Applicable Analysis and Discrete Mathematics
available online at http://pefmath.etf.rs

Appl. Anal. Discrete Math. **16** (2022), 288–306.
https://doi.org/10.2298/AADM180713023B

CHARACTERIZATION OF STRONGLY REGULAR INTEGRAL CIRCULANT GRAPHS BY SPECTRAL APPROACH

Milan Bašić

The integral circulant graph $\mathrm{ICG}_n(D)$ has the vertex set $Z_n = \{0, 1, 2, \ldots, n-1\}$ and vertices a and b are adjacent if $\gcd(a-b, n) \in D$, where $D \subseteq D_n$, $D_n = \{d : d \mid n,\ 1 \leq d < n\}$. Motivated by the incorrect proof of a previously published result, in this paper we characterize the class of integral circulant graphs that are strongly regular. More precisely, connected $\mathrm{ICG}_n(D)$ is strongly regular if and only if n is composite and $D = \{d \in D_n \mid m \nmid d\}$ for some $m \mid n$ and $n - 1 \geq m \geq 2$.

1. INTRODUCTION

Circulant graphs are Cayley graphs over a cyclic group. A graph is called integral if all the eigenvalues of its adjacency matrix are integers. In other words, the corresponding adjacency matrix of a circulant graph is the circulant matrix (a special kind of Toeplitz matrix where each row vector is rotated one element to the right relative to the preceding row vector). Integral graphs are extensively studied in the literature and there has been a vast research on some types of classes of graphs with integral spectrum. The interest for circulant graphs in graph theory and applications has grown during the last two decades. They appear in coding theory, VLSI design, Ramsey theory and other areas. Since they possess many interesting properties (such as vertex transitivity called mirror symmetry), circulants are applied in quantum information transmission and proposed as models for quantum spin networks that permit the quantum phenomenon called perfect state transfer [**1, 13**]. In the quantum communication scenario, the important feature of

2020 Mathematics Subject Classification. 05C50, 05E30.
Keywords and Phrases. Circulant graphs, Integral graphs, Strongly regular graphs.

this kind of quantum graphs (especially those with integral spectrum) is the ability of faithfully transferring quantum states without modifying the network topology.

Strongly regular graphs are regular graphs that have the property that the number of common neighbors of two distinct vertices depends only on whether they are adjacent or nonadjacent. There has been a vast research on distance regular graphs and recently on strongly regular graphs (primitive distance regular graphs with diameter two) and numerous examples of strongly regular graphs along with their applications can be found in [**6**]. In particular a special emphasis has been put on strongly regular Cayley graphs. Such graphs are equivalent to regular partial difference sets (subset of a finite group with certain properties), and many results on strongly regular Cayley graphs are formulated in the language of partial difference sets (see [**10**] for a survey of this topic). Strong regularity of circulants has been investigated by several authors and a characterization of strongly regular circulants was obtained by Ma [**9**] and Miklavič et al. [**12**]. The techniques that are used mostly come from group theory (therefore are not close to graph theoreticians) and the obtained classification results in these papers can stand alone as pure abstract algebraic facts.

On the other hand, motivated by the incorrect proof of the published result given by Theorem 4.2 in [**3**] in which the authors try to characterize the class of integral circulant graphs that are strongly regular, in this paper we prove the result only by using tools and techniques from combinatorial and spectral graph theory. The only attempt at a proof using spectral graph theory can be seen in [**3**] and also in [**11**] where only a partial solution is given for the circulants with prime power order. Not only that we managed to find the full characterization of strongly regular integral circulant graphs, but we go a step forward by finding numerous spectral properties of integral circulant graphs which we believe will be useful in further studying of integral circulant graphs and their applications in quantum information theory.

We will now explain how the proof of Theorem 4.2 given in [**3**] fails to be correct. The key idea of the proof is showing that the second largest value λ_2 of the circulant graph G is equal to zero using the method of contradiction. In the paragraph in which the authors assume that λ_2 is greater than zero, they obtain that G is not a complete d-partite graph, whence it is further concluded that G is not circulant (according to Theorem 3.4), which is a contradiction. However, Theorem 3.4 says that a graph G is a complete d-partite graph if and only if it is circulant graph with certain set of symbols S. Thus, from the fact that G is not a complete d-partite graph, we can only conclude that it is not a circulant graph of a special kind. Therefore, in the general case it can be circulant and it is clear that the authors do not get a contradiction and can not proceed as they do to finish the proof. Moreover, the fact that the authors did not use any of the properties neither of integral nor circulant graphs, speaks for itself that the result can not be proved in the proposed fashion.

In this paper we proceed with the study of (integral) circulant graphs initiated

in many recent papers. Moreover, studying the property of strong regularity on integral circulant graphs can also be interpreted as a contribution to the spectral theory of circulant or integral graphs. For example, by analyzing the existence of perfect state transfer in quantum circulant graphs [**1**], different properties of the Ramanujan functions and eigenvalues of integral circulant graphs (as the sums of the Ramanujan functions) are observed and these results can stand alone in the literature concerning the spectral theory of circulant graph.

After a preliminary section where we introduce the appropriate notation and notions concerning integral circulant and strongly regular graphs, in Section 3 we go step further in describing some new properties of the Ramanujan functions (given in Lemmas 5 and 6) which are essential in proving Theorem 8 where we give a general characterization of the class of integral circulant graphs that have all even elements with odd indices of the spectrum that is arranged in a certain order (mentioned in Section 2). This fact helps us find all strongly regular integral circulant graphs for which both of the two smallest eigenvalues are either even or odd (Theorem 9 and Theorem 10). Furthermore, after proving the assertions given by Theorem 11 and Theorem 13 which examine the properties of the eigenvalues of integral circulant graphs, in Theorem 14 we give a general characterization of the class of integral circulant graphs with two smallest eigenvalues of different parity. The proof requires an extensive discussion and falls into a good many of distinct cases. In Theorem 15 we characterize all strongly regular integral circulant graphs. We conclude that section with the fact that every strongly regular integral circulant graph must be imprimitive, which actually follows up the result from Proposition 2.2 in [**11**] where some necessary and sufficient conditions are given for the existence of primitive strongly regular integral circulant graphs.

2. PRELIMINARIES

A *circulant graph* $G(n;S)$ is a graph on vertices $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$ such that vertices i and j are adjacent if and only if $i-j \equiv s \pmod n$ for some $s \in S$. Such a set S is called the *symbol* of the graph $G(n;S)$. As we will consider undirected graphs without loops, we assume that $S = n - S = \{n-s \mid s \in S\}$ and $0 \notin S$. Note that the degree of the graph $G(n;S)$ is $|S|$. The eigenvalues and eigenvectors of $G(n;S)$ are given by

$$\lambda_j = \sum_{s\in S} \omega_n^{js}, \quad v_j = [1\ \omega_n^j\ \omega_n^{2j} \cdots \omega_n^{(n-1)j}]^T,$$

where $\omega_n = e^{i\frac{2\pi}{n}}$ is the n-th root of unity [**5**].

Circulant graphs are a subclass of the wider class of Cayley graphs. Let Γ be a multiplicative group with identity e. For $S \subset \Gamma$, $e \notin S$ and $S^{-1} = \{s^{-1} \mid s \in S\} = S$, the Cayley graph $X = Cay(\Gamma, S)$ is the undirected graph having vertex set $V(X) = \Gamma$ and edge set $E(X) = \{\{a,b\} \mid ab^{-1} \in S\}$. It is not hard to see that a graph is circulant if it is a Cayley graph on some cyclic group, i.e. its adjacency matrix is cyclic.

A graph is *integral* if all its eigenvalues are integers. A circulant graph $G(n;S)$ is integral if and only if

$$S = \bigcup_{d\in D} G_n(d),$$

for some set of divisors $D \subseteq D_n$ [**14**]. Here $G_n(d) = \{k \ : \ \gcd(k,n) = d,\ 1 \le k \le n-1\}$, and D_n is the set of all divisors of n, different from n.

Therefore an *integral circulant graph* (in further text ICG) $G(n;S)$ is defined by its order n and the set of divisors D. An integral circulant graph with n vertices, defined by the set of divisors $D \subseteq D_n$ will be denoted by $\mathrm{ICG}_n(D)$. From the above characterization of integral circulant graphs we have that the degree of an integral circulant graph is $\deg \mathrm{ICG}_n(D) = \sum_{d\in D} \varphi(n/d)$. Here $\varphi(n)$ denotes the Euler-phi function [**7**]. If $D = \{d_1, \ldots, d_k\}$, it can be seen that $\mathrm{ICG}_n(D)$ is connected if and only if $\gcd(d_1, \ldots, d_k) = 1$, given that $G(n;S)$ is connected if and only if $\gcd(n,S) = 1$ [**8**].

Denote by $c(j,n)$ the following expression

$$c(j,n) = \mu(t_{n,j})\frac{\varphi(n)}{\varphi(t_{n,j})}, \quad t_{n,j} = \frac{n}{\gcd(n,j)}, \tag{1}$$

where n and j are non negative integers such that $n \ge 2$, and μ is the Möbius function defined as follows

$$\mu(n) \quad = \quad \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n \text{ is not square–free} \\ (-1)^k, & \text{if } n \text{ is product of } k \text{ distinct prime numbers.} \end{cases}$$

The expression $c(j,n)$ is known as the *Ramanujan function* ([**7**, p. 309]). The spectrum $(\lambda_0, \ldots, \lambda_{n-1})$ of $\mathrm{ICG}_n(D)$ can be expressed in terms of the Ramanujan function (see [**14**]) as follows

$$\lambda_j = \sum_{d\in D} c(j, n/d), \tag{2}$$

where $0 \le j \le n-1$.

Let us observe that the Ramanujan function has the following basic but very useful properties.

Proposition 1. *For any positive integers n, j, d and a prime p such that $d \mid n$ and $p \mid n$, the following are satisfied*

$$\begin{aligned} c(0, n/d) &= \varphi(n/d), \\ c(1, n/d) &= \mu(n/d), \\ c(j, 2) &= \begin{cases} -1, & 2 \not| j \\ 1, & 2 \mid j, \end{cases} \\ c(n/p, n/d) &= \begin{cases} \varphi(n/d), & p \mid d \\ -\frac{\varphi(n/d)}{p-1}, & p \nmid d \end{cases}. \end{aligned} \tag{3}$$

Proof. First two assertions can be proven directly using the relation (1) and as an illustration, we prove the last relation.

Note that for arbitrary divisor d and prime $p \mid n$, it holds

$$\gcd(n/p, n/d) = \begin{cases} \frac{n}{d}, & p \mid d \\ \frac{n}{pd}, & p \nmid d \end{cases}$$

and

$$t_{n/d,n/p} = \begin{cases} 1, & p \mid d \\ p, & p \nmid d \end{cases} .$$

Now using the relation (1) we obtain desired relation. □

First, let us remind that the spectral radius of a connected $r-$regular graph X is equal to the regularity r and it is a simple eigenvalue of X. According to (3), in the case of an integral circulant graph with the spectrum $(\lambda_0, \ldots, \lambda_{n-1})$ given by (2), λ_0 is equal to the regularity of the graph.

A $r-$regular graph of the order n is called *strongly regular* with parameters (n, r, a, c) if it is neither complete, nor empty, every pair of adjacent vertices has a common neighbours, and every pair of nonadjacent vertices has c common neighboring vertices.

The parameters of a strongly regular graph are not independent of each other. In fact, the following relations hold $n-1 > r \geq c \geq 0$ and $r-1 \geq a \geq 0$. Moreover, the following more complex relation can be obtained

$$r(r-a-1) = (n-r-1)c. \tag{4}$$

For more details, see the equation (10.1) in [**6**, p. 219]).

A strongly regular graph X is called *primitive* if each of the graphs X and $\overline{X}$ is connected; otherwise it is *imprimitive*. The following lemma offers a characterization of the class of imprimitive strongly regular graphs.

Lemma 2. *[**6**] Let X be a strongly regular graph with parameters (n, r, a, c). Then the following assertions are equivalent*

(a) X is not connected,

(b) $c = 0$,

(c) $a = r - 1$

(d) X is isomorphic to mK_{r+1}, for $m \geq 2$.

It is straightforward to show that if X is strongly regular with parameters (n, r, a, c), then its complement $\overline{X}$ is also strongly regular with parameters $(n, \overline{r}, \overline{a}, \overline{c})$, where $\overline{r} = n - r - 1$, $\overline{a} = n - 2 - 2r + c$ and $\overline{c} = n - 2r + a$.

Lemma 3. *[**2**] A connected regular graph is strongly regular if and only if it has exactly three distinct eigenvalues.*

For a strongly regular X with parameters (n, r, a, c) by r, θ and τ we will denote the eigenvalues of its adjacency matrix.

Lemma 4. *[**6**] The adjacency matrix of a strongly regular graph with parameters (n, r, a, c) has eigenvalues r, θ and τ, where θ and τ are given by the following formulas*

$$\theta = \frac{a - c + \sqrt{\Delta}}{2}$$
$$\tau = \frac{a - c - \sqrt{\Delta}}{2},$$

where $\Delta = (a - c)^2 + 4(r - c)$.

Notice that from Vieta's formula we have that

$$\theta\tau = c - r. \tag{5}$$

Since $c \leq r$, we have that θ and τ have opposite sings, provided that $\theta\tau \neq 0$.

Since the multiplicity of the eigenvalue r is equal to 1 and the sum of the eigenvalues is equal to the trace of the adjacency matrix (which is equal to zero), the multiplicity can be computed in the following way:

$$\begin{aligned} m_\theta + m_\tau &= n - 1 \\ m_\theta\theta + m_\tau\tau &= -r. \end{aligned} \tag{6}$$

From the above expressions we can obtain the relation (10.2) from [**6**]:

$$m_\theta = -\frac{(n-1)\tau + r}{\theta - \tau} \quad m_\tau = \frac{(n-1)\theta + r}{\theta - \tau}. \tag{7}$$

Using these equations together with (4), we obtain the very useful relation which is actually the statement of Lemma 10.3.1 from [**6**]:

$$m_\theta m_\tau (\theta - \tau)^2 = nr\overline{r}. \tag{8}$$

The relations (7) and (8) will be used in Theorem 14.

3. STRONGLY REGULAR INTEGRAL CIRCULANT GRAPHS

In Lemmas 5 and 6 we present some important properties of the Ramanujan function.

Throughout the section, we let $2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ be the prime factorization of n, and $\alpha_i \geq 1$ for $1 \leq i \leq k$ and $\alpha_0 \geq 0$.

Also, for a given prime number p and an integer $n \in \mathbb{N}$, denote by $S_p(n)$ the maximal number α such that $p^\alpha \mid n$ i.e., $p^\alpha \parallel n$.

In the following lemma we find necessary and sufficient conditions for $c(j,n/d)$ being odd, where $1 \leq j \leq n-1$ is a fixed number with the following prime factorization $j = 2^{\gamma_0} p_{i_1}^{\gamma_{i_1}} \dots p_{i_s}^{\gamma_{i_s}} p_{i_{s+1}}^{\alpha_{i_{s+1}}} \dots p_{i_k}^{\alpha_{i_k}}$, where $0 \leq \gamma_0 \leq \alpha_0$, $0 \leq \gamma_i < \alpha_i$, for $1 \leq i \leq s$ and $(i_1, \dots, i_k)$ is a permutation of the numbers $\{1, \dots, k\}$. We may notice that since $j < n$, then at least one of the following conditions $\gamma_0 < \alpha_0$ or $s \geq 1$ holds. In the following statement of the lemma, without loss of generality we assume that the permutation $(i_1, \dots, i_k)$ is equal to $(1, \dots, k)$ to simplify notation.

Lemma 5. *Let $1 \leq j \leq n-1$ be an arbitrary number with the prime factorization $j = 2^{\gamma_0} p_1^{\gamma_1} \dots p_s^{\gamma_s} p_{s+1}^{\alpha_{s+1}} \dots p_k^{\alpha_k}$, for $0 \leq \gamma_0 \leq \alpha_0$, $0 \leq \gamma_i < \alpha_i$, $1 \leq i \leq s$ and $0 \leq s \leq k$. Then for an arbitrary divisor d of n, the integer $c(j,n/d)$ is odd if and only if $d = 2^{\beta_0} p_1^{\beta_1} \dots p_k^{\beta_k}$, where $\beta_0 \in \{\alpha_0 - 1, \alpha_0\}$, $\beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}$ (for $1 \leq i \leq s$) and $\beta_i = \alpha_i$ (for $s+1 \leq i \leq k$).*

Proof. ($\Rightarrow$:) Suppose that $c(j,n/d)$ is an odd integer. Since $c(j,n/d) = \mu(t_{n/d,j})\varphi(n/d)/\varphi(t_{n/d,j})$, then $c(j,n/d)$ is odd if and only if $\mu(t_{n/d,j}) = \pm 1$, i.e. $t_{n/d,j}$ is square-free and $\varphi(n/d)/\varphi(t_{n/d,j})$ is an odd integer.

Since $t_{n/d,j} = n/(d \gcd(n/d, j))$ we obtain that

$$S_{p_i}(t_{n/d,j}) = S_{p_i}(n/d) - \min\{S_{p_i}(n/d), S_{p_i}(j)\},$$

for $0 \leq i \leq k$, where we put $p_0 = 2$.

If $s+1 \leq i \leq k$, then $S_{p_i}(j) = \alpha_i \geq S_{p_i}(n/d)$ and therefore $S_{p_i}(t_{n/d,j}) = 0$. If $p_i \mid n/d$, then $p_i - 1 \mid \varphi(n/d)/\varphi(t_{n/d,j})$, which is a contradiction since we previously concluded that $\varphi(n/d)/\varphi(t_{n/d,j}) \in 2\mathbb{N}+1$. Thus, we have that $p_i \nmid n/d$ and $S_{p_i}(d) = \alpha_i$, for each $s+1 \leq i \leq k$.

If $0 \leq i \leq s$, then we have

$$S_{p_i}(t_{n/d,j}) = \begin{cases} 0, & S_{p_i}(n/d) \leq \gamma_i \\ S_{p_i}(n/d) - \gamma_i, & S_{p_i}(n/d) > \gamma_i. \end{cases}$$

Moreover, for $0 \leq i \leq s$, since $t_{n/d,j}$ is square-free we have that $0 \leq S_{p_i}(t_{n/d,j}) \leq 1$. For $1 \leq i \leq s$, if $p_i \nmid t_{n/d,j}$ and $p_i \mid n/d$, similarly like in the previous case we conclude that $\varphi(n/d)/\varphi(t_{n/d,j}) \in 2\mathbb{N}$, which is a contradiction. Thus, if $p_i \nmid t_{n/d,j}$, we conclude that $p_i \nmid n/d$ and $S_{p_i}(d) = \alpha_i$. Now, in the remaining case for $p_i \mid t_{n/d,j}$, since $t_{n/d,j}$ is square-free we have $S_{p_i}(t_{n/d,j}) = 1$ and therefore $S_{p_i}(n/d) = \gamma_i + 1$, whence we finally obtain that $S_{p_i}(d) = \alpha_i - \gamma_i - 1$. Notice that in this case $p_i - 1 \nmid \varphi(n/d)/\varphi(t_{n/d,j})$ also holds and thus $\varphi(n/d)/\varphi(t_{n/d,j})$ is always odd in the all above cases (in the opposite case, even $\varphi(n/d)/\varphi(t_{n/d,j})$ would imply even $c(j,n/d)$, which would be a contradiction).

For $i = 0$, we have already observed that $0 \leq S_2(t_{n/d,j}) \leq 1$. If $S_2(n/d) \geq 2$ i.e. $S_2(d) \leq \alpha_0 - 2$, we have that $\varphi(n/d)/\varphi(t_{n/d,j}) \in 2\mathbb{N}$, which is a contradiction. Thus we conclude that $\alpha_0 - 1 \leq \beta_0 \leq \alpha_0$.

($\Leftarrow$:) Suppose that $d = 2^{\beta_0} p_1^{\beta_1} \dots p_k^{\beta_k}$, where $\beta_0 \in \{\alpha_0 - 1, \alpha_0\}$, $\beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}$ (for $1 \leq i \leq s$) and $\beta_i = \alpha_i$ (for $s+1 \leq i \leq k$). Therefore, $n/d = 2^{\delta_0} p_1^{\delta_1} \dots p_k^{\delta_k}$, where $\delta_0 \in \{0,1\}$, $\delta_i \in \{0, \gamma_i + 1\}$ (for $1 \leq i \leq s$) and $\delta_i = 0$ (for $s+1 \leq i \leq k$).

Furthermore, $t_{n/d,j} = 2^{\epsilon_0} p_1^{\epsilon_1} \dots p_s^{\epsilon_s}$, where $\epsilon_i \in \{0,1\}$, $\delta_i = 0 \Leftrightarrow \epsilon_i = 0$, for $1 \leq i \leq k$. Finally, we conclude that $t_{n/d,j}$ is square-free and $\varphi(n/d)/\varphi(t_{n/d,j}) \in 2\mathbb{N}+1$, implying that $c(j, n/d)$ is odd. □

Lemma 6. *Let d be an arbitrary divisor of n such that $n/d \in 2\mathbb{N}+1$ and $0 \leq j \leq n-1$ be an arbitrary integer, then $c(j, n/d) = -c(j, 2n/d)$ for $j \in 2\mathbb{N}+1$ and $c(j, n/d) = c(j, 2n/d)$ for $j \in 2\mathbb{N}$.*

Proof. As $n/d \in 2\mathbb{N}+1$ we conclude that $\varphi(2n/d) = \varphi(n/d)$.

Suppose that $j \in 2\mathbb{N}+1$. Then $\gcd(2n/d, j) = \gcd(n/d, j)$ and

$$t_{2n/d,j} = \frac{2n}{d\gcd(2n/d, j)} = 2\frac{n}{d\gcd(n/d, j)} = 2t_{n/d,j}.$$

Furthermore, it holds that $\varphi(t_{2n/d,j}) = \varphi(t_{n/d,j})$ since $t_{n/d,j}$ is odd. Also we have that $t_{2n/d,j}$ is square-free if and only if $t_{n/d,j}$ is square-free, and therefore $\mu(t_{2n/d,j}) = -\mu(t_{n/d,j})$. Now we can directly conclude that

$$c(j, 2n/d) = \mu(t_{2n/d,j})\frac{\varphi(2n/d)}{\varphi(t_{2n/d,j})} = -\mu(t_{n/d,j})\frac{\varphi(n/d)}{\varphi(t_{n/d,j})} = -c(j, n/d).$$

Now suppose that $j \in 2\mathbb{N}$. Using similar arguments as in the previous discussion, we obtain $\gcd(2n/d, j) = 2\gcd(n/d, j)$ and also $t_{2n/d,j} = t_{n/d,j}$. This directly yields that $c(j, 2n/d) = c(j, n/d)$. □

In the rest of the paper, by $(\lambda_0, \dots, \lambda_{n-1})$ we denote the spectrum of integral circulant graph $\mathrm{ICG}_n(D)$, which is given by the equation (2).

For the sake of clarity and to enhance readability of the following statements, let us introduce the following notation for the subsets of the divisor set D, $D_0 = \{d \in D \mid n/d \in 2\mathbb{N}+1\}$ and $D_1 = \{d \in D \mid n/d \in 4\mathbb{N}+2\}$.

Also, for a positive integer k and a set A of positive integers, by kA we will mean the set $\{ka \mid a \in A\}$.

Lemma 7. *Let $\mathrm{ICG}_n(D)$ be an integral circulant graph such that $D = D_0 \cup D_1$. The following statements are equivalent:*

i) Every λ_j is even for odd $0 \leq j \leq n-1$.

ii) $D_0 = 2D_1$.

iii) Every $\lambda_j = 0$ for odd $0 \leq j \leq n-1$.

Proof.

$(ii) \Rightarrow (iii)$ Suppose that $D_0 = 2D_1$ and $D = D_1 \cup 2D_1$. That is, every $d \in D_0$ if and only if $d/2 \in D_1$. Let $j \in 2\mathbb{N}+1$. According to Lemma 6 we have $c(j, n/d) = -c(j, 2n/d)$ for any $d \in D_0$ and therefore

$$\lambda_j = \sum_{d \in D_1 \cup 2D_1} c(j, \frac{n}{d}) = \sum_{d \in D_0} c(j, \frac{n}{d/2}) + \sum_{d \in D_0} c(j, \frac{n}{d}) = \sum_{d \in D_0} c(j, \frac{n}{d}) - c(j, \frac{n}{d}) = 0.$$

We conclude that all eigenvalues with odd indices are equal to 0.

$(i) \Rightarrow (ii)$ Assume that $D_0 \neq 2D_1$.

Let $D_1'' = \{d \in D_1 \mid 2d \in D_0\}$ and $D'' = D_1'' \cup 2D_1''$.

Let $D' = D \setminus D''$. By the assumption, D' is a non-empty set. According to the first part of the proof it holds that $c(j, n/d) + c(j, 2n/d) = 0$, for odd j and every $d \in 2D_1''$. Let $d'_{max} = \max D'$. Since d'_{max} is a divisor of n, it can be represented in the form $d'_{max} = 2^{\beta_0} p_1^{\beta_1} \cdots p_k^{\beta_k}$, where $\alpha_0 - 1 \leq \beta_0 \leq \alpha_0$ and $0 \leq \beta_i \leq \alpha_i$ for $1 \leq i \leq k$. Without loss of generality, we can suppose that there either exists $1 \leq s \leq k$ such that $\beta_i < \alpha_i$ for $1 \leq i \leq s$ and $\beta_i = \alpha_i$ for $s+1 \leq i \leq k$ or $\beta_0 = \alpha_0 - 1$ and $\beta_i = \alpha_i$ for $1 \leq i \leq k$, i.e. $d'_{max} = n/2$. Denote by

$$j_0 = p_1^{\alpha_1 - \beta_1 - 1} \cdots p_s^{\alpha_s - \beta_s - 1} p_{s+1}^{\alpha_{s+1}} \cdots p_k^{\alpha_k}.$$

It holds trivially that $0 \leq j_0 \leq n-1$. In each of the cases Lemma 5 directly yields that $c(j_0, n/d'_{max})$ is odd.

Let $d \in D' \setminus \{d'_{max}\}$ be an arbitrary divisor with its prime factorization $d = 2^{\gamma_0} p_1^{\gamma_1} \cdots p_k^{\gamma_k}$.

We will show that there exists $1 \leq i \leq k$ such that $0 \leq \gamma_i < \beta_i \leq \alpha_i$. Suppose this is not the case, which means that $0 \leq \beta_i \leq \gamma_i \leq \alpha_i$ for $1 \leq i \leq k$. If $\beta_0 \leq \gamma_0$, then $d'_{max} \mid d$, which is a contradiction. Similarly, if $\beta_0 = \gamma_0 + 1$, then it holds that $d'_{max} \mid 2d$, which implies $d = d'_{max}/2$ and therefore $d'_{max}/2, d'_{max} \in D'$, providing a contradiction with the definition of the set D''.

Let $1 \leq i \leq k$ be an arbitrary index such that $\gamma_i < \beta_i$. If $\alpha_i - \beta_i \geq 1$, then $1 \leq i \leq s$ holds and $S_{p_i}(d) = \gamma_i < \beta_i < \alpha_i$. Suppose that $c(j_0, n/d)$ is odd, according to Lemma 5 we have that $S_{p_i}(d) \in \{\alpha_i, \alpha_i - (\alpha_i - \beta_i - 1) - 1\} = \{\alpha_i, \beta_i\}$, which is a contradiction and we conclude that $c(j_0, n/d)$ is even. Now suppose that $\alpha_i = \beta_i$. Then $i > s$ and therefore we have $S_{p_i}(d) = \gamma_i$ and $S_{p_i}(j_0) = \alpha_i$. Again if $c(j_0, n/d)$ is odd, according to Lemma 5, $S_{p_i}(d) = \alpha_i > \gamma_i$ which is a contradiction and $c(j_0, n/d)$ is even.

This implies that there exists an odd index j_0 such that $c(j_0, n/d'_{max})$ is odd and $c(j_0, n/d)$ is even for every $d \in D' \setminus \{d'_{max}\}$. Now we have

$$\lambda_{j_0} = c(j_0, n/d'_{max}) + \sum_{d \in D' \setminus \{d'_{max}\}} c(j_0, n/d) + \sum_{d \in D''} c(j_0, n/d) \in 2\mathbb{N}+1,$$

since the second sum in the last expression is zero, which yields a contradiction. Finally, we conclude that $D' = \emptyset$ and thus $D_0 = 2D_1$.

The direction $(iii) \Rightarrow (i)$ is obvious, which finishes the proof.

□

Theorem 8. *Let* $\mathrm{ICG}_n(D)$ *be an integral circulant graph. The following statements are equivalent:*

i) *Every* λ_j *is even for odd* $0 \leq j \leq n-1$.

ii) $D_0 = 2D_1$.

iii) *Every* $\lambda_j = 0$ *for odd* $0 \leq j \leq n-1$.

Proof. Let $\widetilde{D_1} = D_0 \cup D_1$ and $0 \leq j \leq n-1$ be an arbitrary odd index. For $d \in D \setminus \widetilde{D_1}$ we have that n/d is divisible by 4 and thus $\gcd(j, n/d) \in 2\mathbb{N}+1$, which implies that $4 \mid t_{n/d,j}$, $\mu(t_{n/d,j}) = 0$ and therefore $c(j, n/d) = 0$. According to the last conclusion, the formula for j-th eigenvalue of $\mathrm{ICG}_n(D)$ can be boiled down to

$$\lambda_j = \sum_{d \in \widetilde{D_1}} c(j, n/d).$$

By μ_j, $0 \leq j \leq n-1$, we denote the eigenvalues of the integral circulant graph $\mathrm{ICG}_n(\widetilde{D_1})$. Therefore, it holds that $\lambda_j = \mu_j$ for every odd $0 \leq j \leq n-1$. From Lemma 7 we conclude that for all eigenvalues μ_j the statements of the theorem are mutually equivalent, and thus since $\lambda_j = \mu_j$ the same conclusion holds for the eigenvalues λ_j. □

Now, we are ready to prove the first result concerning strong regularity on arbitrary $\mathrm{ICG}_n(D)$. In the sequel, by θ and τ we denote two smallest eigenvalues of the strongly regular $\mathrm{ICG}_n(D)$. Furthermore, according to (5) and (6) we can assume that $\theta \geq 0$ and $\tau < 0$.

Theorem 9. *If* θ *and* τ *are two even eigenvalues of a given strongly regular* $\mathrm{ICG}_n(D)$*, then the complement graph of* $\mathrm{ICG}_n(D)$*, denoted by* $\overline{\mathrm{ICG}_n(D)}$*, is not connected.*

Proof.

According to Lemma 2, part (d), it can be concluded that if strongly regular graph is disconnected, then -1 is an eigenvalue of its spectrum. Therefore, since θ and τ are even then $\mathrm{ICG}_n(D)$ is connected and hence λ_0 is the only eigenvalue of the spectrum of $\mathrm{ICG}_n(D)$ equal to r. Furthermore, as $\theta, \tau \in 2\mathbb{N}$ we see that all eigenvalues λ_j are even for odd $0 \leq j \leq n-1$ and according to Theorem 8 holds that $\theta = 0$. Furthermore, according to (5) we have that $c = r$. If we denote by $n, \overline{r}, \overline{a}, \overline{c}$ the parameters of the complement of $\mathrm{ICG}_n(D)$, then

$$\overline{a} = n - 2 - 2r + c = n - r - 2 = \overline{r} - 1,$$

and using Lemma 2 we see that $\overline{\mathrm{ICG}_n(D)}$ is not connected, i.e. $\mathrm{ICG}_n(D)$ is imprimitive.

□

Theorem 10. *If θ and τ are two odd eigenvalues of a given strongly regular $\mathrm{ICG}_n(D)$, then it is not connected.*

Proof. Let λ_i, for $1 \leq i \leq n-1$, be the eigenvalues of $\mathrm{ICG}_n(D)$, which are all odd. The eigenvalues of the complement graph of the graph $\mathrm{ICG}_n(D)$ are $-1-\lambda_i$ (for example, see Lemma 8.5.1 from [**6**]), thus they are even, whence by Theorem 9 we conclude that the complement graph of $\overline{\mathrm{ICG}_n(D)}$ is disconnected, i.e. $\mathrm{ICG}_n(D)$ is disconnected. □

In Theorems 9 and 10 in each of the mentioned cases we establish that every strongly regular $\mathrm{ICG}_n(D)$ is imprimitive.

Let us further examine the properties of the eigenvalues of $\mathrm{ICG}_n(D)$ and establish yet some other assertions about them.

Theorem 11. *For a given graph $\mathrm{ICG}_n(D)$, prime $p \mid n$ and the eigenvalues $\lambda_0, \ldots, \lambda_{n-1}$ of $\mathrm{ICG}_n(D)$, it holds that $p \mid \lambda_{p^{\beta+1}j} - \lambda_{p^\beta j}$, for $p \nmid j$ and $0 \leq p^{\beta+1}j, p^\beta j \leq n-1$.*

Proof. According to the relation (1) and the following equation

$$\gcd(p^{\beta+1}j, n/d) = \begin{cases} \gcd(p^\beta j, n/d), & S_p(n/d) \leq \beta \\ p \cdot \gcd(p^\beta j, n/d), & S_p(n/d) > \beta \end{cases}$$

we have that

$$t_{n/d,p^{\beta+1}j} = \frac{n}{d\gcd(n/d, p^{\beta+1}j)} = \begin{cases} t_{n/d,p^\beta j}, & S_p(n/d) \leq \beta \\ \frac{1}{p} \cdot t_{n/d,p^\beta j}, & S_p(n/d) > \beta \end{cases}.$$

Furthermore, it holds that $c(p^\beta j, n/d) = \mu(t_{n/d,p^\beta j})\frac{\varphi(n/d)}{\varphi(t_{n/d,p^\beta j})}$ and hence

$$c(p^\beta j, n/d) = \begin{cases} c(p^{\beta+1}j, n/d), & S_p(n/d) \leq \beta \\ \mu(p \cdot t_{n/d,p^{\beta+1}j})\frac{\varphi(n/d)}{\varphi(p \cdot t_{n/d,p^{\beta+1}j})}, & S_p(n/d) > \beta \end{cases}. \tag{9}$$

Let us prove that for every $d \in D$ holds that $p \mid c(p^{\beta+1}j, n/d) - c(p^\beta j, n/d)$, which by (2) implies that
$p \mid \lambda_{p^{\beta+1}j} - \lambda_{p^\beta j}$. To this end, we distinguish the following cases.

If $S_p(n/d) \leq \beta$, it is clear that $c(p^\beta j, n/d) = c(p^{\beta+1}j, n/d)$.

Let $S_p(n/d) > \beta$. If $p \mid t_{n/d,p^{\beta+1}j}$, then $p^2 \mid p \cdot t_{n/d,p^{\beta+1}j}$, and thus $\mu(p \cdot t_{n/d,p^{\beta+1}j}) = 0$, i.e. $c(p^\beta j, n/d) = 0$. If $p^2 \mid t_{n/d,p^{\beta+1}j}$ we have $c(p^{\beta+1}j, n/d) = 0$,

so the difference $c(p^{\beta+1}j, n/d) - c(p^{\beta}j, n/d) = 0$ is divisible by p. In the case for $p \parallel t_{n/d,p^{\beta+1}j}$, from the definition of $t_{n/d,p^{\beta+1}j}$ it must be $\beta+1 = S_p(n/d)-1$, whence we obtain that $p^2 \mid n/d$. Furthermore, it holds that $p \mid \varphi(n/d)/\varphi(t_{n/d,p^{\beta+1}j})$, implying that $p \mid c(p^{\beta+1}j, n/d)$ and $p \mid c(p^{\beta+1}j, n/d) - c(p^{\beta}j, n/d)$.

If $p \nmid t_{n/d,p^{\beta+1}j}$, according to the relation (9) we obtain

$$c(p^{\beta}j, n/d) = -\mu(t_{n/d,p^{\beta+1}j})\frac{\varphi(n/d)}{(p-1)\varphi(t_{n/d,p^{\beta+1}j})} = -\frac{c(p^{\beta+1}j, n/d)}{p-1},$$

from where we finally conclude that $c(p^{\beta+1}j, n/d) - c(p^{\beta}j, n/d) = -p \cdot c(p^{\beta}j, n/d)$, which is what had to be proven. □

According to the relation

$$\lambda_{p^{\alpha}j} - \lambda_{p^{\beta}j} = (\lambda_{p^{\alpha}j} - \lambda_{p^{\alpha-1}j}) + (\lambda_{p^{\alpha-1}j} - \lambda_{p^{\alpha-2}j}) + \ldots + (\lambda_{p^{\beta+1}j} - \lambda_{p^{\beta}j})$$

for $\alpha > \beta$ we have the following assertion.

Corollary 12. *For a given graph* $\mathrm{ICG}_n(D)$*, prime* $p \mid n$ *and the eigenvalues* $\lambda_0, \ldots, \lambda_{n-1}$ *of* $\mathrm{ICG}_n(D)$*, it holds that* $p \mid \lambda_{p^{\alpha}j} - \lambda_{p^{\beta}j}$*, for* $p \nmid j$*,* $\alpha > \beta$ *and* $0 \le p^{\alpha}j, p^{\beta}j \le n-1$*.*

Theorem 13. *Let* $p_i \mid n$ *be a prime number and let* $\lambda_0, \ldots, \lambda_{n-1}$ *be the eigenvalues of* $\mathrm{ICG}_n(D)$*. Then, it holds that* $p_i^{\alpha_i} \mid \lambda_0 - \lambda_{n/p_i}$*.*

Proof. According to Proposition 1 we conclude that

$$\begin{aligned}\lambda_0 - \lambda_{n/p_i} &= \sum_{\{d \in D \mid p_i \mid d\}} (\varphi(n/d) - \varphi(n/d)) + \sum_{\{d \in D \mid p_i \nmid d\}} \left(\varphi(n/d) + \frac{\varphi(n/d)}{p_i - 1}\right) \\ &= \sum_{\{d \in D \mid p_i \nmid d\}} \frac{p_i\ \varphi(n/d)}{p_i - 1}.\end{aligned}$$

For $p_i \nmid d$, we have that $p_i^{\alpha_i} \mid n/d$, so we can write that $\frac{n}{d} = p_i^{\alpha_i}\frac{n'}{d}$, where $n = p_i^{\alpha_i}n'$ and $\frac{n'}{d} \in \mathbb{Z}$. Finally, it holds that

$$\lambda_0 - \lambda_{n/p} = \sum_{\{d \in D \mid p_i \nmid d\}} \frac{p_i p_i^{\alpha_i - 1}(p_i - 1)\ \varphi(\frac{n'}{d})}{p_i - 1} = p_i^{\alpha_i} \sum_{\{d \in D \mid p_i \nmid d\}} \varphi(\frac{n'}{d}).$$

□

Theorem 14. *If* θ *and* τ *are two eigenvalues of distinct parity of the strongly regular graph* $\mathrm{ICG}_n(D)$*, then the graph is imprimitive.*

Proof. Let $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the prime factorization of n.

Case 1. Suppose that there exists $p_i \nmid \theta - \tau$ and without loss of generality we also suppose that $i = 1$.

Case 1.1. n is odd. Thus, we write $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

Without loss of generality we may assume that $n/p_1 \notin D$. If $n/p_1 \in D$ the proof can be carried out for the complement graph of $\mathrm{ICG}_n(D)$, that is $\mathrm{ICG}_n(D_n \setminus D)$, which is a strongly regular integral circulant with $n/p_1 \notin D_n \setminus D$.

We will prove by induction that any divisor d of n such that $p_1^{\alpha_1} \nmid d$ does not belong to D.

First we prove that any divisor d_i with the factorization $d_i = p_1^i p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ does not belong to D, $0 \le i \le \alpha_1 - 1$. If $i = \alpha_1 - 1$, we see that $d_{\alpha_1 - 1} = n/p_1$ and thus $d_{\alpha_1 - 1} \notin D$, according to the assumption of this case. For $0 \le i \le \alpha_1 - 1$, define the indices $j_i = p_1^{\alpha_1 - i - 1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Using Lemma 5, we may notice that $c(j_i, n/d) \in 2\mathbb{Z} + 1$ if and only if $d = d_i$. Furthermore, as $d_{\alpha_1 - 1} \notin D$ it holds that $c(j_{\alpha_1 - 1}, n/d) \in 2\mathbb{Z}$, for every $d \in D$, thus we obtain that $\lambda_{j_{\alpha_1 - 1}} \in 2\mathbb{Z}$. On the other hand, according to Corollary 12, we have that $p_1 \mid \lambda_{j_{\alpha_1 - 1}} - \lambda_{j_i}$, and using the assumption of this case we also have that $p_1 \nmid \theta - \tau$. This implies that $\lambda_{j_i} = \lambda_{j_{\alpha_1 - 1}} \in \{\theta, \tau\}$, for every $0 \le i \le \alpha_1 - 2$. Thus, $\lambda_{j_i} \in 2\mathbb{Z}$ and by Lemma 5 we conclude that for each $d \in D$, $c(j_i, n/d)$ must be even and therefore $d_i \notin D$.

Now, we assume that for any divisor d of n such that exactly $p_1^{\alpha_1}, p_{i_2}^{\alpha_{i_2}}, \dots, p_{i_l}^{\alpha_{i_l}} \nmid d$, for some $1 \le l \le s \le k-1$ and $2 \le i_2, \dots, i_l \le k$, does not belong to D. We will prove that an arbitrary divisor d of n such that exactly $p_1^{\alpha_1}, p_{i_2}^{\alpha_{i_2}}, \dots, p_{i_{s+1}}^{\alpha_{i_{s+1}}} \nmid d$, $1 \le i_2, \dots, i_{s+1} \le k$, does not belong to D. Notice that we proved the induction hypothesis in the case for $s = 1$ in the above discussion.

We prove that the divisor $d_l = p_1^l p_2^{\alpha_2 - \gamma_2 - 1} \dots p_{s+1}^{\alpha_{s+1} - \gamma_{s+1} - 1} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \notin D$, for $0 \le l \le \alpha_1 - 1$ and $0 \le \gamma_i \le \alpha_i - 1$ (with out loss of generality we assume $i_j = j$ for $2 \le j \le s+1$). Define the indices $j_l = p_1^{\alpha_1 - l - 1} p_2^{\gamma_2} \dots p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k}$ for $0 \le l \le \alpha_1 - 1$ and $0 \le \gamma_i \le \alpha_i - 1$. Using Lemma 5 we conclude that $c(j_l, n/d) \in 2\mathbb{Z}+1$ if and only if $d \in D^{\alpha_1, l}$, where $D^{\alpha_1, l} = \{p_1^{\beta_1} \dots p_{s+1}^{\beta_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \mid \beta_1 \in \{l, \alpha_1\}, \beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}, 2 \le i \le s+1\}$.

On the other hand, we define the index $j_{\alpha_1} = p_1^{\alpha_1} p_2^{\gamma_2} \dots p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k}$. Similarly, $c(j_{\alpha_1}, n/d) \in 2\mathbb{Z} + 1$ if and only if $d \in D^{\alpha_1}$, where $D^{\alpha_1} = \{p_1^{\alpha_1} p_2^{\beta_2} \dots p_{s+1}^{\beta_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \mid \beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}, 2 \le i \le s+1\}$. From the definition of the sets $D^{\alpha_1, l}$ and D^{α_1} we have the following relation

$$D^{\alpha_1, l} = D^{\alpha_1} \cup \{d_l\} \cup D^l,$$

where $D^l = \{p_1^l p_2^{\beta_2} \dots p_{s+1}^{\beta_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \mid (\forall\ 2 \le i \le s+1)\ \beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}$ and $(\exists\ 2 \le i \le s+1)\ \beta_i = \alpha_i\}$.

By the induction hypothesis we have that $D^l \cap D = \emptyset$. Furthermore, according to Corollary 12 we obtain that $p_1 \mid \lambda_{j_{\alpha_1}} - \lambda_{j_l}$, and since $p_1 \nmid \theta - \tau$, it holds that $\lambda_{j_{\alpha_1}} = \lambda_{j_l}$ (trivially $\lambda_{j_{\alpha_1}}$ and λ_{j_l} have the same parity).

Let $D' = D^{\alpha_1} \cap D$. If $d_l \in D$, the eigenvalues $\lambda_{j_{\alpha_1}}$ and λ_{j_l} can be written in

the following way

$$\begin{aligned}\lambda_{j_{\alpha_1}} &= \sum_{d\in D\setminus D'} c(j_{\alpha_1},\frac{n}{d})+\sum_{d\in D'} c(j_{\alpha_1},\frac{n}{d})\\ \lambda_{j_l} &= \sum_{d\in D\setminus(D'\cup\{d_l\})} c(j_l,\frac{n}{d})+\sum_{d\in D'} c(j_l,\frac{n}{d})+c(j_l,\frac{n}{d_l}).\end{aligned}$$

Since $D^l\cap D=\emptyset$, we have that $c(j_{\alpha_1},n/d)$ and $c(j_l,n/d)$ are even, for all $d\in D\setminus(D'\cup\{d_l\})$ and $c(j_{\alpha_1},n/d_l)$ is even. Therefore, we obtain

$$\lambda_{j_{\alpha_1}}\equiv_2\sum_{d\in D'} c(j_{\alpha_1},\frac{n}{d})\equiv_2\lambda_{j_l}\equiv_2\sum_{d\in D'} c(j_l,\frac{n}{d})+c(j_l,\frac{n}{d_l}).$$

Moreover, since $c(j_{\alpha_1},n/d),c(j_l,n/d)$ is odd for $d\in D'$ this implies that $c(j_l,n/d_l)\equiv_2\sum_{d\in D'}c(j_{\alpha_1},n/d)-c(j_l,n/d)\equiv_2 0$. Finally, $c(j_l,n/d_l)\equiv_2 0$ yields that $d_l\notin D^{\alpha_1,l}$, which is a contradiction and we conclude that $d_l\notin D$.

Thus, we prove if $d\in D$, then $p_1^{\alpha_1}\mid d$, implying that $\gcd(\{d\mid d\in D\})=p_1^{\alpha_1}$ and thus $\mathrm{ICG}_n(D)$ is not connected and therefore imprimitive.

Case 1.2. n is even.

We will prove by induction that $D_0=2(D_1\setminus\{n/2\})$.

First we prove that for any divisor d_i with the factorization $d_i=2^{\alpha_0-1}p_1^i\cdots p_k^{\alpha_k}$ holds that $d_i\in D\Leftrightarrow 2d_i\in D$, $0\le i\le\alpha_1-1$. For $0\le i\le\alpha_1-1$, define the indices $j_i=p_1^{\alpha_1-i-1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ and for $i=\alpha_1$ we define j_{α_1} to be $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$. Using Lemma 5, if $0\le i\le\alpha_1-1$ we may notice that $c(j_i,n/d)\in 2\mathbb{Z}+1$ if and only if $d\in D^i$, where $D^i=\{d_i,2d_i,n/2\}$ and $c(j_{\alpha_1},n/d)\in 2\mathbb{Z}+1$ if and only if $d=d_{\alpha_1}=n/2$. Therefore, we conclude that $\lambda_{j_{\alpha_1}}\in 2\mathbb{Z}+1\Leftrightarrow n/2\in D$ and $\lambda_{j_i}\in 2\mathbb{Z}+1\Leftrightarrow D^i\subseteq D\veebar|D^i\cap D|=1$. On the other hand, according to Corollary 12, we have that $p_1\mid\lambda_{j_{\alpha_1}}-\lambda_{j_i}$, and according to the assumption of this case we have that $p_1\nmid\theta-\tau$, implying that $\lambda_{j_i}=\lambda_{j_{\alpha_1}}\in\{\theta,\tau\}$, for every $0\le i\le\alpha_1-1$. Thus, λ_{j_i} and $\lambda_{j_{\alpha_1}}$ have the same parity, whence we obtain that $\lambda_{j_{\alpha_1}}\in 2\mathbb{Z}+1\Leftrightarrow\lambda_{j_i}\in 2\mathbb{Z}+1\Leftrightarrow n/2\in D\Leftrightarrow D^i\subseteq D\veebar|D^i\cap D|=1$. Finally, the last equivalence is satisfied if and only if $d_i,2d_i\in D$ or $d_i,2d_i\notin D$, implying that $d_i\in D\Leftrightarrow 2d_i\in D$. In the same fashion we can show that for $d=2^{\alpha_0-1}p_1^{\alpha_1}\dots p_{l-1}^{\alpha_{l-1}}p_l^ip_{1+1}^{\alpha_{l+1}}\dots p_k^{\alpha_k}$ holds $d\in D$ if and only if $2d\in D$.

Now, we assume that for any divisor d of n such that exactly $2^{\alpha_0-1}\parallel d$ and $p_{i_1}^{\alpha_{i_1}},p_{i_2}^{\alpha_{i_2}},\dots,p_{i_l}^{\alpha_{i_l}}\nmid d$, for some $1\le l\le s\le k-1$ and $1\le i_1,i_2,\dots,i_s\le k$, belongs to D if and only if $2d\in D$. We will prove that an arbitrary divisor d of n such that $2^{\alpha_0-1}\parallel d$ and exactly $p_1^{\alpha_{i_1}},p_{i_2}^{\alpha_{i_2}},\dots,p_{i_{s+1}}^{\alpha_{i_{s+1}}}\nmid d$, for $1\le s\le k$ and $1\le i_1,i_2,\dots,i_{s+1}\le k$, belongs to D if and only if $2d\in D$. Notice that we proved the hypothesis for $s=1$ in the above discussion.

We prove that the following equivalence

$$d_{\gamma_1}=2^{\alpha_0-1}p_1^{\alpha_1-\gamma_1-1}p_2^{\alpha_2-\gamma_2-1}\dots p_{s+1}^{\alpha_{s+1}-\gamma_{s+1}-1}p_{s+2}^{\alpha_{s+2}}\dots p_k^{\alpha_k}\in D\Leftrightarrow 2d_{\gamma_1}\in D,$$

for $0 \leq \gamma_i \leq \alpha_i - 1$ (with out loss of generality we assume $i_j = j$ for $1 \leq j \leq s+1$). Define the indices $j_{\gamma_1} = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k}$, for $0 \leq \gamma_i \leq \alpha_i - 1$, $1 \leq i \leq s+1$. Using Lemma 5 we conclude that $c(j_{\gamma_1}, n/d) \in 2\mathbb{Z}+1$ if and only if $d \in D^{\alpha_1,\gamma_1}$, where $D^{\alpha_1,\gamma_1} = \{2^{\beta_0} p_1^{\beta_1} \dots p_{s+1}^{\beta_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \mid \beta_0 \in \{\alpha_0 - 1, \alpha_0\}, \beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}, 1 \leq i \leq s+1\}$.

On the other hand, we define the index $j_{\alpha_1} = p_1^{\alpha_1} p_2^{\gamma_2} \dots p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k}$. Similarly, $c(j_{\alpha_1}, n/d) \in 2\mathbb{Z}+1$ if and only if $d \in D^{\alpha_1}$, where

$$D^{\alpha_1} = \{2^{\beta_0} p_1^{\alpha_1} p_2^{\beta_2} \dots p_{s+1}^{\beta_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \quad | \quad \beta_0 \in \{\alpha_0 - 1, \alpha_0\}, \\ \beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\}, 2 \leq i \leq s+1\}.$$

From the definition of the sets D^{α_1,γ_1} and D^{α_1} we have the following relation

$$D^{\alpha_1,\gamma_1} = D^{\alpha_1} \cup \{d_{\gamma_1}, 2d_{\gamma_1}\} \cup D^{\gamma_1},$$

where $D^{\gamma_1} = \{2^{\beta_0} p_1^{\alpha_1 - \gamma_1 - 1} p_2^{\beta_2} \dots p_{s+1}^{\beta_{s+1}} p_{s+2}^{\alpha_{s+2}} \dots p_k^{\alpha_k} \mid \beta_0 \in \{\alpha_0 - 1, \alpha_0\}, (\forall\ 2 \leq i \leq s+1)\ (\beta_i \in \{\alpha_i - \gamma_i - 1, \alpha_i\})$ and $(\exists\ 2 \leq i \leq s+1)\ (\beta_i = \alpha_i)\}$.

By the induction hypothesis for an arbitrary $d \in D^{\alpha_1} \cup D^{\gamma_1}$ we have that $d \in D$ if and only if $2d \in D$. Let $D' = D^{\alpha_1} \cap D$ and $D'' = (D^{\alpha_1} \cup D^{\gamma_1}) \cap D$. Suppose that $d_{\gamma_1} \in D$ and $2d_{\gamma_1} \notin D$, the eigenvalues $\lambda_{j_{\alpha_1}}$ and $\lambda_{j_{\gamma_1}}$ can be written in the following way

$$\begin{aligned} \lambda_{j_{\alpha_1}} &= \sum_{d \in D \setminus D'} c(j_{\alpha_1}, \frac{n}{d}) + \sum_{d \in D'} c(j_{\alpha_1}, \frac{n}{d}) \\ \lambda_{j_{\gamma_1}} &= \sum_{d \in D \setminus (D'' \cup \{d_l\})} c(j_{\gamma_1}, \frac{n}{d}) + \sum_{d \in D''} c(j_{\gamma_1}, \frac{n}{d}) + c(j_{\gamma_1}, \frac{n}{d_{\gamma_1}}). \end{aligned}$$

Since $j_{\alpha_1}, j_{\gamma_1} \in 2\mathbb{N}+1$, according to Lemma 6, we obtain that $\sum_{d \in D'} c(j_{\alpha_1}, n/d) = 0$ and $\sum_{d \in D''} c(j_{\gamma_1}, n/d) = 0$. Since $c(j_{\alpha_1}, n/d) \in 2\mathbb{Z}$, for $d \in D \setminus D'$ it holds that $\lambda_{j_{\alpha_1}} \in 2\mathbb{Z}$ and since $c(j_{\gamma_1}, n/d) \in 2\mathbb{Z}$, for $d \in D \setminus (D'' \cup \{d_l\})$ and $c(j_{\gamma_1}, n/d_{\gamma_1}) \in 2\mathbb{Z}+1$ it holds that $\lambda_{j_{\gamma_1}} \in 2\mathbb{Z}+1$. According to Corollary 12, we have that $p_1 \mid \lambda_{j_{\alpha_1}} - \lambda_{j_{\gamma_1}}$, and using the assumption of this case we have that $p_1 \nmid \theta - \tau$, we obtain that $\lambda_{j_{\alpha_1}} = \lambda_{j_{\gamma_1}} \in \{\theta, \tau\}$, for every $0 \leq \gamma_1 \leq \alpha_1 - 1$. This means that $\lambda_{j_{\alpha_1}} \equiv_2 \lambda_{j_l}$, and it is clearly a contradiction. So, we proved that $d_l \in D \Rightarrow 2d_l \in D$ and in the same way we can prove that $2d_l \in D \Rightarrow d_l \in D$, therefore we obtain that $D_0 = 2(D_1 \setminus \{n/2\})$. Finally, for $n/2 \notin D$ from Theorem 8 it can be concluded that $\theta = 0$. Thus, we obtain that $c = r$, i.e. $\overline{a} = \overline{r} - 1$ implying that $\overline{\mathrm{ICG}_n(D)}$ is not connected, according to Lemma 2. If $n/2 \in D$, according to Proposition 1 it holds that $c(j, 2) = -1$ for $j \in 2\mathbb{N}+1$, which further implies that $\lambda_j = -1$ for all odd $0 \leq j \leq n-1$. Now, we see that one eigenvalue of the graph $\overline{\mathrm{ICG}_n(D)}$ is equal to zero, and therefore $\mathrm{ICG}_n(D)$ is not connected, from the same reason as in the case for $n/2 \notin D$.

Case 2. Suppose that $p_1 p_2 \dots p_k \mid \theta - \tau$. Let $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the prime factorization of n and $p_0 = 2$.

The relations (7) can be rewritten as

$$-m_\theta(\theta-\tau) = n\tau + (r-\tau)$$
$$m_\tau(\theta-\tau) = n\theta + (r-\theta),$$

from where we see that $p_1p_2\dots p_k \mid r-\tau$ and $p_1p_2\dots p_k \mid r-\theta$. According to Theorem 13 it holds that $p_i^{\alpha_i} \mid \lambda_0 - \lambda_{n/p_i}$, for $1 \le i \le k$. Furthermore, since $\lambda_0 - \lambda_{n/p^i} \in \{r-\tau, r-\theta\}$, we conclude that there exists $1 \le s \le k$ such that $p_{i_1}^{\alpha_{i_1}} \dots p_{i_s}^{\alpha_{i_s}} p_{i_{s+1}} \dots p_{i_k} \mid r-\tau$ and $p_{i_1} \dots p_{i_s} p_{i_{s+1}}^{\alpha_{i_{s+1}}} \dots p_{i_k}^{\alpha_{i_k}} \mid r-\theta$, where $(i_1, \dots, i_k)$ is a permutation of $(1, \dots, k)$. Without loss of generality we assume that $i_j = j$ for all $1 \le j \le k$.

Now using the relation (7) again, we obtain that $p_1^{\alpha_1} \dots p_s^{\alpha_s} p_{s+1} \dots p_k \mid m_\theta(\theta-\tau)$ and $p_1 \dots p_s p_{s+1}^{\alpha_{s+1}} \dots p_k^{\alpha_k} \mid m_\tau(\theta-\tau)$. According to (8) we finally conclude that

$$p_1^{\alpha_1} \dots p_s^{\alpha_k} p_1 \dots p_k \mid nr\overline{r},$$

and so $p_1 \dots p_k \mid r\overline{r}$. In the case for $p_i \mid r$, it is clear that $p_i \mid \theta$ and $p_i \mid \tau$. On the other hand, if $p_i \mid \overline{r}$, then $r \equiv_{p_i} -1$ and $\theta \equiv_{p_i} -1$, $\tau \equiv_{p_i} -1$ also. Observe that λ_1 can be represented in the following way (according to Proposition 1) $\lambda_1 = \sum_{d \in D} \mu(\frac{n}{d})$. Suppose that $|\lambda_1| \ge 1$ and let $m_1 = \prod_{\{1 \le i \le k \mid p_i \mid\mid \lambda_1|\}} p_i$. We also define $m_2 = \prod_{\{1 \le i \le k \mid p_i \mid\mid \lambda_1|+1\}} p_i$, if $\lambda_1 > 0$, and $m_2 = \prod_{\{1 \le i \le k \mid p_i \mid\mid \lambda_1|-1\}} p_i$, if $\lambda_1 < 0$. Thus, it can be concluded that $m_1 \mid |\lambda_1|$ and $m_2 \mid |\lambda_1|+1$, if $\lambda_1 > 0$, and $m_2 \mid |\lambda_1|-1$, if $\lambda_1 < 0$. Since one of the numbers $|\lambda_1|$ or $|\lambda_1| \pm 1$ is even we have that $2m_1 \mid |\lambda_1|$ or $2m_2 \mid |\lambda_1| \pm 1$. Finally, in all of the cases it holds that $|\lambda_1| \ge \max\{2m_1, m_2 - 1\}$ or $|\lambda_1| \ge \max\{m_1, 2m_2 - 1\}$. On the other hand, $|\mu(n/d)| = 1$ if and only if $p_i^{\alpha_i - 1} \mid d$ for all $0 \le i \le k$, but if we take into account the signs of $\mu(n/d)$, it can be concluded that $-2^k \le \lambda_1 \le 2^k$ implying that $|\lambda_1| \le 2^k$. From the last two conclusions we obtain $\max\{2m_1, m_2 - 1\} \le 2^k$ or $\max\{m_1, 2m_2 - 1\} \le 2^k$. If $\max\{2m_1, m_2 - 1\} \le 2^k$ holds we have that $2m_1 \ne 2^k$ (except in the trivial case $n = 2$ which can be excluded immediately), which further yields $2m_1 \le 2^k - 1$ and $m_2 \le 2^k + 1$ and therefore

$$2p_1 \dots p_k = 2m_1m_2 \le (2^k - 1)(2^k + 1) = 4^k - 1.$$

Similarly, in the remaining case, if $\max\{m_1, 2m_2 - 1\} \le 2^k$ we have that $2m_2 - 1 \ne 2^k$, which further yields $2m_2 \le 2^k$ and $m_1 \le 2^k$ and therefore

$$2p_1 \dots p_k = 2m_1m_2 \le 2^k 2^k = 4^k.$$

The last inequality is never satisfied, since $2p_1 > 4$ and $p_i > 4$, for $2 \le i \le k$, which is a contradiction. Thus, we obtain that $\lambda_1 = 0$, which yields that $c = r$ i.e., $\overline{a} = \overline{r} - 1$ implying that $\overline{\mathrm{ICG}_n(D)}$ is not connected according to Lemma 2.

□

Theorem 15. *Let* $\mathrm{ICG}_n(D)$ *be an arbitrary connected integral circulant graph* $\mathrm{ICG}_n(D)$. *Then,* $\mathrm{ICG}_n(D)$ *is strongly regular if and only if* n *is a composite integer and* $D = \{d \in D_n \mid m \nmid d\}$, *for some divisor* $n - 1 \ge m \ge 2$ *of* n.

Proof. Suppose that $\mathrm{ICG}_n(D)$ be an arbitrary connected strongly regular graph. From Theorems 9, 10 and 14 we see that every such strongly regular $\mathrm{ICG}_n(D)$ must be imprimitive. Now, using Lemma 2, we conclude that $\overline{\mathrm{ICG}_n(D)}$ is isomorphic to $mK_{\overline{r}+1}$ and hence $\mathrm{ICG}_n(D)$ is isomorphic to the complete multipartite graph $K_{\underbrace{\overline{r}+1,\ldots,\overline{r}+1}_{m}}$, where $\overline{r}$ is the regularity of $\overline{\mathrm{ICG}_n(D)}$ for some $n-1 \geq m \geq 2$. This yields $n = (\overline{r}+1)m$ and thus n must be composite. Denote the color classes of $K_{\underbrace{\overline{r}+1,\ldots,\overline{r}+1}_{m}}$ by $C_i = \{0 \leq j \leq n-1 \mid j \equiv_m i\}$, for $0 \leq i \leq m-1$. Therefore, we obtain that two vertices a and b are not adjacent in $\mathrm{ICG}_n(D)$ if and only if $a - b \equiv_m 0$. The last equivalence is true if and only if $a - b \in \{G_n(d) \mid m \mid d\}$. Therefore, we conclude that a and b are adjacent if and only if $a-b \in \{G_n(d) \mid m \nmid d\}$ and thus $K_{\underbrace{\overline{r}+1,\ldots,\overline{r}+1}_{m}} \cong \mathrm{ICG}_n(\{d \in D_n \mid m \nmid d\})$, which was to be shown.

On the other hand, $\mathrm{ICG}_n(\{d \in D_n \mid m \nmid d\})$ is strongly regular as it is isomorphic to the complete multipartite graph $K_{\underbrace{\overline{r}+1,\ldots,\overline{r}+1}_{m}}$. Now we can calculate the parameters r, a and c of the integral circulant graph $\mathrm{ICG}_n(\{d \in D_n \mid m \nmid d\})$. Notice first that Lemma 2 directly yields that $\overline{c} = 0$ and $\overline{a} = \overline{r} - 1 = n/m - 2$. Now, it holds that $r = n - \overline{r} - 1 = (m-1)\frac{n}{m}$, $a = n - 2 - 2\overline{r} + \overline{c} = (m-2)\frac{n}{m}$ and $c = n - 2\overline{r} + \overline{a} = (m-1)\frac{n}{m}$. Using Lemma 2 and the equalities (7) , we can very easily calculate the eigenvalues of the graph together with their multiplicities as well. We have already concluded that $\theta = 0$ and since $\Delta = (a-c)^2 + 4(r-c) = \frac{n^2}{m^2}$ we obtain that $\tau = -\frac{n}{m}$. Finally, from the equalities (7) follow that $m_\theta = n - m$ and $m_\tau = m - 1$. □

Similarly, we can prove that disconnected $\mathrm{ICG}_n(D)$ is strongly regular if and only if $\{d \in D_n \mid m \mid d\}$. Indeed, as $\mathrm{ICG}_n(D)$ is strongly regular, then $\overline{\mathrm{ICG}_n(D)}$ is connected strongly regular and therefore $D_n \setminus D = \{d \in D_n \mid m \nmid d\}$, according to the above theorem. This directly yields that $D = \{d \in D_n \mid m \mid d\}$.

4. CONCLUSION

In this paper we characterize strongly regular integral circulant graphs by proving that these graphs must be imprimitive. Generally, the proofs presented in this paper are based on the connection between number theory and spectral graph theory and fall into a good many of distinct cases. Attempts to classify the class of integral circulant graphs with four distinct eigenvalues would be much more demanding and probably require considering a significantly greater number of cases and we leave it for future research. We think that it is worthwhile to carry out further investigation on this topic as there are not many results in the literature that consider graphs with four distinct eigenvalues compared to results on graphs with three distinct eigenvalues (either regular or nonregular). A closer look at connected

regular graphs with four distinct eigenvalues is taken in [**4**], where some properties, constructions and examples are given. Another possible and challenging direction in research would be the classification of all strongly (distant) regular circulant graphs, respectively, using only techniques from spectral graph theory. More precisely, we wonder if this could be done using tools from combinatorics, polynomial and number theory without any help of abstract algebra? Some preliminary results show that number-theoretic tools such as quadratic residues might be promising line of research in strong regularity of circulant. Namely, it seems that the following can be proven: any two eigenvalues λ_i and λ_j are equal, for $0 \leq i, j \leq n-1$, if and only if i and j are either both quadratic residues or both quadratic nonresidues modulo n, for any circulant of the prime order n.

REFERENCES

1. M. Bašić: *Which weighted circulant networks have perfect state transfer?.* Inf. Sciences, **257** (2014), 193–209.
2. D. Cvetkovic, M. Doob, H. Sachs: *Spectra of Graphs: Theory and Application.* Academic Press, New York, 1980.
3. T. T. Chelvam, S. Raja, I. Gutman: *Strongly regular integral circulant graphs and their enegies.* Bull. Inter. Math. Virtual Inst., **2** (2012), 9–16.
4. E. R. van Dam: *Regular Graphs With Four Eigenvalues.* Linear Algebra Appl., **226–228** (1995), 139–162.
5. P. J. Davis: *Circulant Matrices.* Wiley, New York, 1970.
6. C. Godsil, G. Royle: *Algebraic graph theory.* Springer-Verlag, New York, 2001.
7. G.H. Hardy, E.M. Wright, D.R. Heath-Brown, J.H. Silverman: *An introduction to the Theory of Numbers.* 6th ed, Oxford University Press, 2008.
8. F.K. Hwang: *A survey on multi-loop networks.* Theor Comput Sci., **299** (2003), 107–121.
9. S.L. Ma: *Partial difference sets.* Discrete Math., **52** (1984), 75–89.
10. S.L. Ma: *A survey of partial difference sets.* Des. Codes Cryptogr., **4** (1994), 221–261.
11. D. Marušič: *Strong regularity and circulant graphs.* Discrete Math., **78** (1989), 119–125.
12. Š. Miklavič, P. Potočnik: *Distance-regular circulants.* Eur J Comb., **24** (2003), 777–784.
13. N. Saxena, S. Severini, I. Shparlinski: *Parameters of integral circulant graphs and periodic quantum dynamics.* Int. J. Quantum Inf., **5** (2007), 417–430.
14. W. So: *Integral circulant graphs.* Discrete Math., **306** (2006), 153–158.

Milan Bašić
Faculty of Sciences and Mathematics,
Department of Computer Science
University of Niš,
Niš, Serbia
E-mail: *basic_milan@yahoo.com; milan.basic@pmf.edu.rs*

(Received 13. 07. 2018.)
(Revised 23. 08. 2022.)