KYUNGPOOK Math. J. 59(2019), 591-601
https://doi.org/10.5666/KMJ.2019.59.4.591
pISSN 1225-6951 eISSN 0454-8124

The Zero-divisor Graph of the Ring of Integers Modulo n

Seung Jun Pi
Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu, 41566, Republic of Korea
e-mail : seungjunpi0@gmail.com

Se Hun Kim
Department of Mathematics, Seoul National University, Seoul, 03080, Republic of Korea
e-mail : shunhun33@gmail.com

Jung Wook Lim*
Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu, 41566, Republic of Korea
e-mail : jwlim@knu.ac.kr

Abstract. Let $\mathbb{Z}_n$ be the ring of integers modulo n and $\Gamma(\mathbb{Z}_n)$ the zero-divisor graph of $\mathbb{Z}_n$. In this paper, we study some properties of $\Gamma(\mathbb{Z}_n)$. More precisely, we completely characterize the diameter and the girth of $\Gamma(\mathbb{Z}_n)$. We also calculate the chromatic number of $\Gamma(\mathbb{Z}_n)$.

1. Introduction

1.1. Preliminaries

In this subsection, we review some concepts from basic graph theory. Let G be a (undirected) graph. Recall that G is *connected* if there is a path between any two distinct vertices of G. The graph G is *complete* if any two distinct vertices are adjacent. The complete graph with n vertices is denoted by K_n. The graph G is a *complete bipartite graph* if G can be partitioned into two disjoint nonempty vertex sets A and B such that two distinct vertices are adjacent if and only if they are in distinct vertex sets. If one of the vertex sets is a singleton set, then we call

* Corresponding Author.
Received October 15, 2018; revised September 5, 2019; accepted November 11, 2019.
2010 Mathematics Subject Classification: 05C15, 05C25, 05C38.
Key words and phrases: zero-divisor graph, ring of integers modulo n, diameter, girth, clique, chromatic number.

G a *star*. We denote the complete bipartite graph by $K_{m,n}$, where m and n are the cardinal numbers of A and B, respectively. For vertices a and b in G, $d(a,b)$ denotes the length of the shortest path from a to b. If there is no such path, then $d(a,b)$ is defined to be ∞; and $d(a,a)$ is defined to be zero. The *diameter* of G, denoted by $\mathrm{diam}(G)$, is the supremum of $\{d(a,b) \mid a \text{ and } b \text{ are vertices of } G\}$. The *girth* of G, denoted by $\mathrm{g}(G)$, is defined as the length of the shortest cycle in G. If G contains no cycles, then $\mathrm{g}(G)$ is defined to be ∞. A subgraph H of G is an *induced subgraph* of G if two vertices of H are adjacent in H if and only if they are adjacent in G. The *chromatic number* of G is the minimum number of colors needed to color the vertices of G so that no two adjacent vertices share the same color, and is denoted by $\chi(G)$. A *clique* C in G is a subset of the vertex set of G such that the induced subgraph of G by C is a complete graph. The *clique number* of G, denoted by $cl(G)$, is the greatest integer $n \geq 1$ such that $K_n \subseteq G$. If $K_n \subseteq G$ for all integers $n \geq 1$, then $cl(G)$ is defined to be ∞. A *maximal clique* in G is a clique that cannot be extended by including one more adjacent vertex. It is easy to see that $\chi(G) \geq cl(G)$.

1.2. The Zero-divisor Graph of a Commutative Ring

Let R be a commutative ring with identity and $\mathrm{Z}(R)$ the set of nonzero zero-divisors of R. The *zero-divisor graph* of R, denoted by $\Gamma(R)$, is the simple graph with vertex set $\mathrm{Z}(R)$, and for distinct $a, b \in \mathrm{Z}(R)$, a and b are adjacent if and only if $ab = 0$. Clearly, $\Gamma(R)$ is the null graph if and only if R is an integral domain.

In [4], Beck first introduced the concept of the zero-divisor graphs of commutative rings and in [3], Anderson and Nazeer continued the study. In their papers, all elements of R are vertices of the graph and they were mainly interested in colorings. In [2], Anderson and Livingston gave the present definition of $\Gamma(R)$ in order to emphasize the study of the interplay between graph-theoretic properties of $\Gamma(R)$ and ring-theoretic properties of R. It was shown that $\Gamma(R)$ is connected with $\mathrm{diam}(\Gamma(R)) \leq 3$ [2, Theorem 2.3]; and $\mathrm{g}(\Gamma(R)) \leq 4$ [5, (1.4)].

For more on the zero-divisor graph of a commutative ring, the readers can refer to a survey article [1].

Let $\mathbb{Z}_n$ be the ring of integers modulo n. The purpose of this paper is to study some properties of the zero-divisor graph of $\mathbb{Z}_n$. If n is a prime number, then $\mathbb{Z}_n$ has no zero-divisors; so $\Gamma(\mathbb{Z}_n)$ is the null graph. Hence in this paper, we only consider the case that n is a composite. In Section 2, we completely characterize the diameter and the girth of $\Gamma(\mathbb{Z}_n)$. In Section 3, we calculate the chromatic number of $\Gamma(\mathbb{Z}_n)$. Note that all figures are drawn via website http://graphonline.ru/en/.

2. The Diameter and the Girth of $\Gamma(\mathbb{Z}_n)$

Our first result in this section is the complete characterization of the diameter of $\Gamma(\mathbb{Z}_n)$.

Theorem 2.1. *The following statements hold.*

(1) $\mathrm{diam}(\Gamma(\mathbb{Z}_n)) = 0$ *if and only if* $n = 4$.

(2) $\operatorname{diam}(\Gamma(\mathbb{Z}_n)) = 1$ *if and only if* $n = p^2$ *for some prime* $p \geq 3$.

(3) $\operatorname{diam}(\Gamma(\mathbb{Z}_n)) = 2$ *if and only if* $n = p^r$ *for some prime* p *and some integer* $r \geq 3$, *or* $n = pq$ *for some distinct primes* p *and* q.

(4) $\operatorname{diam}(\Gamma(\mathbb{Z}_n)) = 3$ *if and only if* $n = pqr$ *for some distinct primes* p, q *and some integer* $r \geq 2$.

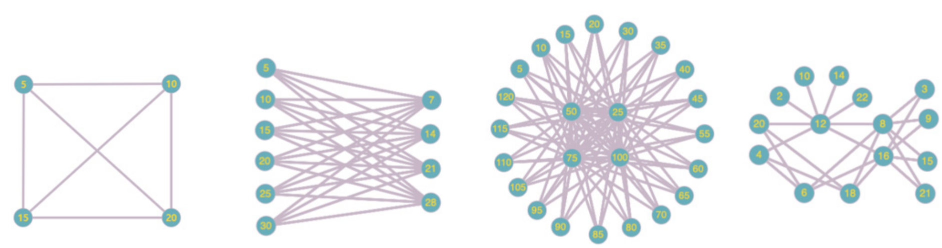
Proof. (1) If $n = 4$, then $\mathrm{Z}(\mathbb{Z}_4) = \{2\}$; so $\operatorname{diam}(\Gamma(\mathbb{Z}_4)) = 0$.

(2) If $n = p^2$ for some prime $p \geq 3$, then $\mathrm{Z}(\mathbb{Z}_{p^2}) = \{p, 2p, \ldots, (p-1)p\}$; so the product of any two elements of $\mathrm{Z}(\mathbb{Z}_{p^2})$ is zero. Hence $\Gamma(\mathbb{Z}_{p^2})$ is the complete graph K_{p-1}. Thus $\operatorname{diam}(\Gamma(\mathbb{Z}_{p^2})) = 1$.

(3) If $n = p^r$ for some prime p and some integer $r \geq 3$, then $\mathrm{Z}(\mathbb{Z}_{p^r}) = \{p, 2p, \ldots, (p^{r-1}-1)p\}$; so $ap^{r-1} = 0$ for all $a \in \mathrm{Z}(\mathbb{Z}_{p^r})$. Hence $\operatorname{diam}(\Gamma(\mathbb{Z}_{p^r})) \leq 2$. Note that $p((p^{r-1}-1)p) \neq 0$. Thus $\operatorname{diam}(\Gamma(\mathbb{Z}_{p^r})) = 2$.

If $n = pq$ for some distinct primes p and q, then $\mathrm{Z}(\mathbb{Z}_{pq}) = \{p, 2p, \ldots, (q-1)p, q, 2q, \ldots, (p-1)q\}$; so $(ip)(jq) = 0$ for all $i = 1, \ldots, q-1$ and $j = 1, \ldots, p-1$. Note that for any $a, b \in \{p, 2p, \ldots, (q-1)p\}$ and $c, d \in \{q, 2q, \ldots, (p-1)q\}$, $ab \neq 0$ and $cd \neq 0$. Hence $\Gamma(\mathbb{Z}_{pq})$ is the complete bipartite graph $K_{p-1,q-1}$. Thus $\operatorname{diam}(\Gamma(\mathbb{Z}_{pq})) = 2$.

(4) Suppose that $n = pqr$ for some distinct primes p, q and some integer $r \geq 2$. Then $p, q \in \mathrm{Z}(\mathbb{Z}_{pqr})$ with $pq \neq 0$; so $\operatorname{diam}(\Gamma(\mathbb{Z}_{pqr})) \geq 2$. If there exists an element $a \in \mathrm{Z}(\mathbb{Z}_{pqr})$ such that $p \sim a \sim q$ is a path, then a is a nonzero multiple of pr and qr; so a is nonzero a multiple of pqr. This is a contradiction. Hence $\operatorname{diam}(\Gamma(\mathbb{Z}_{pqr})) \geq 3$. Thus $\operatorname{diam}(\Gamma(\mathbb{Z}_{pqr})) = 3$ [2, Theorem 2.3]. □



$\operatorname{diam}(\Gamma(\mathbb{Z}_{25})) = 1$ $\operatorname{diam}(\Gamma(\mathbb{Z}_{35})) = 2$ $\operatorname{diam}(\Gamma(\mathbb{Z}_{125})) = 2$ $\operatorname{diam}(\Gamma(\mathbb{Z}_{24})) = 3$

Figure 1: The diameters of some zero-divisor graphs

We next study the girth of $\Gamma(\mathbb{Z}_n)$.

Lemma 2.2. *If* $\mathrm{g}(\Gamma(\mathbb{Z}_n)) = 3$, *then* $\mathrm{g}(\Gamma(\mathbb{Z}_{mn})) = 3$ *for all integers* $m \geq 1$.

Proof. Note that if $a \sim b \sim c \sim a$ is a cycle in $\Gamma(\mathbb{Z}_n)$, then $am \sim bm \sim cm \sim am$ is a cycle in $\Gamma(\mathbb{Z}_{mn})$. Thus $\mathrm{g}(\Gamma(\mathbb{Z}_{mn})) = 3$. □

The next example shows that Lemma 2.2 cannot be extended to the case of girth 4.

Example 2.3.

(1) Note that $g(\Gamma(\mathbb{Z}_{12})) = 4$. In fact, $3 \sim 4 \sim 6 \sim 8 \sim 3$ is a cycle of length 4 in $\Gamma(\mathbb{Z}_{12})$. However, $g(\Gamma(\mathbb{Z}_{24})) = 3$ because $6 \sim 8 \sim 12 \sim 6$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{24})$.

(2) In general, $g(\Gamma(\mathbb{Z}_{4q})) = 4$ but $g(\Gamma(\mathbb{Z}_{2^r q})) = 3$ for all primes $q \geq 3$ and all integers $r \geq 3$. (See Proposition 2.6.)

Proposition 2.4. *If $t \geq 3$ is an integer and $p_1, \ldots, p_t$ are distinct primes, then $g(\Gamma(\mathbb{Z}_{p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}})) = 3$ for all positive integers $r_1, \ldots, r_t$.*

Proof. If $t = 3$, then $p_1^{r_1} p_2^{r_2} \sim p_2^{r_2} p_3^{r_3} \sim p_1^{r_1} p_3^{r_3} \sim p_1^{r_1} p_2^{r_2}$ is a cycle in $\Gamma(\mathbb{Z}_{p_1^{r_1} p_2^{r_2} p_3^{r_3}})$; so $g(\Gamma(\mathbb{Z}_{p_1^{r_1} p_2^{r_2} p_3^{r_3}})) = 3$.

If $t > 3$, then the result follows directly from Lemma 2.2. □

Proposition 2.5. *Let p be a prime and $r \geq 2$ an integer. Then the following assertions hold.*

(1) $g(\Gamma(\mathbb{Z}_{p^r})) = \infty$ *if and only if* $p^r = 4, 8$ *or* 9.

(2) $g(\Gamma(\mathbb{Z}_{p^r})) = 3$ *if and only if each of the following conditions holds.*

(a) $p = 2$ *and* $r \geq 4$.

(b) $p = 3$ *and* $r \geq 3$.

(c) $p \geq 5$ *and* $r \geq 2$.

Proof. (1) It is obvious that $\Gamma(\mathbb{Z}_4)$, $\Gamma(\mathbb{Z}_8)$ and $\Gamma(\mathbb{Z}_9)$ have no cycles. Thus the equivalence follows.

(2) If $p = 2$ and $r \geq 4$, then $2^{r-1}, 2^{r-2}, 3 \cdot 2^{r-2} \in Z(\mathbb{Z}_{2^r})$. Since the product of any two of them is zero, $2^{r-1} \sim 2^{r-2} \sim 3 \cdot 2^{r-2} \sim 2^{r-1}$ is a cycle in $\Gamma(\mathbb{Z}_{2^r})$. Thus $g(\Gamma(\mathbb{Z}_{2^r})) = 3$.

If $p = 3$ and $r \geq 3$, then $3^{r-1}, 2 \cdot 3^{r-1}, 3^{r-2} \in Z(\mathbb{Z}_{3^r})$. Since the product of any two of them is zero, $3^{r-1} \sim 2 \cdot 3^{r-1} \sim 3^{r-2} \sim 3^{r-1}$ is a cycle in $\Gamma(\mathbb{Z}_{3^r})$. Thus $g(\Gamma(\mathbb{Z}_{3^r})) = 3$.

If $p \geq 5$ and $r \geq 2$, then $p^{r-1}, 2p^{r-1}, 3p^{r-1} \in Z(\mathbb{Z}_{p^r})$. Since the product of any two of them is zero, $p^{r-1} \sim 2p^{r-1} \sim 3p^{r-1} \sim p^{r-1}$ is a cycle in $\Gamma(\mathbb{Z}_{p^r})$. Thus $g(\Gamma(\mathbb{Z}_{p^r})) = 3$. □

Proposition 2.6. *Let n be a positive integer which has only two distinct prime divisors. Then the following assertions hold.*

(1) $g(\Gamma(\mathbb{Z}_n)) = \infty$ *if and only if* $n = 2q$ *for some prime* $q \geq 3$.

(2) $g(\Gamma(\mathbb{Z}_n)) = 3$ *if and only if one of the following holds.*

(a) $n = 2^r q^s$ *for some prime* $q \geq 3$ *and some integers* $r \geq 1$ *and* $s \geq 2$.

(b) $n = 2^r q$ *for some prime* $q \geq 3$ *and some integer* $r \geq 3$.

(c) $n = 3^r q^s$ *for some prime* $q \geq 5$ *and some integers* $r \geq 1$ *and* $s \geq 2$.

(d) $n = 3^r q$ *for some prime* $q \geq 5$ *and some integer* $r \geq 2$.

(e) $n = p^r q^s$ *for some primes* $q > p \geq 5$ *and some integers* $r, s \geq 1$ *except for* $r = s = 1$.

(3) $\mathrm{g}(\Gamma(\mathbb{Z}_n)) = 4$ *if and only if* $n = pq$ *for some distinct primes* $p, q \geq 3$, *or* $n = 4q$ *for some prime* $q \geq 3$.

Proof. (1) If $n = 2q$ for some prime $q \geq 3$, then $\Gamma(\mathbb{Z}_{2q})$ is a star graph $K_{1,q-1}$ by the proof of Theorem 2.1(3). Hence $\Gamma(\mathbb{Z}_{2q})$ has no cycles, and thus $\mathrm{g}(\Gamma(\mathbb{Z}_{2q})) = \infty$.

(2) Let p and q be the only distinct prime divisors of n. Without loss of generality, we may assume that $p < q$.

Cases (a) and (b). $p = 2$. In this case, $q \sim 2q \sim 4q \sim q$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{2q^2})$; so $\mathrm{g}(\Gamma(\mathbb{Z}_{2q^2})) = 3$. Hence by Lemma 2.2, $\mathrm{g}(\Gamma(\mathbb{Z}_{2^r q^s})) = 3$ for all integers $r \geq 1$ and $s \geq 2$. Also, $4 \sim 2q \sim 4q \sim 4$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{8q})$; so $\mathrm{g}(\Gamma(\mathbb{Z}_{8q})) = 3$. Hence by Lemma 2.2, $\mathrm{g}(\Gamma(\mathbb{Z}_{2^r q})) = 3$ for all integers $r \geq 3$.

Cases (c) and (d). $p = 3$. In this case, $q \sim 3q \sim 6q \sim q$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{3q^2})$; so $\mathrm{g}(\Gamma(\mathbb{Z}_{3q^2})) = 3$. Hence by Lemma 2.2, $\mathrm{g}(\Gamma(\mathbb{Z}_{3^r q^s})) = 3$ for all integers $r \geq 1$ and $s \geq 2$. Also, $3 \sim 3q \sim 6q \sim 3$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{9q})$; so $\mathrm{g}(\Gamma(\mathbb{Z}_{9q})) = 3$. Hence by Lemma 2.2, $\mathrm{g}(\Gamma(\mathbb{Z}_{3^r q})) = 3$ for all integers $r \geq 2$.

Case (e). $p \geq 5$. In this case, $q \geq 7$; so by Proposition 2.5(2), $\mathrm{g}(\Gamma(\mathbb{Z}_{p^r})) = 3 = \mathrm{g}(\Gamma(\mathbb{Z}_{q^s}))$ for all integers $r, s \geq 2$. Hence by Lemma 2.2, $\mathrm{g}(\Gamma(\mathbb{Z}_{p^r q^s})) = 3$ for all integers $r, s \geq 1$ except for $r = s = 1$.

(3) If $n = pq$ for some distinct primes $p, q \geq 3$, then $\Gamma(\mathbb{Z}_{pq})$ is the complete bipartite graph $K_{p-1,q-1}$ by the proof of Theorem 2.1(3). Hence there does not exist a cycle of odd length. Note that $p \sim 2q \sim 2p \sim q \sim p$ is a cycle of length 4. Thus $\mathrm{g}(\Gamma(\mathbb{Z}_{pq})) = 4$.

Let $n = 4q$ for some prime $q \geq 3$, and suppose to the contrary that there exists a cycle $a \sim b \sim c \sim a$ in $\Gamma(\mathbb{Z}_{4q})$. Since ab, bc and ca are divisible by $4q$, q divides at least two of a, b and c. Without loss of generality, we may assume that q divides a and b. If 2 divides a, then $a = 2q$. Since ab is divisible by $4q$, b is divisible by 2; so $b = 2q$. This is absurd. If 2 does not divide a, then $a = q$ or $a = 3q$. Since $4q$ divides ab, b is divisible by 4; so b is a multiple of $4q$. This is a contradiction. Hence there do not exist cycles of length 3 in $\Gamma(\mathbb{Z}_{4q})$. Note that $q \sim 4 \sim 2q \sim 8 \sim q$ is a cycle of length 4. Thus $\mathrm{g}(\Gamma(\mathbb{Z}_{4q})) = 4$. □

In the next remark, we construct a cycle of length 3 in $\Gamma(\mathbb{Z}_n)$ in each case of Proposition 2.6(2).

Remark 2.7.

(1) Let $n = 2^r q^s$ for some prime $q \geq 3$ and some integers $r \geq 1$ and $s \geq 2$. Then $2^r q^{s-1} \sim 2^{r+1} q^{s-1} \sim 2^{r-1} q^s \sim 2^r q^{s-1}$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{2^r q^s})$.

(2) Let $n = 2^r q$ for some prime $q \geq 3$ and some integer $r \geq 3$. Then $2^r \sim 2q \sim 2^{r-1} q \sim 2^r$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{2^r q})$.

(3) Let $n = 3^r q^s$ for some prime $q \geq 5$ and some integers $r \geq 1$ and $s \geq 2$. Then $3^{r-1}q^s \sim 3^r q^{s-1} \sim 2 \cdot 3^r q^{s-1} \sim 3^{r-1}q^s$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{3^r q^s})$.

(4) Let $n = 3^r q$ for some prime $q \geq 5$ and some integer $r \geq 2$. Then $3^r \sim 3^{r-1}q \sim 2 \cdot 3^{r-1}q \sim 3^r$ is a cycle of length 3 in $\Gamma(\mathbb{Z}_{3^r q})$.

(5) Let $n = p^r q^s$ for some primes $q > p \geq 5$ and some integers $r, s \geq 1$ except for $r = s = 1$. If $r \neq 1$ and $s \neq 1$, then $p^r q^{s-1} \sim p^{r-1}q^s \sim 2p^{r-1}q^s \sim p^r q^{s-1}$ and $p^r q^{s-1} \sim 2p^r q^{s-1} \sim 3p^r q^{s-1} \sim p^r q^{s-1}$ are cycles of length 3 in $\Gamma(\mathbb{Z}_{p^r q^s})$, respectively.

By Propositions 2.4, 2.5, and 2.6, we obtain

Theorem 2.8. The following statements hold.

(1) $\mathrm{g}(\Gamma(\mathbb{Z}_n)) = \infty$ if and only if each of the following conditions holds.

  (a) $n = 4, 8, 9$.

  (b) $n = 2q$ for some prime $q \geq 3$.

(2) $\mathrm{g}(\Gamma(\mathbb{Z}_n)) = 4$ if and only if each of the following conditions holds.

  (a) $n = pq$ for some distinct primes $p, q \geq 3$.

  (b) $n = 4q$ for some prime $q \geq 3$.

(3) $\mathrm{g}(\Gamma(\mathbb{Z}_n)) = 3$ in all other cases.

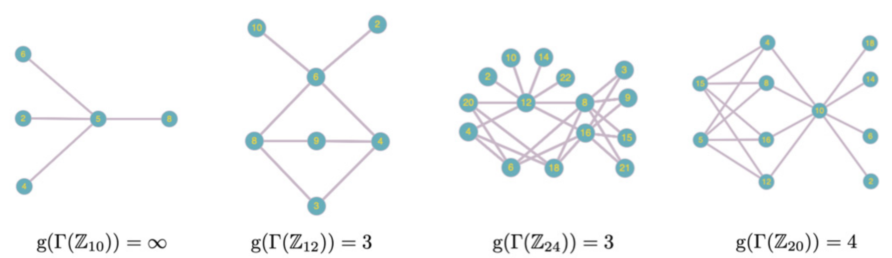


Figure 2: The girth of some zero-divisor graphs

3. The Chromatic Number of $\Gamma(\mathbb{Z}_n)$

In this section, we calculate the chromatic number of $\Gamma(\mathbb{Z}_n)$. Clearly, if there exists a clique in a graph, then the chromatic number of the graph is greater than or equal to the size of the clique; so our method to find the chromatic number of $\Gamma(\mathbb{Z}_n)$ is based on the following three steps:

Step 1. Find a maximal clique C in $\Gamma(\mathbb{Z}_n)$ and color vertices in C.

Step 2. Color vertices in $Z(\mathbb{Z}_n) \setminus C$ by colors used in Step 1.

Step 3. Confirm that there are no adjacent vertices having the same color.

Lemma 3.1. *If $r \geq 2$ is an integer, $n = p_1 \cdots p_r$ for distinct primes $p_1, \ldots, p_r$, and $C = \{\frac{n}{p_i} \,|\, i = 1, \ldots, r\}$, then C is a maximal clique of $\Gamma(\mathbb{Z}_n)$.*

Proof. Note that the product of any two distinct members of C is a multiple of n; so C is a clique. Suppose that there exists an element $a \in Z(\mathbb{Z}_n) \setminus C$ such that ca is a multiple of n for all $c \in C$. Then for all $i = 1, \ldots, r$, p_i divides a; so n divides a. This is a contradiction. Thus C is a maximal clique of $\Gamma(\mathbb{Z}_n)$. □

Theorem 3.2. *If $r \geq 2$ is an integer and $n = p_1 \cdots p_r$ for distinct primes $p_1, \ldots, p_r$, then $\chi(\Gamma(\mathbb{Z}_n)) = r$.*

Proof. Let $C = \{\frac{n}{p_i} \,|\, i = 1, \ldots, r\}$. Then by Lemma 3.1, C is a maximal clique of $\Gamma(\mathbb{Z}_n)$; so the chromatic number of the induced subgraph of $\Gamma(\mathbb{Z}_n)$ induced by C is r. For each $i = 1, \ldots, r$, let $\bar{i}$ be the color of $\frac{n}{p_i}$. Clearly, $Z(\mathbb{Z}_n) \setminus C$ is nonempty. For each $a \in Z(\mathbb{Z}_n) \setminus C$, let $S_a = \{c \in C \,|\, a \text{ and } c \text{ are not adjacent}\}$. Note that by Lemma 3.1, C is a maximal clique; so S_a is a nonempty set. Hence we can find the smallest integer $k \in \{1, \ldots, r\}$ such that a and $\frac{n}{p_k}$ are not adjacent. In this case, we color a with $\bar{k}$.

To complete the proof, we need to check that any two elements in $Z(\mathbb{Z}_n)$ with the same color cannot be adjacent. Let a and b be distinct elements in $Z(\mathbb{Z}_n)$ with the same color $\bar{k}$. Since C is a clique, a and b cannot belong to C at the same time. Suppose that $a \in C$ and $b \in Z(\mathbb{Z}_n) \setminus C$. Then $a = \frac{n}{p_k}$; so by the coloring of b, a and b are not adjacent. Suppose that $a, b \in Z(\mathbb{Z}_n) \setminus C$. Then $\frac{n}{p_k}a$ and $\frac{n}{p_k}b$ are not divisible by n; so neither a nor b is divisible by p_k. Therefore ab is not divisible by n, and hence a cannot be adjacent to b. Thus $\chi(\Gamma(\mathbb{Z}_n)) = r$. □

Example 3.3. Consider $\Gamma(\mathbb{Z}_{15})$. Let $C = \{3, 5\}$. Then by Theorem 3.2, we color 5 and 3 with $\bar{1}$ and $\bar{2}$, respectively. Let $R = \{6, 9, 12\}$ and let $v \in R$. Then v is not adjacent to 3; so we color v with $\bar{2}$. Note that 10 is not adjacent to 5; so we color 5 with $\bar{1}$.

For the detail, see Figure 3. Note that in Figure 3, $\bar{1}$ and $\bar{2}$ are represented by blue and red, respectively.

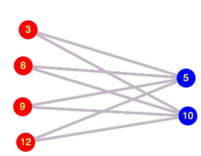


Figure 3: The coloring of $\Gamma(\mathbb{Z}_{15})$

Lemma 3.4. *Let* $n = p_1^{2a_1} \cdots p_r^{2a_r}$ *for distinct primes* $p_1, \ldots, p_r$ *and positive integers* $a_1, \ldots, a_r$*, and let* $C = \{k\sqrt{n} \,|\, k = 1, \ldots, \sqrt{n} - 1\}$*. Then* C *is a clique of* $\Gamma(\mathbb{Z}_n)$*.*

Proof. Note that the product of any two distinct elements of C is a multiple of n. Thus C is a clique. □

Theorem 3.5. *Let* $n = p_1^{2a_1} \cdots p_r^{2a_r}$ *for distinct primes* $p_1, \ldots, p_r$ *and positive integers* $a_1, \ldots, a_r$*. Then* $\chi(\Gamma(\mathbb{Z}_n)) = \sqrt{n} - 1$*.*

Proof. Let $C = \{k\sqrt{n} \,|\, k = 1, \ldots, \sqrt{n} - 1\}$. Then by Lemma 3.4, C is a clique of $\Gamma(\mathbb{Z}_n)$ with $\sqrt{n} - 1$ elements. For each $k \in \{1, \ldots, \sqrt{n} - 1\}$, let $\widehat{k}$ denote the color of $k\sqrt{n}$.

Case 1. $n = p_1^2$. In this case, $\Gamma(\mathbb{Z}_n)$ is a complete graph by Theorem 2.1. Hence $\mathrm{Z}(\mathbb{Z}_n) = C$. Thus $\chi(\Gamma(\mathbb{Z}_n)) = \sqrt{n} - 1$.

Case 2. $n \neq p_1^2$. In this case, $\Gamma(\mathbb{Z}_n)$ is not a complete graph by Theorem 2.1; so $\mathrm{Z}(\mathbb{Z}_n) \setminus C \neq \emptyset$. Let $v \in \mathrm{Z}(\mathbb{Z}_n) \setminus C$. Then there exists an element $m \in \{1, \ldots, r\}$ such that $p_m^{a_m}$ does not divide v. Take the positive integer $s \leq a_m$ such that p_m^{s-1} divides v but p_m^s does not divide v. Then $v((\sqrt{n}/p_m^s)\sqrt{n})$ is not a multiple of n; so v and $(\sqrt{n}/p_m^s)\sqrt{n}$ are not adjacent. We color v with $\widehat{\sqrt{n}/p_m^s}$.

Now, it remains to check that any two vertices with the same color cannot be adjacent. Let v_1 and v_2 be distinct elements of $\mathrm{Z}(\mathbb{Z}_n)$ which have the same color. Since C is a clique, v_1 and v_2 cannot both belong to C. Suppose that $v_1 \in C$ and $v_2 \in \mathrm{Z}(\mathbb{Z}_n) \setminus C$. Let $\widehat{\sqrt{n}/p_m^s}$ be the color of v_2 for some $m \in \{1, \ldots, r\}$ and $s \in \{1, \ldots, a_m\}$. Then v_2 is not divisible by p_m^s by the coloring of v_2. Since $v_1 \in C$, $v_1 = (\sqrt{n}/p_m^s)\sqrt{n}$. Therefore $p_m^{2a_m}$ does not divide $v_1 v_2$. Hence v_1 is not adjacent to v_2. Suppose that $v_1, v_2 \in \mathrm{Z}(\mathbb{Z}_n) \setminus C$, and let $\widehat{\sqrt{n}/p_m^s}$ be the color of v_1 and v_2 for some $m \in \{1, \ldots, r\}$ and $s \in \{1, \ldots, a_m\}$. Then by the coloring of v_1 and v_2, p_m^s divides neither v_1 nor v_2; so p_m^{2s} does not divide $v_1 v_2$. Since $s \leq a_m$, $p_m^{2a_m}$ does not divide $v_1 v_2$. Hence $v_1 v_2$ is not a multiple of n, which means that v_1 and v_2 are not adjacent.

In either case, $\Gamma(\mathbb{Z}_n)$ is $(\sqrt{n}-1)$-colorable. Note that by Lemma 3.4, $\chi(\Gamma(\mathbb{Z}_n)) \geq \sqrt{n} - 1$. Thus $\chi(\Gamma(\mathbb{Z}_n)) = \sqrt{n} - 1$. □

Example 3.6. Consider $\Gamma(\mathbb{Z}_{36})$. Let $C = \{6, 12, 18, 24, 30\}$. Then by Theorem 3.5, we color $6, 12, 18, 24$ and 30 with $\widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}$ and $\widehat{5}$, respectively. Let $R = \{2, 4, 8, 10, 14, 16, 20, 22, 26, 28, 32, 34\}$ and let $v \in R$. Then v is not divisible by 3; so we color v with $\widehat{2}$. Let $B = \{3, 9, 15, 21, 27, 33\}$ and let $v \in B$. Then v is not divisible by 2; so we color v with $\widehat{3}$.

For the detail, see Figure 4. Note that in Figure 4, $\widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}$ and $\widehat{5}$ are represented by green, red, blue, pink and brown, respectively.

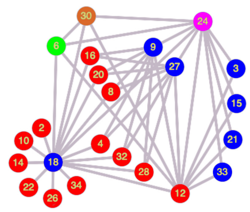


Figure 4: The coloring of $\Gamma(\mathbb{Z}_{36})$

Lemma 3.7. *Let $p_1, \ldots, p_r, q_1, \ldots, q_s$ be distinct primes, $a_1, \ldots, a_r, b_1, \ldots, b_s$ nonnegative integers, not all zero, and let $n = p_1^{2a_1} \cdots p_r^{2a_r} q_1^{2b_1+1} \cdots q_s^{2b_s+1}$. If $C_1 = \{kp_1^{a_1} \cdots p_r^{a_r} q_1^{b_1+1} \cdots q_s^{b_s+1} \mid k = 1, \ldots, p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} - 1\}$ and $C_2 = \{p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1+1} \cdots q_s^{b_s+1}/q_i \mid i = 1, \ldots, s\}$, then $C_1 \cup C_2$ is a maximal clique of $\Gamma(\mathbb{Z}_n)$.*

Proof. We first note that $C_1 \cap C_2 = \emptyset$. Let $C = C_1 \cup C_2$. Then for any distinct elements $\alpha, \beta \in C$, $\alpha\beta$ is a multiple of n; so C is a clique. Suppose that C is not a maximal clique. Then there exists an element $m \in Z(\mathbb{Z}_n) \setminus C$ such that $mc = 0$ for all $c \in C$. Therefore m is a multiple of $p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_{i-1}^{b_{i-1}} q_i^{b_i+1} q_{i+1}^{b_{i+1}} \cdots q_s^{b_s}$ for all $i = 1, \ldots, s$. Hence m is a multiple of $p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1+1} \cdots q_s^{b_s+1}$, which implies that $m \in C_1$. This contradicts the choice of m. Thus C is a maximal clique of $\Gamma(\mathbb{Z}_n)$. □

Theorem 3.8. *Let $p_1, \ldots, p_r, q_1, \ldots, q_s$ be distinct primes and $a_1, \ldots, a_r, b_1, \ldots, b_s$ nonnegative integers, not all zero. If $n = p_1^{2a_1} \cdots p_r^{2a_r} q_1^{2b_1+1} \cdots q_s^{2b_s+1}$, then $\chi(\Gamma(\mathbb{Z}_n)) = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} - 1 + s$.*

Proof. Let $x = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$ and $y = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1+1} \cdots q_s^{b_s+1}$. Then $n = xy$. Let $C_1 = \{ky \mid k = 1, \ldots, x-1\}$, $C_2 = \{y/q_i \mid i = 1, \ldots, s\}$, and $C = C_1 \cup C_2$. Then by Lemma 3.7, C is a maximal clique of $\Gamma(\mathbb{Z}_n)$. For each $k = 1, \ldots, x-1$, let $\widehat{k}$ be the color of ky and for each $i = 1, \ldots, s$, let $\bar{i}$ be the color of y/q_i. Note that by Theorem 2.1, $\Gamma(\mathbb{Z}_n)$ is not a complete graph. Let $v \in Z(\mathbb{Z}_n) \setminus C$.

Case 1. There exists an element $c \in C_1$ which is not adjacent to v. In this case, v is not divisible by x. If $q_1^{b_1} \cdots q_s^{b_s}$ divides v, then $p_m^{a_m}$ does not divide v for some $m \in \{1, \ldots, r\}$; so we can take the positive integer $\alpha \leq a_m$ such that $p_m^{\alpha-1}$ divides v but p_m^{α} does not divide v. Hence v is not adjacent to $(x/p_m^{\alpha})y$. We color v with $\widehat{x/p_m^{\alpha}}$. If $q_t^{b_t}$ does not divide v for some $t \in \{1, \ldots, s\}$, then we can find the positive integer $\beta \leq b_t$ such that $q_t^{\beta-1}$ divides v but q_t^{β} does not divide v. Hence v is not adjacent to $(x/q_t^{\beta})y$. We color v with $\widehat{x/q_t^{\beta}}$.

Case 2. v is adjacent to c for all $c \in C_1$. In this case, v is a multiple of x. If $q_1^{b_1+1} \cdots q_s^{b_s+1}$ divides v, then $v \in C_1$, which is a contradiction to the choice of v. Therefore we can find an element $i \in \{1, \ldots, s\}$ such that $q_i^{b_i}$ divides v but $q_i^{b_i+1}$

does not divide v. Clearly, $v(y/q_i)$ is not a multiple of n. Hence v and y/q_i are not adjacent. We color v with $\bar{i}$.

It remains to show that there are no adjacent vertices with the same color. Let $v_1, v_2 \in Z(\mathbb{Z}_n)$ have the same color. Since C is a clique, at least one of v_1 and v_2 does not belong to C. Suppose that $v_1 \in C$ but $v_2 \in Z(\mathbb{Z}_n) \setminus C$. If the color of v_1 and v_2 is $\widehat{x/p_m^\alpha}$ for some $m \in \{1, \ldots, r\}$ and $\alpha \in \{1, \ldots, a_m\}$, then by the coloring of v_1 and v_2, $v_1 = (x/p_m^\alpha)y$ and p_m^α does not divide v_2; so v_1v_2 is not a multiple of n. Hence v_1 is not adjacent to v_2. If the color of v_1 and v_2 is $\widehat{x/q_t^\beta}$ for some $t \in \{1, \ldots, s\}$ and $\beta \in \{1, \ldots, b_t\}$, then by the coloring of v_1 and v_2, $v_1 = (x/q_t^\beta)y$ and q_t^β does not divide v_2; so v_1v_2 is not a multiple of n. Hence v_1 is not adjacent to v_2. If $\bar{i}$ is the color of v_1 and v_2 for some $i \in \{1, \ldots, s\}$, then $v_1 = y/q_i$ and so by the coloring of v_2, v_1 and v_2 are not adjacent. We next suppose that $v_1, v_2 \in Z(\mathbb{Z}_n) \setminus C$. If $\widehat{x/p_m^\alpha}$ is the color of v_1 and v_2 for some $m \in \{1, \ldots, r\}$ and $\alpha \in \{1, \ldots, a_m\}$, then by Case 1, p_m^α divides neither v_1 nor v_2; so $p_m^{2a_m}$ does not divide v_1v_2. Hence v_1 and v_2 are not adjacent. If $\widehat{x/q_t^\beta}$ is the color of v_1 and v_2 for some $t \in \{1, \ldots, s\}$ and $\beta \in \{1, \ldots, b_t\}$, then by Case 1, q_t^β divides neither v_1 nor v_2; so $q_t^{2b_t}$ does not divide v_1v_2. Hence v_1 and v_2 are not adjacent. If $\bar{i}$ is the color of v_1 and v_2 for some $i \in \{1, \ldots, s\}$, then by Case 2, $q_i^{b_i+1}$ divides neither v_1 nor v_2. Hence $q_i^{2b_i+1}$ cannot divide v_1v_2, which means that v_1 and v_2 are not adjacent. Consequently, $\Gamma(\mathbb{Z}_n)$ is $(p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} - 1 + s)$-colorable. Note that by Lemma 3.7, $\chi(\Gamma(\mathbb{Z}_n)) \geq p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} - 1 + s$. Thus $\chi(\Gamma(\mathbb{Z}_n)) = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} - 1 + s$. □

Example 3.9. Consider $\Gamma(\mathbb{Z}_{18})$. Let $C_1 = \{6, 12\}$ and $C_2 = \{3\}$. Then by Theorem 3.8, we color $6, 12$ and 3 with $\hat{1}, \hat{2}$ and $\bar{1}$, respectively. Let $R = \{2, 4, 8, 10, 14, 16\}$ and let $v \in R$. Then v is not adjacent to 6. Note that v is not divisible by 3; so we color v with $\hat{1}$. Let $B = \{9, 15\}$ and let $v \in B$. Then v is adjacent to all elements in C_1. Note that v is not divisible by 2; so we color v with $\bar{1}$.

For the detail, see Figure 5. Note that in Figure 5, $\hat{1}, \hat{2}$ and $\bar{1}$ are represented by red, green and blue, respectively.

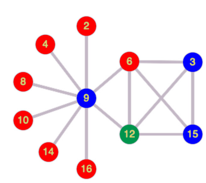


Figure 5: The coloring of $\Gamma(\mathbb{Z}_{18})$

Example 3.10. Consider $\Gamma(\mathbb{Z}_{72})$. Let $C_1 = \{12, 24, 36, 48, 60\}$ and $C_2 = \{6\}$. Then by Theorem 3.6, we color $6, 12, 24, 36, 48$ and 60 with $\bar{1}, \hat{1}, \hat{2}, \hat{3}, \hat{4}$ and $\hat{5}$, respectively.

Let $P = \{2, 4, 8, 10, 14, 16, 20, 22, 26, 28, 32, 34, 38, 40, 44, 46, 50, 52, 56, 58, 62, 64, 68, 70\}$ and let $v \in P$. Then v is not adjacent to 12. Note that v is a multiple of 2 but not a multiple of 3; so we color v with $\widehat{2}$. Let $B = \{3, 9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69\}$ and let $v \in B$. Then v is not adjacent to 12. Note that v is not divisible by 2; so we color v with $\widehat{3}$. Let $Y = \{18, 30, 42, 54, 66\}$ and let $v \in Y$. Then v is adjacent to all elements in C_1. Since v and 6 are not adjacent, we color v with $\overline{1}$.

For the detail, see Figure 6. Note that in Figure 6, $\overline{1}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}$ and $\widehat{5}$ are represented by yellow, red, pink, blue, sky-blue and green, respectively.

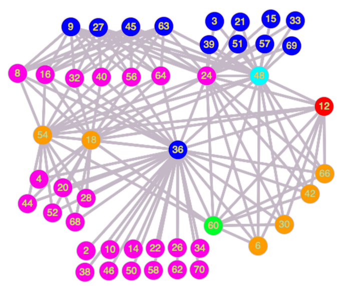


Figure 6: The coloring of $\Gamma(\mathbb{Z}_{72})$

Acknowledgements. The authors would like to thank the referee for his/her several valuable suggestions. The third author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2017R1C1B1008085).

References

[1] D. F. Anderson, M. C. Axtell, and J. A. Stickles, Jr, *Zero-divisor graphs in commutative rings*, Commutative Algebra: Noetherian and Non-Noetherian Perspectives, 23–45, Springer, New York, 2011.

[2] D. F. Anderson and P. S. Livingston, *The zero-divisor graph of a commutative ring*, J. Algebra, **217**(1999), 434–447.

[3] D. D. Anderson and M. Naseer, *Beck's coloring of a commutative ring*, J. Algebra, **159**(1993), 500–514.

[4] I. Beck, *Coloring of commutative rings*, J. Algebra, **116**(1988), 208–226.

[5] S. Mulay, *Cycles and symmetries of zero-divisors*, Comm. Algebra, **30**(2002), 3533–3558.