Tengxia Ju; Meiyun Wu

On iteration digraph and zero-divisor graph of the ring $\mathbb{Z}_n$

Czechoslovak Mathematical Journal, Vol. 64 (2014), No. 3, 611–628

Persistent URL: `http://dml.cz/dmlcz/144048`

Czechoslovak Mathematical Journal, 64 (139) (2014), 611–628

ON ITERATION DIGRAPH AND ZERO-DIVISOR GRAPH OF THE RING $\mathbb{Z}_n$

Tengxia Ju, Meiyun Wu, Nantong

(Received February 4, 2013)

Abstract. In the first part, we assign to each positive integer n a digraph $\Gamma(n,5)$, whose set of vertices consists of elements of the ring $\mathbb{Z}_n=\{0,1,\dots,n-1\}$ with the addition and the multiplication operations modulo n, and for which there is a directed edge from a to b if and only if $a^5\equiv b \pmod n$. Associated with $\Gamma(n,5)$ are two disjoint subdigraphs: $\Gamma_1(n,5)$ and $\Gamma_2(n,5)$ whose union is $\Gamma(n,5)$. The vertices of $\Gamma_1(n,5)$ are coprime to n, and the vertices of $\Gamma_2(n,5)$ are not coprime to n. In this part, we study the structure of $\Gamma(n,5)$ in detail.

In the second part, we investigate the zero-divisor graph $G(\mathbb{Z}_n)$ of the ring $\mathbb{Z}_n$. Its vertex- and edge-connectivity are discussed.

Keywords: iteration digraph; zero-divisor graph; tree; cycle; vertex-connectivity

MSC 2010: 11A07, 05C20

1. Introduction

In this paper we consider the properties of iteration graphs associated with the map $x\to x^5$ over the ring $\mathbb{Z}_n$, extending the results given in the work [7] which provided an interesting connection between number theory, graph theory and group theory.

We recall that a *directed graph* is a finite set of vertices together with directed edges. The *iteration digraph* of a map $f\colon S\to S$ on a finite set S is a directed graph, whose vertices are elements of S and whose directed edges connect each $x\in S$ with its image $f(x)\in S$. The iteration graphs of the function $f(x)=x^k$ on the rings $S=\mathbb{Z}_n$ have interesting connections to number theory and have been extensively discussed (see [8]–[12]). These digraphs reflect the properties of $\mathbb{Z}_n$ and f. For each positive integer n, we denote such an iteration graph on the ring $\mathbb{Z}_n$ by $\Gamma(n,k)$.

The research has been supported by the NSFC Grant 11271208.

A *component* of the iteration digraph is a subdigraph which is a maximal connected subgraph of the associated nondirected graph. The *indegree* of a vertex a of $\Gamma(n,k)$, denoted by $\mathrm{indeg}_n(a)$, is the number of directed edges coming into a, and the *outdegree* of a is the number of directed edges leaving the vertex a. For simplicity, the subscript n will be omitted from now on. By the definition of f, the outdegree of each vertex of $\Gamma(n,k)$ is always equal to 1. It is well known that each component has exactly one cycle, i.e., the number of components of $\Gamma(n,k)$ is equal to the number of its cycles, since each vertex of the component has outdegree 1 and the component has only a finite number of vertices. Let us call a cycle of length 1 a *fixed point*, a cycle of length t a t-cycle, and a fixed point a an *isolated fixed point* if $\mathrm{indeg}(a) = \mathrm{outdeg}(a) = 1$. The cycles can be isolated or not isolated (see Figure 1).

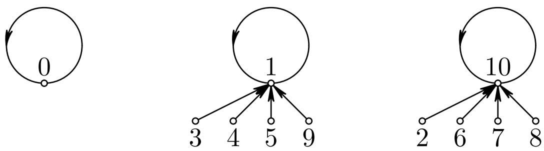

Figure 1. The digraph of $\Gamma(11,5)$.

A digraph is *regular* if the indegree of each vertex is equal to 1. Every component of such a regular digraph is a cycle. A digraph is *semiregular* if there exists a positive integer d such that each vertex has either indegree d or 0. A digraph is an m*-ary directed tree* with *root* r if $\mathrm{indeg}(r) = m$, every vertex adjacent to the root also has indegree m (has exactly m neighbours), similarly every vertex from all these m neighbours also has the indegree m and so on.

In this article, we study the iteration graph $\Gamma(n,5)$ for an arbitrary positive integer n. We can specify two subdigraphs of $\Gamma(n,5)$. Denote by $\Gamma_1(n,5)$ the subdigraph whose vertices are coprime to n and by $\Gamma_2(n,5)$ the subdigraph whose vertices are not coprime with n. It is easy to see that $\Gamma_1(n,5)$ and $\Gamma_2(n,5)$ are disjoint and $\Gamma(n,5) = \Gamma_1(n,5) \cup \Gamma_2(n,5)$. It is clear that the vertices of $\Gamma_1(n,5)$ form a group of order $\varphi(n)$ with respect to multiplication modulo n, where $\varphi(n)$ is the Euler function. We will need the following definition and results.

Definition 1.1 ([4]). Let n be a positive integer. The Carmichael λ-function $\lambda(n)$ is defined as follows:

$$\begin{aligned}
&\lambda(1) = 1 = \varphi(1), \quad \lambda(2) = 1 = \varphi(2), \quad \lambda(4) = 2 = \varphi(4),\\
&\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k) \quad \text{for } k \geqslant 3,\\
&\lambda(p^k) = (p-1)p^{k-1} = \varphi(p^k) \quad \text{for any odd prime } p \text{ and } k \geqslant 1,
\end{aligned}$$

$\lambda(p_1^{k_1}p_2^{k_2}\dots p_s^{k_s}) = [\lambda(p_1^{k_1}),\lambda(p_2^{k_2}),\dots,\lambda(p_s^{k_s})]$, where $p_1,p_2,\dots,p_s$ are distinct primes for $k_i \geqslant 1$, $i \in \{1,\dots,s\}$, and $[a_1,\dots,a_s]$ stands for the least common multiple of the numbers $a_1,\dots,a_s$.

From this definition, it follows that $\lambda(n) \mid \varphi(n)$ for all n and that $\lambda(n) = \varphi(n)$ if and only if $n \in \{1,2,4,q^k,2q^k\}$ where q is an odd prime and $k \geqslant 1$.

The following theorem generalizes the well-known Euler's theorem which says that $a^{\varphi(n)} \equiv 1 \pmod n$ if and only if $(a,n) = 1$. It shows that $\lambda(n)$ is the least possible order modulo n.

Theorem 1.1 (Carmichael's theorem, see [4] and [6]). *Let $a,n \in N$. Then $a^{\lambda(n)} \equiv 1 \pmod n$ if and only if $(a,n) = 1$. Moreover, there exists an integer g such that $\operatorname{ord}_n g = \lambda(n)$, where $\operatorname{ord}_n g$ denotes the multiplicative order of g modulo n.*

Theorem 1.2 ([10], [12]). *Let $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where $p_1 < p_2 < \dots < p_r$ are primes and $\alpha_i \geqslant 1$, and let a be a vertex of positive indegree in $\Gamma_1(n,k)$. Then*

$$\operatorname{indeg}(a) = \varepsilon\prod_{i=1}^{r}(\lambda(p_i^{\alpha_i}),k), \tag{1.1}$$

where $\varepsilon = 2$ if $2 \mid k$ and $8 \mid n$, and $\varepsilon = 1$ otherwise.

Theorem 1.3 ([10]). *Let $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where $p_1 < p_2 < \dots < p_r$ are primes and $\alpha_i \geqslant 1$, and let a be a vertex of positive indegree in $\Gamma_2(n,k)$. Suppose $a = Q\prod_{i=1}^{r} p_i^{\beta_i}$, where $(Q,n) = 1$, $\beta_i \geqslant 0$ for $1 \leqslant i \leqslant r$, and $\beta_i \geqslant 1$ for at least one value of i. Then for $1 \leqslant i \leqslant r$, either $\beta_i \geqslant \alpha_i$ or both $\beta_i < \alpha_i$ and $\beta_i = kt_i$ for some nonnegative integer t_i. Moreover,*

$$\operatorname{indeg}(a) = \prod_{i=1}^{r} A_iB_i, \tag{1.2}$$

where

$$\mathrm{A_i} = \begin{cases} p_i^{\alpha_i - \lceil \alpha_i/k \rceil}, & \text{if } \beta_i \geqslant \alpha_i, \\ p_i^{(k-1)t_i}, & \text{if } 0 \leqslant \beta_i < \alpha_i, \end{cases} \tag{1.3}$$

the symbol $\lceil a \rceil$ means the smallest natural number greater than or equal to a, and

$$B_i = \varepsilon_i(\lambda(p_i^{\alpha_i - \min(\alpha_i - \beta_i)}),k),$$

where $\varepsilon_i = 2$ if $p_i = 2$, $2 \mid k$ and $\alpha_i - \beta_i \geqslant 3$, otherwise, $\varepsilon_i = 1$.

2. Structure of the digraph $\Gamma(n,5)$ of congruence $x^5 \equiv y \pmod n$

The following results are generalizations of work [7] by Skowronek-Kaziów.

Proposition 2.1. *Let $k, l \in \{1, \ldots, n-1\}$. Then*

(1) *the number k is mapped into 0 (or into $n/2$ for an even n) if and only if $n-k$ is mapped into 0 (or into $n/2$ for an even n);*

(2) *the number k is mapped into l if and only if $n-k$ is mapped into $n-l$;*

(3) *the number k is an isolated fixed point if and only if $n-k$ is an isolated fixed point;*

(4) *the number k is a part of a t-cycle if and only if $n-k$ is an element of some t-cycle. Moreover, the isolation of one of these t-cycles implies the isolation of the other.*

Lemma 2.2. *The numbers $0, 1$ and $n-1$ are fixed points of $\Gamma(n,5)$. Moreover, 0 is an isolated fixed point of $\Gamma(n,5)$ if and only if n is square-free.*

P r o o f. It is clear that

$$0^5 \equiv 0 \pmod n, \quad 1^5 \equiv 1 \pmod n, \quad (n-1)^5 \equiv n-1 \pmod n.$$

Now, if n is not square-free then $p^2 \mid n$ for some prime p and

$$\left(\frac{n}{p}\right)^5 = n \cdot n \cdot \frac{n}{p} \cdot \frac{n}{p^2} \cdot \frac{n}{p^2} \equiv 0 \pmod n.$$

Hence, n/p is mapped into 0 and 0 is not an isolated fixed point. Conversely, if n is square-free, then there does not exist k, $2 \leqslant k \leqslant n-2$, such that $n \mid k^5$, thus 0 is isolated. $\square$

Lemma 2.3. (1) *The number of quintic roots (if they exist) of any quintic residue in $\Gamma_1(n,5)$ is equal to the number of quintic roots of 1 modulo n, i.e., each vertex of digraph $\Gamma_1(n,5)$ has the same positive indegree d or 0.*

(2) *Let $\omega_0(n)$ be the number of distinct primes dividing n which are congruent to 1 modulo 5. Then the number of quintic roots of 1 modulo n is $5^{\omega(n)}$, where*

$$\omega(n) = \begin{cases} \omega_0(n) + 1, & 5^2 \mid n, \\ \omega_0(n), & 5^2 \nmid n. \end{cases} \tag{2.1}$$

P r o o f. We can prove it directly by the formula for the indegree (see Theorem 1.2), but, here, we prove it by the methods of number theory. The proof of (1) is obvious. Assume $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, where $p_1 < p_2 < \dots p_r$ are primes and $\alpha_i \geqslant 1$. Since

$$x^5 \equiv 1 \pmod n \Leftrightarrow \begin{cases} x^5 \equiv 1 \pmod{p_1^{\alpha_1}}, \\ \quad\vdots \\ x^5 \equiv 1 \pmod{p_r^{\alpha_r}}, \end{cases} \tag{2.2}$$

we only need to consider the number of solutions of $x^5 \equiv 1 \pmod{p^\alpha}$. The trivial solution of this congruence is 1. Suppose $1 \neq a$ is a nontrivial solution of $x^5 \equiv 1 \pmod n$; we note that

$$a^5 \equiv 1 \pmod{p^\alpha} \Rightarrow a^5 \equiv 1 \pmod p,$$

thus $(a, p) = 1$ and $\mathrm{ord}_p a = 5$. We note that $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1$, thus $5 \mid (p - 1)$. Hence there exists a nontrivial solution of $x^5 \equiv 1 \pmod p$ if and only if $p \equiv 1 \pmod 5$.

If $p \equiv 1 \pmod 5$, then there exist five solutions of $x^5 \equiv 1 \pmod p$, and also for $x^5 \equiv 1 \pmod{p^\alpha}$, where $\alpha > 1$. If $p = 5$, then there exists exactly one solution $x = 1$ of $x^5 \equiv 1 \pmod 5$, but the number of solutions of $x^5 \equiv 1 \pmod{5^\alpha}$ is 5, provided $\alpha > 1$. As for other primes p, there exists exactly one solution $x = 1$ of $x^5 \equiv 1 \pmod{p^\alpha}$, provided $\alpha \geqslant 1$. The result now follows, since the function

$$\varrho_f(n) = |\{0 \leqslant m \leqslant n - 1\colon\ f(m) \equiv 0 \pmod n\}|$$

is multiplicative (see [5]). □

Corollary 2.4. *The digraph $\Gamma_1(n, 5)$ is always semiregular, and every vertex of $\Gamma_1(n, 5)$ has indegree either $5^{\omega(n)}$ or 0. Moreover, the digraph $\Gamma_1(n, 5)$ is regular (each vertex of $\Gamma_1(n, 5)$ has indegree 1, i.e., each component of $\Gamma_1(n, 5)$ is a cycle) if and only if $5 \nmid \varphi(n)$.*

P r o o f. If $5 \nmid \varphi(n)$, then $(5, \varphi(n)) = 1$, thus there exist two integers s, t such that $5s + \varphi(n)t = 1$. We therefore have

$$a = a^1 = a^{5s+\varphi(n)t} = a^{5s} a^{\varphi(n)t} \equiv (a^s)^5 \pmod n,$$

which means that there exists a solution of $x^5 \equiv a \pmod n$. Then by Lemma 2.3(2) or Theorem 1.2, the number of solutions of $x^5 \equiv a \pmod n$ is exactly one, i.e., for each vertex $a \in \Gamma_1(n, 5)$, $\mathrm{indeg}(a) = 1$, hence $\Gamma_1(n)$ is regular.

If $5 \mid \varphi(n)$, then $5^2 \mid n$ or there exists a prime $p \equiv 1 \pmod 5$ such that $p \mid n$, thus by Lemma 2.3 it follows that $\mathrm{indeg}(a) = 0,$ or $5^{\omega(n)} (> 1)$, i.e., $\Gamma_1(n, 5)$ is semiregular, but not regular. □

Lemma 2.5. *Every component of the digraph $\Gamma(n,5)$ is a cycle if and only if $5 \nmid \varphi(n)$ and n is square-free.*

P r o o f. If every component of the digraph $\Gamma(n,5)$ is a cycle, then $\Gamma(n,5)$ is regular. It is obvious that $\Gamma_1(n,5)$ is regular and $\operatorname{indeg}(0)=1$. Then by Lemma 2.2 and Corollary 2.4, $5 \nmid \varphi(n)$ and n is square-free.

Conversely, assume n is square-free and $5 \nmid \varphi(n)$. By Corollary 2.4, $\Gamma_1(n,5)$ is regular. We only need to verify that the digraph of $\Gamma_2(n,5)$ is regular.

Let $a \neq 0$ be an arbitrary vertex of $\Gamma_2(n,5)$. Then $d=(a,n)>1$ and $n=d\cdot n/d$. Next, suppose $p \mid n$, thus $p \mid d$ or $p \mid n/d$.

If $p \mid d$ for some prime $p \geqslant 2$, then the solution b of the congruence $b^5 \equiv a \pmod n$ satisfies $b \equiv 0 \pmod p$ for all primes $p \mid d$. Hence, $b^5 \equiv a \equiv 0 \pmod p$ for each prime p dividing d. The solution b is unique by Lemma 2.2.

If $p \nmid d$, then $p \mid (n/d)$, and $p \nmid a$. Since $5 \nmid \varphi(n)$, $5 \nmid \varphi(p)=p-1$, it follows that there exists x such that $5x \equiv 1 \pmod{p-1}$. Set $b \equiv a^x \pmod p$, then $b^5 \equiv a^{5x} \equiv a \pmod p$ by Fermat's little theorem. If there exists another c such that $c^5 \equiv a \pmod p$, then $(bc^{-1})^5 \equiv 1 \pmod p$, i.e., order ${}_p(bc^{-1})=1$ or 5. Since $\mathbb{Z}_p\setminus\{0\}$ is a cyclic group of order $p-1$ and $5 \nmid p-1$, it follows that $bc^{-1} \equiv 1 \pmod p$, i.e., $b \equiv c \pmod p$ and the solution b is unique.

Hence, by the Chinese remainder theorem, the solution of $x^5 \equiv a \pmod n$ is unique, i.e., $\operatorname{indeg}(a)=1$ for each vertex $a \in \Gamma_2(n,5)$, thus $\Gamma_2(n,5)$ is regular. $\square$

We give a formula for the number of fixed points of the digraph $\Gamma(n,5)$.

Theorem 2.6. *Let $n=2^m p_1^{\alpha_1} p_2^{\alpha_2}\dots p_s^{\alpha_s}$ be the prime power factorization of n, where $p_1<p_2<\dots<p_s$ are distinct, odd primes, $\alpha_i \geqslant 1, m \geqslant 0$ and $s \geqslant 0$. Denote by $\omega(n)$ the number of distinct odd prime divisors p_i of n satisfying $p_i \equiv 1 \pmod 4$. Then the number $L(n)$ of fixed points of $\Gamma(n,5)$ is equal to*

$$L(n)=\begin{cases} 3^{s-\omega(n)}\cdot 5^{\omega(n)} & \text{if } m=0,\\ 2\cdot 3^{s-\omega(n)}\cdot 5^{\omega(n)} & \text{if } m=1,\\ 3\cdot 3^{s-\omega(n)}\cdot 5^{\omega(n)} & \text{if } m=2,\\ 5\cdot 3^{s-\omega(n)}\cdot 5^{\omega(n)} & \text{if } m=3,\\ 9\cdot 3^{s-\omega(n)}\cdot 5^{\omega(n)} & \text{if } m\geqslant 4.\end{cases} \tag{2.3}$$

P r o o f. It is clear that a is a fixed point of $\Gamma(n,5)$ if and only if a is the zero of the polynomial $f(x) \equiv x^5-x \pmod n$. We denote

$$\varrho_f(n)=|\{0 \leqslant m \leqslant n-1\colon\ f(m) \equiv 0 \pmod n\}|,$$

i.e., $\varrho_f(n)$ is the number of solutions of $f(x) \equiv 0 \pmod{n}$. It is easy to see that $\varrho_f(2) = 2$, $\varrho_f(2^2) = 3$, and $\varrho_f(2^3) = 5$. If $m \geqslant 4$, then $\varrho_f(2^m) = 9$. In fact, for $n = 2^m$, $m \geqslant 3$, $x^5 \equiv x \pmod{2^m}$ is equivalent to $x^5 - x = x(x^4 - 1) \equiv 0 \pmod{2^m}$, the trivial solution being $x = 0$. Next we consider the nontrivial solution $0 < x < 2^m - 1$. The parities of x and $x^4 - 1$ are opposite. Then either $2^m \mid x$ or $2^m \mid (x^4 - 1)$. But $0 < x < 2^m - 1$, $2^m \nmid x$, and the solution x must satisfy $2^m \mid (x^4 - 1)$, which means that $x^4 \equiv 1 \pmod{2^m}$. Suppose $y = x^2$ while $y^2 \equiv 1 \pmod{2^m}$ has four solutions $\{1, 2^{m-1}-1, 2^{m-1}+1, 2^m-1\}$. We only need to consider the solutions of

$$x^2 \equiv 1 \pmod{2^m}; \quad x^2 \equiv 2^{m-1} - 1 \pmod{2^m};$$
$$x^2 \equiv 2^{m-1} + 1 \pmod{2^m}; \quad x^2 \equiv 2^m - 1 \pmod{2^m},$$

respectively.

When $m \geqslant 3$, neither $x^2 \equiv 2^{m-1} - 1 \pmod{2^m}$ nor $x^2 \equiv 2^m - 1 \pmod{2^m}$ has a solution. As for the other two congruences, $x^2 \equiv 1 \pmod{2^m}$ $(m \geqslant 3)$ has four solutions and $x^2 \equiv 2^{m-1}+1 \pmod{2^m}$ $(m \geqslant 4)$ has four solutions by number theory. Hence, $\varrho_f(2^m) = 9$, where $m \geqslant 4$. Then

$$\varrho_f(2^m) = \begin{cases} 2 & \text{if } m = 1, \\ 3 & \text{if } m = 2, \\ 5 & \text{if } m = 3, \\ 9 & \text{if } m \geqslant 4. \end{cases} \tag{2.4}$$

Now set $n = p^\alpha$, where $p \geqslant 3$ is an odd prime and $\alpha \geqslant 1$. We note that $x^5 - x \equiv 0 \pmod{p^\alpha} \Rightarrow x^5 - x \equiv 0 \pmod{p}$, i.e., $p \mid x(x^2 - 1)(x^2 + 1)$. Suppose x is a solution of $x^5 - x \equiv 0 \pmod{p^\alpha}$. We can investigate it in the following three cases. If $p \mid x$, then $(p, x^2 - 1) = (p, x^2 + 1) = 1$, thus $x \equiv 0 \pmod{p^\alpha}$. If $p \mid (x^2 - 1)$, then $(p, x) = 1$ and $(p, x^2 + 1) = 1$, which means that in this case, $x^5 \equiv x \pmod{p^\alpha} \Rightarrow x^2 - 1 \equiv 0 \pmod{p^\alpha}$, the latter congruence having two solutions. If $p \mid (x^2 + 1)$, then $(p, x) = 1$ and $(p, x^2 - 1) = 1$, which means that in this case, $x^5 \equiv x \pmod{p^\alpha} \Rightarrow x^2 \equiv -1 \pmod{p^\alpha}$. It is well known that the latter congruence has solutions if and only if $p \equiv 1 \pmod{4}$, and if it has solutions, it has exactly two solutions. Then

$$\varrho_f(p^\alpha) = \begin{cases} 3 & \text{if } p \equiv 3 \pmod{4}, \\ 5 & \text{if } p \equiv 1 \pmod{4}. \end{cases} \tag{2.5}$$

The function $\varrho_f(n)$ is a multiplicative function, which completes the proof. $\square$

Theorem 2.7. *Let $n > 2$. Then there exists a cycle of length t in the digraph $\Gamma(n, 5)$ if and only if $t = \mathrm{ord}_d 5$ for some even, positive divisor d of $\lambda(n)$.*

P r o o f. Suppose that a is a vertex of a t-cycle in $\Gamma(n)$. Then t is the least positive integer satisfying $a^{5^t} \equiv a \pmod{n}$, i.e., t is the least positive integer such that

$$a^{5^t} - a \equiv a(a^{5^t-1} - 1) \equiv 0 \pmod{n}.$$

Set $n_1 = (a, n)$, and $n_2 = n/n_1$. It follows that t is the least positive integer such that $a \equiv 0 \pmod{n_1}$, $a^{5^t-1} \equiv 1 \pmod{n_2}$ and $(n_1, n_2) = 1$, since $(a, a^{5^t-1} - 1) = 1$. Then, by the Chinese remainder theorem, there exists an integer b such that $b \equiv 1 \pmod{n_1}$, $b \equiv a \pmod{n_2}$.

Hence, t is the least positive integer such that $b^{5^t-1} \equiv 1 \pmod{n_1}$, $b^{5^t-1} \equiv a^{5^t-1} \equiv 1 \pmod{n_2}$, which means that $b^{5^t-1} \equiv 1 \pmod{n}$. Set $c = \mathrm{ord}_n b$. Then $5^t \equiv 1 \pmod{c}$. If c is odd then since $5^t \equiv 1 \pmod{2}$, we get that t is the least positive integer such that $5^t \equiv 1 \pmod{2c}$.

Let

$$d = \begin{cases} 2c & \text{if } c \text{ is odd,} \\ c & \text{if } c \text{ is even.} \end{cases} \tag{2.6}$$

Then $t = \mathrm{ord}_d 5$, and by Carmichael's theorem, $d \mid \lambda(n)$. Conversely, suppose that d is an even positive divisor of $\lambda(n)$ and let $t = \mathrm{ord}_d 5$. By Carmichael's theorem, there exists a residue g modulo n such that $\mathrm{ord}_n g = \lambda(n)$. Let $h = g^{\lambda(n)/d}$. Then $\mathrm{ord}_n h = d$. Since $d \mid (5^t - 1)$ but $d \nmid (5^k - 1)$ for $1 \leqslant k < t$, we see that t is the least positive integer such that $h^{5^t-1} \equiv 1 \pmod{n}$, and $h \cdot h^{5^t-1} = h^{5^t} \equiv h \pmod{n}$. Thus, h is a vertex of a t-cycle of $\Gamma(n, 5)$. $\square$

Theorem 2.8. *The number of components of $\Gamma(n, 5)$ is 2 if and only if $n = 2$.*

Theorem 2.9. *The number of components of $\Gamma(n, 5)$ is 3 if and only if $n = 4$ or n is a prime of the form $n = 2 \cdot 5^k + 1$, for some integer $k \geqslant 0$.*

P r o o f. If $\Gamma(n, 5)$ has exactly 3 components, then there exist 3 fixed points at most, and by Theorem 2.6, either $n = 4$ or n is the power of some odd prime number p for which $p \equiv 3 \pmod{4}$. Of course, there is no t-cycle for $t > 1$, otherwise, there are more than 3 components of $\Gamma(n, 5)$. Hence, by Theorem 2.7, $d \nmid 5^t - 1$ for every $t > 1$ and every even divisor $d > 2$ (if such d exists) of the Carmichael λ-function $\lambda(n)$. Therefore, $5 \mid d$ and $\lambda(n) = 2 \cdot 5^l$ for some natural number l. Finally, n must be 4 or a prime number of the form $n = 2 \cdot 5^k + 1$, $k \geqslant 0$.

Conversely, if $n = 4$, then we have exactly 3 components. If n is a prime of the form $n = 2 \cdot 5^k + 1$, then we have exactly 3 fixed points by Theorem 2.6, and

$\lambda(n) = 2 \cdot 5^k$. If we have more than 3 components, then there exists a cycle of length $t > 1$ and $t = \mathrm{ord}_d 5$ for some even positive divisor d of $\lambda(n)$. Then t is the least positive number such that $5^t \equiv 1 \pmod d$ and $d \mid (5^t - 1)$. Since also $d \mid \lambda(n) = 2 \cdot 5^k$, we get $d = 2$. Then $t = \mathrm{ord}_d 5 = \mathrm{ord}_2 5 = 1$, which is a contradiction. Hence, the only cycles of $\Gamma(n, 5)$ are the fixed points at 0, 1 and at $n - 1$. $\square$

Example 2.1. For $n = 3, 4$ or 11 (see Figures 2, 3 and Figure 1), the digraph $\Gamma(n, 5)$ has three components.

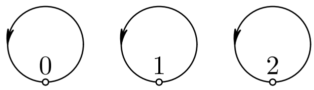

Figure 2. The digraph of $\Gamma(3, 5)$.

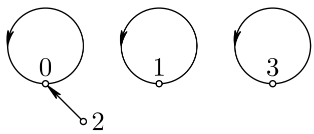

Figure 3. The digraph of $\Gamma(4, 5)$.

Theorem 2.10. *The number of components of* $\Gamma(n, 5)$ *is* 5 *if* $n = 8$ *or* $n = 5^k$, $k \geqslant 1$.

Proof. Of course, $\Gamma(8, 5)$ has exactly 5 components. If $n = 5^k$, $k \geqslant 1$, clearly, there is no t-cycle for $t > 1$ by Theorem 2.7. Hence, by Theorem 2.6, $\Gamma(5^k, 5)$ has exactly 5 fixed points. Therefore $\Gamma(5^k, 5)$ has 5 components. $\square$

Example 2.2. For $n = 8$, or 25, the digraph $\Gamma(n, 5)$ has 5 components (see Figures 4 and 5).

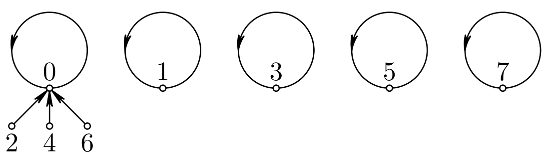

Figure 4. The digraph of $\Gamma(8, 5)$.

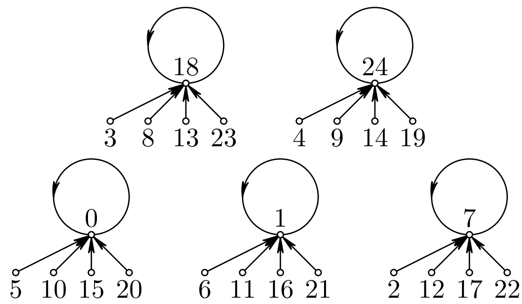

Figure 5. The digraph of $\Gamma(25,5)$.

Question 2.1. If $\Gamma(n,5)$ has 5 components for $n = p^k$, $k \geqslant 1$, where $p \equiv 3 \pmod 4$ is an odd prime, then there exist exactly 3 fixed points. Of course, there must exist exactly two cycles of length bigger than 1. In this case, what is the necessity for n in order that $\Gamma(n,5)$ have 5 components?

Example 2.3. For $n = 7$ or 9, the digraph $\Gamma(n,5)$ has 5 components. However, when $n = 19$, the digraph $\Gamma(n,5)$ has 7 components (see Figures 6, 7 and 8).

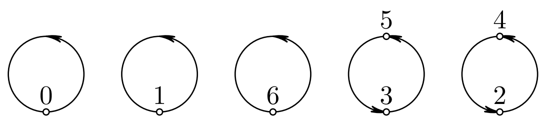

Figure 6. The digraph of $\Gamma(7,5)$.

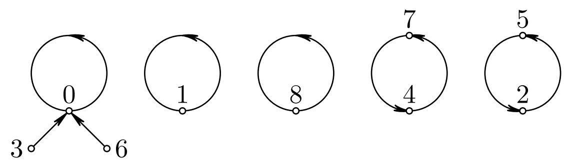

Figure 7. The digraph of $\Gamma(9,5)$.

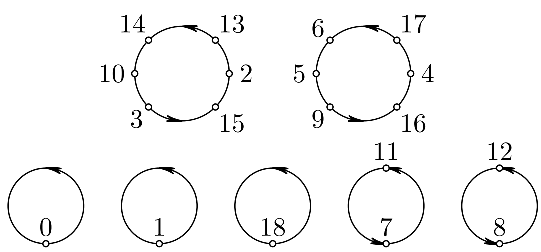

Figure 8. The digraph of $\Gamma(19,5)$.

Next we consider three kinds of digraphs $\Gamma(2^k, 5)$, $\Gamma(3^k, 5)$, and $\Gamma(5^k, 5)$.

Theorem 2.11. *Let $k \geqslant 5$ be a natural number. The digraph $\Gamma_1(2^k, 5)$ contains (except for 8 fixed points) only cycles of lengths which are powers of 2 and $\Gamma_2(2^k, 5)$ is a tree with the root 0. Moreover,* $\operatorname{indeg}(0) = 2^{k-\lceil k/5 \rceil}$*, where $\lceil a \rceil$ is the smallest natural number greater than or equal to a.*

Proof. If $n = 2^k$, then each of the digraphs $\Gamma_1(n, 5)$ and $\Gamma_2(n, 5)$ contains exactly $\varphi(n) = 2^{k-1}$ vertices. Of course $5 \nmid \varphi(n)$ and hence, $\Gamma_1(2^k, 5)$ contains only cycles by Corollary 2.4. It is easy to check that there exist exactly 8 fixed points in $\Gamma_1(2^k, 5)$, namely $1, 2^{k-1}-1, 2^{k-1}+1, 2^k-1, 2^{k-2}+1, 2^k-2^{k-2}-1, 2^{k-2}-1$, and $2^k-2^{k-2}+1$. We know that there exists a cycle of length t if and only if $t = \operatorname{ord}_d 5$ for some divisor d of $\lambda(n) = 2^{k-2.}$ Then $5^t \equiv 1 \pmod{d}$. Noting that $d \mid \lambda(n) \mid \varphi(n)$ and $5 \nmid \varphi(n)$, it follows that $(5, d) = 1$ and $5^{\lambda(d)} \equiv 1 \pmod{d}$ by Theorem 1.1. Therefore, $t \mid \lambda(d)$. Hence, t is a power of 2. It is easy to see that we have $2^{k-\lceil k/5 \rceil}$ elements in $\Gamma_2(2^k, 5)$, namely $2^{\lceil k/5 \rceil}, 2 \cdot 2^{\lceil k/5 \rceil}, 3 \cdot 2^{\lceil k/5 \rceil}, \ldots, 2^{k-\lceil k/5 \rceil} \cdot 2^{\lceil k/5 \rceil} = 0$ which are mapped into 0. Of course, all vertices w of $\Gamma_2(2^k, 5)$ are multiples of 2 and the greater the power of 2 which is a divisor of w, the shorter the directed path from w to 0. $\square$

The digraph $\Gamma_1(2^4, 5)$ contains 8 isolated fixed points, and $\Gamma_2(2^4, 5)$ is a directed tree with the root 0 (see Figure 9). The digraph $\Gamma_1(2^5, 5)$ contains 8 isolated fixed points and 4 cycles of length 2, and $\Gamma_2(2^5, 5)$ is a directed tree with the root 0.

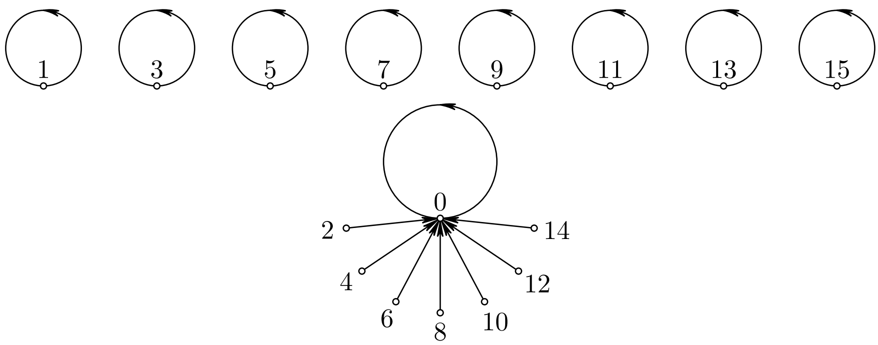

Figure 9. The digraph of $\Gamma(16, 5)$.

The digraph $\Gamma_1(3^2, 7)$ contains 2 fixed points and 2 cycles of length 2, and $\Gamma_2(3^2, 5)$ is a directed tree with the root 0 (see Figure 7).

The digraph $\Gamma_1(3^3, 5)$ contains 2 fixed points, 2 cycles of length 2, and 2 cycles of length 6, and $\Gamma_2(3^3, 5)$ is a directed tree with the root 0 (see Figure 10).

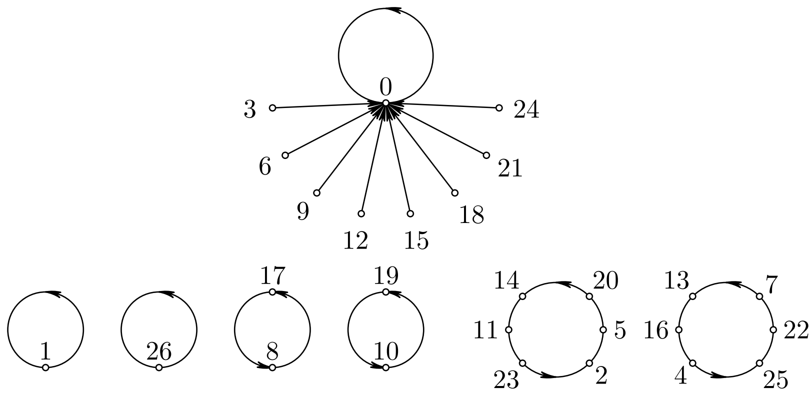

Figure 10. The digraph of $\Gamma(27, 5)$.

Then we can conjecture as follows:

Theorem 2.12. *Let $k \geqslant 2$ be a natural number. The digraph $\Gamma_1(3^k, 5)$ consists of 2 fixed points, 2 cycles of length 2, 6, 18, 54, …, $2 \cdot 3^{k-2}$, respectively. Moreover, $\Gamma_2(3^k, 5)$ is a tree with the root 0 and $\operatorname{indeg}(0) = 3^{k-\lceil k/5 \rceil}$. Suppose $a = 3^q b \in \Gamma_2(3^k, 5)$, where $(b, 3) = 1$, and $1 \leqslant q < k$. Then the height of the vertex a from the root 0 is $h = \lceil \log_5 k/q \rceil$.*

In the process of trying to prove Theorem 2.12, we find the interesting fact that 5 is a primitive root mod 3^k for all positive integers k.

Lemma 2.13. *If $3^{k+1} \mid (5^{3^{k-1}} + 1)$ for some positive integer $k \geqslant 2$, then $3^k \mid (5^{3^{k-2}} + 1)$.*

Proof. Suppose $5^{3^{k-2}} \equiv a \pmod{3^k}$, then there exists an integer such that $5^{3^{k-2}} = 3^k l + a$. It follows that $5^{3^{k-1}} = 5^{3^{k-2} \cdot 3} + 1 = (3^k l + a)^3 + 1 \equiv a^3 + 1 \pmod{3^{k+1}}$, which means that $a^3 + 1 = (a+1)(a^2 - a + 1) \equiv 0 \pmod{3^{k+1}}$. We note that

$$a^2 - a + 1 \equiv \begin{cases} 1 & \text{if } a \equiv 0,\ 1 \pmod 3, \\ 0 & \text{if } a \equiv 2 \pmod 3, \end{cases} \tag{2.7}$$

and

$$a^2 - a + 1 \equiv \begin{cases} 1 & \text{if } a \equiv 0, 1 \pmod 9, \\ 3 & \text{if } a \equiv 2, 5, 8 \pmod 9, \\ 4 & \text{if } a \equiv 4, 6 \pmod 9, \\ 7 & \text{if } a \equiv 3, 7 \pmod 9, \end{cases} \tag{2.8}$$

hence $9 \nmid (a^2 - a + 1)$. Of course, $3^k \mid (a + 1)$, hence $5^{3^{k-2}} + 1 = 3^k l + a + 1 \equiv 0 \pmod{3^k}$. $\square$

Proposition 2.14. *5 is a primitive root mod 3^k for all positive integers k.*

P r o o f. It is easy to see that 5 is a primitive root mod 3, and also a primitive root mod 9. Next suppose 5 is a primitive root mod 3^k, i.e., $\operatorname{ord}_{3^k}5 = \varphi(3^k) = 2\cdot 3^{k-1}$. We only need to show that 5 is a primitive root mod 3^{k+1} by induction. Set $\lambda = \operatorname{ord}_{3^{k+1}}5$. Then λ is the smallest positive integer such that $5^\lambda \equiv 1 \pmod{3^{k+1}}$. We also know $\lambda \mid \varphi(3^{k+1})$ by the group theory. It follows that $2\cdot 3^{k-1} \mid \lambda \mid 2\cdot 3^k$, since $5^\lambda \equiv 1 \pmod{3^k}$, 5 is a primitive root mod 3^k, and $\varphi(3^{k+1}) = 2\cdot 3^k$. Hence, $\lambda = 2\cdot 3^{k-1}$ or $2\cdot 3^k$. If $\lambda = 2\cdot 3^{k-1}$, then $5^{2\cdot 3^{k-1}} \equiv 1 \pmod{3^{k+1}}$, i.e., $(5^{3^{k-1}}-1)(5^{3^{k-1}}+1) \equiv 0 \pmod{3^{k+1}}$. We know that $5^{3^{k-1}} - 1 \equiv -2 \pmod 3$, which means that $3 \nmid (5^{3^{k-1}}-1)$, so $3^{k+1} \mid (5^{3^{k-1}}+1)$. Therefore, by Lemma 2.14, $3^k \mid 5^{3^{k-2}}+1$, i.e., $5^{2\cdot 3^{k-2}} - 1 \equiv 0 \pmod{3^k}$, which is a contradiction. $\square$

We draw the following general conclusion:

Proposition 2.15. *Let $p \neq 5$ be an odd prime. If 5 is a primitive root mod p, where p is an odd prime, then 5 is a primitive root mod p^k for all positive integers k.*

P r o o f. We first show that if $p^{k+1} \mid (5^{(p-1)/2\cdot p^{k-1}}+1)$ for some positive integer $k \geqslant 2$, then $p^k \mid (5^{(p-1)/2\cdot p^{k-2}}+1)$. Suppose $5^{(p-1)/2\cdot p^{k-2}} \equiv a \pmod{p^k}$, then $5^{(p-1)/2\cdot p^{k-2}} = p^k l + a$. It follows that $5^{(p-1)/2\cdot p^{k-1}} + 1 = (p^k l + a)^p + 1 \equiv a^p + 1 \equiv 0 \pmod{p^{k+1}}$. By Fermat's little theorem, $a^p \equiv a \pmod p$. Then $(a+1)(a^{p-1} - a^{p-2} + \ldots + a^2 - a + 1) = a^p + 1 \equiv a + 1 \pmod p$. If $a + 1 \not\equiv 0 \pmod p$, then $a^{p-1} - a^{p-2} + \ldots + a^2 - a + 1 \equiv 1 \pmod p$, since $a+1$ is invertible in the multiplicative group $\mathbb{Z}_p^*$. We have

$$a^{p-1} - a^{p-2} + \ldots + a^2 - a + 1 \equiv \begin{cases} 1 & \text{if } a \not\equiv -1 \pmod p, \\ 0 & \text{if } a \equiv -1 \pmod p. \end{cases} \tag{2.9}$$

In the case $a \equiv -1 \pmod p$, i.e., $a = pt - 1$ for some integer t, one has

$$a^{p-1} - a^{p-2} + \ldots + a^2 - a + 1 = \frac{a^p+1}{a+1} = \frac{(pt-1)^p+1}{pt} \equiv p \pmod{p^2}, \tag{2.10}$$

thus $p^2 \nmid (a^{p-1} - a^{p-2} + \ldots + a^2 - a + 1)$. Clearly $a+1$ must be divisible by p^k. Then $5^{(p-1)/2\cdot p^{k-2}} + 1 = p^k l + a + 1 \equiv 0 \pmod{p^k}$. Finally, we show that if 5 is a primitive root mod p, then 5 also is a primitive root mod p^k. We prove this by induction. Suppose 5 is a primitive root mod p^k, i.e., $\operatorname{ord}_{p^k}5 = \varphi(p^k) = (p-1)\cdot p^{k-1}$. Set $\lambda = \operatorname{ord}_{p^{k+1}}5$. Then λ is the smallest positive integer such that $5^\lambda \equiv 1 \pmod{p^{k+1}}$. It follows that $(p-1)\cdot p^{k-1} \mid \lambda \mid (p-1)\cdot p^k$, since $5^\lambda \equiv 1 \pmod{p^k}$, 5 is a primitive root mod p^k, and $\varphi(p^{k+1}) = (p-1)\cdot p^k$. Hence, $\lambda = (p-1)\cdot p^{k-1}$ or $(p-1)\cdot p^k$. If $\lambda = (p-1)\cdot p^{k-1}$, then $5^{(p-1)\cdot p^{k-1}} \equiv 1 \pmod{p^{k+1}}$, and moreover,

$(5^{(p-1)/2\cdot p^{k-1}}-1)(5^{(p-1)/2\cdot p^{k-1}}+1)\equiv 0 \pmod{p^{k+1}}$. But $5^{(p-1)/2\cdot p^{k-1}}-1\equiv -2 \pmod p$, since 5 is a primitive root mod p. Thus $p\nmid (5^{(p-1)/2\cdot p^{k-1}}-1)$, which implies that $p^{k+1}\mid (5^{(p-1)/2\cdot p^{k-1}}+1)$. By the previous discussion, $p^k\mid (5^{(p-1)/2\cdot p^{k-2}}+1)$. Thus, $5^{(p-1)\cdot p^{k-2}}-1\equiv 0 \pmod{p^k}$, which is a contradiction. This completes the proof. $\square$

Proof of Theorem 2.12. Suppose d is an even divisor of $\lambda(3^k)=2\cdot 3^{k-1}$, then $d=2$ or $2\cdot 3^m$, where $1\leqslant m\leqslant k-1$. We only need to compute the value of $\operatorname{ord}_d 5$ by Theorem 2.7. Let $t=\operatorname{ord}_{2\cdot 3^m}5$, i,e., t is the least positive integer such that

$$\begin{cases} 5^t\equiv 1 \pmod 2,\\ 5^t\equiv 1 \pmod{3^m}. \end{cases} \tag{2.11}$$

Since $5^t\equiv 1 \pmod 2$ holds for each positive integer t, it follows that $t=\varphi(3^m)=2\cdot 3^{m-1}$ by Proposition 2.14. Thus, by Proposition 2.1 and Theorem 2.7, the digraph $\Gamma_1(3^k,5)$ contains 2 fixed points, 2 cycles of length 2, 6, 18, 54, $\ldots$, $2\cdot 3^{k-2}$, respectively. Finally, suppose $a=3^q b\in\Gamma_2(3^k,5)$, where $(b,3)=1$. Then the height of a from the root 0 is the least integer h such that $a^{5^h}\equiv 0 \pmod{3^k}$. Since $a^{5^h}\equiv 3^{q\cdot 5^h}b^{5^h}\equiv 0 \pmod{3^k}$ and $(b,3)=1$, we have $3^{q\cdot 5^h}\equiv 0 \pmod{3^k}$. Then $h=\lceil\log_5 k/q\rceil$. $\square$

Theorem 2.16. *Let $k\geqslant 2$ be a natural number. The digraph $\Gamma_1(5^k,5)$ consists of four isomorphic quinary trees with roots 1, 5^k-1, and two other fixed points. Moreover, $\Gamma_2(5^k,5)$ is a tree with the root 0 and $\operatorname{indeg}(0)=5^{k-\lceil k/5\rceil}$. Suppose $a=5^q b\in\Gamma_2(5^k,5)$, where $(b,5)=1$, and $1\leqslant q<k$. Then the height of the vertex a from the root 0 is $h=\lceil\log_5 k/q\rceil$.*

Proof. By Theorem 2.6 and 2.10, the digraph $\Gamma(5^k,5)$ has exactly 5 components with fixed points at 0, 1, 5^k-1, and two other fixed points. The even divisors of $\lambda(5^k)=4\cdot 5^{k-1}$ are 2, 4, $2\cdot 5^m$, or $4\cdot 5^m$, where $1\leqslant m\leqslant k-1$. Then by Theorem 2.7, there only exists a cycle of length 1 in the digraph $\Gamma(n,5)$. Moreover, $\Gamma_1(5^k,5)$ is a semiregular digraph and every vertex has degree either 0 or 5, since $5\mid\varphi(5^k)=4\cdot 5^{k-1}$. By simple observations, the digraph $\Gamma_1(5^k,5)$ consists of four isomorphic, quinary trees with 5^{k-1} vertices in every tree.

It is easy to see that we have $5^{k-\lceil k/5\rceil}$ elements in $\Gamma_2(5^k,5)$, namely $5^{\lceil k/5\rceil}$, $2\cdot 5^{\lceil k/5\rceil}$, $3\cdot 5^{\lceil k/5\rceil}$, $\ldots$, $5^{k-\lceil k/5\rceil}\cdot 5^{\lceil k/5\rceil}$ which are mapped into 0. Of course, all vertices w of $\Gamma_2(5^k,5)$ are multiples of 5 and the greater the power of 5 which is a divisor of w, the shorter the directed path from w to 0. $\square$

Example 2.4. The digraph $\Gamma_1(5^2,5)$ consists of four isomorphic quinary trees with roots 1, 7, 18 and 24, and $\Gamma_2(5^2,5)$ is a directed tree with the root 0 and $\operatorname{indeg}(0)=5$ (see Figure 6).

The digraph $\Gamma_1(5^3, 5)$ consists of four isomorphic quinary trees with roots in 1, 57, 68 and 124, and $\Gamma_2(5^3, 5)$ is a directed tree with the root 0 and $\mathrm{indeg}(0) = 25$.

3. On the zero-divisor graph of the ring $\mathbb{Z}_n$

In this section, we give formulas calculating the vertex-connectivity, edge-connectivity, and minimal degree of the zero-divisor graph of the ring $\mathbb{Z}_n$, and point out some mistakes of formulas for the clique number and the maximum degree of $G(\mathbb{Z}_n)$ in [7].

We recall that zero-divisor graphs of commutative rings were introduced by I. Beck [3] in 1988. Such graphs establish a connection between the graph theory and the commutative ring theory and help us to study the algebraic properties of rings using graph theoretical tools.

The *zero-divisor graph* of the ring $\mathbb{Z}_n$, denoted by $G(\mathbb{Z}_n)$, is the graph whose vertices are the nonzero zero-divisors of $\mathbb{Z}_n$, in which two vertices x and y are adjacent if and only if $x \neq y$ and $x \cdot y \equiv 0 \pmod{n}$.

The *chromatic number* (*edge chromatic number*) of the graph is the minimal number of colors which can be assigned to the vertices (edges) in such a way that every two adjacent vertices (edges) have different colors. A subgraph K_m with m vertices is called a *clique* of size m if any two distinct vertices in it are adjacent. The *clique number* is the least upper bound of the size of the cliques. In 1988, I. Beck showed that the chromatic number of $G(\mathbb{Z}_n)$ is equal to its clique number. In 2004, S. Akbari and A. Mohammadian proved that the edge chromatic number of $G(\mathbb{Z}_n)$ is equal to its maximum degree (see [1]).

A graph G is said to be *k-vertex-connected* (or *k-connected*) if it has more than k vertices and the result of deleting any (perhaps empty) set of fewer than k vertices is a connected graph. The *vertex-connectivity*, or just connectivity, of a graph is the largest k for which the graph is k-vertex-connected. A graph is said to be *k-edge-connected* if it remains connected whenever fewer than k edges are removed. The *edge-connectivity*, or just connectivity, of a graph is the largest k for which the graph is k-vertex-connected. We denote the vertex-connectivity, edge-connectivity, and minimal degree of graph G, respectively by $\kappa(G)$, $\lambda(G)$, and $\delta(G)$. It is well-known that $\kappa(G) \leqslant \lambda(G) \leqslant \delta(G)$ from elementary graph theory.

In [2], the following result was proved concerning the vertex-connectivity, edge-connectivity, and minimal degree of the zero-divisor graph $G(R)$ for a finite commutative ring R. Let $a \in R$, and $S \subseteq R$. Denote the annihilator of a and S in R, respectively by $\mathrm{ann}(a)$ and $\mathrm{ann}(S)$, i.e., $\mathrm{ann}(a) = \{r \in R\colon\ ra = 0\}$, and $\mathrm{ann}(S) = \{r \in R\colon\ \forall s \in S,\ rs = 0\}$.

Theorem 3.1 ([2]). *Let R be a finite commutative ring, and $G(R)$ the zero-divisor graph of R. Then:*

(1) *For any R, $\lambda(G(R)) = \delta(G(R))$.*

(2) *If R is nonlocal, $\kappa(G(R)) = \delta(G(R))$.*

(3) *If R is local with maximal ideal $\mathfrak{m}$, let r be the index of nilpotency of $\mathfrak{m}$, and $\alpha = |\mathfrak{m}| - 1$. Then:*

(i) *If $\mathfrak{m}^2 = 0$, then $\alpha - 1 = \kappa(G(R)) = \delta(G(R))$.*

(ii) *If $\mathfrak{m}^2 \neq 0$, then $\alpha \leqslant \kappa(G(R)) \leqslant \delta(G(R))$. If there exists $x \in \mathfrak{m}$ such that $\operatorname{ann}(x) = \operatorname{ann}(\mathfrak{m})$, then $\alpha = \kappa(G(R)) = \delta(G(R))$.*

(iii) *If $\mathfrak{m}^2 \neq 0$ and there is no $x \in \mathfrak{m}$ such that $\operatorname{ann}(x) = \operatorname{ann}(\mathfrak{m})$, then $\alpha < \kappa(G(R))$ if $r \geqslant 4$.*

If $n = p$, then $\mathbb{Z}_n$ is a field with none zero-divisors. In this case, $G(\mathbb{Z}_n)$ is a null graph, so we only consider the other two cases:

Theorem 3.2. *Let $G(\mathbb{Z}_n)$ be the zero-divisor graph of the ring $\mathbb{Z}_n$. Then:*

(1) *For any natural number n, $\lambda(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n))$.*

(2) *If $n = p_1^{k_1} \dots p_s^{k_s}$, where $s > 1$, $p_1 < p_2 < \dots p_s$ are distinct primes and $k_i \geqslant 1$, then $\mathbb{Z}_n$ is nonlocal, $\kappa(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n)) = p_1 - 1$, and the vertex p_1 has the minimum degree $p_1 - 1$.*

(3) *If $n = p^k$, where p is a prime and k is a positive integer bigger than 1, then $\mathbb{Z}_n$ is local. Moreover, if $k = 2$, then $\kappa(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n)) = p - 2$, and the vertex p has the minimum degree $p - 2$; if $k > 2$, then $\kappa(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n)) = p - 1$, and the vertex p has the minimum degree $p - 1$. In a word, the vertex-connectivity, edge-connectivity, and minimal degree of the zero-divisor graph of ring $\mathbb{Z}_n$ always coincide.*

Proof. It is a well-known fact from the group theory that each additive subgroup of the cyclic group $\mathbb{Z}_n$ with the addition operation modulo n is an ideal of the ring $\mathbb{Z}_n$, i.e., $\mathbb{Z}_n$ is a principal ideal ring. Suppose $n = p_1^{k_1} \dots p_s^{k_s}$, where $s > 1$, and p_i is a prime. Let $m_i = p_1^{k_1} \dots p_i^{k_i - 1} \dots p_s^{k_s}$. Then each principal ideal (m_i) is the maximal ideal of $\mathbb{Z}_n$, and $\mathbb{Z}_n$ is nonlocal. In this case, $\kappa(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n))$ by Theorem 3.1.

If $n = p^2$, then $\mathbb{Z}_n$ is local and $\mathfrak{m} = (p)$ is the unique maximal ideal. Thus $\mathfrak{m}^2 = 0$ and $\operatorname{ann}(\mathfrak{m}) = \{x;\ 0 \leqslant x < p^k$, and $p \mid x\}$. Then from the number theory, $\alpha = |\mathfrak{m}| - 1 = [p^2/p] - 1 = p - 1$, where $[a]$ denotes the greatest integer number smaller than or equal to a. Hence, $\kappa(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n)) = p - 2$.

If $n = p^k$ and $k > 2$, then $\mathbb{Z}_n$ is local and $\mathfrak{m} = (p)$ is the unique maximal ideal, but $\mathfrak{m}^2 \neq 0$ and $\operatorname{ann}(\mathfrak{m}) = \operatorname{ann}(p) = \{x;\ 0 \leqslant x < p^k$, and $p^{k-1} \mid x\}$. Then $\alpha = |\mathfrak{m}| - 1 = [p^k/p^{k-1}] - 1 = p - 1$. Hence, by Theorem 3.1, $\kappa(G(\mathbb{Z}_n)) = \delta(G(\mathbb{Z}_n)) = p - 1$. □

We correct Propositions 1 and 2 in [7] as follows.

Proposition 3.3. (1) *If* $n = p_1^{k_1} \dots p_s^{k_s}$, *where* $s > 1$, $p_1 < p_2 < \dots p_s$ *are distinct primes and* $k_i \geqslant 1$, *then the vertex* n/p_1 *has the maximal degree in* $G(\mathbb{Z}_n)$. *Moreover, if* $k_1 = 1$, *then the maximum degree is equal to* $n/p_1 - 1$; *if* $k_1 > 1$, *then the maximum degree is equal to* $n/p_1 - 2$;

(2) *if* $n = p^k$, *where* p *is a prime and* k *is a positive integer bigger than* 1, *then the vertex* n/p *has the maximal degree in* $G(\mathbb{Z}_n)$, *and the maximum degree is equal to* $n/p - 2$.

Proof. It is easy to see that if $k_1 = 1$, the vertex n/p_1 has exactly $(n/p_1 - 1)$ neighbors in $G(\mathbb{Z}_n)$, namely the elements: p_1, $2p_1$, $3p_1$, $\dots$, $(n/p_1 - 1)p_1$. It is clear that these elements are not including the vertex n/p_1. The number p_1 is the smallest prime in the factorization of n. Hence, $n/p_1 - 2$ is the maximum degree of $G(\mathbb{Z}_n)$. Similarly, if $k_1 > 1$, the vertex n/p_1 has exactly $n/p_1 - 2$ neighbors in $G(\mathbb{Z}_n)$, namely the elements: p_1, $2p_1$, $3p_1$, $\dots$, $(n/p_1 - 1)p_1$, deleting the vertex n/p_1 itself. $\square$

Proposition 3.4. (1) *If* n *is square-free, then the clique number of the graph* $G(\mathbb{Z}_n)$ *is* s.

(2) *If* α_i *are even numbers for all* $1 \leqslant i \leqslant s$, *then the clique number is* $p_1^{\alpha_1/2} p_2^{\alpha_2/2} \dots p_s^{\alpha_s/2} - 1$. *Otherwise the clique number is* $p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, *where* $\beta_i = \alpha_i/2$ *for even* α_i *and* $\beta_i = (\alpha_i - 1)/2$ *for odd* α_i. *(See* [7]*.)*

Proof. Let $n = p_1 p_2 \dots p_s$, where p_i are distinct primes, $1 \leqslant i \leqslant s$. Then there exists a clique of the size s with the vertices n/p_i, $i = 1, 2, \dots, s$. $\square$

Example 3.1. (1) Consider the zero-divisor graph $G(\mathbb{Z}_{30})$. Of course $n = 30 = 2 \cdot 3 \cdot 5$. Hence, the vertex 15 has the maximum degree $3 \cdot 5 - 1 = 14$. The clique number is 3.

(2) Let $n = 60 = 2^2 \cdot 3 \cdot 5$. Hence, the vertex 30 has the maximum degree $\frac{60}{2} - 2 = 28$, and its neighbors are the vertices 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58. The clique number is 2.

Acknowledgement. The authors are grateful to the referees for their careful reading of the original version of this paper. Their detailed comments and suggestions much improved the quality of the paper.

References

[1] *S. Akbari, A. Mohammadian*: On the zero-divisor graph of a commutative ring. J. Algebra *274* (2004), 847–855.

[2] *R. Akhtar, L. Lee*: Connectivity of the zero-divisor graph of finite rings. https//www.researchgate.net/publication/228569713.

[3] *I. Beck*: Coloring of commutative rings. J. Algebra *116* (1988), 208–226.

[4] *R. D. Carmichael*: Note on a new number theory function. Amer. Math. Soc. Bull. (2) *16* (1910), 232–238.

[5] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory (2nd, ed.). Graduate Texts in Mathematics 84, Springer, New York, 1990.

[6] *M. Křížek, F. Luca, L. Somer*: 17 Lectures on Fermat Numbers. From Number Theory to Geometry. CMS Books in Mathematics 9, Springer, New York, 2001.

[7] *J. Skowronek-Kaziów*: Some digraphs arising from number theory and remarks on the zero-divisor graph of the ring $\mathbb{Z}_n$. Inf. Process. Lett. *108* (2008), 165–169.

[8] *L. Somer, M. Křížek*: On a connection of number theory with graph theory. Czech. Math. J. *54* (2004), 465–485.

[9] *L. Somer, M. Křížek*: Stucture of digraphs associated with quadratic congruences with composite moduli. Discrete Math. *306* (2006), 2174–2185.

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

[11] *T. Vasiga, J. Shallit*: On the iteration of certain quadratic maps over GF(p). Discrete Math. *277* (2004), 219–240.

[12] *B. Wilson*: Power digraphs modulo n. Fibonacci Q. *36* (1998), 229–239.

Authors' address: Tengxia Ju, Meiyun Wu, Faculty of Science, Nantong University, No. 9, Seyuan Road, Nantong, Jiangsu Province, 226007, P. R. China, e-mail: `jtxntu@163.com`; `meiyun@ntu.edu.cn`.