ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 4, Fall 1989

RESIDUACITY OF PRIMES

RONALD EVANS

ABSTRACT. Let q,p be distinct primes with $p = ef + 1$. A variant of the Kummer-Dedekind theorem is proved for Gaussian periods, which shows in particular that q is an e-th power $(\bmod p)$ if and only if the Gaussian period polynomial of degree e has e (not necessarily distinct) linear factors $(\bmod q)$. This is applied to give a simple criterion in terms of the parameters in the partitions $p = 8f+1 = \mathbf{X}^2+\mathbf{Y}^2 = \mathbf{C}^2+2\mathbf{D}^2$ for an odd prime q to be an octic residue $(\bmod p)$. Some consequences and a generalization of an analogous quartic residuacity law (proved by E. Lehmer in 1958) are also given.

1. Introduction. Throughout, let p and q be distinct primes with $p = ef + 1$. In [**8**], E. Lehmer gave elegant criteria for an odd prime q to be an e-th power residue $(\bmod p)$, for $e = 3, 4$. The result given for $e = 4$ was essentially the following theorem.

THEOREM 1.1. *Let p be a prime $\equiv 1 (\bmod 4)$ and write*

$$p = \mathbf{X}^2 + \mathbf{Y}^2, \quad \mathbf{X} \equiv 1 \pmod 4. \tag{1.1}$$

Then an odd prime $q \neq p$ is quartic $(\bmod p)$ if and only if

$$\left(\frac{(2/p)}{q}\right) = 1, q|\mathbf{Y}, \text{ or } \left(\frac{2(2/p)(p+\mathbf{X}s)}{q}\right) = 1, \quad q \nmid \mathbf{Y}, \tag{1.2}$$

where s is any integer satisfying $p \equiv s^2 (\bmod q)$, and $(2/p)$ is the Legendre symbol.

In view of the congruence $(p+\mathbf{Y}s)(2p+2\mathbf{X}s) \equiv (p+\mathbf{X}s+\mathbf{Y}s)^2 (\bmod q)$, one can replace (1.2) by the equivalent condition

$$\left(\frac{2(2/p)}{q}\right) = 1, q|\mathbf{X}, \text{ or } \left(\frac{(2/p)(p+\mathbf{Y}s)}{q}\right) = 1, q \nmid \mathbf{X}. \tag{1.3}$$

AMS *Subject classification*: Primary 11A15, 11T21; Secondary 11T06.
Received by the editors on January 22, 1987.

In §2, we apply Theorem 1.1 to answer some questions posed in [**10**] and to extend some results given in [**6, 9**]. In §3, we prove an extension of Theorem 1.1 which also slightly generalizes a result of Williams, Hardy, and Friesen [**14**]. Our proof in §3 is considerably shorter than that in [**14**], at the expense of being less elementary.

The main results of this paper are Theorems 4.1 and 5.1. Theorem 5.1 is the counterpart of Theorem 1.1 for $e = 8$. It gives a simple criterion in terms of the parameters in the partitions $p = 8f + 1 = \mathbf{X}^2 + \mathbf{Y}^2 = \mathbf{C}^2 + 2\mathbf{D}^2$ for an odd prime $q \neq p$ to be an octic residue $(\bmod\, p)$. Special cases have been given by von Lienen [**11**]. The proof of Theorem 5.1 is based on the fact that a prime $q \neq p$ is an e-th power $(\bmod\, p)$ if and only if the Gaussian period polynomial of degree e has e (not necessarily distinct) linear factors over $\mathbf{GF}(q)$. This fact is a special case of Theorem 4.1.

2. Applications of Theorem 1.1. Throughout this section, p is a prime $\equiv 1 \pmod 4$ such that (1.1) holds, q is an odd prime $\neq p$, and s is an integer such that $p \equiv s^2 (\bmod\, q)$. If, further, $p \equiv 1 (\bmod\, 8)$, write

$$p = \mathbf{C}^2 + 2\mathbf{D}^2, \quad \mathbf{C} \equiv 1 (\bmod\, 4). \tag{2.1}$$

In [**10**, p. 478], E. Lehmer asks for a characterization of the (odd prime) divisors of $\mathbf{C}$ and $\mathbf{D}$ which are quartic $(\bmod\, p)$. This is given in the following theorem.

THEOREM 2.1. *Suppose that* $p \equiv 1 (\bmod\, 8)$. *If* $q | \mathbf{D}$, *then* q *is quartic* $(\bmod\, p)$ *if and only if*

$$q | \mathbf{Y} \text{ or } \left(\frac{2p + 2\mathbf{XC}}{q} \right) = 1. \tag{2.2}$$

If $q | \mathbf{C}$, *then* q *is quartic* $(\bmod\, p)$ *if and only if*

$$q | \mathbf{Y} \text{ or } \left(\frac{2p + 2\mathbf{XD}\sqrt{2}}{q} \right) = 1, \tag{2.3}$$

where $\sqrt{2}$ *denotes any square root of* $2 (\bmod\, q)$ (*which exists since* $p \equiv 2\mathbf{D}^2 (\bmod\, q)$).

PROOF. Choose s to be $\mathbf{C}$ or $\mathbf{D}\sqrt{2}$ according to whether $q|\mathbf{D}$ or $q|\mathbf{C}$, and use (1.2). □

A direct proof of the following theorem was solicited by E. Lehmer in [**10**, p. 478].

THEOREM 2.2. *Suppose that* $p \equiv 1 \pmod 8$ *and* q *divides* $\mathbf{C}^4 - p\mathbf{X}^2$ *or* $4\mathbf{D}^4 - p\mathbf{Y}^2$. *Then* q *is quartic* $\pmod p$.

PROOF. All congruences in this proof are $\pmod q$. If $q|\mathbf{Y}$, then q is quartic by (1.2), so let $q \nmid \mathbf{Y}$. Suppose that $q|\mathbf{X}$. If $q|\mathbf{C}^4 - p\mathbf{X}^2)$, then $q|\mathbf{C}$ and $\mathbf{Y}^2 \equiv p \equiv 2\mathbf{D}^2$ so that $(2/q) = 1$. If $q|(4\mathbf{D}^4 - p\mathbf{Y}^2)$, then $4\mathbf{D}^4 \equiv \mathbf{Y}^4$ so that $\mathbf{Y}^2 \equiv \pm 2\mathbf{D}^2$. If the plus sign is valid, then $(2/q) = 1$, otherwise $\mathbf{Y}^2 \equiv -2\mathbf{D}^2 = \mathbf{C}^2 - p \equiv \mathbf{C}^2 - \mathbf{Y}^2$ so that $2\mathbf{Y}^2 \equiv \mathbf{C}^2$, and again $(2/q) = 1$. Therefore, if $q|\mathbf{X}$, then $(2/q) = 1$, so q is quartic by (1.3). It remains to consider the case $q\mathbf{X} \nmid \mathbf{Y}$.

Suppose first that $q|(4\mathbf{D}^4 - p\mathbf{Y}^2)$. If $q|\mathbf{C}$, then $p^2 \equiv 4\mathbf{D}^4 \equiv p\mathbf{Y}^2$ and so $q|\mathbf{X}$. Thus $q \nmid \mathbf{C}$. For some choice of $s \equiv \sqrt{p}, s\mathbf{Y} \equiv -2\mathbf{D}^2$, so $p + s\mathbf{Y} \equiv \mathbf{C}^2 \not\equiv 0$. Thus q is quartic by (1.3).

Finally, suppose that $q|(\mathbf{C}^4 - p\mathbf{X}^2)$. If $q|\mathbf{D}$, then $p^2 \equiv \mathbf{C}^4 \equiv p\mathbf{X}^2$, giving $q|\mathbf{Y}$. Thus $q \nmid \mathbf{D}$. For some choice of $s \equiv \sqrt{p}, s\mathbf{X} \equiv -\mathbf{C}^2$, and then $2p + 2s\mathbf{X} \equiv 4\mathbf{D}^2 \equiv 0$. Thus q is quartic by (1.2). □

Special cases of the next two theorems were given by the Lehmers. D.H. and E. Lehmer [**6**] obtained the special cases $t = 1, k = 1, -3$ of Theorem 2.3 by looking at cyclotomic resultants. E. Lehmer [**9**] obtained the special case $t = 0, k = 3$ of Theorem 2.4.

THEOREM 2.3. *Suppose that* $q \nmid \mathbf{Y}$ *and* $(t^2 + k^2 p - 2(2/p)p)^2 \equiv 4p(\mathbf{X} - kt)^2 \pmod q$ *for some integers* k, t. *Then* q *is quartic* $\pmod p$.

PROOF. For some choice of $s \equiv \sqrt{p} \pmod q$,

$$2s(2/p)(\mathbf{X} - kt) \equiv -2(2/p)p + t^2 + k^2 p \pmod q.$$

Thus

$$(2/p)(2p+2s\mathbf{X}) \equiv 2(2/p)skt + t^2 + k^2p \equiv (ks+t(2/p))^2 (\bmod q).$$

The members of this congruence are nonzero $(\bmod q)$, otherwise $0 \equiv (2p+2s\mathbf{X})(2p-2s\mathbf{X}) \equiv 4p\mathbf{Y}^2 (\bmod q)$. Thus q is quartic by (1.2). □

THEOREM 2.4. *Suppose that* $q \nmid \mathbf{X}$ *and* $(t^2+k^2p-(2/p)p)^2 \equiv p(\mathbf{Y}-2kt)^2 (\bmod q)$ *for some integers* k, t. *Then* q *is quartic* $(\bmod p)$.

PROOF. For some choice of $s \equiv \sqrt{p} (\bmod q)$,

$$s(2/p)(\mathbf{Y}-2kt) \equiv -(2/p)p + t^2 + k^2p (\bmod q).$$

Thus,

$$(2/p)(p+s\mathbf{Y}) \equiv 2(2/p)skt + t^2 + k^2p \equiv (ks+t(2/p))^2 (\bmod q).$$

The members of the above congruence are nonzero $(\bmod q)$, otherwise $0 \equiv (p+s\mathbf{Y})(p-s\mathbf{Y}) \equiv p\mathbf{X}^2 (\bmod q)$. Thus q is quartic by (1.3). □

3. Extension of Theorem 1.1. Throughout this section, let q be an odd prime and let $\varepsilon = (-1)^{(q-1)/2}$. Let m be a squarefree positive integer $\not\equiv 0 (\bmod q)$ such that $s = \sqrt{m}$ exists $(\bmod q)$, and let $\mathbf{M}$ denote the largest odd factor of m. Let $\mathbf{A}, \mathbf{B}, \mathbf{C}$ be pairwise relatively prime integers such that $\mathbf{A} > 0, q \nmid \mathbf{ABC}, 2 \nmid \mathbf{B}$, and $\mathbf{A}^2 = m(\mathbf{B}^2 + \mathbf{C}^2)$. Observe that any odd prime p dividing $\mathbf{A}$ satisfies $p \equiv 1 (\bmod 4)$, since $\mathbf{B}^2 + \mathbf{C}^2 = \mathbf{A}^2/m \equiv 0 (\bmod p)$. Thus $\mathbf{M} \equiv 1 (\bmod 4)$.

Let x, y, and z denote the number of primes p dividing $\mathbf{M}$ for which $q^{(p-1)/4} \equiv \mathbf{C}/\mathbf{B}, -\mathbf{C}/\mathbf{B}$, and $-1 (\bmod p)$, respectively. In the case that every prime factor of m is a square $(\bmod q)$, we have $x = y = 0$ and Theorem 3.1 below reduces to the result [**14**, p. 257] of Williams, Hardy, and Friesen. Taking $m = p, \mathbf{A} = p, \mathbf{B} = \mathbf{X}, \mathbf{C} = \mathbf{Y}$, with $p, \mathbf{X}, \mathbf{Y}$ as in (1.1), we see that Theorem 3.1 implies Theorem 1.1 in the case $q \nmid \mathbf{XY}$.

THEOREM 3.1. *We have*

$$\left(\frac{2\mathbf{A}+2\mathbf{C}s}{q}\right) = \left(\frac{\mathbf{A}+\mathbf{B}s}{q}\right) = (-1)^{(8z+4x-4y+(q-1)(M+q)+(m-1)(q-\varepsilon))/8}.$$

Our proof of Theorem 3.1 depends on the well-known properties (3.1)-(3.4) listed below for the quartic residue symbol $\chi_\alpha(\beta)$ defined as in [**4**, p. 122] for $\alpha, \beta \in \mathbf{Z}[i]$ with $(\alpha, 2\beta) = 1, \alpha \nmid 1$.

$$\chi_\alpha(\beta)\chi_{\overline{\alpha}}(\overline{\beta}) = 1 \quad [\mathbf{4}, \text{ p. } 122]; \tag{3.1}$$

$$\chi_\alpha(\beta) = 1, \text{ if } \alpha, \beta \in \mathbf{Z} \quad [\mathbf{4}, \text{ p. } 122]; \tag{3.2}$$

$$\chi_q(1+i) = i^{(q-\varepsilon)/4} \quad [\mathbf{4}, \text{ p. } 136]; \tag{3.3}$$

$$\chi_\beta(\alpha) = \chi_\alpha(\beta)(-1)^{bd/4}, \quad \text{if } a, b, c, d \in \mathbf{Z} \text{ are} \tag{3.4}$$

chosen such that $\alpha = a + bi$ and $\beta = c + di$ are primary.

(Recall that $\alpha = a + bi$ is *primary* is a is odd, b is even, and $a + b \equiv 1 (\operatorname{mod} 4)$.) Formula (3.4) is a version of the law of quartic reciprocity [**4**, p. 123].

To facilitate the proof of Theorem 3.1, we prove the following lemma.

LEMMA 3.2. *For $a, b \in \mathbf{Z}, \chi_q^2(a + bi) = \left(\frac{a^2+b^2}{q}\right)$.*

PROOF. If $q \equiv -1 (\operatorname{mod} 4)$, then q is prime in $\mathbf{Z}[i]$, so

$$\begin{aligned}\chi_q^2(a+bi) &\equiv (a+bi)^{(q^2-1)/2} \equiv \Big((a+bi)^q(a+bi)\Big)^{(q-1)/2} \\ &\equiv ((a-bi)(a+bi))^{(q-1)/2} \equiv \Big(\frac{a^2+b^2}{q}\Big) (\operatorname{mod} q)\end{aligned}$$

and the result follows. If $q \equiv 1 (\operatorname{mod} 4)$, then $q = \alpha\overline{\alpha}$ for some primary $\alpha, \overline{\alpha} \in \mathbf{Z}[i]$, so, by (3.1),

$$\begin{aligned}\chi_q^2(a+bi) &= \chi_\alpha^2(a+bi)\chi_{\overline{\alpha}}^2(a+bi) = \chi_\alpha^2(a+bi)\chi_\alpha^2(a-bi) \\ &= \chi_\alpha^2(a^2+b^2) \equiv (a^2+b^2)^{(q-1)/2} \equiv \Big(\frac{a^2+b^2}{q}\Big)(\operatorname{mod} \alpha),\end{aligned}$$

and the result follows.

PROOF OF THEOREM 3.1. Since

$$2(\mathbf{A}+\mathbf{B}s)(\mathbf{A}+\mathbf{C}s) \equiv (\mathbf{A}+\mathbf{B}s+\mathbf{C}s)^2 \not\equiv 0 (\operatorname{mod} q),$$

the first equality is proved.

Without loss of generality, we now fix the signs of $\mathbf{B}$ and $\mathbf{C}$ so that $\mathbf{B}+\mathbf{C} \equiv 1 \pmod 4$ or $\mathbf{B} \equiv \mathbf{C} \equiv 1 (\operatorname{mod} 4)$ according to whether $\mathbf{C}$ is even or odd. Define

$$\alpha = \begin{cases} B+iC, & \text{if } 2|C, \\ (B+iC)/(1+i), & \text{if } 2 \nmid C. \end{cases}$$

Then α is primary and

$$\alpha\overline{\alpha} = MA^2/m^2 \equiv 1 (\operatorname{mod} 2). \tag{3.6}$$

Let p be any odd prime divisor of $\mathbf{A}$. Write $p = \pi\overline{\pi}$ for distinct primary primes $\pi, \overline{\pi} \in \mathbf{Z}[i]$. We may suppose that $\pi|\alpha$ (otherwise interchange π and $\overline{\pi}$).

We proceed by evaluating $\chi_q(\alpha)$ in two different ways. First, by (3.6),

$$\chi_q(\alpha) = \Pi_{q|M}(\chi_q(\pi)) \cdot \Pi_{p^k||A/m}(\chi_q(\pi^{2k})). \tag{3.7}$$

By Lemma 3.2,

$$\Pi_{p^k||A/m}(\chi_q^{2k}(\pi)) = \Pi_{p^k||A/m}\left(\frac{p}{q}\right)^k = \left(\frac{A/m}{q}\right) = \left(\frac{A}{q}\right),$$

since $A > 0$. By (3.4), for each $p|M$,

$$\chi_q(\pi) = \chi_{q\varepsilon}(\pi) = \chi_\pi(q\varepsilon),$$

since $q\varepsilon$ is primary. Since

$$\Pi_{p|M}(\chi_\pi(\varepsilon)) = \varepsilon^{(M-1)/4} = (-1)^{(q-1)(M-1)/8},$$

(3.7) becomes

$$\left(\frac{A}{q}\right)\chi_q(\alpha) = (-1)^{(q-1)(M-1)/8}\Pi_{p|M}(\chi_\pi(q)). \tag{3.8}$$

For each $p|M$, $\chi_\pi(q) \equiv q^{(p-1)/4} (\mathrm{mod}\, \pi)$. Since $\pi|(B+iC), i \equiv C/B (\mathrm{mod}\, \pi)$; thus $\chi_\pi(q) = i, -i, -1$, or 1 depending on whether $q^{(p-1)/4} \equiv C/B, -C/B, -1$ or $1 (\mathrm{mod}\, p)$. Thus (3.8) becomes

$$\left(\frac{A}{q}\right)\chi_q(\alpha) = (-1)^{(q-1)(M-1)/8} i^{x-y}(-1)^z. \tag{3.9}$$

Next, since $A^2 = m(B^2 + C^2)$,

$$0 \equiv 2(As + Bm)(B + iC) - (A + sB + siC)^2 (\mathrm{mod}\, q).$$

Thus, by (3.2),

$$\chi_q(B + iC) = \chi_q^2(A + sB + siC).$$

Then, by Lemma 3.2,

$$\chi_q(B + iC) = \left(\frac{2A}{q}\right)\left(\frac{A + Bs}{q}\right). \tag{3.10}$$

Since $M \equiv 1$ (mod 4), we have $m \equiv 1$ or $2 (\mathrm{mod}\, 4)$ depending on whether C is even or odd. Thus, by (3.3) and (3.5),

$$\chi_q(B + iC) = \chi_q(\alpha) i^{(m-1)(q-\varepsilon)/4}. \tag{3.11}$$

Combining (3.9)-(3.11), we obtain

$$\left(\frac{A + Bs}{q}\right) = \left(\frac{2}{q}\right) i^{(m-1)(q-\varepsilon)/4}(-1)^{(q-1)(M-1)/8} i^{x-y}(-1)^z,$$

and the result follows. □

4. Splitting of the period polynomial over GF(q). Let n be a squarefree positive integer, and write $\zeta_n = \exp(2\pi i/n)$. Let G be the group of $\phi(n)$ reduced residues (mod n) and let H be an arbitrary subgroup of index e in G. Thus, if n is prime, then H is the group of e-th power residues (mod n). For $c \in G$, define $\sigma_c \in \mathrm{Gal}\,(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ by $\sigma_c(\zeta_n) = \zeta_n^c$. We sometimes identify G with the Galois group, as in (4.3) below.

By [**1**, p. 218], the generalized Gaussian period

$$\eta = \sum_{h \in H} \sigma_h(\zeta_n) \tag{4.1}$$

is nonzero (since n is squarefree), and in fact η has degree $e = |G/H|$ over $\mathbf{Q}$. Thus, for $c \in G$,

$$\sigma_c(\eta) = \eta \text{ if and only if } c \in H. \tag{4.2}$$

The minimal polynomial of η over $\mathbf{Q}$, viz.

$$\psi(x) = \Pi_{\tau \in G/H}(x - \tau(\eta)), \tag{4.3}$$

is called the period polynomial of η, and its discriminant is denoted by $D(\psi)$.

Let q be a rational prime with $q \nmid n$ (q is not required to be odd in this section). Then q is unramified in $\mathbf{Q}(\zeta_n)$. Often q is viewed as an element of G; for example, $q \in H$ means $q \equiv h (\operatorname{mod} n)$ for some $h \in H$. In view of (4.2), the Frobenius automorphism σ_q is trivial on $\mathbf{Q}(\eta)$ if and only if $q \in H$. Thus [**5**, p. 100]

$$q \text{ splits completely in } \mathbf{Q}(\eta) \text{ if and only if } q \in H. \tag{4.4}$$

It follows immediately from (4.4) and the Kummer-Dedekind factorization theorem [**5**, pp. 32, 33] that if $q \nmid D(\psi)$, then $q \in H$ if and only if $\psi(x)(\operatorname{mod} q)$ has e distinct linear factors. The following theorem shows that, whether $q|D(\psi)$ or not, $q \in H$ if and only if $\psi(x)(\operatorname{mod} q)$ has e (not necessarily distinct) linear factors. For example, if $n = 73$, $e = 4$, $q = 2$, then q divides $D(\psi) = 256X73^2, q$ is in the set H of 4-th power residues (mod 73), and $\psi(x) = x(x+1)^3(\operatorname{mod} q)$ [**1**, (4.3), (4.4)]. (Please replace the misprint $-2p + (-1)^f(3-p)$ by $-2p(-1)^f + 3 - p$ in [**1**, (4.3)].) On the other hand, if $n = 37, e = 4, q = 3$, then q divides $D(\psi) = 37^3X441, q$ is *not* in the set H of 4-th powers (mod 37), and $\psi(x) = (x-1)^2(x^2+1)(\operatorname{mod} q)$, so $\psi(x)$ has only two linear factors $(\operatorname{mod} q)$.

THEOREM 4.1. *Let n be squarefree and let q be a prime with $q \nmid n$. Let H be a subgroup of index e in the group G of reduced residues* $(\operatorname{mod} n)$.

Define $\psi(x)$ as in (4.3). Let F denote the smallest positive integer for which $q^F \in H$. Then F equals the least common multiple of the degrees of the irreducible factors of $\psi(x) \pmod q$. In particular, $q \in H$ if and only if $\psi(x) \pmod q$ has e linear factors.

PROOF. Let R_K denote the ring of integers in $K = \mathbf{Q}(\eta)$. Let Q be a prime ideal dividing q in R_K. View $\mathbf{Z}/q\mathbf{Z}$ as a subfield of R_K/Q. By [**13**, p. 247], $F = |R_K/Q : \mathbf{Z}/q\mathbf{Z}|$. By (4.3), R_K/Q contains the splitting field of $\psi(x) \pmod Q$ (so the degree of each irreducible factor of $\psi(x) \pmod q$ divides F), and it remains to show that R_K/Q equals this splitting field.

Since n is squarefree, the elements $\sigma_c(\zeta_n)(c \in G)$ form a $\mathbf{Z}$-basis for $\mathbf{Q}(\zeta_n)$. Taking the traces of these basis elements from $\mathbf{Q}(\zeta_n)$ down to K, we see [**5**, p.165] that $\tau_1(\eta), \dots, \tau_e(\eta)$ form a $\mathbf{Z}$-basis for K, where $\tau_1, \dots, \tau_e$ denote a complete set of coset representatives for G/H. In particular,

$$R_K = \mathbf{Z}[\tau_1(\eta), \dots, \tau_e(\eta)]. \tag{4.5}$$

This proves that R_K/Q is the splitting field of $\psi(x) \pmod Q$. □

It would be interesting to determine the extent to which (4.5) holds for *general* integers n.

5. Criterion for octic residuacity. In this section we will apply Theorem 4.1 with $e = 8$ and n a prime $p \equiv 1 \pmod 8$. Thus H is the group of octic residues $\pmod p$. Write

$$p = 8f + 1 = X^2 + Y^2 = C^2 + 2D^2, \quad C \equiv X \equiv 1 \pmod 4). \tag{5.1}$$

It is well-known that 2 is octic $\pmod p$ if and only if $Y \equiv 8f \pmod{16}$ [**3**, p. 111], [**12**]. In Theorem 5.1 below, we give a criterion for an *odd* prime $q \neq p$ to be octic $\pmod p$. Corollaries 5.2, 5.3, and 5.4 illustrate the special cases $q = 3$, $q = 5$, $q = 7$, respectively. These and further cases ($q \leq 41$) are considered by von Lienen [**11**, p. 114]. Corollary 5.5 shows that the result on octic residuacity in [**7**] can also be deduced from Theorem 5.1.

THEOREM 5.1. *Let p be a prime satisfying* (5.1) *and let q be an odd prime $\neq p$. Define $E = (-1)^f$. If $q|Y$, then q is octic* $(\bmod p)$ *if and only if*

$$\left(\frac{2EX(X+C)}{q}\right) = 1 \text{ or } \left(\frac{EX(X-C)}{q}\right) = 1. \tag{5.2}$$

If $q \nmid Y$, then q is octic $(\bmod p)$ *if and only if*

(5.3)

$$s^2 \equiv p(\bmod q), r^2 \equiv 2p - 2sX(\bmod q), \text{ and } \left(\frac{2E(s-C)(2s+r)}{q}\right) = 1$$

for some $s, r \in \mathbf{Z}$.

PROOF. From [**2**, p. 390], the eight zeros of $\psi(x)$ in $\mathbf{Q}(\eta)$ are

$$(-1+S+R\pm\sqrt{U})/8,\ (-1+S-R\pm\sqrt{V})/8,$$
$$(-1-S+R_1\pm\sqrt{U_1})/8,\ (-1-S-R_1\pm\sqrt{V_1})/8,$$

where $S=\sqrt{p}, R=\sqrt{2p-2SX},\ R_1=\sqrt{2p+2SX}$,

$$U=2E(S-C)(2S+ENR),\ U_1=2E(S+C)(2S-ENR_1),$$
$$V=2E(S-C)(2S-ENR),\ V_1=2E(S+C)(2S+ENR_1),$$

with $N=1$ or -1 according to whether 2 is quartic or not $(\bmod p)$. Therefore, by Theorem 4.1, q is octic $(\bmod p)$ if and only if there exist integers s, r, r_1 such that

$$s^2 \equiv p(\bmod q),\ r^2 \equiv 2p-2sX(\bmod q),\ r_1^2 \equiv 2p+2sX(\bmod q), \tag{5.4}$$
$$\left(\frac{u}{q}\right) \geq 0,\ \left(\frac{u_1}{q}\right) \geq 0,\ \left(\frac{v}{q}\right) \geq 0, \text{ and } \left(\frac{v_1}{q}\right) \geq 0,$$

where

$$\begin{aligned} u&=2E(s-C)(2s+ENr),\ u_1=2E(s+C)(2s-ENr_1),\\ v&=2E(s-C)(2s-ENr),\ v_1=2E(s+C)(2s+ENr_1).\end{aligned} \tag{5.5}$$

Case 1. $q|Y$. First, (5.2) is equivalent to

$$\left(\frac{2EX(X+C)}{q}\right) \geq 0 \text{ and } \left(\frac{EX(X-C)}{q}\right) \geq 0, \tag{5.6}$$

because $q \nmid 2EX$ and

$$2(X+C)(X-C) = 2(X^2 - C^2) \equiv 2(p - C^2) \equiv (2D)^2 (\operatorname{mod} q),$$

Thus we must show that (5.4) and (5.6) are equivalent. By (5.1), the three congruences in (5.4) automatically hold with $s = -X, r = 2X$, and $r_1 = 0$. With this choice of s, r, r_1, (5.5) yields $u = 4EX(X + C)(1 - EN)$, $v = 4EX(X + C)(1 + EN)$, and $v_1 = u_1 = 4EX(X - C)$. Thus (5.6) holds if and only if

$$\text{(5.7)} \qquad \left(\frac{u}{q}\right) \geq 0, \quad \left(\frac{u_1}{q}\right) \geq 0, \quad \left(\frac{v}{q}\right) \geq 0, \quad \text{and} \left(\frac{v_1}{q}\right) \geq 0.$$

Case 2. $q \nmid Y$. Here we must show that (5.3) and (5.4) are equivalent. Assume that (5.4) holds. We have $r^2 r_1^2 \equiv 4pY^2 \not\equiv 0 (\operatorname{mod} q)$. Clearly q cannot divide both $s - C$ and $s + C$. Assume without loss of generality that $q \nmid (s - C)$; otherwise, replace s by $-s$, which has the effect of interchanging r and r_1, u and u_1, and v and v_1. Then, since $uv \equiv 4(s - C)^2 r_1^2 \not\equiv 0 (\operatorname{mod} q)$, we have $(uv/q) = 1$; by (5.4), $(u/q) = (v/q) = 1$. This proves

$$\text{(5.8)} \qquad \left(\frac{2E(s - C)(2s + r)}{q}\right) = 1,$$

so (5.3) follows.

Conversely, suppose that (5.3) holds. To prove (5.4), we must show that there exists an integer r_1 such that (5.7) holds and

$$\text{(5.9)} \qquad r_1^2 \equiv 2p + 2sX (\operatorname{mod} q).$$

Choose $r_1 \equiv 2sY/r (\operatorname{mod} q)$. Since

$$\text{(5.10)} \qquad (2p + 2sX)r^2 \equiv 4pY^2 \equiv r_1^2 r^2 \not\equiv 0 (\operatorname{mod} q),$$

(5.9) holds. It remains to prove (5.7). There are two subcases.

Subcases 2A. $q | D$. Here $s^2 \equiv p \equiv C^2 (\operatorname{mod} q)$, so $s \equiv \pm C (\operatorname{mod} q)$. By (5.8), $s \equiv -C (\operatorname{mod} q)$. Thus, $u_1 \equiv v_1 \equiv 0 (\operatorname{mod} q)$. By (5.10), $uv \equiv 4(s - C)^2 r_1^2 \not\equiv 0 (\operatorname{mod} q)$, so $(uv/q) = 1$. By (5.8), at least one of $(u/q), (v/q)$ equals 1, so $(u/q) = (v/q) = 1$. This proves (5.7).

Subcase 2B. $q \nmid D$. Here $(s-C)(s+C) \equiv 2D^2 \not\equiv 0 (\bmod q)$, so by (5.10), $uv \equiv 4(s-C)^2 r_1^2 \not\equiv 0(\bmod q)$ and $u_1 v_1 \equiv 4(s+C)^2 r^2 \not\equiv 0(\bmod q)$. Moreover, $0 \not\equiv uu_1 \equiv 4D^2(r - r_1 + 2ENs)^2$. Thus

$$\left(\frac{uv}{q}\right) = \left(\frac{u_1 v_1}{q}\right) = \left(\frac{uu_1}{q}\right) = 1.$$

By (5.8), $(u/q) = 1$ or $(v/q) = 1$, and so $(u/q) = (v/q) = (u_1/q) = (v_1/q) = 1$. This proves (5.7). □

COROLLARY 5.2. *Let p be a prime satisfying* (5.1). *Then* 3 *is octic* $(\bmod p)$ *if and only if* $3|Y$ *and* $C \equiv EX(\bmod 3)$, *where* $E = (-1)^f$.

COROLLARY 5.3. *Let p be a prime satisfying* (5.1). *Then* 5 *is octic* $(\bmod p)$ *if and only if* $5|Y$ *and* $C \equiv X$ *or* $3X(\bmod 5)$.

COROLLARY 5.4. *Let p be a prime satisfying* (5.1). *Then* 7 *is octic* $(\bmod p)$ *if and only if either* $7|C, 7|Y, E = 1$ *or* $7|C, 7|X, E = -1$ *or* $7|X, C \equiv \pm(2+3E)Y(\bmod 7)$ *or* $7|Y, C \equiv \pm(2-3E)X(\bmod 7)$, *where* $E = (-1)^f$.

COROLLARY 5.5. ([**7**, Theorem 4]). *Let p be a prime satisfying* (5.1) *with* $E = -1, X = -3C$. *Then any odd divisor q of* $7p + C^2$ *is octic* $(\bmod p)$.

PROOF. It suffices to consider the case when q is an odd prime $\neq p$. If $q|Y$, then q divides $7X^2 + C^2 = 64C^2$, so q divides $-3C = X$. Thus $q \nmid Y$. Since $4C^2 \equiv -7D^2(\bmod q)$, there exists an integer t such that $t^2 \equiv -7 \ (\bmod q)$. Thus there exists an integer s such that $s^2 \equiv p(\bmod q)$ and $C \equiv -st(\bmod q)$. Define $r = s(t-3)$, so $r^2 \equiv 2p - 2sX(\bmod q)$. Then

$$2E(s-C)(2s+r) \equiv -2(s+st)(st-s) \equiv (4s)^2 \not\equiv 0(\bmod q),$$

so q is octic $(\bmod p)$ by Theorem 5.1.

REFERENCES

1. R.J. Evans, *Period polynomials for generalized cyclotomic periods*, Manuscripta Math. **40** (1982), 217-243.

2. ———, *The octic period polynomial*, Proc. Amer. Math. Soc. **87** (1983), 389-393.

3. R.H. Hudson and K.S. Williams, *Extensions of theorems of Cunningham-Aigner and Hasse-Evans*, Pacific J. Math. **104** (1983), 111-132.

4. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, N.Y., 1982.

5. G. Janusz, *Algebraic Number Fields*, Academic Press, N.Y., 1973.

6. D.H. Lehmer and E. Lehmer, *Cyclotomic resultants*, Math. Comp. **48** (1987), 211-216.

7. E. Lehmer, *Period equations applied to difference sets*, Proc. Amer. Math. Soc. **6** (1955), 433-442.

8. ———, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20-29.

9. ———, *Problem* 85:01, Western Number Theory Conference, Asilomar, 1985.

10. ———, *On special primes*, Pacific J. Math. **118** (1985), 471-478.

11. H. von Lienen, *Primzahlen als achte Potenzreste*, J. Reine Angew. Math. **266** (1974), 107-117.

12. G. Meyerson, (Review of [**3**]), Math. Reviews **84e**, #10005.

13. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warsaw, 1974.

14. K.S. Williams, K. Hardy, and C. Friesen, *On the evaluation of the Legendre symbol* $\left(\frac{A+B\sqrt{m}}{p}\right)$, Acta Arith. **45** (1985), 255-272.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SAN DIEGO, LA JOLLA, CA 92093