + \ldots + 2^2 + 2^1 + 1) + \ldots + 2^{3d}(2^{d-1} + 2^{d-2} + \ldots + 2^2 + 2^1 + 1) + 2^d(2^{d-1} + 2^{d-2} + \ldots + 2^2 + 2^1 + 1) + 1 =$
$= (2^{jd-1} + 2^{jd-2} + 2^{jd-3} + \ldots + 2^{jd-d}) + (2^{(j-2)d-1} + 2^{(j-2)d-2} + 2^{(j-2)d-3} + \ldots + 2^{(j-3)d}) + \ldots + (2^{4d-1} + 2^{4d-2} + \ldots + 2^{3d}) + (2^{2d-1} + 2^{2d-2} + \ldots + 2^{d+2} + 2^{d+1} + 2^d + 1)$.
The highest component in the expression is 2^{jd-1},
so $le\Gamma_q > [\log_2(q+1)] = jd\text{-}1$. The choice $le\Gamma_q = 2d(j+1)$ follows.
(f) The correctness follows immediately from Theorem 3.4.c and 3.4.cd.
(g,h) Let us denote $le\Gamma_q = leq$, $le\Gamma_a = lea$ and $le\Gamma_b = leb$.
We know that $a \mid (2^{lea} - 1)$ and $b \mid (2^{leb} - 1)$.
Consequently, $a \mid (2^{nlea} - 1)$ and $b \mid (2^{mleb} - 1)$.
If $leq = \text{lcm}(lea, leb)$, then $a \mid (2^{leq} - 1)$ and $b \mid (2^{leq} - 1)$.
Hence, $q \mid (2^{leq} - 1)$.
At the same time, $T_0(leq) = 2^{leq} - 1$ is the least term of the stream T_0 satisfying the above conditions.
Thus $le\Gamma_{ab} = \text{lcm}(le\Gamma_a, le\Gamma_b)$.
If the number of coprime factors exceeds 2, the reasoning is identical.

According to (a), $lea \le a\text{-}1$, $leb \le b\text{-}1$.
For a-1 i b-1 are even, $leq = \text{lcm}(le\Gamma_a, le\Gamma_b) \le ((a\text{-}1)(b\text{-}1))/2 = ((ab - a - b + 1)/2 = (ab - (a + b) + 1)/2 \le (q - 2\sqrt{q} + 1)/2 = (1/2)(\sqrt{q} - 1)^2$, because $ab - (a+b) + 1$ is the least when $a = b = \sqrt{q}$.
Hence, if q is the product of two coprimes, then $le\Gamma_q$ is less than $(1/2)(\sqrt{q} - 1)^2$.
If a and b, $a \ne b$, are primes, we get: $lea = (a\text{-}1)/m$,
$leb = (b\text{-}1)/n$, so $\text{lcm}(lea, leb) = (a\text{-}1)(b\text{-}1)/(2mnk)$, $k \in N$, and finally, $le\Gamma_q * 2kmn = (ab\text{-}1) - (a\text{-}1) - (b\text{-}1) = (q\text{-}1) - (a\text{-}1) - (b\text{-}1)$.

EXAMPLE
- Determine $le\Gamma_{127}$.
  $127 = T_0(7)$. It follows from Theorem 3.6.a that $le\Gamma_{127} = 7$.
- Determine $le\Gamma_{341}$.
  $341 = 2^8 + 2^6 + 2^4 + 2^2 + 1$ is a smooth number $q_{li}(2,4)$.
  So, $le\Gamma_{341} = 2(4+1) = 10$.
- Determine $le\Gamma_{625}$.
  $625 = 5^4$.
  According to Theorem 3.6.f, $le\Gamma_{625} = 5^3 le\Gamma_5 = 125*4 = 500$.
- Given $629 = 17*37$, $le\Gamma_{17} = 8$, $le\Gamma_{37} = 36$.
  Determine $le\Gamma_{629}$.
  It follows from Theorem 3.6.g that $le\Gamma_{629} = \text{lcm}(le\Gamma_{17}, le\Gamma_{37}) = \text{lcm}(8, 36) = 72$.

Theorem 3.7

For every odd number q there is $(T_0(kle\Gamma_q + i))_q = \delta_q^{\,i}0$ and $(T_0(kle\Gamma_q - i))_q = \beta_q^{\,i}0$.

Proof.
It was showed above that $(T_0(kle\Gamma_q))_q = 0$.
So, according to Axiom 3.6, we can write $T_0(kle\Gamma_q + i)_q = \delta_q^{\,i}0$ and $T_0(kle\Gamma_q - i)_q = \beta_q^{\,i}0$.

EXAMPLE
- Given $le\Gamma_{15} = 4$. Calculate the reminder when $2^{47} - 1$ is divided by 15.
  According Theorem 3.7,
  we can write $(T_0(47))_{15} = (T_0(11*4+3))_{15} = \delta_{15}^{\,3}0 = 7$,
  as well as $(T_0(47))_{15} = (T_0(12*4 - 1))_{15} = \beta_{15}^{\,1}0 = \beta_{15}^{\,1}15 = 7$
- Given $le\Gamma_{341} = 10$. Calculate the reminder when $2^{47} - 1$ is divided by 341.
  As above, we can write $(T_0(47))_{341} = (T_0(5*10 - 3))_{341} = \beta_{341}^{\,3}0 = \beta_{341}^{\,3}341 = 127$, but also
  $(T_0(47))_{341} = (T_0(4*10 + 7))_{341} = \delta_{341}^{\,7}0 = (T_0(7))_{341} = 127$.

Theorem 3.8, presented below, is partly a repetition, partly a development of Theorem 3.5, with this particularity, however, that a special stress will be put on the appurtenance of any given source to the generating cycle or to the set of dead sources of number $q \in Q$.

Theorem 3.8 (for the periodicity in streams)
Let $q \in Q$ and $s \in E$.
(a) If $(s)_q = q\text{-}1$, then for any i there is $(\underline{T}_s(i))_q = q\text{-}1$.
(b) If $(s)_q \in \Psi_q$, then the complete stream $(\underline{T}_s)_q$ is periodical, with a period equal to $le\Theta(s)_q$.
Moreover, $le\Theta(s)_q$ divides $le\Gamma_q$.
(c) If $(s)_q \in \Gamma_q$, then the complete stream $(\underline{T}_s)_q$ is periodical, with a period equal to $le\Gamma_q$.

Proof.
(a) Refer to the proof of Theorem 3.5.c1.
(b) The proof follows immediately from Theorem 3.5.a, 3.5.b and 3.5.c2.
(c) The proof follows immediately from Theorem 3.5.b and 3.5.c3.

EXAMPLE
Given $q = 55 = 5*11$.
$\Gamma_{55} = 0, 1, 3, 7, 15, 31, 8, 17, 35, 16, 33, 12, 25, 51, 48, 42, 30, 6, 13, 27$
$le\Gamma_{55} = 20$
$\Psi_{55} = \{2, 4, 10, 14, 18, 20, 22, 24, 26, 28, 32, 34, 36, 38, 40, 44, 46, 50, 52\}$
According to Theorem 3.5.b, $5–1=4 \in \Psi_{55}$ and $11–1=10 \in \Psi_{55}$.
- 4 is a term of the loop $\Theta(4)_{55} = \{4, 9, 19, 39, 24, 49, 44, 34, 14, 29\}$
  4 is a source of the stream $T_4 = 4, 9, 19, 39, 79, 159, 319, \ldots$
  Observe that $\Theta(4)_{55} \in (T_4)_{55}$.
- 10 is a term of the loop $\Theta(10)_{55} = \{10, 21, 43, 32\}$ and a source of the stream $T_{10} = 10, 21, 43, 87, 175, 351, 703, \ldots$
  Observe that $\Theta(10)_{55} \in (\underline{T}_{10})_{55}$.
  We have $\Gamma_5 = 0, 1, 3, 2$, where $le\Gamma_5 = 4$
  $\Gamma_{11} = 0, 1, 3, 7, 4, 9, 8, 6, 2, 5$, where $le\Gamma_{11} = 10$.
  Note that, according to Theorem 3.6.g,
  $le\Gamma_{55} = 20 = lcm(le\Gamma_5, le\Gamma_{11}) = lcm(4,10)$.

EXAMPLE
Given $8 \in \Gamma_{55}$.
- $\underline{T}_8 = 8, 17, 35, 71, 143, 287, 575, 1151, 2303, 4607, 9215, 18431, 36863, 73727, 147455, 294911, 589823, 1179647, 2359295, 4718591, 9437183, 18874367, \ldots$
- $(\underline{T}_8)_{55} = 8, 17, 35, 16, 33, 12, 25, 51, 48, 42, 30, 6, 13, 27, 0, 1, 3, 7, 15, 31, 8, 17, 35, 16, 33, 12, 25, 51, 48, 42, 30, 6, 13, 27, 0, \ldots$
  Observe, according to Theorem 3.8.c, that $\Gamma_{55} \in (\underline{T}_8)_{55}$, that $(\underline{T}_8)_{55}$ is periodical, that there are no terms other than the terms belonging to Γ_{55}, and, finally, that there is in $\underline{T}_8$ the infinite number of terms divisible by 55, distant one from another of $le\Gamma_{55} = 20$.
  Observe also that $(8)_{11} \in \Gamma_{11}$ and $(8)_5 = 3 \in \Gamma_5$.
- $(\underline{T}_8)_5 = 3, 2, 0, 1, 3, 2, 0, 1, 3, 2, 0, 1, 3, 2, 0, 1, 3, 2, 0, 1, \ldots$.
  Note that $\Gamma_5 \in (\underline{T}_8)_5$, that $(\underline{T}_8)_5$ is periodical and that in $\underline{T}_8$ there is the infinite number of terms divisible by 5, distant one from another of $le\Gamma_5 = 4$.
- The same for 11.

EXAMPLE
- Give some examples of streams, where there are no terms divisible by 23.
  We find $\Gamma_{23} = 0, 1, 3, 7, 15, 8, 17, 12, 2, 5, 11$ and
  $\Psi_{23} = \{4, 6, 10, 14, 16, 18, 20, 22\}$.
  According to Theorem 3.8a, there are no terms divisible by 23 in $T_{22}, T_{45}, T_{68}, T_{91}, T_{114}$, etc.
  According to Theorem 3.8c, there are no terms divisible by 23 in $T_4, T_6, T_{10}, T_{50}, T_{96}, T_{14}, T_{16}$, etc.
- Given $q = T_{16}(1) = 33 = 3 * 11$.
  What are other terms of the stream T_{16}, divisible by 11 ?
  We find $\Gamma_{11} = 0, 1, 3, 7, 4, 9, 8, 6, 2, 5$ and $le\Gamma_{11} = 10$
  The source of T_{16} modulo 11 equals $(16)_{11} = 5 \in \Gamma_{11}$.
  So, according to Theorem 3.8b, the stream $(T_{16})_{11}$ is periodical, with a period 10.
  Hence the terms divisible by 11 are $T_{16}(11) = 34815$,
  $T_{16}(21) = 35651583$, $T_{16}(31)$, $T_{16}(41)$, $T_{16}(51)$, $T_{16}(61)$, etc.

Theorem 3.9 (for the periodicity in cascades)
Given sources r, s.
If $s – r = pq$, $q \in Q$, $p \in E$, then $(K_r(i))_q = (K_s(i))_q$.

Proof.
According to Definition 3.2,
$K_s(i) = T_s(i) = (s+1)2^i – 1 = (r + pq + 1)\, 2^i – 1$. Then
$(K_s(i))_q = ((r+pq+1)\, 2^i–1)_q = ((r+1)\, 2^i–1)_q = (T_r(i))_q = (K_r(i))_q$

EXAMPLE
Does 11 divide $127926271 = T_{60}(21)$?
According to Theorem 3.9, if 11 divides $T_{60}(21)$, then 11 must divide $T_{60 - 4*11}(21) = T_{16}(21)$.
We have $(16)_{11} = 5 \in \Gamma_{11}$
and we know that $\Gamma_{11} = 0, 1, 3, 7, 15, 8, 17, 12, 2, 5, 11$.
According to Theorem 3.8.b, 11 should divide
$T_{16}(21–n le\Gamma_{11}) = T_{16}(21–2*10) = T_{16}(1) = 33$, which is true.
So 11 divides $T_{60}(21) = 127926271$.

Axiom 3.10
Consider some $T_s(i)$ and $q \in Q$.
Let us denote $n = le\Gamma_q$ if $(s)_q \in \Gamma_q$ or $n = le\Theta(s)_q$ if $(s)_q \in \Psi_q$.
If we perform any number of jumps of the length n in the stream T_s, reaching the term $T_s(j)$, and the even number of jumps of the length q in the cascade $K(j)$, reaching the term $T_t(j)$, then $(T_t(j))_q$ will be equal to $(T_s(i))_q$.

EXAMPLE
Does $q = 7$ divide 25599 ?
Instead of calculating $(25599)_7$, we will apply Axiom 3.10.
We have $25599 = T_{24}(10) = T_s(i)$.
We find $(24)_7 = 3 \in \Gamma_7$. We know that $n = le\Gamma_7 = 3$.
Hence, $(T_{24}(10))_7 = (T_{24–2^*7}(10))_7 = (T_{10}(10\text{-}3^*3))_7 = (T_{10}(1))_7 = (21)_7 = 0$.
Hence, 7 divides 25599.

Theorem 3.10
Given $q>1$, $q \in Q$, $s \in E$ and some term $T_s(i)$.
Let $r = (s)_q$.
(a) There is $(T_s(i))_q = (L_r(i))_q$, where L_r is a substream.
(b) If $r \in Q$, that is, if $r + 1 = m2^u$,
then $(T_s(i))_q = (T_{m–1}(i+u))_q$.
(c) If $r \in E$, then $(T_s(i))_q = (T_r(i))_q$.

Proof.
(a) It was assumed $s = mq + r$. Thus, $T_s(i) = (s+1)2^i – 1 = (mq + r + 1)2^i – 1$, as well as $L_r(i) = (r+1)2^i – 1$, where L_r is a substream, because, in the general case, r can be both, odd or even. Hence, $(T_s(i))_q = (L_r(i))_q$.
(b) If $r \in Q$, then r is a local source of the substream L_r.
According to Axiom 3.1, there is $r+1 = m2^u$, $m \in Q$, which permits to write $L_r(i) = T_{m–1}(i+u)$ and $(T_s(i))_q = (T_{m–1}(i+u))_q$.
(c) If $r \in E$, then r is a source of the stream T_r and Theorem 3.10 takes a form $(T_s(i))_q = (T_r(i))_q$.

EXAMPLE
- Determine $(9087)_{39}$.
  We know that $le\Gamma_{39} = 12$ and that $9087 = T_{70}(7)$.
  According to Theorem 3.10, we get $r = (s)_q = (70)_{39} = 31$,
  so $(T_{70}(7))_{39} = (L_{31}(7))_{39} = (4095)_{39}$.

Simultaneously, $r = 31 = 2^5 - 1$, hence $m = 1$, $u = 5$ and $(T_{70}(7))_{39} = (T_0(12))_{39}$.
From Theorem 3.8.c, we have $(T_0(12))_{39} = (T_0(12 - 12))_{39} = (T_0(0))_{39} = 0$. So, finally, $(9087)_{39} = (T_0(0))_{39} = 0$.

- We asked whether 7 divides 25599 in the previous example. The answer was "yes", because 7 divides $T_{10}(1) = 21$.
  Thanks to Theorem 3.10, we can make one step more:
  $r = (10)_7 = 3$, hence $(T_{10}(1))_7 = (T_3(1))_7 = (7)_7 = 0$, and finally, 7 divides $25599 = T_{24}(10)$ because 7 divides $T_3(1)=7$.

The following theorem will partly repeat, what was said above, but, first of all, it will deliver some new information about the numbers from the range $\{0,.., q-1\}$.

Theorem 3.11
Consider an odd, composite number $q = ab\ldots z$,
where $a, b, \ldots, z$ are the non-trivial divisors of q.
We will distinguish two subsets, EW i EV, in the set of dead sources Ψ_q . The subset EW contains all dead sources such w such that $w+1$ are coprimes to q (i.e. $(w+1, q) = 1$), while the subset EV contains all dead sources such v such that $v+1$ do not divide q but, at the same time, are not coprimes to q.
The source $v = q - 1$ belongs to the subset EV.
We will denote by QW the set of all odd numbers belonging to all loops $\Theta(w)_q$, and by QV - the set of all odd numbers belonging to all loops $\Theta(v)_q$.
There is, of course, EW $\cap$ EV = Ø and QW $\cap$ QV = Ø.
So, we get $\Psi_q = \{a\text{-}1, b\text{-}1, \ldots, z\text{-}1\} \cup$ EW $\cup$ EV.
According to Axiom 3.8.f, there is

$$\{0,.., q-1\} = \Gamma_q \cup \Psi_q \cup QW \cup QV.$$

Thus, we can write

$$\{0,.., q-1\} = \Gamma_q \cup \Theta(a\text{-}1)_q \cup \Theta(b\text{-}1)_q \cup \ldots \cup \Theta(z\text{-}1)_q \cup EW \cup EV \cup QW \cup QV.$$

Then

(a1) For every non-trivial divisors a of q, there is
$le\Theta(a\text{-}1)_q = le\Gamma_{q/a} \le le\Gamma_q$.
For any term d of the loop $\Theta(a\text{-}1)_q$, there is
$(d+1, q) = ka$, $1 \le k < q/a$.

(a2) For every source $v \in$ EV, there is
$le\Theta(v)_q = le\Gamma_k$, where $k = q / (v+1, q)$.
For any term d of the loop $\Theta(v)_q$, there is
$(d+1, q) = j(v+1, q)$, where $1 \le j < q/(v+1, q)$.

(a3) For every source $w \in$ EW, there is $le\Theta(w)_q = le\Gamma_q$.
Every element of generating cycle Γ_q and every element of the loop $\Theta(w)_q$, increased of 1, is coprime to q.

(a4) Except for the loop $\Theta(q\text{-}1)_q$ of length 1, the shortest loop is the loop of divisor m, which corresponds to the divisor q/m possessing the shortest generating cycle.

(b) If q is a prime, then
- Ψ_q = EW,
- $\{0,.., q-1\} = \Gamma_q \cup$ EW $\cup$ QW,
- q is a sum of $le\Gamma_q$ and of the lengths $le\Theta(w)_q$ of all dead sources $w \in$ EW, equal always to $le\Gamma_q$, except for $le\Theta(q\text{-}1)_q$ equal to 1.
  Hence $q = k le\Gamma_q + 1$, $k>0$.

(c) The sum of $le\Gamma_q$ and of the lengths $le\Theta(w)_q$ of all dead sources $w \in$ EW is equal to Euler function $\varphi(q)$, defined as a number of integers not exceeding q and coprime to q.
Simultaneously, $le\Gamma_q$ divides $\varphi(q)$.

Proof
(a1) According to Theorem 3.5.c2, if n a non-trivial divisor of q, then $le\Theta(n\text{-}1)_q = le\Gamma_{q/n} \le le\Gamma_q$.
According to Theorem 3.5.a, $le\Gamma_{q/n}$ divides $le\Gamma_q$.
Any term d of the loop $\Theta(n\text{-}1)_q$ is, at the same time, a term of the stream $\underline{T}_{n-1}$, which, increasing of 1, according to Axiom 3.4.b, is divisible by n. Hence, $(d+1, q) = kn$, $1 \le k < q/n$.
(a2) According to Lemma 3.2.b3, if $(r+1, q) = m > 1$, then $q = km$ and the sequence $\underline{T}_r = ((r+1)\underline{T}_0 + (r+1) - 1)_q$ is periodical with the period $le\Gamma_k$..
If d is any term of the stream $\underline{T}_r$, then this term, increasing of 1, according to Axiom 3.4.a, is divisible by $r+1$, and, generally, there is $(d+1, q) = j\,(r+1, q)$, $1 \le j < q/(r+1, q)$.
(a3) If $r \in$ EW, then, by definition, $(r+1, q) = 1$. According to Theorem 3.5.c3, T_r is periodical, with a period equal to $le\Gamma_q$.
Any term of the stream $\underline{T}_{r,}$ increased of 1, is divisible by $r+1$ and by a power of 2, according to Axiom 3.4.a.
As a loop $\Theta(r)_q$ is periodically congruent modulo q to $\underline{T}_{r,}$ all terms of the loop are coprimes to q as well.
It follows from (a1) that there are no terms p such that $(p+1, q) > 1$ in the generating cycle Γ_q.
If it was the case, the length of the loop containing p would be less than $le\Gamma_q$ and would divide $le\Gamma_q$.
(a4) Follows immediately from (a1) and (a2).
(b) It follows from (a), (a1), (a2) and (a3) that for any term $d<q$ of the stream T_r could be coprime to q, the source r should belong to EW. Consequently, for a prime number q, all even numbers $r < q$ belong to generating cycle Γ_q, or to the subset EW, and all odd numbers, less than q, belong to generating cycle, or to the subset QW. It was showed in (a3), then if $r \in$ EW, then $le\Theta(r)_q = le\Gamma_q$, except for $le\Theta(q\text{-}1)_q = 1$.
Hence, there is $q = k le\Gamma_q + 1$, $k>0$.
(c) Follows immediately from (b).

EXAMPLE
Given $q = 63 = 9*7$.
Euler function $\varphi(63) = \varphi(9) * \varphi(7) = 6*6 = 36$.
According to Theorem 3.6.g, $le\Gamma_{63} = (le\Gamma_9, le\Gamma_7) = (6,3) = 6$.
It follows from Theorem 3.11.c that the sum of $le\Gamma_q$ and of the lengths $le\Theta(w)_q$ of all dead sources $w \in$ EW should be equal to Euler function $\varphi(63)$. Let us see.
$le\Gamma_{63} = 6$.
EW = {4, 10, 12, 16, 18, 22, 24, 28, 30, 36, 40, 42, 46, 52, 54, 58, 60}
The elements of EW belong to 5 loops with the length 6:

$le\Theta(4)_{63} = 6$
$le\Theta(10)_{63} = 6$
$le\Theta(12)_{63} = 6$
$le\Theta(22)_{63} = 6$
$le\Theta(30)_{63} = 6$

Indeed, we have $le\Gamma_{63} + le\Theta(4)_{63} + le\Theta(10)_{63} + le\Theta(12) + le\Theta(22) + le\Theta(30) = 36 = \varphi(63)$.

Remark 3.5
It follows immediately from Theorem 3.11.c that for any q, prime or composite, the length of the generating cycle $le\Gamma_q$ is

- as important source of information on possible factors of q as Euler function $\varphi(q)$ is,
- a fraction of the Euler function $\varphi(q)$.

4. In the binary system

Let us reserve a symbol $B_s(i)$ for the term
$T_s(i) = (s+1)2^i - 1$ in a binary notation.

Theorem 4.1
$B_s(i)$ is a natural concatenation of two binary numbers, the lower one corresponding to 2^i-1, and the higher one corresponding to s.
So, $B_s(i) = s_{(2)} \oplus (2^i - 1)_{(2)}$, where index (2) denotes the binary notation.

The *Proof* is immediate:
$T_s(i) = (s+1)2^i - 1 = s2^i + 2^i - 1$. In a binary number $(s2^i+2^i-1)_{(2)}$, the group of ones, corresponding to the $2^i - 1$, occupies i positions from the end, while an even part $(s)_{(2)}$ (even, so always terminated by a zero) precedes the group of ones.

Hence:

Remark 4.1
In the notation $B_s(i)$, i represents the number of ones in the low part and s in the high part – the source of the stream.

EXAMPLE
(1)
Give a decimal form $T_s(i)$ of 10000001111111111111111111.
We have 1000000⊕1111111111111111111, so i = 19 and s = 64, hence
$10000001111111111111111111_{(2)} = T_{64}(19) = 34078719$.
(2)
Give a binary form of $T_{10}(3) = 87$.
$87 \Rightarrow (10)_{(2)} \oplus (3)_{(2)} \Rightarrow 1010 \oplus 111 \Rightarrow 1010111$.

Remark 4.2
(a)
It is easy to recognize a smooth number $q_{li}(d,j)$ in binary notation: there are j groups of d-1 zeroes enclosed and separated by the single ones.
(EXAMPLE: $q_{li}(d,j) = q_{li}(5, 4) = 100001000010000100001_{(2)}$.)
(b)
It is also easy to recognize a sparkling number $q_{br}(d,j)$ in binary notation: the number has a form of $j/2$ group, where every group is composed of d ones on the higher position, and d zeroes on the lower position, with one irregularity in form of "1" that always occupies the lowest position in the number.
(EXAMPLE: $q_{br}(d,j) = q_{br}(3,4) = 2^{12}-2^9+2^6-2^3+1 = \underline{111000}111001_{(2)}$, where the example of a composite group is underlined.)

Remark 4.3
To execute the operation $\delta^i B_s(i)$ in the binary version, one should add i ones at the end of $B_s(i)$ (on the lower part of $B_s(i)$).
On the contrary, to execute the operation $\beta^i B_s(i)$ in the binary version, one should delete i ones at the end of $B_s(i)$.

EXAMPLE
Given $10011 \sim T_4(2) = 19$.
$\delta^3 10011 = 10011 \oplus 111 = 10011111 \sim \delta^3 T_4(2) = T_4(5) = 159$.
$\beta 10011 = 1001 \dotplus = 1001 \sim \beta T_4(2) = T_4(1) = 9$

EXAMPLE of determining the length of generating cycle of the number q
Given $T_{10}(2) = 43 = 101011_{(2)}$. Determine $le\Gamma_{43}$.
To simplify the procedure, we will take profit from Axiom 3.7.b, where it was said that when $\delta x > q$, then $\delta_q x$ is always even. So, if $x > \beta q$, then $\delta_q x = 2(x - \beta q)$.
We have $\beta 101011_{(2)} = 10101_{(2)} = B_{10}(1)$.
The first term of $le\Gamma_{43}$ is, by definition, zero.
Let us start:

0	$\sim 0_{(10)}$	
1	$\sim 1_{(10)}$	
11	$\sim 3_{(10)}$	
111	$\sim 7_{(10)}$	
1111	$\sim 15_{(10)}$	
11111	$\sim 31_{(10)}$	(> β101011 = 10101)
10100	$\sim 20_{(10)}$	(11111– 10101)+(11111– 10101) = 10100
101001	$\sim 41_{(10)}$	(> 10101)
101000	$\sim 40_{(10)}$	...
100110	$\sim 38_{(10)}$	
100010	$\sim 34_{(10)}$	
11010	$\sim 26_{(10)}$	
1010	$\sim 10_{(10)}$	
10101	$\sim 21_{(10)}$	

There is 14 terms in the generating cycle,
so $le\Gamma_{43} = 14 = \varphi(43) / 3$.

Remark 4.4
As we can see, in the procedure of determining $le\Gamma_{43}$, there was no division nor multiplication.
As operations, there were only

- comparison with 10101
- writing 1 at the end, when $\Gamma_{10}(i) < 10101$
- subtraction $\Gamma_{10}(i) - 10101$
  and addition $\Gamma_{10}(i) + \Gamma_{10}(i)$, when $\Gamma_{10}(i) > 10101$

The procedure is terminated when $\Gamma_{10}(i) = 10101$ and the number of steps equals $le\Gamma_q$.

Remark 4.5
Of course, instead of adding 5 times the successive ones between 0 and 11111, it would be clever to add 5 ones in one step, according to the inequality $11111 \geq 10101$. And so, every time we find $\Gamma_{10}(i) < 10101$.

Remark 4.6
We can directly write down 11111 as $\Gamma_{43}(6)$, which corresponds to $T_0(i)$ greater than $\beta 43$ and less than 43.
Thus, it would be more clever again, not to execute the first 5 steps, writing 11111 and substituting initially $le\Gamma_{43} = 6$.
Besides, all what was said above in Remark 4.5 remains valid and should be applied in every step except for the first one.

EXAMPLE
Thanks to Remark 4.6, the above example of determining $le\Gamma_{43}$, could be rewritten as follows:

11111	$le\Gamma_{43} = 6$
10100	$le\Gamma_{43} = 7$
101001	$le\Gamma_{43} = 8$
101000	$le\Gamma_{43} = 9$
100110	$le\Gamma_{43} = 10$
100010	$le\Gamma_{43} = 11$
11010	$le\Gamma_{43} = 12$
1010	$le\Gamma_{43} = 13$
10101	$le\Gamma_{43} = 14$

EXAMPLE.
Given $T_{38}(2) = 155$. Determine $le\Gamma_{155}$.
We have $\beta 155 = 77 = 1001101_{(2)}$.

1111111	$le\Gamma_{155} = 8$	(!)
1100100	$le\Gamma_{155} = 9$	
101110	$le\Gamma_{155} = 10$	
1011101	$le\Gamma_{155} = 11$	
100000	$le\Gamma_{155} = 12$	
10000011	$le\Gamma_{155} = 14$	(!)
1101100	$le\Gamma_{155} = 15$	
111110	$le\Gamma_{155} = 16$	
1111101	$le\Gamma_{155} = 17$	
1100000	$le\Gamma_{155} = 18$	
100110	$le\Gamma_{155} = 19$	
1001101	$le\Gamma_{155} = 20$	

There is 20 terms in the generating cycle,
so $le\Gamma_{155} = 20 = \varphi(155) / 6$.

Remark 4.7
There exist better algorithms to determine $le\Gamma_q$ in the binary environment but above procedure contains some didactic qualities.

EXAMPLE of application of the algorithm 3.1 (compare it with its decimal version)
Calculate $(536187)_{487}$.
So $q = 536187_{(10)} = 10000010111001111011$
and $a = 487_{(10)} = 111100111$
(Attention, in every $T_{a-1}(j)$ the decimal form of j will be conserved.)

0. $d = 10000010111001111011$.
1. $T_{a-1}(j) = T_{111100110}(10) = 111100110 \oplus 1111111111 = 1111001101111111111 < d$
2. $d := 10000010111001111011 - (1111001101111111111 + 1) = 1001001001111011$
3. $d > a$ ➔ **1**

1. $T_{111100110}(6) = 111100110111111 < d$
2. $d := 1001001001111011 - (111100110111111 + 1) = 1100010111011$
3. $d > a$ ➔ **1**

1. $T_{111100110}(3) = 111100110111 < d$
2. $d := 1100010111011 - (111100110111 + 1) = 100110000011$
3. $d > a$ ➔ **1**

1. $T_{111100110}(2) = 11110011011 < d$
2. $d := 100110000011 - (11110011011 + 1) = 111100111$
3. d is not greater then a
4. $d = a$, print "$536187 \equiv 0 \pmod{487}$" and terminate.

SYMBOLS

N	set of natural numbers
Z^+	set of all positive integers (with zero)
$a, .., z$	integer
p	even number
q	odd number
E	set of even positive integers (with zero)
Q	set of odd positive integers
K	set of stones (generators of primes)
δn	number generated by n
βq	generator of q
T_s	stream generated by a source s
$\underline{T_s}$	complete stream (with its source s)
L_z	substream generated by local source z
$\underline{L_z}$	complete substream (with its local source z)
$K(i)$	cascade i
Γ_q	generating cycle of q
Ψ_q	set of dead sources of q
$\Theta(a)_q$	loop modulo q of a
Ø	empty set
$\subset\subset$	"is congruent periodically" symbol
$a \mid q$	a is a non-trivial divisor of q
$(q)_a$	residue of q modulo a
lcm	the least common multiple
gcd	the greatest common divisor
(a,b)	gcd(a,b)
$x_1 \oplus x_2$	concatenation of x_1 and x_2
~	corresponds to
$[x]$	int(x)

REFERENCES

1. Vangalur S. Alagar, 1989. Fundamentals of computing. Prentice-Hall, Inc.

2. Gérald Tenenbaum et Michel Mendès France, 1997. Les nombres premiers. Presses Universitaires de France