



---

*Research article*

## Structural properties of generalized power congruence graphs over sets of moduli

Muhammad Awais Raza<sup>1</sup>, Muhammad Khalid Mahmood<sup>1,\*</sup> and Daniele Ettore Otera<sup>2,\*</sup>

<sup>1</sup> Institute of Mathematics, University of the Punjab, Lahore 54590, Pakistan

<sup>2</sup> Institute of Data Science and Digital Technologies, Vilnius University, Akademijos st. 4, LT-08663 Vilnius, Lithuania

\* **Correspondence:** Email: [khalid.math@pu.edu.pk](mailto:khalid.math@pu.edu.pk), [daniele.otera@mif.vu.lt](mailto:daniele.otera@mif.vu.lt).

**Abstract:** In this article, we introduce and study a novel class of graphs called power congruence graphs (PCGs) that are constructed over the sets of moduli of the form  $M_p = \{p^t : t \geq 1, p^t < n\}$ , where  $p$  is a prime. For  $n \in \mathbb{Z}^+$ , consider  $V = \{0, 1, \dots, n - 1\}$  as the vertex set. We construct a simple, undirected graph  $G(n, k, M_p)$  without loops or multiple edges over  $V$  in which two distinct vertices  $a, b \in V$  are adjacent if  $a^k \equiv b \pmod{m}$  for some  $m \in M_p$  and fixed  $k \in \mathbb{Z}^+$ . We present a comprehensive structural characterization of PCGs for the cases  $p = 2, 3, 5$  and extend the framework to an arbitrary prime  $p$ . When  $p = 2$ , the graph decomposes into two disjoint complete components for all  $k$ . When  $p = 3$ , the graph structure is governed by  $k \pmod{2}$ ; for odd value of  $k$ , the graph is a disjoint union of three complete components; and for even value of  $k$ , the graph is a disjoint union of one complete component and one component  $K_n^F$  obtained from a complete graph  $K_n$  by deleting a specified set of edges  $F \subseteq E(K_n)$ . When  $p = 5$ , the graph becomes more intricate and depends on  $k \pmod{4}$ , producing configurations that include both complete components and components  $K_n^F$  obtained from a complete graph  $K_n$  by deleting a specified set of edges  $F \subseteq E(K_n)$ . In general, for a prime  $p$ , the structure of the graph is determined by the residue class of  $k \pmod{p - 1}$ , giving rise to up to  $p - 1$  distinct structural types. This highlights a systematic transition from simple to increasingly complex graph configurations as the prime modulus increases. Furthermore, we investigate several graph invariants associated with these graphs. This study provides a framework for understanding power congruence-based graph constructions bridging number theory with graph theory.

**Keywords:** power congruence graphs; prime power moduli; graph decomposition; spectral graph theory; Laplacian matrix; spectra

**Mathematics Subject Classification:** 05C15, 05C25, 05C69

---

## 1. Introduction

Number theory is one of the earliest branches of mathematics. Congruence relations are a key concept in number theory with applications in algebra and computer science. The interaction between number theory and graph theory has led to the development of graph models defined through modular relationships. Studying congruence relations within a graph theoretic framework leads naturally to the notion of congruence graphs. In these graphs, integers serve as vertices, and edges are defined according to prescribed congruence conditions. In recent years, various graph models based on congruence relations have been introduced where adjacency is determined through modular conditions. A basic instance of such relations is the linear congruence  $a \equiv b \pmod{m}$  for integers  $a, b$  and modulus  $m \in \mathbb{N}$ . In contrast to linear congruences, relations of the form  $a^k \equiv b \pmod{m}$  for a fixed integer  $k \in \mathbb{N}$  introduce additional structure and lead to richer graph theoretic behavior. Congruence-based graphs have attracted considerable interest because they translate algebraic properties into combinatorial structures. Mateen and Mahmood [1] explored these models to investigate graph invariants. Nathanson and Ruzsa [2] introduced and studied graphs defined by congruences, exploring their additive properties and applications in number theory. Peranginangin [3] discussed the application of number theory in cryptography, highlighting its significance in developing secure communication systems. Daoub et al. [4] explored the structural properties of graphs defined over quadratic congruences, analyzing their degree distributions and subgraph characteristics based on the modulus. Several graph constructions based on number-theoretic relations have been studied in the literature. For instance, Nathanson [5] considered graphs where adjacency is determined by additive congruences of the form  $a + b \equiv r \pmod{m}$ . Quadratic relations were used by Blanton et al. [6], where directed edges arise from  $a^2 \equiv b \pmod{n}$ . More generally, Lucheta et al. [7] introduced graphs defined via arithmetic functions  $f$  satisfying  $f(a) \equiv b \pmod{m}$ . Further structural aspects of power-based relations were examined by Somer and Krizek [8], where edges are induced by congruences of the form  $x^k \equiv y \pmod{n}$ . The importance of power digraphs in computer science has been highlighted in the study by Mateen et al. [9], where the structural properties of digraphs defined by the relation  $x^k \equiv y \pmod{n}$  are explored for applications in data structures, cryptography, and parallel computation. Mateen et al. [10] examined the symmetry of complete graphs constructed over quadratic and cubic residues, contributing to the classification of modular graphs under residue-based adjacency rules. Mahmood and Ahmad [11] investigated order structured graphs of cyclic groups, providing a classification based on group order and exploring their structural properties. Deng and Yuan [12] investigated the symmetry of power digraphs defined by the congruence  $x^k \equiv y \pmod{n}$ . They established criteria under which the digraph  $G(n, k)$  is symmetric with attention on its structural characteristics and the decomposition of connected components into isomorphic pairs. Although some studies such as [1] explored power digraphs using a fixed modulus, the generalization to a set of moduli has not been formally defined yet in the literature. A significant advancement in this field was made by researchers [13–15], who generalized the fixed modulus approach by defining graphs over a set of moduli  $M = \{m_1, m_2, \dots, m_n\}$ . In this construction, an edge between  $a$  and  $b$  exists if  $a \equiv b \pmod{m}$  for some  $m \in M$ . Asif et al. [16] formally developed the structural and distance-based properties of such graphs and examined several key parameters including chromatic number, domination number, and graph energy.

Recent studies have also shown interest in using modulus-based rules for defining labeling functions, edge weights, and adjacency conditions that are rooted in number-theoretic structures.

However, none of these studies have fully explored graphs defined by power congruence  $a^k \equiv b \pmod{m}$  over sets of moduli, which presents a clear gap in the current literature. The present research bridges this gap by introducing power congruence graphs (PCGs), where adjacency is based on the relation  $a^k \equiv b \pmod{m}$  for some  $m \in M$ . Despite their theoretical significance, congruences over sets of moduli have received limited attention in the context of graph construction. Our research defines and analyzes a new class of graphs called PCGs, where adjacency is determined by the power congruence relation  $a^k \equiv b \pmod{m}$  for some  $m \in M$ , and  $M = \{m_1, m_2, \dots, m_n\}$ . The set  $M \subset \mathbb{N}$  may consist of finite sets of residues from a complete set of residues of any integer. Various graph-theoretic properties such as degree sequence, chromatic number, metric dimension, graph energy, and eccentricity will be investigated. This direction offers a promising link between algebraic number theory and discrete mathematical modeling. In number theory, power congruences of the form  $a^k \equiv b \pmod{m}$ ,  $k \in \mathbb{Z}^+$  play a fundamental role. Quadratic and higher-power residues are central to reciprocity laws, the structure of multiplicative groups modulo  $m$ , and the study of primitive roots. Exponential congruences also underpin cryptographic systems such as Rivest-Shamir-Adleman (RSA) and Diffie–Hellman, whose security relies on the difficulty of computing discrete logarithms in modular settings. Moreover, the iterative dynamics of power maps modulo  $m$  naturally give rise to functional graphs, with cycles corresponding to periodic orbits and trees representing preperiodic trajectories.

## 2. Preliminaries

In this section, we recall some essential definitions from number theory [17] and graph theory [18].

### 2.1. Graph theoretic preliminaries

A graph  $G = (V, E)$  consists of a non-empty vertex set  $V$  and an edge set  $E$ . The order and size of  $G$  are  $|V|$  and  $|E|$ , respectively. The degree of a vertex  $v \in V$  is the number of edges incident to  $v$ , and a vertex of degree zero is called isolated. A graph is called regular if all its vertices have equal degree. A graph is complete if every pair of distinct vertices is adjacent, and it is connected if there exists a path between every pair of vertices. A path is a sequence of adjacent vertices, while a cycle is a closed path. A connected graph is Hamiltonian if it contains a cycle passing through every vertex exactly once. An independent set is a subset of vertices with no edges between them, and its maximum size is denoted by  $\alpha(G)$ . The chromatic number  $\chi(G)$  is the minimum number of colors required to color the vertices such that adjacent vertices receive different colors. A dominating set is a subset of vertices such that every vertex outside the set is adjacent to at least one vertex in it, and its minimum size is called the domination number. The clique number  $\omega(G)$  is the size of the largest complete subgraph. The distance between two vertices is the length of a shortest path between them, and the diameter of  $G$  is the maximum such distance.

### 2.2. Congruences and power congruences

Let  $m \in \mathbb{N}$  and  $a, b \in \mathbb{Z}$ . The notation  $a \equiv b \pmod{m}$  indicates that the difference  $a - b$  is a multiple of  $m$ . For a fixed exponent  $k \geq 2$ , a power congruence refers to an expression of the form  $a^k \equiv b \pmod{m}$ , where  $a, b \in \mathbb{Z}$ .

### 2.3. Congruence graphs over set of moduli

Fix a positive integer  $n$  and let  $M$  be a nonempty set of moduli. We consider the vertex set consisting of integers  $\{0, 1, \dots, n-1\}$ . A graph is obtained by joining two distinct vertices whenever they satisfy a congruence relation modulo at least one element of  $M$ . In a similar manner, one can define a PCG by replacing the above condition with a power relation. Specifically, two distinct vertices are connected if there exists  $m \in M$  such that  $a^k \equiv b \pmod{m}$  for a fixed exponent  $k \in \mathbb{Z}^+$ .

**Definition 2.1.** Let  $n \in \mathbb{N}$  and consider the vertex set  $V = \{0, 1, \dots, n-1\}$ . Let  $p$  be a prime and define  $M_p = \{p^t : t \in \mathbb{N}, p^t < n\}$ . For a fixed exponent  $k \in \mathbb{Z}^+$ , the PCG associated with  $M_p$ , denoted by  $G(n, k, M_p)$ , is the simple undirected graph on  $V$  in which two distinct vertices  $a, b \in V$  are adjacent whenever there exists  $m \in M_p$  such that  $a^k \equiv b \pmod{m}$ .

$$a \sim b \iff a^k \equiv b \pmod{m} \text{ for some } m \in M_p.$$

**Remark 2.1.** Although the adjacency relation is determined by congruences modulo  $p$ , we retain the family  $M_p$  to emphasize the broader framework of graph constructions over sets of moduli and to facilitate future restricted variants involving selected powers of  $p$ .

**Definition 2.2.** Let  $K_n$  be the complete graph on  $n$  vertices. Let  $R$  be the adjacency relation defined by  $a^k \equiv b \pmod{m}$  for some  $m \in M_p$ . Let  $E_R \subseteq E(K_n)$  denote the set of edges induced by the relation  $R$ , and define  $F = E(K_n) \setminus E_R$  as the set of edges not induced by  $R$ . We define the graph  $K_n^F$  as

$$K_n^F = (V(K_n), E(K_n) \setminus F).$$

Equivalently,  $K_n^F$  is the graph complement of the edge set  $F$  in  $K_n$ .

## 3. Structural analysis of power congruence graphs

In this section, we investigate the structure of PCGs defined over modulus sets of the form  $M_p = \{p^t : t \in \mathbb{N}, p^t < n\}$ , where  $p$  is a prime. These moduli sets give rise to distinct families of graphs whose connectivity, completeness, and component structure depend intricately on the exponent  $k$ . For  $p = 2$ , the resulting graphs decompose into two disjoint complete components for all values of  $k$ . In the case  $p = 3$ , the structure varies with the parity of  $k$ , leading to either three complete components or a combination of complete and  $K_n^F$  components. For  $p = 5$ , a richer and more intricate behavior emerges, where the structure depends on  $k \pmod{4}$  and includes configurations involving both complete and  $K_n^F$  components. We establish that the components arising in these graphs are either complete or  $K_n^F$  components and we derive explicit expressions for the completion closure of  $K_n^F$  components. Furthermore, we analyze the adjacency relations and provide a detailed decomposition of these graphs into their constituent components.

### 3.1. Structural analysis of power congruence graphs over modulus sets of the form $2^t$

In this subsection, we investigate the structure of PCGs defined over the modulus set  $M_2 = \{2^t : t \in \mathbb{Z}^+, 2^t < n\}$ . We study several graph invariants of the constructed graphs. The following result provides a structural characterization of the graph in terms of its decomposition into complete subgraphs.

**Theorem 3.1.** For  $n \geq 3$  and the moduli set  $M_2$ , the proposed graph  $G(n, k, M_2)$  in Definition 2.1 is decomposed as the union of two disjoint complete sub-graphs  $K_{\lceil n/2 \rceil}$  and  $K_{\lfloor n/2 \rfloor}$  for all  $k \in \mathbb{Z}^+$ . That is,

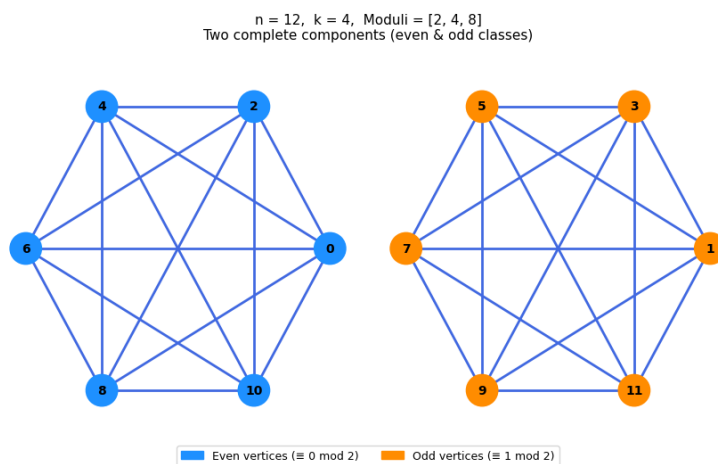
$$G \cong K_{\lceil n/2 \rceil} \cup K_{\lfloor n/2 \rfloor}.$$

*Proof.* In modulus set  $M_2$ , we take all powers of 2 that are strictly less than  $n$ . Consider the vertex set  $V = \{0, 1, 2, \dots, n - 1\}$ . In an even modulus, the elements of  $V$  split into two classes, namely, evens and odds. This division is absolute, in the sense that every higher power of 2 as modulus refines but never contradicts the initial even and odd separation. In other words, once an element is even, it remains even modulo every  $2^t$ ; once it is odd, it remains odd modulo every  $2^t$ . In the set of even vertices, let  $a = 2u$  and  $b = 2v$ . Since both  $a$  and  $b$  are divisible by 2, their powers remain divisible by sufficiently high powers of 2. Thus, by choosing an appropriate modulus  $m = 2^t$  from  $M$ , we can always achieve the congruence relation  $a^k \equiv b \pmod{m}$  for some exponent  $k$ . Therefore, any two even vertices are adjacent, which means the even class forms a complete subgraph. On the other hand, for odd vertices  $a$  and  $b$ , note that in modulo 2, all odd numbers are congruent to 1. Since raising an odd number to any positive power keeps it odd, the congruence  $a^k \equiv b \pmod{2}$  is always satisfied since the difference of any two odd integers yields an even integer. Hence, every pair of odd vertices is adjacent under modulo 2, and therefore the odd class also induces a complete subgraph. Finally, we confirm that no adjacency exists between an even vertex  $a$  and an odd vertex  $b$ . For modulo 2, we have  $a \equiv 0$  and  $b \equiv 1$ . Raising either to any positive power preserves its parity, so the residues never match. For every moduli  $2^t$ , the distinction remains intact, as no even number can ever become congruent to an odd number modulo of a power of 2. Hence, there are no edges between the two classes. Putting all these facts together, we conclude that the graph decomposes into two disjoint complete subgraphs, one induced by the even vertices of size  $\lceil n/2 \rceil$  and one induced by the odd vertices of size  $\lfloor n/2 \rfloor$ . Thus,

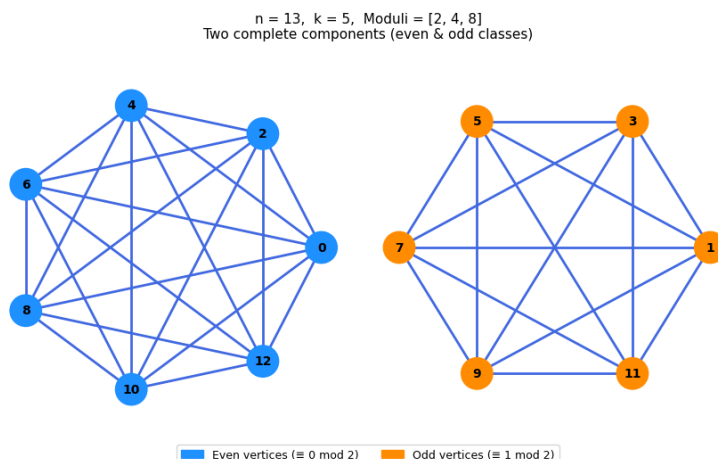
$$G \cong K_{\lceil n/2 \rceil} \cup K_{\lfloor n/2 \rfloor}.$$

□

Figures 1 and 2 illustrate the application of Theorem 3.1.



**Figure 1.** The graph  $G(12, 4, M_2)$  decomposes into two complete subgraphs.



**Figure 2.** The graph  $G(13, 5, M_2)$  decomposes into two complete subgraphs.

**Corollary 3.1.** *The following results are direct consequences of Theorem 3.1 and are stated without detailed proofs. In particular, the following statements hold:*

1. *The Eulerian components of  $G(n, k, M_2)$  are regular.*
2. *For  $G(n, k, M_2)$ , the two components  $K_{n_1}$  and  $K_{n_2}$  are isomorphic if and only if  $n$  is even.*
3. *For  $n \geq 4$ ,  $G(n, k, M_2)$  has no isolated vertex.*
4. *If  $n = 2t$ , then  $G(n, k, M_2)$  is the disjoint union of two  $(t - 1)$ -regular components and each is isomorphic to  $K_t$ , and if  $n = 2t + 1$ , then  $G(n, k, M_2)$  is the disjoint union of  $K_{t+1}$ , which is  $t$ -regular, and  $K_t$ , which is  $(t - 1)$ -regular.*
5. *The graph  $G(n, k, M_2)$  is not Hamiltonian, but the larger component of size  $n_1$  is Hamiltonian for  $n_1 \geq 3$ , i.e., for  $n \geq 5$ , and the smaller component of size  $n_2$  is Hamiltonian for  $n_2 \geq 3$ , i.e., for  $n \geq 6$ .*

**Corollary 3.2.** *Let  $G(n, k, M_2)$  be the disjoint union of two complete components  $K_{n_1}$  and  $K_{n_2}$  with  $n_1 \geq n_2$ . Then,*

1. *The chromatic number and clique number are equal:  $\chi(G(n, k, M_2)) = \omega(G(n, k, M_2)) = n_1$ .*
2. *The domination and independence number are equal:  $\gamma(G(n, k, M_2)) = \alpha(G(n, k, M_2)) = 1$  if  $n = 1$ , and 2 if  $n \geq 2$ .*

**Remark 3.1.** *Since  $G(n, k, M_2) \cong K_{n_1} \cup K_{n_2}$ , all matrix and spectral properties follow immediately from the well-known properties of complete graphs. In particular,*

$$A(G(n, k, M_2)) = \begin{pmatrix} J_{n_1} - I_{n_1} & O \\ O & J_{n_2} - I_{n_2} \end{pmatrix}, \quad L(G(n, k, M_2)) = \begin{pmatrix} n_1 I_{n_1} - J_{n_1} & O \\ O & n_2 I_{n_2} - J_{n_2} \end{pmatrix},$$

and

$$\text{spec}(A(G(n, k, M_2))) = \{n_1 - 1, n_2 - 1, (-1)^{(n-2)}\}, \quad \text{spec}(L(G(n, k, M_2))) = \{0^{(2)}, n_1^{(n_1-1)}, n_2^{(n_2-1)}\}.$$

Furthermore, if  $E = \binom{n_1}{2} + \binom{n_2}{2}$ , then

$$LE(G(n, k, M_2)) = 2 \left\lfloor \frac{2E}{n} \right\rfloor + (n_1 - 1) \left\lfloor n_1 - \frac{2E}{n} \right\rfloor + (n_2 - 1) \left\lfloor n_2 - \frac{2E}{n} \right\rfloor.$$

### 3.2. Structural analysis of power congruence graphs over modulus sets of the form $3^t$

In this subsection, we investigate the structure of PCGs defined over the modulus set  $M_3 = \{3^t : t \in \mathbb{Z}^+, 3^t < n\}$ . The structure of the graph is governed by the parity of the exponent  $k$ . For odd  $k$ , the graph decomposes into three disjoint complete components, whereas for even  $k$ , it consists of a complete component together with a  $K_n^F$  component. Based on this structural decomposition, we analyze key graph-theoretic parameters. We further examine some global properties. The following result provides a complete structural characterization of the graph.

**Theorem 3.2.** For  $n \geq 4$  and the moduli set  $M_3$ , the proposed graph  $G(n, k, M_3)$  in Definition 2.1

1. decomposes into three disjoint complete subgraphs if  $k$  is odd,

$$G(n, k, M_3) \cong K_{n_0} \cup K_{n_1} \cup K_{n_2},$$

where  $n_0 = \lfloor \frac{n}{3} \rfloor$ ,  $n_1 = \lfloor \frac{n-1}{3} \rfloor$ , and  $n_2 = \lfloor \frac{n}{3} \rfloor$ ;

2. decomposes into two disjoint subgraphs, one complete subgraph, and one  $K_n^F$  subgraph if  $k$  is even,

$$G(n, k, M_3) \cong K_{n_0} \cup K_{n_s}^F,$$

where  $n_0 = \lfloor \frac{n}{3} \rfloor$ ,  $n_s = \lfloor \frac{2n}{3} \rfloor$ ,  $F = \binom{\lfloor n/3 \rfloor}{2}$ , and  $K_{n_s}^F$  denotes the graph with exactly  $F$  edges less in complete graph  $K_{n_s}$ .

*Proof.* For  $n \geq 4$ , consider  $V = \{0, 1, 2, \dots, n-1\}$  as the vertex set and  $M_3 = \{3^t : 3^t < n, t \in \mathbb{Z}^+\}$  the modulus set. The partition of  $V$  into residue classes modulo 3 is:

$$V_0 = \{v \in V : v \equiv 0 \pmod{3}\}, V_1 = \{v \in V : v \equiv 1 \pmod{3}\}, V_2 = \{v \in V : v \equiv 2 \pmod{3}\}.$$

The sizes of these classes are  $n_0 = \lfloor \frac{n}{3} \rfloor$ ,  $n_1 = \lfloor \frac{n-1}{3} \rfloor$ , and  $n_2 = \lfloor \frac{n}{3} \rfloor$ , so that  $n_0 + n_1 + n_2 = n$ .

Since  $k \in \mathbb{Z}^+$ , we have two cases:

**Case I:** For odd  $k$ , the map  $x \mapsto x^k \pmod{3}$  fixes each residue class, i.e.,  $0^k \equiv 0$ ,  $1^k \equiv 1$ , and  $2^k \equiv 2 \pmod{3}$ . Thus two vertices from different residue classes can never be adjacent since for  $m = 3 \in M_3$ , their  $k$ -th powers remain distinct. On the other hand, if  $a, b \in V_i$  for some  $i \in \{0, 1, 2\}$ , then  $a^k \equiv a \equiv b \pmod{3}$ , so  $a$  and  $b$  are adjacent via modulus 3. Hence, each  $V_i$  induces a complete subgraph  $K_{n_i}$ , and no edges join different classes. Therefore,

$$G(n, k, M_3) \cong K_{n_0} \cup K_{n_1} \cup K_{n_2}.$$

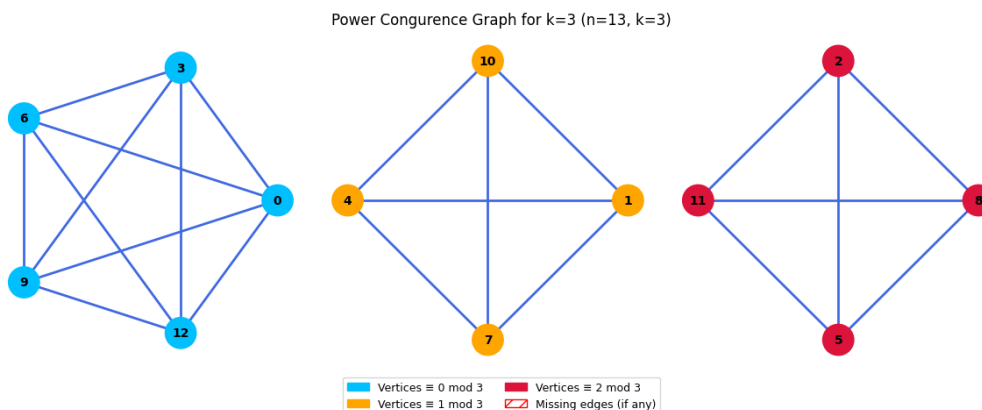
**Case II:** For even  $k$ , the reduction modulo 3 behaves differently, i.e.,  $0^k \equiv 0$ ,  $1^k \equiv 1$ , and  $2^k \equiv 1 \pmod{3}$ . Thus, all vertices in  $V_0$  remain mutually adjacent, forming a complete subgraph  $K_{n_0}$  where  $n_0 = |V_0| = \lfloor \frac{n}{3} \rfloor$ . Vertices in  $V_1 \cup V_2$  all map to residue 1 under  $x^k \pmod{3}$ . This ensures that every vertex in  $V_1 \cup V_2$  is adjacent to each vertex of  $V_1$ , but vertices in  $V_2$  may fail to connect among themselves for higher powers of 3 in  $M$ . Hence, the induced subgraph on  $n_s = n_1 + n_2 = \lfloor \frac{n-1}{3} \rfloor + \lfloor \frac{n}{3} \rfloor = \lfloor \frac{2n}{3} \rfloor$  is  $K_{n_s}^F$ , and it is  $K_{n_s}$  with precisely  $F$  edges missing. The number of missing edges inside the  $K_{n_s}^F$  component equals the number of unordered pairs lying entirely inside  $V_2$ , namely,  $F = \binom{n_2}{2} = \binom{\lfloor n/3 \rfloor}{2}$ .

Thus, for even  $k$ , we obtain

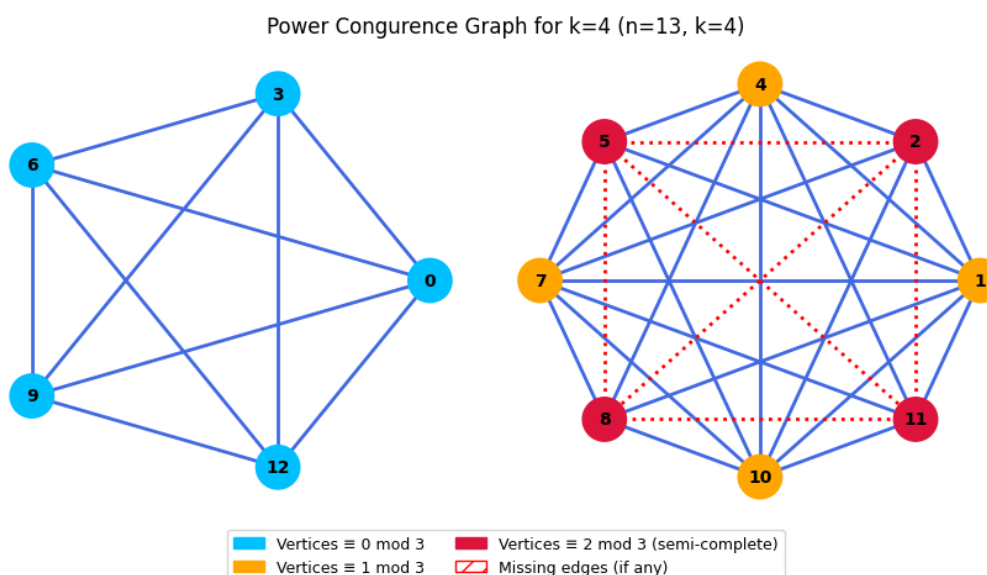
$$G(n, k, M_3) \cong K_{n_0} \cup K_{n_s}^F,$$

where  $K_{n_s}^F$  denotes the complete graph  $K_{n_s}$  with  $F$  edges less. □

Figures 3 and 4 illustrate an application of Theorem 3.2.



**Figure 3.** The graph  $G(13, 3, M_3)$  shows that the graph decomposes into three complete subgraphs for odd  $k$ .



**Figure 4.** The graph  $G(13, 4, M_3)$  shows that the graph decomposes into one complete and one  $K_n^F$  subgraph for even  $k$ .

**Theorem 3.3.** For an even power  $k$ , the only pairs of non-adjacent vertices inside the  $K_n^F$  component are

$$F = \{ \{3s + 2, 3t + 2\} : 0 \leq s < t, 3t + 2 \leq n - 1 \}.$$

Further, if  $r = \{v \in V : v \equiv 2 \pmod{3}\} = \lfloor \frac{n}{3} \rfloor$ , then  $|F| = \binom{r}{2} = \frac{r(r-1)}{2}$ .

*Proof.* The partition of the vertex set  $V = \{0, 1, \dots, n - 1\}$  over  $M_3$  is  $V_0 = \{v \in V : v \equiv 0 \pmod{3}\}$ ,  $V_1 = \{v \in V : v \equiv 1 \pmod{3}\}$ , and  $V_2 = \{v \in V : v \equiv 2 \pmod{3}\}$ . Write  $r = |V_2| = \lfloor \frac{n}{3} \rfloor$ . We show that when  $k$  is even, the only non-edges inside the  $K_n^F$  component are exactly the unordered pairs of vertices from  $V_2$ .

**Step 1:** For any integer  $x$ , we have  $x \equiv 0 \pmod{3} \Rightarrow x^k \equiv 0 \pmod{3}$ ,  $x \equiv 1 \pmod{3} \Rightarrow x^k \equiv 1 \pmod{3}$ , and  $x \equiv 2 \pmod{3} \Rightarrow x \equiv -1 \pmod{3} \Rightarrow x^k \equiv (-1)^k \pmod{3}$ . Since  $k$  is even,  $(-1)^k = 1$ . Thus, for even  $k$ , the map  $x \mapsto x^k \pmod{3}$  sends residues as  $0 \mapsto 0$ ,  $1 \mapsto 1$ , and  $2 \mapsto 1$ .

**Step 2:** Recall the adjacency rule of the proposed graph: Distinct vertices  $a, b$  are adjacent if  $a^k \equiv b \pmod{3}$ . Examine all residue class combinations.

- Pairs inside  $V_0$ : If  $u, v \in V_0$ , then  $u^k \equiv 0 \equiv v \pmod{3}$ . Hence,  $u^k \equiv v$  and  $u$  is adjacent to  $v$ . So,  $V_0$  is a clique.
- Pairs inside  $V_1$ : If  $x, y \in V_1$ , then  $x^k \equiv 1 \equiv y \pmod{3}$ . Hence,  $x^k \equiv y$  and  $x$  is adjacent to  $y$ . So,  $V_1$  is a clique.
- Between  $V_1$  and  $V_2$ : Take  $x \in V_1$ ,  $y \in V_2$ . Then  $y^k \equiv 1 \equiv x \pmod{3}$ , so  $y^k \equiv x$ ; therefore, every vertex of  $V_1$  is adjacent to every vertex of  $V_2$ . In graph language,  $V_1$  is completely joined to  $V_2$ .
- Pairs inside  $V_2$ : Let  $y_1, y_2 \in V_2$  be distinct. We have  $y_1^k \equiv 1$  and  $y_2^k \equiv 1 \pmod{3}$ . Because  $y_1 \equiv y_2 \equiv 2 \pmod{3}$ , neither  $y_1^k$  nor  $y_2^k$  can be congruent to 2 modulo 3. Thus, neither  $y_1^k \equiv y_2$  nor  $y_2^k \equiv y_1$  holds, so  $y_1$  and  $y_2$  are not adjacent.

**Step 3:** From the previous items, the union  $V_1 \cup V_2$  is a single subgraph in which every pair is adjacent except pairs lying entirely inside  $V_2$ . In other words, this subgraph is the complete graph on  $|V_1| + |V_2|$  vertices with exactly the missing edges coming from all unordered pairs of  $V_2$ , is, precisely a  $K_n^F$  graph  $K_{n_s}^F$  where the missing-edge set is

$$F = \{3s + 2, 3t + 2\} : 0 \leq s < t, 3t + 2 \leq n - 1\}$$

and the number of such missing edges is

$$|F| = \binom{r}{2} = \frac{r(r-1)}{2}.$$

□

**Example 1.** For  $n = 14$ , consider  $V = \{0, 1, 2, \dots, 13\}$  as the vertex set and  $M_3 = \{3^t : 3^t < 14\} = \{3, 9\}$  as the modulus set and fix an even power  $k = 4$ . Construct the graph  $G(14, 4, M_3)$  on  $V$  by declaring two distinct vertices  $a, b \in V$  adjacent if and only if, for some  $m \in M_3$ , the power congruence  $a^4 \equiv b \pmod{m}$  is satisfied.

*Proof.* Using Theorem 3.2, for an even  $k$ , the graph decomposes as  $G(n, k, M_3) \cong K_{n_0} \cup K_{n_s}^F$ , where  $n_0 = \lceil \frac{n}{3} \rceil = 5$ ,  $n_s = \lfloor \frac{2n}{3} \rfloor = 9$ , and  $F = \binom{\lfloor n/3 \rfloor}{2} = \binom{4}{2} = 6$ .

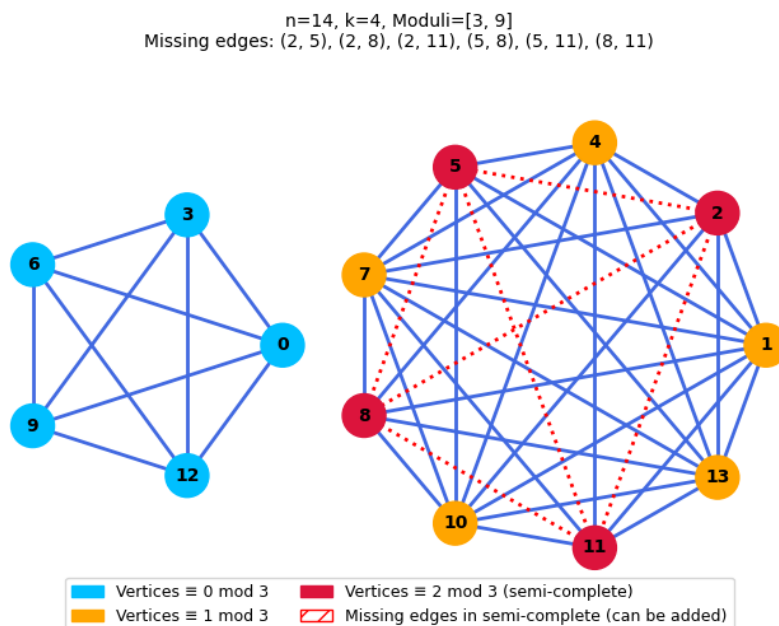
$$\Rightarrow G(14, 4, M_3) \cong K_5 \cup K_9^6.$$

Using Theorem 3.3, the missing edges in the  $K_n^F$  component are  $F = \{3s + 2, 3t + 2\} : 0 \leq s < t, 3t + 2 \leq n - 1\}$ . For  $n = 14$ ,  $R_2 = \{2, 5, 8, 11\}$ , so the missing edges are

$$\{2, 5\}, \{2, 8\}, \{2, 11\}, \{5, 8\}, \{5, 11\}, \{8, 11\},$$

as shown in Figure 5.

□



**Figure 5.** The graph  $G(14, 4, M_3)$  is  $K_5 \cup K_9^6$  and shows that it has six missing edges in the  $K_n^F$  component.

**Corollary 3.3.** For  $G(n, k, M_3)$ , the following statements hold:

1. The degree of a vertex  $u$  in  $G(n, k, M_3)$  depends on  $k$ .  $k$  is odd, then  $\deg(u) = n_i - 1$  if  $u \in V_i$ , and if  $k$  is even, then  $\deg(u) = n_0 - 1$  if  $u \in V_0$ ,  $\deg(u) = n_s - 1$  if  $u \in V_1$ , and  $\deg(u) = n_s - r$  if  $u \in V_2$ .
2. The number of edges for  $G(n, k, M_3)$  is  $\binom{n_0}{2} + \binom{n_1}{2} + \binom{n_2}{2}$  if  $k$  is odd and  $\binom{n_0}{2} + \binom{n_s}{2} - \binom{r}{2}$  if  $k$  is even.
3. If  $k$  is odd, the number of Eulerian components equals the number of those  $n_i$  that are odd.  $k$  is even, then  $K_{n_0}$  is Eulerian if and only if  $n_0$  is odd. The component  $K_{n_s}^F$  is Eulerian if and only if both  $n_s$  and  $r = \lfloor n/3 \rfloor$  are odd.
4. If  $n \geq 6$ , then  $G(n, k, M_3)$  has no isolated vertex.
5. Each complete component  $K_t$  of  $G(n, k, M_3)$  is  $(t - 1)$ -regular. Moreover, the number and degrees of the components are determined by the residue-class partition  $n_0, n_1, n_2$  when  $k$  is odd or  $n_0, n_s$  when  $k$  is even, not solely by the parity of  $n$ .
6. If  $k$  is odd and  $n$  is a multiple of 3, then components are regular and mutually isomorphic.
7.  $G(n, k, M_3)$  is not Hamiltonian, but every complete component  $K_t$  in  $G(n, k, M_3)$  is Hamiltonian for  $t \geq 3$ , and the  $K_n^F$  component  $K_{n_s}^F$  is Hamiltonian if it is sufficiently dense.

**Corollary 3.4.** For  $G(n, k, M_3)$ , the chromatic, clique, domination, and independence numbers are

$$\chi(G(n, k, M_3)) = \omega(G(n, k, M_3)) = \begin{cases} \max\{n_0, n_1, n_2\}, & \text{if } k \text{ is odd,} \\ \max\{n_0, n_s + 1\}, & \text{if } k \text{ is even.} \end{cases}$$

$$\gamma(G(n, k, M_3)) = \begin{cases} 3, & \text{if } k \text{ is odd,} \\ 2, & \text{if } k \text{ is even.} \end{cases}$$

$$\alpha(G(n, k, M_3)) = \begin{cases} 3, & \text{if } k \text{ is odd,} \\ 1 + n_2, & \text{if } k \text{ is even.} \end{cases}$$

Let us notice that, as done in the previous section, Theorem 3.2 allows us to calculate both the adjacency and the Laplacian matrices. We omit the details since they follow easily from what we have proved until now.

### 3.3. Structural analysis of power congruence graphs over modulus sets of the form $5^t$

In this subsection, we investigate the structure of PCGs defined over the modulus set  $M_5 = \{5^t : t \in \mathbb{Z}^+, 5^t < n\}$ . In contrast to the cases  $p = 2$  and  $p = 3$ , the resulting graphs exhibit more intricate structural behavior. In particular, the structure depends on the residue of the exponent  $k \pmod{4}$ , leading to multiple distinct configurations involving both complete and  $K_n^F$  components. Based on this structural decomposition, we analyze key graph-theoretic parameters. The following theorem provides a complete structural characterization of the graph.

**Theorem 3.4.** *For  $n \geq 6$  and the moduli set  $M_5$ , the proposed graph  $G(n, k, M_5)$  in Definition 2.1 depends on the residue of  $k$  modulo 4 as follows:*

1. If  $k \equiv 1 \pmod{4}$  (i.e.,  $k = 1, 5, 9, \dots$ ), then

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_1} \cup K_{n_2} \cup K_{n_3} \cup K_{n_4}.$$

2. If  $k \equiv 2 \pmod{4}$  (i.e.,  $k = 2, 6, 10, \dots$ ), then

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_s}^F,$$

where  $n_s = n - n_0$  and

$$F = \binom{n_s}{2} - \binom{n_1}{2} - n_4(n_1 + n_2 + n_3).$$

3. If  $k \equiv 3 \pmod{4}$  (i.e.,  $k = 3, 7, 11, \dots$ ), then

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_1} \cup K_{n_4} \cup K_{n_2+n_3}^F,$$

where

$$F = \binom{n_2}{2} + \binom{n_3}{2}.$$

4. If  $k \equiv 0 \pmod{4}$  (i.e.,  $k = 4, 8, 12, \dots$ ), then

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_s}^F,$$

where  $n_s = n - n_0$  and

$$F = \binom{n_s - 1}{2},$$

where  $K_{n_s}^F$  denotes a complete graph  $K_{n_s}$  with exactly  $F$  edges less, and  $n_i$ 's are the partitions of  $V$  according to residue classes modulo 5 as  $V_i = \{x \in V : x \equiv i \pmod{5}\}$ ,  $i = 0, 1, 2, 3, 4$ , with sizes

$$n_0 = \left\lfloor \frac{n+4}{5} \right\rfloor, \quad n_1 = \left\lfloor \frac{n+3}{5} \right\rfloor, \quad n_2 = \left\lfloor \frac{n+2}{5} \right\rfloor, \quad n_3 = \left\lfloor \frac{n+1}{5} \right\rfloor, \quad n_4 = \left\lfloor \frac{n}{5} \right\rfloor.$$

*Proof.* Let  $V = \{0, 1, 2, \dots, n-1\}$  and consider the modulus set  $M_5 = \{5^t : t \in \mathbb{N}, 5^t < n\}$ . Partition of  $V$  into residue classes modulo 5 is  $V_i = \{x \in V : x \equiv i \pmod{5}\}$ ,  $i = 0, 1, 2, 3, 4$ . Since congruence modulo  $5^t$  preserves residue classes modulo 5, the adjacency between vertices is governed by the behavior of  $k$  modulo 4, due to the cyclic structure of the multiplicative residues modulo 5.

**Case 1:**  $k \equiv 1 \pmod{4}$ . In this case, exponentiation preserves each residue class, that is, for any  $a \in V_i$ , we have  $a^k \equiv a \pmod{5}$ . Hence, vertices within the same class  $V_i$  are mutually adjacent, forming complete subgraphs. Since no residue class maps into another, there are no edges between different classes. Therefore,

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_1} \cup K_{n_2} \cup K_{n_3} \cup K_{n_4}.$$

**Case 2:**  $k \equiv 2 \pmod{4}$ . Here, exponentiation induces interactions between different residue classes. The class  $V_0$  remains invariant and forms a complete component  $K_{n_0}$ . The remaining vertices form a subgraph on  $n_s = n - n_0$  vertices. However, not all pairs are adjacent, as certain residue combinations do not satisfy the defining congruence. Starting from the complete graph  $K_{n_s}$ , the number of missing edges corresponds to forbidden adjacencies within  $V_1$  and between  $V_4$  and the sets  $V_1, V_2$ , and  $V_3$ . Counting these exclusions yields

$$F = \binom{n_s}{2} - \binom{n_1}{2} - n_4(n_1 + n_2 + n_3),$$

and hence

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_s}^F.$$

**Case 3:**  $k \equiv 3 \pmod{4}$ . In this case, exponentiation permutes residue classes differently. The classes  $V_0, V_1$ , and  $V_4$  remain internally complete and mutually disconnected, forming  $K_{n_0}, K_{n_1}$ , and  $K_{n_4}$ . The union  $V_2 \cup V_3$  induces a subgraph that is not complete, as edges within  $V_2$  and within  $V_3$  are restricted. Starting from  $K_{n_2+n_3}$ , the missing edges correspond exactly to the internal pairs of  $V_2$  and  $V_3$ , giving

$$F = \binom{n_2}{2} + \binom{n_3}{2}.$$

Thus,

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_1} \cup K_{n_4} \cup K_{n_2+n_3}^F.$$

**Case 4:**  $k \equiv 0 \pmod{4}$ . In this case, exponentiation collapses residue distinctions further. The class  $V_0$  again forms a complete component  $K_{n_0}$ , while the remaining vertices form a subgraph on  $n_s = n - n_0$  vertices with missing edges. From  $K_{n_s}$ , the excluded edges correspond to restricted adjacencies determined by the exponent, yielding

$$F = \binom{n_s - 1}{2}.$$

Hence,

$$G(n, k, M_5) \cong K_{n_0} \cup K_{n_s}^F.$$

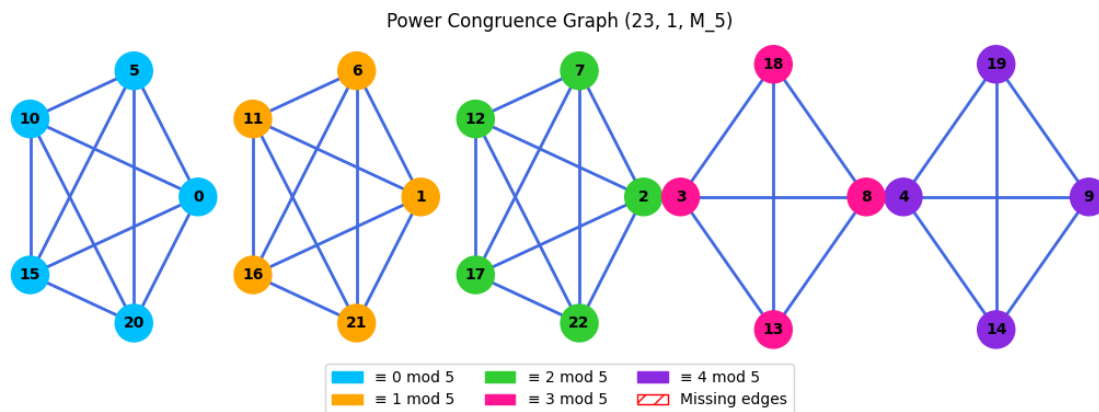
Combining all cases, the structure of  $G(n, k, M_5)$  is completely determined by the residue class of  $k$  modulo 4.  $\square$

**Example 2.** Consider  $n = 23$  and the modulus set  $M_5 = \{5\}$ . By Theorem 3.4,  $n_0 = \lfloor \frac{n+4}{5} \rfloor = \lfloor \frac{23+4}{5} \rfloor = 5$ ,  $n_1 = \lfloor \frac{23+3}{5} \rfloor = 5$ ,  $n_2 = \lfloor \frac{23+2}{5} \rfloor = 5$ ,  $n_3 = \lfloor \frac{23+1}{5} \rfloor = 4$ , and  $n_4 = \lfloor \frac{23}{5} \rfloor = 4$ .

**Case 1:**  $k = 1$  ( $k \equiv 1 \pmod{4}$ ). Each residue class induces a complete component. Hence,

$$G(23, 1, M_5) \cong K_5 \cup K_5 \cup K_5 \cup K_4 \cup K_4,$$

as shown in Figure 6.

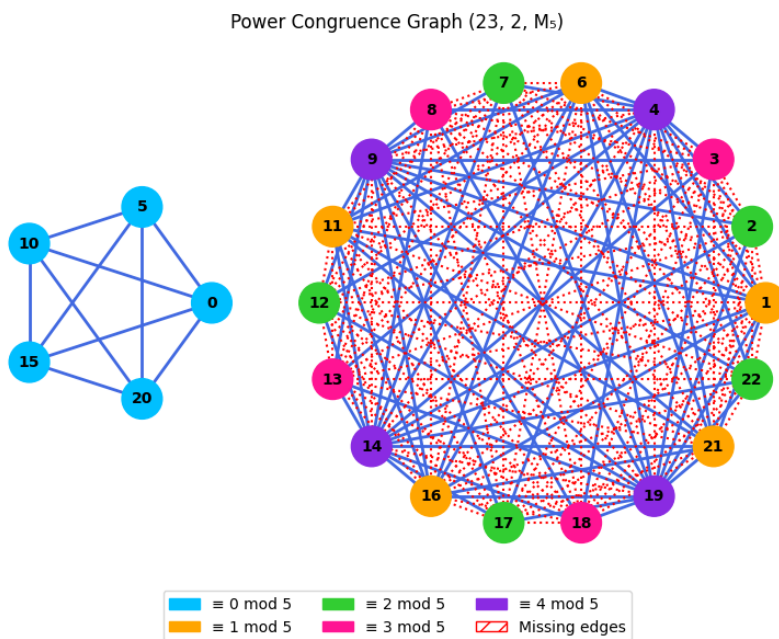


**Figure 6.** The graph  $G(23, 1, M_5)$  shows that it decomposes to  $K_5 \cup K_5 \cup K_5 \cup K_4 \cup K_4$ .

**Case 2:**  $k = 2$  ( $k \equiv 2 \pmod{4}$ ). The graph decomposes into a complete component and a  $K_n^F$  component. Hence,

$$G(23, 2, M_5) \cong K_5 \cup K_{18}^{87},$$

where  $F = \binom{18}{2} - \binom{5}{2} - 4(5 + 5 + 4) = 153 - 10 - 56 = 87$ , as shown in Figure 7.

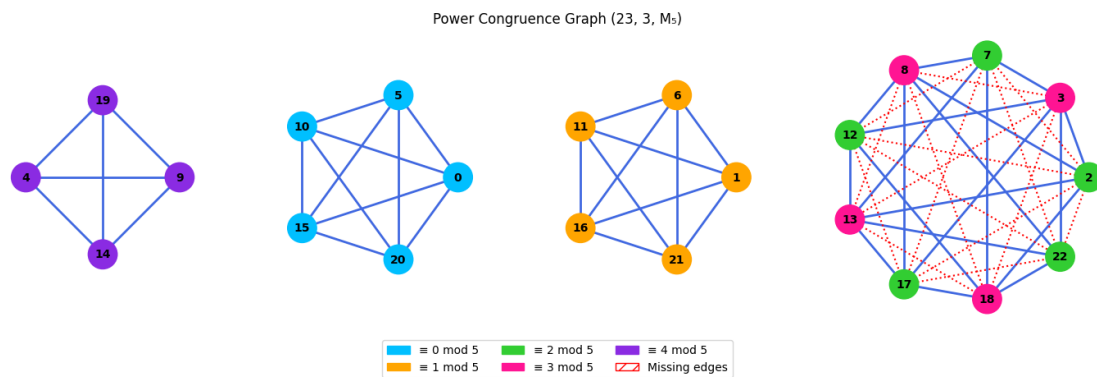


**Figure 7.** The graph  $G(23, 2, M_5)$  shows that it decomposes to  $K_5 \cup K_{18}^{87}$ .

**Case 3:**  $k = 3$  ( $k \equiv 3 \pmod{4}$ ). The graph decomposes as

$$G(23, 3, M_5) \cong K_5 \cup K_5 \cup K_4 \cup K_9^{16},$$

where  $F = \binom{5}{2} + \binom{4}{2} = 10 + 6 = 16$ , as shown in Figure 8.

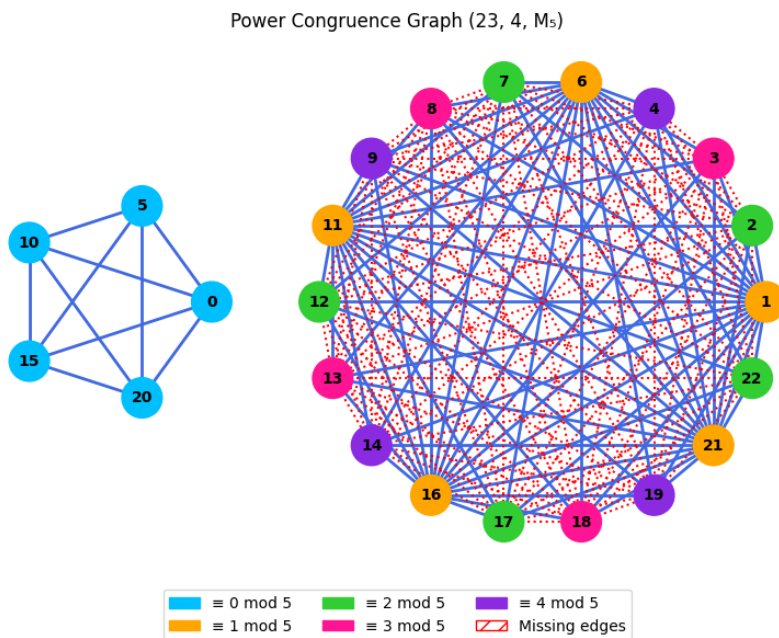


**Figure 8.** The graph  $G(23, 3, M_5)$  shows that it decomposes to  $K_5 \cup K_5 \cup K_4 \cup K_9^{16}$ .

**Case 4:**  $k = 4$  ( $k \equiv 0 \pmod{4}$ ). The graph decomposes as

$$G \cong K_5 \cup K_{18}^{136},$$

where  $F = \binom{17}{2} = 136$ , as shown in Figure 9.



**Figure 9.** The graph  $G(23, 4, M_5)$  shows that it decomposes to  $K_5 \cup K_{18}^{136}$ .

This example clearly illustrates how the structure of  $G(23, k, M_5)$  varies with  $k \pmod{4}$ , producing both complete and  $K_n^F$  components.

The following results are direct consequences of Theorem 3.4 and are stated without proof, since the methods are the same as in the previous sections.

**Corollary 3.5.** Consider  $G(n, k, M_5)$  as defined in Theorem 3.4. Then, the degree of each vertex depends on the component it belongs to:

1. If  $k \equiv 1 \pmod{4}$ , then for  $v \in V_i$ ,

$$\deg(v) = n_i - 1.$$

2. If  $k \equiv 2 \pmod{4}$  or  $k \equiv 0 \pmod{4}$ , then

$$\deg(v) = \begin{cases} n_0 - 1, & v \in V_0, \\ \leq n_s - 1, & v \in V \setminus V_0. \end{cases}$$

3. If  $k \equiv 3 \pmod{4}$ , then

$$\deg(v) = \begin{cases} n_0 - 1, & v \in V_0, \\ n_1 - 1, & v \in V_1, \\ n_4 - 1, & v \in V_4, \\ \leq (n_2 + n_3) - 1, & v \in V_2 \cup V_3. \end{cases}$$

**Corollary 3.6.** The size of  $G(n, k, M_5)$  as defined in Theorem 3.4 is the following:

1. If  $k \equiv 1 \pmod{4}$ , then

$$|E(G(n, k, M_5))| = \sum_{i=0}^4 \binom{n_i}{2}.$$

2. If  $k \equiv 2 \pmod{4}$  or  $k \equiv 0 \pmod{4}$ , then

$$|E(G(n, k, M_5))| = \binom{n_0}{2} + \binom{n_s}{2} - F.$$

3. If  $k \equiv 3 \pmod{4}$ , then

$$|E(G(n, k, M_5))| = \binom{n_0}{2} + \binom{n_1}{2} + \binom{n_4}{2} + \binom{n_2 + n_3}{2} - F.$$

**Corollary 3.7.** For  $G(n, k, M_5)$  as in Theorem 3.4, the chromatic number and clique number are the following:

1. If  $k \equiv 1 \pmod{4}$ , then

$$\chi(G(n, k, M_5)) = \omega(G(n, k, M_5)) = \max\{n_0, n_1, n_2, n_3, n_4\}.$$

2. If  $k \equiv 2 \pmod{4}$  or  $k \equiv 0 \pmod{4}$ , then

$$\chi(G(n, k, M_5)) = \omega(G(n, k, M_5)) = \max\{n_0, n_s\}.$$

3. If  $k \equiv 3 \pmod{4}$ , then

$$\chi(G(n, k, M_5)) = \omega(G(n, k, M_5)) = \max\{n_0, n_1, n_4, n_2 + n_3\}.$$

**Corollary 3.8.**  $G(n, k, M_5)$  is Eulerian if and only if all vertex degrees are even. Each complete component  $K_{n_i}$  is Hamiltonian for  $n_i \geq 3$ .

**Remark 3.2.** The adjacency matrix  $A(G(n, k, M_5))$  is block diagonal, with each block corresponding to a component of  $G(n, k, M_5)$ . Each complete component contributes a matrix of the form  $J - I$ , where  $J$  is the all-ones matrix. The Laplacian matrix  $L(G(n, k, M_5)) = D(G(n, k, M_5)) - A(G(n, k, M_5))$  is also block diagonal, with each block corresponding to the Laplacian of the respective component.

**Remark 3.3.** For each complete component  $K_r$ , the adjacency spectrum is  $\{(r - 1)^1, (-1)^{r-1}\}$ . The Laplacian spectrum of  $K_r$  is  $\{0^1, r^{r-1}\}$ . The energy of  $G$  is the sum of the energies of its components. In particular, for complete components  $E(K_r) = 2(r - 1)$ . The Laplacian energy is obtained similarly from the Laplacian eigenvalues of each component.

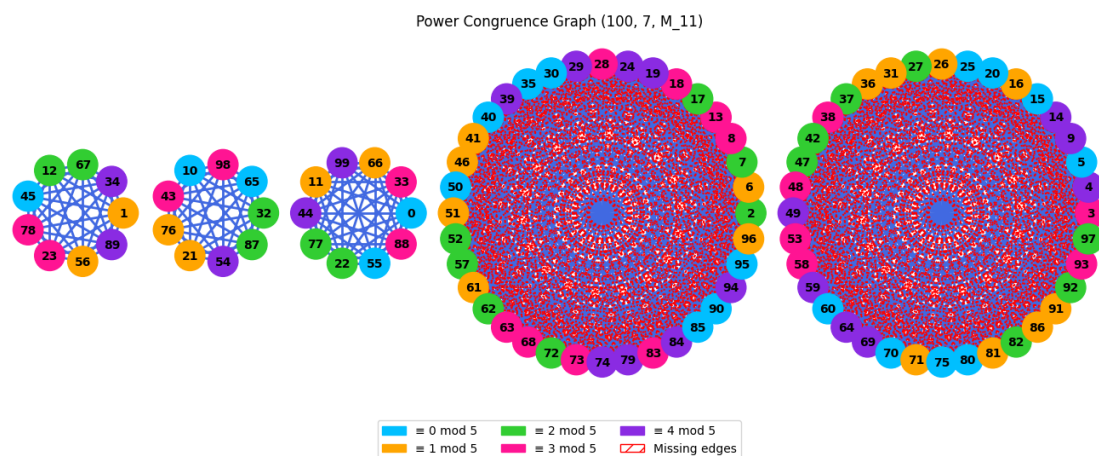
### 3.4. Generalization of power congruence graphs over modulus sets of the form $p^t$

We now extend the preceding analysis to modulus sets of the form  $M_p = \{p^t : t \in \mathbb{N}, p^t < n\}$ , where  $p$  is a prime. Let  $G(n, k, M_p)$  denote the corresponding PCG. The structural behavior of  $G(n, k, M_p)$  is governed by the arithmetic properties of exponentiation modulo  $p$ . In particular, since the multiplicative group modulo a prime  $p$  is cyclic of order  $p - 1$ , the structure of the graph depends on the residue of  $k$  modulo  $p - 1$ .

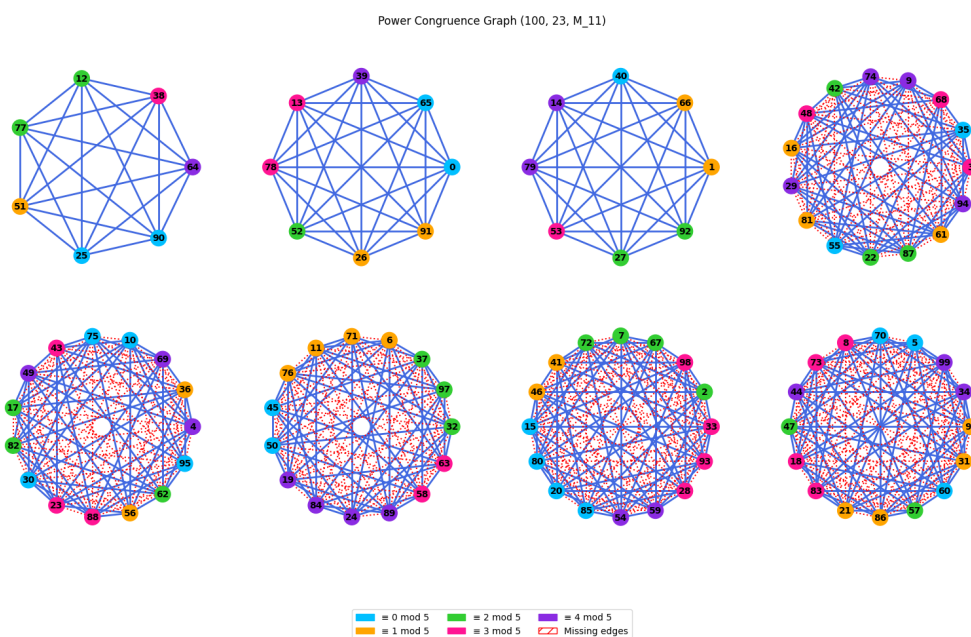
**Theorem 3.5.** Let  $p$  be a prime and consider the PCG  $G(n, k, M_p)$ . Then the structure of  $G$  is determined by the residue class of  $k \pmod{p - 1}$ . In particular, up to  $p - 1$ , distinct structural types of graphs arise as  $k$  varies.

**Remark 3.4.** As  $p$  increases, the resulting graphs exhibit progressively richer structural behavior, including configurations that are not restricted to unions of complete graphs. This highlights the non-trivial nature of the proposed construction and its dependence on both the modulus and the exponent.

To further illustrate the structural richness of the proposed graph family, we present computational experiments and corresponding visualizations for selected parameter sets in Figures 10 and 11, which reveal unexpectedly intricate connectivity patterns and motivate deeper investigation of their topological and Hamiltonian properties.



**Figure 10.** The graph  $G(100, 7, M_{11})$  is a disjoint union of three complete and two  $K_n^F$  components.



**Figure 11.** The graph  $G(100, 23, M_{13})$  is a disjoint union of three complete and five  $K_n^F$  components.

These computational observations suggest that the structural behavior of  $G(n, k, M_p)$  is highly sensitive to parameter selection.

**Theorem 3.6.** Let  $G(n, k, M_p)$  be the graph constructed on the vertex set  $V$ . Since every connected component of  $G(n, k, M_p)$  is either a complete graph or a graph of the form  $K_r^F$  for some  $F \subseteq E(K_r)$ , where  $K_r^F$  is obtained from a complete graph by deleting a set of edges  $F$ , each component of  $G(n, k, M_p)$  is Hamiltonian.

#### 4. Applications of power congruence graphs over sets of moduli

PCGs provide a natural bridge between number theory and graph theory by converting power congruence relations into structures. The defining relation  $a^k \equiv b \pmod{m}$  induces adjacency patterns that reflect residue class behavior and modular symmetries. The structural results obtained in this article show that the graph behavior depends strongly on the choice of modulus set  $M_p = \{p^f\}$  and the exponent  $k$ . Modular exponentiation is central to many cryptographic systems. PCGs provide a structural representation of power mappings and residue transitions that offers insight into the connectivity and distribution of modular states, which may be useful in analyzing exponentiation-based transformations. PCGs can be used to model systems where nodes are partitioned according to residue classes and connections are governed by modular rules. The decomposition into components reflects modular clustering and controlled interaction patterns. PCGs offer a graphical interpretation of power residues and modular transformations. Classical graph invariants such as clique number, chromatic number, independence number, and spectral properties provide tools to study the distribution and interaction of residue classes. Modern digital systems including microcontrollers and digital signal processors operate under modular arithmetic due to finite precision. In such systems, transformations of the form  $x \mapsto x^k \pmod{m}$  arise naturally in pseudo random number generators, cyclic counters,

and residue number systems. Overall, PCGs provide a flexible framework for understanding systems governed by modular exponentiation. Their structure, which becomes increasingly rich for larger primes, offers both theoretical insight and potential applications in computational and engineering settings.

## 5. Conclusions and future work

In this article, we studied the structural properties of PCGs arising from relations of the form  $a^k \equiv b \pmod{m}$ , with modulus sets of the form  $M_p = \{p^t : p^t < n\}$ . We provided a systematic analysis for the cases  $p = 2$ ,  $p = 3$ , and  $p = 5$ , showing that the structure of these graphs is governed by the interplay between the modulus and the exponent  $k$ . For  $p = 2$ , the graphs decompose into two complete components for all values of  $k$ . For  $p = 3$ , the structure depends on the parity of  $k$  with either three complete components or a combination of complete and  $K_n^F$  components. For  $p = 5$ , we observed a significantly richer behavior, where the structure depends on  $k \pmod{4}$  and includes configurations involving  $K_n^F$  components. More generally, for a prime  $p$ , the structure of  $G(n, k, M_p)$  depends on  $k \pmod{p-1}$ , leading to up to  $p-1$  distinct structural configurations. These results demonstrate that the complexity of the graph increases with the modulus and that the structure is closely tied to residue class interactions. Beyond structural characterization, we derived key graph theoretic parameters and spectral properties. Together, these results establish a coherent framework for understanding graphs generated by power congruence relations and highlight the transition from simple to more intricate structures as the modulus varies.

The present study opens several directions for further research. A natural extension is the investigation of PCGs for general prime moduli, where the structure is expected to depend on  $k \pmod{p-1}$ , potentially leading to up to  $p-1$  distinct graph types. A deeper analysis of spectral characteristics including adjacency and Laplacian eigenvalues and energy may reveal additional structural insights. Further work may also focus on domination parameters, labeling problems, and automorphism groups of these graphs. Another promising direction is the study of more general congruence relations, such as quadratic or higher-order mappings, which may produce structurally different graph families. Overall, PCGs provide a flexible and structured framework that connects modular arithmetic with graph theory, and they offer a foundation for future investigations into number-theoretic graph constructions.

## Author contributions

Muhammad Awais Raza: Conceptualization, methodology, formal analysis, investigation, visualization, writing – original draft; Muhammad Khalid Mahmood: Conceptualization, supervision, validation, writing – review & editing; Daniele Ettore Otera: Validation, formal analysis, resources, writing – review & editing. All authors have read and agreed to the published version of the manuscript.

## Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

## Acknowledgments

We acknowledge that the work present in this manuscript will be used for the final PhD thesis preparation of Mr. Muhammad Awais Raza, pursuing his PhD degree at Institute of Mathematics, University of the Punjab, Lahore, Pakistan.

## Conflict of interest

All authors declare no conflicts of interest in this paper.

## References

1. M. H. Mateen, M. K. Mahmood, Power digraphs associated with the congruence  $x^n \equiv y \pmod{m}$ , *Punjab Univ. J. Math.*, **51** (2020).
2. M. B. Nathanson, I. Z. Ruzsa, Additive number theory: Inverse problems and the geometry of sumsets, *B. Lond. Math. Soc.*, **31** (1999), 108.
3. A. P. Peranginangin, Application of number theory in cryptography, *Int. J. Educ. Res. Excell. (IJERE)*, **3** (2024), 67–76. <https://doi.org/10.55299/ijere.v3i1.733>
4. H. Daoub, O. Shafah, A. A. Almutlg, Exploring a graph complement in quadratic congruence, *Symmetry*, **16** (2024), 213. <https://doi.org/10.3390/sym16020213>
5. M. B. Nathanson, Connected components of arithmetic graphs, *Monatsh. Math.*, **89** (1980), 219–222. <https://doi.org/10.1007/BF01295437>
6. E. L. Blanton Jr, S. P. Hurd, J. S. McCranie, On a digraph defined by squaring modulo  $n$ , *Fibonacci Quart.*, **30** (1992), 322–333. <https://doi.org/10.1080/00150517.1992.12429334>
7. C. Lucheta, E. Miller, C. Reiter, Digraphs from powers modulo  $p$ , *Fibonacci Quart.*, **34** (1996), 226–239. <https://doi.org/10.1080/00150517.1996.12429067>
8. L. Somer, M. Křížek, On symmetric digraphs of the congruence  $x^k \equiv y \pmod{n}$ , *Discrete Math.*, **309** (2009), 1999–2009.
9. M. H. Mateen, M. K. Mahmood, S. Ali, *Importance of power digraph in computer science*, In: International Conference on Innovative Computing (ICIC), 2019, 1–6. <https://doi.org/10.1109/ICIC48496.2019.8966737>
10. M. H. Mateen, S. Ali, M. A. Alam, On symmetry of complete graphs over quadratic and cubic residues, *J. Chemistry*, **2021** (2021), 4473637. <https://doi.org/10.1155/2021/4473637>
11. M. K. Mahmood, D. Ahmad, Order structured graphs of cyclic groups and their classification, *VFAST T. Math.*, **12** (2024), 220–233. <https://doi.org/10.21015/vtm.v12i1.1756>
12. G. Deng, P. Yuan, Symmetric digraphs from powers modulo  $n$ , *Open J. Discrete Math.*, **1** (2011), 103.
13. S. Asif, M. K. Mahmood, Structural properties of the graphs arising from congruences over set of moduli, *JP J. Algebr. Number T.*, **64** (2025), 81–98. <https://doi.org/10.3917/gdsh.081.0098>
14. A. D. Christopher, A class of graphs based on a set of moduli, *Integers*, **22** (2022), 1–15.

15. A. Almutlg, M. A. Raza, Symmetry and structural analysis of power congruence graphs over a set of moduli, *Symmetry*, **18** (2026), 582. <https://doi.org/10.3390/sym18040582>
16. S. Asif, M. K. Mahmood, A. S. Alali, A. A. Zaagan, Structures and applications of graphs arising from congruences over moduli, *AIMS Math.*, **9** (2024), 21786–21798. <https://doi.org/10.3934/math.20241059>
17. Z. I. Borevich, I. R. Shafarevich, *Number theory*, volume 20. Academic press, 1986.
18. P. Zhang, G. Chartrand, *Introduction to graph theory*, volume 2, Tata McGraw-Hill, New York, 2006.



AIMS Press

©2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0>)