Yangjiang Wei; Jizhu Nan; Gaohua Tang
The cubic mapping graph for the ring of Gaussian integers modulo n

Czechoslovak Mathematical Journal, Vol. 61 (2011), No. 4, 1023–1036

Persistent URL: `http://dml.cz/dmlcz/141804`

Czechoslovak Mathematical Journal, 61 (136) (2011), 1023–1036

THE CUBIC MAPPING GRAPH FOR THE RING OF GAUSSIAN INTEGERS MODULO n

Yangjiang Wei, Dalian, Jizhu Nan, Dalian,
Gaohua Tang, Nanning

(Received July 21, 2010)

Abstract. The article studies the cubic mapping graph $\Gamma(n)$ of $\mathbb{Z}_n[\mathrm{i}]$, the ring of Gaussian integers modulo n. For each positive integer $n > 1$, the number of fixed points and the in-degree of the elements $\overline{1}$ and $\overline{0}$ in $\Gamma(n)$ are found. Moreover, complete characterizations in terms of n are given in which $\Gamma_2(n)$ is semiregular, where $\Gamma_2(n)$ is induced by all the zero-divisors of $\mathbb{Z}_n[\mathrm{i}]$.

Keywords: Gaussian integers modulo n, cubic mapping graph, fixed point, semiregularity

MSC 2010: 05C05, 11A07, 13M05

1. Introduction

The set of all complex number $a+b\mathrm{i}$, where a and b are integers, forms a Euclidean domain which is denoted by $\mathbb{Z}[\mathrm{i}]$, with the usual complex number operations. Let $n > 1$ be an integer and $\langle n\rangle$ the principal idea generated by n in $\mathbb{Z}[\mathrm{i}]$, and $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ the ring of integers modulo n. Then the factor ring $\mathbb{Z}[\mathrm{i}]/\langle n\rangle$ is isomorphic to $\mathbb{Z}_n[\mathrm{i}] = \{\overline{a} + \overline{b}\mathrm{i}\colon \overline{a}, \overline{b} \in \mathbb{Z}_n\}$. The ring $\mathbb{Z}_n[\mathrm{i}]$ is called the ring of *Gaussian integers modulo n*.

In this paper, we investigate some properties of the digraph $\Gamma(n)$, whose vertex set consists of all elements of $\mathbb{Z}_n[\mathrm{i}]$, and for which there is a directed edge from $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathbb{Z}_n[\mathrm{i}]$ to $\beta = \overline{x} + \overline{y}\,\mathrm{i} \in \mathbb{Z}_n[\mathrm{i}]$ if and only if $\alpha^3 = \beta$. This digraph $\Gamma(n)$

This research was supported by the National Natural Science Foundation of China (11161006, 11171142), the Guangxi natural Science Foundation (2011GXNSFA018139), the Guangxi New Century 1000Talents Project and the Scientific Research Foundation of Guangxi Educational Committee (201012MS140).

is called the *cubic mapping graph* of $\mathbb{Z}_n[\mathrm{i}]$. In [4], [5] and [9], some properties of the cubic mapping graph of $\mathbb{Z}_n$ were investigated.

Let R be a commutative ring, let $\mathrm{U}(R)$ denote the unit group of R, $\mathrm{D}(R)$ the zero-divisor set of R. For $\alpha \in \mathrm{U}(R)$, $o(\alpha)$ denotes the multiplicative order of α in R. If $R = \mathbb{Z}_n$, then we write $\mathrm{ord}_n\,\alpha$ instead of $o(\alpha)$. We specify two particular subdigraphs $\Gamma_1(n)$ and $\Gamma_2(n)$ of $\Gamma(n)$, i.e., $\Gamma_1(n)$ induced by all the vertices of $\mathrm{U}(\mathbb{Z}_n[\mathrm{i}])$, and $\Gamma_2(n)$ induced by all the vertices of $\mathrm{D}(\mathbb{Z}_n[\mathrm{i}])$.

Let G be a finite abelian group of order $p_1^{t_1}\dots p_m^{t_m}$, where $p_1,\dots,p_m$ are distinct primes and $t_1,\dots,t_m$ are positive integers. Then we can write $G = G_1 \times \dots \times G_m$ where G_k is a group of order $p_k^{t_k}$ for $k = 1,\dots,m$. Furthermore, for an arbitrary element g of the group G, we can write $g = (g_1,\dots,g_m)$ with $g_k \in G_k$.

In $\Gamma(n)$, if $\alpha_1,\dots,\alpha_t$ are pairwise distinct vertices and $\alpha_1^3 = \alpha_2,\dots,\alpha_{t-1}^3 = \alpha_t$, $\alpha_t^3 = \alpha_1$, then the elements $\alpha_1,\alpha_2,\dots,\alpha_t$ 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 $\alpha^{3^t} = \alpha$. Let $A_t(\Gamma(n))$, $A_t(\Gamma_1(n))$, and $A_t(\Gamma_2(n))$ denote the number of t-cycles in $\Gamma(n)$, $\Gamma_1(n)$, and $\Gamma_2(n)$, respectively.

A *component* of $\Gamma(n)$ is a subdigraph which is a maximal connected subgraph of the associated nondirected graph of $\Gamma(n)$. Clearly, the number of components in $\Gamma(n)$ is equal to the number of all cycles in $\Gamma(n)$. If $\sigma_1,\dots,\sigma_k$ $(k \geqslant 1)$ are distinct components of $\Gamma(n)$ (i.e., there exist no common vertices between σ_t and σ_j whenever $t \neq j$, $1 \leqslant t, j \leqslant k$), then the disjoint union $\sigma_1 \cup \dots \cup \sigma_k$ denotes a subdigraph of $\Gamma(n)$, such a subdigraph contains precisely k components, namely, $\sigma_1,\dots,\sigma_k$. Let $\mathrm{Com}(\alpha)$ denote the component containing the element α. The vertex set of $\Gamma(n)$ is denoted by $V(\Gamma(n))$. Suppose $\alpha \in V(\Gamma(n))$, if $\alpha^3 = \alpha$, then α is called a *fixed point*. For $\alpha \in V(\Gamma(n))$, the in-degree $\mathrm{indeg}(\alpha)$ of α denotes the number of directed edges coming into α. If α is a fixed point and $\mathrm{indeg}(\alpha) = 1$, then α is called an *isolated fixed point*.

We call a digraph *semiregular* if there exists a positive integer d such that the in-degree of each vertex is either d or 0 ([6]). In particular, if every component of the digraph is exactly a cycle, we also call this digraph semiregular.

Similarly, we can assign to a cyclic group C_n of order n a cubic mapping graph whose vertex set consists of all 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 digraph will be denoted by $\Gamma_c(n)$.

2. Some lemmas

Lemma 2.1 (9, Theorem 2.1). *Let C_n denote the cyclic group of order n, and let 1 be the identity of C_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.*

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

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

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

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

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

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.

The following results were shown in [1] and [7].

Lemma 2.2. *Let $n > 1$.*

(1) *The element $\overline{a} + \overline{b}\mathrm{i}$ is a unit of $\mathbb{Z}_n[\mathrm{i}]$ if and only if $\overline{a}^2 + \overline{b}^2$ is a unit of $\mathbb{Z}_n$.*

(2) *If $n = \prod\limits_{j=1}^{s} p_j^{k_j}$ is the prime power decomposition of n, then the function*

$$\theta\colon\ \mathbb{Z}_n[\mathrm{i}] \to \bigoplus_{j=1}^{s} \mathbb{Z}_{p_j^{k_j}}[\mathrm{i}] \tag{2.1}$$

such that $\theta(\overline{a} + \overline{b}\mathrm{i}) = ((a \bmod p_j^{k_j}) + (b \bmod p_j^{k_j})\mathrm{i})_{j=1}^{s}$ is an isomorphism.

(3) *$\mathbb{Z}_n[\mathrm{i}]$ is a local ring if and only if $n = p^t$, where $p = 2$ or p is a prime congruent to 3 modulo 4, $t \geqslant 1$.*

(4) *$\mathbb{Z}_n[\mathrm{i}]$ is a field if and only if n is a prime congruent to 3 modulo 4.*

According to papers [2] and [8], we have the following lemma.

Lemma 2.3.

(1) $\mathrm{U}(\mathbb{Z}_2[\mathrm{i}]) \cong \mathbb{Z}_2$, $\mathrm{U}(\mathbb{Z}_{2^2}[\mathrm{i}]) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^2}$, $\mathrm{U}(\mathbb{Z}_{2^t}[\mathrm{i}]) \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^{t-1}} \times \mathbb{Z}_{2^{t-2}}$ *for $t > 2$. Hence,* $|\mathrm{U}(\mathbb{Z}_{2^t}[\mathrm{i}])| = 2^{2t-1}$, $|\mathrm{D}(\mathbb{Z}_{2^t}[\mathrm{i}])| = 2^{2t-1}$.

(2) *Let q be a prime congruent to* 3 *modulo* 4*. Then* $\mathrm{U}(\mathbb{Z}_{q^t}[\mathrm{i}]) \cong \mathbb{Z}_{q^{t-1}} \times \mathbb{Z}_{q^{t-1}} \times \mathbb{Z}_{q^2-1}$ *for* $t \geqslant 1$*. Hence,* $|\mathrm{U}(\mathbb{Z}_{q^t}[\mathrm{i}])| = q^{2t} - q^{2t-2}$, $|\mathrm{D}(\mathbb{Z}_{q^t}[\mathrm{i}])| = q^{2t-2}$.

(3) *Let p be a prime congruent to* 1 *modulo* 4*. Then* $\mathrm{U}(\mathbb{Z}_{p^t}[\mathrm{i}]) \cong \mathbb{Z}_{p^{t-1}} \times \mathbb{Z}_{p^{t-1}} \times \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ *for* $t \geqslant 1$*. Hence,* $|\mathrm{U}(\mathbb{Z}_{p^t}[\mathrm{i}])| = (p^t - p^{t-1})^2$, $|\mathrm{D}(\mathbb{Z}_{p^t}[\mathrm{i}])| = 2p^{2t-1} - p^{2t-2}$.

By Lemma 2.2 (2), we have the following lemma concerning the in-degree of an arbitrary vertex in $\Gamma(n)$.

Lemma 2.4. *Suppose* $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathbb{Z}_n[\mathrm{i}]$*, and let* $n = \prod_{j=1}^{s} p_j^{k_j}$ *be the prime power decomposition of n. Then* $\mathrm{indeg}(\alpha) = \mathrm{indeg}(\alpha_1) \times \ldots \times \mathrm{indeg}(\alpha_s)$*, where* $\alpha_j = (a \bmod p_j^{k_j}) + (b \bmod p_j^{k_j})\mathrm{i}$ *and* $\mathrm{indeg}(\alpha_j)$ *is the in-degree of α_j in* $\Gamma(p_j^{k_j})$*,* $j = 1, \ldots, s$.

3. Structure of the digraph $\Gamma(n)$

Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in V(\Gamma(n))$. Then α is a fixed point of $\Gamma(n)$ if and only if $\alpha^3 = \alpha$, i.e., the following system of equations holds

$$a^3 - 3ab^2 \equiv a \pmod{n}, \tag{3.1}$$

$$3a^2 b - b^3 \equiv b \pmod{n}. \tag{3.2}$$

Now, let

$$n = 2^k \times \prod_{j=1}^{m} q_j^{t_j} \times \prod_{s=1}^{l} p_s^{\lambda_s} \tag{3.3}$$

be the prime power factorization of n, where $k, m, l \geqslant 0$, $t_j, \lambda_s \geqslant 1$, $q_1, \ldots, q_m$ are distinct primes congruent to 3 modulo 4, and $p_1, \ldots, p_l$ are distinct primes congruent to 1 modulo 4. The following theorem gives the formula for the number of fixed points in $\Gamma(n)$.

Theorem 3.1. *Let n be as in* (3.3)*. The number $L(n)$ of fixed points in $\Gamma(n)$ equals*

$$L(n) = \begin{cases} 3^k \times 3^m \times 9^l, & k = 0, 1, \\ 5 \times 3^m \times 9^l, & k = 2, \\ 9 \times 3^m \times 9^l, & k \geqslant 3. \end{cases}$$

P r o o f. Let $\alpha=\overline{a}+\overline{b}\mathrm{i}\in\mathbb{Z}_n[\mathrm{i}]$ and $\alpha^3=\alpha$. By Lemma 2.4, it suffices to consider the cases of n being a power of a prime.

(1) Suppose $n=2^k$ $(k\geqslant 1)$. By inspection, $L(2)=3$ and $L(2^2)=5$.

Now, let $k\geqslant 3$. Then by Lemma 2.2 (3), $\mathbb{Z}_{2^k}[\mathrm{i}]$ is a local ring. If $\alpha\in\mathrm{D}(\mathbb{Z}_{2^k}[\mathrm{i}])$, then clearly α is a vertex of $\mathrm{Com}(\overline{0})$. Note that $\alpha^3=\alpha$, therefore $\alpha=\overline{0}$.

Now suppose $\alpha\in\mathrm{U}(\mathbb{Z}_{2^k}[\mathrm{i}])$. Since $\alpha^3=\alpha$, we have $\alpha^2=\overline{1}$, and the following system of equations holds

$$a^2-b^2\equiv 1 \pmod n, \tag{3.4}$$

$$2ab\equiv 0 \pmod n. \tag{3.5}$$

Clearly, a and b have different parity. First, if a is even while b is odd, then it follows from (3.5) that $2^{k-1}\mid a$. Hence, we derive from (3.4) that $b^2\equiv -1 \pmod{2^k}$, which is impossible because $k>2$. So a must be odd while b is even. In this case we have $2^{k-1}\mid b$ and $a^2\equiv 1\pmod{2^k}$. By [6, Lemma 2.5] and since $k>2$, the number of solutions of $a^2\equiv 1\pmod{2^k}$ is 2^2. Therefore, the number of solutions of the system of equations (3.4) and (3.5) is 2^3.

Hence, we can conclude that $L(2^k)=1+2^3=9$ for $k\geqslant 3$.

(2) Suppose $n=q^t$ $(t\geqslant 1)$, where q is a prime congruent to 3 modulo 4. Then by Lemma 2.2 (3), $\mathbb{Z}_{q^t}[\mathrm{i}]$ is a local ring. If $\alpha\in\mathrm{D}(\mathbb{Z}_{q^t}[\mathrm{i}])$, then clearly α is a vertex of $\mathrm{Com}(\overline{0})$. Therefore, $\alpha=\overline{0}$.

Now suppose $\alpha\in\mathrm{U}(\mathbb{Z}_{q^t}[\mathrm{i}])$. By Lemma 2.2 (1) we have $q\nmid a^2+b^2$. It follows from (3.5) that $q^t\mid a$ while $q\nmid b$, or $q^t\mid b$ while $q\nmid a$. First, if $q^t\mid a$, $q\nmid b$, by (3.4), we have $b^2\equiv -1\pmod{q^t}$ and this equation has no solutions because $q\equiv 3\pmod 4$. So we have $q^t\mid b$ and $q\nmid a$. By (3.4), $a^2\equiv 1\pmod{p^t}$ and the number of solutions of this equation is 2 ([6, Lemma 2.5]). Therefore, we can conclude that $L(q^t)=1+2=3$.

(3) Suppose $n=p^\lambda$ $(\lambda\geqslant 1)$, where p is a prime congruent to 1 modulo 4. If $\alpha\in\mathrm{D}(\mathbb{Z}_{p^\lambda}[\mathrm{i}])$ with $\alpha\neq\overline{0}$, by Lemma 2.2 (1) we have $p\mid a^2+b^2$. It follows immediately from (3.1) and (3.2) that $p\nmid a$ and $p\nmid b$. Hence, $a^2-3b^2\equiv 1\pmod{p^\lambda}$, $3a^2-b^2\equiv 1\pmod{p^\lambda}$. Thus, $4a^2\equiv 1\pmod{p^\lambda}$ and $4b^2\equiv -1\pmod{p^\lambda}$. Clearly, each of the last two equations has exactly 2 solutions. Moreover, note that $\overline{0}^3=\overline{0}$, so the system of equations (3.1) and (3.2) has exactly $2\times 2+1=5$ solutions.

Now suppose $\alpha\in\mathrm{U}(\mathbb{Z}_{p^\lambda}[\mathrm{i}])$ and by Lemma 2.2 (1), we have $p\nmid a^2+b^2$. It can be derived from (3.5) that exactly one of a and b must be divisible by p^λ. First, if $p^\lambda\mid a$ and $p\nmid b$, then the number of solutions of equation (3.2) is 2. Secondly, if $p^\lambda\mid b$ and $p\nmid a$, then the number of solutions of equation (3.1) is 2. Therefore, if $\alpha\in\mathrm{U}(\mathbb{Z}_{p^\lambda}[\mathrm{i}])$ with $\alpha^3=\alpha$, then the system of equations (3.1) and (3.2) has exactly $2+2=4$ solutions.

Therefore, we can conclude that $L(p^\lambda)=5+4=9$. $\square$

For example, $\Gamma(2^2)$ has exactly 5 fixed points, see Figure 1.

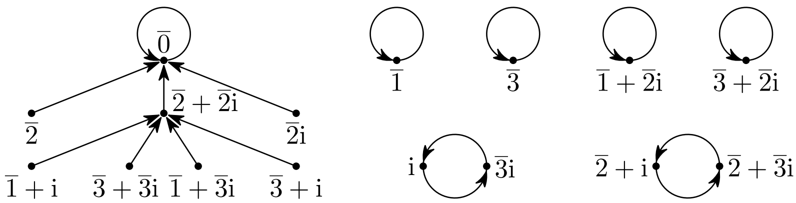

Figure 1. The cubic mapping graph of $\mathbb{Z}_{2^2}[\mathrm{i}]$.

Theorem 3.2. *For $n > 1$, $\Gamma_1(n)$ is semiregular.*

Proof. Suppose $\mathrm{U}(\mathbb{Z}_n[\mathrm{i}]) = U_1 \times \ldots \times U_t$, $t \geqslant 1$, $U_1, \ldots, U_t$ being cyclic groups. If $3 \nmid |\mathrm{U}(\mathbb{Z}_n[\mathrm{i}])|$, then $3 \nmid |U_s|$ for $s = 1, \ldots, t$. By Lemma 2.1 (2), $\mathrm{indeg}(\alpha_s) = 1$ for $\alpha_s \in U_s$. Therefore by Lemma 2.4, $\mathrm{indeg}(\alpha) = 1$ for $\alpha \in \mathrm{U}(\mathbb{Z}_n[\mathrm{i}])$.

Now suppose $3 \mid |\mathrm{U}(\mathbb{Z}_n[\mathrm{i}])|$. Without loss of generality, we can assume that $3 \mid |U_1|, \ldots, 3 \mid |U_v|$ with $1 \leqslant v \leqslant t$, and $3 \nmid |U_{v+1}|, \ldots, 3 \nmid |U_t|$. By Lemma 2.1 and Lemma 2.4, $\mathrm{indeg}(\alpha) = 3^v$ or 0 for $\alpha \in \mathrm{U}(\mathbb{Z}_n[\mathrm{i}])$.

So we conclude that $\Gamma_1(n)$ is semiregular. $\square$

Theorem 3.3. *Let $n = 2^v 3^k \times \prod_{j=1}^{m} q_j^{\alpha_j} \times \prod_{s=1}^{h} p_s^{\beta_s} \times \prod_{\lambda=1}^{l} g_\lambda^{\gamma_\lambda}$, where $v, k, m, h, l \geqslant 0$, $\alpha_j, \beta_s, \gamma_\lambda \geqslant 1$, $3 < q_1 < \ldots < q_m$ are primes congruent to 3 modulo 4, $p_1, \ldots, p_h$ are distinct primes congruent to 1 modulo 12, and $g_1, \ldots, g_l$ are distinct primes congruent to 5 modulo 12. Then the in-degree of $\overline{1}$ in $\Gamma(n)$ is*

$$\mathrm{indeg}(\overline{1}) = \begin{cases} 3^{m+2h}, & k = 0, 1, \\ 3^{m+2h+2}, & k \geqslant 2. \end{cases}$$

Proof. By Lemma 2.4, it suffices to consider the cases of n being a power of a prime.

(1) Suppose $n = 2^v$ ($v \geqslant 1$). By Lemma 2.1 (2), the in-degree of the identity 1 of a cyclic group C_m with $3 \nmid m$ is equal to 1. Therefore, by Lemma 2.3 (1) and Lemma 2.4, the in-degree of $\overline{1}$ in $\Gamma(n)$ is equal to 1.

(2) Suppose $n = 3^k$. If $k = 1$, then by an argument similar to (1), we have $\mathrm{indeg}(\overline{1}) = 1$. If $k \geqslant 2$, by Lemma 2.1, 2.3 (2) and Lemma 2.4, $\mathrm{indeg}(\overline{1}) = 3^2$.

(3) Suppose $n = q^j$, where $q > 3$ is a prime congruent to 3 modulo 4, $j \geqslant 1$. Since $3 \nmid q$, exactly one of $q-1$, $q+1$ is divisible by 3. It follows from Lemma 2.1 (3) and Lemma 2.3 (2), 2.4 that $\mathrm{indeg}(\overline{1}) = 3$.

(4) Suppose $n = p^s$, where p is a prime congruent to 1 modulo 4, $s \geqslant 1$. Clearly, $4 \mid p-1$ and $3 \mid p-1$ if and only if $12 \mid p-1$. So by Lemma 2.1 and 2.3 (3), if $p \equiv 1 \pmod{12}$, then $\mathrm{indeg}(\overline{1}) = 3^2$. If $p \equiv 5 \pmod{12}$, then $\mathrm{indeg}(\overline{1}) = 1$. $\square$

Theorem 3.4. *Let* $n = 2^m \times \prod_{j=1}^{s} p_j^{t_j}$, *where* $p_1, \ldots, p_s$ *are distinct odd primes,* $m, s \geqslant 0$, $t_j \geqslant 1$. *Then the in-degree of* $\overline{0}$ *in* $\Gamma(n)$ *is*

$$\operatorname{indeg}(\overline{0}) = \begin{cases} 2^{2(m-\lceil m/3\rceil)} \times \prod\limits_{j=1}^{s} p_j^{2(t_j-\lceil t_j/3\rceil)}, & m \equiv 0, 2 \pmod 3, \\ 2^{2(m-\lceil m/3\rceil)+1} \times \prod\limits_{j=1}^{s} p_j^{2(t_j-\lceil t_j/3\rceil)}, & m \equiv 1 \pmod 3. \end{cases}$$

Proof. By Lemma 2.4, it suffices to consider the cases of n being a power of a prime, i.e., $n = p^m$, where p is a prime, $m \geqslant 1$.

First, let $m = 1$, then clearly $\operatorname{indeg}(\overline{0}) = 2$ if $p = 2$, and $\operatorname{indeg}(\overline{0}) = 1$ if p is an odd prime.

Now, let $m > 1$. Assume that $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathbb{Z}_n[\mathrm{i}]$ with $\alpha^3 = \overline{0}$. Clearly $p \mid a$ and $p \mid b$. Let $a = p^u a_1$, $b = p^v b_1$, where u, v are positive integers, $p \nmid a_1$ and $p \nmid b_1$. Set $k = \min\{u, v\}$. Then $\alpha = p^k\beta$, where $\beta = p^{u-k}\overline{a_1} + p^{v-k}\overline{b_1}\mathrm{i}$.

On the one hand, it is clear that if $k \geqslant \lceil m/3\rceil$, then $\alpha^3 = \overline{0}$.

Conversely, suppose $1 \leqslant k \leqslant \lceil m/3\rceil - 1$. If $u \neq v$, then $\beta \in \mathrm{U}(\mathbb{Z}_n[\mathrm{i}])$, which implies that $\beta^3 \neq \overline{0}$. So $\alpha^3 \neq \overline{0}$. If $u = v$, then $\alpha = p^k(\overline{a_1} + \overline{b_1}\mathrm{i})$. Hence, $\alpha^3 = \overline{0}$ if and only if $a_1^3 - 3a_1b_1^2 \equiv 0 \pmod{p^{m-3k}}$ and $3a_1^2b_1 - b_1^3 \equiv 0 \pmod{p^{m-3k}}$, if and only if $a_1^2 - 3b_1^2 \equiv 0 \pmod{p^{m-3k}}$ and $3a_1^2 - b_1^2 \equiv 0 \pmod{p^{m-3k}}$. Now there are two cases to consider.

First, if p is an odd prime with $m > 1$, or $p = 2$ with $m \equiv 0$ or $2 \pmod 3$, then it is not difficult to show that $\alpha^3 \neq \overline{0}$. So $\alpha^3 = \overline{0}$ if and only if $p^{\lceil m/3\rceil} \mid a$ and $p^{\lceil m/3\rceil} \mid b$. So we have $\operatorname{indeg}(\overline{0}) = p^{2m-2\lceil m/3\rceil}$.

Secondly, assume that $p = 2$ and $m \equiv 1 \pmod 3$, $\alpha = 2^k(\overline{a_1} + \overline{b_1}\mathrm{i})$. Since $2 \parallel a_1^2 - 3b_1^2$, we have $2^{m-3k} \mid a_1^2 - 3b_1^2$ if and only if $m - 3k = 1$, if and only if $k = \lceil m/3\rceil - 1$. Similarly, $2^{m-3k} \mid 3a_1^2 - b_1^2$ if and only if $k = \lceil m/3\rceil - 1$. Therefore, $\alpha^3 = \overline{0}$ if and only if $2^{\lceil m/3\rceil} \mid a$ and $2^{\lceil m/3\rceil} \mid b$, or $2^{\lceil m/3\rceil-1} \parallel a$ and $2^{\lceil m/3\rceil-1} \parallel b$. So we have $\operatorname{indeg}(\overline{0}) = 2^{2m-2\lceil m/3\rceil+1}$. □

Theorem 3.5. *Suppose* $p \equiv 1 \pmod 4$ *is a prime. Let* $\alpha \in \mathrm{D}(\mathbb{Z}_p[\mathrm{i}])$ *with* $\alpha \neq \overline{0}$. *If* $\operatorname{indeg}(\alpha) > 0$, *then*

$$\operatorname{indeg}(\alpha) = \begin{cases} 3, & p \equiv 1 \pmod{12}, \\ 1, & p \equiv 5 \pmod{12}. \end{cases}$$

Proof. Since $p \equiv 1 \pmod 4$, by Lemma 2.2 (3), $\mathbb{Z}_p[\mathrm{i}]$ is not local. Therefore, there exists $\alpha = \overline{c} + \overline{d}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_p[\mathrm{i}])$ and $\alpha \neq \overline{0}$ such that $\operatorname{indeg}(\alpha) > 0$. We readily see that $p \nmid c$ and $p \nmid d$. Let $\beta = \overline{a} + \overline{b}\mathrm{i}$ be such that $\beta^3 = \alpha$. Then we have

$$a^3 - 3ab^2 \equiv c \pmod{p}, \tag{3.6}$$

$$3a^2b - b^3 \equiv d \pmod{p}. \tag{3.7}$$

Since $p \mid a^2 + b^2$, by (3.6) and (3.7) we have $4a^3 \equiv c \pmod{p}$ and $4b^3 \equiv -d \pmod{p}$, i.e., $a^3 \equiv c_0 \pmod{p}$ and $b^3 \equiv d_0 \pmod{p}$ for some integers c_0 and d_0 because p is odd. By [3, p. 228, Theorem 8], each of the last two equations has precisely $\gcd(3, p-1)$ solutions. Therefore, if $p \equiv 2 \pmod 3$ then $\gcd(3, p-1) = 1$ and hence $\mathrm{indeg}(\alpha) = 1$. If $p \equiv 1 \pmod 3$ then $\gcd(3, p-1) = 3$ and we can claim $\mathrm{indeg}(\alpha) = 3$. In fact, assume that $a^3 - 3ab_1^2 \equiv a^3 - 3ab_2^2 \equiv c \pmod{p}$, then $b_1^2 \equiv b_2^2 \pmod{p}$. If $b_1 \equiv -b_2 \pmod{p}$, then it follows from $b_1^3 \equiv b_2^3 \equiv d_0 \pmod{p}$ that $d_0 \equiv -d_0 \pmod{p}$, i.e., $p \mid 2d_0$. Thus $p \mid d_0$, which is impossible. Therefore, $b_1 \equiv b_2 \pmod{p}$. So we can conclude that $\mathrm{indeg}(\alpha) = 3$ if $p \equiv 1 \pmod 3$. $\square$

For example, see Figure 2, where $n = 37$, $\mathrm{indeg}(\overline{0}) = 1$, while $\mathrm{indeg}(\alpha) = 3$ if $\alpha \in \mathrm{D}(\mathbb{Z}_{37}[\mathrm{i}])$, $\alpha \neq \overline{0}$ and $\mathrm{indeg}(\alpha) > 0$.

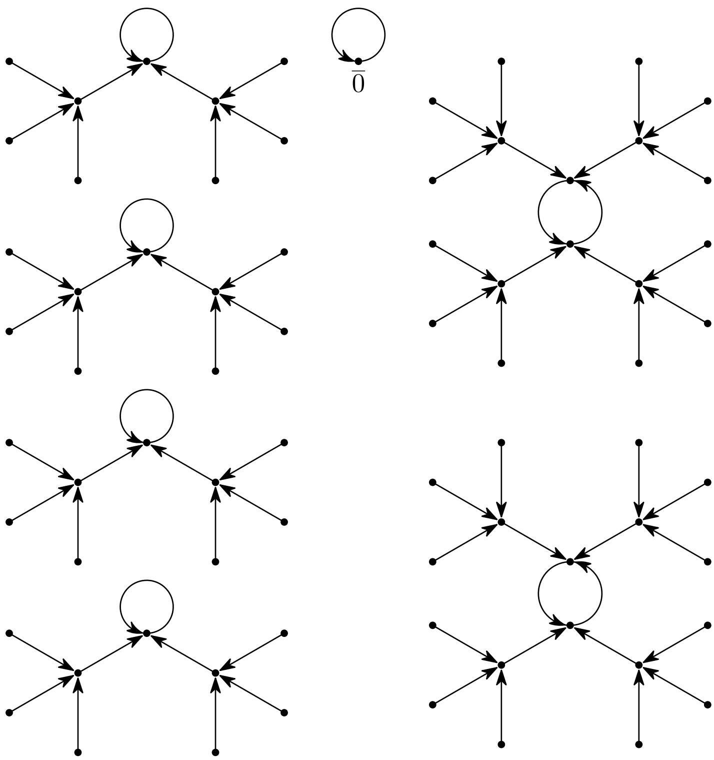

Figure 2. The subdigraph $\Gamma_2(37)$.

Theorem 3.6. *Let $n > 1$.*

(1) *The identity $\overline{1}$ is an isolated fixed point in $\Gamma(n)$ if and only if $n = 2^v 3^k \prod_{\lambda=1}^{l} g_\lambda^{\gamma_\lambda}$, where $v, l \geqslant 0$, $k = 0, 1$, $\gamma_\lambda \geqslant 1$, and $g_1 < \ldots < g_l$ are primes congruent to 5 modulo 12.*

(2) *The element $\overline{0}$ is an isolated fixed point in $\Gamma(n)$ if and only if n is odd and n is square-free.*

Proof. Since $\overline{1}$ or $\overline{0}$ is an isolated fixed point if and only if $\operatorname{indeg}(\overline{1}) = 1$ or $\operatorname{indeg}(\overline{0}) = 1$, the result follows by Theorem 3.3 or 3.4, respectively. □

Theorem 3.7. *Let $n > 1$.*

(1) *Each component in $\Gamma_1(n)$ is exactly a cycle if and only if $n = 2^v 3^k \prod_{\lambda=1}^{l} g_\lambda^{\gamma_\lambda}$, where $v, l \geqslant 0$, $k = 0, 1$, $\gamma_\lambda \geqslant 1$, and $g_1, \ldots, g_l$ are distinct primes congruent to 5 modulo 12.*

(2) *Each component in $\Gamma_2(n)$ is exactly a cycle if and only if $n = \prod_{s=1}^{m} p_s$, where $m \geqslant 1$, and $p_1, \ldots, p_m$ are distinct primes congruent to 3 modulo 4 or congruent to 5 modulo 12.*

(3) *Each component in $\Gamma(n)$ is exactly a cycle if and only if $n = 3^k \prod_{s=1}^{m} p_s$, where $k = 0, 1$, $m \geqslant 0$, and $p_1, \ldots, p_m$ are distinct primes congruent to 5 modulo 12.*

Proof. (1) By Theorem 3.2, each component in $\Gamma_1(n)$ is exactly a cycle if and only if $\overline{1}$ is an isolated fixed point. So by Theorem 3.6 (1), the result follows.

(2) On the one hand, suppose that each component in $\Gamma_2(n)$ is exactly a cycle. Then $\overline{0}$ is an isolated fixed point, hence n is odd and n is square-free due to Theorem 3.6 (2). First, let n be an odd prime, say p. If $p \equiv 3 \pmod 4$, then by Lemma 2.2 (4), $\mathbb{Z}_p[\mathrm{i}]$ is a field, hence $\overline{0}$ is the unique zero-divisor of $\mathbb{Z}_p[\mathrm{i}]$ and $\operatorname{Com}(\overline{0})$ is a cycle. If $p \equiv 1 \pmod 4$, by Theorem 3.5, then each component in $\Gamma_2(p)$ is exactly a cycle if and only if $p \equiv 5 \pmod{12}$. Secondly, let $n = \prod_{s=1}^{m} g_s$, where $g_1, \ldots, g_m$ are distinct odd primes, $m > 1$. By Lemma 2.4 and the above argument, we have that each component in $\Gamma_2(n)$ is exactly a cycle if and only if $g_1, \ldots, g_m$ are distinct primes congruent to 3 modulo 4 or congruent to 5 modulo 12, as desired.

(3) It follows directly from (1) and (2). □

It is easy to show that the following theorem holds.

Theorem 3.8. *Suppose $\alpha \in \mathrm{U}(\mathbb{Z}_n[\mathrm{i}])$. Then α is a vertex of a t-cycle if and only if $t = \operatorname{ord}_{o(\alpha)} 3$.*

Theorem 3.9. *Let $n > 1$.*

(1) *For $t > 1$, $A_t(\Gamma_1(n)) = 0$ if and only if $n = 2$.*

(2) *For $t > 1$, $A_t(\Gamma_2(n)) = 0$ if and only if $n = q^m$, where $m \geqslant 1$, $q = 2$ or q is a prime congruent to 3 modulo 4.*

Proof. (1) If $n = 2$, we readily see that each component of $\Gamma_1(n)$ is a 1-cycle. On the other hand, if $n > 2$, then $o(\mathrm{i}) = 4$. Hence, $\mathrm{ord}_{o(\mathrm{i})} 3 = 2$. By Theorem 3.8, i is a vertex of a 2-cycle.

(2) Suppose that $A_t(\Gamma_2(n)) = 0$ for $t > 1$. If n has at least two distinct prime factors, let $n = g^d n_1$, where g is an odd prime, $d \geqslant 1$, $g \nmid n_1$. Then clearly i is a vertex of a 2-cycle in $\Gamma_1(g^d)$. By the Chinese Remainder Theorem, there exists a positive integer b such that $b \equiv 1 \pmod{g^d}$ and $b \equiv 0 \pmod{n_1}$. Since $\overline{b}\mathrm{i}$ is equal to i in $\mathbb{Z}_{g^d}[\mathrm{i}]$ while $\overline{b}\mathrm{i}$ is equal to $\overline{0}$ in $\mathbb{Z}_{n_1}[\mathrm{i}]$, we have that $\alpha = \overline{b}\mathrm{i}$ is a vertex of a 2-cycle in $\Gamma_2(n)$. This is a contradiction. So we can conclude that if $A_t(\Gamma_2(n)) = 0$ for $t > 1$, then n must be a power of a prime.

Now let $n = p^m$, where p is a prime congruent to 1 modulo 4, $m \geqslant 1$. Let $p^m = 4k+1$ for some positive integer k. Then by [3, p. 211, Exercises 12], there exits a positive integer x such that $x^2 \equiv k \pmod{p^m}$. Set $\beta = \overline{x}+\overline{y}\mathrm{i}$, where $y = \frac{1}{2}(p^m+1)$. We can show that $x^2 + y^2 \equiv 0 \pmod{p^m}$, and by computation, we readily see that $\beta^3 \neq \beta$, while $\beta^{3^2} = \beta$. This implies that β is a vertex of a 2-cycle in $\Gamma_2(n)$.

Conversely, let n be a power of 2 or q, where q is a prime congruent to 3 modulo 4. Then by Lemma 2.2 (3), $\mathbb{Z}_n[\mathrm{i}]$ is local. It is not difficult to show that $\mathrm{Com}(\overline{0})$ is the unique component in $\Gamma_2(n)$. Hence, the result follows. □

4. The semiregularity of $\Gamma_2(n)$

By Theorem 3.2, we know that for $n > 1$, $\Gamma_1(n)$ is semiregular. Now, we study the semiregularity of $\Gamma_2(n)$. In the sequel we need the following lemma which is proved similarly to [9, Theorem 3.7].

Lemma 4.1. *Let $n = p_1^{t_1} \ldots p_s^{t_s}$, where $s > 1$, $p_1 < \ldots < p_s$ are distinct primes, $t_1, \ldots, t_s$ are positive integers. Then the following statements are equivalent:*

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

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

(3) *$\Gamma(p_j^{t_j})$ is semiregular for $j = 1, \ldots, s$.*

Theorem 4.2.

(1) *$\Gamma_2(2^m)$ is semiregular if and only if $m = 1, 2$.*

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

(3) *Suppose* p *is a prime congruent to* 7 *modulo* 12. *Then* $\Gamma_2(p^m)$ *is semiregular if and only if* $m = 1, 2, 3$.

(4) *Suppose* p *is a prime congruent to* 11 *modulo* 12. *Then* $\Gamma_2(p^m)$ *is semiregular if and only if* $m = 1, 2, 3, 4$.

(5) *Suppose* p *is a prime congruent to* 5 *modulo* 12. *Then* $\Gamma_2(p^m)$ *is semiregular if and only if* $m = 1$.

(6) *Suppose* p *is a prime congruent to* 1 *modulo* 12. *Then* $\Gamma_2(p^m)$ *is not semiregular for* $m \geqslant 1$.

(7) *Suppose* n *is not a power of a prime. Then* $\Gamma_2(n)$ *is semiregular if and only if* $n = 3^k \prod\limits_{j=1}^{m} p_j$, *where* $p_1, \ldots, p_m$ *are distinct primes congruent to* 5 *modulo* 12, $k = 0, 1, 2$ *and* $m \geqslant 1$.

Proof. (1) By inspection, it is easy to see that $\Gamma_2(2)$ and $\Gamma_2(2^2)$ are semiregular.

On the other hand, let $m > 2$. Clearly, $\operatorname{indeg}(\beta) > 0$ where $\beta = (\overline{1}+\mathrm{i})^3 = \overline{-2}+\overline{2}\mathrm{i} \in \mathbb{Z}_{2^m}[\mathrm{i}]$. Suppose $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{2^m}[\mathrm{i}])$ such that $\alpha^3 = \beta$. Then we have

$$a^3 - 3ab^2 \equiv -2 \pmod{2^m}, \tag{4.1}$$

$$3a^2b - b^3 \equiv 2 \pmod{2^m}. \tag{4.2}$$

It follows from (4.1) and (4.2) that both a and b are odd, $a^4 - b^4 \equiv 2(b-a) \pmod{2^m}$. Hence, $2^{m-1} \mid (b-a)[\frac{1}{2}(a^2+b^2)(a+b)+1]$. Since both a^2+b^2 and $a+b$ are even, we have $2 \nmid \frac{1}{2}(a^2+b^2)(a+b)+1$. Thus, $a \equiv b \pmod{2^{m-1}}$ and by (4.1), $a^3 \equiv 1 \pmod{2^{m-1}}$. The last equation has precisely one solution ([3, p. 192, Exercise 12 (i)]), namely, $a \equiv 1 \pmod{2^{m-1}}$. Similarly, we have $b \equiv 1 \pmod{2^{m-1}}$. Therefore, the solutions of system of (4.1) and (4.2) are $a \equiv 1, 2^{m-1}+1 \pmod{2^m}$ and $b \equiv 1, 2^{m-1}+1 \pmod{2^m}$. So $\operatorname{indeg}(\beta) = 4$. Moreover, by Theorem 3.4, $\operatorname{indeg}(\overline{0}) > 4$ in $\Gamma(2^m)$ when $m > 2$. Thus $\Gamma_2(2^m)$ is not semiregular for $m > 2$.

(2) If $m = 1, 2, 3, 4, 5$, by inspection, $\Gamma_2(3^m)$ is semiregular.

Now, let $p = 3$ and $m > 5$. Clearly, $\operatorname{indeg}(\overline{p^3}) > 0$. Suppose $\alpha = \overline{a}+\overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$ is such that $\alpha^3 = \overline{p^3}$. It is obvious that $p \mid a$ and $p \mid b$. Let $a = p^{t_1}a_1$, $b = p^{t_2}b_1$, where t_1 and t_2 are positive integers, $p \nmid a_1$ and $p \nmid b_1$. Then we have

$$p^{3t_1}a_1^3 - 3 \times p^{t_1}a_1 \times p^{2t_2}b_1^2 \equiv p^3 \pmod{p^m}, \tag{4.3}$$

$$3 \times p^{2t_1}a_1^2 \times p^{t_2}b_1 - p^{3t_2}b_1^3 \equiv 0 \pmod{p^m}. \tag{4.4}$$

If $t_1 > 1$, then by (4.3), $p^{3t_1-3}a_1^3 - 3p^{t_1+2t_2-3}a_1b_1^2 \equiv 1 \pmod{p^{m-3}}$, which is impossible. So $t_1 = 1$. Hence, by (4.4), we have

$$3p^{t_2+2}a_1^2 - p^{3t_2}b_1^2 \equiv 0 \pmod{p^m}. \tag{4.5}$$

Note that $p = 3$. Then if $t_2 = 1$, by (4.5) we have $3a_1^2 \equiv b_1^2 \pmod{3^{m-3}}$, which is impossible. Hence, $t_2 > 1$. Therefore, we derive from (4.5) that $3^m \mid 3^{t_2+3}$. So $t_2 \geqslant m-3$, i.e., $3^{m-3} \mid b$. It is easy to see that from 1 to 3^m, the number of multiples of 3^{m-3} is 3^3. In addition, since $m > 5$, we have $2t_2 + 2 - m \geqslant m - 4 > 0$. Thus, by (4.3), $3^3 a_1^3 \equiv 3^3 \pmod{3^m}$. Therefore, $a_1^3 \equiv 1 \pmod{3^{m-3}}$, and this equation has exactly 3 solutions. So $|\mathbb{A}| = 3^3$ when $p = 3$, where

$$\mathbb{A} = \{a\colon\ 1 \leqslant a \leqslant p^m,\ a = pa_1,\ a_1^3 \equiv 1 \pmod{p^{m-3}}\}. \tag{4.6}$$

Hence, $\operatorname{indeg}(\overline{3^3}) = 3^3 \times 3^3 = 3^6$. However, by Theorem 3.4, $\operatorname{indeg}(\overline{0}) > 3^6$ in $\Gamma(3^m)$ when $m > 5$. Thus $\Gamma_2(3^m)$ is not semiregular for $m > 5$.

(3) Since $p \equiv 7 \pmod{12}$, we have $p \equiv 3 \pmod 4$. If $m = 1, 2, 3$, by Lemma 2.3 (2) and Theorem 3.4 we readily show that $|\mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])| = \operatorname{indeg}(\overline{0})$. Therefore, $\Gamma_2(p^m)$ is semiregular for $m = 1, 2, 3$.

On the other hand, suppose $m > 3$. Clearly, $\operatorname{indeg}(\overline{p^3}) > 0$. Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$ be such that $\alpha^3 = \overline{p^3}$. By an argument similar to (2) above, we have $a = p^{t_1}a_1$, $b = p^{t_2}b_1$, where t_1 and t_2 are positive integers, $p \nmid a_1$ and $p \nmid b_1$. Then the equations (4.3) and (4.4) hold. Therefore, analogously, we derive $t_1 = 1$, $t_2 > 1$, $a_1^3 \equiv 1 \pmod{p^{m-3}}$ and by (4.5), $p^{m-2} \mid b$. Clearly, from 1 to p^m, the number of multiples of p^{m-2} is p^2. Moreover, since $p \equiv 7 \pmod{12}$, we have $p \equiv 1 \pmod 3$, and the equation $a_1^3 \equiv 1 \pmod{p^{m-3}}$ has exactly 3 solutions. So $|\mathbb{A}| = 3p^2$, and the set $\mathbb{A}$ is of the form (4.6). Hence, $\operatorname{indeg}(\overline{p^3}) = 3p^2 \times p^2 = 3p^4$. However, by Theorem 3.4, $\operatorname{indeg}(\overline{0}) \neq 3p^4$ in $\Gamma(p^m)$ when $m > 3$. Thus $\Gamma_2(p^m)$ is not semiregular for $m > 3$.

(4) Suppose $m > 4$. Since $p \equiv 11 \pmod{12}$, we have $p \equiv 2 \pmod 3$, and the equation $a_1^3 \equiv 1 \pmod{p^{m-3}}$ has exactly one solution. So $|\mathbb{A}| = p^2$, and the set $\mathbb{A}$ is of the form (4.6). Hence, by an argument similar to (3) above, $\operatorname{indeg}(\overline{p^3}) = p^2 \times p^2 = p^4$. Nevertheless, by Theorem 3.4, $\operatorname{indeg}(\overline{0}) > p^4$ in $\Gamma(p^m)$ for $m > 4$. Thus $\Gamma_2(3^m)$ is not semiregular for $m > 4$.

Now, suppose $m = 4$. Let

$$\mathbb{B} = \{p^3(\overline{x} + \overline{y}\mathrm{i})^3 \in \mathrm{D}(\mathbb{Z}_{p^4}[\mathrm{i}])\colon\ x, y = 0, 1, \ldots, p-1\}.$$

Obviously, $\operatorname{indeg}(\beta) > 0$ for $\beta \in \mathbb{B}$ and by an argument similar to the above, we have $\operatorname{indeg}(\beta) = \operatorname{indeg}(\overline{p^3}) = p^4$. It is not difficult to show that $|\mathbb{B}| = p^2$. Since $|\mathrm{D}(\mathbb{Z}_{p^4}[\mathrm{i}])| = p^6 = p^2 \times p^4$, we have $\operatorname{indeg}(\gamma) = 0$ whenever $\gamma \in \mathrm{D}(\mathbb{Z}_{p^4}[\mathrm{i}])$ but $\gamma \notin \mathbb{B}$. Hence, $\Gamma_2(p^4)$ is semiregular.

Finally, let $m = 1, 2, 3$. Since $p \equiv 11 \pmod{12}$, we have $p \equiv 3 \pmod 4$. By Lemma 2.3 (2) and Theorem 3.4, we readily show that $|\mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])| = \operatorname{indeg}(\overline{0})$. So $\Gamma_2(p^m)$ is semiregular for $m = 1, 2, 3$.

(5) On the one hand, since $p \equiv 5 \pmod{12}$, by Theorem 3.7 (2), each component of $\Gamma_2(p)$ is exactly a cycle. Therefore, $\Gamma_2(p)$ is semiregular.

On the other hand, suppose $m > 1$. Since $p \equiv 1 \pmod 4$, there exist positive integers x and y such that $p = x^2 + y^2$. Now let

$$\mathbb{C} = \{d^3(\overline{x} + \overline{y}\mathrm{i})^3 \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])\colon\ d = 0 \text{ or } d \in \mathrm{U}(\mathbb{Z}_{p^m})\}. \tag{4.7}$$

Obviously, for $\alpha \in \mathbb{C}$, $\operatorname{indeg}(\alpha) > 0$. If $d_1, d_2 \in \mathrm{U}(\mathbb{Z}_{p^m})$, then $d_1^3(\overline{x}+\overline{y}\mathrm{i})^3 = d_2^3(\overline{x}+\overline{y}\mathrm{i})^3$ if and only if $d_1^3 \equiv d_2^3 \pmod{p^m}$, if and only if $d_1 = d_2$. This is because $p \equiv 5 \pmod{12}$, so $p \equiv 2 \pmod 3$, and the equation $d^3 \equiv d_0 \pmod{p^m}$ has a unique solution. Hence $|\mathbb{C}| = \varphi(p^m) + 1 = p^m - p^{m-1} + 1$. If $\Gamma_2(p^m)$ is semiregular, then $\operatorname{indeg}(\alpha) = \operatorname{indeg}(\overline{0}) = p^{2(m-\lceil m/3 \rceil)}$ for $\alpha \in \mathbb{C}$. However, by Lemma 2.3 (3), $|\mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])| = 2p^{2m-1} - p^{2m-2}$ and clearly $|\mathbb{C}| \times \operatorname{indeg}(\overline{0}) > |\mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])|$ when $m > 1$, which is impossible. So $\Gamma_2(p^m)$ is not semiregular for $m > 1$.

(6) Since $p \equiv 1 \pmod{12}$, by Theorem 3.5, $\operatorname{indeg}(\alpha) = 3$ if $\operatorname{indeg}(\alpha) > 0$ for $\alpha \in \mathrm{D}(\mathbb{Z}_p[\mathrm{i}])$ and $\alpha \neq \overline{0}$. However, by Theorem 3.4, $\operatorname{indeg}(\overline{0}) = 1$ in $\Gamma(p)$. Therefore, $\Gamma_2(p)$ is not semiregular.

Now, suppose $m > 1$. Since $p \equiv 1 \pmod{12}$, we have $p \equiv 1 \pmod 3$, and the equation $d^3 \equiv d_0 \pmod{p^m}$ has precisely three solutions. Hence, $|\mathbb{C}| = \frac{1}{3}\varphi(p^m)+1 = \frac{1}{3}(p-1)p^{m-1} + 1$, and the set $\mathbb{C}$ is of the form (4.7). Then by an argument similar to (5), we derive that $\Gamma_2(p^m)$ is not semiregular for $m > 1$. Therefore, $\Gamma_2(p^m)$ is not semiregular for $m \geqslant 1$.

(7) By Theorem 3.3, Theorem 3.4 and the results above, we derive that if n is a power of a prime, then $\Gamma(n)$ is semiregular if and only if $n = 3, 3^2$, or n is a prime congruent to 5 modulo 12. Therefore, if n is not a power of a prime, then by Lemma 4.1 the result follows. $\square$

Corollary 4.3. *$\Gamma(n)$ is semiregular if and only if $n = 3^k \prod\limits_{j=1}^{m} p_j$, where $p_1, \ldots, p_m$ are distinct primes congruent to* 5 *modulo* 12, $k = 0, 1, 2$ *and* $m \geqslant 0$.

References

[1] *E. Abu Osba, M. Henriksen, O. Alkam, F. A. Smith*: The maximal regular ideal of some commutative rings. Commentat. Math. Univ. Carol. *47* (2006), 1–10.

[2] *J. Cross*: The Euler φ-function in the Gaussian integers. Am. Math. Mon. *90* (1983), 518–528.

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

[4] *J. Skowronek-Kaziów*: Properties of digraphs connected with some congruence relations. Czech. Math. J. *59* (2009), 39–49.

[5] *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.

[6] *L. Somer, M. Křížek*: On a connection of number theory with graph theory. Czech. Math. J. *54* (2004), 465–485.
[7] *H. D. Su, G. H. Tang*: The prime spectrum and zero-divisors of $\mathbb{Z}_n[\mathrm{i}]$. J. Guangxi Teach. Edu. Univ. *23* (2006), 1–4.
[8] *G. H. Tang, H. D. Su, Z. Yi*: The structure of the unit group of $\mathbb{Z}_n[\mathrm{i}]$. J. Guangxi Norm. Univ., Nat. Sci. *28* (2010), 38–41.
[9] *Y. J. Wei, J. Z. Nan, G. H. Tang, H. D. Su*: The cubic mapping graphs of the residue classes of integers. Ars Combin. *97* (2010), 101–110.

Authors' addresses: Y. J. Wei (corresponding author), J. Z. Nan, School of Mathematical Sciences, Dalian University of Technology, Dalian 116024, P. R. China, e-mail: `weiyangjiang2004@yahoo.com.cn`, `jznan@163.com`; G. H. Tang, School of Mathematical Sciences, Guangxi Teachers Education University, Nanning 530023, P. R. China, e-mail: `tanggaohua@163.com`.