Yangjiang Wei; Jizhu Nan; Gaohua Tang

Structure of cubic mapping graphs for the ring of Gaussian integers modulo n

Czechoslovak Mathematical Journal, Vol. 62 (2012), No. 2, 527–539

Persistent URL: `http://dml.cz/dmlcz/142844`

Czechoslovak Mathematical Journal, 62 (137) (2012), 527–539

STRUCTURE OF CUBIC MAPPING GRAPHS FOR THE RING OF GAUSSIAN INTEGERS MODULO n

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

(Received March 3, 2011)

Abstract. Let $\mathbb{Z}_n[\mathrm{i}]$ be the ring of Gaussian integers modulo n. We construct for $\mathbb{Z}_n[\mathrm{i}]$ a cubic mapping graph $\Gamma(n)$ whose vertex set is all the elements of $\mathbb{Z}_n[\mathrm{i}]$ and for which there is a directed edge from $a \in \mathbb{Z}_n[\mathrm{i}]$ to $b \in \mathbb{Z}_n[\mathrm{i}]$ if $b = a^3$. This article investigates in detail the structure of $\Gamma(n)$. We give suffcient and necessary conditions for the existence of cycles with length t. The number of t-cycles in $\Gamma_1(n)$ is obtained and we also examine when a vertex lies on a t-cycle of $\Gamma_2(n)$, where $\Gamma_1(n)$ is induced by all the units of $\mathbb{Z}_n[\mathrm{i}]$ while $\Gamma_2(n)$ is induced by all the zero-divisors of $\mathbb{Z}_n[\mathrm{i}]$. In addition, formulas on the heights of components and vertices in $\Gamma(n)$ are presented.

Keywords: cubic mapping graph, cycle, height

MSC 2010: 05C05, 11A07, 13M05

1. Preliminaries

This work is motivated by [3] and [4], and extends some results given in the paper [9], which investigated properties of the cubic mapping graphs for the ring $\mathbb{Z}_n[\mathrm{i}]$ of Gaussian integers modulo n. 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 $\mathbb{Z}_n[\mathrm{i}] = \{\overline{a} + \overline{b}\mathrm{i} \colon \overline{a}, \overline{b} \in \mathbb{Z}_n\}$ which is called the ring of *Gaussian integers modulo n*. The digraph $\Gamma(n)$, whose vertex

This research was supported by the National Natural Science Foundation of China (11161006, 11171142), the Guangxi Natural Science Foundation (2011GXNSFA018139) and the Guangxi New Century 1000 Talents Project.

set consists of all the elements of $\mathbb{Z}_n[\mathrm{i}]$, and for which there is a directed edge from $\alpha \in \mathbb{Z}_n[\mathrm{i}]$ to $\beta \in \mathbb{Z}_n[\mathrm{i}]$ if and only if $\alpha^3 = \beta$, is called the *cubic mapping graph* of $\mathbb{Z}_n[\mathrm{i}]$.

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

In $\Gamma(n)$, a *cycle* with precisely t vertices is called 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 $\alpha^{3^t} = \alpha$. A *component* of $\Gamma(n)$ is a subdigraph which is a maximal connected subgraph of the associated nondirected graph of $\Gamma(n)$. The vertex set of $\Gamma(n)$ is denoted by $V(\Gamma(n))$.

If p is a prime number and t is a nonnegative integer, then we use the notation $p^t \parallel a$ to mean that $p^t \mid a$ and $p^{t+1} \nmid a$. If $a = 0$, $p^t \parallel a$ implies that $t = \infty$. If $p \nmid a$, then $p^t \parallel a$ if and only if $t = 0$. Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathbb{Z}_n[\mathrm{i}]$, 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 $N(\alpha\beta) \equiv N(\alpha)N(\beta) \pmod n$. For $\alpha = \overline{a} + \overline{b}\mathrm{i}$, we denote $\mathrm{Re}(\alpha) = \overline{a}$.

Similarly, we can assign to a finite abelian group G a cubic mapping graph $\Gamma_g(G)$ whose vertex set consists of all the elements in G and for which there is a directed edge from $f \in G$ to $h \in G$ if and only if $f^3 = h$. The following lemma concerning the structure of $\Gamma_g(C_n)$ of the cyclic group C_n with order n was shown in [8, Theorem 2.1].

Lemma 1.1.

(1) *Suppose $n = 3^k$, $k \geqslant 1$. Then $\Gamma_g(C_n)$ is a ternary tree of height k with the root in the identity e of C_n.*
(2) *Suppose $3 \nmid n$. Then each component of $\Gamma_g(C_n)$ is precisely a cycle.*
(3) *Suppose $n = 3^k m$, $k \geqslant 1$, $m > 1$, $3 \nmid m$. Then each vertex of each cycle in $\Gamma_g(C_n)$ is attached to a ternary tree of height k.*

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

(1) *The element α is a unit of $\mathbb{Z}_n[\mathrm{i}]$ if and only if $\gcd(N(\alpha), n) = 1$.*
(2) *If $n = \prod\limits_{j=1}^{s} p_j^{k_j}$ is the prime power decomposition of n, then the function*

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

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.

By Lemma 1.2 (2), we can write $\alpha = (\alpha_1, \ldots, \alpha_s)$ for $\alpha \in \mathbb{Z}_n[\mathrm{i}]$, where $\alpha_j \in \mathbb{Z}_{p_j^{k_j}}[\mathrm{i}]$ for $j = 1, \ldots, s$.

Lemma 1.3 ([2], [7]). *Let* Z_n *denote the additive group of integers modulo* n.
(1) $\mathrm{U}(\mathbb{Z}_2[\mathrm{i}]) \cong Z_2$, $\mathrm{U}(\mathbb{Z}_{2^2}[\mathrm{i}]) \cong Z_2 \times Z_{2^2}$, $\mathrm{U}(\mathbb{Z}_{2^t}[\mathrm{i}]) \cong Z_{2^2} \times Z_{2^{t-2}} \times Z_{2^{t-1}}$ *for* $t \geqslant 3$.
(2) *Let* q *be a prime congruent to* 3 *modulo* 4. *Then* $\mathrm{U}(\mathbb{Z}_{q^t}[\mathrm{i}]) \cong Z_{q^{t-1}} \times Z_{q^{t-1}} \times Z_{q^2-1}$ *for* $t \geqslant 1$.
(3) *Let* p *be a prime congruent to* 1 *modulo* 4. *Then* $\mathrm{U}(\mathbb{Z}_{p^t}[\mathrm{i}]) \cong Z_{p^{t-1}} \times Z_{p^{t-1}} \times Z_{p-1} \times Z_{p-1}$ *for* $t \geqslant 1$.

For $\alpha \in V(\Gamma(n))$, the in-degree $\mathrm{indeg}(\alpha)$ of α denotes the number of directed edges coming into α. 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* $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathbb{Z}_n[\mathrm{i}]$, *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* $\Gamma(p_j^{k_j})$, $j = 1, \ldots, s$.

2. Cycles

The *exponent* $\exp(G)$ of a finite group G is the least positive integer n such that $g^n = e$ for all $g \in G$, where e is the identity of G. It is easy to show that if G is abelian, then there exists an element g in G such that $o(g) = \exp(G)$. In this paper, we denote the λ-function by $\lambda(n) = \exp(\mathrm{U}(\mathbb{Z}_n[\mathrm{i}]))$. Let p and q be as given in Lemma 1.3. Then clearly $\lambda(1) = 1$, $\lambda(2^j) = 2^j$ for $j = 1$ or 2, $\lambda(2^j) = 2^{j-1}$ for $j \geqslant 3$, $\lambda(q^j) = q^{j-1}(q^2-1)$ for $j \geqslant 1$, $\lambda(p^j) = p^{j-1}(p-1)$ for $j \geqslant 1$, and $\lambda(rs) = \mathrm{lcm}[\lambda(r), \lambda(s)]$ when $\gcd(r, s) = 1$. In this section, we study the properties of cycles in $\Gamma(n)$ via the λ-function $\lambda(n)$ and the norm $N(\alpha)$.

Theorem 2.1. *Let* $n > 1$.
(1) *There exists a* t*-cycle* ($t \geqslant 2$) *in* $\Gamma(n)$ *if and only if there exists* $\beta \in \mathrm{U}(\mathbb{Z}_n[\mathrm{i}])$ *such that* $o(\beta) \mid 3^t - 1$ *but* $o(\beta) \nmid 3^k - 1$ *whenever* $1 \leqslant k < t$.

(2) *There exists a t-cycle ($t \geqslant 1$) in $\Gamma(n)$ if and only if $t = \operatorname{ord}_d 3$ for some positive divisor d of $\lambda(n)$, where $3 \nmid d$.*

(3) *Let $n = \prod_{j=1}^{s} p_j^{k_j}$ 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 $p_j \mid N(\alpha)$. Furthermore, if α and β lie on the same cycle, then $p_j \mid N(\alpha)$ if and only if $p_j \mid N(\beta)$.*

Proof. In the following, let $R = \mathbb{Z}_n[\mathrm{i}]$.

(1) Suppose that t is the least positive integer such that $o(\beta) \mid 3^t - 1$. Then $\beta^{3^t} = \beta$ and $\beta^{3^k} \neq \beta$ for $1 \leqslant k < t$. Therefore, β is a vertex of a t-cycle.

Conversely, suppose that α is a vertex of a t-cycle ($t \geqslant 2$). Clearly $\alpha \neq \overline{0}$ and t is the least positive integer such that $\alpha^{3^t} = \alpha$, so

$$\alpha(\alpha^{3^t-1} - \overline{1}) = \overline{0}. \tag{2.1}$$

If $\alpha \in \mathrm{U}(R)$, by (2.1) we obtain $\alpha^{3^t-1} - \overline{1} = \overline{0}$, thus t is the least positive integer such that $\alpha^{3^t-1} = \overline{1}$. In this case, let $\beta = \alpha$. Then t is the least positive integer such that $o(\beta) \mid 3^t - 1$, and the result holds. Now we assume $\alpha \notin \mathrm{U}(R)$. Let $A = \langle \alpha \rangle$, the principal ideal of R generated by α. Let $B = \operatorname{Ann}(\alpha)$, the annihilator of α in R. Then $AB = \{\overline{0}\}$. By the above hypothesis,

$$\alpha^{3^t-1} - \overline{1} \in B, \quad \alpha^{3^k-1} - \overline{1} \notin B \ \text{ for } \ 1 \leqslant k < t. \tag{2.2}$$

It follows from $\alpha^{3^t-1} \in A$, $\alpha^{3^t-1} - (\alpha^{3^t-1} - \overline{1}) = \overline{1}$ and (2.2) that $A + B = R$, hence $A \cap B = AB = \{\overline{0}\}$. By the Chinese Remainder Theorem, we have a ring isomorphism

$$\mathcal{F}\colon R \to R / A \oplus R / B$$

such that $\mathcal{F}(\gamma) = (\gamma + A, \gamma + B)$ for each $\gamma \in R$. Let $\beta = \overline{1} + \alpha - \alpha^{3^t-1}$. Clearly, $\beta \neq \overline{1}$ and $\mathcal{F}(\beta) = (\beta + A, \beta + B) = (\overline{1} + A, \alpha + B)$. So we have $\mathcal{F}(\beta^{3^t-1}) = (\overline{1} + A, \alpha^{3^t-1} + B) = (\overline{1} + A, \overline{1} + B)$. Since $\mathcal{F}$ is a ring isomorphism, $\beta^{3^t-1} = \overline{1}$. Moreover, by (2.2), t is the least positive integer for which $\beta^{3^t-1} = \overline{1}$. This completes the proof.

(2) Clearly, $\overline{1}$ is a vertex of a 1-cycle. By Lemma 1.3, 2 is a divisor of $|\mathrm{U}(R)|$ for $n > 1$. So $2 \mid \lambda(n)$ and $\operatorname{ord}_2 3 = 1$. Next, let $t > 1$ and assume that there exists a t-cycle in $\Gamma(n)$. By part (1) above, there exists $\beta \in \mathrm{U}(R)$ for which t is the least positive integer such that $o(\beta) \mid 3^t - 1$. Now, let $d = o(\beta)$. It is obvious that $3 \nmid d$, $d \mid \lambda(n)$ and $t = \operatorname{ord}_d 3$. Conversely, suppose that there exists a positive divisor d of $\lambda(n)$, where $3 \nmid d$ and $t = \operatorname{ord}_d 3$. By the property of the exponent of a finite group, there exists an element g of $\mathrm{U}(R)$ such that $o(g) = \lambda(n)$. Let $h = g^{\lambda(n)/d}$.

Then $o(h) = d$. Moreover, since $d \mid 3^t - 1$ but $d \nmid 3^k - 1$ for $1 \leqslant k < t$, t is the least positive integer such that $h^{3^t-1} = \overline{1}$. Therefore, h is a vertex of a t-cycle.

(3) Since α is a vertex of a t-cycle, t is the least positive integer such that $\alpha^{3^t} = \alpha$. By the definition of the norm, we have $N(\alpha)^{3^t} \equiv N(\alpha^{3^t}) \equiv N(\alpha) \pmod{n}$. Therefore,

$$N(\alpha)(N(\alpha)^{3^{t-1}} - 1) \equiv 0 \pmod{n}. \tag{2.3}$$

Since $\gcd(N(\alpha),\ N(\alpha)^{3^{t-1}} - 1) = 1$, it follows from the congruence (2.3) that if $p_j \mid N(\alpha)$ then $p_j^{k_j} \mid N(\alpha)$.

Now suppose α and β are on the same t-cycle of $\Gamma(n)$. Then $\beta = \alpha^{3^{t-k}}$ and $\alpha = \beta^{3^k}$ for some $k \in \{1, 2, \ldots, t-1\}$. Hence we have

$$N(\beta) \equiv N(\alpha)^{3^{t-k}} \pmod{n} \quad \text{and} \quad N(\alpha) \equiv N(\beta)^{3^k} \pmod{n}. \tag{2.4}$$

We see from (2.4) that $p_j \mid N(\alpha)$ if and only if $p_j \mid N(\beta)$. □

Corollary 2.2. *For $\alpha \in V(\Gamma_1(n))$, α is a vertex of a k-cycle if and only if $3 \nmid o(\alpha)$ and $k = \operatorname{ord}_{o(\alpha)} 3$.*

Let $A_t(\Gamma_1(n))$ and $A_t(\Gamma_2(n))$ denote the number of t-cycles in $\Gamma_1(n)$ and $\Gamma_2(n)$, respectively. By the proof of [9, Theorem 3.1], we can derive $A_1(\Gamma_1(n))$ and $A_1(\Gamma_2(n))$ for $n > 1$. The following theorem computes $A_t(\Gamma_1(n))$ for $t \geqslant 1$.

Theorem 2.3. *Let $t \geqslant 1$ and let the prime power factorization of n be given by*

$$n = 2^s \prod_{q_j \mid n} q_j^{\alpha_j} \cdot \prod_{p_k \mid n} p_k^{\beta_k},$$

where $q_j \equiv 3 \pmod 4$, $p_k \equiv 1 \pmod 4$, $s \geqslant 0$, $\alpha_j \geqslant 1$ and $\beta_k \geqslant 1$.

(1) *Let $\lambda(n) = uv$, where u is the largest factor of $\lambda(n)$ relatively prime to 3. Then $A_t(\Gamma_1(n)) > 0$ if and only if $t = \operatorname{ord}_d 3$ for some positive divisor d of u. In particular, $A_t(\Gamma_1(n)) > 0$ if $t = \operatorname{ord}_u 3$.*

(2) *Let $C(t, 2^s, n)$ be defined as follows:*

$$C(t, 2^s, n) = \begin{cases} 1, & s = 0, \\ \gcd(2, 3^t - 1) = 2, & s = 1, \\ \gcd(2, 3^t - 1) \cdot \gcd(2^2, 3^t - 1) = 2\gcd(2^2, 3^t - 1), & s = 2, \\ \gcd(2^2, 3^t - 1) \cdot \gcd(2^{s-2}, 3^t - 1) \cdot \gcd(2^{s-1}, 3^t - 1), & s \geqslant 3. \end{cases}$$

Let

$$B(t,n) = C(t,2^s,n)\prod_{q_j\,|n}([\gcd(q_j^{\alpha_j-1},3^t-1)]^2\cdot\gcd(q_j^2-1,3^t-1))$$
$$\times\prod_{p_k\,|n}([\gcd(p_k^{\beta_k-1},3^t-1)]^2\cdot[\gcd(p_k-1,3^t-1)]^2).$$

Then

$$A_t(\Gamma_1(n)) = \frac{1}{t}\Bigg[B(t,n)-\sum_{\substack{d|t\\ d\neq t}} dA_d(\Gamma_1(n))\Bigg].$$

Proof. Part (1) follows from Theorem 2.1. The proof of part (2) is similar to the proof of [5, Theorem 5.6] upon making use of Lemma 1.3 in this paper. □

As immediate applications of Theorem 2.3, we will compute $A_t(\Gamma_1(n))$ for $n=2^m$, 3^m and 5^m, respectively, where $m\geqslant 1$, in Theorems 2.4, 2.5 and 2.6.

Theorem 2.4.

(1) *Each component of* $\Gamma_1(2^m)$ *is precisely a cycle with* 1 *or* 2 *vertices for* $m=1,2,3$. *Each component of* $\Gamma_1(2^m)$ *is precisely a cycle with* 2^k *vertices for* $m\geqslant 4$, *where* $k=0,1,\ldots,m-3$.

(2) $A_1(\Gamma_1(2))=2$; $A_1(\Gamma_1(2^2))=4$, $A_2(\Gamma_1(2^2))=2$; $A_1(\Gamma_1(2^3))=8$, $A_2(\Gamma_1(2^3))=12$; $A_1(\Gamma_1(2^4))=8$, $A_2(\Gamma_1(2^4))=60$.

(3) *Let* $m\geqslant 5$. *Then* $A_1(\Gamma_1(2^m))=8$, $A_2(\Gamma_1(2^m))=124$, $\ldots$, $A_{2^k}(\Gamma_1(2^m))=3\times 2^{k+4}$ $(2\leqslant k\leqslant m-4)$, $A_{2^{m-3}}(\Gamma_1(2^m))=2^{m+1}$.

Theorem 2.5. *For* $m\geqslant 1$, $A_1(\Gamma_1(3^m))=2$, $A_2(\Gamma_1(3^m))=3$, $A_t(\Gamma_1(3^m))=0$ *for* $t\geqslant 3$.

Theorem 2.6.

(1) *The lengths of the cycles in* $\Gamma_1(5)$ *are precisely* 1 *and* 2. *For* $m\geqslant 2$, *the lengths of the cycles in* $\Gamma_1(5^m)$ *are precisely* 1, 2 *and* $4\times 5^{s-1}$, *where* $s=1,\ldots,m-1$.

(2) $A_1(\Gamma_1(5))=4$ *and* $A_2(\Gamma_1(5))=6$.

(3) *For* $m\geqslant 2$ *we have* $A_1(\Gamma_1(5^m))=4$, $A_2(\Gamma_1(5^m))=6$, $A_{4\times 5^{s-1}}(\Gamma_1(5^m))=96\times 5^{s-1}$, *where* $s=1,\ldots,m-1$.

Next, we turn to the study of the properties of $\Gamma_2(n)$. First, it is easy to show that if $\mathbb{Z}_n[\mathrm{i}]$ is a local ring, then $\Gamma_2(n)$ has a unique component containing the 1-cycle with $\overline{0}$ as its only vertex. By Lemma 1.2 (2), (3), Corollary 2.2 and the following Theorem 2.7, it suffices to consider the case of n being a power of a prime congruent to 1 modulo 4.

Theorem 2.7. *Let* $n = \prod_{j=1}^{s} p_j^{k_j}$ *be the prime power decomposition of* n, *and* $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}_n[\mathrm{i}]$, *where* $\alpha_j \in \mathbb{Z}_{p_j^{k_j}}[\mathrm{i}]$ *for* $j = 1, \ldots, s$. *Then*

(1) *α lies on a t-cycle of $\Gamma(n)$ if and only if α_j lies on a t_j-cycle of $\Gamma(p_j^{k_j})$, where* $\mathrm{lcm}[t_1, \ldots, t_s] = t$;

(2) *α lies on a t-cycle of $\Gamma_2(n)$ if and only if α_j lies on a t_j-cycle of $\Gamma(p_j^{k_j})$, where* $\mathrm{lcm}[t_1, \ldots, t_s] = t$ *and* $\alpha_d \in \mathrm{D}(\mathbb{Z}_{p_d^{k_d}}[\mathrm{i}])$ *for some* $d \in \{1, \ldots, s\}$.

Proof. (1) Suppose that α lies on a t-cycle of $\Gamma(n)$. Then t is the least positive integer such that $\alpha^{3^t} = \alpha$. Hence, for $j = 1, \ldots, s$, we have $\alpha_j^{3^t} = \alpha_j$. Therefore, α_j lies on a t_j-cycle of $\Gamma(p_j^{k_j})$, and t_j is the least positive integer such that $\alpha_j^{3^{t_j}} = \alpha_j$, thus $t_j \leqslant t$. Moreover, by $\alpha_j^{3^t} = \alpha_j = \alpha_j^{3^{t_j}}$ we derive $t_j \mid t$. Finally, it is easy to see that $\mathrm{lcm}[t_1, \ldots, t_s] = t$.

Conversely, suppose that α_j lies on a t_j-cycle of $\Gamma(p_j^{k_j})$, $j = 1, \ldots, s$. Since $\mathrm{lcm}[t_1, \ldots, t_s] = t$, let $t = t_j \times m_j$. Then

$$\alpha^{3^t} = (\alpha_1^{3^t}, \ldots, \alpha_s^{3^t}) = (\alpha_1^{3^{t_1 \times m_1}}, \ldots, \alpha_s^{3^{t_s \times m_s}}) = (\alpha_1, \ldots, \alpha_s) = \alpha.$$

(2) Since $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathrm{D}(\mathbb{Z}_n[\mathrm{i}])$ if and only if $\alpha_d \in \mathrm{D}(\mathbb{Z}_{p_d^{k_d}}[\mathrm{i}])$ for some $d \in \{1, \ldots, s\}$, by part (1) above the result follows. $\square$

Theorem 2.8. *Let* $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$, *where* $\alpha \neq \overline{0}$ *and* p *is a prime congruent to* 1 *modulo* 4, $m \geqslant 1$. *Then*

(1) *α lies on a t-cycle of $\Gamma_2(p^m)$ if and only if $p^m \mid N(\alpha)$, $p \nmid \gcd(a, b)$ and t is the least positive integer such that* $(2a)^{3^t - 1} \equiv 1 \pmod{p^m}$;

(2) *α lies on a t-cycle of $\Gamma_2(p^m)$ if and only if $p^m \mid N(\alpha)$, $p \nmid \gcd(a, b)$ and* $t = \mathrm{ord}_{o(2a)} 3$.

Proof. (1) Suppose that α lies on a t-cycle of $\Gamma_2(p^m)$. Then $\alpha \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$, which implies that $p \mid N(\alpha)$ and hence $p^m \mid N(\alpha)$ due to Theorem 2.1 (3). If $p \mid \gcd(a, b)$, then there exists a positive integer j such that $\alpha^{3^j} = \overline{0}$, hence $\alpha = \overline{0}$, which is a contradiction. So we have $p \nmid \gcd(a, b)$ and clearly $p \nmid a$, $p \nmid b$. Furthermore, by $\alpha^3 = (\overline{a^3} - \overline{3ab^2}) + (\overline{3a^2b} - \overline{b^3})\mathrm{i}$ we have $\alpha^3 = 4(\overline{a^3} - \overline{b^3}\mathrm{i})$ because $p^m \mid N(\alpha)$. We observe that α^{3^d} lies on the t-cycle for $d \geqslant 0$, hence

$$\alpha^{3^t} = 4^{\sum\limits_{s=0}^{t-1} 3^s}(\overline{a^{3^t}} + (-1)^t\overline{b^{3^t}}\mathrm{i}) = 2^{3^t-1}(\overline{a^{3^t}} + (-1)^t\overline{b^{3^t}}\mathrm{i}). \tag{2.5}$$

Since $\alpha^{3^t} = \alpha$, by (2.5) we derive that $2^{3^t-1}a^{3^t} \equiv a \pmod{p^m}$ and $(-1)^t 2^{3^t-1}b^{3^t} \equiv b \pmod{p^m}$. Therefore,

$$(2a)^{3^t-1} \equiv 1 \pmod{p^m}, \quad (2b)^{3^t-1} \equiv (-1)^t \pmod{p^m}. \tag{2.6}$$

Let λ be the least positive integer which satisfies

$$(2a)^{3^\lambda-1} \equiv 1 \pmod{p^m}. \tag{2.7}$$

By (2.6), $\lambda \mid t$. Moreover, note that $(2a)^{3^g-1} \equiv (-1)^g(2b)^{3^g-1} \pmod{p^m}$ for any positive integer g because $a^2 \equiv -b^2 \pmod{p^m}$. Therefore, by (2.7), we have $(2b)^{3^\lambda-1} \equiv (-1)^\lambda \pmod{p^m}$ and hence $\alpha^{3^\lambda} = \alpha$. Since t is the least positive integer such that $\alpha^{3^t} = \alpha$, thus $t \mid \lambda$ and therefore $\lambda = t$.

Conversely, suppose that $p^m \mid N(\alpha)$, $p \nmid \gcd(a,b)$ and t is the least positive integer such that $(2a)^{3^t-1} \equiv 1 \pmod{p^m}$. We immediately see that $(2b)^{3^t-1} \equiv (-1)^t \pmod{p^m}$. So we have $\alpha^{3^t} = \alpha$ and therefore α lies on a λ-cycle of $\Gamma_2(p^m)$, where $\lambda \mid t$. Then by the above proof of necessity we have that λ is the least positive integer which satisfies (2.7), and hence $\lambda = t$. Thus α lies on a t-cycle of $\Gamma_2(p^m)$.

(2) If $p^m \mid N(\alpha)$ and $p \nmid \gcd(a,b)$, then clearly $p \nmid a$. So $2a \in \mathrm{U}(\mathbb{Z}_{p^m}[\mathrm{i}])$. By Corollary 2.2 and part (1) above, the result follows. □

Corollary 2.9. *Let p be a prime congruent to 1 modulo 4, $m \geqslant 1$.*

(1) *There exists a t-cycle in $\Gamma_2(p^m)$ if and only if the following two conditions hold:*
  (a) *$t = \mathrm{ord}_d 3$ for some positive divisor d of $\lambda(p^m)$, where $3 \nmid d$.*
  (b) *There exists $b \in \mathrm{U}(\mathbb{Z}_{p^m})$ such that $p^m \mid (2^{-1}a)^2 + b^2$, where $a \in \mathrm{U}(\mathbb{Z}_{p^m})$ and $o(a) = d$, while 2^{-1} is the inverse of 2 in $\mathbb{Z}_{p^m}$.*

(2) *Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$, $p \nmid \gcd(a,b)$ and $p^m \mid N(\alpha)$. Then α lies on a t-cycle of $\Gamma_2(p^m)$ if and only if $\beta = \overline{2a}$ lies on a t-cycle of $\Gamma_1(p^m)$.*

(3) *$\alpha = \overline{a} + \overline{b}\mathrm{i}$ ($\alpha \neq \overline{0}$) lies on a 1-cycle of $\Gamma_2(p^m)$ if and only if $\beta = \overline{b} + \overline{a}\mathrm{i}$ lies on a 2-cycle of $\Gamma_2(p^m)$.*

(4) *$A_1(\Gamma_2(p^m)) = 5$, $A_2(\Gamma_2(p^m)) = 2$ for $m \geqslant 1$.*

(5) *If $p \equiv 5 \pmod{12}$, then $\alpha = \overline{a} + \overline{b}\mathrm{i}$ ($\neq \overline{0}$) lies on a cycle of $\Gamma_2(p^m)$ if and only if $p \nmid \gcd(a,b)$ and $p^m \mid N(\alpha)$.*

P r o o f. Parts (1) and (2) follow easily from Theorem 2.8.

(3) It follows from the proof of Theorem 2.8 that if $\alpha^3 = \alpha$, then $\beta^3 = -\beta$ and $\beta^9 = (-\beta)^3 = \beta$. Part (3) now follows.

(4) Note that $\overline{0}$ is a vertex in a 1-cycle. Suppose that $\alpha \neq \overline{0}$ and $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$. Then by Theorem 2.8 (2), α is a vertex in a 1-cycle if and only if $p^m \mid N(\alpha)$, $p \nmid \gcd(a,b)$ and $\mathrm{ord}_{o(2a)} 3 = 1$. Clearly, $\mathrm{ord}_{o(2a)} 3 = 1$ if and only if $o(2a) = 1$ or 2. Thus, $2a \equiv 1$ or $-1 \pmod{p^m}$. Moreover, $N(\alpha) \equiv a^2 + b^2 \equiv 0 \pmod{p^m}$ if and only if $b \equiv ra \pmod{p^m}$, where $r^2 \equiv -1 \pmod{p^m}$. Since $p \equiv 1 \pmod 4$, there exist exactly two values for r modulo p^m. Thus, there exist exactly 4 nonzero vertices $\alpha \in \mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$ such that α is a vertex in a 1-cycle. Hence, $A_1(\Gamma_2(p^m)) = 5$.

Now note that $\mathrm{ord}_{o(2a)} 3 = 2$ if and only if $o(2a) = 4$ or 8. By an argument similar to that given above, we see that there are exactly 4 vertices in $\mathrm{D}(\mathbb{Z}_{p^m}[\mathrm{i}])$ that are parts of 2-cycles. Hence, $A_2(\Gamma_2(p^m)) = 2$.

(5) Note that if $p \equiv 5 \pmod{12}$, then $3 \nmid \lambda(p^m)$. The rest of part (5) follows from Theorem 2.8. □

3. Height

For $m \geqslant 0$, we say a vertex α in $\Gamma(n)$ or $\Gamma_g(G)$ (G is a finite abelian group) is of height m if m is the least nonnegative integer such that α^{3^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. The height of a component is the largest height of all vertices lying in this component. In this section, we will study the heights of components and vertices of $\Gamma(n)$. First, we have the following lemma which is proved similarly to [8, Theorem 3.2].

Lemma 3.1. *Let $G = C_{n_1} \times \ldots \times C_{n_s}$, where $s \geqslant 1$ and $C_{n_1}, \ldots, C_{n_s}$ are cyclic groups of order $n_1, \ldots, n_s$, respectively. Then the height of each component of $\Gamma_g(G)$ is equal to $\max\{h_1, \ldots, h_s\}$, where $3^{h_j} \parallel n_j$ for $j = 1, \ldots, s$.*

Theorem 3.2. *Let $n = 2^t 3^m q_1^{k_1} \ldots q_s^{k_s} p_1^{j_1} \ldots p_r^{j_r}$, where $t, m \geqslant 0$, $k_1, \ldots, k_s$, $j_1, \ldots, j_r \geqslant 1$, $q_1, \ldots, q_s$ are distinct primes congruent to 3 modulo 4 ($q_a \neq 3$ for $a = 1, \ldots, s$), while $p_1, \ldots, p_r$ are distinct primes congruent to 1 modulo 4. Suppose $3^{\lambda_a} \parallel q_a^2 - 1$ for $a = 1, \ldots, s$, and $3^{l_c} \parallel p_c - 1$ for $c = 1, \ldots, r$. Then the height of each component of $\Gamma_1(n)$ is equal to $\max\{m-1, \lambda_1, \ldots, \lambda_s, l_1, \ldots, l_r\}$.*

P r o o f. By Lemmas 1.1, 1.3 and 3.1, the result follows. □

Theorem 3.3. *Let* $n = \prod_{j=1}^{s} p_j^{k_j}$ *be the prime power decomposition of* n, $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}_n[\mathrm{i}]$, *where* $\alpha_j \in \mathbb{Z}_{p_j^{k_j}}[\mathrm{i}]$ *for* $j = 1, \ldots, s$. *Then the height* h_α *of* α *is equal to* $\max\{h_{\alpha_1}, \ldots, h_{\alpha_s}\}$, *where* h_{α_j} *is the height of* α_j *in* $\Gamma(p_j^{k_j})$, $j \in \{1, \ldots, s\}$.

Proof. If $h_{\alpha_1} = \ldots = h_{\alpha_s} = 0$, i.e., α_j lies on a cycle of $\Gamma(p_j^{k_j})$ for $j = 1, \ldots, s$, then by Theorem 2.7 (1), α lies also on a cycle of $\Gamma(n)$. Hence, $h_\alpha = 0$.

Now suppose that at least one of $h_{\alpha_1}, \ldots, h_{\alpha_s}$ is not equal to 0. Let $m = \max\{h_{\alpha_1}, \ldots, h_{\alpha_s}\} > 0$, where $m = h_{\alpha_x}$ for some $x \in \{1, \ldots, s\}$. Since the height of α_j in $\Gamma(p_j^{k_j})$ is h_{α_j}, clearly $\alpha_j^{3^{d_j}}$ lies on a cycle of $\Gamma(p_j^{k_j})$ for $d_j \geqslant h_{\alpha_j}$. Note that $\alpha^{3^m} = (\alpha_1^{3^m}, \ldots, \alpha_s^{3^m})$ and $m \geqslant h_{\alpha_j}$ for $j \in \{1, \ldots, s\}$, we derive that α^{3^m} lies on a cycle of $\Gamma(n)$ due to Theorem 2.7 (1). If the height of α is h with $h < m$, then α^{3^h} lies on a cycle of $\Gamma(n)$, which implies that $\alpha_x^{3^h}$ lies on a cycle of $\Gamma(p_x^{k_x})$. This is impossible, because $h_{\alpha_x} = m$ is the least nonnegative integer such that $\alpha_x^{3^m}$ lies on a cycle of $\Gamma(p_x^{k_x})$. Therefore, we can conclude that the height of α is m. The theorem follows. □

By Lemma 1.1, we see that any vertex in $\Gamma_g(C_n)$ of in-degree 0 has the same height. So we are interested in the similar problem which is proved in the next theorem.

Theorem 3.4. *Let* q_j $(q_j \neq 3)$ *be primes congruent to* 3 *modulo* 4 *for* $j \geqslant 1$, *let* p_s *be primes congruent to* 1 *modulo* 12 *for* $s \geqslant 1$, *and let* g_λ *be primes congruent to* 5 *modulo* 12 *for* $\lambda \geqslant 1$. *Then the height of any vertex in* $\Gamma_1(n)$ *of in-degree* 0 *is equal to a fixed positive integer* w *if and only if* n *is of the form*

$$n = 2^k 3^t \prod_{j=1}^{e} q_j^{a_j} \prod_{s=1}^{m} p_s^{b_s} \prod_{\lambda=1}^{l} g_\lambda^{r_\lambda} \tag{3.1}$$

where $t \in \{0, 1, w+1\}$, $k, e, m, l \geqslant 0$, $e + m \geqslant 1$ *if* $t \in \{0, 1\}$, $a_j, b_s, r_\lambda \geqslant 1$, *while* $3^w \parallel q_j^2 - 1$ *for* $j \in \{1, \ldots, e\}$ *and* $3^w \parallel p_s - 1$ *for* $s \in \{1, \ldots, m\}$.

Proof. By [9, Theorem 3.7], each component in $\Gamma_1(n)$ is exactly a cycle if and only if $n = 2^k 3^t \prod_{\lambda=1}^{l} g_\lambda^{r_\lambda}$, where $k, l \geqslant 0$, $t \in \{0, 1\}$, $r_\lambda \geqslant 1$. Hence, by Lemma 1.4, it suffices to consider the vertex of in-degree 0 in $\Gamma_1(3^t)$ $(t \geqslant 2)$, $\Gamma_1(q_j^{a_j})$ and $\Gamma_1(p_s^{b_s})$.

By Lemma 1.3 (2), $\mathrm{U}(\mathbb{Z}_{3^t}[\mathrm{i}]) \cong Z_{3^{t-1}} \times Z_{3^{t-1}} \times Z_8$. It follows from Lemma 1.1 that for $a \in Z_{3^{t-1}}$, $\mathrm{indeg}(a) = 0$ in $\Gamma_g(Z_{3^{t-1}})$ $(t \geqslant 2)$ if and only if $h_a = t - 1$, while there exist no vertices in $\Gamma_g(Z_8)$ with in-degree 0. Therefore, by Theorem 3.3, for $\alpha \in \mathrm{U}(\mathbb{Z}_{3^t}[\mathrm{i}])$, $\mathrm{indeg}(\alpha) = 0$ if and only if $h_\alpha = t - 1$. Similarly, we derive that for $\beta_j \in \mathrm{U}(\mathbb{Z}_{q_j^{a_j}}[\mathrm{i}])$, $\mathrm{indeg}(\beta_j) = 0$ if and only if $h_{\beta_j} = u_j$, where $3^{u_j} \parallel q_j^2 - 1$. For $\gamma_s \in \mathrm{U}(\mathbb{Z}_{p_s^{b_s}}[\mathrm{i}])$, $\mathrm{indeg}(\gamma_s) = 0$ if and only if $h_{\gamma_s} = v_s$, where $3^{v_s} \parallel p_s - 1$. Hence, the theorem follows from Theorem 3.3. □

Next, we will investigate the height of vertices in $\Gamma_2(n)$, where n is a power of a prime.

Theorem 3.5. *Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{2^t}[\mathrm{i}])$, $t \geqslant 1$. Then the height h_α of α is*

$$h_\alpha = \begin{cases} \lceil \log_3 t/k \rceil, & 2^x \parallel a,\ 2^y \parallel b,\ x, y \geqslant 1,\ x \neq y,\ k = \min\{x, y\}, \\ \lceil \log_3 (2t+1)/(2k+1) \rceil, & 2^k \parallel a,\ 2^k \parallel b,\ k \geqslant 0. \end{cases}$$

Proof. First of all, we observe that $\Gamma_2(2^t)$ has a unique component because $\mathbb{Z}_{2^t}[\mathrm{i}]$ is a local ring. It follows from Lemma 1.2 (1) that $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{2^t}[\mathrm{i}])$ if and only if $2 \mid a^2 + b^2$, if and only if a and b have the same parity.

Let $2^x \parallel a$ and $2^y \parallel b$, where $x, y \geqslant 0$. Set $k = \min\{x, y\} \geqslant 0$. Then $\alpha = 2^k(\overline{a_0} + \overline{b_0}\mathrm{i})$ for some integers a_0 and b_0, and clearly $2 \nmid \gcd(a_0, b_0)$.

First, suppose $x \neq y$. Then clearly $(\overline{a_0} + \overline{b_0}\mathrm{i})^{3^j} \in \mathrm{U}(\mathbb{Z}_{2^t}[\mathrm{i}])$ for $j \geqslant 0$. Therefore, $\alpha^{3^j} = (2^k)^{3^j}(\overline{a_0} + \overline{b_0}\mathrm{i})^{3^j} = \overline{0}$ if and only if $3^j k \geqslant t$, if and only if $j \geqslant \log_3 t/k$. So we have $h_\alpha = \lceil \log_3 t/k \rceil$.

Secondly, suppose $x = y$. Then $\alpha = 2^k \alpha_0$, where $\alpha_0 = \overline{a_0} + \overline{b_0}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{2^t}[\mathrm{i}])$, $2 \nmid a_0$ and $2 \nmid b_0$. Since $\alpha_0^3 = \overline{a_0}(\overline{a_0^2 - 3b_0^2}) + \overline{b_0}(\overline{3a_0^2 - b_0^2})\mathrm{i}$, we derive that $\alpha_0^3 = 2(\overline{a_1} + \overline{b_1}\mathrm{i})$ where $2 \nmid a_1$ and $2 \nmid b_1$ because $2 \parallel a_0^2 - 3b_0^2$ and $2 \parallel 3a_0^2 - b_0^2$. Similarly, $(\overline{a_1} + \overline{b_1}\mathrm{i})^3 = 2(\overline{a}_2 + \overline{b_2}\mathrm{i})$ where $2 \nmid a_2$ and $2 \nmid b_2$. Therefore, we have

$$\alpha_0^{3^j} = 2^{\sum\limits_{m=0}^{j-1} 3^m}(\overline{a_j} + \overline{b_j}\mathrm{i}) = 2^{(3^j-1)/2}(\overline{a_j} + \overline{b_j}\mathrm{i}),$$

where $2 \nmid a_j$ and $2 \nmid b_j$, $j \geqslant 1$. Hence, $\alpha^{3^j} = (2^k)^{3^j}\alpha_0^{3^j} = 2^{3^j k + (3^j-1)/2}(\overline{a_j} + \overline{b_j}\mathrm{i})$, which implies that $\alpha^{3^j} = \overline{0}$ if and only if $3^j k + \frac{1}{2}(3^j - 1) \geqslant t$, if and only if $j \geqslant \log_3(2t+1)/(2k+1)$. So we have $h_\alpha = \lceil \log_3(2t+1)/(2k+1) \rceil$. □

Theorem 3.6. *Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{q^t}[\mathrm{i}])$, where q is a prime congruent to 3 modulo 4, $t \geqslant 2$. Then the height of α is $h_\alpha = \lceil \log_3 t/k \rceil$, where $q^x \parallel a$ and $q^y \parallel b$, $x, y \geqslant 1$ and $k = \min\{x, y\}$.*

Proof. First, we observe that $\Gamma_2(q^t)$ has a unique component because $\mathbb{Z}_{q^t}[\mathrm{i}]$ is a local ring for $t \geqslant 1$. It follows from Lemma 1.2 (1) and $q \equiv 3 \pmod 4$ that $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{q^t}[\mathrm{i}])$ if and only if $q \mid \gcd(a, b)$. Let $q^x \parallel a$ and $q^y \parallel b$, where $x, y \geqslant 1$. Set $k = \min\{x, y\}$. Then $\alpha = q^k(\overline{a_0} + \overline{b_0}\mathrm{i})$ for some integers a_0 and b_0, and clearly $q \nmid \gcd(a_0, b_0)$. Hence, $(\overline{a_0} + \overline{b_0}\mathrm{i})^{3^j} \in \mathrm{U}(\mathbb{Z}_{q^t}[\mathrm{i}])$ for $j \geqslant 0$. Therefore, $\alpha^{3^j} = \overline{0}$ if and only if $3^j k \geqslant t$, if and only if $j \geqslant \log_3 t/k$. So we have $h_\alpha = \lceil \log_3 t/k \rceil$. □

Theorem 3.7. *Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^t}[\mathrm{i}])$, where p is a prime congruent to* 1 *modulo* 4, $t \geqslant 1$. *Then the height h_α of α is*

$$h_\alpha = \begin{cases} \lceil \log_3 t/k \rceil, & p^x \parallel a,\ p^y \parallel b,\ x, y \geqslant 1,\ k = \min\{x, y\}, \\ j, & p \nmid a,\ p \nmid b, \text{ and } j \text{ is the least nonnegative integer} \\ & \text{such that both } p^t \mid (N(\alpha))^{3^j} \text{ and } 3 \nmid o(2\,\mathrm{Re}(\alpha^{3^j})). \end{cases}$$

P r o o f. Since $p \equiv 1 \pmod 4$, by Lemma 1.2 (1), $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^t}[\mathrm{i}])$ if and only if $p \mid a^2 + b^2$.

Case 1. Let $p^x \parallel a$ and $p^y \parallel b$, where $x, y \geqslant 1$. Then $\alpha^{3^j} = \overline{0}$ for some $j \geqslant 1$. Set $k = \min\{x, y\}$. Then $\alpha = p^k(\overline{a_0} + \overline{b_0}\mathrm{i})$ for some integers a_0 and b_0, and clearly $p \nmid \gcd(a_0, b_0)$. Let $(\overline{a_0}+\overline{b_0}\mathrm{i})^3 = \overline{a_1}+\overline{b_1}\mathrm{i}$, where $a_1 = a_0(a_0^2-3b_0^2)$ and $b_1 = b_0(3a_0^2-b_0^2)$. We can claim that $p \nmid \gcd(a_1, b_1)$. This is because, by virtue of $p \nmid \gcd(a_0, b_0)$, if exactly one of a_0 and b_0 is not divisible by p, then without loss of generality we may assume that $p \mid a_0$ while $p \nmid b_0$, hence obviously $p \nmid b_0(3a_0^2 - b_0^2)$, i.e., $p \nmid b_1$. On the other hand, if $p \nmid a_0$ and $p \nmid b_0$, assume that $p \mid \gcd(a_1, b_1)$, i.e., $a_0(a_0^2 - 3b_0^2) \equiv b_0(3a_0^2 - b_0^2) \equiv 0 \pmod p$. Then we derive that $3a_0^2 - 9b_0^2 \equiv 3a_0^2 - b_0^2 \equiv 0 \pmod p$ and hence $8b_0^2 \equiv 0 \pmod p$, which is impossible. Therefore, we must have $p \nmid \gcd(a_1, b_1)$. Similarly, we have $\alpha^{3^j} = p^{3^j k}(\overline{a_j} + \overline{b_j}\mathrm{i})$ with $p \nmid \gcd(a_j, b_j)$ for $j \geqslant 0$. Therefore, $\alpha^{3^j} = \overline{0}$ if and only if $3^j k \geqslant t$, if and only if $j \geqslant \log_3 t/k$. Thus $h_\alpha = \lceil \log_3 t/k \rceil$.

Case 2. Let $p \mid a^2 + b^2$ while $p \nmid \gcd(a, b)$. Then $\alpha^{3^j} \neq \overline{0}$ for $j \geqslant 0$ and it is easy to check that if $\alpha^{3^j} = \overline{c} + \overline{d}\mathrm{i}$ then $p \nmid c$ and $p \nmid d$. Moreover, since $N(\alpha^{3^j}) \equiv N(\alpha)^{3^j} \pmod{p^t}$, by Theorem 2.8, α^{3^j} lies on a cycle of $\Gamma_2(p^t)$ if and only if j is the least nonnegative integer such that both $p^t \mid (N(\alpha))^{3^j}$ and $3 \nmid o(2\,\mathrm{Re}(\alpha^{3^j}))$. Hence, the result follows. □

By Corollary 2.9 (5) and Theorem 3.7, if p is a prime congruent to 5 modulo 12, the formula of the height of any vertex in $\Gamma_2(p^t)$ is as follows.

Corollary 3.8. *Let $\alpha = \overline{a} + \overline{b}\mathrm{i} \in \mathrm{D}(\mathbb{Z}_{p^t}[\mathrm{i}])$, where p is a prime congruent to* 5 *modulo* 12, $t \geqslant 1$. *Then the height h_α of α is*

$$h_\alpha = \begin{cases} \lceil \log_3 t/k \rceil, & p^x \parallel a,\ p^y \parallel b,\ x, y \geqslant 1,\ k = \min\{x, y\}, \\ j, & p \nmid a,\ p \nmid b,\ p^t \parallel (N(\alpha))^{3^j}. \end{cases}$$

Acknowledgement. The authors would like to thank the referee for valuable suggestions. The referee improved the statements of Theorems 2.3, 2.6 and 2.7, improved the proofs of Theorem 2.7 and Corollary 2.9, and provided a new reference [5] for this paper.

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

[3] *Y. Meemark, N. Wiroonsri*: The quadratic digraph on polynomial rings over finite fields. Finite Fields Appl. *16* (2010), 334–346.

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

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

[6] *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.

[7] *G. H. Tang, H. D. Su, Z. Yi*: Structure of the unit group of $\mathbb{Z}_n[\mathrm{i}]$. J. Guangxi Norm. Univ., Nat. Sci. *28* (2010), 38–41. (In Chinese.)

[8] *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.

[9] *Y. J. Wei, J. Z. Nan, G. H. Tang*: The cubic mapping graph for the ring of Gaussian integers modulo n. Czech. Math. J. *61* (2011), 1023–1036.

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.