PACIFIC JOURNAL OF MATHEMATICS
Vol. 61, No. 2, 1975

ON EULER'S CRITERION FOR QUINTIC NONRESIDUES

KENNETH S. WILLIAMS

Let p be a prime $\equiv 1 \pmod 5$. If 2 is a quintic nonresidue $\pmod p$ then $2^{p-1/5} \equiv \alpha \pmod p$ for some fifth root of unity $\alpha_5 (\not\equiv 1) \pmod p$. Emma Lehmer has given an explicit expression for α_5 in terms of a particular solution of a certain quadratic partition of p. In this paper we show how in principle the corresponding result can be obtained for any quintic nonresidue $D \pmod p$. Full details are given for $D = 2, 3, 5$.

1. Introduction. Let k be an integer $\geqq 2$ and let p be a prime $\equiv 1 \pmod k$. Euler's criterion states that $D^{(p-1)/k} \equiv 1 \pmod p$ if and only if D is a kth power residue $\pmod p$. Thus if D is not a kth power residue $\pmod p$, for some kth root of unity $\alpha_k (\not\equiv 1)$ moduo p we have $D^{(p-1)/k} \equiv \alpha_k \pmod p$. Clearly $\alpha_2 = -1$. For $k > 2$ Emma Lehmer [3] has proposed the problem of specifying which α_k corresponds to a given D. For $D = 2$, $k = 3, 4, 5, 8$, she has given explicit expressions for α_k in terms of certain quadratic partitions of p. Elsewhere the author [6] has given a complete treatment of the case $k = 3$. In this paper we treat the case $k = 5$. Full details are given for $D = 2, 3, 5$. The method used is described in § 4 and can be applied to any value of D if the reader has the patience to supply the many details.

2. Two lemmas involving the domain $Z[\zeta]$. We set $\zeta = \exp(2\pi i/5)$. If Q denotes the field of rational numbers, the cyclotomic field formed by adjoining ζ to Q is denoted by $Q(\zeta)$. The domain of integers of $Q(\zeta)$ is denoted by $Z[\zeta]$. Every element of $Z[\zeta]$ can be written in the form $a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4$, where a_1, a_2, a_3, a_4 are rational integers. The domain $Z[\zeta]$ is a unique factorization domain. The element $1 - \zeta$ is a prime in $Z[\zeta]$ which divides 5. The units of $Z[\zeta]$ are given by $\pm\zeta^i(\zeta + \zeta^4)^j$, where i and j are integers with $0 \leqq i \leqq 4$. If α and β are associated nonzero elements, that is α/β is a unit, we write $\alpha \sim \beta$. The complex conjugate of an element $\alpha \in Z[\zeta]$ will be denoted by $\bar{\alpha} (\in Z[\zeta])$. We will need the following two results.

LEMMA 1. *If $\alpha \in Z[\zeta]$ is such that $\alpha \not\equiv 0 \pmod{1 - \zeta}$ then α possesses an associate α' such that $\alpha' \equiv -1 \pmod{(1 - \zeta)^2}$.*

Proof. Set $\alpha = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4$, $b = a_1 + a_2 + a_3 + a_4$, $c =$

$a_1 + 2a_2 + 3a_3 + 4a_4$. As $\alpha \not\equiv 0 \pmod{1-\zeta}$ we have $b \not\equiv 0 \pmod 5$. We define d uniquely by $2^d b \equiv -1 \pmod 5$, $0 \leqq d \leqq 3$. Then we have only to choose $\alpha' = \zeta^{c2^d}(\zeta + \zeta^4)^d \alpha$, as $\zeta + \zeta^4 \equiv 2 \pmod{(1-3)^2}$ and $\zeta^{c2^d} \equiv b \pmod{(1-\zeta)^2}$.

LEMMA 2. *If* $\alpha, \beta \in Z[\zeta]$ *are such that*

(a) $\alpha\bar{\alpha} = \beta\bar{\beta}$

(b) $\alpha, \beta \not\equiv 0 \pmod{1-\zeta}$,

(c) $\alpha \equiv \beta \pmod{(1-\zeta)^2}$,

(d) $\alpha \sim \beta$,

then

$$\alpha = \beta .$$

Proof. By (d) we have $\alpha = \pm\zeta^i(\zeta + \zeta^4)^j\beta$, for integers i and j with $0 \leqq i \leqq 4$. Thus using (a) we obtain $\alpha\bar{\alpha} = (\zeta + \zeta^4)^{2j}\beta\bar{\beta} = (\zeta + \zeta^4)^{2j}\alpha\bar{\alpha}$. Now (b) guarantees that $\alpha \neq 0$, so that $\alpha\bar{\alpha} \neq 0$, and we must have $(\zeta + \zeta^4)^{2j} = 1$. As $\zeta + \zeta^4 = \frac{1}{2}(\sqrt{5} - 1) > 0$ we have $j = 0$ and so $\alpha = \pm\zeta^i\beta$, $0 \leqq i \leqq 4$. From (b) and (c) we have $(\pm\zeta^i - 1)\beta \equiv 0 \pmod{(1-\zeta)^2}$, $\beta \not\equiv 0 \pmod{1-\zeta}$, so that

$$\pm\zeta^i - 1 \equiv 0 \pmod{(1-\zeta)^2} .$$

As $i = 0, 1, 2, 3, 4$ this can only hold with the positive sign and $i = 0$, so that $\alpha = \beta$.

3. Dickson's diophantine system. Throughout the rest of this paper p denotes a prime $\equiv 1 \pmod 5$. Our results involve the diophantine system

$$\begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2 , \quad x \equiv 1 \pmod 5 , \\ xw &= v^2 - 4uv - u^2 . \end{aligned} \tag{3.1}$$

A theorem of Dickson [1] asserts that (3.1) has exactly four solutions. If (x, u, v, w) is one of these, the other three are given by $(x, -u, -v, w)$, $(x, v, -u, -w)$, $(x, -v, u, -w)$. Taking the first equation in (3.1) modulo 8 and the second one modulo 4 we can show (after a little calculation) that $x + 2u - w \equiv x + 2v + w \equiv 0 \pmod 4$ for *any* solution of (3.1). This enables us to make the following definition.

DEFINITION 1. For any solution (x, u, v, w) of (3.1) we define $\psi \equiv \psi(x, u, v, w) \in Z[\zeta]$ by

$$\psi = c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 , \tag{3.2}$$

where $c_i \equiv c_i(x, u, v, w) \in Z (1 \leqq i \leqq 4)$ are given by

$$
\begin{aligned}
4c_1 &= -x + 2u + 4v + 5w\ , \\
4c_2 &= -x + 4u - 2v - 5w\ , \\
4c_3 &= -x - 4u + 2v - 5w\ , \\
4c_4 &= -x - 2u - 4v + 5w\ .
\end{aligned} \tag{3.3}
$$

The properties of ψ that we shall need are given in the next lemma.

LEMMA 3. (a) $\psi\bar{\psi} = p$.
(b) $\psi \equiv -1 \pmod{(1-\zeta)^2}$.
(c) *If* $\sigma_i (1 \leqq i \leqq 4)$ *is the automorphism of* $Q(\zeta)$ *defined by* $\sigma_i(\zeta) = \zeta^i$ *then G.C.D.* (ψ_1, ψ_2) *is a prime of* $Z[\zeta]$, *where* $\psi_i = \sigma_i(\psi)(1 \leqq i \leqq 4)$.

Proof. (a) As $\zeta + \zeta^4 = 1/2(-1+\sqrt{5})$, $\zeta^2 + \zeta^3 = 1/2(-1-\sqrt{5})$, we have from (3.2)

$$
\begin{aligned}
\psi\bar{\psi} &= \Big\{(c_1^2 + c_2^2 + c_3^2 + c_4^2) - \frac{1}{2}(c_1c_2 + c_2c_3 + c_3c_4 + c_1c_3 \\
&\quad + c_1c_4 + c_2c_4) + \frac{\sqrt{5}}{2}(c_1c_2 + c_2c_3 + c_3c_4 - c_1c_3 \\
&\quad - c_1c_4 - c_2c_4)\Big\} \\
&= \frac{1}{16}(x^2 + 50u^2 + 50v^2 + 125w^2) - \frac{5\sqrt{5}}{8} \\
&\quad \times (v^2 - 4uv - u^2 - xw) = p\ .
\end{aligned}
$$

(b) From (3.1) and (3.3) we have

$$
c_1 + c_2 + c_3 + c_4 = -x \equiv -1,\ c_1 + 2c_2 + 3c_3 + 4c_4 \equiv 0 \pmod 5\ ,
$$

so that $\psi \equiv -1 \pmod{(1-\zeta)^2}$.

(c) Let π be a prime dividing p. As $p \equiv 1 \pmod 5$ we have $p = \pi_1\pi_2\pi_3\pi_4$, where $\pi_i = \sigma_i(\pi)$, $1 \leqq i \leqq 4$. By (a) ψ is (up to multiplication by a unit) one of $\pi_1\pi_2$, $\pi_1\pi_3$, $\pi_2\pi_4$, $\pi_3\pi_4$. In each case G.C.D. (ψ_1, ψ_2) is a prime.

Lemma 1 and Lemma 3(c) enable us to define a *prime* $\mathscr{K}$ of $Z[\zeta]$ as follows.

DEFINITION 2. For any solution (x, u, v, w) of (3.1) we let $\mathscr{K} \equiv \mathscr{K}(x, u, v, w) \in Z[\zeta]$ be such that

$$
\mathscr{K} \sim \text{G.C.D.}\,(\psi_1, \psi_2)\ , \quad \mathscr{K} \equiv -1 \pmod{(1-\zeta)^2}\ .
$$

We remark that $\mathscr{K}$ is not unique, indeed all such $\mathscr{K}$ are given by

$(-1)^r(\zeta+\zeta^4)^{2r}\mathscr{K}(r \in Z)$. However this does not matter for our purposes. Next we give the prime decomposition of ψ using Lemma 2.

LEMMA 4. $\psi = -\mathscr{K}_1\mathscr{K}_3$.

Proof. As $\mathscr{K} \sim$ G.C.D. (ψ_1, ψ_2) we have $\mathscr{K}_1 | \psi_1$, say, $\psi_1 = \mathscr{K}_1\lambda_1$. Hence $\psi_2 = \mathscr{K}_2\lambda_2$ and as $\mathscr{K}_1 | \psi_2$ we must have $\mathscr{K}_1 | \lambda_2$, that is $\mathscr{K}_3 | \lambda_1$, say $\lambda_1 = \mathscr{K}_3\mu$. Then $\psi_1 = \mathscr{K}_1\mathscr{K}_3\mu$ and so we have

$$\begin{aligned}\mathscr{K}_1\mathscr{K}_2\mathscr{K}_3\mathscr{K}_4 = p = \psi_1\bar{\psi}_1 &= (\mathscr{K}_1\mathscr{K}_3\mu)(\mathscr{K}_4\mathscr{K}_2\bar{\mu}) \\ &= \mathscr{K}_1\mathscr{K}_2\mathscr{K}_3\mathscr{K}_4\mu\bar{\mu} .\end{aligned}$$

Hence we have $\mu\bar{\mu} = 1$, so that μ is a unit of $Z[\zeta]$, proving that $\psi \sim \mathscr{K}_1\mathscr{K}_3$. Clearly ψ and $-\mathscr{K}_1\mathscr{K}_3$ satisfy the conditions of Lemma 2 so that $\psi = -\mathscr{K}_1\mathscr{K}_3$.

Finally in this section we set for any solution (x, u, v, w) of (3.1):

$$\alpha(x,u,v,w) = \frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)} \tag{3.4}$$

and prove

LEMMA 5. $\alpha(x, u, v, w) \equiv \zeta \pmod{\mathscr{K}}$.

Proof. From (3.2) and $\psi_1 \equiv \psi_2 \equiv 0 \pmod{\mathscr{K}}$ we obtain modulo $\mathscr{K}$:

$$\begin{aligned} 5c_1 &\equiv (\zeta^2 - 1)\psi_3 + (\zeta - 1)\psi_4 , \\ 5c_2 &\equiv (\zeta^4 - 1)\psi_3 + (\zeta^2 - 1)\psi_4 , \\ 5c_3 &\equiv (\zeta - 1)\psi_3 + (\zeta^3 - 1)\psi_4 , \\ 5c_4 &\equiv (\zeta^3 - 1)\psi_3 + (\zeta^4 - 1)\psi_4 . \end{aligned}$$

Appealing to (3.3) we get

$$\begin{aligned} x &\equiv \psi_3 + \psi_4 , & 25u &\equiv \alpha\psi_3 + \beta\psi_4 , \\ 25v &\equiv \beta\psi_3 - \alpha\psi_4 , & 25w &\equiv -\gamma\psi_3 + \gamma\psi_4 , \end{aligned}$$

where

$$\begin{aligned} \alpha &= -2\zeta + \zeta^2 - \zeta^3 + 2\zeta^4 , \\ \beta &= \zeta + 2\zeta^2 - 2\zeta^3 - \zeta^4 , \\ \gamma &= \zeta - \zeta^2 - \zeta^3 + \zeta^4 . \end{aligned}$$

It is easy to check that

$$\alpha\beta = \alpha^2 - \beta^2 = 5\gamma , \quad \gamma^2 = 5 .$$

After some calculation we find that

$$25\{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)\} \\ \equiv 4\gamma\psi_3\psi_4((2 + 2\zeta)\psi_3 + 2\zeta^3\psi_4)$$

and

$$25\{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)\} \\ \equiv 4\gamma\psi_3\psi_4((2 + 2\zeta^4)\psi_3 + 2\zeta^2\psi_4)$$

from which the result follows immediately.

4. Outline of method. We start with the necessary and sufficient condition for D (without loss of generality we may take D to be a (positive) prime) to be a quintic residue (mod p) in terms of congruences (mod D) involving a solution of (3.1). These have been given for $D = 2, 3, 5, 7$ in [4] and for $D = 11, 13, 17, 19$ in [9]. Results for other values of D could be obtained using the period equation as in [9]. If D is a quintic nonresidue (mod p) this condition is used to specify a unique solution of (3.1) by means of congruences (mod D). This unique solution is specified in such a way that after using Lemma 4 we find that the corresponding $\mathscr{K}$ satisfies $(\mathscr{K}/D)_5 = \zeta$. If $D \neq 5$ we can then appeal to Eisenstein's reciprocity law

"If $\alpha \equiv -1 \pmod{(1-\zeta)^2}$ and a is a rational integer prime to 5 then $(\alpha/a)_5 = (a/\alpha)_5$"

to obtain $(D/\mathscr{K})_5 = \zeta$, so that $D^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod{\mathscr{K}}$ by Lemma 5. As both $D^{(p-1)/5}$ and $\alpha(x, u, v, w)$ are rational we have $D^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod p$ as required. If $D = 5$ we must replace the use of Eisenstein's reciprocity law by Kummer's supplement to the law of quintic reciprocity involving the prime $1 - \zeta$ [7]. Unfortunately, this requires working modulo 25 rather than modulo 5 and so involves a large number of cases. We thus give an alternative approach based on a result of Muskat [5].

5. $D = 2$. Lehmer [2] has shown that 2 is a quintic residue (mod p) if and only if $x \equiv 0 \pmod 2$, where (x, u, v, w) is any solution of (3.1). Thus if 2 is a quintic nonresidue (mod p) we can find by Dickson's theorem a unique solution (x, u, v, w) of (3.1) such that

$$(5.1) \qquad x \equiv 1 \pmod 2\,, \quad u \equiv 0 \pmod 2\,, \quad x + u - v \equiv 0 \pmod 4\,.$$

In terms of this solution a simple calculation using (3.3) shows that $\psi \equiv \zeta^3 \pmod 2$. Then by an examination of cases in conjunction with $\psi = -\mathscr{K}_1\mathscr{K}_3$ (Lemma 4) we find that

$$\mathscr{K} \equiv \zeta^2\,, \quad \zeta + \zeta^3 \quad \text{or} \quad \zeta + \zeta^2 + \zeta^3 \pmod 2\,,$$

so that $(\mathscr{K}/2)_5 = \zeta$. Appealing to Eisenstein's reciprocity theorem as indicated in § 4 we have reproved

THEOREM 1 (Lehmer [3]). *Let p be a* prime $\equiv 1 \pmod 5$ *for which* 2 *is a quintic nonresidue* $(\bmod p)$. *Let* (x, u, v, w) *be the unique solution of* (3.1) *satisfying* (5.1). *Then we have*

$$2^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod p .$$

6. $D = 3$. (Lehmer [2] has shown that 3 is a quintic residue $(\bmod p)$ if and only if $u \equiv v \equiv 0 \pmod 3$, where (x, u, v, w) is any solution of (3.1).) Thus if 3 is a quintic nonresidue $(\bmod p)$ we can find by Dickson's theorem a unique solution (x, u, v, w) of (3.1) satisfying one of

$$(6.1)\quad \begin{array}{lllll} \text{(a)} & x \equiv 1, & u \equiv 1, & v \equiv 0, & w \equiv 2 \pmod 3, \\ \text{(b)} & x \equiv 2, & u \equiv 2, & v \equiv 0, & w \equiv 1 \pmod 3, \\ \text{(c)} & x \equiv 1, & u \equiv 2, & v \equiv 1, & w \equiv 1 \pmod 3, \\ \text{(d)} & x \equiv 2, & u \equiv 1, & v \equiv 2, & w \equiv 2 \pmod 3 . \end{array}$$

In terms of this solution a simple calculation using (3.3) shows that

$$\begin{array}{lll} \psi \equiv -\zeta - \zeta^2 + \zeta^4 \pmod 3, & \text{if} & \text{(a) holds}, \\ \psi \equiv \zeta + \zeta^2 - \zeta^4 \pmod 3, & \text{if} & \text{(b) holds}, \\ \psi \equiv -\zeta^4 \pmod 3, & \text{if} & \text{(c) holds}, \\ \psi \equiv \zeta^4 \pmod 3, & \text{if} & \text{(d) holds}. \end{array}$$

Then by an examination of cases (mod 3) in conjunction with Lemma 4 we find that

$$\begin{array}{ll} \mathscr{K} \equiv \pm(\zeta - \zeta^2 - \zeta^4),\ \pm(\zeta - \zeta^2 + \zeta^3 + \zeta^4) \pmod 3, & \text{if (a) holds}, \\ \mathscr{K} \equiv \pm(\zeta^3 - \zeta^4),\ \pm(\zeta - \zeta^2 - \zeta^3) \pmod 3, & \text{if (b) holds}, \\ \mathscr{K} \equiv \pm\zeta,\ \pm(\zeta - \zeta^3 - \zeta^4) \pmod 3, & \text{if (c) holds}, \\ \mathscr{K} \equiv \pm(\zeta^3 + \zeta^4),\ \pm(\zeta + \zeta^3 + \zeta^4) \pmod 3, & \text{if (d) holds}, \end{array}$$

so that in every case $(\mathscr{K}/3)_5 = \zeta$. Appealing to Eisenstein's reciprocity theorem as before we have the following result.

THEOREM 2. *Let p be a* prime $= 1 \pmod 5$ *for which* 3 *is a quintic nonresidue* $(\bmod p)$. *Let* (x, u, v, w) *be the unique solution of* (3.1) *satisfying* (6.1). *Then we have*

$$3^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod p .$$

7. $D = 5$. For p a prime $\equiv 1 \pmod 5$, g a primitive root $(\bmod p)$,

h, k integers selected from 0, 1, 2, 3, 4, the cyclotomic number $(h, k)_5$ is defined to be the number of solutions (s, t) with $0 \leqq s, t < (p-1)/5$ of $g^{5s+h} + 1 \equiv g^{5t+k} \pmod{p}$. Let (x, u, v, w) be *any* solution of (3.1). Choose g such that $(g/\mathscr{K})_5 = \zeta$. Then it can be shown that

$$\begin{aligned}
25(0, 0)_5 &= p - 14 + 3x \, , \\
100(0, 1)_5 = 100(1, 0)_5 = 100(4, 4)_5 &= 4p - 16 - 3x + 50v + 25w \, , \\
100(0, 2)_5 = 100(2, 0)_5 = 100(3, 3)_5 &= 4p - 16 - 3x + 50u - 25w \, , \\
100(0, 3)_5 = 100(3, 0)_5 = 100(2, 2)_5 &= 4p - 16 - 3x - 50u - 25w \, , \\
100(0, 4)_5 = 100(4, 0)_5 = 100(1, 1)_5 &= 4p - 16 - 3x - 50v + 25w \, , \\
100(1, 2)_5 = 100(1, 4)_5 = 100(2, 1)_5 &= 100(3, 4)_5 = 100(4, 1)_5 \\
&= 100(4, 3)_5 = 4p + 4 + 2x - 50w \, , \\
100(1, 3)_5 = 100(2, 3)_5 = 100(2, 4)_5 &= 100(3, 1)_5 = 100(3, 2)_5 \\
&= 100(4, 2)_5 = 4p + 4 + 2x + 50w \, ,
\end{aligned}$$

and Muskat [5] has shown that

$$\mathrm{ind}_g (5) \equiv (0, 4)_5 - (0, 1)_5 + 2((0, 3)_5 - (0, 2)_5) \pmod{5}$$

so that

$$\mathrm{ind}_g (5) \equiv -2u - v \pmod{5} \, .$$

Thus if 5 is a quintic nonresidue $\pmod{p}$ $2u + v \not\equiv 0 \pmod{5}$ and by Dickson's theorem there is a unique solution of (3.1) satisfying $2u + v \equiv 4 \pmod{5}$. With this solution we have $\mathrm{ind}_g (5) \equiv 1 \pmod{5}$ and so

$$5^{(p-1)/5} \equiv g^{\mathrm{ind}_g(5) \cdot (p-1)/5} \equiv g^{(p-1)/5} \equiv \left(\frac{g}{\mathscr{K}}\right)_5 \equiv \zeta \pmod{\mathscr{K}} \, .$$

Thus we have proved

THEOREM 3. *Let p be a* prime $\equiv 1 \pmod{5}$ *for which* 5 *is a quintic nonresidue* $\pmod{p}$. *Let (x, u, v, w) be the unique solution of* (3.1) *satisfying* $2u + v \equiv 4 \pmod{5}$. *Then we have*

$$5^{(p-1)/5} \equiv \alpha(x, u, v, w) \pmod{p} \, .$$

8. EXAMPLE. We take $p = 311$. A solution of (3.1) in this case is $(-49, 7, 0, 1)$ (see for example [8]) so none of 2, 3, 5 is a quintic residue (mod 311). The unique solution given by Theorem 1 is $(-49, 0, 7, -1)$ so that

$$2^{(p-1)/5} = 2^{62} \equiv \frac{2276 - 98.46}{2276 + 98.94} \equiv \frac{-2232}{11488} \equiv \frac{-55}{-19} \equiv 52 \pmod{311} \, .$$

The unique solution given by Theorem 2 is $(-49, -7, 0, 1)$ so that

$$3^{(p-1)/5} = 3^{62} \equiv \frac{-2276 + 98.66}{-2276 - 98.214} \equiv \frac{4192}{-23248} \equiv \frac{149}{77} \equiv 216 \pmod{311} .$$

The unique solution given by Theorem 3 is $(-49, 7, 0, 1)$ so that

$$5^{(p-1)/5} = 5^{62} \equiv \frac{-2276 - 98.214}{-2276 + 98.66} \equiv \frac{-23248}{4192} \equiv \frac{77}{149} \equiv 36 \pmod{311} .$$

REFERENCES

1. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., **57** (1935), 391-424.

2. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J., **18** (1951), 11-18.

3. ———, *On Euler's criterion*, J. Austral. Math. Soc., **1** (1959) 64-70.

4. ———, *On the divisors of the discriminant of the period equation*, Amer. J. Math., **90** (1968), 375-379.

5. J. B. Muskat, *On the solvability of* $x^e \equiv e \pmod{p}$, Pacific J. Math., **14** (1964), 257-260.

6. K. S. Williams, *On Euler's criterion for cubic nonresidues*, Proc. Amer. Math. Soc., **49** (1975), 277-283.

7. ———, *Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity*, J. für Math., (to appear).

8. ———, *Table of solutions* (x, u, v, w) *of the diophantine system* $16p = x^2 + 50u^2 + 50v^2 + 125w^2$, $xw = v^2 - 4uv - u^2$, $x \equiv 1 \pmod 5$, *for primes* $p < 10,000$, $p \equiv 1 \pmod 5$, Unpublished Mathematical Tables File of American Mathematical Society (with B. Lowe).

9. ———, *Explicit criteria for quintic residuality* (submited for publication).

Received June 4, 1974 and in revised form August 8, 1975. Research supported by National Research Council of Canada Grant No. A-7233.

CARLETON UNIVERSITY