Perfect and Near-Perfect Matchings in Bilinear Congruence Graphs over $\mathbb{Z}_n$

Hamza A. Daoub
Department of Mathematics, School of Basic Sciences name of Libyan Academy for Postgraduate Studies, Tripoli, Libya
h.daoub@academy.edu.ly

Abstract: We study matching and covering parameters of the bilinear congruence graph $\boldsymbol{G_n}$ over the ring $\mathbb{Z}_n$. The graph has vertex set $\mathbb{Z}_n^2$, and two distinct vertices $(\boldsymbol{a},\boldsymbol{b})$ and $(\boldsymbol{x},\boldsymbol{y})$ are adjacent whenever $\boldsymbol{ay \equiv bx \pmod n}$. This adjacency is a determinant-zero condition, so it describes modular dependence between ordered pairs rather than the usual product-zero relation from zero-divisor graphs. We prove that, for every odd integer $\boldsymbol{n \geq 3}$, the map $(\boldsymbol{a},\boldsymbol{b}) \mapsto (\boldsymbol{-a},\boldsymbol{-b})$ gives a near-perfect matching of $\boldsymbol{G_n}$. Consequently,

$$\nu(G_n) = \frac{n^2-1}{2}, \rho(G_n) = \frac{n^2+1}{2}.$$

For an odd prime $\boldsymbol{p}$, the proportionality class decomposition gives

$$\boldsymbol{\alpha(G_p) = p+1, \tau(G_p) = p^2 - p - 1}.$$

For distinct primes $\boldsymbol{p}$ and $\boldsymbol{q}$, we prove the exact independence formula

$$\alpha(G_{pq}) = (p+1)(q+1),$$

and hence

$$\tau(G_{pq}) = p^2q^2 - (p+1)(q+1).$$

In the case $\boldsymbol{n = 2q}$, where $\boldsymbol{q}$ is an odd prime, we construct a perfect matching and deduce

$$\nu(G_{2q}) = \rho(G_{2q}) = 2q^2.$$

Finally, computations for $\boldsymbol{2 \leq n \leq 30}$ support the study and suggest that $\boldsymbol{G_n}$ may have a perfect matching for every even $\boldsymbol{n \geq 4}$.

Keywords: Bilinear Congruence Graph, Matching Number, Perfect Matching, Near-Perfect Matching, Edge Cover, Vertex Cover, Finite Rings, Modular Dependence, Determinant-Zero Congruence.

I. INTRODUCTION

The study of graphs associated with algebraic structures has become an active area connecting ring theory, graph theory, and finite algebraic systems. One of the most important examples is the zero-divisor graph of a commutative ring. This direction began with Beck's work on colorings of commutative rings [1], and was later developed in its modern form by Anderson and Livingston [2]. Since then, several structural properties of zero-divisor graphs, such as diameter, girth, coloring, and ideal-based variants, have been studied in different settings [3, 4, 5].

A related but different direction is to define graphs by congruence relations over the ring of integers modulo n. In this paper, we focus on the bilinear congruence graph G_n, whose vertex set is $V(G_n) = \mathbb{Z}_n^2$. Two distinct vertices (a,b) and (x,y) are adjacent whenever $ay \equiv bx \pmod n$. Thus adjacency is not defined by a product-zero condition, but by a determinant-zero condition. This makes G_n closer to modular dependence and projective-type behavior over finite rings than to the usual zero-divisor graph. Projective lines over rings and related modular dependence structures have been studied in different forms in [6, 7]. The bilinear congruence graph itself was studied structurally in [8], where adjacency, independent sets, complete subgraphs, Hamiltonian behavior, and connectivity were considered.

The present paper develops a matching-theoretic and covering-theoretic study of G_n. Matching theory is a central part of graph theory, with classical foundations going back to Berge and Tutte [9, 10]. The standard theory is developed in detail in Lovász and Plummer [11], and general graph theory background may be found in [12, 13, 14]. We shall use the matching number $\nu(G)$, the independence number $\alpha(G)$, the vertex-cover number $\tau(G)$, and the edge-cover number $\rho(G)$. These parameters are connected by the classical Gallai identities [15]:

$$\alpha(G) + \tau(G) = |V(G)|,$$

and, when G has no isolated vertices,

$$\nu(G) + \rho(G) = |V(G)|.$$

These identities allow matching results to produce covering results in a natural way.

The motivation for this work comes partly from recent attempts to study maximum matchings in algebraic graphs, especially zero-divisor graphs [16]. However, in the zero-divisor graph of $\mathbb{Z}_{pq}$, where $p < q$ are primes, the graph is a complete bipartite graph, so the matching number follows directly from the sizes of the two parts. In contrast, the bilinear congruence graph G_n has a richer modular structure. Its matching behavior is controlled by the universal vertex $(0,0)$, proportionality classes when n is prime, the symmetry $(a,b) \mapsto (-a,-b)$, and the Chinese Remainder Theorem when n is composite. The required background on modular rings and finite rings is standard and can be found in [17, 18].

The main contributions of this paper are as follows. First, we prove a general near-perfect matching theorem for every odd modulus. More precisely, for every odd integer $n \geq 3$, the

involution $(a,b) \mapsto (-a,-b)$ pairs every nonzero vertex with an adjacent vertex and fixes only $(0,0)$. Consequently,

$$\nu(G_n) = \frac{n^2-1}{2}, \rho(G_n) = \frac{n^2+1}{2}.$$

This includes, the case $n = pq$, where p and q are distinct odd primes.

Second, for an odd prime p, we use the proportionality-class decomposition of $\mathbb{Z}_p^2 \backslash \{(0,0)\}$ to determine the independence number and the vertex-cover number:

$$\alpha(G_p) = p+1, \tau(G_p) = p^2 - p - 1.$$

Thus the odd prime case gives a complete matching and covering profile.

Third, we study the composite family $n = 2q$, where q is an odd prime. In this case, the negative-pair involution has four fixed points, so the odd-modulus construction does not apply directly. We give a local modification of the negative-pair matching that covers these fixed points and proves that G_{2q} has a perfect matching. Hence

$$\nu(G_{2q}) = \rho(G_{2q}) = 2q^2.$$

Fourth, we determine the independence number of G_{pq} for distinct primes p and q. Using the Chinese Remainder Theorem and the projective classes of $\mathbb{Z}_p^2$ and $\mathbb{Z}_q^2$, we prove that

$$\alpha(G_{pq}) = (p+1)(q+1).$$

Therefore, the vertex-cover number is also exact:

$$\tau(G_{pq}) = p^2q^2 - (p+1)(q+1).$$

This completes the covering profile for products of two distinct primes.

Fifth, we include computational verification for $2 \le n \le 30$. The computed values agree with the proved formulas for odd n, for $n = 2q$, and for the exceptional case $n = 2$. The computations also suggest that G_n has a perfect matching for every even integer $n \ge 4$. We state this as a conjecture:

$$\nu(G_n) = \frac{n^2}{2} \ (n \ge 4 \text{ even}).$$

The main novelty is that the matching behavior of G_n is not obtained from a complete bipartite decomposition, as often happens in elementary zero-divisor graph computations. Instead, it is controlled by a global involution on $\mathbb{Z}_n^2$, namely $(a,b) \mapsto (-a,-b)$, and by the fixed points of this involution. For odd moduli, this involution has only one fixed point and produces a near-perfect matching. For the family $n = 2q$, it has four fixed points, and the proof requires a local modification of the negative-pair matching. This gives a structural matching argument rather than a direct application of a standard complete graph or complete bipartite graph formula.

These results show that the bilinear congruence graph is highly matchable. For all odd moduli, the graph reaches the largest matching size allowed by the odd number of vertices. For the even family $n = 2q$, the graph admits a perfect matching. Moreover, the exact independence number of G_{pq} gives exact vertex-cover formulas for products of two distinct primes. The proofs use the determinant-zero structure of the adjacency relation, the universal vertex, proportionality over finite fields, modular symmetry, and the Chinese Remainder Theorem.

II. PRELIMINARIES

In this section, we recall the basic notions used throughout the paper. For a positive integer n, we denote by $\mathbb{Z}_n$ the ring of integers modulo n. Unless otherwise stated, all graphs considered in this paper are finite, simple, and undirected.

For any integer $n \ge 2$, the bilinear congruence graph G_n is defined on the vertex set $\mathbb{Z}_n^2$, where two distinct vertices (a,b) and (x,y) are adjacent if and only if $ay \equiv bx \pmod{n}$. Equivalently,

$$\det \begin{pmatrix} a & b \\ x & y \end{pmatrix} \equiv 0 \pmod{n}.$$

Thus adjacency in G_n is a determinant-zero condition. It records modular dependence between two ordered pairs in $\mathbb{Z}_n^2$. This is different from the usual zero-divisor graph, where adjacency is defined by a product-zero condition.

Consider a vertex $v = (a,b)$ in $V(G_n)$. The neighborhood of v consists of:

$$N(v) = \{(x,y) \in \mathbb{Z}_n^2 : (x,y) \ne (a,b),\ ay \equiv bx \pmod{n}\},$$

and the degree of v is denoted by $\deg(v)$.

The structure of G_n is closely related to proportionality. This connection is especially clear when the modulus is prime. If $n = p$ (a prime), then $\mathbb{Z}_p$ is a field. The condition $ay \equiv bx \pmod{p}$ then just says that the vectors (a,b) and (x,y) are linearly dependent over $\mathbb{Z}_p$.

For a nonzero vector $v = (a,b) \in \mathbb{Z}_p^2$, define its proportionality class by

$$[v] = \{\lambda(a,b) : \lambda \in \mathbb{Z}_p^{\times}\}.$$

Each class has $p-1$ vertices. The nonzero vectors of $\mathbb{Z}_p^2$ split into

$$\frac{p^2-1}{p-1} = p+1$$

different proportionality classes. Therefore, the nonzero part of G_p is naturally decomposed into $p+1$ cliques, each of order $p-1$. The vertex $(0,0)$ is adjacent to all remaining vertices, because

$$0 \cdot y \equiv 0 \cdot x \pmod{p}$$

for all $(x,y) \in \mathbb{Z}_p^2$.

For composite moduli, the situation is more delicate. The ring $\mathbb{Z}_n$ has zero-divisors, and determinant-zero congruence is no longer the same as ordinary linear dependence over a field. To handle composite moduli, we shall use the Chinese Remainder Theorem.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the prime decomposition of n, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}.$$

DOI: **10.5281/zenodo.20705080**

Consequently,

$$\mathbb{Z}_n^2 \cong \mathbb{Z}_{p_1^{\alpha_1}}^2 \times \mathbb{Z}_{p_2^{\alpha_2}}^2 \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}^2.$$

Under this decomposition, the adjacency condition $ay \equiv bx \pmod{n}$ is equivalent to the system of congruences

$$ay \equiv bx \pmod{p_i^{\alpha_i}}, \qquad i = 1,2,\dots,r.$$

Thus two vertices are adjacent in G_n exactly when the determinant-zero condition holds modulo every prime-power factor of n.

Now, we recall the graph-theoretic parameters used in the paper. Let G be a finite simple graph. A matching in G is a set of edges no two of which share a common vertex. The maximum size of a matching is called the matching number of G, and it is denoted by $\nu(G)$. A matching is called perfect if it covers every vertex of G. If $|V(G)|$ is odd, a matching that covers all vertices except one is called near-perfect.

An independent set in a graph $G$is a set of vertices no two of which are adjacent. The maximum size of an independent set is denoted by $\alpha(G)$. A vertex cover is a set of vertices meeting every edge, and its minimum size is denoted by $\tau(G)$. An edge cover is a set of edges incident with every vertex, and its minimum size is denoted by $\rho(G)$. A graph has an edge cover if and only if it has no isolated vertices. The following standard identities will be used repeatedly to pass from matching and independence results to covering results.

Lemma 1 (Gallai's identities). *Let G be a finite simple graph. Then $\alpha(G) + \tau(G) = |V(G)|$. If G has no isolated vertices, then $\nu(G) + \rho(G) = |V(G)|$.*

These identities are standard in matching and covering theory; see, for example, Gallai [15] or standard graph theory references [11, 12, 13, 14].

Since $|V(G_n)| = n^2$, if n is odd, then G_n cannot have a perfect matching. The largest possible matching size is then

$$\frac{n^2 - 1}{2}.$$

If n is even, then a perfect matching is possible only if

$$\nu(G_n) = \frac{n^2}{2}.$$

We shall also use the standard formula

$$\nu(K_m) = \left\lfloor \frac{m}{2} \right\rfloor.$$

Indeed, in the complete graph K_m, every vertex is adjacent to every other vertex. Hence we may pair the vertices arbitrarily. If m is even, all vertices can be paired and the matching has $m/2$ edges. If m is odd, one vertex must remain unmatched and the matching has $(m-1)/2$ edges. Therefore,

$$\nu(K_m) = \left\lfloor \frac{m}{2} \right\rfloor.$$

More generally, if

$$G = K_{m_1} \cup K_{m_2} \cup \cdots \cup K_{m_t},$$

where the union is disjoint, then a matching in G is obtained by choosing a matching inside each component. Since there are no edges between different components, the maximum matching number is the sum of the maximum matching numbers of the components. Thus

$$\nu(G) = \sum_{i=1}^{t} \left\lfloor \frac{m_i}{2} \right\rfloor.$$

The purpose of the paper is to study matching and covering parameters of the bilinear congruence graph G_n, especially

$$\nu(G_n), \rho(G_n), \tau(G_n),$$

together with the existence of perfect and near-perfect matchings. The next section records the structural properties of G_n that will be used in the main results.

III. THE STRUCTURE OF THE BILINEAR CONGRUENCE GRAPH

The results of this paper depend on a few structural features of G_n that are simple but powerful. First, there is a universal vertex, which guarantees that the graph has no isolated vertices and allows edge-cover identities to be applied. The second is the proportionality-class decomposition that appears when the modulus is prime. The third is the way composite moduli separate into prime-power conditions through the Chinese Remainder Theorem. These facts will be used later to construct large matchings and to derive covering parameters.

For every vertex $(x, y) \in \mathbb{Z}_n^2$, we have

$$0 \cdot y \equiv 0 \cdot x \pmod{n}.$$

Therefore, $(0,0)$ is adjacent to each other vertex of G_n.

Proposition 1. *For every integer $n \geq 2$, the vertex $(0,0)$ is a universal vertex of G_n, with $\deg(0,0) = n^2 - 1$.*

Proof. See [8]. □

This observation is small, but it has an important consequence. Since $(0,0)$ is universal, the graph G_n has no isolated vertices. Therefore, for every $n \geq 2$ the edge-cover number $\rho(G_n)$ is defined, and Gallai's identity

$$\nu(G_n) + \rho(G_n) = |V(G_n)|$$

can be applied once $\nu(G_n)$ is known.

We next describe the prime case, where the determinant-zero relation has its clearest form. Let p be prime and set

$$V_p^* = \mathbb{Z}_p^2 \backslash \{(0,0)\}.$$

For a nonzero vertex $v = (a, b) \in V_p^*$, define its proportionality class by

$$[v] = \{\lambda(a, b) : \lambda \in \mathbb{Z}_p^\times\}.$$

Since $\mathbb{Z}_p^\times$ has $p - 1$ elements, each class $[v]$ has exactly $p - 1$ vertices.

Proposition 2. *Let p be prime. Two nonzero vertices $u, v \in V_p^*$ are adjacent in G_p if and only if they belong to the same proportionality class.*

Proof. Let $u = (a, b), v = (x, y)$ be nonzero vertices in $\mathbb{Z}_p^2$.

Assume first that u and v belong to the same proportionality class. Then there exists $\lambda \in \mathbb{Z}_p^\times$ such that $(x, y) = \lambda(a, b)$. Hence

$$x = \lambda a, y = \lambda b.$$

Therefore, $ay = a(\lambda b) = \lambda ab$, and $bx = b(\lambda a) = \lambda ab$. Thus $ay \equiv bx \pmod p$, so u and v are adjacent.

Conversely, suppose that u and v are adjacent. Then $ay \equiv bx \pmod p$. Since $u = (a, b) \neq (0,0)$, at least one of a, b is nonzero.

If $a \neq 0$, take $\lambda = xa^{-1}$. Then $x = \lambda a$. Also, from $ay \equiv bx \pmod p$, we get

$$y \equiv a^{-1}bx = \lambda b \pmod p.$$

Thus $v = \lambda u$, and so $v \in [u]$.

If $a = 0$, then $b \neq 0$. The adjacency condition becomes $0 \cdot y \equiv bx \pmod p$, so $x \equiv 0 \pmod p$. Hence $v = (0, y)$. Since $v \neq (0,0)$, we have $y \neq 0$. Taking $\lambda = yb^{-1}$, we get $v = \lambda(0, b)$. Thus $v \in [u]$. Therefore, in all cases, u and v belong to the same proportionality class. □

This proposition gives a complete description of the nonzero part of G_p. The nonzero vectors of $\mathbb{Z}_p^2$ split into the one-dimensional subspaces of $\mathbb{Z}_p^2$, and their number is

$$\frac{p^2 - 1}{p - 1} = p + 1.$$

Corollary 1. *Let p be prime. The subgraph of G_p induced by $V_p^* = \mathbb{Z}_p^2 \backslash \{(0,0)\}$ is the disjoint union of $p + 1$ complete graphs, each of order $p - 1$. That is,*

$$G_p[V_p^*] \cong \underbrace{K_{p-1} \cup K_{p-1} \cup \cdots \cup K_{p-1}}_{p+1 \text{ copies}}.$$

Moreover, the full graph G_p is obtained from this disjoint union by adding the universal vertex $(0,0)$.

Proof. By the previous proposition, two nonzero vertices are adjacent exactly when they lie in the same proportionality class. Each proportionality class therefore induces complete graph, that is, a clique, of order $p - 1$. Distinct proportionality classes have no edges between them. Since there are $p + 1$ such classes, the result follows. The vertex $(0,0)$ is universal by the first proposition of this section. □

This decomposition explains why the prime case can be handled explicitly. It also shows why G_p is not merely a complete bipartite graph. Instead, its nonzero part splits into several disjoint cliques, and the zero vertex connects to all of them.

For composite n, the structure is more delicate. The ring $\mathbb{Z}_n$ has zero-divisors, and the congruence $ay \equiv bx \pmod n$ does not always mean that one vector is a unit multiple of the other. Still, scalar multiples always give adjacent vertices, as the next elementary observation shows.

Proposition 3. *Let $n \geq 2$ be composite. Then there exist adjacent vertices in G_n whose adjacency is caused by zero-divisors and does not come from unit proportionality.*

Proof. Since n is composite, there exists a proper divisor d of n, with $1 < d < n$. Let

$$e = \frac{n}{d}.$$

Then $de = n \equiv 0 \pmod n$, so d and e are nonzero zero-divisors in $\mathbb{Z}_n$.

Consider the two vertices

$$u = (d, 0), v = (0, e)$$

of G_n. They are distinct and nonzero. Moreover,

$$d \cdot e \equiv 0 \cdot 0 \pmod n,$$

because $de \equiv 0 \pmod n$.

Hence $u \sim v$ in G_n.

It remains to note that this adjacency does not come from unit proportionality. If $v = \lambda u$ for some unit $\lambda \in \mathbb{Z}_n^\times$, then

$$(0, e) = \lambda(d, 0) = (\lambda d, 0).$$

This would force

$$e \equiv 0 \pmod n,$$

which is impossible because $0 < e < n$. Similarly, u cannot be a unit multiple of v.

Thus u and v are adjacent because the product of two nonzero zero-divisors vanishes modulo n, not because they lie in the same unit-proportionality class. □

This proposition shows exactly where the composite case differs from the prime case. Over a field, determinant-zero adjacency among nonzero vectors is the same as proportionality. Over $\mathbb{Z}_n$ with n composite, zero-divisors can force the determinant $ay - bx$ to vanish modulo n even when the two vertices are not related by a unit multiple. These extra adjacencies are one reason why the composite case has a richer structure.

The Chinese Remainder Theorem gives the main tool for separating the composite case into simpler congruence conditions.

Proposition 4. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Two vertices (a, b) and (x, y) are adjacent in G_n if and only if $ay \equiv bx \pmod{p_i^{\alpha_i}}$ for every $i = 1,2, \ldots, r$.*

Proof. The congruence $ay \equiv bx \pmod n$ is equivalent to saying that $n \mid ay - bx$. Since the prime-power factors $p_i^{\alpha_i}$ are pairwise coprime, this is equivalent to $p_i^{\alpha_i} \mid ay - bx$ for every $i = 1,2, \ldots, r$. Hence $ay \equiv bx \pmod{p_i^{\alpha_i}}$ for every i. The converse follows from the Chinese Remainder Theorem. □

In particular, if $n = pq$, where p and q are distinct primes, then adjacency modulo pq is equivalent to the two simultaneous conditions $ay \equiv bx \pmod p$ and $ay \equiv bx \pmod q$. This will be used later when products of two distinct primes are considered.

These structural facts guide the rest of the paper. For odd n, the number of vertices is odd, so a perfect matching is impossible and the best possible matching size is

$$\frac{n^2 - 1}{2}.$$

For even n, a perfect matching is possible in principle, but it must be constructed from the graph structure. Finally, for prime p, the clique decomposition of $G_p[V_p^*]$ gives a direct way to compute matching and independence parameters.

Remark 1. *The purpose of this paper is not only to compute one graph invariant. The matching number $\nu(G_n)$ is the main object, but it also determines the edge-cover number $\rho(G_n)$ through Gallai's identity. Similarly, known or proved values of the independence number $\alpha(G_n)$ determine the vertex-cover number $\tau(G_n)$. In this way, the bilinear congruence structure gives a connected family of matching and covering parameters.*

IV. THE PRIME CASE

We apply the structural description of G_p to determine its matching, independence, and vertex-cover parameters. The prime case is useful because $\mathbb{Z}_p$ is a field, so the determinant-zero condition is exactly linear dependence over $\mathbb{Z}_p$.

Let $V_p^* = \mathbb{Z}_p^2 \backslash \{(0,0)\}$. By the previous section, the nonzero vertices split into $p+1$ proportionality classes, each of size $p-1$. Each class induces a complete graph K_{p-1}, and there are no edges between distinct classes inside V_p^*. The vertex $(0,0)$ is adjacent to every other vertex. Hence

$$G_p[V_p^*] \cong \underbrace{K_{p-1} \cup K_{p-1} \cup \cdots \cup K_{p-1}}_{p+1 \text{ cliques}},$$

and G_p is obtained from this disjoint union by adding the universal vertex $(0,0)$.

The case $p = 3$ gives the smallest nontrivial example of this structure, as shown in **Figure 1**.

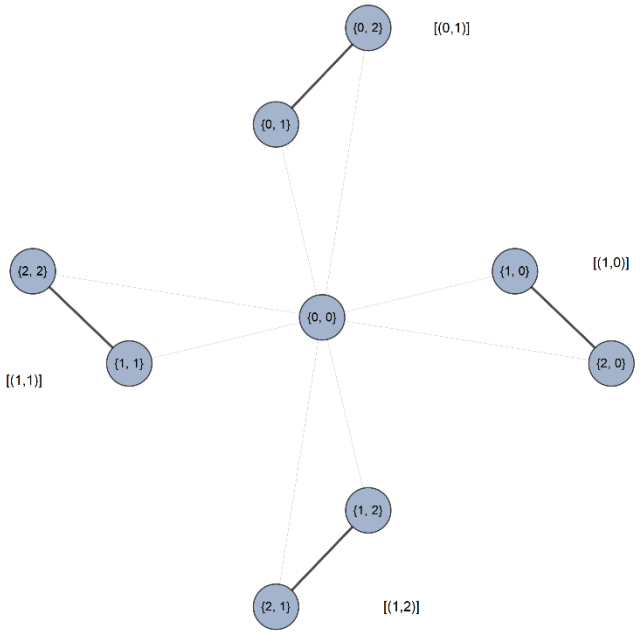

Figure 1: *The structural decomposition of G_3. The vertex $(0,0)$ is universal, and the nonzero vertices split into four proportionality classes, each inducing a copy of K_2.*

We first determine the matching number of G_p. The case $p = 2$ is exceptional, because the nonzero part of G_2 has no edges.

Theorem 1. *Let p be a prime number. Then*

$$\nu(G_p) = \begin{cases} 1, & p = 2, \\ \dfrac{p^2-1}{2}, & p \text{ is odd.} \end{cases}$$

Proof. First suppose that $p = 2$. Then G_2 has four vertices:

$$(0,0), \quad (1,0), \quad (0,1), \quad (1,1).$$

The vertex $(0,0)$ is adjacent to every other vertex. The three nonzero vertices are not adjacent to one another, because each nonzero proportionality class over $\mathbb{Z}_2$ contains only one vertex. Hence $G_2 \cong K_{1,3}$, and therefore $\nu(G_2) = 1$.

Now, assume that p is odd. Then each proportionality class has $p-1$ vertices. Since $p-1$ is even, each clique K_{p-1} has a perfect matching of size

$$\frac{p-1}{2}.$$

There are $p+1$ such cliques in $G_p[V_p^*]$. Taking a perfect matching inside each clique gives a matching of size

$$(p+1)\frac{p-1}{2} = \frac{p^2-1}{2}.$$

This matching covers all nonzero vertices and leaves only $(0,0)$ uncovered.

Since p^2 is odd, no matching can have more than

$$\frac{p^2-1}{2}$$

edges. Hence

$$\nu(G_p) = \tfrac{p^2-1}{2}. \square$$

Thus, for odd prime p, the prime graph G_p has a near-perfect matching. The matching is obtained by matching vertices inside each proportionality clique and leaving only the universal vertex $(0,0)$ unmatched.

We next determine the independence number. This is also controlled by the proportionality classes: inside each class all vertices are adjacent, while vertices from distinct classes are not adjacent inside the nonzero part.

Proposition 5. *Let p be an odd prime. Then $\alpha(G_p) = p+1$.*

Proof. The nonzero vertices of G_p split into $p+1$ proportionality classes. Inside each class, every two distinct vertices are adjacent. Therefore, an independent set can contain at most one vertex from each class. Hence

$$\alpha(G_p) \le p+1.$$

Conversely, choose one vertex from each proportionality class. Since there are no edges between distinct proportionality classes inside V_p^*, these chosen vertices form an independent set of size $p+1$. Therefore,

$$\alpha(G_p) = p+1. \square$$

The vertex-cover number now follows immediately from Gallai's identity

$$\alpha(G) + \tau(G) = |V(G)|.$$

Corollary 2. *Let p be an odd prime. Then*

$$\tau(G_p) = p^2 - p - 1.$$

Proof. Since $\alpha(G_p) = p + 1$ and $|V(G_p)| = p^2$, Gallai's identity gives

$$\tau(G_p) = p^2 - \alpha(G_p) = p^2 - (p + 1) = p^2 - p - 1. \square$$

The results of this section are summarized in **Table 1**. The edge-cover number $\rho(G_p)$ will be collected later as part of the general covering consequences.

***Table 1**: Main parameters of G_p for odd prime p.*

Parameter	Value for G_p, p odd prime
$\lvert V(G_p)\rvert$	p^2
$\nu(G_p)$	$\frac{p^2-1}{2}$
$\alpha(G_p)$	$p + 1$
$\tau(G_p)$	$p^2 - p - 1$

V. PERFECT AND NEAR-PERFECT MATCHINGS

We now study perfect and near-perfect matchings in G_n. Since $|V(G_n)| = n^2$, whether n is odd or even gives the first obstruction. If n is odd, then n^2 is odd, so G_n cannot have a perfect matching. If n is even, then a perfect matching is possible by parity, but it is not guaranteed by parity alone.

We begin with the general upper bound for the matching number.

Proposition 6. *For every integer $n \geq 2$, $\nu(G_n) \leq \left\lfloor \frac{n^2}{2} \right\rfloor$.*

Proof. A matching consists of pairwise disjoint edges. Each edge covers exactly two vertices. Since G_n has n^2 vertices, every matching has at most

$$\left\lfloor \frac{n^2}{2} \right\rfloor$$

edges. Hence

$$\nu(G_n) \leq \left\lfloor \frac{n^2}{2} \right\rfloor. \square$$

Thus, if n is odd, the largest possible matching size is

$$\frac{n^2 - 1}{2}.$$

If this value is attained, the graph has a near-perfect matching. If n is even, the largest possible matching size is

$$\frac{n^2}{2}.$$

If this value is attained, the graph has a perfect matching.

We first treat the odd case. The next proposition records the basic parity obstruction.

Proposition 7. *If n is odd, then G_n has no perfect matching.*

Proof. If n is odd, then $|V(G_n)| = n^2$ is odd. A perfect matching covers all vertices by disjoint pairs, so the number of vertices must be even. Therefore, G_n cannot have a perfect matching. $\square$

The following theorem shows that, for odd n, this parity obstruction is the only obstruction. The proof uses the negative-pair involution.

Theorem 2. *Let $n \geq 3$ be odd. Then G_n has a near-perfect matching. In particular, $\nu(G_n) = \frac{n^2-1}{2}$.*

Proof. Since n is odd, the number of vertices of G_n is odd. Hence every matching in G_n has size at most

$$\frac{n^2 - 1}{2}.$$

Consider the map

$$\varphi: \mathbb{Z}_n^2 \to \mathbb{Z}_n^2, \qquad \varphi(a, b) = (-a, -b).$$

This map is an involution. We determine its fixed points. If $(a, b) = (-a, -b)$, then

$$2a \equiv 0 \pmod{n}, \qquad 2b \equiv 0 \pmod{n}.$$

Since n is odd, 2 is a unit in $\mathbb{Z}_n$. Hence

$$a \equiv 0 \pmod{n}, \qquad b \equiv 0 \pmod{n}.$$

Thus the only fixed point of φ is $(0,0)$. Therefore, all nonzero vertices of G_n are partitioned into disjoint pairs $\{(a, b), (-a, -b)\}$. Each such pair is an edge of G_n, because $a(-b) = -ab$ and $b(-a) = -ab$. Hence

$$a(-b) \equiv b(-a) \pmod{n}.$$

Thus the negative pairs form a matching that covers all vertices except $(0,0)$. This matching has

$$\frac{n^2 - 1}{2}$$

edges. Since this reaches the largest possible value, we obtain

$$\nu(G_n) = \frac{n^2 - 1}{2}.$$

Therefore, G_n has a near-perfect matching. $\square$

Remark 2. *The proof of Theorem 2. also shows that the induced subgraph $G_n^* = G_n[\mathbb{Z}_n^2 \backslash \{(0,0)\}]$ has a perfect matching whenever $n \geq 3$ is odd. Indeed, this perfect matching is obtained by pairing each nonzero vertex (a, b) with its negative $(-a, -b)$.*

This theorem applies to every odd modulus $n \geq 3$, not only to prime moduli. In particular, it applies to $n = pq$, where p and q are distinct odd primes. The key point is that the matching is controlled by the global symmetry

$$(a, b) \mapsto (-a, -b),$$

not by a decomposition into complete or complete bipartite graphs.

The universal vertex also gives a useful reduction principle. Let

$$G_n^* = G_n[\mathbb{Z}_n^2 \backslash \{(0,0)\}].$$

Thus G_n^* is the graph obtained from G_n by deleting the universal vertex.

For even n, the same deleted-vertex subgraph G_n^* can be used in the opposite direction. If the nonzero part has a near-perfect matching, then the remaining unmatched nonzero vertex can be paired with $(0,0)$.

Proposition 8. *Let $n \geq 2$ be even. If G_n^* has a near-perfect matching, then G_n has a perfect matching.*

Proof. Since n is even, n^2 is even and $|V(G_n^*)| = n^2 - 1$ is odd. Suppose that G_n^* has a near-perfect matching. Then exactly one vertex $v \in V(G_n^*)$ is not covered. Since $(0,0)$ is adjacent to every nonzero vertex, the edge $\{(0,0), v\}$ can be added to the matching. The resulting matching covers every vertex of G_n. Hence G_n has a perfect matching. □

Now, we record the safe general statement for even moduli. When n is even, the graph G_n has an even number of vertices. Therefore, a perfect matching is not excluded by parity. However, parity alone does not guarantee its existence. The case $n = 2$ already shows this, because $G_2 \cong K_{1,3}$, and therefore G_2 has no perfect matching.

Proposition 9. *Let $n \geq 2$ be even. Then*

$$\nu(G_n) \leq \frac{n^2}{2}.$$

Moreover, G_n has a perfect matching if and only if

$$\nu(G_n) = \frac{n^2}{2}.$$

Proof. Since G_n has n^2 vertices and n^2 is even, every matching has at most

$$\frac{n^2}{2}$$

edges. Equality holds exactly when the matching covers every vertex of G_n. This is precisely the definition of a perfect matching. □

Thus, in the even case, the main problem is not the parity of the vertex set, but the construction of a matching that covers all vertices. In the next section, we prove such a construction for the family $n = 2q$, where q is an odd prime.

VI. THE CASE pq

We study G_{pq}, where p and q are distinct primes. The case in which both primes are odd follows directly from the general odd-modulus theorem proved in the previous section. The main new point here is the mixed even case $n = 2q$, where q is an odd prime.

Throughout this section, the graph G_{pq} has vertex set $V(G_{pq}) = \mathbb{Z}_{pq}^2$, and two distinct vertices (a, b) and (x, y) are adjacent if and only if $ay \equiv bx \pmod{pq}$. By the Chinese Remainder Theorem,

$$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Hence the adjacency condition $ay \equiv bx \pmod{pq}$ is equivalent to the two simultaneous congruences

$$ay \equiv bx \pmod{p}, \qquad ay \equiv bx \pmod{q}.$$

Thus two vertices are adjacent in G_{pq} exactly when they satisfy the bilinear dependence condition modulo both p and q.

We first record the odd case. Since the product of two odd primes is odd, the general odd-modulus theorem applies immediately.

Corollary 3. *Let p and q be distinct odd primes. Then G_{pq} has a near-perfect matching. In particular,*

$$\nu(G_{pq}) = \frac{p^2q^2 - 1}{2}.$$

Proof. Since p and q are odd, pq is odd. The result follows directly from Theorem 2. by taking $n = pq$. □

Figure 2 illustrates the general odd-modulus construction in a schematic way.

Figure 2: *Schematic representation of the negative-pair matching for odd modulus. For odd n, the map $(a, b) \mapsto (-a, -b)$ fixes only $(0,0)$, and every other vertex is paired with its negative.*

We next consider the mixed even case $n = 2q$, where q is an odd prime. Here

$$|V(G_{2q})| = (2q)^2 = 4q^2,$$

so a perfect matching is not excluded by the number of vertices. However, the negative-pair map

$$(a, b) \mapsto (-a, -b)$$

does not behave as in the odd case. It has four fixed points:

$$(0,0), \qquad (q, 0), \qquad (0, q), \qquad (q, q).$$

Thus the odd-modulus construction must be modified.

Theorem 3. *Let q be an odd prime. Then G_{2q} has a perfect matching. Consequently, $\nu(G_{2q}) = 2q^2$.*

Proof. Let $n = 2q$. Consider the involution

$$\varphi: \mathbb{Z}_{2q}^2 \to \mathbb{Z}_{2q}^2, \qquad \varphi(a, b) = (-a, -b).$$

The fixed points of φ satisfy

$$2a \equiv 0 \pmod{2q}, \qquad 2b \equiv 0 \pmod{2q}.$$

Hence $a, b \in \{0, q\}$. Therefore, the fixed points are exactly

$$(0,0), \qquad (q, 0), \qquad (0, q), \qquad (q, q).$$

Every non-fixed vertex can be paired with its negative. If $(a, b) \neq (-a, -b)$, then (a, b) and $(-a, -b)$ are adjacent in G_{2q}, because $a(-b) = -ab$ and $b(-a) = -ab$. Thus the negative pairs form a matching on all non-fixed vertices.

It remains to cover the four fixed vertices. We do this by removing two negative pairs and replacing them with four edges incident with the fixed vertices. Consider the two negative pairs $\{(1,0), (-1,0)\}$ and $\{(2,2), (-2,-2)\}$. In $\mathbb{Z}_{2q}$, these are $\{(1,0), (2q-1,0)\}$ and $\{(2,2), (2q-2, 2q-2)\}$. Since q is odd, the vertices

$$(1,0), \quad (2q-1,0), \quad (2,2), \quad (2q-2, 2q-2)$$

are non-fixed and pairwise distinct. Hence removing the two negative pairs above does not affect any fixed vertex, and it leaves exactly these four non-fixed vertices available for a new matching. Moreover, none of these four vertices appears in any other negative pair after the two selected pairs are

removed, because the negative-pair decomposition is a partition of the non-fixed vertices.

Now, match the fixed vertices as follows:

$$(0,0) \sim (1,0),$$

$$(q,0) \sim (2q-1,0),$$

$$(0,q) \sim (2,2),$$

$$(q,q) \sim (2q-2,2q-2).$$

We verify that these are edges of G_{2q}. The first edge is valid because $(0,0)$ is universal. For the second edge,

$$q \cdot 0 \equiv 0 \cdot (2q-1) \pmod{2q}.$$

For the third edge, $0 \cdot 2 = 0$ and $q \cdot 2 = 2q \equiv 0 \pmod{2q}$. For the fourth edge,

$$q(2q-2) \equiv q(2q-2) \pmod{2q}.$$

Therefore, all four displayed pairs are edges of G_{2q}.

The modified construction covers every vertex of G_{2q}. All non-fixed vertices not involved in the replacement remain covered by their negative pairs, the four selected non-fixed vertices are covered by the four new edges, and the four fixed vertices are also covered by the four new edges. Hence G_{2q} has a perfect matching.

Since $|V(G_{2q})| = 4q^2$, a perfect matching has

$$\frac{4q^2}{2} = 2q^2$$

edges. Therefore, $\nu(G_{2q}) = 2q^2$. □

The local modification used in the proof is shown in **Figure 3**. The figure emphasizes that the proof does not simply use the negative-pair matching unchanged. Instead, two negative pairs are removed so that the four fixed vertices can be covered.

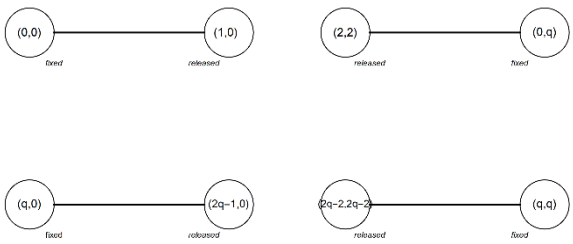

Figure 3: *Local modification in the mixed even case $n = 2q$. The four fixed vertices of the negative-pair map are covered by replacing two negative pairs with four new matching edges.*

Combining the odd case and the mixed even case gives the following formula for the matching number of G_{pq}.

Theorem 4. *Let $p < q$ be distinct primes. Then*

$$\nu(G_{pq}) = \begin{cases} \dfrac{p^2q^2-1}{2}, & p \text{ and } q \text{ are both odd,} \\ 2q^2, & p = 2. \end{cases}$$

Proof. If p and q are both odd, then pq is odd, and the result follows from the odd-modulus theorem. If $p = 2$, then $n = 2q$, and the result follows from the perfect matching construction proved above. □

The odd case is controlled by the fact that the negative-pair involution fixes only $(0,0)$. The case $n = 2q$ is different because the same involution has four fixed points. The proof above shows that these fixed points can be covered by a local modification of the negative-pair matching. The corresponding edge-cover values will be collected in the next section using Gallai's identity.

VII. COVERING CONSEQUENCES

We collect the covering consequences of the matching results proved above. The main point is that edge covers and vertex covers do not require separate long arguments once the matching number and the independence number are known.

Since the graph G_n has no isolated vertices for every $n \geq 2$. Therefore, Gallai's edge-cover identity applies:

$$\nu(G_n) + \rho(G_n) = |V(G_n)| = n^2.$$

Hence

$$\rho(G_n) = n^2 - \nu(G_n).$$

Similarly, Gallai's vertex-cover identity gives

$$\alpha(G_n) + \tau(G_n) = |V(G_n)| = n^2,$$

and therefore

$$\tau(G_n) = n^2 - \alpha(G_n).$$

We first derive the edge-cover numbers from the matching results of the previous sections.

Theorem 5. *Let $n \geq 3$ be odd. Then $\rho(G_n) = \frac{n^2+1}{2}$.*

Proof. By the odd-modulus matching theorem,

$$\nu(G_n) = \frac{n^2-1}{2}.$$

Since G_n has no isolated vertices,

$$\rho(G_n) = n^2 - \nu(G_n).$$

Thus

$$\rho(G_n) = n^2 - \frac{n^2-1}{2} = \frac{n^2+1}{2}.$$ □

As an immediate consequence, we obtain the edge-cover number for products of two odd primes.

Corollary 4. *Let p and q be distinct odd primes. Then*

$$\rho(G_{pq}) = \frac{p^2q^2+1}{2}.$$

Proof. Since p and q are odd, $n = pq$ is odd. The result follows from **Theorem 5**. by taking $n = pq$. □

For the mixed even case $n = 2q$, the perfect matching constructed in the previous section gives the edge-cover number directly.

Theorem 6. *Let q be an odd prime. Then $\rho(G_{2q}) = 2q^2$.*

Proof. By the perfect matching result for G_{2q},

$$\nu(G_{2q}) = 2q^2.$$

Also,

$$|V(G_{2q})| = (2q)^2 = 4q^2.$$

Since G_{2q} has no isolated vertices, Gallai's edge-cover identity gives

$$\rho(G_{2q}) = 4q^2 - 2q^2 = 2q^2. \square$$

We now turn to vertex covers. The vertex-cover number is determined by the independence number:

$$\tau(G_n) = n^2 - \alpha(G_n).$$

Thus, whenever $\alpha(G_n)$ is known exactly, the value of $\tau(G_n)$ follows immediately.

For the prime case, the independence number was obtained from the proportionality-class decomposition.

Theorem 7. *Let p be an odd prime. Then*

$$\tau(G_p) = p^2 - p - 1.$$

Proof. By the prime-case independence result,

$$\alpha(G_p) = p + 1.$$

Since

$$|V(G_p)| = p^2,$$

Gallai's vertex-cover identity gives

$$\tau(G_p) = p^2 - \alpha(G_p) = p^2 - (p+1) = p^2 - p - 1. \square$$

The next result uses a different idea from the matching constructions above. Instead of using the negative-pair involution, we use the Chinese Remainder Theorem to label each vertex of G_{pq} by its projective directions modulo p and modulo q. This allows us to count the largest possible independent set.

Theorem 8. *Let p and q be distinct primes. Then*

$$\alpha(G_{pq}) = (p+1)(q+1).$$

Consequently,

$$\tau(G_{pq}) = p^2q^2 - (p+1)(q+1).$$

Proof. By the Chinese Remainder Theorem, $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Hence, $\mathbb{Z}_{pq}^2 \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q^2$. Thus each vertex $v \in \mathbb{Z}_{pq}^2$ can be written in the form $v = (v_p, v_q)$, where

$$v_p \in \mathbb{Z}_p^2, v_q \in \mathbb{Z}_q^2.$$

If $u = (u_p, u_q)$ and $v = (v_p, v_q)$, then u and v are adjacent in G_{pq} if and only if the determinant-zero condition holds modulo both p and q. Equivalently, u_p and v_p "are linearly dependent over" $\mathbb{Z}_p$, and u_q and v_q "are linearly dependent over" $\mathbb{Z}_q$.

We describe the possible directions in each component. Let $\mathcal{P}_p$ be the set of one-dimensional subspaces of $\mathbb{Z}_p^2$, and let $\mathcal{P}_q$ be the set of one-dimensional subspaces of $\mathbb{Z}_q^2$. Equivalently, $\mathcal{P}_p$ is the set of proportionality classes of nonzero vectors in $\mathbb{Z}_p^2$, and $\mathcal{P}_q$ is defined similarly. Since

$$|\mathbb{Z}_p^2 \backslash \{(0,0)\}| = p^2 - 1$$

and each one-dimensional subspace contains $p-1$ nonzero vectors, we have

$$|\mathcal{P}_p| = \frac{p^2-1}{p-1} = p + 1.$$

Similarly, $|\mathcal{P}_q| = q + 1$.

We first prove the lower bound. For each pair $(L, M) \in \mathcal{P}_p \times \mathcal{P}_q$, choose one vertex $v_{L,M} \in \mathbb{Z}_{pq}^2$ such that its component modulo p lies in $L\backslash\{0\}$, and its component modulo q lies in $M\backslash\{0\}$. Such a vertex exists by the Chinese Remainder Theorem.

Define

$$S = \{v_{L,M} : L \in \mathcal{P}_p,\ M \in \mathcal{P}_q\}.$$

Then

$$|S| = |\mathcal{P}_p|\,|\mathcal{P}_q| = (p+1)(q+1).$$

We claim that S is independent. Let $v_{L,M}$ and $v_{L',M'}$ be two distinct vertices of S. Since they are distinct choices from the set indexed by $\mathcal{P}_p \times \mathcal{P}_q$, we have

$$(L, M) \neq (L', M').$$

Hence either $L \neq L'$ or $M \neq M'$. If $L \neq L'$, then the two components modulo p lie in different one-dimensional subspaces of $\mathbb{Z}_p^2$. Therefore, they are linearly independent over $\mathbb{Z}_p$, so the determinant-zero condition fails modulo p. If $M \neq M'$, the same argument shows that the determinant-zero condition fails modulo q. In either case, the two vertices are not adjacent in G_{pq}. Therefore, S is independent, and so

$$\alpha(G_{pq}) \geq (p+1)(q+1).$$

We now prove the upper bound. We assign a label to each vertex according to its directions modulo p and modulo q. If $v_p \neq 0$, let $L(v_p)$ be the unique one-dimensional subspace of $\mathbb{Z}_p^2$ containing v_p. If $v_p = 0$, assign the special label 0_p. Similarly, if $v_q \neq 0$, let $L(v_q)$ be the unique one-dimensional subspace of $\mathbb{Z}_q^2$ containing v_q, and if $v_q = 0$, assign the special label 0_q.

Thus every vertex receives a label of the form

$$(A, B) \in (\mathcal{P}_p \cup \{0_p\}) \times (\mathcal{P}_q \cup \{0_q\}).$$

Two distinct vertices with the same label are adjacent, because their modulo p components are dependent and their modulo q components are also dependent. Therefore, an independent set contains at most one vertex with each label.

Let I be an independent set. We count how many labels can occur in I. There are four possible types of labels:

$$(A, B), A \in \mathcal{P}_p,\ B \in \mathcal{P}_q,$$

$$(0_p, B), B \in \mathcal{P}_q,$$

$$(A, 0_q), A \in \mathcal{P}_p,$$

and

$$(0_p, 0_q).$$

The label $(0_p, 0_q)$ corresponds to the zero vertex $(0,0)$. This vertex is adjacent to every other vertex. Hence an independent set containing this label has size at most one. Since we already constructed an independent set of size $(p+1)(q+1) > 1$, this label cannot occur in a maximum independent set.

Now suppose that I contains labels of the form

$$(0_p, B), B \in \mathcal{P}_q.$$

Let $T \subseteq \mathcal{P}_q$ be the set of such B's, and let

$$|T| = s.$$

For a fixed $B \in T$, no label of the form

$$(A, B), A \in \mathcal{P}_p,$$

can also occur in I. Indeed, the zero component modulo p is dependent with every vector modulo p, and the two modulo q components lie in the same projective class B. Therefore, the corresponding vertices would be adjacent.

Thus, for each $B \in T$, the one label $(0_p, B)$ excludes all $p+1$ labels

$$(A, B), A \in \mathcal{P}_p.$$

Hence the total number of labels that can occur is at most

$$s + (q + 1 - s)(p + 1).$$

This equals

$$(p+1)(q+1) - sp.$$

Since $s \geq 0$, we get

$$s + (q + 1 - s)(p + 1) \leq (p+1)(q+1).$$

Therefore, labels of the form $(0_p, B)$ cannot produce an independent set larger than $(p+1)(q+1)$.

Similarly, suppose that I contains labels of the form

$$(A, 0_q), A \in \mathcal{P}_p.$$

Let there be t such labels. For each such A, no label of the form

$$(A, B), B \in \mathcal{P}_q,$$

can occur in I, because the two modulo p components lie in the same projective class A, and the zero component modulo q is dependent with every vector modulo q. Therefore, the number of labels is at most

$$t + (p + 1 - t)(q + 1).$$

This equals

$$(p+1)(q+1) - tq,$$

and so

$$t + (p + 1 - t)(q + 1) \leq (p+1)(q+1).$$

Thus labels of the form $(A, 0_q)$ also cannot increase the size beyond $(p+1)(q+1)$.

It remains to note that labels of the two zero-component types cannot be used together. A label of the form $(0_p, B)$ is adjacent to every label of the form $(A, 0_q)$, because the first components are dependent modulo p, and the second components are dependent modulo q. Hence an independent set cannot contain both types at the same time.

Therefore, every independent set in G_{pq} has size at most

$$(p+1)(q+1).$$

Together with the lower bound, this gives

$$\alpha(G_{pq}) = (p+1)(q+1).$$

Finally, by Gallai's vertex-cover identity,

$$\alpha(G_{pq}) + \tau(G_{pq}) = |V(G_{pq})| = p^2q^2.$$

Hence

$$\tau(G_{pq}) = p^2q^2 - (p+1)(q+1).$$

□

For general composite moduli, the exact value of $\alpha(G_n)$ is more delicate. The following simple construction gives a useful lower bound.

Proposition 10. *For every integer* $n \geq 2$, $\alpha(G_n) \geq n$. *Consequently,* $\tau(G_n) \leq n^2 - n$.

Proof. Consider the set

$$S_n = \{(1, t) : t \in \mathbb{Z}_n\}.$$

This set has n vertices. If $t_1 \neq t_2$, then the vertices $(1, t_1)$ and $(1, t_2)$ are adjacent if and only if

$$1 \cdot t_2 \equiv t_1 \cdot 1 \pmod{n},$$

that is,

$$t_2 \equiv t_1 \pmod{n}.$$

This is impossible when $t_1 \neq t_2$. Hence S_n is independent, and so

$$\alpha(G_n) \geq n.$$

Using

$$\tau(G_n) = n^2 - \alpha(G_n),$$

we obtain

$$\tau(G_n) \leq n^2 - n. \square$$

For prime moduli, the lower bound $\alpha(G_n) \geq n$ is not sharp, because

$$\alpha(G_p) = p + 1.$$

For products of two distinct primes, the previous theorem gives the exact value

$$\alpha(G_{pq}) = (p+1)(q+1).$$

For higher prime powers and more general composite moduli, determining $\alpha(G_n)$ remains a separate problem.

The covering consequences obtained in this section are summarized in **Table 2**. The table separates exact values from

expressions that depend on the still unknown independence number.

Table 2: *Matching and covering parameters for the main cases.*

Graph	$\nu(G)$	$\rho(G)$	$\tau(G)$
G_n, $n \geq 3$ odd	$\frac{n^2-1}{2}$	$\frac{n^2+1}{2}$	$n^2 - \alpha(G_n)$
G_p, p odd prime	$\frac{p^2-1}{2}$	$\frac{p^2+1}{2}$	$p^2 - p - 1$
G_{pq}, p, q odd distinct primes	$\frac{p^2q^2-1}{2}$	$\frac{p^2q^2+1}{2}$	$p^2q^2 - (p+1)(q+1)$
G_{2q}, q odd prime	$2q^2$	$2q^2$	$4q^2 - 3(q+1)$

VIII. EXAMPLES AND COMPUTATIONAL VERIFICATION

In this section, we give examples and computational checks for the main formulas. The purpose is not to repeat the proofs, but to show how the structural results appear in small cases and how the matching formulas behave for a wider range of moduli.

The smallest nontrivial odd example is G_3. Here

$$|V(G_3)| = 3^2 = 9.$$

Since 3 is odd, the general odd-modulus theorem gives

$$\nu(G_3) = \frac{3^2-1}{2} = 4, \rho(G_3) = \frac{3^2+1}{2} = 5.$$

The nonzero vertices of $\mathbb{Z}_3^2$ split into four proportionality classes:

$$[(1,0)] = \{(1,0),(2,0)\},$$

$$[(0,1)] = \{(0,1),(0,2)\},$$

$$[(1,1)] = \{(1,1),(2,2)\},$$

and

$$[(1,2)] = \{(1,2),(2,1)\}.$$

Each class induces a copy of K_2. Therefore, a near-perfect matching is

$$M = \{\{(1,0),(2,0)\},\{(0,1),(0,2)\},\{(1,1),(2,2)\},\{(1,2),(2,1)\}\}.$$

This matching covers all vertices except the universal vertex $(0,0)$.

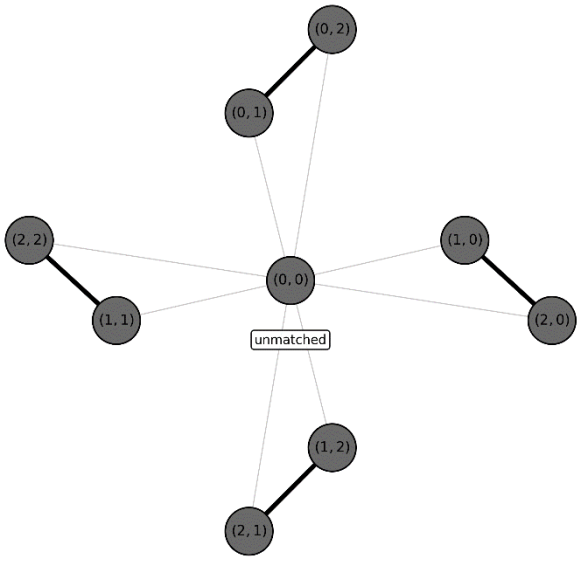

Figure 4: *A near-perfect matching of G_3. The four matching edges cover all nonzero vertices and leave only the universal vertex* $(0,0)$ *unmatched.*

Figure 4 gives a visual verification of the formula $\nu(G_3) = 4$. Moreover, since

$$\alpha(G_3) = 3 + 1 = 4,$$

we obtain

$$\tau(G_3) = 9 - 4 = 5.$$

The next table summarizes several exact examples. The values for $n = 3$ and $n = 5$ come from the prime case. The values for $n = 10,15$, and 21 use the formula

$$\alpha(G_{pq}) = (p+1)(q+1)$$

for products of two distinct primes.

Table 3: *Exact matching and covering values for selected moduli*

n	$\lvert V(G_n)\rvert$	$\nu(G_n)$	$\rho(G_n)$	$\alpha(G_n)$	$\tau(G_n)$
3	9	4	5	4	5
5	25	12	13	6	19
10	100	50	50	18	82
15	225	112	113	24	201
21	441	220	221	32	409

For example, when $n = 15 = 3 \cdot 5$, we have

$$\alpha(G_{15}) = (3+1)(5+1) = 24,$$

and hence

$$\tau(G_{15}) = 15^2 - 24 = 201.$$

Similarly, when $n = 10 = 2 \cdot 5$,

$$\alpha(G_{10}) = (2+1)(5+1) = 18,$$

and therefore

$$\tau(G_{10}) = 10^2 - 18 = 82.$$

To further check the matching formulas, we computed maximum matchings for all moduli $2 \le n \le 30$.

The results agree with the proved formulas for odd n, with the theorem for $n = 2q$, and with the exceptional case $n = 2$. They also suggest that G_n may have a perfect matching for every even integer $n \ge 4$. This is stated only as a computational observation, not as a theorem.

***Table 4**: Computed matching and edge-cover values for $2 \le n \le 30$.*

n	$\lvert V(G_n)\rvert$	$\nu(G_n)$	$\rho(G_n)$	Type
2	4	1	3	exceptional
3	9	4	5	near-perfect
4	16	8	8	perfect
5	25	12	13	near-perfect
6	36	18	18	perfect
7	49	24	25	near-perfect
8	64	32	32	perfect
9	81	40	41	near-perfect
10	100	50	50	perfect
11	121	60	61	near-perfect
12	144	72	72	perfect
13	169	84	85	near-perfect
14	196	98	98	perfect
15	225	112	113	near-perfect
16	256	128	128	perfect
17	289	144	145	near-perfect
18	324	162	162	perfect
19	361	180	181	near-perfect
20	400	200	200	perfect
21	441	220	221	near-perfect
22	484	242	242	perfect
23	529	264	265	near-perfect
24	576	288	288	perfect
25	625	312	313	near-perfect
26	676	338	338	perfect
27	729	364	365	near-perfect
28	784	392	392	perfect
29	841	420	421	near-perfect
30	900	450	450	perfect

The odd rows in **Table 4** agree with the formula

$$\nu(G_n) = \frac{n^2 - 1}{2}, \rho(G_n) = \frac{n^2 + 1}{2}.$$

The row $n = 2$ confirms the exceptional graph

$$G_2 \cong K_{1,3}, \nu(G_2) = 1.$$

For every even value $4 \le n \le 30$, the computation gives a perfect matching. This leads to the following n conjecture.

Conjecture 1. *For every even integer $n \ge 4$, the graph G_n has a perfect matching. Equivalently, $\nu(G_n) = \frac{n^2}{2}$ for every even $n \ge 4$.*

We finish by describing the computational method used to produce **Table 4**. For a fixed integer $n \ge 2$, the graph is constructed from $V(G_n) = \mathbb{Z}_n^2$ and

$$E(G_n) = \{\{(a,b),(x,y)\}: (a,b) \ne (x,y),\ ay \equiv bx \pmod{n}\}.$$

A maximum matching algorithm is then applied to the finite graph $\big(V(G_n), E(G_n)\big)$. Thus the computation supports the proved odd-modulus and $2q$-case results, and it points to the even-modulus conjecture as a natural next problem.

CONCLUSION

In this paper, we studied matching and covering parameters of the bilinear congruence graph G_n over $\mathbb{Z}_n$. The graph has vertex set $\mathbb{Z}_n^2$, and adjacency is defined by the determinant-zero congruence

$$ay \equiv bx \pmod{n}.$$

This separates the graph from the usual zero-divisor graph setting, where adjacency is defined by a product-zero condition.

The main result shows that G_n is nearly matchable for every odd integer $n \ge 3$. The involution

$$(a,b) \mapsto (-a,-b)$$

fixes only $(0,0)$ and pairs every other vertex with an adjacent vertex. Hence

$$\nu(G_n) = \frac{n^2 - 1}{2}, \rho(G_n) = \frac{n^2 + 1}{2}$$

for every odd $n \ge 3$.

For an odd prime p , the proportionality-class decomposition gives

$$\alpha(G_p) = p + 1, \tau(G_p) = p^2 - p - 1.$$

For distinct primes p and q, a CRT-based projective-label argument gives

$$\alpha(G_{pq}) = (p+1)(q+1),$$

and therefore

$$\tau(G_{pq}) = p^2q^2 - (p+1)(q+1).$$

Thus the vertex-cover profile is exact for products of two distinct primes.

We also treated the mixed even case $n = 2q$, where q is an odd prime. A local modification of the negative-pair matching gives a perfect matching, and therefore

$$\nu(G_{2q}) = \rho(G_{2q}) = 2q^2.$$

The computations for $2 \le n \le 30$ support the proved formulas and suggest that G_n may have a perfect matching for every even integer $n \ge 4$. Future work may focus on proving or disproving this conjecture and on studying the prime-

power case G_{p^k} , where zero-divisors create additional adjacency relations that do not appear over fields.

REFERENCES

[1] I. Beck, "Coloring of commutative rings," *Journal of Algebra*, vol. 116, no. 1, pp. 208–226, 1988.

[2] D. F. Anderson and P. S. Livingston, "The zero-divisor graph of a commutative ring," Journal of Algebra, vol. 217, no. 2, pp. 434–447, 1999.

[3] D. F. Anderson, A. Frazier, A. Lauve, and P. S. Livingston, "The zero-divisor graph of a commutative ring II," in Ideal Theoretic Methods in Commutative Algebra, Lecture Notes in Pure and Applied Mathematics, vol. 220, Marcel Dekker, New York, pp. 61–72, 2001.

[4] S. P. Redmond, "An ideal-based zero-divisor graph of a commutative ring," Communications in Algebra, vol. 30, no. 9, pp. 4425–4443, 2002.

[5] D. F. Anderson and S. B. Mulay, "On the diameter and girth of a zero-divisor graph," Journal of Pure and Applied Algebra, vol. 210, no. 2, pp. 543–550, 2007.

[6] A. Blunck and H. Havlicek, "Projective representations I: Projective lines over rings," Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, vol. 70, pp. 287–299, 2000.

[7] A. Blunck and H. Havlicek, "The connected components of the projective line over a ring," Advances in Geometry, vol. 1, no. 1, pp. 107–117, 2001.

[8] H. Daoub and O. Lasfar, "Structural properties of graphs defined by bilinear congruence on the ring of integers modulo n," University of Zawia Journal of Natural and Applied Sciences, vol. 1, no. 1, pp. 56–70, 2025.

[9] C. Berge, "Two theorems in graph theory," Proceedings of the National Academy of Sciences of the United States of America, vol. 43, no. 9, pp. 842–844, 1957.

[10] W. T. Tutte, "The factorization of linear graphs," Journal of the London Mathematical Society, vol. 22, no. 2, pp. 107–111, 1947.

[11] L. Lovász and M. D. Plummer, Matching Theory, Annals of Discrete Mathematics, vol. 29, North-Holland, Amsterdam, 1986.

[12] J. A. Bondy and U. S. R. Murty, Graph Theory, Graduate Texts in Mathematics, vol. 244, Springer, New York, 2008.

[13] R. Diestel, Graph Theory, 5th ed., Graduate Texts in Mathematics, vol. 173, Springer, Berlin, 2017.

[14] D. B. West, Introduction to Graph Theory, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2001.

[15] T. Gallai, "Über extreme Punkt- und Kantenmengen," Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae, Sectio Mathematica, vol. 2, pp. 133–138, 1959.

[16] O. Lasfar, "Maximum matching of zero-divisor graph over a commutative ring," Alqalam Journal of Medical and Applied Sciences, vol. 8, no. 4, pp. 2155–2157, 2025.

[17] D. S. Dummit and R. M. Foote, Abstract Algebra, 3rd ed., John Wiley & Sons, Hoboken, NJ, 2004.

[18] B. R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.