The Cubic Mapping Graph of the Residue Classes of Integers

Yangjiang Wei[1,2*], Jizhu Nan[1], Gaohua Tang[2], Huadong Su[2]

1. School of Mathematical Sciences, Dalian University of Technology, Dalian, 116024, China
2. School of Mathematical Sciences, Guangxi Teachers Education University, Nanning, 530023, China

Abstract

In this paper, we study the connection of number theory with graph theory via investigating some uncharted properties of the directed graph $\Gamma(n)$ whose vertex set is $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, and for which there is a directed edge from $a \in \mathbb{Z}_n$ to $b \in \mathbb{Z}_n$ if and only if $a^3 \equiv b \pmod{n}$. For an arbitrary prime p, the formula for the decomposition of the graph $\Gamma(p)$ is established. We specify two subgraph $\Gamma_1(n)$ and $\Gamma_2(n)$ of $\Gamma(n)$. Let $\Gamma_1(n)$ be induced by the vertices which are coprime to n and $\Gamma_2(n)$ by induced by the set of vertices which are not coprime to n. We determine the level of every component of $\Gamma_1(n)$, and establish necessary and sufficient conditions when $\Gamma_1(n)$ or $\Gamma_2(n)$ has no cycles with length greater than 1, respectively. Moreover, the conditions for the semiregularity of $\Gamma_2(n)$ are presented.

Keywords: Cubic mapping graph, Carmichael λ-function, Chinese remainder theorem, Component of a graph

Mathematics Subject Classification: 05C05; 11A07;13M05.

1 Introduction

In this paper, we investigate some uncharted properties of the directed graph $\Gamma(n)$, whose vertex set is all the elements of $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, the ring of integers modulo n, and for which there is a directed edge from $a \in \mathbb{Z}_n$ to $b \in \mathbb{Z}_n$ if and only if $a^3 \equiv b \pmod{n}$. This graph $\Gamma(n)$ is called

*E-mail address: weiyangjiang2004@yahoo.com.cn

the *cubic mapping graph* of $\mathbb{Z}_n$ and some properties of $\Gamma(n)$ were studied in [5] and [6]. Our study is motivated by some results of [4] and [7].

For $n > 1$, let $U(\mathbb{Z}_n)$ denote the unit group of $\mathbb{Z}_n$, $D(\mathbb{Z}_n)$ the zero-divisor set of $\mathbb{Z}_n$. For $b \in U(\mathbb{Z}_n)$, $\mathrm{ord}_n b$ denotes the multiplicative order of b modulo n. We specify two particular directed subgraphs $\Gamma_1(n)$ and $\Gamma_2(n)$ of $\Gamma(n)$, i.e., $\Gamma_1(n)$ is induced by all the vertices of $U(\mathbb{Z}_n)$, and $\Gamma_2(n)$ is induced by all the vertices of $D(\mathbb{Z}_n)$.

Let G be a finite abelian group of order $p_1^{t_1} \cdots p_m^{t_m}$, where $p_1, \ldots, p_m$ are distinct primes and $t_1, \ldots, t_m$ are positive integers. Then we can write $G = G_1 \times \cdots \times G_m$ with G_i is a group of order $p_i^{t_i}$ for $i = 1, \ldots, m$. Let g be an element of the group G, then we can write $g = (g_1, \ldots, g_m)$ where $g_i \in G_i$.

In $\Gamma(n)$, if $a_1, \ldots, a_t$ are pairwise distinct vertices and $a_1^3 \equiv a_2 \pmod{n}$, $\ldots$, $a_{t-1}^3 \equiv a_t \pmod{n}$, $a_t^3 \equiv a_1 \pmod{n}$, then the elements $a_1, a_2, \ldots, a_t$ constitute a *cycle* of length t, and such a cycle is called a *t-cycle*. Cycles are assumed to be oriented counterclockwise. It is obvious that α is a vertex of a t-cycle if and only if t is the least positive integer such that $\alpha^{3^t} \equiv \alpha \pmod{n}$. Let $A_t(\Gamma(n))$ and $A_t(\Gamma_1(n))$, $A_t(\Gamma_2(n))$ denote the number of t-cycles in $\Gamma(n)$ and $\Gamma_1(n)$, $\Gamma_2(n)$, respectively.

A *component* of $\Gamma(n)$ is a directed subgraph which is a maximal connected subgraph of the associated undirected graph of $\Gamma(n)$. The vertex set of $\Gamma(n)$ is denoted by $V(\Gamma(n))$. Suppose $\alpha \in V(\Gamma(n))$, if $\alpha^3 \equiv \alpha \pmod{n}$, then α is called a *fixed point*. For $\alpha \in V(\Gamma(n))$, let us denote *indeg*(α) the number of directed edges coming into α. If the in-degree *indeg*(α) of a fixed point α is equal to 1, then α is called an *isolated fixed point*. Clearly the number of components of $\Gamma(n)$ is equal to the number of all cycles in $\Gamma(n)$.

A vertex α of $\Gamma(n)$ is said to be at *level* k ($k \geqslant 1$), if there exists a directed path of maximum length k which terminates at α and contains no directed edge belonging to a cycle. If α is a vertex of a cycle, then we will call the vertex α to be at *level* 0. If the highest level of all vertices in a component is k, then we say that this component has *level* $k+1$.

Similarly, we can also assign to a cyclic group C_n of order n a cubic mapping graph whose vertex set is all the elements in C_n and for which there is a directed edge from $g \in C_n$ to $h \in C_n$ if and only if $g^3 = h$, and such a graph will be denoted by $\Gamma_c(n)$.

2 The cubic mapping graphs of cyclic groups

Theorem 2.1. *Let C_n denote the cyclic group of order n.*

(1) *Suppose $n = 3^k$, $k \geqslant 1$. Then $\Gamma_c(n)$ is a ternary tree of height k with the root in* 1 *(for example, see* Fig.1*).*

(2) *Suppose* $3 \nmid n$. *Then* $\Gamma_c(n)$ *is the disjoint union*

$$\Gamma_c(n) = \bigcup_{d|n} \underbrace{(\sigma(\mathrm{ord}_d 3) \cup \cdots \cup \sigma(\mathrm{ord}_d 3))}_{\varphi(d)/\mathrm{ord}_d 3}$$

where $\sigma(l)$ *is the cycle of length* l, $\varphi(d)$ *is Euler totient function (for example, see* Fig.2*).*

(3) *Suppose* $n = 3^k m$, $k \geqslant 1$, $m > 1$, $3 \nmid m$. *Then*

$$\Gamma_c(n) = \bigcup_{d|m} \underbrace{(\sigma(\mathrm{ord}_d 3, k) \cup \cdots \cup \sigma(\mathrm{ord}_d 3, k))}_{\varphi(d)/\mathrm{ord}_d 3}$$

where $\sigma(l, k)$ *consists of a cycle of length* l *with a copy of the ternary tree of height* k *attached to each vertex (for example, see* Fig.3*).*

Proof. (1) Suppose that C_{3^k} is generated by a, i.e., $C_{3^k} = \langle a \rangle$, $a^{3^k} = 1$. First, for $b \in C_{3^k}$, it is obvious that the order of b is a power of 3. Hence, there exists a positive integer d such that $b^{3^d} = 1$. So $\Gamma_c(n)$ has exactly a component. On the other hand, it is not difficult to check that for $b \in C_{3^k}$, the number of solutions in C_{3^k} of $x^3 = b$ is 0 or 3. Therefore, we easily see that $\Gamma_c(n)$ is a ternary tree of height k with the root in 1.

(2) Let $C_n = \bigcup_{d|n} G_d$, where G_d is the set of elements with order d in C_n. Since $3 \nmid n$, we have $3 \nmid d$ and $\mathrm{ord}_d 3 \geqslant 1$ for $d|n$. So for $g \in G_d$, $\mathrm{ord}_d 3$ is the least positive integer such that $g^{3^{\mathrm{ord}_d 3}} = g$. This implies that each G_d is the disjoint union of cycles of length $\mathrm{ord}_d 3$. Moreover, by $|G_d| = \varphi(d)$ we have the formula.

(3) Since $3 \nmid m$, $C_n = C_{3^k} \times C_m$. Let $\alpha = (\alpha_1, \alpha_2)$ be a vertex of a t-cycle in $\Gamma_c(n)$, where $\alpha_1 \in C_{3^k}$ and $\alpha_2 \in C_m$. Obviously, t is the least positive integer such that $\alpha^{3^t} = \alpha$, so $\alpha_i^{3^t} = \alpha_i$ for $i = 1, 2$. By the argument of (1), we have $\alpha_1 = 1$, and $indeg(1) = 3$ in $\Gamma_c(3^k)$. By (2), $indeg(\alpha_2) = 1$ in $\Gamma_c(m)$. So $indeg(\alpha) = 3 \times 1 = 3$ in $\Gamma_c(n)$. By the similar argument in (1), we have the formula. □

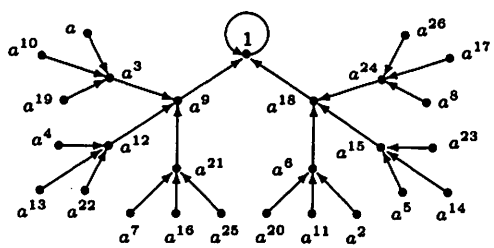

Fig.1. The cubic mapping graph of cyclic group $C_{27} = \langle a \rangle$, $a^{27} = 1$.

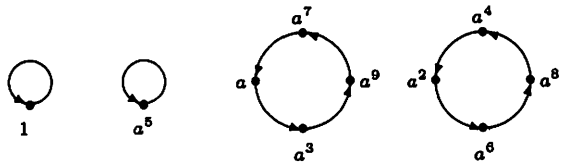

Fig.2. The cubic mapping graph of cyclic group $C_{10} = \langle a \rangle$, $a^{10} = 1$.

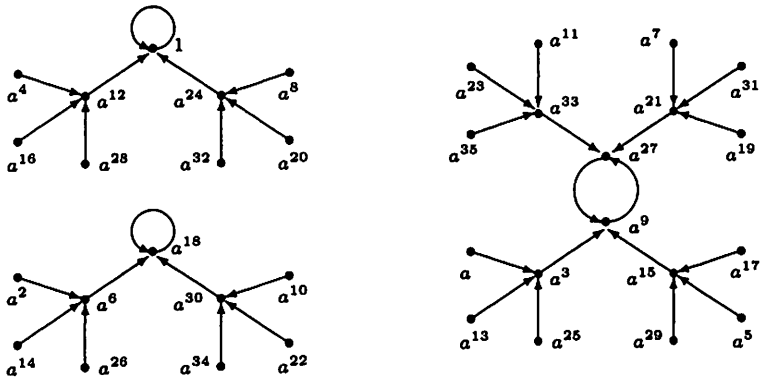

Fig.3. The cubic mapping graph of cyclic group $C_{36} = \langle a \rangle$, $a^{36} = 1$.

3 Structure of the directed graph $\Gamma(n)$

Let n be a positive integer, the Carmichael λ-function $\lambda(n)$, which was first defined in [1], is defined as follows.

$$\lambda(1) = \varphi(1) = 1,\ \lambda(2) = \varphi(2) = 1,\ \lambda(4) = \varphi(4) = 2,$$
$$\lambda(2^k) = \frac{1}{2}\varphi(2^k) = 2^{k-2} \text{ for } k \geqslant 3,$$
$$\lambda(p^k) = \varphi(p^k) = (p-1)p^{k-1} \text{ for any odd prime } p \text{ and } k \geqslant 1,$$
$$\lambda(p_1^{k_1} \cdots p_r^{k_r}) = \mathrm{lcm}[\lambda(p_1^{k_1}), \ldots, \lambda(p_r^{k_r})]$$

where $p_1, \ldots, p_r$ are distinct primes and $k_i \geqslant 1$ for all $i \in \{1, \ldots, r\}$.

The following lemma is easy to check.

Lemma 3.1. *Let $n = p_1^{t_1} \cdots p_s^{t_s}$, where $p_1 < \cdots < p_s$ are distinct primes, $t_i \geqslant 1$ and $s \geqslant 1$. Suppose $\alpha \in \mathbb{Z}_n$, and $\alpha_i \in \mathbb{Z}_{p_i^{t_i}}$ such that $\alpha \equiv \alpha_i \pmod{p_i^{t_i}}$.*

(1) If $indeg(\alpha) = k$ in $\Gamma(n)$, and $indeg(\alpha_i) = k_i$ in $\Gamma(p_i^{t_i})$, then $k = k_1 \cdots k_s$.

(2) The element α is a vertex of a cycle in $\Gamma(n)$ if and only if α_i is a vertex of a cycle in $\Gamma(p_i^{t_i})$ for $i \in \{1, \ldots, s\}$.

Theorem 3.2. *Suppose $n > 1$, then each component of $\Gamma_1(n)$ has exactly level $\omega + 1$, where $3^\omega \parallel \lambda(n)$.*

Proof. Let $n = p_1^{t_1} \cdots p_s^{t_s}$, where $p_1 < \cdots < p_s$ are distinct primes, $t_i \geqslant 1$ and $s \geqslant 1$. Clearly, $\mathrm{U}(\mathbb{Z}_n) = \mathrm{U}_1 \times \cdots \times \mathrm{U}_s$, where $\mathrm{U}_i = \mathrm{U}(\mathbb{Z}_{p_i^{t_i}})$ for $i = 1, \ldots, s$. For $\alpha \in \mathrm{U}(\mathbb{Z}_n)$, we have $\alpha = (\alpha_1, \ldots, \alpha_s)$ with $\alpha_i \in \mathrm{U}_i$.

Case 1. Suppose $3 \nmid \varphi(n)$, then $3 \nmid \varphi(p_i^{t_i})$ for $i = 1, \ldots, s$. So $3 \nmid \lambda(n)$ and hence $\omega = 0$. If $p_1 = 2$, by [6, Theorem 4], each component of $\Gamma_1(p_1^{t_1})$ is exactly a cycle. If $p_i > 2$, then U_i is a cyclic group of order $\varphi(p_i^{t_i})$ ([2]). Since $3 \nmid \varphi(p_i^{t_i})$, by Theorem 2.1 (2), each component of $\Gamma_1(p_i^{t_i})$ is exactly a cycle. Hence, by Lemma 3.1 (1), for $\alpha \in V(\Gamma_1(n))$, we have $indeg(\alpha) = 1$. So each component of $\Gamma_1(n)$ is exactly a cycle and hence each component has level 1.

Case 2. Suppose $3|\varphi(n)$. Let $|\mathrm{U}_i| = \varphi(p_i^{t_i}) = 3^{k_i} m_i$, where $k_i \geqslant 0$ and $3 \nmid m_i$ for $i = 1, \ldots, s$. If $k_i > 0$, then $p_i > 2$ and U_i is a cyclic group, so by Theorem 2.1 (3), each component of $\Gamma_1(p_i^{t_i})$ has exactly level $k_i + 1$. Otherwise, if $k_i = 0$, then $3 \nmid \varphi(p_i^{t_i})$, by the argument of Case 1, each component of $\Gamma_1(p_i^{t_i})$ has exactly level 1. Now let $k_\nu = max\{k_1, \ldots, k_s\}$, $1 \leqslant \nu \leqslant s$. Since $3|\varphi(n)$, we have $k_\nu \geqslant 1$.

Let $\mathscr{A}$ be an arbitrary component of $\Gamma_1(n)$, and the unique cycle in $\mathscr{A}$ is denoted by $\mathscr{A}_c$. Let $\gamma = (\gamma_1, \ldots, \gamma_s)$ be a vertex of the cycle $\mathscr{A}_c$, where $\gamma_i \in V(\Gamma_1(p_i^{t_i}))$. By Lemma 3.1 (2), γ_i is a vertex of a cycle which is denoted by $\mathscr{B}_i$, in $\Gamma_1(p_i^{t_i})$ for $i \in \{1, \ldots, s\}$. Since $k_\nu \geqslant 1$, it follows from Theorem 2.1 (3) that $indeg(\gamma_\nu) = 3$ in $\Gamma_1(p_\nu^{t_\nu})$. Hence, there exists $g_\nu \in V(\Gamma_1(p_\nu^{t_\nu}))$ such that $g_\nu^{3^\mu}$ does not belong to $\mathscr{B}_\nu$ for $0 \leqslant \mu < k_\nu$, and $g_\nu^{3^{k_\nu}} \equiv \gamma_\nu \pmod{p_\nu^{t_\nu}}$. In addition, let a_j be a vertex of $\mathscr{B}_j$ such that $a_j^{3^{k_\nu}} \equiv \gamma_j \pmod{p_j^{t_j}}$ for $j \neq \nu$. Now, let $\alpha = (\alpha_1, \ldots, \alpha_s)$ where $\alpha_\nu = g_\nu$ and $\alpha_j = a_j$ for $j \neq \nu$. Clearly, $\alpha \in V(\Gamma_1(n))$. By Lemma 3.1 (2), α does not belong to any cycle in $\Gamma_1(n)$ and k_ν is the least positive integer for which $\alpha^{3^{k_\nu}} \equiv \gamma \pmod{n}$. So α belongs to the component $\mathscr{A}$. Moreover, if there exists an integer k ($0 \leqslant k < k_\nu$) such that α^{3^k} belongs to the cycle $\mathscr{A}_c$, then $g_\nu^{3^k}$ is a vertex of the cycle $\mathscr{B}_\nu$ of $\Gamma_1(p_\nu^{t_\nu})$, a contradiction. So the level of component $\mathscr{A}$ is at least $k_\nu + 1$.

Next, suppose that the component $\mathscr{A}$ has exactly level $l+1$ with $l > k_\nu$. Then there exists $\beta = (\beta_1, \ldots, \beta_s) \in V(\mathscr{A})$ where $\beta_i \in V(\Gamma_1(p_i^{t_i}))$, such that l is the least nonnegative integer for which β^{3^l} belongs to the cycle $\mathscr{A}_c$. By Lemma 3.1 (2), $\beta_i^{3^l}$ is a vertex of a cycle in $\Gamma_1(p_i^{t_i})$ for $i \in \{1, \ldots, s\}$. We can check that there must exists $m \in \{1, \ldots, s\}$ such that $\beta_m^{3^{l-1}}$ does not belong to any cycle in $\Gamma_1(p_m^{t_m})$. Hence, the level of $\Gamma_1(p_m^{t_m})$ is at least $l+1$, which is impossible, for the level of $\Gamma_1(p_m^{t_m})$ is exactly $k_m + 1 \leqslant k_\nu + 1 < l + 1$. So the component $\mathscr{A}$ has exactly level $k_\nu + 1$. Hence, each component of $\Gamma_1(R)$ has level $k_\nu + 1$. Finally, notice that $3^{k_\nu} \parallel |\mathrm{U}_\nu|$, i.e., $3^{k_\nu} \parallel \varphi(p_\nu^{t_\nu})$, thus $3^{k_\nu} \parallel \lambda(n)$, so $\omega = k_\nu$. This completes the proof. □

By [5, Lemma 2, Theorem 3], we have the following lemma.

Lemma 3.3.

(1) *Suppose* $\alpha \in V(\Gamma_1(n))$, *then* α *is a vertex of a cycle in* $\Gamma_1(n)$ *if and only if* $3 \nmid \mathrm{ord}_n\alpha$.

(2) *Suppose that* α *and* β *belong to one and the same cycle of* $\Gamma_1(n)$, *then* $\mathrm{ord}_n\alpha = \mathrm{ord}_n\beta$.

Theorem 3.4.

(1) *Let* $n > 1$, *then* $\Gamma_2(n)$ *has exactly one component if and only if* $n = p^t$ *for some prime* p *and positive integer* t.

(2) *For* $t \geqslant 1$, *if* $A_t(\Gamma_2(n)) \geqslant 1$, *then* $A_t(\Gamma_1(n)) \geqslant 1$.

Proof. (1) It is not difficult to check.

(2) Suppose $A_t(\Gamma_2(n)) \geqslant 1$. Let α be a vertex of a t-cycle in $\Gamma_2(n)$. Then t is the least positive integer such that

$$\alpha(\alpha^{3^t-1} - 1) \equiv 0 \pmod{n}. \tag{3-1}$$

Let $n_1 = \gcd(\alpha, n)$, $\alpha = \alpha_0 n_1$, $n = n_0 n_1$. Then $\gcd(\alpha_0, n_0) = 1$. By (3-1), we have $n_0 n_1 | \alpha(\alpha^{3^t-1} - 1)$. Hence, $n_0 | \alpha_0(\alpha^{3^t-1} - 1)$. Since n_0 is coprime to α_0, we have $n_0 | \alpha^{3^t-1} - 1$. Moreover, by $n_1 | \alpha$ and $\gcd(\alpha, \alpha^{3^t-1} - 1) = 1$, we have $\gcd(n_0, n_1) = 1$. Now, set $\beta = 1 + \alpha - \alpha^{3^t-1}$, then $\beta \equiv 1 \pmod{n_1}$, $\beta \equiv \alpha \pmod{n_0}$. Hence, $\beta^{3^t-1} \equiv 1 \pmod{n_1}$ and $\beta^{3^t-1} \equiv \alpha^{3^t-1} \equiv 1 \pmod{n_0}$. It follows from $\gcd(n_0, n_1) = 1$, $n = n_0 n_1$ and (3-1) that t is the least positive integer such that $\beta^{3^t-1} \equiv 1 \pmod{n}$. So β is a vertex of a t-cycle in $\Gamma_1(n)$. Thus, $A_t(\Gamma_1(n)) \geqslant 1$. □

By inspection, we have the following lemma.

Lemma 3.5. *Let* $n > 1$. *Then* $\lambda(n) = 2 \cdot 3^m$ *for some* $m \geqslant 0$ *if and only if* $n = 2^s 3^t p_1 \cdots p_k$, *where* $s = 0, 1, 2, 3$ *and* $t \geqslant 0$, $k \geqslant 0$, p_i *is a prime of the form* $2 \cdot 3^{t_i} + 1$ *for some* $t_i \geqslant 1$, $i = 1, \ldots, k$.

Theorem 3.6.

(1) *Let* $n > 1$. *Then for* $t > 1$, $A_t(\Gamma_1(n)) = 0$ *if and only if* $\lambda(n) = 1$ *or* $2 \cdot 3^m$ *where* $m \geqslant 0$.

(2) *Let* $n > 1$. *Then for* $t > 1$, $A_t(\Gamma_2(n)) = 0$ *if and only if* n *is a power of a prime, or* $\lambda(n) = 2 \cdot 3^m$ *where* $m \geqslant 0$.

Proof. (1) Suppose $A_t(\Gamma_1(n)) = 0$ for $t > 1$. Clearly, if $n = 2$, then $\lambda(n) = 1$ and $A_t(\Gamma_1(2)) = 0$ for $t > 1$. Now we assume that $n > 2$. If $p \geqslant 5$ is a prime such that $p | \lambda(n)$, then by Lemma 3.3 (1), there exists a cycle with length larger than 1 in $\Gamma_1(n)$, a contradiction. So we have $p < 5$. Further, clearly $A_t(\Gamma_2(n)) = 0$ for $t > 1$ by Theorem 3.4 (2). This implies that $A_t(\Gamma(n)) = 0$ for $t > 1$. By [6, Theorem 2], for any even positive divisor d of $\lambda(n)$ with $3 \nmid d$, we must have $\mathrm{ord}_d 3 = 1$. So $d = 2$

and therefore $2 \parallel \lambda(n)$. By the argument above, we have $\lambda(n) = 1$ or $2 \cdot 3^m$ where $m \geqslant 0$, as desired.

The converse is easy to check by [6, Theorem 2].

(2) Suppose that $A_t(\Gamma_2(n)) = 0$ for $t > 1$. If n is not a power of a prime, let $n = p_1^{t_1} \cdots p_\mu^{t_\mu}$, where $\mu > 1$, $p_1 < \cdots < p_\mu$ are distinct primes and $t_1, \ldots, t_\mu$ are positive integers.

Case 1. Suppose $p_1 = 2$. If $t_1 \geqslant 4$, then $t_1 - 2 \geqslant 2$ and $\lambda(2^{t_1}) = 2^{t_1-2}$, so $4|\lambda(2^{t_1})$. Since $\mathrm{ord}_4 3 = 2$, by [6, Theorem 2], there exists a cycle of length 2 in $\Gamma(2^{t_1})$. Let α be a vertex of a 2-cycle in $\Gamma(2^{t_1})$. Then $\alpha^{3^2} \equiv \alpha \pmod{2^{t_1}}$ but $\alpha^3 \not\equiv \alpha \pmod{2^{t_1}}$. By the Chinese remainder theorem, there exists an integer β such that $\beta \equiv \alpha \pmod{2^{t_1}}$ and $\beta \equiv 0 \pmod{p_i^{t_i}}$ for $i = 2, \ldots, \mu$. Clearly, $\beta^{3^2} \equiv \beta \pmod{n}$ but $\beta^3 \not\equiv \beta \pmod{n}$. So β is a vertex of a 2-cycle in $\Gamma_2(n)$, a contradiction. So $t_1 \leqslant 3$.

Case 2. Suppose that $p_i \geqslant 5$ for some $i \in \{1, \ldots, \mu\}$. By the similar argument of Case 1, we can show that $t_i = 1$. So $\lambda(p_i^{t_i}) = \lambda(p_i) = p_i - 1 = 2^{k_i} q_i$, where $2 \nmid q_i$ and by the similar argument of Case 1, we have $k_i = 1$. Moreover, if there exists a prime $d_i > 3$ such that $d_i | q_i$, then $\mathrm{ord}_{2d_i} 3 > 2$, by [6, Theorem 2], there exists a cycle of length $\mathrm{ord}_{2d_i} 3 > 2$ in $\Gamma(p_i)$. By the similar argument of Case 1, we will also derive a contradiction. Hence, $q_i = 3^{m_i}$ for some positive integer m_i, and we have $p_i = 2 \cdot 3^{m_i} + 1$.

So we can conclude that n is a power of a prime, or by Lemma 3.5, $\lambda(n) = 2 \cdot 3^m$ for some $m \geqslant 0$.

The proof of converse is easy. □

We call a directed graph *semiregular* if there exists a positive integer d such that the in-degree of each vertex is d or 0. Specially, if every component of the directed graph is a cycle, we also call this directed graph semiregular. For example, $\Gamma_2(3^4)$ (see Fig.4) is semiregular. By [5, Corollary 1], $\Gamma_1(n)$ is semiregular for $n > 1$. Now, we study the semiregularity of $\Gamma_2(n)$.

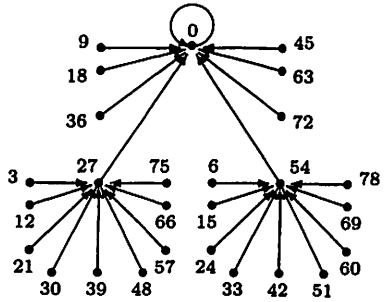

Fig.4. The subgraph $\Gamma_2(3^4)$.

Theorem 3.7.

(1) $\Gamma_2(3^t)$ *is semiregular if and only if* $t = 1, 2, 3, 4, 5$.

(2) *Suppose that* p *is a prime and* $3 \mid p-1$. *Then* $\Gamma_2(p^t)$ *is semiregular if and only if* $t = 1, 2, 3$.

(3) *Suppose that* p *is a prime,* $3 \nmid p-1$ *and* $p \neq 3$. *Then* $\Gamma_2(p^t)$ *is semiregular if and only if* $t = 1, 2, 3, 4$.

(4) *Suppose that* $n = p_1^{t_1} \cdots p_s^{t_s}$ *where* $s > 1$, $p_1 < \cdots < p_s$ *are distinct primes,* $t_1, \ldots, t_s$ *are positive integers. Then the following statements are equivalent:*

(a) $\Gamma(n)$ *is semiregular.*

(b) $\Gamma_2(n)$ *is semiregular.*

(c) $\Gamma(p_i^{t_i})$ *is semiregular for* $i \in \{1, \ldots, s\}$.

(5) *Suppose that* n *is not a power of a prime. Then* $\Gamma_2(n)$ *is semiregular if and only if* $n = 3^t p_1 \cdots p_s$, *where* $p_1 < \cdots < p_s$ *are distinct primes with* $p_i \neq 3$ *and* $3 \nmid p_i - 1$ *for* $i = \{1, \ldots, s\}$, $s \geqslant 1$, $t = 0, 1, 2$.

Proof. (1) If $t = 1, 2, 3, 4, 5$, it is easy to inspect that $\Gamma_2(3^t)$ is semiregular.

Now, let $t \geqslant 6$. Clearly $indeg(3^3) > 0$ and it is easily seen that $\alpha^3 \equiv 3^3 \pmod{3^t}$ if and only if $\alpha \equiv 3\beta \pmod{3^t}$ for some integer β such that

$$\beta^3 \equiv 1 \pmod{3^{t-3}} \tag{3-2}$$

Obviously $\beta = 3k+1$ for some integer $k \geqslant 0$. By (3-2), we have $3^{t-3} \mid 9k(3k^2+3k+1)$. Hence, $3^{t-4} \mid 3k$. This implies that $\beta = 3^{t-4}m + 1$ for some integer $m \geqslant 0$. Moreover, $3(3^{t-4}m_1 + 1) \equiv 3(3^{t-4}m_2 + 1) \pmod{3^t}$ if and only if $m_1 \equiv m_2 \pmod{3^3}$. Thus, $indeg(3^3) = 3^3$. On the other hand, by [6, Theorem 5], $indeg(0) = 3^{t-\lceil \frac{t}{3} \rceil}$. It follows from $t \geqslant 6$ that $t - \lceil \frac{t}{3} \rceil \geqslant 4$, whereas $indeg(3^3) = 3^3$ and hence $\Gamma_2(3^t)$ is not semiregular for $t \geqslant 6$.

(2) If $t = 1, 2, 3$, clearly $\Gamma_2(p^t)$ is semiregular.

Conversely, suppose that $t \geqslant 4$. Clearly $indeg(p^3) > 0$ and it is easily seen that $\alpha^3 \equiv p^3 \pmod{p^t}$ if and only if $\alpha \equiv p\beta \pmod{p^t}$ for some integer β such that

$$\beta^3 \equiv 1 \pmod{p^{t-3}} \tag{3-3}$$

Since $3 \mid p-1$, by [3, p.231, 8(i)], there are exactly $\gcd(3, p-1) = 3$ solutions of (3-3), namely $\beta \equiv \beta_i \pmod{p^{t-3}}$, $i = 1, 2, 3$, where $\beta_1, \beta_2, \beta_3$ are distinct positive integers less than p^{t-3}. Moreover, $p(\beta_i + k_1 p^{t-3}) \equiv p(\beta_i + k_2 p^{t-3}) \pmod{p^t}$ if and only if $k_1 \equiv k_2 \pmod{p^2}$. In addition, if $i \neq j$, then $p(\beta_i + k_1 p^{t-3}) \not\equiv p(\beta_j + k_2 p^{t-3}) \pmod{p^t}$ for $k_1, k_2 \geqslant 0$. Thus, $indeg(p^3) = 3p^2$. On the other hand, there are exactly $p^{t-\lceil \frac{t}{3} \rceil}$ elements in $\Gamma_2(p^t)$ namely $p^{\lceil \frac{t}{3} \rceil}$, $2 \cdot p^{\lceil \frac{t}{3} \rceil}, \ldots, p^{t-\lceil \frac{t}{3} \rceil} \cdot p^{\lceil \frac{t}{3} \rceil}$ which are mapped into 0. Hence, $indeg(0) = p^{t-\lceil \frac{t}{3} \rceil}$. Since $p > 3$ and $t \geqslant 4$, we have $indeg(0) \neq indeg(p^3)$ and hence $\Gamma_2(p^t)$ is not semiregular for $t \geqslant 4$.

(3) Suppose $t \geqslant 5$. Clearly $indeg(p^3) > 0$ and it is easily seen that $\alpha^3 \equiv p^3 \pmod{p^t}$ if and only if $\alpha \equiv p\beta \pmod{p^t}$ for some integer β such that the congruence (3-3) holds. Since $3 \nmid p-1$, by [3, p.231, 8(i)], the number of solutions of (3-3) is equal to $\gcd(3, p-1) = 1$, i.e., $\beta \equiv 1 \pmod{p^{t-3}}$. Moreover, $p(1+k_1p^{t-3}) \equiv p(1+k_2p^{t-3}) \pmod{p^t}$ if and only if $k_1 \equiv k_2 \pmod{p^2}$. So $indeg(p^3) = p^2$. Further, $indeg(0) = p^{t-\lceil \frac{t}{3} \rceil}$ and $t - \lceil \frac{t}{3} \rceil \geqslant 3$ for $t \geqslant 5$. Hence, $indeg(0) \neq indeg(p^3)$. So $\Gamma_2(p^t)$ is not semiregular for $t \geqslant 5$.

Conversely, let $t = 4$. It is not difficult to show that for $\gamma \in \{1, \ldots, p-1\}$, there exists $\gamma_0 \in \{1, \ldots, p-1\}$ such that $\gamma \equiv \gamma_0^3 \pmod{p}$. So $\gamma p^3 \equiv \gamma_0^3 p^3 \pmod{p^4}$. Therefore, $indeg(\gamma p^3) > 0$. By the similar argument above, we have $indeg(\gamma p^3) = p^2$. Moreover, since $t = 4$, $indeg(0) = p^{t-\lceil \frac{t}{3} \rceil} = p^2$. So we can conclude that there are p vertices in $\Gamma_2(p^t)$, namely $0, p^3, 2p^3, \ldots, (p-1)p^3$, with in-degree p^2, and we have $p \times p^2 = p^3$. Since the number of vertices in $\Gamma_2(p^t)$ is p^3, the in-degree of any vertex in $\Gamma_2(p^t)$ is p^2 or 0. Hence $\Gamma_2(p^t)$ is semiregular if $t = 4$. Moreover, it is easy to see that $\Gamma_2(p^t)$ is semiregular for $t = 1, 2, 3$.

(4) (a) $\Rightarrow$ (b) is clear.

(b) $\Rightarrow$ (c) Suppose that $\Gamma_2(n)$ is semiregular. In each $\Gamma(p_i^{t_i})$, set $indeg(0) = k_i \geqslant 1$. By Lemma 3.1 (1), $indeg(0) = k_1 \cdots k_s$ in $\Gamma(n)$. Let $i \in \{1, \ldots, s\}$. Suppose that β_i is an arbitrary vertex in $\Gamma(p_i^{t_i})$ with $indeg(\beta_i) = d_i \neq 0$. By the Chinese remainder theorem, there exists a positive integer β such that $\beta \equiv \beta_i \pmod{p_i^{t_i}}$ and $\beta \equiv 0 \pmod{p_j^{t_j}}$ for $j \in \{1, \ldots, s\}$ and $j \neq i$. Then by Lemma 3.1 (1), $indeg(\beta) = k_1 \cdots k_{i-1} d_i k_{i+1} \cdots k_s \neq 0$ in $\Gamma(n)$. Since $\Gamma_2(n)$ is semiregular, $indeg(0) = indeg(\beta)$ in $\Gamma_2(n)$, i.e., $k_1 \cdots k_s = k_1 \cdots k_{i-1} d_i k_{i+1} \cdots k_s$. Hence, $d_i = k_i$. Thus $\Gamma(p_i^{t_i})$ is semiregular for $i \in \{1, \ldots, s\}$.

(c) $\Rightarrow$ (a) Suppose that $\Gamma(p_i^{t_i})$ is semiregular for each i. In every $\Gamma(p_i^{t_i})$, let $indeg(0) = indeg(1) = k_i \geqslant 1$. Obviously, $indeg(0) = indeg(1) = k_1 \cdots k_s$ in $\Gamma(n)$. Assume $\alpha \in \mathbb{Z}_n$ and $\alpha \equiv \alpha_i \pmod{p_i^{t_i}}$, then $indeg(\alpha) = indeg(\alpha_1) \times \cdots \times indeg(\alpha_s)$. Since $\Gamma(p_i^{t_i})$ is semiregular, we have either $indeg(\alpha_i) = 0$ or $indeg(\alpha_i) = indeg(0) = k_i$ in $\Gamma(p_i^{t_i})$. So $indeg(\alpha) = 0$ or $indeg(\alpha) = k_1 \cdots k_s = indeg(0) = indeg(1)$ in $\Gamma(n)$. Moreover, by [6, Lemma 2], $\Gamma_1(n)$ is semiregular for $n > 1$, so $\Gamma(n)$ is semiregular.

(5) By (1), (2) and (3) above, we have $\Gamma(p^t)$ is semiregular if and only if $p^t = 3^2$ or $3 \nmid p-1$ with $t = 1$. Therefore, by (4), the result holds. $\square$

Acknowdgements

This research was supported by the National Natural Science Foundation of China (10771095), the Guangxi Science Foundation (0832107, 0991102) and the Scientific Research Foundation of Guangxi Educational Committee (200911LX284, 200911LX275).

References

[1] R.D. Carmichael, Note on a new number theory function, Bull. Amer. Math. Soc. 16 (1910) 232-238.

[2] R.W. Gilmer, Finite rings having a cyclic group of units, Am. J. Math. 85 (3) (1963) 447–452.

[3] C. D. Pan, C. B. Pan, Elementary number Theory, 2nd edition, Beijing University Publishing Company, Beijing, 2005 (In Chinese).

[4] T.D. Rogers, The graph of the square mapping on the prime fields, Discrete Math. 148 (1996) 317–324.

[5] J. Skowronek-Kaziów, Zielona Góra, Properties of digraphs connected with some congruence relations, Czechoslovak Math. J. 59 (134) (2009) 39–49.

[6] J. Skowronek-Kaziów, Some digraphs arising from number theory and remarks on the zero-divisor graph of the ring Z_n, Information Processing Letters 108 (2008) 165–169.

[7] L. Somer, M. Křížek, On a connection of number theory with graph theory, Czechoslovak Math. J. 54 (129) (2004) 465–485.