ISRAEL JOURNAL OF MATHEMATICS, Vol. 44, No. 1, 1983

ON THE FIRST OCCURRENCE OF CERTAIN PATTERNS OF QUADRATIC RESIDUES AND NON-RESIDUES

BY
RICHARD H. HUDSON†

ABSTRACT
Effective upper bounds are obtained for the first occurrence of certain mixed patterns of quadratic residues and non-residues using the character sum estimates of D. A. Burgess and a proof of a conjecture of E. Lehmer.

1. Introduction and summary

Around 1939 Issai Schur proved the following interesting theorem.

THEOREM 1. *Let f be a totally multiplicative function (that is $f(rs)=f(r)f(s)$ for every $r, s \in \mathbf{Z}^+$) which takes on only the values ± 1. If there are no positive integers a, $a+1$, $a+2$ with*

$$(1.1)\qquad f(a)=f(a+1)=f(a+2)=+1,$$

then f must be one of the two functions defined for each positive integer k and n by

$$(1.2)\qquad f_1(n)=(n/3),\qquad (n,3)=1,\qquad f_1(3^k n)=f_1(n),$$

$$(1.3)\qquad f_2(n)=(n/3),\qquad (n,3)=1,\qquad f_2(3^k n)=(-1)^k f_2(n).$$

The proof of Theorem 1 was prepared for publication by the first author, appearing in [15].

Let $r_i(p)$ and $n_i(p)$ denote respectively the least positive quadratic residue and non-residue such that r_i, r_i+1, $r_i+2,\cdots,r_i+i-1$ are all quadratic residues and n_i, n_i+1, $n_i+2,\cdots$, n_i+i-1 are all quadratic non-residues of p. An upper bound for n_2 has been given by Elliott [6], improving results in [3, th. 3] and in [5, p. 52]. Using Theorem 1, bounds for r_3 have been given by the first author [8],

† Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233.

Received September 20, 1981 and in revised form June 16, 1982

[9]. Upper bounds for n_3 or for r_4 better than those which are immediate consequences of the work of Weil [16] (see, in connection, Gelfond and Linnik [7, p. 198]) appear quite difficult to obtain. In §4 of this paper we show how proofs of conjectures of Emma Lehmer [12], [13] together with the estimates of Burgess [4] lead to non-trivial upper bounds for certain mixed patterns of four consecutive integers only three of which are required to be quadratic residues.

In particular, let $r_{4,1}(p)$ denote the smallest positive integer such that

$$\left(\frac{r_{4,1}}{p}\right)=\left(\frac{r_{4,1}+1}{p}\right)=\left(\frac{r_{4,1}+3}{p}\right)=+1,$$

and let $r_{4,2}(p)$ denote the smallest positive integer such that

$$\left(\frac{r_{4,2}}{p}\right)=\left(\frac{r_{4,2}+2}{p}\right)=\left(\frac{r_{4,2}+3}{p}\right)=+1.$$

In §2 (see Theorem 2) we use Weil's estimates to establish the existence of $r_{4,1}(p)$ for $p>11$, $r_{4,2}(p)$ for $p>7$, and $r_4(p)$ for $p \gtrdot 53$. This generalizes a result of Jacobsthal [11] for $r_4(p)$, $p\equiv 3 \pmod 4$. In §3 we prove the following conjecture of Emma Lehmer [12] which has been reformulated to serve our needs in §4.

THEOREM 3. *Let f be a totally multiplicative function taking on only the values* ± 1, *with* $f(2)=-1$, *for which there exists a least positive integer* $q\not\equiv 0 \pmod 5$ *with* $f(q)\neq(q/5)$. *Then there is function* $g(q)$ *and integers* a, $a+2$, $a+3$ *with* $1\leqq a\leqq g(q)$ *for which* $f(a)=f(a+2)=f(a+3)=+1$.

In Theorem 3, any function g depending solely on q suffices to establish Lehmer's conjecture. For our purposes, since our bounds depend directly on the size of $g(q)$, it is desirable to find as small a value as possible for $g(q)$ even though this lengthens the proof of Theorem 3 markedly. By showing that $g(q)$ can be taken (at least) as small as $12q$ in Theorem 3, and using an analogous theorem obtained in [10] together with Theorem 2 of this paper and the character sum estimates of Burgess [4], we derive in §4 the following upper bounds for $r_{4,1}(p)$ and $r_{4,2}(p)$.

THEOREM 4. *Let p be a prime* $\geqq 13$. Then

$$r_{4,1}(p)<203.602p^{1/4}\log p+51. \tag{1.4}$$

THEOREM 5. *Let p be a prime* $\equiv \pm 3 \pmod 8 \geqq 11$, *then*

$$r_{4,2}(p)<174.516p^{1/4}\log p+48. \tag{1.5}$$

Unfortunately, we are unable to obtain a similar result for $r_{4,2}(p)$ when $p \equiv \pm 1 \pmod 8$ due to our inability to obtain a result analogous to Theorem 3 when $f(2) = +1$. Lehmer's conjecture, with $f(2) = +1$, is identical to Theorem 3 except that 5, when it appears, is replaced by 7. Any proof of this conjecture would be of interest in itself.

2. Existence of $r_4(p)$, $r_{4,1}(p)$, and $r_{4,2}(p)$ for $p > 53$

The exact number of quadruples of consecutive quadratic residues of a prime p has been known for 75 years, see, e.g., [11], if p is a prime $\equiv 3 \pmod 4$. From this result it follows that $r_4(p)$ exists if p is any prime $\equiv 3 \pmod 4$ $\geqq 19$.

In what follows we assume only that p is a prime > 3 and, for brevity, throughout this section we write r for $r_4(p)$.

THEOREM 2. *There exists an integer r, $1 \leqq r \leqq p-4$, with*

$$\left(\frac{r}{p}\right) = \left(\frac{r+1}{p}\right) = \left(\frac{r+2}{p}\right) = \left(\frac{r+3}{p}\right) = +1, \tag{2.1}$$

for every prime $p > 53$.

PROOF. If

$$S = \sum_{r=1}^{p-4} \left(1 + \left(\frac{r}{p}\right)\right)\left(1 + \left(\frac{r+1}{p}\right)\right)\left(1 + \left(\frac{r+2}{p}\right)\right)\left(1 + \left(\frac{r+3}{p}\right)\right) > 0 \tag{2.2}$$

then there clearly exists an integer r satisfying (2.1).

Expanding (2.2) we have

$$\begin{aligned} S = p - 4 &+ \sum_{r=1}^{p-4}\left(\frac{r}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r+1}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r+2}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r+3}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r(r+1)}{p}\right) \\ &+ \sum_{r=1}^{p-4}\left(\frac{r(r+2)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r(r+3)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{(r+1)(r+2)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{(r+1)(r+3)}{p}\right) \\ &+ \sum_{r=1}^{p-4}\left(\frac{(r+2)(r+4)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r(r+1)(r+2)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r(r+1)(r+3)}{p}\right) \\ &+ \sum_{r=1}^{p-4}\left(\frac{r(r+2)(r+3)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{(r+1)(r+2)(r+3)}{p}\right) + \sum_{r=1}^{p-4}\left(\frac{r(r+1)(r+2)(r+3)}{p}\right). \end{aligned} \tag{2.3}$$

For brevity we denote the 15 sums in (2.3) by

S_{1i}, $i = 1, \cdots, 4$, $\quad S_{2i}$, $i = 1, \cdots, 6$, $\quad S_{3i}$, $i = 1, \cdots, 4$, $\quad$ and S_{41}.

It is easy to see that $|S_{1i}| \leqq 3$ for $i = 1, \cdots, 4$ as, e.g.,

$$|S_{11}| = \left| \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) - \left(\frac{0}{p}\right) - \left(\frac{p-3}{p}\right) - \left(\frac{p-2}{p}\right) - \left(\frac{p-1}{p}\right) \right|$$
$$= |-(\pm 1) - (\pm 1) - (\pm 1)| \leqq 3.$$

Now, as

$$\sum_{\substack{r=0 \\ p \nmid a}}^{p-1} \left(\frac{ax^2 + bx + c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2 - 4ac \\ -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2 - 4ac \end{cases} \tag{2.4}$$

summing over primes $p \nmid a$, we have for $k \neq l$ that

$$\sum_{r=0}^{p-1} \left(\frac{(r+k)(r+l)}{p}\right) = -1. \tag{2.5}$$

It follows that $|S_{2i}| \leqq 3$ for $i = 1, \cdots, 6$.

Now, A. Weil [16] (see, e.g., [2]) has shown that

$$\left| \sum_{r=0}^{p-1} \left(\frac{(r+a)(r+b)(r+c)}{p}\right) \right| \leqq 2p^{1/2} \qquad \text{for } a \neq b, b \neq c, c \neq a.$$

It follows that $|S_{3i}| \leqq 2p^{1/2} + 1$ for $i = 1, \cdots, 4$. Moreover, as

$$|S_{41}| = \left| \sum_{r=1}^{p-4} \left(\frac{r(r+1)(r+2)(r+3)}{p}\right) \right| = \left| \sum_{r=0}^{p-1} \left(\frac{r(r+1)(r+2)(r+3)}{p}\right) \right| \leqq 3p^{1/2}$$

we have, putting together the above,

$$|S - (p-4)| \leqq 4 \cdot 3 + 6 \cdot 3 + 4(2p^{1/2} + 1) + 3p^{1/2} = 11p^{1/2} + 34.$$

It is easily checked that

$$S \geqq p - 4 - (11p^{1/2} + 34) = p - 11p^{1/2} - 38 > 0$$

for every prime $p \geqq 191$ and computer data for $53 < p < 191$ completes the proof of Theorem 2.

Corollary. *$r_{4,1}(p)$ exists if $p \geqq 13$ and $r_{4,2}(p)$ exists if $p \geqq 11$.*

Proof. The above argument clearly establishes the existence of $r_{4,1}(p)$ and $r_{4,2}(p)$ if $p \geqq 191$. Computer data establishes the existence of $r_{4,1}(p)$ if $p \geqq 13$ and of $r_{4,2}(p)$ if $p \geqq 11$.

3. A Proof of Theorem 3.

We now prove Theorem 3 in the stronger form that $g(q) \leqq 12q$. As a necessary preliminary we show that $q > 7$.

Case 0a. If $q = 3$, then $f(1) = f(3) = f(4) = +1$.

Case 0b. If $q = 7$, then $f(4) = f(6) = f(7) = +1$.

Henceforth, we assume that $q \geqq 11$ and we adopt the following notation. When $t > 1$ is not required in the proof of a case we simply write $aq + b$. When the value of $f((aq + b)/t)$ is $+1$ or -1 according to one of the following reasons, we give as the reason for its value one of the letters A, B, or C where these letters have the following meanings:

A. $f(aq) = -f(a)(q/5)$ in view of the definition of q in Theorem 3.

B. $f((aq + b)/t) = +1$ as $(aq + b)/lt \equiv 1, 2$, or $4 \pmod 7$ $< q$.

C. $f((aq + b)/t) = -1$ since $f((aq + b - 3t)/t) = f((aq + b - 2t)/t)$.

When B is the reason given in the following proof, a value for l (not necessarily the largest) is given immediately after the letter B. The last three steps in each of the cases yield the desired integers a, $a + 2$, $a + 3$ specified in Theorem 3.

The first column in the proof of each case gives the expression $(aq + b)/t$, the second column the value of $f((aq + b)/t)$, and the third column the reason for the assigned value in the second column. We first consider the cases where $q \not\equiv 1$ (mod 5).

Case 1a. $q \equiv 2 \pmod 5$			Case 1b. $q \equiv 3 \pmod 5$			Case 2. $q \equiv 4 \pmod 5 \equiv 1 \pmod 3$		
q	$+1$	A	q	$+1$	A	$2q$	$+1$	A
$q-1$	$+1$	B1	$q+1$	$+1$	B2	$2q+1$	$+1$	B3
$q-3$	$+1$	B1	$q-2$	$+1$	B1	$2q-2$	$+1$	B3

Case 3. $q \equiv 4 \pmod 5 \equiv 2 \pmod 3 \equiv 3 \pmod 4$		
$3q$	$+1$	A
$3q-1$	$+1$	B4
$3q-3$	$+1$	B6

Case 4. $q \equiv 29 \pmod{180} \equiv 4 \pmod 5 \equiv 2 \pmod 9 \equiv 1 \pmod 4$		
$7q$	$+1$	A
$7q+1$	$+1$	B12
$7q-2$	-1	C
$(7q-2)/3$	$+1$	$f(3) = -1$
$(7q-5)/3$	$+1$	B9
$(7q-11)/3$	$+1$	B12

Case 5. $q \equiv 149 \pmod{180} \equiv 4 \pmod 5 \equiv 5 \pmod 9 \equiv 1 \pmod 4$		
$7q$	$+1$	A
$7q+1$	$+1$	B18
$7q-2$	-1	C
$(7q-2)/3$	$+1$	$f(3)=-1$
$(7q-11)/3$	$+1$	B12
$(7q-5)/3$	-1	C
$(7q-5)/6$	$+1$	$f(2)=-1$
$(7q+1)/6$	$+1$	B18
$(7q-17)/6$	$+1$	B18

Case 6. $q \equiv 4 \pmod 5 \equiv 8 \pmod 9 \equiv 1 \pmod 4$		
$7q$	$+1$	A
$7q+1$	$+1$	B12
$7q-1$	$+1$	B9

The rest of the proof (the cases for $q \equiv 1 \pmod 5$) is more involved and we adopt the following abbreviation in the third column: D5, D10, or D15 means that $f((aq+b)/t) = +1$ because $(aq+b)/t = 5$, 10, or 15 $(5k+\alpha)$ and $f(5)$, $f(10)$, or $f(15)$, respectively, is equal to $(\alpha/5)$, $\alpha = 1, 2, 3$, or 4; $5k+\alpha < q$.

Case 7. $q \equiv 91, 211, 331 \pmod{360} \equiv 1 \pmod 3 \equiv 3 \pmod 8$		
$7q$	$+1$	A
$7q-1$	$+1$	B12
$7q-3$	-1	C
$(7q-3)/2$	$+1$	$f(2)=-1$
$(7q-5)/2$	$+1$	B
$(7q-9)/2$	-1	C
$(7q-9)/4$	$+1$	$f(2)=-1$
$(7q-13)/4$	$+1$	B8
$(7q-21)/4$	$+1$	B8

Case 8. $q \equiv 31, 151, 271 \pmod{360} \equiv 1 \pmod 3 \equiv 7 \pmod 8$		
$7q$	$+1$	A
$7q-1$	$+1$	B8
$7q-3$	-1	C
$(7q-3)/2$	$+1$	$f(2)=-1$
$(7q-9)/2$	$+1$	B8
$(7q-5)/2$	-1	C
$(7q-5)/4$	$+1$	$f(2)=-1$
$(7q-1)/4$	$+1$	B24
$(7q-13)/4$	$+1$	B12

Case 9. $q \equiv 41, 131, 221, 311 \pmod{360} \equiv 5 \pmod 9$		
$2q$	$+1$	A
$2q-1$	$+1$	B9
$2q-3$	-1	C
$4q-6$	$+1$	$f(2)=-1$
$4q-8$	$+1$	B4
$4q-5$	-1	C
$(4q-5)/3$	$+1$	$f(3)=-1$
$(4q-2)/3$	$+1$	B6
$(4q-11)/3$	$+1$	B9

Case 10. $q \equiv 71, 161, 251, 341 \pmod{360} \equiv 8 \pmod 9$		
$2q$	$+1$	A
$2q-1$	$+1$	B3
$2q-3$	-1	C
$4q-6$	$+1$	$f(2)=-1$
$4q-5$	$+1$	B9
$4q-8$	$+1$	B4

Case 11. $q \equiv 281 \pmod{360} \equiv 2 \pmod 9 \equiv 1 \pmod 8$		
$7q$	$+1$	A
$7q-3$	-1	assumption
$(7q-3)/2$	$+1$	$f(2)=-1$
$(7q-5)/2$	$+1$	B18
$(7q-9)/2$	-1	C
$7q-9$	$+1$	$f(2)=-1$
$7q-11$	$+1$	B12
$7q-8$	-1	C
$(7q-8)/3$	$+1$	$f(3)=-1$
$(7q-5)/3$	$+1$	B18
$(7q-14)/3$	$+1$	B9
$7q-3$	$+1$	contradiction
$7q-1$	-1	C
$(7q-1)/2$	$+1$	$f(2)=-1$
$(7q+1)/2$	$+1$	B24
$(7q-5)/2$	$+1$	B18

Case 12. $q \equiv 101 \pmod{360} \equiv 2 \pmod 9 \equiv 5 \pmod 8$		
$7q$	$+1$	A
$7q-3$	$+1$	B8
$7q-1$	-1	C
$(7q-1)/2$	$+1$	$f(2)=-1$
$(7q+1)/2$	$+1$	B12
$(7q-5)/2$	$+1$	B18

Apart from $q \equiv 11 \pmod{180}$, the missing cases all have $q \equiv 1 \pmod{60}$ and these are resolved in Cases 13–21.

Case 13. $q \equiv 1, 301, 601, 121, 421, 721 \pmod{900}$, $f(5)=+1$; $q \equiv 181, 481, 781, 241, 541, 841 \pmod{900}$, $f(5)=-1$		
$2q$	$+1$	A
$2q+2$	$+1$	B4
$2q+3$	$+1$	D5

Case 14. $q \equiv 181, 481, 781 \pmod{900}$, $f(5)=-1$; $q \equiv 61, 361, 661, 121, 421, 721 \pmod{900}$, $f(5)=+1$		
$3q$	$+1$	A
$3q+2$	$+1$	D5
$3q+3$	$+1$	B6

Case 15. $q \equiv 361 \pmod{900}$, $f(5)=+1$; $q \equiv 1 \pmod{900}$, $f(5)=-1$		
$7q$	$+1$	A
$7q+2$	$+1$	B9
$7q+3$	$+1$	D10

Case 16. $q \equiv 61 \pmod{900}$, $f(5)=+1$; $q \equiv 601 \pmod{900}$, $f(5)=-1$		
$7q$	$+1$	A
$7q+3$	$+1$	D10
$7q+2$	-1	C
$(7q+2)/3$	$+1$	$f(3)=-1$
$(7q+5)/3$	$+1$	B9
$(7q-4)/3$	$+1$	B9

Case 17. $q \equiv 301 \pmod{900}$, $f(5)=-1$		
$12q$	$+1$	A
$12q+3$	$+1$	D15
$12q+2$	-1	C
$6q+1$	$+1$	$f(2)=-1$
$6q+3$	$+1$	B9
$6q+2$	-1	D10

Case 18. $q \equiv 541 \pmod{900}$, $f(5) = +1$		
$8q$	$+1$	A
$8q+1$	$+1$	B9
$8q-2$	-1	C
$(8q-2)/3$	$+1$	$f(3) = -1$
$(8q+4)/3$	$+1$	B12
$(8q+7)/3$	$+1$	D15

Case 19. $q \equiv 241 \pmod{900}$, $f(5) = +1$		
$8q$	$+1$	A
$8q-2$	$+1$	B18
$8q+1$	-1	C
$(8q+1)/3$	$+1$	$f(3) = -1$
$(8q+7)/3$	$+1$	D15
$(8q+10)/3$	-1	C
$(8q+10)/6$	$+1$	$f(2) = -1$
$(8q+16)/6$	$+1$	B24
$(8q-2)/6$	$+1$	B18

Case 20. $q \equiv 661 \pmod{900}$, $f(5) = +1$		
$7q$	$+1$	A
$7q+3$	$+1$	B10
$7q+2$	-1	C
$(7q+2)/3$	$+1$	$f(3) = -1$
$(7q+8)/3$	$+1$	D15
$(7q+11)/3$	-1	C
$(7q+11)/6$	$+1$	$f(2) = -1$
$(7q+17)/6$	$+1$	B18
$(7q-1)/6$	$+1$	B18

Case 21. $q \equiv 841 \pmod{900}$, $f(5) = +1$		
$7q$	$+1$	A
$7q-1$	$+1$	B9
$7q-3$	-1	C
$(7q-3)/2$	$+1$	$f(2) = -1$
$(7q+1)/2$	$+1$	B8 (if $q \equiv 1 \pmod 8$)
$(7q+3)/2$	$+1$	D10
$(7q+1)/2$	-1	C (if $q \equiv 5 \pmod 8$)
$(7q+1)/4$	$+1$	$f(2) = -1$
$(7q-7)/4$	$+1$	D10
$(7q-11)/4$	$+1$	B8 (if $q \equiv 5 \pmod 8$)

The cases for which $q \equiv 191 \pmod{360}$ are resolved in Case 22. If $q \equiv 731$ or $1091 \pmod{1800}$ and $f(5) = -1$ the proof is as in Case 13; if $q \equiv 11$ or $371 \pmod{1800}$ and $f(5) = -1$ the proof as in Case 14; if $q \equiv 731$ or $1451 \pmod{1800}$ and $f(5) = -1$ the proof is as in Case 14. Cases 23 and 24 complete the proof of Theorem 3.

Case 22. $q \equiv 191, 551, 911, 1271, 1631 \pmod{1800}$		
$7q$	$+1$	A
$7q-1$	$+1$	B8
$7q-3$	-1	C
$(7q-3)/2$	$+1$	$f(2) = -1$
$(7q-5)/2$	$+1$	B18
$(7q-9)/2$	$+1$	B8

Case 23. $q \equiv 371, 1091 \pmod{1800}$, $f(5) = +1$; $q \equiv 1451 \pmod{1800}$, $f(5) = -1$		
$2q$	$+1$	A
$2q-1$	$+1$	B3
$2q-3$	-1	C
$4q-6$	$+1$	$f(2) = -1$
$4q-8$	$+1$	B4
$4q-5$	-1	C
$(4q-5)/3$	$+1$	$f(3) = -1$
$(4q+1)/3$	$+1$	D5
$(4q+4)/3$	$+1$	B12

Case 24. $q \equiv 11 \pmod{1800}$, $f(5) = +1$		
$2q$	$+1$	A
$2q-1$	$+1$	B3
$2q-3$	-1	C
$6q-9$	$+1$	$f(3) = -1$
$6q-11$	$+1$	D5
$6q-8$	-1	C
$3q-4$	$+1$	$f(2) = -1$
$3q-3$	$+1$	B3
$3q-6$	$+1$	B3

4. Upper bounds for $r_{4,1}(p)$ and for $r_{4,2}(p)$

THEOREM 4. *For every prime $p \geqq 13$ we have*

$$r_{4,1}(p) < 203.602p^{1/4}\log p + 51. \tag{4.1}$$

PROOF. Note that (4.1) holds trivially for $p \leqq 20000$ as then $r_{4,1}(p) < p < 203.602p^{1/4}\log p + 51$. Assume now that $p > 20000$ and define q as in Theorem 3 with f taken to be a totally multiplicative function with values coinciding with those of the Legendre symbol (m/p) for $1 \leqq m < p$. We may clearly assume that $(2/p) = -1$ as otherwise $r_{4,1}(p) = 1$.

For, if $q \equiv \alpha \pmod 5$, $\alpha = 1,2,3,4$, the $(q-\alpha)/5$ integers (mod p), $\alpha/5$, $(5+\alpha)/5, \cdots, (q-5)/5$, are consecutive quadratic residues or consecutive quadratic non-residues of p. By Theorem 2 we have $q < r_{4,1}(p) + 4 \leqq p$ so that $q - 5 < p$. From this it follows that $s \geqq (q-\alpha)/5$ or, equivalently, $q \leqq 5s + \alpha \leqq 5s + 4$.

Now Karl Norton, see, e.g., [14, p. 38], has shown that $s < 2.9086p^{1/4}\log p$ for all p for which $(2/p) = -1$. It is easy to see that

$$14q - 2 \leqq 70s + 54 < 70(2p)^{1/2} + 194 < p \tag{4.2}$$

if $p > 20000$ as A. Brauer [1] has shown that $s < (2p)^{1/2} + 2$ for every prime p.

Finally, appealing to the proof of the theorem in [10], we have from (4.2) that $r_{4,1}(p) \leqq 14q - 5 \leqq 70s + 51$ from which Theorem 4 follows at once for $p > 20000$ in view of Norton's result and the corollary following the proof of Theorem 2.

THEOREM 5. *For every prime $\equiv \pm 3 \pmod 8$ $\geqq 11$ we have*

$$r_{4,2}(p) < 174.516p^{1/4}\log p + 48. \tag{4.3}$$

PROOF. As in the proof of Theorem 4 we have $q \leqq 5s + 4$ and $s < 2.9086p^{1/4}\log p$. Moreover, we have

$$(4.4) \qquad 12q+3 \leqq 60s+51 < 60(2p^{1/2})+171 < p \qquad \text{if } p > 20000,$$

and the result is immediate, as before, if $p < 20000$. Theorem 5 follows, then, from the corollary following the proof of Theorem 2 and the inequality $r_{4,2}(p) \leqq 12q \leqq 60s+48$ which follows from the proof of Theorem 3 with $g(q)=12q$.

Acknowledgement

I am grateful to Kenneth S. Williams for several helpful suggestions, and particularly for his help in the proof of Theorem 2.

References

1. A. Brauer, *Über die Verteilung der Potenzreste*, Math. Z. **35** (1932), 39–50.
2. D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112.
3. D. A. Burgess, *On Dirichlet characters of polynomials*, Proc. London Math. Soc. (3) **13** (1963), 537–548.
4. D. A. Burgess, *A note on the distribution of residues and non-residues*, J. London Math. Soc. **38** (1963), 253–256.
5. P.D.T.A. Elliott, *On the mean value of $f(p)$*, Proc. London Math. Soc. (3) **21** (1970), 28–96.
6. P.D.T.A. Elliott, *On the least pair of consecutive quadratic non-residues* (mod p), Proc. Conf. Number Theory, Univ. Colorado, Boulder, Colorado, 1972, pp. 75–79.
7. A. O. Gelfond and Yu. V. Linnik, *Elementary Methods in Analytic Number Theory*, Chicago, Illinois, 1965.
8. Richard H. Hudson, *A note on Dirichlet characters*, Math. Comp. **27** (1973), 973–975.
9. Richard H. Hudson, *Totally multiplicative sequences with values* ± 1 *which exclude four consecutive values of* 1, J. Reine Angew. Math. **271** (1974), 218–220.
10. Richard H. Hudson, *On a conjecture of Emma Lehmer*, Manuscr. Math., to appear.
11. Ernst Jacobsthal, *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Diss., Univ. Berlin, 1906, pp. 1–39.
12. Emma Lehmer, *Problem Session of the Western Number Theory Conference*, Tucson, Arizona, 1980.
13. Emma Lehmer, *Patterns of power residues*, J. Number Theory, to appear.
14. Karl K. Norton, *Numbers with small prime factors and the least k-th power non-residue*, Mem. Am. Math. Soc. (1971), #106.
15. Issai Schur, *Multiplikativ signierte Folgen positiver ganzer Zahlen, Gesammelte Abhandlungen von Issai Schur 3*, Berlin–Göttingen–Heidelberg, 1973, pp. 392–399.
16. A. Weil, *Sur les courbes algébriques et les variétes qui s'en déduisent*, Actualités Math. Sci., No. 1041 (Paris, 1945), deuxième partie, §IV.

Department of Mathematics and Statistics
University of South Carolina
Columbia, SC 29208 USA