A Graph Associated with Group of Units and Irreducible Elements in $\mathbb{Z}_n$

Augustine Musukwa
Department of Mathematics,
Mzuzu University, P/Bag 201,
Luwinga, Mzuzu 2, Malawi
augulela@yahoo.com

Abstract: A nonzero nonunit $a$ in the ring $\mathbb{Z}_n$ is called an irreducible element if $a = bc$ implies that either $b$ or $c$ (not both) is a unit in $\mathbb{Z}_n$. We define a graph in which the group of units in $\mathbb{Z}_n$ is a vertex-set and the set of all pairs of units which are both factors of an irreducible element is an edge-set. We study this graph to an extent of determining some of its properties such as the girth, circumference, cliques, cycles and connectivity. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with some $\alpha_i > 1$ and define $P = \{p_i | p_i$ is a prime factor of $n$ with $\alpha_i > 1\}$. We prove that this graph is $\sum_{p \in P} (p - 1)$-regular and contains isomorphic components, each of which is a union of $K_p$ where $p \in P$. More importantly, we use this graph to conclude that the distribution of units in factors of irreducible elements of $\mathbb{Z}_n$ is the same if $|P| = 1$ and different if $|P| > 1$.

Keywords: clique, circumference, component, girth, irreducible element, regular graph

MSC 2010: 57M15, 97K30

1 Introduction

Through out this paper we study a graph which involves elements of the ring of integers modulo $n$, usually denoted by $\mathbb{Z}_n$. We associate this graph with the group of units and irreducible elements $\mathbb{Z}_n$. Units in the factors of irreducible elements seems to have a particular distribution which could be of interest. Consequently, we define a graph in such a way that the group of units is a vertex-set and the set of all pairs of units which are both factors of an irreducible element is an edge-set. This graph has been proposed with an aim of establishing the distribution of units in factors of irreducible elements.

We study this graph via group action. We 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 in the ring $\mathbb{Z}_n$. Our interest is to find the orbits induced in group of units under the action of the group of maps. We show that there is an important relationship between the orbits induced and the graph we are studying. This relationship plays a big role in proving our results. We study this graph to an extent of determining some of its properties such as the girth, circumference, cliques, components, cycles and connectivity.

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 The ring of integers modulo $n$

In the ring of integers modulo $n$, denoted $\mathbb{Z}_n$, we consider some concepts and results which are useful in this paper and we refer the reader to [3, 4, 5, 6, 7, 8] if more details are sought. We view $\mathbb{Z}_n$ as the set $\{0, 1, \ldots, n-1\}$ 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 under multiplication 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 $a$ in the ring $\mathbb{Z}_n$ is called an irreducible element if $a = bc$ implies that either $b$ or $c$ (not both) is a unit in $\mathbb{Z}_n$. 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 is irreducible if all the factors of $a$ satisfy the condition in the definition. For instance, $2 = 1 \cdot 2 = 3 \cdot 2$ in $\mathbb{Z}_4$. So 2 is an irreducible element since all factors satisfy the condition in the definition of an irreducible element.

Definition 2.1.1. 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 2.1.2. 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) $|\mathcal{I}_n| = \sum_{p \in \mathcal{P}} \phi(n)/p$.

Remark 2.1.3. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ with some $\alpha_i > 1$. Then, by Theorem 2.1.2 (ii), it is not hard to observe that the set of irreducible elements can as well be written as $\mathcal{I}_n = \{up_i | u \in U_n, p_i \in \mathcal{P}\}$.

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 $(g_1g_2)x = g_1(g_2x)$ 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 $O_x$. Let $\mathcal{O}$ denote the set of all orbits in $X$ under the action of $G$, i.e., $\mathcal{O} = \{O_x \mid x \in X\}$. 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 $|\mathcal{O}|$. 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 2.2.1 (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 in graph theory

Here we discuss some concepts in graph theory and the reader is referred to [1, 2, 8, 9] if more details are sought. A simple graph $\Gamma = (V, E)$ consists of a nonempty finite set $V(\Gamma)$ of elements called vertices and a finite set $E(\Gamma)$ of distinct unordered pairs of distinct elements of $V(\Gamma)$ called edges. We call $V(\Gamma)$ the vertex-set and $E(\Gamma)$ the edge-set of $\Gamma$. 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 $x$. If all of the vertices of a graph $\Gamma$ have the same degree, then $\Gamma$ is a regular graph. If every vertex of $\Gamma$ has degree $r$, then $\Gamma$ is $r$-regular.

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 $V'(\Gamma') \subseteq V(\Gamma)$ and $E'(\Gamma') \subseteq E(\Gamma)$, then $\Gamma' = (V', E')$ is a subgraph of $\Gamma$. A graph $\Gamma' = (V', E')$ is called an induced subgraph of a graph $\Gamma = (V, E)$ if $V' \subseteq V$ and all edges of $\Gamma$ having both ends in $V'$ form edge set $E'$. A clique of $\Gamma$ is a complete subgraph of $\Gamma$. A clique of order $k$ is a $k$-clique. The maximum order of a clique of $\Gamma$ is called the clique number of $\Gamma$ and is denoted by $\omega(\Gamma)$. A graph is called connected if any two vertices are connected by some path; it is called disconnected otherwise. A maximal connected subgraph of $\Gamma$ is called a component of $\Gamma$.

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. A cycle in $\Gamma$ that contains every vertex of $\Gamma$ is called a Hamiltonian cycle of $\Gamma$. The girth of a graph is the length of a shortest cycle, denoted by $g(\Gamma)$. The circumference of a graph $\Gamma$ is the maximum length of a cycle in $\Gamma$, denoted by $c(\Gamma)$. A graph without cycles is called acyclic graph. Two graphs $\Gamma$ and $\Gamma'$ are isomorphic if there is a one-one correspondence between the vertices of $\Gamma$ and those of $\Gamma'$ such that the number of edges joining any two vertices of $\Gamma$ is equal to the number of edges joining the corresponding vertices of $\Gamma'$.

3 Main Results

We divide this section into two: we first study group action on group of units of $\mathbb{Z}_n$ and use it later to study a graph we are going to construct.

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

Here 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 $p_i$ distinct primes, that is, we assume that $|P| \neq 0$. The results we obtain here are so useful in proving most of the results in the next subsection.

Definition 3.1.1. Let $P$ be as defined in Definition 2.1.1. Define $A = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{|P|}}$ where $p_i \in P$.

Remark 3.1.2. 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 $|A| = \prod_{p \in P} p$.

Definition 3.1.3. Let $P$ be as defined in Definition 2.1.1. For $u$ in $U_n$ and $s = (s_1, \ldots, s_{|P|})$ in $A$, we define the maps $\pi_s$ by $\pi_s : u \mapsto \sum_{i=1}^{|P|} s_i n/p_i + u$ where $p_i \in P$ and $0 \leq s_i \leq p_i - 1$.

Definition 3.1.4. We define the set of maps by $\Theta_A = \{\pi_s | s \in A\}$.

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

© JGRMA 2018, All Rights Reserved
Lemma 3.1.5. \(\pi_s\) 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 \(\pi_s(u) - u = \sum_{i=1}^{[P]} s_in/p_i = tp_1\) where \(s = (s_1, ..., s_{[P]})\) in \(A\), \(p_i \in P\), for some integers \(m\) and \(t\). Since \(\sum_{i=1}^{[P]} s_in/p_i + u = \bar{u}\) implies \(u = \bar{u} - \sum_{i=1}^{[P]} s_in/p_i = p_1(m - t)\) 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 \(\Theta_A\) together with the operation of composition of maps \(\circ\) form a group.

**Lemma 3.1.6.** \(\Theta_A\) together with the operation of composition of maps \(\circ\) is a group.

**Proof.** Firstly, we show that \(\Theta_A\) is closed under the operation of composition of maps \(\circ\). Let \(\pi_s\) and \(\pi_{s'}\), with \(s = (s_1, ..., s_{[P]})\) and \(s' = (s_1', ..., s'_{[P]})\) in \(A\), be any two elements of \(\Theta_A\). So, for \(u \in U_n\),

\[
\pi_s \circ \pi_{s'}(u) = \sum_{i=1}^{[P]} s_in/p_i + \left(\sum_{i=1}^{[P]} s_i'n/p_i + u\right) = \sum_{i=1}^{[P]} (s_i + s_i')n/p_i + u = \sum_{i=1}^{[P]} s_i'n/p_i + u
\]

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 \(\pi_s\) 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 3.1.7.** \(\Theta_A\) acts on \(U_n\).

**Proof.** Let \(u \in U_n\). It is clear that \(\pi_{(0,...,0)}(u) = u\). Let \(\pi_s\) and \(\pi_{s'}\), with \(s = (s_1, ..., s_{[P]})\) and \(s' = (s_1', ..., s'_{[P]})\) in \(A\), be any two elements of \(\Theta_A\). Since

\[
(\pi_s \circ \pi_{s'})(u) = \pi_{s''}(u) = \sum_{i=1}^{[P]} (s_i + s_i')n/p_i + u = \sum_{i=1}^{[P]} s_in/p_i + \left(\sum_{i=1}^{[P]} (s_i)n/p_i + u\right)
\]

where \(s'' = (s_1 + s_1', ..., s_{[P]} + s'_{[P]})\), we conclude that \(\Theta_A\) acts on \(U_n\).

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

**Definition 3.1.8.** Let \(u \in U_n\). Then the orbit in \(U_n\) containing \(u\) under the action of \(\Theta_A\) is \(\mathcal{O}_u = \{\pi_s(u) | s \in A\}\).

**Lemma 3.1.9.** For any \(u \in U_n\), \(|\mathcal{O}_u| = \prod_{p \in P} p\).

**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 3.1.2 we noted that \(|A| = \prod_{p \in P} p\).

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

**Theorem 3.1.10.** \(|\mathcal{O}| = \frac{\phi(n)}{\prod_{p \in P} p}\).
Example 3.1.11. Consider \( \mathbb{Z}_{25} \). So we have \( \Theta_A = \{ \pi_s | s \in A \} \) where \( A = \mathbb{Z}_5 \) and \( U_{25} = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 1, 8, 19, 21, 22, 23, 24 \} \). The orbits are \( \mathcal{O}_1 = \{1, 6, 11, 16, 21\} \), \( \mathcal{O}_2 = \{2, 7, 12, 17, 22\} \), \( \mathcal{O}_3 = \{3, 8, 13, 18, 23\} \) and \( \mathcal{O}_4 = \{4, 9, 14, 19, 24\} \). Observe that \( \bigcup \mathcal{O}_i = U_{25} \) and \( U_{25} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_3 \cup \mathcal{O}_4 \).

Example 3.1.12. Consider \( \mathbb{Z}_{36} \). We have \( U_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \) and \( \Theta_A = \{ \pi_s | s \in A \} \) 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 \( \bigcup \mathcal{O}_i = U_{36} \) and \( U_{36} = \mathcal{O}_1 \cup \mathcal{O}_5 \).

### 3.2 A graph associated with \( U_n \) and \( \mathcal{I}_n \) in \( \mathbb{Z}_n \)

In this section we study a graph associated with group of units and irreducible elements in \( \mathbb{Z}_n \). In this graph, the group of units in \( \mathbb{Z}_n \) is a vertex-set and an edge-set is the set of all pairs of units which are both factors of an irreducible element in \( \mathbb{Z}_n \). Recall that the set of irreducible elements in \( \mathbb{Z}_n \) can be written as \( \mathcal{I}_n = \{ up | u \in U_n, p \in \mathcal{P} \} \) (see Remark 2.1.3). We formally define our graph in the definition that follows.

**Definition 3.2.1.** Given \( U_n \) of \( \mathbb{Z}_n \), we define a graph \( \Gamma = (V, E) \) as follows

\[
V(\Gamma) = U_n \\
[v_1, v_2] \in E(\Gamma) \iff v_1, v_2 \in U_n, v_1 \neq v_2 \text{ and } v_1p \equiv v_2p \pmod{n} \text{ where } p \in \mathcal{P}.
\]

Note that in our definition both \( v_1p \) and \( v_2p \) are in \( \mathcal{I}_n \). Since for cases where \( \mathbb{Z}_n \) does not contain irreducible elements we simply have empty graphs then we only consider \( \mathbb{Z}_n \) with irreducible elements (i.e., \( |\mathcal{P}| \geq 1 \)). This graph is associated with units in \( \mathbb{Z}_n \) so we denote it by \( \Gamma_n \), \( V(\Gamma) \) is denoted by \( V_n \) and \( E(\Gamma) \) is denoted by \( E_n \). We first give some examples.

**Example 3.2.2.** In \( \mathbb{Z}_{18} \), we have \( U_{18} = \{1, 5, 7, 11, 13, 17\} \), \( \mathcal{P} = \{3\} \), \( \mathcal{I}_{18} = \{3, 15\} \) and \( E_{18} = \{[1, 7], [1, 13], [7, 13], [5, 11], [5, 17], [11, 17]\} \). See \( \Gamma_{18} \) in the figure below.

![Figure 1: A graph of \( \Gamma_{18} \)](image)

**Example 3.2.3.** In \( \mathbb{Z}_{36} \), we have \( U_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \), \( \mathcal{P} = \{2, 3\} \) and \( \mathcal{I}_{36} = \{2, 3, 10, 14, 15, 21, 22, 26, 33, 34\} \). See \( \Gamma_{36} \) in the figure below.

![Figure 2: A graph of \( \Gamma_{36} \)](image)
Example 3.2.4. Let \( n = 3^2 5^3 \) or \( n = 3^2 5^3 \prod_{i=1}^{k} p_i \), that is, \( \mathcal{P} = \{3, 5\} \). The figure that follows shows a component of \( \Gamma_n \).

![Figure 3: A component of \( \Gamma_n \) with \( \mathcal{P} = \{3, 5\} \)](image)

In the lemma that follows we show that any element in \( \mathcal{O}_u \), where \( u \in U_n \), has all its adjacent elements in the same orbit. Equivalently, if an irreducible element has a unit factor in \( \mathcal{O}_u \) then it implies that all its unit factors are in \( \mathcal{O}_u \).

**Lemma 3.2.5.** Let \( u \in U_n \). Then if \( v \in \mathcal{O}_u \) is a unit factor of \( w \in \mathcal{I}_n \) then all unit factors of \( w \) are in \( \mathcal{O}_u \).

**Proof.** Any element in \( \mathcal{O}_u \) is of the form \( \pi(s_1, ..., s_{|\mathcal{P}|})(u) = \sum_{j=1}^{|\mathcal{P}|} s_j n / p_j + u \) where \( (s_1, ..., s_{|\mathcal{P}|}) \in \mathcal{A} \) and \( s_j \in \{0, ..., p_j - 1\} \) and \( p_j \in \mathcal{P} \) (see Definition 3.1.3). Without loss of generality, suppose that \( w \) is generated by \( p_1 \), that is \( w = vp_1 \) where \( v \in \mathcal{O}_u \). 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 \( v_i = \pi(i, s_2, ..., s_{|\mathcal{P}|})(u) \), for all \( i \) (\( 0 \leq i \leq p_1 - 1 \)), are also unit factors of \( w \). This must be true since, for any \( k, l \in \{0, ..., p_1 - 1\} \), we have \( v_k p_1 = \pi(k, s_2, ..., s_{|\mathcal{P}|})(u)p_1 = \frac{kn}{p_1} + \left( \sum_{j=2}^{|\mathcal{P}|} s_j n / p_j + u \right)p_1 = \frac{kn}{p_1} + \left( \sum_{j=2}^{|\mathcal{P}|} s_j n / p_j + u \right)p_1 = \pi(l, s_2, ..., s_{|\mathcal{P}|})(u)p_1 = vp_1 (\mod n) \) (i.e., \( v_k \) and \( v_l \) are both unit factors of \( w \) since \( v_k p_1 = vp_1 (\mod n) \)).

We claim that \( w \) does not contain any unit factor in other orbits other than \( \mathcal{O}_u \). For sake of contradiction, suppose \( w \) has another unit factor \( v'_l = \pi(l, s_2, ..., s_{|\mathcal{P}|})(u') \) 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 \( v'_l p_1 = v_j p_1 (\mod n) \). This implies that \( v'_l \equiv v_j (\mod n/p_1) \) 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 \( s_1 = s_i - 1 = s_{i+1} = \cdots = s_{|\mathcal{P}|} = 0 \) and \( 0 \leq s_i \leq p_i - 1 \) so that we have \( \Theta_{A'} = \{\pi_{s'}|s' \in A'\} \), 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 \( A' = \mathbb{Z}_{p_i} \). For \( u' \in \mathcal{O}_{u'} \), we denote the orbit containing \( u' \) under the action of \( \Theta_{A'} \) on \( \mathcal{O}_u \) by \( \mathcal{O}_{u u'} = \{s n / p_i + u'|0 \leq s_i \leq p_i - 1\} \). We show that elements in \( \mathcal{O}_{u u'} \) are all adjacent to each other. Equivalently, we show that elements in \( \mathcal{O}_{u u'} \) are all unit factors of one irreducible element generated by \( p_i \), implying that \( \mathcal{O}_{u u'} \) induces a clique \( K_{p_i} \).

**Lemma 3.2.6.** Let \( \Theta_{A'} = \{\pi_{s'}|s' \in A'\} \) 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 induced 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 \( \Theta_A \). Also note that \( \Theta_{A'} \) acts on \( \mathcal{O}_u \) since, for all \( u' \in \mathcal{O}_{u} \), \( \pi_{0}(u') = u' \) and \( \pi_{s}(\pi_{u'}(u')) = (\pi_{s} u')(u) \), for all \( \pi_{s}, \pi_{s'} \in \Theta_{A'} \). Let the orbit containing \( u' \in \mathcal{O}_u \) be denoted by \( \mathcal{O}_{u u'} = \{s n / p_i + u'|0 \leq s_i \leq p_i - 1\} \). We show that if an irreducible element generated by \( p_i \) has a factor in \( \mathcal{O}_{u u'} \) then all elements in \( \mathcal{O}_{u u'} \) are also factors of it.
Suppose that $v \in O_{uu'}$ such that $w = vp_i$. Write $v = kn/p_i + u'$ for some $k \in \{0, \ldots, p_i - 1\}$. For any $v'$ in $O_{uu'}$, we have $v' = gn/p_i + u'$ where $g \in \{0, \ldots, p_i - 1\}$. 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 $O_{uu'}$ are factors of $w$.

We claim that $O_{uu'}$ is the only orbit with factors of $w$. For sake of contradiction, suppose that $v'' \in O_{uu''}$, where $u''$ is in $O_u$ but not in $O_{uu'}$, is also a factor of $w$. So let $O_{uu''} = \{s_i n/p_i + u'\} \{0 \leq s_i \leq p_i - 1\}$ and write $v'' = tn/p_i + u''$ for some $t \in \{0, \ldots, p_i - 1\}$. So $t n/p_i \equiv v p_i = w \pmod{n} \Rightarrow (t n/p_i + u'')p_i \equiv (kn/p_i + u')p_i \pmod{n} \Rightarrow (t n/p_i + u')p_i \equiv kn + u'p_i \pmod{n} \Rightarrow (t n/p_i + u')p_i \equiv u'p_i \pmod{n} \Rightarrow t n/p_i + u'' \equiv u' \pmod{n/p_i} \Rightarrow t n/p_i + u'' \equiv h n/p_i + u'$. But $t n/p_i + u'' \equiv u' \pmod{n/p_i}$ implies an element in $O_{uu'}$ is equal to an element in $O_{uu''}$ which is a contradiction since $O_{uu'}$ and $O_{uu''}$ two different orbits in $O_u$ under the action of $\Theta_{A'}$.

**Remark 3.2.7.** Suppose the orbit containing $u' \in O_u$ is $O_{uu'} = \{s_i n/p_i + u'\} \{0 \leq s_i \leq p_i - 1\}$ under the action of $\Theta_{A'}$, with $A' = \mathbb{Z}_{p_i}$. Then

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

(ii) by (i) and Lemma 3.2.6, it implies that there are $p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|P|}$ irreducible elements which are generated by $p_i$ and have their unit factors in $O_u$.

(iii) it also follows from (i) that if $|P| > 1$ then there are $\sum_{i=1}^{P} |P| \sigma_i$, where $\sigma_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|P|}$, orbits under the actions of $\Theta_{A'}$ (with $A' = \mathbb{Z}_{p_i} \forall p_i \in P$) in $O_u$ and 1 if $|P| = 1$.

**Lemma 3.2.8.** 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 $O_u$ where $u \in U_n$ contain at most 1 element in common.

**Proof.** Suppose some orbits induced in $O_u$ 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 $s_i \in \{0, \ldots, p_i - 1\}$ and $s_j \in \{0, \ldots, p_j - 1\}$. 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 3.2.9.** Each component in $\Gamma_n$ is a $\sum_{P \in P} (p - 1)$-regular graph.

**Proof.** By Lemma 3.2.5, we observe that each $O_u$ induces a component in $\Gamma_n$. It is a fact that when $\Theta_{A'}$ is acted upon $O_u$ where $u \in U_n$ and $A' = \mathbb{Z}_{p_i}$ with $p_i \in P$, every element in $O_u$ belongs to exactly one orbit of the form $O_{uu'} = \{s_i n/p_i + u'\} \{0 \leq s_i \leq p_i - 1\}$ where $p_i \in \mathbb{P}$ otherwise it would be a contradiction. In this case, by Lemma 3.2.6, every element in $O_{uu'}$ is adjacent to $p_i - 1$ vertices. Thus, for all $i (1 \leq i \leq |P|)$, every element in $O_u$ belongs to $|P|$ different orbits and from each orbit it gains degree $p_i - 1$ so that its total degree is $\sum_{i=1}^{P} (p_i - 1)$ if we consider all $|P|$ orbits it is contained in.

We remark that Theorem 3.2.9 indicates that if 2 is in $\mathbb{P}$ then every vertex has odd degree, as is the case in Examples 3.2.2 and 3.2.3, whereas if 2 is not in $\mathbb{P}$ then every vertex has even degree, as is the case in Example 3.2.4.

**Theorem 3.2.10.** $\Gamma_n$ contains $\frac{\varphi(n)}{\prod_{P \in P} P}$ isomorphic components.

**Proof.** By Lemma 3.2.5, $G_n$ must contain components since if an irreducible element has a unit factor in $O_u$ 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 $O_u$ is connected because all elements in an orbit induced under the action of $\Theta_{A'}$ on $O_u$ occur as elements in other orbits induced under the actions of $\Theta_{A''}$ (we know that $A' = \mathbb{Z}_{p_i}$ and $A'' = \mathbb{Z}_{p_j}$, with $i \neq j$, see Lemma 3.2.8).
Since all orbits $O_u$ in $U_n$ when acted upon by $\Theta_A$ have the same structure then all components obtained from these orbits must be isomorphic. Since, by Lemma 3.1.9, $|O_u| = \prod_{p \in P} p$ then we conclude that there are $\phi(n)/\prod_{p \in P} p$ components.

As a consequence of Theorem 3.2.10, we remark that the graph $G_n$ is a disconnected graph with isomorphic components. We denote a component of $\Gamma_n$ by $C_{\Gamma_n}$. Since all the components in $\Gamma_n$ are isomorphic then $C_{\Gamma_n}$ can be used to study some properties for $\Gamma_n$. For this reason, in the rest of this section we mostly study a component and generalise results to $\Gamma_n$.

**Theorem 3.2.11.** Let $O_{uu'}$ be the orbit in $O_u$ containing $u'$, where $u \in U_n$ and $u' \in O_u$, under the action of $\Theta_{A'}$ with $A' = \mathbb{Z}_p$, $p_i \in P$. Then $O_{uu'}$ induces a clique in a component associated with $O_u$ in $\Gamma_n$. Furthermore, in each component there are $\sum_{i=1}^{\sigma_i} \sigma_i$, where $\sigma_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|P|}$, cliques induced by orbits under the actions of $\Theta_{A'}$ for all $i$, if $|P| > 1$ and 1 clique if $|P| = 1$.

**Proof.** By Lemma 3.2.6, all elements in $O_{uu'}$ induce a clique. To find the number of cliques induced in each component, we simply count all the orbits obtained in $O_u$ under the actions of $\Theta_{A'}$ with $A' = \mathbb{Z}_p$ for all $p \in P$. If $|P| = 1$ it is not hard to see that $O_{uu'} = O_u$, that is, there is 1 clique. So we count cliques when $|P| > 1$. By Remark 3.2.7 (iii), we have the result.

In Example 3.2.2, we considered the graph $\Gamma_9$ where $P = \{3\}$, i.e., $|P| = 1$ so there is 1 clique in each component. Example 3.2.3 considers the graph $\Gamma_{36}$ and since $P = \{2, 3\}$ so there are $2 + 3 = 5$ cliques induced by orbits in each component. In Example 3.2.4, we considered $\Gamma_n$ with $n = 3^3 5^2$ or $n = 3^\alpha 5^\beta \prod_{i=1}^k p_i$. In this case we have $P = \{3, 5\}$. So the number of cliques induced by orbits in each component is $3 + 5 = 8$.

**Corollary 3.2.12.** $C_{\Gamma_n}$ is a union of cliques $K_p$ where $p \in P$ and $\omega(\Gamma_n) = \max(P)$.

**Proof.** By Theorem 3.2.11, $O_u$ where $u \in U_n$ contains orbits $O_{uu'}$ (under the action of $\Theta_{A'}$ with $A = \mathbb{Z}_p$) which induce cliques in $C_{\Gamma_n}$ associated with $O_u$. Since $|O_{uu'}| = p_i$ (recall that $O_{uu'} = \{ s_i n / p_i + u' | 0 \leq s_i \leq p_i - 1 \}$, where $p_i \in P$) we conclude that each component is a union of $K_{p_i}$, for all $p_i \in P$.

It is easy to observe that since all cliques are of the form $K_p$ where $p \in P$ so a maximum clique must be $K_{\max(P)}$ implying that $\omega(\Gamma_n) = \max(P)$.

In Example 3.2.2, $C_{\Gamma_9}$ is just a $K_2$ and so $\omega(\Gamma_9) = 2$. In Example 3.2.3, $C_{\Gamma_{36}}$ is union of $K_2$ and $K_3$ so that $\omega(\Gamma_{36}) = 3$ whereas in Example 3.2.4, $C_{\Gamma_n}$ is a union of $K_3$ and $K_5$ so that $\omega(\Gamma_n) = 5$ where $n = 3^\alpha 5^\beta$ or $n = 3^\alpha 5^\beta \prod_{i=1}^k p_i$ with $\alpha, \beta > 1$.

**Proposition 3.2.13.** The order of $C_{\Gamma_n}$ is $\prod_{p \in P} p$ and its size is $\sum_{i=1}^{\sigma_i} \sigma_i \binom{p_i}{2}$, where $\sigma_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|P|}$, if $|P| > 1$ and $\binom{p_i}{2}$ if $P = \{p\}$.

**Proof.** The order of a component of $C_{\Gamma_n}$ is equal to the cardinality of an orbit in $U_n$. By Lemma 3.1.9, $|O_u| = \prod_{p \in P} p$, where $u \in U_n$. To find the size of $C_{\Gamma_n}$ we simply count the edges of all cliques induced by orbits $O_{uu'}$. Each clique induced by $O_{uu'} = \{ s_i n / p_i + u' | 0 \leq s_i \leq p_i - 1 \}$ has $|E(K_{p_i})| = \binom{p_i}{2}$ edges. It is clear that if $P = \{p\}$ then $O_u = O_{uu'}$ and so $C_{\Gamma_n}$ is simply a clique $K_n$ of size $\binom{n}{2}$. Now assume that $|P| > 1$. By Remark 3.2.7 (ii), for each $i (1 \leq i \leq |P|)$, there are $\sigma_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_{|P|}$ orbits $O_{uu'}$ in $O_u$ under the action of $\Theta_{A'}$ with $A' = \mathbb{Z}_p$, $p_i \in P$. Thus, for each $i$, there are $\sigma_i \binom{p_i}{2}$ edges in $C_{\Gamma_n}$. Hence there are $\sum_{i=1}^{\sigma_i} \binom{p_i}{2}$, for all $i$.

In Example 3.2.2, we observe that $P = \{3\}$ so $C_{\Gamma_9}$ is a clique $K_3$ and so we have 3 vertices and $\binom{3}{2} = 3$ edges. In example 3.2.3, we have $P = \{2, 3\}$ so in $C_{\Gamma_{36}}$ we have $2 \cdot 3 = 6$ vertices and $3 \binom{2}{2} + 2 \binom{3}{2} = 9$ edges. In Example 3.2.4, $n = 3^\alpha 5^\beta$ or $n = 3^\alpha 5^\beta \prod_{i=1}^k p_i$ so $P = \{3, 5\}$. Thus in $C_{\Gamma_n}$ we have $3 \cdot 5 = 15$ vertices and $5 \binom{3}{2} + 3 \binom{5}{2} = 45$ edges.
Theorem 3.2.14. Let $|P| \geq 1$. Then $C_{\Gamma_n}$ contains a cycle if and only if $P \neq \{2\}$.

Proof. Suppose $C_{\Gamma_n}$ contains a cycle. Then $V(C_{\Gamma_n})$ contains some elements with at least degree 2. By Theorem 3.2.11, $C_{\Gamma_n}$ is a union of cliques induced by orbits of the form $O_{uu'} = \{s_i n/p_i + u'|0 \leq s_i \leq p_i - 1\}$ in $O_u$ where $u \in U_n$. Since $|O_{uu'}| = p_i$ then in each clique every vertex has degree $p_i - 1$. Thus $P$ must contain some prime $p > 2$ for $C_{\Gamma_n}$ to have a cycle (i.e., we cannot have $P = \{2\}$).

Conversely, suppose that $P \neq \{2\}$. Since $|P| \geq 1$ then $P$ contains some odd prime, say $p$. By Theorem 3.2.11, there is a clique of order $p$ in $C_{\Gamma_n}$. But $p$ is an odd prime so there exist a cycle $C_p$.

Theorem 3.2.15. If $C_{\Gamma_n}$ contains cycles then $g(C_{\Gamma_n}) = 3$.

Proof. By Theorem 3.2.11, $C_{\Gamma_n}$ contains cliques of the form $K_p$. Suppose $C_{\Gamma_n}$ contains cycles. Then, by Theorem 3.2.14, $C_{\Gamma_n}$ contains some clique $K_p$ with $p > 2$. Hence the result follows.

Theorem 3.2.16. If $C_{\Gamma_n}$ contains cycles then $c(C_{\Gamma_n}) = \prod_{p \in P} p$.

Proof. Suppose $C_{\Gamma_n}$ contains cycles. From Lemma 3.2.8 we note that, for $i \neq j$, it is impossible for the groups $\Theta_{A_i}$ and $\Theta_{A_j}$, with $A' = \mathbb{Z}_{p_i}$ and $A'' = \mathbb{Z}_{p_j}$, to induce the same orbit when acted upon $O_u$ where $u \in U_n$; in fact the orbits contain at most 1 element in common. This implies that one element in $O_u$ belongs to $|P|$ different orbits under the actions of $\Theta_{A_i}$, for all $i (1 \leq i \leq |P|)$. That is one element in $O_u$ belongs to $|P|$ cliques of the form $K_p$ where $p \in P$. Since, by Theorem 3.2.11, $C_{\Gamma_n}$ is a union of cliques $K_p$ then it is always possible to find a cycle which passes through all vertices of one clique to another thereby passing through all vertices in $V(C_{\Gamma_n})$. Since the number of vertices in $C_{\Gamma_n}$ is $\prod_{p \in P} p$, so the result follows.

In Example 3.2.2, we have $P = \{3\}$ so in $C_{\Gamma_3}$ we have $g(C_{\Gamma_3}) = c(C_{\Gamma_3}) = 3$. In Example 3.2.3, $P = \{2, 3\}$, so $C_{\Gamma_{36}}$ contains cycles with $g(C_{\Gamma_{36}}) = 3$ and $c(C_{\Gamma_{36}}) = 6$. In Example 3.2.4, $n = 3^5 5^3$ or $n = 3^5 5^3 \prod_{i=1}^{k} p_i$, so $P = \{3, 5\}$ and $C_{\Gamma_n}$ contains cycles with $g(C_n) = 3$ and $c(C_n) = 15$.

Corollary 3.2.17. $C_{\Gamma_n}$ contains a Hamiltonian cycle if it has cycles.

Proof. This is a consequence of Theorem 3.2.16.

Remark 3.2.18. From the family of all $n$ which are such that $P$ is the same, $\Gamma_n$ has the same $C_{\Gamma_n}$. The number of $C_{\Gamma_n}$ in such graphs increases with an increase in the value of $n$.

We finish this section by discussing some significance of the graph $\Gamma_n$. This graph was proposed with an aim of establishing the distribution of units in the factors of irreducible elements in the ring $\mathbb{Z}_n$. What we learn from this graph is that the distribution of units in the factors of irreducible elements depends on the elements in the set $P$ and this is shown in the corollary below.

Corollary 3.2.19. The distribution of units in factors of irreducible elements is different with a minimum of $\min(P)$ and a maximum of $\max(P)$.

Proof. We know from Theorem 2.1.2 and Remark 2.1.3 that the set of irreducible elements is generated by $P$ and $U_n$, and can represented as $\mathcal{Z}_n = \{up|p \in P, u \in U_n\}$. According to Lemma 3.2.6, all elements in an orbit $O_{uu'} = \{s_i n/p_i + u'|0 \leq s_i \leq p_i - 1\}$ of $O_u$ under the action of $\Theta_{A'}$, where $A' = \mathbb{Z}_{p_i}$, are all unit factors of one irreducible element generated by $p_i$. So all irreducible elements generated by $p$ in $P$ have the same number of unit factors (i.e., have equal distribution of unit factors) and since we know that $|O_{uu'}| = p$ then each has $p$ unit factors. This implies that if $|P| = 1$ then the distribution of unit factors is the same and if $|P| > 1$ then the distribution is different. It also implies that the irreducible elements generated by $\max(P)$ have the highest number of unit factors and those generated by $\min(P)$ have the minimum number. This is also evidenced in Corollary 3.2.12 in which we found out that the maximum clique number of $\Gamma_n$ is $\max(P)$; implying that some irreducible elements have $\max(P)$ unit factors.
4 Conclusion

In this paper we studied a graph in which the group of units in the ring of integers modulo $n$ is a vertex-set and an edge-set is the set of all pairs of units which are both factors of an irreducible element. We studied properties such as the girth, circumference, cliques, components, cycles and connectivity. We showed that this graph is regular and contains isomorphic components. Furthermore, we used this graph to conclude that the distribution of units in the factors of irreducible elements is different and we were able to enumerate unit factors for each irreducible element.

References


