Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2015) 39: 872 – 883
© TÜBİTAK
doi:10.3906/mat-1503-2

# The iteration digraphs of finite commutative rings

**Yangjiang WEI***, **Gaohua TANG**
School of Mathematical Sciences, Guangxi Teachers Education University, Nanning, P.R. China

**Received:** 01.03.2015 • **Accepted/Published Online:** 28.05.2015 • **Printed:** 30.11.2015

**Abstract:** For a finite commutative ring $S$ (resp., a finite abelian group $S$) and a positive integer $k \geqslant 2$, we construct an iteration digraph $G(S,k)$ whose vertex set is $S$ and for which there is a directed edge from $a \in S$ to $b \in S$ if $b = a^k$. We generalize some previous results of the iteration digraphs from the ring $\mathbb{Z}_n$ of integers modulo $n$ to finite commutative rings, and establish a necessary and sufficient condition for $G(S,k_1)$ and $G(S,k_2)$ to be isomorphic for any finite abelian group $S$.

**Key words:** Iteration digraph, isomorphic component, isomorphic digraph

## 1. Introduction

In 1992, motivated by [6], Szalay investigated properties of the iteration digraph representing a dynamical system occurring in number theory [12]. Subsequently, Rogers' published paper [7] concerned the graph of the square mapping on the prime fields, which was a topic appended as a kind of postscript to his talks on discrete dynamical systems. In recent years, there has been growing interest in the iteration digraphs associated with the ring $\mathbb{Z}_n$ of integers modulo $n$, the quotient ring of polynomials over finite fields, and the ring of Gaussian integers modulo $n$, etc. (e.g., see [1, 3, 4, 11, 13, 14, 15]).

We describe this iteration digraph below. Let $S$ be a finite commutative ring (resp., a finite abelian group). The graph $G(S,k)$ ($k \geqslant 2$ is a positive integer) is a digraph whose vertices are the elements of $S$ and for which there is a directed edge from $a \in S$ to $b \in S$ if $b = a^k$. In this paper, we generalize some previous results of iteration digraphs from $\mathbb{Z}_n$ to finite commutative rings and establish a necessary and sufficient condition for $G(S,k_1)$ and $G(S,k_2)$ to be isomorphic for any finite abelian group $S$.

A *component* of a digraph is a directed subgraph that is a maximal connected subgraph of the associated undirected graph. If $\alpha$ is a vertex of a component in $G(S,k)$, we use $\mathrm{Com}_S(\alpha)$ to denote this component.

Suppose $\alpha$ is a vertex of $G(S,k)$. The in-degree of $\alpha$, denoted by $\mathrm{indeg}_S(\alpha)$, is the number of directed edges entering $\alpha$. We will simply write $\mathrm{indeg}(\alpha)$ when it is understood that $\alpha$ is a vertex in $G(S,k)$.

Cycles of length $t$ are called $t$-cycles, and cycles of length one are called *fixed points*. For an *isolated fixed point* $\alpha$, the in-degree and out-degree (i.e. the number of edges leaving $\alpha$) are both one. Suppose that $\alpha$ is a vertex in $G(S,k)$; $\alpha$ is said to be of *height* $h \geqslant 0$, if $h$ is the minimal nonnegative integer such that $\alpha^{k^h}$

*Correspondence: gus02@163.com
2010 *AMS Mathematics Subject Classification:* 05C05; 11A07; 13M05.
This research was supported by the National Natural Science Foundation of China (11161006, 11461010), and the Guangxi Natural Science Foundation (2014GXNSFAA118005).

is a cycle vertex. If the maximal height of all vertices in a component is $\lambda$, then we say that this component has height $\lambda$. Attached to each cycle vertex $\alpha$ of $G(S,k)$ is a tree $T_S(\alpha)$ whose root is $\alpha$ and whose additional vertices are the noncycle vertices $\beta$ for which $\beta^{k^i} = \alpha$ for some positive integers $i$, but $\beta^{k^{i-1}}$ is not a cycle vertex.

Further, if $R$ is a ring, let $\mathrm{U}(R)$ denote the unit group of $R$ and $\mathrm{D}(R)$ the zero-divisor set of $R$. For $\alpha \in \mathrm{U}(R)$, $o(\alpha)$ denotes the multiplicative order of $\alpha$ in $R$. If $R = \mathbb{Z}_n$, then we write $\mathrm{ord}_n\alpha$ instead of $o(\alpha)$. Moreover, we specify two particular subdigraphs $G_1(R,k)$ and $G_2(R,k)$ of $G(R,k)$, i.e. $G_1(R,k)$ is induced by all the vertices of $\mathrm{U}(R)$, and $G_2(R,k)$ is induced by all the vertices of $\mathrm{D}(R)$.

This paper is organized as follows. After this introduction, we obtain some results in Section 2 on cycles and components of $G(R,k)$ for finite commutative rings $R$. These results generalize the work [15] on the digraph associated to the square mapping. In Section 3, we employ the digraphs products to explore the symmetric digraphs and obtain results parallel to those of Somer and Křížek [10]. Section 4 gives a necessary and sufficient condition for $G(H,k_1)$ and $G(H,k_2)$ to be isomorphic, where $H$ is a finite abelian group. This result extends the work in [1] for the multiplicative group of a prime field $\mathbb{F}_p$.

## 2. Cycles and components

The *exponent* $\exp(H)$ of a finite group $H$ is the least positive integer $n$ such that $g^n = 1$ for all $g \in H$. By the finite group theories, it is easy to show that if $H$ is abelian; then there exists an element $g \in H$ such that $o(g) = \exp(H)$. In papers [9, 10, 11], the *Carmichael lambda-function* $\lambda(n)$ played the key role in the structure of $G(\mathbb{Z}_n,k)$. In fact, the function $\lambda(n)$ is equal to $\exp(\mathrm{U}(\mathbb{Z}_n))$. Throughout this paper, we simply write $\lambda(R)$ instead of $\exp(\mathrm{U}(R))$, where $R$ is a ring.

It is well known that if $R$ is a finite commutative ring with identity 1, then $R$ can be uniquely expressed as a direct sum of local rings:

$$R = R_1 \oplus \cdots \oplus R_s, \quad s \geqslant 1 \tag{2.1}$$

where $R_i$ is a local ring for $i = 1,\ldots,s$.

**Lemma 2.1** ([5, Theorem 2]) *Let $R$ be a finite local ring with identity element 1 that is not necessarily commutative. Let $M$ be the unique maximal ideal of $R$. Then $|R| = p^{nr}$, $|M| = p^{(n-1)r}$, $M^n = \{0\}$, and $\mathrm{char}(R) = p^k$, where $\mathrm{char}(R)$ is the characteristic of $R$, $p$ is a prime, $n$, $r$, $k$ are positive integers, and $1 \leqslant k \leqslant n$.*

Note by Lemma 2.1 that if $n = 1$, then $R$ is the field $\mathbb{F}_{p^r}$ with $|\mathbb{F}_{p^r}| = p^r$.

Since the unit group of a finite commutative ring is a product of some cyclic groups, we give some results concerning the iteration digraphs of cyclic groups that have been shown in paper [8].

**Lemma 2.2** *Let $k \geqslant 2$ be an integer. Let $C_n = \langle a \rangle$ be a cyclic group with $o(a) = n$. Suppose $\gcd(n,k) = d$. Then in $G(C_n,k)$ we have the following conclusions.*

1. For $a^x \in C_n$, $\mathrm{indeg}(a^x) > 0$ if and only if $d \mid x$.

2. If $d \mid x$, then $\mathrm{indeg}(a^x) = d$.

3. $G(C_n, k)$ has exactly one component if and only if $q \mid k$ for any prime factor $q$ of $n$.

A digraph is regular if all its vertices have the same in-degree, while the digraph $G(R, k)$ is said to be semiregular if there exists a positive integer $d$ such that each vertex of $G(R, k)$ has either in-degree 0 or $d$.

**Theorem 2.3** *For any finite commutative ring $R$ and $k \geqslant 2$, $G_1(R, k)$ is regular or semiregular. In particular, if $\mathrm{U}(R) = C_{n_1} \times \cdots \times C_{n_t}$, where $C_{n_i}$ is a cyclic group with order $n_i$, and $\gcd(n_i, k) = d_i$ for $i \in \{1, \ldots, t\}$, $t \geqslant 1$. Then for $\alpha \in \mathrm{U}(R)$, $\mathrm{indeg}(\alpha) = 0$ or $d_1 \cdots d_t$.*

**Proof** Let $\alpha = (a_1, \ldots, a_t) \in \mathrm{U}(R)$, where $a_i \in C_{n_i}$ for $i \in \{1, \ldots, t\}$. If $\mathrm{indeg}(\alpha) > 0$; then $\mathrm{indeg}_{C_{n_i}}(a_i) > 0$ for $i \in \{1, \ldots, t\}$, and hence

$$\mathrm{indeg}_R(\alpha) = \mathrm{indeg}_{C_{n_1}}(a_1) \times \cdots \times \mathrm{indeg}_{C_{n_t}}(a_t) = d_1 \cdots d_t$$

by Lemma 2.2. Therefore, if $d_1 = \cdots = d_t = 1$, then $\mathrm{indeg}_R(\alpha) = 1$ and $G_1(R, k)$ is regular. Otherwise, $G_1(R, k)$ is semiregular. □

Let $\Gamma_i$ be a subdigraph of $G(S, k_i)$, $i = 1, 2$. We say that $\Gamma_1 \cong \Gamma_2$ if there exists a mapping $f$ from the vertex set of $\Gamma_1$ to that of $\Gamma_2$ for which $f$ satisfies the following conditions:

1. $f$ is one-to-one and onto.

2. $f$ sends vertices of height $h$ into vertices of the same height $h$.

3. $f$ is edge-preserving, that is, $[f(a)]^{k_2} = f(a^{k_2})$ for $a \in \Gamma_1$.

Similarly to the proof of Theorem 29 of [3], we have the following theorem.

**Theorem 2.4** *Let $R$ be a finite commutative ring. Let $\beta \in \mathrm{U}(R)$ be a cycle vertex of $G(R, k)$ for $k \geqslant 2$. Then the tree $T_R(1)$ is isomorphic to the tree $T_R(\beta)$.*

**Proof** Let $i \geqslant 0$ be an integer. Let $\beta_i$ be the unique vertex in $G_1(R, k)$ that is in the same cycle as $\beta$ and such that $\beta_i^{k^i} = \beta$, i.e. $\beta_i$ is the cycle vertex $i$ vertices before $\beta$. We define the mapping $f$ from $T_R(1)$ into $T_R(\beta)$ by $f(\alpha) = \alpha\beta_h$ for any vertex $\alpha$ with height $h \geqslant 1$ in $T_R(1)$. It is easy to show that the mapping $f$ is one-to-one and onto. Further,

$$[f(\alpha)]^k = (\alpha\beta_h)^k = \alpha^k \beta_h^k = \alpha^k \beta_{h-1} = f(\alpha^k),$$

where $\beta_h^k = \beta_{h-1}$ is derived by the uniqueness of $\beta_h$, while $f(\alpha^k) = \alpha^k \beta_{h-1}$ because the height of $\alpha^k$ is $h-1$. Thus the mapping $f$ is edge-preserving and hence the tree $T_R(1)$ is isomorphic to the tree $T_R(\beta)$. □

**Theorem 2.5** *Let $R$ be a finite commutative ring. Let $u$ be the largest divisor of $\lambda(R)$ relatively prime to $k \geqslant 2$.*

1. The vertex $\alpha$ is a cycle vertex in $G_1(R, k)$ if and only if $\gcd(o(\alpha), k) = 1$.

2. The vertex $\alpha$ is a cycle vertex in $G_1(R, k)$ if and only if $o(\alpha) \mid u$.

**Proof** (1) If $\alpha$ lies on a $t$-cycle, then $t$ is the least positive integer such that $\alpha^{k^t} = \alpha$. Therefore, $o(\alpha) \,|\, (k^t - 1)$ and clearly $\gcd(o(\alpha), k) = 1$. Conversely, if $\gcd(o(\alpha), k) = 1$, then there is a least positive integer $t$ such that $k^t \equiv 1 \pmod{o(\alpha)}$, and hence $\alpha^{k^t} = \alpha$. Thus $\alpha$ lies on a $t$-cycle.

(2) Let $\lambda(R) = uv$. Then for any prime factor $q$ of $v$, we have $q \,|\, k$. If $\gcd(o(\alpha), k) = 1$, then $\gcd(o(\alpha), v) = 1$. It is obvious that $o(\alpha) \,|\, u$ since $o(\alpha) \,|\, \lambda(R)$. Conversely, if $o(\alpha) \,|\, u$, then $\gcd(o(\alpha), k) = 1$. Therefore, by (1) above, case (2) holds. □

**Theorem 2.6** *Let $R$ be a finite commutative ring and $k \geqslant 2$.*

1. The element $0$ is an isolated fixed point in $G(R, k)$ if and only if $R$ is a direct sum of fields.

2. The identity $1$ is an isolated fixed point in $G(R, k)$ if and only if $\gcd(\lambda(R), k) = 1$.

**Proof** Let $R$ be as in (2.1).

(1) Suppose $\alpha = (a_1, \ldots, a_s) \in R$ satisfies $\alpha^k = 0$. Then $0$ is an isolated fixed point in $G(R, k)$ if and only if $\text{indeg}_R(0) = 1$, if and only if $a_i^k = 0$ and $\text{indeg}_{R_i} a_i = 1$, if and only if $R_i$ is a field for $i \in \{1, \ldots, s\}$.

(2) Suppose that $\gcd(\lambda(R), k) = 1$. Then $\gcd(\lambda(R_i), k) = 1$ for each $i \in \{1, \ldots, s\}$. Then for $\alpha \in \mathrm{U}(R_i)$, $\gcd(o(\alpha), k) = 1$. By Theorem 2.5, $\alpha$ lies on a $t$-cycle in $G(R_i, k)$ for some $t \geqslant 1$. Therefore, $\text{indeg}_R(1) = 1$. The converse is clear. □

**Theorem 2.7** *Let $R$ be a finite commutative ring and $k \geqslant 2$.*

1. $G_1(R, k)$ is regular if and only if $\gcd(\lambda(R), k) = 1$.

2. $G_1(R, k)$ is semiregular if and only if $\gcd(\lambda(R), k) > 1$.

3. $G_2(R, k)$ is regular if and only if $R$ is a direct sum of $s \geqslant 2$ fields with $\gcd(\lambda(R), k) = 1$, or $R$ is a field.

4. $G(R, k)$ is regular if and only if $R$ is a direct sum of $s \geqslant 1$ fields and $\gcd(\lambda(R), k) = 1$.

**Proof** By Theorems 2.3 and 2.5, we derive (1) and (2).

Now suppose that $G_2(R, k)$ is regular. Let $R$ be as in (2.1). Then for $\alpha \in \mathrm{D}(R)$, we have $\text{indeg}_R(\alpha) = 1$. If there exists $i \in \{1, \ldots, s\}$ such that $R_i$ is not a field, without loss of generality, we assume that $R_1$ is not a field. Then there exists $0 \neq a \in \mathrm{D}(R_1)$ such that $a^k = 0$. Therefore, $\alpha = (a, 0, \ldots, 0) \in \mathrm{D}(R)$. Then $\alpha^k = 0$, and hence $\text{indeg}_R(0) > 1$, which implies that $G_2(R, k)$ is not regular, a contradiction. Thus we assume that each $R_i$ is a field for $i \in \{1, \ldots, s\}$, $s \geqslant 1$. If $s = 1$, clearly $G_2(R, k)$ is regular. If $s \geqslant 2$ but $\gcd(\lambda(R), k) > 1$, then there exists a prime $p$ such that $p \,|\, \lambda(R)$ and $p \,|\, k$. Therefore, we have an element $b_t \in \mathrm{U}(R_t)$ for some $t \in \{1, \ldots, s\}$ with $o(b_t) = p$. Hence $b_t^p = b_t^k = 1$. For convenience, let $t = 1$ and $\beta = (1, 0, \ldots, 0) \in \mathrm{D}(R)$. It is clear that $\text{indeg}_R(\beta) > 1$ since $(b_1, 0, \ldots, 0)^k = \beta$. Therefore, $G_2(R, k)$ is not regular, a contradiction, and so we derive that $\gcd(\lambda(R), k) = 1$. The converse of case (3) is clear.

Finally, note that $G(R, k)$ is regular if and only if both $G_1(R, k)$ and $G_2(R, k)$ are regular. Therefore, case (4) follows from cases (1) and (3). □

By Theorem 2.3, for any finite commutative ring $R$ and $k \geqslant 2$, $G_1(R,k)$ is either regular or semiregular, and, by Theorem 2.7, we characterize all regular digraphs $G_2(R,k)$. However, the semiregularity of $G_2(R,k)$ is not easy to obtain (e.g., see Theorem 4.4 of [9] and Theorem 4.2 of [13]). In the following theorem, we present a condition when $G_2(R,k)$ is semiregular.

**Theorem 2.8** *Let $R$ be a finite commutative local ring with unique maximal ideal $M$ and $\mathrm{char}(R) = p^t$ for some odd prime $p$. If $2 \mid k$, then $G_2(R,k)$ is semiregular if and only if $\alpha^k = 0$ for $\alpha \in M$.*

**Proof** Suppose that $G_2(R,k)$ is semiregular. If there exists $b \in M$ such that $b^k = c \neq 0$, then $\mathrm{indeg}(c) \geqslant 1$. Consider the solutions in $R$ of the equation $x^k = c$. We see that whenever $y^k = c$ for $y \in M$, then $(-y)^k = c$ since $2 \mid k$. Moreover, if $-y = y$, then $2y = 0$, which contradicts the fact that the characteristic of $R$ is odd. Thus $-y \neq y$. Further, 0 is not a solution of $x^k = c$, and so the number of solutions of this equation is even, i.e. $\mathrm{indeg}(c)$ is even. On the other hand, 0 is a solution of the equation $x^k = 0$. Similarly, whenever $z^k = 0$ for $0 \neq z \in M$, then $(-z)^k = 0$ with $-z \neq z$. Therefore, the number of solutions of the equation $x^k = 0$ is odd. Consequently, $\mathrm{indeg}(0)$ is odd. Hence, $\mathrm{indeg}(0) \neq \mathrm{indeg}(c)$. Therefore, $G_2(R,k)$ is not semiregular, which is a contradiction. This implies that for $a \in M$, $a^k = 0$. The converse is obvious. □

**Theorem 2.9** *Let $R$ be a finite commutative ring. If $G_2(R,k)$ contains a $t$-cycle $(t \geqslant 2)$, then $G_1(R,k)$ also contains a $t$-cycle.*

**Proof** Let $R$ be as in (2.1). If $G_2(R,k)$ contains a $t$-cycle $(t \geqslant 2)$, then it is obvious that $s \geqslant 2$. Suppose that $\alpha = (a_1, \ldots, a_s)$ lies on a $t$-cycle of $G_2(R,k)$, where $a_i \in \mathrm{D}(R_i)$ or $\mathrm{U}(R_i)$. Then $a_i$ lies on a $t_i$-cycle of $G(R_i,k)$ for $i \in \{1, \ldots, s\}$. For convenience, we can suppose that $a_1 = \cdots = a_m = 0$, where $s-1 \geqslant m \geqslant 1$, while $a_j \in \mathrm{U}(R_j)$ for $j \in \{m+1, \ldots, s\}$. It is evident that $\mathrm{lcm}[t_1, \ldots, t_s] = t$. Since $t_1 = \cdots = t_m = 1$, we have $\mathrm{lcm}[t_{m+1}, \ldots, t_s] = t$. Let $\beta = (b_1, \ldots, b_s)$, where $b_1 = \cdots = b_m = 1$, while $b_j = a_j$ for $j \in \{m+1, \ldots, s\}$. Clearly, $\beta \in \mathrm{U}(R)$ and $\beta$ lies on a $t$-cycle of $G_1(R,k)$. □

Recall that the Carmichael lambda-function $\lambda(n)$ is defined as follows: $\lambda(1) = \lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^k) = 2^{k-2}$ for $k \geqslant 3$, $\lambda(p^k) = (p-1)p^{k-1}$ for any odd prime $p$ and $k \geqslant 1$, $\lambda(p_1^{k_1} \cdots p_r^{k_r}) = \mathrm{lcm}[\lambda(p_1^{k_1}), \ldots, \lambda(p_r^{k_r})]$, where $p_1, \ldots, p_r$ are distinct primes and $k_i \geqslant 1$ for $i \in \{1, \ldots, r\}$. Let $L(G(R,k))$ denote the length of the longest cycle in $G(R,k)$. In the following theorem, we obtain $\max_{k \geqslant 2} L(G(R,k))$ via $\lambda(n)$, where $n = \lambda(R)$.

**Theorem 2.10** *Let $R$ be a finite commutative ring. Then $\max_{k \geqslant 2} L(G(R,k)) = \lambda(\lambda(R))$.*

**Proof** By Theorem 2.9, $L(G(R,k)) = L(G_1(R,k))$. Further, let $u$ be the largest divisor of $\lambda(R)$ relatively prime to $k$. Then there is an element $g \in \mathrm{U}(R)$ with $o(g) = u$. By Theorem 2.5, $g$ lies on a $t$-cycle. Then $u \mid (k^t - 1)$. Let $\gamma \in \mathrm{U}(R)$ be a cycle vertex. Then by Theorem 2.5 again, $o(\gamma) \mid u$. Assume that $\gamma$ lies on a $m$-cycle. Then $m$ is the least positive integer for which $k^m \equiv 1 \pmod{o(\gamma)}$. Since $o(\gamma) \mid u$, we have $o(\gamma) \mid u \mid (k^t - 1)$. Hence, $m \mid t$ and so we can conclude that $L(G_1(R,k)) = \mathrm{ord}_u k$.

Let $n = \lambda(R)$. By the properties of the exponent of finite groups, it is well known that there is a positive integer $z \in \mathrm{U}(\mathbb{Z}_n)$ such that $\mathrm{ord}_n z = \lambda(n)$. Hence, by the argument above, $L(G_1(R,z)) = \mathrm{ord}_n z = \lambda(n) = \lambda(\lambda(R))$ since $\gcd(z,n) = \gcd(z, \lambda(R)) = 1$.

Now let $k \geqslant 2$ be an arbitrary integer. Then $L(G_1(R,k)) = \mathrm{ord}_u k$, where $u$ is the largest divisor of $\lambda(R)$ relatively prime to $k$. Thus $t$ is the least positive integer such that $k^t \equiv 1 \pmod{u}$. Moreover, since $k \in \mathrm{U}(\mathbb{Z}_u)$, we have $k^{\lambda(u)} \equiv 1 \pmod{u}$. Therefore, we derive that $t \mid \lambda(u)$. Note that $u \mid \lambda(R)$. Thus we have $t \mid \lambda(u) \mid \lambda(\lambda(R))$. The assertion now follows. □

## 3. Digraphs products and symmetric digraphs

Given two digraphs $\Gamma_1$ and $\Gamma_2$, let $\Gamma_1 \times \Gamma_2$ denote the digraph whose vertices are the ordered pairs $(a_1, a_2)$, where $a_i$ is an arbitrary vertex of $\Gamma_i$ for $i = 1, 2$. In addition, there is a directed edge in $\Gamma_1 \times \Gamma_2$ from $(a_1, a_2)$ to $(b_1, b_2)$ if and only if there is a directed edge in $\Gamma_1$ from $a_1$ to $b_1$ and there is a directed edge in $\Gamma_2$ from $a_2$ to $b_2$. In general, if $S \cong S_1 \oplus \cdots \oplus S_t$, where $S$, $S_1$, ..., $S_t$ are rings (or groups), then $G(S,k) \cong G(S_1,k) \times \cdots \times G(S_t,k)$. In this section, we employ the digraphs products as the key tool and obtain results parallel to the work of Somer and Křížek, et al.

**Lemma 3.1** *Let $\Gamma_1$, $\Gamma_2$, $\Gamma_1^*$, and $\Gamma_2^*$ be digraphs with $\Gamma_1 \cong \Gamma_1^*$, $\Gamma_2 \cong \Gamma_2^*$. Then $\Gamma_1 \times \Gamma_2 \cong \Gamma_1^* \times \Gamma_2^*$.*

**Proof** Let $f_m$ be the digraph isomorphism from $\Gamma_m$ onto $\Gamma_m^*$, where $m = 1, 2$. We define the mapping $F$ from $\Gamma_1 \times \Gamma_2$ into $\Gamma_1^* \times \Gamma_2^*$ by

$$F((a,b)) = (f_1(a), f_2(b)),$$

where $(a,b)$ is an arbitrary vertex of $\Gamma_1 \times \Gamma_2$, $a \in \Gamma_1$ and $b \in \Gamma_2$. It is easy to check that $F$ is a digraph isomorphism from $\Gamma_1 \times \Gamma_2$ into $\Gamma_1^* \times \Gamma_2^*$. □

Let $M \geqslant 2$ be an integer. The digraph $\Gamma$ is said to be symmetric of order $M$ if its set of components can be partitioned into subsets of size $M$, each containing $M$ isomorphic components. Paper [10] investigated the symmetric digraphs of $G(\mathbb{Z}_n, k)$. Now we generalize some results and improve their proofs from [10].

**Theorem 3.2** *Suppose that $R = R_1 \oplus R_2$, where $R_1$ and $R_2$ are finite commutative rings. Let $k \geqslant 2$ and $M \geqslant 2$ be integers. Let $J(R_1,k)$ be a disjoint union of exactly $M$ distinct components of $G(R_1,k)$ such that these components are all isomorphic. Let $L(R_2,k)$ be a disjoint union of components of $G(R_2,k)$. Then $J(R_1,k) \times L(R_2,k)$ is a disjoint union of components of $G(R,k) = G(R_1,k) \times G(R_2,k)$ that is symmetric of order $M$.*

**Proof** Suppose that the $M$ isomorphic components in $J(R_1,k)$ are $J_1, \ldots, J_M$ with $J_i \cong J_t$ for $i,t \in \{1,\ldots,M\}$ and each cycle in $J(R_1,k)$ is an $s$-cycle. Let $L$ be any component of $L(R_2,k)$ with a $d$-cycle. Then $J(R_1,k) \times L \cong \bigcup_{i=1}^{M} (J_i \times L)$. Clearly, there are exactly

$$\frac{sd}{\mathrm{lcm}[s,d]} = \gcd(s,d)$$

components in each subdigraph $J_i \times L$ for $i \in \{1,\ldots,M\}$. By Lemma 3.1, $J_i \times L \cong J_t \times L$ for $i,t \in \{1,\ldots,M\}$, which implies that for each component $\mathbb{A}_{i,r}$ in $J_i \times L$, where $r = 1, \ldots, \gcd(s,d)$, there exists a component $\mathbb{A}_{t,r}$ in $J_t \times L$ so that $\mathbb{A}_{i,r} \cong \mathbb{A}_{t,r}$. Hence, $\mathbb{A}_{1,r} \cong \mathbb{A}_{2,r} \cong \cdots \cong \mathbb{A}_{M,r}$. Therefore, $J(R_1,k) \times L$ is symmetric of order $M$, and hence $J(R_1,k) \times L(R_2,k)$ is symmetric of order $M$. □

Theorems 5.1 and 5.7 of [10] determined the symmetric digraph of order $M$ associated to $\mathbb{Z}_n$ for various integers $M \geqslant 2$ when $n$ was given. Similarly, we have the following results for finite commutative rings.

**Theorem 3.3** *Let $R = R_1 \oplus R_2$, where $R_1$ and $R_2$ are finite commutative rings.*

1. Suppose that $R_1$ is a local ring with unique maximal ideal $M$ such that $|R_1| = 2|M| = 2^n$, $n \geqslant 1$. Then $G(R,k)$ is symmetric of order 2 if one of the following conditions hold.

   (a) $n \leqslant 2 \leqslant k$ and $2 \,|\, k$.

   (b) $n = 3$ and $4 \,|\, k$.

   (c) $n \geqslant 4$ and $2^{n-2} \,|\, k$.

2. Suppose that $R_1$ is a local ring with unique maximal ideal $M$ such that $|R_1| = p|M| = p^n$, $p$ is an odd prime, $n \geqslant 1$. Suppose further that $(p-1) \,|\, (k-1)$ and $p^{n-1} \,|\, k$. Then $G(R,k)$ is symmetric of order $p$.

3. Suppose that $R_1 = \mathbb{F}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{F}_{p_s^{t_s}}$, where $p_1, \dots, p_s$ are primes, $t_1, \dots, t_s$ and $s$ are positive integers. Suppose further that $\prod_{i=1}^{s}(p_i^{t_i} - 1) \,|\, (k-1)$. Then $G(R,k)$ is symmetric of order $p_1^{t_1} \cdots p_s^{t_s}$.

4. Suppose that $R_1 = R_0 \oplus \mathbb{F}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{F}_{p_s^{t_s}}$, where $R_0$ is a local ring with unique maximal ideal $M$, $|R_0| = p_0|M| = p_0^n$, $p_0$ is an odd prime, $n \geqslant 2$, $t_1, \dots, t_s$ and $s$ are positive integers, $p_1, \dots, p_s$ are primes such that $p_0 \neq p_i$ and $p_0 \nmid p_i^{t_i} - 1$ for $i \in \{1, \dots, s\}$. Then there is a positive integer $k$ such that

$$k \equiv 1 \pmod{(p_0 - 1)\prod_{i=1}^{s}(p_i^{t_i} - 1)}, \quad k \equiv 0 \pmod{p_0^{n-1}}. \tag{3.1}$$

   Moreover, $G(R,k)$ is symmetric of order $p_0 p_1^{t_1} \cdots p_s^{t_s}$.

**Proof** (1) If $n = 1$, then $R_1 = \mathbb{F}_2$. Therefore, $G(R_1,k)$ is symmetric of order 2 for $k \geqslant 2$. If $n = 2$, then $R_1 = \mathbb{Z}_4$ if $char(R_1) = 2^2$. Otherwise, if $\mathrm{char}(R_1) = 2$, then by Theorem 3 of [5], $R_1$ is isomorphic to the ring of upper triangular matrices $R^*$ over $\mathbb{F}_2$, where

$$R^* = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}.$$

Obviously, $R^* \cong \mathbb{Z}_2[x]/\langle x^2 \rangle$ and $R^*$ is commutative. Hence, for $\alpha \in R_1$, either $\alpha^k = 0$ or $\alpha^k = 1$ if $2 \,|\, k$. Thus $G(R_1,k)$ has precisely two components, one with fixed point 0 and the other with fixed point 1, and both components are isomorphic. By Theorem 3.2, part (a) of case (1) holds.

Now suppose $n = 3$ and $4 \,|\, k$. Clearly $\alpha^k = 0$ or $\alpha^k = 1$ for $\alpha \in R_1$ since $|M| = |\mathrm{U}(R_1)| = 4$. By Theorem 3.2, part (b) of case (1) holds.

We now prove part (c) of case (1). Suppose that $n \geqslant 4$ and $2^{n-2} \,|\, k$. By assumption, $|M| = |\mathrm{U}(R_1)| = 2^{n-1}$, and by Lemma 2.1, $M^n = \{0\}$. Note that $k \geqslant n$ since $n \geqslant 4$ and $2^{n-2} \,|\, k$. We see that $\alpha^k = 0$ for $\alpha \in M$. Furthermore, by the work of Gilmer in [2], if $|S| = 2^t$, where $S$ is a local ring and $t \geqslant 4$, then $\mathrm{U}(S)$ is not a cyclic group. Thus $\mathrm{U}(R_1) \cong C_{2^{n_1}} \times \cdots \times C_{2^{n_s}}$, where $s \geqslant 2$, $1 \leqslant n_i \leqslant n-2$, $C_{2^{n_i}}$ is a cyclic group with order $2^{n_i}$ for $i \in \{1, \dots, s\}$, and $n_1 + \cdots + n_s = n - 1$. Therefore, the exponent $\lambda(R_1)$ of $\mathrm{U}(R_1)$ is equal to $2^{n-t}$ for some $t \in \{2, \dots, n-1\}$. It follows that $\beta^{2^{n-2}} = 1$ for $\beta \in \mathrm{U}(R_1)$. Moreover, since $2^{n-2} \,|\, k$, we have

$\beta^k = 1$ for $\beta \in \mathrm{U}(R_1)$. Thus $G(R_1,k)$ has precisely two components, and both components are isomorphic. Theorem 3.2 establishes part (c) of case (1).

(2) By hypothesis, $|\mathrm{U}(R_1)| = p^{n-1}(p-1)$. Therefore, $\mathrm{U}(\mathrm{R}_1) \cong H_1 \times H_2$, where $H_1$ and $H_2$ are abelian groups, $|H_1| = p^{n-1}$ and $|H_2| = p-1$. Thus, $\alpha^{p^{n-1}} = 1$, and hence $\alpha^k = 1$ for $\alpha \in H_1$ since $p^{n-1} \,|\, k$. Therefore, $G(H_1,k)$ has exactly one component and $\mathrm{indeg}_{H_1}(1) = p^{n-1}$. On the other hand, for $\beta \in H_2$, $\beta^{p-1} = 1$, and hence $\beta^k = \beta^{k-1}\beta = \beta$ since $(p-1) \,|\, (k-1)$. Thus we can conclude that each vertex of $G(H_2,k)$ is an isolated fixed point. By the definition of diagraphs products, we have

$$G_1(R_1,k) = G(\mathrm{U}(\mathrm{R}_1),k) \cong G(H_1,k) \times G(H_2,k).$$

Therefore, $G_1(R_1,k)$ has precisely $p-1$ components, each of them is of height 1, and each cycle vertex is a fixed point with in-degree $p^{n-1}$. Moreover, by Lemma 2.1, $M^n = \{0\}$. Since $p^{n-1} \,|\, k$, we derive that $k > n$. Thus for $\gamma \in M$, $\gamma^k = 0$, and so $\mathrm{indeg}_{R_1}(0) = |M| = p^{n-1}$. Hence we can see that $G(R_1,k)$ has precisely $p$ components, and these components are all isomorphic. Therefore, case (2) follows by Theorem 3.2.

(3) It is obvious that $\alpha^{p_i^{t_i}-1} = 1$ for $\alpha \in \mathbb{F}_{p_i^{t_i}} \setminus \{0\}$. Since $\prod_{i=1}^{s}(p_i^{t_i}-1) \,|\, (k-1)$, we have $(p_i^{t_i}-1) \,|\, (k-1)$ for $i \in \{1,\ldots,s\}$. Hence, $\alpha^k = \alpha^{k-1}\alpha = \alpha$ for $\alpha \in \mathbb{F}_{p_i^{t_i}} \setminus \{0\}$. Therefore, each vertex in $G(\mathbb{F}_{p_i^{t_i}},k)$ is an isolated fixed point. Thus, each vertex in $G(R_1,k)$ is an isolated fixed point, and, by Theorem 3.2, case (3) holds.

(4) By assumption, $\gcd(p_0, p_i^{t_i}-1) = 1$ for $i = 1,\ldots,s$. Hence, by the Chinese Remainder Theorem, it is indeed possible to find a positive integer $k$ such that (3.1) holds. Further, by the proof of (2), $G(R_0,k)$ has precisely $p_0$ components, and these components are all isomorphic. Moreover, by (3) above, each vertex in $G(\mathbb{F}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{F}_{p_s^{t_s}},k)$ is an isolated fixed point. Therefore, it is evident that $G(R_1,k)$ has precisely $p_0 p_1^{t_1}\cdots p_s^{t_s}$ components, and these components are all isomorphic. Thus this case follows by Theorem 3.2. □

## 4. Isomorphic digraphs

Theorem 3.2 in paper [1] established a necessary and sufficient condition for $G(\mathbb{F}_p,k_1) \cong G(\mathbb{F}_p,k_2)$, where $p$ is a prime. In this section, we extend Theorem 3.2 of [1] to any finite abelian group. Before proceeding further, we present the following propositions on the structure of iteration digraphs of finite groups.

**Proposition 4.1** *Suppose that $H = C_{n_1} \times \cdots \times C_{n_s}$ is a finite abelian group. Let $k_2 > k_1$ be positive integers. Then $G(H,k_1) = G(H,k_2)$ if and only if $\mathrm{lcm}[n_1,\ldots,n_s]$ divides $k_2 - k_1$.*

**Proof** Let $C_{n_i} = \langle g_i \rangle$ for $i \in \{1,\ldots,s\}$. Let $g = (g_1,\ldots,g_s) \in H$. Then $o(g) = \mathrm{lcm}[n_1,\ldots,n_s]$. Assume that $G(H,k_1) = G(H,k_2)$. Then $g^{k_1} = g^{k_2}$. Hence, $o(g) \,|\, (k_2-k_1)$, i.e. $\mathrm{lcm}[n_1,\ldots,n_s] \,|\, (k_2-k_1)$.

Conversely, assume that $\mathrm{lcm}[n_1,\ldots,n_s] \,|\, (k_2-k_1)$. Then for $\beta = (g_1^{d_1},\ldots,g_s^{d_s}) \in H$, where $1 \leqslant d_i \leqslant n_i$ $(i = 1,\ldots,s)$, since $o(\beta) \,|\, o(g)$, we obtain $\beta^{o(g)} = 1$. Accordingly, $\beta^{k_2-k_1} = 1$, i.e. $\beta^{k_1} = \beta^{k_2}$. Thus $G(H,k_1) = G(H,k_2)$. □

**Proposition 4.2** *Let $C_n$ be a cyclic group with order $n$ and $k \geqslant 2$.*

1. Suppose $\gcd(n,k)=1$. Then $G(C_n,k)$ is the disjoint union

$$G(C_n,k)=\bigcup_{d\,|\,n}\underbrace{(\sigma(\mathrm{ord}_d k)\cup\cdots\cup\sigma(\mathrm{ord}_d k))}_{\varphi(d)/\mathrm{ord}_d k},$$

   where $\sigma(l)$ is the cycle of length $l$ and $\varphi(d)$ is the Euler totient function.

2. Suppose that $\gcd(n,k)>1$ and $n=uv$, where $u$ is the largest divisor of $n$ relatively prime to $k$. Then

$$G(C_n,k)=\bigcup_{d\,|\,u}\underbrace{(\sigma(\mathrm{ord}_d k,T(C_v)))\cup\cdots\cup\sigma(\mathrm{ord}_d k,T(C_v)))}_{\varphi(d)/\mathrm{ord}_d k},$$

   where $\sigma(l,T(C_v))$ consists of a cycle of length $l$ with a copy of the tree $T(C_v)$ attached to each vertex, and $T(C_v)$ is isomorphic to the tree attached to the fixed point 1 in $G(C_v,k)$.

**Proof** (1) Let $C_n=\bigcup_{d\,|\,n} H_d$, where $H_d$ is the set of elements with order $d$ in $C_n$, $d\,|\,n$. Since $\gcd(n,k)=1$, we have $\gcd(d,k)=1$ for $d\,|\,n$. Therefore, for $g\in H_d$, $\mathrm{ord}_d k$ is the least positive integer such that $g^{k^{\mathrm{ord}_d k}}=g$. This implies that each element of $H_d$ lies on a cycle of length $\mathrm{ord}_d k$. Moreover, since $|H_d|=\varphi(d)$, the formula is established.

(2) Since $u$ is the largest divisor of $n$ relatively prime to $k$, $p\,|\,k$ for each prime factor $p$ of $v$. By Lemma 2.2, the digraph $G(C_v,k)$ has exactly one component. Moreover, $C_n\cong C_u\times C_v$ since $\gcd(u,v)=1$. Hence, $G(C_n,k)\cong G(C_u,k)\times G(C_v,k)$. By case (1) above, each vertex of $G(C_u,k)$ lies on a cycle. Thus by the definition of digraph products, the result follows. □

**Proposition 4.3**

1. *Suppose that $\Gamma_1=G(C_{p^t},p^\lambda)$ and $\Gamma_2=G(C_{p^t},p^\lambda m)$, where $\lambda,t$, and $m$ are positive integers and $p$ is a prime with $p\nmid m$. Then $\Gamma_1\cong\Gamma_2$.*

2. *Suppose that $k_1$ and $k_2$ are positive integers. If $p\,|\,k_j$ for any prime factor $p$ of $n$ ($j=1,2$) and $\gcd(n,k_1)=\gcd(n,k_2)$, then $G(C_n,k_1)\cong G(C_n,k_2)$.*

**Proof** (1) If $\lambda\geqslant t$, then $g^{p^\lambda}=g^{p^\lambda m}=1$ for $g\in C_{p^t}$. Accordingly, $\Gamma_1\cong\Gamma_2$. Now we assume that $1\leqslant\lambda<t$. By Lemma 2.2 (3), $\Gamma_i$ has exactly one component, and the indegree of any vertex of $\Gamma_i$ is either 0 or $p^\lambda$, $i=1,2$. Let $C_{p^t}=\langle a\rangle$. In $\Gamma_1$, for $x\in\{1,\ldots,p^t\}$, the height of $a^x$ is $h$ if and only if $h$ is the least positive integer for which $(a^x)^{p^{\lambda h}}=1$, i.e. $p^t\,|\,xp^{\lambda h}$. Analogously, in $\Gamma_2$, for $y\in\{1,\ldots,p^t\}$, the height of $a^y$ is $h$ if and only if $h$ is the least positive integer for which $(a^y)^{p^{\lambda h}m^h}=1$, i.e. $p^t\,|\,yp^{\lambda h}m^h$. Since $p\nmid m$, we deduce that the height of $a^y$ in $\Gamma_2$ is $h$ if and only if $h$ is the least positive integer such that $p^t\,|\,yp^{\lambda h}$. Accordingly, the number of vertices with height $h$ in $\Gamma_1$ is equal to that of $\Gamma_2$ for $h\geqslant 1$. Hence, $\Gamma_1\cong\Gamma_2$.

(2) By Lemma 2.2 (3), $G(C_n,k_j)$ has exactly one component, $j=1,2$. By hypothesis, one can assume that

$$n=p_1^{t_1}\cdots p_s^{t_s},\quad k_1=p_1^{\lambda_1}\cdots p_s^{\lambda_s}m_1,\quad k_2=p_1^{l_1}\cdots p_s^{l_s}m_2,$$

where $p_1 < \cdots < p_s$ are primes, $\gcd(n, m_1) = \gcd(n, m_2) = 1$, $t_i$, $\lambda_i$ and $l_i$ are positive integers for $i = 1, \ldots, s$. Moreover, $\min\{t_i, \lambda_i\} = \min\{t_i, l_i\}$ for $i \in \{1, \ldots, s\}$.

It is obvious that $G(C_n, k_j) \cong G(C_{p_1^{t_1}}, k_j) \times \cdots \times G(C_{p_s^{t_s}}, k_j)$ for $j = 1, 2$. Therefore, if $G(C_{p_i^{t_i}}, k_1) \cong G(C_{p_i^{t_i}}, k_2)$ for $i = 1, \ldots, s$, then, by Lemma 3.1, one can deduce that $G(C_n, k_1) \cong G(C_n, k_2)$.

Indeed, since $\min\{t_i, \lambda_i\} = \min\{t_i, l_i\}$, one has $l_i \geqslant t_i$, provided that $\lambda_i \geqslant t_i$, and so $p_i^{t_i} \mid k_j$ for $j = 1, 2$ and $i \in \{1, \ldots, s\}$. Thus, it follows from Proposition 4.1 that $G(C_{p_i^{t_i}}, k_1) = G(C_{p_i^{t_i}}, p_i^{t_i}) = G(C_{p_i^{t_i}}, k_2)$. On the other hand, if $\lambda_i < t_i$, then one has $l_i = \lambda_i$. Therefore, for $j = 1, 2$, $k_j \equiv p_i^{\lambda_i} n_{i,j} \pmod{p_i^{t_i}}$ for some $n_{i,j}$ with $p_i \nmid n_{i,j}$. By Proposition 4.1 again, one has $G(C_{p_i^{t_i}}, k_j) = G(C_{p_i^{t_i}}, p_i^{\lambda_i} n_{i,j})$. Moreover, by the result of above (1), clearly $G(C_{p_i^{t_i}}, p_i^{\lambda_i} n_{i,1}) \cong G(C_{p_i^{t_i}}, p_i^{\lambda_i}) \cong G(C_{p_i^{t_i}}, p_i^{\lambda_i} n_{i,2})$. Accordingly, we obtain $G(C_{p_i^{t_i}}, k_1) \cong G(C_{p_i^{t_i}}, k_2)$.
□

**Lemma 4.4** *Suppose that*

$$\prod_{i=1}^{s} \gcd(n_i, a) = \prod_{i=1}^{s} \gcd(n_i, b), \tag{4.1}$$

*where* $n_1, \ldots, n_s$, $a$, $b$, *and* $s$ *are positive integers. If* $d \mid \gcd(n_i, a)$ *for some* $i \in \{1, \ldots, s\}$, *then* $d \mid \gcd(n_i, b)$. *In particular,* $\gcd(n_i, a) = \gcd(n_i, b)$ *for* $i \in \{1, \ldots, s\}$.

**Proof** Assume that

$$n_i = p_1^{t_{1,i}} \cdots p_k^{t_{k,i}}, \quad a = p_1^{l_1} \cdots p_k^{l_k}, \quad b = p_1^{h_1} \cdots p_k^{h_k},$$

where $k \geqslant 1$, $i \in \{1, \ldots, s\}$, $p_1 < \cdots < p_k$ are primes, $t_{j,i}$, $l_j$, $h_j \geqslant 0$ for $j \in \{1, \ldots, k\}$ and $i \in \{1, \ldots, s\}$. Without loss of generality, we prove $d \mid \gcd(n_1, b)$ if $d \mid \gcd(n_1, a)$, and it suffices to show that $h_j \geqslant \min\{l_j, t_{j,1}\}$ for $j \in \{1, \ldots, k\}$. By way of contradiction, we suppose that $h_m < \min\{l_m, t_{m,1}\}$ for some $m \in \{1, \ldots, k\}$. For convenience, assume that $h_1 < \min\{l_1, t_{1,1}\}$. Then $h_1 < l_1$ and $h_1 < t_{1,1}$. Moreover, by (4.1), we have

$$\begin{aligned} &\min\{l_1, t_{1,1}\} + \min\{l_1, t_{1,2}\} + \cdots + \min\{l_1, t_{1,s}\} \\ =\ &\min\{h_1, t_{1,1}\} + \min\{h_1, t_{1,2}\} + \cdots + \min\{h_1, t_{1,s}\}. \end{aligned} \tag{4.2}$$

By assumption, $\min\{l_1, t_{1,1}\} > h_1 = \min\{h_1, t_{1,1}\}$. Furthermore, for $\lambda \geqslant 2$, we have either

$$\min\{l_1, t_{1,\lambda}\} = l_1 > h_1 \geqslant \min\{h_1, t_{1,\lambda}\}$$

or

$$\min\{l_1, t_{1,\lambda}\} = t_{1,\lambda} \geqslant \min\{h_1, t_{1,\lambda}\}.$$

Hence

$$\min\{l_1, t_{1,\lambda}\} \geqslant \min\{h_1, t_{1,\lambda}\}$$

for $\lambda \in \{2, \ldots, s\}$, and note that

$$\min\{l_1, t_{1,1}\} > \min\{h_1, t_{1,1}\},$$

which contradicts (4.2). Therefore, we derive that $h_j \geqslant \min\{l_j, t_{j,1}\}$ for $j \in \{1, \ldots, k\}$. The result now holds immediately. □

The following theorem extends Theorem 3.2 of [1] to any finite abelian group.

**Theorem 4.5** *Let $H = C_{n_1} \times \cdots \times C_{n_s}$, where $C_{n_i}$ is a cyclic group with order $n_i \geqslant 2$ for $i \in \{1, \dots, s\}$, $s \geqslant 1$. Then $G(H, k_1) \cong G(H, k_2)$ if and only if the following two conditions are satisfied for $i \in \{1, \dots, s\}$.*

1. $\gcd(n_i, k_1) = \gcd(n_i, k_2)$.
2. There exists a positive integer $u_i$ such that $n_i = u_i v_i$, $u_i$ is the largest divisor of $n_i$ relatively prime to $k_1$ and is also the largest divisor of $n_i$ relatively prime to $k_2$. Moreover, for any $d \mid u_i$, $\mathrm{ord}_d k_1 = \mathrm{ord}_d k_2$.

**Proof** First, we prove the necessity of this theorem. Assume that $G(H, k_1) \cong G(H, k_2)$. By Lemma 2.2, the in-degree of $1$ in each $G(C_{n_i}, k_m)$ is equal to $\gcd(n_i, k_m)$, where $m = 1, 2$. Hence, in the digraph $G(H, k_m)$, the in-degree of $1$ is $\prod_{i=1}^{s} \gcd(n_i, k_m)$. Since $G(H, k_1) \cong G(H, k_2)$, we have

$$\prod_{i=1}^{s} \gcd(n_i, k_1) = \prod_{i=1}^{s} \gcd(n_i, k_2).$$

By Lemma 4.4, $\gcd(n_i, k_1) = \gcd(n_i, k_2)$ for $i \in \{1, \dots, s\}$. Thus the condition (1) holds and the first part of (2) follows from (1).

Now consider the remainder part of (2). Let $E_{i,m}$ denote the set of length of cycles in $G(C_{n_i}, k_m)$. By Proposition 4.2, $E_{i,m} = \{\mathrm{ord}_d k_m : \ d \mid u_i\}$, $m = 1, 2$. Further, let $M_m$ denote the set of length of cycles in $G(H, k_m)$. Then it is evident that

$$M_m = \left\{ \ \mathrm{lcm}[t_1, \dots, t_s] : \ t_i \in E_{i,m}, \ i \in \{1, \dots, s\} \ \right\}. \tag{4.3}$$

As the number of solutions in $C_{n_i}$ of the equation $g^k = 1$ is equal to $\gcd(n_i, k)$, the number of solutions in $H$ of the equation $g^k = 1$ is equal to $\prod_{i=1}^{s} \gcd(n_i, k)$. Similarly to Theorem 5.6 of [10], we obtain the number $A_t^{(m)}$ of $t$-cycles in $G(H, k_m)$:

$$A_t^{(m)} = \frac{1}{t} \left[ \prod_{i=1}^{s} \gcd(n_i, k_m^t - 1) - \sum_{\substack{d \mid t \\ d \neq t}} d A_d^{(m)} \right], \ m = 1, 2.$$

Since $G(H, k_1) \cong G(H, k_2)$, it is obvious that $M_1 = M_2$ and $A_t^{(1)} = A_t^{(2)}$ for $t \in M$. Let $M_1 = M_2 = M$. As $1 \in M$, we derive that

$$\prod_{i=1}^{s} \gcd(n_i, k_1 - 1) = \prod_{i=1}^{s} \gcd(n_i, k_2 - 1).$$

By induction on the length of cycles we have

$$\prod_{i=1}^{s} \gcd(n_i, k_1^t - 1) = \prod_{i=1}^{s} \gcd(n_i, k_2^t - 1)$$

for $t \in M$. Now if $d \mid u_i$, then $\gcd(d, k_m) = 1$ for $m = 1, 2$. Let $l_1 = \mathrm{ord}_d k_1$ and $l_2 = \mathrm{ord}_d k_2$. Then $l_1 \in E_{i,1}$ while $l_2 \in E_{i,2}$. Since each digraph $G(C_{n_i}, k_m)$ has cycles with length one, by (4.3), we see that $l_1, l_2 \in M$.

Therefore, we have

$$\prod_{i=1}^{s} \gcd(n_i, k_1^{l_1} - 1) = \prod_{i=1}^{s} \gcd(n_i, k_2^{l_1} - 1).$$

Note that $d \mid u_i$, $u_i \mid n_i$, and $d \mid (k_1^{l_1} - 1)$, clearly $d \mid \gcd(n_i, k_1^{l_1} - 1)$. By Lemma 4.4, $d \mid \gcd(n_i, k_2^{l_1} - 1)$. Thus $d \mid (k_2^{l_1} - 1)$, which implies that $l_2 \mid l_1$. Similarly, we derive that $l_1 \mid l_2$. Hence, $l_1 = l_2$, that is, $\mathrm{ord}_d k_1 = \mathrm{ord}_d k_2$ for $d \mid u_i$, establishing the necessity of this theorem.

Conversely, suppose the conditions (1) and (2) are satisfied. Note that $C_{n_i} \cong C_{u_i} \times C_{v_i}$, and then

$$G(H, k_m) \cong G(C_{u_1}, k_m) \times \cdots \times G(C_{u_s}, k_m) \times G(C_{v_1}, k_m) \times \cdots \times G(C_{v_s}, k_m)$$

for $m = 1, 2$. Since $\gcd(u_i, k_1) = \gcd(u_i, k_2) = 1$, by condition (2) and Proposition 4.2 (1), $G(C_{u_i}, k_1) \cong G(C_{u_i}, k_2)$. Further, it is clear that $\gcd(v_i, k_1) = \gcd(v_i, k_2)$ by condition (1), and $p \mid k_m$ for any prime factor $p$ of $v_i$, $m = 1, 2$. Therefore, by Proposition 4.3, $G(C_{v_i}, k_1) \cong G(C_{v_i}, k_2)$. Hence, by Lemma 3.1, we conclude that $G(H, k_1) \cong G(H, k_2)$, as desired. □

## References


[1] Deng G, Yuan P. Isomorphic digraphs from powers modulo $p$. Czech Math J 2011; 61: 771–779.

[2] Gilmer RW Jr. Finite rings having a cyclic multiplicative group of units. Am J Math 1963; 85: 447–452.

[3] Lucheta C, Miller E, Reiter C. Digraphs from powers modulo $p$. Fibonacci Quant 1996; 34: 226–239.

[4] Meemark Y, Wiroonsri N. The digraph of the $k$th power mapping of the quotient ring of polynomials over finite fields. Finite Fields Th Appl 2012; 18: 179–191.

[5] Raghavendran R. Finite associative rings. Compos Math 1969; 21: 195–229.

[6] Robert F. Discrete Iterations. Springer Series in Comput Math Vol 6. Berlin, Germany: Springer-Verlag, 1986.

[7] Rogers TD. The graph of the square mapping on the prime fields. Discrete Math 1996; 148: 317–324.

[8] Sha M. Digraphs from endomorphisms of finite cyclic groups. ArXiV 2010.

[9] Somer L, Křížek M. On semiregular digraphs of the congruence $x^k \equiv y \pmod{n}$. Comment Math Univ Carolin 2007; 48: 41–58.

[10] Somer L, Křížek M. On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math 2009; 309: 1999–2009.

[11] Somer L, Křížek M. The structure of digraphs associted with the congruence $x^k \equiv y \pmod{n}$. Czech Math J 2011; 61: 337–358.

[12] Szalay L. A discrete iteration in number theory. BDTF Tud Közl 1992; 8: 71–91 (in Hungarian).

[13] Wei YJ, Nan JZ, Tang GH. The cubic mapping graph for the ring of Gaussian integers modulo $n$. Czech Math J 2011; 61: 1023–1036.

[14] Wei YJ, Nan JZ, Tang GH. Structure of cubic mapping graph for the ring of Gaussian integers modulo $n$. Czech Math J 2012; 62: 527–539.

[15] Wei YJ, Tang GH, Su HD. The square mapping graphs of finite commutative rings. Algebr Colloq 2012; 19: 569–580.