Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2015, Article ID 163092, 5 pages
http://dx.doi.org/10.1155/2015/163092

Research Article

Counting Quadratic Nonresidues in Shifted Subsets of the Set of Quadratic Nonresidues for Primes $p = 4k + 1$

Rocío Meza-Moreno and Mario Pineda-Ruelas

Departamento de Matemáticas, Universidad Autónoma Metropolitana-Iztapalapa, Avenida San Rafael Atlixco No. 186, Col. Vicentina, Iztapalapa, C.P. 09340 Ciudad de México, DF, Mexico

Correspondence should be addressed to Mario Pineda-Ruelas; mpr@xanum.uam.mx

Received 23 February 2015; Accepted 7 April 2015

Academic Editor: Shyam L. Kalla

Let $p = 4k + 1$ be a prime number and $\mathbb{F}_p$ the finite field with p elements. For $x \in [\![1, n]\!]$, N_x will denote the set of quadratic nonresidues less than or equal to x. In this work we calculate the number of quadratic nonresidues in the shifted set $N_{(p-1)/2} + a$.

1. Introduction

Let p be an odd prime, $\mathbb{F}_p$ the finite field with p elements, and $\mathbb{F}_p^*$ the multiplicative group of $\mathbb{F}_p$. We will write $[\![a, n]\!]$ to denote the set $\{a, a+1, \ldots, n\}$ and $(\,/p)$ to denote the Legendre symbol. Let R be the set of quadratic residues modulo p, including 0, and $N = \mathbb{F}_p \setminus R$. The distribution of quadratic residues and nonresidues has been studied with great interest in the literature [1–3]. In [2] Perron finds the number of quadratic residues and nonresidues in the shifted sets $R + a$ and $N + a$, where $a \in \mathbb{F}_p^*$, in particular, with $a = 1$; his result gives the number of pairs of consecutive quadratic residues and of nonresidues. Perron also gives nonsquare matrices having two properties: each row has the same number of elements in common with every other row and the corresponding elements of every two rows have the same difference. According to Brauer [4], Paley [5] found these matrices and used them in the construction of Hadamard matrices. Following Perron, we can ask what happens to the number of quadratic residues when we shift some subset of R or N. Let $R_x = \{r \in R : 1 \le r \le x\}$. In [6] the authors study the number of quadratic residues in the shifted set $R_{(p-1)/2}+a$. Let $N_x = \{n \in N : 1 \le n \le x\}$ and let $p = 4k + 1$ be a prime number. In this work we use Perron's results and elementary techniques to determine the number of quadratic nonresidues (and hence the number of residues) in the set $N_{(p-1)/2} + a$.

Theorem 1 (O. Perron). *Let $p = 4k + 1$ be a prime number and N the set of quadratic nonresidues modulo p.*

(1) *If $a \in R$ and $a \neq 0$, then $|(N+a) \cap R| = |(N+a) \cap N| = k$.*

(2) *If $a \in N$, then $|(N+a) \cap R| = k+1$ and $|(N+a) \cap N| = k - 1$.*

Proof. See [2]. □

2. Some Properties of R

If $p \equiv 1 \pmod 4$ is a prime number, then a is a quadratic residue if and only if $p - a$ is also a quadratic residue modulo p. We will call this property the *elementary symmetry*. The elementary symmetry implies that

$$\sum_{n=1}^{(p-1)/2} \left(\frac{n}{p}\right) = 0. \tag{1}$$

If we consider smaller intervals the elementary symmetry is lost, but we still have some useful properties. In general, if $p = 2k + 1$, then

$$\left(\frac{k}{p}\right) = \left(\frac{(p-1)/2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if and only if } p \equiv 1, 3 \pmod 8, \\ -1 & \text{if and only if } p \equiv 5, 7 \pmod 8. \end{cases} \tag{2}$$

In particular, if $p = 4k + 1$ we get the following.

Corollary 2. *If $p \equiv 1 \mod 4$ is a prime number, then*

$$\left(\frac{(p-1)/2}{p}\right) = \begin{cases} 1 & \textit{if and only if } p \equiv 1 \pmod 8, \\ -1 & \textit{if and only if } p \equiv 5 \pmod 8. \end{cases} \tag{3}$$

Theorem 3. *If $p = 4k + 1$ is a prime number, then*

$$\begin{aligned} &(1)\left(\frac{(p-1)/2 - n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2n+1}{p}\right). \\ &(2)\left(\frac{(p-1)/2 + n}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2n-1}{p}\right). \end{aligned} \tag{4}$$

Proof. The first assertion follows from $((p-1-2n)/p) = (2/p)(((p-1-2n)/2)/p)$ and the elementary symmetry. The proof of the second assertion is similar to the one of the first assertion. □

According to the first assertion of the previous theorem we have that if $p \equiv 1 \pmod 8$, then the numbers $(p-1)/2-n$ and $2n+1$ are both quadratic residues or are both nonresidues modulo p. If $p \equiv 5 \pmod 8$, then one of these numbers is a residue and the other one is a nonresidue. This fact gives a correspondence between the numbers $(p-1)/2-n$ and $2n+1$. We can give a similar interpretation to the second assertion.

3. Main Results

In this section we count the number of nonresidues in the set $N_{(p-1)/2} + a$. To do this we arrange the elements in $N + a$ in pairs such that the first element of the pair is in the set $N_{(p-1)/2} + a$ and the second one is not, and then we make use of Theorem 1.

Lemma 4. *If $p = 4k + 1$ is a prime number and $n = n_i + a \in N + a$ is a quadratic nonresidue modulo p, then $p - n_i$ is also a quadratic nonresidue and $p - n_i \in N + a$.*

We will call the pair of quadratic nonresidues in $N + a$ given by $(n_i + a, p - n_i)$ a *corresponding pair* of quadratic nonresidues. If the pair also satisfies $n_i + a < p - n_i$ we will say that $(n_i + a, p - n_i)$ is an *ordered corresponding pair* of quadratic nonresidues.

Note that as n_i runs in $1 \le n_i < (p-a)/2$ then $1 + a \le n_i + a < (p-a)/2 + a$ and the corresponding pair $p - n_i$ satisfies $(p-a)/2 + a < p - n_i \le p - 1$. In particular, for a corresponding pair to be ordered the following condition must be met:

$$n_i < \frac{p-a}{2}. \tag{5}$$

In $N + a$ eventually appear some of the integers in $[\![0, a]\!]$, but if $a \le (p-1)/2$, these are not in $N_{(p-1)/2} + a$ and so we have to take these numbers out of consideration. If n_j is the maximum nonresidue such that $n_j \le \lfloor (p-a)/2 \rfloor$, $n_j + a \in N$ and its corresponding pair satisfy $p - n_j > (p-1)/2 + a$, then half of the nonresidues left in $N + a$ are elements of $N_{(p-1)/2} + a$ (the ones of the form $n_i + a$) and the other half are not (the corresponding pairs $p - n_i$). Therefore, by Theorem 1 we get the following.

Theorem 5. *Let $p = 4k + 1$ be a prime number, $a \in [\![1, (p-1)/2]\!]$,*

$$\begin{aligned} n_j &= \max\left\{n_i \in N : n_i \le \left\lfloor \frac{p-a}{2} \right\rfloor,\ n_i + a \in N\right\}, \\ S &= \{0, 1, \ldots, a-1, a\} \cap (N + a) \\ &= \{i \in [\![0, a]\!] : a - i \in N\} \end{aligned} \tag{6}$$

and $s = |S \cap N|$. Suppose n_j satisfies the condition

$$p - n_j > \frac{p-1}{2} + a. \tag{7}$$

Then the following assertions hold:

(1) *If $a \in R$, then $|(N_{(p-1)/2} + a) \cap N| = (k - s)/2$.*

(2) *If $a \in N$, then $|(N_{(p-1)/2} + a) \cap N| = (k - 1 - s)/2$.*

If $(p-a)/2 \in N$, then in the previous theorem $n_j = (p-a)/2$ and when this happens $n_j + a = p - n_j$. In this case the theorem does not apply because we get the equality in condition (7). When a corresponding pair satisfies $n_i + a = p - n_i$ we will call it an *overlap*.

An overlap only occurs when $n_j = (p-a)/2 \in \mathbb{Z}$ and $n_j \in N$. In this situation it is possible to count nonresidues in $N_{(p-1)/2} + a$ using basically the same idea with a slight modification: we must take the overlap into account because $n_j + a = p - n_j \in N_{(p-1)/2} + a$. Thus, if an overlap occurs, we must take 1 off in the result of Theorem 5 before dividing by 2 and then we add 1.

Condition (7) may also fail when the left side is smaller than the right side; this happens when there is at least one corresponding pair whose elements are both in the set $N_{(p-1)/2} + a$; thus in this case both of the pair elements must be taken into account. We call such pair an *inner pair*. The necessary modification to the result of Theorem 5 is clear: we add 1 for every existing inner pair.

Summarizing, for a given a and a prime $p = 4k + 1$, if o_a is the number of overlaps (there is at most 1 overlap) and p_a is the number of inner pairs, we get the following result.

Theorem 6. *Let $p = 4k+1$ be a prime number and $a \in [\![1, (p-1)/2]\!]$ and s as in Theorem 5. Then the following assertions hold:*

(1) *If $a \in R$, then $|(N_{(p-1)/2}+a) \cap N| = (k-s-o_a)/2+o_a+p_a$.*

(2) *If $a \in N$, then $|(N_{(p-1)/2}+a) \cap N| = (k-1-s-o_a)/2+o_a+p_a$.*

For particular values of a it is possible to give conditions on the prime p so that hypothesis of Theorem 5 holds; moreover, it is possible to determine if an overlap occurs and the number of inner pairs.

4. Examples

In this section we use particular values of a to exemplify the results of the previous section.

Proposition 7. *Let $p = 4k + 1$ be a prime number.*

(1) *If $p \equiv 1 \mod 8$, then $|(N_{(p-1)/2} + 1) \cap N| = k/2$.*

(2) *If $p \equiv 5 \mod 8$, then $|(N_{(p-1)/2} + 1) \cap N| = (k+1)/2$.*

Proof. For $a = 1$, we get $S = \emptyset$ so that $s = 0$ and an overlap can occur only if $(p-1)/2 \in N$. From Corollary 2 this happens if and only if $(2/p) = -1$. By Theorem 6 the result follows. □

From the previous proposition, we get the number of pairs of consecutive quadratic residues in the interval $[\![1, (p-1)/2]\!]$ for a prime number $p = 4k + 1$.

Corollary 8. *Let $p = 4k + 1$ be a prime number. The number of pairs of consecutive quadratic residues in $[\![1, (p-1)/2]\!]$ is*

(1) $(k-2)/2$ *if* $p \equiv 1 \pmod 8$,

(2) $(k-1)/2$ *if* $p \equiv 5 \pmod 8$.

Proposition 9. *Let $p = 4k + 1$ be a prime number.*

(1) *If $(2/p) = 1$, then $|(N_{(p-1)/2} + 2) \cap N| = k/2$.*

(2) *If $(2/p) = (3/p) = -1$, then $|(N_{(p-1)/2} + 2) \cap N| = (k-1)/2$.*

(3) *If $(2/p) = -1$ and $(3/p) = 1$, then $|(N_{(p-1)/2}+2) \cap N| = (k+1)/2$.*

Proof. For this value of a there is no overlap; thus $o_a = 0$. For the first assertion, if $(2/p) = 1$ then $S = \emptyset$, so $s = 0$, and there are no inner pairs. From Theorem 6 it follows that there are $(k-s)/2 = k/2$ nonresidues in $N_{(p-1)/2} + 2$. The second and third assertions follow from the fact that if $n_i = \lfloor (p-2)/2 \rfloor = (p-1)/2 - 1$ and $n_i + 2 = (p-1)/2 + 1$ are both nonresidues, then there is an inner pair given by $(n_i + 2, p - n_i)$, which occurs if and only if $(2/p) = -1$ and $(3/p) = 1$. □

Proposition 10. *Let $p = 4k + 1$ be a prime number.*

(1) *If $(2/p) = 1$, then $|(N_{(p-1)/2} + 3) \cap N| = k/2$.*

(2) *If $(2/p) = (3/p) = -1$ and $(5/p) = 1$ or $(2/p) = (5/p) = -1$ and $(3/p) = 1$, then $|(N_{(p-1)/2} + 3) \cap N| = (k+1)/2$.*

(3) *If $(2/p) = (3/p) = (5/p) = -1$, then $|(N_{(p-1)/2} + 3) \cap N| = (k-1)/2$.*

(4) *If $(2/p) = -1$ and $(3/p) = (5/p) = 1$, then $|(N_{(p-1)/2} + 3) \cap N| = (k+3)/2$.*

Table 1

$\left\lvert\left(N_{(p-1)/2}+1\right)\cap N\right\rvert$	$\left\lvert\left(N_{(p-1)/2}+(p-1)\right)\cap N\right\rvert$	$p \pmod 8$
$\frac{k+1}{2}$	$\frac{k-1}{2}$	5
$\frac{k}{2}$	$\frac{k}{2}$	1

Table 2

$\left\lvert\left(N_{(p-1)/2}+2\right)\cap N\right\rvert$	$\left\lvert\left(N_{(p-1)/2}+(p-2)\right)\cap N\right\rvert$	$p \pmod{24}$
$\frac{k}{2}$	$\frac{k}{2}$	1, 17
$\frac{k-1}{2}$	$\frac{k-1}{2}$	5
$\frac{k+1}{2}$	$\frac{k-3}{2}$	13

Proof. Note that $s = 0$ in every case. If $(p-3)/2 \in N$, then there is an overlap, which happens if $(2/p) \neq (3/p)$. On the other hand, if $n_i = (p-1)/2 - 2$ and $n_i + 3 = (p-1)/2 + 1$ are both nonresidues, we get the inner pair $(n_i + 3, p - n_i)$. This occurs when $(2/p) = -1$ and $(5/p) = 1$. Analyzing each case and making use of Theorem 6 the result follows. □

Proposition 11. *Let $p = 4k + 1$ be a prime number.*

(1) *If $(2/p) = (5/p) = 1$ or $(2/p) = (3/p) = 1$, then $|(N_{(p-1)/2} + 4) \cap N| = k/2$.*

(2) *If $(2/p) = (7/p) = -1$ and $[(3/p) = -1$ or $(5/p) = -1]$, then*

$$\left|\left(N_{(p-1)/2} + 4\right) \cap N\right| = \frac{k-1}{2}. \tag{8}$$

(3) *If $(2/p) = -1, (7/p) = 1$ and $[(3/p) = -1$ or $(5/p) = -1]$, then*

$$\left|\left(N_{(p-1)/2} + 4\right) \cap N\right| = \frac{k+1}{2}. \tag{9}$$

(4) *If $(2/p) = (7/p) = -1$ and $(3/p) = (5/p) = 1$, then*

$$\left|\left(N_{(p-1)/2} + 4\right) \cap N\right| = \frac{k+1}{2}. \tag{10}$$

(5) *If $(2/p) = 1$ and $(3/p) = (5/p) = -1$, then $|(N_{(p-1)/2} + 4) \cap N| = (k+2)/2$.*

(6) *If $(2/p) = -1$ and $(3/p) = (5/p) = (7/p) = 1$, then*

$$\left|\left(N_{(p-1)/2} + 4\right) \cap N\right| = \frac{k+3}{2}. \tag{11}$$

Table 3

$\lvert(N_{(p-1)/2}+3)\cap N\rvert$	$p \pmod{120}$	$\lvert(N_{(p-1)/2}+(p-3))\cap N\rvert$	$p \pmod{120}$
$\frac{k-1}{2}$	53, 77	$\frac{k-1}{2}$	13, 37, 53, 77
$\frac{k}{2}$	1, 17, 41, 49, 73, 89, 97, 113	$\frac{k}{2}$	1, 49, 73, 97
$\frac{k+1}{2}$	13, 29, 37, 101	$\frac{k-2}{2}$	17, 41, 89, 113
$\frac{k+3}{2}$	61, 109	$\frac{k-3}{2}$	29, 61, 101, 109

Table 4

$\lvert(N_{(p-1)/2}+4)\cap N\rvert$	$\lvert(N_{(p-1)/2}+(p-4))\cap N\rvert$	$p \pmod{840}$
$\frac{k-1}{2}$	$\frac{k+1}{2}$	13, 101, 157, 173, 269, 293, 341, 397, 437, 461, 493, 509, 517, 629, 677, 733, 773, 797
$\frac{k}{2}$	$\frac{k}{2}$	1, 41, 73, 89, 97, 121, 169, 193, 209, 241, 281, 289, 313, 337, 361, 401, 409, 433, 449, 457, 481, 521, 529, 569, 577, 601, 641, 649, 673, 689, 697, 761, 769, 793, 809, 817
$\frac{k+1}{2}$	$\frac{k-1}{2}$	29, 37, 53, 61, 149, 181, 197, 221, 229, 253, 277, 317, 349, 373, 389, 533, 557, 613, 653, 661, 701, 757, 821, 829
$\frac{k+2}{2}$	$\frac{k-2}{2}$	17, 113, 137, 233, 257, 353, 377, 473, 593, 617, 713, 737
$\frac{k+3}{2}$	$\frac{k-3}{2}$	109, 421, 541, 589, 709, 781

Proof. Since $a = 4$ is even, then there is no overlap; thus $o_a = 0$. But if $n_i = \lfloor (p-4)/2 \rfloor = (p-1)/2 - 2$ and $n_i + 4$ are both nonresidues, we get the inner pair $(n_i + 4, p - n_i)$. This happens if and only if $(2/p) \neq (5/p)$ and $(2/p) \neq (3/p)$. If also $n_i = \lfloor (p-4)/2 \rfloor - 1 = (p-1)/2 - 3$ and $n_i + 4$ are both nonresidues, again $(n_i+4, p-n_i)$ is an inner pair, which occurs if and only if $(2/p) \neq (7/p)$ and $(2/p) = -1$. Finally, the set S has a nonresidue only if $2 \in N$. Therefore, in the first case one has $s = 0$ and $p_a = 0$; in the second case, $s = 1$ and $p_a = 0$; in the third and fourth cases, $s = 1$ and $p_a = 1$; in the fifth case, $s = 0$ and $p_a = 1$; and in the sixth case, $s = 1$ and $p_a = 2$. The result follows using Theorem 6. □

In order to count the number of nonresidues in $N_{(p-1)/2} + a$ for $a = p - b$ and $b \in [\![1, (p-1)/2]\!]$ we use the same idea; that is, we consider corresponding pairs $(n_i + a, p - n_i)$ of nonresidues; only this time the nonresidues in the set S are of interest and if an overlap occurs it must not be counted. Also, in this case, it is possible to have pairs whose elements are neither in $N_{(p-1)/2}+a$, so they must not be counted. We call such a pair an *outer pair*. Letting o_a be the number of overlaps and p_a the number of outer pairs, we get the following result.

Theorem 12. *Let $p = 4k + 1$ be a prime and $a = p - b$, where $b \in [\![1, (p-1)/2]\!]$.*

(1) *If $a \in R$, then $\lvert(N_{(p-1)/2}+a)\cap N\rvert = (k-s-o_a)/2-p_a+s$.*

(2) *If $a \in N$, then $\lvert(N_{(p-1)/2}+a)\cap N\rvert = (k-1-s-o_a)/2-p_a+s$.*

s is as it is in Theorem 5.

It can be shown that the number of overlaps is the same for a and for $p - a$ and that the number of inner pairs for a equals the number of outer pairs for $p - a$; thus we get the following.

Corollary 13. *If $p = 4k+1$ is a prime number and $a \in [\![1, (p-1)/2]\!]$, then there is $m \in \mathbb{Z}$ such that if $a \in R$, then*

$$\begin{aligned} \left\lvert\left(N_{(p-1)/2}+a\right)\cap N\right\rvert &= \frac{k+m}{2}, \\ \left\lvert\left(N_{(p-1)/2}+(p-a)\right)\cap N\right\rvert &= \frac{k-m}{2}, \end{aligned} \tag{12}$$

and if $a \in N$, then

$$\begin{aligned} \left\lvert\left(N_{(p-1)/2}+a\right)\cap N\right\rvert &= \frac{k-1+m}{2}, \\ \left\lvert\left(N_{(p-1)/2}+(p-a)\right)\cap N\right\rvert &= \frac{k-1-m}{2}, \end{aligned} \tag{13}$$

where $m = 2p_a + o_a - s$ and s is as it is in Theorem 5.

As a consequence of the previous corollary, we easily get the number of quadratic nonresidues in the set $N_{(p-1)/2} + (p - a)$ for $a = 1, 2, 3, 4$ using Propositions 7, 9, 10, and 11. In Tables 1–4 we show these results along with the number of quadratic nonresidues in the set $N_{(p-1)/2} + a$.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The first author acknowledges support from the National Council of Science and Technology (CONACYT) of México (Grant no. 25351).

References

[1] K. Burde, "Zur Verteilung quadratischer Reste," *Mathematische Zeitschrift*, vol. 105, pp. 150–152, 1968.

[2] O. Perron, "Bemerkungen uber die Verteilung der quadratischen Reste," *Mathematische Zeitschrift*, vol. 56, pp. 122–130, 1952.

[3] A. Winterhof, "On the distribution of powers in finite fields," *Finite Fields and their Applications*, vol. 4, no. 1, pp. 43–54, 1998.

[4] A. Brauer, "On a new class of Hadamard determinants," *Mathematische Zeitschrift*, vol. 58, pp. 219–225, 1953.

[5] R. E. A. C. Paley, "On orthogonal matrices," *Journal of Mathematical Physics*, vol. 12, pp. 311–320, 1933.

[6] R. Meza-Moreno and M. Pineda-Ruelas, "Counting quadratic residues," *JP Journal of Algebra, Number Theory and Applications*, vol. 30, no. 2, pp. 151–171, 2013.