International Journal of Applied Mathematics

Volume 31 No. 1 2018, 149-169
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v31i1.10

A BIPARTITE GRAPH ASSOCIATED WITH IRREDUCIBLE ELEMENTS AND GROUP OF UNITS IN $\mathbb{Z}_n$

Augustine Musukwa[1 §], Khumbo Kumwenda[2]

[1]Department of Mathematics
University of Trento
Via Della Malpensada 140, Trento TN, ITALY

[1,2]Department of Mathematics
Mzuzu University, MALAWI

Abstract: A nonzero nonunit a of a ring R is called an irreducible element if, for some $b, c \in R$, $a = bc$ implies that either b or c (not both) is a unit. We construct a bipartite graph in which the union of the set of irreducible elements and group of units is a vertex-set and an edge-set is the set of pairs between irreducible elements and their unit factors in the ring of integers modulo n. Many properties of this constructed bipartite graph are studied. We show that this bipartite graph contains components which are isomorphic. We also note that each component of this bipartite graph can be presented in some form which we call star form presentation. Some examples of graphs in star form presentation are provided for illustration purposes. Furthermore, we prove that the girth of this bipartite graph is 8. Most of the results in this paper are arrived at via group action.

AMS Subject Classification: 57M15, 68R10
Key Words: irreducible elements, units, bipartite graph, components, star form presentation

1. Introduction

In this paper we study a bipartite graph associated with irreducible elements

Received: December 27, 2017

§Correspondence author

and group of units in a ring of integers modulo n. We construct a bipartite graph in which we define a vertex-set as the union of the set of irreducible elements and group of units and an edge-set as the set of pairs between irreducible elements and their unit factors. Our interest is to study and establish relationships between the set of irreducible elements and the group of units by using the properties of the graph we are going to construct. Since we are going to work with elements in the ring of integers modulo n, in Section 2, we give an overview of this ring and we also give some results, available in [7], on how to determine the set of irreducible elements and its cardinality. We also present some results, which are crucial to our work, on group action and graph theory.

First part of Section 3 we are going to define some maps which are defined on group of units and show that the set of these maps is a group which acts on group of units. Our interest is to find orbits induced in group of units which are useful in proving some results in this paper. Lastly, we define and study a bipartite graph to an extent of determining some properties such as the components, degrees, connectivity, girth, circumference and others. More interestingly, we show that all components in this bipartite graph are isomorphic.

2. Preliminaries

In this section we give a quick overview of the ring of integers modulo n, group action and graph theory, respectively.

2.1. An overview of the ring of integers modulo n

In this section the reader is referred to [3, 4, 5, 6, 7, 9] if more details are sought. We view the ring of integers modulo n, denoted $\mathbb{Z}_n$, as the set $\{0, 1, ..., n-1\}$ which is called the *complete set of residues modulo* n. $\mathbb{Z}_n$ is a commutative ring with identity 1. For a nonzero $\mathbb{Z}_n$, we use the notation $\mathbb{Z}_n^*$. An element $u \in \mathbb{Z}_n$ is a *unit* if there exists $v \in \mathbb{Z}_n$ such that $uv = 1$; in this case v is called a *multiplicative inverse* of u. All elements which are not units are said to be *nonunits*. The set of all units forms a group called the *group of units*. We denote a group of units by U_n. Any element a is in the group of units of $\mathbb{Z}_n$ if $\gcd(a, n) = 1$, that is, the group of units is the set $\{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}$. *Euler's phi function* states that if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, a prime power factorization, then $\phi(n) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$ and $\phi(nm) = \phi(n)\phi(m)$ if n and m are positive integers such that $\gcd(n, m) = 1$. Note that $\phi(n)$ is the number of units in $\mathbb{Z}_n$.

A nonzero nonunit a of a ring R is called an *irreducible element* if, for some

$b, c \in R$, $a = bc$ implies that either b or c (not both) is a unit. In this paper we denote the set of irreducible elements by $\mathcal{I}_n$. Since in $\mathbb{Z}_n$ elements do not have unique factors then a nonzero nonunit a is irreducible if all its factors satisfy the condition in the definition. For instance, $6 = 1 \cdot 6 = 2 \cdot 3 = 5 \cdot 3 = 8 \cdot 3 = 4 \cdot 6$ in $\mathbb{Z}_9$. So 6 is an irreducible element since all factors satisfy the condition in the definition.

Definition 1. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with p_i distinct primes. We define $\mathcal{P}$ as the set of all p_i with $\alpha_i > 1$, i.e., $\mathcal{P} = \{p_i | p_i \text{ is factor of } n \text{ with } \alpha_i > 1\}$.

To determine and count all irreducible elements in $\mathbb{Z}_n$ we are going to use results in [7].

Theorem 2. *Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where p_i are distinct primes. Then*
(i) $\mathcal{I}_n = \emptyset$, if $\mathcal{P} = \emptyset$,
(ii) $\mathcal{I}_n = \{a \in \mathbb{Z}_n | \gcd(a, n) = p, p \in \mathcal{P}\}$,
(iii) $|\mathcal{I}_n| = \sum_{p \in \mathcal{P}} \frac{\phi(n)}{p}$.

Remark 3. Suppose that $|\mathcal{P}| \neq 0$. Then, by Theorem 2 (ii), it is not hard to observe that the set of irreducible elements can as well be written as $\mathcal{I}_n = \{up | u \in U_n, p \in \mathcal{P}\}$.

2.2. Group Action

Here we give an overview of group action which is a powerful tool in solving different problems in algebra and other branches of mathematics. Here we give some definitions and results which are relevant to what we study in this paper. If more details are sought, the reader is referred to [4, 6].

Let X be an arbitrary set, and let G be a group. A function $f : G \times X \to X$ is called *group action* by G on X if and only if $ex = x$ for all $x \in X$ and $(g_1 g_2)x = g_1(g_2 x)$ for all $g_1, g_2 \in G$ and $x \in X$, where e is the identity of G. If G is acting on X then X is called a *G-set*. If G acts on a set X and $x, y \in X$, then x is said to be *G-equivalent* to y if there exists a $g \in G$ such that $gx = y$. We write $x \sim y$ if two elements are G-equivalent. Let X be a G-set. Then G-equivalence is an equivalence relation on X.

If X is a G-set, then each partition of X associated with G-equivalence is called an *orbit* of X under G. We denote the orbit that contains an element x of X by $\mathcal{O}_x$. Let $\mathbb{O}$ denote the set of all orbits in X under the action of G, i.e,

$\mathbb{O} = \{\mathcal{O}_x | x \in X\}$. Let G be a group acting on a set X and let g be an element of G. Then the *fixed point set* of g in X, denoted by X_g, is the set of all $x \in X$ such that $gx = x$. Note that $X_g \subseteq X$. The number of elements in the fixed point set of an element $g \in G$ is denoted by $|X_g|$ and the number of orbits in X is denoted by $|\mathbb{O}|$. A group acts *faithfully* on a G-set X if the identity is the only element of G that leaves every element of X fixed.

Theorem 4 (Cauchy Frobenius Theorem)**.** *Let G be a finite group acting on a set X and let k denote the number of orbits in X under the action of G. Then*

$$k = \frac{1}{|G|} \sum_{g \in G} |X(g)|.$$

2.3. Some Concepts on Graph Theory

In this section we consider some definitions and results in graph theory and the reader is referred to [1, 2, 8, 11] if more details are sought.

A *simple graph* $G = (V, E)$ consists of a nonempty finite set $V(G)$ of elements called *vertices* and a finite set $E(G)$ of distinct unordered pairs of distinct elements of $V(G)$ called *edges*. We call $V(G)$ the *vertex-set* and $E(G)$ the *edge-set* of G. Each edge has a set of one or two vertices associated to it, which are called its *endpoints* and an edge is said to *join* its endpoints. Two edges of a graph are called *adjacent* if they share a vertex. Similarly, two vertices are called adjacent if they share an edge. An edge and a vertex on that edge are called *incident*. For a given vertex x, the number of all vertices adjacent to it is called *degree of the vertex* x, denoted by $d(x)$. For a graph G, the minimum degree over all vertices is called the *minimum degree of* G, denoted by $\delta(G)$ and the maximum degree over all vertices is called the *maximum degree of* G, denoted by $\Delta(G)$.

If in a simple graph every pair of vertices are adjacent then the graph is called a *complete graph* and is denoted by K_n. A graph with no edges is called an *empty graph*. If $V'(G') \subseteq V(G)$ and $E'(G') \subseteq E(G)$, then $G' = (V', E')$ is a *subgraph* of G. A graph is called *connected* if any two vertices are connected by some path; it is called *disconnected* otherwise. A connected subgraph H is *maximal* provided H is not properly contained in a connected subgraph of G. In other words, H is said to be a *maximal connected subgraph* of G if H is a subgraph of H' and H' is a connected subgraph of G, then $H = H'$. A maximal connected subgraph of G is called a *component* of G. A connected graph in which every vertex has degree 2 is called a *cycle*. A cycle is denoted

by C_n where n is the number of vertices. If n is an even number then C_n is called *even cycle*. If n is odd then C_n is *odd cycle*. The *girth* of a graph is the length of a shortest cycle, denoted by $g(G)$. The *circumference* of a graph G is the maximum length of a cycle in G, denoted by $c(G)$

Two graphs G and G' are *isomorphic* if there is a one-to-one correspondence between the vertices of G, and those of G' such that the number of edges joining any two vertices of G is equal to the number of edges joining the corresponding vertices of G'. A graph $G = (V, E)$ is called *bipartite* if its vertex-set $V(G)$ can be partitioned into two disjoint sets V_1 and V_2 in such a way that every edge connects vertices from different sets. We denoted it as $G = (V_1 \cup V_2, E)$. A *complete bipartite graph* is a bipartite graph in which every vertex from part V_1 is adjacent to every vertex from V_2. If in a complete bipartite graph $|V_1| = r$ and $|V_2| = s$, then the graph itself is denoted by $K_{r,s}$ and the number of edges in $K_{r,s}$ equals rs. The complete bipartite graph $K_{1,n}$ is called a *star*.

3. Main Results

3.1. Group Action on group of units of $\mathbb{Z}_n$

In this section we are interested in determining and enumerating all orbits induced in U_n under the action of a group which is shortly defined. Since in this paper we are concerned with $\mathbb{Z}_n$ which contains irreducible elements, from now on, we assume that $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with some $\alpha_i > 1$ and distinct primes p_i, i.e., we assume that $|\mathcal{P}| \neq 0$. The results we obtain in this section are so useful in proving most of the results in the next section.

Definition 5. Let $\mathcal{P}$ be as defined in Definition 1. Define $A = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{|\mathcal{P}|}}$ where $p_i \in \mathcal{P}$.

Remark 6. It is well known that A is a group called *direct product of groups* under binary operation addition. It is not hard to observe that $|A| = \prod_{p \in \mathcal{P}} p$.

Definition 7. Let $\mathcal{P}$ be as defined in Definition 1. For u in U_n and $s = (s_1, ..., s_{|\mathcal{P}|})$ in A, we define the maps π_s by $\pi_s : u \mapsto \sum_{i=1}^{|\mathcal{P}|} s_i n/p_i + u$ where $p_i \in \mathcal{P}$ and $0 \leq s_i \leq p_i - 1$.

Definition 8. We define the set of maps by $\Theta_A = \{\pi_s | s \in A\}$.

Note that when $|\mathcal{P}| = 1$ then we simply have $A = \mathbb{Z}_p$. In the next lemma we show that the set of maps Θ_A is defined on group of units U_n.

Lemma 9. *π_s is a map defined on U_n.*

Proof. We require that $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with some $\alpha_i > 1$ and p_i distinct primes. Let $u \in U_n$ and suppose that $\pi_s(u) = \bar{u}$ such that $\bar{u} \notin U_n$. This means that $\bar{u}$ must be divisible by some p_i. Without loss of generality, suppose it is divisible by p_1, a factor of n. We can write $\bar{u} = mp_1$ and $\pi_s(u) - u = \sum_{i=1}^{|\mathcal{P}|} s_i n/p_i = tp_1$ where $s = (s_1, ..., s_{|\mathcal{P}|})$ in A, $p_i \in \mathcal{P}$, for some integers m and t. Since $\sum_{i=1}^{|\mathcal{P}|} s_i n/p_i + u = \bar{u}$ implies $u = \bar{u} - \sum_{i=1}^{|\mathcal{P}|} s_i n/p_i = p_1(m - t)$ then $u \notin U_n$ contradicting our earlier assumption that $u \in U_n$. This completes our proof. □

In the next lemma we show that the set of maps Θ_A together with the operation of composition of maps $\circ$ form a group.

Lemma 10. *Θ_A together with the operation of composition of maps $\circ$ is a group.*

Proof. Firstly, we show that Θ_A is closed under the operation of composition of maps $\circ$. Let π_s and $\pi_{s'}$, with $s = (s_1, ..., s_{|\mathcal{P}|})$ and $s' = (s'_1, ..., s'_{|\mathcal{P}|})$ in A, be any two elements of Θ_A. So, for $u \in U_n$,

$$\pi_s \circ \pi_{s'}(u) = \sum_{i=1}^{|\mathcal{P}|} s_i n/p_i + \left(\sum_{i=1}^{|\mathcal{P}|} s'_i n/p_i + u \right) = \sum_{i=1}^{|\mathcal{P}|} (s_i + s'_i) n/p_i + u$$
$$= \sum_{i=1}^{|\mathcal{P}|} s''_i n/p_i + u = \pi_{s''}(u),$$

where $s''_i = (s_i + s_i) \pmod{p_i}$. Thus it is closed under the operation of composition of maps $\circ$.

Secondly, associativity follows from the associativity of mappings. Thirdly, it is clear that $\pi_{(0,...,0)}$ is the identity. Finally, given π_s then it is not hard to see that its inverse $\pi_s^{-1} = \pi_{s^{-1}}$ where s^{-1} is inverse of s in A. □

Theorem 11. *Θ_A acts on U_n.*

Proof. Let $u \in U_n$. It is clear that $\pi_{(0,...,0)}(u) = u$. Let π_s and $\pi_{s'}$, with $s = (s_1, ..., s_{|\mathcal{P}|})$ and $s' = (s'_1, ..., s'_{|\mathcal{P}|})$ in A, be any two elements of Θ_A. Since

$$(\pi_s \circ \pi_{s'})(u) = \pi_{s''}(u) = \sum_{i=1}^{|\mathcal{P}|}(s_i + s'_i)n/p_i + u$$
$$= \sum_{i=1}^{|\mathcal{P}|} s_i n/p_i + \left(\sum_{i=1}^{|\mathcal{P}|}(s'_i)n/p_i + u\right) = \pi_s(\pi_{s'}(u)),$$

where $s'' = (s_1 + s'_1, ..., s_{|\mathcal{P}|} + s'_{|\mathcal{P}|})$, we conclude that Θ_A acts on U_n. □

It worth noting that since it is only the identity in Θ_A that leaves every element in U_n fixed, so Θ_A acts faithfully on U_n.

Definition 12. Let $u \in U_n$. Then the orbit in U_n containing u under the action of Θ_A is $\mathcal{O}_u = \{\pi_s(u) | s \in A\}$.

Lemma 13. *For any $u \in U_n$, $|\mathcal{O}_u| = \prod_{p\in\mathcal{P}} p$.*

Proof. Observe that, for $u \in U_n$, $\pi_s(u) = \pi_{s'}(u)$ implies that $s = s'$. So it should be easy to see that $|\mathcal{O}_u|$ must be equal to $|A|$. In Remark 6 we noted that $|A| = \prod_{p\in\mathcal{P}} p$. □

Let $\mathbb{O}$ denote the set of all orbits in U_n under the action of Θ_A, that is, $\mathbb{O} = \{\mathcal{O}_u : u \in U_n\}$.

Theorem 14. $|\mathbb{O}| = \frac{\phi(n)}{\prod_{p\in\mathcal{P}} p}$.

Proof. We know that $\mathbb{O} = \{\mathcal{O}_u : u \in U\}$. All orbits in U_n are of the same size. Since $|U_n| = \phi(n)$ and by Lemma 13, $|\mathcal{O}_u| = \prod_{p\in\mathcal{P}} p$ so the result follows. □

We consider two examples which illustrate the action of Θ_A on U_n.

Example 15. Consider $\mathbb{Z}_{25}$. So we have $\Theta_A = \{\pi_s | s \in A\}$ where $A = \mathbb{Z}_5$ and $\mathcal{O}_1 = \{1, 6, 11, 16, 21\}$, $\mathcal{O}_2 = \{2, 7, 12, 17, 22\}$, $\mathcal{O}_3 = \{3, 8, 13, 18, 23\}$ and

$\mathcal{O}_4 = \{4, 9, 14, 19, 24\}$. Observe that $\mathbb{O} = \{\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3, \mathcal{O}_4\}$ and $U_{25} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_3 \cup \mathcal{O}_4$.

Example 16. Consider $\mathbb{Z}_{36}$. Then we have $\Theta_A = \{\pi_s | s \in A\}$ where $A = \mathbb{Z}_2 \times \mathbb{Z}_3$. So $\mathcal{O}_1 = \{1, 7, 13, 19, 25, 31\}$ and $\mathcal{O}_5 = \{5, 11, 17, 23, 29, 35\}$. Observe that $\mathbb{O} = \{\mathcal{O}_1, \mathcal{O}_5\}$ and $U_{36} = \mathcal{O}_1 \cup \mathcal{O}_5$.

3.2. A Bipartite Graph Associated with $\mathcal{I}_n$ and U_n

In this section we construct a bipartite graph which is associated with the set of irreducible elements and group of units in the ring $\mathbb{Z}_n$. We begin by defining our new graph in line with the set of irreducible elements in $\mathbb{Z}_n$ presented in Remark 3. Recall that the set of irreducible elements can be written as $\mathcal{I}_n = \{up | u \in U_n, p \in \mathcal{P}\}$.

Definition 17. Let $\mathcal{P}$ be defined as in Definition 1. Define a graph $G = (V, E)$ as follows:

$$V(G) = \mathcal{I}_n \cup U_n,$$

$$[v, w] \in E(G) \Leftrightarrow v \in U_n \text{ and } w = vp, p \in \mathcal{P}.$$

It is clear in our definition that $w \in \mathcal{I}_n$. Recall that if $|\mathcal{P}| = 0$, then $\mathbb{Z}_n$ does not contain irreducible elements (see Theorem 2) and so in such case we simply have an empty graph. We thus consider the ring which contains irreducible elements, i.e., $|\mathcal{P}| \geq 1$. Since this graph is associated with elements in $\mathbb{Z}_n$, we denote this graph by G_n instead of G, $V(G)$ is denoted by V_n and $E(G)$ is denoted by E_n.

Remark 18. Observe that since $|\mathcal{I}_n| = \sum_{p \in \mathcal{P}} \frac{\phi(n)}{p}$ (by Theorem 2) and $|U_n| = \phi(n)$ then $|V_n| = \phi(n)(\sum_{p \in \mathcal{P}} p^{-1} + 1)$.

Example 19. In $\mathbb{Z}_8$, we have $U_8 = \{1, 3, 5, 7\}$, $\mathcal{I}_8 = \{2, 6\}$ and $E_8 = \{[1, 2], [3, 6], [5, 2], [7, 6]\}$. See G_8 in the figure that follows.

Example 20. If we consider $\mathbb{Z}_{36}$, we have $U_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$ and $\mathcal{I}_{36} = \{2, 3, 10, 14, 15, 21, 22, 26, 33, 34\}$. See G_{36} in the figure that follows.

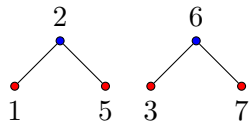

Figure 1: A graph of G_8

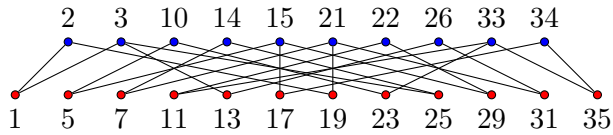

Figure 2: A graph of G_{36}

Example 21. In $\mathbb{Z}_{54}$, we have $\mathcal{I}_{54} = \{3, 15, 21, 33, 39, 51\}$ and $U_{54} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53\}$. We represent G_{54} in the figure as follows.

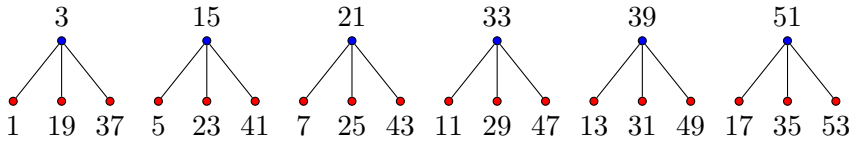

Figure 3: A graph of G_{54}

We next show how the set $\mathcal{I}_n$ is related to orbits induced in U_n under the action of Θ_A and subsequently, use the established relationship in proving some of the results which are of importance in this paper.

Lemma 22. *For $u \in U_n$, if $v \in \mathcal{O}_u$ is a unit factor of $w \in \mathcal{I}_n$ then all unit factors of w are in the same $\mathcal{O}_u$.*

Proof. A typical element in $\mathcal{O}_u$ is of the form $\pi_s(u) = \sum_{i=1}^{|\mathcal{P}|} s_i n/p_i + u$ where $s = (s_1, ..., s_{|\mathcal{P}|})$ in A, $0 \leq s_i \leq p_i - 1$ and $p_i \in \mathcal{P}$ (see Definition 7). Without loss of generality, suppose w is generated by p_1, that is $w = vp_1$ for $v \in \mathcal{O}_u$. We need to show that all other unit factors of w are in $\mathcal{O}_u$. Set $v = v_0$ so that $v_0 = \pi_{(0,s_2,...,s_{|\mathcal{P}|})}(u)$ with fixed $s_2, ..., s_{|\mathcal{P}|}$. We claim that $v_j = \pi_{(j,s_2,...,s_{|\mathcal{P}|})}(u)$,

for all j $(1 \leq j \leq p_1 - 1)$, are also unit factors of w. Observe that for, $j, k \in \{0, ..., p_1 - 1\}$, $v_j p_1 = \pi_{(j,s_2,...,s_{|\mathcal{P}|})}(u)p_1 = (\frac{jn}{p_1} + \frac{s_2 n}{p_2} + \cdots + \frac{s_{|\mathcal{P}|}n}{p_{|\mathcal{P}|}} + u)p_1 = (jn + \frac{s_2 n}{p_2}p_1 + \cdots + \frac{s_{|\mathcal{P}|}n}{p_{|\mathcal{P}|}}p_1 + up_1) \equiv (kn + \frac{s_2 n}{p_2}p_1 + \cdots + \frac{s_{|\mathcal{P}|}n}{p_{|\mathcal{P}|}}p_1 + up_1) = (\frac{kn}{p_1} + \frac{s_2 n}{p_2} + \cdots + \frac{s_{|\mathcal{P}|}n}{p_{|\mathcal{P}|}} + u)p_1 = \pi_{(k,s_2,...,s_{|\mathcal{P}|})}(u)p_1 = v_k p_1 \pmod{n}$. That is $w = v_j p_1$, for all j $(1 \leq j \leq p_1 - 1)$. It must be not hard to see that these are the only factors in $\mathcal{O}_u$ which are factors of w.

We claim that w does not contain any unit factor in other orbits. For sake of contradiction, suppose w has another unit factor $v_l' = \pi_{(l,z_2,...,z_{|\mathcal{P}|})}(u')$ in $\mathcal{O}_{u'}$ where $u' \in U_n$ and $u' \notin \mathcal{O}_u$. That is $v_l' \notin \mathcal{O}_u$. It means that, for any $v_j \in \mathcal{O}_u$, a unit factor of w we have $v_l' p_1 \equiv v_j p_1 \pmod{n}$. This implies that $v_l' \equiv v_j \pmod{n/p_1}$ from which we get that $v_l' = mn/p_1 + v_j = mn/p_1 + \pi_{(j,s_2,...,s_{|\mathcal{P}|})}(u) = \pi_{(m+j,s_2,...,s_{|\mathcal{P}|})}(u) \in \mathcal{O}_u$ contrary to our assumption that $v_l' \notin \mathcal{O}_u$. □

In the next lemma we show that if we let $s_1 = \cdots = s_{i-1} = s_{i+1} = \cdots = s_{|\mathcal{P}|} = 0$ and $0 \leq s_i \leq p_i - 1$ so that we have $\Theta_{A'} = \{\pi_{s'} | s' = (0, ..., 0, s_i, 0, ..., 0), s_i \in A'\}$, where $A' = \mathbb{Z}_{p_i}$ and $p_i \in \mathcal{P}$, then further acting $\Theta_{A'}$ on $\mathcal{O}_u$ other orbits are induced. We will simply write $\Theta_{A'} = \{\pi_{s'} | s' \in A'\}$ where $A' = \mathbb{Z}_p$. For $u' \in \mathcal{O}_u$, we denote the orbit containing u' under the action of $\Theta_{A'}$ on $\mathcal{O}_u$ by $\mathcal{O}_{uu'} = \{s_i n/p_i + u' | 0 \leq s_i \leq p_1 - 1\}$. We also show that elements in each $\mathcal{O}_{uu'}$ are all unit factors of one irreducible element generated by p_i.

Lemma 23. *Let $\Theta_{A'} = \{\pi_{s_i'} | s_i' \in A'\}$ where $A' = \mathbb{Z}_{p_i}$ and $p_i \in \mathcal{P}$. Then, for $u \in U_n$, $\Theta_{A'}$ acts on $\mathcal{O}_u$ and elements in each orbit are all unit factors of one irreducible element generated by p_i. Furthermore, these are the only unit factors of this irreducible element.*

Proof. It is not hard to see that $\Theta_{A'}$ is a subgroup of Θ_A. Also note that $\Theta_{A'}$ acts on $\mathcal{O}_u$ since, for all $u' \in \mathcal{O}_u$, $\pi_0(u') = u'$ and $\pi_s(\pi_{s'}(u')) = (\pi_s \pi_{s'})(u)$, for all $\pi_s, \pi_{s'} \in \Theta_{A'}$. Let the orbit containing $u' \in \mathcal{O}_u$ be denoted by $\mathcal{O}_{uu'} = \{s_i n/p_i + u' | 0 \leq s_i \leq p_i - 1\}$. We show that if an irreducible element generated by p_i has a factor in $\mathcal{O}_{uu'}$ then all elements in $\mathcal{O}_{uu'}$ are also factors of it.

Suppose that $v \in \mathcal{O}_{uu'}$ such that $w = vp_i$. Write $v = kn/p_i + u'$ for some $k \in \{0, ...p_i - 1\}$. For any v' in $\mathcal{O}_{uu'}$, we have $v' = gn/p_i + u'$ where $g \in \{0, ..., p_i - 1\}$. So $v'p_i = (gn/p_i + u')p_i = gn + u'p_i \equiv kn + u'p_i = (kn/p_i + u')p_i = vp_i = w \pmod{n}$ implies that all elements in $\mathcal{O}_{uu'}$ are factors of w.

We claim that $O_{uu'}$ is the only orbit with factors of w. For sake of contradiction, suppose that $v'' \in \mathcal{O}_{uu''}$, where u'' is in $\mathcal{O}_u$ but not in $\mathcal{O}_{uu'}$, is also a factor

of w. So let $\mathcal{O}_{uu''} = \{s_i n/p_i + u'' | 0 \leq s_i \leq p_i - 1\}$ and write $v'' = tn/p_i + u''$ for some $t \in \{0, .., p_i - 1\}$. So $v''p_i \equiv vp_i = w \pmod{n} \Rightarrow (tn/p_i + u'')p_i \equiv (kn/p_i + u')p_i \pmod{n} \Rightarrow (tn/p_i + u'')p_i \equiv kn + u'p_i \pmod{n} \Rightarrow (tn/p_i + u'')p_i \equiv u'p_i \pmod{n} \Rightarrow tn/p_i + u'' \equiv u' \pmod{n/p_i} \Rightarrow tn/p_i + u'' = hn/p_i + u'$. But $tn/p_i + u'' = hn/p_i + u'$ implies an element in $\mathcal{O}_{uu'}$ is equal to an element in $\mathcal{O}_{uu''}$ which is a contradiction since $\mathcal{O}_{uu'}$ and $\mathcal{O}_{uu''}$ two different orbits in $\mathcal{O}_u$ under the action of $\Theta_{A'}$. □

Remark 24. Suppose the orbit containing $u' \in \mathcal{O}_u$ is $\mathcal{O}_{uu'} = \{s_i n/p_i + u' | 0 \leq s_i \leq p_i - 1\}$ under the action of $\Theta_{A'}$, with $A' = \mathbb{Z}_{p_i}$. Then

(i) it is easily observed that $|\mathcal{O}_{uu'}| = p_i$ from which we conclude that there are
$|\mathcal{O}_u|/|\mathcal{O}_{uu'}| = p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|\mathcal{P}|}$ orbits in $\mathcal{O}_u$.

(ii) by (i) and Lemma 23, it implies that there are $p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|\mathcal{P}|}$ irreducible elements which are generated by p_i and have their unit factors in $\mathcal{O}_u$.

(iii) it follows from (ii) that if $|\mathcal{P}| > 1$ then there are $\sum_{i=1}^{|\mathcal{P}|} \sigma_i$, where $\sigma_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|\mathcal{P}|}$, irreducible elements which have factors in $\mathcal{O}_u$ and 1 if $|\mathcal{P}| = 1$.

Lemma 25. *Let $A' = \mathbb{Z}_{p_i}$ and $A'' = \mathbb{Z}_{p_j}$, for $i \neq j$. Then all orbits induced by $\Theta_{A'}$ and $\Theta_{A''}$ in $\mathcal{O}_u$ where $u \in U_n$ contain at most 1 element in common.*

Proof. Suppose some orbits induced in $\mathcal{O}_u$ by the actions of $\Theta_{A'}$ and $\Theta_{A''}$ contain more than one element in common. Suppose u' is one of the elements in such orbits. So we have $\{s_i n/p_i + u' | 0 \leq s_i \leq p_i - 1\}$ as an orbit induced by $\Theta_{A'}$ and $\{s_j n/p_j + u' | 0 \leq s_j \leq p_j - 1\}$ as an orbit induced by $\Theta_{A''}$. We show that u' must be the only element in common. Suppose $s_i n/p_i + u' = s_j n/p_j + u'$, for some $s_i \in \{0, ..., p_i - 1\}$ and $s_j \in \{0, ..., p_j - 1\}$. If $s_i = s_j = 0$ we obviously have u' which we already know that is present in both orbits. Suppose s_i and s_j are both nonzero. Since $s_i n/p_i + u' = s_j n/p_j + u'$ implies $s_i p_j = s_j p_i$ then p_j divides either s_j or p_i and p_i divides either s_i or p_j which is a contradiction as $p_i \neq p_j$, $s_i < p_i$ and $s_j < p_j$. □

Theorem 26. *G_n contains $\frac{\phi(n)}{\prod_{p \in \mathcal{P}} p}$ isomorphic components.*

Proof. By Lemma 22, G_n must contain components since if an irreducible

element has a unit factor in $\mathcal{O}_u$ where $u \in U_n$ then all factors for that irreducible element are also in the same orbit. We are assured that the component associated with $\mathcal{O}_u$ is connected because all elements in an orbit induced under the action of $\Theta_{A'}$ on $\mathcal{O}_u$ occur as elements in other orbits induced under the actions of $\Theta_{A''}$ (we know that $A' = \mathbb{Z}_{p_i}$ and $A' = \mathbb{Z}_{p_i}$ with $i \neq j$, see Lemma 25).

Since all orbits $\mathcal{O}_u$ in U_n when acted upon by Θ_A have the same structure then all components obtained from these orbits must be isomorphic. Since, by Lemma 13, $|\mathcal{O}_u| = \prod_{p\in\mathcal{P}} p$ then we conclude that there are $\phi(n)/\prod_{p\in\mathcal{P}} p$ components. □

From Theorem 26 we remark that the graph G_n is a disconnected graph with isomorphic components. Since all the components in G_n are isomorphic then the whole graph can be described by a single component. For this reason, in the rest of this section we mostly use a component to study properties of G_n.

Lemma 27. *No two irreducible elements in $\mathcal{I}_n$ generated by the same prime are adjacent to a common unit in U_n.*

Proof. This is a direct consequence of Lemma 23. Also by Remark 3, any irreducible element generated by p can be written in the form up where $u \in U_n$ and so with this presentation it must be impossible for any two elements generated p to be adjacent to a common unit in U_n. □

Proposition 28. *In G_n, $d(v) = |\mathcal{P}|$, for all $v \in U_n$ and $d(w) = p$ if $w = v'p$ for some $v' \in U_n$ and $p \in \mathcal{P}$.*

Proof. By lemma 27, no two irreducible element generated by the same prime are adjacent to a common unit factor. But irreducible elements generated by different primes can have common unit factor. So each unit in U_n must be adjacent to $|\mathcal{P}|$ irreducible element.

By Remark 24, if the orbit containing $u' \in \mathcal{O}_u$ is $\mathcal{O}_{uu'} = \{s_i n/p_i + u' | 0 \leq s_i \leq p_i - 1\}$ under the action of $\Theta_{A'}$ then we have $|\mathcal{O}_{uu'}| = p_i$. By Lemma 23, we conclude that only elements in $\mathcal{O}_{uu'}$ are adjacent to one irreducible element generated by p_i. So if such irreducible element is w then the $d(w) = p_i$. □

Remark 29. Since, by Proposition 28, any vertex in $\mathcal{I}_n$ has degree p where $p \in \mathcal{P}$ and any vertex in U_n has degree $|\mathcal{P}|$ then $\delta(G_n) = \min_{p\in\mathcal{P}}\{p, |\mathcal{P}|\}$

and $\Delta(G_n) = \max_{p \in \mathcal{P}}\{p, |\mathcal{P}|\}$.

Proposition 30. *The total sum of degrees for all vertices in G_n is $2\phi(n)|\mathcal{P}|$.*

Proof. Since, by Proposition 28, the degree for each vertex in U_n is $|\mathcal{P}|$ and there are $\phi(n)$ elements in U_n then the sum of degrees on unit vertices is $\phi(n)|\mathcal{P}|$. Again all irreducible elements generated by prime p have degree p. Since there are $\frac{\phi(n)}{p}$ irreducible elements generated by p then they contribute $\phi(n)$ degrees. Since there are $|\mathcal{P}|$ primes which generate $\mathcal{I}_n$ then the sum of degrees on irreducible vertices is $\phi(n)|\mathcal{P}|$. Thus G_n has a total of $2\phi(n)|\mathcal{P}|$ degrees.

□

Corollary 31. *The total number of edges in G_n is $\phi(n)|\mathcal{P}|$.*

Proof. There are $\phi(n)$ elements in U_n. By Lemma 28, each unit vertex has degree $|\mathcal{P}|$. Hence G_n has $\phi(n)|\mathcal{P}|$ edges. □

Proposition 32. *A component of G_n is a union of copies of the star $K_{1,|\mathcal{P}|}$.*

Proof. By Proposition 28, the degree of any unit in U_n is $|\mathcal{P}|$ so the results follows. □

Remark 33. By Proposition 28, the degree of an irreducible element generated by p is p so Proposition 32 is also equivalent to saying that each component is a union of copies of the stars $K_{1,p}$ where $p \in \mathcal{P}$.

Proposition 34. *If $\mathcal{P} = \{p\}$ then each component of G_n is $K_{1,p}$.*

Proof. Suppose $\mathcal{P} = \{p\}$. Then all irreducible elements in $\mathcal{I}_n$ are generated by the same prime p. Hence by Lemma 27 and Proposition 28, each irreducible element is adjacent to p units and these units are not adjacent to any other irreducible element. Thus the result follows. □

Proposition 35. *G_n contains a cycle if and only if $|\mathcal{P}| > 1$.*

Proof. Suppose that G_n contains a cycle. It implies that some vertices in both $\mathcal{I}_n$ and U_n have at least degree 2. $|\mathcal{P}| = 0$ implies that G_n is an empty graph. If $|\mathcal{P}| = 1$, G_n does not contain a cycle since in this case all unit vertices have degree 1. Since if $|\mathcal{P}| > 1$ all vertices in both $\mathcal{I}_n$ and U_n contain at least degree 2 then G_n must contain a cycle. The converse is obvious. □

Theorem 36. *Let $\mathcal{P} = \{p_1, p_2\}$. Then between any two irreducible elements generated by prime $p \in \mathcal{P}$ there are p paths of length 4 in each component of G_n. Furthermore, there are $\frac{p(p-1)}{2}$ cycles of length 8 that pass through any such two irreducible elements.*

Proof. Suppose $\mathcal{P} = \{p_1, p_2\}$. By Theorem 2, $\mathcal{I}_n$ is generated by p_1 and p_2. Since $|\mathcal{P}| = 2 > 1$ then, by Theorem 35, G_n contains cycles. By Remark 3, recall that an irreducible element generated by p can be written as up, for some $u \in U_n$. Consider the maps $\pi_{(s,t)}$ with $(s,t) \in A = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$ as defined in Definition 7. Denote by w_s all irreducible elements generated by p_2 and w'_t those generated by p_1 where $0 \leq s \leq p_1 - 1$ and $0 \leq t \leq p_2 - 1$. For $i \neq j$, $\pi_{(i,t)}(u)p_1 = (\frac{in}{p_1} + \frac{tn}{p_2} + u)p_1 = in + \frac{p_1 tn}{p_2} + up_1 \equiv jn + \frac{p_1 tn}{p_2} + up_1 = (\frac{jn}{p_1} + \frac{tn}{p_2} + u)p_1 = \pi_{(j,t)}(u)p_1 \pmod{n}$ implies that if w'_t is adjacent to $\pi_{(i,t)}(u)$ then it is also adjacent to $\pi_{(j,t)}(u)$. Similarly, for $g \neq f$, if w_s is adjacent $\pi_{(s,g)}(u)$ then it is also adjacent to $\pi_{(s,f)}(u)$. So it is immediate that between any two irreducible elements generated by p_2 (this is also true with those generated by p_1) we have the paths below:

$$w_i, \pi_{(i,t)}(u), w'_t, \pi_{(j,t)}(u), w_j$$

for all $0 \leq i < j \leq p_1 - 1$ and $0 \leq t \leq p_2 - 1$. We represent these paths in Figure 4 below.

It is not hard to observe, in Figure 4, that between any two irreducible elements generated by p_2 there are p_2 paths of length 4, each passing through some w'_t where $0 \leq t \leq p_2 - 1$ and similarly, between any two irreducible elements generated by p_1 there are p_1 paths of length 4. Thus it is immediate that any two of the p_j paths of length 4 between any two irreducible elements generated by p_j form a cycle of length 8 which pass through such two irreducible elements. So there are $\binom{p_j}{2} = \frac{p_j(p_j-1)}{2}$ such cycles. □

Remark 37. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with some $\alpha_i > 1$ and p_i distinct primes. If you consider the maps $\pi_{(s_1,\ldots,s_{|\mathcal{P}|})} : u \mapsto \sum_{j=1}^{|\mathcal{P}|} \frac{s_j n}{p_j} + u$, where $p_j \in \mathcal{P}$ and $0 \leq s_j \leq p_j - 1$, and (without loss) let $s_i, s_j \neq 0$ and all others equal 0 so that

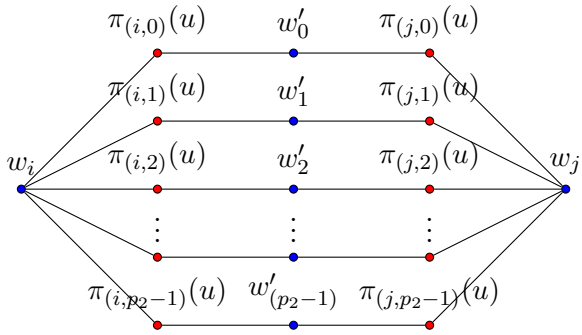

Figure 4: Paths between w_i and w_j in a component of G_n

we have $\pi_{(s_i,s_j)}$ then arguing by Theorem 36 one can easily find two irreducible elements generated by same prime p_j in a component of G_n with p_j paths of length 4 between them and $\frac{p_j(p_j-1)}{2}$ cycles of length 8 that pass through them.

Theorem 36 and Remark 37 suggest that any component of G_n can be presented in some form. From Figure 4 we observe that any component of G_n can be presented in a form which we will call *star form presentation* by putting all elements generated by any prime in the center and all others around them. If the irreducible elements put in the center are those that are generated by p then our graph in star form presentation takes the shape of $K_{1,p}$ since the degree of each such irreducible elements is p by Proposition 28. To illustrate this idea, we provide three examples and in each we present a component of G_n in a star form presentation. Since if $|\mathcal{P}| = 1$, by Proposition 34, each component is a star then we already have a star form presentation. This can also be observed in Examples 19 and 21. We therefore consider examples in which we have $|\mathcal{P}| > 1$. In the examples to be given, the blue vertices are for irreducible elements and the red vertices are for units. Each irreducible element can be identified by its degree since by Proposition 28 we know that any irreducible element generated by p has a degree p.

Example 38. Let $n = 3^\alpha 5^\beta$ or $n = 3^\alpha 5^\beta \prod_{i=1}^{k} p_i$ with $\alpha, \beta > 1$, that is, $\mathcal{P} = \{3, 5\}$. G_n contains $\frac{\phi(n)}{15}$ isomorphic components. Figure 5 and Figure 6 display two different star form presentations of a component of G_n. Note that in Figure 5 all 3 units in each "branch" form some orbit in $\mathcal{O}_u$ under the action of $\Theta_{A'}$ with $A' = \mathbb{Z}_3$ and in Figure 6 all 5 units in each "branch" form some

orbit under the action of $\Theta_{A''}$ with $A'' = \mathbb{Z}_5$.

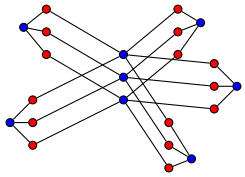

Figure 5: A component of G_n irreducible elements generated by 5 in center

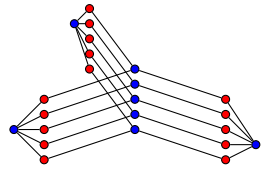

Figure 6: A component of G_n with irreducible elements generated by 3 in center

Example 39. Let $n = 5^\alpha 7^\beta$ or $n = 5^\alpha 7^\beta \prod_{i=1}^{k} p_i$ with $\alpha, \beta > 1$, that is, $\mathcal{P} = \{5, 7\}$. G_n contains $\frac{\phi(n)}{35}$ isomorphic components. Figure 7 shows a component in a star form presentation with irreducible elements generated by 5 put in the center. Note that in Figure 7 all 7 units in each "branch" form some orbit in $\mathcal{O}_u$ under the action of $\Theta_{A'}$ with $A' = \mathbb{Z}_7$. We could also put irreducible elements generated by 7 in the center; in this case 7 "branches" are expected and in each "branch" we expect 5 units from some orbit in $\mathcal{O}_u$ under the action of $\Theta_{A''}$ with $A'' = \mathbb{Z}_5$.

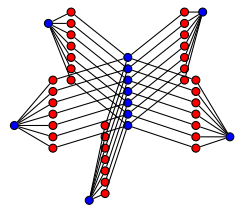

Figure 7: A component of G_n in star form presentation with irreducible elements generated by 5 in center

Example 40. We consider a component of G_n when $n = 3^\lambda 5^\alpha 7^\beta$ or $n = 3^\lambda 5^\alpha 7^\beta \prod_{i=1}^{k} p_i$ with $\lambda, \alpha, \beta > 1$ and there are $\frac{\phi(n)}{105}$ isomorphic such components. We observe that $\mathcal{P} = \{3, 5, 7\}$ which implies that all irreducible elements are generated by 3,5 and 7. In our star form presentation in Figure 8 all irreducible elements generated by 3 are put in center. Note that we could also put all

irreducible elements generated by 5 or 7 in the center.

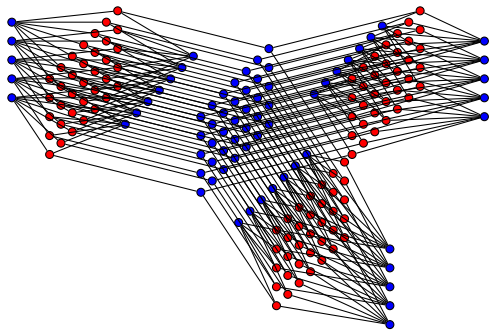

Figure 8: A component of G_n with irreducible elements generated by 3 put in the center

We point out few things in the construction of Figure 8. Red vertices are units all from $\mathcal{O}_u$. All unit vertices in each column form an orbit in $\mathcal{O}_u$ under the action of $\Theta_{A'}$ where $A' = \mathbb{Z}_5$ and in this case there $21 = 3 \times 7$ orbits. Also all unit vertices in each row form an orbit in $\mathcal{O}_u$ under the action of $\Theta_{A''}$ where $A'' = \mathbb{Z}_7$ and there are $15 = 3 \times 5$ orbits. Both cases satisfy Remark 24 (i).

As it was observed in Lemma 25, orbits induced by $\Theta_{A'}$ and $\Theta_{A''}$ have at most one element in common and this element is in the intersection of a row and a column. And the star form presentation is always possible because of the just said fact about orbits in each $\mathcal{O}_u$. For $|\mathcal{P}| > 3$, the star form presentation is more funnier and complex. For instance, if $|\mathcal{P}| = 4$ then unit vertices in each "branch" have to be arranged in 3 dimensional.

Theorem 41. *If $|\mathcal{P}| > 1$ then $g(G_n) = 8$.*

Proof. Suppose that $|\mathcal{P}| > 1$. So by Proposition 35 we are assured that there are cycles. In bipartite graphs cycles always have even length so we expect an even girth. It is clear from Definition 17 that G_n is a simple graph so we cannot have cycles of length 2. We claim that cycles of length 4 and 6 are not possible. Suppose we have a cycle of length 4 as in Figure 9 where r_1, r_2 are two different irreducible elements and u_1, u_2 are two different unit vertices.

Observe that r_1 and r_2 are not generated by the same prime since that would contradict Lemma 27. Without loss of generality, assume that r_1 and r_2 are generated by p_1 and p_2, respectively. Since both r_1 and r_2 are adjacent to u_1 and u_2 then we have $r_1 = u_1 p_1 \equiv u_2 p_1 \pmod{n}$ and $r_2 = u_1 p_2 \equiv u_2 p_2$

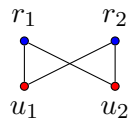

Figure 9: A cycle of length 4

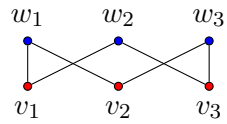

Figure 10: A cycle of length 6

(mod n) which imply that $u_1 \equiv u_2 \pmod{n/p_1}$ and $u_1 \equiv u_2 \pmod{n/p_2}$ from which obtain $u_1 = u_2 + ns_1/p_1$ and $u_1 = u_2 + ns_2/p_2$ for some $s_1 \in \{0, ..., p_1 - 1\}$ and $s_2 \in \{0, ..., p_2 - 1\}$. It follows that $u_1 = u_2 + ns_1/p_1 = u_2 + ns_2/p_2$ from which we obtain $s_1p_2 = s_2p_1$. So it implies that p_1 divides s_1 or p_2 and p_2 divides s_2 or p_1 which is only possible if $s_1 = s_2 = 0$, meaning that $u_1 = u_2$ contrary to our assumption that they are different.

Next we suppose that we have a cycle of length 6 as in Figure 10 where w_1, w_2, w_3 are three different irreducible elements and v_1, v_2, v_3 are three different unit vertices. All the three irreducible elements must be generated by different primes otherwise it would mean that some irreducible elements generated by the same prime have a common unit factor contrary to Lemma 27. So we further suppose that $|\mathcal{P}| > 2$ otherwise there is nothing to prove. Without loss of generality, assume that w_1, w_2 and w_3 are generated by p_1, p_2 and p_3, respectively. That is $w_1 = v_1p_1 \equiv v_2p_1 \pmod{n}$, $w_2 = v_1p_2 \equiv v_3p_2 \pmod{n}$ and $w_3 = v_2p_1 \equiv v_3p_1 \pmod{n}$. We note that $w_1 = v_1p_1 \equiv v_2p_1 \pmod{n} \Rightarrow v_1 \equiv v_2 \pmod{n/p_1} \Rightarrow v_1 = v_2 + ns_1/p_1$ where $0 \leq s_1 \leq p_1 - 1$. Similarly, $w_2 = v_1p_2 \equiv v_3p_2 \pmod{n}$ implies that $v_1 = v_3 + ns_2/p_2$ where $0 \leq s_2 \leq p_2 - 1$ and $w_3 = v_2p_1 \equiv v_3p_1 \pmod{n}$ implies that $v_2 = v_3 + ns_3/p_2$ where $0 \leq s_3 \leq p_3 - 1$. So we have the equations:

$$\begin{array}{lcllll} v_1 & = & v_2 & + & ns_1/p_1 & \cdots \text{ (i)} \\ v_1 & = & v_3 & + & ns_2/p_2 & \cdots \text{ (ii)} \\ v_2 & = & v_3 & + & ns_3/p_3 & \cdots \text{ (iii)} \end{array}$$

By (i) and (ii) we obtain:

$$v_2 + ns_1/p_1 \quad = \quad v_3 + ns_2/p_2 \quad \cdots \text{ (iv)}$$

Substituting (iii) in (iv) we obtain:

$$v_3 + ns_3/p_3 \quad + ns_1/p_1 \quad = \quad v_3 + ns_2/p_2 \quad \cdots \text{ (v)}$$

From (v) we have:

$$s_3p_1p_2 + s_1p_2p_3 \quad = \quad s_2p_1p_3 \quad \cdots \text{ (vi)}$$

It follows that p_1 must divide left side of Equation (vi). But $p_1|(s_3p_1p_2 + s_1p_2p_3) \Rightarrow p_1|s_1p_2p_3$. Since $0 \leq s_1 \leq p_1 - 1$ so the only possibility is that $s_1 = 0$ and from Equation (i) it implies that $v_1 = v_2$ contrary to our assumption v_1, v_2 and v_3 are different. Thus a cycle of length 6 is also impossible.

By Theorem 36 and Remark 37, if $|\mathcal{P}| > 1$ there always exist a cycle of length 8 which passes through some two irreducible elements generated by the same prime. Hence we conclude that $g(G_n) = 8$. □

In Examples 38, 39 and 40 one can easily check that $g(G_n) = 8$.

In the next proposition we discuss about the circumference of G_n when $|\mathcal{P}| = 2$.

Proposition 42. *Let $\mathcal{P} = \{p_1, p_2\}$. If $p_1 < p_2$ then $c(G_n) = 4p_1$.*

Proof. By Remark 24 (ii), we conclude that in each component there are p_1 irreducible elements generated by p_2 and p_2 irreducible elements generated by p_1. Since $p_1 < p_2$ then a possible longest cycle must contain all the p_1 irreducible elements generated by p_2 and also p_1 irreducible elements generated by p_1 otherwise if a cycle contains more than p_1 irreducible elements generated by p_1 it would mean that some two irreducible elements generated by p_1 have a common unit factor contrary to Lemma 27. Denote by w_s all irreducible elements generated by p_2 and by w'_t those generated by p_1 where $0 \leq s \leq p_1 - 1$ and $0 \leq t \leq p_2 - 1$. As in Theorem 36 , for $i \neq j$, $\pi_{(i,t)}(u)p_1 = (\frac{in}{p_1} + \frac{tn}{p_2} + u)p_1 = in + \frac{p_1tn}{p_2} + up_1 \equiv jn + \frac{p_1tn}{p_2} + up_1 = (\frac{jn}{p_1} + \frac{tn}{p_2} + u)p_1 = \pi_{(j,t)}(u)p_1 \pmod{n}$ implies that if w'_t is adjacent to $\pi_{(i,t)}(u)$ then it is also adjacent to $\pi_{(j,t)}(u)$. Similarly, for $l \neq k$, if w_s is adjacent $\pi_{(s,l)}(u)$ then it is also adjacent to $\pi_{(s,k)}(u)$. Hence the cycle that follows is always possible:

$$\begin{aligned} &w_0, \pi_{(0,0)}(u), w'_0, \pi_{(1,0)}(u), w_1, \pi_{(1,1)}(u), w'_2, \pi_{(2,1)}(u), \\ &w_2, \pi_{(2,2)}(u), w'_2, \pi_{(3,2)}(u), w_3, \pi_{(3,3)}(u), w'_3, \pi_{(4,3)}(u), \\ &w_4, \cdots, w_{(p_1-1)}, \pi_{(p_1-1,p_1-1)}(u), w'_{(p_1-1)}, \pi_{(p-1,0)}(u), w_0. \end{aligned} \qquad (*)$$

We notice that all p_1 irreducible elements generated by p_2, highlighted by red, have been used in the cycle and also p_1 of p_2 irreducible elements generated by p_1 have been used in the cycle. That is the cycle include the same number

of irreducible elements generated by p_1 and p_2. If there exist a cycle which is longer than the cycle in $(*)$ then it means that it includes more irreducible elements generated by p_1 and that would mean some two irreducible elements generated by p_1 are adjacent to one unit contrary to Lemma (27). So the cycle in $(*)$ must be a longest cycle in G_n.

Observe that between any two consecutive irreducible elements generated by the same prime in the cycle in $(*)$ there there is a path of length 4 so its clear that the length of this cycle must be $4p_1$. So we conclude that the circumference of G_n is $4p_1$. □

It can easily be checked that $c(G_n)$ of graphs in Examples 38 and 39 satisfy Proposition 42.

Lastly, we provide a conjecture about the circumference of G_n which was arrived at by using an idea of star form presentation and also by using some insights from Theorem 36, Remarks 24 (ii) and 37 and Proposition 42.

Conjecture 43. *Let* $|\mathcal{P}| > 1$. *Then* $c(G_n) = \frac{4\prod_{p\in\mathcal{P}} p}{\max(\mathcal{P})}$.

4. Conclusion

In this paper we constructed a bipartite graph with the union of the set of irreducible elements and group of units as a vertex-set and the set of pairs between irreducible elements and their unit factors as an edge-set in the ring of integers modulo n. Many properties of this graph were studied. We proved that this bipartite graph is not connected but contains isomorphic components, each of which is a union of copies of the star $K_{1,|\mathcal{P}|}$ where $\mathcal{P}$ is a set which contains all prime factors of n whose powers are greater than 1. For a given value of n, we determined when this graph has cycles or not. Furthermore, we proved that the girth of this bipartite graph is 8.

References

[1] A. Benjamin, G. Chartrand, P. Zhang, *The Fascinating World of Graph Theory*, Princeton University Press, Oxford (2015).

[2] G. Chartrand, P. Zhang, *Chromatic Graph Theory*, Chapman and Hall/CRC, London (2009).

[3] J. Coykendall, D.E. Dobbs, and B. Mullins, Exploring irreducible elements: An abstract algebra project, *Alabama Journal of Mathematics (Education)*, Fall 2002.

[4] J.A. Gallian, *Contemporary Abstract Algebra*, 7th Edition, Richard Stratton, United Kingdom (2010).

[5] G.A. Jones, J.A. Jones, *Elementary Number Theory*, Springer Science, United Kingdom (2005).

[6] T.W. Judson, *Abstract Algebra, Theory and Application*, Cambridge University Press, London (2009).

[7] A. Musukwa, K. Kumwenda, A Special Subring Associated with Irreducible Elements in $\mathbb{Z}_n$, *MAYFEB Journal of Mathematics*, **2** (2017), 1-7.

[8] M. Pranjali, M. Acharya, Graphs Associated with Finite Zero Ring, *Gen. Math. Notes*, **24**, No 2 (2014), 53-69.

[9] B. Steinberg, *Representation Theory of Finite Group: An Introductory Approach*, Springer Science, New York (2012)

[10] J.J. Tattersall, *Elementary Number Theory in Nine Chapters*, 2nd Edition, Cambridge University Press, New York (2005).

[11] V.I. Voloshin, *Introduction to Graph Theory*, Nova Science, New York (2009).