# ไดกราฟของการส่งกำลังสองบนจำนวนเต็มเกาส์เซียน

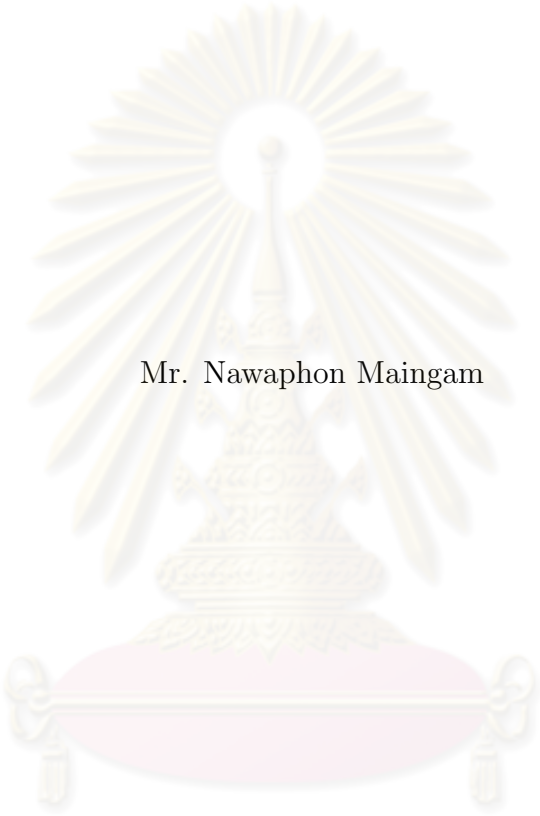
นายนวพล หมายงาม



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

# THE DIGRAPH OF THE SQUARE MAPPING ON GAUSSIAN INTEGERS

Mr. Nawaphon Maingam





A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics
Faculty of Science
Chulalongkorn University
Academic Year 2010

| | |
|---|---|
| Thesis Title | THE DIGRAPH OF THE SQUARE MAPPING ON GAUSSIAN INTEGERS |
| By | Mr. Nawaphon Maingam |
| Field of Study | Mathematics |
| Thesis Advisor | Assistant Professor Yotsanan Meemark, Ph.D. |

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

S. Hannongbua ..... Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

Ajchara Hamchoowong ..... Chairman

(Associate Professor Ajchara Hamchoowong, Ph.D.)

Yotsanan Meemark ..... Thesis Advisor

(Assistant Professor Yotsanan Meemark, Ph.D.)

..... Examiner

(Assistant Professor Chariya Uiyyasathian, Ph.D.)

Nittiya Pabhapote ..... External Examiner

(Associate Professor Nittiya Pabhapote, Ph.D.)

นวพล หมายงาม : ไดกราฟของการส่งกำลังสองบนจำนวนเต็มเกาส์เซียน. (THE DIGRAPH OF THE SQUARE MAPPING ON GAUSSIAN INTEGERS) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : ผู้ช่วยศาสตราจารย์ ดร. ยศนันต์ มีมาก, 32 หน้า.

ในวิทยานิพนธ์นี้ เราศึกษาโครงสร้างของไดกราฟ $G_\gamma^2$ ที่นิยามจากการส่งกำลังสองบนริงของจำนวนเต็มเกาส์โดยอาศัยเครื่องมือหลักคือเลขชี้กำลังของกรุปยูนิตมอดุโล $\gamma$ โดยเราพบความเชื่อมโยงของความยาววัฏจักรกับเลขชี้กำลังของกรุปยูนิต นอกจากนี้ เรายังได้สูตรของจำนวนจุดตรึงและระยะทางมากสุดจากจุดไปยังวัฏจักรบนแต่ละองค์ประกอบของไดกราฟนี้



ภาควิชา.....คณิตศาสตร์..... ลายมือชื่อนิสิต.....นวพล หมายงาม.....

สาขาวิชา.....คณิตศาสตร์..... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก.....

ปีการศึกษา.....2553..... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์ร่วม.....-.....

##5172334023 : MAJOR MATHEMATICS
KEYWORDS : CHINESE REMAINDER THEOREM / DIGRAPHS / EXPONENTS / GAUSSIAN INTEGERS

NAWAPHON MAINGAM : THE DIGRAPH OF THE SQUARE MAPPING ON GAUSSIAN INTEGERS. THESIS ADVISOR : ASSISTANT PROFESSOR YOTSANAN MEEMARK, Ph.D., 32 pp.

In this work, we investigate the structure of the digraph $G_\gamma^{(2)}$ associated with the square mapping on the ring of Gaussian integers by using the exponent of the unit group modulo $\gamma$. The formula for the fixed points of $G_\gamma^{(2)}$ is established. Some connections of the lengths of cycles with the exponent of the unit group modulo $\gamma$ are presented. Furthermore, we study the maximum distance from the cycle on each component.



Department : ....Mathematics.... Student's Signature : Nawaphon Maingam
Field of Study : ....Mathematics.... Advisor's Signature : Yotsanan Meemark.
Academic Year : .....2010..... Co-Advisor's Signature : .....

# ACKNOWLEDGEMENTS

Since the thesis is done beautifully and it met my expectations, I would not have fulfilled without supports from these people. First and foremost, I am deeply indepted to Assistant Professor Yotsanan Meemark, Ph.D., my thesis supervisor, for his kind, helpful suggestions and guidance. His assistance and careful reading are of great value to me in the preparation and completion of this thesis.

I would also like to express my gratitude to my thesis committees; Associate Professor Ajchara Harnchoowong, Ph.D., Associate Professor Nittiya Pabhapote, Ph.D. and Assistant Professor Chariya Uiyyasathian, Ph.D., for their valuable comments and to all teachers who have taught me all along.

Last but not least, I would like to thank my family and my dear friends for their love, understanding, encouragement, and constant inspiration throughtout my study.

# CONTENTS

# CHAPTER I

# PRELIMINARIES

## 1.1 Introduction

Let $\mathbb{Z}[i]$ be the ring of Gaussian integers. Let $\gamma = a + bi$ be a nonzero element in $\mathbb{Z}[i]$ and $\mathbb{Z}[i]/(\gamma)$ the quotient ring of $\mathbb{Z}[i]$ modulo $\gamma$. We know that $\mathbb{Z}[i]/(\gamma)$ is a commutative finite ring with $N(\gamma) = a^2 + b^2$, the *norm of* $\gamma$, elements (see, Theorem 4 of [3]). We denote its unit group by $(\mathbb{Z}[i]/(\gamma))^* = \{[\mu]_\gamma : [\mu]_\gamma \in \mathbb{Z}[i]/(\gamma) \text{ and } \gcd(\mu, \gamma) = 1\}$ whose structure is completely determined by Cross [2].

Let $G_\gamma^{(2)}$ be the digraph whose vertex set is $V_\gamma = \mathbb{Z}[i]/(\gamma)$ and the edge set is given by

$$E_\gamma^{(2)} = \{([\mu]_\gamma, [\mu^2]_\gamma) : [\mu] \in \mathbb{Z}[i]/(\gamma)\}.$$

For simplicity, we shall abuse notation by writing $\mu \in \mathbb{Z}[i]$ and considering it modulo $\gamma$. It is obvious that $G_\gamma^{(2)}$ has $a^2 + b^2$ vertices and exactly $a^2 + b^2$ directed edges.

This digraph is defined by using the idea of Somer and Křížek [6, 7] who studied the structure of digraphs $G(n)$ associated with a quadratic congruence modulo $n$. Their digraph $G(n)$ has the ring of integers modulo $n$, $\mathbb{Z}_n$, as a vertex set $V$ and there exists a directed edge from $a \in V$ to $b \in V$ if $b \equiv a^2 \mod n$. An application of this digraph on elliptic curves can be found in [4].

A *component* of a digraph is a subdigraph which is a maximal connected subgraph. The *indegree* [resp. *outdegree*] of a vertex $\mu \in V_\gamma$ of $G_\gamma^{(2)}$, is the number of directed edges entering [resp. leaving] the vertex $\mu$ and denoted by $\text{indeg}_\gamma \mu$ [resp. $\text{outdeg}_\gamma \mu$]. The definition of $G_\gamma^{(2)}$ implies that the outdegree of each vertex

is equal to 1. This yields the fact that each component has a unique cycle. We call a cycle of length one a *fixed point*. For an *isolated fixed point*, the indegree and outdegree are both one.

A cycle of length $t \geq 1$ is said to be a *t-cycle* and we assume that all cycles are oriented counterclockwise. The distance from a vertex $\mu \in V_\gamma$ to a cycle is the length of the directed path from $\mu$ to a vertex in the cycle.

It can be shown that every component of $G(n)$ contains a unique cycle (Proposition 1.1 of [7]). In addition, Somer and Křížek determined the number of fixed points, the number of cycles and distance from any vertex to the unique cycle in the component of $G(n)$ in §3 of [7]. Their main tool is the *Carmichael λ-function* $\lambda(n)$, which was first introduced in 1910 (see [1]). It turns out that $\lambda(n)$ is the universal order modulo $n$, i.e., $a^{\lambda(n)} \equiv 1 \mod n$ if and only if $\gcd(a, n) = 1$. Its properties are recalled in §2 of [7].

The *exponent* of a finite group $G$, $\exp G$, is the least positive integer $n$ such that $g^n = e$ for all $g \in G$. It plays the role of the universal order for a group. Note that $\exp G$ divides $|G|$. We briefly discuss some properties of the exponent of a group in our first theorem.

**Theorem 1.1.1.** *Let $G$ be a finite group and $H$ a subgroup of $G$.*

*(1)* $\exp G = \operatorname{lcm}\{o(a) : a \in G\}$, *where $o(a)$ is the order of $a$ in $G$.*

*(2)* $\exp H$ *divides* $\exp G$.

*(3) If* $G = G_1 \times G_2$, *then* $\exp G = \operatorname{lcm}\{\exp G_1, \exp G_2\}$.

*(4) If $G$ is abelian, then there exists a $g$ in $G$ such that* $o(g) = \exp G$.

*Proof.* (1) – (3) are clear. To prove (4), assume that $G$ is abelian. By the elementary divisor theorem, there exist positive integers $n_1, n_2, \ldots, n_t \geq 1$ such that $n_1 \mid n_2 \mid \cdots \mid n_t$ and

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}.$$

Thus, $\exp G = n_t$ and $(0, 0, \ldots, 0, 1)$ in the rightmost group has order $n_t$. □

Our goal is to replace the Carmichael $\lambda$-function with $\lambda(\gamma) = \exp(\mathbb{Z}[i]/(\gamma))^*$, the exponent of the unit group $(\mathbb{Z}[i]/(\gamma))^*$ and study the digraph $G_\gamma^{(2)}$, defined above. We obtain results analogous to the work of Somer and Křížek for the structure of our new digraphs.

The thesis is organized as follows. The next section recalls some properties of the quotient rings over the Gaussian integers including the formulas for computing the Carmichael $\lambda$-function (Proposition 1.2.6). Basic structures and semiregularity are presented in Section 2.1. Cycles, components and distances are studied in Section 2.2. The final chapter gives five examples of square mapping digraphs demonstrating the results in the previous chapters.

This work will appear in the International Journal of Number Theory [5].

## 1.2 Quotient Rings over the Gaussian Integers

Consider the meaning of divisibility and congruences in the Gaussian integer. Recall that in the Gaussian integer $\gamma \mid \beta$ means there is a Gaussian integers $\alpha$ such that $\alpha \cdot \gamma = \beta$, and $\alpha \equiv \beta \mod \gamma$ means that $\gamma \mid (\alpha - \beta)$. This congruence relation is an equivalence relation. Dresden and Dymàček [3] gave representatives for equivalence classes of the corresponding quotient ring of $\mathbb{Z}[i]$ modulo $\gamma$ in the following proposition.

**Proposition 1.2.1.** *If $d = \gcd(a, b)$ so that $\gamma = d(a_1 + b_1 i)$, then the equivalence classes of $\mathbb{Z}[i]/(\gamma)$ are $\{[x + yi]_\gamma : 0 \le x < d(a_1^2 + b_1^2), 0 \le y < d\}$.*

*Proof.* We first show that the equivalence classes are distinct. Let $[x_1 + y_1 i]_\gamma$ and $[x_2 + y_2 i]_\gamma$ be any equivalence classes of $\mathbb{Z}[i]/(\gamma)$. If $[x_1 + y_1 i]_\gamma = [x_2 + y_2 i]_\gamma$, then $d \mid (x_1 - x_2) + (y_1 - y_2)i$, so $d \mid y_2 - y_1$. But $|y_2 - y_1| < d$, hence $y_1 = y_2$. Now $\gamma \mid x_2 - x_1$; but the least rational integer that $\gamma$ divides is $d\,(a_1^2 + b_1^2)$ so either $|x_2 - x_1| \ge d\,(a_1^2 + b_1^2)$ or $x_2 = x_1$. Since the first of these is impossible by definition of representation, we have that $x_1 = x_2$. Therefore, the equivalence classes are distinct.

Finally, we demonstrate that any $x + yi$ falls into one of these equivalence classes. Now determine $q_1$ and $r$ so that $y = dq_1 + r$, where $0 \leq r < d$. Since $\gcd(a, b) = d$, there are integers $u$ and $v$ such that $av + bu = dq_1$. Now

$$x + yi - (a + bi)(u + vi) = x - au + bv + ri.$$

Determine $q_2$ and $s$ so that $x - au + bv = d(a_1^2 + b_1^2) q_2 + s, 0 \leq s < d(a_1^2 + b_1^2)$. Now

$$x + yi - (a + bi)(u + vi + q_2(a_1 - b_1)i) = s + ri;$$

that is $x + yi \equiv s + ri \mod \gamma, 0 \leq s < d(a_1^2 + b_1^2)$ and $0 \leq r < d$. Hence any Gaussian integer is congruent to an element of these equivalence classes. □

The above proposition yields an immediate corollary.

**Corollary 1.2.2.** *The cardinality of the equivalence classes of* $\mathbb{Z}[i]/(\gamma)$ *is* $N(\gamma) = d^2(a_1^2 + b_1^2) = a^2 + b^2$.

Note that there are four units in $\mathbb{Z}[i]$, namely $\pm 1$ and $\pm i$. Without any loss of generality, $\gamma$ can be restricted to being in the first quadrant. For, if $u$ is a unit, then the ideals $(\gamma)$ and $(u\gamma)$ coincide, so $\mathbb{Z}[i]/(\gamma) = \mathbb{Z}[i]/(u\gamma)$.

**Remark.** If $\gamma = a + bi$ is element of $\mathbb{Z}[i]$ its norm $N(\gamma)$, is defined to be $\gamma\bar{\gamma} = |\gamma|^2 = a^2 + b^2$, where $\bar{\gamma}$ is the complex-conjugate of $\gamma$.

Let $\gamma, \gamma_1$ and $\gamma_2$ be Gaussian integers. The following list contains the fundamental properties of the norm.

(1) If $\gamma$ is in $\mathbb{Z}$ as well as in $\mathbb{Z}[i]$, then $N(\gamma) = \gamma^2$.

(2) $N(\gamma_1\gamma_2) = N(\gamma_1) N(\gamma_2)$.

(3) $N(\gamma) = 1$ if and only if $\gamma$ is a unit.

(4) $N(\gamma)$
$$\begin{cases} = 0, & \text{if } \gamma = 0; \\ = 1, & \text{if } \gamma = \pm 1 \text{ or } \pm i; \\ > 1, & \text{otherwise.} \end{cases}$$

(5) If $N(\gamma)$ is prime in $\mathbb{Z}$, then $\gamma$ is prime in $\mathbb{Z}[i]$.

**Notation.** It is convenient in the classification to call two Gaussian integers *associates*, written $\alpha \sim \beta$, if $\alpha \mid \beta$ and $\beta \mid \alpha$, that is, if $\alpha = \beta\epsilon$ where $\epsilon$ is a unit.

**Lemma 1.2.3.** *If $q$ is a positive prime in $\mathbb{Z}$ of the form $4m+1$, then $q \mid (n^2+1)$, where $n = (2m)!$.*

*Proof.* Consider the two sets of numbers

$$-1, -2, ..., -2m$$

$$4m, 4m-1, ..., 2m+1.$$

Each element of the lower row is congruent modulo $q$ to the element of the upper row directly above, since their difference is $q$. Then

$$4m(4m-1)\cdots(2m+1) \equiv (-1)(-2)\cdots(-2m) \mod q.$$

which yields

$$(4m)! \equiv \{(2m)!\}^2 \mod q.$$

Let $n = (2m)!$. Since $(4m)! = (q-1)! \equiv -1 \mod q$ by Wilson's theorem, it follows that $n^2 \equiv -1 \mod q$. □

We now identify all primes in the Gaussian integers:

**Proposition 1.2.4.** *Up to multiplication by units, the primes in $\mathbb{Z}[i]$ are of three types:*

*(1) $p$, where $p$ is a prime in $\mathbb{Z}$ satisfying $p \equiv 3 \mod 4$;*

*(2) $\alpha = 1+i$ and*

*(3) $\pi$ or $\bar{\pi}$, where $q = \pi\bar{\pi}$ is a prime in $\mathbb{Z}$ satisfying $q \equiv 1 \mod 4$.*

*Proof.* To prove the proposition, we show first that any prime $\sigma$ in $\mathbb{Z}[i]$ divides exactly one positive rational prime $r$. For, $N(\sigma) = \sigma\bar{\sigma}$, so $\sigma \mid N(\sigma)$. Let $N(\sigma) = r_1 r_2 \cdots r_j$ be the factorization in $\mathbb{Z}$ of $N(\sigma)$ into positive primes. Then $\sigma \mid r_1 r_2 \cdots r_n$, so $\sigma$ divides one of the $r_j$. Thus, $\sigma$ divides at least one rational prime. Suppose $\sigma$ divides two distinct rational primes $r_1$ and $r_2$. Then there exist rational integers $x$ and $y$ such that

$$r_1 x + r_2 y = 1.$$

This gives $\sigma \mid 1$, so $\sigma$ is a unit, not a prime, which is a contradiction.

Hence, we can get each prime in $\mathbb{Z}[i]$ once and only once by considering the factorization of all positive rational primes, treated as elements of $\mathbb{Z}[i]$.

Now, let $\sigma$ be a prime in $\mathbb{Z}[i]$, and $r$ the positive rational prime for which $\sigma \mid r$. Then $N(\sigma) \mid N(r)$. But $N(r) = r^2$, since $r$ is a rational integer. Hence, $N(\sigma) = r$ or $N(\sigma) = r^2$. If $\sigma = x + yi$ then $x^2 + y^2 = r$ or $x^2 + y^2 = r^2$.

Divide $r$ by 4. According to the division algorithm, this leaves a remainder of $1, 2$ or 3. We consider the three cases separately.

*Case* 1. $r \equiv 3 \mod 4$. As stated just above, $x^2 + y^2 = r$ or $x^2 + y^2 = r^2$. It will be shown now that the first of theses two possibilities cannot occur. Since $r$ is odd, one of $x$ and $y$, say $x$, must be even, the other odd; otherwise the sum of their squares would be even. Let $x = 2a$, $y = 2b + 1$. If $x^2 + y^2 = r$,

$$\begin{aligned} r = x^2 + y^2 &= a^2 + (2b+1)^2 \\ &= 4\left(a^2 + b^2 + b\right) + 1 \equiv 1 \mod 4, \end{aligned}$$

whereas $r \equiv 3 \mod 4$. Thus, in this case $x^2 + y^2 = r^2$, and $N(\sigma) = N(r)$. Since $\sigma \mid r$, $r = \sigma\tau$, where $\tau \in \mathbb{Z}[i]$. Then $N(r) = N(\sigma) N(\tau), N(\tau) = 1, \tau$ is a unit, and $\sigma \sim r$. This accounts for the first part of Proposition 1.2.4.

*Case* 2. $r \equiv 2 \mod 4$. In this case $r = 2$, since this is the only even prime. But $2 = (1+i)(1-i)$, and $\sigma \mid 2$, so $\sigma \mid (1+i)$ or $\sigma \mid (1-i)$. Note that $N(1+i) = 2 = N(1-i)$, a rational prime. By property of the norm, $1+i$ and $1-i$ are prime. Thus, $\sigma \sim 1+i$ or $\sigma \sim 1-i$. Since $(1+i)/(1-i) = i$,

$(1+i) \sim (1-i)$, and hence the second part of the proposition is done.

*Case* 3. $r \equiv 1 \mod 4$. Since $r$ is the form $1+4m$, by Lemma 1.2.3, $r \mid n^2+1$ for some rational integer $n$. But $n^2+1 = (n+i)(n-i)$ and $\sigma \mid r$, so $\sigma \mid n+i$ or $\sigma \mid n-i$. But $r$ does not divide $n+i$ or $n-i$, for otherwise one of $(n \pm i)/r$ would be a Gaussian integer; this cannot be, for $1/p$ is not a rational integer. Hence $\sigma$ and $r$ are not associated. It follows that $N(\sigma) \neq N(r)$, so $x^2+y^2 \neq r^2$. This leaves only alternative $x^2+y^2 = r$.

Then $\sigma\bar{\sigma} = r$. Now $\sigma = x+yi$ is a prime by assumption; so is $\bar{\sigma} = x-yi$, since $N(\bar{\sigma}) = r$. They are not associated, for otherwise $x+yi = \epsilon(x-yi)$, where $\epsilon = 1, -1, i$ or $-i$. If $\epsilon = 1, x = 0, x^2 = r$, so $r$ is not a prime. If $\epsilon = -1, x = 0, y^2 = r$, and the same conclusion follows. If $\epsilon = \pm i, x = \pm y$ and $r$ is even. All of these eventualities are impossible, so $x+yi$ and $x-yi$ are not associated. □

Let $p_k$ and $q_l$ be positive primes in $\mathbb{Z}$ satisfying $p_k \equiv 3 \mod 4$, and $q_l \equiv 1 \mod 4$, $\pi_l$ denote a prime factor of $q_l$ in $\mathbb{Z}[i]$, and $\alpha = 1+i$. By the Chinese remainder theorem, if we factor $\gamma$ in $\mathbb{Z}[i]$ as

$$\gamma = i^d \alpha^a \prod_{k=1}^{n_1} p_k^{b_k} \prod_{l=1}^{n_2} \pi_l^{c_l}, \tag{1.1}$$

where each $\alpha$, $p_k$ and $\pi_l$ are distinct primes in $\mathbb{Z}[i]$, $a, d \geq 0$ and $b_k$,$c_l$ are positive integers, then we have

$$\mathbb{Z}[i]/(\gamma) \cong \mathbb{Z}[i]/(\alpha^a) \times \prod_{k=1}^{n_1} \mathbb{Z}[i]/(p_k^{b_k}) \times \prod_{l=1}^{n_2} \mathbb{Z}[i]/(\pi_l^{c_l}) \tag{1.2}$$

and

$$(\mathbb{Z}[i]/(\gamma))^* \cong (\mathbb{Z}[i]/(\alpha^a))^* \times \prod_{k=1}^{n_1} (\mathbb{Z}[i]/(p_k^{b_k}))^* \times \prod_{l=1}^{n_2} (\mathbb{Z}[i]/(\pi_l^{c_l}))^*. \tag{1.3}$$

Let $\omega(\gamma)$ denote the number of distinct primes in $\mathbb{Z}[i]$ dividing $\gamma$.

From Cross 's result [2], the structure for units group of $\mathbb{Z}[i]/(\sigma^n)$, where $\sigma$ is prime in $\mathbb{Z}[i]$, was completely solved for all $n \in \mathbb{N}$. We record his result in:

**Lemma 1.2.5.** *[2] Let $n$ be a positive integer and $\pi, p$ and $\alpha$ given in Proposition 1.2.4 Then:*

*(1)* $(\mathbb{Z}[i]/(p^n))^* \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}$.

*(2)* $(\mathbb{Z}[i]/(\pi^n))^* \cong \mathbb{Z}_{q^n-q^{n-1}}$.

*(3)* $(\mathbb{Z}[i]/(\alpha))^* \cong \{[1]\}$, $(\mathbb{Z}[i]/(\alpha^2))^* \cong \mathbb{Z}_2$, $(\mathbb{Z}[i]/(\alpha^3))^* \cong \mathbb{Z}_4$, $(\mathbb{Z}[i]/(\alpha^4))^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ *and*

$$(\mathbb{Z}[i]/(\alpha^n))^* \cong \begin{cases} \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_4, & \text{if } n = 2m; \\ \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_4, & \text{if } n = 2m+1, \end{cases}$$

*when* $n \geq 5$.

Following the work of Cross, we can explicitly describe the values of the Carmichael $\lambda$-function in the next proposition. Note that $\lambda(u\mu) = \lambda(\mu)$ for all units $u$. The following proposition is an immediate application of Theorem 1.1.1 and Lemma 1.2.5.

**Proposition 1.2.6.** *[2] Let $p$ and $q$ be positive primes in $\mathbb{Z}$ satisfying $p \equiv 3 \mod 4$, and $q \equiv 1 \mod 4$, $\pi$ denote a prime factor of $q$ in $\mathbb{Z}[i]$, and $\alpha = 1+i$. Then*

*(1)* $\lambda(\pi^n) = |(\mathbb{Z}[i]/(\pi^n))^*| = q^{n-1}(q-1)$ *for all positive integers $n$.*

*(2)* $\lambda(p^n) = \frac{1}{p^{n-1}}|(\mathbb{Z}[i]/(p^n))^*| = p^{n-1}(p^2-1)$ *for all positive integers $n$.*

*(3)* $\lambda(\alpha^j) = |(\mathbb{Z}[i]/(\alpha^j))^*| = 2^{j-1}$ *for* $j \in \{1,2,3\}$, $\lambda(\alpha^4) = \frac{1}{2}|(\mathbb{Z}[i]/(\alpha^4))^*| = 4$, $\lambda(\alpha^5) = \frac{1}{4}|(\mathbb{Z}[i]/(\alpha^5))^*| = 4$, *and for all* $n \geq 6$,

$$\lambda(\alpha^n) = \begin{cases} \frac{1}{2^m}|(\mathbb{Z}[i]/(\alpha^n))^*| = 2^{m-1}, & \text{if } n = 2m; \\ \frac{1}{2^{m+1}}|(\mathbb{Z}[i]/(\alpha^n))^*| = 2^{m-1}, & \text{if } n = 2m+1. \end{cases}$$

*(4)* $\lambda(\sigma_1^{j_1}\sigma_2^{j_2}\ldots\sigma_s^{j_s}) = \operatorname{lcm}\{\lambda(\sigma_1^{j_1}), \lambda(\sigma_2^{j_2}), \ldots, \lambda(\sigma_s^{j_s})\}$, *where $\sigma_1, \sigma_2, \ldots, \sigma_s$ are distinct primes in $\mathbb{Z}[i]$ for $j_l \geq 1$ and $l \in \{1,2,\ldots,s\}$.*

In the remainder of the thesis, we shall continue with the following notation: $p$ and $q$ denote positive primes in $\mathbb{Z}$ satisfying $p \equiv 3 \mod 4$ and $q \equiv 1 \mod 4$, $\pi$ stands for a prime factor of $q$ in $\mathbb{Z}[i]$, and $\alpha = 1+i$.

# CHAPTER II

# STRUCTURES OF THE DIGRAPH $G_\gamma^{(2)}$

## 2.1 Preliminary Structures

In this section, we present elementary results on our digraph.

**Proposition 2.1.1.** *Each component of the digraph $G_\gamma^{(2)}$ has exactly one cycle. Therefore, the number of components of this digraph is equal to the number of its cycles.*

*Proof.* Let $\mu$ be a vertex in a component $C$ of $G_\gamma^{(2)}$. Consider the path

$$\mu \to \mu^2 \to \mu^4 \to \cdots \to \mu^{2^j} \to \cdots.$$

If there is no cycle, then the above path is infinite and so is the order of $\mu$, which is impossible. Thus, $C$ contains a cycle. Moreover, if $C$ possesses more than one cycle, then there is a vertex with outdegree greater than one, which is a contradiction. □

The following two propositions tell us about isolated fixed points and isolated cycles.

**Proposition 2.1.2.** *The zero 0 is an isolated fixed point of $G_\gamma^{(2)}$ if and only if $\gamma$ is square-free.*

*Proof.* If $\eta^2 \mid \gamma$ for some prime $\eta$, then $\gamma/\eta \in \mathbb{Z}[i]$ and

$$\left(\frac{\gamma}{\eta}\right)^2 = \gamma \cdot \frac{\gamma}{\eta^2} \equiv 0 \mod \gamma.$$

Thus, 0 is not an isolated fixed point. Conversely, assume that $\gamma$ is square-free. If $x^2 \equiv 0 \mod \gamma$, then $x \equiv 0 \mod \gamma$. Hence, 0 is an isolated fixed point of $G_\gamma^{(2)}$. □

**Proposition 2.1.3.** *If* $\gcd(2,\gamma) = 1$, *then there are no isolated cycles in* $G_\gamma^{(2)}$ *except the isolated fixed point* 0.

*Proof.* Assume that $\alpha^2 \nmid \gamma$ and $\mu$ is a vertex in an isolated cycle of $G_\gamma^{(2)}$. Let $\nu \in \mathbb{Z}[i]$ such that $\nu^2 \equiv \mu \mod \gamma$. Then $(-\nu)^2 \equiv \mu \mod \gamma$. Since $\mu$ is in an isolated cycle, $\nu \equiv -\nu \mod \gamma$, so $2\nu \equiv 0 \mod \gamma$. Since $\gcd(\alpha^2, \gamma) = 1$, $\nu \equiv 0 \mod \gamma$ which implies that $\nu \equiv 0 \mod \gamma$. □

A graph is *regular* if all its vertices have the same degree. The digraph $G_\gamma^{(2)}$ is said to be *semiregular* if there exists a positive integer $d$ such that each vertex of $G_\gamma^{(2)}$ either has indegree 0 or $d$.

If $\gamma = i^d \alpha^a \prod_{k=1}^{n_1} p_k^{b_k} \prod_{l=1}^{n_2} \pi_l^{c_l}$ with $a, d \geq 0$ and $b_k$,$c_l$ are positive integers, define

$$\rho_1 = \begin{cases} 0, & \text{if} \quad a \neq 2; \\ 1, & \text{if} \quad a = 2, \end{cases} \qquad \rho_2 = \begin{cases} 0, & \text{if} \quad a \neq 3; \\ 1, & \text{if} \quad a = 3, \end{cases}$$

$$\rho_3 = \begin{cases} 0, & \text{if} \quad a \text{ is even}; \\ 1, & \text{if} \quad a \text{ is odd}, \end{cases} \quad \text{and} \quad \rho_4 = \begin{cases} 0, & \text{if} \quad a \text{ is odd}; \\ 1, & \text{if} \quad a \text{ is even}. \end{cases}$$

Next, we consider two disjoint subdigraphs $G_{\gamma,1}^{(2)}$ and $G_{\gamma,2}^{(2)}$ of $G_\gamma^{(2)}$ induced on the set of vertices which are in the unit group $(\mathbb{Z}[i]/(\gamma))^*$ and induced on the remaining vertices which are not invertible modulo $\gamma$, respectively. They are called the *unit subdigraph* and the *zero divisor subdigraph*, respectively. Observe that there are no edges between $G_{\gamma,1}^{(2)}$ and $G_{\gamma,2}^{(2)}$, that is, $G_\gamma^{(2)} = G_{\gamma,1}^{(2)} \cup G_{\gamma,2}^{(2)}$.

**Lemma 2.1.4.** *Let* $a, b$ *and* $c$ *denote positive integers. Then we have the following statements.*

*(1) The number of solutions of* $x^2 \equiv \mu \mod p^b$ *is* 0 *or* 2.

*(2) The number of solutions of* $x^2 \equiv \mu \mod \pi^c$ *is* 0 *or* 2.

*(3) The number of solutions of* $x^2 \equiv \mu \mod \alpha^a$ *is*

*(i)* $0$ *or* $2^{\rho_1+\rho_2}$ *if* $0 \le a \le 3$,

*(ii)* $0$ *or* $4$ *if* $a = 4$, *and*

*(iii)* $0$ *or* $2^{2\rho_3+2\rho_4+1}$ *if* $a > 4$.

*Proof.* By Lemma 1.2.5 (2), $(\mathbb{Z}[i]/(\pi^c))^* \cong \mathbb{Z}_{q^c-q^{c-1}}$. Multiplication in $(\mathbb{Z}[i]/(\pi^c))^*$ corresponds to addition in $\mathbb{Z}_{q^c-q^{c-1}}$, so $x^2$ corresponds to $2x$. The map

$$\varphi : \mathbb{Z}_{q^c-q^{c-1}} \to \mathbb{Z}_{q^c-q^{c-1}} \quad \text{defined by} \quad \varphi(x) = 2x$$

is a $\gcd(2, q^c - q^{c-1})$-to-one map, so an element in $\mathbb{Z}_{q^c-q^{c-1}}$ is either the image of $\gcd(2, q^c - q^{c-1}) = 2$ elements or none.

For modulus $p^b$, Lemma 1.2.5 (1) says $(\mathbb{Z}[i]/(p^b))^* \cong \mathbb{Z}_{p^{b-1}} \times \mathbb{Z}_{p^{b-1}} \times \mathbb{Z}_{p^2-1}$. In $\mathbb{Z}_{p^{b-1}} \times \mathbb{Z}_{p^{b-1}} \times \mathbb{Z}_{p^2-1}$, the multiplication by 2 map is $\left(\gcd(2, p^{b-1})\right)^2 \gcd(2, p^2-1)$-to-one, so an element in $\mathbb{Z}_{p^{b-1}} \times \mathbb{Z}_{p^{b-1}} \times \mathbb{Z}_{p^2-1}$ is either the image of $\left(\gcd(2, p^{b-1})\right)^2 \gcd(2, p^2 - 1) = 2$ elements or none.

Finally, for modulus $\alpha^a$, Lemma 1.2.5 (1) gives

$$(\mathbb{Z}[i]/(\alpha^a))^* \cong \begin{cases} \mathbb{Z}_2^{\rho_1} \times \mathbb{Z}_4^{\rho_2}, & \text{if } 0 \le a \le 3; \\ \mathbb{Z}^{\rho_3}_{2^{\frac{a-1}{2}-1}} \times \mathbb{Z}^{\rho_3}_{2^{\frac{a-1}{2}-1}} \times \mathbb{Z}^{\rho_4}_{2^{\frac{a}{2}-1}} \times \mathbb{Z}^{\rho_4}_{2^{\frac{a}{2}-2}} \times \mathbb{Z}_4, & \text{if } a > 3. \end{cases}$$

If $0 \le a \le 3$, then the multiplication by 2 map is $(\gcd(2,2))^{\rho_1} (\gcd(2,4))^{\rho_2}$-to-one, so an element in $\mathbb{Z}_2^{\rho_1} \times \mathbb{Z}_4^{\rho_2}$ is either the image of $(\gcd(2,2))^{\rho_1} (\gcd(2,4))^{\rho_2} = 2^{\rho_1+\rho_2}$ elements or none. If $a > 3$, then the multiplication by 2 map is $2\left(\gcd(2^{\frac{a-1}{2}-1}, 2)\right)^{2\rho_3}$ $\left(\gcd(2^{\frac{a}{2}-1}, 2)\right)^{\rho_4} \left(\gcd(2^{\frac{a}{2}-2}, 2)\right)^{\rho_4}$-to-one, establishing our result. □

**Proposition 2.1.5.** *For every nonzero element* $\gamma \in \mathbb{Z}[i]$, *we have the digraph* $G^{(2)}_{\gamma,1}$ *is semiregular. More precisely,*

*(1) if* $0 \le a \le 3$ *and* $\mu$ *is a vertex of* $G^{(2)}_{\gamma,1}$, *then* $\operatorname{indeg}_\gamma \mu = 0$ *or* $\operatorname{indeg}_\gamma \mu = 2^{\rho_1+\rho_2+n_1+n_2}$,

*(2) If* $a = 4$ *and* $\mu$ *is a vertex of* $G^{(2)}_{\gamma,1}$, *then* $\operatorname{indeg}_\gamma \mu = 0$ *or* $\operatorname{indeg}_\gamma \mu = 2^{\omega(\gamma)+1}$, *and*

*(3) If $a > 4$ and $\mu$ is a vertex of $G^{(2)}_{\gamma,1}$, then* $\mathrm{indeg}_\gamma \mu = 0$ *or* $\mathrm{indeg}_\gamma \mu = 2^{2\rho_3+2\rho_4+\omega(\gamma)}$.

*Proof.* Let $E := \prod_{k=1}^{n_1}(\mathbb{Z}[i]/(p_k^{b_k}))^* \times \prod_{l=1}^{n_2}(\mathbb{Z}[i]/(\pi_l^{c_l}))^*$.
From (1.3) and Lemma 1.2.5 (3),

$$(\mathbb{Z}[i]/(\gamma))^* \cong \begin{cases} \mathbb{Z}_2^{\rho_1} \times \mathbb{Z}_4^{\rho_2} \times E, & \text{if } 0 \le a \le 3; \\ \mathbb{Z}^{\rho_3}_{2^{\frac{a-1}{2}}-1} \times \mathbb{Z}^{\rho_3}_{2^{\frac{a-1}{2}}-1} \times \mathbb{Z}^{\rho_4}_{2^{\frac{a}{2}}-1} \times \mathbb{Z}^{\rho_4}_{2^{\frac{a}{2}}-2} \times \mathbb{Z}_4 \times E, & \text{if } a > 3. \end{cases}$$

For $\mu \in (\mathbb{Z}[i]/(\gamma))^*$, $x^2 \equiv \mu \mod \gamma$ is equivalent to

$$\begin{aligned} x^2 &\equiv \mu \mod \alpha^a, \\ x^2 &\equiv \mu \mod p_k^{b_k}, \\ x^2 &\equiv \mu \mod \pi_l^{c_l}. \end{aligned} \qquad (*)$$

By Lemma 2.1.4, we know that for $k \in \{1, 2, \ldots, n_1\}, l \in \{1, 2, \ldots, n_2\}, x^2 \equiv \mu \mod p_k^{b_k}$ and $x^2 \equiv \mu \mod \pi_l^{c_l}$ have 0 or 2 solutions. For $0 \le a \le 3$, $x^2 \equiv \mu \mod \alpha^a$ has 0 or $2^{\rho_1+\rho_2}$ solutions. The system (*) thus has 0 or $2^{\rho_1+\rho_2+n_1+n_2}$. When $a = 4$, $x^2 \equiv \mu \mod \alpha^4$ has 0 or 4 solutions which implies that the system (*) has 0 or $2^{n_1+n_2+2} = 2^{\omega(\gamma)+1}$. For $a > 4$, $x^2 \equiv \mu \mod \alpha^a$ has 0 or $2^{2\rho_3+2\rho_4+1}$ solutions. This again gives 0 or $2^{2\rho_3+2\rho_4+n_1+n_2+1} = 2^{2\rho_3+2\rho_4+\omega(\gamma)}$ solutions for the system (*). □

## 2.2 Cycles, Components and Distances

We prove the main theorem about the $t$-cycles for the digraph $G^{(2)}_\gamma$ (Theorem 2.2.1) and derive its consequences in this section. Our main tool is the $\lambda$-function given by $\lambda(\gamma) = \exp(\mathbb{Z}[i]/(\gamma))^*$ and their values given in Proposition 1.2.6. Furthermore, we work on the number of components and study the maximum distance from the cycle on each component.

**Notation.** If $R$ is the ring of integers $\mathbb{Z}$ or the ring of Gaussian integers $\mathbb{Z}[i]$, for

each $\mu, \gamma \in R$ with $\gcd(\mu, \gamma) = 1$, we write $\operatorname{ord}_\gamma \mu = t$ if $t$ is the least positive integer such that $\mu^t \equiv 1 \mod \gamma$.

We also repeatedly use the following two facts.

(i) $\operatorname{ord}_d(ab) = \operatorname{lcm}(\operatorname{ord}_d a, \operatorname{ord}_d b)$, and

(ii) $\operatorname{ord}_d a^n = \dfrac{\operatorname{ord} a}{\gcd(n, \operatorname{ord}_d a)}$ for all $n \in \mathbb{N}$.

**Theorem 2.2.1.** *Let $\gamma$ be a nonzero element in $\mathbb{Z}[i]$ and have the factorization given in* (1.1)*. Then we have the following statements.*

*(1) There exists a $t$-cycle in the digraph $G_\gamma^{(2)}$ if and only if $t = \operatorname{ord}_d 2$ for some odd positive divisor $d$ of $\lambda(\gamma)$.*

*(2) Let $\eta$ be a prime factor of $\gamma$ and $h$ be the highest power of $\eta$ in $\gamma$. If $\mu$ is an element of a cycle, then $\eta^h \mid \mu$ whenever $\eta \mid \mu$. Furthermore, if $\mu$ and $\nu$ lie on the same cycle, then $\eta \mid \mu$ if and only if $\eta \mid \nu$.*

*(3) If $\mu$ is a vertex of a $t$-cycle, then $\operatorname{ord}_{\gamma'} \mu = d$ where $\gamma' = \gamma/\gcd(\mu, \gamma)$, $d$ is odd, and $\operatorname{ord}_d 2 = t$. In addition, if $\nu$ is on the same $t$-cycle as $\mu$, then $\operatorname{ord}_{\gamma'} \mu = \operatorname{ord}_{\gamma'} \nu$.*

*Proof.* Clearly, $G_\gamma^{(2)}$ contains the fixed point 0 and $\operatorname{ord}_d 2 = 1$ when $d = 1$. Next assume that $\mu$ is a fixed point of $G_\gamma^{(2)}$. Then

$$\mu(\mu - 1) \equiv \mu^2 - \mu \equiv 0 \mod \gamma.$$

Since $\gcd(\mu, \mu - 1) = 1$, $\eta \mid \gamma$ implies $\eta^h \mid \gamma$. Since $\gcd(\mu, \gamma) \mid \mu$, $\mu \equiv 1 \mod \gamma'$ where $\gamma' = \mu/\gcd(\mu, \gamma)$. Hence, $\operatorname{ord}_{\gamma'} \mu = d = 1$ and so $\operatorname{ord}_d 2 = t = 1$.

Assume that $t > 1$ and $G_\gamma^{(2)}$ has a $t$-cycle containing a vertex $\mu$. Then $t$ is the least positive integer such that

$$\mu^{2^t} \equiv \mu \mod \gamma.$$

Thus, we have

$$\mu(\mu^{2^t - 1} - 1) \equiv \mu^{2^t} - \mu \equiv 0 \mod \gamma.$$

Since $\gcd(\mu, \mu^{2^t-1} - 1) = 1$ and $\gcd(\mu, \gamma) \mid \mu$, $t$ is the least positive integer such that $\mu^{2^t-1} \equiv 1 \mod \gamma'$ and therefore $\gcd(\gcd(\mu, \gamma), \gamma') = 1$. Hence, we get $\eta^h \mid \gamma$ whenever $\eta \mid \gamma$.

Now, assume that $\mu$ and $\nu$ are in the same $t$-cycle of $G_\gamma^{(2)}$. Then there exists a $j \in \{1, 2, \ldots, t\}$ such that

$$\nu \equiv \mu^{2^j} \mod \gamma \quad \text{and} \quad \mu \equiv \nu^{2^{t-j}} \mod \gamma. \tag{2.1}$$

It follows that $\eta \mid \mu$ if and only if $\eta \mid \nu$.

Let $\mu$ be an element of a $t$-cycle in $G_\gamma^{(2)}$. Since $\mu^{2^t-1} \equiv 1 \mod \gamma'$, we have $\gcd(\mu, \gamma') = 1$. Let $d = \operatorname{ord}_{\gamma'} \mu$. Then $t$ is the least positive integer such that $d \mid (2^t - 1)$. Thus, $t = \operatorname{ord}_d 2$ and $d$ is odd. Moreover, $d \mid \lambda(\gamma')$ by the definition of $\lambda$. Since $\gamma' \mid \gamma$, $\lambda(\gamma') \mid \lambda(\gamma)$ and so $d \mid \lambda(\gamma)$. Noting that $\gcd(2^j, d) = 1$ for all $j \geq 0$, we derive from (2.1) that $\operatorname{ord}_{\gamma'} \mu = \operatorname{ord}_{\gamma'} \nu$ if $\mu$ and $\nu$ lie on the same cycle in $G_\gamma^{(2)}$.

It remains to show the necessity part of (1). Let $t = \operatorname{ord}_d 2$ for some odd positive divisor $d$ of $\lambda(\gamma)$. By Theorem 1.1.1 (4), there exists a vertex $\mu \in \mathbb{Z}[i]/(\gamma)$ such that $\operatorname{ord}_\gamma \mu = \lambda(\gamma)$. Let $\nu = \mu^{\lambda(\gamma)/d}$. Then $\operatorname{ord}_\gamma \nu = d$. Since $d \mid 2^t - 1$ but $d \nmid 2^j - 1$ if $1 \leq j < t$ , we see that $t$ is the least positive integer for which

$$\nu^{2^t-1} \equiv 1 \mod \gamma,$$

so we finally reach

$$\nu^{2^t} = \nu\nu^{2^t-1} \equiv \nu \mod \gamma.$$

Therefore, $\nu$ is a vertex of a $t$-cycle in $G_\gamma^{(2)}$. □

**Corollary 2.2.2.** *(1) If there exists a $t$-cycle in $G_\gamma^{(2)}$, then there exists a $t$-cycle in $G_{\gamma,1}^{(2)}$.*

*(2) The unit subdigraph $G_{\gamma,1}^{(2)}$ contains a $t$-cycle if and only if there exists a positive odd integer $d$ such that $t = \operatorname{ord}_d 2$ and $d \mid \lambda(\gamma)$.*

*Proof.* (1) It suffices to assume that there exists a $t$-cycle in $G^{(2)}_{\gamma,2}$ and $t > 1$. Let $\mu$ be a vertex of this $t$-cycle. As in the proof of Theorem 2.2.1, we obtain

$$\mu \equiv 0 \mod \gcd(\mu, \gamma) \quad \text{and} \quad \mu^{2^t-1} \equiv 1 \mod \gamma'. \tag{2.2}$$

Since $\gcd(\gcd(\mu, \gamma), \gamma') = 1$, by the Chinese remainder theorem, there exists a $\nu \in (\mathbb{Z}[i]/(\gamma))^*$ such that

$$\nu \equiv 1 \mod \gcd(\mu, \gamma) \quad \text{and} \quad \nu \equiv \mu \mod \gamma'. \tag{2.3}$$

It follows from (2.2) and (2.3) that $t$ is the least positive integer such that

$$\nu^{2^t-1} \equiv 1 \mod \gamma.$$

That is, $\nu$ is an element of the $t$-cycle. This proves (1).

(2) follows from (1) and Theorem 2.2.1 (1). □

The numbers of fixed points in $G^{(2)}_{\gamma,1}$ and $G^{(2)}_{\gamma,2}$ are studied in:

**Corollary 2.2.3.** *Let $C^t_{\gamma,1}$ and $C^t_{\gamma,2}$ denote the number of $t$-cycles in $G^{(2)}_{\gamma,1}$ and $G^{(2)}_{\gamma,2}$, respectively. Then*

$$C^1_{\gamma,1} = 1 \quad \textit{and} \quad C^1_{\gamma,2} = 2^{\omega(\gamma)} - 1.$$

*Proof.* Let $\gamma$ be a nonzero element in $\mathbb{Z}[i]$ and have the factorization given in (1.1). We shall first show that $C^1_\gamma = 2^{n_1+n_2+1} = 2^{\omega(\gamma)}$. It is easy to see that 0 and 1 are the only fixed points modulo $\eta^h$ for any prime factor $\eta$ of $\gamma$, where $h$ is the highest power of $\eta$ in $\gamma$. If $\mu$ is a fixed point modulo $\gamma$, then certainly $\mu$ is a fixed point modulo $\eta^h$ for any prime factor $\eta$ of $\gamma$, so for each $\eta$ we know that $\mu \equiv 0 \mod \eta^h$ or $\mu \equiv 1 \mod \eta^h$. Conversely, by the Chinese remainder theorem, for each $\varepsilon, \varepsilon_k, \varepsilon_l \in \{0, 1\}$ there is a unique $\mu \in \mathbb{Z}[i]$ such that

$$\mu \equiv \varepsilon \mod \alpha^a,$$

for $k \in \{1, \ldots, n_1\}$,

$$\mu \equiv \varepsilon_k \mod p_k^{b_k},$$

and for $l \in \{1, \ldots, n_2\}$,

$$\mu \equiv \varepsilon_l \mod \pi_l^{c_l}.$$

Thus, $\mu$ is a fixed point modulo $\gamma$. Since there are $2^{n_1+n_2+1}$ distinct ways to choose the $\varepsilon, \varepsilon_k$ and $\varepsilon_l$, $G_\gamma^{(2)}$ has exactly $2^{n_1+n_2+1}$ fixed points.

Next, we shall prove that $C_{\gamma,1}^1 = 1$. Let $\mu$ be a fixed point in $G_{\gamma,1}^{(2)}$. Then we have

$$0 \equiv \mu^2 - \mu \equiv \mu(\mu - 1) \mod \gamma.$$

Since $\gcd(\mu, \gamma) = 1$, $\mu \equiv 1 \mod \gamma$, so $C_{\gamma,1}^1 = 1$. Finally, $C_{\gamma,2}^1 = C_\gamma^1 - C_{\gamma,1}^1 = 2^{\omega(\gamma)} - 1$. □

**Corollary 2.2.4.** *Let $\gamma$ be a nonzero element in $\mathbb{Z}[i]$ and have the factorization given in* (1.1)*. The zero divisor subdigraph $G_{\gamma,2}^{(2)}$ contains a $t$-cycle if and only if there exist a positive odd integer $d$ and a prime factor $\eta$ of $\gamma$ such that $t = \operatorname{ord}_d 2$ and $d \mid \lambda(\gamma/\eta^h)$, where $h$ is the highest power of $\eta$ in $\gamma$.*

*Proof.* It is clear for $t = 1$. Assume that $t > 1$ and let $\mu$ be a vertex of a $t$-cycle in $G_{\gamma,2}^{(2)}$. Then $\gcd(\mu, \gamma) > 1$. Since $\gcd(\gcd(\mu, \gamma), \gamma') = 1$, there exists a prime factor $\eta$ of $\gamma$ such that $\gamma' \mid (\gamma/\eta^h)$, where $h$ is the highest power of $\eta$ in $\gamma$. By Theorem 1.1.1 (2), $\lambda(\gamma') \mid \lambda(\gamma/\eta^h)$. Let $d = \operatorname{ord}_{\gamma'} \mu$. It directly follows from Theorem 2.2.1 (3) that $d$ is odd, $t = \operatorname{ord}_d 2$ and $d \mid \lambda(\gamma')$ which implies that $d \mid \lambda(\gamma/\eta^h)$.

Conversely, suppose that there exist a positive odd integer $d$ and a prime factor $\eta$ of $\gamma$ such that $t = \operatorname{ord}_d 2$ and $d \mid \lambda(\gamma/\eta^h)$, where $h$ is the highest power of $\eta$ in $\gamma$. Let $\gamma'' = \gamma/\eta^h$. By Theorem 1.1.1 (4), there exists a $\nu \in (\mathbb{Z}[i]/(\gamma''))^*$ such that $\operatorname{ord}_{\gamma''} \nu = \lambda(\gamma'')$. Then $\operatorname{ord}_{\gamma''} \nu^{\lambda(\gamma'')/d} = d$. Since $d \mid 2^t - 1$ but $d \nmid 2^j - 1$ whenever $1 \le j < t$, $t$ is the least positive integer for which

$$\nu^{(\lambda(\gamma'')/d)^{2^t-1}} \equiv 1 \mod \gamma''.$$

By the Chinese remainder theorem, we have $\mu \in \mathbb{Z}[i]$ such that

$$\mu \equiv 0 \mod \eta^h \quad \text{and} \quad \mu \equiv \nu^{\lambda(\gamma'')/d} \mod \gamma''$$

since $\gcd(\eta^h, \gamma'') = 1$. Thus,

$$\mu^{2^t} - \mu \equiv \mu(\mu^{2^t-1} - 1) \equiv 0 \mod \gamma.$$

Since $t$ is the least positive integer for which $\mu^{2^t-1} \equiv 1 \mod \gamma''$ and $\eta^h \mid \mu$, $\mu$ is a vertex of a $t$-cycle in $G^{(2)}_{\gamma,2}$. □

Recall that a *Fermat prime* is a prime number of the form $2^{2^m} + 1$ for some nonnegative integer $m$.

**Corollary 2.2.5.** *Suppose that $\gamma$ is a prime power. Suppose further that for each positive integer $t$, $G^{(2)}_{\gamma,1}$ has a $t$-cycle if and only if $G^{(2)}_{\gamma,2}$ has a $t$-cycle. Then $\gamma = \alpha^a$ for $a \geq 1$ or $\gamma = \pi$, where $\pi$ is a prime factor of a Fermat prime $q$.*

*Proof.* Since 0 and 1 are fixed points of $G^{(2)}_{\gamma}$, both $G^{(2)}_{\gamma,1}$ and $G^{(2)}_{\gamma,2}$ have a cycle of length 1. By Corollary 2.2.4 and the fact that $\gamma$ is a prime power, the only cycle in $G^{(2)}_{\gamma,2}$ is the fixed point 0.

Now suppose that $\gamma$ is not a number of the form $\alpha^a$ for $a \geq 1$ or $q$ a Fermat prime. If $\gamma = \pi^j$ and $j \geq 2$, then by Proposition 1.2.6 (1), $\lambda(\gamma) = q^{j-1}(q-1)$ and so $q \mid \lambda(\gamma)$. Let $t = \operatorname{ord}_q 2$. Thus, $t > 1$ and $G^{(2)}_{\gamma,1}$ has a $t$-cycle by Corollary 2.2.2 (2). If $\gamma = p^j$ and $j \geq 1$, then by Proposition 1.2.6 (2), $\lambda(\gamma) = p^{j-1}(p^2 - 1)$ and so $(p-1) \mid \lambda(\gamma)$. Since $p \equiv 3 \mod 4$, $p$ is not a Fermat prime. Thus, $p - 1$ has an odd prime divisor $r$. Let $t = \operatorname{ord}_r 2$. Hence, $t > 1$ and $G^{(2)}_{\gamma,1}$ again has a $t$-cycle which is not in $G^{(2)}_{\gamma,2}$.

We finally suppose that $\gamma = \alpha^a$ for $a \geq 1$ or $\gamma = \pi$, where $\pi$ is a prime factor of a Fermat prime $q$. Then $\lambda(\gamma) = 2^j$, where $j \geq 0$. By Corollary 2.2.2, the only cycles in $G^{(2)}_{\gamma,1}$ are of length 1. The result now follows. □

**Remark.** For $\gamma = 3 + 4i = (2+i)^2$, the digraph $G^{(2)}_{\gamma,1}$ has a 4-cycle but $G^{(2)}_{\gamma,2}$ does not have a 4-cycle. Since $1 + 2i$ is a prime, $G^{(2)}_{1+2i}$ provides an example in which both $G^{(2)}_{\gamma,1}$ and $G^{(2)}_{\gamma,2}$ only have one fixed point.

The following example gives an instance in which $G^{(2)}_{\gamma,1}$ has a $t$-cycle but $G^{(2)}_{\gamma,2}$ does not have a $t$-cycle when $\omega(\gamma) = 2$.

**Example 2.2.6.** By inspection, we find that a nonzero Gaussian integer $\gamma$ for which $\omega(\gamma) \geq 2$ and there exists a positive $t$ for which $G^{(2)}_{\gamma,1}$ has a $t$-cycle but $G^{(2)}_{\gamma,2}$ does not have a $t$-cycle, is $\gamma = 147 + 196i = 7^2(2+i)^2$. In this case $G^{(2)}_{147+196i,1}$ has a 12-cycle, whereas $G^{(2)}_{147+196i,2}$ does not have a 12-cycle. Note that $\lambda(147 + 196i) = 2^4 \cdot 3 \cdot 5 \cdot 7$ and $35 \mid \lambda(147 + 196i)$. However, $35 \nmid \lambda(7^2) = 2^4 \cdot 3 \cdot 7$ and $35 \nmid \lambda((2+i)^2) = 2^2 \cdot 5$. Moreover, $\operatorname{ord}_{35} 2 = 12$, whereas $\operatorname{ord}_3 2 = 2$, $\operatorname{ord}_5 2 = 4$ and $\operatorname{ord}_7 2 = 3$.

We know from Proposition 2.1.1 that the number of components is the same as the number of cycles. Theorem 2.2.7 given below counts the number of $t$-cycles in $G^{(2)}_{\gamma,1}$ and $G^{(2)}_{\gamma,2}$ and yields hence the number of components.

**Theorem 2.2.7.** *Let $S$ be the complete system of residues of $\mathbb{Z}[i]/(\gamma)$ given as in Proposition 1.2.1. Let $N^d_\gamma$ be the number of Gaussian integers $\mu$ in $S$ such that $d = \operatorname{ord}_\gamma \mu$. Then*

$$C^t_{\gamma,1} = \frac{1}{t} \sum_d N^d_\gamma, \tag{2.4}$$

*where $d$ runs over all positive odd integers such that $d \mid \lambda(\gamma)$ and $t = \operatorname{ord}_d 2$, and*

$$C^t_{\gamma,2} = \frac{1}{t} \sum N^{d'}_{\gamma'}, \tag{2.5}$$

*where the summation is taken over all nonzero Gaussian integers $\gamma'$ such that $\gamma' \in S, \gamma' \mid \gamma$ and $\gcd(\gamma/\gamma', \gamma') = 1$, and for a given $\gamma'$ the number $d'$ varies over all positive odd integers for which $d' \mid \lambda(\gamma')$ and $t = \operatorname{ord}_{d'} 2$.*

*Proof.* (2.4): Observe that it suffices to show that

$$\bigcup_d \{\mu \in (\mathbb{Z}[i]/(\gamma))^* : \operatorname{ord}_\gamma \mu = d\}$$
$$= \{\mu \in \mathbb{Z}[i]/(\gamma) : \ \mu \text{ is a vertex in a } t\text{-cycle of } G^{(2)}_{\gamma,1}\},$$

where $d$ runs over all positive odd integers such that $d \mid \lambda(\gamma)$ and $t = \operatorname{ord}_d 2$. Assume that there exists an odd integer $d$ with $d \mid \lambda(\gamma)$ and $t = \operatorname{ord}_d 2$. By Corollary 2.2.2 (2), $G^{(2)}_{\gamma,1}$ contains a $t$-cycle. Let $\mu \in (\mathbb{Z}[i]/(\gamma))^*$ be such that

$\operatorname{ord}_\gamma \mu = d$. Then $\mu^d \equiv 1 \mod \gamma$. Since $t = \operatorname{ord}_d 2$, $t$ is the least positive integer such that $\mu^{2^t-1} \equiv 1 \mod \gamma$, and hence $\mu^{2^t} \equiv \mu \mod \gamma$ which implies that $\mu$ is a vertex of a $t$-cycle. Theorem 2.2.1 (3) gives the converse.

(2.5): Similar to (2.4), it suffices to prove that

$$\bigcup \{\mu \in \mathbb{Z}[i]/(\gamma) : \operatorname{ord}_{\gamma'} \mu = d'\}$$
$$= \{\mu \in \mathbb{Z}[i]/(\gamma) : \ \mu \text{ is a vertex in a } t\text{-cycle of } G^{(2)}_{\gamma,2}\},$$

where the union is taken over all nonzero Gaussian integers $\gamma'$ such that $\gamma' \in S, \gamma' \mid \gamma$ and $\gcd(\gamma/\gamma', \gamma') = 1$, and for a given $\gamma'$ the number $d'$ varies over all positive odd integers for which $d' \mid \lambda(\gamma')$ and $t = \operatorname{ord}_{d'} 2$. Assume that there exists a nonzero Gaussian integer $\gamma' \in S, \gamma' \mid \gamma$ and $\gcd(\gamma/\gamma', \gamma') = 1$, and let $d'$ be a positive odd integer for which $d' \mid \lambda(\gamma')$, $t = \operatorname{ord}_{d'} 2$ and $\operatorname{ord}_{\gamma'} \mu = d'$. Then $\mu^{d'} \equiv 1 \mod \gamma'$. Thus, $t$ is the least positive integer such that $\mu^{2^t-1} - 1 \equiv 0 \mod \gamma'$. Since $\gcd(\gamma', \gamma/\gamma') = 1$, by the Chinese remainder theorem, we have $\nu \in \mathbb{Z}[i]$ which satisfies

$$\nu \equiv 0 \mod \gamma' \quad \text{and} \quad \nu \equiv \mu \mod \gamma/\gamma',$$

and hence

$$\nu^{2^t} - \nu \equiv \nu(\nu^{2^t-1} - 1) \equiv 0 \mod \gamma.$$

Since $t$ is the least positive integer for which $\nu^{2^t-1} \equiv 1 \mod \gamma/\gamma'$ and $\gamma' \mid \mu$, $\mu$ is a vertex of a $t$-cycle in $G^{(2)}_{\gamma,2}$. Again, Theorem 2.2.1 (3) yields the converse. Therefore, we have the theorem. □

Theorem 2.2.8 determines the distance from any vertex in $G^{(2)}_\gamma$ to the unique cycle in its component.

**Theorem 2.2.8.** *Let $S$ be the complete system of residues of $\mathbb{Z}[i]/(\gamma)$ given as in Proposition 1.2.1. Let $\mu \in S$ be such that*

$$\mu = \beta\alpha^{a_1} \prod_{k=1}^{n_1} p_k^{f_k} \prod_{l=1}^{n_2} \pi_l^{g_l},$$

*where the primes* $\alpha$, $p_k$ *and* $\pi_l$ *are given in* (1.1), $\gcd(\beta,\gamma)=1$ *and* $a_1$, $f_k$, $g_l$ *are nonnegative integers. For* $a_1$, *we define the nonnegative integer* $A_{a_1}$ *by*

$$A_{a_1}=\begin{cases}0, & \text{if} \quad a_1=0;\\ a, & \text{if} \quad 1\le a_1\le a;\\ a_1, & \text{if} \quad a_1>a,\end{cases}$$

*for* $k=1,\dots,n_1$, *the nonnegative integer* $B_k$ *by*

$$B_k=\begin{cases}0, & \text{if} \quad f_k=0;\\ b_k, & \text{if} \quad 1\le f_k\le b_k;\\ f_k, & \text{if} \quad f_k>b_k,\end{cases}$$

*and for* $l=1,\dots,n_2$, *the nonnegative integer* $C_l$ *by*

$$C_l=\begin{cases}0, & \text{if} \quad g_l=0;\\ c_l, & \text{if} \quad 1\le g_l\le c_l;\\ g_l, & \text{if} \quad g_l>c_l.\end{cases}$$

*Let*

$$\gamma' = \alpha^{a-\min(A_{a_1},a)}\prod_{k=1}^{n_1}p_k^{b_k-\min(B_k,b_k)}\prod_{l=1}^{n_2}\pi_l^{c_l-\min(C_l,c_l)}.$$

*Suppose that* $\operatorname{ord}_{\gamma'}\mu=2^e d$, *where* $d$ *is odd. Let* $t=\operatorname{ord}_d 2$. *Then the component of* $G_\gamma^{(2)}$ *containing the vertex* $\mu$ *has a unique* $t$*-cycle. Moreover, the distance from the vertex* $\mu$ *to this* $t$*-cycle is equal to*

$$\max\left(\max_{1\le k\le n_1}\left\lceil\log_2\frac{B_k}{f_k}\right\rceil,\max_{1\le l\le n_2}\left\lceil\log_2\frac{C_l}{g_l}\right\rceil,\left\lceil\log_2\frac{A_{a_1}}{a_1}\right\rceil,e\right),$$

*where* $A_{a_1}/a_1=B_k/f_k=C_l/g_l=1$ *if* $A_{a_1}=a_1=B_k=f_k=C_l=g_l=0$.

*Proof.* Let $C$ be the component of $G_\gamma^{(2)}$ containing the vertex $\mu$. Let $\nu$ be the vertex in the unique cycle of $C$ which is of least distance $s\ge 0$ from $\mu$. Then

$$\nu\equiv\mu^{2^s}\equiv\beta^{2^s}\alpha^{a_1 2^s}\prod_{k=1}^{n_1}p_k^{f_k 2^s}\prod_{l=1}^{n_2}\pi_l^{g_l 2^s}\mod\gamma.$$

By Theorem 2.2.1 (2), $\eta^h \mid \nu$ whenever $\eta \mid \mu$, where $\eta$ is a prime factor of $\gamma$ and $h$ is the highest power of $\eta$ in $\gamma$. Thus, for each $k \in \{1, \ldots, n_1\}$ such that $p_k \mid \mu$, we have

$$f_k 2^s \geq b_k.$$

Similarly, for each $l \in \{1, \ldots, n_2\}$ such that $\pi_l \mid \mu$, for $a_1$ such that $\alpha \mid \mu$, we also have

$$g_l 2^s \geq c_l \quad \text{and} \quad a_1 2^s \geq a.$$

These imply that $s \geq \left\lceil \log_2 \frac{b_k}{f_k} \right\rceil$, $s \geq \left\lceil \log_2 \frac{c_l}{g_l} \right\rceil$ and $s \geq \left\lceil \log_2 \frac{a}{a_1} \right\rceil$ for these values of $k$, $l$, $a_1$. If $\eta \nmid \mu$ then $\eta \nmid \nu$. It now follows that

$$s \geq \max_{1 \leq k \leq n_1} \left\lceil \log_2 \frac{B_k}{f_k} \right\rceil, \quad s \geq \max_{1 \leq l \leq n_2} \left\lceil \log_2 \frac{C_l}{g_l} \right\rceil \quad \text{and} \quad s \geq \left\lceil \log_2 \frac{A_{a_1}}{a_1} \right\rceil.$$

From the observations that $\eta^h \mid \nu$ whenever $\eta \mid \mu$ and $\eta \nmid \nu$ implies $\eta \nmid \mu$, we obtain that $\gamma' = \gamma / \gcd(\nu, \gamma)$ and $\gcd(\gamma/\gamma', \gamma') = 1 = \gcd(\nu, \gamma')$. Let $m = \operatorname{ord}_{\gamma'} \nu$. Since $\nu$ is on a $t$-cycle, it follows from Theorem 2.2.1 (3) that $m$ is odd and $t = \operatorname{ord}_m 2$. Note that if $0 \leq j < e$, then $\operatorname{ord}_{\gamma'} \mu^{2^j} = 2^{e-j} d$. Since $\gcd(2^j, d) = 1$ for $j \geq 0$, we see that if $j \geq e$, then $\operatorname{ord}_{\gamma'} \mu^{2^j} = d$. Thus, $s \geq e$, $m = \operatorname{ord}_{\gamma'} \nu = \operatorname{ord}_{\gamma'} \mu^{2^s} = d$ and $t = \operatorname{ord}_d 2$. Recall that $\nu$ is the vertex on the $t$-cycle closest to $\mu$, our result now follows from above. □

We have an immediate corollary of Theorem 2.2.8.

**Corollary 2.2.9.** *If $\mu$ is a vertex in the subdigraph $G^{(2)}_{\gamma,1}$, then the distance from $\mu$ to the cycle in its component is equal to $\nu_2(\operatorname{ord}_\gamma \mu)$, where $\nu_2(m)$ stands for the integer $j$ such that $2^j \| m$. In particular, if $\mu \in (\mathbb{Z}[i]/(\gamma))^*$, then $\mu$ is on a cycle if and only if $\operatorname{ord}_\gamma \mu$ is odd.*

The next theorem tells us that each vertex on a cycle of $G^{(2)}_{\gamma,1}$ has a directed path of length $v$, where $2^v \| \lambda(\gamma)$ terminating at this vertex. Somer and Křížek also had this result for their quadratic digraph. Their proof in [6] used the existence of a primitive root modulo $p^n$ which is not the case for $\mathbb{Z}[i]/(\eta^h)$. However, we

found that only the existence of an element of order $2^v$ in $(\mathbb{Z}[i]/(\gamma))^*$ obtaining from Theorem 1.1.1 (4) is enough.

**Theorem 2.2.10.** *For each component of $G^{(2)}_{\gamma,1}$, the maximum distance from a vertex in the component to the unique cycle of the component is equal to $\nu_2(\lambda(\gamma))$.*

*Proof.* Let $v = \nu_2(\lambda(\gamma))$. From Theorem 1.1.1 (4), there exists a $\mu \in (\mathbb{Z}[i]/(\gamma))^*$ such that $\operatorname{ord}_\gamma \mu = \lambda(\gamma) = 2^v m$, where $m$ is odd. Choose $\nu = \mu^m$. Then

$$\operatorname{ord}_\gamma \nu = \operatorname{ord}_\gamma \mu^m = \frac{\operatorname{ord}_\gamma \mu}{\gcd(m, \operatorname{ord}_\gamma \mu)} = 2^v.$$

Let $\omega \in (\mathbb{Z}[i]/(\gamma))^*$ be such that $\operatorname{ord}_\gamma \omega$ is odd. By Corollary 2.2.9, $\omega$ is on a $t$-cycle for some $t = \operatorname{ord}_2 d$ and $d \mid m$. We shall find a vertex in the component to $\omega$ of distance $v$. Observe that $\operatorname{ord}_\gamma \omega^{2^j} = \operatorname{ord}_\gamma \omega$, $\operatorname{ord}_\gamma \nu\omega^{2^j} = 2^v \operatorname{ord}_\gamma \omega$ and $(\nu\omega^{2^j})^{2^v} = \nu^{2^v}\omega^{2^{j+v}} = \omega^{2^{j+v}}$ for all nonnegative integers $j$. Write $-v \mod t$ for the remainder when $t$ divides $-v$. Hence, $\nu\omega^{2^{-v \bmod t}}$ is the initial vertex of a directed path of length $v$ to $\omega$, so the maximum distance from a vertex in the component to its unique cycle is equal to $v$. □

**Remark.** Let $\mu$ be an element of $G^{(2)}_{\gamma,1}$ of maximum distance $v$ to the cycle in its component. By Theorem 2.2.10, if $\gamma = \pm 1$, $\pm i$ or $\alpha$, then $v = 0$ and $\mu$ is the fixed point 1 of indegree 1. If $N(\gamma) > 2$, then $\mu$ lies outside of the cycle in $C$, and consequently has indegree 0.

Let

$$T = \{\mu \in (\mathbb{Z}[i]/(\gamma))^* : \mu^{2^j} = 1 \text{ for some } j \in \{0, \ldots, v\}\},$$

where $v = \nu_2(\lambda(\gamma))$. We know that 1 is a fixed point and every vertex in $T$ is pointing to 1. Hence, we have the following result.

**Theorem 2.2.11.** *If $\nu_2(\lambda(\gamma)) = v$, then*

$$T = \{\mu \in (\mathbb{Z}[i]/(\gamma))^* : \mu^{2^j} = 1 \textit{ for some } j \in \{0, \ldots, v\}\}$$

*consists of all vertices of the component containing* 1*. Moreover, every vertex in $T$ is on the tree attached to the fixed point* 1*.*

If $\omega \in (\mathbb{Z}[i]/(\gamma))^*$ is of odd order and is on a $t$-cycle, the proof of Theorem 2.2.10 shows that

$$T_\omega = \{\nu\omega^{2^{-\nu_2(\mathrm{ord}_\gamma\,\nu)}} : \nu \in T\}$$

is a vertex on the tree attached to $\omega$. Furthermore, a simple calculation shows that $|T_\omega| = |T|$. On the other hand, let $\mu \in (\mathbb{Z}[i]/(\gamma))^*$ be a vertex on this tree pointing to $\omega$. Then $\mu^{2^j} = \omega$ for some $j \in \{0, \ldots, l\}$. Note that $\xi \in (\mathbb{Z}[i]/(\gamma))^*$ is a root $x^{2^j} = \omega$ if and only if $\xi\mu^{-1}$ is a root of $x^{2^j} = 1$. Hence, we have a one-to-one correspondence between $T$ and $T_\omega$ preserving the tree structure. Therefore, we have shown:

**Theorem 2.2.12.** *Let $\omega \in (\mathbb{Z}[i]/(\gamma))^*$ be a vertex on a $t$-cycle. Then the tree attached to $\omega$ is isomorphic to the tree attached to* 1.

Our final result is on the maximum distance from a vertex in $G^{(2)}_{\gamma,2}$.

Let $w$ be the maximum value of $\nu_2(\lambda(\gamma'))$, where $N(\gamma') < N(\gamma)$, $\gamma' \mid \gamma$ and $\gcd(\gamma/\gamma', \gamma') = 1$.

**Theorem 2.2.13.** *Let $\delta$ be the maximum distance from a vertex in $G^{(2)}_{\gamma,2}$ to the cycle in its component. Then*

$$\delta = \max\left(\max_{1\le k\le n_1}(\lceil\log_2 b_k\rceil), \max_{1\le l\le n_2}(\lceil\log_2 c_l\rceil), \lceil\log_2 a\rceil, w\right).$$

*Proof.* Let $\mu \in \mathbb{Z}[i]/(\gamma)$ be a vertex in a component $C$ of $G^{(2)}_{\gamma,2}$ and let $s$ be the distance from $\mu$ to the cycle in $C$. Let

$$\mu = \beta\alpha^{a_1}\prod_{k=1}^{n_1} p_k^{f_k}\prod_{l=1}^{n_2}\pi_l^{g_l},$$

where the primes $\alpha$, $p_k$ and $\pi_l$ are given in (1.1), $\gcd(\beta, \gamma) = 1$ and $a_1$, $f_k$, $g_l$ are nonnegative integers. But for at least one $j \in \{a_1, f_k, g_l\}$, $j \ge 1$. Let $A_{a_1}$, $B_k$, $C_l$ and $\gamma'$ be defined as in Theorem 2.2.8. Then $\gamma' \mid \gamma$ and $\gcd(\gamma/\gamma', \gamma') = 1 = \gcd(\mu, \gamma)$. Let $\mathrm{ord}_{\gamma'}\,\mu = 2^e d$, where $\gcd(2, d) = 1$. Then by Theorem 2.2.8,

$$s = \max\left(\max_{1\le k\le n_1}\left\lceil\log_2\frac{B_k}{f_k}\right\rceil, \max_{1\le l\le n_2}\left\lceil\log_2\frac{C_l}{g_l}\right\rceil, \left\lceil\log_2\frac{A_{a_1}}{a_1}\right\rceil, e\right).$$

From the definition of $B_k$, $C_l$ and $A_{a_1}$, we have

$$\max_{1\le k\le n_1}\left\lceil \log_2 \frac{B_k}{f_k}\right\rceil \le \max_{1\le l\le n_2}(\log_2 b_k),$$

$$\max_{1\le l\le n_2}\left\lceil \log_2 \frac{C_l}{g_l}\right\rceil \le \max_{1\le l\le n_2}(\log_2 c_l) \quad \text{and} \quad \left\lceil \log_2 \frac{A_{a_1}}{a_1}\right\rceil \le \log_2 a.$$

It follows from the definition of $\gamma'$ and from the definition of $\lambda$ that

$$e \le w.$$

Thus,

$$s \le \max\left(\max_{1\le k\le n_1}\lceil \log_2 b_k\rceil, \max_{1\le l\le n_2}\lceil \log_2 c_l\rceil, \lceil \log_2 a\rceil, w\right).$$

Next, we shall show that we can find vertices in $G^{(2)}_{\gamma,2}$ such that the distances are equal to $\max(\max_{1\le k\le n_1}\lceil \log_2 b_k\rceil, \max_{1\le l\le n_2}\lceil \log_2 c_l\rceil, \lceil \log_2 a\rceil)$ and $w$, respectively.

Consider the cycle containing the fixed point 0. Then $\alpha\prod_{k=1}^{n_1} p_k \prod_{l=1}^{n_2}\pi_l$ is in the same component as 0 and the distances from 0 is equal to

$$\max\left(\max_{1\le k\le n_1}\lceil \log_2 b_k\rceil, \max_{1\le l\le n_2}\lceil \log_2 c_l\rceil, \lceil \log_2 a\rceil\right).$$

Let $\gamma' \in \mathbb{Z}[i]/(\gamma)$ be such that $\gamma' \mid \gamma$ and $\gcd(\gamma/\gamma', \gamma') = 1$. By Theorem 1.1.1, there exists a $\mu \in \mathbb{Z}[i]/(\gamma)$ such that

$$\nu_2(\mathrm{ord}_{\gamma'}\,\mu) = \nu_2(\lambda(\gamma')).$$

By the Chinese remainder theorem, we can find $\omega \in G^{(2)}_{\gamma,2}$ such that

$$\omega \equiv 0 \mod \gamma/\gamma' \quad \text{and} \quad \omega \equiv \mu \mod \gamma'.$$

Hence, we see that the distance from $\omega$ to the cycle in its component is

$$\nu_2(\mathrm{ord}_{\gamma'}\,\omega) = \nu_2(\lambda(\gamma')).$$

Since the number of $\gamma'$ for which $\gamma' \mid \gamma$ is finite, we can find such $\gamma'$ for which $\nu_2(\lambda(\gamma'))$ is a maximum and this value is $w$. □

The above theorem yields an immediate corollary.

**Corollary 2.2.14.** *Let $\mu \in G^{(2)}_{\gamma,2}$ be of the maximum possible distance $\delta$ from the cycle in its component. The following statements hold.*

*(1) if $\gamma = \eta^h$, where $\eta$ is a prime in $\mathbb{Z}[i]$ and $h > 1$, then $\delta = \lceil \log_2 h \rceil$.*

*(2) If $\gamma$ is square-free, then $\delta = w$.*

*(3) if $\gamma$ is a prime in $\mathbb{Z}[i]$, then $\mu$ is the fixed point $0$ of indegree $1$ and $\delta = 0$.*

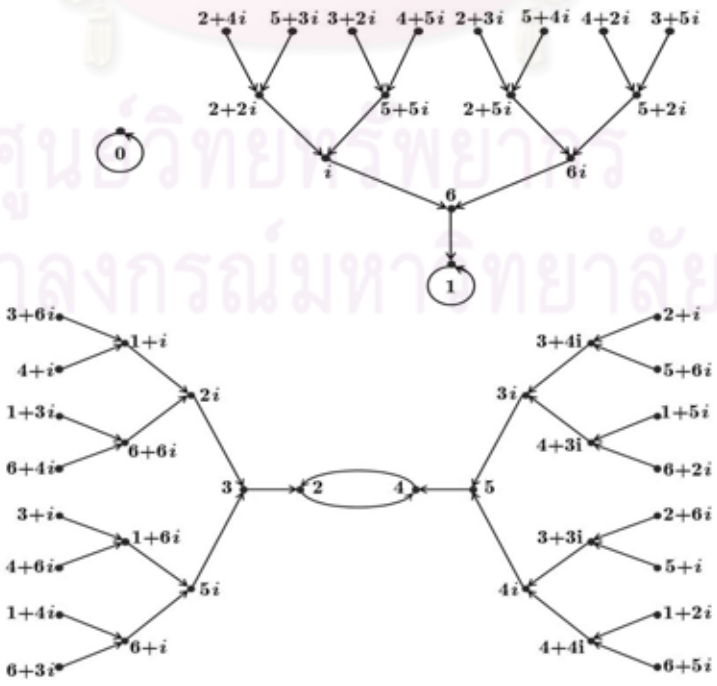
*(4) If $\gamma$ is not a prime in $\mathbb{Z}[i]$, then $\mu$ lies outside the cycle in its component and $\mu$ has indegree $0$.*

# CHAPTER III

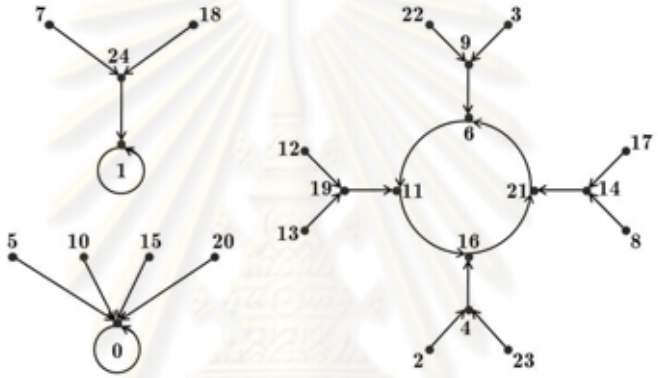
# EXAMPLES

We illustrate the results of the previous chapters by the following examples.

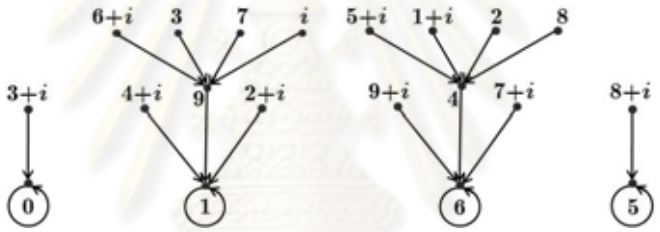
1. Let $\gamma = 7$. Note that 7 is a prime in $\mathbb{Z}[i]$ and $N(7) = 49$. Then $\omega(\gamma) = 1$ and by Lemma 1.2.1, $|\mathbb{Z}[i]/(\gamma)| = |\{[x + yi]_\gamma : 0 \leq x < 7(1^2 + 0^2), 0 \leq y < 7\}| = N(7) = 49$. Since $\omega(\gamma) = 1$, by Corollary 2.2.3, the number of fixed points is $C_\gamma^1 = 2^{\omega(\gamma)} = 2$. Observe that $\gamma$ is square-free, and Proposition 2.1.2 implies that 0 is an isolated fixed point. By Proposition 1.2.6, $\lambda(\gamma) = 3 \cdot 2^4$, so $v = \nu_2(\lambda(\gamma)) = 4$ and the odd numbers dividing $\lambda(\gamma)$ are 1 and 3 which give $t = 1$ and $t = 2$, respectively. Thus, $G_{\gamma,2}^{(2)}$ has only 0 as an isolated fixed point but $G_{\gamma,1}^{(2)}$ contains one fixed point and one 2-cycle. We display the digraph $G_\gamma^{(2)}$ below.



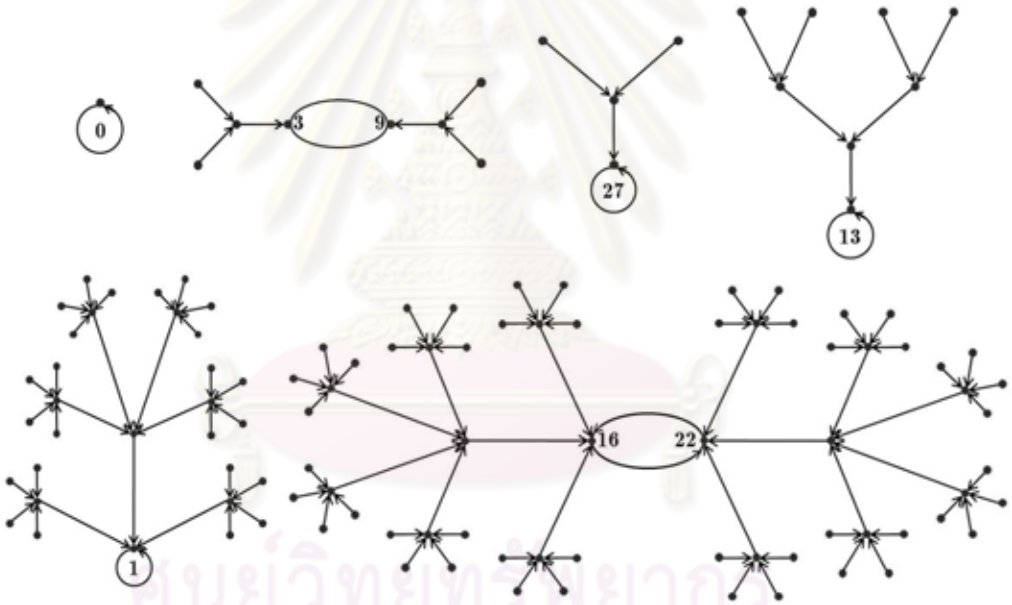
2. Let $\gamma = 3+4i = (2+i)^2$. By Corollary 2.2.14 (1), $\delta = \lceil \log_2 2 \rceil = 1$. Note that $|\mathbb{Z}[i]/(\gamma)| = |\{[x+yi]_\gamma : 0 \le x < 1(3^2+4^2), 0 \le y < 1\}| = N(3+4i) = 25$. Since $\omega(\gamma) = 1$, by Corollary 2.2.3, the number of fixed points is $C_\gamma^1 = 2^{\omega(\gamma)} = 2$. By Proposition 1.2.6, $\lambda(\gamma) = 5 \cdot 2^2$, so $v = \nu_2(\lambda(\gamma)) = 2$ and the odd numbers dividing $\lambda(\gamma)$ are 1 and 5 which yield $t = 1$ and 4, respectively. Thus, the number of 4-cycles is 1 and the trees attached to $6, 11, 16$ and 21 are isomorphic to the tree attached to 1. The digraph $G_\gamma^{(2)}$ is shown below.



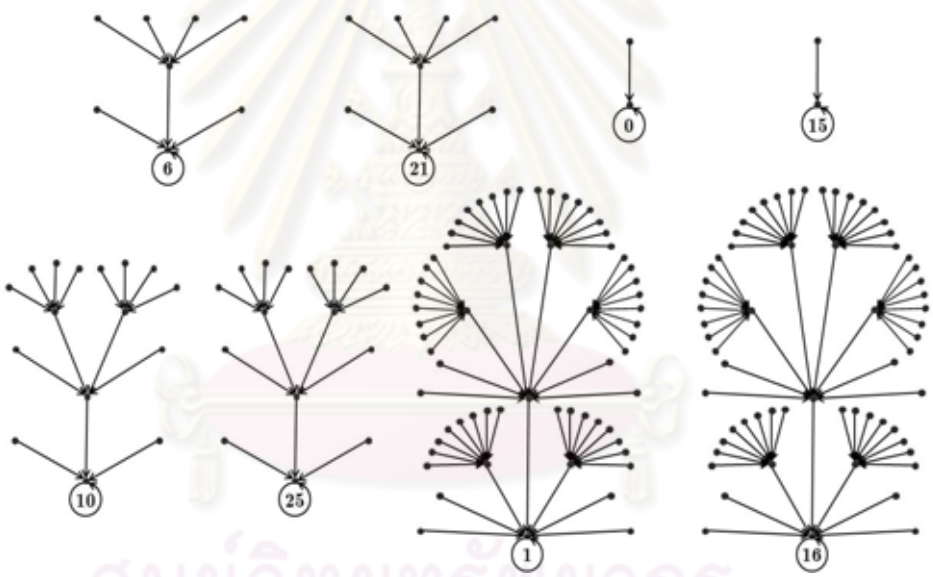
3. Let $\gamma = 2 + 4i = (2 - i)\alpha^2$. Since $\omega(\gamma) = 2$, by Corollary 2.2.3, the number of fixed points is $C_\gamma^1 = 2^{\omega(\gamma)} = 4$. By Proposition 1.2.6, we have that $\lambda(\gamma) = \text{lcm}\{\lambda(\alpha^2), \lambda(2 - i)\} = 2^2$, so $v = \nu_2(\lambda(\gamma)) = 2$ and the only odd number dividing $\lambda(\gamma)$ is 1, which yields $t = 1$. Also, for each $\eta \in \{\alpha, 2 - i\}$, the only odd number dividing $\lambda(\gamma/\eta^h)$ is 1. Then both $G_{\gamma,1}^{(2)}$ and $G_{\gamma,2}^{(2)}$ contain only 1-cycles. Let $w$ be the maximum value of $\nu_2(\lambda(\gamma'))$, where $\gamma' \mid \gamma, N(\gamma') < N(\gamma)$ and $\gcd(\gamma/\gamma', \gamma') = 1$. Thus, $w = \max(\nu_2(\lambda(1)), \nu_2(\lambda(\alpha^2)), \nu_2(\lambda(2 - i))) = 2$. We know that $|\mathbb{Z}[i]/(\gamma)| = |\{[x + yi]_\gamma : 0 \leq x < 2(1^2 + 2^2), 0 \leq y < 2\}| = N(2 + 4i) = 20$. By Theorem 2.2.13, $\delta = \max(\lceil \log_2 1 \rceil, \lceil \log_2 2 \rceil, w) = 2$. We display the digraph $G_\gamma^{(2)}$ below.



4. Let $\gamma = 9 + 6i = 3(3 + 2i)$. Then $\omega(\gamma) = 2, \gamma$ is square-free and so 0 is an isolated fixed point. Since $\omega(\gamma) = 2$, by Corollary 2.2.3, the number of fixed points is $C_\gamma^1 = 2^{\omega(\gamma)} = 4$. It follows that from Proposition 1.2.6 (4), $\lambda(\gamma) = \text{lcm}\{\lambda(3), \lambda(3 + 2i)\} = 3 \cdot 2^3$. Thus, $v = \nu_2(\lambda(\gamma)) = 3$ and the odd numbers dividing $\lambda(\gamma)$ are 1 and 5 which provide $t = 1$ and 2, respectively. By Corollary 2.2.14 (2), $\delta = w = \max(\nu_2(\lambda(1)), \nu_2(\lambda(3)), \nu_2(\lambda(3 + 2i))) = 3$. Note that $|\mathbb{Z}[i]/(\gamma)| = |\{[x + yi]_\gamma : 0 \leq x < 3(3^2 + 2^2), 0 \leq y < 3\}| = N(9 + 6i) = 117$, and hence the number of 2-cycles is 2. The digraph $G_\gamma^{(2)}$ is shown below.



5. Let $\gamma = 12+6i = 3(1-2i)\alpha^2$. Then $\lambda(\gamma) = \text{lcm}\{\lambda(3), \lambda(1-2i), \lambda(\alpha^2)\} = 2^3$, so $v = \nu_2(\lambda(\gamma)) = 3$ and the only odd number dividing $\lambda(\gamma)$ is 1, which yields $t = 1$. Since $\omega(\gamma) = 3$, by Corollary 2.2.3, $C^1_{\gamma,2} = 2^{\omega(\gamma)} - 1 = 7$ and $C^1_{\gamma,1} = 1$. This implies that $G^{(2)}_{\gamma,1}$ has only one component and $G^{(2)}_{\gamma,2}$ has seven components. Let $w$ be the maximum value of $\nu_2(\lambda(\gamma'))$, where $\gamma' \mid \gamma, N(\gamma') < N(\gamma)$ and $\gcd(\gamma/\gamma', \gamma') = 1$. Thus, $w = 3$. By Theorem 2.2.13, we have that $\delta = \max(\lceil \log_2 1 \rceil, \lceil \log_2 1 \rceil, \lceil \log_2 2 \rceil, w) = 3$. Also, $|\mathbb{Z}[i]/(\gamma)| = |\{[x+yi]_\gamma : 0 \le x < 6(2^2+1^2), 0 \le y < 6\}| = N(12+6i) = 180$. The digraph $G^{(2)}_\gamma$ is displayed below.



# REFERENCES


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

[2] J. T. Cross, The Euler $\phi$-function in the Guassian integers, *Amer. Math. Monthly*, **90** (1983) 518–528.

[3] G. Dresden and W. M. Dymàček, Finding factors of factor rings over the Gaussian integers, *Amer. Math. Monthly*, **112** (2005) 602–611.

[4] K. Glaeser, *The Digraph of the Square Mapping on Elliptic Curves*. Preprint available at http://www.rose-hulman.edu/ holden/REU/Reports/glaeser.pdf, 2009.

[5] Y. Meemark and N. Maingam, The digraph of the square mapping on quotient rings over the Gaussian integers, *Int. J. Number Theory*, to appear.

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

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

# VITA

**Name** Mr. Nawaphon Maingam

**Date of Birth** 28 October 1985

**Place of Birth** Suphanburi, Thailand

**Education** B.Sc. (Mathematics, Second Class Honours),
Kasetsart University, 2008