#A89 INTEGERS 22 (2022)

A CLASS OF GRAPHS BASED ON A SET OF MODULI

A. David Christopher
Department of Mathematics, The American College, Tamil Nadu, India
davidchristopher@americancollege.edu.in

Received: 10/11/20, Revised: 2/13/22, Accepted: 8/31/22, Published: 9/12/22

Abstract

This article is concerned with the graph, denoted $G(n, M)$, with vertex set $\{0, 1, \cdots, n-1\}$ and edge set $\{uv : u \equiv v \pmod m$ for some $m \in M \subseteq \{2, 3, \ldots, n-1\}\}$. The problem addressed here is to find the conditions over M that makes $G(n, M)$, (i) a bipartite graph, (ii) a graph with no isolated vertex, (iii) a regular graph, (iv) a path graph, (v) a connected graph, (vi) a Hamiltonian graph, (vii) an Eulerian graph and (viii) a graph decomposable into complete graphs. Some of these conditions are found to be necessary as well.

1. Motivation

In recent literature one can find several classes of graphs based on congruence conditions. M. B. Nathanson [6] introduced a class of graphs whose vertex set is $\{1, 2, \cdots, m\}$ and its edge ab is defined when $a + b \equiv r \pmod m$ for some $r \in R \subseteq \{1, 2, \cdots, m\}$. E. L. Blanton et al. [1] introduced a class of digraphs whose vertex set is $\{0, 1, 2 \ldots, n-1\}$ and its arc ab is defined when $a^2 \equiv b \pmod n$. C. Lucheta et al. [4] introduced a class of graphs whose vertex set is $\{0, 1, 2, \ldots, n-1\}$ and its edge ab is defined when $f(a) \equiv b \pmod m$, where f is any arithmetic function defined modulo m. L. Somer and M. Křìžek [7] investigated the symmetric properties of the digraphs whose vertex set is $\{0, 1, 2, \ldots, n-1\}$ and its arc (x, y) is defined when $x^k \equiv y \pmod n$. M. A. Malik and M. K. Mahmood [5] introduced a class of graphs whose vertex set is $\{0, 1, \ldots, n-1\}$ and its edge ab is defined if the congruence equation: $a^x \equiv b \pmod n$ admits an integer solution x.

The purpose of this paper is to introduce and investigate a new class of graphs whose vertex set is $\{0, 1, , \ldots, n-1\}$ and the edge set is determined by the congruent residues modulo m for $m \in M \subseteq \{2, 3, \ldots, n-1\}$. The class of graphs considered in this article is defined below.

Definition 1. Let $n \geq 3$ be a positive integer and let $M \subseteq \{2, 3, \ldots, n-1\}$. A graph, denoted $G(n, M)$, is defined as follows: the vertex set of $G(n, M)$ is

$\{0, 1, \ldots, n-1\}$ and an edge uv of $G(n, M)$ is defined if $u \equiv v \pmod{m}$ for some $m \in M$. The graph $G(n, M)$ is called a *congruence graph*. The set M is called the *Moduli set*.

The following graphs illustrate this definition.

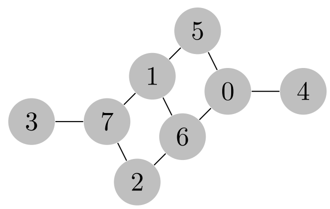

Figure 1: $G(8, \{4, 5, 6\})$

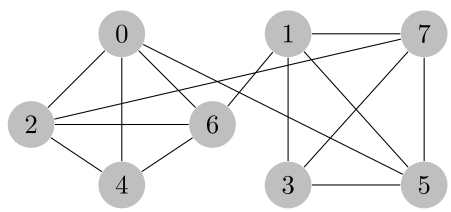

Figure 2: $G(8, \{2, 5\})$

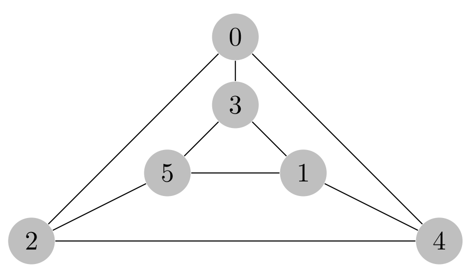

Figure 3: $G(6, \{2, 3\})$

From these graphs and other similar examples, one can guess that the degree sequence: $\deg(0), \deg(1), \ldots, \deg(n-1)$ of $G(n, M)$ follows a palindromic pattern. In Section 2, this observation is found to be an actual fact in view of an expression for the degree sequence. Also, one can observe from the above graphs that $|\deg(k) - \deg(k-1)| \leq 1$ for each $k \in \{1, 2, \cdots, n\}$. This observation is confirmed through a criterion of Section 2 which states that $\deg(v+1) - \deg(v) = \pm 1, 0$. Other consequences of this criterion are recorded in Section 2. The graph in Figure 1 is non-regular and non-Hamiltonian. The graph in Figure 2 is non-regular and Hamiltonian. The graph in Figure 3 is regular and Hamiltonian. Graphs in Figure 1, Figure 2 and Figure 3 are all non-Eulerian. The graph in Figure 1 is bipartite and the others are non-bipartite. All the three graphs are connected and none is a tree. All the three graphs can be decomposable into complete graphs. None of the three graphs has an isolated vertex. Section 3 is concerned with obtaining conditions, some necessary, some sufficient and some both necessary and sufficient for $G(n, M)$ to lie in the aforementioned classifications of graphs.

Throughout this paper, the terminologies of graph theory by G. Chartrand and L. Lesniak [2] were used.

2. Degree Sequence and Regularity

The first result of this paper is an expression for the degree of each vertex in $G(n, M)$.

Proposition 1. *Let $G(n, \{m_1, m_2, \ldots, m_r\})$ be a congruence graph and let $v \in \{0, 1, \ldots, n-1\}$. Then*

$$\deg(v) = \sum_i \left(\lfloor \frac{n-v-1}{m_i} \rfloor + \lfloor \frac{v}{m_i} \rfloor \right) - \sum_{i<j} \left(\lfloor \frac{n-v-1}{lcm(m_i, m_j)} \rfloor + \lfloor \frac{v}{lcm(m_i, m_j)} \rfloor \right)$$
$$+ \sum_{i<j<k} \left(\lfloor \frac{n-v-1}{lcm(m_i, m_j, m_k)} \rfloor + \lfloor \frac{v}{lcm(m_i, m_j, m_k)} \rfloor \right) - \cdots$$

where lcm stands for the least common multiple function, $\lfloor \cdot \rfloor$ denotes the floor function and $\deg(v)$ *denotes the degree of the vertex v.*

Proof. Let v be a vertex of the graph $G(n, \{m_1, m_2, \ldots, m_r\})$. Observe that the number of vertices in the set $\{v+1, v+2, \ldots, n-1\}$ that are adjacent to v equals the number of multiples of $m_i s$ in the set $\{1, 2, \ldots, n-v-1\}$. The latter enumeration equals

$$\sum_i \lfloor \frac{n-v-1}{m_i} \rfloor - \sum_{i<j} \lfloor \frac{n-v-1}{lcm(m_i, m_j)} \rfloor + \sum_{i<j<k} \lfloor \frac{n-v-1}{lcm(m_i, m_j, m_k)} \rfloor - \cdots.$$

Also, the number of vertices in the set $\{0, 1, \ldots, v-1\}$ which are adjacent to v equals the number of multiples of $m_i s$ in the set $\{1, 2 \ldots, v\}$. The latter enumeration equals

$$\sum_i \lfloor \frac{v}{m_i} \rfloor - \sum_{i<j} \lfloor \frac{v}{lcm(m_i, m_j)} \rfloor + \sum_{i<j<k} \lfloor \frac{v}{lcm(m_i, m_j, m_k)} \rfloor - \cdots.$$

The sum of the above two expressions gives $\deg(v)$. Now the result follows. $\square$

Following result is a direct consequence of the result above.

Corollary 1. *Let $G(n, M)$ be a congruence graph. Then*

(a) $\deg(v) = deg(n-v-1)$ *for every* $v \in \{0, 1, \ldots, n-1\}$*. In other words,* $\deg(0), \deg(1), \ldots, \deg(n-1)$ *is a palindromic sequence.*

(b) If n *is odd, then* $\deg(\frac{n-1}{2})$ *is even.*

In some special instances, it is possible to express the degree of the vertices of congruence graphs in a simple form. The following result gives one such simple expression when $M \subseteq \{\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, \ldots, n-1\}$.

Proposition 2. *The following hold:*

(a) Let $M \subseteq \{n, n+1, \ldots, 2n-2\}$ *and let* v *be a vertex of* $G(2n-1, M)$*. Then*

$$\deg(v) = \begin{cases} |M| & \text{if } v = 0; \\ |M \setminus \{2n-1-v, \ldots, 2n-2\}| & \text{if } v \in \{1, 2, \ldots, n-2\}; \\ 0 & \text{if } v = n-1; \\ \deg(2n-2-v) & \text{if } v \in \{n, n+1, \ldots, 2n-2\}. \end{cases}$$

(b) Let $M \subseteq \{n, n+1, \ldots, 2n-1\}$ *and let* v *be a vertex of* $G(2n, M)$*. Then*

$$\deg(v) = \begin{cases} |M| & \text{if } v = 0; \\ |M \setminus \{2n-v, \ldots, 2n-1\}| & \text{if } v \in \{1, 2, \ldots, n-1\}; \\ \deg(2n-2-v) & \text{if } v \in \{n, n+1, \ldots, 2n-1\}. \end{cases}$$

Proof. Let $M \subseteq \{n, n+1, \ldots, 2n-2\}$ and let v be a vertex in $G(2n-1, M)$.

`Case i.` If $v = 0$ then obviously $deg(v) = |M|$.

`Case ii.` Suppose that $v \in \{1, \ldots, n-2\}$. Since $\min M \geq n$, it follows that v is not adjacent with the vertices $\{0, 1, \ldots, v-1\}$. But it is adjacent with $v+m$ for every $m \in M$ satisfying $v + m \leq 2n-2$. That is, for $m \in M$ satisfying the bound $m \leq 2n-2-v$. In set theory notation, $m \in M \setminus \{2n-1-v, \ldots, 2n-2\}$. Hence $\deg(v) = |M \setminus \{2n-1-v, \ldots, 2n-2\}|$.

`Case iii.` Suppose that $v \in \{n, n+1, \ldots, 2n-2\}$. Then from (a) of Corollary 1 it follows that $\deg(v) = \deg(2n-2-v)$.

`Case iv.` Suppose that $v = n-1$. Since $\min M \geq n$, it follows that v is isolated. That is, $\deg(v) = 0$. Now (a) follows.

A similar approach will settle (b). $\square$

It is interesting to note that, given any vertex v in $G(n, M)$,

$$\deg(v+1) - \deg(v) \in \{1, -1, 0\}.$$

The following result has separate criterions that ascertain the value of $\deg(v+1) - \deg(v)$.

Proposition 3. *Let $G(n, \{m_1, m_2, \ldots, m_r\})$ be a congruence graph and let $v \in \{0, 1, \ldots, n-1\}$.*

(a) If $v + 1 \equiv 0 \pmod{m_i}$ for some i and $n - v - 1 \equiv 0 \pmod{m_j}$ for some j, then $\deg(v+1) = \deg(v)$.

(b) If $v + 1 \equiv 0 \pmod{m_i}$ for some i and $n - v - 1 \not\equiv 0 \pmod{m_j}$ for every j, then $\deg(v+1) = \deg(v) + 1$.

(c) If $v + 1 \not\equiv 0 \pmod{m_i}$ for every i and $n - v - 1 \equiv 0 \pmod{m_j}$ for some j, then $\deg(v+1) = \deg(v) - 1$.

(d) If $v + 1 \not\equiv 0 \pmod{m_i}$ for every i and $n - v - 1 \not\equiv 0 \pmod{m_j}$ for every j, then $\deg(v+1) = \deg(v)$.

Proof. Let $M(v)$ denotes the number of multiples of m_is in the set $\{1, 2, \cdots, v\}$. From the proof of Proposition 1 it follows that

$$deg(v) = M(v) + M(n-1-v).$$

In a similar way,

$$deg(v+1) = M(v+1) + M(n-1-(v+1)).$$

Assume that $v+1$ is a multiple of m_i for some i. It follows that $M(v+1) = 1 + M(v)$. Moreover, if $n-1-v$ is a multiple of m_j for some j, then it follows that $M(n-1-(v+1)) + 1 = M(n-1-v)$. Consequently,

$$\begin{aligned} deg(v+1) &= M(v+1) + M(n-1-(v+1)) \\ &= 1 + M(v) + M(n-1-v) - 1 \\ &= deg(v). \end{aligned}$$

Now (a) follows.

Assume that $v+1$ is a multiple of m_i for some i. If $n-1-v$ is not a multiple of m_j for every j, it follows that $M(n-1-(v+1)) = M(n-1-v)$. Consequently,

$$\begin{aligned} deg(v+1) &= M(v+1) + M(n-1-(v+1)) \\ &= 1 + M(v) + M(n-1-v) \\ &= deg(v) + 1. \end{aligned}$$

Now (b) follows.

Assume that $v+1$ is not a multiple of m_i for every i. It follows that $M(v+1) = M(v)$. Now if $n-1-v$ is a multiple of m_j for some j, it follows that $M(n-1-(v+1)) = M(n-1-v)-1$. Consequently, $deg(v+1) = deg(v)-1$. Now (c) follows.

Assume that $v+1$ is not a multiple of m_i for every i. It follows that $M(v+1) = M(v)$. If $n-v-1$ is not a multiple of m_j for every j, then $M(n-1-(v+1)) = M(n-1-v)$. Consequently, $deg(v+1) = deg(v)$. Now (d) follows. □

Corollary 2. *Let $G(n, M)$ be a congruence graph. Then*

$$|deg(v) - deg(v+1)| \leq 1$$

for each $v \in \{0, 1, \ldots, n-1\}$.

Corollary 3. *Let $n > 1$ be an odd integer and let $M \subseteq \{2, \ldots, n-1\}$. Define $M^* = \{km : k \in \mathbb{N}, m \in M, km \leq n-1\}$. If $|M^*| \geq \frac{n}{2}$ and each $v \in \{0, 1, \ldots, n-1\}$ satisfies either (a) or (d) of Proposition 3 then $G(n, M)$ is both Hamiltonian and Eulerian.*

Proof. Since n is odd, from (b) of Corollary 1, it follows that $\deg\left(\frac{n-1}{2}\right)$ is even. Observe that $\deg(0) = |M^*|$. Since each $v \in \{0, 1, \ldots, n-1\}$ satisfies either (a) or (d) of Proposition 3, it follows that $G(n, M)$ is $|M^*|$- regular. Since $\deg\left(\frac{n-1}{2}\right)$ is even, from the $|M^*|$-regularity of $G(n, M)$ it follows that $|M^*|$ is even. Since $|M^*| \geq \frac{n}{2}$, it follows from a sufficient condition for Hamiltonian graphs due to Dirac [3], that $G(n, M)$ is Hamiltonian. Since $G(n, M)$ is Hamiltonian, it is connected. And since $|M^*|$ is even, it follows from the $|M^*|$-regularity of $G(n, M)$, that $G(n, M)$ is Eulerian as well. □

In the result above, a particular class of regular congruence graph is found to be Eulerian. Surprisingly, the converse is always true.

Corollary 4. *Every Eulerian congruence graph is regular.*

Proof. Assume that $G(n, M)$ is Eulerian. Recall that a connected graph is Eulerian if and only if it has no odd degree vertex. From Proposition 3 it follows that: $\deg(v)$ and $\deg(v+1)$ are either identical or differ by one. If $G(n, M)$ is non-regular then there exist two consecutive vertices whose degrees differ by one, which leads to the existence of an odd degree vertex. This implies that $G(n, M)$ is non-Eulerian. Hence, $G(n, M)$ must be regular. □

The following proposition is a characterization for regularity in congruence graphs.

Proposition 4. *The congruence graph $G(n, M)$ is regular if, and only if, either (a) or (b) of the following conditions holds for every $v \in \{0, 1, \ldots, n-1\}$:*

(a) $v+1 \equiv 0 \pmod{m_i}$ *for some* i *and* $n-v-1 \equiv 0 \pmod{m_j}$ *for some* j*;*

(b) $v+1 \not\equiv 0 \pmod{m_i}$ *for every* i *and* $n-v-1 \not\equiv 0 \pmod{m_j}$ *for every* j.

Proof. From Proposition 3 it follows that $\deg(v) = \deg(v+1)$ when either condition (a) or condition (b) is satisfied and vice versa. This is the contention of this result. □

Corollary 5. *If* M *is a subset of the proper divisors of* n *then the congruence graph* $G(n, M)$ *is regular.*

Proof. If $v + 1 \equiv 0 \pmod{m}$ for some $m \in M$ then it follows that $n - v - 1 \equiv 0 \pmod{m}$. On the other hand, if $v+1 \not\equiv 0 \pmod{m}$ for every $m \in M$ then it follows that $n - (v + 1) \not\equiv 0 \pmod{m}$. Now, from Proposition 4 it follows that $G(n, M)$ must be a regular graph. □

Corollary 6. *If* M *is the set of all prime divisors of* n*, then the congruence graph* $G(n, M)$ *is* $n-1-\phi(n)$ *regular, where* $\phi(n)$ *denotes the number of positive integers less than* n *and relatively prime to* n*.*

Proof. From Corollary 5 it follows that $G(n, M)$ is regular. Observe that $\deg(0)$ is the number of multiples of prime divisors of n in $\{1, 2, \cdots, n-1\}$, which is clearly the number of elements in $\{1, 2, \cdots, n-1\}$ that are not relatively prime to n. Since that number is $n - 1 - \phi(n)$, the result follows. □

Corollary 7. *Let* $n \neq 2^k$ *be a composite number and let* $M = \{p_1, p_2, \ldots, p_m\}$ *be the set of all prime divisors of* n*. Then the congruence graph* $G(n, M)$ *is Hamiltonian.*

Proof. Assuming the constraints over n, one can have $\phi(n) \leq \frac{n}{2} - 1$. Hence from Corollary 6 it follows that $deg(v) \geq \frac{n}{2}$ for every vertex v of $G(n, M)$. Now a sufficient condition for Hamiltonian graph due to Dirac [3] implies that $G(n, M)$ is Hamiltonian. □

Corollary 8. *Let* $n \neq 2^k$ *be a composite number and let* $M = \{p_1, p_2, \ldots, p_m\}$ *be the set of all prime divisors of* n*. Then the congruence graph* $G(n, M)$ *is Eulerian if, and only if,* n *is odd.*

Proof. Observe that $n - 1 - \phi(n) \geq \frac{n}{2}$. Now Corollary 7 implies that $G(n, M)$ is Hamiltonian and hence is connected. Recall the fact that $\phi(n)$ is even for every $n \geq 3$. Since $G(n, M)$ is Eulerian only if degree of each vertex in $G(n, M)$ is even, the result follows from Corollary 6. □

3. Structural Analysis

This section begins with the characterization theorems for a congruence graph to be a bipartite graph, graph with no isolated vertex, and a path. Note that there are bipartite congruence graphs with none of its vertex isolated, refer Figure 1.

Also, a necessary condition for a congruence graph to be a tree, a sufficient condition for a congruence graph to be a Hamiltonian graph, a necessary condition for connected congruence graphs and a sufficient condition for connected congruence graph were presented.

Theorem 1. *The congruence graph $G(n, M)$ is bipartite if, and only if, $m \geq \frac{n}{2}$ for every $m \in M$.*

Proof. Assume that $G(n, M)$ is bipartite. If there exists some $m \in M$ such that $m < \frac{n}{2}$, then the vertices 0, m and $2m$ are mutually adjacent to each other in $G(n, M)$, forming a triangle. Thus $G(n, M)$ is non-bipartite, since every cycle in a bipartite graph needs to have an even number of edges. Consequently, $m \geq \frac{n}{2}$ for every $m \in M$.

Conversely, assume that $m \geq \frac{n}{2}$ for every $m \in M$. Consider the set partition $\left\{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor - 1\right\} \cup \left\{\lfloor \frac{n}{2} \rfloor, \ldots, n-1\right\}$ of the vertex set of $G(n, M)$. Since the congruence equation $x \equiv y \pmod{m}$ has no solution in $\left\{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor - 1\right\}$ for every $m \in M$, no two vertices in $\left\{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor - 1\right\}$ are adjacent. Similarly, one can see that no two vertices in $\left\{\lfloor \frac{n}{2} \rfloor, \ldots, n-1\right\}$ are adjacent. Hence $G(n, M)$ is bipartite. □

Consider the following graph; it satisfies the conditions of the theorem above

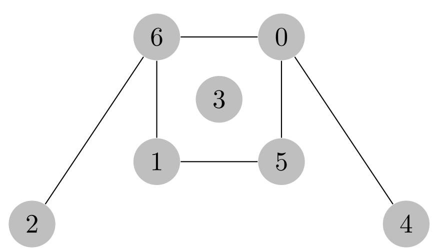

Figure 4: $G(7, \{4, 5, 6\})$

and hence is bipartite. However, it has an isolated vertex, namely 3. Following is a characterization theorem for $G(n, M)$ without isolated vertex, which ensures that every bipartite congruence graph of odd order has an isolated vertex.

Theorem 2. *The congruence graph $G(n, M)$ contains no isolated vertex if, and only if, there exists at least one $m \in M$ such that $m \leq \lfloor \frac{n}{2} \rfloor$.*

Proof. Note that $G(n, M)$ contains an isolated vertex, say v, if, and only if, every $m \in M$ does not divide the numbers $\{1, 2, \ldots v-1, v\} \cup \{1, 2, \ldots, n-v-1\}$.

`Case 1.` Assume that $v \geq \lfloor \frac{n}{2} \rfloor$ and $G(n, M)$ has an isolated vertex. Then it follows that every $m \in M$ does not divide the numbers $v, v-1, \cdots, \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor - 1, \ldots, 2, 1$. This non-divisibility is possible only with $m > v \geq \lfloor \frac{n}{2} \rfloor$ for every $m \in M$.

`Case 2.` Assume that $v < \lfloor \frac{n}{2} \rfloor$ and that $G(n, M)$ has an isolated vertex. Then it follows that $n - v - 1 > n - \lfloor \frac{n}{2} \rfloor - 1 \geq \lfloor \frac{n}{2} \rfloor - 1$. Since $G(n, M)$ has an isolated vertex, every $m \in M$ should not divide the numbers in the set $\{1, 2, \ldots, n-v-1\} = \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor, \ldots\}$. This non-divisibility is possible only when $m > \lfloor \frac{n}{2} \rfloor$. □

The following result has an expression for the number of isolated vertices of $G(n, M)$.

Corollary 9. *The following hold:*

(a) Let $G(2n, M)$ be a congruence graph with $\min M > n$. Then the number of isolated vertices of $G(2n, M)$ is $2(\min M - n)$.

(b) Let $G(2n-1, M)$ be a congruence graph with $\min M \geq n$. Then the number of isolated vertices of $G(2n-1, M)$ is $2(\min M - n) + 1$.

Proof. Let v be a vertex of $G(n, M)$ such that $v \in \{1, 2, \cdots, n-1\}$. From (b) of Proposition 2 it follows that, if v is an isolated vertex then $\min M \geq 2n - v$ and vice versa. Hence $v \geq 2n - \min M$. Note that 0 is not an isolated vertex. Therefore the number of isolated vertices not exceeding $n-1$ is $n-1-(2n-\min M-1) = \min M-n$. Now from the relation $\deg(v) = \deg(2n-1-v)$ it follows that the number of isolated vertices of $G(2n, M)$ is $2(\min M - n)$. Now (a) follows.

A similar approach will settle (b). □

Remark 1. *Let n be a positive integer.*

(a) Assume $n \equiv 1 \pmod 2$. Then the congruence graph $G(n, M)$ is bipartite if, and only if, it contains an isolated vertex.

(b) Assume $n \equiv 0 \pmod 2$ and $\frac{n}{2} \notin M$. Then the congruence graph $G(n, M)$ is bipartite if, and only if, it contains an isolated vertex.

(c) The congruence graph $G(n, M)$ is triangle-free if, and only if, $m \geq \frac{n}{2}$ for every $m \in M$.

(d) Assume $n \equiv 1 \pmod 2$. Then the congruence graph $G(n, M)$ is not a tree (since every tree is bipartite) for any choice of moduli set M, in particular, the congruence graph $G(n, M)$ is not a path for any choice of M.

The following theorem is a characterization for a congruence graph to be a path, provided it has an even number of vertices.

Theorem 3. *The congruence graph $G(2n, M)$ is a path if, and only if, $M = \{n, n+1\}$.*

Proof. Assume that $G(2n, M)$ is a path. Since every path is bipartite, from Theorem 1 it follows that $m \geq n$ for every $m \in M$. If $n \notin M$, then from (b) of Remark 1 it follows that $G(2n, M)$ contains an isolated vertex; which is not the case. Thus, $n \in M$. Since $G(2n, M)$ is a path, $2 \geq \deg(0) \geq |M|$. If $|M| = 1$ then $G(2n, M)$ is a union of complete graphs of order 2, which is not the case. Consequently, $|M| = 2$. Since $n \in M$, the other element in M must be $n+k$ for some k such that $1 \leq k \leq n-1$. Suppose that $k > 1$. Observe that the modulus n contribute exactly n edges namely $(0, n), (1, n+1), (2, n+2), \ldots, (n-1, 2n-1)$, and the modulus $n+k$ contribute exactly $n-k$ edges namely $(0, n+k), (1, n+k+1), \ldots, (n-k-1, 2n-1)$ which leaves with the conclusion that, the total number of edges in $G(2n, M)$ is $n + n - k = 2n - k$; which is impossible. This forces us to conclude that $k = 1$.

To prove the converse part, assume that $M = \{n, n+1\}$. Observe that the edge set of the graph $G(2n, M)$ is $\{(0, n), (1, n+1), \ldots, (n-1, 2n-1)\} \cup \{(0, n+1), (1, n+2), \ldots, (n-2, 2n-1)\}$ which forms the path: $n \to 0 \to n+1 \to 1 \to n+2 \to \cdots \to (2n-1) \to (n-1)$. $\square$

Theorem 4. *The congruence graph $G(n, \{k, k+1\})$ is connected if, and only if, $k \leq \lfloor \frac{n}{2} \rfloor$.*

Proof. Assume $k = \lfloor \frac{n}{2} \rfloor$. If n is even, then in view of Theorem 3, $G(n, \{k, k+1\})$ is a path and hence connected. If n is odd, then the path $0 \to \lfloor \frac{n}{2} \rfloor + 1 \to 1 \to \lfloor \frac{n}{2} \rfloor + 2 \to \cdots \lfloor \frac{n}{2} \rfloor - 1 \to \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2} \rfloor \to \lfloor \frac{n}{2} \rfloor$ passes through every vertex of $G(n, \{k, k+1\})$ making $G(n, \{k, k+1\})$ connected.

Assume that $k < \lfloor \frac{n}{2} \rfloor$. In accordance with the division algorithm: $n - 1 = qk + r$ for a unique positive integer q and $0 \leq r \leq k-1$. Now consider the walk $0 \to k+1 \to 1 \to k+2 \to 2 \to \cdots \to k-2 \to k+(k-1) \to k-1 \to 2k \to k \to 2k+1 \to k+1 \to 2k+2 \to k+2 \cdots \to k+k-1 \to 3k \to 2k \to 3k+1 \to 2k+1 \to \cdots \to qk \to (q-1)k \to qk+1 \to (q-1)k+1 \to qk+2 \to \cdots \to (q-1)k+r-1 \to qk+r$; which passes through every vertex of $G(n, \{k, k+1\})$ making $G(n, \{k, k+1\})$ connected.

To prove the converse part, assume to the contrary that $k > \lfloor \frac{n}{2} \rfloor$. Then from Theorem 2 it follows that $G(n, \{k, k+1\})$ has an isolated vertex. That is, $G(n, \{k, k+1\})$ is disconnected. Hence, $k \leq \lfloor \frac{n}{2} \rfloor$. $\square$

Definition 2. Let M be a set of positive integers. A pair of positive integers, say $\{a, b\} \subseteq M$, is said to be a *closed pair* of M, if there exists some positive integer d such that $a - d, b - d \in M$.

Theorem 5. *If a congruence graph $G(2n, M)$ is a tree then M satisfies the following properties:*

(a) $\min M = n$,

(b) $\sum_{m\in M}(2n - m) = 2n - 1$,

(c) M is void of closed pairs.

Proof. Assume that $G(2n, M)$ is a tree. Since every tree is bipartite, from Theorem 1 it follows that $m \geq n$ for every $m \in M$. If $n \notin M$, then from (b) of Remark 1 it follows that $G(2n, M)$ contains an isolated vertex; which is not the case. Thus, $n \in M$. Consequently, $\min M = n$.

Since $\min M = n$, every $m \in M$ contribute exactly $2n - m$ edges namely $(0, m), (1, m + 1), \ldots, (2n - m - 1, 2n - 1)$ in $G(2n, M)$. Therefrom the relation $\sum_{m\in M}(2n - m) = 2n - 1$ holds, since every tree with p vertices has $p - 1$ edges.

Assume the contrary to condition (c), that M contains a closed pair $\{a, b\}$. Then there exists a positive integer d such that $a - d, b - d \in M$. Clearly, $d \leq n - 1$. Consequently, one can realize the cycle: $0 - a - d - b - 0$; which is a contradiction. Hence, M must be void of closed pair. □

The converse of the theorem above need not be true. For example, the graph $G(18, \{9, 14, 15, 17\})$ satisfies the conditions mentioned in Theorem 5, but one can see that it is not a tree. Nevertheless, those necessary conditions can be used to characterize tree structure in congruence graphs when $|M| = 2$.

Theorem 6. *Let $G(2n, M)$ be a congruence graph with $|M| = 2$. Then $G(2n, M)$ is a tree if, and only if, $M = \{n, n + 1\}$.*

Proof. Assume that $G(2n, M)$ is a tree with $|M| = 2$. From condition (a) of Theorem 5 it follows that $\min M = n$. Consequently, $M = \{n, n + r\}$ for some $r \in \{1, 2, \cdots, n - 1\}$. Now from condition (b) of Theorem 5 it follows that $n + 2n - (n + r) = 2n - 1$. This gives $r = 1$. Thus $M = \{n, n + 1\}$. Theorem 3 is the converse. □

Theorem 7. *For $n \geq 4$, the congruence graph $G(n, M)$ is not a cycle for any choice of moduli set M.*

Proof. Assume that a congruence graph $G(n, M)$ is a cycle for some choice of M. Observe that $2 = \deg(0) \geq |M|$. If $|M| = 1$ then $G(n, M)$ is a union of complete graphs, which is not the case. Hence $|M| = 2$. Let $M = \{m_1, m_2\}$ with $m_1 < m_2$.

Case i. Assume that $n \equiv 0 \pmod 2$. Then from Theorem 1 it follows that $m_1 \geq \frac{n}{2}$. Since $G(n, M)$ has no isolated vertex, from Theorem 2 it follows that $m_1 \leq \frac{n}{2}$. Consequently, $m_1 = \frac{n}{2}$. Put $m_2 = \frac{n}{2} + k$ for some $k \geq 1$. Since the modulus m_2 contributes exactly $\frac{n}{2} - k$ edges, namely, $(0, \frac{n}{2} + k)$, $(1, \frac{n}{2} + k + 1) \ldots (\frac{n}{2} - k - 1, n - 1)$, and the modulus m_1 contributes exactly $\frac{n}{2}$ edges, namely, $(0, \frac{n}{2})$, $(1, \frac{n}{2}+1) \ldots (\frac{n}{2}-1, n-1)$, the total number of edges in $G(n, M)$ is $\frac{n}{2} + \frac{n}{2} - k = n - k$; which is impossible.

Case ii. Assume that $n \equiv 1 \pmod 2$. Since $G(n, M)$ has no isolated vertex, from Theorem 2 it follows that $m_1 \leq \lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$. This modulus m_1 produces a triangle, namely, $0 \to m_1 \to 2m_1 \to 0$; this contradicts the assumption.

Consequently, for any choice of moduli set M, the congruence graph $G(n, M)$ cannot be a cycle. □

Though congruence graph is not a cycle for any choice of moduli set, there are instances where some congruence graphs were possesed with a Hamiltonian cycle. A sufficient condition is given below to ascertain a class of congruence graphs having Hamiltonian cycle.

Theorem 8. *let n and a be two positive integers such that $1 < a < \frac{n}{2}$ and $\gcd(a, n) = 1$. Then the congruence graph $G(n, \{a, n-a\})$ is Hamiltonian.*

Proof. For $0 \leq k \leq a-1$, define m_k to be the greatest positive integer such that $k + m_k a \leq n - 1$. Then it follows that

$$\{0, 1, \ldots, n-1\} = \cup_{k=0}^{a-1} \{k, k+a, k+2a, \ldots, k+m_k a\}.$$

Observation 1. Let $0 \leq k \leq a-1$. The bound $0 \leq k + m_k a - (n-a) \leq a-1$ holds. For if $k + m_k a - (n-a) < 0$, then rearranging gives $k + (m_k+1)a \leq n-1$. This damages the maximality assumption of m_k. Also if $k + m_k a - (n-a) \geq a$, then

$$\begin{aligned} a &\leq k + m_k a - (n-a) \\ &\leq n - 1 - n + a \\ &= a - 1, \end{aligned}$$

which is a contradiction.

Observation 2. For $0 \leq k, s \leq a-1$ with $k \neq s$, the inequality $k + m_k a - (n-a) \neq s + m_s a - (n-a)$ holds. For if $k + m_k a - (n-a) = s + m_s a - (n-a)$ for some $k \neq s$, then $(m_k - m_s)a = s - k$. This leads to the conclusion that $a \mid (s-k)$, which is not possible, since $|s-k| \leq a-1$.

Let $k_0 = 0$ and let s_1 be the largest positive integer such that $s_1 a \leq n-1$. Put $k_1 = s_1 a - (n-a)$. For $2 \leq r \leq a-1$, define s_r to be the largest positive integer such that $k_{r-1} + s_r a \leq n-1$. Define $k_r = k_{r-1} + s_r a - (n-a)$.

The Hamiltonian cycle to be constructed needs to passes through each k_i. To meet that end, the condition $\gcd(a, n) = 1$ is required. For otherwise, $d = \gcd(a, n) \geq 2$ will imply that $d | k_r$ for every r. Consequently $k_1, k_2, \ldots$ constitute the set of multiples of d in the set $\{1, 2, \ldots, n-1\}$. Therefore, if one assumes that $\gcd(a, n) = 1$ then from the above observations it follows that $\{k_1, k_2, \ldots, k_{a-1}\} = \{1, 2, \ldots, a-1\}$.

Observe that $k_a = 0$. For otherwise, $k_a = l = k_r$ for some $l, r \in \{1, 2 \cdots, a-1\}$. This gives $k_{a-1} - k_{r-1} = (s_r - s_a)a$, which in view of the observation 1 gives $k_{a-1} = k_{r-1}$ which contradicts the observation 2.

Now consider the cycle: $0 \to a \to 2a \to \cdots \to s_1 a \to k_1 \to k_1 + a \to \cdots \to k_1 + s_2 a \to k_2 \to k_2 + a \to \cdots \to k_{a-1} + s_a a \to 0$. From the maximality restriction of each s_i it follows that this cycle passes through all congruence classes modulo a of the set $\{0, 1, \cdots, n-1\}$ altogether satisfying the congruence conditions. □

Remark 2. *The sufficient condition mentioned in the theorem above need not be necessarily hold. For the graphs in Figure 2 and Figure 3 are Hamiltonian, but the above condition does not hold in both graphs.*

Connectedness is a most desirable attribute of a graph. The following result is a sufficient condition for a congruence graph to be connected.

Theorem 9. *Let $n \geq 4$ be a positive integer and let $M \subseteq \{2, 3, \ldots, n-1\}$. If there exist $a, b \in M$ such that $\gcd(a, b) = 1$ and $a + b \leq n + 1$, then the congruence graph $G(n, M)$ is connected.*

Proof. For $0 \leq i \leq a-1$, define M_i to be a complete graph having the vertices $i, i+a, \ldots, i+s_i a$, where s_i is the largest integer such that $i + s_i a \leq n-1$. Define a simple graph, say G^*, whose vertex set is $\{M_0, M_1, \ldots, M_{a-1}\}$ and adjacency in G^* is defined as follows: M_i and M_j are adjacent if either there exists an edge between $i + s_i a$ and $j + s'_j a$ or there exists an edge between $j + s_j a$ and $i + s'_i a$ in $G(n, M)$, where $s'_i \leq s_i$ and $s'_j \leq s_j$. Note that if there exists a path joining all the vertices in G^*, then $G(n, M)$ is connected. The rest of the proof is concerned with constructing such a path.

Observation 1. The inequality $i + s_i a - b \neq i + s'_i a$ holds for every $s'_i < s_i$. For otherwise, $(s_i - s'_i)a = b$; which is absurd, since $\gcd(a, b) = 1$.

Observation 2. The incongruence $i + s_i a - b \not\equiv j + s_j a - b \pmod{a}$ holds for $i \neq j$. For otherwise, $(s_i - s_j)a \equiv (j-i) \pmod{a}$; which is absurd, since $1 \leq |j-i| \leq a-1$.

Define $k_0 = 0$. For $1 \leq r \leq a-1$, define k_r to be the least non-negative integer such that $k_{r-1} + s_{k_{r-1}} a - b \equiv k_r \pmod{a}$.

The path to be constructed in G^* needs to passes through each k_i. To achieve that end, the condition $\gcd(a, b) = 1$ is required. For if $d = \gcd(a, b) \geq 2$ then from the recursive definition of k_r it follows that every k_i is a multiple of d. Now from the assumption $\gcd(a, b) = 1$, observation 1 and observation 2 it follows that $\{k_0, k_1, \cdots, k_{a-1}\} = \{0, 1, \ldots, a-1\}$.

Based on the above observations, by reducing b modulo a from each $i + s_i a$, one can find a path passing through all M_is. Hence G^* is connected. Consequently, $G(n, M)$ is connected. □

The converse of the above theorem is not true as one can see that $G(16, \{6, 10, 15\})$

is connected but its moduli set does not have a relatively prime pair. However, $\gcd(M)$ should be necessarily equal to one if $G(n, M)$ is connected.

Theorem 10. *If the congruence graph $G(n, M)$ is connected then* $\gcd(M) = 1$.

Proof. If M^* is obtained from M by replacing its elements by some of its non-trivial divisors (if any), then $G(n, M)$ is a spanning subgraph of $G(n, M^*)$. Now if $d = \gcd(M) \geq 2$ then $G(n, M)$ is a spanning subgraph of $G(n, \{d\})$. Since $G(n, \{d\})$ is a union of complete graphs, the non-connectivity of $G(n, M)$ is clear. Hence, $\gcd(M) = 1$. □

The closing result is a characterization for the decomposition of $G(n, M)$ into complete graphs.

Theorem 11. *The congruence graph $G(n, M)$ can be decomposable into complete graphs if, and only if, $lcm(m_i, m_j) > n - 1$ for every two elements $m_i, m_j \in M$.*

Proof. Observe that for every modulus $m \in M$, the graph $G(n, \{m\})$ can be decomposable into complete graphs. Denote the edge set of $G(n, \{m\})$ by E_m.

Assume that $lcm(m_i, m_j) > n - 1$ for every pair of elements say $m_i, m_j \in M$. To prove the decomposability of $G(n, M)$ into complete graphs it is enough to show that $E_{m_i} \cap E_{m_j} = \emptyset$. If $ab \in E_{m_i} \cap E_{m_j}$ for some $m_i, m_j \in M$, then $a \equiv b \pmod{m_i}$ and $a \equiv b \pmod{m_j}$. This gives $a \equiv b \pmod{lcm(m_i, m_j)}$; this is impossible since $|a - b| \leq n - 1$. Thus, decomposability is assured.

To prove the converse part, assume that $G(n, M)$ can be decomposable into complete graphs. We need to show that $lcm(m_i, m_j) > n - 1$ for every pair of elements say $m_i, m_j \in M$. If it is not so, there exist some pair of elements in M say (m_i, m_j) such that $lcm(m_i m_j) \leq n - 1$. Then one can find two vertices a and b such that $a \equiv b \pmod{lcm(m_i, m_j)}$. Consequently, $a \equiv b \pmod{m_i}$ and $a \equiv b \pmod{m_j}$. That is, $ab \in E_{m_i} \cap E_{m_j}$. In other words, $G(n, M)$ is a graph which is non-decomposable into complete graphs. Thus, $lcm(m_i, m_j) > n - 1$ for every $m_i, m_j \in M$. □

Acknowledgement. I would like to thank the editor and the referee for their constructive comments which helped improve the presentation and content of this paper.

References

[1] E. L. Blanton, Jr., S. P. Hurd and J. S. McCranie, On a digraph defined by squaring modulo n, *Fibonacci Quart.* **30** (1992), 322-334.

[2] G. Chartrand, L. Lesniak, *Graphs and digraphs*, Third edition, Chapman Hall, London, 1996.

[3] G. A. Dirac, Some theorems on abstract graphs, *Proc. Lond. Math. Soc.* **2** (1952), 69-81.

[4] C. Lucheta, E. Miller, C. Reiter, Digraphs from powers modulo p, *Fibonacci Quart.* **34** (1996), 226-239.

[5] M. A. Malik and M. K. Mahmood, On simple graphs arising from exponential congruences, *J. Appl. Math.* (2012), 1-10.

[6] M. B. Nathanson, Connected components of arithmetic graphs, *Monatsh. Math.* **89** (1980), 219-222.

[7] L. Somer, M. Kr̆ìžek, On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$, *Discrete Math.* **309** (2009), 1999-2009.