# Characterizations of Quadratic, Cubic, and Quartic Residue Matrices

Evan P. Dummit

University of Rochester

AMS Contributed Paper Session in Number Theory

Joint Mathematics Meetings

January 4, 2017

# Outline

Goals of talk:

1. Describe the construction of "quadratic residue matrices" and give a simple characterization of such matrices.
2. Generalize construction and characterization results to "cubic" and "quartic" residue matrices.
3. Mention generalization to function-field case.

These results are partly joint work with D. Dummit and H. Kisilevsky.

# Quadratic Residue Configurations

Recall: for $p$ is an odd prime, the quadratic residue symbol is defined as $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \text{ is divisible by } p \\ +1 & \text{if } a \text{ is a nonzero square mod } p \\ -1 & \text{if } a \text{ is a nonsquare mod } p \end{cases}$.

**Question 1**

*Suppose that $p_1, p_2, \ldots, p_n$ are distinct odd primes. What possibilities are there for the collection of $n^2$ quadratic residue symbols $\left(\frac{p_i}{p_j}\right)$ for $1 \leq i, j \leq n$?*

This question originally arose in the context of studying "splitting configurations" of minimally tamely ramified multiquadratic extensions in algebraic number theory.

# Sign Matrices and Quadratic Residue Matrices

We have $n^2$ pieces of data: let's put them into a matrix!

**Definition**

*The quadratic residue matrix associated to the distinct odd primes $p_1, p_2, \ldots, p_n$ is the $n \times n$ matrix $M_{i,j}$ whose $(i,j)$-entry is $\left(\frac{p_i}{p_j}\right)$.*

These matrices all have a particular form:

**Definition**

*A sign matrix is a matrix with entries of 0 on the diagonal and $\pm 1$ off the diagonal.*

By definition, every quadratic residue matrix is a sign matrix.

# Quadratic Residue Matrices, I

**Example**

*For the primes* $p_1 = 3$, $p_2 = 7$, *and* $p_3 = 13$, *the associated quadratic residue matrix is*

$$M = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$

Natural questions:

- Is there a nice way to tell if a given sign matrix is a quadratic residue matrix for some set of primes?
- How many quadratic residue matrices are there?

# Quadratic Residue Matrices, II

Can make a few simple observations:

- Classes of sign matrices and quadratic residue matrices are invariant under conjugation by permutation matrices.
- Quadratic reciprocity clearly imposes some conditions. Can neatly deal with them if we rearrange the primes first.

# Quadratic Residue Matrices, II

Can make a few simple observations:

- Classes of sign matrices and quadratic residue matrices are invariant under conjugation by permutation matrices.
- Quadratic reciprocity clearly imposes some conditions. Can neatly deal with them if we rearrange the primes first.
- So: order $p_1, \ldots, p_n$ so that the first $s$ are 3 mod 4 and the remaining $n - s$ are 1 mod 4.
- Then the associated quadratic residue matrix has the form $\begin{pmatrix} A & B \\ B^t & S \end{pmatrix}$ where $A$ is an $s \times s$ skew-symmetric sign matrix, $S$ is an $(n-s) \times (n-s)$ symmetric sign matrix, and $B$ is an $s \times (n-s)$ matrix of entries $\pm 1$.

# Characterization of Quadratic Residue Matrices

**Theorem 2 (D. Dummit, E.D., Kisilevsky)**

*If $M$ is an $n \times n$ sign matrix, the following are equivalent:*

1. *There exists an integer $1 \leq s \leq n$ such that $M$ can be conjugated by a permutation matrix into the form $\begin{pmatrix} A & B \\ B^t & S \end{pmatrix}$ where $A$ is an $s \times s$ skew-symmetric sign matrix, $S$ is an $(n-s) \times (n-s)$ symmetric sign matrix, and $B$ is an $s \times (n-s)$ matrix of entries $\pm 1$.*
2. *The matrix $M$ is a quadratic residue matrix associated to some set of distinct odd primes.*
3. *There exists an integer $s$ with $1 \leq s \leq n$ such that the diagonal entries of $M^2$ consist of $s$ occurrences of $n + 1 - 2s$ and $n - s$ occurrences of $n - 1$.*

# Identifying Quadratic Residue Matrices

Using criterion (c) of Theorem 2, we can easily check whether a given matrix is a QR matrix:

**Example**

*For* $M = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}$*, the diagonal entries of* $M^2$ *are* $0$*,* $0$*,* $-2$*, so this matrix is not a quadratic residue matrix as it fails condition (3).*

What about counting? Results do not seem to give an immediate counting method.

# Counting Quadratic Residue Matrices

Here are some numbers:

| $n$ | $QR$ classes | $QR$ matrices | Sign matrices $(= 2^{n(n-1)})$ |
|---|---|---|---|
| 2 | 3 | 4 | 4 |
| 3 | 10 | 40 | 64 |
| 4 | 47 | 768 | 4096 |
| 5 | 314 | 27648 | 1048576 |
| 6 | 3360 | 1900544 | 1073741824 |
| 7 | 59744 | 253755392 | 4398046511104 |

# Counting Quadratic Residue Matrices

Here are some numbers:

| $n$ | $QR$ classes | $QR$ matrices | Sign matrices ($= 2^{n(n-1)}$) |
|---|---|---|---|
| 2 | 3 | 4 | 4 |
| 3 | 10 | 40 | 64 |
| 4 | 47 | 768 | 4096 |
| 5 | 314 | 27648 | 1048576 |
| 6 | 3360 | 1900544 | 1073741824 |
| 7 | 59744 | 253755392 | 4398046511104 |

**Theorem 3 (E.D.)**

*There are precisely $(2^n - n)2^{n(n-1)/2}$ quadratic residue matrices among the $n \times n$ sign matrices.*

# Generalizations to Higher Degree

Natural generalization: use $m$th power residue symbols over a ground field containing the $m$th roots of unity.

**Definition**

*A cyclotomic sign matrix of mth roots of unity is a matrix with entries of 0 on the diagonal and mth roots of unity off the diagonal.*

We will consider the cases $m = 3$ and $m = 4$, of cubic and quartic sign matrices over $\mathbb{Q}$. For $m > 4$, things appear to become more difficult (primarily, though not exclusively, because the ideals in $\mathbb{Z}(\zeta_m)$ are no longer always principal).

# Cubic Residue Matrices

## Definition

*The cubic residue matrix associated to the distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ not dividing 3 of $\mathbb{Q}(\sqrt{-3})$ is the $n \times n$ matrix $M_{i,j}$ whose $(i,j)$-entry is the cubic residue symbol $\left(\frac{\pi_i}{\pi_j}\right)_3$, where $\pi_k$ is the unique 3-primary generator for $\mathfrak{p}_k$ for $1 \leq k \leq n$.*

# Cubic Residue Matrices

**Definition**

*The cubic residue matrix associated to the distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ not dividing 3 of $\mathbb{Q}(\sqrt{-3})$ is the $n \times n$ matrix $M_{i,j}$ whose $(i,j)$-entry is the cubic residue symbol $\left(\frac{\pi_i}{\pi_j}\right)_3$, where $\pi_k$ is the unique 3-primary generator for $\mathfrak{p}_k$ for $1 \leq k \leq n$.*

Cubic reciprocity is symmetric, so the analogue of our theorem ends up being much simpler in this case:

**Theorem 4 (D. Dummit, E.D., Kisilevsky)**

*A cubic sign matrix is a cubic residue matrix if and only if it is symmetric.*

# Quartic Residue Matrices

The quartic residue matrices have a similar construction to the cubic residue matrices:

**Definition**

*The quartic residue matrix associated to the distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ not dividing 2 of $\mathbb{Q}(i)$ is the $n \times n$ matrix $M_{i,j}$ whose $(i,j)$-entry is the quartic residue symbol $\left(\frac{\pi_i}{\pi_j}\right)_4$, where $\pi_k$ is the unique 2-primary generator for $\mathfrak{p}_k$ for $1 \leq k \leq n$.*

Quartic reciprocity has a similar flavor to quadratic reciprocity, and the analogue of our theorem has a similar statement.

# Characterization of Quartic Residue Matrices

**Theorem 5 (D. Dummit, E.D., Kisilevsky)**

*If $M$ is an $n \times n$ quartic sign matrix, the following are equivalent:*

1. *There exists an integer $1 \leq s \leq n$ such that $M$ can be conjugated by a permutation matrix into the form $\begin{pmatrix} A & B \\ B^t & S \end{pmatrix}$ where $A$ is an $s \times s$ skew-symmetric quartic sign matrix, $S$ is an $(n-s) \times (n-s)$ symmetric quartic sign matrix, and $B$ is an $s \times (n-s)$ matrix of entries $\pm 1, \pm i$.*
2. *The matrix $M$ is a quartic residue matrix.*
3. *If $M = (m_{j,k})$, then $m_{j,k} = \pm m_{k,j}$ for all $j, k$ with $1 \leq j, k \leq n$, and there exists an integer $s$ with $1 \leq s \leq n$ such that the diagonal entries of $M\overline{M}$ consist of $s$ occurrences of $n + 1 - 2s$ and $n - s$ occurrences of $n - 1$.*

# The Function-Field Case

The $d$th power residue symbol also makes sense over function fields, and we can pose similar questions in that setting.

Briefly: let $q$ be a prime power and $d$ be a positive integer with $d$ dividing $q-1$, let $\mathbb{F}_q$ denote the finite field with $q$ elements, and let $\left(\frac{a}{P}\right)_d$ be the $d$th-power residue symbol over $\mathbb{F}_q[t]$.

## Definition

*The <u>$d$th-power residue matrix</u> associated to the monic irreducible polynomials $P_1, P_2, \ldots, P_n$ in $\mathbb{F}_q[t]$ is the $n \times n$ matrix whose $(i,j)$-entry is the $d$th power residue symbol $\left(\frac{P_i}{P_j}\right)_d$.*

Each $d$th-power residue matrix is a "cyclotomic sign matrix of $d$th roots of unity": an $n \times n$ matrix whose diagonal entries are all 0 and whose off-diagonal entries are all complex $d$th roots of unity.

# The Function-Field Case, II

We can give a characterization of which $n \times n$ cyclotomic sign matrices are $d$th-power residue matrices:

**Theorem 6 (E.D.)**

*If $(q-1)/d$ is even, then $M$ is a $d$th-power residue matrix if and only if $M$ is symmetric.*

**Theorem 7 (E.D.)**

*If $(q-1)/d$ is odd, then $M$ is a $d$th-power residue matrix if and only if $M$ can be conjugated by a permutation matrix into the form $\begin{pmatrix} A & B \\ B^t & S \end{pmatrix}$ where $A$ is an $s \times s$ skew-symmetric cyclotomic sign matrix, $S$ is an $(n-s) \times (n-s)$ symmetric cyclotomic sign matrix, and $B$ is an $s \times (n-s)$ matrix of $d$th roots of unity.*

# Further Avenues

Here are a few things that remain unresolved:

- What happens if we allow non-primary generators of ideals? (This would expand the class of possible matrices when $m > 2$: for example we can get non-symmetric matrices in the $m = 3$ case.)
- Can the results in the number-field case be extended in a pleasant way for $m > 4$, or over larger ground fields?
- What if we try using composites of other types of minimally tamely ramified extensions? Are there equally simple objects (like the residue matrices) attached to these extensions that capture number-theoretic information?
- Are there any combinatorial applications of the quadratic residue matrices?

# End

Thank you for attending my talk!