Can. J. Math., Vol. XXXVII, No. 5, 1985, pp. 1008-1024

EULER'S CRITERION FOR QUINTIC NONRESIDUES

S. A. KATRE AND A. R. RAJWADE

1. Introduction. Let e be an integer $\geqq 2$, and p a prime $\equiv 1 \pmod{e}$. Euler's criterion states that for $D \in \mathbf{Z}$,

$$(1.1)\quad D^{(p-1)/e} \equiv 1 \pmod{p}$$

if and only if D is an e-th power residue (mod p). If D is not an e-th power (mod p), one has

$$(1.2)\quad D^{(p-1)/e} \equiv \alpha \pmod{p}$$

for some e-th root $\alpha(\neq 1)$ of unity (mod p). Sometimes expressions for roots of unity (mod p) can be given in terms of quadratic partitions of p. For example,

$$(1.3)\quad 1,\ -1,\ a/b,\ -a/b$$

are the four distinct fourth roots of unity (mod p) for a prime $p \equiv 1 \pmod{4}$ in terms of a solution (a, b) of the diophantine system

$$p = a^2 + b^2,\ a \equiv 1 \pmod{3}$$

(a, b^2 unique), whereas for $p \equiv 1 \pmod{3}$, a solution (L, M) of the system

$$4p = L^2 + 27M^2,\ L \equiv 1 \pmod{3}\quad (L,\ M^2 \text{ unique}),$$

gives

$$(1.4)\quad 1,\ (L + 9M)/(L - 9M),\ (L - 9M)/(L + 9M)$$

as the three distinct cuberoots of unity (mod p).

A problem concerning Euler's criterion is to determine for a given e-th power nonresidue D an e-th root of unity α (mod p) in terms of the solutions of the corresponding diophantine system so that (1.2) holds. (One may also consider the problem of obtaining congruence conditions on the solutions of the corresponding diophantine system so that (1.1) holds, i.e., D is an e-th power residue (mod p).) When $D = 2$, for $e = 2$, the result is well known, for $e = 4$, it is due to Gauss, for $e = 8$, due to Western and Lehmer, and for $e = 16$ and 32 it is due to Hudson and Williams (see **[2]** and its references). (Hudson and Williams extend the results of Cunningham-Aigner and Hasse-Evans.) When $e = 3$, the

Received August 29, 1984.

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

problem was solved by Lehmer for $D = 2$ [**4**] and by Williams for any $D \in \mathbf{Z}$ (explicit results when D a prime $\leqq 19$) [**10**].

When $e = 5$, ($p \equiv 1 \pmod 5$)), one has the diophantine system of Dickson (see (2.1)) which has four solutions. In terms of these solutions, Lehmer [**4**] has derived (cubic) expressions for fifth roots of unity (mod p) (see (3.1) and (3.2)) using Gauss-type congruences for binomial coefficients and the Jacobsthal sums of order 5. She gives Euler's criterion for $D = 2$ and $D = 4$ in terms of (3.1) and (3.2) respectively, by fixing a solution of (2.1). The expression (3.1) was subsequently used by Williams [**12**] to treat any $D \in \mathbf{Z}$ ($D = 3, 5$ explicitly). In Section 3, we show that the expressions (3.1) and (3.2) are not always well defined (mod p) so that in general the criteria of Lehmer and Williams are incomplete. (We show, however, that the result of Lehmer for $D = 2$ is always correct. For other values of D we produce counter examples.) In Section 4, we derive new correct expressions (simpler than those of Lehmer and Williams, being only quadratic in the numerator and the denominator) for fifth roots of unity (mod p) (see Theorem 1 and its corollary) using properties of a Jacobi sum of order 5 (see 2.2)). In Section 5, we give an outline of the method to fix a unique solution of the system so that we can get for $D \in \mathbf{Z}$, the value of $D^{(p-1)/5} \pmod p$ in terms of our expression. Our method simplifies that of Williams in Section 4 of [**12**]. In Section 6, we give explicit correct results for $D = 2, 3, 5$ and 7, and also for powers of these primes (see Theorems 2-5, Remark, Proposition and Example).

2. Preliminaries. In what follows, let p be a prime $\equiv 1 \pmod 5$. Let $\mathbf{Z}$ be the ring of rational integers, $\mathbf{Q}$ the field of rational numbers, $\zeta = \exp(2\pi i/5)$. The ring $\mathbf{Z}[\zeta]$ of integers of the cyclotomic field $\mathbf{Q}(\zeta)$ is a principal ideal domain. The units of $\mathbf{Z}[\zeta]$ are

$$\pm\zeta^i(\zeta + \zeta^4)^j,\ i, j \in \mathbf{Z},\ 0 \leqq i \leqq 4.$$

$1 - \zeta$ is a prime in $\mathbf{Z}[\zeta]$ and $(5) = (1 - \zeta)^4$ as ideals.

Dickson ([**1**], Section 13) showed that for $p \equiv 1 \pmod 5$ the diophantine system

$$(2.1)\quad \begin{aligned} 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw &= v^2 - 4uv - u^2,\ x \equiv 1 \pmod 5), \end{aligned}$$

has exactly four solutions. If (x, u, v, w) is one of these, then the other three are given by

$$(x, -u, -v, w), (x, v, -u, -w), (x, -v, u, -w).$$

As in ([**12**], Section 3), for any solution (x, u, v, w) of (2.1) we define $\psi = \psi(x, u, v, w) \in \mathbf{Z}[\zeta]$ by

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

$$\psi = c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4, \tag{2.2}$$

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

$$\begin{aligned} 4c_1 &= -x + 2u + 4v + 5w, \\ 4c_2 &= -x + 4u - 2v - 5w, \\ 4c_3 &= -x - 4u + 2v - 5w, \\ 4c_4 &= -x - 2u - 4v + 5w. \end{aligned} \tag{2.3}$$

(That $c_i \in \mathbf{Z}$ follows e.g. from Section 3 of [**12**]. It may also be noted that ψ is nothing but a conjugate of the Jacobi sum

$$J = \sum_{\nu} \zeta^{\operatorname{ind}(\nu(\nu+1))}$$

where $\nu \in \mathbf{F}_p$, $\nu \neq 0, -1$, and ind denotes the index with respect to some fixed primitive root (mod p).) Let $\sigma_i (1 \leqq i \leqq 4)$ be the automorphisms of $\mathbf{Q}(\zeta)$ defined by

$$\sigma_i(\zeta) = \zeta^i.$$

Let

$$\psi_i = \sigma_i(\psi), \quad 1 \leqq i \leqq 4.$$

The following properties of ψ were proved by Williams in [**12**, Section 3].

LEMMA 1. $\psi\bar{\psi} = p$, $\psi \equiv -1 \pmod{(1 - \zeta)^2}$.

LEMMA 2. G.C.D.(ψ_1, ψ_2) *is a prime of* $\mathbf{Z}[\zeta]$. *There is an algebraic integer* $\mathcal{K} \equiv \mathcal{K}(x, u, v, w) \in \mathbf{Z}[\zeta]$, (*not unique*), *such that* $(\mathcal{K}) =$ G.C.D.(ψ_1, ψ_2) *as ideas*, $\mathcal{K} \equiv -1 \pmod{(1 - \zeta)^2}$. (*Any two such* $\mathcal{K}$ *differ by a factor* $(-1)^r(\zeta + \zeta^4)^{2r}$, $r \in \mathbf{Z}$.) *For such a* $\mathcal{K}$, $\psi = -\mathcal{K}_1\mathcal{K}_3$.

3. An analysis of the results of Lehmer and Williams. E. Lehmer [**4**] obtained the expressions

$$\frac{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x + 20u - 10v)}{w(125w^2 - x^2) + 2(xw + 5uv)(25w - x - 20u + 10v)} \tag{3.1}$$

and

$$\frac{w(125w^2 - x^2) - 2(xw + 5uv)(25w + x + 10u + 20v)}{w(125w^2 - x^2) - 2(xw + 5uv)(25w + x - 10u - 20v)} \tag{3.2}$$

for fifth roots of unity (mod p) where (x, u, v, w) is a solution of the Dickson's system (2.1). Lehmer has shown how to obtain a solution of (2.1) so that for this solution (3.1) gives the expression for $2^{(p-1)/5}$ (mod p), and (3.2) for $4^{(p-1)/5}$ (mod p). K. S. Williams has again used (3.1) to give the results for $D^{(p-1)/5}$ ($D = 2, 3, 5$ in detail) in terms of a

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

fixed solution of (2.1). But it may well happen that the denominators in (3.1) and (3.2) can become zero (mod p). (See the derivation of (4.3) from (4.2) in [**4**] and the proof of Lemma 5 in [**12**].) We shall presently see that for certain values of p the denominators of (3.1) and (3.2) are zero (mod p) and then these expressions would not be well defined (mod p).

However we note here that it follows from the work of these authors that

i) if the denominators of (3.1) and (3.2) are nonzero (mod p) then these expressions are well-defined (mod p) and that their results for $D^{(p-1)/5}$ (D a quintic non residue) in terms of (3.1) and (3.2) are correct for the right choice of a solution of (2.1).

ii) The numerator of (3.1) $\equiv 0 \pmod p$ if and only if the denominators of (3.1) $\equiv 0 \pmod p$. Similarly for (3.2).

LEMMA 3 a) *The expression* (3.1) *is not well defined* (mod p) *if and only if* $v = 2u$ (*as rational integers*) (*or equivalently* $v \equiv 2u \pmod p$).

b) *The expression* (3.2) *is not well defined* (mod p) *if and only if* $u + 2v = 0$ (*as rational integers*) (*or equivalently* $u + 2v \equiv 0 \pmod p$).

Proof. a) The expression (3.1) is not well defined (mod p) if and only if the denominator is 0 (mod p). But this implies that the numerator is 0 (mod p) by (ii). Hence by subtraction

$$(xw + 5uv)(v - 2u) \equiv 0 \pmod p.$$

Now for any solution of (2.1),

$$xw + 5uv \not\equiv 0 \pmod p.$$

For otherwise by (2.1)

$$v^2 + uv - u^2 \equiv 0 \pmod p.$$

But by $(2.1)_1$,

$$|v^2 + uv - u^2| < p,$$

so

$$v^2 + uv - u^2 = 0.$$

This gives $u = 0$ and $v = 0$, so $xw = 0$. This contradicts (2.1). Hence

$$v \equiv 2u \pmod p.$$

But this gives $v = 2u$, since $|v - 2u| < p$ by (2.1). Conversely if $v = 2u$, then

$$xw + 5uv = 5u^2$$

and using (2.1) one easily sees that denominator of (3.1) is 0 (mod p).

b) The proof is similar.

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

We note that if there is a solution of (2.1) satisfying $v = 2u$ or $u + 2v = 0$, then out of the four solutions of (2.1), two satisfy $v = 2u$ and the remaining two satisfy $u + 2v = 0$. Thus for two solutions (3.1) is not well defined and for the remaining two (3.2) is not.

Remarks 1. If 2 is a quintic nonresidue of p, x in (2.1) is odd [**3**] and the fixation of the unique solution of (2.1) given by Lehmer (see (46) in [**4**]) demands that

$$u \equiv 0 \pmod 2, \ v \equiv (-1)^{u/2}x \pmod 4,$$

thus v is also odd and $v = 2u$ cannot be true. Hence for this fixed solution, the result of Lehmer, viz.

$$2^{(p-1)/5} \equiv (3.1) \pmod p$$

is always correct.

2. For $p = 211$, the conditions

$$u \equiv 0 \pmod 2, \ v \equiv (-1)^{u/2}x \pmod 4)$$

of Lehmer demand that $x = 1$, $u = 2$, $v = -1$, $w = 5$. Thus $u + 2v = 0$, so the expression (3.2) is not well defined. Thus Lehmer's result

$$4^{(p-1)/5} \equiv (3.2) \pmod p \quad [\mathbf{4}]$$

is not correct for $p = 211$. One similarly shows that the result is false for $p = 1871, 3001, 4621, 9931, 25951, 72931$ etc.

3. For $p = 211$, to obtain $3^{(p-1)/5}$, the conditions of Williams (see [**12**], (6.1)) demand that $x = 1$, $u = -1$, $v = -2$, $w = -5$, thus $v = 2u$. Hence (3.1) is not well defined, giving a counter example to Theorem 2 [**12**] of Williams. Other counter examples are $p = 3001, 4621, 9931, 25951, 72931$ etc.

4. For $p = 211$, to obtain $5^{(p-1)/5}$, the condition

$$2u + v \equiv 4 \pmod 5)$$

in Theorem 3 [**12**] demands $x = 1$, $u = 1$, $v = 2$, $w = -5$, so $v = 2u$, so (3.1) is not well defined, giving a counter example to Theorem 3 [**12**]. Other counter examples are $p = 1871, 3001, 72931$ etc.

5. For other values of D also Williams wishes to use (3.1) for $D^{(p-1)/5}$ (see Section 4, [**12**]). The above observations indicate that this would not be correct in general.

4. A correct expression for the fifth roots of unity (mod p).

THEOREM 1. *Let* $p \equiv 1 \pmod 5$. *For any solution* (x, u, v, w) *of Dickson's diophantine system* (2.1), *let*

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

$$A = x^2 - 125w^2 \quad \textit{and} \quad B = 2xu - xv - 25vw.$$

Then $A - 10B$ *and* $A + 10B$ *are nonzero* (mod p) *and*

(4.1) $\alpha = \alpha(x, u, v, w) = (A - 10B)/(A + 10B)$

(*which can be considered as an integer* (mod p)) *is a primitive fifth root of unity* (mod p) *and for this* α,

(4.2) $\alpha \equiv \zeta \pmod{\mathcal{K}}$

where $\mathcal{K}$ *is defined in Lemma* 2. *Conversely, if an integer* α (mod p) *satisfies* (4.2) *then*

$$\alpha \equiv (A - 10B)/(A + 10B) \pmod{p}.$$

Remark. We give two proofs of the theorem. The first proof is constructive, whereas the second proof is useful only if one already knows an expression for a fifth root of unity (mod p). We have given here both the proofs because we feel that for the higher cases, namely for the considerations of the seventh or the higher roots of unity (of prime order) (mod p), even after obtaining, by the method of the first proof of Theorem 1, expressions for the roots of unity in terms of the corresponding diophantine systems (viz. for 7 or 11 the systems of Leonard and Williams [**6**] [**7**] and for any odd prime ℓ the system of Parnami, Agrawal and Rajwade [**9**]), because of the complicated nature of these expressions, it will be quite difficult to show that these expressions are well defined (mod p), and then the authors expect that the method of second proof will be very useful to accomplish this. In our case we could prove that the expression $(A - 10B)/(A + 10B)$ is well-defined independently of the method of the second proof because of the extreme simplicity of this expression.

First proof of the theorem. Let α be an integer (mod p). We have

$$\alpha \equiv \zeta \pmod{\mathcal{K}} \text{ if and only if } \alpha - \zeta \equiv 0 \pmod{\mathcal{K}_1}$$

(where $\mathcal{K}_i = \sigma_i(\mathcal{K})$, $1 \leqq i \leqq 4$), i.e., if and only if

$$\alpha - \zeta^3 \equiv 0 \pmod{\mathcal{K}_3}$$

i.e., if and only if

$$(\alpha - \zeta)(\alpha - \zeta^3) \equiv 0 \pmod{\mathcal{K}_1\mathcal{K}_3}.$$

(Here the ‘only if’ part is clear. Conversely let

$$\mathcal{K}_1\mathcal{K}_3 | (\alpha - \zeta)(\alpha - \zeta^3).$$

Then either

$$\mathcal{K}_1 | (\alpha - \zeta) \text{ or } \mathcal{K}_1 | (\alpha - \zeta^3),$$

since $\mathcal{K}_1$ is a prime of $\mathbf{Z}[\zeta]$. If $\mathcal{K}_1 | (\alpha - \zeta)$ then

$$\mathcal{K}_3 | (\alpha - \zeta^3).$$

But if not, then $\mathcal{K}_1 | (\alpha - \zeta^3)$, giving

$$\mathcal{K}_3 | (\alpha - \zeta^4).$$

Again since

$$\mathcal{K}_1\mathcal{K}_3 | (\alpha - \zeta)(\alpha - \zeta^3)$$

hence $\mathcal{K}_3 | (\zeta - \zeta^4)$ or $\mathcal{K}_3 | (\zeta^3 - \zeta^4)$. But this leads to a contradiction, since the norm of $\mathcal{K}_3$ in $\mathbf{Q}(\zeta)$ is p, whereas that of $\zeta - \zeta^4$ or $\zeta^3 - \zeta^4$ is 5 and $p \nmid 5$.) i.e., if and only if

$$\psi | (\alpha^2 - (\zeta + \zeta^3)\alpha + \zeta^4) \text{ in } \mathbf{Z}[\zeta],$$

(recall that $\psi = -\mathcal{K}_1\mathcal{K}_3$), i.e., if and only if

$$p | (\alpha^2 - (\zeta + \zeta^3)\alpha + \zeta^4)\bar{\psi},$$

i.e.,

$$p | (\alpha^2 - (\zeta + \zeta^3)\alpha + \zeta^4)(c_4\zeta + c_3\zeta^2 + c_2\zeta^3 + c_1\zeta^4),$$

i.e.,

$$p | (E_1\zeta + E_2\zeta^2 + E_3\zeta^3 + E_4\zeta^4),$$

where

$$(4.3) \quad \begin{aligned} E_1 &= \alpha^2 c_4 + \alpha(c_1 - c_2 + c_3) + (c_3 - c_4), \\ E_2 &= \alpha^2 c_3 + \alpha(c_3 - c_4) + (c_2 - c_4), \\ E_3 &= \alpha^2 c_2 + \alpha c_1 + (c_1 - c_4), \\ E_4 &= \alpha^2 c_1 + \alpha(c_1 - c_2 + c_3 - c_4) - c_4, \end{aligned}$$

i.e., if and only if

$$(4.4) \quad E_1 \equiv 0,\ E_2 \equiv 0,\ E_3 \equiv 0,\ E_4 \equiv 0 \pmod{p}.$$

At this stage we note that (4.4) always has a solution $\alpha \pmod{p}$. To see this we have for a quintic nonresidue $D \pmod{p}$

$$\zeta^5 - D^5 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Hence

$$(\zeta - 1)(\zeta - D)\ldots(\zeta - D^4) \equiv 0 \pmod{\mathcal{K}},$$

(as $\mathcal{K} | p$). Since $\mathcal{K}$ is prime in $\mathbf{Z}[\zeta]$ and $\mathcal{K} \nmid (\zeta - 1)$ we get

$$\mathcal{K} | (\zeta - D^i) \quad \text{for some } 1 \leqq i \leqq 4$$

(in fact unique), and then we may take $\alpha = D^i$.

Thus the system (4.4), considered as a system of linear equations $\pmod{p}$ in α and α^2, is consistent. Hence at most two of the four

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

equations in (4.4) are linearly independent (mod p). We presently show that $E_1 \equiv 0$ and $E_2 \equiv 0 \pmod p$ are certainly so. Since, for a solution $\alpha \pmod p$ of these equations, we get,

$$\alpha[c_4^2 + c_3(c_1 - c_2 + c_3 - c_4)]$$
$$\equiv -c_3^2 + c_4(c_2 + c_3 - c_4) \pmod p.$$

Now multiplying both the sides by 16, substituting for $4c_1$, $4c_2$ etc. from (2.3), and again multiplying both the sides by $5/2$ we get

$$(4.5) \quad \alpha(A + 10B) \equiv (A - 10B) \pmod p,$$

where

$$A = x^2 - 125w^2, \quad B = 2xu - xv - 25vw.$$

If $A + 10B \equiv 0 \pmod p$, then so is $A - 10B$, hence $2A \equiv 0 \pmod p$ and so $A \equiv 0 \pmod p$. But

$$A = x^2 - 125w^2 \equiv -50(u^2 + v^2 + 5w^2) \not\equiv 0 \pmod p,$$

since by (2.1),

$$0 < u^2 + v^2 + 5w^2 < p.$$

Thus

$$A + 10B \not\equiv 0 \pmod p, \text{ and } E_1 \equiv 0 \text{ and } E_2 \equiv 0 \pmod p$$

are linearly independent. It is also clear that their unique solution α is given by

$$\alpha \equiv (A - 10B)/(A + 10B) \pmod p.$$

This discussion proves that $\alpha \equiv \zeta \pmod{\mathscr{K}}$ if and only if

$$\alpha \equiv (A - 10B)/(A + 10B) \pmod p.$$

This proves the theorem. (The authors are thankful to Dr. J. C. Parnami for enlightening discussions simplifying the original version of this proof of the theorem.)

Remark. It can be shown that in fact any two of the equations in (4.4) are linearly independent (mod p) and solving them one can get an expression for a fifth root of unity (mod p) which is congruent to our expression (4.1) (mod p).

Second proof of the theorem. From the calculations of Williams in the proof of Lemma 5 of [**12**], we have, for any solution (x, u, v, w) of (2.1), with ψ and $\mathscr{K}$ defined as in our Lemma 2,

$$x = \psi_3 + \psi_4, \quad 25u \equiv \delta\psi_3 + \beta\psi_4,$$
$$25v \equiv \beta\psi_3 - \delta\psi_4, \quad 25w \equiv -\gamma\psi_3 + \gamma\psi_4,$$

where

$$\delta = -2\zeta + \zeta^2 - \zeta^3 + 2\zeta^4,$$
$$\beta = \zeta + 2\zeta^2 - 2\zeta^3 - \zeta^4,$$
$$\gamma = \zeta - \zeta^2 - \zeta^3 + \zeta^4.$$

(Here the congruences are modulo $\mathscr{K}$. It may also be noted that

$$\psi_1 \equiv \psi_2 \equiv 0 \pmod{\mathscr{K}}$$

but $\mathscr{K} \nmid \psi_3$ or ψ_4). It is easy to check that

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

After some calculation we find that

$$A \equiv 4\psi_3\psi_4 \pmod{\mathscr{K}},$$

and

$$10B \equiv -4(\zeta - \zeta^2 + \zeta^3 - \zeta^4)\psi_3\psi_4 \pmod{\mathscr{K}}.$$

Therefore

$$(4.6) \quad A + 10B \equiv -8\psi_3\psi_4(\zeta + \zeta^3) \pmod{\mathscr{K}},$$

and

$$(4.7) \quad A - 10B \equiv -8\psi_3\psi_4(\zeta^2 + \zeta^4) \pmod{\mathscr{K}}.$$

Hence

$$A + 10B \not\equiv 0, A - 10B \not\equiv 0 \pmod{p},$$

and

$$(A - IOB)/(A + 10B) \equiv \zeta \pmod{\mathscr{K}}$$

(in the sense that any integer (mod p) which is congruent to $(A - IOB)/(A + 10B)$ (mod p) is congruent to ζ (mod $\mathscr{K}$)). Again, since $\mathscr{K}$ is a prime divisor of p in $\mathbf{Z}[\zeta]$, at most one integer (mod p) can be congruent to ζ (mod $\mathscr{K}$). This proves the theorem.

COROLLARY. *Let, for any solution,* (x, u, v, w), *of the Dickson's diophantine system* (2.1),

$$A = x^2 - 125w^2,$$

$$B = 2xu - xv - 25vw, B' = xu + 2xv - 25uw.$$

Then

$$Z_1 = (A - 10B)/(A + 10B), Z_2 = (A + 10B')/(A - 10B'),$$
$$Z_3 = (A - 10B')/(A + 10B'), Z_4 = (A + 10B)/(A - 10B),$$

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

are well-defined (mod p) *and are the four distinct primitive fifth roots of unity* (mod p). *Also,*

$$Z_1 \equiv Z_2^i \pmod{p} \quad \textit{for } i = 1, 2, 3, 4.$$

(Z_2, Z_3, Z_4 *may also be obtained from* $\mathbf{Z}_1$ *by the transformations*

$$(x, u, v, w) \rightarrow (x, -v, u, -w), (x, v - u, -w), (x, -u, -v, w)$$

respectively).

Proof.

$$\psi_2 = (\psi)_{\zeta \rightarrow \zeta^2} = (\psi)_{(x,u,v,w) \rightarrow (x,v,-u,-w)}.$$

Hence

$$\left(\frac{A - 10B}{A + 10B}\right)_{(x,u,v,w) \rightarrow (x,v\ ,-u,-w)} \equiv \zeta \pmod{\mathscr{K}_2}.$$

i.e.,

$$(A - 10B')/(A + 10B') \equiv \zeta \pmod{\mathscr{K}_2}.$$

i.e.,

$$(A - 10B')/(A + 10B') \equiv \zeta^3 \pmod{\mathscr{K}}.$$

i.e.,

$$Z_3 \equiv \zeta^3 \pmod{\mathscr{K}}.$$

Similarly,

$$Z_2 \equiv \zeta^2 \pmod{\mathscr{K}} \quad \text{and} \quad Z_4 \equiv \zeta^4 \pmod{\mathscr{K}}.$$

This proves the corollary.

Example. For $p = 61$, take $x = 1$, $u = 1$, $v = 4$, $w = -1$ as a solution of (2.1). Then $A \equiv -2 \pmod{61}$, $10B \equiv 4 \pmod{61}$, and so

$$Z_1 = (A - 10B)/(A + 10B) \equiv (-2 - 4)/(-2 + 4) = -3.$$

Therefore (or similarly),

$$Z_1 \equiv -3,\ Z_2 \equiv 9,\ Z_3 \equiv -27,\ Z_4 \equiv 20 \pmod{61},$$

are the four primitive fifth roots of unity (mod 61).

Remark. When well-defined, the expression (3.1) used by Lehmer and Williams is congruent (mod p) to our expression $(A - 10B)/(A + 10B)$.

5. Outline of the method.

LEMMA 4. *Let for any solution* (x, u, v, w) *of* (2.1), ψ, $\mathscr{K}$ *and* α *be defined by* (2.2), *Lemma* 2, *and* (4.1) *respectively. Let* D *be a rational integer prime*

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

to 5. *Then*

i) *D is a fifth power* (mod p) *if and only if* $(\psi/D)_5 = 1$.

ii) $D^{(p-1)/5} \equiv \alpha \pmod{p}$ *if and only if* $(\psi/D)_5 = \zeta^4$.

To prove Lemma 4, we use

Eisenstein's Reciprocity Law. Let $\beta \in \mathbf{Z}[\zeta]$, $(\beta, 5) = 1$, *such that* β *is congruent to a rational integer* $(\mathrm{mod}(1 - \zeta)^2)$. *Let* $D \in \mathbf{Z}$, $5 \nmid D$, *such that* $(\beta, D) = 1$. *Then*

$$(\beta/D)_5 = (D/\beta)_5.$$

Proof of Lemma 4. We give a proof of (ii). To prove (i), note that D is a fifth power (mod p) if and only if

$$D^{(p-1)/5} \equiv 1 \pmod{p},$$

and reason analogously.

To prove (ii), we have

$$D^{(p-1)/5} \equiv \alpha \pmod{p}$$

if and only if

$$D^{(p-1)/5} \equiv \alpha \pmod{\mathscr{K}},$$

by Theorem 1, i.e., $(D/\mathscr{K})_5 = \zeta$, i.e., if and only if

$$(\mathscr{K}/D)_5 = \zeta$$

(in view of Eisenstein's reciprocity law),

i.e., if and only if

$$(-\mathscr{K}\mathscr{K}_3/D)_5 = \zeta \cdot \zeta^3 = \zeta^4$$

(a small check), i.e.,

$$(\psi/D)_5 = \zeta^4.$$

LEMMA 5. *For any solution* (x, u, v, w) *of* (2.1) *and for* α *as in* (4.1),

(i) ([**8**], [**5**]) 5 *is a fifth power* (mod p) *if and only if* $u \equiv 2v \pmod{5}$.

(ii) $5^{(p-1)/5} \equiv \alpha \pmod{p}$ *if and only if* $2u + v \equiv 4 \pmod{5}$.

Proof. Choose a primitive root g (mod p) by

$$(g/\mathscr{K})_5 = \zeta.$$

Then as has been done by Williams in the proof of Theorem 3 in [**12**] we have

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

Thus (i) 5 is a fifth power (mod p) if and only if

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

$$-2u - v \equiv 0 \pmod{5},$$

i.e., $u \equiv 2v \pmod{5}$.

(ii) $5^{(p-1)/5} \equiv \alpha \pmod{p}$ if and only if

$$5^{(p-1)/5} \equiv \alpha \pmod{\mathscr{K}},$$

i.e.,

$$5^{(p-1)/5} \equiv \zeta \pmod{\mathscr{K}},$$

by Theorem 1, i.e.,

$$5^{(p-1)/5} \equiv g^{(p-1)/5} \pmod{\mathscr{K}},$$

by the choice of g, i.e.,

$$\text{ind}_g^5 \equiv 1 \pmod{5}$$

i.e.,

$$-2u - v \equiv 1 \pmod{5},$$

i.e.,

$$2u + v \equiv 4 \pmod{5}.$$

Remark. Lemma 4(i) gives a condition that D (coprime to 5) is a quintic residue (mod p). The case $D = 5$ is treated in Lemma 5(i). For another condition (when D is a prime), which goes back to Kummer, see Theorem 1 of [**11**].

Let $(D, 10) = 1$. Since $(\psi/D)_5$ depends only on the congruences of ψ (mod D), which are in turn determined by the congruences of x, u, v, w (mod D) (since D is odd), to obtain a congruence condition that D is a fifth power (mod p) for a prime $p \equiv 1 \pmod{5}$, or, when D is a quintic nonresidue (mod p) to obtain the solution of (2.1) for which

$$D^{(p-1)/5} \equiv \alpha \pmod{p},$$

one considers the congruences of the solutions x, u, v, w of (2.1) (mod D). For some congruences (mod D), $(\psi/D)_5$ will be 1 so that D is a fifth power (mod p). For the other congruences

$$(\psi/D)_5 = \zeta^i, \quad 1 \leqq i \leqq 4,$$

and D is not a fifth power (mod p). In this case one replaces the solution (x, u, v, w) if necessary by one of the four solutions of (2.1) so that

$$(\psi/D)_5 = \zeta^4.$$

(To do this, if $i = 1$, let $(x, u, v, w) \rightarrow (x, -u, -v, w)$, if $i = 2$, let $(x, u, v, w) \rightarrow (x, v, -u, -w)$, and if $i = 3$ let $(x, u, v, w) \rightarrow (x, -v, u, -w)$). For this choice of the solution, $D^{(p-1)/5}$ will be $\equiv \alpha \pmod{p}$, where α is

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

given by (4.1). If D is a power of 2 or 5, we give the corresponding result in the next section. (If D is a power of 2 one has to consider congruences of x, u, v, w (mod 4).)

Combining these results one gets $D^{(p-1)/5} \pmod{p}$ for any $D \in \mathbf{Z}$. One might as well first find the result for prime values of D and from that obtain the result when D is a prime power or any composite number. It is clear that if

$$D^{(p-1)/5} \equiv \alpha \pmod{p},$$

then

$$D^{j(p-1)/5} \equiv Z_1, Z_2, Z_3, Z_4 \pmod{p}$$

according as $j \equiv 1, 2, 3, 4 \pmod{5}$, so if the expression is known for prime values of D, a similar one is also known for prime powers.

In the next section we explicitly deal with the cases $D = 2, 3, 5, 7$. In these cases we of course get the same congruence conditions on x, u, v, w as the previous ones in the literature by other methods, for D to be a quintic residue $\pmod{p}$ [**3**] [**5**] [**11**]. For $D = 2, 3, 5$, in case these are quintic nonresidues $\pmod{p}$, we get the same conditions as those of [**4**] and [**12**] for the choice of the solution for which

$$D^{(p-1)/5} \equiv \alpha \pmod{p}$$

with the difference that we now have a simpler and correct α at our disposal. Also in our method we could dispense with the congruences of $\mathscr{K}$ which were required by Williams for $D = 2$ and 3 or for general D [**12**]. We shall explain the so far untreated case $D = 7$ in some more detail and only state the results for $D = 2, 3, 5$. We also note that for the cases $D = 2, 3, 7$ which we are treating here we have the added advantage that D is a prime $\equiv 2, 3 \pmod{5}$, so that it stays prime in $\mathbf{Z}[\zeta]$, so

$$(\psi/D)_5 = 1, \zeta^i$$

if and only if

$$\psi^{(D^4-1)/5} \equiv 1, \zeta^i \pmod{D} \quad (1 \leqq i \leqq 4).$$

If, however, D is a prime $\equiv 1, 4 \pmod{5}$, $(D \neq p)$, one has to use prime factors of D in $\mathbf{Z}[\zeta]$.

6. The cases $D = 2, 3, 5, 7$. In this section for any solution (x, u, v, w) of (2.1),

$$\alpha = \alpha(x, u, v, w) = (A - 10B)/(A + 10B), \ (p \equiv 1 \pmod{5}).$$

THEOREM 2. (i) 2 *is a fifth power* $\pmod{p}$ *if and only if* $w \equiv 0 \pmod{4}$ (*or equivalently* $u \equiv v \equiv 0 \pmod{2}$ *or equivalently* $x \equiv u \equiv v \equiv w \equiv 0 \pmod{2}$ *or equivalently* $w \equiv 0 \pmod{2}$ *etc.*).

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

(ii) *If* 2 *is a quintic nonresidue,* $2^{(p-1)/5} \equiv \alpha \pmod{p}$ *for the unique solution of* (2.1) *given by*

$$u \equiv 0 \pmod{2}, \quad v \equiv (-1)^{u/2} x \pmod{4}.$$

THEOREM 3. (i) 3 *is a fifth power* (mod p),

$$3^{(p-1)/5} \equiv \alpha \pmod{p}$$

if and only if $u \equiv v \equiv 0 \pmod{3}$ (*or equivalently* $xw \equiv 0 \pmod{3}$).

(ii) *If* 3 *is a quintic nonresidue* (mod p),

$$3^{(p-1)/5} \equiv \alpha \pmod{p}$$

for the unique solution of (2.1) *given by either*

$$u \equiv -w, \ v \equiv 0 \pmod{3},$$

or

$$u \equiv -w, \ v \equiv w \pmod{3}.$$

THEOREM 4. (i) 5 *is a fifth power* (mod p) *if and only if*

$$u \equiv 2v \pmod{5}.$$

(ii) *If* 5 *is a quintic nonresidue* (mod p),

$$5^{(p-1)/5} \equiv \alpha \pmod{p}$$

for the unique solution given by

$$2u + v \equiv 4 \pmod{5}.$$

Theorem 4 is immediate from Lemma 5. The proofs of Theorem 2 and Theorem 3 are similar to the proof of the following:

THEOREM 5. (i) 7 *is a fifth power* (mod p) *if and only if either*

(a) $u \equiv v \equiv 0 \pmod{7}$ (*i.e., equivalently* $xw \equiv 0 \pmod{7}$), *or there is a solution of* (2.1) *satisfying*

(b) $u \equiv w$, $v \equiv 2w \pmod{7}$, *or*

(c) $u \equiv 0$, $v \equiv 2w \pmod{7}$

(*here for* (b) *and* (c), $w \not\equiv 0 \pmod{7}$).

(ii) *If* 7 *is a quintic nonresidue* (mod p) *then*

$$7^{(p-1)/5} \equiv \alpha \pmod{p}$$

for the unique solution satisfying exactly one of

$$(u/w, v/w) \equiv (1, 0), (1, 3), (2, 2), (2, 3), (3, 3), (0, 3),$$
$$(-1, -1), (-1, 2), (2, -3), (-3, -1) \pmod{7}.$$

(Note that in (i), $(p/7) = 1$ in the case (a) if $x \not\equiv 0$, and in the case (b). Otherwise $(p/7) = -1$. Also in (ii), $w \not\equiv 0 \pmod{7}$ and $(p/7) = 1$ in the first five cases whereas $(p/7) = -1$ in the remaining five cases.)

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

Proof. As mentioned in Section 5,

$$(\psi/7)_5 \equiv \zeta^i \pmod 7 \quad (0 \leqq i \leqq 4)$$

if and only if

$$\psi^{(7^4-1)/5} \equiv \zeta^i \pmod 7$$

i.e.,

$$\psi^{480} \equiv \zeta^i \pmod 7.$$

Note that

$$\psi^7 \equiv \psi_2, \psi^{49} \equiv \psi_2^7 \equiv \psi_4 = \bar{\psi},$$
$$\psi^{343} \equiv \psi_4^7 \equiv \psi_3 = \bar{\psi}_2 \pmod 7.$$

Hence

$$\begin{aligned}\psi^{480} &= \psi^{343}(\psi^{49})^2(\psi^7)^5\psi^4 \\ &\equiv \bar{\psi}_2\bar{\psi}^2\psi_2^5\psi^4 \pmod 7 \\ &= p^3\psi^2\psi_2^4.\end{aligned}$$

Thus $\psi^{480} \equiv \zeta^i \pmod 7$ if and only if

$$\begin{aligned}C = p^3[\,(c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4)(c_3\zeta + c_1\zeta^2 \\ + c_4\zeta^3 + c_2\zeta^4)^2]^2 \equiv \zeta^i \pmod 7.\end{aligned}$$

(It is clear from (2.1) that $p^3 \equiv (x^2 + u^2 + v^2 - w^2)^3 \pmod 7$.) We note that if $w \equiv 0 \pmod 7$ then so are u and v, but $x \not\equiv 0 \pmod 7$ and in this case $C \equiv 1 \pmod 7$, so that 7 is a fifth power (mod p). Next if $w \not\equiv 0 \pmod 7$, then the congruence for $(u/w, v/w) \pmod 7$ determines the congruence for $x/w \pmod 7$ in view of (2.1). This in turn gives the congruence for p^3, c_1, c_2, c_3, c_4 in terms of w. Since $w^6 \equiv 1 \pmod 7$, the congruence of C (and also of p^3) (mod 7) will depend only upon $(u/w, v/w)$ (mod 7). Thus we have to consider only the 49 cases $(u/w, v/w)$ for u/w and v/w (mod 7). If $(u/w, v/w) \equiv (0, 0)$, again one sees that 7 is a fifth power. So 48 cases remain. These can be divided into classes of four each taking e.g. (i, j), $(-i, -j)$, $(j, -i)$, $(-j, i)$ (mod 7) in the same class. Thus

$$u/w \equiv 0, 1, 2, 3 \pmod 7$$

and

$$v/w \equiv 1, 2, 3 \pmod 7$$

give a set of representatives for the 12 classes. We obtain the congruence of C (mod 7) in all these cases. We find that in the cases (i) (b) and (i) (c), $C \equiv 1 \pmod 7$, so that 7 is a fifth power (mod p). In the remaining cases

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

we find that $C \equiv \zeta^i \pmod 7$ for some $1 \leqq i \leqq 4$ and so 7 is a quintic nonresidue $(\text{mod } p)$. We want to fix the solution satisfying $C \equiv \zeta^4 \pmod 7$, for this will ensure that

$$7^{(p-1)/5} \equiv \alpha \pmod p$$

by Lemma 4 (ii). To do this, suppose

$$(u/w, v/w) \equiv (h, k) \pmod 7.$$

If $i = 1$, let $(h, k) \to (-h, -k)$. If $i = 2$, let $(h, k) \to (k, -h)$. If $i = 3$, let $(h, k) \to (-k, h)$. This will demand the replacement of ψ by one of its conjugates so that for this new ψ,

$$(\psi/7)_5 = \zeta^4.$$

This process gives the 10 possibilities in (ii). (Since $p^3 \equiv \pm 1 \pmod 7$, we might as well forget it in C and just conclude the results from $C \equiv \pm\zeta^i \pmod 7$.)

(We thank Mr. Vinod Parnami for helping in some preliminary calculations in this case.)

Remark. For $D = 2, 3, 5, 7$, if D is a quintic nonresidue $(\text{mod } p)$, then one fixes a unique solution by the conditions in (ii) of Theorems 2, 3, 4, 5 and for this solution

$$D^{j(p-1)/5} \equiv Z_1, Z_2, Z_3, Z_4 \pmod p$$

according as $j \equiv 1, 2, 3, 4 \pmod 5$. (See the corollary to Theorem 1.) In particular we have

PROPOSITION. *If* 2 *is a quintic nonresidue* $(\text{mod } p)$ $(p \equiv 1 \pmod 5))$, *then for the unique solution* (x, u, v, w) *of* (2.1) *given by* $u \equiv 0 \pmod 2$,

$$v \equiv (-1)^{u/2}x \pmod 4,$$

$$4^{(p-1)/5} \equiv (A + 10B')/(A - 10B') \pmod p$$

where $A = x^2 - 125w^2$, *and* $B' = xu + 2xv - 25uw$.

This corrects and simplifies the result of E. Lehmer in the equation (48) of [**4**].

An example. Let $p = 211$. The four solutions of the Dickson's system (2.1) are $(1, 1, 2, -5)$, $(1, -2, 1, 5)$, $(1, 2, -1, 5)$, $(1, -1, -2, -5)$. If we denote the fifth roots of unity obtained from these four solutions by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, then we see from the corollary to Theorem 1 that

$$\alpha_i \equiv \alpha_1^i \pmod{211} \quad (i = 1, 2, 3, 4).$$

So evaluating one of these by the formula $(A - 10B)/(A + 10B)$ we get all of them, viz.

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press

$$\alpha_1 \equiv 55, \alpha_2 \equiv 71, \alpha_3 \equiv 107, \alpha_4 \equiv -23 \pmod{211}.$$

The unique solutions fixed by (ii) of Theorems 2, 3, 4, 5 are respectively $(1, 2, -1, 5)$, $(1, -1, -2, -5)$, $(1, 1, 2, -5)$ and $(1, -2, 1, 5)$. Hence we get

$$2^{(p-1)/5} = 2^{42} \equiv 107, 3^{42} \equiv -23, 5^{42} \equiv 55,$$
$$7^{42} \equiv 71 \pmod{211}.$$

Also

$$4^{42} = (2^{42})^2 \equiv (\alpha_3)^2 \equiv \alpha_1 \equiv 71 \pmod{211}.$$
$$(2^4 \cdot 3^8 \cdot 7^{12})^{42} \equiv (\alpha_3)^4(\alpha_4)^8(\alpha_2)^{12} \equiv (\alpha_3)^4(\alpha_4)^3(\alpha_2)^2$$
$$\equiv (\alpha_1)^{3\cdot 4+4\cdot 3+2\cdot 2} = \alpha_1^{28} \equiv \alpha_3 \equiv 107 \pmod{211}.$$

For $p = 211$, although the expression (3.1) of Lehmer and Williams does not work for $D = 2, 3, 5$, it works for $D = 7$ and we get the same result.

$$(14)^{42} = 2^{42} \cdot 7^{42} \equiv \alpha_3 \cdot \alpha_2 \equiv 1 \pmod{211},$$

so that 14 is a quintic residue (mod 211).

References

1. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. *57* (1935), 391-424.
2. R. H. Hudson and K. S. Williams, *Extensions of theorems of Cunningham-Aigner and Hasse-Evans*, Pacific J. Math. *104* (1983), 111-132.
3. E. Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. *18* (1951), 11-18.
4. ——— *On Euler's criterion*, J. Austral. Math. Soc. (1959/61), Part I, 64-70.
5. ——— *On the divisors of the discriminant of the period equation*, Amer. J. Math. *90* (1968), 375-379.
6. P. A. Leonard and K. S. Williams, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc. *51* (1975), 295-300.
7. ——— *The cyclotomic numbers of order eleven*, Acta Arith. *26* (1975), 365-383.
8. J. B. Muskat, *On the solvability of $x^e \equiv e \pmod{p}$*, Pacific J. Math. *14* (1964), 257-260.
9. J. C. Parnami, M. K. Agrawal and A. R. Rajwade, *Jacobi sums and cyclotomic numbers*, Acta Arith. *41* (1982), 1-13.
10. K. S. Williams, *On Euler's criterion for cubic nonresidues*, Proc. Amer. Math. Soc. *49* (1975), 277-283.
11. ——— *Explicit criteria for quintic residuacity*, Math. Comp. *30* (1976), 847-853.
12. ——— *On Euler's criterion for quintic nonresidues*, Pacific J. Math. *51* (1975), 543-550.

Panjab University,
Chandigarh, India

https://doi.org/10.4153/CJM-1985-054-2 Published online by Cambridge University Press