Publ. Math. Debrecen
63/3 (2003), 389–400

Babbage equation on the circle

By WITOLD JARCZYK (Zielona Góra and Katowice)

Abstract. Given a positive integer n a description of all continuous self-mappings of the unit circle, having the identity as the n-th iterate, is presented.

Introduction

It seems that it was CH. BABBAGE ([1]; cf. also [5, Chap. XV] and [6, Chap. 11]) who still in 1815 dealt with the equation

$$\varphi^n(x) = x \tag{1}$$

where φ is an unknown self-mapping of a set and, for a given positive integer n, φ^n stands for the n-th iterate of φ. Equation (1) is intensively investigated till now (cf., for instance, [3, Section 2] and the bibliography therein). Its solutions are named *n-th iterative roots of identity*. In the case $n = 2$ such roots are called *involutions*. If n is the smallest positive integer such that φ is an n-th root we say that n is the *order of* φ.

Studying solutions of (1) we may actually confine ourselves to roots of order n which can be read from the following.

Proposition 1. *Let $\varphi : X \to X$ be an iterative root of order n of identity. If $m \in \mathbb{N}$ and $\varphi^m = \mathrm{id}_X$ then n divides m.*

Mathematics Subject Classification: Primary 39B12; Secondary 26A18, 58F08.
Key words and phrases: iterative root, Babbage equation, unit circle.

Proof. Fix a positive integer m such that $\varphi^m = \mathrm{id}_X$. Then $m = pn + r$ with $p \in \mathbb{N}$ and $r \in \{0, \dots, n-1\}$. Moreover,

$$\varphi^r = \mathrm{id}_X \circ \varphi^r = (\varphi^n)^p \circ \varphi^r = \varphi^{pn+r} = \varphi^m = \mathrm{id}_X .$$

Therefore, in view of the definition of n, we have $r = 0$, that is $m = pn$. □

Thus, given a positive integer m, to determine all m-th roots of identity it is enough to find all roots of order n for every divisor n of m.

Corollary 1. *Let $f : X \to X$, $x_0 \in X$ and let n be the smallest positive integer such that $f^n(x_0) = x_0$. If $m \in \mathbb{N}$ and $f^m(x_0) = x_0$ then n divides m.*

Proof. Apply Proposition 1 to the restriction of f to $\{x_0, \dots, f^{n-1}(x_0)\}$ or simply repeat the argument proving it. □

Clearly every solution of (1) is a bijection of its domain. What concerns monotonic and/or continuous solutions of (1) defined on a set of reals we have what follows.

1. *Every monotonic self-mapping of a set of reals satisfying* (1) *is either the identity function, or a decreasing involution* (E. Vincze [8], N. McShane [7]; cf. also M. Kuczma [5, Theorem 15.2], M. Kuczma, B. Choczewski, R. Ger [6, Theorems 11.7.1 and 11.2.1]).

2. *For solutions of* (1) *defined on a real interval monotonicity and continuity are equivalent* (cf. [5, Theorem 5.3] and [6, Theorem 11.2.1]).

3. *All decreasing involutions defined on a real interval I are given by*

$$\varphi(x) = \begin{cases} \varphi_0(x) & \textit{for } x \in I \cap (-\infty, x_0], \\ \varphi_0^{-1}(x) & \textit{for } x \in I \cap (x_0, \infty), \end{cases}$$

where $x_0 \in I$ and φ_0 is an arbitrary decreasing bijection mapping $I \cap (-\infty, x_0]$ onto $I \cap [x_0, \infty)$ (cf. [5, Lemma 15.2] and [6, Theorem 11.7.2]).

Thus, for an interval domain, continuous solutions of (1), different from the identity function, *depend on an arbitrary function.* The aim of the present paper is to show a similar effect for self-mappings of the unit circle S^1; we will find all continuous iterative roots of identity defined on S^1, that is all continuous functions $\phi : S^1 \to S^1$ satisfying the Babbage equation

$$\phi^n(z) = z \tag{2}$$

with a positive integer n. As continuous bijections of a compact set they are necessarily homeomorphisms. (In particular, every continuous involution defined on S^1 is a homeomorphism.) For this reason we recall a terminology useful in studying homeomorphisms of the circle. In what follows, homeomorphicity of a self-mapping F of S^1 means, among others, that F maps S^1 *onto* S^1.

Given points $z_0, \dots, z_{m-1} \in S^1$ with $m \geq 2$ we write

$$z_0 < \cdots < z_{m-1}$$

if there are reals $t_1, \dots, t_{m-1}$ such that

$$0 < t_1 < \cdots < t_{m-1} < 1 \text{ and } z_j = z_0 \, \mathrm{e}^{2\pi i t_j} \quad \text{for } j \in \{1, \dots, m-1\}.$$

This is a modification of the notion of *cyclic order* proposed by M. Bajger [2]. The following is almost obvious and is a simple consequence of the above definition.

Remark 1. If $z_0, \dots, z_{m-1} \in S^1$ with $m \geq 2$ and $z_0 < \cdots < z_{m-1}$ then

$$z_{j \,(\bmod m)} < \cdots < z_{(j+m-1)\,(\bmod m)}$$

for every $j \in \mathbb{N}$.

For any different points $z_1, z_2 \in S^1$ define the *arcs* $(z_1, z_2), [z_1, z_2)$ and $(z_1, z_2]$ by

$$(z_1, z_2) := \{z \in S^1 : z_1 < z < z_2\},$$

$$[z_1, z_2) := (z_1, z_2) \cup \{z_1\} \quad \text{and} \quad (z_1, z_2] := (z_1, z_2) \cup \{z_2\},$$

respectively. A standard argument allows us to state that

$$(z_1, z_2) = \left\{\mathrm{e}^{2\pi i t} \in S^1 : t \in (t_1, t_2)\right\}$$

where t_1, t_2 are the unique reals satisfying the conditions

$$z_1 = \mathrm{e}^{2\pi i t_1}, \; z_2 = \mathrm{e}^{2\pi i t_2}, \quad 0 \leq t_1 < t_2 < t_1 + 1 < 2.$$

It is well-known (cf., for instance, [4, Chap. 2, Section 3] or [9, Chap. 6]) that for every homeomorphism $F: S^1 \to S^1$ there is a (unique up to an additive integer constant) homeomorphism $f: \mathbb{R} \to \mathbb{R}$ such that

$$F\left(\mathrm{e}^{2\pi it}\right) = \mathrm{e}^{2\pi if(t)} \quad \text{for } t \in \mathbb{R}$$

and f satisfies the Abel equations

$$f(t+1) = f(t) + 1$$

if it is increasing and

$$f(t+1) = f(t) - 1$$

if f is decreasing; every such an f is called a *lift of* F. In the first case we say that F *preserves orientation*. Otherwise F *reverses orientation*.

1. Roots of identity having fixed points

We start with

Theorem 1. *Let ϕ be a homeomorphism of S^1 satisfying* (2) *and having a fixed point.*

(i) *If ϕ preserves orientation then it is the identity function.*

(ii) *If ϕ reverses orientation then it is an involution.*

Proof. Denote by φ a lift of ϕ. Therefore $\varphi: \mathbb{R} \to \mathbb{R}$ is a homeomorphism and

$$\phi\left(\mathrm{e}^{2\pi it}\right) = \mathrm{e}^{2\pi i\varphi(t)} \quad \text{for } t \in \mathbb{R}. \tag{3}$$

Let $t_0 \in \mathbb{R}$ be such that $\phi\left(\mathrm{e}^{2\pi it_0}\right) = \mathrm{e}^{2\pi it_0}$. Then, by (3), $\varphi(t_0) = t_0 + p$ for an integer p. Replacing the lift φ by $\varphi - p$, if necessary, we may additionally assume that $p = 0$, that is $\varphi(t_0) = t_0$. Since ϕ satisfies (2) and (3) and it is continuous, there is an integer k such that

$$\varphi^n(t) = t + k \quad \text{for } t \in \mathbb{R}. \tag{4}$$

Applying (4) to t_0 we get

$$t_0 = \varphi^n(t_0) = t_0 + k,$$

which means that $k = 0$ and, consequently, φ satisfies equation (1).

Put $\varepsilon = 1$ if the homeomorphism φ is increasing and $\varepsilon = 2$ otherwise. Then φ^ε is strictly increasing. Thus, if $\varphi^\varepsilon(t) \neq t$, say $\varphi^\varepsilon(t) > t$ for a $t \in \mathbb{R}$ then, since φ satisfies (1), we would have

$$t < \varphi^\varepsilon(t) < \cdots < \varphi^{n\varepsilon}(t) = t$$

which is impossible. Consequently, $\varphi^\varepsilon(t) = t$ for each $t \in \mathbb{R}$ and both the statements follow. □

As an immediate corollary we obtain the first of our main results.

Theorem 2. *The only homeomorphism of S^1 satisfying* (2)*, preserving orientation and having a fixed point is the identity function.*

Now, following Theorem 1, we will study involutions reversing orientation.

Proposition 2. *For every different points $z_0, z_1 \in S^1$ and every invertible function ϕ_0 mapping $[z_0, z_1)$ onto $(z_1, z_0]$ and sending z_0 to z_0 the formula*

$$\phi(z) = \begin{cases} \phi_0(z), & \text{if} \quad z \in [z_0, z_1), \\ z_1, & \text{if} \quad z = z_1, \\ \phi_0^{-1}(z), & \text{if} \quad z \in (z_1, z_0), \end{cases} \tag{5}$$

defines a unique extension $\phi : S^1 \to S^1$ of ϕ_0 to an involution.

Proof. It is enough to observe that $\phi_0((z_0, z_1)) = (z_1, z_0)$ and make a standard computation. □

Theorem 3. *For every different points $z_0, z_1 \in S^1$ any homeomorphism ϕ_0 mapping $[z_0, z_1)$ onto $(z_1, z_0]$ can be uniquely extended to an involution $\phi : S^1 \to S^1$. Moreover, ϕ is a reversing orientation homeomorphism with z_0 and z_1 as unique fixed points and it is defined by* (5).

Conversely: if $\phi : S^1 \to S^1$ is a continuous involution and reverses orientation then it has exactly two fixed points $z_0, z_1 \in S^1$ and maps $[z_0, z_1)$ onto $(z_1, z_0]$.

Proof. Fix $z_0, z_1 \in S^1, z_0 \neq z_1$, and a homeomorphism ϕ_0 mapping $[z_0, z_1)$ onto $(z_1, z_0]$. Then $\phi_0(z_0) = z_0$ and $\lim_{z\to z_1} \phi_0(z) = z_1$. Thus, by

Proposition 2, formula (5) defines a unique extension $\phi : S^1 \to S^1$ of ϕ_0 to an involution which, in addition, is a homeomorphism having z_0 and z_1 as unique fixed points. Since ϕ_0 cannot be the identity function, Theorem 2 implies that ϕ reverses orientation.

Now let $\phi : S^1 \to S^1$ be a continuous involution which reverses orientation and take an arbitrary lift $\varphi : \mathbb{R} \to \mathbb{R}$ of ϕ. As a decreasing continuous function, defined on the real line, φ has exactly one fixed point, say t_0. Then

$$\varphi(t_0) - t_0 + 1 = 1 > 0.$$

Moreover, since

$$\varphi(t+1) = \varphi(t) - 1 \quad \text{for } t \in \mathbb{R},$$

we have

$$\varphi(t_0 + 1) - (t_0 + 1) + 1 = -1 < 0.$$

Thus, by continuity and strict monotonicity of the function $\mathbb{R} \ni t \mapsto \varphi(t) - t + 1$, we can find a unique $t_1 \in (t_0, t_0 + 1)$ such that $\varphi(t_1) = t_1 - 1$; in addition, $\varphi([t_0, t_1)) = (t_1 - 1, t_0]$ and t_0, t_1 are the unique reals $t \in [t_0, t_0 + 1)$ satisfying the condition $\varphi(t) \in t + \mathbb{Z}$. Consequently, according to (3), $z_0 := \mathrm{e}^{2\pi i t_0}$ and $z_1 := \mathrm{e}^{2\pi i t_1}$ are the unique fixed points of ϕ and $\phi([z_0, z_1)) = (z_1, z_0]$. $\square$

2. Roots of identity without fixed points

Any lift of a reversing orientation homeomorphism of a circle, being a decreasing continuous function defined on $\mathbb{R}$, has a fixed point. Therefore, homeomorphisms with no fixed points necessarily preserve orientation.

Proposition 3. *For every integer $k \in \{1, \dots, n-1\}$ relatively prime to n, points $z_0, \dots, z_{n-1} \in S^1$ such that $z_0 < \cdots < z_{n-1}$ and every invertible function ϕ_0 mapping $[z_0, z_{n-1})$ onto $[z_k, z_{k-1})$ and satisfying the condition*

$$\phi_0([z_{j-1}, z_j)) = [z_{j-1+k}, z_{j+k}) \quad \textit{for } j \in \{1, \dots, n-1\} \tag{6}$$

(*with* $z_j := z_{j\,(\bmod\, n)}$ *for* $j \geq n$) *the formula*

$$\phi(z) = \begin{cases} \phi_0(z), & \text{if} \quad z \in [z_0, z_{n-1}), \\ (\phi_1 \circ \cdots \circ \phi_{n-1})^{-1}(z), & \text{if} \quad z \in [z_{n-1}, z_0), \end{cases} \tag{7}$$

where

$$\phi_j := \phi_0|_{[z_{j(n-k)-1}, z_{j(n-k)})} \quad \text{for } j \in \{1, \ldots, n-1\} \tag{8}$$

defines a unique extension $\phi : S^1 \to S^1$ *of* ϕ_0 *to a solution of* (2)*; if* $z \in S^1$, $j \in \{1, \ldots, n\}$ *and* $\phi^j(z) = z$ *then* $j = n$.

PROOF. Fix an integer $k \in \{1, \ldots, n-1\}$ relatively prime to n, and points $z_0, \ldots, z_{n-1} \in S^1$ with $z_0 < \cdots < z_{n-1}$. Put $z_j := z_{j\,(\bmod\, n)}$ for $j \geq n$. Let ϕ_0 be an invertible function mapping $[z_0, z_{n-1})$ onto $[z_k, z_{k-1})$ and satisfying (6). By (8) and (6) we have

$$\phi_{j+1}([z_{(j+1)(n-k)-1}, z_{(j+1)(n-k)})) = [z_{j(n-k)-1}, z_{j(n-k)})$$

for $j \in \{1, \ldots, n-2\}$ whenever $n \geq 3$ and

$$\phi_1([z_{n-k-1}, z_{n-k})) = [z_{n-1}, z_n) = [z_{n-1}, z_0).$$

Since $(n-1)(n-k) = n(n-k-1)+k$, we have $[z_{(n-1)(n-k)-1}, z_{(n-1)(n-k)}) = [z_{k-1}, z_k)$. Thus $\phi_1 \circ \cdots \circ \phi_{n-1}$ maps $[z_{k-1}, z_k)$ onto $[z_{n-1}, z_0)$ and formula (7) defines a function $\phi : S^1 \to S^1$; in particular (cf. also (6)),

$$\phi([z_{j-1}, z_j)) = [z_{j-1+k}, z_{j+k}) \quad \text{for } j \in \{1, \ldots, n\}. \tag{9}$$

Fix an arbitrary $z \in S^1$. Then $z \in [z_{l-1}, z_l)$ for a unique $l \in \{1, \ldots, n\}$. Since n and k are relatively prime, there is exactly one $m \in \{0, \ldots, n-1\}$ satisfying $(l + mk)(\bmod\, n) = 0$. If $m = 0$ then $l = n$, $z \in [z_{n-1}, z_0)$ and, by (7), (8) and (6),

$$\phi^n(z) = \phi^{n-1} \circ \phi(z) = \phi_1 \circ \cdots \circ \phi_{n-1} \circ (\phi_1 \circ \cdots \circ \phi_{n-1})^{-1}(z) = z.$$

In the case $m \geq 1$ we have $[z_{l-1}, z_l) = [z_{m(n-k)-1}, z_{m(n-k)})$, whence, again by (7), (8) and (6),

$$\phi^m(z) = \phi_1 \circ \cdots \circ \phi_m(z) \in [z_{n-1}, z_0)$$

and

$$\begin{aligned}\phi^{m+1}(z) &= (\phi_1 \circ \cdots \circ \phi_{n-1})^{-1}(\phi^m(z)) \\ &= \phi_{n-1}^{-1} \circ \cdots \circ \phi_1^{-1} \circ \phi_1 \circ \cdots \circ \phi_m(z) \in [z_{k-1}, z_k) \\ &= [z_{(n-1)(n-k)-1}, z_{(n-1)(n-k)}).\end{aligned}$$

If $m = n-1$ we get $\phi^n(z) = \phi^{m+1}(z) = z$. Otherwise

$$\phi^{m+1}(z) = \phi_{n-1}^{-1} \circ \cdots \circ \phi_{m+1}^{-1}(z)$$

whence

$$\begin{aligned}\phi^n(z) &= \phi^{n-m-1} \circ \phi^{m+1}(z) \\ &= \phi_{m+1} \circ \cdots \circ \phi_{n-1} \circ \phi_{n-1}^{-1} \circ \cdots \circ \phi_{m+1}^{-1}(z) = z.\end{aligned}$$

Consequently, in all the cases we obtain $\phi^n(z) = z$. Suppose that $\phi^j(z) = z$ for a $j \in \{1, \ldots, n-1\}$. By (9) we have $\phi^j([z_{l-1}, z_l)) = [z_{l-1+jk}, z_{l+jk})$. Hence $[z_{l-1}, z_l) \cap [z_{l-1+jk}, z_{l+jk}) \neq \emptyset$, so $[z_{l-1}, z_l) = [z_{l-1+jk}, z_{l+jk})$, that is $z_{l+jk} = z_l$, which means that n divides jk contrary to the fact that $j < n$ and k is relatively prime to n. Thus ϕ is a solution of (2) and for every $z \in S^1$ the number n is the smallest positive integer j with $\phi^j(z) = z$. In particular, ϕ is of order n and it has no fixed points. Clearly $\phi|_{[z_0, z_{n-1})} = \phi_0$. Moreover, if $z \in [z_{n-1}, z_0)$ then

$$\phi(z) = (\phi^{n-1})^{-1}(z) = (\phi_1 \circ \cdots \circ \phi_{n-1})^{-1}(z).$$

Therefore ϕ is the unique extension of ϕ_0 to a solution of (2). □

The next result provides a complete description (cf. also Proposition 1) of continuous solutions of (2) having no fixed points.

Theorem 4. *For every integer $k \in \{1, \ldots, n-1\}$ relatively prime to n and points $z_0, \ldots, z_{n-1} \in S^1$ such that $z_0 < \cdots < z_{n-1}$ any homeomorphism ϕ_0 mapping $[z_0, z_{n-1})$ onto $[z_k, z_{k-1})$ and satisfying condition* (6) *(with $z_j := z_{j \pmod n}$ for $j \geq n$) can be uniquely extended to a solution $\phi : S^1 \to S^1$ of* (2). *Moreover, ϕ is a homeomorphism with no fixed points, it is defined by* (7) *and* (8), *and is a root of identity of order n.*

Conversely: if $\phi : S^1 \to S^1$ is a continuous solution of (2) *of order n and has no fixed points then there are an integer $k \in \{1, \ldots, n-1\}$ relatively prime to n and points $z_0, \ldots, z_{n-1} \in S^1$ such that $z_0 < \cdots < z_{n-1}$*

and ϕ *maps* $[z_{j-1}, z_j)$ *onto* $[z_{(j-1+k)(\bmod n)}, z_{(j+k)(\bmod n)})$ *for every* $j \in \{1, \dots, n-1\}$.

PROOF. Fix an integer $k \in \{1, \dots, n-1\}$ relatively prime to n, points $z_0, \dots, z_{n-1} \in S^1$ such that $z_0 < \dots < z_{n-1}$ and a homeomorphism ϕ_0 mapping $[z_0, z_{n-1})$ onto $[z_k, z_{k-1})$. Put $z_j := z_{j(\bmod n)}$ for $j \geq n$ and assume (6). By Proposition 3 formulas (7) and (8) give a unique extension of ϕ_0 to a solution $\phi : S^1 \to S^1$ of (2). It is a root of order n and has no fixed points. Clearly, (7) and (8) give the continuity of ϕ at every point of (z_0, z_{n-1}) and (z_{n-1}, z_0). Moreover,

$$\lim_{z \to z_{n-1}} \phi_0(z) = z_{k-1} = (\phi_1 \circ \dots \circ \phi_{n-1})^{-1}(z_{n-1}) = \phi(z_{n-1})$$

whence

$$\lim_{z \to z_{n-1}} \phi|_{[z_0, z_{n-1})}(z) = \phi(z_{n-1}).$$

By (7) we have also

$$\begin{aligned}
\lim_{z \to z_0} \phi|_{[z_{n-1}, z_0)}(z) &= \lim_{z \to z_0} (\phi_1 \circ \dots \circ \phi_{n-1})^{-1}(z) = \lim_{z \to z_0} \phi_{n-1}^{-1} \circ \dots \circ \phi_1^{-1}(z) \\
&= \lim_{z \to z_{n-k}} \phi_{n-1}^{-1} \circ \dots \circ \phi_2^{-1}(z) = \dots = \lim_{z \to z_{(n-2)(n-k)}} \phi_{n-1}^{-1}(z) \\
&= z_{(n-1)(n-k)} = z_k = \phi_0(z_0) = \phi(z_0).
\end{aligned}$$

This means that ϕ is also continuous at z_0 and z_{n-1} whence, consequently, it is a homeomorphism.

To prove the converse let $\phi : S^1 \to S^1$ be a continuous solution of (2) of order n, having no fixed points. As ϕ is a bijection it is a homeomorphism. Since it has no fixed points, ϕ preserves orientation. Thus there is an increasing homeomorphism φ mapping $\mathbb{R}$ onto $\mathbb{R}$ such that

$$\varphi(t+1) = \varphi(t) + 1 \quad \text{for } t \in \mathbb{R} \tag{10}$$

and (3) holds.

Since ϕ has no fixed points and it is continuous, by (3) there is an integer p such that

$$t + p < \varphi(t) < t + p + 1 \quad \text{for } t \in \mathbb{R}.$$

Replacing the lift φ by $\varphi - p$, if necessary, we may assume without loss of generality that $p = 0$. In other words

$$t < \varphi(t) < t + 1 \quad \text{for } t \in \mathbb{R}. \tag{11}$$

As ϕ satisfies (2) and is continuous we can find, by (3), an integer k such that (4) holds. Using [10, Lemma 6] or simply repeating a part of its proof we infer that $k \in \{1, \dots, n-1\}$ and k is relatively prime to n.

Since ϕ is a root of identity of order n, there is a $z_0 \in S^1$ with the orbit consisting of exactly n points $z_0, \dots, z_{n-1} \in S^1$. Choose $t_0, \dots, t_{n-1} \in [0,1)$ in such a way that $z_j = \mathrm{e}^{2\pi i t_j}$ for $j \in \{0, \dots, n-1\}$. Without loss of generality we may assume that $0 \le t_0 < \cdots < t_{n-1} < 1$. Clearly $z_0 < \cdots < z_{n-1}$.

We will verify that

$$\phi(z_m) = z_{(m+k) (\bmod n)} \quad \text{for } m \in \{0, \dots, n-1\}. \tag{12}$$

Fix an $m \in \{0, \dots, n-1\}$. Then, according to Remark 1,

$$z_{m (\bmod n)} < \cdots < z_{(m+n-1) (\bmod n)}. \tag{13}$$

If $\varphi^{n-1}(t_m) \le t_m + k - 1$ then, by (4), (10) and (11), we would have

$$\begin{aligned} t_m + k &= \varphi^n(t_m) \\ &= \varphi(\varphi^{n-1}(t_m)) \le \varphi(t_m + k - 1) = \varphi(t_m) + k - 1 < t_m + k, \end{aligned}$$

which is impossible. Thus $\varphi^{n-1}(t_m) > t_m + k - 1$. Moreover, on account of (11) and (4),

$$t_m < \varphi(t_m) < \cdots \le \varphi^{n-1}(t_m) < \varphi^n(t_m) = t_m + k.$$

Therefore, for every $j \in \{0, \dots, k-1\}$ there is an $r_j \in \{0, \dots, n-1\}$ satisfying the condition

$$\varphi^{r_j - 1}(t_m) < t_m + j \le \varphi^{r_j}(t_m).$$

Hence, taking into account strict monotonicity of φ and (10), we infer that

$$\begin{aligned} \varphi^{r_j - 1}(t_m) < t_m + j \le \varphi^{r_j}(t_m) &< \varphi(t_m + j) \\ &= \varphi(t_m) + j \le \varphi^{r_j + 1}(t_m) \end{aligned} \tag{14}$$

for every $j \in \{0, \dots, k-1\}$. This means that

$$\{\phi^{r_0}(z_m), \dots, \phi^{r_{k-1}}(z_m)\} \subset [z_m, \phi(z_m)). \tag{15}$$

By (14) and (11) we have

$$t_m + j \le \varphi^{r_j}(t_m) < \varphi(t_m) + j < t_m + j + 1 \quad \text{for } j \in \{0, \dots, k-1\}$$

whence $r_0, \dots, r_{k-1}$ are distinct and, consequently, the set on the left-hand side of the inclusion (15) consists of exactly k elements of the orbit $\{z_0, \dots, z_{n-1}\}$. On the other hand, if $\phi^s(z_m) \in [z_m, \phi(z_m))$ for an $s \in \{0, \dots, n-1\}$ then (cf. also (4))

$$t_m + j \le \varphi^s(t_m) < \varphi(t_m) + j$$

with an $j \in \{0, \dots, k-1\}$. Thus, since the sequence $(\varphi^i(t_m) : i \in \mathbb{N})$ is strictly increasing, from (14) we get that $s = r_j$. Summarizing, the arc $[z_m, \phi(z_m))$ contains exactly k of the points $z_0, \dots, z_{n-1}$. Thus, according to (13), we have $\phi(z_{m \,(\bmod n)} = z_{(m+k)\,(\bmod n)}$. This completes the proof of (12).

The function $\phi_0 := \phi|_{[z_0, z_{n-1})}$ is a homeomorphism preserving orientation which, by virtue of (12), satisfies condition (6). In particular, $\phi_0([z_0, z_{n-1})) = [z_{k\,(\bmod n)}, z_{(n-1+k)\,(\bmod n)}) := [z_k, z_{k-1})$ and the theorem follows. $\square$

Acknowledgement. The author was supported by the Silesian University Project No. BST/IM/5/2001/.

References

[1] Ch. Babbage, Essay towards the calculus of functions, *Philosoph. Transact*, 1815, 389–423; *II.* ibid. 1816, 179–256.

[2] M. Bajger, On the structure of some flows on the unit circle, *Aequationes Math.* **55** (1998), 106–121.

[3] K. Baron and W. Jarczyk, Recent results on functional equations in a single variable perspectives and open problems, *Aequationes Math.* **61** (2001), 1–48.

[4] I. P. Cornfeld, S. V. Fomin and Y. G. Sinai, Ergodic theory, Grundlehren 245, *Springer Verlag, Berlin – Heidelberg – New York*, 1982.

[5] M. Kuczma, Functional equations in a single variable, Monografie Mat. 46, *Polish Scientific Publishers, Warszawa*, 1968.

[6] M. Kuczma, B. Choczewski and R. Ger, Iterative functional equations, Encyclopedia of Mathematics and its Applications *32*, *Cambridge University Press, Cambridge*, 1990.

[7] N. McShane, On the periodicity of homeomorphisms of the real line, *Amer. Math. Monthly* **68** (1961), 562–563.

[8] E. Vincze, Über die Charakterisierung der assoziativen Funktionen von mehreren Veränderlichen, *Publ. Math. Debrecen* **6** (1959), 241–253.

[9] C. T. C. Wall, A geometric introduction to topology, *Addison–Wesley, Reading*, 1972.

[10] M.C. Zdun, On embedding of homeomorphisms of the circle in a continuous flow, European Conference on Iteration Theory, (Schloss Hofen, 1984), 218–231, Lecture Notes in Mathematics 1163, *Springer Verlag*, *Berlin – Heidelberg – New York*, 1985.

WITOLD JARCZYK
INSTITUTE OF MATHEMATICS
UNIVERSITY OF ZIELONA GÓRA
SZAFRANA 4A, PL-65-516 ZIELONA GÓRA
POLAND
AND
INSTITUTE OF MATHEMATICS
SILESIAN UNIVERSITY
BANKOWA 14, PL-40-007 KATOWICE
POLAND

(Received February 4, 2002; revised December 28, 2002)