Rotation Symmetries of Sequential Matrices with Applications to the Jacobi Symbol

Y. Ayub and C.L. Samuels

Abstract - Suppose that p is an odd prime and $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo p. If p is has the form $p = n^2 + 1$ then one easily verifies that $\left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right)$ for all $a \in \mathbb{Z}/p\mathbb{Z}$. We identify various symmetry properties of sequential matrices over $\mathbb{Z}/(n^2+1)\mathbb{Z}$ regardless of whether n^2+1 is prime. We deduce from these results a collection of symmetries involving the Jacobi symbol modulo n^2+1 which generalize our above observation on the Legendre symbol.

Keywords : sequential matrices; completely multiplicative functions; quadratic reciprocity; Legendre symbol; Jacobi symbol

Mathematics Subject Classification (2010) **:** 11A05; 11A15; 20B30

1 Introduction

If n is a positive integer then the $n \times n$ *sequential matrix* is the unique $n \times n$ matrix over $\mathbb{Z}$ belonging to the list

$$\begin{pmatrix}1\end{pmatrix}, \quad \begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix}, \quad \begin{pmatrix}1 & 2 & 3 & 4\\ 5 & 6 & 7 & 8\\ 9 & 10 & 11 & 12\\ 13 & 14 & 15 & 16\end{pmatrix}, \ \ldots$$

We will write Q_n to denote the $n \times n$ sequential matrix. For any set Ω we shall write $M_{n\times n}(\Omega)$ to denote the set of all $n \times n$ matrices with entries in Ω. Further, if $A \in M_{n\times n}(\Omega)$ we let $A_{i,j}$ denote the entry of A in row i and column j.

Following this notation, we obtain the formula

$$(Q_n)_{i,j} = j + (i-1)n \tag{1}$$

for all $1 \leq i, j \leq n$. As will be common practice throughout this article, we let $m = n^2+1$ and interpret Q_n as a matrix over $\mathbb{Z}/m\mathbb{Z}$. As such, any time we perform arithmetic with Q_n, that arithmetic will be assumed to take place in $\mathbb{Z}/m\mathbb{Z}$.

A function $\varphi : \mathbb{Z}/m\mathbb{Z} \to \{0, 1, -1\}$ is called *completely multiplicative* if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in \mathbb{Z}/m\mathbb{Z}$. Examples of such functions are common objects of study in number theory. For instance, if p is prime then the *Legendre symbol* $\left(\frac{\cdot}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a perfect square in } (\mathbb{Z}/p\mathbb{Z})^\times \\ -1 & \text{if } a \text{ is not a perfect square in } (\mathbb{Z}/p\mathbb{Z})^\times, \end{cases}$$

and it is well-known that $a \mapsto \left(\frac{a}{p}\right)$ defines a completely multiplicative function on $\mathbb{Z}/p\mathbb{Z}$.

If Ω' is another set and $f : \Omega \to \Omega'$ is any map, then for each $A \in M_{n\times n}(\Omega)$ we shall define $f(A)$ so that $f(A)_{i,j} = f(A_{i,j})$. The goal of this article is to study the symmetry properties of $\varphi(Q_n)$ for multiplicative functions φ. In the next section, we shall present our main results concerning those symmetry properties. Our work requires identifying a certain group which is isomorphic to the dihedral group of eight elements. In Section 3, we apply our main results to the Jacobi symbol, a generalization of the Legendre symbol defined above.

2 Main Results

For this section, we shall fix $n \in \mathbb{Z}$ with $n \geq 2$ and let $m = n^2 + 1$. Many objects we define depend on n, however, in order to prevent our notation from becoming excessively cumbersome, we shall often suppress that dependency in our notation.

As noted in the introduction, our goal is to study symmetry properties of $\varphi(Q_n)$ when φ is a completely multiplicative function. In order to make that agenda more precise, we let

$$X = \{(i,j) : 1 \leq i \leq n,\ 1 \leq j \leq n\}$$

and define two maps $\tau, \rho : X \to X$ by

$$\tau(i,j) = (j,i) \quad \text{and} \quad \rho(i,j) = (j, n-i+1). \tag{2}$$

One easily verifies that τ and ρ are both bijections, and therefore, each defines an element of the group S_X of permutations of X. In this interpretation, τ has order 2 while ρ has order 4 in S_X. In fact, we obtain the following important observation.

Theorem 2.1 *If τ and ρ are given as in (2) then $\{1, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\}$ forms a subgroup of S_X which is isomorphic to the dihedral group of eight elements.*

Proof. Let $D = \{1, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\}$ and note that τ clearly has order 2 in S_X. Additionally, we find that

$$\rho^2(i,j) = \rho(j, n-i+1) = (n-i+1, n-j+1) \tag{3}$$

which implies that

$$\rho^4(i,j) = \rho^2(n-i+1, n-j+1) = (n-(n-i+1)+1, n-(n-j+1)+1) = (i,j).$$

Clearly (3) does not define the identity map, so ρ must have order 4 in S_X. Next, we note that

$$\tau\rho(i,j) = \tau(j, n-i+1) = (n-i+1, j)$$

and also that

$$\rho^3\tau(i,j) = \rho^3(j,i) = \rho^2(i, n-j+1) = (n-i+1, n-(n-j+1)+1) = (n-i+1, j).$$

We have now established that $\tau\rho = \rho^3\tau$. Combining this observation with the fact that τ has order 2 and ρ has order 4, we obtain quickly that D is closed under function composition. Further observing that $\rho^{-1} = \rho^3$ while all other elements of D are their own inverses in S_X, we have established that D is a subgroup of S_X.

Certainly D is a non-Abelian group of order 8, so it must be isomorphic to the dihedral group or the quaternion group. It cannot be latter as the quaternion group has 6 elements of order 4 while D only has 2. □

We shall now write D_X for the subgroup of S_X described in Theorem 2.1. For any set Ω, there is a useful action of D_X on $M_{n\times n}(\Omega)$ given by

$$\sigma(A)_{i,j} = A_{\sigma(i,j)}.$$

This means, in particular, that

$$\tau(A)_{i,j} = A_{j,i} \quad \text{and} \quad \rho(A)_{i,j} = A_{j,n-i+1}. \tag{4}$$

Clearly $\tau(A) = A^T$ so that τ flips a matrix across its main diagonal. Although it is less obvious from (4), a brief examination reveals that ρ rotates a matrix counter-clockwise by 90°. For example, if $n = 2$ then

$$\rho\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix}.$$

Along with our knowledge that $\tau(A) = A^T$, we find that $\tau\rho$ flips a matrix across its vertical center line as in the example

$$\tau\rho\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}.$$

All elements of D_X can be described in a similar way:

Element $\sigma \in D_X$	Description of $\sigma(A)$
1	Identity Map
ρ	90° counter-clockwise rotation
ρ^2	180° counter-clockwise rotation
ρ^3	270° counter-clockwise rotation
τ	Flip across the main diagonal
$\tau\rho$	Flip across the vertical center line
$\tau\rho^2$	Flip across the cross diagonal
$\tau\rho^3$	Flip across the horizontal center line

A matrix fixed by some element of D_X is often considered to have a symmetry property. For example, in classical linear algebra, students are taught that A is called *symmetric* if $\tau(A) = A$. Additionally, A is called *centro-symmetric* if $\rho^2(A) = A$ and *Hankel-symmetric* if $\tau\rho^2(A) = A$. Such symmetries have been studied extensively in various contexts (see [1–4], for example). In the case of the $n \times n$ sequential matrix, our main result asserts that the rotation maps can be described by some simple arithmetic in $\mathbb{Z}/m\mathbb{Z}$.

Theorem 2.2 *If n is a positive integer and $m = n^2 + 1$ then $\rho(Q_n) = nQ_n$.*

Proof. Let i and j be integers such that $1 \leq i, j \leq n$. According to (4) and (1), we find that

$$\rho(Q_n)_{i,j} = (Q_n)_{j,n-i+1} = n - i + 1 + (j-1)n = -i + 1 + jn = jn + (i-1)(-1).$$

We also know that $n^2 \equiv -1 \mod m$, so in $\mathbb{Z}/m\mathbb{Z}$ we have that

$$\rho(Q_n)_{i,j} = jn + (i-1)n^2 = n(j + (i-1)n) = n(Q_n)_{i,j} = (nQ_n)_{i,j}.$$

This equality holds for all $1 \leq i, j \leq n$ so that $\rho(Q_n) = nQ_n$ as required. □

Certainly we have that $n^2 \equiv -1 \mod m$. Furthermore, multiplication by n commutes with all elements of D_X, and hence, we obtain the following list of values of $\sigma(Q_n)$ for all non-identity elements $\sigma \in D_X$.

$$\rho(Q_n) = nQ_n, \quad \rho^2(Q_n) = -Q_n, \quad \rho^3(Q_n) = -nQ_n$$

$$\tau(Q_n) = Q_n^T, \quad \tau\rho(Q_n) = nQ_n^T, \quad \tau\rho^2(Q_n) = -Q_n^T, \quad \tau\rho^3(Q_n) = -nQ_n^T.$$

As we noted above, our plan is to study the symmetry properties of $\varphi(Q_n)$, where $\varphi : \mathbb{Z}/m\mathbb{Z} \to \{0, 1, -1\}$ is a completely multiplicative function. Thanks to Theorem 2.2, we obtain a corollary which addresses this issue in relation to the rotation maps.

Corollary 2.3 *Suppose that n is a positive integer and $m = n^2 + 1$. If $\varphi : \mathbb{Z}/m\mathbb{Z} \to \{0, 1, -1\}$ is a completely multiplicative function then $\varphi(\rho(Q_n)) = \varphi(n)\varphi(Q_n)$.*

It is worth noting that the expression $\sigma(\varphi(A))$ makes sense for all $\sigma \in D_X$ and all $A \in M_{n\times n}(\mathbb{Z}/m\mathbb{Z})$, and moreover, $\sigma(\varphi(A)) = \varphi(\sigma(A))$. As a result, we may interpret Corollary 2.3 as a statement about symmetry properties of $\varphi(Q_n)$. These observations also enable us to deduce information about $\varphi(\sigma(Q_n))$ for other points $\sigma \in D_X$. For instance, we find that

$$\varphi(\rho^2(Q_n)) = \varphi(-1)\varphi(Q_n) \quad \text{and} \quad \varphi(\rho^3(Q_n)) = \varphi(-1)\varphi(n)\varphi(Q_n).$$

These assertions could also be concluded directly from Theorem 2.2 in conjunction with our above list of values of $\sigma(Q_n)$.

3 The Jacobi Symbol

If p is an odd prime and $a \in \mathbb{Z}$ recall that the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined so that

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a perfect square in } (\mathbb{Z}/p\mathbb{Z})^\times \\ -1 & \text{if } a \text{ is not a perfect square in } (\mathbb{Z}/p\mathbb{Z})^\times. \end{cases}$$

Certainly $a \mapsto \left(\frac{a}{p}\right)$ is well-defined on $\mathbb{Z}/p\mathbb{Z}$, and moreover, this map defines a completely multiplicative function. That is, for all $a, b \in \mathbb{Z}/p\mathbb{Z}$ we have that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

For each odd integer $m > 2$, write

$$m = \prod_{k=1}^{K} p_k$$

for its factorization into (not necessarily distinct) primes. If $a \in \mathbb{Z}$ we define the *Jacobi symbol* $\left(\frac{a}{m}\right)$ by

$$\left(\frac{a}{m}\right) = \prod_{k=1}^{K} \left(\frac{a}{p_k}\right).$$

Like the Legendre symbol that it generalizes, the Jacobi symbol is a completely multiplicative function which is well-defined on $\mathbb{Z}/m\mathbb{Z}$. For the purposes of applying Corollary 2.3, we are particularly interested in the case where $m = n^2 + 1$ for some positive even integer n. If A is a matrix with entries in $\mathbb{Z}/m\mathbb{Z}$ then we shall write $\left(\frac{A}{m}\right)$ for the matrix obtained by applying the Jacobi symbol to each entry.

Theorem 3.1 *If n is a positive even integer and $m = n^2+1$ then*

$$\left(\frac{\rho(Q_n)}{m}\right) = \begin{cases} \left(\frac{Q_n}{m}\right) & \textit{if } n \equiv 0 \mod 4 \\ -\left(\frac{Q_n}{m}\right) & \textit{if } n \equiv 2 \mod 4. \end{cases} \tag{5}$$

Proof. Define the map $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by $f(a) = na$, and since n is relatively prime to m, we note that f is a permutation of $\mathbb{Z}/m\mathbb{Z}$. Then according to Zolotarev's Lemma [5], we have

$$\left(\frac{n}{m}\right) = \operatorname{sgn}(f), \tag{6}$$

where $\operatorname{sgn}(f)$ denotes the signature of f, i.e., $\operatorname{sgn}(f) = 1$ if f is an even permutation and $\operatorname{sgn}(f) = -1$ if f is an odd permutation.

By Theorem 2.2, applying f to each entry of Q_n performs a rotation of Q_n counterclockwise by 90°. Therefore, every non-zero element $a \in \mathbb{Z}/m\mathbb{Z}$ satisfies $f^4(a) = a$. Moreover, since n is even, there is no center entry of Q_n, which implies that $f^k(a) \neq a$ for all $0 < k < 4$. In view of these observations, when we represent f as a product of disjoint cycles, f is a product of $n^2/4$ cycles of length four and (0). We know that $\operatorname{sgn}((0)) = 1$, and for every cycle g of length four, we have that $\operatorname{sgn}(g) = -1$. It now follows that $\operatorname{sgn}(f) = (-1)^{n^2/4}$ and we conclude from (6) that

$$\left(\frac{n}{m}\right) = (-1)^{n^2/4}. \tag{7}$$

By applying Corollary 2.3 with the Jacobi symbol in place of φ and utilizing (7), we immediately obtain that

$$\left(\frac{\rho(Q_n)}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{Q_n}{m}\right) = (-1)^{n^2/4}\left(\frac{Q_n}{m}\right). \tag{8}$$

If $n \equiv 0 \mod 4$ then $n^2/4$ is even and $(-1)^{n^2/4} = 1$. Otherwise, $n \equiv 2 \mod 4$ and n has the form $n = 4k+2$ for some $k \in \mathbb{Z}$. This observation yields

$$\frac{n^2}{4} = \frac{(4k+2)^2}{4} = \frac{16k^2+16k+4}{4} = 4k^2+4k+1$$

which is certainly odd meaning that $(-1)^{n^2/4} = -1$. The result now follows from (8). □

We note that Theorem 3.1 excludes the case where n is odd as the Jacobi symbol is undefined for that case. More importantly, Theorem 3.1 generalizes a well-known fact about the symmetry properties of the Jacobi symbol. Under the assumptions of Theorem 3.1, -1 is certainly a square modulo m, and therefore, -1 is a square modulo every prime which divides m. We conclude that $\left(\frac{-1}{m}\right) = 1$ and

$$\left(\frac{a}{m}\right) = \left(\frac{-a}{m}\right) \quad \text{for all } a \in \mathbb{Z}/m\mathbb{Z}. \tag{9}$$

By applying Theorem 3.1 twice, we can deduce (9) in another way. Indeed, it follows from Theorem 3.1 that

$$\left(\frac{\rho^2(Q_n)}{m}\right) = \left(\frac{Q_n}{m}\right),$$

which is equivalent to the assertion that $\left(\frac{Q_n}{m}\right)$ is centro-symmetric. Now we immediately obtain (9). In view of these observations, we may interpret Theorem 3.1 as an improvement to the well-known fact (9).

As a basic example of Theorem 3.1, consider the case where $n = 4$ so that $m = 17$ and we are in the situation of the first line of (5). After applying the Jacobi symbol to the 4×4 sequential matrix, as predicted by Theorem 3.1, we obtain a matrix which is fixed under all rotations.

$$\left(\frac{Q_4}{17}\right) = \begin{pmatrix} +1 & +1 & -1 & +1 \\ -1 & -1 & -1 & +1 \\ +1 & -1 & -1 & -1 \\ +1 & -1 & +1 & +1 \end{pmatrix}$$

Of course, Theorem 3.1 also applies in cases where m is not prime or where $n \equiv 2 \mod 4$. For $n = 6$ we obtain the matrix

$$\left(\frac{Q_6}{37}\right) = \begin{pmatrix} +1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & +1 & +1 & +1 & +1 \\ -1 & -1 & -1 & +1 & -1 & -1 \\ -1 & -1 & +1 & -1 & -1 & -1 \\ +1 & +1 & +1 & +1 & -1 & +1 \\ -1 & -1 & +1 & +1 & -1 & +1 \end{pmatrix}$$

This matrix is not preserved under a 90° counter-clockwise rotation, but rather the sign is flipped after performing a 90° counter-clockwise rotation. This is exactly as predicted by Theorem 3.1. When $n = 8$ we get

$$\left(\frac{Q_8}{65}\right) = \begin{pmatrix} +1 & +1 & -1 & +1 & 0 & -1 & +1 & +1 \\ +1 & 0 & -1 & -1 & 0 & +1 & 0 & +1 \\ -1 & +1 & -1 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & -1 & +1 & +1 & 0 & -1 & +1 \\ +1 & -1 & 0 & +1 & +1 & -1 & 0 & 0 \\ -1 & -1 & -1 & -1 & 0 & -1 & +1 & -1 \\ +1 & 0 & +1 & 0 & -1 & -1 & 0 & +1 \\ +1 & +1 & -1 & 0 & +1 & -1 & +1 & +1 \end{pmatrix}$$

In this case, some entries are equal to 0 due to the fact that the corresponding elements of $\mathbb{Z}/65\mathbb{Z}$ are not relatively prime to 65.

References

[1] I.T. Abu-Jeib, Centrosymmetric matrices: properties and an alternative approach, *Can. Appl. Math. Q.*, **10** (2002), 429–445.

[2] I.T. Abu-Jeib, Centrosymmetric and skew-centrosymmetric matrices and regular magic squares, *New Zealand J. Math.*, **33** (2004), 105–112.

[3] R.A. Brualdi and S.-M. Ma, Centrosymmetric, symmetric and Hankel-symmetric matrices, in *Mathematics across contemporary sciences*, volume 190 of *Springer Proc. Math. Stat.*, pages 17–31. Springer, Cham, 2017.

[4] F. Yilmaz, T. Sogabe, E. Kirklar, On the Pfaffians and determinants of some skew-centrosymmetric matrices, *J. Integer Seq.*, **20** (2017), Art. 17.4.6, 9.

[5] G. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouv. Ann. Math*, **11** (1872), 354–362. Also available online at the URL: `http://www.numdam.org/item/NAM_1872_2_11__354_0/`

Yemeen Ayub
George Mason University
4400 University Drive
Fairfax, VA 22030
E-mail: `yayub@gmu.edu`

Charles L. Samuels
Christopher Newport University
1 Avenue of the Arts
Newport News, VA 23606
E-mail: `charles.samuels@cnu.edu`

Received: April 9, 2019 **Accepted**: May 23, 2019
Communicated by Kevin J. McGown