Indian J. Pure Appl. Math., **42**(5): 387-402, October 2011

THE COMMUTING GRAPHS OF SOME SUBSETS IN THE QUATERNION ALGEBRA OVER THE RING OF INTEGERS MODULO N

Yangjiang Wei, Gaohua Tang and Huadong Su

School of Mathematical Sciences, Guangxi Teachers Education University, Nanning, 530023, *Peoples' Republic of China*
e-mails: weiyangjiang2004@yahoo.com.cn; tanggaohua@163.com

(*Received* 26 *March* 2010; *after final revision* 2 *September* 2011; *accepted* 18 *September* 2011)

Let R be an arbitrary ring, S be a subset of R, and $Z(S) = \{s \in S \mid sx = xs \ for\, every\, x \in S\}$. The commuting graph of S, denoted by $\Gamma(S)$, is the graph with vertex set $S \setminus Z(S)$ such that two different vertices x and y are adjacent if and only if $xy = yx$. In this paper, let $\mathcal{I}_n, \mathcal{N}_n$ be the sets of all idempotents, nilpotent elements in the quaternion algebra $\mathbb{Z}_n[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, respectively. We completely determine $\Gamma(\mathcal{I}_n)$ and $\Gamma(\mathcal{N}_n)$. Moreover, it is proved that for $n \geqslant 2$, $\Gamma(\mathcal{I}_n)$ is connected if and only if n has at least two odd prime factors, while $\Gamma(\mathcal{N}_n)$ is connected if and only if $n \neq 2, 2^2, p, 2p$ for all odd primes p.

Key words : Commuting graph, quaternion algebra, connected component.

1. INTRODUCTION

There are many papers on investigating connections between ring theory and graph theory (see [1-4]). Let R be an arbitrary ring, S be a subset of R, and $Z(S) = \{s \in S \mid sx = xs \ for\, every\, x \in S\}$. The commuting graph of S, denoted by $\Gamma(S)$, is

the graph with vertex set $S \setminus Z(S)$ such that two different vertices x and y are adjacent if and only if $xy = yx$. In this paper, we study the connections among quaternion theory, number theory and graph theory by the commuting graphs of the quaternion algebra over $\mathbb{Z}_n$, the ring of integers modulo n.

Recall that the quaternion ring $\mathrm{H}_n = \{\overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \,|\, \overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{Z}_n\}$ is an algebra over $\mathbb{Z}_n$, where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are formal symbols called basic units defined by $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$. Recall that the commuting graphs of H_n has been investigated in [9]. For an element $\alpha = \overline{a}+\overline{b}\mathbf{i}+\overline{c}\mathbf{j}+\overline{d}\mathbf{k} \in \mathrm{H}_n$, $\overline{\alpha} = \overline{a}-\overline{b}\mathbf{i}-\overline{c}\mathbf{j}-\overline{d}\mathbf{k}$ is called the conjugate of α, and $N(\alpha) = \overline{a}^{\,2}+\overline{b}^{\,2}+\overline{c}^{\,2}+\overline{d}^{\,2}$ is said to be the norm of α. For any subset X of a ring R, we define $X^* = X \setminus \{0\}$, and $|X|$ denotes the cardinality of X. The set of all zero-divisors in a ring R is denoted by $D(R)$, and the group of units of R is denoted by $U(R)$. Let $p > 2$ be a prime, we define the Legendre symbol $\left(\frac{b}{p}\right)$ to equal $0, 1$ or -1, as follows:

$$\left(\frac{b}{p}\right) = \begin{cases} 0, & if\ p|b; \\ 1, & if\ b\ is\ a\ quadratic\ residue\ mod\ p; \\ -1, & if\ b\ is\ a\ nonresidue\ mod\ p. \end{cases}$$

For a connected graph G, the diameter of G is denoted by $diam(G)$. The degree of a vertex v of G is the number of edges incident to v and is denoted by $d(v)$. A $path$ of length r from a vertex x to a vertex y in G is a sequence of $r + 1$ different vertices starting with x and ending with y such that consecutive vertices are adjacent. An induced subgraph of G that is maximal, subject to being connected, is called a $connected\ component$ of G.

In this paper, let $\mathcal{I}_n, \mathcal{N}_n$ be the sets of all idempotents, nilpotent elements in H_n, respectively. We completely determine $\Gamma(\mathcal{I}_n)$ and $\Gamma(\mathcal{N}_n)$. It is proved that for $n \geqslant 2$, $\Gamma(\mathcal{I}_n)$ is connected if and only if n has at least two odd prime factors, while $\Gamma(\mathcal{N}_n)$ is connected if and only if $n \neq 2, 2^2, p, 2p$ for all odd primes p.

2. LEMMAS

Lemma 2.1 [6, p.161, Exercise 12] — The number of solutions of congruence equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b \pmod{m}$$

in $x_1, \ldots, x_k$, where $a_1, \ldots, a_k, b, m$ $(m \geqslant 2)$ are integers, is equal to m^{k-1} $gcd(a_1, a_2, \ldots, a_k, m)$ if $gcd(a_1, a_2, \ldots, a_k, m)|b$.

Lemma 2.2 [6, p.443, Example 4] — Suppose that p is a prime, $r \geqslant 1$ and a are integers. Let $T(r, a)$ denote the number of solutions of congruence equation

$$x_1^2 + \cdots + x_r^2 \equiv a \pmod{p} \tag{2-1}$$

Then

$$T(r,a) = \begin{cases} p^{r-1} + (p-1)p^{\frac{r}{2}-1}, & p|a, 2|r,\ p \equiv 1 \pmod 4 \\ p^{r-1} + (-1)^{\frac{r}{2}}(p-1)p^{\frac{r}{2}-1}, & p|a, 2|r,\ p \equiv 3 \pmod 4 \\ p^{r-1}, & p|a, 2 \nmid r \\ p^{r-1} - p^{\frac{r}{2}-1}, & p \nmid a, 2|r,\ p \equiv 1 \pmod 4 \\ p^{r-1} - (-1)^{\frac{r}{2}}p^{\frac{r}{2}-1}, & p \nmid a, 2|r,\ p \equiv 3 \pmod 4 \\ p^{r-1} + \left(\frac{a}{p}\right)p^{\frac{r-1}{2}}, & p \nmid a, 2 \nmid r,\ p \equiv 1 \pmod 4 \\ p^{r-1} - (-1)^{\frac{r+1}{2}}\left(\frac{a}{p}\right)p^{\frac{r-1}{2}}, & p \nmid a, 2 \nmid r,\ p \equiv 3 \pmod 4 \end{cases}$$

Lemma 2.3 — Suppose that p is an odd prime, r, a, t are integers and $p \nmid a$, $r \geqslant 1, t \geqslant 2$. Let T be the number of solutions of (2-1), then the number of solutions of the congruence equation

$$x_1^2 + \cdots + x_r^2 \equiv a \pmod{p^t} \tag{2-2}$$

is equal to $p^{(r-1)(t-1)}T$.

PROOF : It is clear that if $x_1^2 + \cdots + x_r^2 \equiv a \pmod{p^m}$, then $x_1^2 + \cdots + x_r^2 \equiv a \pmod{p^n}$ for $1 \leqslant n \leqslant m$.

First assume that $t = 2$. Suppose $a_1^2 + \cdots + a_r^2 \equiv a \pmod{p}$. Note that $p \nmid a$, so at least one of $a_1, \ldots, a_r$ is not equal to 0 modulo p. Let X be the number of solutions of

$$(a_1 + pb_1)^2 + \cdots + (a_r + pb_r)^2 \equiv a \pmod{p^2} \tag{2-3}$$

in $b_1, \ldots, b_r$ where $b_\lambda \equiv g_\lambda \pmod{p^2}$, $0 \leqslant g_\lambda \leqslant p-1$ for $\lambda = 1, \ldots, r$. Then the number of solutions of (2-2) is equal to TX.

By (2-3), we have

$$2a_1b_1 + \cdots + 2a_rb_r \equiv m_1 \pmod{p} \tag{2-4}$$

where $a - (a_1^2 + \cdots + a_r^2) = m_1 p$. Observe that $gcd(2a_1, \ldots, 2a_r, p) = 1$, by Lemma 2.1, the number of solutions of (2-4) in $b_1, \ldots, b_r$ is p^{r-1}. So we have $X = p^{r-1}$. Hence, the number of solutions of (2-2) is $TX = p^{r-1}T = p^{(r-1)(t-1)}T$, since $t = 2$.

Now let $t = 3$. Suppose $c_1^2 + \cdots + c_r^2 \equiv a \pmod{p^2}$. Let Y be the number of solutions of

$$(a_1 + pc_1 + p^2d_1)^2 + \cdots + (a_r + pc_r + p^2d_r)^2 \equiv a \pmod{p^3} \tag{2-5}$$

in $d_1, \ldots, d_r$ where $d_\lambda \equiv h_\lambda \pmod{p^3}$, $0 \leqslant h_\lambda \leqslant p-1$ for $\lambda = 1, \ldots, r$. Then the number of solutions of (2-2) is equal to TXY. By (2-5), we have

$$2a_1d_1 + \cdots + 2a_rd_r \equiv m_2 \pmod{p} \tag{2-6}$$

where $a-(a_1+pc_1)^2-\cdots-(a_r+pc_r)^2 = m_2p^2$. Since $gcd(2a_1, \ldots, 2a_r, p) = 1$, by Lemma 2.1, the number of solutions of (2-6) in $d_1, \ldots, d_r$ is p^{r-1}. So we have $Y = p^{r-1}$. Thus the number of solutions of (2-2) is equal to $TXY = p^{r-1}p^{r-1}T = p^{2(r-1)}T = p^{(r-1)(t-1)}T$, since $t = 3$.

Therefore, by induction on t, we can conclude that for $t \geqslant 2$, the number of solutions of (2-2) is $(p^{r-1})^{t-1}T = p^{(r-1)(t-1)}T$. □

Lemma 2.4 — If R_1 and R_2 are two noncommutative rings, $S_1 \subseteq R_1$ and $S_2 \subseteq R_2$ are two non-central subsets, then $diam(\Gamma(S_1 \times S_2)) \leqslant 3$.

PROOF : Let (a, b) and (a', b') be two arbitrary vertices of $\Gamma(S_1 \times S_2)$. If a and b' are non-central, then (a, b) — $(a, 0)$ — $(0, b')$ — (a', b') is a path in $\Gamma(S_1 \times S_2)$ of length at most 3. If a, a' are non-central and b, b' are central, then (a, b) — (a, x) — $(0, x)$ — (a', b') is a path in $\Gamma(S_1 \times S_2)$ of length at most 3, for some $x \in S_2 \setminus Z(S_2)$. Therefore, $diam(\Gamma(S_1 \times S_2)) \leqslant 3$. □

Lemma 2.5 (1) [7, Lemma 3.6] — Let $n = p_1^{t_1} \cdots p_m^{t_m}$, where $p_1, \ldots, p_m$ are different primes and $t_1, \ldots, t_m$ are positive integers. Then $\mathrm{H}_n \cong \mathrm{H}_{p_1^{t_1}} \oplus \cdots \oplus \mathrm{H}_{p_m^{t_m}}$.

(2) [7, Theorem 2.3] $\alpha \in D(\mathrm{H}_n)$ if and only if $N(\alpha) \in D(\mathbb{Z}_n)$.

3. COMMUTING GRAPHS OF IDEMPOTENTS OF H_n

In this section, we study $\Gamma(\mathcal{I}_n)$, the commuting graphs of idempotents of H_n. Note that if $R_1, \ldots, R_r$ are arbitrary rings, then clearly $\mathcal{I}(R_1 \times \cdots \times R_r) = \mathcal{I}(R_1) \times \cdots \times \mathcal{I}(R_r)$, where $\mathcal{I}(R)$ is the set of all idempotents in the ring R. Hence, by Lemma 2.5(1), it suffices to investigate the idempotents of H_{p^t}, where p is a prime and t is a positive integer.

***Theorem* 3.1** — *Let $n = p^t$, where p is a prime and t is a positive integer.*

(1) If $p = 2$, then $\mathcal{I}_n = \{\overline{0}, \overline{1}\}$.

(2) If $p \neq 2$, then

(i) $\mathcal{I}_n = \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathrm{H}_n \;\middle|\; p^t | 2a - 1,\ p^t | a^2 + b^2 + c^2 + d^2 \right\} \cup \{\overline{0}, \overline{1}\}$,

(ii) $|\mathcal{I}_n| = p^{2t-1}(p + 1) + 2$, *and*

(iii) $Z(\mathcal{I}_n) = \{\overline{0}, \overline{1}\}$.

PROOF : (1) By [7, Theorem 3.7], we know that H_n is local if and only if $n = 2^t$. By [5, p.301, Corollary 19.19], H_{2^t} has no nontrival idempotents. Hence, $\mathcal{I}_{2^t} = \{\overline{0}, \overline{1}\}$.

(2) Suppose $\alpha = \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathrm{H}_n$. Then $\alpha^2 = \alpha$ if and only if the following statements hold

$$a^2 - b^2 - c^2 - d^2 \equiv a \pmod{n} \tag{3-1}$$

$$2ab \equiv b \pmod{n} \tag{3-2}$$

$$2ac \equiv c \pmod{n} \tag{3-3}$$

$$2ad \equiv d \pmod{n} \tag{3-4}$$

(i) Suppose $\alpha \in \mathcal{I}_n$. Then by (3-2), (3-3) and (3-4), $p^t|b(2a-1), p^t|c(2a-1), p^t|d(2a-1)$.

Case 1 : If $p \nmid 2a-1$, then $p^t|b$, $p^t|c$, $p^t|d$. By (3-1), we derive $p^t|a$ or $p^t|a-1$. Hence $\alpha = \overline{0}$ or $\overline{1}$.

Case 2 : If $p^t|2a-1$, then by (3-1), we have $b^2 + c^2 + d^2 \equiv a^2 - a \equiv a(2a-1) - a^2 \equiv -a^2 \pmod{p^t}$. This follows that $p^t|N(\alpha)$.

Case 3 : If $p^s \parallel 2a-1$ for some $1 \leqslant s \leqslant t-1$ ($t \geqslant 2$), then it is not difficult to verify that $p \nmid a$. Moreover, by (3-2), (3-3) and (3-4), we derive $p|b$, $p|c$ and $p|d$, so $p|b^2+c^2+d^2$. By (3-1), we have $b^2+c^2+d^2 \equiv a^2-a \equiv a(2a-1)-a^2 \pmod{p^t}$, which is impossible. Therefore, if $t \geqslant 2$, then there exists no integer s with $1 \leqslant s \leqslant t-1$, such that $p^s \parallel 2a-1$.

Consequently, for $\alpha = \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathcal{I}_n$, we have either $p \nmid 2a-1$ or $p^t|2a-1$, hence the result follows.

(ii) Clearly, $p \nmid (\frac{p^t+1}{2})^2$, and we have the Legendre symbol

$$\left(\frac{-(\frac{p^t+1}{2})^2}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & if\ p \equiv 1 \pmod 4 \\ -1, & if\ p \equiv 3 \pmod 4 \end{cases}$$

Thus by Lemma 2.2, the number of solutions of $b^2+c^2+d^2 \equiv -(\frac{p^t+1}{2})^2 \pmod p$ in b, c, d is $T = p^2+p$. So by Lemma 2.3, the number of solutions of $b^2+c^2+d^2 \equiv -(\frac{p^t+1}{2})^2 \pmod{p^t}$ is $p^{2(t-1)}T = p^{2t-1}(p+1)$. Hence, $|\mathcal{I}_n| = p^{2t-1}(p+1)+2$.

(iii) Let $\alpha = \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k},\ \beta = \overline{w} + \overline{x}\mathbf{i} + \overline{y}\mathbf{j} + \overline{z}\mathbf{k} \in \mathcal{I}_n$. Then $\alpha\beta = \beta\alpha$ if and only if the following statements hold

$$2cz \equiv 2dy \pmod n \tag{3-5}$$

$$2dx \equiv 2bz \pmod n \tag{3-6}$$

$$2by \equiv 2cx \pmod n \tag{3-7}$$

By Lemma 2.2, the congruence equation $x_1^2 + x_2^2 \equiv -\left(\frac{p^t+1}{2}\right)^2 \pmod p$ in x_1 and x_2 has integer solutions. So by Lemma 2.3, there exist integers m_1 and m_2 such that $m_1^2+m_2^2 \equiv -\left(\frac{p^t+1}{2}\right)^2 \pmod{p^t}$. Let $\beta_1 = \overline{\frac{p^t+1}{2}} + \overline{m_1}\mathbf{i} + \overline{m_2}\mathbf{j}$, then we have $\beta_1 \in \mathcal{I}_n$ by (i). Suppose that $\alpha \in Z(\mathcal{I}_n)$, then $\alpha\beta_1 = \beta_1\alpha$. By (3-5) and (3-6), we have $p^t|2dm_1$ and $p^t|2dm_2$. Observe that $gcd(m_1, m_2, p) = 1$, so $p^t|d$. Similarly, let $\beta_2 = \overline{\frac{p^t+1}{2}} + \overline{m_1}\mathbf{i} + \overline{m_2}\mathbf{k}$, $\beta_3 = \overline{\frac{p^t+1}{2}} + \overline{m_1}\mathbf{j} + \overline{m_2}\mathbf{k} \in \mathcal{I}_n$, then we have $p^t|c$ and $p^t|b$. Therefore, $\alpha = \overline{0}$ or $\overline{1}$, i.e., $Z(\mathcal{I}_n) = \{\overline{0}, \overline{1}\}$.

***Theorem* 3.2** — *Let $n \geqslant 2$ be an integer.*

(1) Suppose $n = p^t$, where p is an odd prime and t is a positive integer. Then for $\alpha, \beta \in \mathcal{I}_n \setminus Z(\mathcal{I}_n)$, $\alpha\beta = \beta\alpha$ if and only if $\beta = \alpha$ or $\overline{\alpha}$. Moreover, $\Gamma(\mathcal{I}_n)$ is a graph with $\frac{p^{2t-1}(p+1)}{2}$ edges which any two different edges are not incident.

(2) Suppose $n = 2^s p^t$, where p is an odd prime, s and t are positive integers. Then for $\alpha, \beta \in \mathcal{I}_n \setminus Z(\mathcal{I}_n)$, $\alpha\beta = \beta\alpha$ if and only if $\beta = \alpha$ or $\overline{\alpha}, 1-\alpha, 1-\overline{\alpha}$. Moreover, $\Gamma(\mathcal{I}_n)$ is a graph with $\frac{p^{2t-1}(p+1)}{2}$ connected components of size 4 which each of them is a complete graph.

(3) Suppose $n = 2^\tau p_1^{t_1} \cdots p_m^{t_m}$, where $\tau \geqslant 0$, $m \geqslant 2$, $p_1, \ldots, p_m$ are different odd primes, $t_1, \ldots, t_m$ are positive integers. Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_m) \in \mathcal{I}_n \setminus Z(\mathcal{I}_n)$, where $\alpha_0 \in \mathcal{I}_{2^\tau}$, $\alpha_\lambda \in \mathcal{I}_{p_\lambda^{t_\lambda}}$ for $\lambda = 1, \ldots, m$. Let $I = \{s \,|\, 1 \leqslant s \leqslant m, \alpha_s = 0 \text{ or } 1\}$, $f(\tau) = \begin{cases} 0, \ if\ \tau = 0 \\ 1, \ if\ \tau \geqslant 1 \end{cases}$. Then $d(\alpha) = 2^{f(\tau)} \Big[4^{m-|I|} \prod_{s\in I}(p_s^{2t_s} + p_s^{2t_s-1} + 2) - 2^m\Big] - 1$. Moreover, $\Gamma(\mathcal{I}_n)$ is a connected graph with $diam(\Gamma(\mathcal{I}_n)) = 3$.

PROOF : (1) By Theorem 3.1 (2), let $\alpha = \frac{\overline{p^t+1}}{2} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k}$ and $\beta = \frac{\overline{p^t+1}}{2} + \overline{x}\mathbf{i} + \overline{y}\mathbf{j} + \overline{z}\mathbf{k}$ be nontrival idempotents of H_n. Certainly, if $\beta = \alpha$ or $\overline{\alpha}$, then $\alpha\beta = \beta\alpha$.

Conversely, suppose $\alpha\beta = \beta\alpha$. It is clear that $\alpha \neq \overline{\alpha}$ and $\alpha\overline{\alpha} = \overline{\alpha}\alpha$. So in $\Gamma(\mathcal{I}_n)$, $d(\alpha) \geqslant 1$. Moreover, by Theorem 3.1(2), we have $p^t | N(\alpha)$ and $p^t | N(\beta)$, i.e.,

$$b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 \equiv -(\frac{p^t+1}{2})^2 \ (\mathrm{mod}\, p^t) \tag{3-8}$$

Since $p \nmid \frac{p^t+1}{2}$, by (3-8), $p \nmid b^2 + c^2 + d^2$. Without loss of generality, one can assume that $p \nmid c$. Then there exists an integer c' such that $c'c \equiv 1 \ (\mathrm{mod}\, p^t)$. Since $\alpha\beta = \beta\alpha$, by (3-5), we have $cz \equiv dy \ (\mathrm{mod}\, p^t)$. So $c'cz \equiv c'dy \ (\mathrm{mod}\, p^t)$, i.e., $z \equiv c'dy \ (\mathrm{mod}\, p^t)$. By (3-7), we also have $x \equiv c'by \ (\mathrm{mod}\, p^t)$. Substituting these expressions for x, z into (3-8), we get

$$y^2(1 + c'^2 d^2 + c'^2 b^2) \equiv -(\frac{p^t+1}{2})^2 \ (\mathrm{mod}\, p^t) \tag{3-9}$$

By [6, p.193, Theorem 1], if the equation (3-9) in y has solutions, then the number of solutions of (3-9) must be 2. Notice that $d(\alpha) \geqslant 1$, hence (3-9) has exactly two solutions, say y_1, y_2. So we have $x_\lambda \equiv c'by_\lambda \pmod{p^t}$ and $z_\lambda \equiv c'dy_\lambda \pmod{p^t}$, $\lambda = 1, 2$. Therefore $\{x_1, y_1, z_1\}$ and $\{x_2, y_2, z_2\}$ are the only two solutions which satisfy conditions (3-5), (3-6) and (3-7). Hence, $\beta = \alpha$ or $\overline{\alpha}$. Furthermore, there are precisely $\dfrac{p^{2t-1}(p+1)}{2}$ edges by Theorem 3.1(2) in $\Gamma(\mathcal{I}_n)$ which any two different edges are not incident.

(2) Suppose that $\alpha, \beta \in \mathcal{I}_n \setminus Z(\mathcal{I}_n)$. By Lemma 2.5 and Theorem 3.1, one can write $\alpha = (0, \alpha')$ or $(1, \alpha')$, while $\beta = (0, \beta')$ or $(1, \beta')$, where $\alpha', \beta' \in \mathcal{I}_{p^t} \setminus Z(\mathcal{I}_{p^t})$. If $\alpha\beta = \beta\alpha$, then $\alpha'\beta' = \beta'\alpha'$. By (1) above, $\beta' = \alpha'$ or $\overline{\alpha'}$. So it is easy to see that $\beta = \alpha$ *or* $\overline{\alpha}, 1-\alpha, 1-\overline{\alpha}$.

Furthermore, it is easy to verify that $\alpha, \overline{\alpha}, 1-\alpha$ and $1-\overline{\alpha}$ are pairwise different. Hence, the result follows.

(3) The computation of $d(\alpha)$ is derived from Theorem 3.1. Furthermore, by Lemma 2.4, $diam(\Gamma(\mathcal{I}_n)) \leqslant 3$. Let $n = p^t n'$, where p is an odd prime, $t, n' \geqslant 1$ are integers, $p \nmid n'$. Suppose $\alpha = (\alpha_1, 0)$, $\beta = (\beta_1, 0)$, where $\alpha_1, \beta_1 \in \mathcal{I}_{p^t} \setminus Z(\mathcal{I}_{p^t})$ and $\beta_1 \neq \alpha_1, \overline{\alpha_1}$. Then $\alpha, \beta \in \mathcal{I}_n \setminus Z(\mathcal{I}_n)$. However, by (1) above, there exists no $\gamma \in \mathcal{I}_n \setminus Z(\mathcal{I}_n)$ such that α — γ — β is a path of $\Gamma(\mathcal{I}_n)$. Therefore, $diam(\Gamma(\mathcal{I}_n)) = 3$.

Corollary 3.3 — For $n \geqslant 2$, $\Gamma(\mathcal{I}_n)$ is connected if and only if n has at least two odd prime factors.

4. Commuting Graphs of Nilpotent Elements of H_n

In this section, we study $\Gamma(\mathcal{N}_\setminus)$, the commuting graphs of nilpotent elements of H_n. Note that if $R_1, \ldots, R_r$ are arbitrary rings, then clearly $\mathcal{N}(R_1 \times \cdots \times R_r) =$

$\mathcal{N}(R_1) \times \cdots \times \mathcal{N}(R_r)$, where $\mathcal{N}(R)$ is the set of all nilpotent elements in the ring R. Hence, by Lemma 2.5(1), it suffices to investigate the nilpotent elements of H_{p^t}, where p is a prime and t is a positive integer.

Lemma 4.1 — If R is a finite local ring, then $\alpha \in R$ is nilpotent if and only if $\alpha \in D(R)$.

***Theorem* 4.2** — *Let $n = p^t$, where p is a prime and t is a positive integer.*

(1) If $p = 2$, then

$$\mathcal{N}_n = D(\mathrm{H}_n) = \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathrm{H}_n \,\middle|\, 2|a^2 + b^2 + c^2 + d^2 \right\}, \quad |\mathcal{N}_n| = 2^{4t-1}$$

$$Z(\mathcal{N}_n) = \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathrm{H}_n \,\middle|\, 2|a;\ b, c, d \equiv 0 \text{ or } 2^{t-1} (\mathrm{mod}\, 2^t) \right\},$$

$|Z(\mathcal{N}_n)| = 2^{t+2}$.

(2) If $p \neq 2$, then

$$\mathcal{N}_n = \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathrm{H}_n \,\middle|\, p|a;\ p|a^2 + b^2 + c^2 + d^2 \right\}, \ |\mathcal{N}_n| = p^{4t-2}$$

$$Z(\mathcal{N}_n) = \left\{ \overline{a} \in \mathbb{Z}_n \,\middle|\, p|a \right\}, \ |Z(\mathcal{N}_n)| = p^{t-1}.$$

PROOF : (1) By Lemma 4.1 and recall that H_{2^t} is a local ring [7, Theorem 3.7], we have $\mathcal{N}_n = D(\mathrm{H}_n)$. By [8, Theorem 1.1], $|D(\mathrm{H}_n)| = 2^{4t-1}$. Also, it is not difficult to obtain $Z(\mathcal{N}_n)$ and $|Z(\mathcal{N}_n)|$.

(2) There are two cases to consider.

Case 1 : Assume that $t = 1$. For $\alpha = \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in D(\mathrm{H}_p)$, if $p|a$, then by Lemma 2.5 (2), we have $p|b^2 + c^2 + d^2$. Hence, it is certainly that $\alpha^2 = 0$.

Conversely, suppose that $\beta = \overline{w} + \overline{x}\mathbf{i} + \overline{y}\mathbf{j} + \overline{z}\mathbf{k} \in D(\mathrm{H}_p)$ but $p \nmid w$. Note that $p|w^2 + x^2 + y^2 + z^2$, let $x^2 + y^2 + z^2 = -w^2 + sp$, where s is a positive integer.

Then we have

$$\begin{aligned}\beta^2 &= \overline{w^2} - \overline{x^2} - \overline{y^2} - \overline{z^2} + 2\overline{w}(\overline{x}\mathbf{i} + \overline{y}\mathbf{j} + \overline{z}\mathbf{k}) \\ &= 2\overline{w^2} - sp + 2\overline{w}(\overline{x}\mathbf{i} + \overline{y}\mathbf{j} + \overline{z}\mathbf{k}) = 2\overline{w}\beta - sp\end{aligned}$$

Therefore, for any integer $\delta > 1$, we have $\beta^\delta \neq 0$ if $p \nmid w$.

Furthermore, notice that the number of solutions of $b^2 + c^2 + d^2 \equiv 0 \pmod p$ in b, c, d is p^2, so $|\mathcal{N}_n| = p^2$.

Case 2 : Assume that $t \geqslant 2$. Suppose $\beta = \overline{w} + \overline{x}\mathbf{i} + \overline{y}\mathbf{j} + \overline{z}\mathbf{k} \in \mathrm{H}_{p^t}$. One can assume that $w = w' + s_1 p$, $x = x' + s_2 p$, $y = y' + s_3 p$, $z = z' + s_4 p$, where w', x', y' and z' are nonnegative integers less than p, while s_1, s_2, s_3 and s_4 are nonnegative integers. Then $\beta_1 = \overline{w'} + \overline{x'}\mathbf{i} + \overline{y'}\mathbf{j} + \overline{z'}\mathbf{k} \in \mathrm{H}_p$. We can claim that $\beta \in \mathcal{N}_{p^t}$ if and only if $\beta_1 \in \mathcal{N}_p$. In fact, if $\beta \in \mathcal{N}_{p^t}$, clearly, we have $\beta_1 \in \mathcal{N}_p$. Conversely, if $\beta_1 \in \mathcal{N}_p$, then there exist positive integers r and k such that ${\beta_1}^r = kp\beta_2$ for some $\beta_2 \in \mathrm{H}_p$. Then

$$\beta^r = [\beta_1 + p(\overline{s_1} + \overline{s_2}\mathbf{i} + \overline{s_3}\mathbf{j} + \overline{s_4}\mathbf{k})]^r = {\beta_1}^r + p\beta_3 = (kp\beta_2)^r + p\beta_3 = p(k^r p^{r-1}{\beta_2}^r + \beta_3)$$

for some $\beta_3 \in \mathrm{H}_p$. Hence $\beta^{rt} = 0$, i.e., $\beta \in \mathcal{N}_{p^t}$. Consequently, by Case 1, the result follows.

In the following, we will study the connectivity of $\Gamma(\mathcal{N}_n)$ for $n \geqslant 2$. We recall that with similar arguments to the proof of Theorem 2.4(3), 2.5(2) and 2.8(2) of [9], if $n = 2^t$ for $t \geqslant 3$, or $n = p^s$ for arbitrary odd prime p and $s \geqslant 2$, or n has at least two odd prime divisors with $n \neq 2p$ for any odd prime p, then $\Gamma(\mathcal{N}_n)$ is connected with $diam(\Gamma(\mathcal{N}_n)) = 3$. Therefore, it suffices to study the properties of $\Gamma(\mathcal{N}_n)$ with $n = 2, 2^2, p, 2p$, where p is an odd prime and the following theorem is clear.

***Theorem* 4.3** — *Suppose* $n = 2^t$, $t = 1$ *or* 2.

(1) If $t = 1$, then $\Gamma(\mathcal{N}_n)$ is null.

(2) If $t = 2$, then $\Gamma(\mathcal{N}_n)$ is a graph with 7 connected components of size 2^4 which each of them is a complete graph. Moreover, for $\alpha, \beta \in \mathcal{N}_{2^2} \setminus Z(\mathcal{N}_{2^2})$, $\alpha\beta = \beta\alpha$ if and only if α and β belong to the same set of M_λ for some $\lambda \in \{1, \ldots, 7\}$.

$$\begin{aligned}
M_1 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{a}, \overline{b} \in U(\mathbb{Z}_4); \overline{c}, \overline{d} \in D(\mathbb{Z}_4) \right\} \\
M_2 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{a}, \overline{c} \in U(\mathbb{Z}_4); \overline{b}, \overline{d} \in D(\mathbb{Z}_4) \right\} \\
M_3 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{a}, \overline{d} \in U(\mathbb{Z}_4); \overline{b}, \overline{c} \in D(\mathbb{Z}_4) \right\} \\
M_4 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{c}, \overline{d} \in U(\mathbb{Z}_4); \overline{a}, \overline{b} \in D(\mathbb{Z}_4) \right\} \\
M_5 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{b}, \overline{d} \in U(\mathbb{Z}_4); \overline{a}, \overline{c} \in D(\mathbb{Z}_4) \right\} \\
M_6 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{b}, \overline{c} \in U(\mathbb{Z}_4); \overline{a}, \overline{d} \in D(\mathbb{Z}_4) \right\} \\
M_7 &= \left\{ \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \middle| \, \overline{a}, \overline{b}, \overline{c}, \overline{d} \in U(\mathbb{Z}_4) \right\}
\end{aligned}$$

It is well known that if p is a prime congruent to 1 modulo 4, then there exist exactly two positive integers which less than p say λ_1, λ_2 such that $\lambda^2 \equiv -1 \pmod{p}$. Furthermore, we assume that the ordered pairs of positive integers $\{\sigma_\nu, \tau_\nu\}$ satisfy (4-1), where $1 \leqslant \sigma_\nu, \tau_\nu \leqslant p-1$, $\nu = 1, \ldots, S$ $(resp.,\ \nu = 1, \ldots, S')$, while S $(resp.,\ S')$ is the number of solutions of

$$1 + \sigma^2 + \sigma^2\tau^2 \equiv 0 \pmod{p}, \quad \sigma, \tau \neq 0 \tag{4-1}$$

in σ, τ where p is a prime congruent to 1 $(resp.,\ 3)$ modulo 4. In the following theorem, we will obtain S and S', and completely determine the structure of $\mathcal{N}_p$ for arbitrary odd prime p.

***Theorem* 4.4** — *Let p be an odd prime, $\alpha, \beta \in \mathcal{N}_p \setminus Z(\mathcal{N}_p)$.*

(1) If $p = 5$, then $\alpha\beta = \beta\alpha$ if and only if α and β belong to the same set of B_μ, C_μ and D_μ for some $\mu \in \{1, 2\}$.

(2) If $p \equiv 1 \pmod 4$ with $p > 5$, then $S = p - 5$. Moreover, $\alpha\beta = \beta\alpha$ if and only if α and β belong to the same set of B_μ, C_μ, D_μ and E_ν for some $\mu \in \{1, 2\}$, or some $\nu \in \{1, \ldots, p - 5\}$.

(3) If $p \equiv 3 \pmod 4$, then $S' = p + 1$. Moreover, $\alpha\beta = \beta\alpha$ if and only if α and β belong to the same set of E_ν for some $\nu \in \{1, \ldots, p + 1\}$.

$$B_\mu = \left\{ \overline{b}\mathbf{i} + \lambda_\mu \overline{b}\mathbf{j} \in \mathrm{H}_p \,\middle|\, \overline{b} \in \mathbb{Z}_p^* \right\},\ \mu = 1, 2 \tag{4-2}$$

$$C_\mu = \left\{ \overline{b}\mathbf{j} + \lambda_\mu \overline{b}\mathbf{k} \in \mathrm{H}_p \,\middle|\, \overline{b} \in \mathbb{Z}_p^* \right\},\ \mu = 1, 2 \tag{4-3}$$

$$D_\mu = \left\{ \overline{b}\mathbf{i} + \lambda_\mu \overline{b}\mathbf{k} \in \mathrm{H}_p \,\middle|\, \overline{b} \in \mathbb{Z}_p^* \right\},\ \mu = 1, 2 \tag{4-4}$$

$$E_\nu = \left\{ \overline{e}\mathbf{i} + \sigma_\nu \overline{e}\mathbf{j} + \sigma_\nu \tau_\nu \overline{e}\mathbf{k} \in \mathrm{H}_p \,\middle|\, \overline{e} \in \mathbb{Z}_p^* \right\} \tag{4-5}$$

(4) $\Gamma(\mathcal{N}_p)$ is a graph with $p+1$ connected components of size $p-1$ which each of them is a complete graph.

PROOF : By Theorem 4.2(2), $\alpha = \overline{a} + \overline{b}\mathbf{i} + \overline{c}\mathbf{j} + \overline{d}\mathbf{k} \in \mathcal{N}_p$ if and only if $a = 0$ and $p | b^2 + c^2 + d^2$. By [9, Theorem 2.5 (1)], each nonzero nilpotent element of H_p must be one of the form: $\overline{b}\mathbf{i} + \lambda\overline{b}\mathbf{j}$, $\overline{b}\mathbf{i} + \lambda\overline{b}\mathbf{k}$, $\overline{b}\mathbf{j} + \lambda\overline{b}\mathbf{k}$, $\overline{e}\mathbf{i} + \sigma\overline{e}\mathbf{j} + \sigma\tau\overline{e}\mathbf{k}$, where $\overline{b}, \overline{e} \in \mathbb{Z}_p^*$, λ, σ and τ are positive integers.

(1) Since $p = 5$, for $\overline{b} \in \mathbb{Z}_5^*$, $b^2 + \lambda^2 b^2 \equiv 0 \pmod 5$ if and only if $1 + \lambda^2 \equiv 0 \pmod 5$. Clearly, $|B_\mu| = |C_\mu| = |D_\mu| = p - 1$ for $\mu = 1, 2$. Moreover, by Theorem 4.2(2), $|\mathcal{N}_5 \setminus Z(\mathcal{N}_5)| = 24 = 6(5 - 1)$. Therefore, $\alpha \in \mathcal{N}_5 \setminus Z(\mathcal{N}_5)$ if and only if α belongs to one of the sets of (4-2), (4-3) and (4-4) for some $\mu = 1, 2$. Hence, $\Gamma(\mathcal{N}_5)$ has exactly 6 connected components of size 4 which each of them is a complete graph.

(2) Suppose $p \equiv 1 \pmod 4$ with $p > 5$. By the similar argument of (1) above, every element of B_μ, C_μ and D_μ is a nonzero nilpotent element of H_p, $\mu = 1, 2$. Clearly, $|B_1| + |B_2| + |C_1| + |C_2| + |D_1| + |D_2| = 6(p - 1)$, while

$|\mathcal{N}_p \setminus Z(\mathcal{N}_p)| = p^2 - 1 > 6(p-1)$ by Theorem 4.2(2). So in $\mathrm{H_p}$, there must exist $p^2 - 1 - 6(p-1) = (p-5)(p-1)$ nonzero nilpotent elements of the form $\overline{e}\mathbf{i} + \sigma\overline{e}\mathbf{j} + \sigma\tau\overline{e}\mathbf{k}$ where $e \neq 0$ which is stated in the sets E_ν (4-5) for some $\nu \in \{1, \ldots, S\}$, since for $\overline{e} \in \mathbb{Z}_p^*$, $p|e^2 + e^2\sigma^2 + e^2\sigma^2\tau^2$ if and only if σ and τ satisfy (4-1).

Moreover, since $|E_\nu| = p - 1$ for ν, by $S(p-1) = (p-5)(p-1)$, we have $S = p - 5$. Therefore, $\Gamma(\mathcal{N}_p)$ has exactly $6 + S = p + 1$ connected components of size $p - 1$ which each of them is a complete graph.

(3) Suppose $p \equiv 3 \pmod 4$. Then the congruence equation $b^2 + c^2 \equiv 0 \pmod p$ in b, c has a unique solution $b \equiv c \equiv 0 \pmod p$. Therefore any nonzero nilpotent element of $\mathrm{H_p}$ must be of the form $\overline{e}\mathbf{i} + \sigma\overline{e}\mathbf{j} + \sigma\tau\overline{e}\mathbf{k}$ where $e \neq 0$ which is stated in the sets E_ν (4-5) for some $\nu \in \{1, \ldots, S'\}$, since for $\overline{e} \in \mathbb{Z}_p^*$, $p|e^2 + e^2\sigma^2 + e^2\sigma^2\tau^2$ if and only if σ and τ satisfy (4-1). By Theorem 4.2 (2), $|\mathcal{N}_p \setminus Z(\mathcal{N}_p)| = p^2 - 1$. Moreover, since $|E_\nu| = p - 1$ for ν, by $S'(p-1) = p^2 - 1$, we have $S' = p + 1$. Consequently, $\Gamma(\mathcal{N}_p)$ has exactly $p + 1$ connected components of size $p - 1$ which each of them is a complete graph.

(4) It has been shown in (1), (2) and (3) above.

***Theorem* 4.5** — *Let $n = 2p$, where p is an odd prime. Then $\Gamma(\mathcal{N}_{2p})$ is a graph with $p+1$ connected components of size $8(p-1)$ which each of them is a complete graph.*

PROOF : For $\alpha, \beta \in \mathcal{N}_{2p} \setminus Z(\mathcal{N}_{2p})$, since $\mathrm{H}_{2p} \cong \mathrm{H}_2 \oplus \mathrm{H}_p$, let $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$, where $\alpha_1, \beta_1 \in \mathcal{N}_2 = D(\mathrm{H}_2)$, and $\alpha_2, \beta_2 \in \mathcal{N}_p \setminus Z(\mathcal{N}_p)$. Since H_2 is a commutative ring, $\alpha\beta = \beta\alpha$ if and only if $\alpha_2\beta_2 = \beta_2\alpha_2$, if and only if α_2 and β_2 belong to the same connected component of $\Gamma(\mathcal{N}_p)$. By Theorem 4.4, we derive that $\Gamma(\mathcal{N}_{2p})$ is a graph with $p + 1$ connected components which each of

them is a complete graph. Furthermore, since $|\mathcal{N}_2| = |D(\mathrm{H}_2)| = 2^3$, the size of each connected component of $\Gamma(\mathcal{N}_{2p})$ is equal to $8(p-1)$.

Corollary 4.6 — For $n \geqslant 2$, $\Gamma(\mathcal{N}_{\setminus})$ is connected if and only if $n \neq 2, 2^2, p, 2p$, where p is an odd prime.

ACKNOWLEDGEMENT

This research was supported by the National Natural Science Foundation of China (11161006, 11171142), the Guangxi Natural Science Foundation (2011GXNSFA018139, 2010GXNSFB013048), the Guangxi New Century 1000 Talents Project and the Scientific Research Foundation of Guangxi Educational Committee (200911LX284, 201012MS140).

REFERENCES

1. David F. Anderson and Ayman Badawi, The total graph of a commutative ring, *J. of Algebra*, **320** (2008), 2706-2719.
2. David F. Anderson and P.S. Livingston, The zero-divisor graph of a commutative ring, *J. of Algebra*, **217** (1999), 434-447.
3. S. Akbari, M. Ghandehari, M. Hadian and A. Mohammadian, On commuting graphs of semisimple rings, *Linear Algebra Appl*., **390** (2004), 345-355.
4. S. Akbari and P. Raja, Commuting graphs of some subsets in simple rings, *Linear Algebra Appl*., **416** (2006), 1038-1047.
5. T. Y. Lam, *A first course in noncommutative rings*, Springer Verlag, New York, 1991.
6. C. D. Pan and C. B. Pan, *Elementary number theory* (second edition), Beijing university publishing company, Beijing, 2005.

7. Y. J. Wei and G. H. Tang, The spectrum and radicals of quaternion algebra $\mathbb{Z}_n[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, *J. Guangxi Teachers Education University*, **26**(1) (2009), 1-10.

8. Y. J. Wei and G. H. Tang, The zero-divisors and unit group of quaternion algebra $\mathbb{Z}_n[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, *Guangxi Sciences*, **16**(2) (2009), 147-150.

9. Y. J. Wei, G. H. Tang and H. D. Su, The commuting graph of the quaternion algebra over residue classes of integers, *Ars Combinatoria*, **95** (2010), 113-127.