Rotational Symmetries of Sequential Matrices

Yemeen Ayub and Charles L. Samuels

Legendre Symbol

Definition

An integer q is called a quadratic residue modulo n if it satisfies $x^2 \equiv q \pmod{n}$ where $x, n \in \mathbb{Z}$.

Definition

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

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

Legendre Symbol

a	$\left(\frac{a}{5}\right)$	$\left(\frac{a}{7}\right)$	$\left(\frac{a}{11}\right)$	$\left(\frac{a}{13}\right)$
1	+	+	+	+
2	-	+	-	-
3	-	-	+	+
4	+	+	+	+
5	0	-	+	+
6	+	-	-	-
7	-	0	-	-
8	-	+	-	-
9	+	+	+	+
10	0	-	-	+
11	+	+	0	-
12	-	-	+	+

Legendre Symbol

1. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$
2. If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
5. $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$
6. $\left(\frac{a}{p}\right) = sgn(f)$ where $f(x) = ax$ for $a, x \in (\mathbb{Z}/p\mathbb{Z})^\times$

Sequential Matrices

Definition

Suppose n is a positive integer and $m = n^2 + 1$, then the $n \times n$ matrix $A = (a_{i,j})$ is called sequential if $a_{i,j} = j + (i - 1)n$ where $a_{i,j} \in \mathbb{Z}/m\mathbb{Z}$

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

Sequential Matrices

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \xrightarrow{(\frac{\cdot}{5})} \begin{bmatrix} + & - \\ - & + \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix} \xrightarrow{(\frac{\cdot}{17})} \begin{bmatrix} + & + & - & + \\ - & - & - & + \\ + & - & - & - \\ + & - & + & + \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \\ 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 \end{bmatrix} \xrightarrow{(\frac{\cdot}{37})} \begin{bmatrix} + & - & + & + & - & - \\ + & - & + & + & + & + \\ - & - & - & + & - & - \\ - & - & + & - & - & - \\ + & + & + & + & - & + \\ - & - & + & + & - & + \end{bmatrix}$$

Exchange Matrix

$$J_n = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 1 & \ldots & 0 & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 & 0 \end{bmatrix}$$

- $J^T = J$
- $J^2 = I$
- $JA = \forall$
- $AJ = \mathrm{A}$

Matrix Symmetries

$\sigma \in D_4(n)$	Value of $\sigma(A)$	Description of $\sigma(A)$
1	A	Identity Map
ρ	$A^T J$	90° clockwise rotation
ρ^2	JAJ	180° clockwise rotation
ρ^3	JA^T	270° clockwise rotation
τ	A^T	Flip across the main diagonal
$\tau\rho$	JA	Flip across the horizontal center line
$\tau\rho^2$	$JA^T J$	Flip across the off diagonal
$\tau\rho^3$	AJ	Flip across the vertical center line

Rotosymmetry

Theorem

If $p = n^2 + 1$ is a prime and Q_n denotes the $n \times n$ sequential matrix, then

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

Rotosymmetry

Lemma

If Q_n denotes the $n \times n$ sequential matrix, then

$$\rho(Q_n) = Q_n^T J = nQ_n$$

Proof.

Let $Q_n = (a_{i,j})$, then because $\rho(Q_n) = a_{j,n-i+1}$, we have

$$a_{j,n-i+1} = n-i+1+(j-1)n = -i+1+jn = jn+(i-1)(-1) = na_{i,j}$$

□

Rotosymmetry

Lemma

If $p = n^2 + 1$ is a prime, then

$$\left(\frac{n}{p}\right) = (-1)^{n^2/4}$$

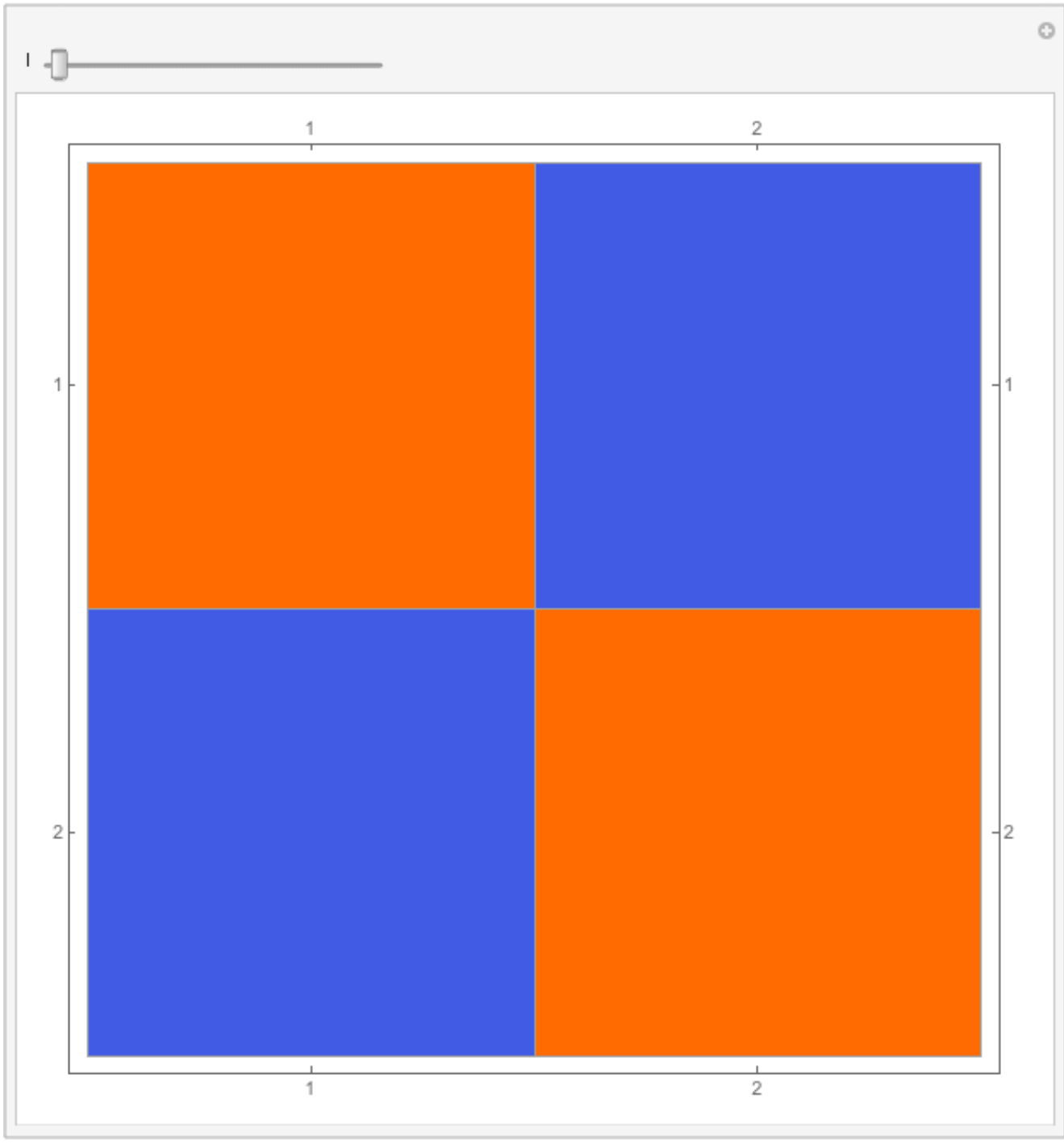
Rotosymmetry

Proof.

$$\left(\frac{\rho(Q_n)}{p}\right) = \left(\frac{nQ_n}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{Q_n}{p}\right) = (-1)^{n^2/4}\left(\frac{Q_n}{p}\right)$$

$$\implies \rho(Q_n) = \begin{cases} \left(\frac{Q_n}{p}\right) & \text{if } n \equiv 0 \mod 4 \\ -\left(\frac{Q_n}{p}\right) & \text{if } n \equiv 2 \mod 4. \end{cases}$$

□


1
2
1
2
1
2
1
2

Jacobi Symbol

Definition

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

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

Jacobi Symbol

1. If $a \equiv b \pmod{m}$, then $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$
2. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
4. If m and n are distinct odd positive and coprime, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$
5. $\left(\frac{-1}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod{4} \\ -1 & \text{if } m \equiv 3 \pmod{4} \end{cases}$

Completely Multiplicative Functions

Theorem

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 $\varphi(\rho(Q_n)) = \varphi(n)\varphi(Q_n)$.

Future Work

- What happens when you change the sequence in the sequential matrix?
- What about cubic residues and quartic residues?
- How do these rotosymmetric matrices behave?
- What are some applications of the rotation operation?
- What are some connections with Hadamard matrices?

Thank you for attending!