



THE QUARTIC RESIDUES LATIN SQUARE

Christian Aebi

Collège Calvin, Geneva, Switzerland
christian.aebi@edu.ge.ch

Grant Cairns

La Trobe University, Melbourne, Australia
G.Cairns@latrobe.edu.au

Received: 12/14/16, Accepted: 7/27/17, Published: 8/7/17

Abstract

We establish an elementary, but rather striking pattern concerning the quartic residues of primes p that are congruent to 5 modulo 8. Let g be a generator of the multiplicative group of \mathbb{Z}_p and let M be the 4×4 matrix whose $(i+1), (j+1)$ -th entry is the number of elements x of \mathbb{Z}_p of the form $x \equiv g^k \pmod{p}$ where $k \equiv i \pmod{4}$ and $\lfloor 4x/p \rfloor = j$, for $i, j = 0, 1, 2, 3$. We show that M is a Latin square, provided the entries in the first row are distinct, and that M is essentially independent of the choice of g . As an application, we prove that the sum in \mathbb{Z} of the quartic residues is $\frac{p}{5}(M_{11} + 2M_{12} + 3M_{13} + 4M_{14})$.

1. Introduction

Let p be prime with $p \equiv 5 \pmod{8}$, identify the finite field \mathbb{Z}_p with the set $\{0, 1, \dots, p-1\}$, and let g be an arbitrary generator of the multiplicative group \mathbb{Z}_p^* . For $i = 0, 1, 2, 3$, let B_i be the set of elements x of \mathbb{Z}_p^* of the form $x \equiv g^k \pmod{p}$, where $k \equiv i \pmod{4}$. Note that although k is not unique, its value modulo 4 is unique, by Fermat's little theorem. Now divide \mathbb{Z}_p^* into 4 consecutive subintervals; for $j = 0, \dots, 3$, let

$$I_j = \left\{ x \in \mathbb{Z}_p^* : \frac{jp}{4} < x < \frac{(j+1)p}{4} \right\}.$$

Consider the 4×4 matrix M whose $(i+1), (j+1)$ -th entry is the number of elements in the intersection $B_i \cap I_j$. Note that the first row counts the quartic residues in the intervals I_0, I_1, I_2, I_3 . For example, consider the prime $p = 109$ and the generator $g = 6$. The quartic residues are:

1, 3, 5, 7, 9, 15, 16, 21, 22, 25, 26, 27|35, 38, 45, 48, 49|63, 66, 73, 75, 78, 80, 81|89, 97, 105.

One finds that M is a Latin square:

$$M = \begin{bmatrix} 12 & 5 & 7 & 3 \\ 7 & 12 & 3 & 5 \\ 3 & 7 & 5 & 12 \\ 5 & 3 & 12 & 7 \end{bmatrix}.$$

This pattern is surprising, as the sets B_i are given by the multiplicative structure, while the sets I_j are related to the additive structure. So the definition of M is rather peculiar, if not downright perverse. Nevertheless, we will show that the pattern given above always occurs, provided $p \equiv 5 \pmod{8}$, and M is essentially independent of the choice of generator g .

Recall that in \mathbb{Z}_p^* the number of generators is given by the Euler function $\varphi(p-1)$. In particular, there is an even number of generators. In fact, half of the generators g have the property $2 \equiv g^k \pmod{p}$ where $k \equiv 1 \pmod{4}$, and half have $2 \equiv g^k \pmod{p}$ with $k \equiv 3 \pmod{4}$. To see this, notice that 2 is not a quadratic residue as $p \equiv 5 \pmod{8}$, so if $2 \equiv g^k \pmod{p}$, then k is necessarily odd. Furthermore, if g is a generator, then so too is g^{-1} , and $g^k \equiv (g^{-1})^{-k} \equiv (g^{-1})^{p-1-k} \pmod{p}$, by Fermat's little theorem. And as $p \equiv 1 \pmod{4}$, one has $k \equiv 1 \pmod{4}$ if and only if $p-1-k \equiv 3 \pmod{4}$.

Theorem 1. *Suppose that p is prime with $p \equiv 5 \pmod{8}$ and choose a generator g of the multiplicative group \mathbb{Z}_p^* . Then the matrix M has one the following two forms:*

$$\begin{bmatrix} a & b & c & d \\ c & a & d & b \\ d & c & b & a \\ b & d & a & c \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} a & b & c & d \\ b & d & a & c \\ d & c & b & a \\ c & a & d & b \end{bmatrix}, \tag{1}$$

depending on whether $2 \equiv g^k \pmod{p}$ with $k \equiv 1 \pmod{4}$ or $k \equiv 3 \pmod{4}$ respectively. In particular, in both cases, if the entries in the first row are distinct, the matrix M is a Latin square.

Remark 1. The first row of the matrix M is independent of the generator g , as it depends only on the quartic residues. So the theorem shows that M is independent of the choice of generator, up to a transposition of rows 2 and 4.

The paper is organised as follows. In Section 2 we prove Theorem 1 and we show how M may be defined in a different manner. In Section 3, as an application of Theorem 1, we give a formula for the sum of the quartic residues, in terms of p and the entries in the first row of M .

2. Proof of Theorem 1

Proof of Theorem 1. Let g be a generator of \mathbb{Z}_p^* . First note that writing $p = 8n + 5$, one has $-1 \equiv g^{4n+2}$ in \mathbb{Z}_p^* . So modulo p , multiplication by -1 sends B_i to B_{i+2} , for $i = 0, 1$. Hence, considering the map $x \mapsto p - x$, we see that the first row of M equals the third row in reverse order, and visa versa. Similarly, the second row equals the fourth row in reverse order. To enable us to refer to this property below, let us record it formally:

$$M_{ij} = M_{(i+2),(5-j)}, \tag{2}$$

where $1 \leq i \leq 2$ and $1 \leq j \leq 4$. So it remains to consider how row 2 is obtained from row 1. Let us suppose that $2 \equiv g^k \pmod{p}$ with $k \equiv 1 \pmod{4}$, so modulo p , multiplication by 2 sends B_i to B_{i+1} for $i = 0, 1, 2$. (The case $k \equiv 3 \pmod{4}$ is entirely analogous; multiplication by 2 sends B_i to B_{i-1}). We claim that

$$M_{21} = M_{13}, \quad M_{22} = M_{11}. \tag{3}$$

Let us see how (3) gives the theorem. To lighten the notation, let $M_{11} = a, M_{12} = b, M_{13} = c, M_{14} = d$. By (2) and (3), M has the following form:

$$M = \begin{bmatrix} a & b & c & d \\ c & a & * & * \\ d & c & b & a \\ * & * & a & c \end{bmatrix}.$$

Now notice that the rows and columns of M all have the same sum, $(p - 1)/4$. Comparing the first row with the four columns we obtain the form of the left hand side of (1).

It remains to establish (3). For this, we require some further notation. We will look at the bottom and top halves of the intervals I_{j-1} , and then the various quarters of the I_{j-1} . For each $i, j, k = 1, \dots, 4$, let

$$\begin{aligned} b_{ij} &= |B_{i-1} \cap \{x \in \mathbb{Z}_p^* : (j-1)p/4 < x < (2j-1)p/8\}|, \\ t_{ij} &= |B_{i-1} \cap \{x \in \mathbb{Z}_p^* : (2j-1)p/8 < x < jp/4\}|, \\ q_{jk} &= |B_0 \cap \{x \in \mathbb{Z}_p^* : (4j-5+k)p/16 < x < (4j-4+k)p/16\}|, \end{aligned}$$

so that by definition,

$$M_{ij} = b_{ij} + t_{ij} \tag{4}$$

and

$$b_{1j} = q_{j1} + q_{j2}, \quad t_{1j} = q_{j3} + q_{j4}. \tag{5}$$

Considering the effect modulo p of multiplication of the elements of B_{i-1} by 2, we have for $i = 1, 2$ and 3,

$$M_{(i+1)1} = b_{i1} + b_{i3}, \quad M_{(i+1)2} = t_{i1} + t_{i3}, \quad M_{(i+1)3} = b_{i2} + b_{i4}, \quad M_{(i+1)4} = t_{i2} + t_{i4}. \tag{6}$$

Similarly,

$$b_{22} = q_{13} + q_{33}, \quad b_{24} = q_{23} + q_{43}, \tag{7}$$

and

$$t_{22} = q_{14} + q_{34}, \quad t_{24} = q_{24} + q_{44}. \tag{8}$$

Thus, (2) with $i = 1, j = 1, 2$, (6) with $i = 2$, (7) and (8) give

$$\begin{aligned} M_{11} = M_{34} &= t_{22} + t_{24} = q_{14} + q_{24} + q_{34} + q_{44}, \\ M_{12} = M_{33} &= b_{22} + b_{24} = q_{13} + q_{23} + q_{33} + q_{43}. \end{aligned}$$

Adding the above two equations and using (5), we get $M_{11} + M_{12} = t_{11} + t_{12} + t_{13} + t_{14}$, and thus by (4),

$$b_{11} + b_{12} = t_{13} + t_{14}. \tag{9}$$

As the first row of M has the same sum as the first column of M , we have

$$M_{12} + M_{13} + M_{14} = M_{21} + M_{31} + M_{41}.$$

But by (2), we have $M_{31} = M_{14}$ and $M_{41} = M_{24}$. Hence, using (6) with $i = 1$, we have $M_{12} + M_{13} = M_{21} + M_{24} = b_{11} + b_{13} + t_{12} + t_{14}$, and hence by (4),

$$b_{12} + t_{13} = b_{11} + t_{14}, \tag{10}$$

Solving (9) and (10) we obtain $b_{11} = t_{13}, b_{12} = t_{14}$. Finally, by (4) and (6) with $i = 1$,

$$\begin{aligned} M_{21} = b_{11} + b_{13} &= b_{13} + t_{13} = M_{13} \\ M_{22} = t_{11} + t_{13} &= b_{11} + t_{11} = M_{11}. \end{aligned}$$

which gives (3) as required. □

Remark 2. As we saw in the proof of Theorem 1, if x is a quartic residue, so too is $-4x$, modulo p , and similarly, so too is $-x/4$. In particular, 1 is a quartic residue since $p \equiv 1 \pmod{4}$, and hence $p - 4$ and $(p - 1)/4$ are quartic residues too.

We now show that the matrix M can be defined in a different manner, by replacing the sets I_0, \dots, I_3 by a different partition of \mathbb{Z}_p^* into 4 subsets of equal cardinality. For $j = 1, \dots, 4$, let $J_j = \{x \in \mathbb{Z}_p^* : x \equiv j \pmod{4}\}$. We will show that the distribution of the quartic residues amongst the intervals I_0, \dots, I_3 is identical to the distribution of the quartic residues amongst the conjugacy classes J_1, \dots, J_4 .

Proposition 1. *For all $i, j = 1, \dots, 4$, one has $M_{ij} = |B_{i-1} \cap J_j|$.*

For example, consider $p = 109$. The quartic residues, collected in the intervals I_0, \dots, I_3 are:

1, 3, 5, 7, 9, 15, 16, 21, 22, 25, 26, 27|35, 38, 45, 48, 49|63, 66, 73, 75, 78, 80, 81|89, 97, 105,

while collected in the intervals J_1, \dots, J_4 , they are:

1, 5, 7, 21, 25, 45, 49, 73, 81, 89, 97, 105|22, 26, 38, 66, 78|3, 7, 15, 27, 35, 63, 75|16, 48, 80.

The collections are different, but as the Proposition asserts, the cardinalities are the same.

Proof of Proposition 1. We only treat the first row of M ; the other rows are dealt with in exactly the same manner. First suppose that the generator g is such that $2 \equiv g^k \pmod{p}$ where $k \equiv 1 \pmod{4}$. We will show that working modulo p , the map $x \mapsto -4x$ establishes the required bijections.

Recall that $M_{11} = |B_0 \cap I_0|$. Multiplying the set $B_0 \cap I_0$ by 2 gives the even elements of $B_1 \cap (I_0 \cup I_1)$. Multiplying again by 2, we obtain the elements of B_2 that are divisible by 4. Finally, multiplying the latter set by -1 and adding $p \equiv 1 \pmod{4}$ to the products we obtain the elements of B_0 congruent to 1 $\pmod{4}$, as asserted by the proposition. Symbolically, we can represent the above bijective transformations in the following way:

$$B_0 \cap I_0 \xrightarrow[\cong]{2x} B_1 \cap (I_0 \cup I_1) \cap (J_2 \cup J_4) \xrightarrow[\cong]{2x} B_2 \cap J_4 \xrightarrow[\cong]{-x+p} B_0 \cap J_1.$$

Using the above convention, we obtain concerning M_{12} :

$$B_0 \cap I_1 \xrightarrow[\cong]{2x} B_1 \cap (I_2 \cup I_3) \cap (J_2 \cup J_4) \xrightarrow[\cong]{2x-p} B_2 \cap J_3 \xrightarrow[\cong]{-x+p} B_0 \cap J_2.$$

Similarly concerning M_{13} and then M_{14} we get:

$$B_0 \cap I_2 \xrightarrow[\cong]{2x-p} B_1 \cap (I_0 \cup I_1) \cap (J_1 \cup J_3) \xrightarrow[\cong]{2x} B_2 \cap J_2 \xrightarrow[\cong]{-x+p} B_0 \cap J_3,$$

$$B_0 \cap I_3 \xrightarrow[\cong]{2x-p} B_1 \cap (I_2 \cup I_3) \cap (J_1 \cup J_3) \xrightarrow[\cong]{2x-p} B_2 \cap J_1 \xrightarrow[\cong]{-x+p} B_0 \cap J_4.$$

This establishes the proposition when $2 \equiv g^k \pmod{p}$ with $k \equiv 1 \pmod{4}$. The case where $k \equiv 3 \pmod{4}$ is treated in exactly the same manner, with B_1 replaced by B_3 . □

3. The Sum of the Quartic Residues

In this section, as an application of Theorem 1, we show that the sum of the quartic residues can be computed from the entries in the first row of M . To place this result in context, let us first recall that some well-known facts about sums of quartic residues.

Suppose that $p \equiv 3 \pmod{4}$. Then every quadratic residue is a quartic residue. Indeed, the map $x \mapsto p - x$ interchanges the quadratic residues with the non-quadratic residues. So if in \mathbb{Z}_p we have $a \equiv b^2$, then either b is a quadratic residue,

in which case a is a quartic residue, or b is not a quadratic residue, in which case $p-b$ is a quadratic residue and $a \equiv (p-b)^2$, and once again a is a quartic residue. In particular, the sum of the quartic residues equals the sum of the quadratic residues, and we can use V.-A. Lebesgue's results [1].

Suppose that $p \equiv 1 \pmod{8}$. By Gauss, -1 is a quartic residue. So the map $x \mapsto p-x$ fixes the quartic residues. Thus, for each quartic residue a , the element $p-a$ is also a quartic residue and the sum of this pair is therefore p . So the sum of the quartic residues is $p/2$ times the number $(p-1)/4$ of the quartic residues. Thus the sum of the quartic residues is $p(p-1)/4$.

The above comments show that the interesting case is when $p \equiv 5 \pmod{8}$.

Theorem 2. *For all primes p with $p \equiv 5 \pmod{8}$, the sum in \mathbb{Z} of the quartic residues is*

$$\frac{p}{5}(M_{11} + 2M_{12} + 3M_{13} + 4M_{14}).$$

Proof. Choose a generator g of \mathbb{Z}_p^* such that $2 \equiv g^k \pmod{p}$ where $k \equiv 1 \pmod{4}$, and let M be the resulting matrix, as in Theorem 1. Let b_i denote the sum of the elements of B_i , for $i = 0, \dots, 3$. Consider multiplication of the elements of B_0 by 2. Modulo p , the set B_0 is sent bijectively to B_1 . In fact, the elements of $B_0 \cap (I_1 \cup I_2)$ are sent directly to elements of B_1 , while for each element $x \in B_0 \cap (I_3 \cup I_4)$, one has $2x - p \in B_1$. Since there are $M_{13} + M_{14}$ elements in $B_0 \cap (I_3 \cup I_4)$, we have

$$b_1 = 2b_0 - p(M_{13} + M_{14}).$$

Similarly,

$$b_2 = 2b_1 - p(M_{23} + M_{24}), \quad b_3 = 2b_2 - p(M_{33} + M_{34}), \quad b_0 = 2b_3 - p(M_{43} + M_{44}).$$

Rearranging, and applying Theorem 1, we have

$$\begin{aligned} 2b_0 &= b_1 + p(M_{13} + M_{14}) \\ 2b_1 &= b_2 + p(M_{14} + M_{12}) \\ 2b_2 &= b_3 + p(M_{12} + M_{11}) \\ 2b_3 &= b_0 + p(M_{11} + M_{13}). \end{aligned}$$

Solving this system of 4 equations for b_0 gives the required result. □

References

[1] C. Aebi and G. Cairns, Sums of quadratic residues and nonresidues, *Amer. Math. Monthly* **124** (2017), 166-169.