PORTUGALIAE MATHEMATICA
Vol. 57 Fasc. 3 – 2000

A CELLULAR AUTOMATON ON A TORUS

C.I. Cobeli, M. Crâşmaru and A. Zaharescu

Abstract: In this paper we prove a conjecture of Brian Thwaites concerning the evolution function of a certain cellular automaton on a torus.

In the seventies, when more and more people had access to personal computers, John Conway's game of life became very popular. Since then, the study of this type of game grew up into the theory of cellular automata. In [4] (see also [1, page 311]) Brian Thwaites proposes a conjecture which leads to such a cellular automaton.

Thwaites's conjecture is: *Given any finite sequence of rational numbers, take the positive differences of successive members (including differencing the last member with the first); iteration of this operation eventually produces a set of zeros if and only if the size of the set is a power of 2.*

Our aim in this note is to prove that Thwaites conjecture holds true.

Let $a_0, ..., a_{d-1}$ be the given d rational numbers, which we may think as the heights of d poles situated around a circle. These numbers are replaced at the next step by d rational numbers given by the difference in heights of successive poles, and then the process is repeated.

Being an iteration of the same operation, it resembles Conway's life game. For now the field of play is a 1-dimensional torus and since, as we will see only finitely many numbers which depend on the initial configuration are involved, in the long run, we will end up with a cycle. Finding the lengths of these cycles, which depend mostly on d — the size of the torus —, is the interesting problem. In other words, if d is a power of 2, Thwaites conjecture says that the length of any cycle is equal to 1 (the shortest possible). We examine the lengths of the cycles that occur and provide conditions on d which guarantee that these lengths are small or long. A criterion which tests if a given integer is a period for this evolution function is given in section 3.

Received: December 20, 1998; *Revised*: March 22, 1999.
AMS Subject Classification: 11B85, 11A07.

1 – Proof of Thwaites conjecture

We begin by making some notations which set the problem in a clearer framework. Let $a_0, ..., a_{d-1}$ be the given rational numbers. For convenience, we *unpack* this ordered set of numbers by associating to it the infinite sequence $(a_0, a_1, ...)$, where the components are defined by

$$a_k = a_{k+d} \quad \text{for} \quad k \geq 0 \ . \tag{1}$$

Let us denote by $\mathbb{Q}_d$ and by $\mathbb{N}_d$ the set of all the sequences with rational and natural components respectively, satisfying (1). The evolution function $\phi : \mathbb{Q}_d \to \mathbb{Q}_d$ is defined by $\phi(a_0, a_1, ...) = (a'_0, a'_1, ...)$, where

$$a'_k = |a_k - a_{k+1}| \quad \text{for} \quad k \geq 0 \ . \tag{2}$$

With these notations, Thwaites conjecture says that for any sequence $(a_0, a_1, ...) \in \mathbb{Q}_d$, $\phi^{(n)}(a_0, a_1, ...) = (0, 0, ...)$ for all sufficiently large $n \in \mathbb{N}$ iff d is a power of 2. (Here $\phi^{(n)}$ is the repeated composition of n samples of ϕ.)

Let's note that all the components of $\phi^{(n)}(a_0, a_1, ...)$ are nonnegative if $n \geq 1$ and by multiplying all the components of the initial sequence $(a_0, a_1, ...)$ by the least common multiple of their denominators, we may assume that the domain of our evolution function is $\mathbb{N}_d$.

Let $M = \max\{a_0, ..., a_{d-1}\}$. By the definition of ϕ, it is easy to see that all the components of $\phi^{(n)}(a_0, a_1, ...)$ are integers belonging to $[0, M]$. Because there are only finitely many such periodic sequences in $\mathbb{N}_d$, it follows that given any initial configuration $(a_0, a_1, ...)$, the repeated application of the evolution function will eventually produce a cycle of sequences which keep repeating.

The next lemma shows that after sufficiently many steps we always end up with sequences with components having at most 2 distinct values.

Lemma 1. *Let d be a positive integer, $(a_0, a_1, ...)$ a sequence of nonnegative integers satisfying (1) and suppose the function ϕ is defined as above. Then there is a positive integer a such that for sufficiently large n all the components of $\phi^{(n)}(a_0, a_1, ...)$ belong to $\{0, a\}$.*

Proof: The proof is by (inverse) induction. Let us look at a portion of the sequence of numbers we get at some step. We write them on a line as follows:

$$..., b, \underbrace{0, ..., 0}_{s \text{ zeros}}, \underbrace{m, ..., m}_{u \text{ numbers}}, \underbrace{0, ..., 0}_{t \text{ zeros}}, c, ... \tag{3}$$

Here m is the maximum of all our numbers at this step, b and c are nonzero, $m > b$, $m > c$, $s \geq 0$, $t \geq 0$, $u \geq 1$ and the part of the sequence that begins and ends with m contains only 0's or m's. Then, after at most $s + u + t$ steps, the maximum of the numbers that are produced out by this portion of the sequence will be $\leq \max\{m - b, m - c\} < m$. Of course at a given step the sequence of numbers we obtain might contain several subsequences of the form (3), but what happens is that after at most d steps the maximum of the numbers at that step will be strictly less than m. The lemma then follows by induction. ∎

By multiplying all the components of the initial configuration by a^{-1}, where a is given by Lemma 1, we may assume that after sufficiently many steps all the components of the sequences we obtain are 0 or 1. Then our operation (taking the positive differences of successive members of the sequence) is nothing else than addition in the group $(\mathbb{Z}/2\mathbb{Z}, +)$.

Now there is a transparent way to generalize the game by replacing $\mathbb{Z}/2\mathbb{Z}$ by a more general finite monoid and also by playing on a multidimensional field. The operation in this case is to take the sum (or product if the multiplicative notation is used) of the closest neighbors. We only mention here that if we keep the same group $\mathbb{Z}/2\mathbb{Z}$, but play on a multidimensional torus, then we eventually obtain a sequence of zeros if and only if the size of one of the dimensions is a power of 2. This can be showed by following the same lines of proof.

Returning to our problem, let us observe that by starting with an arbitrary sequence of 0's and 1's, by applying repeatedly the evolution function, we obtain the following table which is filled with the beginning of the sequences obtained in the first few iterations.

Step	1	2	3	$\cdots$
0.	a_0	a_1	a_2	$\cdots$
1.	$a_0 + a_1$	$a_1 + a_2$	$a_2 + a_3$	$\cdots$
2.	$a_0 + a_2$	$a_1 + a_3$	$a_2 + a_4$	$\cdots$
3.	$a_0 + a_1 + a_2 + a_3$	$a_1 + a_2 + a_3 + a_4$	$a_2 + a_3 + a_4 + a_5$	$\cdots$
4.	$a_0 + a_4$	$a_1 + a_5$	$a_2 + a_6$	$\cdots$
5.	$a_0 + a_1 + a_4 + a_5$	$a_1 + a_2 + a_5 + a_6$	$a_2 + a_3 + a_6 + a_7$	$\cdots$
6.	$a_0 + a_2 + a_4 + a_6$	$a_1 + a_3 + a_5 + a_7$	$a_2 + a_4 + a_6 + a_8$	$\cdots$
7.	$a_0 + a_1 + \cdots + a_7$	$a_1 + a_2 + \cdots + a_8$	$a_2 + a_3 + \cdots + a_9$	$\cdots$
8.	$a_0 + a_8$	$a_1 + a_9$	$a_2 + a_{10}$	$\cdots$
9.	$a_0 + a_1 + a_8 + a_9$	$a_1 + a_2 + a_9 + a_{10}$	$a_2 + a_3 + a_{10} + a_{11}$	$\cdots$
10.	$a_0 + a_2 + a_8 + a_{10}$	$a_1 + a_3 + a_9 + a_{11}$	$a_2 + a_4 + a_{10} + a_{12}$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Now it is easy to see by induction that in the above table if $d = 2^m$ then the d-th row (and consequently all that follow after it) contains only 0's. Also, there are sequences of 0's and 1's, namely those containing an odd number of 1's, for which on the $(d-1)$-th row all the numbers are equal to 1. Thus, if d is a power of 2 and we start with an arbitrary set of 0's and 1's, then the process will produce 0's in d steps and only for particular a_k's in less then d steps.

The outcome in the case $d \neq 2^m$ can be also deduced easily by induction. Thus, if we start for example with the periodic sequence given by $a_0 = 1$ and $a_k = 0$ for $1 \le k \le d-1$, then 1 will always be the first number on the rows representing the steps of order a power of 2. Therefore, if d is not a power of 2 then there are sequences which will never produce a set of 0's.

We summarize our result in the following theorem which proves the Thwaites conjecture.

Theorem 1. *Let d be a positive integer and suppose the evolution function ϕ is defined as above. Then there is a rational number $r > 0$ such that the repeated application of ϕ to any initial sequence of rational numbers $(a_0, a_1, ...)$ satisfying (1) will eventually produce a cycle of sequences with the property (1) with all their components in $\{0, r\}$. Moreover, the cycle will contain only the sequence $(0, 0, ...)$ independently on the initial sequence if and only if d is a power of 2.* ∎

2 – The length of cycles

We assume in this section that the evolution function ϕ is defined on $\mathbb{U}_d$, where $\mathbb{U}_d$, is the set of all the sequences with components in $\{0, 1\}$, satisfying (1). This is not restrictive as we saw above and also has the advantage that it makes ϕ to be additive.

Theorem 1 shows that if d is a power of 2 then the length of any cycle is equal to 1. Suppose from now on that d is not a power of 2. Write $d = 2^k r$ with $k \ge 0$ and r odd, $r > 1$. Let s be the order of 2 modulo r. Thus $2^s - 1 \equiv 0 \pmod{r}$.

Let $F = \{0, 1\}$ be the field with 2 elements and let I be the ideal of $F[X]$ generated by $X^d - 1$. Map the sequence $\mathbf{a} = (a_0, ..., a_{d-1})$ to the coset

$$\psi(\mathbf{a}) \;=\; I + \sum_{i=0}^{d-1} a_i \, X^i$$

in the ring $F[X]/I$. Then $\phi(\mathbf{a}) = I + 0$ if and only if $\mathbf{a} = 0$. Moreover $\psi(\phi(\mathbf{a})) = (1 + X)\,\phi(\mathbf{a})$. It follows that we get a cycle of length n, starting with $\mathbf{e}_0 =$

$(1, 0, ..., 0)$ precisely when n is the least positive integer for which

$$(1+X)^{n+c} \equiv (1+X)^c \pmod{X^d - 1} \tag{4}$$

in $F[X]$, for some positive integer c.

We now prove that $n = 2^k(2^s - 1)$ is always a period (thus the length of a cycle will be a divisor of this number). We have:

$$(1+X)^{2^{k+s}} = 1 + X^{2^{k+s}}$$

since we are working in characteristic 2. But

$$X^{2^{k+s}} - X^{2^k} = X^{2^k}(X^{2^k(2^s-1)} - 1) \equiv 0 \pmod{X^d - 1}$$

since d divides $2^k(2^s - 1)$. Hence

$$(1+X)^{2^{k+s}} \equiv 1 + X^{2^k} = (1+X)^{2^k} \pmod{X^d - 1}$$

and we see that (4) is satisfied with $n = 2^k(2^s - 1)$ and $c = 2^k$.

Let us assume now that $d = r$ is a prime number and that s is even, $s = 2t$ say. In this case we want to show that $d(2^t - 1)$ is a period. We have $2^t \equiv -1 \pmod{d}$, so that $2^t = dm - 1$ for some integer m. Since $X^d - 1$ is coprime to X it will suffice to prove that

$$X^d(1+X)^{d(2^t-1)+d} \equiv X^d(1+X)^d \pmod{X^d - 1}\ , \tag{5}$$

taking the integer c to be d. However

$$(1+X)^{d(2^t-1)+d} = \{(1+X)^{2^t}\}^d = (1+X^{2^t})^d = (1+X^{md-1})^d$$

from which it follows that

$$X^d(1+X)^{d(2^t-1)+d} \equiv X^d(1+X^{md-1})^d = (X + X^{md})^d \pmod{X^d - 1}\ .$$

The congruence (5) then follows since we may replace every occurrence of X^d by 1, modulo $X^d - 1$. We have proved the following

Theorem 2.

(i) *Let $d = 2^k r$, r odd and let s be the order of 2 modulo r. Then $2^k(2^s - 1)$ is a period.*

(ii) *If d is an odd prime and s is even, $s = 2t$, then $d(2^t - 1)$ is a period.*

One can ask about *short* and *long* periods.

Let us assume that d is a prime. Then the period provided by Theorem 2 has length 2^s-1 or $d(2^t-1)$. In both cases the length is a multiple of d.

Short periods:

If d is a Mersenne prime, i.e. a prime d of the form $d = 2^p - 1$ the length of the above period is d. In this case each such period will actually be a cycle. One doesn't know if there are infinitely many such primes. The first Mersenne primes are 3, 7, 31, $127, \ldots$. As examples, we show below the cycles produced by the initial configuration $\mathbf{e}_0$ when $d = 3$ and $d = 7$:

$$(1,0,0) \to (1,0,1) \to (1,1,0) \to (0,1,1) \to (1,0,1) \to \cdots$$

and

$$\begin{aligned} &(1,0,0,0,0,0,0) \to (1,0,0,0,0,0,1) \to (1,0,0,0,0,1,0) \to \\ &\to (1,0,0,0,1,1,1) \to (1,0,0,1,0,0,0) \to (1,0,1,1,0,0,1) \to \\ &\to (1,1,0,1,0,1,0) \to (0,1,1,1,1,1,1) \to (1,0,0,0,0,0,1) \to \cdots \end{aligned}$$

respectively.

Long periods:

In case 2 is a primitive root modulo d, the period provided by Theorem 2 is as large as $d(2^{\frac{d-1}{2}}-1)$. Artin's conjecture, still unsolved, says that there are infinitely many such primes. The first prime numbers which satisfy Artin's conjecture are 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, ...

We give below the cycle obtained in case $d = 5$.

$$\begin{aligned} &(1,0,0,0,0) \to (1,0,0,0,1) \to (1,0,0,1,0) \to (1,0,1,1,1) \to \\ &\to (1,1,0,0,0) \to (0,1,0,0,1) \to (1,1,0,1,1) \to (0,1,1,0,0) \to \\ &\to (1,0,1,0,0) \to (1,1,1,0,1) \to (0,0,1,1,0) \to (0,1,0,1,0) \to \\ &\to (1,1,1,1,0) \to (0,0,0,1,1) \to (0,0,1,0,1) \to (0,1,1,1,1) \to \\ &\to (1,0,0,0,1) \to \cdots \end{aligned}$$

In their papers on Artin's conjecture Rajiv Gupta and M. Ram Murty [2] and Heath-Brown [3] use results by Bombieri, Friedlander, Fouvry, Deshouillers and Iwaniec to show that there are infinitely many primes p for which all the prime factors of $\frac{p-1}{2}$ are larger than $p^{1/4}$,

This shows that there are primes p for which the lengths of our periods are huge, more precisely they are larger than $2^{p^{1/4}}$.

The lengths of cycles obtained for all primes $d \leq 47$ are given in the following Table.

d	length of cycle	s	$2^s - 1$	$d(2^{s/2} - 1)$
3	3	2	3	3
5	$15 = 5 \cdot 3$	4	15	15
7	7	3	7	
11	$341 = 11 \cdot 31$	10	$341 \cdot 3$	341
13	$819 = 13 \cdot 63$	12	$819 \cdot 5$	819
17	$255 = 17 \cdot 15$	8	255	255
19	$9709 = 19 \cdot 511$	18	$9709 \cdot 3^3$	9709
23	$2047 = 23 \cdot 89$	11	2047	
29	$475107 = 29 \cdot 16383$	28	$475107 \cdot 5 \cdot 113$	475107
31	31	5	31	
37	$3233097 = 37 \cdot 87381$	36	$3233097 \cdot 3 \cdot 5 \cdot 13 \cdot 109$	$3233097 \cdot 3$
41	$41943 = 41 \cdot 1023$	20	$41943 \cdot 5^2$	41943
43	$5461 = 43 \cdot 127$	14	$5461 \cdot 3$	5461
47	$8388607 = 47 \cdot 178481$	23	8388607	

3 – A more general evolution function

In this section we introduce a more general evolution function and give a useful method to calculate its repeated composition by itself. Finally, we deduce a criterion which discerns if a given integer is or is not the length of a cycle of chains produced by our original evolution function.

Let d be a positive integer and $\mathcal{S} = \{0,1\}^d$. We denote by $\rho(\mathbf{x})$ the circular rotation to the right of the vector $\mathbf{x} \in \mathcal{S}$ (e.g. for $d = 7,\ \rho(1,1,0,1,0,0,0) = (0,1,1,0,1,0,0)$) and $\cdot\colon \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ the *xor* function (which is the componentwise addition mod 2).

Let $a_1, a_2, ..., a_s$ be s positive integers and define the evolution function $\phi\colon \mathcal{S} \to \mathcal{S}$ by

$$\phi(\mathbf{x}) \;=\; \rho^{(a_1)}(\mathbf{x}) \,\cdots\, \rho^{(a_s)}(\mathbf{x}) \;.$$

Note that for $s = 2,\ a_1 = 0$ and $a_2 = 1$ we get our previous evolution function.

The following lemma adds together some properties of these functions.

Lemma 2. *For any nonnegative integers k, m, n and any $\mathbf{x}, \mathbf{y} \in \mathcal{S}$ we have:*

1. $\rho(\mathbf{x}\mathbf{y}) = \rho(\mathbf{x})\,\rho(\mathbf{y})$,
2. $\phi(\mathbf{x}\mathbf{y}) = \phi(\mathbf{x})\,\phi(\mathbf{y})$,
3. $\phi(\rho(\mathbf{x})) = \rho(\phi(\mathbf{x}))$,
4. $\phi^{(m)}(\mathbf{x}\mathbf{y}) = \phi^{(m)}(\mathbf{x})\,\phi^{(m)}(\mathbf{y})$,
5. $\phi^{(m)}(\rho(\mathbf{x})) = \rho(\phi^{(m)}(\mathbf{x}))$,
6. $\phi^{(m)}(\rho^{(n)}(\mathbf{x})) = \rho^{(n)}(\phi^{(m)}(\ x))$,
7. $\phi^{(2^k)}(\mathbf{x}) = \rho^{(2^k a_1)}(\mathbf{x}) \cdots \rho^{(2^k a_s)}(\mathbf{x})$.

Proof: Everything follows easily by definitions and/or by induction. ∎

As a consequence, we immediately obtain the following:

Corollary 1. *Suppose $d = 2^k$. Then, for any $\mathbf{x} \in \mathcal{S}$ and $n \geq 1$ we have that $\phi^{(d+n-1)}(\mathbf{x}) = \mathbf{0}$ if s is even and $\phi^{(nd)}(\mathbf{x}) = \mathbf{x}$ if s is odd.* ∎

Remark. It is easy to see that properties **1**–**7** from Lemma 2 do not depend essentially on $\mathcal{S}$. Thus we may replace $\{0,1\}$ by a more general monoid (a nilpotent one may be of particular interest), for which similar consequences still hold true. Let

(6) $$k = 2^{l_0} + 2^{l_1} + \cdots + 2^{l_\mu}$$

be the representation in base 2 of the positive integer k and assume $l_0 < \ldots < l_\mu$. We denote

(7) $$r_{ij} \equiv 2^{l_i} a_j \pmod{d}, \qquad 0 \leq r_{ij} \leq d-1$$

for $0 \leq i \leq \mu$ and $1 \leq j \leq s$. □

The next proposition gives an algorithm for the calculation of $\phi^{(k)}(\mathbf{x})$ in $O_s(\log k)$ steps.

Proposition 1. *Let $\mathbf{x} \in \mathcal{S}$ and*

$$\mathbf{y}_0 = \rho^{r_{01}}(\mathbf{x}) \cdots \rho^{r_{0s}}(\mathbf{x}) .$$

Define inductively

$$\mathbf{y}_j = \rho^{r_{j1}}(\mathbf{y}_{j-1}) \cdots \rho^{r_{js}}(\mathbf{y}_{j-1})$$

for $1 \leq j \leq \mu$. Then

$$\phi^{(k)}(\mathbf{x}) = \mathbf{y}_\mu .$$

Proof: Let $k = k_1 + 2^{l_0}$. Using Lemma 2 we have

$$\begin{aligned}
\phi^{(k)}(\mathbf{x}) &= \phi^{(k_1+2^{l_0})}(\mathbf{x}) = \phi^{(k_1)}\Big(\phi^{(2^{l_0})}(\mathbf{x})\Big) \\
&= \phi^{(k_1)}\Big(\rho^{(2^{l_0}a_1)}(\mathbf{x})\cdots\rho^{(2^{l_0}a_s)}(\mathbf{x})\Big) \\
&= \phi^{(k_1)}\Big(\rho^{(r_{01})}(\mathbf{x})\cdots\rho^{(r_{0s})}(\mathbf{x})\Big) = \phi^{(k_1)}(\mathbf{y}_0) .
\end{aligned}$$

Similarly, let $k_1 = k_2 + 2^{l_1}$. Then we have

$$\begin{aligned}
\phi^{(k_1)}(\mathbf{y}_0) &= \phi^{(k_2+2^{l_1})}(\mathbf{y}_0) = \phi^{(k_2)}\Big(\phi^{(2^{l_1})}(\mathbf{y}_0)\Big) \\
&= \phi^{(k_2)}\Big(\rho^{(2^{l_1}a_1)}(\mathbf{y}_0)\cdots\rho^{(2^{l_1}a_s)}(\mathbf{y}_0)\Big) \\
&= \phi^{(k_2)}\Big(\rho^{(r_{11})}(\mathbf{y}_0)\cdots\rho^{(r_{1s})}(\mathbf{y}_0)\Big) = \phi^{(k_2)}(\mathbf{y}_1) .
\end{aligned}$$

It is clear now that the proposition follows by induction following the same procedure. ∎

A direct way to calculate $\phi^{(k)}(\mathbf{x})$ is given in the next theorem.

Theorem 3. *For any positive integer k represented as in (6), we have*

$$\phi^{(k)}(\mathbf{x}) = \prod_{1\le i_1,\ldots,i_{\mu+1}\le s} \rho^{(r_{0\,i_1}+\cdots+r_{\mu\,i_{\mu+1}})}(\mathbf{x}) .$$

Proof: The proof is by induction on μ.
If $\mu = 0$, then $k = 2^{l_0}$ and by Lemma 2

$$\phi^{(2^{l_0})}(\mathbf{x}) = \rho^{(2^{l_0}a_1)}(\mathbf{x})\cdots\rho^{(2^{l_0}a_s)}(\mathbf{x}) = \rho^{(r_{01})}(\mathbf{x})\cdots\rho^{(r_{0s})}(\mathbf{x}) .$$

Suppose the statement is true for $\mu-1$. Let $k_1 = k - 2^{l_\mu}$. Then the representation of k_1 in base 2 has μ digits and we can apply to it the induction hypothesis. Thus, by Lemma 2 we have

$$\begin{aligned}
\phi^{(k)}(\mathbf{x}) &= \phi^{(2^{l_\mu}+k_1)}(\mathbf{x}) = \phi^{(2^{l_\mu})}\Big(\phi^{(k_1)}(\mathbf{x})\Big) \\
&= \phi^{(2^{l_\mu})}\left(\prod_{1\le i_1,\ldots,i_\mu\le s} \rho^{(r_{0\,i_1}+\cdots+r_{\mu-1\,i_\mu})}(\mathbf{x})\right) .
\end{aligned}$$

By the definition of $\phi(\mathbf{x})$, (7) and Lemma 2 this is

$$= \prod_{j=1}^{s} \rho^{(2^{l_\mu} a_j)} \Bigg(\prod_{1 \le i_1,\dots,i_\mu \le s} \rho^{(r_{0\,i_1} + \cdots + r_{\mu-1\,i_\mu})}(\mathbf{x}) \Bigg)$$
$$= \prod_{j=1}^{s} \rho^{(r_{\mu j})} \Bigg(\prod_{1 \le i_1,\dots,i_\mu \le s} \rho^{(r_{0\,i_1} + \cdots + r_{\mu-1\,i_\mu})}(\mathbf{x}) \Bigg)$$
$$= \prod_{1 \le i_1,\dots,i_{\mu+1} \le s} \rho^{(r_{0\,i_1} + \cdots + r_{\mu\,i_{\mu+1}})}(\mathbf{x}) \ ,$$

which concludes the proof of the theorem. ∎

Now we apply this result to the particular evolution function from the previous sections. Thus, from now on we assume that $s = 2$, $a_1 = 0$ and $a_2 = 1$, that is $\phi(\mathbf{x}) = \mathbf{x}\,\rho(\mathbf{x})$.

Corollary 2. *Let* $k = 2^{l_0} + 2^{l_1} + \cdots + 2^{l_\mu}$ *be the representation in base 2 of the positive integer* k*, where* $l_0 < \cdots < l_\mu$*, and* $\phi(\mathbf{x}) = \mathbf{x}\,\rho(\mathbf{x})$*. Denote*

$$\mathcal{R}_k \;=\; \Big\{ r :\ r \equiv 2^{l_i} \pmod{d},\ \ 0 \le r \le d-1,\ \ \textit{for some}\ 0 \le i \le \mu \Big\}\ .$$

Then

$$\phi^{(k)}(\mathbf{x}) \;=\; \mathbf{x} \prod_{R \subset \mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{x})$$

for any $\mathbf{x} \in \mathcal{S}$.

Proof: By Theorem 3

$$\phi^{(k)}(\mathbf{x}) \;=\; \prod_{1 \le i_1,\dots,i_{\mu+1} \le 2} \rho^{(r_{0\,i_1} + \cdots + r_{\mu\,i_{\mu+1}})}(\mathbf{x}) \ . \tag{8}$$

By (7) and our hypothesis $r_{j1} = 0$ and $r_{j2} \equiv 2^{l_j} \pmod{d}$, $0 \le r_{j2} < d$ for $0 \le j \le \mu$. The corollary then follows by isolating in (8) the term with $i_1 = \ldots = i_{\mu+1} = 1$, that is $\rho^{(0)}(\mathbf{x})$ $(= \mathbf{x})$ and using the fact that

$$\rho^{\left(\sum_{r\in\emptyset} r\right)}(\mathbf{x}) \;=\; \mathbf{0}\ .\ ∎$$

From Corollary 2 we deduce a criterion for cycling. Thus, $\phi^{(k)}(\mathbf{x}) = \mathbf{x}$ is equivalent to

$$\prod_{R \subset \mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum_{r\in R} r\right)}(\mathbf{x}) \;=\; \mathbf{0}\ . \tag{9}$$

Starting with $\mathbf{x} = \mathbf{e}_0 = (1, 0, ..., 0)$, we get $\phi(\mathbf{e}_0) = \mathbf{e}_0\, \rho(\mathbf{e_0}) = (1, 1, 0, ..., 0) = \mathbf{e}_1$. Then, by (9) and Lemma 2, we deduce

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum\limits_{r\in R} r\right)}(\mathbf{e}_0) \cdot \prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(1+\sum\limits_{r\in R} r\right)}(\mathbf{e}_0) \;=\; \mathbf{0}\;,$$

which can be written as

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum\limits_{r\in R} r\right)}(\mathbf{e}_0) \;=\; \prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(1+\sum\limits_{r\in R} r\right)}(\mathbf{e}_0)$$

or

$$\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum\limits_{r\in R} r\right)}(\mathbf{e}_0) \;=\; \rho\Bigg(\prod_{R\subset\mathcal{P}(\mathcal{R}_k)} \rho^{\left(\sum\limits_{r\in R} r\right)}(\mathbf{e}_0)\Bigg)\;. \tag{10}$$

For any $m \in \{1, ..., d\}$ let

$$\nu_{k,d}(m) \;=\; \#\Big\{R \subset \mathcal{R}_k\colon \sum_{r\in\mathcal{R}} r \equiv m \pmod d\Big\}\;.$$

Then (10) becomes

$$\prod_{m=1}^{d} \rho^{\,\nu_k(m)}(\mathbf{e}_0) \;=\; \rho\Big(\prod_{m=1}^{d} \rho^{\,\nu_k(m)}(\mathbf{e}_0)\Big)\;.$$

Since the only invariants of ρ are $(0, ..., 0)$ and $(1, ..., 1)$ we obtain the following:

Corollary 3. *A positive integer k is a period for $\phi(\mathbf{x}) = \mathbf{x}\,\rho(\mathbf{x})$ if and only if the numbers $\nu_{k,d}(m)$, $1 \le m \le d$ have the same parity.* ∎

We checked the values of $\nu_{k,d}(m)$ with k being the length of the shortest cycle for different values of d and we found some interesting regularity properties. Thus, $\nu_{k,d}(m)$ not only have the same parity but most of the time they are equal. Some nontrivial examples are:

1. If $d = 11$ then $k = 341 = 101010101_2$,
$\nu_{341,11}(11) = 1$ and $\nu_{341,11}(m) = 3$ for $1 \le m \le 10$.

2. If $d = 13$ then $k = 819 = 1100110011_2$,
$\nu_{819,13}(13) = 3$ and $\nu_{819,13}(m) = 5$ for $1 \le m \le 12$.

3. If $d = 19$ then $k = 9709 = 10010111101101_2$,
$\nu_{9709,19}(19) = 25$ and $\nu_{9709,19}(m) = 27$ for $1 \le m \le 18$.

4. If $d = 29$ then $k = 475107 = 1110011111111100011_2$,
$\nu_{475107,29}(29) = 563$ and $\nu_{475107,29}(m) = 565$ for $1 \le m \le 28$.

5. If $d = 37$ then $k = 3233097 = 1100010101010101001001$ and

m	1	2	3	4	5	6	7	8	9	10
$\nu_{3233097,37}(m)$	23	27	25	23	27	29	25	23	27	29

m	11	12	13	14	15	16	17	18	19	20
$\nu_{3233097,37}(m)$	27	29	33	33	31	31	31	29	29	31

m	21	22	23	24	25	26	27	28	29	30
$\nu_{3233097,37}(m)$	31	31	33	33	29	27	29	27	23	25

m	31	32	33	34	35	36	37
$\nu_{3233097,37}(m)$	29	27	23	25	27	23	19

5′. If $d = 37$ and we take k' to be defined by $k' = 3233097 * 3 = 9699291 = 10010011111111111011011_2$, then
$\nu_{9699291,37}(37) = 7083$ and $\nu_{9699291,37}(m) = 7085$ for $1 \le m \le 36$.

6. If $d = 41$ then $k = 41943 = 1010001111010111_2$,
$\nu_{41943,41}(41) = 23$ and $\nu_{41943,41}(m) = 25$ for $1 \le m \le 40$.

7. If $d = 43$ then $k = 5461 = 1010101010101_2$,
$\nu_{5461,43}(43) = 1$ and $\nu_{5461,43}(m) = 3$ for $1 \le m \le 42$.

This leads us to make the following

Conjecture. *Suppose d is a prime number, s is the order of $2 \bmod d$, s is even and $k = d(2^{s/2} - 1)$. Then*

$$\nu_{k,d}(1) = \nu_{k,d}(2) = \cdots = \nu_{k,d}(d-1) = \nu_{k,d}(d) + 2 \,. \blacksquare$$

ACKNOWLEDGEMENT – We are very grateful to the referee for providing us with a slightly different approach, which we follow in the proof of Theorem 2, which is simpler than our original approach and gives better results (precisely, it provides proofs for both parts (i) and (ii) of Theorem 2, while in the original version of the paper we only proved part (i) and proposed (ii) as a conjecture).

REFERENCES

[1] Campbell, J.P. – Reviews, *Mathematics Magazine,* 69(4) (October 1996), 311–313.

[2] Gupta, R. and Ram Murty, M. – A Remark on Artin's conjecture, *Invent. Math.,* 78 (1984), 127–130.

[3] Heath-Brown, D.R. – Artin's conjecture for primitive roots, *Quart. J. Math. Oxford,* 37(2), (1986), 27–38.

[4] Thwaites, B. – Two conjectures or how to win £ 1100, *Mathematical Gazette,* 80 (March 1996), 35–36.

Cristian Ioan Cobeli,
Mathematics Research Institute of the Romanian Academy,
P.O. Box 1-764, Bucharest, 70700 – ROMANIA
E-mail: ccobeli@stoilow.imar.ro

and

Marcel Crâşmaru,
Vatra Dornei, 5975 – ROMANIA
E-mail: mi@assist.cccis.ro

and

Alexandru Zaharescu,
McGill University, Department of Mathematics and Statistics, Burnside Hall,
805 Sherbrooke Street West, Montreal, Quebec, Canada, H3A-2K6 – CANADA
and
Mathematics Research Institute of the Romanian Academy,
P.O. Box 1-764, Bucharest, 70700 – ROMANIA
E-mail: zaharesc@math.mcgill.ca