Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2012, Article ID 292895, 10 pages
doi:10.1155/2012/292895

Research Article

On Simple Graphs Arising from Exponential Congruences

M. Aslam Malik and M. Khalid Mahmood

Department of Mathematics, University of the Punjab, Lahore 54590, Pakistan

Correspondence should be addressed to M. Khalid Mahmood, khalid.math@pu.edu.pk

Received 19 March 2012; Revised 17 June 2012; Accepted 3 September 2012

Academic Editor: Maurizio Porfiri

We introduce and investigate a new class of graphs arrived from exponential congruences. For each pair of positive integers a and b, let $G(n)$ denote the graph for which $V = \{0, 1, \ldots, n-1\}$ is the set of vertices and there is an edge between a and b if the congruence $a^x \equiv b \pmod{n}$ is solvable. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime power factorization of an integer n, where $p_1 < p_2 < \cdots < p_r$ are distinct primes. The number of nontrivial self-loops of the graph $G(n)$ has been determined and shown to be equal to $\prod_{i=1}^{r}(\phi(p_i^{k_i}) + 1)$. It is shown that the graph $G(n)$ has 2^r components. Further, it is proved that the component Γ_p of the simple graph $G(p^2)$ is a tree with root at zero, and if n is a Fermat's prime, then the component $\Gamma_{\phi(n)}$ of the simple graph $G(n)$ is complete.

1. Introduction

The notion of congruence is intrinsic in number theory. Modular arithmetic has clutched a vital contrivance for most of the number theoretic mathematics. In recent years, studying graphs through congruences is of charismatic and an independent interest of number theorists. It has cemented a novel approach to introduce a premium connection between Number Theory and Graph Theory. On behalf of modular arithmetic, we can manipulate many fascinating features of graphs. We first encounter the ideas used in [1–5], where digraphs from congruences were discussed. The conditions for regularity and semiregularity of such digraphs are presented in [1, 2]. The necessary and sufficient conditions for the existence of isolated fixed points have been established in [3]. The structures of symmetric digraphs have been studied in [4, 5]. In this paper we discuss the graph $G(n)$ arriving from exponential congruences. We assign to each pair of positive integers a and b an edge (a, b) of the graph $G(n)$ if the congruence $a^x \equiv b \pmod{n}$ is solvable, where $V = \{0, 1, \ldots, n-1\}$ is the set of vertices of $G(n)$ and $E \subseteq V \times V$ is the set of edges of $G(n)$. Then the graph $G(n)$

has a loop at a vertex a if and only if $a^x \equiv a \pmod{n}$ admits a solution. Since the congruence relation is an equivalence relation, so $a^x \equiv a \pmod{n}$, $a \in \{0, 1, \ldots, n-1\}$ always admits a solution $x = 1$. Thus we call $x = 1$ a trivial solution and, so far, the loops due to trivial solution are called trivial loops. Thus it becomes interesting to find the number of vertices in $\{0, 1, \ldots, n-1\}$ such that the congruence $a^x \equiv a \pmod{n}$ admits a nontrivial solution. The loops at vertices corresponding to nontrivial solutions are called nontrivial loops. Since for each $\alpha \geq 2$, the congruence $a^\alpha \equiv a \pmod{n}$, for $a = 0, 1$, so the loops at vertices 0 and 1 will be considered as nontrivial loops. We denote the number $L(n)$ for nontrivial loops of the graph $G(n)$. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime power factorization of an integer n, where $p_1 < p_2 < \cdots < p_r$ are distinct primes. The number $L(n)$ of the graph $G(n)$ has been determined and shown to be equal to $\prod_{i=1}^{r} (\phi(p_i^{k_i}) + 1)$, where ϕ is the Euler's phi function. It has been shown that the graph $G(n)$ has 2^r components. We label these components as Γ_d, where $d \mid n$ or $d = \phi(n)$. The order of each component of the graph $G(n)$ has been determined. Further, it is proved that the component Γ_p of the simple graph $G(p^2)$ is always a tree with root at zero. Also if n is a Fermat's prime, then the component $\Gamma_{\phi(n)}$ of the simple graph $G(n)$ is a complete graph.

2. Preliminaries

A graph G is simple if it is free from loops and multiedges. The vertices $a_1, a_2, \ldots, a_{k-1}, a_k$ will constitute a cycle of length k if each of the following congruences is solvable:

$$\begin{aligned} a_1^x &\equiv a_2 \pmod{n}, \\ a_2^x &\equiv a_3 \pmod{n}, \\ &\vdots \\ a_k^x &\equiv a_1 \pmod{n}. \end{aligned} \tag{2.1}$$

A graph G is said to be connected if there is a path from x to y, for each pair of vertices x and y. A maximal connected subgraph is called a component [6].

In Figure 1, the simple graph $G(30)$ has eight components. A graph G is complete if every two distinct vertices of G are adjacent. Thus $G(n)$ is complete if $a^x \equiv b \pmod{n}$ is solvable for each distinct pair of vertices in V. The degree of a vertex v in G is the number of edges incident with v. It is denoted by $\deg(v)$. If $\deg(v) = r$ for each vertex v of $G(n)$, then $G(n)$ is called r-regular or regular graph of degree r. The simple graph $G(30)$ has two 3-regular and two 1-regular components.

We recall the definition of Euler's phi function [7], and some of its properties.

Definition 2.1. For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n which are relatively prime to n. Note that $\phi(1) = 1$, because $\gcd(1, 1) = 1$. Thus we can write

$$\phi(n) = \begin{cases} 1, & \text{if } n = 1, \\ \text{Number of integers less than } n \text{ and co-prime to } n, & \text{if } n \neq 1. \end{cases} \tag{2.2}$$

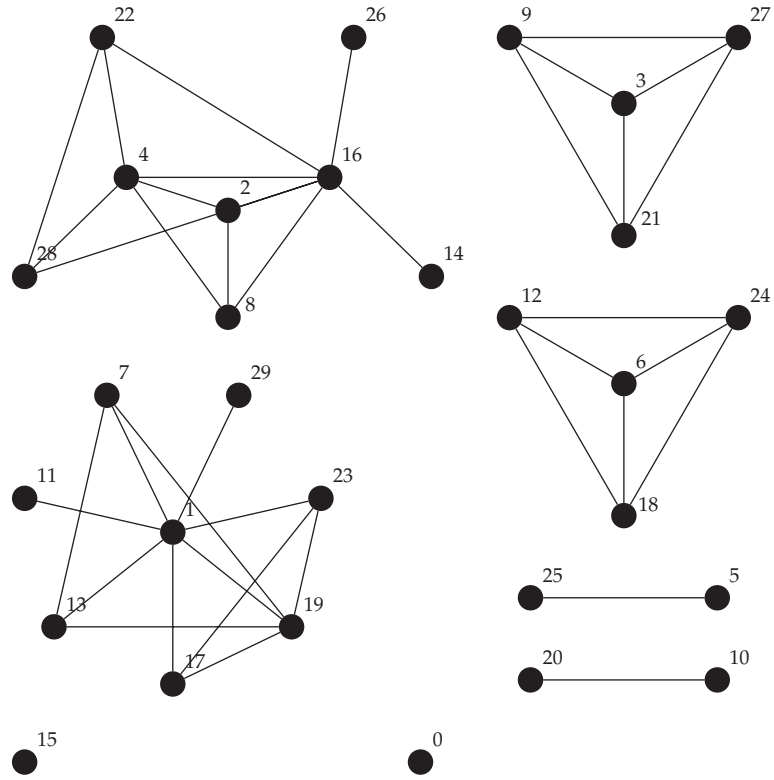

Figure 1: The simple graph of $G(30)$.

By the definition of Euler's phi function, it is clear that if $a \mid b$, then $\phi(a) \mid \phi(b)$. Also $\phi(p) = p - 1$ if and only if p is a prime number. We will need the following results of [7], regarding Euler's phi function, for use in the sequel.

Theorem 2.2. *If p is a prime and $k > 0$, then*

$$\phi\left(p^k\right) = p^{k-1}(p-1). \tag{2.3}$$

Let f be an arithmetic function. One recalls that f is said to be multiplicative if $f(mn) = f(m)f(n)$, $\gcd(m,n) = 1$.

The following theorem is the generalization of the well-known Fermat's Little theorem which states that if $(a,p) = 1$, then $a^p \equiv 1 \pmod{p}$.

Theorem 2.3 (Euler). *If $n \geq 1$ and $(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Definition 2.4 (see [7]). A set of k integers is a complete residue system (CRS) modulo k if every integer is congruent to exactly one of the modulo k. If we delete integers from CRS, which are not prime to k, then the remaining integers will constitute the reduced residue system (RRS) modulo k.

Theorem 2.5 (counting principle [8]). *If a work is distributed over $r_1, r_2, \ldots, r_t$, objects with r_1 object occuring s_1 ways, r_2 object occuring s_2 ways, and r_t object occuring s_t ways, then the work can be done in $s_1 s_2 \cdots s_t$ ways.*

Theorem 2.6 (the inclusion-exclusion principle [9]). *Let $A_1, A_2, \ldots, A_n$ be n finite sets. Then*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} A_i\right|. \tag{2.4}$$

3. Applications of Euler's Phi Function

In Graph Theory, a loop or a self-loop is an edge that connects a vertex to itself. A vertex of an undirected graph is called an isolated vertex if it is not the endpoint of any edge. This means that it is not connected with any other vertex of the graph. Thus in our case, the vertex v is an isolated vertex if and only if $v^x \equiv u \pmod{n}$, $v \neq u$ is not solvable. Now if we omit the condition of simplicity in our graph, then this isolated vertex will contribute twice in the degree as there will be a self-loop at v as the congruence $v^x \equiv v \pmod{n}$ is solvable. This leads to the following results.

Theorem 3.1. *Let $n = 2p_1p_2\cdots p_k$ be the prime factorization of n, where $p_1 < p_2 < \cdots < p_k$ are distinct, odd primes. Then 0 and $p_1p_2\cdots p_k$ are isolated vertices of $G(n)$. That is, the vertices 0 and $p_1p_2\cdots p_k$ are not the endpoints of any edge in graph $G(n)$ except loop at these vertices.*

Proof. The element a, where $0 \le a \le n-1$, is an isolated point of the graph $G(n)$ if and only if the solvability of $a^x \equiv b \pmod{n}$ implies that $a = b$. It is trivial that 0 is an isolated point of $G(n)$ as $a^x \equiv 0 \pmod{2p_1p_2\cdots p_k}$ is solvable if and only if $a \equiv 0 \pmod{2p_1p_2\cdots p_k}$. Moreover, $p_1 < p_2 < \cdots < p_k$ are distinct, odd primes, so for some integer $\beta > 1$, $(p_1p_2\cdots p_k)^{\beta-1} - 1$ is an even integer. Thus $2p_1p_2\cdots p_k \mid p_1p_2\cdots p_k((p_1p_2\cdots p_k)^{\beta-1} - 1)$ and hence $(p_1p_2\cdots p_k)^x \equiv p_1p_2\cdots p_k \pmod{2p_1p_2\cdots p_k}$ is solvable with root β. Next, we claim that the congruence $(p_1p_2\cdots p_k)^x \equiv a \pmod{2p_1p_2\cdots p_k}$, $a \not\equiv p_1p_2\cdots p_k \pmod{2p_1p_2\cdots p_k}$ is not solvable. To prove our assertion, let $a \not\equiv p_1p_2\cdots p_k \pmod{2p_1p_2\cdots p_k}$ and suppose there exists an integer $\alpha \ge 1$, such that the congruence, $(p_1p_2\cdots p_k)^\alpha \equiv a \pmod{2p_1p_2\cdots p_k}$ is balanced. Then there exists some integer t such that

$$(p_1p_2\cdots p_k)^\alpha = a + 2p_1p_2\cdots p_k t. \tag{3.1}$$

This implies that $p_1p_2\cdots p_k((p_1p_2\cdots p_k)^{\alpha-1} - 2t) = a$. But then $p_1p_2\cdots p_k \mid a$. Let $a = t_1p_1p_2\cdots p_k$ for some integer t_1. If t_1 is even, then $2p_1p_2\cdots p_k \mid a$ and hence by (3.1), $2p_1p_2\cdots p_k \mid (p_1p_2\cdots p_k)^\alpha$, a contradiction as $(p_1p_2\cdots p_k)^\alpha$ is an odd integer. So let $t_1 = 2r+1$, for some integer r. Then $a = t_1p_1p_2\cdots p_k = (2r+1)p_1p_2\cdots p_k$ and this shows that $2p_1p_2\cdots p_k \mid a - p_1p_2\cdots p_k$ which is a contradiction against the fact that $a \not\equiv p_1p_2\cdots p_k \pmod{2p_1p_2\cdots p_k}$. Finally, the congruence $(p_1p_2\cdots p_k)^x \equiv 0 \pmod{2p_1p_2\cdots p_k}$ is not solvable since an odd integer is not divisible by an even integer. Hence 0 and $p_1p_2\cdots p_k$ are not adjacent as well. □

Corollary 3.2. *If n is an odd square free integer, then 0 is the only isolated vertex of the graph $G(n)$.*

Theorem 3.3. *Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ be the prime power factorization of a non-square-free integer n, where $p_1 < p_2 < \cdots < p_k$ are distinct primes, $k_i \geq 1$ and $r \geq 1$. Then 0 and kp, where $k = 0, 1, \ldots, \lfloor n/p \rfloor$, and $p = p_1p_2\cdots p_k$, are always adjacent vertices in $G(n)$.*

Proof. We show that the congruence $(kp)^x \equiv 0 \pmod{n}$ is solvable for all $k = 0, 1, \ldots, \lfloor n/p \rfloor$. Let p, q be two distinct primes such that $n = pq^2$. Then $(kpq)^2 = k^2p^2q^2 = k^2p(pq^2) \equiv 0 \pmod{n}$. Thus $x = 2$ is the solution of the congruence $(kpq)^x \equiv 0 \pmod{pq^2}$. We follow the fashion explained above. For this, take $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Let $t = \operatorname{lcm}(p_1, p_2, \ldots, p_k)$, then there exist integers $t_1, t_2, \ldots, t_k$ such that $t = t_ik_i$, for each $i = 1, 2, \ldots, k$. Let $m = \prod_{i=1}^{r} p_i^{k_i(t_i-1)}$. Then it is easy to see that

$$(kp)^t = k^t p_1^{t_1k_1}p_2^{t_2k_2}\cdots p_r^{t_rk_r} = k^t mn \equiv 0 \pmod{n}. \tag{3.2}$$

This shows that $x = t = \operatorname{lcm}(p_1, p_2, \ldots, p_k)$ is the solution of the congruence, $(kp)^x \equiv 0 \pmod{n}$. Hence, kp and 0 are the adjacent vertices in $G(n)$. □

The following results give a formula for finding the number of nontrivial self-loops of the graph $G(n)$.

Lemma 3.4. *Let p be a prime number. Let $n = p^k$, $k \geq 2$ and let ϕ be the Euler's phi function. Then $L(n) = \phi(p^k) + 1$.*

Proof. Let $n = p^k$, $k \geq 2$. A vertex v of the graph $G(n)$ has a self-loop if and only if $v^x \equiv v \pmod{n}$ is solvable. Thus to find the number of self-loops in $G(n)$, we need to count the number of vertices v in CRS $\pmod{n}$ such that the congruence $v^x \equiv v \pmod{n}$ is solvable. By Euler's Theorem, if $(a, n) = 1$, then $a^x \equiv 1 \pmod{n}$ is solvable with $x = \phi(n)$ as its root, whence $a^x \equiv a \pmod{n}$ is solvable with $x = \phi(n) + 1$. Since $p, 2p, \ldots, p^{k-1} \cdot p$ are the p^{k-1} integers which are not prime to p^k, so there are $p^k - p^{k-1} = \phi(p^k)$ integers in CRS $\pmod{n}$ for which the congruence $a^x \equiv a \pmod{n}$ is solvable. Also, for each $k \geq 1$, the vertex 0 has self-loop in $G(p^k)$. Thus there are $\phi(p^k)+1$ self-loops. For the case, if $a \in \{p, 2p, \ldots, p^{k-1}\cdot p\}$, with α as the solution of $a^x \equiv a \pmod{p^k}$. Then $a^{\alpha-1} \equiv 1 \pmod{p^{k-1}}$ implies that $a^{\alpha-1} \equiv 1 \pmod{p}$. This yields a contradiction against the fact that if $a \in \{p, 2p, \ldots, p^{k-1} \cdot p\}$, then $a^{\alpha-1} \equiv 0 \pmod{p}$. Hence, there exist no vertex $a \in \{p, 2p, \ldots, p^{k-1} \cdot p\}$, for which $a^x \equiv a \pmod{n}$ is solvable. Thus $\phi(p^k) + 1$ are the only vertices for which the graph $G(n)$ has self-loops. □

The following theorem provides us the cardinality of the set of those vertices of $G(n)$ which have nontrivial self-loops, where $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ and $r \geq 2$.

Theorem 3.5. *Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ be the prime power factorization of an integer n, where $p_1 < p_2 < \cdots < p_r$ are distinct primes, $k_i \geq 1$ and $r \geq 2$. Then*

$$L(n) = \prod_{i=1}^{r} \left(\phi\left(p_i^{k_i}\right) + 1\right). \tag{3.3}$$

Proof. We apply induction on r. By Lemma 3.4, result is true for $r = 1$. Suppose result is true for $r - 1$ distinct prime factors. That is, if $m = p_1^{k_1}p_2^{k_2}\cdots p_{r-1}^{k_{r-1}}$, then $L(m) = \prod_{i=1}^{r-1}(\phi(p_i^{k_i}) + 1)$. Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r} = mp_r^{k_r}$. Now, the congruence $a^x \equiv a \pmod{mp_r^{k_r}}$ is solvable if and only if the congruences $a^x \equiv a \pmod{m}$ and $a^x \equiv a \pmod{p_r^{k_r}}$ are solvable. But by induction, the

graph $G(m)$ has $\prod_{i=1}^{r-1}(\phi(p_i^{k_i})+1)$ self-loops and, by Lemma 3.4, the graph $G(p_r^{k_r})$ has $\phi(p_r^{k_r})+1$ self-loops. Hence, by Theorem 2.5, the graph $G(n)$ has $\prod_{i=1}^{r}(\phi(p_i^{k_i})+1)$ self-loops. This through our result. In Figure 2, we depict Theorem 3.5 for $n = 24$. □

Corollary 3.6. *Let $n = p_1p_2\cdots p_r$ be the prime factorization of a square-free integer n, where $p_1 < p_2 < \cdots < p_k$ are distinct primes and $r \geq 2$. Then*

$$L(n) = p_1p_2\cdots p_r. \tag{3.4}$$

Proof. It is easy to see that $\phi(p) + 1 = p$, for any prime p. Thus by Theorem 3.5, corollary follows. That is,

$$L(n) = p_1p_2\cdots p_r. \tag{3.5}$$

□

Corollary 3.7. *Let m and n be two non-square-free integers such that* $\gcd(m, n) = 1$. *Then,*

$$L(mn) = L(m)L(n). \tag{3.6}$$

4. Components and Their Characteristics

Recall that a maximal connected subgraph of a graph G is called a component. For instance, the vertices $v_1, v_2, \ldots, v_r$ from CRS $(\bmod n)$ will constitute a component of the graph $G(n)$ if for each $i, 1 \leq i \leq r$, there exist some $j, 1 \leq j \leq r$ such that $v_i^x \equiv v_j \pmod{n}$ is solvable, for all $i \neq j$. The following theorem explores some interesting characteristics of components for the simple graph $G(n)$.

Theorem 4.1 (main theorem). *Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ be the prime power factorization of an integer n, where $p_1 < p_2 < \cdots < p_r$ are distinct primes, $k_i \geq 1$ and $r \geq 1$. Then,*

(a) *$G(n)$ has 2^r components,*

(b) *if $n = p^2$, p is a prime number, then Γ_p is a tree with root at 0,*

(c) *if n is a Fermat's prime, then $\Gamma_{\phi(n)}$ is complete.*

Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Then $p_1, p_2, \ldots, p_r, p_1p_2, \ldots, p_1p_r, \ldots, p_1p_2\cdots p_r$ are the possible square-free positive divisors of n. We see that the sets of vertices generated by these divisors will constitute components of $G(n)$. We label these components by $\Gamma_{p_1}, \Gamma_{p_2}, \ldots, \Gamma_{p_r}, \Gamma_{p_1p_2}, \ldots, \Gamma_{p_1p_2\cdots p_r}$. Moreover, the set of all those residues of n which are prime to n will provide us another component. Since this set contains $\phi(n)$ vertices from $V = \{0, 1, 2, \ldots, n-1\}$, so, for the sake of convenience, we label this component by $\Gamma_{\phi(n)}$. Before giving the proof of Theorem 4.1, we prove the following results.

Lemma 4.2. (a) *Let $n = p^k, k > 0$, where p is a prime number. Then $G(n)$ has 2 components, namely, $\Gamma_{\phi(n)}$ and Γ_p.*

(b) *Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ and $k = \Pi_{i=1}^{s}p_i$, $1 \leq s \leq r$. Then the order of the component Γ_k is*

$$|V(\Gamma_k)| = \left\lfloor \frac{n}{k} \right\rfloor - \sum_{s<j\leq r}\left\lfloor \frac{n}{kp_j} \right\rfloor + \sum_{s<j<k\leq r}\left\lfloor \frac{n}{kp_jp_k} \right\rfloor + \cdots + (-1)^{r-s}\left\lfloor \frac{n}{kp_{s+1}p_{s+2}\cdots p_r} \right\rfloor. \tag{4.1}$$

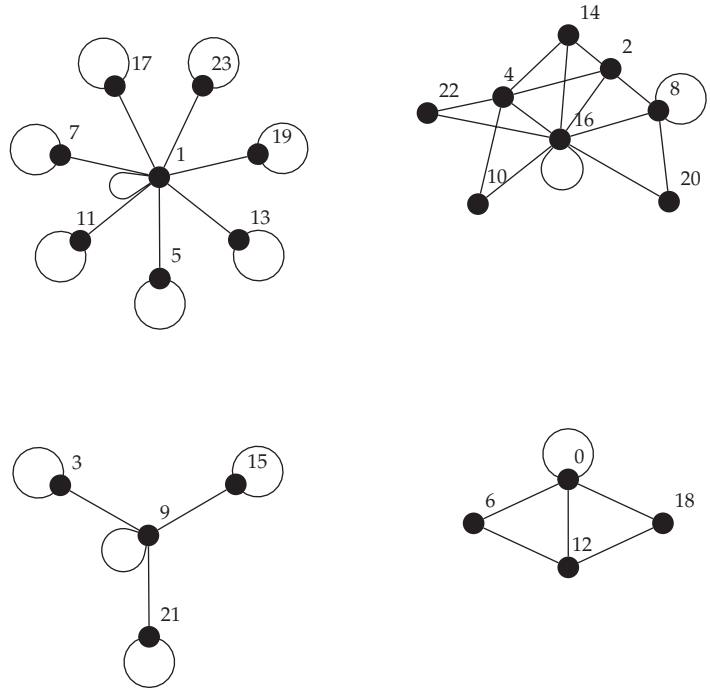

Figure 2: The graph $G(24)$ has 15 nontrivial self-loops.

Proof. (a) Recall that an integer a such that $(a, p^k) = 1$ is called a primitive root modulo p^k only if a is of order $p^{k-1}(p-1)$. Let r be a primitive root of p^k. Then the smallest integer k is called the index of a with respect to r if $r^k \equiv a \pmod{p^k}$. Moreover, it is well known that the exponential congruence $a^x \equiv b \pmod{p^k}$ is solvable if and only if $d \mid \text{ind}_r b$, where $d = (\text{ind}_r a, p^{k-1}(p-1))$. We divide the numbers $0, 1, 2, \ldots, (p-1)p^k$ into two sets, one of which is $\{0, p, 2p, \ldots, (p-1)p^{k-1}\}$ and the other is RRS modulo p^k. We claim that these two sets constitute independent components of $G(p^k)$. Let $V = \{r_1, r_2, \ldots, r_{\phi(p^k)}\}$ where each $r_i, 1 \le i \le \phi(p^k)$ is prime to p^k, the set of vertices of the component $\Gamma_{\phi(p^k)}$. Then every vertex of $\Gamma_{\phi(p^k)}$ must have some index with respect to primitive root r. Thus the exponential congruence $a^x \equiv 1 \pmod{p^k}$ is solvable since $\text{ind}_r 1 = 0$ and is divisible by d, where, $d = (\text{ind}_r a, p^{k-1}(p-1))$. This means that each vertex of the set $\Gamma_{\phi(p^k)}$ is adjacent with 1. So it must contribute as one component of the graph $G(p^k)$. Moreover, for any integer $m \ge 0$, $p^k \mid (mp)^k$ and hence $(mp)^x \equiv 0 \pmod{p^k}$ is solvable with $x = k$ as its root. Thus each vertices of the set $\{0, p, 2p, \ldots, (p-1)p^{k-1}\}$ is adjacent with 0. Then $V(\Gamma_p) = \{0, p, 2p, \ldots, (p-1)p^{k-1}\}$ will form another component of the graph $G(p^k)$. Next we claim that none of the vertex $\Gamma_{\phi(p^k)}$ is adjacent with any of the vertex Γ_p. To prove our assertion, let u and v be two vertices of $G(p^k)$ such that $u \in \Gamma_{\phi(p^k)}$ and $v \in \Gamma_p$. Then there exist integers r and s such that

$$u^r \equiv 1 \left(\text{mod } p^k\right), \qquad v^s \equiv 0 \left(\text{mod } p^k\right). \tag{4.2}$$

Let $t = \operatorname{lcm}(r, s)$, then there exist integers r_1 and s_1 such that $t = rr_1 = ss_1$. Hence by (4.2), we get

$$u^t \equiv 1 \pmod{p^k}, \qquad v^t \equiv 0 \pmod{p^k}. \tag{4.3}$$

Now, if u and v are adjacent, then there must be some integer α such that $u^\alpha \equiv v \pmod{p^k}$. Then by (4.3), we obtain, $0 \equiv 1 \pmod{p^k}$ which is absurd. This is through the claim. Hence $\Gamma_{\phi(n)}$ and Γ_p are the only components of $G(p^k)$. The part (b) is the direct consequence of Theorem 2.6. □

Corollary 4.3. *For $k = 1$, $V(\Gamma_p) = \{0\}$.*

Two graphs or two components of a graph are said to be isomorphic to each other if there is an isomorphism between their vertex sets. Thus, if $G(n)$ and $G(m)$ are isomorphic, then $|V(G(n))| = |V(G(m))|$. Moreover if the vertices u and v are adjacent in $G(n)$, then $f(u)$ and $f(v)$ must be adjacent in $G(m)$, where f is an isomorphism between their sets of vertices. The following corollary can easily be proved by using Lemma 4.2 and Corollary 3.7.

Corollary 4.4. *If $n = 2p_1p_2\cdots p_r$ and l, m are prime divisors of n, then Γ_l and Γ_m, are nonisomorphic components of $G(n)$.*

Proof. Since both l and m are prime numbers, so by Lemma 4.2 (b), the order of components Γ_l and Γ_m must be different. Hence both can never be isomorphic. For instance, take $n = 30$, $l = 3$, and $m = 5$. Then by Lemma 4.2 (b),

$$\begin{aligned} |V(\Gamma_3)| &= \left\lfloor \frac{30}{3} \right\rfloor - \left(\left\lfloor \frac{30}{3.2} \right\rfloor + \left\lfloor \frac{30}{3.5} \right\rfloor \right) + \left\lfloor \frac{30}{3.2.5} \right\rfloor = 4, \\ |V(\Gamma_5)| &= \left\lfloor \frac{30}{5} \right\rfloor - \left(\left\lfloor \frac{30}{5.2} \right\rfloor + \left\lfloor \frac{30}{5.3} \right\rfloor \right) + \left\lfloor \frac{30}{5.2.3} \right\rfloor = 2. \end{aligned} \tag{4.4}$$

Hence by (4.4), the components Γ_3 and Γ_5 are not isomorphic in $G(30)$. However, $|V(\Gamma_3)| = |V(\Gamma_6)| = 4$. Thus the isomorphism can be established between the components Γ_3 and Γ_6 in $G(30)$ if they possess the same structure as well. This leads to the following corollary. □

Corollary 4.5. *Let $n = 2p_1p_2\cdots p_r$ and $d \mid n$. If Γ_d and Γ_{2d} are the components of $G(n)$, then $\Gamma_d \cong \Gamma_{2d}$.*

Proof of Main Theorem. (a) It is well known that $a^x \equiv b \pmod{p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}}$ is solvable if and only if the congruence $a^x \equiv b \pmod{p_i^{k_i}}$ is solvable for each $i = 1, 2, \ldots, r$. Then the proof is analogous to Theorem 2.5 together with Lemma 4.2.

(b) It is easy to see that each element of $V(\Gamma_p) = \{0, p, \ldots, (p-1)p\}$ in $G(p^2)$ is connected with 0 since for each $\alpha \geq 2$, $(tp)^\alpha \equiv 0 \pmod{p^2}$, $1 \leq t \leq p-1$ is satisfied. This shows that the congruence $a^x \equiv 0 \pmod{p^2}$ is solvable for each $a \in V(\Gamma_p)$ in $G(p^2)$. To show that Γ_p in $G(p^2)$ is a tree, we claim that the nonzero vertices in $V(\Gamma_p)$ are not connected to each other. To prove our assertion, let $(t_1p)^\alpha \equiv t_2p \pmod{p^2}$ for $\alpha \geq 2$ and $1 \leq t_1 < t_2 \leq p-1$. Then by Cancelation Law of congruences, we obtain, $t_1^\alpha p^{\alpha-1} \equiv t_2 \pmod{p}$. As $p \mid t_1^\alpha p^{\alpha-1} - t_2$ and $p \mid t_1^\alpha p^{\alpha-1}$, so by

the simple divisibility rules, $p \mid t_2$. But $t_2 \leq p-1 < p$, thus we arrive at a contradiction. This through our claim and finally the component Γ_p in $G(p^2)$ is a tree with root at zero.

(c) It is wellknown that F_n, $n > 4$ is always composite. Thus the only Fermat's primes are 3, 5, 17, 257, and 65537. Let us write $n = 2^k + 1$, $k = 1, 2, 4, 8, 16$. Then $\phi(n) = 2^k$, $k = 1, 2, 4, 8, 16$ since n is prime. To show that the component $\Gamma_{\phi(n)}$ is complete, we need to show that the congruence $a^x \equiv b \pmod{n}$ is solvable for each $a, b \in \{1, 2, \ldots, n-1\}$. By [9], every odd prime p has a primitive root. Since Fermat's numbers are always odd, so each of the Fermat's prime has a primitive root. Let it be r. Then the congruence $a^x \equiv b \pmod{n}$ is solvable if and only if the congruence $x \operatorname{ind}_r a \equiv \operatorname{ind}_r b \pmod{2^k}$ is solvable, where $k = 1, 2, 4, 8, 16$. As $\operatorname{ind}_r a, \operatorname{ind}_r b \in \{1, 2, \ldots, n-1\}$, so the later congruence reduced to the linear congruence $\alpha x \equiv \beta \pmod{2^k}$, where $\alpha = \operatorname{ind}_r a$ and $\beta = \operatorname{ind}_r b$. Then the simple graph $G(n)$ will be complete if the congruence $\alpha x \equiv \beta \pmod{2^k}$, or the congruence $\beta x \equiv \alpha \pmod{2^k}$, is solvable. To prove our assertion, it is easy to see that either $(\alpha, 2^k) = 1 = (\beta, 2^k)$ or $(\alpha, 2^k) = 2^t = (\beta, 2^k)$, where $1 \leq t \leq 2^k$. For the first case, the congruence $\alpha x \equiv \beta \pmod{2^k}$, is solvable and has a unique solution. To discuss the rest of the case, we let $(\alpha, 2^k) = 2^{t_1}$ and $(\beta, 2^k) = 2^{t_2}$, $1 \leq t_1, t_2 \leq 2^k$. If $t_1 \leq t_2$, then $(\alpha, 2^k) \mid (\beta, 2^k)$, so the linear congruence $\alpha x \equiv \beta \pmod{2^k}$ is solvable and has 2^{t_1} solutions. But if $t_2 < t_1$, we replace α and β and solve the congruence $\beta x \equiv \alpha \pmod{2^k}$, which is solvable and has 2^{t_2} solutions. Thus in either case, we see that there is an edge (α, β), $\alpha, \beta \in \{1, 2, \ldots, n-1\}$ in component $\Gamma_{\phi(n)}$ of the simple graph $G(n)$ when n is a Fermat's prime. □

The following corollaries are the direct consequences of Theorem 4.1.

Corollary 4.6. *Let $n = t^2$, where t is square free integer. Then Γ_t is a tree with root at zero.*

Corollary 4.7. *If n is Fermat prime, then $\Gamma_{\phi(n)}$ is regular of degree $\phi(n) - 1$.*

5. Conclusions

This piece of work describes the relationship of exponential congruences with graphs. It has been explored that an exponential congruence yields a set of graphs. Also certain components of the graphs form trees if self-loops are suppressed. The types of graphs and trees were hence yielded form a pattern based on the nature of variables within the congruence. The major results formed show that the component $\Gamma_{\phi(n)}$ of the simple graph $G(n)$ is complete if n is Fermat's prime and also that the component Γ_{t^2}, where t is a square free integer, is always a tree. Intuitively, the results formed find their place in various applications of number theory, encryption, and algorithms. In various problems of data decryption using brute force method it is desirable to find the nature of a number and establish if it is divisible by some other prime number or not. Such problems can be tackled by forming a graph of its exponential congruence and determine the pattern formed by its components. Moreover these exponential congruences can be established as a succinct representation of graphs of a specific nature for their applications in various computer algorithms.

Acknowledgment

The authors are very thankful to the referees for their valuable comments and advices. This has made the paper more interesting and informative.

References

[1] J. Skowronek-Kaziów, "Some digraphs arising from number theory and remarks on the zero-divisor graph of the ring Z_n," *Information Processing Letters*, vol. 108, no. 3, pp. 165–169, 2008.
[2] B. Wilson, "Power digraphs modulo n," *The Fibonacci Quarterly*, vol. 36, no. 3, pp. 229–239, 1998.
[3] L. Somer and M. Křížek, "On a connection of number theory with graph theory," *Czechoslovak Mathematical Journal*, vol. 54, no. 2, pp. 465–485, 2004.
[4] G. Deng and P. Yuan, "Symmetric digraphs from powers modulo n," *Open Journal of Discrete Mathematics*, vol. 1, no. 3, pp. 103–107, 2011.
[5] G. Deng and P. Yuan, "On the symmetric digraphs from powers modulo n," *Discrete Mathematics*, vol. 312, no. 4, pp. 720–728, 2012.
[6] G. Chartrand and L. Lesniak, *Graphs and Digraphs,*, Chapman & Hall, London, UK, 3rd edition, 1996.
[7] A. Adler and J. E. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers, Boston, Mass, USA, 1995.
[8] K. H. Rosen, *Discrete Mathematics and its Application*, WCB/McGraw-HillPress, New York, NY, USA, 1999.
[9] T. Koshy, *Elementry Numbers Theory with Applications*, Academic Press, Elsevier Inc., New York, NY, USA, 2007.