Characterizations of Quadratic, Cubic, and Quartic Residue Matrices

Evan P. Dummit

University of Rochester

April 30, 2016

Outline

Outline of talk:

1. Discuss an unusual bias in prime-counting observed by D. Dummit, Granville, Kisilevsky.
2. Motivate the construction of "quadratic residue matrices" and state a simple characterization of such matrices.
3. Generalize construction and characterization results to cubic and quartic residue matrices.

This is joint work with D. Dummit and Kisilevsky.

Prime Biases, I

Consider the set of all odd integers $n < x$ that are the product of two primes $n = pq$.

- Natural expectation: Approximately equally many n have $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 4$.

Prime Biases, I

Consider the set of all odd integers $n < x$ that are the product of two primes $n = pq$.

- Natural expectation: Approximately equally many n have $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 4$.
- This is true: assuming the appropriate version of GRH, difference is $x^{1/2+o(1)}$.
- Equally reasonable expectation: also get an even split among the 4 possible pairs $(p, q) \equiv (1, 1), (1, 3), (3, 1), (3, 3) \bmod 4$.

Prime Biases, I

Consider the set of all odd integers $n < x$ that are the product of two primes $n = pq$.

- Natural expectation: Approximately equally many n have $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 4$.
- This is true: assuming the appropriate version of GRH, difference is $x^{1/2+o(1)}$.
- Equally reasonable expectation: also get an even split among the 4 possible pairs $(p, q) \equiv (1, 1), (1, 3), (3, 1), (3, 3) \bmod 4$.
- This is "less true"! There is a big bias towards pairs with $(p, q) \equiv (3, 3) \bmod 4$.

Prime Biases, II

Specifically, define $r_2(x) = \dfrac{\#\{pq \leq x \,:\, p \equiv q \equiv 3 \pmod 4\}}{\frac{1}{4}\#\{pq \leq x\}}$.

Prime Biases, II

Specifically, define $r_2(x) = \dfrac{\#\{pq \le x \,:\, p \equiv q \equiv 3 (\mathrm{mod}\ 4)\}}{\frac{1}{4}\#\{pq \le x\}}$.

Some values:

x	10^3	10^4	10^5	10^6	10^7
$r_2(x)$	1.347	1.258	1.212	1.183	1.162

Prime Biases, II

Specifically, define $r_2(x) = \dfrac{\#\{pq \le x \,:\, p \equiv q \equiv 3 (\text{mod } 4)\}}{\frac{1}{4}\#\{pq \le x\}}$.

Some values:

x	10^3	10^4	10^5	10^6	10^7
$r_2(x)$	1.347	1.258	1.212	1.183	1.162

These values are converging to 1 extremely slowly! (But why?)

Prime Biases, III

Theorem 1 (D. Dummit, Granville, Kisilevsky)

Let χ be a quadratic character of conductor d. For $\eta = -1$ or 1,

$$\frac{\#\{pq \leq x \,:\, \chi(p) = \chi(q) = \eta\}}{\frac{1}{4}\#\{pq \leq x \,:\, \gcd(pq, d) = 1\}} = 1 + \eta \frac{(\mathcal{L}_\chi + o(1))}{\log \log x}$$

where $\mathcal{L}_\chi = \sum_p \frac{\chi(p)}{p}$.

Prime Biases, IV

When χ is the quadratic character modulo 4, can compute $\mathcal{L}_\chi \approx -0.334$, yielding an approximation $s(x) = 1 + \dfrac{1}{3 \log \log x - 1}$ which is fairly good:

x	10^3	10^4	10^5	10^6	10^7
$r_2(x)$	1.347	1.258	1.212	1.183	1.162
$s(x)$	1.357	1.273	1.230	1.205	1.187

Natural question: when else does this kind of bias appear?

Splitting Configurations, I

Observation: The four possible pairs of (p, q) mod 4 correspond to different splitting behaviors of p and q in the biquadratic extension $\mathbb{Q}(\sqrt{p^*}, \sqrt{q^*})$, where $r^* = (-1)^{(r-1)/2} r$.

Splitting Configurations, I

Observation: The four possible pairs of (p, q) mod 4 correspond to different splitting behaviors of p and q in the biquadratic extension $\mathbb{Q}(\sqrt{p^*}, \sqrt{q^*})$, where $r^* = (-1)^{(r-1)/2} r$.

New problem: Study "splitting configurations" in extensions of the form $K = \mathbb{Q}(\sqrt{p_1^*}, \ldots, \sqrt{p_k^*})$, where p^* denotes $(-1)^{(p-1)/2} p$.

- In other words: what are the possible ways in which the primes p_i could split in K?
- For 3 primes, one possibility would be to have each p_i split into a product of 4 primes in K.

Splitting Configurations, II

Let's rephrase this question more sensibly:

- Splitting behavior of the p_i in K is completely determined by splitting in each quadratic subextensions of K.

Splitting Configurations, II

Let's rephrase this question more sensibly:

- Splitting behavior of the p_i in K is completely determined by splitting in each quadratic subextensions of K.
- Behavior in quadratic extensions in turn completely characterized by Legendre symbols $\left(\frac{p_i}{p_j}\right)$.
- So, question is equivalent to asking what sets of Legendre symbols $\left(\frac{p_i}{p_j}\right)$ for $1 \leq i, j \leq k$ can occur if the p_i are primes.

Splitting Configurations, II

Let's rephrase this question more sensibly:

- Splitting behavior of the p_i in K is completely determined by splitting in each quadratic subextensions of K.
- Behavior in quadratic extensions in turn completely characterized by Legendre symbols $\left(\frac{p_i}{p_j}\right)$.
- So, question is equivalent to asking what sets of Legendre symbols $\left(\frac{p_i}{p_j}\right)$ for $1 \leq i, j \leq k$ can occur if the p_i are primes.

Natural way to organize this information: put it into a matrix!

Sign Matrices and Quadratic Residue Matrices

Definition

A <u>sign matrix</u> is a matrix with entries of 0 on the diagonal and ± 1 off the diagonal.

Note that there are $2^{n(n-1)}$ sign matrices that are $n \times n$.

Definition

The <u>quadratic residue</u> matrix associated to the primes p_1, p_2, ..., p_n is the $n \times n$ matrix $M_{i,j}$ whose (i,j)-entry is the Legendre symbol $\left(\frac{p_i}{p_j}\right)$.

Studying splitting configurations is then equivalent to studying quadratic residue matrices.

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:

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? Are they common or uncommon among all sign matrices?

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 ± 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 ± 1.*
2. *The matrix M is a quadratic residue matrix for some set of 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

The Theorem allows us to easily determine whether particular matrices are quadratic residue matrices:

Example

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

Identifying Quadratic Residue Matrices

The Theorem allows us to easily determine whether particular matrices are quadratic residue matrices:

Example

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

Can also use the Theorem to count $n \times n$ quadratic residue matrices for small n (as well as equivalence classes under the permutation action), though condition (1) turns out to be better for computation.

Counting Quadratic Residue Matrices

Here are some counts:

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 counts:

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

Corollary 1

The proportion of $n \times n$ sign matrices that are quadratic residue matrices tends to zero (very fast) as $n \to \infty$.

QR Matrices VII: The Prime Bias Awakens

Can use quadratic residue matrices to find more examples of prime-counting biases. Here is one example:

- As seen in the table, there are 10 splitting configurations for three odd primes p, q, r in the extension $\mathbb{Q}(\sqrt{p^*}, \sqrt{q^*}, \sqrt{r^*})$.
- Using the 3×3 quadratic residue matrices, can compute the expected frequencies with which each splitting configuration occurs (essentially the size of the permutation orbit).

QR Matrices VII: The Prime Bias Awakens

Can use quadratic residue matrices to find more examples of prime-counting biases. Here is one example:

- As seen in the table, there are 10 splitting configurations for three odd primes p, q, r in the extension $\mathbb{Q}(\sqrt{p^*}, \sqrt{q^*}, \sqrt{r^*})$.
- Using the 3×3 quadratic residue matrices, can compute the expected frequencies with which each splitting configuration occurs (essentially the size of the permutation orbit).
- Computing all 306386 examples with $pqr < 2457615$ yields the frequencies $\{0.037,\ 0.043,\ 0.062,\ 0.090,\ 0.108,\ 0.108,\ 0.123,\ 0.127,\ 0.138,\ 0.163\}$.
- Actual values are $\{0.031,\ 0.063,\ 0.063,\ 0.094,\ 0.094,\ 0.094,\ 0.094,\ 0.094,\ 0.188,\ 0.188\}$.

Generalizations to Higher Degree

Natural generalization: use mth power residue symbols over a ground field containing the mth 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 respectively. 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 Extensions

Here is the setup in the cubic case:

- For $m = 3$, most natural base field is $K = \mathbb{Q}(\sqrt{-3})$.
- Splitting question then concerns splitting of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ not dividing 3 of K in composites of cyclic cubic extensions of K.
- Any prime ideal of K not dividing 3 is principal and has a unique "3-primary" generator π with $\pi \equiv 1 \bmod 3$ in K.

Cubic Extensions

Here is the setup in the cubic case:

- For $m = 3$, most natural base field is $K = \mathbb{Q}(\sqrt{-3})$.
- Splitting question then concerns splitting of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ not dividing 3 of K in composites of cyclic cubic extensions of K.
- Any prime ideal of K not dividing 3 is principal and has a unique "3-primary" generator π with $\pi \equiv 1 \bmod 3$ in K.
- The minimally ramified cyclic cubic extensions of K are then the Kummer extensions $K(\sqrt[3]{\pi})$.
- The natural matrices then involve the cubic residue symbols on ideals $\mathfrak{p}_i$, which can be equivalently computed using the 3-primary generators π_i.

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 π_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:

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* π_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 2 (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 essentially the same construction as the cubic residue matrices, except we work with prime ideals of the ground field $K = \mathbb{Q}(i)$ not dividing 2, and each such ideal has a "2-primary" generator $\pi \equiv 1 \bmod 2(1+i)$.

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 π_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 3 (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 $n - 1$.*

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 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 natural 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!