Available online at www.tjnsa.com
J. Nonlinear Sci. Appl. 9 (2016), 5041–5060
Research Article

A converse result concerning the periodic structure of commuting affine circle maps

José Salvador Cánovas Peña[a], Antonio Linero Bas[b], Gabriel Soler López[c,*]

[a]*Departamento de Matemática Aplicada y Estadística, Universidad Politécnica de Cartagena, Campus Muralla del Mar, 30203–Cartagena, Spain.*

[b]*Departamento de Matemáticas, Universidad de Murcia, Campus de Espinardo, 30100-Murcia, Spain.*

[c]*Departamento de Matemática Aplicada y Estadística, Universidad Politécnica de Cartagena, Alfonso XIII 52, 30203–Cartagena, Spain.*

Communicated by R. Saadati

Abstract

We analyze the set of periods of a class of maps $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$ defined by $\phi_{d,\kappa}(x) = dx + \kappa$, $d, \kappa \in \mathbb{Z}_\Delta$, where Δ is an integer greater than 1. This study is important to characterize completely the period sets of alternated systems $f, g, f, g, \dots$, where $f, g : \mathbb{S}^1 \to \mathbb{S}^1$ are affine circle maps that commute, and to solve the converse problem of constructing commuting affine circle maps having a prescribed set of periods.

Keywords: Affine maps, alternated system, periods, circle maps, degree, combinatorial dynamics, ring of residues modulo m, Abelian multiplicative group of residues modulo m, Euler function, congruence, order, generator.
2010 MSC: 11A07, 37E10, 37E99.

1. Introduction

In general, a *non autonomous discrete dynamical system* $(X, (f)_n)$ is a pair where X is a topological space, called *phase space*, $\mathbb{N} = \{1, 2, \dots\}$ is the set of natural numbers and $(f_n)_{n\in\mathbb{N}}$ is a sequence of continuous functions $f_n : X \to X$. By $C(X)$ we denote the set of continuous maps from X into itself. Write $(X, (f)_n) \equiv (X, f_{1,\infty})$. The main goal when dealing with non-autonomous dynamical systems is to analyze, for any $x \in X$,

*Corresponding author
Email addresses: Jose.Canovas@upct.es (José Salvador Cánovas Peña), lineroba@um.es (Antonio Linero Bas), gabriel.soler@upct.es (Gabriel Soler López)

Received 2016-02-24

the asymptotic behavior of the *orbits*

$$\mathrm{Orb}_{f_{1,\infty}}(x) := \{x_0, x_1, x_2, \dots, x_n, \dots\},$$

where $x_0 = x$ and $x_n = f_n(x_{n-1}) = f_n \circ \dots \circ f_1(x) =: f_1^n(x)$ for $n \geq 1$, or equivalently to study how the orbits of the system behave when n goes to infinity. When $f_n = f$ for any $n \in \mathbb{N}$, then we denote the system $(X, f_{1,\infty})$ by (X, f) and we receive the classical notion of *(autonomous) dynamical system*.

The easiest asymptotical behavior occurs when x is a *periodic point* of *period* $p \in \mathbb{N}$, that is, $f_{1,\infty}^p(x) = x$ and $f_{1,\infty}^n(x) \neq x$ for any $0 < n < p$ (when a point $x \in X$ has finite, but not periodic, orbit we say that x is *eventually periodic*). In the case of autonomous discrete systems the above conditions read as $f^p(x) = x$ and $f^n(x) \neq x$ for any $0 < n < p$, being f^0 the identity map and $f^m = f \circ f^{m-1}, m \geq 1$. Observe that for $p = 1$ we obtain the definition of *fixed point*.

An interesting problem is to compute its periods set, that is,

$$\mathrm{Per}(f_{1,\infty}) = \{n \in \mathbb{N} : \text{there exists a periodic point } x \in (X, f_{1,\infty}) \text{ of period } n\}.$$

This problem has a long tradition in the setting of autonomous dynamical systems: when $X = I := [0, 1]$ and $f_n = f$ is continuous, $n \in \mathbb{N}$, the result which describes the set $\mathrm{Per}(f)$ is the celebrated Sharkovsky's theorem (see [7–9]). A lot of works in this direction has appeared in the literature by changing the phase space or by considering non-autonomous dynamical systems, a wide review on this subject was made in [6]. A remarkable case consists of studying the periodicity of systems (X, f) when $X = \mathbb{S}^1$ is the circle (see [1, Ch. 3]). In addition, when we consider non-autonomous dynamical systems on $X = I$ and $(f_n)_n = (f, g, f, g, f, g, \dots)$, this system is called *alternated system* and is represented by $[f, g]$. In [4] the set $\mathrm{Per}[f, g]$ is completely characterized. So, it is a natural question to extend the results from [4] for alternated systems $[f, g]$, where f and g are continuous circle maps. However, as we pointed out in [5], this problem for arbitrary continuous circle maps seems to be quite difficult. Then, we started by analyzing the particular case of affine circle maps. Before explaining it, we recall some basic notations on circle maps.

Let $e : \mathbb{R} \to \mathbb{S}^1$ be the standard universal covering given by $e(x) = e^{2\pi i x}$. If $f \in C(\mathbb{S}^1)$, we find a (non-unique) map $F : [0, 1] \to \mathbb{R}$ such that the diagram

$$\begin{array}{ccc} [0,1] & \xrightarrow{F} & \mathbb{R} \\ e\downarrow & & \downarrow e \\ \mathbb{S}^1 & \xrightarrow{f} & \mathbb{S}^1 \end{array}$$

commutes. We call F a *lifting* of f. Notice that $e(0) = e(1) = 1$ and then $e(F(1)) = f(e(1)) = f(e(0)) = e(F(0))$, which implies that $d := F(1) - F(0) \in \mathbb{Z}$. The integer d is said to be the *degree* of f, denoted by $\deg(f)$. Moreover, it is possible to extend the lifting F from $[0, 1]$ to $\mathbb{R}$ by considering $\widetilde{F} : \mathbb{R} \to \mathbb{R}$ as $\widetilde{F}(x) = F(x - [x]) + [x]\deg(f)$, where $[\cdot]$ is the entire part of a real number x. To simplify the notation we denote $\widetilde{F}$ by F.

In [5], the present authors have studied alternated systems $[f, g]$ for affine circle maps, that is, continuous circle maps whose liftings $F, G : \mathbb{R} \to \mathbb{R}$ are of the form $F(x) = d_1 x + \alpha$ and $G(x) = d_2 x + \beta$. The main difficulty in characterizing the set $\mathrm{Per}[f, g]$ is to show the existence of odd periods, that is, the set $\Lambda = \mathrm{Per}[f, g] \cap \mathbb{O}$, where $\mathbb{O}$ denotes the set of odd non-negative integers. We proved that f and g must commute to have $\Lambda \neq \emptyset$, see [5, Theorems A-B]. In addition, Λ is finite and characterized by the set of periods of an affine map defined on a commutative finite group as follows.

As usual, given integers a, b and m, we write $a|b$ if a divides b, the *congruence* $a \equiv b \bmod (m)$ means that $a - b$ is an integer multiple of m; also $b \bmod (m)$ (when it is not in a congruence) denotes the remainder of the Euclidean division between b and m, thus $b \bmod (m) \in \mathbb{Z}_m = \{0, 1, \dots, m - 1\}$. Let $\Delta = |d_1 - d_2|$ and $\kappa = \beta(d_1 - 1) - \alpha(d_2 - 1)$. The affine circle maps f and g commute if and only if $\kappa \in \mathbb{Z}$. Then, we define $\phi_{d_i,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$, $i \in \{1, 2\}$, by

$$\phi_{d_i,\kappa}(m) := (d_i m + \kappa) \bmod (\Delta). \tag{1.1}$$

Since $d_1 \equiv d_2 \bmod (\Delta)$, we have

$$\phi_{d_1,\kappa} = \phi_{d_2,\kappa} =: \phi$$

and the following result connects Λ and $\mathrm{Per}(\phi)$.

Theorem 1.1 ([5]). *Let $f, g \in C(\mathbb{S}^1)$ be with associate liftings $F(x) = d_1x + \alpha$ and $G(x) = d_2x + \beta$ and $d_1 \neq d_2$. If $\kappa \notin \mathbb{Z}$, then $\Lambda = \emptyset$, otherwise, $\kappa \in \mathbb{Z}$ and $\Lambda = \mathrm{Per}(\phi) \cap \mathbb{Q}$.*

Additionally, for the case $\kappa \in \mathbb{Z}$, $d_1 \neq d_2$, $d_1 \in \{-1, 0, 1\}$, Λ is either empty or a singleton, $\Lambda = \{N\}$, see [5, Theorem C-(1)], and it is possible to construct affine maps having the desired set of periods, see [5, Table 4, Proposition 32 and Corollary 33].

However, in the case $\kappa \in \mathbb{Z}$, $d_1 \neq d_2$, $\{d_1, d_2\} \cap \{-1, 0, 1\} = \emptyset$, for which $\mathrm{Per}[f, g] = 2\mathbb{N} \cup \Lambda$ ([5, Theorem C-(2)]), again in [5, Section 7] we mention that given a finite set $\Omega \subset \mathbb{N}$ of odd numbers, "it would be interesting to analyze if it is possible to find affine circle maps, f and g, with liftings $F(x) = d_1x + \alpha$ and $G(x) = d_2x + \beta$ in such a way that $\mathrm{Per}[f, g] = 2\mathbb{N} \cup \Omega$" and we affirm that "to this end, it is necessary to improve the knowledge of the set $\mathrm{Per}(\phi) \cap \mathbb{Q}$, which is our main objective for the near future". The present work answers this question (consult Proposition 4.10 and Theorem D) via the analysis of the periodic structure of ϕ.

Although the map ϕ is quite natural, its periodic structure is unknown, probably due to finite sets cannot exhibit any complicated dynamic behavior (in fact, only periodic and eventually periodic points can appear). Our main goal in this paper is to establish such characterization, which allows us to finish the study of the periodic structure of affine circle maps started in [5]. It is worth pointing out that our present study on the set $\mathrm{Per}(\phi)$ will rely on a combinatorial approach based on elementary number theory, and no topological structure on the phase space $X = \mathbb{Z}_\Delta$ is needed.

Recall that gcd is the (positive) greatest common divisor of two positive integer numbers, additionally, it is assumed $\gcd(0, a) = a$ for any $a \in \mathbb{N}$. By $\mathrm{lcm}(n_1, \ldots, n_k)$ we denote the least common multiple of natural numbers $n_1, \ldots, n_k$ for $k \geq 2$. Two natural numbers p, s and the following are given:

$$\sigma(p, s) := \begin{cases} 1 & \text{if } p \text{ is odd or } p = 2 \text{ and } s = 2, \\ 2 & \text{otherwise.} \end{cases}$$

We characterize the periods of $\phi = \phi_{d,\kappa}$ by the following two main theorems, jointly with Theorems C and D (stated in Sections 4 and 5, respectively), where the reader can find a more precise description of the set of periods, which is too technical for an introduction.

Theorem A. *Let $\Delta = p^s$ where p is a prime and $s \geq 1$ and let $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$ be defined by $\phi_{d,\kappa}(x) = dx + \kappa$, $d, \kappa \in \mathbb{Z}_\Delta$. Then $\mathrm{Per}(\phi_{d,\kappa})$ is one of the following sets:*

(A-1) $\{1\} \cup \{Np^j\}_{j=0}^{\ell}$ *where N is a divisor of $p - 1$ and $\ell \in \{0, 1, \ldots, s - \sigma(p, s)\}$;*

(A-2) $\{p^\ell\}$ *for some $\ell \in \{0, 1, \ldots, s\}$.*

Conversely, let p be a prime, $\Delta = p^s$ with $s \geq 1$, and A be one of the above sets, then there exists $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$ such that $\mathrm{Per}(\phi_{d,\kappa}) = A$.

As a consequence of this theorem and a technical result we obtain the set of periods for the general case.

Theorem B. *Let $\Delta = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$ be a decomposition into prime factors. Then, $n \in \mathrm{Per}(\phi_{d,\kappa})$ if and only if $n = \mathrm{lcm}(n_1, n_2, ..., n_k)$ for some $n_i \in \mathrm{Per}(\phi_{d,\kappa_i})$.*

The paper is organized as follows: In Section 2 we present some basic facts about number theory and prove a characterization for the periodic points of $\phi_{d,\kappa}$. In Section 3 we describe the sets of periods for the case $d \in \{0, 1, \Delta - 1\}$. The case $\Delta = p^s$ with p prime, $s \geq 1$, is analyzed in Section 4. Here, we distinguish two subsections devoted to the cases $\gcd(d, \Delta) > 1$ and $\gcd(d, \Delta) = 1$. In this last subsection it is also necessary to study separately the cases $\gcd(d - 1, \Delta) = 1$ and $\gcd(d - 1, \Delta) > 1$. Sections 3 and 4 are summarized in Theorem C, from which we derive the proof of Theorem A. Finally, in Section 5 we consider the general case with Δ an arbitrary positive integer, and prove Theorems B and D.

2. Preliminaries

For a given set $A \subset \mathbb{R}$ and $n \in \mathbb{N}$, by nA we denote the set $\{na : a \in A\}$ and $\mathrm{Card}A$ denotes the

cardinality of A. In what follows, $\varphi : \mathbb{N} \to \mathbb{N}$ indicates the Euler function, that is, $\varphi(n)$ is Card$\{m \in \mathbb{N} : 1 \leq m \leq n, \gcd(m,n) = 1\}$. In particular, $\varphi(p^s) = p^{s-1}(p-1)$ if p is prime, $s \geq 1$, and $\varphi(ab) = \varphi(a)\varphi(b)$ whenever $\gcd(a,b) = 1$ (see [2]).

As usual, given a positive integer Δ, $\mathbb{Z}_\Delta = \{a \bmod(\Delta) : a \in \mathbb{Z}\}$ is the ring of the residues modulo Δ and $\mathbb{Z}_\Delta^* = \{a \bmod(\Delta) : a \in \mathbb{Z} \text{ and } \gcd(a,\Delta) = 1\}$ is the Abelian multiplicative group of residues modulo Δ. Recall that $(\mathbb{Z}_\Delta, +, \cdot)$ is a commutative ring with Δ elements ($+$ and $\cdot$ refer the sum and the product of integers modulo Δ, respectively). Moreover, $(\mathbb{Z}_\Delta^*, \cdot)$ is an Abelian group with $\text{Card}(\mathbb{Z}_\Delta^*) = \varphi(\Delta)$ (in the literature, it is also called Euler group, see [3, 10]). The following well–known result can be found in [2, Theorem 5.17].

Lemma 2.1 (Euler's Theorem)**.** *Let a, m be integers with $\gcd(a,m) = 1$. Then*

$$a^{\varphi(m)} \equiv 1 \bmod(m).$$

The following elementary results will be fruitful in our study.

Lemma 2.2. *Let $p, q \in \mathbb{Z} \setminus \{0\}$. Then $\gcd(q,p) = 1$ if and only if*

$$q^n \equiv 1 \bmod(p)$$

for some $n \in \mathbb{N}$.

Proof. Let $d = \gcd(q,p)$. The condition $q^n \equiv 1 \bmod(p)$ for some positive integer n (or $q^n - 1 = up$ for some $n \in \mathbb{N}$ and some $u \in \mathbb{Z}$) is equivalent to have $\frac{q^n}{d} - \frac{up}{d} = \frac{1}{d}$ for some $n \in \mathbb{N}$ and some $u \in \mathbb{Z}$. Being $\frac{q^n}{d} - \frac{up}{d} \in \mathbb{Z}$ the initial condition is equivalent to have $d = 1$. □

Remark 2.3. From the above result, if $\gcd(q,p) = 1$ we define the order of q modulo p as the smallest positive integer s satisfying $q^s \equiv 1 \bmod(p)$. Notice that if N is this order, and we have $q^n \equiv 1 \bmod(p)$, then necessarily $N|n$ ([2, Theorem 10.1]). In particular, $N|\varphi(p)$ by Lemma 2.1. □

Lemma 2.4. *Let a, b be positive integers. For any non-negative integer κ,*

$$\text{Card}\left\{(ja + \kappa) \bmod(b) : j = 0, 1, \ldots, b-1\right\} = \frac{b}{\gcd(a,b)}. \tag{2.1}$$

In particular, this cardinal is b whenever $\gcd(a,b) = 1$.

Proof. Let $i, j \in \{0, \ldots, b-1\}$, with $i \geq j$. Since $ja + \kappa \equiv ia + \kappa \bmod(b)$ is equivalent to have $(i-j)\frac{a}{\gcd(a,b)} = u\frac{b}{\gcd(a,b)}$ for some non-negative integer u, we deduce that the first congruence holds if and only if $i \equiv j \bmod(\frac{b}{\gcd(a,b)})$ as a consequence of $\frac{b}{\gcd(a,b)}$ and $\frac{a}{\gcd(a,b)}$ being coprime. Additionally, by a similar reasoning we have that all the elements $\kappa, a+\kappa, \ldots, \left(\frac{b}{\gcd(a,b)} - 1\right)a + \kappa$ are pairwise distinct and Eq. (2.1) follows. □

If $(\mathbb{Z}_\Delta^*, \cdot)$ is a cyclic group, we say that $g \in \mathbb{Z}_\Delta^*$ is a generator whenever $\{g^n \bmod(\Delta) : n \geq 1\} = \mathbb{Z}_\Delta^*$. Necessarily, the order of a generator g modulo Δ is equal to $\varphi(\Delta)$. In [2], a generator g is also called a primitive root.

Next result establishes when $(\mathbb{Z}_\Delta^*, \cdot)$ is cyclic.

Theorem 2.5 ([2])**.** *$(\mathbb{Z}_\Delta^*, \cdot)$ is a cyclic group if and only if $\Delta \in \{p^s : p \text{ is an odd prime and } s \in \mathbb{N}\} \cup \{2p^s : p \text{ is an odd prime and } s \in \mathbb{N}\} \cup \{1, 2, 4\}$.*

It is well-known that the number of generators of these cyclic groups is given by $\varphi(\varphi(\Delta))$. We will be interested in the search of primitive roots g for $(\mathbb{Z}_{p^s}^*, \cdot)$, with $p \geq 3$ prime, $s \geq 1$, such that they also generate the cyclic group $(\mathbb{Z}_p^*, \cdot)$. To this end, we need the following result whose proof can be consulted in [2, Theorem 10.6].

Theorem 2.6. *Let p be an odd prime. Then:*

(a) *If g is a primitive root $\bmod p$ then g is also a primitive root $\bmod p^s$ for all $s \geq 1$, if and only if, $g^{p-1} \not\equiv 1 \bmod (p^2)$.*

(b) *There is at least one primitive root $g \bmod p$ which satisfies the above condition, hence there exists at least one primitive root $\bmod p^s$ if $s \geq 2$.*

The next significant property in our study relates the orders of d modulo p^j, $j \geq 1$, in the following way.

Lemma 2.7. *Let p, d be positive integers, with $\gcd(p,d) = 1$, p prime and $d \neq 1$. Denote the order of d modulo p^j by δ_j, $j \geq 1$. If $d^{\delta_1} - 1 = p^\alpha \cdot q$, for some positive integers $\alpha \geq 1$ and q, with $\gcd(p,q) = 1$, then for $p \geq 3$ or $p = 2$ and $\alpha \geq 2$ we have that*

$$\delta_1 = \delta_j \ \text{ for } \ j \in \{1, \ldots, \alpha\}$$

and

$$\delta_{r+1} = p \cdot \delta_r \ \text{ for } \ r \geq \alpha.$$

Proof. From $\gcd(d,p) = 1$, Lemma 2.2 yields the existence of δ_j for all $j \geq 1$. Assume that $d^{\delta_1} = 1 + p^\alpha \cdot q$, with $\gcd(p,q) = 1$ and $\alpha \geq 1$. To establish $\delta_1 = \delta_j$, for all $j \in \{1, \ldots, \alpha\}$, take into account that $d^{\delta_1} - 1 = p^j p^{\alpha - j} q$ and simply use the definition of the order as the smallest positive integer n satisfying the congruence $d^n \equiv 1 \bmod (p^j)$.

We now prove that $\delta_{\alpha+1} = p \cdot \delta_\alpha$. Since $d^{\delta_{\alpha+1}} - 1$ is a multiple of $p^{\alpha+1}$, at the same time p^α divides $d^{\delta_{\alpha+1}} - 1$, so by the definition of order and its properties (see Remark 2.3) we obtain

$$\delta_\alpha < \delta_{\alpha+1} \ \text{ and } \ \delta_\alpha | \delta_{\alpha+1} \tag{2.2}$$

(notice that the inequality is strict because $d^{\delta_\alpha} - 1 \not\equiv 0 \bmod (p^{\alpha+1})$). On the other hand, from $d^{\delta_\alpha} \equiv 1 \bmod (p^\alpha)$ we deduce the existence of some non-negative integer u (in fact, $u = q$) such that $(d^{\delta_\alpha})^p = (p^\alpha \cdot u + 1)^p$, and by the binomial formula we find

$$\begin{aligned}
\left(d^{\delta_\alpha}\right)^p &= (p^\alpha \cdot u + 1)^p \\
&= 1 + p \cdot p^\alpha \cdot u + \frac{p(p-1)}{2} p^{2\alpha} \cdot u^2 + \ldots + p \cdot p^{(p-1)\alpha} \cdot u^{p-1} + p^{p\alpha} \cdot u^p \\
&= 1 + p^{\alpha+1} \cdot u \left(1 + \frac{(p-1)}{2} p^\alpha \cdot u + \ldots + p^{(p-2)\alpha} \cdot u^{p-2} + p^{(p-1)\alpha} \cdot u^{p-1}\right) \\
&= 1 + p^{\alpha+1} \cdot u \cdot (1 + p^\alpha \cdot r) = 1 + p^{\alpha+1} \cdot u \cdot s
\end{aligned}$$

for suitable positive integers r, s (realize that $\alpha p > \alpha + 1$ in the cases $p \geq 3$ or $p = 2, \alpha \geq 2$). Notice that $s = 1 + p^\alpha r$ is coprime with p, so we can write

$$d^{p\delta_\alpha} - 1 = p^{\alpha+1} \cdot q_1$$

for some positive integer q_1 holding $\gcd(p, q_1) = 1$. Then $d^{p\delta_\alpha} \equiv 1 \mod (p^{\alpha+1})$ and consequently

$$\delta_{\alpha+1} \leq p\delta_\alpha \ \text{ with } \ \delta_{\alpha+1} | p\delta_\alpha. \tag{2.3}$$

Since p is prime, by (2.2) and (2.3) we conclude that $\delta_{\alpha+1} = p\delta_\alpha$. Additionally, we observed that $d^{\delta_{\alpha+1}} - 1 = p^{\alpha+1} q_1$, with $\gcd(p, q_1) = 1$.

To finish the proof, we proceed by the induction. Suppose that $\delta_{\alpha+j} = p^j \delta_\alpha$ and $d^{\delta_{\alpha+j}} - 1 = p^{\alpha+j} q_j$ with $\gcd(p, q_j) = 1$ for all $j \in \{1, \ldots, j_0\}$, and prove that $\delta_{\alpha+j_0+1} = p^{j_0+1} \delta_\alpha$ and $d^{\delta_{\alpha+j_0+1}} - 1 = p^{\alpha+j_0+1} q_{j_0+1}$ for some positive integer q_{j_0+1} such that $\gcd(p, q_{j_0+1}) = 1$.

A similar reasoning to that given at the beginning of the first step of the induction leads us to $\delta_{\alpha+j_0}|\delta_{\alpha+j_0+1}$ and $\delta_{\alpha+j_0+1}|p\delta_{\alpha+j_0}$. Consequently, since p is prime, either $\delta_{\alpha+j_0+1}=\delta_{\alpha+j_0}$ or $\delta_{\alpha+j_0+1}=p\delta_{\alpha+j_0}$.

If $\delta_{\alpha+j_0+1}=\delta_{\alpha+j_0}$, we would obtain $d^{\delta_{\alpha+j_0+1}}=1+p^{\alpha+j_0+1}\widetilde{q}$, for some integer $\widetilde{q}$, and on the other hand $d^{\delta_{\alpha+j_0}}=1+p^{\alpha+j_0}q_{j_0}$. Thus, $q_{j_0}=p\widetilde{q}$, which contradicts that q_{j_0} and p are coprime. Therefore, $\delta_{\alpha+j_0+1}=p\delta_{\alpha+j_0}$. To establish that $d^{\delta_{\alpha+j_0+1}}-1=p^{\alpha+j_0+1}w$ for some integer w coprime with p, develop $(d^{\delta_{\alpha+j_0}})^p=(1+q_{j_0}p^{\alpha+j_0})^p$ as in the case of $\delta_{\alpha+1}$. □

Remark 2.8. The above result does not work if $p=2$ and $\alpha=1$. For instance, take $d=3$. In this case $d-1=2$ and $\alpha=1$. Here, $\delta_2=2$ but $\delta_3=2$. Nevertheless, notice that $\delta_4=2^2$, $\delta_5=2^3$, and in general, $\delta_n=2^{n-2}$ if $n\geq 3$. □

The particular case $p=2$ and $\alpha=1$ requires to be analyzed separately.

Lemma 2.9. *Let $d=2q+1$, with $\gcd(2,q)=1$, $q\geq 1$, and let δ_j be the order of d modulo 2^j. Then*

$$\delta_1=1,\ \delta_2=\delta_3=2. \tag{2.4}$$

Moreover, if $d^2-1=2^\gamma q_2$ with q_2 odd (by force $\gamma\geq 3$),

$$\delta_j=2 \text{ for all } j=2,\dots,\gamma, \tag{2.5}$$

$$\delta_{\gamma+i}=2^{i+1} \text{ for all } i\geq 1. \tag{2.6}$$

Proof. By definition of order, it is immediate to see that $\delta_1=1$. To obtain $\delta_2=2$, notice that $d-1\not\equiv 0\,\mathrm{mod}(2^2)$ and that $d^2-1=(d-1)(d+1)$ is the product of two even natural numbers. Moreover, note that $(d-1)^2=d^2-2d+1=4q^2$, then $d^2-1=4q(q+1)$ with $q+1$ even and we obtain $\delta_3=2$. This proves (2.4).

To obtain (2.5), simply use that $d^2-1=2^\gamma q_2$ with $\gamma\geq 3$ and q_2 odd, and apply the definition of order of d modulo 2^j.

Finally, the proof of (2.6) proceeds by the induction in an analogous way to that done at the proof of Lemma 2.7 (realize that now $\gamma\geq 3$, hence $\gamma p>\gamma+1$), so we will omit it. □

Since $\mathbb{Z}_\Delta$ is finite, the dynamics of $\phi_{d,\kappa}$ is simple: any point $x\in\mathbb{Z}_\Delta$ is either periodic or eventually periodic. Moreover, the following result is immediate.

Lemma 2.10. *Let $\phi_{d,\kappa}:\mathbb{Z}_\Delta\to\mathbb{Z}_\Delta$ be defined by* (1.1).

(a) *If $\Delta=1$, $\mathrm{Per}(\phi_{d,\kappa})=\{1\}$.*
(b) *If $\Delta=2$, $\mathrm{Per}(\phi_{0,\kappa})=\{1\}$ for $\kappa\in\{0,1\}$, $\mathrm{Per}(\phi_{1,0})=\{1\},\mathrm{Per}(\phi_{1,1})=\{2\}$.*

So, in the sequel we assume that $\Delta\geq 3$.

To analyze the set of periods of $\phi_{d,\kappa}$, notice that by the induction it is easily seen that

$$\phi^n_{d,\kappa}(x)=\left(d^nx+\kappa\frac{d^n-1}{d-1}\right)\ \mathrm{mod}(\Delta) \text{ for all } n\geq 1,\ \text{ if } d\neq 1 \tag{2.7}$$

and

$$\phi^n_{1,\kappa}(x)=(x+n\kappa)\ \mathrm{mod}(\Delta) \text{ for all } n\geq 1,\ \text{ if } d=1. \tag{2.8}$$

Next, we distinguish between periodic and eventually periodic points.

Proposition 2.11. *Let $x,d,\kappa\in\mathbb{Z}_\Delta$, $d\notin\{0,1\}$. The following statements are equivalent.*

(a) *x is a periodic point of $\phi_{d,\kappa}$;*
(b) $\gcd(d,\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)})=1$.

Additionally, if x is periodic, its period N is exactly the order of d modulo $\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}$.

Proof. (a) ⇒ (b). Assume that $x\in\mathbb{Z}_\Delta$ is a periodic point of order N. If $N=1$ (so $(d-1)x+\kappa\equiv 0\,\mathrm{mod}(\Delta)$) the result follows directly from the facts $\gcd(\Delta,(d-1)x+\kappa)=\Delta$ and $\gcd(d,d-1)=1$. So, we suppose

that $N \geq 2$. According to (2.7) we find

$$\phi_{d,\kappa}^N(x) = \left(d^N x + \kappa \frac{d^N - 1}{d-1}\right) \equiv x \bmod(\Delta) \tag{2.9}$$

and

$$\phi_{d,\kappa}^i(x) = \left(d^i x + \kappa \frac{d^i - 1}{d-1}\right) \not\equiv x \bmod(\Delta) \text{ for all } 0 < i < N. \tag{2.10}$$

From (2.9) we have

$$\frac{d^N - 1}{d-1} \frac{((d-1)x + \kappa)}{\gcd(\Delta, (d-1)x + \kappa)} = w \frac{\Delta}{\gcd(\Delta, (d-1)x + \kappa)} \text{ for some } w \in \mathbb{Z}.$$

Since $\frac{\Delta}{\gcd(\Delta,(d-1)x+\kappa)}$ and $\frac{(d-1)x+\kappa}{\gcd(\Delta,(d-1)x+\kappa)}$ are coprime, we obtain

$$\frac{d^N - 1}{d-1} \equiv 0 \bmod \left(\frac{\Delta}{\gcd(\Delta, (d-1)x + \kappa)}\right),$$

or

$$d^N \equiv 1 \bmod \left(\frac{(d-1)\Delta}{\gcd(\Delta, (d-1)x + \kappa)}\right). \tag{2.11}$$

By Lemma 2.2 we deduce that $\gcd(d, \frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}) = 1$. This ends the proof of (a) $\Rightarrow$ (b).

Additionally, notice that if x is N-periodic, from (2.10) we obtain

$$d^i \not\equiv 1 \bmod \left(\frac{(d-1)\Delta}{\gcd(\Delta, (d-1)x + \kappa)}\right) \text{ for } 0 < i < N. \tag{2.12}$$

Thus, by (2.11) and (2.12) N is the order of d modulo $\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}$.

(b) $\Rightarrow$ (a). By Lemma 2.2, there exists the order, say N, of d modulo $\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}$. We claim that x is then periodic of period N. Reasoning in a similar way that done in the previous implication, from $d^N \equiv 1 \bmod \left(\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}\right)$ we obtain (2.9), and $d^i \not\equiv 1 \bmod \left(\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}\right)$ $(0 < i < N)$ leads to (2.10). Therefore, x is a periodic point of $\phi_{d,\kappa}$ of period N. □

3. The dynamics for $d \in \{0, 1, \Delta - 1\}$

The set of periods of $\phi_{d,\kappa}(x)$ in these cases is obtained in the following result.

Proposition 3.1. *Let Δ be a positive integer and let $\phi_{d,\kappa}$ be defined as in* (1.1).

(i) $\mathrm{Per}(\phi_{0,\kappa}) = \{1\}$ *for all κ;*
(ii) $\mathrm{Per}(\phi_{1,\kappa}) = \{\frac{\Delta}{\gcd(\Delta,\kappa)}\}$ *for all κ (remember that we take* $\gcd(\Delta, 0) = \Delta$*);*
(iii) *when $\Delta \geq 3$ is even, then* $\mathrm{Per}(\phi_{\Delta-1,\kappa}) = \{1, 2\}$ *if κ is even, and* $\mathrm{Per}(\phi_{\Delta-1,\kappa}) = \{2\}$ *if κ is odd;*
(iv) *when $\Delta \geq 3$ is odd, then* $\mathrm{Per}(\phi_{\Delta-1,\kappa}) = \{1, 2\}$ *for all κ.*

Proof.

(i). Note that $\phi_{0,\kappa}(x) = \kappa$ for all $x \in \mathbb{Z}_\Delta$. Then the unique periodic point of $\phi_{0,\kappa}$ is κ, a fixed point, i.e., a periodic point of period 1.

(ii). Let $x \in \mathbb{Z}_\Delta$ and $\Delta \geq 3$. By (2.8), $\phi_{1,\kappa}^n(x) = x + n\kappa \bmod(\Delta)$ for all $n \geq 1$, and $\phi_{1,\kappa}^n(x) = x$ if and only if $n\kappa \equiv 0 \bmod(\Delta)$, that is, $n\kappa = s\Delta$ for some integer s. If $\kappa = 0$ then $\phi_{1,\kappa}(x) = x$ for all $x \in \mathrm{Z}_\Delta$ and $\mathrm{Per}(\phi_{1,\kappa}) = \{1\}$.

Assume that $\kappa \neq 0$. We claim that $\frac{\Delta}{\gcd(\Delta,\kappa)}$ is the smallest positive integer n such that $n\kappa \equiv 0 \bmod(\Delta)$. It is obvious that $\frac{\Delta}{\gcd(\Delta,\kappa)}\kappa \equiv 0 \bmod(\Delta)$. Let $s \leq \frac{\Delta}{\gcd(\Delta,\kappa)}$ be a positive integer satisfying $s\kappa \equiv 0 \bmod(\Delta)$, that is, $s\kappa = q\Delta$ for some (positive) integer q. Then $s\frac{\kappa}{\gcd(\Delta,\kappa)} = q\frac{\Delta}{\gcd(\Delta,\kappa)}$ and $\frac{\Delta}{\gcd(\Delta,\kappa)}$ divides $s\frac{\kappa}{\gcd(\Delta,\kappa)}$. Since $\frac{\kappa}{\gcd(\Delta,\kappa)}$ and $\frac{\Delta}{\gcd(\Delta,\kappa)}$ are coprime, we deduce that $\frac{\Delta}{\gcd(\Delta,\kappa)}$ divides s and consequently $s = \frac{\Delta}{\gcd(\Delta,\kappa)}$, which ends the claim. Hence, it is easily seen that $\mathrm{Per}(\phi_{1,\kappa}) = \{\frac{\Delta}{\gcd(\Delta,\kappa)}\}$. The case $\Delta \leq 2$ follows from Lemma 2.10.

(iii)-(iv). Suppose that $d = \Delta - 1$ and $\Delta \geq 3$. Note that $\phi^2_{\Delta-1,\kappa}(x) = x$ for all $x \in \mathbb{Z}_\Delta$ and since $\phi_{\Delta-1,\kappa}$ is not the identity, we have $2 \in \mathrm{Per}(\phi_{\Delta-1,\kappa})$. Now, let $x \in \mathbb{Z}_\Delta$ be such that $\phi_{\Delta-1,\kappa}(x) = x$, which is equivalent to $2x \equiv \kappa \mod(\Delta)$. This equation has solution if and only if $\gcd(\Delta, 2)$ divides κ. Now, if Δ is odd, then $\gcd(\Delta, 2) = 1$, which obviously divides κ and hence $1 \in \mathrm{Per}(\phi_{\Delta-1,\kappa})$ and Part (iv) is proved. Assume that Δ is even. Then, $\gcd(\Delta, 2) = 2$, which divides κ if and only if it is even. Then, we have that $1 \in \mathrm{Per}(\phi_{\Delta-1,\kappa})$ if and only if κ is even, which proves Part (iii) and finishes the proof.

□

4. The case $\Delta = p^s$, with p prime, $s \geq 1$

According to the previous section, besides $\Delta \geq 3$, we assume that $d \notin \{0, 1, \Delta - 1\}$. In this section, we are going to obtain the different sets of periods of $\phi_{d,\kappa}$ when $\Delta = p^s$ is a power of a prime number p, with $s \geq 1$.

If $\kappa = 0$, then $\phi_{d,0} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$, $\phi_{d,0}(x) = dx$, is a group homomorphism. As $\phi_{d,0}(0) = 0$, we have $1 \in \mathrm{Per}(\phi_{d,0})$. Recall that the kernel of $\phi_{d,0}$ is defined as $\mathrm{Ker}(\phi_{d,0}) = \{x \in \mathbb{Z}_\Delta : dx = 0\}$. It is well–known that $\mathrm{Ker}(\phi)$ is a subgroup of $\mathbb{Z}_\Delta$. On the other hand, since $\mathbb{Z}_\Delta$ is finite, any point $x \in \mathbb{Z}_\Delta$ is either periodic or eventually periodic. The kernel of $\phi_{d,0}$ allows us to characterize when eventually periodic points do exist. By $\mathrm{P}(\cdot)$ we denote the set of periodic points of a map.

Lemma 4.1. *Let $\phi_{d,0} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$, $\phi_{d,0}(x) = dx$. Suppose that $d \neq 0$. Then, the following statements are equivalent:*

(a) $\mathrm{P}(\phi_{d,0}) = \mathbb{Z}_\Delta$;

(b) $\mathrm{Ker}(\phi_{d,0}) = \{0\}$;

(c) $\gcd(d, \Delta) = 1$.

In this case, the period of any point $x \neq 0$ divides the order of d modulo Δ.

Proof. (a) ⇒ (b). Suppose that $\mathrm{P}(\phi_{d,0}) = \mathbb{Z}_\Delta$. Let $x \in \mathrm{Ker}(\phi_{d,0})$. Then $\phi_{d,0}(x) = 0$. Since $\phi_{d,0}(0) = 0$ and x is not eventually periodic, we deduce that $x = 0$, so $\mathrm{Ker}(\phi_{d,0}) = \{0\}$.

(b) ⇒ (c). Put $\delta := \gcd(d, \Delta)$. Then $\phi_{d,0}(\frac{\Delta}{\delta}) = d\frac{\Delta}{\delta} = \frac{d}{\delta}\Delta \equiv 0 \bmod(\Delta)$. Since $\mathrm{Ker}(\phi_{d,0}) = \{0\}$, we have $\frac{\Delta}{\delta} \equiv 0 \bmod(\Delta)$ and hence $\delta = 1$.

(c) ⇒ (a). If $\gcd(d, \Delta) = 1$, by Lemma 2.2 $d^n \equiv 1 \bmod(\Delta)$ for some positive integers n. In this case, we obtain $\phi^n_{d,0}(x) = d^n x \equiv x \bmod(\Delta)$ for all $x \in \mathbb{Z}_\Delta$, and consequently, $\mathrm{P}(\phi_{d,0}) = \mathbb{Z}_\Delta$. Notice that the period of x divides the order of d modulo Δ. □

For instance, if $\Delta = 15$ and $d = 8$, it is immediate to check that the set of periods of $\phi_{d,0}$ is {1,2,4}. In this case, the order of $d = 8$ modulo $\Delta = 15$ is 4. Recall that the period of a periodic point x is given by the order of d modulo $\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}$ (see Proposition 2.11).

However, if Δ is prime and $\gcd(d, \Delta) = 1$, we guarantee that aside from the fixed point $x = 0$, all non-zero elements of $\mathbb{Z}_\Delta$ are periodic of the same period, namely, the order N of d modulo Δ. Indeed, by Lemma 4.1 we already know that the period of $x \neq 0$, say q_x, divides N. On the other hand, Proposition 2.11 yields $d^{q_x} \equiv 1 \bmod(\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x)})$, or $d^{q_x} \equiv 1 \bmod((d-1)\Delta)$ since Δ and $(d-1)x$ are coprime. Consequently, also $d^{q_x} \equiv 1 \bmod(\Delta)$ and by the definition of order (see Remark 2.3), we obtain $N | q_x$ and hence $q_x = N$. Thus, we obtain the following:

Lemma 4.2. *Assume that Δ is prime. Let $d \in \mathbb{Z}_\Delta, d \neq 0$. Then* $\mathrm{Per}(\phi_{d,0}) = \{1, N\}$*, where N is the order of d modulo Δ, that is, the smallest positive integer n satisfying $d^n \equiv 1 \bmod(\Delta)$.*

In the following two subsections, we assume that $\Delta = p^s$, with p prime and $s \geq 1$, $\Delta \geq 3$.

4.1. The case $\gcd(d, \Delta) > 1$

Let $\kappa \in \{0, 1, ..., \Delta - 1\}$ and fix $d \neq 0$ such that $\gcd(d, \Delta) > 1$, that is, $d = p^\gamma q$ with $\gamma \geq 1$ and $\gcd(p, q) = 1$.

Proposition 4.3. *Consider $\Delta = p^s \geq 3$, p prime, $s \geq 1$, and $d \neq 1$ such that* $\gcd(d, \Delta) > 1$*. Then,* $\mathrm{Per}(\phi_{d,\kappa}) = \{1\}$ *for all κ.*

Proof. Let $x \in \mathbb{Z}_\Delta$ be a periodic point of $\phi_{d,\kappa}$ of period N, so $\phi^N_{d,\kappa}(x) = x$. Since $d \neq 1$, by (2.7) we deduce

$$\frac{d^N - 1}{d - 1}((d-1)x + \kappa) \equiv 0 \bmod(\Delta)$$

or

$$(1 + d + \ldots + d^{N-1})((d-1)x + \kappa) \equiv 0 \bmod(\Delta).$$

Taking into account that $\gcd(1+d+\ldots+d^{N-1}, p) = \gcd(1+d+\ldots+d^{N-1}, \Delta) = 1$ because $1+d+\ldots+d^{N-1} = 1+p\cdot u$ for some integer u, the last congruence holds only if $((d-1)x+\kappa) \equiv 0 \bmod(\Delta)$, or $\phi_{d,\kappa}(x) \equiv x \bmod(\Delta)$. Hence, $N = 1$ and $\phi_{d,\kappa}$ has only fixed points. □

4.2. The case $\gcd(d, p) = 1$

Let $\kappa \in \{0, 1, ..., \Delta - 1\}$ and fix d such that $\gcd(d, \Delta) = 1$ and $d \notin \{0, 1, \Delta - 1\}$ (realize that the sets of periods $\mathrm{Per}(\phi_{d,\kappa})$ with $d = 0, 1, \Delta - 1$, have been obtained in Proposition 3.1). In turn we distinguish two cases:

a) If $\gcd(d - 1, p) = 1$.

b) If $\gcd(d - 1, p) > 1$.

4.2.1. The case $\gcd(d - 1, p) = 1$

Recall that by δ_j we denote the order of d modulo p^j, $j \in \{1, \ldots, s\}$. Realize that, necessarily, it must be $p \geq 3$.

Theorem 4.4. *Let $\Delta = p^s \geq 3$, with p prime and $s \geq 1$. Let $d \notin \{0, 1\}$, with* $\gcd(d, p) = \gcd(d - 1, p) = 1$*. Then*

$$\mathrm{Per}(\phi_{d,\kappa}) = \{1\} \cup \{\delta_j\}_{j=1}^{s} = \{1\} \cup \left\{\delta_1 p^j\right\}_{j=0}^{\max\{0, s-\alpha\}}$$

for all $\kappa \in \{0, 1, 2, ..., \Delta - 1\}$, where $d^{\delta_1} - 1 = p^\alpha q_d$ with $\gcd(p, q_d) = 1$, and δ_j is the order of d modulo p^j, $j = 1, \ldots, s$.

Proof. Firstly, notice that all the elements of $\mathbb{Z}_\Delta$ are periodic points of $\phi_{d,\kappa}$, since $\gcd\left(d, \frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}\right) = 1$ and Proposition 2.11 applies.

Next, use Lemma 2.4 to deduce that the cardinality of the set $\{(d-1)x + \kappa \bmod(\Delta) : x \in \mathbb{Z}_\Delta\}$ is Δ. Consequently,

$$\{\gcd(\Delta, (d-1)x + \kappa) : x \in \mathbb{Z}_\Delta\} = \{1, p, \ldots, p^s\}.$$

Let $x_j \in \mathbb{Z}_\Delta$ satisfy $\gcd(\Delta, (d-1)x + \kappa) = p^j$, $j = 0, 1, \ldots, s$, and denote by N_j, $j = 0, 1, \ldots, s-1, s$, the order of d modulo $\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x_j+\kappa)} = (d-1)p^{s-j}$. Again Proposition 2.11 jointly with the above observation lead to

$$\mathrm{Per}(\phi_{d,\kappa}) = \{N_j : j = 0, 1, \ldots, s\}.$$

For $j = s$ we obtain $N_s = 1$, because $d \equiv 1 \bmod(d - 1)$.

On the other hand, denote by δ_i, $i = 1, \ldots, s$ the order of d modulo p^i. We claim that $N_r = \delta_{s-r}$ for $r = 0, 1, \ldots, s-1$. Since $d^{N_r} \equiv 1 \bmod((d-1)p^{s-r})$, we deduce that also $d^{N_r} \equiv 1 \bmod(p^{s-r})$. Therefore, $\delta_{s-r} | N_r$ by Remark 2.3. To finish the claim, again the definition of order gives $d^{\delta_{s-r}} \equiv 1 \bmod(p^{s-r})$, and since $d-1$ and p are coprime and $d^{\delta_{s-r}} - 1 = (d-1)(1+d+\ldots+d^{\delta_{s-r}-1})$ we deduce that $p^{s-r} | (1+d+\ldots+d^{\delta_{s-r}-1})$, and also $p^{s-r} | (d^{\delta_{s-r}} - 1)$, which implies $d^{\delta_{s-r}} \equiv 1 \bmod((d-1)p^{s-r})$, and $N_r | \delta_{s-r}$, thus the claim is proved.

Finally, by Lemma 2.7 (it holds for $p \geq 3$), we have $\delta_1 = \ldots = \delta_\alpha$, and $\delta_{\alpha+i} = p^i \delta_\alpha = p^i \delta_1$, for $i = 1, \ldots, s-\alpha$. □

Corollary 4.5. *Let $\Delta = p \geq 3$ be a prime integer. Let $d \notin \{0, 1, \Delta - 1\}$. Then $\mathrm{Per}(\phi_{d,\kappa}) = \{1, N\}$ for all $\kappa \in \{0, 1, 2, ..., \Delta - 1\}$, where N is the order of d modulo Δ.*

Notice that the above result extends Lemma 4.2 to arbitrary values of κ.

Next, we characterize the periods of $\phi_{d,\kappa}$ when Δ is a prime number and $d \notin \{0, 1\}$.

Theorem 4.6. *Let Δ be prime and $\Delta \geq 3$. Let $n \neq 1$ be a divisor of $\Delta - 1 = \varphi(\Delta)$. Then, there exists $d \in \{2, \ldots, \Delta - 1\}$ such that $\mathrm{Per}(\phi_{d,\kappa}) = \{1, n\}$ for all $\kappa \in \{0, 1, ..., \Delta - 1\}$. In fact,*

$$\bigcup_{d \in \{2,\ldots,\Delta-1\}} \mathrm{Per}(\phi_{d,0}) = \{\textit{divisors of } \varphi(\Delta)\}.$$

Proof. By Theorem 4.4, it suffices to prove the result for $\kappa = 0$. Let $\mathbb{Z}_\Delta^* = \mathbb{Z}_\Delta \setminus \{0\}$ be the Abelian multiplicative group with generator δ of order $\Delta - 1$, that is, $\Delta - 1$ is the smallest positive integer such that $\delta^{\Delta-1} \equiv 1 \bmod(\Delta)$. Take $n \neq 1$ dividing $\Delta - 1$ and let $d = \delta^{\frac{\Delta-1}{n}}$. Then, the order of d is n, that is, n is the smallest positive integer such that $d^n \equiv 1 \bmod(\Delta)$. Take $\phi_{d,0}$. By Theorem 4.4, we have $\mathrm{Per}(\phi_{d,0}) = \{1, n\}$. To finish, notice that the reasoning can be applied to all divisors of $\varphi(\Delta) = \Delta - 1$. □

Table 1 shows the periods for several prime numbers Δ when $d \in \{2, 3, ..., \Delta - 1\}$. We take $\kappa = 0$ and write $P_{d,0} := \mathrm{Per}(\phi_{d,0})$.

Table 1: Set of periods of $\phi_{d,\kappa}$ when $\gcd(d, \Delta) = 1$ and $\gcd(d-1, \Delta) = 1$.

Δ	5			7				
d	2	3	4	2	3	4	5	6
elements in $P_{d,0}$	1,4	1,4	1,2	1,3	1,6	1,3	1,6	1,2

Δ	11								
d	2	3	4	5	6	7	8	9	10
elements in $P_{d,0}$	1,10	1,5	1,5	1,5	1,10	1,10	1,10	1,5	1,2

Δ	3^3								
d	2	5	8	11	14	17	20	23	26
elements in $P_{d,0}$	1,2 6,18	1,2 6,18	1,2 6	1,2 6,18	1,2 6,18	1,2 6	1,2 6,18	1,2 6,18	1,2

Δ	5^2														
d	2	3	4	7	8	9	12	13	14	17	18	19	22	23	24
$P_{d,0}$	1 4 20	1 4 20	1 2 10	1 4	1 4 20	1 2 10	1 4 20	1 4 20	1 2 10	1 4 20	1 4	1 2 10	1 4 20	1 4 20	1 2

4.2.2. The case $\gcd(d-1,p)>1$

Now, we assume that

$$d-1=p^{\alpha}q_d$$

for some positive integer α, $s-1\geq\alpha$, and an integer q_d coprime with p. Recall that we use the notation δ_j to denote the order of d modulo p^j, $j\geq 1$. By Lemma 2.7, we have

$$\delta_1=\ldots=\delta_{\alpha}=1 \text{ and } \delta_{\alpha+r}=p^r\delta_1=p^r \text{ for } r\geq 1 \tag{4.1}$$

if either $p\geq 3$ or $p=2,\alpha\geq 2$, whereas Lemma 2.9 gives

$$\delta_1=1,\delta_2=\ldots=\delta_{\gamma}=2 \text{ and } \delta_{\gamma+i}=2^{i+1} \text{ for } i\geq 1, \tag{4.2}$$

whenever $p=2,\alpha=1$ and $d^2-1=2^{\gamma}q_2$, with $\gcd(2,q_2)=1$.

In this new setting we cannot guarantee the existence of fixed points, it will be depended on the corresponding value of κ.

Lemma 4.7. *Let* $\Delta=p^s$, $s\geq 1$ *and* $d\in\{2,\ldots,\Delta-1\}$ *with* $\gcd(\Delta,d)=1$ *and* $\gcd(d-1,\Delta)=p^{\alpha}$, $1\leq\alpha\leq s-1$. *Take* $\kappa\in\{1,\ldots,\Delta\}$. *Then* $1\in\mathrm{Per}(\phi_{d,\kappa})$ *if and only if* $p^{\alpha}|\kappa$.

Proof. Suppose that $x\in\mathbb{Z}_{\Delta}$ is a fixed point of $\phi_{d,\kappa}$. Using Proposition 2.11 gives

$$d\equiv 1\bmod\left(\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}\right).$$

Hence,

$$(d-1)=q\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)}=q\frac{\Delta}{\gcd(\Delta,(d-1)x+\kappa)}(d-1)$$

for some integers q. Since the previous three factors are positive integers we deduce that $q=1$ and $\gcd(\Delta,(d-1)x+\kappa)=\Delta$, which means $(d-1)x+\kappa=p^su$ for some integer $u\geq 1$. Now it is immediate to establish that p^{α} divides κ.

Conversely, suppose that $p^{\alpha}|\kappa$, that is, $\kappa=p^sh$ for some $h\geq 1$. Since $\gcd(p,q_d)=1$ (recall that $d-1=p^{\alpha}q_d$), by Lemma 2.4 there exists $x\in\mathbb{Z}_{\Delta}$ such that $q_dx+h\equiv p^{s-\alpha}\bmod(\Delta)$, so $q_dx+h=p^{s-\alpha}+\omega\Delta$ for some integer ω. In this case, $(d-1)x+\kappa=(p^{\alpha}q_d)x+(hp^{\alpha})=p^{\alpha}(q_dx+h)=p^s+\omega\Delta p^{\alpha}$, and $(d-1)x+\kappa\equiv 0\bmod(\Delta)$. Therefore, x is a fixed point of $\phi_{d,\kappa}$. □

Lemma 4.8. *Let* $\Delta=p^s$ *and* $s\geq 1$ *and* $d\in\{2,\ldots,\Delta-1\}$ *with* $\gcd(\Delta,d)=1$ *and* $\gcd(d-1,\Delta)=p^{\alpha}$, $d-1=p^{\alpha}q_d$, *and* $1\leq\alpha\leq s-1$. *Let* $\kappa\in\{1,\ldots,\Delta\}$. *Suppose that* $x\in\mathbb{Z}_{\Delta}$ *is a periodic point of* $\phi_{d,\kappa}$ *of period* N, *with* $\gcd(\Delta,(d-1)x+\kappa)=p^j$ *for some* $0\leq j\leq s$. *Then*

$$N=\delta_{s+\alpha-j},$$

the order of d *modulo* $p^{s+\alpha-j}$. *In particular:*

(a) $N=p^{s-j}$ *if* $p\geq 3$ *or* $p=2,\alpha\geq 2$;

(b) *If* $p=2,\alpha=1$ *and* $d^2-1=p^{\gamma}q_2$, *with* $gcd(2,q_2)=1$ *(by force* $\gamma\geq 3$*), in turn:*

(b.1) $N=1$ *if* $j=s$;

(b.2) $N=2$ *if* $1\leq s-j\leq\gamma-1$;

(b.3) $N=2^{s-j-\gamma+2}$ *if* $s-j\geq\gamma-1$.

Proof. By Proposition 2.11, N is the order of d modulo $\frac{(d-1)\Delta}{\gcd(\Delta,(d-1)x+\kappa)} = p^{s+\alpha-j}q_d$. So, $d^N \equiv 1 \bmod(p^{s+\alpha-j}q_d)$ and also

$$d^N \equiv 1 \bmod(p^{s+\alpha-j}).$$

Therefore, by the definition of order

$$\delta_{s+\alpha-j}|N.$$

To short the notation, write $\delta := \delta_{s+\alpha-j}$. Next, we proceed to show that $\phi_{d,\kappa}^{\delta}(x) = x$, and according to the definition of period N we will obtain $N|\delta$, and thus $N = \delta = \delta_{s+\alpha-j}$.

By (2.7), $\phi_{d,\kappa}^{\delta}(x) - x = \frac{d^\delta - 1}{d-1}\left((d-1)x+\kappa\right) = \frac{p^{\alpha+s-j}u}{p^\alpha q_d}p^j q_j$, where we have used the definition of δ, so $d^\delta - 1 = p^{\alpha+s-j}u$ for some integer u, and that $\gcd(\Delta,(d-1)x+\kappa) = p^j$, so $(d-1)x+\kappa = p^j q_j$ for some integer q_j. Then $\phi_{d,\kappa}^{\delta}(x) - x = p^s\frac{uq_j}{q_d}$, and taking into account $\phi_{d,\kappa}^{\delta}(x) - x \in \mathbb{Z}$ and $\gcd(q_d,p) = 1$, we deduce that $\phi_{d,\kappa}^{\delta}(x) - x \equiv 0 \bmod(\Delta)$, hence $N|\delta$.

By using Lemmas 2.7 and 2.9, we obtain the descriptions for N in cases (a) and (b), respectively. □

Theorem 4.9. *Let $\Delta = p^s \geq 3$, with p prime and $s \geq 1$. Let $d \in \{2,\dots,\Delta-1\}$ verify $\gcd(d,p) = 1$ and $d-1 = p^\alpha q_d$ with $1 \leq \alpha < s$ and $\gcd(p,q_d) = 1$. Put $\kappa = p^\beta q_k$, $0 \leq \kappa < p^s$, with $\gcd(p,q_k) = 1$ and $0 \leq \beta < s$. Then:*

(a) *If $\beta < \alpha$,*

(a.1) *If $p \geq 3$ or $p = 2, \alpha \geq 2$,*

$$\mathrm{Per}(\phi_{d,\kappa}) = \{p^{s-\beta}\}.$$

(a.2) *If $p = 2, \alpha = 1$ (thus, $\beta = 0$), with $d^2 - 1 = 2^\gamma q_2$, $\gamma \geq 3$ and q_2 odd,*

$$\mathrm{Per}(\phi_{d,\kappa}) = \{2^{\max\{1,s-\gamma+2\}}\}.$$

(b) *If $\beta \geq \alpha$, $\mathrm{Per}(\phi_{d,\kappa}) = \{\delta_\alpha, \delta_{\alpha+1},\dots,\delta_{s-1},\delta_s\}$, where $\delta_{\alpha+j}$ is the order of d modulo $p^{\alpha+j}$, $j = 0,1,\dots,s-\alpha$. In particular:*

(b.1) *If $p \geq 3$ or $p = 2, \alpha \geq 2$,*

$$\mathrm{Per}(\phi_{d,\kappa}) = \{1, p, \dots, p^{s-\alpha}\}.$$

(b.2) *If $p = 2$ and $\alpha = 1$, with $d^2 - 1 = 2^\gamma q_2$, $\gamma \geq 3$ and q_2 odd,*

$$\mathrm{Per}(\phi_{d,\kappa}) = \{2^j : j = 0,1,\dots,\max\{1, s-\gamma+1\}\}.$$

Proof.

(a) Let x be an arbitrary periodic point of $\phi_{d,\kappa}$. Then

$$(d-1)x+\kappa = p^\alpha q_d x + p^\beta q_k = p^\beta\left(q_k + p^{\alpha-\beta}q_d x\right)$$

with $\alpha - \beta \geq 1$ and $\gcd(p, q_k + p^{\alpha-\beta}q_d x) = 1$. Consequently, $\gcd(\Delta,(d-1)x+\kappa) = p^\beta$ for any periodic point $x \in \mathbb{Z}$ and part-(a) follows directly from Lemma 4.8 (notice that case-(b.1) of Lemma 4.8 is not admissible because $s + \alpha - \beta > 1$).

(b) First, since $(d-1)x+\kappa = p^\alpha\left(p^{\beta-\alpha}q_k + q_d x\right)$ and $\gcd(q_d,p) = 1$, use Lemma 2.4 to state that

$$\mathrm{Card}\left(\{(p^{\beta-\alpha}q_k + q_d x)\bmod(\Delta) : x \in \mathbb{Z}_\Delta\}\right) = \Delta.$$

From here, we deduce that there exist $x_j \in \mathbb{Z}_\Delta$ so that

$$(d-1)x_j + \kappa = p^\alpha(p^{\beta-\alpha}q_k + q_d x_j) = p^\alpha\left(p^j + \omega_j p^s\right) = p^{\alpha+j} + \widetilde{\omega}_j p^s \tag{4.3}$$

for some integers $\omega_j, \widetilde{\omega}_j = p^\alpha\omega_j$, $0 \le j \le s-\alpha$. If $j = s-\alpha$, it is obvious that $\gcd((d-1)x_{s-\alpha}+\kappa, \Delta) = p^s$, and it is a simple matter to see that $\gcd((d-1)x_j+\kappa, \Delta) = p^{\alpha+j}$ if $0 \le j < s-\alpha$. The point x_j is either periodic or eventually periodic, $j = 0, 1, \ldots, s-\alpha$.

If x_j is a periodic point of $\phi_{d,\kappa}$ of period N_j, being $\gcd(\Delta, (d-1)x_j+\kappa) = p^{\alpha+j}$, Lemma 4.8 ensures that $N_j = \delta_{s-j}$, being δ_{s-j} the order of d modulo p^{s-j}.

If x_j is eventually periodic, not periodic, we observe that also $\phi_{d,\kappa}(x_j)$ verifies the property $\gcd(\Delta, (d-1)\phi_{d,\kappa}(x_j)+\kappa) = p^{\alpha+j}$. Indeed, by (4.3),

$$\begin{aligned}(d-1)\phi_{d,\kappa}(x_j)+\kappa &= \kappa + (d-1)(\kappa + dx_j) = \kappa + (d-1)[x_j + \kappa + (d-1)x_j] \\ &= \kappa + (d-1)[x_j + p^{\alpha+j} + \widetilde{\omega}_j p^s] \\ &= [\kappa + (d-1)x_j] + (d-1)p^{\alpha+j} + (d-1)\widetilde{\omega}_j p^s \\ &= p^{\alpha+j} + \widetilde{\omega}_j p^s + (d-1)p^{\alpha+j} + (d-1)\widetilde{\omega}_j p^s \\ &= dp^{\alpha+j} + d\widetilde{\omega}_j p^s = d(p^{\alpha+j} + \widetilde{\omega}_j p^s),\end{aligned}$$

thus $\gcd(\Delta, (d-1)\phi_{d,\kappa}(x_j)+\kappa) = p^{\alpha+j}$, because $\gcd(d, \Delta) = 1$. Similarly, by the induction on n (we assume that $(d-1)\phi^n_{d,\kappa}(x_j)+\kappa = d^n(p^{\alpha+j} + \widetilde{\omega}_j p^s)$, with $\gcd(\Delta, (d-1)\phi^n_{d,\kappa}(x_j)+\kappa) = p^{\alpha+j}$) we find

$$\begin{aligned}(d-1)\phi^{n+1}_{d,\kappa}(x_j)+\kappa &= \kappa + (d-1)(\kappa + d\phi^n_{d,\kappa}(x_j)) \\ &= \kappa + (d-1)[\phi^n_{d,\kappa}(x_j) + d^n(p^{\alpha+j} + \widetilde{\omega}_j p^s)] \\ &= [\kappa + (d-1)\phi^n_{d,\kappa}(x_j)] + (d-1)d^n(p^{\alpha+j} + \widetilde{\omega}_j p^s) \\ &= d^n(p^{\alpha+j} + \widetilde{\omega}_j p^s) + (d-1)d^n(p^{\alpha+j} + \widetilde{\omega}_j p^s) \\ &= d^{n+1}(p^{\alpha+j} + \widetilde{\omega}_j p^s)\end{aligned}$$

with $\gcd(\Delta, (d-1)\phi^{n+1}_{d,\kappa}(x_j)+\kappa) = p^{\alpha+j}$. Following this process and taking into account that x_j is eventually periodic, for some m we finally obtain a periodic point $\widetilde{x}_j = \phi^m_{d,\kappa}(x_j)$ such that $\gcd(\Delta, (d-1)\widetilde{x}_j+\kappa) = p^{\alpha+j}$, and by Lemma 4.8 its period is δ_{s-j}.

Being j an arbitrary value, $0 \le j \le s-\alpha$, we have proved that $\{\delta_s, \delta_{s-1}, \ldots, \delta_\alpha\} \subseteq \mathrm{Per}(\phi_{d,\kappa})$. To finish, realize that if x is periodic of period N, being $\beta \ge \alpha$ we find $\gcd(\Delta, (d-1)x+\kappa) = p^{\alpha+j}$ for some $0 \le j \le s-\alpha$, and Lemma 4.8 yields $N = \delta_{s-j}$. Therefore, $\mathrm{Per}(\phi_{d,\kappa}) = \{\delta_s, \delta_{s-1}, \ldots, \delta_\alpha\}$.

In particular:

(b.1) if $p = 3$ or $p = 2, \alpha \ge 2$, by Lemma 2.7 or (4.1), we obtain $\delta_{\alpha+i} = p^i$ for $i \ge 0$. Therefore,

$$\mathrm{Per}(\phi_{d,\kappa}) = \{1, p, \ldots, p^{s-\alpha}\};$$

(b.2) if $p = 2$ and $\alpha = 1$, then $\mathrm{Per}(\phi_{d,\kappa}) = \{\delta_s, \delta_{s-1}, \ldots, \delta_\alpha\}$. If $\gamma \ge s$, by Lemma 2.9 (or (4.2)),

$$\mathrm{Per}(\phi_{d,\kappa}) = \{1, 2\}.$$

If $\gamma < s$, again Lemma 2.9 yields $\delta_1 = 1, \delta_2 = \ldots = \delta_\gamma = 2, \delta_{\gamma+1} = 2^2, \ldots, \delta_s = \delta_{\gamma+(s-\gamma)} = 2^{s-\gamma+1}$, so

$$\mathrm{Per}(\phi_{d,\kappa}) = \{1, 2, 2^2, \ldots, 2^{s-\gamma+1}\}.$$

□

In Table 2 we show some examples of the set of periods for different values of d, p and s.

Table 2: Set of periods of $\phi_{d,\kappa}$ when $\gcd(d,\Delta)=1$ and $\gcd(d-1,\Delta)>1$.

Δ	2^3				
d	3		5		
κ	$2\|\kappa$	$2\nmid\kappa$	$4\|\kappa$	$2\|\kappa,\ 4\nmid\kappa$	$2\nmid\kappa$
elements in $\mathrm{Per}(\phi_{d,0})$	1,2	4	1,2	4	8

Δ	3^2		3^3				
d	4, 7		4, 7, 13, 16, 22, 25		10, 19		
κ	$3\|\kappa$	$3\nmid\kappa$	$3\|\kappa$	$3\nmid\kappa$	$9\|\kappa$	$3\|\kappa,\ 9\nmid\kappa$	$3\nmid\kappa$
elements in $\mathrm{Per}(\phi_{d,0})$	1,3	9	1,3,9	27	1,3	9	27

4.3. Converse result

When $\Delta=p^s$ for a prime p we characterize the set of periods for a given map $\phi_{d,\kappa}:\mathbb{Z}_\Delta\to\mathbb{Z}_\Delta$. We now investigate what fixed sets can be obtained as the periods of a map $\phi_{d,\kappa}:\mathbb{Z}_\Delta\to\mathbb{Z}_\Delta$.

Proposition 4.10. *Let p be a prime number, $s\in\mathbb{N}$ and $\Delta=p^s\geq 3$, then it holds:*

1. *Let N be a divisor of $p-1$ and either $M\in\{0,1,\dots,s-1\}$ if $p\neq 2$ or $\Delta=2^2$, or $M\in\{0,1,\dots,s-2\}$ if $\Delta=2^m, m\geq 3$. Then there exist $d,\kappa\in\mathbb{Z}_\Delta$ such that $\{1\}\cup\{Np^j\}_{j=0}^M=\mathrm{Per}(\phi_{d,\kappa})$.*
2. *Let $M\in\{0,1,2,\dots,s\}$ then there exist $d,\kappa\in\mathbb{Z}_\Delta$ such that $\{p^M\}=\mathrm{Per}(\phi_{d,\kappa})$.*

Proof. We prove the first item of the result for $N\neq 1$, $N|(p-1)$. In this case, by force $p\neq 2$ and Theorem 2.5 we can choose a generator, g, of the multiplicative group $\mathbb{Z}_\Delta^*$. Moreover, g can be chosen in the set of generators of $\mathbb{Z}_p^*$ by Theorem 2.6. Recall that $\mathrm{Card}(\mathbb{Z}_\Delta^*)=\varphi(\Delta)=p^{s-1}(p-1)$ and then $g^{p^{s-1}(p-1)}\equiv 1 \bmod(\Delta)$. Let, as in Lemma 2.7, δ_j be the order of g modulo p^j, $j\in\{1,2,\dots,s\}$, and observe that g is a generator of $\mathbb{Z}_p^*$, so $\delta_1=p-1$ and by Lemma 2.7 $\delta_j=(p-1)p^{j-1}$ for any $j\in\{2,\dots,s\}$.

If $M=0$, Theorem 4.6 ends the proof of the first item. If $M\geq 1$, consider $u=s-M$, so $1\leq u\leq s-1$. Since N divides $p-1$, take the natural t for which $tN=p-1$, then $tNp^{u-1}=(p-1)p^{u-1}=\delta_u$. Take $d:=g^{tp^{u-1}}$ and observe that

$$d^N=g^{Ntp^{u-1}}=g^{\delta_u}\equiv 1 \bmod(p^u). \tag{4.4}$$

Since g is a generator then $\gcd(g,\Delta)=1$ and $\gcd(d,\Delta)=1$. Also $d=g^{tp^{u-1}}\not\equiv 1 \bmod(p^n)$ for any $n\in\{1,2,\dots,s-1\}$, otherwise by Remark 2.3 we have $\delta_n=p^{n-1}(p-1)|tp^{u-1}$, so $tp^{u-1}=hp^{n-1}(p-1)$ for some $h\in\mathbb{Z}$, or $p^{u-n}=h\frac{p-1}{t}$ which implies $t=p-1$ (taking into account that $\gcd(p,p-1)$ and $u\geq n$), that is, $N=1$, a contradiction. Therefore, $\gcd(d-1,\Delta)=1$.

In order to apply Theorem 4.4 we show that the order of d modulo p, say $\widetilde{\delta_1}$, is N. From (4.4) and Remark 2.3 we have $\widetilde{\delta_1}|N$. On the other hand, $d^{\widetilde{\delta_1}}=g^{t\widetilde{\delta_1}p^{u-1}}\equiv 1 \bmod(p)$, again by Remark 2.3 $\delta_1=p-1|t\widetilde{\delta_1}p^{u-1}$ and then $p-1|t\widetilde{\delta_1}$ since $\gcd(p,p-1)=1$. Considering that $p-1=tN$ we obtain $N|\widetilde{\delta_1}$ and therefore $\widetilde{\delta_1}=N$.

Additionally, it is easy to check that $d^N\not\equiv 1 \bmod(p^{u+1})$ and then $d^N-1=p^uq_d$ with $\gcd(p,q_d)=1$. Finally, we apply Theorem 4.4 to obtain $\{1\}\cup N\{p^j\}_{j=0}^{s-u}=\{1\}\cup N\{p^j\}_{j=0}^M=\mathrm{Per}(\phi_{d,\kappa})$ for any $\kappa\in\mathbb{Z}_\Delta$ and we are done.

If $N=1$ in case (1) we define $d=p^{s-M}+1$, $\kappa=p^{s-M}$ and then $\alpha=\beta=s-M$ in Theorem 4.9. If $p\geq 3$ or $p=2, s-M\geq 2$, that is, $p\geq 3$ or $p=2, M\leq s-2$, use Theorem 4.9 (b) to obtain $\mathrm{Per}(\phi_{d,\kappa})=\{p^j\}_{j=0}^{s-(s-M)}=\{p^j\}_{j=0}^M$. To complete case (1) with $N=1$, it remains to analyze $p=2, s-M=1$ and $\Delta=2^2$ (if $\Delta=2^m$, $m\geq 3$, the above reasoning covers the range for $M\in\{0,1,\dots,s-2\}$). Now, $s=2$, $M=1, d=3, \kappa=2$ and it is direct to check that $\mathrm{Per}(\phi_{3,2})=\{1,2\}$ in $\mathbb{Z}_4$.

For the proof of the second item, simply apply Proposition 3.1 (i) to obtain $\mathrm{Per}(\phi_{1,p^{s-\alpha}}) = \left\{\frac{p^s}{p^{s-\alpha}}\right\} = \{p^\alpha\}$. □

We summarize all the results of Sections 3 and 4 on the sets of periods of $\phi_{d,\kappa}$ in the next theorem.

Theorem C. *Let Δ be a positive integer, $d, \kappa \in \mathbb{Z}_\Delta$ and let $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$ be defined by $\phi_{d,\kappa}(x) = dx + \kappa$. Then we distinguish the following cases:*

1. *For any $\Delta \in \mathbb{N}$ we have $\mathrm{Per}(\phi_{0,\kappa}) = \{1\}$ and $\mathrm{Per}(\phi_{1,\kappa}) = \{\frac{\Delta}{\gcd(\Delta,\kappa)}\}$.*
2. *When $\Delta \geq 3$ is even, then $\mathrm{Per}(\phi_{\Delta-1,\kappa}) = \{1, 2\}$ if κ is even and $\mathrm{Per}(\phi_{\Delta-1,\kappa}) = \{2\}$ if κ is odd.*
3. *When $\Delta \geq 3$ is odd, then $\mathrm{Per}(\phi_{\Delta-1,\kappa}) = \{1, 2\}$.*
4. *For $\Delta = p^s$ and p prime, we have:*

Conditions on d, Δ, κ		$\mathrm{Per}(\phi_{d,\kappa})$
$\gcd(d, \Delta) = 1$	$\gcd(d-1, \Delta) = 1$ $d^N \equiv 1 \mod (p^\alpha)$, $\alpha \geq 1$ $d^N \not\equiv 1 \mod (p^{\alpha+1})$ *N is the order of d modulo p*	$\{1\} \cup N \cdot \{p^j\}_{j=0}^{\max\{0, s-\alpha\}}$
	$\gcd(d-1, \Delta) > 1$ $d \equiv 1 \mod (p^\alpha)$, $d \not\equiv 1 \mod (p^{\alpha+1})$ $\kappa \equiv 0 \mod (p^\beta)$, $\kappa \not\equiv 0 \mod (p^{\beta+1})$ $1 \leq \alpha < s$, $0 \leq \beta < s$, *If $p = 2$ this only works when $\alpha > 1$*	$\{p^j\}_{j=0}^{s-\alpha}$ *if* $\beta \geq \alpha$
		$\{p^{s-\beta}\}$ *if* $\beta < \alpha$
$\gcd(d, \Delta) > 1$		$\{1\}$

5. *For $\Delta = 2^s \geq 3$, the missing cases corresponding to $p = 2, \alpha = 1$ are:*

Conditions on d, Δ, κ		$\mathrm{Per}(\phi_{d,\kappa})$
$d \equiv 1 \mod (2)$, $d \not\equiv 1 \mod (2^2)$ $\kappa \equiv 0 \mod (2^\beta)$, $\kappa \not\equiv 0 \mod (2^{\beta+1})$ $d^2 \equiv 1 \mod (2^\gamma)$, $d^2 \not\equiv 1 \mod (2^{\gamma+1})$ $0 \leq \beta < s$, $\gamma \geq 3$	$\beta = 0$	$\{2\}$ *if* $s \leq \gamma - 1$
		$\{2^{s-\gamma+2}\}$ *if* $s > \gamma - 1$
	$\beta \geq 1$	$\{2^j\}_{j=0}^{\max\{1, s-\gamma+1\}}$

Conversely, let p be a prime and let $\Delta = p^s$ with $s \geq 1$ then:

1. *For any divisor N of $p-1$ and any $\alpha \in \{0, 1, 2 \ldots, s-1\}$ if $p \neq 2$ or $\Delta = 2^2$, $\alpha \in \{0, 1, 2 \ldots, s-2\}$ if $p = 2$, there exist $d, \kappa \in \mathbb{Z}_\Delta$ such that $\mathrm{Per}(\phi_{d,\kappa}) = \{1\} \cup \{Np^j\}_{j=0}^{\alpha}$.*
2. *For any $\alpha \in \{0, 1, 2 \ldots, s\}$ there exist $d, \kappa \in \mathbb{Z}_\Delta$ such that $\mathrm{Per}(\phi_{d,\kappa}) = \{p^\alpha\}$.*

Proof. Apply Lemma 2.10, Propositions 3.1, 4.3, 4.10 and Theorems 4.4, 4.9. □

As a consequence of this result we obtain Theorem A.

proof of Theorem A. Take $\Delta = p^s$ and $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$, then $\mathrm{Per}(\phi_{d,\kappa})$ is provided by Theorem C.

- If Theorem C (1) is applied then $\mathrm{Per}(\phi_{d,\kappa})$ is either $\{1\}$ or $\{p^j\}$ for some $j \in \{0, 1, \ldots, s\}$; both sets are of the type (A-2).

- When Theorem C (2) holds, then $p = 2$ with $s \geq 2$, and $\mathrm{Per}(\phi_{d,\kappa})$ is either $\{1, 2\}$ or $\{2\}$, being $\{1, 2\}$ of type (A-1) (notice that $\alpha = 1 \leq s - \sigma(2, s)$ for all $s \geq 2$) and $\{2\}$ is of type (A-2).
- In the case of Theorem C (3), $p \neq 2$ and we have $\mathrm{Per}(\phi_{d,\kappa}) = \{1, 2\}$, of type (A-1) for $N = 2$ (note that it divides $p - 1$) and $\alpha = 0$.
- The fourth item of Theorem C provides as period sets either
  - $\{1\} \cup N \cdot \{p^j\}_{j=0}^{\max\{0,s-\alpha\}}$, of type (A-1) in Theorem A since $\alpha \geq 1$, $0 \leq \max\{0, s - \alpha\} \leq s - 1 = s - \sigma(p, s)$; or
  - $\{p^j\}_{j=0}^{s-\alpha}$, of type (A-1) since $1 \leq s - \alpha \leq s - 1 = s - \sigma(p, s)$; or
  - $\{p^{s-\beta}\}$, of type (A-2) because $\beta < \alpha < s$, $\alpha \geq 1$, so $2 \leq s - \beta \leq s$.
  - To finish case (4), notice that $\{1\}$ is type of both (A-1) and (A-2).
- The sets given by Theorem C (5) are $\{2\}$, $\{2^{s-\gamma+2}\}$ (both sets are of type (A-2) since $s \geq 2$ and $2 \leq s - \gamma + 2 \leq s - 1$, we apply here $\gamma \geq 3$ and $s > \gamma - 1$) or $\{2^j\}_{j=0}^{\max\{1,s-\gamma+1\}}$ (of type (A-1) because $1 \leq \max\{1, s - \gamma + 1\} \leq s - 2 \leq s - \sigma(p, s)$, we apply $\gamma \geq 3$).

The converse follows directly from Proposition 4.10. □

5. The general case and Theorems B and D

Let $\Delta = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ be a decomposition into prime factors and let $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$ defined by $\phi_{d,\kappa}(x) = dx + \kappa$. Our interest is to relate the set $\mathrm{Per}(\phi_{d,\kappa})$ with the sets $\mathrm{Per}(\phi_{d_i,\kappa_i})$ analyzed before, where $\phi_{d_i,\kappa_i} : \mathbb{Z}_{p_i^{s_i}} \to \mathbb{Z}_{p_i^{s_i}}$. To perform this relation we need some technical results.

Lemma 5.1. *Let $\Delta = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ be a decomposition into prime factors and let $g : \mathbb{Z}_\Delta \to \prod_{i=1}^k \mathbb{Z}_{p_i^{s_i}}$ be defined by $g(x) = (x \bmod (p_i^{s_i}))_i$. Then g is a ring isomorphism.*

Proof. It is straightforward to check that g is a homomorphism, that is, g preserves the sum, the product and the unit elements. From the Chinese Remainder Theorem, (see [2, Th. 5.26]), the system of congruences $x \equiv a_1 \bmod p_1^{s_1}, \dots, x \equiv a_k \bmod p_k^{s_k}$ has exactly one solution z modulo the product Δ. Since $g(z) = (a_1, \dots, a_k)$, we obtain both the injectivity and the surjectivity of g and we are done. □

Proof of Theorem B. Let us now take $d_i = d \bmod (p_i^{s_i})$, $\kappa_i = \kappa \bmod (p_i^{s_i})$ and $\phi_{d_i,\kappa_i} : \mathbb{Z}_{p_i^{s_i}} \to \mathbb{Z}_{p_i^{s_i}}$ defined by $\phi_{d_i,\kappa_i}(x) = d_i x + \kappa_i$ for any $i \in \{1, 2, \dots, k\}$. Let $\prod_{i=1}^k \phi_{d_i,\kappa_i}$ be the product map defined from $\prod_{i=1}^k \mathbb{Z}_{p_i^{s_i}}$ into itself by

$$\prod_{i=1}^k \phi_{d_i,\kappa_i}((x_i)_i) = (d_i x_i + \kappa_i)_{i=1}^k .$$

Then, taking into account that $dx + \kappa \equiv d_i x + \kappa_i \bmod (p_i^{s_i})$ for all $x \in \mathbb{Z}_\Delta$, it is a simple matter to verify

$$g \circ \phi_{d,\kappa} = \prod_{i=1}^k \phi_{d_i,\kappa_i} \circ g, \tag{5.1}$$

that is, the systems are *topologically conjugate*. As a direct consequence of Lemma 5.1, (5.1) and $g \circ \phi_{d,\kappa}^m = \left(\prod_{i=1}^k \phi_{d_i,\kappa_i}\right)^m \circ g$ for all $m \geq 1$, we obtain

$$\mathrm{Per}(\phi_{d,\kappa}) = \mathrm{Per}\left(\prod_{i=1}^k \phi_{d_i,\kappa_i}\right)$$

and then Theorem B follows. □

As a consequence of this theorem we will obtain the proof of the below Theorem D, a more precise description of the set of periods in the general case. For given sets of natural numbers $A_1, A_2, \dots A_k$, we use the following definition:

$$\operatorname{lcm}\{A_i\}_{i=1}^k = \{\operatorname{lcm}\{a_i\}_{i=1}^k : a_i \in A_i\}.$$

Let $\Delta = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ be a decomposition into prime numbers with $s_i > 0$ and $\gcd(p_i, p_j) = 1$ for any $i \neq j$, $i, j \in \{1, 2, \dots k\}$. Let $\mathcal{Q}$ be a set, a *partition* of $\mathcal{Q}$ which is a pair of subsets $(\mathcal{R}, \mathcal{T})$ such that $\mathcal{Q} = \mathcal{R} \cup \mathcal{T}$, $\mathcal{R} \cap \mathcal{T} = \emptyset$ (eventually $\mathcal{R}$ or $\mathcal{T}$ can be the empty set). Fix a partition $(\mathcal{R}, \mathcal{T})$ of $\{1, 2, \dots, k\}$. Let $\mathcal{N} = \{n_i\}_{i \in \mathcal{R}}$ be a (fixed) set of positive integers. Consider a subset $E \in \mathcal{P}(\mathcal{R})$ and the corresponding subset $\{n_i\}_{i \in E} \subseteq \mathcal{N}$. Then we define

$$D_{E,\mathcal{N}} := \operatorname{lcm}\{n_i\}_{i \in E}$$

if $E \neq \emptyset$ and $D_{E,\mathcal{N}} = 1$ if $E = \emptyset$.

Write the decomposition of $D_{E,\mathcal{N}}$ into prime factors as follows

$$D_{E,\mathcal{N}} = p_1^{\beta_{1,E}} \cdot p_2^{\beta_{2,E}} \cdot \ldots \cdot p_k^{\beta_{k,E}} \cdot p_{k+1}^{\beta_{k+1,E}} \cdot \ldots \cdot p_{\omega_E}^{\beta_{\omega_E,E}},$$

where $\beta_{i,E} \geq 0$ if $1 \leq i \leq k$ and $\beta_{t,E} > 0$ whenever the prime p_t, with $t > k$, appears in the decomposition of $D_{E,\mathcal{N}}$.

Next, fix a set of natural numbers $\mathcal{A} = \{\alpha_i\}_{i=1}^k$ and for the case $\mathcal{R} \neq \emptyset$, $\mathcal{T} \neq \emptyset$, define

$$P_{\mathcal{N},\mathcal{A}}^E := \left\{ D_{E,\mathcal{N}} \cdot \prod_{i \in E} p_i^{\max\{0, j_i - \beta_{i,E}\}} \cdot \prod_{i \in \mathcal{T}} p_i^{\max\{0, \alpha_i - \beta_{i,E}\}} : 0 \leq j_i \leq \alpha_i \right\}$$

and

$$P_{\mathcal{N},\mathcal{A}}^{\emptyset} := \prod_{i \in \mathcal{T}} p_i^{\max\{0, \alpha_i\}}.$$

If $\mathcal{T} = \emptyset$ or $\mathcal{R} = \emptyset$ we consider that the products $\prod_{i \in \mathcal{T}} p_i^{\max\{0, \alpha_i - \beta_{i,E}\}}$ and $\prod_{i \in E} p_i^{\max\{0, j_i - \beta_{i,E}\}}$ are equal to 1, respectively. We are now in a position to describe and prove the following main result.

Theorem D. *Let $\Delta = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ be a decomposition into prime factors with $s_i > 0$ and $\gcd(p_i, p_j) = 1$ for any $i \neq j$, $i, j \in \{1, 2, \dots k\}$. Let $d, \kappa \in \mathbb{Z}_\Delta$. Then, there exist:*

(a) *a partition $(\mathcal{R}, \mathcal{T})$ of $\{1, 2, \dots, k\}$,*

(b) *a set of positive integers $\mathcal{A} = \{\alpha_i\}_{i=1}^k$, with $0 \leq \alpha_i \leq s_i$ if $i \in \mathcal{T}$ and $0 \leq \alpha_i \leq s_i - \sigma(p_i, s_i)$ whenever $i \in \mathcal{R}$,*

(c) *a set $\mathcal{N} = \{n_i\}_{i \in \mathcal{R}}$ of positive integers satisfying $n_i | (p_i - 1)$,*

for which

$$\operatorname{Per}(\phi_{d,\kappa}) = \bigcup_{E \in \mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E.$$

Conversely, let $(\mathcal{R}, \mathcal{T})$ be a partition of $\{1, 2, \dots, k\}$, let $\{\alpha_i\}_{i=1}^k$ and $\{n_i\}_{i \in \mathcal{R}}$ be sets of naturals verifying the conditions (b) *and* (c) *mentioned before. Then there exist $d, \kappa \in \Delta$ such that $\operatorname{Per}(\phi_{d,\kappa}) = \bigcup_{E \in \mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E$.*

Proof. We begin with the proof of the direct part. By applying Theorem B we obtain:

$$\operatorname{Per}(\phi_{d,\kappa}) = \operatorname{lcm}\{\operatorname{Per}(\phi_{d_i,\kappa_i})\}_{i=1}^k, \text{ where } d_i \equiv d \bmod (p_i^{s_i}),\ \kappa_i \equiv \kappa \bmod (p_i^{s_i}).$$

Now Theorem A is applied to compute each $\operatorname{Per}(\phi_{d_i,\kappa_i})$. Let

$$\mathcal{R} := \{i : 1 \leq i \leq k,\ \operatorname{Per}(\phi_{d_i,\kappa_i}) \text{ is of type (A-1)}\},$$

$$\mathcal{T} := \{i : 1 \leq i \leq k, \text{Per}(\phi_{d_i,\kappa_i}) \text{ is of type (A-2)}\}.$$

Then if $i \in \mathcal{R}$ there exist $n_i|(p_i - 1)$ and $0 \leq \alpha_i \leq s_i - \sigma(p_i, s_i)$ such that $\text{Per}(\phi_{d_i,\kappa_i}) = \{1\} \cup \{n_i p_i^j\}_{j=0}^{\alpha_i}$. If $i \in \mathcal{T}$ there exists $0 \leq \alpha_i \leq s_i$ such that $\text{Per}(\phi_{d_i,\kappa_i}) = \{p_i^{\alpha_i}\}$. We are going to prove now that $\text{Per}(\phi_{d,\kappa}) = \bigcup_{E\in\mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E$ where $\mathcal{N} = \{n_i\}_{i\in\mathcal{R}}$, $\mathcal{A} = \{\alpha_i\}_{i=1}^k$ and

$$P_{\mathcal{N},\mathcal{A}}^E = \left\{ D_{E,\mathcal{N}} \cdot \prod_{i\in E} p_i^{\max\{0,j_i-\beta_{i,E}\}} \cdot \prod_{i\in\mathcal{T}} p_i^{\max\{0,\alpha_i-\beta_{i,E}\}} : 0 \leq j_i \leq \alpha_i \right\}.$$

Let $t \in \text{Per}(\phi_{d,\kappa})$, then Theorem B gives $t = \text{lcm}\{m_i\}_{i=1}^k$ for some $m_i \in \text{Per}(\phi_{d_i,\kappa_i})$, $1 \leq i \leq k$. Moreover, if $i \in \mathcal{T}$ then $m_i = p_i^{\alpha_i}$, however, if $i \in \mathcal{R}$ we have two possibilities: either $m_i = 1$ or $m_i = n_i p_i^{j_i}$ with $0 \leq j_i \leq \alpha_i$. Let $E = \{i \in \mathcal{R} : m_i \neq 1\}$. If $E = \emptyset$, then $t = \prod_{i\in\mathcal{T}} p_i^{\alpha_i} \in P_{\mathcal{N},\mathcal{A}}^{\emptyset}$. If $E \neq \emptyset$, observe that if we write $\text{lcm}\{n_i\}_{i\in E} = p_1^{\beta_{1,E}} p_2^{\beta_{2,E}} \dots p_k^{\beta_{k,E}} p_{k+1}^{\beta_{k+1,E}} \dots p_{u_E}^{\beta_{u_E,E}}$ (the decomposition into prime factors with $\beta_{i,E} \geq 0$ if $1 \leq i \leq k$ and $\beta_{i,E} > 0$ otherwise) then:

$$\begin{aligned}
t &= \text{lcm}\{m_i\}_{i=1}^k \\
&= \text{lcm}\{p_r^{\alpha_r}, n_i p_i^{j_i} : r \in \mathcal{T}, i \in \mathcal{R}\} \\
&= \text{lcm}\{\text{lcm}\{n_l : l \in E\}, p_r^{\alpha_r}, p_i^{j_i} : r \in \mathcal{T}, i \in E\} \\
&= \text{lcm}\{p_1^{\beta_{1,E}} p_2^{\beta_{2,E}} \dots p_k^{\beta_{k,E}} p_{k+1}^{\beta_{k+1,E}} \dots p_{u_E}^{\beta_{u_E,E}}, p_r^{\alpha_r}, p_i^{j_i} : r \in \mathcal{T}, i \in E\} \\
&= p_1^{\beta_{1,E}} p_2^{\beta_{2,E}} \dots p_k^{\beta_{k,E}} p_{k+1}^{\beta_{k+1,E}} \dots p_{u_E}^{\beta_{u_E,E}} \cdot \prod_{i\in E} p_i^{\max\{j_i-\beta_{i,E},0\}} \cdot \prod_{i\in\mathcal{T}} p_i^{\max\{\alpha_i-\beta_{i,E},0\}}.
\end{aligned}$$

Then $t \in P_{\mathcal{N},\mathcal{A}}^E$ and we have shown that $\text{Per}(\phi_{d,\kappa}) \subseteq \bigcup_{E\in\mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E$.

Let now $t \in \bigcup_{E\in\mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E$, then there exists $E \in \mathcal{P}(\mathcal{R})$ and values $0 \leq j_i \leq \alpha_i$ such that

$$\begin{aligned}
t &= D_{E,\mathcal{N}} \cdot \prod_{i\in E} p_i^{\max\{j_i-\beta_{i,E},0\}} \cdot \prod_{i\in\mathcal{T}} p_i^{\max\{\alpha_i-\beta_{i,E},0\}} \\
&= p_1^{\beta_{1,E}} p_2^{\beta_{2,E}} \dots p_k^{\beta_{k,E}} p_{k+1}^{\beta_{k+1,E}} \dots p_{u_E}^{\beta_{u_E,E}} \cdot \prod_{i\in E} p_i^{\max\{j_i-\beta_{i,E},0\}} \cdot \prod_{i\in\mathcal{T}} p_i^{\max\{\alpha_i-\beta_{i,E},0\}} \\
&= \text{lcm}\{p_1^{\beta_{1,E}} p_2^{\beta_{2,E}} \dots p_k^{\beta_{k,E}} p_{k+1}^{\beta_{k+1,E}} \dots p_{u_E}^{\beta_{u_E,E}}, p_s^{\alpha_s}, p_i^{j_i} : s \in \mathcal{T}, i \in E\} \\
&= \text{lcm}\{\text{lcm}\{n_l : l \in E\}, p_s^{\alpha_s}, p_i^{j_i} : s \in \mathcal{T}, i \in E\} \\
&= \text{lcm}\{p_s^{\alpha_s}, n_i p_i^{j_i} : s \in \mathcal{T}, i \in E\}.
\end{aligned}$$

For the indices $r \in \mathcal{R} \setminus E$ we know that $m_r := 1 \in \text{Per}(\phi_{d_r,\kappa_r})$, because these sets of periods are of type (A-1). Therefore,

$$\begin{aligned}
t &= \text{lcm}\{p_s^{\alpha_s}, n_i p_i^{j_i} : s \in \mathcal{T}, i \in E\} \\
&= \text{lcm}\{p_s^{\alpha_s}, n_i p_i^{j_i}, m_r : s \in \mathcal{T}, i \in \mathcal{R}, r \in \mathcal{R} \setminus E\} \\
&= \text{lcm}\{m_\ell\}_{\ell=1}^k.
\end{aligned}$$

Thus $\bigcup_{E\in\mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E = \text{Per}(\phi_{d,\kappa})$.

Let us now prove the converse. For any $i \in \mathcal{R}$, apply Theorem A (A-1) to obtain $\phi_{d_i,\kappa_i} : \mathbb{Z}_{p_i^{s_i}} \to \mathbb{Z}_{p_i^{s_i}}$ such that $\text{Per}(\phi_{d_i,\kappa_i}) = \{1\} \cup \{n_i p^j\}_{j=0}^{\alpha_i}$. Apply now Theorem A (A-2), for any $i \in \mathcal{T}$, to obtain $\phi_{d_i,\kappa_i} : \mathbb{Z}_{p_i^{s_i}} \to \mathbb{Z}_{p_i^{s_i}}$ satisfying $\text{Per}(\phi_{d_i,\kappa_i}) = \{p_i^{\alpha_i}\}$. Now we use Lemma 5.1 and (5.1) to obtain $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$, $\phi_{d,\kappa} = \prod_{i=1}^k \phi_{d_i,\kappa_i}$, satisfying $\text{Per}(\phi_{d,\kappa}) = \text{lcm}\{\text{Per}(\phi_{d_i,\kappa_i})\}_{i=1}^k$ and finally repeating the argument of the direct part we obtain

$$\text{Per}(\phi_{d,\kappa}) = \bigcup_{E\in\mathcal{P}(\mathcal{R})} P_{\mathcal{N},\mathcal{A}}^E.$$

□

5.1. Examples

In the following table we show some examples of the set of periods in the general case.

Δ	10		15	45
d	3, 7		2	2
κ	$2\|\kappa$	$2\nmid\kappa$	any	any
elements in $\mathrm{Per}(\phi_{d,0})$	1,4	2,4	1,2,4	1,2,4,6,12

We analyze now an example by using the converse part of Theorem D. Let $\Delta = 3^2 \cdot 5 \cdot 31 \cdot 29$ with $(p_1, p_2, p_3, p_4) = (3, 5, 31, 29)$, $(s_1, s_2, s_3, s_4) = (2, 1, 1, 1)$, $\mathcal{R} = \{1, 2, 3, 4\}$, $\mathcal{T} = \emptyset$,

$$\mathcal{N} = \{n_1 = 2, n_2 = 2, n_3 = 15, n_4 = 7\}$$

and

$$\mathcal{A} = \{\alpha_1 = 1, \alpha_2 = 0, \alpha_3 = 0, \alpha_4 = 0\}.$$

Then we obtain the existence of $\phi_{d,\kappa} : \mathbb{Z}_\Delta \to \mathbb{Z}_\Delta$ satisfying

$$\mathrm{Per}(\phi_{d,\kappa}) = \bigcup_{E \in \mathcal{P}(\mathcal{R})} P^E_{\mathcal{N},\mathcal{A}} = \{1, 2, 6, 7, 14, 15, 30, 42, 105, 210\}.$$

This set is obtained by applying the calculations of the following table:

E	$D_{E,\mathcal{N}}$	$P^E_{\mathcal{N},\mathcal{A}}$	E	$D_{E,\mathcal{N}}$	$P^E_{\mathcal{N},\mathcal{A}}$
$\emptyset$	1	$\{1\}$	$\{2,3\}$	30	$\{30\}$
$\{1\}$	2	$\{2,6\}$	$\{2,4\}$	14	$\{14\}$
$\{2\}$	2	$\{2\}$	$\{3,4\}$	105	$\{105\}$
$\{3\}$	15	$\{15\}$	$\{1,2,3\}$	30	$\{30\}$
$\{4\}$	7	$\{7\}$	$\{1,2,4\}$	14	$\{14,42\}$
$\{1,2\}$	2	$\{2,6\}$	$\{1,3,4\}$	210	$\{210\}$
$\{1,3\}$	30	$\{30\}$	$\{2,3,4\}$	210	$\{210\}$
$\{1,4\}$	14	$\{14,42\}$	$\{1,2,3,4\}$	210	$\{210\}$

Let us find d and κ. By applying Theorem B, Lemma 5.1 and (5.1) we need to find maps $\phi_{d_i,\kappa_i} : \mathbb{Z}_{p_i^{s_i}} \to \mathbb{Z}_{p_i^{s_i}}$ satisfying $\mathrm{Per}(\phi_{d_1,\kappa_1}) = \{1, 2, 6\}$, $\mathrm{Per}(\phi_{d_2,\kappa_2}) = \{1, 2\}$, $\mathrm{Per}(\phi_{d_3,\kappa_3}) = \{1, 15\}$ and $\mathrm{Per}(\phi_{d_4,\kappa_4}) = \{1, 7\}$. Next, by applying Theorem C we need to find $d_i \in \mathbb{Z}_{p_i^{s_i}}$, $1 \le i \le 4$, satisfying: (1) the order of d_i modulo p_i is n_i $d_i^{n_i} \equiv 1 (p_i)$, (2) $d_i^{n_i} \not\equiv 1 \bmod (p_i^2)$. A solution of these relations is $d_1 = 2$, $d_2 = 4$, $d_3 = 7$, $d_4 = 7$ and the Chinese Remainder Theorem provides a unique $d = 20684 \in \mathbb{Z}_\Delta$ satisfying $d \equiv d_i \bmod (p_i^{s_1})$. Moreover, by Theorem C $\kappa_i = 0$, $1 \le i \le 4$, and $\kappa = 0$. □

Acknowledgment

This paper has been partially supported by the grants MTM2014-52920-P from Ministerio de Economía y Competitividad (Spain). The authors also thank the referee for the helpful suggestions.

References

[1] L. Alsedà, J. Llibre, M. Misiurewicz, *Combinatorial dynamics and entropy in dimension one*, Advanced Series in Nonlinear Dynamics, World Scientific Publishing Co., Inc., River Edge, NJ, (1993). 1

[2] T. M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, (1976). 2, 2.3, 2, 2.5, 2, 5

[3] V. I. Arnold, *The topology of algebra: combinatorics of squaring*, (Russian) Funktsional. Anal. i Prilozhen., **37** (2003), 20–35, translation in Funct. Anal. Appl., **37** (2003), 177–190. 2

[4] J. S. Cánovas, A. Linero, *Periodic structure of alternating continuous interval maps*, J. Difference Equ. Appl., **12** (2006), 847–858. 1

[5] J. S. Cánovas, A. Linero Bas, G. Soler López, *Periods of alternated systems generated by affine circle maps*, J. Difference Equ. Appl., **22** (2016), 441–467. 1, 1.1, 1

[6] A. Linero Bas, *Advances in discrete dynamics (Chapter 1. Periodic structure of discrete dynamical systems and global periodicity)*, Nova Science Publishers, NY, USA, (2013). 1

[7] O. M. Šarkovskiĭ, *Co-existence of cycles of a continuous mapping of the line into itself*, (Russian) Ukrain. Mat. Ž., **16** (1964), 61–71. 1

[8] O. M. Šarkovskiĭ, *On cycles and the structure of a continuous mapping*, (Russian) Ukrain. Mat. Ž., **17** (1965), 104–111.

[9] A. N. Šharkovskiĭ, *Coexistence of cycles of a continuous map of the line into itself*, Translated from the Russian by J. Tolosa, Proceedings of the Conference "Thirty Years after Sharkovskiĭ's Theorem: New Perspectives", Murcia, (1994), Internat. J. Bifur. Chaos Appl. Sci. Engrg., **5** (1995), 1263–1273. 1

[10] R. Uribe-Vargas, *Topology of dynamical systems in finite groups and number theory*, Bull. Sci. Math., **130** (2006), 377–402. 2