$$H_n = [(1 + \sqrt{p})/2]^n + [(1 - \sqrt{p})/2]^n \qquad (n \geq 1).$$

Now, since α and β satisfy $x^2 - x - [(p - 1)/4] = 0$,

$$\begin{aligned} H_{n+2} &= \alpha^{n+2} + \beta^{n+2} = \alpha^n(\alpha^2) + \beta^n(\beta^2) = \alpha^n(\alpha + [(p - 1]/4]) + \beta^n(\beta + [(p - 1)/4]) \\ &= \alpha^{n+1} + \beta^{n+1} + [(p - 1)/4](\alpha^n + \beta^n) = H_{n+1} + [(p - 1)/4]H_n. \end{aligned}$$

Furthermore, $H_1 = (1 + \sqrt{p})/2 + (1 - \sqrt{p})/2 = 1$ and

$$H_2 = [(1 + \sqrt{p})/2]^2 + [(1 - \sqrt{p})/2]^2 = (p + 1)/2.$$

Thus, the analog of Whitford's generalization of the Fibonacci sequence is the generalization of the Lucas sequence,

$$H_1 = 1,\ H_2 = (p + 1)/2,\ H_{n+2} = H_{n+1} + [(p - 1)/4]H_n \qquad (n \geq 1).$$

Note that, of course, the Lucas sequence corresponds to the case $p = 5$.

The following table, analogous to Whitford's gives the first ten terms of the sequences corresponding to the first five positive integers of the form $4k + 1$.

p	$\frac{p - 1}{4}$	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8	G_9	G_{10}
1	0	1	1	1	1	1	1	1	1	1	1
5	1	1	3	4	7	11	18	29	47	76	123
9	2	1	5	7	17	31	65	127	257	511	1025
13	3	1	7	10	31	61	154	337	799	1810	4207
17	4	1	9	13	49	101	297	701	1889	4693	12249

The following are some of the identities satisfied by the sequences H_n and G_n.

(1) $$\lim_{n \to \infty} \frac{H_{n+1}}{H_n} = (1 + \sqrt{p})/2,$$

(2) $$G_{2n} = G_n H_n,$$

(3) $$H_n^2 = H_{2n} + 2[(1 - p)/4]^n,$$

(4) $$H_n = G_{n+1} + [(p - 1)/4]G_{n-1},$$

(5) $$pG_n^2 = H_{2n} - 2[(1 - p)/4]^n.$$

The major change in the generalized identities occurs where $\alpha\beta = -1$ appears in the Fibonacci/Lucas identities, with $\alpha\beta = (1 - p)/4$ in their generalizations.

REFERENCES

1. A. K. Whitford. "Binet's Formula Generalized." *The Fibonacci Quarterly* 15 (1977):21.
2. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969.

*****

ON THE DISTRIBUTION OF QUADRATIC RESIDUES

M. G. MONZINGO

Southern Methodist University, Dallas, TX 75275

For p an odd prime, each of the integers 1, 2, ..., p - 1 is either a quadratic residue or a quadratic nonresidue. In [1], Andrews proves that the number of pairs of consecutive quadratic residues, the number of pairs of consecutive quadratic nonresidues, etc., are the values listed in Table 1. This note is a further investigation of the distribution of the quadratic residues and quadratic nonresidues which will include new proofs of the results in Table 1.

The integers 1, 2, ..., p - 1 can be partitioned into disjoint cells, in an alternate fashion, according to whether they are consecutive quadratic residues or quadratic nonresidues.

For example, for $p = 13$, the quadratic residues are 1, 3, 4, 9, 10, 12, which lead to the partition:

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

(this is much easier to picture when written vertically).

Notation: In this note, "quadratic residue" and "quadratic nonresidue" will be abbreviated by qr and qnr, respectively. For a fixed odd prime p, s will denote the number of singleton cells, e will denote the number of integers which appear as left end points of cells (or right end points since a nonsingleton cell has a left end point and a right end point), and i will denote the number of integers which are interior points in the cells (that is, excluding the end points). Finally, subscripts r and n will denote quadratic residue and quadratic nonresidue, respectively.

TABLE 1

(p =)	$4k + 1$	$4k + 3$
qr-qr pairs	$(p - 5)/4$	$(p - 3)/4$
qr-qnr pairs	$(p - 1)/4$	$(p + 1)/4$
qnr-qr pairs	$(p - 1)/4$	$(p - 3)/4$
qnr-qnr pairs	$(p - 1)/4$	$(p - 3)/4$

For example, for $p = 13$: 1, 2, 11, 12 form singletons, 6 and 7 are interior points, and 3, 5, 9 are left end points; $s = 4$, $i = 2$, and $e = 3$.

Theorem 1: The partitioning into cells is symmetric in that if, for example, there are k elements in the first cell, then there are k elements in the last cell, etc.

Proof: For $p = 4k + 1$, x is a qr if and only if $p - x$ is a qr. Therefore, for a cell of k consecutive qr (qnr), there is a corresponding cell of k consecutive qr (qnr). For $p = 4k + 3$, x is a qr if and only if $p - x$ is a qnr. Therefore, for a cell of k consecutive qr (qnr), there is a corresponding cell of k consecutive qnr (qr).

Corollary 1: If the number of cells is odd, then the middle cell must contain an even number of elements.

Proof: If the middle cell contained an odd number of elements, then due to symmetry (the number of elements in cells preceding the middle cell equaling the number of elements in cells following the middle cell), the partition would contain an odd number of elements. But, this would contradict the fact that there are $p - 1$ elements in the partition.

Corollary 2: The first and last cells are singletons if and only if $p \not\equiv \pm 1 \pmod{8}$.

Proof: The conclusion follows from the fact that 1 is a qr, 2 is a qr if and only if $p \equiv \pm 1 \pmod{8}$, and the partition is symmetric.

The following lemmas, involving the Legendre symbol, are proven in [1]. Lemma 1 also appears as an exercise in [2].

Lemma 1: $\displaystyle\sum_{a=1}^{p-2} \left(\frac{a(a + 1)}{p}\right) = -1.$

In Lemma 2, $\left(\frac{0}{p}\right)$ is defined to be 0.

Lemma 2: $\displaystyle\sum_{a=2}^{p} \left(\frac{(a - 1)(a + 1)}{p}\right) = -1.$

Theorem 2: There are $(p + 1)/2$ cells.

Proof: In the summation in Lemma 1, there are $(p - 3)/2$ plus ones and $(p - 1)/2$ minus ones, since there are $p - 2$ terms with one more minus than plus. Now,

$$\left(\frac{a(a + 1)}{p}\right) = -1$$

if and only if a is in one cell and $a + 1$ is in the next cell. Thus, there are $(p - 1)/2 + 1 = (p + 1)/2$ cells.

The result in the next corollary will be extended considerably in a later theorem.

Corollary 3: The partition must contain at least two singletons, that is, $s \geq 2$.

Proof: Suppose each cell contained at least two elements; then, there are at least

$$2\,\frac{(p+1)}{2} = p + 1$$

elements, a contradiction. By Corollary 1, the middle cell is not a singleton; hence, by symmetry, there must be at least two singletons.

Theorem 3: The following equations are identities:

(1) $$s + e = (p + 1)/2,$$

(2) $$e + i = (p - 3)/2,$$

(3) $$s = i + 2,$$

(4) $$s + 2e + i = p - 1.$$

Proof: Part (1) follows from Theorem 2, since each cell is either a singleton or has a left end point. As seen earlier, there are $(p - 3)/2$ plus ones in the summation in Lemma 1. Now,

$$\left(\frac{a(a + 1)}{p}\right) = 1$$

if and only if a and $a + 1$ are in the same cell. Hence, a must be a left end point or an interior point of a cell, and (2) follows. Part (3) follows from the subtraction of part (2) from part (1). Part (4) follows from the fact that the number of left end points equals the number of right end points, and there are $p - 1$ integers in the partition.

A counterpart to the next lemma will follow Theorem 4.

Lemma 3: Let $p = 4k + 1$; then, a is a qnr singleton if and only if a', the inverse of a, is a qnr interior point.

Proof: First note that $a \neq 1,\ p - 1$. The conclusion follows from the fact that

$$\left(\frac{a - 1}{p}\right) = 1,\ \left(\frac{a}{p}\right) = -1,\ \left(\frac{a + 1}{p}\right) = 1, \text{ if and only if}$$

$$\left(\frac{a' - 1}{p}\right) = -1,\ \left(\frac{a'}{p}\right) = -1,\ \left(\frac{a' + 1}{p}\right) = -1, \text{ where}$$

$$\left(\frac{a' - 1}{p}\right) = \left(\frac{(1 - a)a'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a - 1}{p}\right)\left(\frac{a'}{p}\right) = 1 \cdot 1 \cdot (-1) = -1.$$

Theorem 4: The results in Table 1 hold.

Proof: If $p = 4k + 3$, then there are an even number of cells, the first cell qr and the last cell qnr. A qr followed by a qnr occurs only between a cell of qr followed by a cell of qnr. Hence, there are $1/2\frac{(p + 1)}{2}$ pairs of cells of this type, and so $(p + 1)/4$ pairs of qr followed by qnr. A qnr followed by qr occurs only between a cell of qnr followed by a cell of qr. These pairs occur starting with the second cell and ending with the next to the last cell, yielding $1/2\left[\frac{(p + 1)}{2} - 2\right] = \frac{(p - 3)}{4}$ pairs. Recalling the notation and the symmetry discussed in Theorem 1, $e_r = e_n$. Similarly, $i_r = i_n$. From (2) of Theorem 3, $e_r + e_n + i_r + i_n = (p - 3)/2$, which yields $e_r + i_r = e_n + i_n = (p - 3)/4$. Now, a pair of consecutive qr (qnr) occurs only in a nonsingleton cell, and there are precisely as many such pairs as there are qr (qnr) interior points plus one per such cell. This total is precisely $e_r + i_r(e_n + i_n)$.

If $p = 4k + 1$, then there is an odd number of cells, the first and last consisting of qr. This implies that the number of pairs of a qr followed by a qnr (first cell to second cell, third cell to fourth cell, etc.) equals the number of pairs of a qnr followed by a qr (second cell to third cell, fourth cell to fifth cell, etc.). Since these pairs result in $(p - 1)/2$ minus ones in Lemma 1, there are $(p - 1)/4$ pairs of each type. In particular, it follows that

$$e_n + s_n = \frac{(p - 1)}{4}.$$

Now, from Lemma 3, $s_n = i_n$, and so, from (2), $e_r + e_n + i_r + i_n = (p - 3)/2$. Therefore,

$e_r + i_r = (p - 3)/2 - (e_n + s_n) = (p - 5)/4$. Also, $e_n + i_n = e_n + s_n = (p - 1)/4$. And the conclusion follows as in the previous case.

Lemma 4: Let $p = 4k + 3$ and a an element not its own inverse; then, a is a qr singleton if and only if a', the inverse of a, is a qr right end point.

Proof: The conclusion follows from the fact that

$$\left(\frac{a-1}{p}\right) = -1,\ \left(\frac{a}{p}\right) = 1,\ \left(\frac{a+1}{p}\right) = -1, \text{ if and only if}$$

$$\left(\frac{a'-1}{p}\right) = 1,\ \left(\frac{a'}{p}\right) = 1,\ \left(\frac{a'+1}{p}\right) = -1, \text{ where}$$

$$\left(\frac{a'-1}{p}\right) = \left(\frac{(1-a)a'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a-1}{p}\right)\left(\frac{a'}{p}\right) = (-1)(-1)\cdot 1 = 1.$$

Lemma 5: Suppose that $a \neq p - 1, p$; then, in the summation in Lemma 2, $\left(\frac{(a-1)(a+1)}{p}\right) = 1$ if and only if a is a singleton or an interior point.

Proof: The Legendre symbol $\left(\frac{(a-1)(a+1)}{p}\right) = 1$ if and only if $a - 1$ and $a + 1$ are both qr or both qnr. If a is of the same type, then a is an interior point; if not, then a is a singleton.

TABLE 2

$(p =)$	$8k + 1$	$8k + 3$	$8k + 5$	$8k + 7$
s	$(p - 1)/4$	$(p + 5)/4$	$(p + 3)/4$	$(p + 1)/4$
e	$(p + 3)/4$	$(p - 3)/4$	$(p - 1)/4$	$(p + 1)/4$
i	$(p - 9)/4$	$(p - 3)/4$	$(p - 5)/4$	$(p - 7)/4$

Theorem 5: The results in Table 2 hold.

Proof: With the use of Equations (1) and (3) of Theorem 3, the conclusions will follow once the results are established for the number of singleton cells. For the cases $8k + 3$ and $8k + 7$ consider Lemma 4. If $p = 8k + 7$, then the first and the last cells are not singletons since 2 is a qr. Thus, no singleton is its own inverse, and $s = e$ (recall the symmetry). From (1) of Theorem 3, $s = (p + 1)/4$. If $p = 8k + 3$, 1 and $p - 1$ are both singletons not included in Lemma 4; hence, $s = e + 2$. From (1), $s = (p + 5)/4$. For the cases $8k + 1$ and $8k + 5$, consider Lemma 5. If $p = 8k + 1$, neither 1 nor $p - 1$ is a singleton (2 is a qr), and so there are $s + i + 1$ plus ones in the summation in Lemma 5 (the "1" is for the case $a = p$). As in Lemma 2, there are $(p - 3)/2$ plus ones in the summation in Lemma 5 [also $(p - 1)/2$ minus ones and one zero]. Therefore, $s + i + 1 = (p - 3)/2$ and since $s = i + 2$ [part (3) of Theorem 3], $s = (p - 1)/4$.

If $p = 8k + 5$, then 1 and $p - 1$ are singletons not included in Lemma 5; thus, there are $(s - 2) + i + 1$ plus ones. Then, $(s - 2) + i + 1 = (p - 3)/2$ and $s = i + 2$ yield $s = (p + 3)/4$.

It should be noted that Lemma 5 might have been used to prove all cases in Theorem 5. Lemma 4 was used for the two cases to which it applied because it was so easy to apply and the result in Lemma 4 was itself interesting.

REFERENCES

1. George E. Andrews. *Number Theory*. Philadelphia: W. B. Saunders Co., 1971, pp. 128-138.
2. David M. Burton. *Elementary Number Theory*. Boston: Allyn and Bacon, Inc., 1976, p. 202.

*****