Commun. Korean Math. Soc. **38** (2023), No. 3, pp. 937–941
https://doi.org/10.4134/CKMS.c220215
pISSN: 1225-1763 / eISSN: 2234-3024

SQUARE CONGRUENCE GRAPHS

Janardhanan Suresh Kumar and Sarika M. Nair

Abstract. For each positive integer n, a square congruence graph $S(n)$ is the graph with vertex set $H = \{1, 2, 3, \ldots, n\}$ and two vertices a, b are adjacent if they are distinct and $a^2 \equiv b^2 \pmod{n}$. In this paper we investigate some structural properties of square congruence graph and we obtain the relationship between clique number, chromatic number and maximum degree of square congruence graph. Also we study square congruence graph with p vertices or $2p$ vertices for any prime number p.

1. Introduction

The concept of congruence is fundamental to number theory. Somer and Krizek [5] defined for each positive integer n a digraph whose vertex set $H = \{0, 1, 2, \ldots, n-1\}$ and for which there is a directed edge from $a \in b$ to $b \in H$ if $a^2 \equiv b \pmod{n}$. They established the necessary and sufficient conditions for the existence of isolated fixed points and conditions for semiregularity in [5]. These digraphs were studied in detail [6, 8]. The directed graphs attached with the congruence $a^3 \equiv b \pmod{n}$, $a^5 \equiv b \pmod{n}$ were studied in the paper [4] and [3]. In [4] Skowronek specifies two subdigraph induced by the vertices directed graph arising from congruence $a^3 \equiv b \pmod{n}$. In [3] Rahmati determined the number of fixed points and structure of digraphs for $n = 2^k$ and $n = 5^k$ for a natural number k. He also presented a simple condition for the existence of a cycle. Szalay [7] examined the features of iteration digraph representing a dynamic system in number theory. In [2], Asim and Khalid investigated a new class of graphs that arrived from exponential congruences. In this paper, we define a new class of graphs called square congruence graph and investigate its properties. For number theoretic concepts we refer [1].

2. Main results

Definition 2.1. For each positive integer n, a square congruence graph $S(n)$ is the graph with vertex set $H = \{1, 2, 3, \ldots, n\}$ and two vertices a, b are adjacent if they are distinct and $a^2 \equiv b^2 \pmod{n}$.

Received July 18, 2022; Revised August 23, 2022; Accepted September 16, 2022.
2020 *Mathematics Subject Classification.* Primary 11A07, 05C.
Key words and phrases. Congruence, graph congruence, square congruence graph.

Theorem 2.1. *A square congruence graph $S(n)$ has at least one isolated vertex if and only if n is a square-free number.*

Proof. Let $S(n)$ be a square congruence graph with vertex set $\{1, 2, 3, \ldots, n, \}$. We begin the proof by showing all vertices in $S(n)$ other than n, $n/2$ are non isolated.

Choose $k : 1 \leq k \leq \frac{n-2}{2}$ for n is even and $1 \leq k \leq \frac{n-1}{2}$ for n is odd. Then $(n-k)^2 - k^2 = n^2 - 2nk = n(n-2k)$. Hence, $(n-k)^2 \equiv k^2 \pmod{n}$.

Therefore, $(n-k)$ is adjacent to k. To prove there exists at least one isolated vertex, assume the converse of n is a square-free number. Let p be a prime number such that p^2 divides n. Then $(n/p)^2 = n\left(n/p^2\right) = mn \equiv n^2 \pmod{n}$.

Hence n/p is adjacent to n and n is not an isolated vertex.

In the above case when $p = 2$, we get n and $n/2$ are adjacent. Which means $S(n)$ has no isolated vertices. That is, if $S(n)$ has at least one isolated vertex, then n is a square-free number.

Next we have to show that if n is a square-free number, then $S(n)$ has at least one isolated vertex.

Let n be a square-free number. Then $n = p_1 p_2 \cdots p_n$.

If n is not an isolated vertex, there exists a vertex v_i such that

$$(p_1 p_2 \cdots p_n)^2 \equiv v_i^2 \pmod{p_1 p_2 \cdots p_n}.$$

That is, $p_1^2 p_2^2 \cdots p_n^2 - v_i^2 = k(p_1, p_2 \cdots p_n)$ for some integer k. Hence

$$p_1 p_2 \cdots p_n \left(p_1 p_2 \cdots p_n - k\right) = v_i^2.$$

LHS is not a perfect square. Therefore $S(n)$ has at lest one isolated vertex. $\square$

Corollary 2.1. *For a square-free number n, the vertex n is an isolated vertex of $S(n)$.*

Theorem 2.2. *For a square congruence graph $S(n)$, clique number $\omega(S(n))$ is $1 + \Delta(S(n))$.*

Proof. For a graph G, $\omega(G) \leq \chi(G)$ and $\chi(G) \leq 1 + \Delta(G)$. From these two facts we get $\omega(S(n)) \leq 1 + \Delta(S(n))$.

Next we show that $1 + \Delta(S(n)) \leq \omega(S(n))$.

Let $S(n)$ be a square congruence graph with $\Delta(S(n)) = k$ and v_k be a vertex such $\deg(v_k) = k$. That is, v_k is adjacent with k vertices say $v_0, v_1, v_2, \ldots, v_{k-1}$.

That is

$$v_k^2 \equiv v_0^2 \pmod{n}, \tag{1}$$

$$v_k^2 \equiv v_1^2 \pmod{n}, \tag{2}$$

$$v_k^2 \equiv v_2^2 \pmod{n}, \tag{3}$$

$$\vdots$$

$$v_k^2 \equiv v_{k-1}^2 \pmod{n}.$$

Applying symmetric and transitive properties of congruence in equations (1) and (2) gives v_0 is adjacent to v_1. Similarly we get all vertices $v_2, v_3, \ldots, v_{k-1}$ are adjacent to v_0.

Apply this same procedure in equations (2) and (3) we get v_1 is adjacent to v_2, and all other vertices $v_3, v_4, \ldots, v_{k-1}$ are adjacent to v_1. Finally we get a complete graph of order $k+1$ with vertex set $v_0, v_1, \ldots, v_{k-1}, v_k$. If there exists another complete graph K_m with order of K_m is greater than $k+1$, then degree of vertices of K_m is greater than k, which is a contradiction to our assumption $\Delta(S(n)) = k$. Hence $\omega(S(n)) = k+1$. $\square$

Corollary 2.2. *For a square congruent graph $S(n)$, $\chi(S(n)) = 1 + \Delta(S(n))$.*

Proof. For a graph G, $\omega(G) \leq \chi(G) \leq 1+\Delta(G)$. Then for a square congruence graph $S(n)$, $\omega(S(n)) \leq \chi(S(n)) \leq 1 + \Delta(S(n))$. By Theorem 2.2, we have $\omega(S(n)) = 1 + \Delta(S(n))$. Hence $\chi(S(n)) = 1 + \Delta(S(n))$. $\square$

Theorem 2.3. *Let p be a prime number and G be a graph with n vertices. Then size of the graph*

$$S(n) = \begin{cases} \frac{n-1}{2} & \text{if } n = p, \\ \frac{n-2}{2} & \text{if } n = 2p. \end{cases}$$

Proof. Suppose a and b are two adjacent vertices in $S(n)$. Then $a^2 \equiv b^2 \pmod{p}$. That is $a^2 - b^2 = mp$, where m is any positive integer. Which means $(a+b)(a-b) = mp$. Since p is a prime number, either $a+b$ or $a-b$ is a multiple of p. Here maximum value of $a+b$ is $p+p-1 = 2p-1$, which is not a multiple of p. Therefore maximum value of $a+b$ which is a multiple of p is p. For in the case of $a-b$, the maximum value is $p-1$. Hence $a-b$ cannot be a multiple of p. Therefore in the product $(a-b)(a+b)$, $a+b$ should be a multiple of p. Which happens only if $a = p-k$ and $b = k$ for $1 \leq k \leq \frac{n-1}{2}$. Hence $p-k$ is adjacent with exactly one vertex say k for $1 \leq k \leq \frac{n-1}{2}$. Therefore there exist $\frac{n-1}{2}K_2$'s. Since p is a square-free number, by Corollary 2.1 the remaining vertex n is the only isolated vertex. $\square$

Theorem 2.4. *For $n = 2p$, the components of square congruence graph $S(n)$ are the isolated vertices n, $\frac{n}{2}$ and $\frac{n-2}{2}K_2$'s.*

Proof. If a and b are two adjacent vertices in $S(n)$, then $a^2 \equiv b^2 \pmod{2p}$. That is $a^2 - b^2 = m2p$, where m is any positive integer. Which means $(a+b)(a-b) = m2p$. Since p is a prime number, either $a+b$ or $a-b$ is a multiple of p. Here maximum value of $a+b$ is $2p+2p-1 = 4p-1$, which is not a multiple of p. Then possible chances of $a+b$ that are multiples of p are $p, 2p, 3p$.

Case 1: $a+b = p$, which happens when $a = p-k$ and $b = k$ for a positive integer $k \leq p$. Then $a-b = p-2k$ is an odd number and not a multiple of $2m$. Hence this case is not possible.

Case 2: $a + b = 2p$, which happens when $a = 2p - k$ and $b = k$. That is $a = n - k$ and $b = k$. From the proof of Theorem 2.1 it is clear that $n - k$ is adjacent with k for $1 \leq k \leq \frac{n-2}{2}$.

Case 3: $a + b = 3p$ which happens when $a = 2p - k$ and $b = p + k$ for $0 \leq k \leq \frac{p-1}{2}$. Then $a - b = 2p - k - (p + k) = p - 2k$, which is an odd number, not a multiple of $2m$.

For the case of $a - b$, the maximum value of $a - b$ is $2p - 1$. Then possible chance of $a - b$, which is a multiple of p is p. Which happens only if $a = 2p - k$ and $b = p - k$ for $0 \leq k \leq p - 1$. In this case $a + b = 2p - k + p - k = 3p - 2k$. Which is an odd number. Hence this case is not possible. Therefore $2p - k$ is only adjacent with k for $0 \leq k \leq \frac{2p-2}{2}$. Therefore there exist $\frac{n-2}{2} K_2$'s. The remaining vertices are $n, \frac{n}{2}$. Since $2p$ is a square-free number, by Corollary 2.1 n is an isolated vertex.

If $\frac{n}{2}$ is not an isolated vertex, then $(\frac{n}{2})^2 = (\frac{2p}{2})^2 \equiv v^2 \pmod{2p}$. That is, $p^2 \equiv v^2 \pmod{2p}$. Then either $p + v$ or $p - v$ is a multiple of $2p$. Which happens when $v = p$ or $v = 2p$. When $v = p$, $p - v = 0$ and when $v = 2p$, $(p+2p)(p-2p) = -3p^2$, not a multiple of $2p$. Hence $\frac{n}{2}$ is an isolated vertex. $\square$

Theorem 2.5. *For a prime number p, every vertices in the square congruence graph $S(p^n)$ are non-isolated.*

Proof. From the proof of Theorem 2.1 all vertices in $S(p^n)$ other than n, $\frac{n}{2}$ are non isolated. Hence we need to prove only the cases p^n and $\frac{p^n}{2}$. p^n is odd for $p \neq 2$. In the case of $p = 2$, $\frac{n}{2}$ is same as p^{n-1}.

Consider two vertices p^n and p^{n-1}. Then

$$(p^n)^2 - (p^{n-1})^2 = p^{2n} - p^{2n-2} = p^{2n-2}(p^2 - 1).$$

Hence $(p^n)^2 \equiv (p^{n-1})^2 \pmod{p^n}$.

That is, for any prime number p, the vertex p^n is adjacent with p^{n-1}. $\square$

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 2012.

[2] M. A. Malik and M. K. Mahmood, *On simple graphs arising from exponential congruences*, J. Appl. Math. **2012** (2012), Art. ID 292895, 10 pp. https://doi.org/10.1155/2012/292895

[3] M. Rahmati, *Some digraphs attached with the congruence* $x^5 \equiv y \pmod{n}$, J. Math. Ext. **11** (2017), no. 1, 47–56.

[4] J. Skowronek-Kaziów, *Some digraphs arising from number theory and remarks on the zero-divisor graph of the ring* Z_n, Inform. Process. Lett. **108** (2008), no. 3, 165–169. https://doi.org/10.1016/j.ipl.2008.05.002

[5] L. Somer and M. Křížek, *On a connection of number theory with graph theory*, Czechoslovak Math. J. **54(129)** (2004), no. 2, 465–485. https://doi.org/10.1023/B:CMAJ.0000042385.93571.58

[6] L. Somer and M. Křížek, *Structure of digraphs associated with quadratic congruences with composite moduli*, Discrete Math. **306** (2006), no. 18, 2174–2185. https://doi.org/10.1016/j.disc.2005.12.026

[7] L. Szalay, *A discrete iteration in number theory*, BDTF Tud. Kozl. **8** (1992), 71–91.
[8] B. Wilson, *Power digraphs modulo n*, Fibonacci Quart. **36** (1998), no. 3, 229–239.

Janardhanan Suresh Kumar
PG and Research Department of Mathematics
NSS Hindu College, Changanacherry, Kottayam Dist
Kerala 686102, India
Email address: jsuresh.maths@gmail.com

Sarika M. Nair
PG and Research Department of Mathematics
NSS Hindu College, Changanacherry, Kottayam Dist
Kerala 686102, India
Email address: sarikamnair95@gmail.com