Vol. 36 (2016)
No. 4

数 学 杂 志
J. of Math. (PRC)

THE SQUARE MAPPING GRAPHS OF THE RING $\mathbb{Z}_n[\mathbf{i}]$

WEI Yang-jiang, TANG Gao-hua

(*School of Mathematical Sciences, Guangxi Teachers Education University, Nanning 530023, China*)

Abstract: In this paper, we investigate some properties of the square mapping graphs $\Gamma(n)$ of $\mathbb{Z}_n[\mathbf{i}]$, the ring of Gaussian integers modulo n. Using the method of number theory, graph theory and group theory, we obtain the in-degree of $\overline{0}$ and $\overline{1}$. Moreover, we give the complete characterizations in terms of n in which $\Gamma_2(n)$ is semiregular, where $\Gamma_2(n)$ is induced by all the zero-divisors of $\mathbb{Z}_n[\mathbf{i}]$. The formulas on the heights of vertices in $\Gamma(n)$ are also obtained. This paper extends results concerning the square mapping graphs of $\mathbb{Z}_n$ given by Somer.

Keywords: Gaussian integers modulo n; semiregularity; height

2010 MR Subject Classification: 05C05; 11A07; 13F10

Document code: A **Article ID:** 0255-7797(2016)04-0676-07

1 Introduction

Finding the relationship between the algebraic structure of rings using properties of graphs associated to them became an interesting topic in the last years, for example, see [1–3]. In this paper, let $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ be the ring of integers modulo n, and $\mathbb{Z}_n[\mathbf{i}] = \{\overline{a} + \overline{b}\mathbf{i} \,|\, \overline{a}, \overline{b} \in \mathbb{Z}_n\}$ be the ring of Gaussian integers modulo n. We investigate some properties of the square mapping graphs $\Gamma(n)$, whose vertex set is all the elements of $\mathbb{Z}_n[\mathbf{i}]$, and for which there is a directed edge from $\alpha \in \mathbb{Z}_n[\mathbf{i}]$ to $\beta \in \mathbb{Z}_n[\mathbf{i}]$ if and only if $\alpha^2 = \beta$. In [1, 4, 5], some properties of the square mapping graphs of $\mathbb{Z}_n$ were investigated, and the cubic mapping graphs of $\mathbb{Z}_n[\mathbf{i}]$ were studied in [2].

Let R be a commutative ring, $\mathrm{U}(R)$ denotes 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., $\Gamma_1(n)$ is induced by all the vertices of $\mathrm{U}(\mathbb{Z}_n[\mathbf{i}])$, and $\Gamma_2(n)$ is induced by all the vertices of $\mathrm{D}(\mathbb{Z}_n[\mathbf{i}])$.

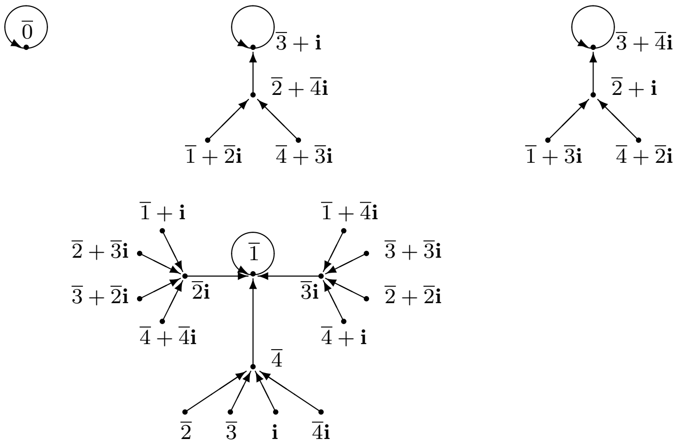
In $\Gamma(n)$, if $\alpha_1, \cdots, \alpha_t$ are pairwise distinct vertices and $\alpha_1^2 = \alpha_2, \cdots, \alpha_{t-1}^2 = \alpha_t$, $\alpha_t^2 = \alpha_1$, then the elements $\alpha_1, \alpha_2, \cdots, \alpha_t$ constitute a t-cycle. It is obvious that α is a vertex of a t-cycle if and only if t is the least positive integer such that $\alpha^{2^t} = \alpha$. For $\alpha \in \mathbb{Z}_n[\mathbf{i}]$, the in-degree $\mathrm{indeg}(\alpha)$ of α, denotes the number of directed edges coming into α.

* **Received date:** 2014-08-25 **Accepted date:** 2015-01-23

Foundation item: Supported by the National Natural Science Foundation of China (11161006; 11461010); the Guangxi Natural Science Foundation (2014GXNSFAA118005).

Biography: Wei Yangjiang (1969–), female, professor, born at Nanning, Guangxi, major in commutative algebra.

Example 1.1 The square mapping graph of $\mathbb{Z}_5[\mathbf{i}]$ is as follows.



The square mapping graph of $\mathbb{Z}_5[\mathbf{i}]$

Lemma 1.2 (see [6]) Let $n > 1$.

(1) The element $\overline{a}+\overline{b}\mathbf{i}$ is a unit of $\mathbb{Z}_n[\mathbf{i}]$ 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 $\mathbb{Z}_n[\mathbf{i}] \cong \oplus_{j=1}^{s}\mathbb{Z}_{p_j^{k_j}}[\mathbf{i}]$.

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

Lemma 1.3 (see [7])

(1) $|\mathrm{U}(\mathbb{Z}_{2^t}[\mathbf{i}])| = 2^{2t-1}$, $|\mathrm{D}(\mathbb{Z}_{2^t}[\mathbf{i}])| = 2^{2t-1}$.

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

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

By Lemma 1.2 (2), we have the following lemma concerning the in-degree of an arbitrary vertex in $\Gamma(n)$.

Lemma 1.4 Suppose $\alpha=\overline{a}+\overline{b}\mathbf{i} \in \mathbb{Z}_n[\mathbf{i}]$, and $n=\prod\limits_{j=1}^{s} p_j^{k_j}$ is the prime power decomposition of n. Then $\mathrm{indeg}(\alpha)=\mathrm{indeg}(\alpha_1)\times\cdots\times\mathrm{indeg}(\alpha_s)$, where $\alpha_j=(a \bmod p_j^{k_j})+(b \bmod p_j^{k_j})\mathbf{i}$ and $\mathrm{indeg}(\alpha_j)$ is the in-degree of α_j in $\Gamma(p_j^{k_j})$, $j=1,\cdots,s$.

2 In-Degree, Semiregularity, Height

By Lemma 1.4, in order to obtain the in-degree of a vertex in $\Gamma(n)$, it suffices to consider the cases of n being a power of a prime.

Theorem 2.5 (1) Let $n=2^k$, $k \geqslant 1$. Then $\mathrm{indeg}(\overline{0})=2^k$.

(2) Let $n=p^k$, where p is an odd prime, $k\geqslant 1$. Then $\operatorname{indeg}(\overline{0})=p^k$ if k is even, while $\operatorname{indeg}(\overline{0})=p^{k-1}$ if k is odd.

Proof (1) Let $n=2^k$. By inspection, we have $\operatorname{indeg}(\overline{0})=2^k$ for $k=1,2$. Now suppose $k\geqslant 3$. Assume that $\alpha=\overline{a}+\overline{b}\mathbf{i}\in\mathbb{Z}_{2^k}[\mathbf{i}]$ with $\alpha^2=\overline{0}$. Clearly $2|a$ and $2|b$. Let $a=2^u a_1$, $b=2^v b_1$, where u,v are positive integers, both a_1 and b_1 are odd. Set $\lambda=\min\{u,v\}$. Then $\alpha=2^\lambda\beta$, where $\beta=2^{u-\lambda}\overline{a_1}+2^{v-\lambda}\overline{b_1}\mathbf{i}$.

Suppose k is even. Clearly $\alpha^2=\overline{0}$ when $\lambda\geqslant\frac{k}{2}$, and $\alpha^2\neq\overline{0}$ when $\lambda\leqslant\frac{k}{2}-1$. Hence, $\alpha^2=\overline{0}$ if and only if $\alpha=2^{k/2}\,\overline{a}_0+2^{k/2}\,\overline{b}_0\mathbf{i}$ with $a_0,b_0\in\{0,1,2,\cdots,2^{k/2}-1\}$. Thus $\operatorname{indeg}(\overline{0})=2^{k/2}\times 2^{k/2}=2^k$.

Suppose k is odd. First, if $\lambda\geqslant\frac{k+1}{2}$, then clearly $\alpha^2=\overline{0}$. Second, if $\lambda=\frac{k-1}{2}$, then $\beta\in\mathrm{U}(\mathbb{Z}_{2^k}[\mathbf{i}])$ when $u\neq v$. Hence, $\alpha^2=2^{2\lambda}\beta^2\neq\overline{0}$. Otherwise, $\alpha^2=2^{2u+1}(\frac{\overline{a_1}^2-\overline{b_1}^2}{2}+\overline{a_1}\overline{b_1}\mathbf{i})=\overline{0}$ when $u=v=\lambda$. Third, if $\lambda\leqslant\frac{k-3}{2}$, then clearly $\alpha^2\neq 0$. Therefore, in the case of k odd, $\alpha^2=\overline{0}$ if and only if $\alpha=2^{(k+1)/2}\,\overline{a}_0+2^{(k+1)/2}\,\overline{b}_0\mathbf{i}$ with $a_0,b_0\in\{0,1,2,\cdots,2^{(k-1)/2}-1\}$, or $\alpha=2^{(k-1)/2}\,\overline{a}_0+2^{(k-1)/2}\,\overline{b}_0\mathbf{i}$ with $a_0,b_0\in\{1,3,5,\cdots,2^{(k+1)/2}-1\}$. Thus $\operatorname{indeg}(\overline{0})=2^{(k-1)/2}\times 2^{(k-1)/2}+2^{(k-1)/2}\times 2^{(k-1)/2}=2^k$.

(2) Let $n=p^k$, where p is an odd prime, $k\geqslant 1$. Suppose k is even, then by an argument similar to (1) above, $\alpha^2=\overline{0}$ if and only if $\alpha=p^{k/2}\,\overline{a}_0+p^{k/2}\,\overline{b}_0\mathbf{i}$ with $a_0,b_0\in\{0,1,2,\cdots,p^{k/2}-1\}$. Thus $\operatorname{indeg}(\overline{0})=p^{k/2}\times p^{k/2}=p^k$.

Suppose k is odd. If $\lambda\geqslant\frac{k+1}{2}$, then clearly $\alpha^2=\overline{0}$. If $\lambda\leqslant\frac{k-1}{2}$, then clearly $\alpha^2\neq\overline{0}$. Therefore, in the case of k odd, $\alpha^2=\overline{0}$ if and only if $\alpha=p^{(k+1)/2}\,\overline{a}_0+p^{(k+1)/2}\,\overline{b}_0\mathbf{i}$ with $a_0,b_0\in\{0,1,2,\cdots,p^{(k-1)/2}-1\}$. Hence, $\operatorname{indeg}(\overline{0})=p^{(k-1)/2}\times p^{(k-1)/2}=p^k$.

Theorem 2.6 (1) Let $n=2^k$, $k\geqslant 1$. Then $\operatorname{indeg}(\overline{1})=2^k$ for $k=1,2$, while $\operatorname{indeg}(\overline{1})=8$ for $k\geqslant 3$.

(2) Let $n=p^k$, where p is an odd prime, $k\geqslant 1$. Then $\operatorname{indeg}(\overline{1})=2$ if $p\equiv 3 \pmod 4$, while $\operatorname{indeg}(\overline{1})=4$ if $p\equiv 1 \pmod 4$.

Proof (1) Let $n=2^k$. By inspection, we have $\operatorname{indeg}(\overline{1})=2^k$ for $k=1,2$. Now suppose $k\geqslant 3$. Assume that $\alpha=\overline{a}+\overline{b}\mathbf{i}\in\mathbb{Z}_{2^k}[\mathbf{i}]$ with $\alpha^2=(\overline{a}^2-\overline{b}^2)+2\overline{a}\overline{b}\mathbf{i}=\overline{1}$. Clearly the parity of a and b is different. If a is even while $b=2t+1$ is odd, then $2^k|2ab$ if and only if $a=0$ or 2^{k-1}. However, $a^2-b^2-1\equiv -4t^2-4t-2\not\equiv 0 \pmod{2^k}$, which contradicts to the fact that $\alpha^2=\overline{1}$. So we must have a is odd and b is even. Then $2^k|2ab$ if and only if $b=0$ or 2^{k-1}. Hence $a^2-b^2\equiv 1 \pmod{2^k}$ if and only if $a^2\equiv 1 \pmod{2^k}$. The number of solutions of $a^2\equiv 1 \pmod{2^k}$ is 4 for $k\geqslant 3$. So we can conclude that $\operatorname{indeg}(\overline{1})=8$ for $k\geqslant 3$.

(2) Let $n=p^k$, where p is an odd prime, $k\geqslant 1$. Assume that $\alpha=\overline{a}+\overline{b}\mathbf{i}\in\mathbb{Z}_{p^k}[\mathbf{i}]$ with $\alpha^2=(\overline{a}^2-\overline{b}^2)+2\overline{a}\overline{b}\mathbf{i}=\overline{1}$. By Lemma 1.2(1), $\gcd(p,a^2+b^2)=1$. So $\gcd(p,a)=1$ or $\gcd(p,b)=1$. Therefore by $p^k|2ab$, we derive that $a=0$ or $b=0$. If $b=0$, then by $a^2-b^2\equiv 1 \pmod{p^k}$, we have $a^2\equiv 1 \pmod{p^k}$, which has exactly two solutions. If $a=0$, then by $a^2-b^2\equiv 1 \pmod{p^k}$, we have $b^2\equiv -1 \pmod{p^k}$, which has exactly two solutions when $p\equiv 1 \pmod 4$, while no solutions when $p\equiv 3 \pmod 4$, as claimed.

We call a digraph semiregular if there exists a positive integer d such that the in-degree of each vertex in this digraph is either d or 0. In Example 1.1, we see that $\Gamma_1(5)$ is semiregular.

In fact, $\Gamma_1(n)$ is semiregular for $n > 1$, by an argument similar to paper [8]. But $\Gamma_2(n)$ is not semiregular for some $n > 1$. For example, in $\Gamma_2(5)$, $\mathrm{indeg}(\overline{0}) = 1$ while $\mathrm{indeg}(\overline{3}+\mathbf{i}) = 2$.

Theorem 2.7 (1) $\Gamma_2(2^k)$ is semiregular if and only if $k = 1, 2, 3, 4$.

(2) Suppose p is a prime congruent to 1 modulo 4. Then $\Gamma_2(p^k)$ is not semiregular for $k \geqslant 1$.

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

Proof (1) By inspection, we readily show that $\Gamma_2(2^k)$ is semiregular for $k = 1, 2, 3, 4$. Now suppose $k \geqslant 5$. Let $\beta = (\overline{1}+\mathbf{i})^2 = \overline{2}\mathbf{i}$. Then $\mathrm{indeg}(\beta) > 0$. Let $\alpha = \overline{a} + \overline{b}\mathbf{i}$ such that $\alpha^2 = \beta$. Then $a^2 - b^2 \equiv 0 \pmod{2^k}$ and $2ab \equiv 2 \pmod{2^k}$. By $2ab \equiv 2 \pmod{2^k}$, we have $ab \equiv 1 \pmod{2^{k-1}}$ and hence $a^2b^2 \equiv 1 \pmod{2^{k-1}}$. Moreover, since $a^2 - b^2 \equiv 0 \pmod{2^k}$, clearly $a^2 \equiv b^2 \pmod{2^{k-1}}$. So $b^4 \equiv 1 \pmod{2^{k-1}}$, which has exactly 4 solutions, since $k \geqslant 5$. Hence, $b = b_j + m2^{k-1}$, where $j \in \{1, 2, 3, 4\}$, $m \in \{0, 1\}$ and $b_j^4 \equiv 1 \pmod{2^{k-1}}$ for $j = 1, 2, 3, 4$. For a fixed odd integer b, the congruence equation $ab \equiv 1 \pmod{2^{k-1}}$ in a has exactly one solution. Therefore $a = a_0 + m2^{k-1}$, where $m \in \{0, 1\}$ and $a_0 b \equiv 1 \pmod{2^{k-1}}$. So we can conclude that $\mathrm{indeg}(\beta) = 16$. However, by Theorem 2.5, $\mathrm{indeg}(\overline{0}) = 2^k > 16$ for $k \geqslant 5$. So $\Gamma_2(2^k)$ is not semiregular for $k \geqslant 5$.

(2) First, by Theorem 2.5, $\mathrm{indeg}(\overline{0}) = 1$ in $\Gamma(p)$. However, the in-degree of $\beta = (\overline{x}+\overline{y}\mathbf{i})^2 \in \mathrm{D}(\mathbb{Z}_p[\mathbf{i}])$ is greater than 1 where $p = x^2 + y^2$, since $(\pm\beta)^2 = \beta$. Hence $\Gamma_2(p)$ is not semiregular. Second, let $A = \{d^2(\overline{x}+\overline{y}\mathbf{i})^2 : \ d \in \mathrm{U}(\mathbb{Z}_{p^2}) \text{ or } d = 0\}$. Then $\mathrm{indeg}(\gamma) > 0$ for $\gamma \in A$. Moreover, since $(\pm d)^2 = d^2$, one can derive that $|A| = \frac{1}{2}|\mathrm{U}(\mathbb{Z}_{p^2})| + 1 = \frac{1}{2}p^2 - \frac{1}{2}p + 1$. If $\Gamma_2(p^2)$ is semiregular, then for $\gamma \in A$, $\mathrm{indeg}(\gamma) = \mathrm{indeg}(\overline{0}) = p^2$ by Theorem 2.5. But one can easily check that $p^2|A| > |\mathrm{D}(\mathbb{Z}_{p^2}[\mathbf{i}])|$, which is impossible. So $\Gamma_2(p^2)$ is not semiregular.

Now, suppose $k \geqslant 3$. Let $\beta = \overline{p}^2 \in \mathrm{D}(\mathbb{Z}_{p^k}[\mathbf{i}])$. Then $\mathrm{indeg}(\beta) > 0$. Assume that $\alpha = \overline{a} + \overline{b}\mathbf{i}$ such that $\alpha^2 = \beta$. Then $a^2 - b^2 \equiv p^2 \pmod{p^k}$ and $2ab \equiv 0 \pmod{p^k}$. It is clear that $p|a$ and $p|b$. Moreover, since $a^2 - b^2 \equiv p^2 \pmod{p^k}$, one can derive that $p \parallel a$ or $p \parallel b$. If $p \parallel a$, then by $2ab \equiv 0 \pmod{p^k}$, we have $b \equiv 0 \pmod{p^{k-1}}$. Hence $b = p^{k-1}b_1$ with $b_1 = 0, 1, \cdots, p-1$. Furthermore, since $a^2 - b^2 \equiv p^2 \pmod{p^k}$, we derive that $a^2 \equiv p^2 \pmod{p^k}$. Therefore, $a = p(mp^{k-2} \pm 1)$ with $m = 0, 1, \cdots, p-1$.

On the other hand, if $p \parallel b$, by an argument similar to above, we have $a = p^{k-1}a_1$ with $a_1 = 0, 1, \cdots, p-1$ and $b = p(mp^{k-2} \pm 1)$ with $m = 0, 1, \cdots, p-1$. Therefore, $\mathrm{indeg}(\beta) = 2p^2 + 2p^2 = 4p^2$. However, by Theorem 2.5, the in-degree of $\overline{0}$ in $\Gamma(p^k)$ is not equal to $4p^2$. So $\Gamma_2(p^k)$ is not semiregular for $k \geqslant 3$.

(3) First, by Lemma 1.2 (4), $\mathbb{Z}_p[\mathbf{i}]$ is a field when $p \equiv 3 \pmod 4$. So $\Gamma_2(p)$ is a 1-cycle and hence is semiregular. Second, by Lemma 1.3 (2), $|\mathrm{D}(\mathbb{Z}_{p^2}[\mathbf{i}])| = p^2 = \mathrm{indeg}(\overline{0})$, which implies that $\alpha^2 = \overline{0}$ for $\alpha \in \mathrm{D}(\mathbb{Z}_{p^2}[\mathbf{i}])$. So $\Gamma_2(p^2)$ is semiregular.

Now, suppose $k \geqslant 3$. Let $\beta = \overline{p}^2 \in \mathrm{D}(\mathbb{Z}_{p^k}[\mathbf{i}])$. Then $\mathrm{indeg}(\beta) > 0$. Assume that $\alpha = \overline{a} + \overline{b}\mathbf{i}$ such that $\alpha^2 = \beta$. Similarly to (2) above, we have $p|a$ and $p|b$, and furthermore, $p \parallel a$ or $p \parallel b$. If $p \parallel b$, then $p^2|a$. Let $a = p^t a_1$, while $b = pb_1$, where $t \geqslant 2$ and $p \nmid b_1$. Then by $\alpha^2 = \beta$, we derive $a^2 - b^2 \equiv p^2 \pmod{p^k}$. Hence, $2t-2 \geqslant 2$ and $p^{2t-2}a_1^2 \equiv b_1^2 + 1 \pmod{p^{k-2}}$, which contradicts to the fact that $b_1^2+1\not\equiv 0 \pmod p$ for any integer b_1, since $p\equiv 3 \pmod 4$. So we must have $p \parallel a$ and hence, by an argument similar to (2) above, we can conclude that $\mathrm{indeg}(\beta)=2p^2\neq \mathrm{indeg}(\overline{0})$. Therefore, $\Gamma_2(p^k)$ is not semiregular for $k\geqslant 3$.

We have observed that α is a vertex of a t-cycle if and only if t is the least positive integer such that $\alpha^{2^t}=\alpha$. So it is easy to derive the following

Lemma 2.8 (1) $\alpha\in \mathrm{U}(\mathbb{Z}_n[\mathbf{i}])$ is a cycle vertex in $\Gamma_1(n)$ if and only if $2\nmid o(\alpha)$.

(2) $\alpha\in \mathrm{U}(\mathbb{Z}_n[\mathbf{i}])$ is a vertex of a t-cycle in $\Gamma_1(n)$ if and only if $t=\mathrm{ord}_{o(\alpha)}2$.

Let $\alpha=\overline{a}+\overline{b}\mathbf{i}\in\mathbb{Z}_n[\mathbf{i}]$, the norm $N(\alpha)$ of α is defined by $1\leqslant N(\alpha)\leqslant n$ and $N(\alpha)\equiv a^2+b^2 \pmod n$. It is easy to check that $N(\alpha\beta)\equiv N(\alpha)N(\beta) \pmod n$. If α is a vertex of a t-cycle, then $\alpha^{2^t}=\alpha$. So $N(\alpha)^{2^t}\equiv N(\alpha^{2^t})\equiv N(\alpha) \pmod n$, i.e., $N(\alpha)(N(\alpha)^{2^t-1})\equiv 0 \pmod n$. Since $\gcd(N(\alpha),N(\alpha)^{2^t-1})=1$, if $p|N(\alpha)$ with $p^t\parallel n$, clearly $p^t|N(\alpha)$. So we have proved the following lemma.

Lemma 2.9 Let $n=\prod\limits_{j=1}^{s}p_j^{k_j}$ be the prime power decomposition of n. If α is a vertex of a t-cycle, then $p_j^{k_j}\mid N(\alpha)$ whenever $p_j\mid N(\alpha)$.

By Lemma 1.2 (3), $\mathbb{Z}_n[\mathbf{i}]$ is a local ring if $n=p^t$, where $p=2$ or p is a prime congruent to 3 modulo 4, $t\geqslant 1$. It is easy to show that $\Gamma_2(n)$ has a unique component containing the 1-cycle with $\overline{0}$ as its only vertex if $\mathbb{Z}_n[\mathbf{i}]$ is a local ring. For the cycle vertices in $\Gamma_2(p^k)$ with p is a prime congruent to 1 modulo 4, we have the following theorem.

Theorem 2.10 Let p be a prime congruent to 1 modulo 4. Then $\alpha=\overline{a}+\overline{b}\mathbf{i}\neq\overline{0}$ lies on a t-cycle of $\Gamma_2(p^k)$ if and only if $p^k|N(\alpha)$ and $\overline{2a}$ lies on a t-cycle of $\Gamma_1(p^k)$.

Proof Suppose that α is a vertex of a t-cycle in $\Gamma_2(p^k)$, then $p|N(\alpha)$. By Lemma 2.9, $p^k|N(\alpha)$. Moreover, since $\alpha\neq\overline{0}$, it is easy to check that $p\nmid a$ and $p\nmid b$. So by $\alpha^2=(\overline{a}^2-\overline{b}^2)+2\overline{a}\overline{b}\mathbf{i}$ and $-b^2\equiv a^2 \pmod{p^k}$, we have $\alpha^2=\overline{2a}(\overline{a}+\overline{b}\mathbf{i})$. Therefore we can conclude that $\alpha^{2^t}=\overline{2a}^{2^t-1}(\overline{a}+\overline{b}\mathbf{i})$. Hence t is the least positive integer such that $(2a)^{2^t-1}\equiv 1 \pmod{p^k}$. Thus due to Lemma 2.8, $\overline{2a}$ lies on a t-cycle of $\Gamma_1(p^k)$.

Conversely, if $p^k|N(\alpha)$ and $\overline{2a}$ lies on a t-cycle of $\Gamma_1(p^k)$, then $\alpha^2=(\overline{a}^2-\overline{b}^2)+2\overline{a}\overline{b}\mathbf{i}=\overline{2a}(\overline{a}+\overline{b}\mathbf{i})$. Hence $\alpha^{2^t}=\overline{2a}^{2^t-1}(\overline{a}+\overline{b}\mathbf{i})$. Furthermore, since t is the least positive integer such that $(2a)^{2^t-1}\equiv 1 \pmod{p^k}$, we can claim that t is the least positive integer such that $\alpha^{2^t}=\alpha$, which implies that α is a vertex of a t-cycle in $\Gamma_2(p^k)$.

For instance, $\overline{3}+\mathbf{i}$ lies on a 1-cycle of $\Gamma_2(5)$ (see Example 1.1), $2\times 3\equiv 1 \pmod 5$ and $\overline{1}$ lies on a 1-cycle of $\Gamma_1(5)$. If $n=5^2$, one can check that $\alpha=\overline{8}+\overline{6}\mathbf{i}$ lies on a 4-cycle of $\Gamma_2(5^2)$, i.e., the cycle $\overline{8}+\overline{6}\mathbf{i}\to\overline{3}+\overline{21}\mathbf{i}\to\overline{18}+\mathbf{i}\to\overline{23}+\overline{11}\mathbf{i}\to\overline{8}+\overline{6}\mathbf{i}$. While $\overline{16}$ lies on a 4-cycle of $\Gamma_1(5^2)$, i.e., the cycle $\overline{16}\to\overline{6}\to\overline{11}\to\overline{21}\to\overline{16}$.

Finally, we investigate the height of an arbitrary vertex of $\Gamma_2(p^k)$ for any prime p. We say a vertex α in $\Gamma(n)$ is of height m if m is the least nonnegative integer such that α^{2^m} is a vertex of a cycle, and we denote $h_\alpha=m$. Clearly, $h_\alpha=0$ if and only if α is a vertex of a cycle.

Theorem 2.11 Suppose $\alpha=\overline{a}+\overline{b}\mathbf{i}\in \mathrm{D}(\mathbb{Z}_{2^k}[\mathbf{i}])$, $k\geqslant 1$. Then the height h_α of α is

$$h_\alpha=\begin{cases}\lceil\log_2\frac{k}{\lambda}\rceil, & 2^x\parallel a,\ 2^y\parallel b,\ x\neq y,\ \lambda=\min\{x,y\}\geqslant 1,\\ \lceil\log_2\frac{2k}{2\lambda+1}\rceil, & 2^\lambda\parallel a,\ 2^\lambda\parallel b,\ \lambda\geqslant 0.\end{cases}$$

Proof Suppose that $2^x\parallel a$, $2^y\parallel b$, $\lambda=\min\{x,y\}$. Then $\alpha=2^\lambda\beta$, where $\beta=\overline{a_1}+\overline{b_1}\mathbf{i}$ with $2\nmid\gcd(a_1,b_1)$.

If $x\neq y$, then $\lambda\geqslant 1$, and $\beta^{2^j}\in \mathrm{U}(\mathbb{Z}_{2^k}[\mathbf{i}])$ for $j\geqslant 0$. Hence $\alpha^{2^j}=(2^\lambda)^{2^j}\beta^{2^j}=\overline{0}$ if and only if $2^j\lambda\geqslant k$, if and only if $j\geqslant\log_2\frac{k}{\lambda}$. So $h_\alpha=\lceil\log_2\frac{k}{\lambda}\rceil$.

If $x=y=\lambda\geqslant 0$, then $\alpha=2^\lambda\beta$ with both a_1 and b_1 are odd. Thus $\beta\in \mathrm{D}(\mathbb{Z}_{2^k}[\mathbf{i}])$. Let $\beta^2=2\gamma$ where $\gamma=\frac{1}{2}(\overline{a_1}^2-\overline{b_1}^2)+\overline{a_1}\overline{b_1}\mathbf{i}$. Then clearly $\gamma\in \mathrm{U}(\mathbb{Z}_{2^k}[\mathbf{i}])$ since $4|a_1^2-b_1^2$. Hence, $\alpha^{2^j}=(2^\lambda)^{2^j}\beta^{2^j}=2^{2^j\lambda}(2\gamma)^{2^{j-1}}=2^{2^j\lambda+2^{j-1}}\gamma^{2^{j-1}}$. So $\alpha^{2^j}=\overline{0}$ if and only if $2^j\lambda+2^{j-1}\geqslant k$, if and only if $j\geqslant\log_2\frac{2k}{2\lambda+1}$. So $h_\alpha=\lceil\log_2\frac{2k}{2\lambda+1}\rceil$.

Theorem 2.12 Suppose $\alpha=\overline{a}+\overline{b}\mathbf{i}\in \mathrm{D}(\mathbb{Z}_{p^k}[\mathbf{i}])$, where p is a prime congruent to 3 modulo 4, $k\geqslant 1$. Then the height h_α of α is $h_\alpha=\lceil\log_2\frac{k}{\lambda}\rceil$, where $p^x\parallel a$, $p^y\parallel b$ and $\lambda=\min\{x,y\}\geqslant 1$.

Proof Since $p\equiv 3 \pmod 4$, $\alpha\in \mathrm{D}(\mathbb{Z}_{p^k}[\mathbf{i}])$ if and only if $p|a$ and $p|b$. Let $p^x\parallel a$, $p^y\parallel b$ and $\lambda=\min\{x,y\}\geqslant 1$. Then $\alpha=p^\lambda\beta$, where $\beta=\overline{a}_1+\overline{b}_1\mathbf{i}$ and $p\nmid\gcd(a_1,b_1)$. Hence $\beta\in \mathrm{U}(\mathbb{Z}_{p^k}[\mathbf{i}])$. So $\alpha^{2^j}=(p^\lambda)^{2^j}\beta^{2^j}=\overline{0}$ if and only if $2^j\lambda\geqslant k$, if and only if $j\geqslant\log_2\frac{k}{\lambda}$. So $h_\alpha=\lceil\log_2\frac{k}{\lambda}\rceil$.

Theorem 2.13 Suppose $\alpha=\overline{a}+\overline{b}\mathbf{i}\in \mathrm{D}(\mathbb{Z}_{p^k}[\mathbf{i}])$, where p is a prime congruent to 1 modulo 4, $k\geqslant 1$. Then the height h_α of α is

$$h_\alpha=\begin{cases}\lceil\log_2\frac{k}{\lambda}\rceil, & p^x\parallel a,\ p^y\parallel b,\ k=\min\{x,y\}\geqslant 1,\\ j, & p\nmid a, p\nmid b,\ \text{and } j \text{ is the least nonnegative integer}\\ & \text{such that both } p^k\mid(N(\alpha))^{2^j} \text{ and } 2\nmid o(2\mathrm{Re}(\alpha^{2^j})),\end{cases}$$

where $\mathrm{Re}(\gamma)=\overline{c}$ if $\gamma=\overline{c}+\overline{d}\mathbf{i}$.

Proof Since $p\equiv 1 \pmod 4$, $\alpha=\overline{a}+\overline{b}\mathbf{i}\in \mathrm{D}(\mathbb{Z}_{p^k}[\mathbf{i}])$ if and only if $p|a^2+b^2$.

First, suppose $p|\gcd(a,b)$. Let $p^x\parallel a$, $p^y\parallel b$, where $x\geqslant 1$ and $y\geqslant 1$. Let $\lambda=\min\{x,y\}$. Then $\alpha=p^\lambda\beta$, where $\beta=\overline{a}_0+\overline{b}_0\mathbf{i}$ with $p\nmid\gcd(a_0,b_0)$. Hence, $\alpha^{2^j}=\overline{0}$ for some $j\geqslant 1$. Now, suppose that $\alpha^2=p^{2\lambda}(\overline{a}_1+\overline{b}_1\mathbf{i})$, where $\overline{a_1}=\overline{a_0}^2-\overline{b_0}^2$ and $\overline{b_1}=2\overline{a_0}\overline{b_0}$. Then, clearly $p\nmid\gcd(a_1,b_1)$ since $p\nmid\gcd(a_0,b_0)$. So we can conclude that $\alpha^{2^j}=p^{2^j\lambda}(\overline{a}_j+\overline{b}_j\mathbf{i})$ with $p\nmid\gcd(a_j,b_j)$. Therefore $\alpha^{2^j}=\overline{0}$ if and only if $2^j\lambda\geqslant k$, if and only if $j\geqslant\log_2\frac{k}{\lambda}$. So $h_\alpha=\lceil\log_2\frac{k}{\lambda}\rceil$.

Second, suppose $p|a^2+b^2$ but $p\nmid\gcd(a,b)$. Then $\alpha^{2^j}\neq\overline{0}$ for any $j\geqslant 0$. It is easy to show that if $\alpha^{2^j}=\overline{c}+\overline{d}\mathbf{i}$, then $p\nmid\gcd(c,d)$. Moreover, by Theorem 2.10 and Lemma 2.8, α^{2^j} lies on a t-cycle of $\Gamma_2(p^k)$ if and only if $p^k|N(\alpha)^{2^j}$ and $\overline{2c}$ lies on a t-cycle of $\Gamma_1(p^k)$, if and only if j is the least nonnegative integer such that both $p^k|N(\alpha)^{2^j}$ and $\mathrm{ord}_{o(\overline{2c})}2=t$, if and only if j is the least nonnegative integer such that both $p^k|N(\alpha)^{2^j}$ and $2\nmid o(\overline{2c})$. Hence the result follows.

References

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

[2] Wei Yangjiang, Nan Jizhu, Tang Gaohua. The cubic mapping graph for the ring of Gaussian integers modulo n[J]. Czech. Math. J., 2011, 61: 1023–1036.

[3] Xu Chengjie, Yi Zhong, Zheng Ying. On the zero-divisor graphs of formal triangular matrix rigns[J]. J. Math., 2013, 33(5): 891–901.

[4] Somer L, Křížek M. Structure of digraphs associated with quadratic congruences with composite moduli[J]. Discrete Math., 2006, 36: 2174–2185.

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

[6] Su Huadong, Tang Gaohua. The prime spectrum and zero-divisors of $\mathbb{Z}_n[\mathbf{i}]$[J]. J. Guangxi Teach. Edu. Univ., 2006, 23(4): 1–4.

[7] Tang Gaohua, Su Huadong, Yi Zhong. The structure of the unit group of $\mathbb{Z}_n[\mathbf{i}]$[J]. J. Guangxi Nor. Univ., 2010, 28(2): 38–41.

[8] Sha Min. Digraphs from endomorphisms of finite cyclic groups [DB]. J. Combin. Math. Combin. Comp., 2011.

$\mathbb{Z}_n[\mathbf{i}]$ 的平方映射图

韦扬江, 唐高华

(广西师范学院数学与统计学院, 广西 南宁 530023)

摘要: 本文研究了模 n 高斯整数环 $\mathbb{Z}_n[\mathbf{i}]$ 的平方映射图 $\Gamma(n)$. 利用数论、图论与群论等方法, 获得了 $\Gamma(n)$ 中顶点 $\bar{0}$ 及 $\bar{1}$ 的入度, 并研究了 $\Gamma(n)$ 的零因子子图的半正则性. 同时, 获得了 $\Gamma(n)$ 中顶点的高度公式. 推广了 Somer 等人给出的模 n 剩余类环平方映射图的相关结论.

关键词: 模 n 高斯整数环; 半正则性; 高度

MR(2010)**主题分类号**: 05C05; 11A07; 13F10 **中图分类号**: O153.3; O156.1; O157.5