$\mathbb{Z}_n$ Graphs

An Application of Graphs to Ring Theory

By
Taha Ameen ur Rahman

Supervised by
Dr. Ayman Badawi

A thesis presented to
The American University of Sharjah
in partial fulfillment of the
requirements for the degree of
Bachelor of Science in Mathematics

Department of Mathematics and Statistics
American University of Sharjah
Sharjah, United Arab Emirates
December 7, 2018

Abstract

The project is an application of graph theory to number theory and abstract algebra. Its primary objective is to study the graphical manifestation of the algebraic properties of the ring of integers modulo n, $\mathbb{Z}_n$. This report initiates by presenting basic concepts and terminology from graph theory and abstract algebra. It delineates the construction of a graph associated with the ring of integers modulo n, and studies its properties. These include conditions required for the connectivity of the graph, as well as descriptions of components, vertices, edges and paths in the graph. Emphasis is provided on the induced subgraph of units and zero divisors, and the interplay between the additive and multiplicative operations of the ring and their exhibition as properties of the subgraphs. Theorems pertaining to these are derived and proved using concepts from abstract algebra and ring theory. The report then provides examples of various graphs, classified based on connectivity. The results are verified using computer simulations, and algorithms to construct graphs and test a variety of these properties are also presented.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Basic Terminology

1.1.1 Graph Theory

- A graph, $\mathcal{G} = (V, E)$ consists of two sets, V and E, where:
  - V is the set of vertices
  - E is the set of edges (note that an edge is undirected line segment that connects two vertices)
- If a vertex $v \in V$ is an endpoint of an edge $e \in E$, then v is said to be *incident* on e.
- Let $u, v \in V$. u and v are said to be *adjacent* if u and v are joined by an edge, i.e. if $(u, v) \in E$. Two adjacent vertices are sometimes referred to as neighbors [1].
- A Graph is said to be *regular* if each vertex of the graph has the same degree. More precisely, if the degree of each vertex is d, then the graph is said to be d-regular.
- A graph is said to be simple if it has no loops and no multi-edges.
- A *path* in a graph is an alternating sequence of distinct vertices and distinct edges. For a simple graph, this can simply be represented as a sequence of vertices, as there can be at most one edge joining two vertices.
- The path can thus be represented as $v_0 - v_1 - ... - v_n$, where the v_i's are distinct vertices such that
  - v_0 is said to be the *initial vertex.*
  - v_n is said to be the *final vertex.*
  - v_i is said to be an *internal vertex.*
- A path is said to be *closed* if the initial and final vertex are the same.
- The *length* of a path is the number of edges that are traversed during the path, for example, $v_1 - v_2 - v_3$ is a path of length 2 and $v_1 - v_2 - v_3 - v_4$ is a path of length 3.
- A *cycle* is a closed path of length at least 3.
- The *girth* of a graph is the length of its smallest cycle and if a graph has no cycles, then we say that the girth is infinity.
- *The Complete Graph on n vertices* is denoted as $\mathbb{K}_n$, and consists of n vertices such that if $u, v \in V$ and $u \neq v$, then $(u, v) \in E$, i.e. $u - v$ is an edge.
- A graph is said to be *bipartite* if its vertices can be partitioned into two sets in such a way that no edge joins two vertices in the same set.
- *The Complete Bipartite Graph on r, s vertices* is denoted as $\mathbb{K}_{r,s}$ is a simple bipartite graph in which V can be partitioned into V_1 and V_2 such that $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \Phi$, $|V_1| = r$, $|V_2| = s$, and each element of V_1 is adjacent to all elements of V_2, and each element of V_2 is adjacent to all elements of V_1, but no edge joins two vertices in V_1 or V_2.

  - The *distance* between two vertices in a graph is the length of the shortest path between them. Let a, b be two distinct vertices in a graph. Then $d(a, b)$ denotes the distance between a and b.

  - The *diameter* of a graph is defined as $Max\{d(u, v) \mid u, v \text{ are distinct vertices}\}$.

- A graph is said to be *connected* if there exists a path between any two pairs of vertices, u and v.

- Two simple graphs, G and H are said to be isomorphic if $\exists \phi : V_G \to V_H$ such that ϕ is bijective, and such that $\forall u, v \in V_G, (u, v) \in E_G \iff (\phi(u), \phi(v)) \in E_H$. If such an isomorphism exists, we denote it as $G \cong H$.

- A *subgraph* H of a graph G is a graph such that $V_H \subset V_G$ and $E_H \subset E_G$.

- An *induced subgraph* H of a graph G, on a vertex set $W = \{w_1, w_2, ..., w_k\} \subseteq V_G$ has $V_H = W$ and $E_H = \{e \in E_G \mid \text{the end points of edge } e \text{ are in } W\}$.

- A *component* of a graph G is a connected subgraph H such that no subgraph of G that properly contains H is connected. Hence, a component of a graph is a *maximally connected subgraph*.

- A path is said to be *Hamiltonian* if it traverses all the vertices $v \in V$ such that no vertex is incident twice. A closed Hamiltonian path has no repeated vertices except the initial and final vertex, and is called a *Hamiltonian cycle*.

- A path is said to be *Eulerian* if it traverses all the edges $e \in E$ such that no edge is incident twice. Further, if the path is closed, then it is called an *Eulerian cycle*.

- The *chromatic number* of a graph $\mathcal{G}$, denoted as $\chi(\mathcal{G})$ is the smallest number of colors required to color $\mathcal{G}$ in such a way that no two neighbors share the same color.

- A graph is said to be *planar* if it can be embedded in a plane. In other words, it can be drawn in such a way that no two edges intersect each other.

- The *clique number* of a graph $\mathcal{G}$ is the cardinality of the largest set W such that $W \subset V_G$ and the induced subgraph on W is a complete graph. It is denoted as $\omega(\mathcal{G})$.

- The *dominating number* of a graph G is the cardinality of the smallest set $B \subset V$ such that $\forall v \in V\ \exists b \in B$ such that $(b, v) \in E_G$. The set B which satisfies this is called a *domminating set*. The dominating number is characteristic of the graph and is unique, but the dominating set need not be unique.

- A *tree* is a connected graph with no cycles.

- A *spanning subgraph*, H of a graph G has its vertex set $V_H = V_G$.

- A *spanning tree* of a graph G is a subgraph of G which is a tree.

1.1.2 Ring Theory and Number Theory

- A *ring* is an algebraic structure on a set A along with operations $(+, \times)$ referred to as addition and multiplication where the following axioms are obeyed [2] [3]:
  - A is an Abelian group under addition.
    * A is closed under addition.
    * Addition is associative, so that $a + (b + c) = (a + b) + c \ \forall a, b, c \in A$.
    * *Additive Identity:* $\exists 0 \in A$ such that $0 + a = a + 0 \ \forall a \in A$.
    * *Additive Inverse:* $\forall a \in A, \exists -a \in A$ such that $a + (-a) = 0$.
    * *Abelian:* $a + b = b + a \ \forall a, b \in A$.
  - A is closed under multiplication.
  - Multiplication is associative, so that $a \times (b \times c) = (a \times b) \times c$.
  - Multiplication distributes over addition, so that $a \times (b + c) = (a \times b) + (a \times c)$.
  - *(Multiplicative Identity):* $\exists 1 \in A$ such that $1 \times a = a \ \forall a \in A$.
- Examples of rings include:
  - $\mathbb{R}$, the set of real numbers
  - $\mathbb{C}$, the set of complex numbers
  - $\mathbb{Q}$, the set of rational numbers
  - $\mathbb{Z}$, the set of integers
  - $\mathbb{Z}_n$, the set of integers (mod n).
- A *subring* of a ring A is a ring B such that $B \subset A$.
- A ring is said to be commutative if $a \times b = b \times a \quad \forall a, b \in A$.
- An *ideal* B of a commutative ring A is a subring of A such that $a \times b \in B \quad \forall b \in B$ and $\forall a \in A$.
- A *principal ideal* of a commutative ring A is an ideal that is generated by a single element, p. It is denoted as (p) and defined as $(p) = pA = \{p \times a \mid a \in A\}$.
- A ring A is said to be a *Principal Ideal Domain (PID)* if it is a commutative ring, and all its ideals are principal ideals.
- *Quotient Ring:* If A is a ring, and B is an ideal of the ring, then the ring $R = {}^{A}/_{B}$ is said to be the quotient ring. Here, $r \in R \implies r = a + B$, where $a \in A$. Addition and Multiplication are defined as:
  - $r_1 + r_2 = (a_1 + B) + (a_2 + B) = (a_1 + a_2) + B$.
  - $r_1 \times r_2 = (a_1 + B) \times (a_2 + B) = (a_1 \times a_2) + B$.
- *Cosets:* The element $r = a + B \in {}^{A}/_{B}$ is called the *left coset* of a. A *right coset* is similarly defined, but for commutative rings, both are the same and we do not distinguish between them.

- A ring is said to be *finite* if $|A| < \infty$.
- Let $a \in A$. Then a is said to be a
  - *Unit Element* if $\exists b \in A$ such that $a \times b = 1$.
  - *Zero Divisor* if $\exists b \in A$ such that $a \times b = 0$ and $b \neq 0$.
- A ring is said to be an *integral domain* if it is commutative and it has no non-zero zero-divisors.
- *Euler's $\phi(\cdot)$ Function:* Let $A = \mathbb{Z}_n$. Then $\phi(n)$ is the number of unit elements in $\mathbb{Z}_n$.
- *Prime Ideals:* An ideal P of a commutative ring R is said to be a prime ideal if it is a proper ideal with the property that $a \times b \in P \implies a \in P$ or $b \in P$.
- *Maximal Ideals:* A proper ideal M of a commutative ring A is said to be maximal if there exists no other proper ideal J of the ring A such that $M \subset J$. In finite commutative rings, prime and maximal ideals are the same.
- *Intersection of Ideals*: If I_1 and I_2 are two ideals of a ring A, then $I = I_1 \cap I_2$ consists of all $i \in A$ such that $i \in I_1$ and $i \in I_2$.
- *Product of Ideals*: If I_1 and I_2 are two ideals of a ring A, then $I = I_1 I_2 = \{\sum_{j=0}^{n} i_1 i_2 \mid i_1 \in I_1, i_2 \in I_2 \text{ for } n = 1, 2, ...\}$.
- *The Fundamental Theorem of Arithmetic:* Each positive integer n can be written as a product of primes in a unique way up to the order of factors.
- *The Chinese Remainder Theorem:* For a commutative ring A, if I_1, I_2,...I_k are pairwise co-prime ideals of A (i.e., $I_k + I_l = R$), then ${}^{R}/_{\bigcap_{j=1}^{k} I_j} = {}^{R}/_{I_1} \times ... \times {}^{R}/_{I_k}$
- *A Complete Reduced System of Residues* (mod n)*:* A set of integers A is said to be a complete reduced system of residues (mod n) if every integer is congruent modulo n to exactly one integer in A and $|A| = n$.

1.2 Graph Construction

This section delineates the construction of a graph whose vertex set is the ring of integers modulo n. Consider the ring $\mathbb{Z}_n$ with addition and multiplication modulo n. Construct the graph $\mathcal{G}(\mathbb{Z}_n)$ as follows:

- Write n in terms of its unique prime factorization.
- Assign $\mathcal{G}(\mathbb{Z}_n)$ with the vertex set $V_{\mathcal{G}} = \mathbb{Z}_n$.
- Connect two distinct vertices a and b with an edge iff $p \mid a + b$ for some prime factor p of n. Therefore, $(a, b) \in E_{\mathcal{G}}$ iff $a \neq b$ and $\exists\ p \mid a + b$ such that p is a prime factor of n.
- The graph is undirected and simple. Hence, there are no multiedges and no loops.

1.3 Notation

In this paper, the following terminology has been used in relation to the definitions presented in Section 1.1:

- $\mathcal{G}(\mathbb{Z}_n)$ is the graph of the ring $\mathbb{Z}_n$.
- $V_{\mathcal{G}(\mathbb{Z}_n)} = \mathbb{Z}_n = \{0, 1, ..., n-1\}$ is the set of vertices of $\mathcal{G}(\mathbb{Z}_n)$.
- $E_{\mathcal{G}(\mathbb{Z}_n)} = \{(a, b) \mid a, b \in V_{\mathcal{G}(\mathbb{Z}_n)}$ and a and b are connected$\}$ is the set of edges of $\mathcal{G}(\mathbb{Z}_n)$.
- $\mathcal{U}(\mathbb{Z}_n)$ is the set of all Unit Elements of $\mathbb{Z}_n$.
- $\mathcal{Z}(\mathbb{Z}_n)$ is the set of all Zero Divisors of $\mathbb{Z}_n$.
- $\mathcal{UG}(\mathbb{Z}_n)$ is the name of the induced subgraph on $\mathcal{U}(\mathbb{Z}_n)$.
- $\mathcal{ZG}(\mathbb{Z}_n)$ is the name of the induced subgraph on $\mathcal{Z}(\mathbb{Z}_n)$.
- $\phi(n) = |\mathcal{U}(\mathbb{Z}_n)|$. It is used in the context of the number of vertices in $\mathcal{UG}(\mathbb{Z}_n)$.
- $\gamma(n)$ is the degree of each of the $\phi(n)$ vertices in $\mathcal{UG}(\mathbb{Z}_n)$.
- If a_1 and a_2 are connected with an edge, then it is represented as $a_1 - a_2$. Similarly, by extension, a path on n vertices is represented as $a_1 - a_2 - ... - a_n$.
- The degree of a vertex x is denoted as $deg(x)$.
- The diameter of the graph is denoted as $diam(\mathcal{G}(\mathbb{Z}_n))$.
- The girth of the graph is denoted as $g(\mathcal{G}(\mathbb{Z}_n))$.
- The chromatic number of the graph is denoted as $\chi(\mathcal{G}(\mathbb{Z}_n))$.
- The clique number of the graph is denoted as $\omega(\mathcal{G}(\mathbb{Z}_n))$.
- $\mathbb{K}_n$ represents the complete graph with n vertices.
- $\mathbb{K}_{p,q}$ represents the complete bipartite graph with partitions V_1 and V_2 such that $|V_1| = p$ and $|V_2| = q$.
- (p) represents the principal ideal generated by p in the commutative ring of interest.
- In the figures, red vertices are the units, and blue vertices are the zero divsiors of the ring.
- In some of the graphs where n is large, the labels on the vertices have been removed for easier visibility of the inherent patterns.

1.4 Objectives

This section outlines some of the objectives of this project.

- Determining the conditions on n so that $\mathcal{G}(\mathbb{Z}_n)$ is connected.
- Describing the components of $\mathcal{G}(\mathbb{Z}_n)$ when it is not connected.
- Assume a and b are two vertices. Find a path $a - v_1 - v_2 - ...v_m - b$ such that $\forall i,\ 1 \leq i \leq m$, there is a prime factor p of n such that $p \mid v_i$.
- Assume a and b are two vertices. Find a path $a - v_1 - v_2 - ...v_m - b$ such that $\forall i,\ 1 \leq i \leq m$, there is no prime factor p of n such that $p \mid v_i$.
- Determine the diameter of $\mathcal{G}(\mathbb{Z}_n)$ when it is connected.
- Determine the dominating number and dominating sets of $\mathcal{G}(\mathbb{Z}_n)$ when it is connected.
- Determine the structure of the induced subgraph of units, $\mathcal{UG}(\mathbb{Z}_n)$ and identify necessary and sufficient conditions for its connectivity.
- Determine the structure of the induced subgraph of zero divisors, $\mathcal{ZG}(\mathbb{Z}_n)$ and identify necessary and sufficient conditions for its connectivity.
- Determine the degrees of vertices in $\mathcal{G}(\mathbb{Z}_n)$, $\mathcal{UG}(\mathbb{Z}_n)$, and $\mathcal{ZG}(\mathbb{Z}_n)$.
- Determine traversability in $\mathcal{G}(\mathbb{Z}_n)$ with respect to Eulerian and Hamiltonian paths and cycles.
- Determine the conditions for planarity of the graph $\mathcal{G}(\mathbb{Z}_n)$.
- Illustrate each of the above statements using computer simulations.
- Present visual examples of $\mathcal{G}(\mathbb{Z}_n)$,$\mathcal{UG}(\mathbb{Z}_n)$ and $\mathcal{ZG}(\mathbb{Z}_n)$ through computer simulations.
- Present algorithms to construct and verify properties of the graph as pseudocode, with examples of implementation.

2 Results

2.1 Results on Connectivity of $\mathcal{G}(\mathbb{Z}_n)$

Theorem 2.1. *If $n = p^\alpha$, where p is a prime number and $\alpha \in \mathbb{Z}^+$, then $\mathcal{G}(\mathbb{Z}_n)$ is not connected.*

Proof. consider $(p) = p\mathbb{Z}_n = \{x \in \mathbb{Z}_n \mid x = kp \text{ and } k \in \mathbb{Z}_n\}$. We show that the vertices in (p) are not connected to any vertex outside (p).

Clearly, $|(p)| = p^{\alpha-1}$. Firstly, it is clear that $a, b \in (p) \implies a$ and b are adjacent. This is true as $a = k_1p$ and $b = k_2p$. Thus, $a + b = (k_1 + k_2)p$ and hence, $p \mid a + b$. Now, pick $x \in (p)$ and $y \notin (p)$. Such a y always exists as $p^{\alpha-1} < p^\alpha \ \forall \ \alpha \geq 1$. By definition of (p), we have $x = pq_1$. Further, by Euclid's division lemma, $y = pq_2 + r$ where $0 \leq r < p$. Since $y \notin (p)$, we know that $r \neq 0$. Hence, $x + y = pq_1 + pq_2 + r = p(q_1 + q_2) + r$ and $0 < r < p$. Clearly, $p \nmid x + y$ and p is the only prime factor of n. Therefore, x and y are not connected.

Hence, the vertices in the ideal (p) are not connected to any vertex outside (p), and $\mathbb{Z}_n \setminus (p) \neq \Phi$. Thus, $\mathcal{G}(\mathbb{Z}_n)$ is not connected. ∎

Theorem 2.2. *$\mathcal{G}(\mathbb{Z}_n)$ is connected iff $n \neq p^m$ for some prime p. Furthermore, if $\mathcal{G}(\mathbb{Z}_n)$ is connected, then its diameter is 2.*

Proof. Since 0 and 1 are not connected, we conclude that $diam(\mathcal{G}(\mathbb{Z}_n)) \neq 1$. We show that $\forall x, y \in \mathbb{Z}_n, \exists w \in \mathbb{Z}_n$ such that $x - w - y$.

Since n is neither prime nor a power of a prime, we can write the prime factorization of n as $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, where $k \geq 2$ and $p_i \neq p_j \forall i \neq j$. Since $gcd(p_1, p_2) = 1$, we have $1 = m_1p_1 + m_2p_2$ for some $m_1, m_2 \ \in \ \mathbb{Z}_n$.
Let $x, y \in \mathbb{Z}_n$ such that $x \neq y$ and x is not adjacent to y. Then $x = x(m_1p_1 + m_2p_2)$ and $y = y(m_1p_1 + m_2p_2)$. Consider $w = -xm_1p_1 - ym_2p_2$.
Then, $x + w = m_2p_2(x - y)$ and $y + w = m_1p_1(y - x)$. Therefore, $p_2 \mid x + w$ and $p_1 \mid y + w$ and hence, both x and y are connected to w.
Hence $x - w - y$ and $diam(\mathcal{G}(\mathbb{Z}_n)) = 2$. Since this argument works for all $x, y \in \mathbb{Z}_n$, we conclude that $n \neq p^m \implies \mathcal{G}(\mathbb{Z}_n)$ is connected.
From Theorem 2.1 and this result, we conclude that $\mathcal{G}(\mathbb{Z}_n)$ is connected iff $n \neq p^m$, where p is prime. ∎

2.2 Results on Disconnected Graphs

Theorem 2.3. *Let $n = p^m$, where p is a prime number, and $m \in \mathbb{Z}^+$. The following is a characterization of the components of $\mathcal{G}(\mathbb{Z}_n)$:*

1. *If $p = 2$. Then $\mathcal{G}(\mathbb{Z}_{2^m})$ is a union of two (complete) $K_{p^{m-1}}$ components.*
2. *If $p \neq 2$:*
   There are $\frac{p+1}{2}$ components of $\mathcal{G}(\mathbb{Z}_{p^m})$, namely:
   (a) *1 Complete Graph: $\mathbb{K}_{p^{m-1}}$.*
   (b) *$\frac{p-1}{2}$ Complete Bipartite Graphs $\mathbb{K}_{p^{m-1},p^{m-1}}$.*

Proof. 1. If $p = 2$

(a) The graph $\mathcal{G}(\mathbb{Z}_{2^m})$ has exactly 2^m vertices. In the quotient ring $\mathbb{Z}_{2^m}/(2)$, where (2) is the principal ideal generated by 2, let $A = (2)$ and $B = 1 + (2)$. We prove that the subgraphs of $\mathcal{G}(\mathbb{Z}_{2^m})$ induced on A and B are the components of this graph, and are complete graphs $\mathbb{K}_{2^{m-1}}$.
Note that $a_i = 2k_i \ \forall \ a_i \in A$ and $b_i = 2k_i + 1 \ \forall \ b_i \in B$, where $k_i \in \mathbb{Z}^+$.
Clearly, a_i is connected to $a_j \ \forall \ i, j$ as $a_i + a_j = 2k_i + 2k_j = 2(k_i + k_j) = 2k$ is divisible by 2. Therefore, the subgraph of $\mathcal{G}(\mathbb{Z}_n)$ induced on A, $\mathcal{G}(A)$, forms a complete graph.
Similarly, b_i is connected to $b_j \ \forall \ i, j$ as $b_i + b_j = (2k_i + 1) + (2k_j + 1) = 2(k_i + k_j + 1)$ is divisible by 2. Therefore, the subgraph of $\mathcal{G}(\mathbb{Z}_n)$ induced on B, $\mathcal{G}(B)$, forms a complete graph.
Further, a_i is not connected to b_j for any i, j as $a_i + b_j = 2k_i + (2k_i + 1) = 2(2k_i) + 1$ is not divisible by 2.
Therefore A and B form the components of $\mathcal{G}(\mathbb{Z}_n)$.
Therefore G(A) $\cong \mathcal{G}(B) \cong \mathbb{K}_{2^{m-1}}$.

2. If $p \neq 2$

(a) We show that the set of zero divisors of $\mathbb{Z}_n$, denoted $\mathcal{Z}(\mathbb{Z}_n)$ forms the complete graph $\mathbb{K}_{p^{m-1}}$. Since $n = p^m$, the only zero divisors are $\mathcal{Z}(\mathbb{Z}_n) = (p) = \{0, p, 2p, 3p, ..., n-p\}$. Since $|(p)| = \frac{p^m}{p} = p^{m-1}$ and all the elements of (p) are connected to each other as $m_1 p + m_2 p = (m_1 + m_2)p$ is divisible by p, $\mathcal{Z}(\mathbb{Z}_n)$ forms the vertex set of the complete graph $\mathbb{K}_{p^{m-1}}$.

(b) We prove that the remaining $\frac{p-1}{2}$ components are isomorphic subgraphs which themselves are complete bipartite graphs $\mathbb{K}_{p^{m-1},p^{m-1}}$.
Consider the quotient ring $D_1 = \mathbb{Z}_{p^m}/(p)$ with $\frac{p^m}{p^{m-1}} = p$ elements. Consider also the modulo p equivalence relation on the set $\mathbb{Z}_{p^m}$. Then, $(p) = [0]$ and all the elements of D_1 uniquely correspond to one of the p equivalence classes. This partitions $\mathbb{Z}_{p^m}$ into p cosets.
We show that for every coset V_1, there exists a coset V_2 such that each element of V_1 is connected to each element of V_2, and that no element of V_1 is connected to any other element of any other coset.
Since $V_1 = a + (p)$ for some $a \in \mathbb{Z}_{p^m}$, choose $V_2 = -a + (p)$, where $-a$ is the additive inverse of a in the ring $\mathbb{Z}_{p^m}$. Then, since $V_1 + V_2 = 0$ in D_1, it is clear that $\forall a_1 \in V_1$ and $\forall a_2 \in V_2$, $a_1 + a_2 \in \ (p)$ and hence a_1 is connected to a_2.
Since the additive inverse is unique for all elements in the quotient ring D_1, no other coset when added to V_1 yields an element in (p). Since p is the only prime factor of n, no element of V_1 is connected to any other element of any coset except $V_2 = -V_1$. Therefore, the sets V_1 and V_2 form the parts of the bipartite graph.
Therefore, the cosets can be paired up when connected to each other. Since $|D_1| = p \neq 2$, no element is the additive inverse of itself except for the identity element. This can be proved by contradiction. Assume $\exists \ x \neq 0 \in D_1$ such that $x = -x$. Then, $2x = 0$ in $\mathbb{Z}_p$ since $2 \nmid p$, we must conclude that $x = 0$. This is a contradiction.
Therefore, based on the above pairing mechanism, (p) is paired with itself, while the remaining $p-1$ elements are paired distinctly and uniquely. This yields $\frac{p-1}{2}$ components, each of which form a bipartite graph. Since the cosets of (p) have the same cardinality, these bipartite graphs are isomorphic to $\mathbb{K}_{p^{m-1},p^{m-1}}$ and hence isomorphic to each other.

■

Theorem 2.4. *Let $n = p^m$. If $x \in V_{\mathcal{G}(\mathbb{Z}_n)}$, then:*

1. *If $p = 2$*
   $deg(x) = 2^{m-1} - 1 \ \forall \ x \in V_{\mathcal{G}(\mathbb{Z}_n)}$

2. *If $p \neq 2$*
   $deg(x) = p^{m-1} - 1 \ \forall \ x \in \ (p)$
   $deg(x) = p^{m-1} \ \forall \ x \notin \ (p)$

Proof. 1. If $p = 2$, then by Theorem 2.3, we have two isomorphic complete subgraphs $\mathbb{K}_{2^{m-1}}$ as the components. Pick any x in either component. Since the graph is complete, this vertex is connected to all other vertices in the component. Therefore, $deg(x) = 2^{m-1} - 1$.

2. If $p \neq 2$, each element of (p) is connected to all elements of (p) (Complete Graph). By the same reasoning as item (1) above, $deg(x) = p^{m-1} - 1$.
   For all vertices outside (p), the vertex belongs to the bipartite graph $\mathbb{K}_{p^{m-1},p^{m-1}}$. Since no vertex here is connected to itself, we have $deg(x) = p^{m-1}$.

■

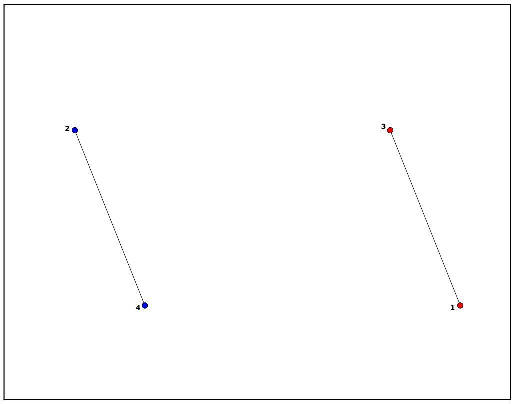
Theorem 2.5. *If $\mathcal{G}(\mathbb{Z}_n)$ is disconnected, it is planar iff n is prime, or $n = 4$ or $n = 8$.*

Proof. Since the graph is disconnected, we have $n = p^m$ for some prime p. If $m = 1$, the graph is always planar as $deg(a) = 1 \ \forall \ a \in \mathbb{Z}_p^*$ and $deg(p) = 0$.

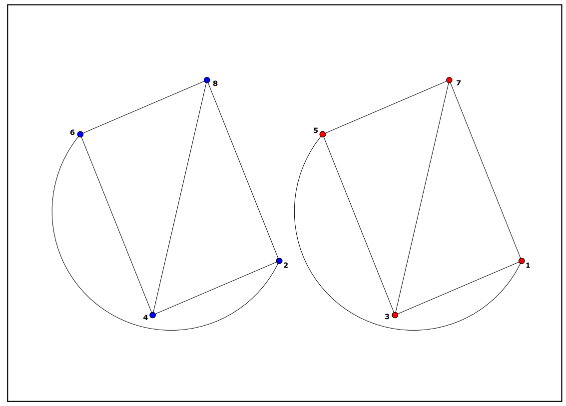
If $p = 2$, it is clear from Figure 1 that the graphs with $V_D = \mathbb{Z}_4$, $\mathbb{Z}_8$ are planar. But, for $n = 2^m$, $m \geq 4$, we have the subgraph with vertices $\{2, 4, 6, 8, 10\}$ which is isomorphic to the complete graph $\mathbb{K}_5$. Hence the graph is not planar.

If $p = 3$, then the graph with $V_D = \mathbb{Z}_9$ is not planar as it contains the subgraph isomorphic to $\mathbb{K}_{3,3}$. Here, the parts are $V_1 = \{1, 4, 7\}$ and $V_2 = \{2, 5, 8\}$. This leaves the case when $n = 3^m$ for $m > 2$. But all such graphs contain $\mathbb{K}_5$ as a subgraph with $V = \{3, 6, 9, 12, 15\}$.

Finally, if $p > 3$ and $m > 1$, then the graph with $V_D = \mathbb{Z}_{p^m}$ is never planar because the subgraph with vertices $\{p, 2p, 3p, 4p, 5p\}$ is isomorphic to $\mathbb{K}_5$ as $5p \leq p^m \ \forall \ m \geq 2$.



(a) $\mathcal{G}(\mathbb{Z}_4)$ is planar



(b) $\mathcal{G}(\mathbb{Z}_8)$ is planar

Figure 1: Disconnected Planar Graphs

■

Theorem 2.6. *If $n = p^m$ (p is prime and m is a positive integer), then $\mathcal{UG}(\mathbb{Z}_n)$ is a regular graph.*

Proof. Recall that $\mathcal{UG}(\mathbb{Z}_n)$ is the induced subgraph on the unit elements of the ring Z_n. ■

Theorem 2.7. *Let $n = p^\alpha$. Then $\mathcal{UG}(\mathbb{Z}_n)$ is connected iff $p = 2$ or $p = 3$.*

Proof. If $p = 2$, then by the proof of Theorem 2.3(1), $\mathcal{UG}(\mathbb{Z}_n)$ is $\mathbb{K}_{2^{m-1}}$.

If $p = 3$, then by Theorem 2.3(2)(b) and its proof, we have $\mathcal{UG}(\mathbb{Z}_n)$ is $\mathbb{K}_{p^{m-1},p^{m-1}}$.
If $p \neq 2$ and $p \neq 3$, then from Theorem 2.3, $\exists$ $\frac{p-1}{2}$ Bipartite graphs $\mathbb{K}_{p^{m-1},p^{m-1}}$. Since $p > 3$, we have $\frac{p-1}{2} > 1$, and therefore $\mathcal{UG}(\mathbb{Z}_n)$ is not connected. ■

2.3 Results on Connected Graphs

This section deals with connected graphs, $\mathcal{G}(\mathbb{Z}_n)$. Here, the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ and $k \geq 2$.

Theorem 2.8. *Let $a \in \mathbb{Z}_n$.*

1. *If n is even, $deg(a) = n - \phi(n) - 1$.*
2. *If n is odd, $deg(a) = \begin{cases} n - \phi(n) & a \in \mathcal{U}(\mathbb{Z}_n) \\ n - \phi(n) - 1 & a \in \mathcal{Z}(\mathbb{Z}_n) \end{cases}$*

Proof. 1. **Case I: n is Even**
Let $a \in \mathbb{Z}_n$. a is connected to b iff $a + b \in \mathcal{Z}(\mathbb{Z}_n)$. In other words, a is connected to b iff $b = x - a$ and $b \neq a$ for some $x \in \mathcal{Z}(\mathbb{Z}_n)$. Since $|\mathcal{Z}(\mathbb{Z}_n)| = n - \phi(n)$, and since $a + a = 2a \in \mathcal{Z}(\mathbb{Z}_n)$ $\forall a \in \mathbb{Z}_n$, we conclude that $deg(a) = n - \phi(n) - 1$ $\forall a \in \mathbb{Z}_n$.

2. **Case II:** n **is Odd**
   We use the same line of reasoning as in Case I. Note that the following condition still holds true: a is connected to b iff $b = x - a$ and $b \neq a$ for some $x \in \mathcal{Z}(\mathbb{Z}_n)$.

   (a) If $a \in \mathcal{U}(\mathbb{Z}_n)$, then $x - a \neq a\ \forall x \in \mathcal{Z}(\mathbb{Z}_n)$. This is true as $\gcd(2, n) = 1$ and $\gcd(a, n) = 1$ implies $gcd(2a, n) = 1$, and hence, $a + a \in \mathcal{U}(\mathbb{Z}_n)$. Thus, $deg(a) = n - \phi(n)$.

   (b) If $a \in \mathcal{Z}(\mathbb{Z}_n)$, then $a + a \in \mathcal{Z}(\mathbb{Z}_n)$. Thus, $\exists x \in \mathcal{Z}(\mathbb{Z}_n)$ such that $a = x - a$. Accounting for this, we conclude that $deg(a) = n - \phi(n) - 1$.

■

Corollary 2.8.1. *$\mathcal{G}(\mathbb{Z}_n)$ is regular iff n is even.*

Theorem 2.9. *The girth of $\mathcal{G}(\mathbb{Z}_n)$, $g(\mathcal{G}(\mathbb{Z}_n)) = 3$.*

Proof. $g(\mathcal{G}(\mathbb{Z}_n)) \neq 1$ as $\mathcal{G}(\mathbb{Z}_n)$ has no loops.
$g(\mathcal{G}(\mathbb{Z}_n)) \neq 2$ as $\mathcal{G}(\mathbb{Z}_n)$ has no multiedges.
Hence, $g(\mathcal{G}(\mathbb{Z}_n))$ is atleast 3.

Since $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, with $k \geq 2$, we have $p_2 \geq 3$. Now consider the set $A = \{p_1, 2p_1, 3p_1\}$. Clearly, $A \subset \mathbb{Z}_n$. But the induced subgraph on A is a cycle of length 3.

Hence, $g(\mathcal{G}(\mathbb{Z}_n)) = 3$. ■

Corollary 2.9.1. *The girth of $\mathcal{ZG}(\mathbb{Z}_n)$, $g(\mathcal{ZG}(\mathbb{Z}_n))$ is 3.*

Theorem 2.10. *Let n be odd and write $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}, k \geq 2$ and $p_1 < p_2 < ... < p_k$. Then, $\exists a, b \in \mathcal{U}(\mathbb{Z}_n)$ such that a is not adjacent to b.*

Proof. Assume $p_1 \neq 3$ and let $a \in \mathcal{U}(\mathbb{Z}_n)$. Then $\exists b = 2a \in \mathcal{U}(\mathbb{Z}_n)$ and hence a and b are not adjacent.

Now assume $p_1 = 3$ and let $a, b \in \mathcal{U}(\mathbb{Z}_n)$. If $a \pmod 3 = b \pmod 3$, then it is clear that a and b are not adjacent. Hence we may assume that $a = 1 \pmod 3$ and $b = 2 \pmod 3$. Then $2a \in \mathcal{U}(\mathbb{Z}_n)$ and hence $2a$ and b are not adjacent. ■

Theorem 2.11. *The induced subgraph of units, $\mathcal{UG}(\mathbb{Z}_n)$, is a connected graph with diameter,*

$$diam(\mathcal{UG}(\mathbb{Z}_n)) = \begin{cases} 1, & \text{n is even} \\ 2, & \text{n is odd} \end{cases}$$

Proof. **Case I:** n is even
Since every unit is an odd number, the sum of any two units is even. Thus, $\mathcal{G}(\mathbb{Z}_n)$ is isomorphic to $\mathbb{K}_{\phi(n)}$ where $\phi(n) = |\mathcal{U}(\mathbb{Z}_n)|$.

Case II: n is odd
Let $a, b \in \mathcal{U}(\mathbb{Z}_n)$ and assume a and b are not adjacent. Note that such a,b exist by Theorem 2.10. It is clear that $p_i \nmid a$ and $p_i \nmid b\ \forall 1 \leq i \leq k$. Hence, $n - a, n - b \in \mathcal{U}(\mathbb{Z}_n)$. Let $m = \frac{n}{p_k^{\alpha_k}}$, and note that $\gcd(m, p_k^{\alpha_k}) = 1$.
By the Chinese Remainder Theorem, $\exists a, c \in \mathbb{Z}_n$ such that $c \cong n - a \pmod m$ and $c \cong n - b$ (mod $p_k^{\alpha_k}$). Since $n - a, n - b \in \mathcal{U}(\mathbb{Z}_n)$, we conclude that $c \in \mathcal{U}(\mathbb{Z}_n)$. It is clear that $m \mid (c + a)$, in particular, $p_1 \mid (c + a)$ and $p_k \mid (c + b)$. Thus we have the path $a - c - b$, and the diameter of $\mathcal{UG}(\mathbb{Z}_n)$ is 2. ■

Theorem 2.12. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ where $k \geq 2$. Then $\mathcal{UG}(\mathbb{Z}_n)$ is connected iff $\mathcal{G}(\mathbb{Z}_n)$ is connected.*

Proof. This follows directly from Theorem 2.7 and Theorem 2.11. ∎

Theorem 2.13. *$\mathcal{UG}(\mathbb{Z}_n)$ is a regular graph. Therefore, the degree of each element in $\mathcal{UG}(\mathbb{Z}_n)$ is the same.*

Proof. Let $f : \mathbb{Z}_n \to \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times ... \times \mathbb{Z}_{p_k}$ be a surjective map such that $f(a) = (a \pmod{p_1}, a \pmod{p_2}, ..., a \pmod{p_k}) = (a_1, a_2, ..., a_k)$. Let $a \in \mathcal{U}(\mathbb{Z}_n)$ so that $f(a) = (a_1, a_2, ..., a_k)$. Clearly, $a_i \neq 0 \; \forall i$. Furthermore, we know that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} \implies |\mathcal{U}(\mathbb{Z}_n)| = \phi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right).$$

Clearly, a is not connected to another unit b iff $f(a+b) = (c_1, c_2, ..., c_k) \implies c_i \neq 0 \; \forall i$. Therefore, if $b \in \mathcal{U}(\mathbb{Z}_n)$ and a and b are not adjacent, then $f(b) = (b_1, b_2, ..., b_k)$ where $b_i \neq 0 \; \forall i$ and $b_i \neq p_i - a_i \; \forall i$. Thus we have $m = \prod_{i=1}^{k}(p_i - 2)p_i^{\alpha_i - 1}$ units not connected to a. Therefore,

$$deg(a) = \gamma(n) = \phi(n) - m = \prod_{i=1}^{k}(p_i - 1)p_i^{\alpha_i - 1} - \prod_{i=1}^{k}(p_i - 2)p_i^{\alpha_i - 1} = \left[\prod_{i=1}^{k} p_i^{\alpha_i - 1}\right]\left[\prod_{i=1}^{k}(p_i - 1) - \prod_{i=1}^{k}(p_i - 2)\right].$$

Since this number is independent of a, the same argument holds for all units and we conclude that the degree of each unit is the same in $\mathcal{UG}(\mathbb{Z}_n)$.

Note also that if n is even, then $m = 0$. This is clear from the definition of m, as well as from the fact that $\mathcal{UG}(\mathbb{Z}_n)$ is a complete graph when n is even. We account for the fact that a is not connected to itself when n is even, and hence,

$$deg(a) \text{ in } \mathcal{UG}(\mathbb{Z}_n) = \begin{cases} \phi(n) - 1, & \text{n is even} \\ \phi(n) - m, & \text{n is odd} \end{cases}$$

∎

Corollary 2.13.1. *Each unit element is adjacent to the same number of zero divisors.*

Proof. Let $a \in \mathcal{U}(\mathbb{Z}_n)$, and $\delta(a)$ represent the number of zero divisors that a is adjacent to. Hence, $\delta(a) = |A|$, where $A = \{z \in \mathcal{Z}(\mathbb{Z}_n) \mid a \text{ is adjacent to } z\}$.

Let $a_1 = deg(a)$ in $\mathcal{G}(\mathbb{Z}_n)$, and $a_2 = deg(a)$ in $\mathcal{UG}(\mathbb{Z}_n)$. Since both a_1 and a_2 are independent of the choice of a, the claim follows immediately.

In particular,

$$\delta(a) = a_1 - a_2 = \begin{cases} (n - \phi(n) - 1) - (\phi(n) - 1) = n - 2\phi(n), & \text{n is even} \\ (n - \phi(n)) - (\phi(n) - m) = n - 2\phi(n) + m, & \text{n is odd} \end{cases}$$

where m is as defined in Theorem 2.13. Substituting these values gives:

$$\delta(a) = \begin{cases} \left[\prod\limits_{i=1}^{k} p_i^{\alpha_i - 1}\right]\left[\prod\limits_{i=1}^{k} p_i - 2\prod\limits_{i=1}^{k}(p_i - 1)\right], & \text{n is even} \\ \left[\prod\limits_{i=1}^{k} p_i^{\alpha_i - 1}\right]\left[\prod\limits_{i=1}^{k} p_i - 2\prod\limits_{i=1}^{k}(p_i - 1) + \prod\limits_{i=1}^{k}(p_i - 2)\right], & \text{n is odd} \end{cases},$$

which is independent of a, provided that $a \in \mathcal{U}(\mathbb{Z}_n)$. Thus, we conclude that each unit element is adjacent to the same numbr of zero divisors. ∎

Theorem 2.14. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ with $k \geq 2$. $\mathcal{ZG}(\mathbb{Z}_n)$ is not regular, but there are at most $2^k - 1$ choices for the degree of $a \in \mathcal{Z}(\mathbb{Z}_n)$.*

Proof. Consider the map f such that $f(a) = (a_1, ..., a_k)$ where $a_i = a \pmod{p_i}$. We partition $\mathbb{Z}_n$ into 2^k classes as follows.

Each class is defined by the number and position a_j such that $a_j = 0$. For example, if only p_2 and p_k divide a, but no other prime factor of n does, then $f(a) = (a_1, 0, a_3, ..., a_{k-1}, 0)$ where $a_i \neq 0\ \forall i$. We say that $a \in$ the $\{1, 0, 1, ..., 1, 0\}$ class.

Clearly, this is a base 2 representation which tells exactly which prime factors divide a.

Vertices in class $\{1, 1, ..., 1\}$ are the units and hence do not belong to $\mathcal{ZG}(\mathbb{Z}_n)$. The claim is that all the vertices in a given class have the same degree.

Let x be an arbitrary element from a given class. Then, $f(x) = (x_1, x_2, ..., x_k)$. Since we know the class of x, we know all j such that $x_j = 0$. We illustrate the remainder of this proof by assuming that the given class is $\{0, 0, 1, 1, ..., 1\}$ without loss of generality.

Since $f(x) = (0, 0, x_3, ..., x_k)\ \forall x$ in the class, and since x is connected to $y \in \mathcal{Z}(\mathbb{Z}_n)$ iff $f(y) = (y_1, ..., y_k)$ has $y_i = 0$ for some $1 \leq i \leq k$ and $y_j = p_j - x_j$ for some $1 \leq j \leq k$. However, the number of such y is fixed and independent of the choice of $x_j, j \geq 3$ provided $x_j \neq 0\ \forall j \geq 3$. But this is exactly the definition of the class in which x belongs, and thus the degree of x is the same for all x in the given class.

Since different classes can have the same degree and there are $2^k - 1$ classes (accounting for the class of units), we conclude that $a \in \mathcal{Z}(\mathbb{Z}_n) \implies deg(a) \in B$, where $|B| \leq 2^k - 1$.

Remark: The exact degree for each class, and hence the set B, can be calculated using combinatorial calculations. However, such a procedure is not pursued in this thesis. ∎

Theorem 2.15. *If $\mathcal{G}(\mathbb{Z}_n)$ is connected, $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ with $p_1 < p_2 < ... < p_k$, the dominating number is p_1. Any complete reduced system of residues* $\pmod{p_1}$ *forms a dominating set, one of which is $D = \mathbb{Z}_{p_1}$.*

Proof. Let $m \in \mathbb{Z}_n$. Then $m = ap_1 + b$ for some positive integer a and for some $b \in D$. Since $y = p_1 - b \in D$, we have $m + y = (a+1)p_1$ and thus $p_1 \mid m + y$. Hence, D is a dominating set.

Now we show that the dominating number is $|D| = p_1$. Assume that $F = a_1, ..., a_i$ is a dominating set. We show that $|F| \geq p_1$. Deny. Hence $|F| < p_1$.

Let $f : \mathbb{Z}_n \to \mathbb{Z}_1 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_k$ such that $f(x) = (x \pmod{p_1}, x \pmod{p_2}, ..., x \pmod{p_k})\ \forall\, x \in \mathbb{Z}_n$. It is clear that f is a surjective ring-homomorphism. Hence $f(a_j) = (c_{j1}, c_{j2}, ..., c_{jk})\ \forall\ a_j \in F,\ 1 \leq j \leq i$.

For each $1 \leq h \leq k$, let $F_h = c_{1h}, c_{2h}, ..., c_{ih}$. Then $F_h \subset \mathbb{Z}_{p_h}\ \forall\ 1 \leq h \leq k$. Since $|F| < p_1$ (i.e., $i < p_1$) and $p_1 < p_j\ \forall\ 2 \leq j \leq k$, we conclude that $F_h \neq \mathbb{Z}_{p_h}$, for each $1 \leq h \leq k$. Thus, $\forall\ 1 \leq h \leq k,\ \exists\ c_h \in \mathbb{Z}_{p_h} \setminus F_h$.

Now let $W = (p_1 - c_1, p_2 - c_2, ..., p_k - c_k) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times ... \times \mathbb{Z}_{p_k}$. Since $c_h \notin F_h\ \forall\ 1 \leq h \leq k$, we conclude that $\forall\ j, 1 \leq j \leq i$, and $\forall\ h, 1 \leq h \leq k$, we have $p_h - c_h + c_{jh} \neq 0$ in $\mathbb{Z}_{p_h}$. Since f is surjective, $\exists\ T \in \mathbb{Z}_n$ such that $f(T) = W$. We show that $p_h \nmid (T + a_j)\ \forall\ a_j \in F$, where $1 \leq h \leq k$.

Assume that for some $1 \leq h \leq k$ and for some $1 \leq j \leq i$, we have $p_h \mid (T + a_j)$. Hence, $f(T + a_j) = f(T) + f(a_j) = W + f(a_j) = (p_1 - c_1 + c_{j1}, ..., p_h - c_h + c_{jh}) = (0, ..., p_k - c_k + c_{jk})$. This is impossible since $p_h - c_h + c_{jh} \neq 0 \in \mathbb{Z}_{p_h}$. Thus, our denial is invalid, and hence $|F| \geq p_1$. Since D is a dominating set and $|D| = p_1$, we conclude that the dominating number is p_1.

Remark: Given an arbitrary set $A \subset \mathbb{Z}_n$, the proof provides an algorithm to determine all $x \in \mathbb{Z}_n$ such that x is not adjacent to a $\forall a \in A$. This is presented in Section 4. ■

Theorem 2.16. *Maximal ideals inside the ring $\mathbb{Z}_n$ manifest as induced complete subgraphs in $\mathcal{G}(\mathbb{Z}_n)$.*

Proof. Since $\mathbb{Z}_n$ is a principal ideal domain (PID), any ideal is of the form (k) where $k \in \mathbb{Z}_n$. For the ideal to be maximal, $k = p_i$, where $p_i \mid n$. Hence $(p_i) = \{p_i z | z \in \mathbb{Z}_n\}$.

Choose any $a, b \in (p_i)$ (not necessarily distinct). Since $a + b \in (p_i)$ as (p_i) is closed under addition, we conclude that $p_i \mid (a + b)$ and hence any two elements in (p_i) are connected. Since $|(p_i)| = \frac{n}{p_i}$, we conclude that the induced subgraph with vertex set $V = (p_i)$ is isomorphic to the complete graph, $\mathbb{K}_{\frac{n}{p_i}}$. ■

Theorem 2.17. *$\mathcal{G}(\mathbb{Z}_6)$ is the only connected planar graph.*

Proof. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}, k \geq 2$ with $p_i < p_{i+1}$ $\forall$ $1 \leq i < k$, if $n \geq 5p_1$, then the subgraph with vertices $V = \{p, 2p, 3p, 4p, 5p\}$ is isomorphic to $\mathbb{K}_5$ and cannot be planar. Therefore, we solve for $n = \prod_{i=1}^{k} p_i^{\alpha_i} < 5p_1$. Since $k \geq 2$, it is clear that $p_i < 5$. The only value of n which satisfies this is $n = 6$, making it a candidate for being planar.

From Figure 2, it is clear that $\mathcal{G}(\mathbb{Z}_6)$ is planar, and the result follows.

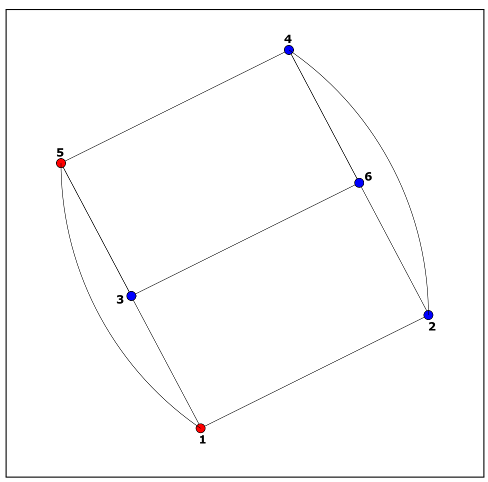


Figure 2: $\mathbb{Z}_6$ is the only connected planar graph.

■

2.4 Results on Traversability

Theorem 2.18. *If $\mathcal{G}(\mathbb{Z}_n)$ is connected, it has no Eulerian cycles and no Eulerian paths.*

Proof. A connected graph is said to have an Eulerian iff there exists a path such that each edge is traversed once and only once. Further, if this path starts and ends at the same vertex, it is an Eulerian cycle.

We show that $\mathcal{G}(\mathbb{Z}_n)$ has no Eulerian paths, and hence has no Eulerian cycles, by showing that the graph always has more than two vertices with odd degree. In this case, all edges cannot be traversed once and only once because of the following reasoning: One edge is used to enter a node and another is used to exit it, and hence, an odd degree at a vertex necessitates that the vertex is an end point. However, an Eulerian path can have atmost two end points.

Case I: n is Odd
Let $a \in \mathbb{Z}_n$. Recall that

$$deg(a) = \begin{cases} n - \phi(n) & a \in U(\mathbb{Z}_n) \\ n - \phi(n) - 1 & a \in Z(\mathbb{Z}_n) \end{cases}$$

Since the graph is connected and n is odd, we have $n \geq 15$. But $\forall$ odd $n > 2$, we have $\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = 2k$ for some $k \in \mathbb{Z}$ because $p_i - 1$ is always even when n is odd. Hence $n - \phi(n)$ is always odd, i.e. The degree of each unit is odd. Clearly, $1, 2, 4 \in U(\mathbb{Z}_n)$ $\forall$ $n \geq 15$ when n is odd. Therefore, we have atleast three vertices with odd degree, and no graph with this property can have an Eulerian path.
Case II: n is Even
Recall that $\deg(a) = n - \phi(n) - 1$ $\forall$ $a \in V_D$. Since the graph is connected, $\exists$ $p_i \mid n$ such that $p_i \neq 2$. Therefore, $\phi(n)$ is always even when $n > 2$. Hence, $n - \phi(n) - 1$ is always odd, and every node in the graph has an odd degree. Therefore, $\mathcal{G}(\mathbb{Z}_n)$ is never has an Eulerian path, and hence never has an Eulerian cycle. ∎

Theorem 2.19. *If n is even, $\mathcal{G}(\mathbb{Z}_n)$ is Hamiltonian.*

Proof. Recall that a graph is said to have a Hamiltonian path if there exists a path in the graph which traverses all the vertices once and only once. Further, if this path has the same initial and final vertex, it is said to be a Hamiltonian cycle.

From graph theory, it is known that for a graph $\mathcal{G}$, if $\forall x, y \in V_{\mathcal{G}}, deg(x) + deg(y) \geq n$, where $n = |V_{\mathcal{G}}|$, then $\mathcal{G}$ is Hamiltonian.

Since n is even, we know that $\mathcal{G}(\mathbb{Z}_n)$ is a regular graph with $deg(x) = n - \phi(n) - 1$ $\forall x \in \mathbb{Z}_n$. Hence, $a, b \in \mathbb{Z}_n \implies deg(a) + deg(b) = 2n - 2\phi(n) - 2$. We now show that $2n - 2\phi(n) - 2 \geq n$.

$$2n - 2\phi(n) - 2 \geq n \implies \phi(n) \leq \frac{n}{2} - 1$$

Since $n = 2^m l$ for some odd l, we use the multiplicative property of the $\phi(\cdot)$ function to write $\phi(n) = \phi(2^m l) = \phi(2^m)\phi(l) = 2^{m-1}\phi(l)$.

Now $n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} \implies l = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Hence,

$$
\begin{aligned}
\phi(n) = 2^{m-1}\phi(l) &= \frac{2^m}{2}\left[\prod_{i=1}^{k} p_i^{\alpha_i}\right]\left[\prod_{i=1}^{k}(\frac{p_i-1}{p_i})\right] \\
&= \frac{n}{2}\left[\prod_{i=1}^{k}(\frac{p_i-1}{p_i})\right] \\
&< \frac{n}{2} \\
&\leq \frac{n}{2} - 1
\end{aligned}
$$

Since this condition is sufficient for the graph to be Hamiltonian, we conclude that $\mathcal{G}(\mathbb{Z}_n)$ is Hamiltonian when n is even. ∎

Theorem 2.20. *$\mathcal{ZG}(\mathbb{Z}_n)$ is always Hamiltonian.*

Proof. We prove that $\mathcal{ZG}(\mathbb{Z}_n)$ always has a Hamiltonian cycle, and hence a Hamiltonian path, by constructing it.

We view $\mathcal{Z}(\mathbb{Z}_n)$ as the union of all prime ideals in $\mathbb{Z}_n$. Let the initial vertex of the path be p_1. Let $\{x_1, x_2, ..., x_r\}$ represent the path $x_1 - x_2 - ... - x_r$. Consider the following sequence of paths:

$$A_{1,1} : \{p_1, 2p_1, ..., n - p_1\} \setminus \bigcup_{j>1}(p_j) \ ; \ A_1 = A_{1,1} \cup \{p_1p_2\}$$

$$A_{2,1} : \{p_2, 2p_2, ..., (p_1 - 1)p_2, (p_1 + 1)p_2, ...(n - p_2)\} \ \setminus \bigcup_{j>2}(p_j) \ ; \ A_2 = A_{2,1} \cup \{p_2p_3\}$$

$$A_{3,1} : \{p_3, 2p_3, ..., (p_2 - 1)p_3, (p_2 + 1)p_3, ..., (n - p_3)\} \ \setminus \bigcup_{j>3}(p_j) \ ; A_3 = A_{3,1} \cup \{p_3p_4\}$$

$$\vdots$$

$$A_{k-1,1} : \{p_{k-1}, 2p_{k-1}, ..., (p_{k-2}-1)p_{k-1}, (p_{k-2}+1)p_{k-1}, ..., (n-p_{k-1})\} \setminus (p_k) \ ; \ A_{k-1} = A_{k-1,1} \cup \{p_{k-1}p_k\}$$

$$A_k : \{p_k, 2p_k, ..., (n - 1)p_k, 0\}$$

Since p_i divides all the vertices in A_i, each A_i is a valid path in $\mathcal{ZG}(\mathbb{Z}_n)$.

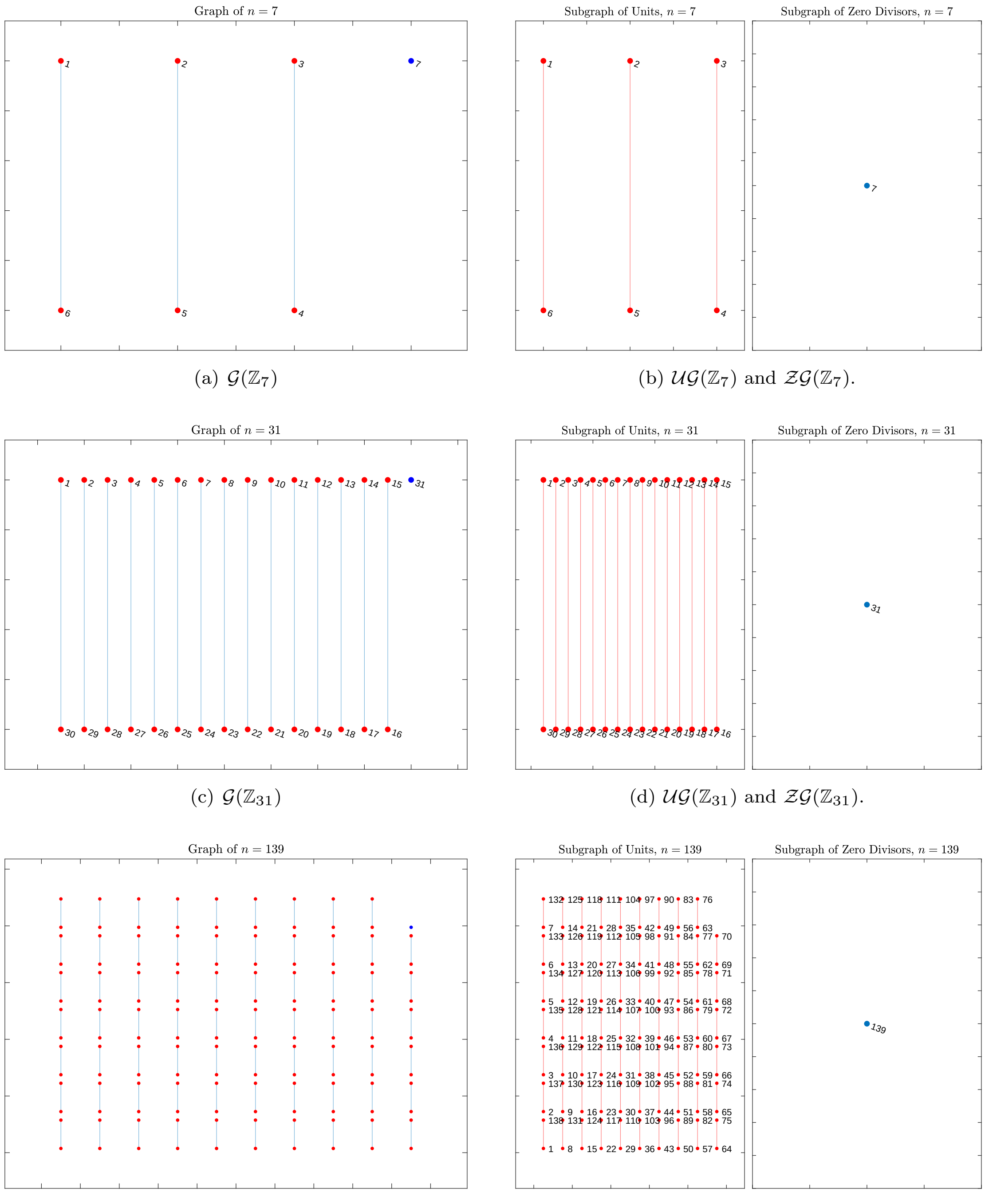
Further, $i \neq j \implies A_i$ and A_j do not share any common vertex.

Now, we concatenate these paths to define the path $A : A_1 - A_2 - ... - A_k$. This is possible as the final vertex of A_i is adjacent to the initial vertex of A_{i+1} $\forall 1 \leq i < k$, as $p_{i+1} \mid p_{i+1}p_i + p_{i+1}$. Further, A contains all the vertices in $\mathcal{Z}(\mathbb{Z}_n)$ once and only once.

Lastly, since the final vertex and initial vertex of A, namely 0 and p_1 are connected as $p_1 \mid 0+p_1$, we connect them to form the Hamiltonian cycle as required. ∎

3 Examples

3.1 $n = p$, where p is prime



(a) $\mathcal{G}(\mathbb{Z}_7)$

(b) $\mathcal{UG}(\mathbb{Z}_7)$ and $\mathcal{ZG}(\mathbb{Z}_7)$.

(c) $\mathcal{G}(\mathbb{Z}_{31})$

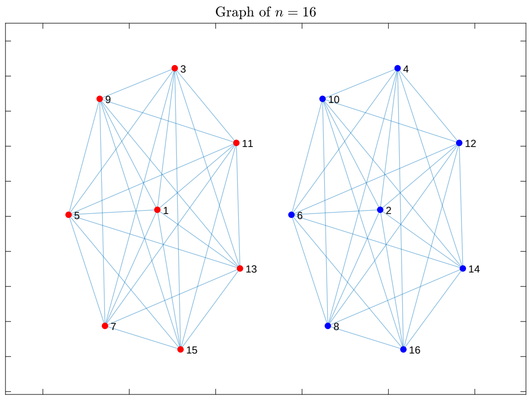
(d) $\mathcal{UG}(\mathbb{Z}_{31})$ and $\mathcal{ZG}(\mathbb{Z}_{31})$.

(e) $\mathcal{G}(\mathbb{Z}_{139})$

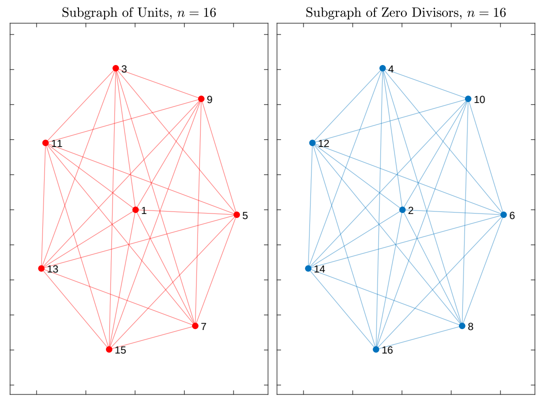
(f) $\mathcal{UG}(\mathbb{Z}_{139})$ and $\mathcal{ZG}(\mathbb{Z}_{139})$.

Figure 3: Examples of Disconnected Graphs with n prime.

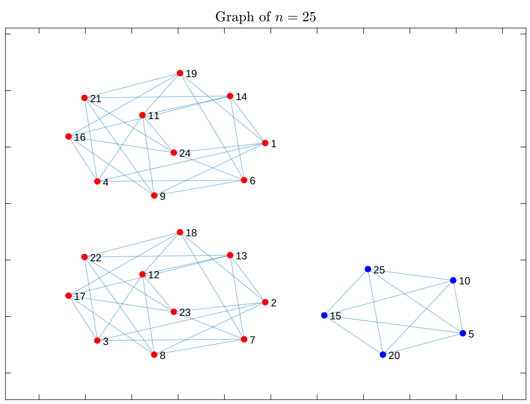
3.2 $n = p^m$, where $m > 1$



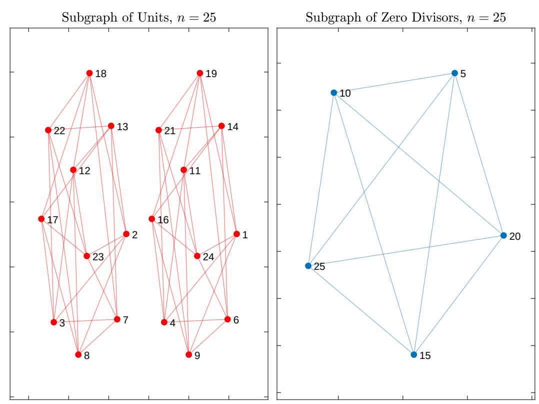
(a) $\mathcal{G}(\mathbb{Z}_{16})$



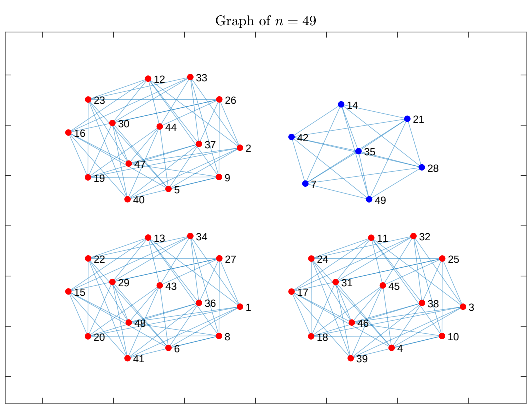
(b) $\mathcal{UG}(\mathbb{Z}_{16})$ and $\mathcal{ZG}(\mathbb{Z}_{16})$.



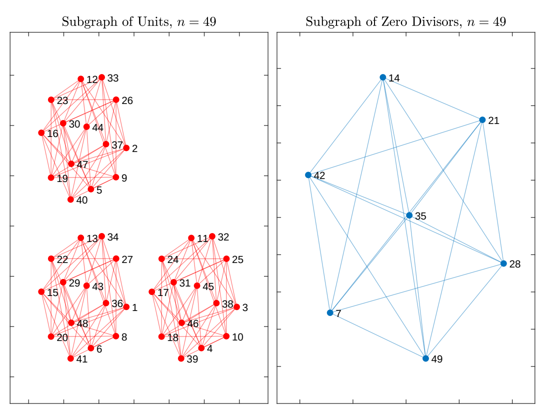
(c) $\mathcal{G}(\mathbb{Z}_25)$



(d) $\mathcal{UG}(\mathbb{Z}_{25})$ and $\mathcal{ZG}(\mathbb{Z}_{25})$.

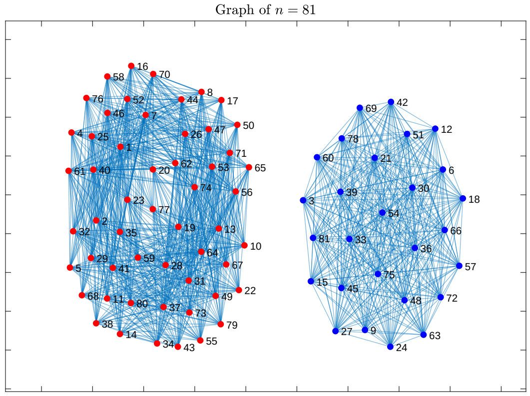


(e) $\mathcal{G}(\mathbb{Z}_{49})$

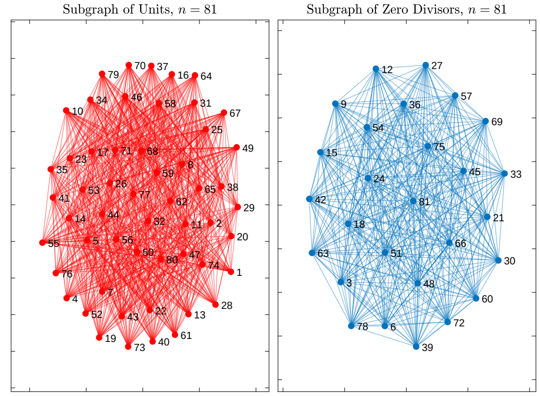


(f) $\mathcal{UG}(\mathbb{Z}_{49})$ and $\mathcal{ZG}(\mathbb{Z}_{49})$.

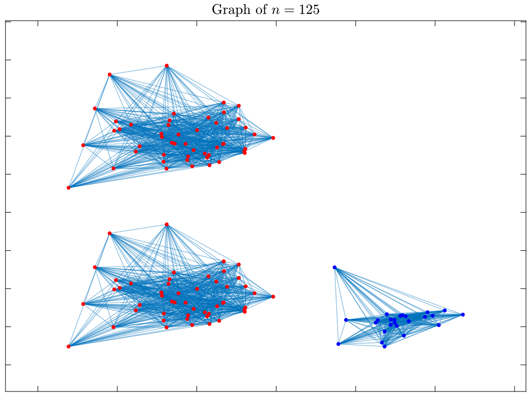
Figure 4: Examples of Disconnected Graphs with n not prime.



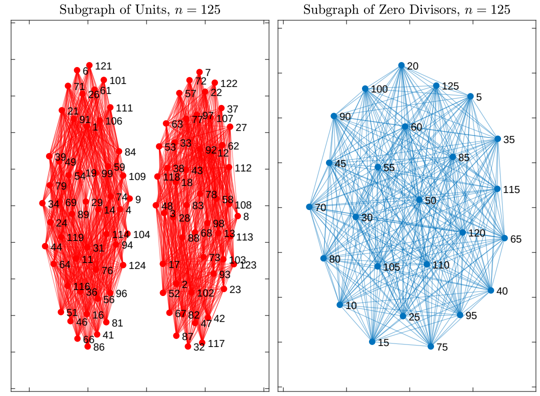
(a) $\mathcal{G}(\mathbb{Z}_{81})$



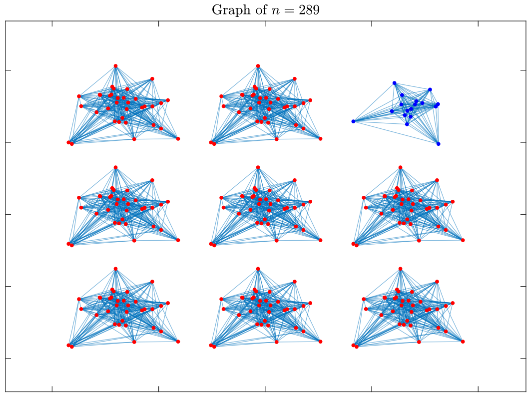
(b) $\mathcal{UG}(\mathbb{Z}_{81})$ and $\mathcal{ZG}(\mathbb{Z}_{81})$.



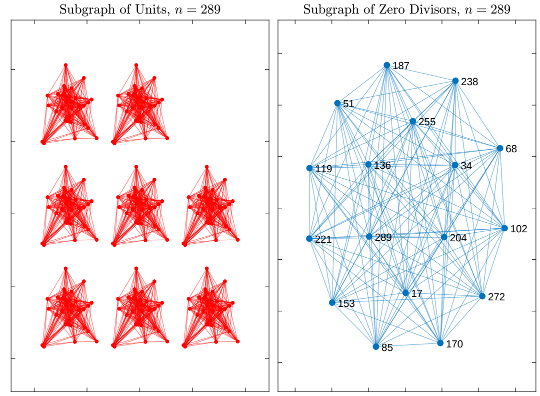
(c) $\mathcal{G}(\mathbb{Z}_{125})$



(d) $\mathcal{UG}(\mathbb{Z}_{125})$ and $\mathcal{ZG}(\mathbb{Z}_{125})$.



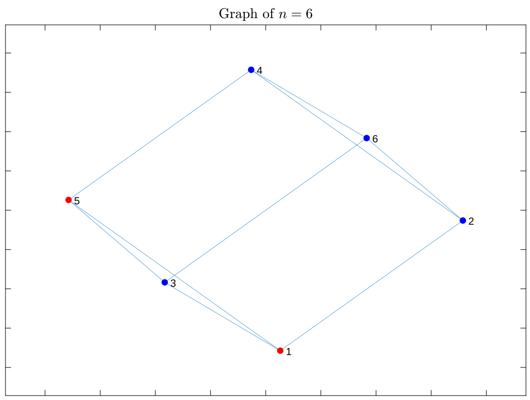
(e) $\mathcal{G}(\mathbb{Z}_{289})$



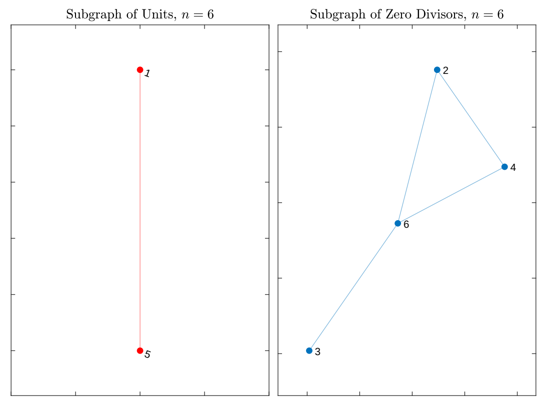
(f) $\mathcal{UG}(\mathbb{Z}_{289})$ and $\mathcal{ZG}(\mathbb{Z}_{289})$.

Figure 5: Examples of Disconnected Graphs with n not prime.

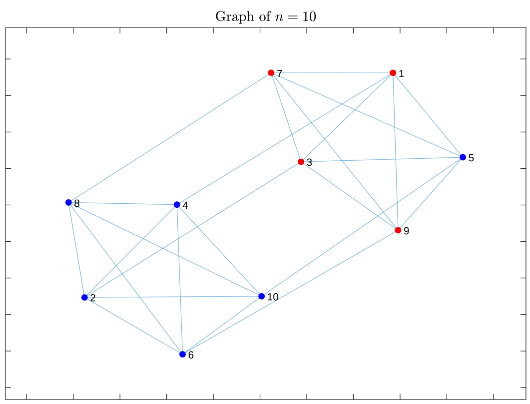
3.3 Connected Graphs: $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}, k \geq 2$



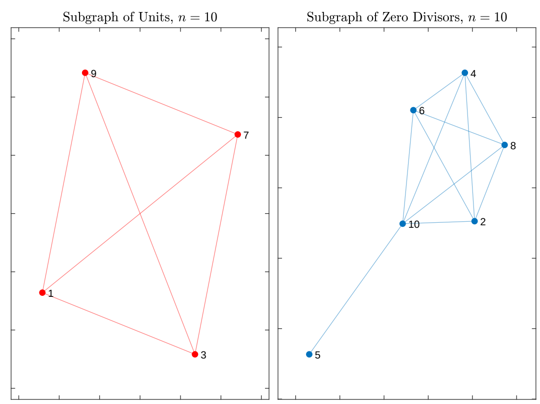
(a) $\mathcal{G}(\mathbb{Z}_6)$



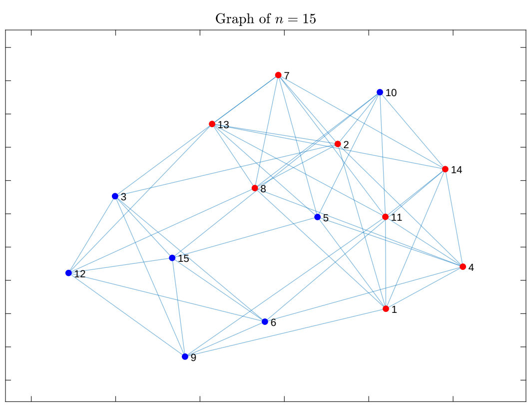
(b) $\mathcal{UG}(\mathbb{Z}_6)$ and $\mathcal{ZG}(\mathbb{Z}_6)$.



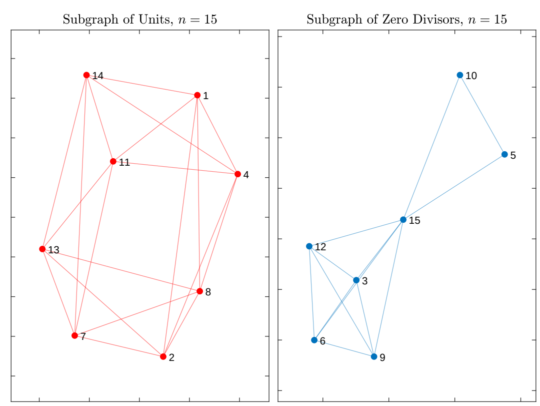
(c) $\mathcal{G}(\mathbb{Z}_{10})$



(d) $\mathcal{UG}(\mathbb{Z}_{10})$ and $\mathcal{ZG}(\mathbb{Z}_{10})$.

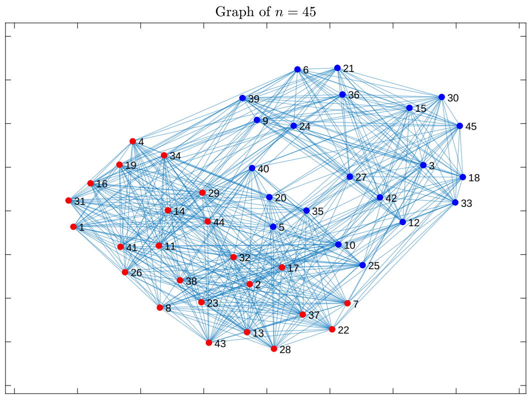


(e) $\mathcal{G}(\mathbb{Z}_{15})$

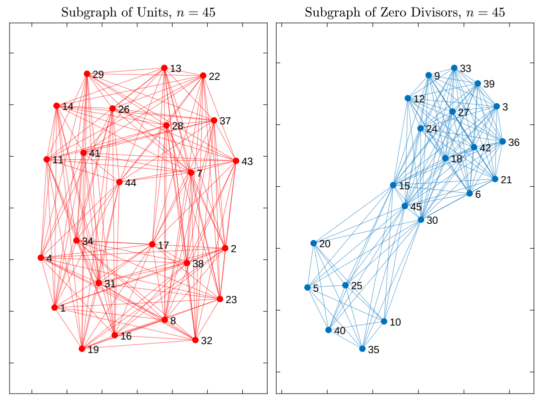


(f) $\mathcal{UG}(\mathbb{Z}_{15})$ and $\mathcal{ZG}(\mathbb{Z}_{15})$.

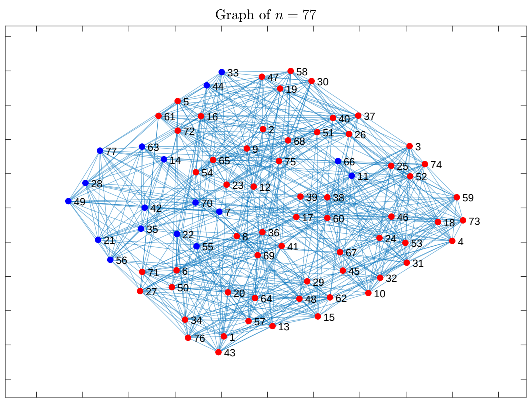
Figure 6: Examples of Connected Graphs.



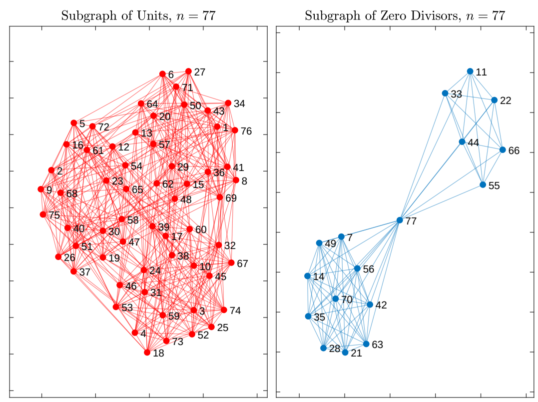
(a) $\mathcal{G}(\mathbb{Z}_{45})$



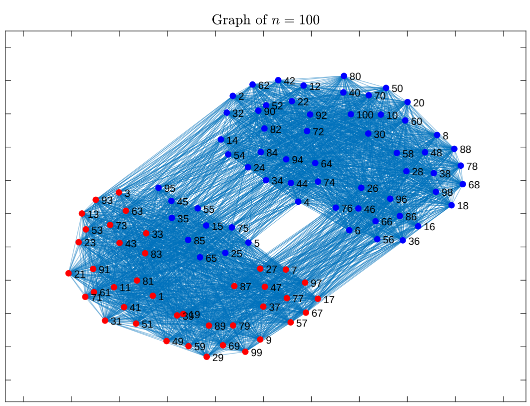
(b) $\mathcal{UG}(\mathbb{Z}_{45})$ and $\mathcal{ZG}(\mathbb{Z}_{45})$.



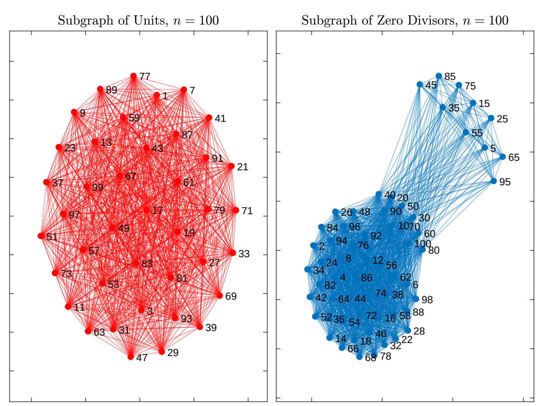
(c) $\mathcal{G}(\mathbb{Z}_{77})$



(d) $\mathcal{UG}(\mathbb{Z}_{77})$ and $\mathcal{ZG}(\mathbb{Z}_{77})$.

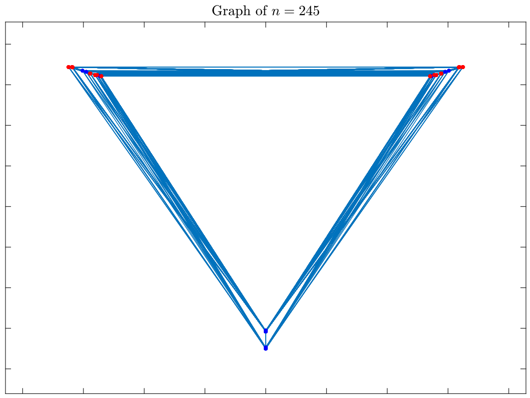


(e) $\mathcal{G}(\mathbb{Z}_{100})$

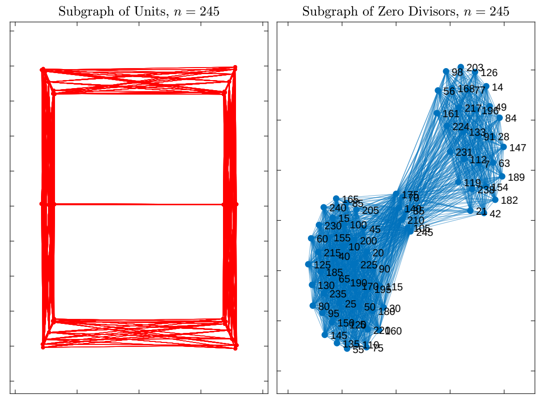


(f) $\mathcal{UG}(\mathbb{Z}_{100})$ and $\mathcal{ZG}(\mathbb{Z}_{100})$.

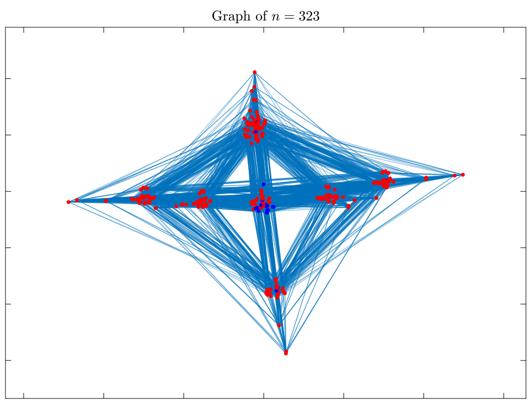
Figure 7: Examples of Connected Graphs.



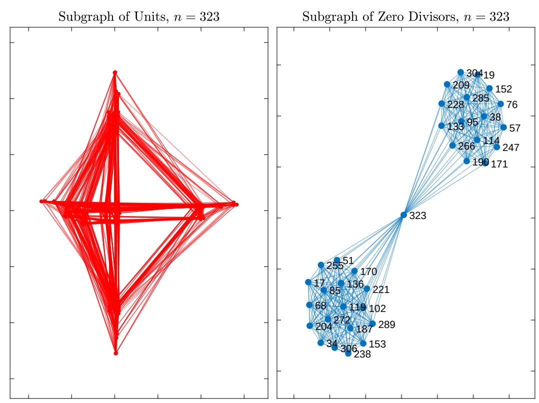
(a) $\mathcal{G}(\mathbb{Z}_{245})$



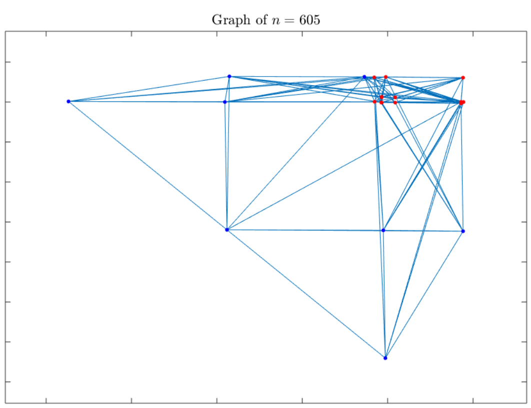
(b) $\mathcal{UG}(\mathbb{Z}_{245})$ and $\mathcal{ZG}(\mathbb{Z}_{245})$.



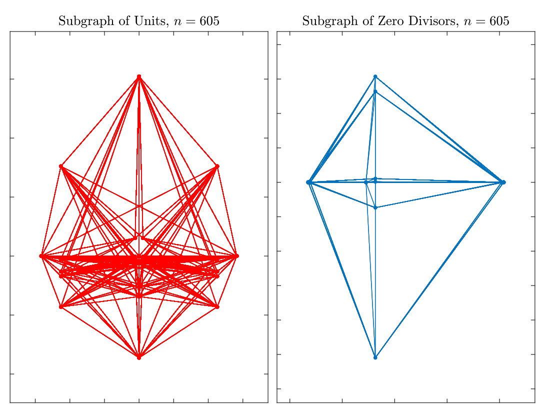
(c) $\mathcal{G}(\mathbb{Z}_{323})$



(d) $\mathcal{UG}(\mathbb{Z}_{323})$ and $\mathcal{ZG}(\mathbb{Z}_{323})$.



(e) $\mathcal{G}(\mathbb{Z}_{605})$



(f) $\mathcal{UG}(\mathbb{Z}_{605})$ and $\mathcal{ZG}(\mathbb{Z}_{605})$.

Figure 8: Examples of Connected Graphs.

4 Algorithms

This section contains proposed computer algorithms for the construction of the presented graphs, as well as the verification of certain properties presented in Section 2.

4.1 Algorithm to Construct $\mathcal{G}(\mathbb{Z}_n)$

Algorithm 1: Algorithm to construct $\mathcal{G}(\mathbb{Z}_n)$

```
   Inputs: n
   Steps :
1  Create n Nodes and label them 0, 1, 2, ..., n − 1;
2  Factorize n into its prime factors, P = {p_1, p_2, ..., p_k};
3  for i = 1, 2, ..., n do
4      for j = i + 1, i + 2, ..., n do
5          for k = p_1, p_2, ..., p_k do
6              if k | (i + j) then
7                  Add Edge between i and j
8              end
9          end
10     end
11 end
```

4.1.1 Description

Algorithm 1 provides a straightforward and simplistic method to construct $\mathcal{G}(\mathbb{Z}_n)$ as a pseudocode. The set of instructions intuitively relies on construction by definition.

The underlying principle is to first create n nodes and label them, after which the prime factorization of n is obtained. Then, each element a is tested with b to see if a prime factor p of n divides $a + b$. If this condition returns a logical true, then an edge is added to the graph.

In order to avoid duplication, and to ensure that $a - b$ and $b - a$ are not treated as separate edges, as well as to ensure that no self-loops are added, the condition that $b > a$ is also imposed as evident from Line 4 of the pseudocode. This is required to uphold the imposed condition that $\mathcal{G}(\mathbb{Z}_n)$ is undirected and simple.

4.2 Algorithm to Construct $\mathcal{UG}(\mathbb{Z}_n)$ and $\mathcal{ZG}(\mathbb{Z}_n)$

Algorithm 2: Algorithm to construct $\mathcal{UG}(\mathbb{Z}_n)$ and $\mathcal{ZG}(\mathbb{Z}_n)$

```
Inputs: n
Steps :
Create $n$ Nodes and label them $N = \{0, 1, 2, ..., n-1\}$;
Factorize $n$ into its prime factors, $P = \{p_1, p_2, ..., p_k\}$;
j = 1;
for $i = P$ do
    k = 1;
    while $k \times i \leq n$ do
        $Z(j) = k \times i$;
    end
end
Obtain set of Units as $U = N \setminus Z$;
for $i = Z$ do
    for $j = Z$ do
        for $k = p_1, p_2, ..., p_k$ do
            if $k \mid (i + j)$ then
                Add Edge between $i$ and $j$ in $\mathcal{ZG}(\mathbb{Z}_n)$
            end
        end
    end
end
for $i = U$ do
    for $j = U$ do
        for $k = p_1, p_2, ..., p_k$ do
            if $k \mid (i + j)$ then
                Add Edge between $i$ and $j$ in $\mathcal{UG}(\mathbb{Z}_n)$
            end
        end
    end
end
```

4.2.1 Description

The algorithm invokes the definitions of $\mathcal{UG}(\mathbb{Z}_n)$ and $\mathcal{ZG}(\mathbb{Z}_n)$ to construct them. The underlying principle is similar to Algorithm 1, but the vertex set is changed according to the graph of interest.

The set of zero divisors, Z is first created by finding all the multiples of the prime factors of n that are less than or equal to n. The set difference between $\mathbb{Z}_n$ and Z are then saved as the units, U. The condition for connectivity is then tested separately on both sets to construct $\mathcal{UG}(\mathbb{Z}_n)$ and $\mathcal{ZG}(\mathbb{Z}_n)$.

4.3 Algorithm to Find Hamiltonian Cycle in $\mathcal{ZG}(\mathbb{Z}_n)$

Algorithm 3: Algorithm to construct Hamiltonian cycle in $\mathcal{ZG}(\mathbb{Z}_n)$

Inputs: n
Steps :
1 Obtain prime factorization of n, $P = \{p_1, p_2, ..., p_k\}$;
2 Obtain set of zero divisors and $\mathcal{ZG}(\mathbb{Z}_n)$;
3 Set Initial Vertex as p_1;
4 Define $A_{1,1} = (p_1) \setminus \bigcup_{j>1}(p_j)$;
5 Define $A_1 = A_{1,1} \cup \{p_1 p_2\}$;
6 **for** $i = 2, 3, ..., k-1$ **do**
7 Define $A_{i,1} = \{p_i, 2p_i, ..., (p_{i-1} - 1)p_i, (p_{i-1} + 1)p_i, ..., (n - p_i)\} \setminus \bigcup_{j>i}(p_j)$;
8 Define $A_i = A_{i,1} \cup p_i p_{i+1}$
9 **end**
10 Define $A_k = \{p_k, 2p_k, ..., (n-1)p_k, 0\}$;
11 Define $A = \{A_1, A_2, ..., A_k\}$;
12 A is a Hamiltonian Path where $\{a_1, a_2, ..., a_m\}$ represents the path $a_1 - a_2 - ... - a_m$. Hence, although set notation is used, the order matters and the ideals are always in increasing order;
13 Connect the final vertex of $A, (0)$ to the initial vertex of $A, (p_1)$ to get the Hamiltonian cycle;

4.3.1 Description

This algorithm is based on the proof presented in Theorem 2.20, and provides a simple and fast method to obtain a Hamiltonian cycle and Hamiltonian path in $\mathcal{ZG}(\mathbb{Z}_n)$.

It relies on the fact that $\mathcal{Z}(\mathbb{Z}_n)$ can be expressed as a union of all principal ideals in $\mathbb{Z}_n$. Clearly, all the elements in an ideal are adjacent to each other by Theorem 2.16. However, to find a Hamiltonian Cycle, we must ensure that no vertex is incident twice. Therefore, we remove all the intersecting ideals as shown in Line 7 of the Algorithm. To ensure that the final vertex of A_i is connected to the initial vertex of A_{i+1}, we make an exception to this removal of intersections as shown in Line 8.

4.3.2 Example

Let $n = 105$ so that the prime factorization of n is $3 \times 5 \times 7$. Clearly, $\mathcal{Z}(\mathbb{Z}_{105}) = (3) \cup (5) \cup (7)$, where $(\cdot)$ is the principal ideal of the respective argument. Hence, we have:

$$A_1 = \{a_1 = 3k \mid k \geq 1, 5 \nmid a_1, 7 \nmid a_1, a_1 < 105\}$$
$$A_2 = \{a_2 = 5k \mid k \geq 1, 7 \nmid a_2, a_2 < 105\}$$
$$A_3 = \{a_3 = 7k \mid k \geq 1\} \cup \{0\}$$

Now consider

$$A = \{3, 6, 9, 12, 18, 21, 24..., 102, 15, 5, 10, 20, 25, 30, 40, ..., 100, 35, 7, 14, 28, 42, 49, 56, ..., 98, 0, 3\}$$

obtained by concatenating A_i with A_{i+1}. Clearly, considering A in sequential order yields a Hamiltonian cycle.

4.4 Algorithm to Find a Walk $a - v_1 - ... - v_m - b$ for $v_i \in \mathcal{ZG}(\mathbb{Z}_n)$, given a and b

Algorithm 4: Algorithm to find a walk $1 - v_1 - v_2 - ... - v_m - b$ with $v_i \in \mathcal{ZG}(\mathbb{Z}_n)$

Inputs: n,a,b
Steps :
Obtain prime factorization of n, $P = \{p_1, p_2, ..., p_k\}$;
Apply the map f such that $f(x) = (x_1, x_2, ..., x_k)$, where $x_j = x \pmod{p_j}$ to a and b;
Set initial vertex as $a = (a_1, a_2, ..., a_k)$;
Store $b = (b_1, b_2, ..., b_k)$ as final vertex;
Choose v_1 and v_m such that $f(v_1) = (0, a_2, a_3, ..., a_{k-1}, -a_k)$ and $f(v_m) = (0, b_2, b_3, ..., b_{k-1}, -b_k)$;
for $i = 2, 3, ..., m-1$ **do**
    Choose v_i such that $f(v_i) = (0, x_2, x_3, ..., x_k)$ where $x_j \in \mathbb{Z}_{p_j}$;
    Since f need not be one-to-one, any choice of v_i satisfying this condition works;
end
The path $v_1 - v_2 - ... - v_m$ is a walk in $\mathcal{ZG}(\mathbb{Z}_n)$;
Since a is adjacent to v_1 and v_m is adjacent to b, we get the walk as required;

4.4.1 Description

This algorithm relies on the manifestation of principal ideals as complete subgraphs. It first finds two zero divisors connected to a and b and then finds a path between the two zero divisors in $\mathcal{ZG}(\mathbb{Z}_n)$. Alternately, such a path can be found using Algorithm 3 because:

- If $a, b \in \mathcal{Z}(\mathbb{Z}_n)$, then the path from a to b can be regarded as a sub-path of the Hamiltonian path in $\mathcal{ZG}(\mathbb{Z}_n)$.
  - If a appears in the path before b, we are done.
  - If b appears in the path before a, we can simply trace the Hamiltonian path in reverse order as the graph is undirected.
- If a and b are not both in $\mathcal{Z}(\mathbb{Z}_n)$, then we rely on the fact that every unit element is connected to atleast one zero divisor. This is true as $a \in \mathcal{U}(\mathbb{Z}_n) \implies f(a) = (a_1, a_2, ..., a_k)$ where $k \geq 2$ and $a_i \neq 0 \; \forall 1 \leq i \leq k$. Since $k \geq 2$, we can always find v such that $f(v) = (0, -a_2, v_3, ...v_k)$. Clearly, $p_1 \mid v$ and hence $v \in \mathcal{Z}(\mathbb{Z}_n)$. Further, $p_2 \mid a + v$ and hence a and v are adjacent.

This reasoning is extended to all the vertices and we get the walk as desired.

4.4.2 Example

Let $n = 45$ so that $\mathcal{G}(\mathbb{Z}_n)$ is connected. The result of a computer algorithm implemented in MATLAB is presented below when $a = 14$ and $b = 5$, in Figure 9. Observe that each internal vertex is a zero divisor.

```
>> disp('A Path in ZG(Z_n) from 14 to 5')
disp(num2str(SPH2R))
A Path in ZG(Z_n) from 14 to 5
14    6    3   15    0   15    6    9   15   10   15   12   15   18   15   20   15   21   24   15   25   15   27   30   33   15   35   15   36   39   15   40   15   40   10    5
>>
>>
>>
>>
```

Figure 9: Walk between 14 and 5 in $\mathcal{ZG}(\mathbb{Z}_{45})$

4.5 Algorithm to Find a Walk $a - v_1 - ... - v_m - b$ for $v_i \in \mathcal{UG}(\mathbb{Z}_n)$, given a and b

First, note that such a path is not possible when $a = 0$ or $b = 0$ because $u \in \mathcal{U}(\mathbb{Z}_n) \implies (0, u) \notin E$.

Algorithm 5: Algorithm to find a walk $1 - v_1 - v_2 - ... - v_m - b$ with $v_i \in \mathcal{UG}(\mathbb{Z}_n)$

Inputs: n,a,b

Steps :

Obtain prime factorization of n, $P = \{p_1, p_2, ..., p_k\}$;

Apply the map f such that $f(x) = (x_1, x_2, ..., x_k)$, where $x_j = x \pmod{p_j}$ to a and b;

Set initial vertex as $a = (a_1, a_2, ..., a_k)$;

Store $b = (b_1, b_2, ..., b_k)$ as final vertex;

if $a == 0$ *or* $b == 0$ **then**

    Display Error Message: "Walk not possible";

    End Program;

end

Let $a_x \neq 0$ and $b_y \neq 0$ for some $1 \leq x, y \leq n$;

Choose v_1 such that $f(v_1) = (1, ..., 1, -a_x, 1, ..., 1)$;

Choose v_2 such that $f(v_2) = (p_1 - 1, 1, ..., 1, p_y - b_y, 1, ..., 1)$;

for $i = 3, 4, ..., m$ **do**

    Let $f(v_i) = (v_{i,1}, ..., v_{i,k})$;

    Choose v_i such that:

- $v_{i,y} = p_y - b_y$;
- $v_{i,j} \neq 0$ $\forall 1 \leq j \leq k$;
- For atleast one $j, j \neq y$, $v_{i,j} = -v_{i-1,j} \pmod{p_j}$;

    Since f need not be one-to-one, any choice of v_i satisfying this condition works;

end

The path $v_1 - v_2 - ... - v_m$ is a walk in $\mathcal{UG}(\mathbb{Z}_n)$;

Since a is adjacent to v_1 and v_m is adjacent to b, we get the walk as required;

4.5.1 Description

This algorithm relies on the fact that $\mathcal{UG}(\mathbb{Z}_n)$ is connected whenever $\mathcal{G}(\mathbb{Z}_n)$ is connected. Hence, it finds two units v_1 and v_m adjacent to a and b respectively. This is always possible when $a \neq 0, b \neq 0$. Then, it finds a path from v_1 to v_m in $\mathcal{UG}(\mathbb{Z}_n)$.

4.5.2 Example

Let $n = 45$ so that $\mathcal{G}(\mathbb{Z}_n)$ is connected. The result of a computer algorithm implemented in MATLAB is presented when $a = 14$ and $b = 5$ in Figure 10. Observe that each internal vertex is a unit element.

```
>> disp('A Path in UG(Z_n) from 14 to 5')
disp(num2str(SPH1R))
A Path in UG(Z_n) from 14 to 5
14   1   2   4   2   7   8   1  11  13  14  16  17  19   2  22  23   1  26  28  29  31  32  34   2  37  38   1  41  43  43   2   1   5
>>
>>
>>
fx >>
```

Figure 10: Walk between 14 and 5 in $\mathcal{UG}(\mathbb{Z}_{45})$

Note that the Algorithms 4 and Algorithm 5 find a walk between a given a and b such that each internal vertex is either a zero divisor or a unit, respectively. However, no constraint has been placed on repetition of vertices. Consequently, the results from MATLAB show some internal vertices being traversed more than once.

For example, in Figure 9, vertex 15 appears more than once, whereas in Figure 10, vertex 1 appears more than once.

It is possible to impose further constraints to ensure that the walk is a path, and hence, no vertices are repeated. This can be done simply by checking conditionally if a vertex has been traversed in every loop iteration.

4.6 Algorithm to find the set of elements not connected to any element of a given non-dominating set, A

Algorithm 6: Algorithm to find all elements not connected to any element of A

Inputs: n, **A**

Steps :

Obtain prime factorization of n, $P = \{p_1, p_2, ..., p_k\}$;

Define $n_1 = \prod_{i=1}^{k} p_i$;

Define $m = |A| < p_1$. Hence $A = a_1, a_2, ..., a_m$;

for $j = 1, 2, ..., k$ **do**

  Define $W_{j,1} = A \pmod{p_j}$;

  Find $W_{j,2} = \mathbb{Z}_{p_j} \setminus W_{j,1}$;

  Find $W_{j,3} = -W_{j,2} \pmod{p_j}$;

end

Consider the sets $W_{j,3}$, $1 \leq j \leq k$;

Define $W = W_{1,3} \times W_{2,3} \times ... \times W_{m,3}$, where $\times$ represents the Cartesian product;

Initialize X as an empty set;

for $i = 1, 2, ..., length(W)$ **do**

  We have $W(i) = (b_{i1}, b_{i2}, ..., b_{im})$;

  Apply the Chinese Remainder Theorem to $W(i)$ as follows:

  Find b_i such that:

  for $j = 1, 2, ..., m$ **do**

    $b_{ij} = b_i \pmod{p_j}\ \forall 1 \leq j \leq m$;

  end

  $X = X \cup \{b_i\}$;

  $y = 1$;

  while $b_i + yn_1 \leq n$ **do**

    $X = X \cup \{b_i + yn_1\}$;

    $y = y + 1$;

  end

end

X is the set of all elements not connected to A;

4.6.1 Description

In Theorem 2.15, it was proved that any complete reduced system of residues (mod p_1) forms a dominating set, and that the dominating number is p_1, where p_1 is the smallest prime factor of n.

In other words, a set $A \subset \mathbb{Z}_n$ is a dominating set iff $A \cong \mathbb{Z}_{p_1}$. However, no set with $|A| < p_1$ can satisfy this property. Algorithm 6 presents an elegant method to find all the elements in $\mathbb{Z}_n$ that are not adjacent to any $a \in A$. The algorithm imitates the proof of the theorem, and is best illustrated with an example as follows.

4.6.2 Example

Let $n = 385$ so that the prime factorization of n is $5 \times 7 \times 11$. We know by Theorem 2.15 that any set, A such that $|A| \leq 4$ cannot be a dominating set. Let us arbitrarily choose an A with 4 elements to illustrate the algorithm, and to find all the elements in $\mathbb{Z}_{385}$ which are not adjacent to any $a \in A$.

Suppose $A = \{11, 28, 140, 202\}$. Then we follow the algorithm and find the equivalence classes of each $a \in A$.

Step I: Find $W_{i,1}$ $\forall i$

Table 1: $W_{j,1}$ for $j = 1, 2, 3$

A	mod 5	mod 7	mod 11
11	1	4	0
28	3	0	6
140	0	0	8
202	2	6	4

Thus we have

$$W_{1,1} = \{1, 3, 0, 2\}$$
$$W_{2,1} = \{4, 0, 0, 6\}$$
$$W_{3,1} = \{0, 6, 8, 4\}$$

Step II: Find $W_{i,2}$ $\forall i$

We find $W_{j,2} = \mathbb{Z}_{p_j} \setminus W_{j,1}$ for $j = 1, 2, 3$. Hence,

$$W_{1,2} = \{4\}$$
$$W_{2,2} = \{1, 2, 3, 5\}$$
$$W_{3,2} = \{1, 2, 3, 5, 7, 9, 10\}$$

Step III: Find $W_{i,3}$ $\forall i$

We find $W_{j,3} = -W_{j,2} \pmod{p_j}$ for $j = 1, 2, 3$, and hence,

$$W_{1,3} = \{1\}$$
$$W_{2,3} = \{6, 5, 4, 2\}$$
$$W_{3,3} = \{10, 9, 8, 6, 4, 2, 1\}$$

Step IV: Find W

Next, we define $W = \{1\} \times \{2, 4, 5, 6\} \times \{1, 2, 4, 6, 8, 9, 10\}$. Note that W is a set of cartesian triples, and $|W| = 1 \times 4 \times 7 = 28$. We can immediately infer that there are 28 elements in $\mathbb{Z}_{385}$ not connected to A. This is valid as $n_1 = n$ in this example, where the notation is as used in the algorithm.

Step V: Apply Chinese Remainder Theorem to W

The next step is to Apply the Chinese Remainder Theorem to all elements in W. For the sake of illustration, we randomly pick $w \in W$. Suppose that $w = (1, 5, 8) \in W$. This is equivalent to solving the following system: We find b such that:

$$b = 1 \pmod 5$$
$$b = 5 \pmod 7$$
$$b = 8 \pmod{11}$$

Since $n = 5 \times 7 \times 11$, there is a unique solution $b \in \mathbb{Z}_{385}$. Note that we consider all the solutions had they not been unique. Solving, we get $b = 96$. It is easy to verify that b indeed satisfies the system.

Therefore, 96 is not adjacent to a $\forall a \in A$.

Step VI: Verify

$$\begin{aligned} 96 + 11 &= 107 & \qquad 5, 7, 11 &\nmid 107 \\ 96 + 28 &= 124 & 5, 7, 11 &\nmid 124 \\ 96 + 140 &= 236 & 5, 7, 11 &\nmid 236 \\ 96 + 202 &= 298 & 5, 7, 11 &\nmid 298 \end{aligned}$$

The same argument works for all $w \in W$, and the resultant numbers are all the vertices in $\mathbb{Z}_{385}$ which are not adjacent to any $a \in A$.

5 Conclusion and Future Work

This thesis is a summary of the work done in MTH 490 - Senior Project in partial fulfillment of the requirements for the degree of Bachelor of Science in Mathematics. It establishes relationships between abstract algebra and graph theory by examining the graphical manifestation of algebraic properties of the ring of integers, modulo n. In particular, results pertaining to the connectivity, planarity and traversablity are derived for $\mathcal{G}(\mathbb{Z}_n)$. Further, results on $\mathcal{UG}(\mathbb{Z}_n)$ and $\mathcal{ZG}(\mathbb{Z}_n)$ are derived, and experimentally verified using computer simulations. Algorithms to construct and verify a wide variety of properties are also presented with examples.

With regard to the study of relationships between properties of the ring and its corresponding graph, scope for future work includes proofs and disproofs of the conjectures presented in the Appendix of the report. Theorems pertaining to the clique number and chromatic number of the graph and their relationship to the ring can provide a deeper insight into the structural properties associated with these graphs. The Appendix also provides interesting patterns and anomalies observed in the degree of vertices in the induced subgraph of units. These patterns are unexplained, but their inherent structure suggests something more than coincidence. Further, spanning trees in $\mathcal{G}(\mathbb{Z}_n)$ as presented in the Appendix suggestively possess properties worth exploring. Similar questions regarding the complement of the graph can establish relationships between the clique number and independent number of the graph.

Graphs that arise from different conditions for adjacency between matrices can provide alternate ways to associate a visual representation of rings. A very interesting takeaway for future research would be to establish relationships between polynomial rings and the Cartesian product of $\mathcal{G}(\mathbb{Z}_n)$ with itself. This can also be an interesting tool to study irreducible polynomials, their structure and occurence within polynomial rings.

References

[1] Jonathan L. and Yellen Gross Jay and Zhang, *Handbook of Graph Theory, Second Edition*, 2nd, Chapman & Hall/CRC, 2013.

[2] J. Gallian, *Contemporary Abstract Algebra*, Cengage Learning, 2016.

[3] A. Badawi, *Abstract Algebra Manual: Problems and Solutions*, Nova Science Publishers, 2004.

A Appendix

A.1 Conjectures

This section contains claims that have not been proven as of yet. They are a result of computer simulations which suggest that they are true.

Conjecture A.1. *A connected $\mathbb{Z}_n$ graph is always a Hamiltonian graph.*

Conjecture A.2. *The clique number, $\omega(n)$, of $\mathcal{G}(\mathbb{Z}_n)$ with $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ and $p_1 < p_i \ \forall \ i$ is $\frac{n}{p_1}$*

By Theorem 2.16, it is clear that $\mathcal{G}(\mathbb{Z}_n)$ has $\mathbb{K}_{\frac{n}{p_1}}$ as a subgraph, and each vertex of $\mathbb{K}_{\frac{n}{p_1}}$ is connected to every vertex except itself. Thus, $\frac{n}{p_1}$ is a lower bound for $\omega(\mathcal{G}(\mathbb{Z}_n))$. The claim is that $\omega(\mathcal{G}(\mathbb{Z}_n)) = \frac{n}{p_1}$.

Conjecture A.3. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, with $p_1 < p_2 < ... < p_k$. The chromatic number of $\mathcal{G}(\mathbb{Z}_n)$, denoted by $\chi(\mathcal{G}(\mathbb{Z}_n)) = \frac{n}{p_1}$.*

Since the clique number is atleast $\frac{n}{p_1}$, the chromatic number too is atleast $\frac{n}{p_1}$ because $\chi(G) \geq \omega(G)$. The claim is that $\chi(G) = \frac{n}{p_1}$. This is illustrated using two examples.

- $n = 15$: Here, $\frac{n}{p_1} = 5$.

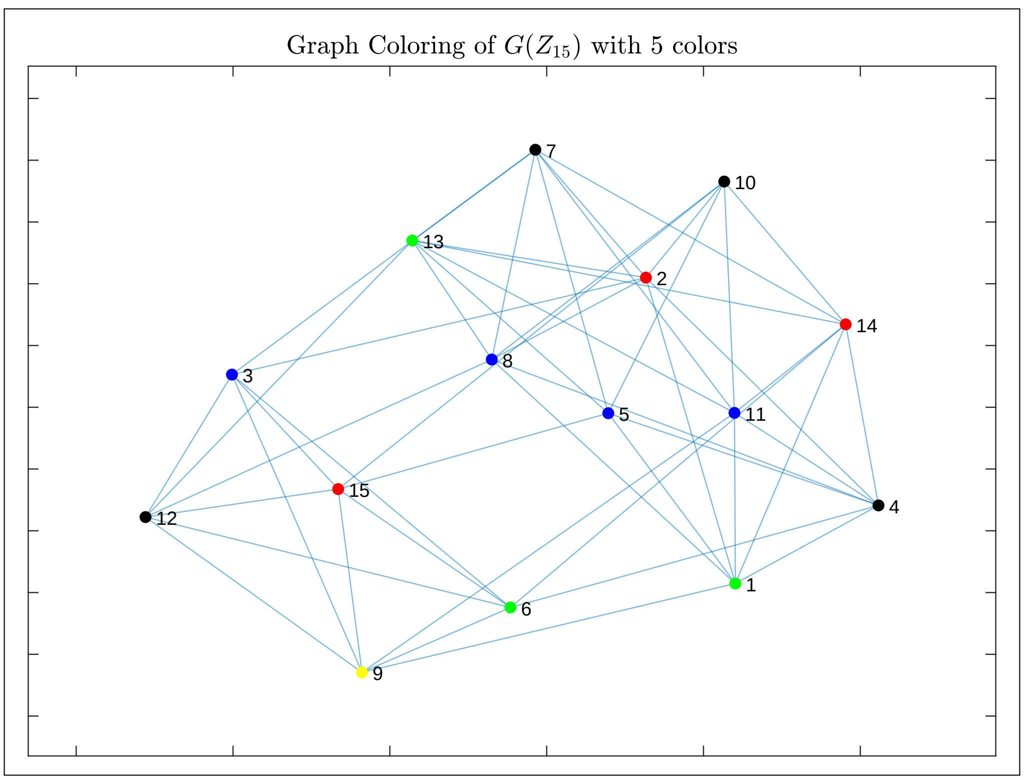


Figure 11: A Coloring of $\mathcal{G}(\mathbb{Z}_{15})$ using 5 Colors

- $n = 35$: Here $\frac{n}{p_1} = 7$.

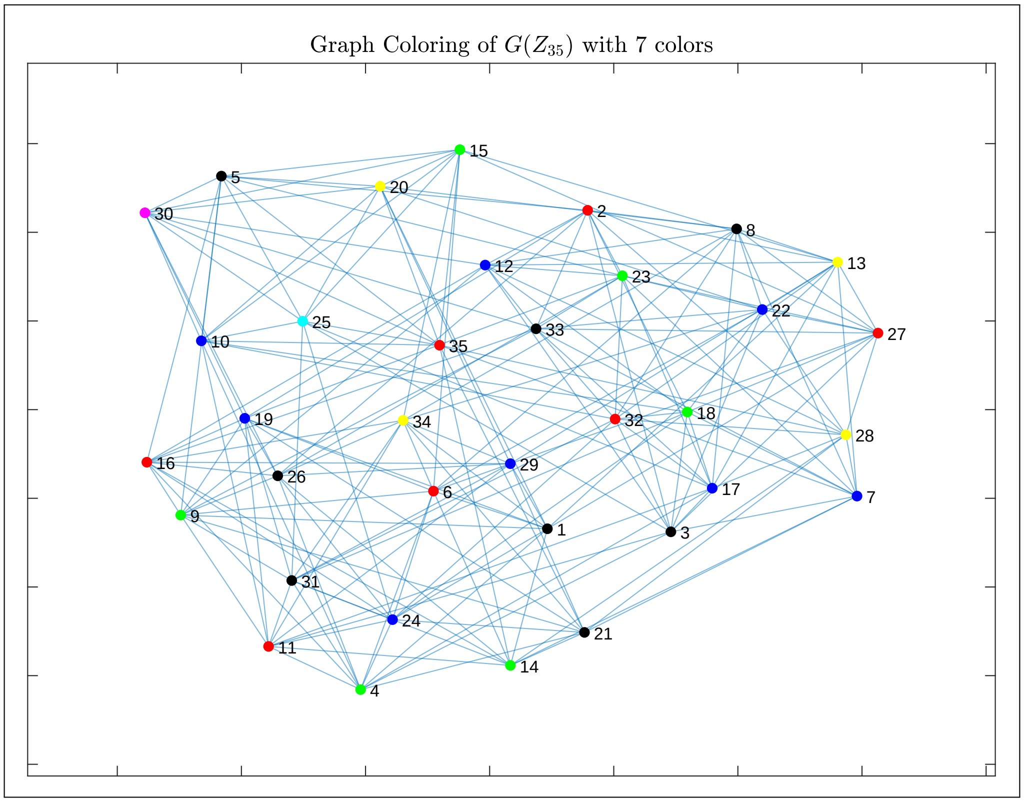


Figure 12: A Coloring of $\mathcal{G}(\mathbb{Z}_{35})$ using 7 Colors

Conjecture A.4. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ with $p_1 < p_2 < ... < p_k$ and $k \geq 2$. Then the diameter of the minimum spanning tree of $\mathcal{G}(\mathbb{Z}_n)$ is $p_1 + 1$.*

Recall that a spanning tree is a spanning subgraph of G which is also a tree, i.e. has no cycles.

This conjecture is based on computer simulations of a large set of choices for n. The idea is to first construct the minimum spanning tree of $\mathcal{G}(\mathbb{Z}_n)$ and display it. The distance from the root to the leaf of the tree is seen to be $p_1 + 1$ in all cases, which also coincides with the diameter of the tree based on the structure.

Some examples of spanning trees for $\mathcal{G}(\mathbb{Z}_n)$ are provided in Figures 13 - 16 to illustrate this. The computer simulations show that the diameter of the spanning tree is $p_1 + 1$ in all cases.

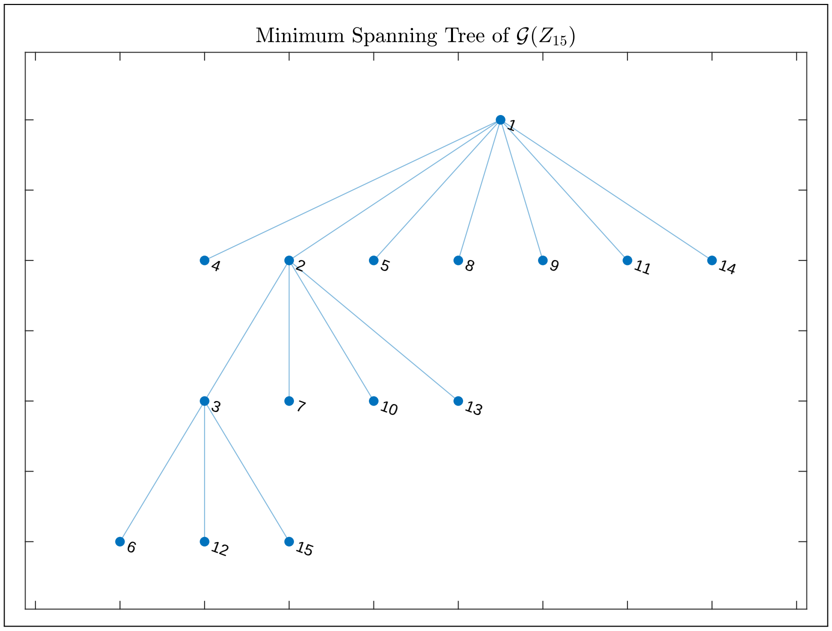


Figure 13: Spanning Tree of $\mathcal{G}(\mathbb{Z}_{15})$

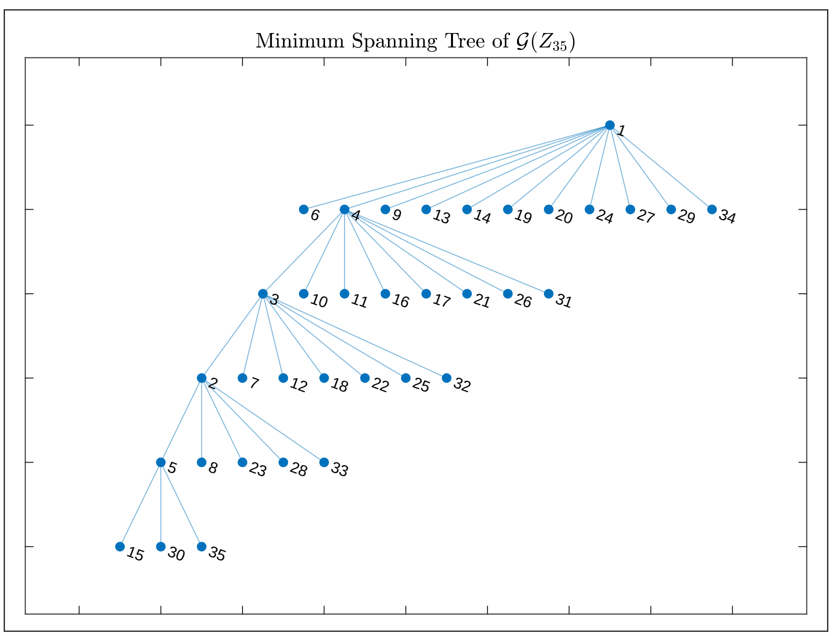


Figure 14: Spanning Tree of $\mathcal{G}(\mathbb{Z}_{35})$

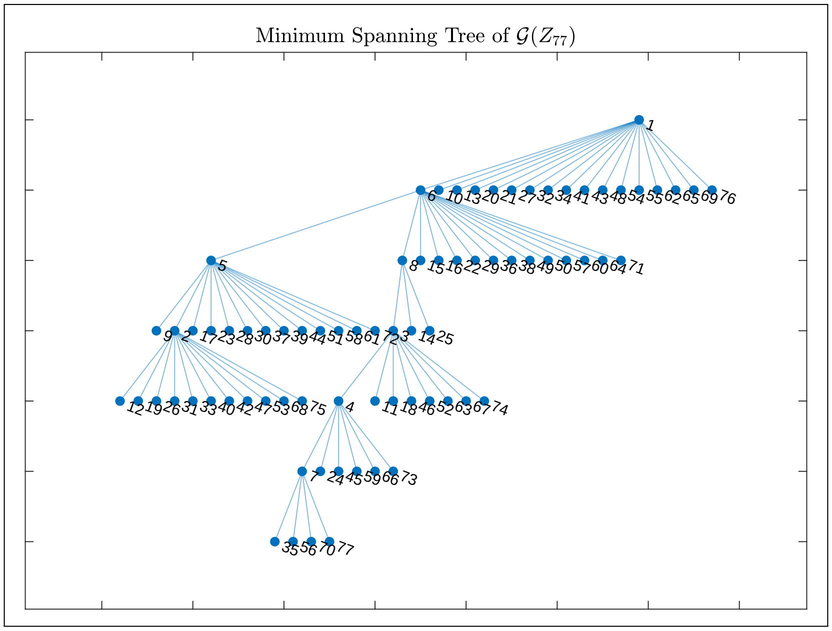


Figure 15: Spanning Tree of $\mathcal{G}(\mathbb{Z}_{77})$

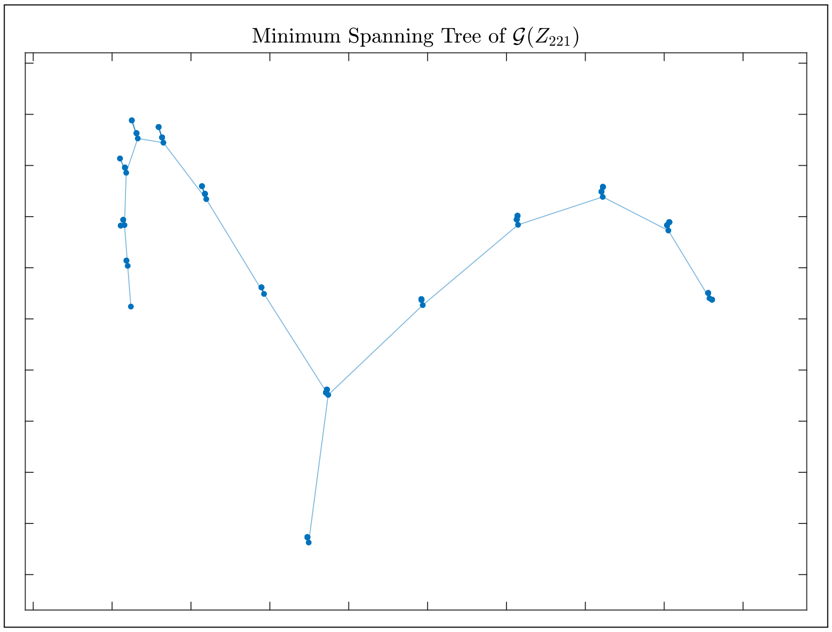


Figure 16: Spanning Tree of $\mathcal{G}(\mathbb{Z}_{221})$

A.2 The Degree of Vertices in $\mathcal{UG}(\mathbb{Z}_n)$

Theorem 2.4 found an explicit formula for the degree of a vertex in the regular graph $\mathcal{UG}(\mathbb{Z}_n)$. This was given by the $\gamma(n)$ function as defined in the Theorem.

Visualizing the $\gamma(n)$ Function:

Let $\gamma(n)$ represent the degree of each vertex of $\mathcal{UG}(\mathbb{Z}_n)$. Then we can plot $\gamma(n)$ with respect to n as shown in Figure 4. It is worth noticing the following:

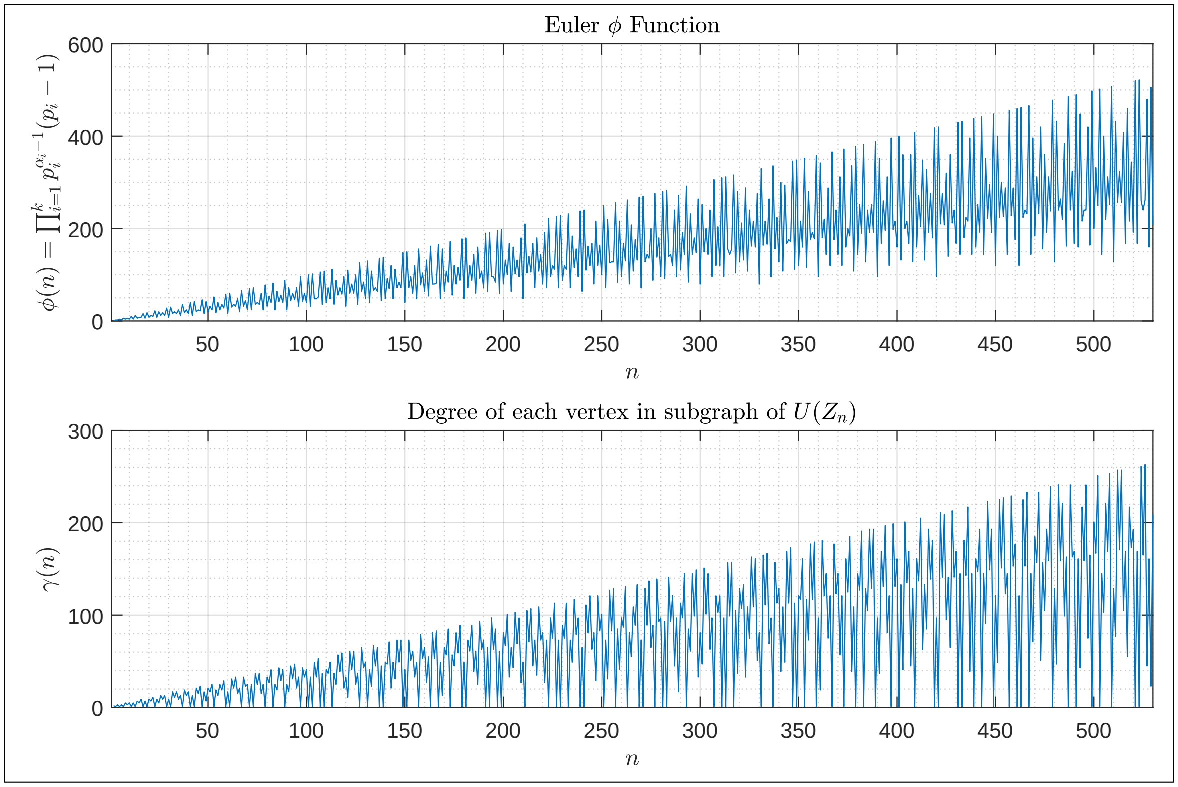


Figure 17: Euler's $\phi(n)$ function and the $\gamma(n)$ Function.

1. The graphs are actually discrete plots but the points have been linearly interpolated for easy visualization.

2. The $\phi(n)$ function is upper bounded by the line $\phi(n) = n - 1$ as this is the maximum number of units that is possible inside $\mathbb{Z}_n$ and occurs when n is prime. By a well known result from number theory, there is no linear lower bound for this function. The lower limit of the Euler $\phi(n)$ graph is proportional to $\frac{n}{\log \log n}$.

3. $\gamma(n) = 1$ whenever n is prime. This is clear as whenever n is prime, $a \neq 0 \implies a \in \mathcal{U}(\mathbb{Z}_n)$. Since $\mathcal{Z}(\mathbb{Z}_n) = \{0\}$, a is adjacent only to $-a \pmod{p}$. Hence the lower bound for $\gamma(n)$ is $\gamma(n) = 1$.

4. The values of n for which $\phi(n)$ equals its upper bound are the same n for which $\gamma(n)$ attains its lower bound. These are the prime numbers.
5. The $\gamma(n)$ function is upper bounded by the line $\gamma(n) = \frac{n}{2}$.
6. The $\gamma(n)$ function follows an interesting pattern. The reader is referred to the appendix for more on this.

Since $\gamma(n)$ is fixed for a given n, we plot $\gamma(n)$ as a discrete plot with respect to n, as shown in Figure 18.

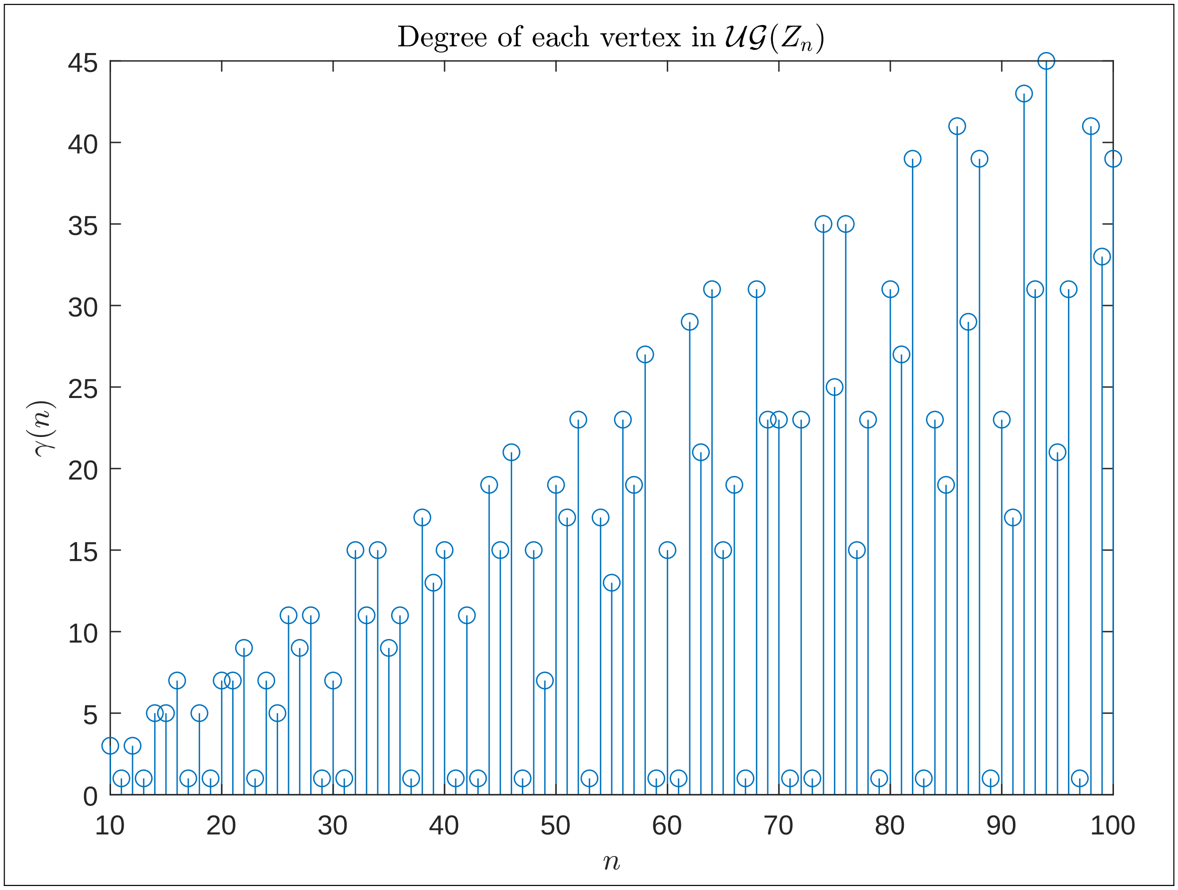


Figure 18: $\gamma(n)$ vs. n: Discrete

Although we can observe some linear trends in periodic intervals, it is not easy to resolve these differences. Hence, we interpolate between the discretized plots to make the image easier to read. This is presented in Figure 19

This yields an interesting pattern. Nowhere in the window frame can we observe two consecutive increases or two consecutive decreases. The function seems to be following an Up-Down-Up-Down

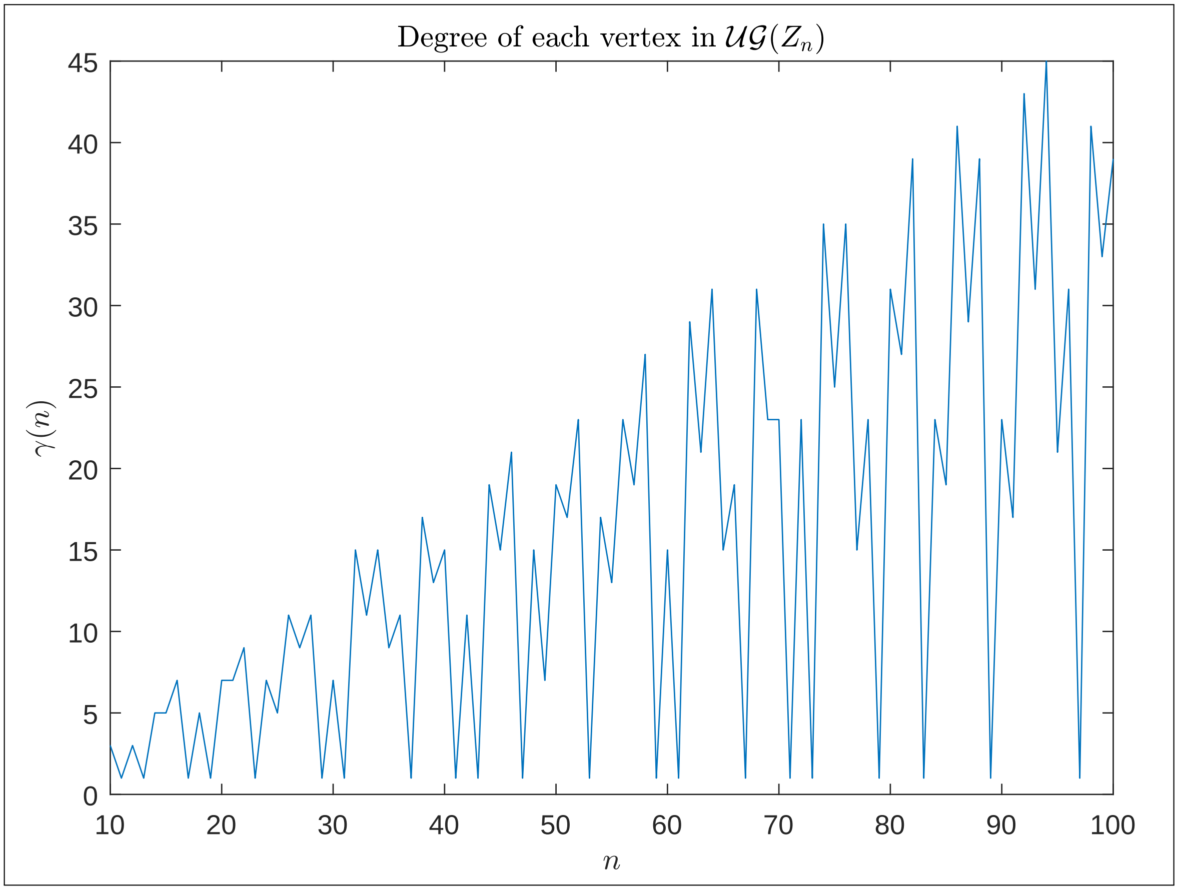


Figure 19: $\gamma(n)$ vs. n: Interpolated

pattern, except at certain indices where it is constant (Refer to $n = 69$ and $n = 70$).

There is no immediate analytical answer to this behaviour, in this range. This is due to the fact that the $\gamma(n)$ function depends, not just on the value of n, but also on the prime factors of n. Since there is no direct relationship between the prime factors of n and the prime factors of $n+1$, we cannot establish a direct relationship between $\gamma(n)$ and $\gamma(n+1)$.

It is interesting to observe what happens as we increase n. Since we have a direct formula for $\gamma(n)$, we can directly use it instead of constructing $\mathcal{UG}(\mathbb{Z}_n)$ and finding the degree of the vertices.

The following observations are made:

- The Up-Down-Up-Down pattern continues beyond $n = 100$. It continues until $n = 769$ where it is broken. Figure 20 shows a breakdown in this pattern at $n = 769$.
- Since $\gamma(769) < \gamma(770) < \gamma(771)$ and we need three vertices to detect two consecutive increases, let us save the first of these indices (i.e 769) as the first occurence of a pattern breakdown.
- Interestingly, there is a pattern breakdown immediately after $n = 769$, at $n = 770$.

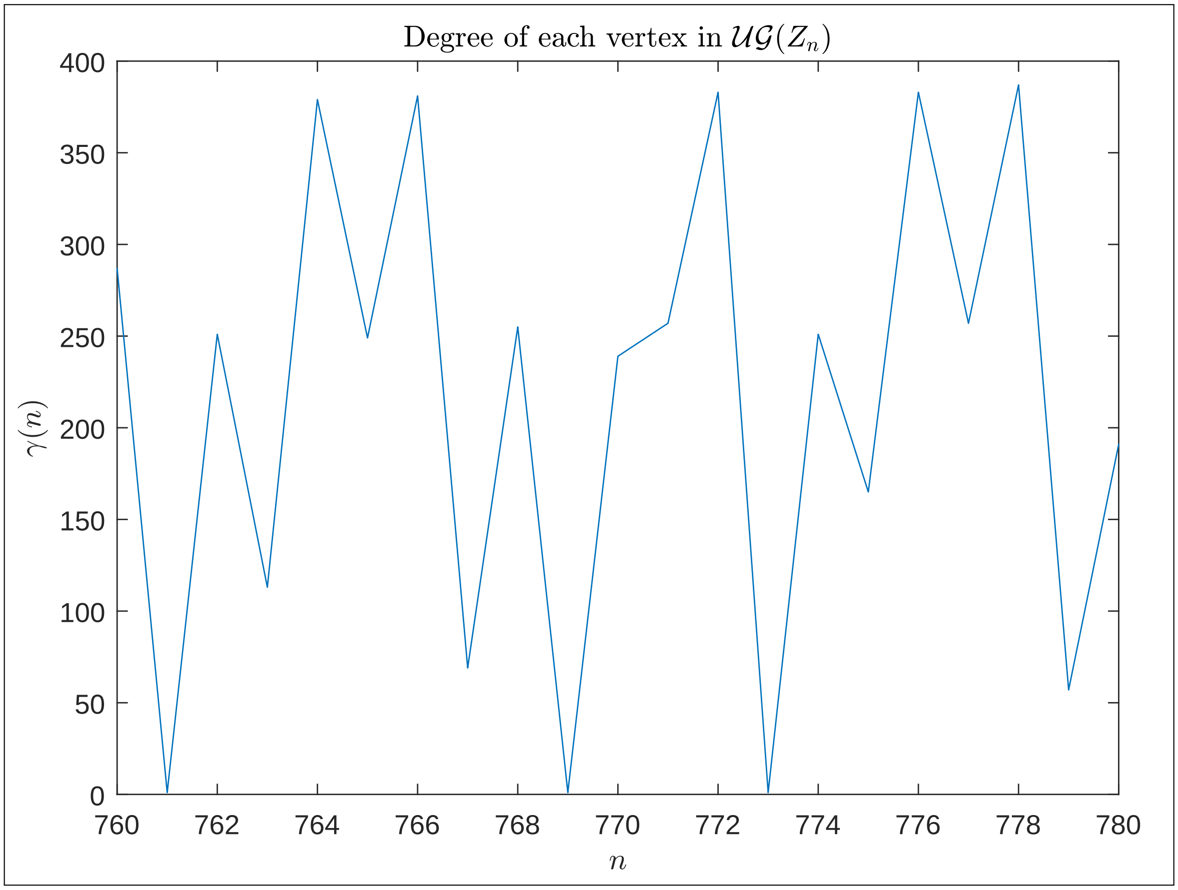


Figure 20: $\gamma(n)$ vs. n: $750 \leq n \leq 770$

- The Up-Down-Up Pattern resumes after this, until it is broken again in the same fashion at $n = 908$, and followed immediately by $n = 909$. This is easily seen from Figure 21.
- This seems to suggest that the Up-Down-Up-Down pattern persists unless it is broken by consecutive increases or consecutive decreases. Further, if there is a consecutive increase (or decrease) with initial vertex n, then there is a consecutive increase (or decrease) with intiial vertex $n + 1$. This claim is tested using a computer algorithm for n upto 1 million.
- This pattern does hold for n upto atleast 1 million. A total of 3802 breakdowns with respect to increase, and 3808 breakdowns with respect to decrease are recorded for $1 \leq n \leq 10^6$. The first few indices for which the pattern is broken are presented in Figure 22 and Figure 23.
- There seems to be a pattern in the breakdown of the Up-Down-Up-Down pattern. More specifically, the breakdowns are consecutive.
- A question that arises immediately is regarding the frequency of these breakdowns, i.e. How

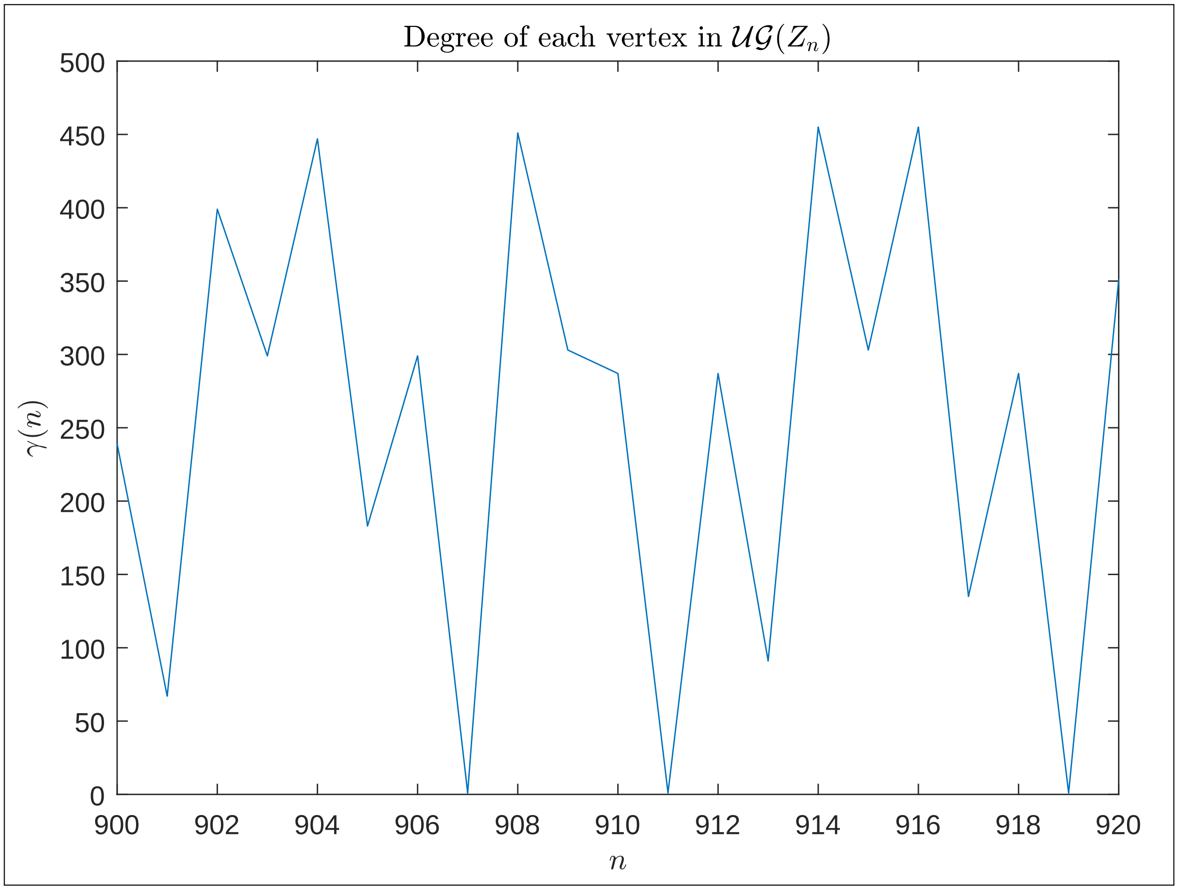


Figure 21: $\gamma(n)$ vs. n: $900 \leq n \leq 920$

far apart are these breakdowns? Pairing each pair of consecutive increases and each pair of consecutive decreases as one, the pairwise difference between two breakdowns is shown separately with respect to increases and decreases in Figures 24 and 25 respectively.

- It seems at first sight, that the difference between two consecutive breakdowns, whether with respect to increase or decrease, are integer multiples of 210. However, there are some exceptions. Figures 26 and 27 display this difference in breakdown modulo 210.

- This pattern seems interesting and is highlighted through the course of this project. It has not been investigated in any greater detail due to it being beyond the scope of this project.

```
Columns 1 through 12

  769    770   1189   1190   1609   1610   1819   1820   2029   2030   2659   2660

Columns 13 through 24

 3079   3080   4339   4340   4549   4550   4759   4760   5389   5390   6439   6440

Columns 25 through 36

 6649   6650   7279   7280   7699   7700   8119   8120   8329   8330  10009  10010

Columns 37 through 48

10639  10640  10849  10850  11269  11270  11899  11900  12319  12320  12739  12740

Columns 49 through 60

14209  14210  14629  14630  15469  15470  16099  16100  16939  16940  17359  17360

Columns 61 through 72

18199  18200  18619  18620  19039  19040  19249  19250  20299  20300  20929  20930

Columns 73 through 84

21559  21560  22609  22610  23659  23660  23869  23870  25759  25760  26179  26180
```

Figure 22: Pattern Breakdown: Initial Indices of Two Consecutive Increases

```
Columns 1 through 12

  908    909   1328   1329   1538   1539   2168   2169   2378   2379   3218   3219

Columns 13 through 24

 3638   3639   3848   3849   4058   4059   5318   5319   5948   5949   6158   6159

Columns 25 through 36

 6368   6369   8048   8049   8468   8469   8678   8679   9098   9099   9308   9309

Columns 37 through 48

 9518   9519  10148  10149  10778  10779  11828  11829  12878  12879  13088  13089

Columns 49 through 60

13298  13299  14558  14559  15188  15189  15398  15399  16238  16239  16658  16659

Columns 61 through 72

17288  17289  17708  17709  20018  20019  20228  20229  21278  21279  21698  21699

Columns 73 through 84

22328  22329  22538  22539  22748  22749  23798  23799  24308  24309  24638  24639
```

Figure 23: Pattern Breakdown: Initial Indices of Two Consecutive Decreases

```
Columns 1 through 12

     420     420     210     210     630     420    1260     210     210     630    1050     210

Columns 13 through 24

     630     420     420     210    1680     630     210     420     630     420     420    1470

Columns 25 through 36

     420     840     630     840     420     840     420     420     210    1050     630     630

Columns 37 through 48

    1050    1050     210    1890     420     210     210     570    1320     630     630     840

Columns 49 through 60

     210    1050     630     630     210    1260     840    1470     420     420     840    1470

Columns 61 through 72

     210     210    1530     360     210     210     240    1020     300     330     420     420

Columns 73 through 84

    1050     420     630     630     390     660     630     630     210     210     210     420
```

Figure 24: Pattern Breakdown (Increase): Difference between Two Consecutive Breakdowns

```
Columns 1 through 12

     420     210     630     210     840     420     210     210    1260     630     210     210

Columns 13 through 24

    1680     420     210     420     210     210     630     630    1050    1050     210     210

Columns 25 through 36

    1260     630     210     840     420     630     420    2310     210    1050     420     630

Columns 37 through 48

     210     210    1050     510     330     630     210    1470     420     840     210     840

Columns 49 through 60

    1680     630     630     690     360     420     210     630     210     810     660     210

Columns 61 through 72

     630     210     840     420     630    1470     210     420     240     180     210    1260

Columns 73 through 84

    1470     630     210    1260     630     420     330     720     420     840     780     690
```

Figure 25: Pattern Breakdown (Decrease): Difference between Two Consecutive Breakdowns

```
Columns 1 through 25

    0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0

Columns 26 through 50

    0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0   150    60     0     0     0     0     0

Columns 51 through 75

    0     0     0     0     0     0     0     0     0     0     0     0    60   150     0     0    30   180    90   120     0     0     0     0     0

Columns 76 through 84

    0   180    30     0     0     0     0     0     0
```

Figure 26: Pattern Breakdown (Increase): Difference between Two Consecutive Pattern Breakdowns (mod 210)

```
Columns 1 through 25

    0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0     0

Columns 26 through 50

    0     0     0     0     0     0     0     0     0     0     0     0     0     0    90   120     0     0     0     0     0     0     0     0     0

Columns 51 through 75

    0    60   150     0     0     0     0   180    30     0     0     0     0     0     0     0     0     0    30   180     0     0     0     0     0

Columns 76 through 84

    0     0     0   120    90     0     0   150    60
```

Figure 27: Pattern Breakdown (Decrease): Difference between Two Consecutive Pattern Breakdowns (mod 210)