ON THE DISTRIBUTION OF CONSECUTIVE TRIPLES OF QUADRATIC RESIDUES AND QUADRATIC NONRESIDUES AND RELATED TOPICS

M. G. MONZINGO
Southern Methodist University, Dallas TX 75275

(Submitted September 1983)

In [1], Andrews proves that the number of consecutive triples of quadratic residues, $n(p)$, is equal to $p/8 + Ep$, where $|Ep| < (1/4)\sqrt{p} + 2$. In addition in [1], it is proved* that for $p \equiv 3 \pmod 4$, $|Ep| < 2$.

In this note, $m(p)$ will denote the number of consecutive triples of quadratic nonresidues. In addition to topics related to those presented in [2], $n(p)$ and $m(p)$ will be determined for all odd primes. Also, the number of triples a, $a + 1$, $a + 2$ will be determined for which

$$\left(\frac{a}{p}\right) = \varepsilon, \quad \left(\frac{a+1}{p}\right) = \eta, \quad \text{and} \quad \left(\frac{a+2}{p}\right) = \nu,$$

where ε, η, and ν each take one of the values ± 1. Finally, an elementary proof of Gauss's "Last Entry" will be presented.

In [2], the decomposition of the integers $1, 2, 3, \ldots, p - 1$ into cells is developed as follows: these integers are partitioned into an array according to whether the consecutive integers are (or are not) quadratic residues. For example, for $p = 11$, the quadratic residues are $1, 3, 4, 5, 9$; hence, the array is

$$1 \qquad 2 \qquad 3, 4, 5 \qquad 6, 7, 8 \qquad 9 \qquad 10.$$

The following are also defined in [2]: a *singleton* is an integer in a singleton cell, e.g., 2; a *left* (*right*) *end point* is the first (last) integer in a nonsingleton cell, e.g., 3 (5); and an *interior point* is an integer, not an end point, in a nonsingleton cell, e.g., 4.

Furthermore, as in [2], the following notation will be used: s, e, and i will denote the numbers of singletons, left end points (or right end points), and interior points, respectively. Values for s, e, and i are given in [2], and these values will be cited later. Quadratic residue and quadratic nonresidue will be denoted by qr and qnr, respectively. The subscript r (n) will be used with s, e, and i to denote the appropriate number of quadratic residues (nonresidues). For example, for $p = 11$, $s_r = 2$ and $e_n = 1$.

<u>Lemma 1</u>

For p an odd prime, $n(p) = i_r$ and $m(p) = i_n$, so that $n(p) + m(p) = i$.

<u>Proof</u>: The middle integer, x, of either type of triple certainly cannot be a singleton or an end point; hence, x must be an interior point. Now, if $a_1, a_2, \ldots, a_k$ are the consecutive interior points of some cell, then there are precisely k consecutive triples: a, a_1, a_2; a_1, a_2, a_3; ...; a_{k-1}, a_k, b, where a and b are the left and right end points, respectively, of this cell.

---

*This case was solved by E. Jacobsthal, "Anwendungen einer Formel aus der Theorie der Quadratischen Reste," Dissertation (Berlin, 1906), pp. 26-32.

Hence, there is a one-to-one correspondence between the number of triples (of either type) and the number of interior points (of the same type), and the conclusion follows.

The next lemma is proven in [2].

Lemma 2

The results in the following table hold.

$(p = \;)$	$8k + 1$	$8k + 3$	$8k + 5$	$8k + 7$
s	$\frac{p - 1}{4}$	$\frac{p + 5}{4}$	$\frac{p + 3}{4}$	$\frac{p + 1}{4}$
e	$\frac{p + 3}{4}$	$\frac{p - 3}{4}$	$\frac{p - 1}{4}$	$\frac{p + 1}{4}$
i	$\frac{p - 9}{4}$	$\frac{p - 3}{4}$	$\frac{p - 5}{4}$	$\frac{p - 7}{4}$

Theorem 1

Let p be a prime $\equiv 3 \pmod 4$.

(a) If $p \equiv 3 \pmod 8$, then $i_r = i_n = n(p) = m(p) = \frac{p - 3}{8}$;

(b) If $p \equiv 7 \pmod 8$, then $i_r = i_n = n(p) = m(p) = \frac{p - 7}{8}$.

Proof: It is shown in [2] that the array of integers $1, 2, \ldots, p - 1$ is symmetric, in that a cell of qr corresponds to a cell of qnr of equal length. (This follows from the fact that a is a qr if and only if $p - a$ is a qnr.) So $i_r = i_n$ and, thus, from Lemma 1, $n(p) = m(p) = i/2$. The conclusion follows by applying Lemma 2.

The fact that for $p \equiv 3 \pmod 4$, both i_r and i_n are determined in Theorem 1 gives justification in also determining s_r, s_n, e_r, and e_n. Hence, this shall be done at this point. At the appropriate juncture, these entities will be determined for primes $\equiv 1 \pmod 4$.

Theorem 2

Let p be a prime $\equiv 3 \pmod 4$.

(a) If $p \equiv 3 \pmod 8$, then $s_r = s_n = \frac{p + 5}{8}$ and $e_r = e_n = \frac{p - 3}{8}$;

(b) If $p \equiv 7 \pmod 8$, then $s_r = s_n = \frac{p + 1}{8}$ and $e_r = e_n = \frac{p + 1}{8}$.

Proof: As in Theorem 1, use symmetry and apply Lemma 2.

Note: The case $p \equiv 1 \pmod 4$ does not follow so easily. The symmetry of the array used in Theorem 1 does not apply; a cell of qr corresponds to another cell of equal length of qr. (This follows from the fact that a is a qr if and only if $p - a$ is a qr.)

Next, as in [1], $S(1)$ will denote the following sum:

$$\sum_{n=1}^{p-3}\left(\frac{n(n+1)(n+2)}{p}\right).$$

Since Lemma 1 relates to the sum of i_r and i_n, in order to solve for i_r and i_n, it is sufficient to discover $i_r - i_n$. Hence, this shall be our goal.

The proof of the next lemma appears in [1]. [The definition and value of $S(\ell)$ will have no bearing on our results; the fact that $S(\ell)/2$, an integer, exists is sufficient.]

Lemma 3

For p a prime $\equiv 1 \pmod 4$,

$$\left(\frac{S(1)}{2}\right)^2 + \left(\frac{S(\ell)}{2}\right)^2 = p.$$

It is well known that p is uniquely expressed as the sum of squares of two integers (other than with a change in sign, or an interchange of the two integers). Furthermore, the two integers have opposite parity. Ultimately, we shall show that $S(1)$, whose value we seek, is such that $S(1)/2$ is ($\pm$) the odd integer which appears in the expression for p in Lemma 3.

The next lemma lists further results from [2] which will be used in determining the value of $S(1)$.

Lemma 4

For p a prime $\equiv 1 \pmod 4$, the following are identities:

(1) $e_n + s_n = \dfrac{p-1}{4}$ and $e_r + s_r = \dfrac{p+3}{4}$. (These follow from an examination of the number of qr and qnr cells in the array.)

(2) $i_r = s_r - 2$ and $i_n = s_n$. (These follow from an examination of the relationship between a qnr singleton and its multiplicative inverse.)

Next, a further investigation of $S(1)$.

Lemma 5

For p a prime $\equiv 1 \pmod 4$,

$$S(1) = \begin{cases} 4(s_r - s_n) - 2, & \text{if } p \equiv 1 \pmod 8, \\ 4(s_r - s_n) - 6, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Proof: First, an examination of $S(1)$ shows that a term in the summation will be positive when $n + 1$ is either a qr singleton, a qnr left or right end point, or a qr interior point. Similarly, the term will be negative when $n + 1$ is either a qnr singleton, a qr left or right end point, or a qnr interior point.

Now, define A and B as follows:

$$\begin{aligned} A &= s_r + 2e_n + i_r \\ &= s_r + 2\left(\frac{p-1}{4} - s_n\right) + (s_r - 2), \quad \text{using Lemma 4;} \end{aligned}$$

$$B = s_n + 2e_r + i_n$$
$$= s_n + 2\left(\frac{p+3}{4} - s_r\right) + s_n, \quad \text{using Lemma 4.}$$

Using the above determination as to when a term is positive or negative, $S(1)$ is almost equal to $A - B$. In the case $p \equiv 5 \pmod 8$, we must subtract 2 from A because 1 and $p - 1$ are singletons counted in s_r which do not appear in the sum (a result of the fact that 1 and $p - 1$ are qr and 2 and $p - 2$ are qnr). Similarly, in case $p \equiv 1 \pmod 8$, we must subtract 2 from B because 1 and $p - 1$ are quadratic residue left and right end points, respectively, which do not appear in the sum (a result of the fact that 1 and $p - 1$ are qr, and, in addition, 2 and $p - 2$ are qr). Finally, incorporating these changes with the appropriate ± 2 to $A - B = 4(s_r - s_n) - 4$, the conclusion follows.

Theorem 3

Let p be a prime $\equiv 1 \pmod 4$ and $p = a^2 + b^2$, where a is positive and odd; then,

$$i_r = n(p) = \begin{cases} \dfrac{p - 15 + 2(-1)^{\frac{a+1}{2}} a}{8}, & \text{if } p \equiv 1 \pmod 8, \\[2ex] \dfrac{p - 7 + 2(-1)^{\frac{a-1}{2}} a}{8}, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$i_n = m(p) = \begin{cases} \dfrac{p - 3 + 2(-1)^{\frac{a-1}{2}} a}{8}, & \text{if } p \equiv 1 \pmod 8, \\[2ex] \dfrac{p - 3 + 2(-1)^{\frac{a+1}{2}} a}{8}, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Proof: The case $p \equiv 1 \pmod 8$ will be examined; the case $p \equiv 5 \pmod 8$ follows similarly. As can be seen from Lemma 5, $S(1)/2$ is odd, and by using Lemma 3, the uniqueness of the odd integer in the sum of squares, and Lemma 5,

$$\frac{4(s_r - s_n) - 2}{2} = \pm a.$$

This, along with Lemma 4, implies that

$$i_r - i_n = \frac{\pm a - 3}{2}.$$

The symmetry of the array guarantees that both i_r and i_n are even; hence, $\pm a - 3$ must be divisible by 4. Since a is odd, $a \equiv 1 \pmod 4$ or $a \equiv 3 \pmod 4$. If $a \equiv 1 \pmod 4$, then we must have $-a - 3$; if $a \equiv 3 \pmod 4$, then we must have $a - 3$. The factor $(-1)^{(a+1)/2}$ yields the appropriate sign. Now, from the table in Lemma 2, $i_r + i_n = (p - 9)/4$. By solving the system of linear equations, we have the conclusion.

For example, let $p = 13$; then, since $13 = 3^2 + 2^2$, $a = 3$. Furthermore, $13 \equiv 5 \pmod{13}$; hence, from Theorem 3, $n(13) = i_r = 0$, and $m(13) = i_n = 2$. Specifically, the two qnr triples occur in the middle cell in the decomposition for $p = 13$,

1   2   3, 4   5, 6, 7, 8   9, 10   11   12.

Finally, having found i_r and i_n, we determine s_r, s_n, e_r, and e_n.

Theorem 4

Let p be a prime $\equiv 1 \pmod 4$ and $p = a^2 + b^2$, where a is odd and positive; then,

$$s_r = \begin{cases} \dfrac{p + 1 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8, \\ \dfrac{p + 9 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$s_n = \begin{cases} \dfrac{p - 3 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8) \\ \dfrac{p - 3 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

$$e_r = \begin{cases} \dfrac{p + 5 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8 \\ \dfrac{p - 3 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8 \end{cases}$$

$$e_n = \begin{cases} \dfrac{p + 1 + 2(-1)^{\frac{a+1}{2}}a}{8}, & \text{if } p \equiv 1 \pmod 8 \\ \dfrac{p + 1 + 2(-1)^{\frac{a-1}{2}}a}{8}, & \text{if } p \equiv 5 \pmod 8 \end{cases}$$

Proof: Use Lemma 4 and Theorem 3.

Theorem 5

Let each of ε, η, and ν take one of the values ± 1, and let T denote the number of triples, a, $a + 1$, $a + 2$, where $a = 1, 2, \ldots, p - 3$, for which

$$\left(\frac{a}{p}\right) = \varepsilon, \quad \left(\frac{a+1}{p}\right) = \eta, \quad \text{and} \quad \left(\frac{a+2}{p}\right) = \nu.$$

Then

$$\begin{aligned} T = \frac{1}{8}\Bigg[(p - 3) &- \varepsilon\left[\left(\frac{-1}{p}\right) + \left(\frac{-2}{p}\right)\right] - \eta\left[1 + \left(\frac{-1}{p}\right)\right] \\ &- \nu\left[1 + \left(\frac{2}{p}\right)\right] - \varepsilon\eta\left[1 + \left(\frac{2}{p}\right)\right] - \varepsilon\nu\left[1 + \left(\frac{-1}{p}\right)\right] \\ &- \eta\nu\left[1 + \left(\frac{2}{p}\right)\right] + \varepsilon\eta\nu S(1)\Bigg]. \end{aligned}$$

Proof: As done with pairs on page 71 of [3] (here, the sums being from 1 to $p - 3$),

$$T = \frac{1}{8}\sum\left[\left(1 + \varepsilon\left(\frac{a}{p}\right)\right)\left(1 + \eta\left(\frac{a+1}{p}\right)\right)\left(1 + \nu\left(\frac{a+2}{p}\right)\right)\right].$$

Next, expand T into eight sums and use the facts that

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0 \quad \text{and} \quad \sum_{a=1}^{p}\left(\frac{a+t}{p}\right)\left(\frac{a+s}{p}\right) = -1 \quad \text{for } (s, t) = 1;$$

then, apply Lemma 5 to substitute for $S(1)$.

We now turn our attention to "The Last Entry," see [4], which refers to the last entry in Gauss's mathematical diary. There, he states:

Theorem (Gauss)

Let p be a prime $\equiv 1 \pmod 4$; then, the number of solutions to

$x^2 + y^2 + x^2y^2 \equiv 1 \pmod p$ is $p + 1 - 2a$,

where $p = a^2 + b^2$, and a is odd.

Note: (1) the sign of a is to be chosen "appropriately," and
(2) there are four points at infinity included in the solution set.

Proof: If either x or y is $\equiv 0 \pmod p$, then the other is $\equiv \pm 1 \pmod p$. In the following, we shall assume that neither x nor y is $\equiv 0 \pmod p$. Now,

(x, y) is a solution $\Longleftrightarrow$

$x^2 + y^2 + x^2y^2 \equiv 1 \pmod p \Longleftrightarrow$

$(x^2 + 1)y^2 \equiv 1 - x^2 \pmod p \Longleftrightarrow$

$x^2 + 1$ and $1 - x^2$ are both qr or $qnr \Longleftrightarrow$

$x^2 + 1$ and $x^2 - 1$ are both qr or qnr [since $p \equiv 1 \pmod 4$] $\Longleftrightarrow$

$x^2 - 1$, x^2, $x^2 + 1$ is such that x^2 is either a qr singleton or a qr interior point [with the exception that for $p \equiv 5 \pmod 8$ and $x \equiv \pm 1 \pmod p$; these values are qr singletons (± 2 are qnr) which have been taken into account]. Hence, the number of solutions is

$4(s_r + i_r) + 8$ for $p \equiv 1 \pmod 8$,

$4(s_r - 2 + i_r) + 8$ for $p \equiv 5 \pmod 8$,

where the "4 times" is for $(\pm x, \pm y)$, and the 8 is for the 4 points at infinity and the 4 solutions $(0, \pm 1)$, $(\pm 1, 0)$. Simplification yields the solution.

REFERENCES

1. G. E. Andrews. *Number Theory*. Philadelphia: W. B. Saunders, 1971.
2. M. G. Monzingo. "On the Distribution of Quadratic Residues." In *A Collection of Manuscripts Related to the Fibonacci Sequence—18th Anniversary Volume*. Ed. V. E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. Santa Clara, CA: The Fibonacci Association, 1980, pp. 94-97.
3. I. M. Vinogradov. *An Introduction to the Theory of Numbers*. New York: The Pergamon Press, 1955.
4. K. Ireland & M. Rosen. *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1982, p. 166.

◆◇◆◇◆