Internat. J. Math. & Math. Sci.
Vol. 5 No. 3 (1982) 565-584

A NEW FORMULATION OF THE LAW OF OCTIC RECIPROCITY FOR PRIMES $\equiv \pm 3$ (MOD 8) AND ITS CONSEQUENCES

RICHARD H. HUDSON
and
KENNETH S. WILLIAMS
Department of Mathematics
Carleton University
Ottawa, Canada K1S 5B6

(Received May 18, 1981 and in revised form September 1, 1981)

ABSTRACT. Let p and q be odd primes with $q \equiv \pm 3 \pmod 8$, $p \equiv 1 \pmod 8 = a^2 + b^2 = c^2 + d^2$ and with the signs of a and c chosen so that $a \equiv c \equiv 1 \pmod 4$. In this paper we show step-by-step how to easily obtain for large q necessary and sufficient criteria to have $(-1^{(q-1)/2} q^{(p-1)/8} \equiv (a-b)d/ac)^j \pmod p$ for $j = 1,\ldots,8$ (the cases with j odd have been treated only recently [3] in connection with the sign ambiguity in Jacobsthal sums of order 4). This is accomplished by breaking the formula of A.E. Western into three distinct parts involving two polynomials and a Legendre symbol; the latter condition restricts the validity of the method presented in section 2 to primes $q \equiv 3 \pmod 8$ and significant modification is needed to obtain similar results for $q \equiv \pm 1 \pmod 8$. Only recently the author has completely resolved the case $q \equiv 5 \pmod 8$, $j = 1,\ldots,8$ and a sketch of the method appears in the closing section of this paper.

Our formulation of the law of octic reciprocity makes possible a considerable extension of the results for $q \equiv \pm 3 \pmod 8$ of earlier authors. In particular, the largest prime $\equiv 3 \pmod 8$ treated to date is $q = 19$, by von Lienen [6] when $j = 4$ or 8 and by Hudson and Williams [3] when $j = 1,2,3,5,6,$ or 7. For $q = 19$ there are 200 distinct choices relating a,b,c,d which are equivalent to $(-q)^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod p$ for one of $j = 1,\ldots,8$. We give explicit results in this paper for primes as large as $q = 83$ where there are 3528 distinct choices.

This paper makes several other minor contributions including a computationally efficient version of Gosset's [2] formulation of Gauss' law of quartic reciprocity, observations on sums $\sum y_{i,j}$ where the $y_{i,j}$'s are the defining parameters for the distinct choices mentioned above, and proof that the results of von Lienen [6] may not only be appreciably abbreviated, but may be put into a form remarkably similar to the case in which q is a quadratic residue but a quartic non-residue of p.

An important contribution of the paper consists in showing how to use Theorems 1 and 3 of [3], in conjunction with Theorem 4 of this paper, to reduce from $(q+1/4)^2$ to $(q-1)/2$ the number of cases which must be considered to obtain the criteria in Theorems 2 and 3.

KEY WORDS AND PHRASES. *Quartic and octic residuacity criteria, A.E. Western's formula, binary quadratic forms.*

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES. *Primary 10A15; Secondary 10G15.*

1. INTRODUCTION.

Let p be a prime $\equiv 1 \pmod 4$ so that $p = a^2 + b^2$ and choose the sign of a so that $a \equiv 1 \pmod 4$. Let $q \neq p$ be an odd prime. Necessary and sufficient criteria in terms of a and b for p to satisfy $(-1)^{(q-1)/2}\, q^{(p-1)/4} \equiv (b/a)^j \pmod p$, $j = 1,2,3,4$, when $q < 50$, have been obtained by Cunningham [1] when j is even, see [8, p. 248], and by Gosset [2] when j is odd. Contained in this paper as a necessary preliminary (section 2, Theorem 1), is a computationally efficient form of Gosset's formulation of Gauss' law of quartic reciprocity which makes it possible to extend considerably the results of Cunningham and Gosset.

The much more difficult problem of giving necessary and sufficient criteria in terms of a,b,c, and d for a prime $p \equiv 1 \pmod 8) = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$, to satisfy $(-1)^{(q-1)/2}\, q^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod p$ has been treated more recently by several authors, most notably by von Lienen [6], in the case that q is a quartic residue ($\Longleftrightarrow j = 4$ or $8 \Longleftrightarrow$ when $((a-b)d/ac)^j \equiv \pm 1 \pmod p)$). The results of von Lienen [6] ($q \leq 41$) extend considerably those of earlier authors (see references in [6]) and clearly entail an enormous amount of work. Very recently Hudson and Williams [3] have given similar criteria for $q \leq 19$ when $j = 1,2,3,5,6$, and 7.

These were obtained for $j = 1,3,5,7$, i.e., when $q^{(p-1)/8}$ is a primitive eighth root of unity, as a necessary step in resolving the remaining outstanding problem regarding the sign ambiguity in the Jacobsthal sums of order 4 (see, e.g., [9],[10]).

The arguments given in Theorems 1 and 3 of [3] for $q = 19$, in conjunction with Theorem 1 of this paper, suggested to the author a strategy for computerizing Western's formula, at least when $q \equiv \pm 3 \pmod 8$, thus making it possible to greatly extend all earlier results for these primes.

Fascinating symmetries exist interrelating the results in Theorem 2,3, and 4. Of particular interest is the fact that the k_j's in all three Theorems can be made to agree in magnitude, sign, and order provided that a very special order is chosen for the parameters u_j relating c and d (see [3, Theorem 4] and the remark following Theorem 3 of this paper).

The extent to which computerization contributes to the extension of earlier results is indicated by the fact that when $q = 19$ (the largest prime $\equiv 3 \pmod 8$ considered by von Lienen [6] or Hudson and Williams [3]), there are only 200 distinct choices relating the parameters a,b,c, and d which are equivalent to $(-q)^{(p-1)/8} \equiv ((a-b)d/ac)^j \pmod p$ for one of the possible values of j, $j=1,\dots,8$ (25 for each j). When $q = 83$ there are a staggering 3528 distinct choices (21 x 21 x 8)! However, the method described here makes it possible to go far beyond $q = 100$.

A more interesting contribution of this paper from a theoretical standpoint is the content of Theorem 4. If one looks at von Lienen's [6, p. 115] result for $q = 19$ and the results for $q = 19$ in Theorems 2 and 3, they appear as results from different planets. Theorem 4 makes it clear that von Lienen's [6] results may be put into a far more compact form and, more significantly, into a form so closely analogous to Theorem 3 that one can immediately read off all results in the cases that $(-q)^{(p-1)/8} \equiv \pm 1 \pmod p$, $q \equiv 3 \pmod 8$, from the results when $(-q)^{(p-1)/8} \equiv b/a \pmod p$. Indeed, it is shown (with $a \equiv c \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 8$)) that the value of $\gamma_{i,j}$ such that $b \equiv \gamma_{i,j}\, c \pmod q \iff (-q)^{(p-1)/8} \equiv b/a \pmod p$, $a \equiv \gamma_i b \pmod q$, is identical with the value of $\gamma_{i,j}$ such that $a \equiv \gamma_{i,j} c \pmod p \iff$

$(-q)^{(p-1)/8} \equiv 1 \pmod{p}$, $b \equiv \lambda_i a \pmod{q}$, if $q \equiv 3 \pmod{16}$; $\gamma_{i,j}$ changes sign (but not magnitude) if $q \equiv 11 \pmod{16}$.

The case $q \equiv 5 \pmod{8}$ is treated in section 5, followed by Tables and Examples.

2. PROGRAMMING THE LAW OF QUARTIC RECIPROCITY FOR PRIMES q AND THE LAW OF OCTIC RECIPROCITY FOR PRIMES q ≡ 3 (MOD 8).

Elsewhere the author and Williams [4] have shown that Gosset's [2] formulation of the law of quartic reciprocity can be used to prove the following computationally useful Theorem.

THEOREM 1. Let q be a prime ≥ 7, $p \equiv 1 \pmod{4} = a^2 + b^2$, $a \equiv 1 \pmod{4}$,

$$q = \begin{cases} 4n+1 & \text{if} \quad q \equiv 1 \pmod{4} \\ 4n-1 & \text{if} \quad q \equiv 3 \pmod{4}. \end{cases}$$

Then $(-1)^{(q-1)/2}\, q^{(p-1)/4} \equiv +1, -1$, or $\pm b/a \pmod{p}$ respectively according as $\lambda(a \equiv \lambda b \pmod{q})$ satisfies

$$\text{(a)} \qquad \sum_{\substack{k=0 \\ n-k \text{ odd}}}^{n} A(k,n)\binom{n}{k}\lambda^k \equiv 0 \pmod{q},$$

$$\text{(b)} \qquad \sum_{\substack{k=0 \\ n-k \text{ even}}}^{n} A(k,n)\binom{n}{k}\lambda^k \equiv 0 \pmod{q},$$

$$\text{(c)} \qquad \sum_{k=0}^{n} A(k,n)\binom{n}{k}\lambda^k \equiv 0 \pmod{q},$$

$$\text{where } A(k,n) = \begin{cases} +1 & \text{if} \quad n-k \equiv 0,1 \pmod{4}, \\ -1 & \text{if} \quad n-k \equiv 2,3 \pmod{4}, \end{cases}$$

where $+b/a$ applies when $q \equiv 3 \pmod{4}$ and $-b/a$ when $q \equiv 1 \pmod{4}$.

Values of λ such that $(-1)^{(q-1)/2}\, q^{(p-1)/4} \equiv \pm b/a \pmod{p}$ are simply the negatives of the values of λ satisfying (c) above and, thus, clearly do not require separate computation.

As mentioned in the introduction, Theorem 1 allows one to considerably extend the results of Cunningham [1] (see [8, p. 248]), and Gosset [2]. For example, when $q = 67$, part (c) of Theorem 1 asserts that the values of $\lambda(a \equiv \lambda b \pmod{q}$ for whi

$(-q)^{(p-1)/4} \equiv b/a \pmod{p}$, $p \equiv 1 \pmod{4} = a^2 + b^2$, $a \equiv 1 \pmod{4}$, are the roots (mod q) of

$$\lambda^{17} + 17\lambda^{16} + 65\lambda^{15} + 57\lambda^{14} + 35\lambda^{13} + 24\lambda^{12} + 19\lambda^{11} + 49\lambda^{10} + 56\lambda^{9}$$
$$+ 56\lambda^{8} + 48\lambda^{7} + 19\lambda^{6} + 24\lambda^{5} + 35\lambda^{4} + 57\lambda^{3} + 65\lambda^{2} + 17\lambda + 1 \,. \tag{2.1}$$

With a little patience (or letting the computer do the work) one sees that (2.1) factors as

$$(\lambda - 66)(\lambda - 14)(\lambda + 24)(\lambda - 20)(\lambda - 57)(\lambda - 23)(\lambda - 35)(\lambda - 30)(\lambda - 38) \ldots$$
$$(\lambda - 26)(\lambda - 49)(\lambda - 33)(\lambda - 65)(\lambda - 19)(\lambda - 60)(\lambda - 39)(\lambda - 55). \tag{2.2}$$

Of course, this factorization yields at once the desired values of λ. Parenthetically, we note that the factors in (2.2) after $\lambda - 66$ have been ordered in reciprocal pairs $(14)(24) \equiv (20)(57) \equiv \ldots \equiv (39)(55) \equiv 1 \pmod{67}$) and the sum of the roots of (2.1) is $\equiv -(q+1)/4 \pmod{q}$. Of course, the reason for the latter congruence is a well known consequence of algebra; see e.g., [7, Theorem 15, p. 84]. More significantly, from the point of octic reciprocity (as we will see in later analysis) is the fact that -1 is a root of (c) if $q \equiv 3 \pmod{16}$ but 1 is a root of (c) if $q \equiv 11 \pmod{16}$.

Programming Western's [8] (see [3], section 2) law of reciprocity requires carrying through step-by-step the process outlined in the proofs of Theorems 1 and 3 of [3]. The first step is to find the values of λ satisfying Theorem 1, parts (a), (b), and (c).

We proceed now for $q \equiv 3 \pmod{8}$ as follows.

STEP 2. Find all values of μ, $\mu = 0,1,\ldots,q-1$ for which $\mu^2 + 2$ is a quadratic residue of q.

STEP 3. Find all values of μ, $\mu = 0,1,\ldots,q-1$ for which $\mu^2 + 2$ is a quadratic non-residue of q.

STEP 4. Taking $m = \frac{q-1}{2}$ and setting

$$H(x) = \sum_{k=0}^{m} (-2)^{\left[\frac{m-k}{2}\right]} \binom{m}{k} x^k = \sum_{k=0}^{m} h_k x^k \,,$$

give the polynomials in $Z_q[x]$,

$$F(x) = h_{m-1}\, x^{m-1} + h_{m-3}\, x^{m-3} + h_{m-5}\, x^{m-5} + \dots + h_0,$$

$$G(x) = h_m x^m + h_{m-2}\, x^{m-2} + h_{m-4}\, x^{m-4} + \dots + h_1\, x.$$

STEP 5. Evaluate $F(x)$ and $G(x)$ for the values of μ in Steps 2 and 3 (for $q = 19$, $F(x) = 9x^8 + 3x^6 + 10x^4 + 16x^2 + 16$, $G(x) = x^9 + 4x^7 + 10x^5 + 12x^3 + 11x$).

EXAMPLE. For the values of μ obtained in Step 3 it is easy to show (indeed, easy to show for arbitrary q) that $G(\mu)$ vanishes. Moreover, with $p \equiv 1 \pmod 8) = a^2 + b^2 = c^2 + 2d^2$, $c \equiv \mu d \pmod q$,

$$F(x) = 9x^8 + 3x^6 + 10x^4 + 16x^2 + 16 \equiv \begin{cases} 16 \text{ if } x = \mu = 0,\ \pm 1,\ \pm 5 \\ 3 \text{ if } x = \mu = \pm 4,\ \pm 7. \end{cases} \tag{2.3}$$

Comparing (2.3) with (3.10) of [3] we see that we have, in fact, evaluated the coefficient of $i\sqrt{2}$ in the computation of $(\mu + i\sqrt{2})^9$ (the most tedious step in applying Western's [8] formula).

STEP 6. Compute $\dfrac{\mu^2 + 2}{\mu^2(\lambda^2 + 1)}$ when $\mu \not\equiv 0$ (q) and $\dfrac{1}{\lambda^2 + 1}$ when $\mu \equiv 0$ (q) for the values λ satisfying Theorem 1, part (b), and the values μ given in Step 2 (see Step 11 if q is large).

STEP 7. Compute $\dfrac{\lambda^2 + 1}{\mu^2 + 2}$ for the values λ satisfying Theorem 1, part (c), and the values μ given in Step 3.

STEP 8. Take the square root (mod q) of all entries in Steps 6 and 7 choosing for the moment the positive square root $\le (q - 1)/2$ (the actual sign to be fixed later).

STEP 9. Evaluate $\hat{R}(\lambda) = (\lambda^2 + 1)^{\left[\frac{q}{8}\right]} R(\lambda)$ where $R(\lambda)$ is the polynomial given on the left-hand side of Theorem 1, part (a); e.g., for $q = 19$, $\hat{R}(\lambda) = (\lambda^2 + 1)^2(1 + 9\lambda^2 + 5\lambda^4)$ (Note that $R(\lambda)$ is the imaginary part of $(\lambda + i)^{(q+1)/4}$).

STEP 10. Evaluate $\hat{R}(\lambda)$ for the values of λ given by Theorem 1, part (c) (see (3.9) of [3]) for the values of λ given by Theorem 1, part (b) (see (5.8) of [3]).

From Steps 7 and 8 we have obtained, up to sign, the values of β given in Theorem 1 of [3] and the values of γ given in Theorem 3 of [3]. Since $\frac{\lambda}{\beta k} \equiv \gamma (\mathrm{mod}\ q)$ (see row 2 of Table 2 and (3.16) of [3], one crucial missing element remains in the evaluation of Western's [8] formula, namely the determination of the sign of the γ's and the sign of the k's. (Once these are determined all the results in Theorems 2 and 3 follow at once). In [3] the author has shown that for primes $q\equiv 3$ (mod 8) (but not, unfortunately, for primes $q \equiv 5$ (mod 8)) the signs of the γ's and the k's in Theorem 2 may be completely determined through knowledge of the Legendre symbol $(\frac{\beta}{q})$, and the signs of the γ's and k's in Theorem 3 may be completely determined through knowledge of the Legendre symbol $(\frac{\mu\gamma}{q})$, $c \equiv \mu d$ (mod q).

T● obtain Theorem 2 we need only multiply together the three parts of Western's formula, namely the values $F(\mu_j)$, $1 \le j \le (q + 1)/4$, the values $\hat{R}(\lambda_i)$, $1\le i\le(q+1)/4$, and the Legendre symbols $(\frac{\beta i,j}{q})$, $1 \le i, j \le (q + 1)/4$. If the product of the 3 numbers is $(\frac{q+1}{2})$ then $(-q)^{(p-1)} \equiv (a - b)d/ac$ (mod p) (the $\frac{1}{2}$ in $\phi = e^{2\pi i/8} = (1 + i\sqrt{2})/2$ is interpreted as the positive integer $< q$ and $\equiv \frac{1}{2}$ (mod q), i.e., $(q + 1)/2$, see (3.10), (3.11), and (3.12) of [3]).

STEP 11. A great deal of CPU time may be saved if one only computes values in the first and second rows and first and second columns if $q \equiv 11$ (mod 16) and in the first and last rows and first and second columns if $q \equiv 3$ (mod 16). Indeed, in extending Theorem 2 beyond $q = 100$, this enormous time-saving device should be entered into the program no later than Step 6 (we were wasteful because we had no proof of the validity of this simplification until after we ran our program for $q < 100$). Henceforth, for brevity, we call the first and second rows the relevant rows if $q \equiv 11$ (mod 16) and the second and last rows the relevant rows if $q \equiv 3$ (mod 16). (Note, e.g., the second row, second column, of Table 2 contains the entry $\gamma_{1,1} = 13$).

The $(q + 1)/4$ entries $\gamma_{i,j}$ which appear in the relevant row (and in the statement of Theorem 2) are now obtained very easily as follows:

$$\begin{aligned} \gamma_{i,j} &= \lambda_i/\beta_{i,j}, \quad 1 \le i \le (q+1)/4, \quad 1 \le j \le (q+1)/4, \\ \frac{\gamma_{i,j}}{q} &= -1 \quad \text{if} \quad F(\mu_j) = \hat{R}(\lambda_i) \\ \frac{\gamma_{i,j}}{q} &= +1 \quad \text{if} \quad F(\mu_j) \ne \hat{R}(\lambda_i). \end{aligned} \tag{2.4}$$

The values of k_j, $1 \le j \le (q+1)/4$ are obtained in Theorem 2 as follows. Each entry in the relevant row is multiplied by 1 or by -1 according as the entry $\lambda_i/\beta_{i,j}$ in the relevant row and second column is 1 or -1 (in order to make $k_1 = 1$). Then the k_j's, $1 \le j \le (q+1)/4$, are simply the reciprocals (mod q) of the entries in the relevant row.

EXAMPLE. For q = 11, q = 19, we have at the end of Step 11 the following values in the relevant rows and columns.

(a): q = 11

$R(\lambda_i)$ \ $F(\mu_j)$		4	4	7	
	λ_i \ $\lvert\mu_j\rvert$	0	2	4	Row 1
4	1	-1	2	4	2
7	3	4			3
7	4	5			4
	Column 1	2	3	4	

(b): q = 19

$R(\lambda_i)$ \ $F(\mu_j)$		16	16	3	16	3	
	λ_i \ $\lvert\mu_j\rvert$	0	1	4	5	7	Row 1
3	3	9					2
3	7	5					3
16	11	2					4
3	13	-3					5
3	18	1	-8	-6	9	-5	6
	Column 1	2	3	4	5	6	

where the signs have been assigned so that $\left(\frac{\beta_{i,j}}{q}\right) = -1$ if $(\hat{R}(\lambda_i))(F(\mu_j)) \equiv -\frac{1}{2}$ (mod q) and $\left(\frac{\beta_{i,j}}{q}\right) = +1$ if $(\hat{R}(\lambda_i))(F(\mu_j)) \equiv \frac{1}{2}$ (mod q). One may use (2.3) and the example following Step 9 to check this assertion for q = 19; q = 11 may be easily checked once $F(x) = 5x^4 + 2x^2 + 4$ and $\hat{R}(\lambda) = (\lambda^2 + 1)(3\lambda^2 - 1)$ have been evaluated.

Multiplying the second row in (a) by -1 (since the second row, second column entry is -1) and then taking reciprocals of entries in the second row of (a) we have $(1)^{-1} \equiv 1$ (mod 11), $(-2)^{-1} \equiv 5$ (mod 11), $(-4)^{-1} \equiv 8$ (mod 11). Moreover, $1 \div -1 \equiv 10$ (mod 11), $3 \div 4 \equiv 9$ (mod 11), $4 \div 5 \equiv 3$ (mod 11). Consequently, k_1, k_2, and k_3 in Theorem 2, for q = 11, are 1,5, and 8 respectively, and the long desired $\gamma_{1,1}$, $\gamma_{2,1}$, $\gamma_{3,1}$ are 10, 9, and 3. (Note that in the Tables, the $\gamma_{i,j}$'s begin in the 2nd and end in the (q+5)/4-th rows.

Similarly, taking reciprocals of entries in the last row of (b) above, we have $(1)^{-1} \equiv 1$ (19), $(-8)^{-1} \equiv 7(19)$, $(-6)^{-1} \equiv 3(19)$, $9^{-1} \equiv 17(19)$ and $(-5)^{-1} \equiv 15(19)$; moreover, $3 \div 9 \equiv 13(19)$, $7 \div 5 \equiv 9(19)$, $11 \div 2 \equiv 15(19)$, $13 \div -3 \equiv 2(19)$ and $18 \div 1 \equiv 18(19)$, yielding Theorem 2, for q = 19.

Glancing at Tables 1 and 2 it should be clear how to generate the $((q-3)/4)^2$ entries not listed, namely by simple multiplication (mod q) (a great saving over going through the entire process described above). For example, the entry 2 in the last row and last column of Table 1, $(\gamma_{3,3})$, is simply $\gamma_{3,1}\, k_3 \equiv 3 \cdot 8 \equiv 2 \pmod{11}$. (The author showed in Theorem 4 of [3] that the k_j's in Theorem 2 which render possible the reduction of cases which need formally be considered coincide with the k_j's in Theorem 3 in magnitude and can be ordered alike (see remark after Theorem 3). It is clear on numerical grounds that they agree also in sign. A proof of this conjecture would be very interesting. Although the time saved by considering just two rows and columns is not great when q = 11, since only 4 cases are eliminated (see (a)), when q = 83, a whopping $((83 - 3)/4)^2 = 400$ cases are eliminated (something even a computer can begin to appreciate).

In proving Theorem 3 which yields values of $\gamma_{i,j}$, $b \equiv \gamma_{i,j}c \pmod q$, for which $(-q)^{(p-1)/8} \equiv b/a \pmod p$, one must multiply together values $G(\mu_j)$, $1 \le j \le (q+1)/4$, $\hat{R}(\lambda_i)$, $1 \le i \le (q+5)/8$, and the Legendre symbols $\frac{\mu_j\gamma_{i,j}}{q}$ $(c \equiv \mu_j d \pmod q))$. If the product of these three numbers is +1, then $(-q)^{(p-1)/8} \equiv b/a \pmod p$, as is evident from (5.7), and (5.8)-(5.11) of [3].

This immediately yields the rule for determining the sign of $\gamma_{i,j}$.

STEP 12. In determining values of $\gamma_{i,j}$, $b \equiv \gamma_{i,j}c \pmod q$ for which $(-q)^{(p-1)/8} \equiv b/a \pmod p$, the relevant rows and columns are the second both for $q \equiv 3$ and 11 (mod 16). The other values may be obtained by straightforward multiplication modulo q.

EXAMPLE: $q = 19$. At the conclusion of Step 10, and after assigning signs in the second row and column, we have

$R(\lambda_i)$ \ $G(\mu_j)$		1	-1	1	-1	-1	
	$\lvert\lambda_i\rvert$ \ $\lvert\mu_j\rvert$	0	2	3	8	9	Row 1
1	0	1	7	-4	-2	3	2
-1	2	2	5	8	4	6	3
1	5	7	8	9	5	2	4
	Column 1	2	3	4	5	6	

($\lvert\mu_1\rvert = 0 \Longleftrightarrow d \equiv 0 \pmod q$ with an abuse of notation) and the signs of $\gamma_{1,1} = 1$, $\gamma_{1,2} = 2$, $\gamma_{1,3} = 7$ are chosen as in (5.17) of [3]). For example, the negative sign is given for the entry $\gamma_{1,4}$ (row 2, column 5) as, then, $\hat{R}(\lambda_1)(G(\mu_4))\left(\frac{\mu_4\gamma_{1,4}}{19}\right) = (1)(-1)\left(\frac{-16}{19}\right) = +1$, precisely the required condition. Indeed, we could obtain the entry $\gamma_{3,5} = 2$ in the last row and last column by precisely the same reasoning ($\hat{R}(\lambda_3)G(\mu_5)\left(\frac{18}{19}\right) = +1$) but how very much simpler it is to simply note $\gamma_{3,1} \times \gamma_{1,5} = 7 \times 3 = 21 \equiv 2 \pmod{19}$!

The fact that there are only $((q+5)/8) + 1$ columns listed in Tables 3-4 rather than the $((q+1)/4) + 1$ columns that are listed in Tables 1-2 follows from the fact (see Step 10) that values of γ given by Theorem 1, part (b), occur in pairs (each the negative of the other) but this is not so for the values of γ given by Theorem 1, part (c). Since, in Theorem 3 (or equivalently in Tables 3-4) the value of $\gamma_{i,j}$ is independent of the choice of sign of γ_i, it is necessary to list only $((q+1)/2) + 1 = (q+5)/8$ columns of $\gamma_{i,j}$'s which makes Tables 3-4 slightly more compact. On the other hand, 0, ±2, ±5 may be thought of as five distinct γ_i's for $q = 19$ (see Table 4), as it is only by means of this delineation that one can show that the row sums in Tables 3-4 must be a multiple of $q(1 + 2 + 2 + 7 + 7 = 19)$. (It is in the latter sense that we say in the introduction that there are 3528 distinct choices when $q = 83$ $((83+1)/4)^2 \times 8 = 3528$)).

3. NECESSARY AND SUFFICIENT CONDITIONS.

We prove necessary and sufficient conditions for primes $p \equiv 1 \pmod 8 =$

$a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$, to satisfy $(-q)^{(p-1)/8} \equiv ((a-b)d/ac)^j$, $j = 1, 2, 3, 5, 6, 7$; $q \equiv 3 \pmod 8 < 100$. In Theorems 2 and 3, λ_i is defined by $a \equiv \lambda_i b \pmod q$ whereas in Theorem 4, it is defined by $b \equiv \lambda_i a \pmod q$. Results in Theorems 2 and 3, and implicitly, results in Theorem 4 are explicitly stated only for $j = 1$, 4, and 8 (i.e., $(a-b)d/ac$, b/a, and 1). Set $a \equiv \gamma_{i,j} d \pmod q$ in Theorem 2, $b \equiv \gamma_{i,j} c \pmod q$ in Theorem 3, $a \equiv \gamma_{i,j} c \pmod q$ in Theorem 4, and set $c \equiv \mu_j d \pmod q$, $d \not\equiv 0 \pmod q$, in each Theorem. If $(a-b)d/ac$, in Theorem 2, is replaced by $((a-b)d/ac)^j$, $j = 3$, 5, or 7, then the congruences in (3.1) are satisfied if and only if λ is replaced by $-\lambda$ if $j = 3$, μ is replaced by $-\mu$ if $j = 5$, λ is replaced by $-\lambda$ and μ is replaced by $-\mu$ if $j = 5$, λ is replaced by $-\lambda$ and μ is replaced by $-\mu$ if $j = 7$ $((a-b)d/ac)^3 \equiv ((a+b)d/ac)$. If b/a in Theorem 3 is replaced by $-b/a$, then the congruences in (3.2) are satisfied if and only if $\gamma_{i,j}$ is replaced by $-\gamma_{i,j}$ and the identical remark clearly applies to the cases $j = 8$ and $j = 4$, i.e., if $(-q)^{(p-1)/8} \equiv \pm 1 \pmod p$ is replaced by $(-q)^{(p-1)/8} \equiv \mp 1 \pmod p$.

Putting together the above, we have

THEOREM 2. Let $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod 8$ be a prime with a and c chosen so that $a \equiv c \equiv 1 \pmod 4$ and let q be a prime $\equiv 3 \pmod 8$. Letting λ_i, μ_j, $\hat{R}(\lambda_i)$, $1 \le i \le (q+1)/4$, $F(\mu_j)$, $1 \le j \le (q+1)/4$, and $\gamma_{i,j}$, $1 \le i, j \le (q+1)/4$ be defined as above we have (with $\gamma_{i,j}$ related to $\beta_{i,j}$ by (2.4))

$$(-q)^{(p-1)/8} \equiv (a-b)d/ac \pmod p \iff \hat{R}(\lambda_i)\ F(\mu_j)\left(\frac{\beta_{i,j}}{q}\right) \equiv \frac{1}{2} \pmod q$$

$$\iff a \equiv \lambda_i b \equiv \gamma_{i,j}\ k_j d \pmod q \qquad (3.1)$$

where the λ_i are the integers for which $(-q)^{(p-1)/4} \equiv b/a \pmod p$ and the values of k_j are determined from the μ_j satisfying $c \equiv \pm\mu_j d \pmod q$.

From Theorem 2 we obtain for $3 < q < 100$,

$q = 11$:

λ_i	1	3	4
$\gamma_{i,j}$	10	9	3
k_j	1	5	8
μ_j	0	2	4

$q = 19$:

λ_i	3	7	11	13	18
$\gamma_{i,j}$	13	9	15	2	18
k_j	1	7	3	17	15
μ_j	0	1	4	5	7

	λ_i	1	2	5	7	16	19	22	26	34	35	37
q = 43:	$\gamma_{i,j}$	42	37	11	33	2	35	40	28	29	27	17
	k_i	1	25	3	11	41	30	8	20	36	34	17
	μ_j	0	1	4	5	7	11	13	14	15	17	19

	λ_i	1	8	9	19	28	36	37	39	41	42	46	49	52	53	56
q = 59:	$\gamma_{i,j}$	1	49	5	20	29	2	43	37	23	12	53	4	34	35	7
	k_j	1	11	34	56	14	22	46	5	36	24	29	40	17	44	49
	μ_j	0	2	3	4	6	9	10	15	17	18	21	22	24	25	27

	λ_i	14	19	20	23	24	26	30	33	35	38	39	49	55	57	60	65	66
q = 67:	$\gamma_{i,j}$	6	40	2	39	10	43	44	11	42	3	51	37	9	20	55	22	1
	k_j	1	13	46	3	28	32	40	10	26	53	37	58	56	17	65	8	60
	μ_j	0	1	3	4	5	6	7	8	12	16	18	19	21	24	26	27	30

	λ_i	2	15	16	23	24	26	30	36	42	43	45	46	56	58	65	71	72	73	74	76	82
q = 83:	$\gamma_{i,j}$	63	7	75	15	58	42	4	22	10	24	46	9	67	28	21	50	77	31	81	18	82
	k_j	1	70	80	38	36	58	4	41	49	17	43	67	65	12	31	6	78	74	20	35	15
	μ_j	0	2	4	8	10	13	14	17	22	24	25	26	27	28	29	30	31	34	36	37	38

Thus, for example, for q = 11, we have

$$(-11)^{(p-1)/8} \equiv (a-b)d/ac \pmod{p} \iff \begin{cases} a \equiv b \equiv 10\, k_j d \pmod{11}, \\ a \equiv 3b \equiv 9\, k_j d \pmod{11}, \\ a \equiv 4b \equiv 3\, k_j d \pmod{11}, \end{cases}$$

where $k_j = 1, 5$, or 8 according as $c \equiv 0, \pm 2d$ or $\pm 4d \pmod{11}$.

THEOREM 3. Let $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod{8}$ be a prime with a and c chosen so that $a \equiv c \equiv 1 \pmod{4}$ and let q be a prime $\equiv 3 \pmod{8}$. Letting λ_i, μ_j,

$R(\lambda_i)$, $1 \le i \le (q + 5)/8$, $G(\mu_j)$, $1 \le j \le (q + 1)/4$, and $\gamma_{i,j}$, $1 \le i \le (q + 5)/8$, $1 \le j \le (q + 1)/4$, be defined as above, we have

$$(-q)^{(p-1)/8} \equiv b/a \pmod p \iff \hat{R}(\lambda_i)\ G(\mu_j)\ \left(\frac{\mu_j\gamma_{i,j}}{q}\right) = +1$$

$$\iff a \equiv \lambda_i b \quad\text{and}\quad b \equiv \gamma_{i,j}\ k_j c \pmod q \qquad (3.2)$$

where the λ_i are the integers for which $(-q)^{(p-1)/4} \equiv -1 \pmod p$ and the values of k_j, $j > 1$, are determined from the μ_j satisfying $c \equiv \pm\mu_j d \pmod q$; $k_1 = 1$, $\mu_1 = 1$ arises when $d \equiv 0 \pmod q$.

From Theorem 3, we obtain for $3 < q < 100$

	λ_i	0	5	
q = 11:	$\gamma_{i,j}$	10	6	
	k_j	1	5	8
	μ_j	0	1	5

	λ_i	0	2	5		
q = 19:	$\gamma_{i,j}$	1	2	7		
	k_j	1	7	3	17	15
	μ_j	0	2	9	8	3

	λ_i	0	10	11	12	14	15					
q = 43:	$\gamma_{i,j}$	42	25	36	32	17	41					
	k_j	1	25	3	11	41	30	8	20	36	34	17
	μ_j	0	2	21	9	12	8	20	6	3	10	18

	λ_i	0	2	5	11	15	21	25	27							
q = 59:	$\gamma_{i,j}$	58	37	5	30	17	36	10	13							
	k_j	1	11	34	56	14	22	46	5	36	24	29	40	17	44	49
	μ_j	0	1	19	29	20	26	12	8	14	13	28	16	5	7	11

	λ_i	0	4	5	6	8	13	15	16	22								
q = 67:	$\gamma_{i,j}$	1	65	7	30	57	11	40	41	50								
	k_j	1	13	46	3	28	32	40	10	26	53	37	58	56	17	65	8	60
	μ_j	0	2	23	33	13	22	29	17	11	25	15	14	32	28	31	10	9

	λ_i	0	3	5	13	14	20	21	31	34	35	39										
q = 83:	$\gamma_{i,j}$	1	5	79	41	65	49	66	12	38	31	70										
	k_J	1	70	80	38	47	58	4	41	49	17	43	67	65	12	31	6	78	74	20	35	15
	μ_j	0	1	41	21	33	19	12	5	15	7	20	32	3	6	40	11	16	39	23	18	35

REMARKS. Values of k in Theorem 3 coincide in order, magnitude and sign with the k's in Theorem 2. In [3, Theorem 4] the author showed that a necessary condition for such an order to coincide, k > 1, is that for $c \equiv \mu_j d \pmod q$ in Theorems 2 and 3 the $|\mu_j|$'s are ordered in Theorems 2 and 3 so that the product of their squares is $\equiv 4 \pmod q$. For example, when q = 83, the eighth value of $|\mu_j|$ in Theorem 2 is 17 whereas the eighth value of $|\mu_{j'}|$ in Theorem 3 is 5. Since $(17)(5) \equiv 2 \pmod{83}$ we have $(17^2)(5^2) \equiv 4 \pmod{83}$.

4. THE BEAUTIFUL SIMILARITY OF THE RESULTS FOR $(-q)^{(p-1)/8} \equiv \pm b/a$ (MOD P) AND THE RESULTS FOR $(-q)^{(p-1)/8} \equiv \pm 1$ (MOD P).

In the following theorem, we show that the results of von Lienen [6], when $q \equiv 3 \pmod 8$ (and the same is true for $q \equiv 5 \pmod 8$), may be put into a far more compact form; more significantly, they may be put into a form almost identical to the form in Theorem 3 (consequently, one may use Tables 3-4 to check numerical examples). Details of the proof of the following Theorem which are clear from the proof of Theorem 3 of [3] are omitted.

THEOREM 4. Let $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod 8$ be a prime with a and c chosen so that $a \equiv c \equiv 1 \pmod 4$ and such that λ_i, μ_j, and $\gamma_{i,j}$, $1 \le i \le (q+5)/8$, $1 \le j \le (q+1)/4$, satisfy $b \equiv \lambda_i a \pmod q$, $a \equiv \gamma_{i,j} c \pmod q$, $c \equiv \mu_j d \pmod q$. Then, if q is a prime $\equiv 3 \pmod 8$, we have

$$(-q)^{(p-1)/8} \equiv 1 \pmod p \tag{4.1}$$

if and only if the conditions in (3.2) are satisfied when b is replaced by a and $\gamma_{i,j}$ is replaced by $-\gamma_{i,j}$ when $q = 11 \pmod{16}$.

PROOF. For brevity, all congruences in this proof are understood to be modulo q unless otherwise stated. If the conditions on the right-hand side of Theorem 3 are altered as indicated above a direct computer search shows that (4.1) holds for each $q \equiv 3 \pmod 8 < 100$.

Conversely, suppose that (4.1) holds and that $b \not\equiv 0 \pmod q$. Then, by Western's [8] formula for $q \equiv 3 \pmod 8$, we have

$$p^{(q-3)/8}\ (a + bi)^{(q+1)/4}\ (c - di\sqrt{2})^{(q-1)/2} \equiv 1 \pmod q \qquad (4.2)$$

where the 1 replaces the i in (5.6) of [3]. From Gosset [2], we have that

$$\frac{a - bi}{a + bi}^{(q+1)/4} \equiv 1 \pmod q \qquad (4.3)$$

and so we have $a \equiv \frac{1}{\lambda_i}\ \mu_j\ \gamma_{i,j}\ d$ provided $d \not\equiv 0 \pmod q$.

But, then, as $d^{q-1} \equiv 1$, $\mu_j\ \gamma_{i,j}{}^{(q-1)/2} \equiv \left(\frac{\mu_j\gamma_{i,j}}{q}\right)$ and $a \equiv \frac{1}{\lambda_i} b$, we have

$$\left(\frac{1}{\lambda_i{}^2} + 1\right)^{(q-3)/8} \left(\frac{1}{\lambda_i} + i\right)^{(q+1)/4} (\mu_j - i\sqrt{2})^{(q-1)/2} \left(\frac{\mu_j\gamma_{i,j}}{q}\right) \equiv 1 \pmod q \qquad (4.4)$$

provided b and d are not $\equiv 0 \pmod q$. It is easy to show from (4.3) (parenthetically, it follows also from (4.2) of this paper and (5.7) of [3] in conjunction with the vanishing of the imaginary part of $(\mu - i\sqrt{2})^{(q-1)/2}$) that the real part of $(\lambda_i + i)^{(q+1)/4}$ and the imaginary part of $\left(\frac{1}{\lambda_i} + 1\right)^{(q+1)/4}$ and the imaginary part of $\left(\frac{1}{\lambda_i} + 1\right)^{(q+1)/4}$ must be $\equiv 0 \pmod q$. But it is clear that the imaginary part of $(\lambda + i)^{(q+1)/4}$ and the real part of $(1 + \lambda_i)^{(q+1)/4}$ differ by a sign if and only if $(q+1)/4 \equiv 3 \pmod 4$, i.e., if and only if $q \equiv 11 \pmod{16}$. The remainder of the argument, provided $b \not\equiv 0 \pmod q$, coincides with the argument in Theorem 3 of [3].

When $b \equiv 0 \pmod q$ (something that cannot happen in Theorem 3 of [3] in light of (4.3)), the argument is again easy. Clearly $b \equiv \lambda_i a$, $b \equiv 0$, parallels the case $a \equiv \lambda_i' b$, $a \equiv 0$, in Theorem 3 of [3]. Indeed, we have in the two cases, from (4.2) above and (5.6) of [3], that (with the conditions on λ_i and λ_i'),

$$b^{(q-3)/4}(bi)^{(q+1)/4} \equiv i(a^{(q-1)/2}) \pmod q \qquad (4.5)$$

from which it is clear that the sign of $\gamma_{i,j}$ must be changed if and only if $q \equiv 11 \pmod{16}$ since $a^{(q-1)/2} \equiv b^{(q-1)/2} \equiv (\mu_j\gamma_{i,j}d)^{(q-1)/2}$ and of course, $i^{(q+1)/4} = i$ or $-i$ according as $q \equiv 3 \pmod{16}$ or $q \equiv 11 \pmod{16}$.

5. A BRIEF TREATMENT OF PRIMES $q \equiv 5$ (MOD 8).

We first treat the case that $q^{(p-1)/8} \equiv \pm 1$, $\pm b/a$ (mod p) ($\Longleftrightarrow$ q is a quartic residue of p). We may give a Theorem exactly in the form of Theorem 3 (although the $\gamma_{i,j}$'s must be determined differently). We will, however, give our results in terms of necessary and sufficient criteria for q to satisfy $q^{(p-1)/8} \equiv 1$ (mod p). As explained in §4 the changes necessary to re-state the criteria for q to satisfy $q^{(p-1)/8} \equiv -1, \pm b/a$ (mod p) follow from Theorem 4 (the roles of 3 and 11 (mod 16) are played by 13 and 5 (mod 16)).

It is easy to see from [8] that if q is an octic residue of p($a \equiv \gamma_{i,j}\ k_j\ c$ (mod q)) then the entry $\gamma_{1,1}$ must be +1 for every $q \equiv 13$ (mod 16) and -1 for every $q \equiv 5$ (mod 16).

The magnitude of $\gamma_{i,j}$ may be determined exactly as in the first ten Steps in §2. Moreover, the sign and magnitude of $\gamma_{i,1}$ may be similarly determined. As $\gamma_{i,j} = (\gamma_{i,1})(\gamma_{1,j})$ for each i and $j \geq 2$ it remains only to show how to choose the sign of $\gamma_{1,j}$. This step (which, of course, now seems obvious) eluded the author for more than a year. One must choose the sign so that $\mu_j\gamma_{1,j} \equiv -G(\mu_j)$(mod q) if $G(\mu_j)$ is a quadratic non-residue of q and so that $\mu_j\gamma_{1,j} \equiv G(\mu_j)$(mod q) if $G(\mu_j)$ is a quadratic residue of q provided $q \equiv 13$ (mod 16) whereas these congruences must be reversed if $q \equiv 5$ (mod 16). The reader may verify these assertions using the proof of Theorem 3 of [3].

We now consider the case that $q^{(p-1)/8} \equiv \pm(a \pm b)d/ac$ (mod p) ($\Longleftrightarrow$ q is not a quartic residue of p). A Theorem exactly in the form of Theorem 2 may be given. Only the determination of the sign of the $\beta_{i,j}$'s (and hence, the $\gamma_{i,j}$'s) differentiates the cases $q \equiv 3$ (mod 8) and $q \equiv 5$ (mod 8). In the latter case it is not difficult to use Theorem 1 of [3] to show that to have $q^{(p-1)/8} \equiv (a-b)d/ac$ (mod p) we must choose the sign of $\beta_{i,j}$ as follows.

If $\hat{R}(\lambda_i)\ F(\mu_j)\ (\beta_{i,j}) \equiv \pm 1/2$ (mod q), we choose the sign of $\beta_{i,j}$ so that it is ± 1 if $\beta_{i,j}$ is a quadratic residue of q and so that it is ± 1 if $\beta_{i,j}$ is a quadratic non-residue of q.

For $q \leq 37$ our results agree with those of von Lienen (our formulation is, of course, much more compact). We will only cite one example here.

For $p = a^2 + b^2 = c^2 + 2d^2 \equiv 1 \pmod 8$, $a \equiv c \equiv 1 \pmod 4$, we have for $c \equiv \mu_j d \pmod q$, $j \geq 2$,

$$37^{(p-1)/8} \equiv 1 \pmod p \iff \begin{cases} a \equiv 36\ k_j c \pmod{37} \\ a \equiv 14\ k_j c \pmod{37} \\ a \equiv \ \ 7\ k_j c \pmod{37} \\ a \equiv 16\ k_j c \pmod{37} \\ a \equiv 19\ k_j c \pmod{37} \end{cases}$$

where k_j = 1, 22, 17, 9, 31, 25, 13, 33, 5, or 3 according as μ_j = 0, 1, 3, 5, 6, 9, 10, 11, 16, or 18.

6. TABLES AND NUMERICAL EXAMPLES.

Tables 1-2

Values of λ_i, $|\mu_j|$, and $\gamma_{i,j}$ such that $a \equiv \lambda_i b \equiv \gamma_{i,j} d \pmod q$ if and only if $(-q)^{(p-1)/8} \equiv ((a-b)d)/ac \pmod p$, $a \equiv \lambda_i b \pmod q$, $c \equiv \mu_j d \pmod q$ $q = 11, 19$, $p \neq q \equiv 1 \pmod 8) = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$, and values of $\Sigma_{\mu_j} \sum_{i=1}^{(q+1)/4} \gamma_{\mu_j}(\lambda_i)$.

Table 1: q = 11

λ_i \ $\|\mu_j\|$	1	3	4	$\Sigma\mu_j$
0	10	9	3	22
2	6	1	4	11
4	3	6	2	11

$$\sum_{j=1}^{(q+1)/4} \Sigma\mu_j = 44 = 4q$$

Table 2: q = 19

λ_i \ $\|\mu_j\|$	3	7	11	13	18	$\Sigma\mu_j$
0	13	9	15	2	18	57
1	15	6	10	14	12	57
4	1	8	7	6	16	38
5	12	1	8	15	2	38
7	5	2	16	11	4	38

$$\sum_{j=1}^{(q+1)/4} \Sigma\mu_j = 228 = 12q$$

Tables 3-4

Values of $|\lambda_i|$, $|\mu_j|$, and $\gamma_{i,j}$ such that $b \equiv \gamma_{i,j}c \pmod q$ if and only if $(-q)^{(p-1)/8} \equiv b/a \pmod p$, $a \equiv \lambda_i b \pmod q$, $c \equiv \mu_j d \pmod q$, $q = 11, 19$, $p \neq q \equiv 1$ $(\mathrm{mod}\ 8) = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$ and values $\Sigma\mu_j = \gamma_{1,j} + 2 \sum_{i=2}^{(q+5)/8} \gamma_{i,j}$. Setting $b \equiv \lambda_i a \pmod q$ and $a \equiv \gamma_{i,j} c \pmod q$, values of $\gamma_{i,j}$ given below occur if and only if $(-q)^{(p-1)/8} \equiv 1 \pmod p$ if $q = 3 \pmod{16}$, and if and only if $(-q)^{(p-1)/8} \equiv -1 \pmod p$ if $q \equiv 11 \pmod{16}$.

Table 3: q = 11

$\lvert\mu_j\rvert \diagdown \lvert\lambda_i\rvert$	0	5	$\Sigma\mu_j$
0	10	6	22
1	6	8	22
5	3	4	11

$$\sum_{j=1}^{(q+1)/4} \Sigma\mu_j = 55 = 5q$$

Table 4: q = 19

$\lvert\mu_j\rvert \diagdown \lvert\lambda_i\rvert$	0	2	5	$\Sigma\mu_j$
0	1	2	7	19
2	7	14	11	57
9	3	6	2	19
8	17	15	5	57
3	15	11	10	57

$$\sum_{j=1}^{(q+1)/4} \Sigma\mu_j = 209 = 11\,q$$

Numerical examples illustrating Tables 1-4 for $q \equiv 3 \pmod 8 \geq 19$, $p \equiv 1$ $(\mathrm{mod}\ 8) = a^2 + b^2 = c^2 + 2d^2$ (congruences are mod q unless stated otherwise).

1. $q = 19$, $p = 41 = 5^2 + 4^2 = (-3)^2 + 2(4)^2$

   $a \equiv 6b \equiv 6d \pmod{19}$, $\lambda_4 \equiv -13$, $\mu_3 \equiv 4 \Longrightarrow (-19)^{(p-1)/8} \equiv (a+b)d/ac \pmod p$ (since the value of λ_4 differs in sign from that in Table 2, but the value $\gamma_{4,3} = 6$ agrees).

   Indeed, $\frac{(a+b)d}{ac} \equiv 14 \equiv (-19)^5 \pmod{41}$.

2. $q = 19$, $p = 17 = 1^2 + 4^2 = (-3)^2 + 2(2^2)$ (see Table 4)

   $b \equiv 5c \pmod{19}$, $\lambda_3 \equiv 5$, $\mu_4 \equiv -8 =\!= (-19)^{(p-1)/8} \equiv b/a \pmod p$

   Indeed, $\frac{b}{a} \equiv 4 \equiv (-19)^2 \pmod{17}$.

3. $q = 19$, $p = 233 = (13)^2 + 8^2 = (-15)^2 + 2(2)^2$ (recall that $b \equiv \lambda_i a$)

$a \equiv 8c \pmod{19}$, $\lambda_3 \equiv 5$, $\mu_2 \equiv 2 \Longrightarrow (-19)^{(p-1)/8} \equiv -1 \pmod p$

(since the entry $\gamma_{3,2}$ in Table 4 is $11 \equiv -8 \pmod{19}$; $q \equiv 3 \pmod{16}$)

Indeed, $-1 \equiv (-19)^{29} \pmod{233}$.

Extended Table

$q = 83$

0	0	37	37	46	37	46	37	46	37	37	46	46	37	46	37	46	46	37	37	37	46	46	0
0	0	2	15	16	23	24	26	30	36	42	43	45	46	56	58	65	71	72	73	74	76	82	0
37	0	63	7	75	15	58	42	4	22	10	24	46	9	67	28	21	50	77	31	81	18	82	10
37	2	11	75	21	54	76	35	31	46	36	20	66	49	42	51	59	14	78	12	26	15	13	10
46	4	60	62	24	38	75	40	71	17	53	11	28	56	48	82	20	16	18	73	6	29	3	10
37	8	70	17	28	72	46	19	69	6	48	82	5	10	56	68	51	74	21	16	7	20	45	10
46	10	56	80	39	41	70	65	22	38	55	49	4	8	78	71	74	26	50	46	72	16	36	12
46	13	2	74	34	40	44	29	66	31	82	64	12	24	68	47	56	78	67	55	50	48	25	12
37	14	3	28	51	60	66	2	16	5	40	13	18	36	19	29	1	34	59	41	75	72	79	9
37	17	10	38	4	34	54	62	81	72	70	71	60	37	8	69	31	58	3	26	1	74	42	11
37	22	16	11	23	71	20	66	30	82	75	14	13	26	46	44	33	43	38	25	68	52	34	10
37	24	75	36	30	6	73	50	68	42	4	76	35	70	60	61	25	20	64	29	49	57	66	12
46	25	53	52	71	64	4	63	6	33	15	36	69	55	59	42	73	75	74	5	80	27	40	12
46	26	71	54	45	9	68	75	19	63	6	31	11	22	7	50	79	30	13	2	32	44	16	9
37	27	28	40	61	62	35	74	11	19	69	66	2	4	39	77	37	13	25	23	36	8	18	9
37	28	9	1	70	14	32	6	48	15	37	39	54	25	57	4	3	19	11	40	59	50	71	8
37	29	44	51	1	50	55	57	41	18	61	80	15	30	2	38	70	56	63	48	21	60	52	11
46	30	46	42	35	7	16	3	24	49	60	61	27	54	70	2	43	51	47	20	71	25	77	10
37	31	17	48	40	8	42	39	63	56	33	46	19	38	80	26	61	82	30	11	10	76	5	10
46	34	14	20	72	31	59	37	47	51	76	33	1	2	61	80	60	48	54	53	18	4	9	10
46	36	15	57	6	51	81	10	80	25	34	65	7	14	12	62	5	4	46	39	43	28	63	9
46	37	47	79	52	27	38	59	57	23	18	10	33	66	21	67	71	7	39	6	13	49	48	10
46	38	32	22	46	59	40	49	60	81	67	28	26	52	9	5	66	3	76	50	53	21	68	11
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	215

$q = 107$

0	0	69	69	69	69	69	69	38	38	38	69	69	69	69	38	38	38	38	38	69	69	69	69	38	69	69	38	69	0
0	0	1	7	9	12	16	40	41	46	47	53	59	64	68	69	74	76	77	78	80	82	87	94	96	99	102	103	105	0
69	0	106	87	94	58	45	22	42	43	48	73	75	51	10	76	26	105	88	72	33	47	63	90	104	38	66	82	68	16
38	2	89	68	87	81	61	75	7	25	8	30	66	62	73	84	40	71	86	12	59	97	64	15	53	42	11	85	47	14
38	4	3	60	39	40	79	41	88	85	70	102	96	61	77	93	29	6	57	105	8	73	25	51	9	100	16	75	10	14
38	6	33	18	1	12	13	23	5	79	21	52	93	29	98	60	105	66	92	85	88	54	61	26	99	30	69	76	3	13
69	7	20	79	46	17	63	95	16	103	3	38	105	50	14	85	15	40	59	58	89	23	24	19	60	96	71	72	31	13
38	8	56	50	86	69	48	52	2	53	94	85	80	33	82	24	42	5	101	34	78	43	3	96	61	12	49	9	44	13
69	14	45	44	50	65	8	80	36	98	87	32	49	59	85	4	7	90	106	77	13	25	54	16	28	2	26	55	43	12
38	17	29	45	56	30	86	4	66	37	106	23	72	19	31	43	102	58	16	52	6	28	99	65	87	75	12	83	61	13
38	18	85	95	35	99	27	56	68	90	93	1	45	52	6	67	37	63	10	86	84	71	102	54	41	87	61	92	105	16
38	21	75	2	12	37	49	62	60	92	38	89	46	27	106	78	83	43	34	57	93	6	90	98	11	39	79	56	36	14
38	22	52	77	34	87	14	33	63	11	72	56	59	23	15	7	39	104	25	1	103	17	41	28	49	57	99	16	102	12
69	23	31	85	82	21	103	67	89	58	10	91	29	24	11	105	50	62	54	15	47	41	80	99	93	106	94	26	32	15
69	24	17	19	7	84	91	54	35	18	40	43	9	96	44	99	93	34	2	60	81	57	106	75	51	103	55	104	21	14
69	29	58	90	5	60	65	8	25	74	105	46	37	38	62	86	97	9	32	104	12	56	91	23	67	43	24	59	15	13
38	30	39	31	79	92	64	105	74	35	54	42	71	44	38	32	56	78	99	81	104	93	4	21	10	16	101	12	23	14
69	32	70	9	54	6	60	65	56	93	64	26	100	68	49	30	106	33	46	96	44	27	84	13	103	15	88	38	55	14
38	33	99	54	3	36	39	69	15	23	63	49	65	87	80	73	101	91	62	41	50	55	76	78	83	90	100	14	9	15
69	34	77	42	38	28	66	18	83	6	49	50	3	32	86	33	31	47	72	20	27	19	71	25	17	70	54	106	7	11
69	35	5	100	65	31	96	104	4	106	81	63	53	66	57	48	84	10	95	68	49	86	6	85	15	24	98	18	88	15
38	38	9	73	10	13	23	16	50	41	103	92	74	76	17	65	87	18	64	101	24	5	75	46	27	86	48	11	30	12
69	40	65	16	96	82	71	68	52	94	90	70	47	2	99	89	22	23	58	28	102	48	78	35	88	98	97	20	74	16
69	41	50	37	8	96	104	77	40	97	61	95	102	18	35	52	91	100	94	38	62	4	60	101	43	26	17	73	24	15
69	42	54	10	60	78	31	96	86	32	83	17	16	28	102	69	94	1	63	71	37	30	22	62	55	88	74	66	73	14
69	43	103	27	55	18	73	88	61	65	85	78	86	97	40	90	104	99	31	74	25	81	38	39	95	45	50	7	58	16
69	47	93	41	32	63	95	94	53	67	30	59	87	72	33	101	43	79	55	45	34	16	26	83	65	104	68	78	96	16
38	48	61	43	44	100	37	49	6	52	68	41	26	99	32	72	19	15	89	102	20	22	9	74	76	36	40	27	25	12
38	52	47	84	76	56	25	36	59	12	98	100	6	64	65	66	62	94	37	40	54	38	35	50	34	33	1	105	14	13
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	375

ACKNOWLEDGEMENT. Research supported by Natural Sciences and Engineering Research Council of Canada, grant No. A-7233. I am also deeply indebted to Mr. Lee-Jeff Bell for valuable assistance with the programming required in this paper.

REFERENCES

1. CUNNINGHAM, ALAN J.C. and GOSSET, THOROLD. 4-tic and 3-bic residuacity-tables, Mess. Math. 50 (1920), 1-30.

2. GOSSET, THOROLD. On the law of quartic reciprocity, Mess. Math. 41 (1911), pp. 65-90.

3. HUDSON, RICHARD H. and WILLIAMS, KENNETH S. An application of a formula of Western to the evaluation of certain Jacobsthal sums, Acta Arithmetica, (to appear).

4. HUDSON, RICHARD H. and WILLIAMS, KENNETH S. Some remarks on the evaluation of quartic and octic residue symbols, (submitted for publication).

5. JACOBSTHAL, ERNST. Über die Darstellung der Primzahlen der Form 4n+1 als Summe zweier Quadrate, J. Reine Angew. Math. 132 (1907), pp. 238-245.

6. VON LIENEN, HORST. Primzahlen als achte Potenzreste, J. Reine Angew. Math. 266 (1974), pp. 107-117.

7. WEISS, MARIE J. Higher Algebra for the Undergraduate, John Wiley and Sons, Inc., New York, 1949, Chapter 5.

8. WESTERN, A.E. Some criteria for the residues of eighth and other powers, Proc. Lond. Math. Soc. 9 (1911), pp. 244-272.

9. WHITEMAN, ALBERT L. Theorems analogous to Jacobsthal, Duke Math. J. 16 (1949), pp. 619-626.

10. WHITEMAN, ALBERT L. Cyclotomy and Jacobsthal sums, Amer. J. Math. 74 (1952), pp. 89-99.