PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 2, June 1975

ON EULER'S CRITERION FOR CUBIC NONRESIDUES[1]

KENNETH S. WILLIAMS

ABSTRACT. If p is a prime $\equiv 1 \pmod 3$ there are integers L and M such that $4p = L^2 + 27M^2$, $L \equiv 1 \pmod 3$. Indeed L and M^2 are unique. If D is a cubic nonresidue (mod p) it is shown how to choose the sign of M so that

$$D^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \pmod p.$$

The case $D = 2$ has been treated by Emma Lehmer.

1. **Introduction.** If p is a prime $\equiv 1 \pmod 3$ there are integers L and M such that

$$4p = L^2 + 27M^2, \qquad L \equiv 1 \pmod 3. \tag{1.1}$$

Indeed L and M^2 are unique. Moreover, $L, M \not\equiv 0 \pmod p$ so that 1, $(L + 9M)/(L - 9M)$ and $(L - 9M)/(L + 9M)$ are the three distinct cube roots of unity (mod p). Thus, if D is an integer not divisible by p, by Euler's criterion we have

$$D^{(p-1)/3} \equiv \begin{cases} 1, & \text{if } D \text{ is a cubic residue (mod } p), \\ (L \pm 9M)/(L \mp 9M), & \text{if } D \text{ is a cubic nonresidue (mod } p). \end{cases}$$

It is the purpose of this paper to show how the sign of M in (1.1) should be chosen so that if D is a cubic nonresidue (mod p) then

$$D^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \pmod p. \tag{1.2}$$

Clearly there is no loss of generality in restricting D to be a prime ≥ 2, and we consider two cases according as $D = 2, 3$ or $D \geq 5$.

The case $D = 2, 3$ is treated in §2 using the theory of cyclotomy. In this case it is well known that D is a cubic residue (mod p) if and only if

Received by the editors December 28, 1973 and, in revised form, April 2, 1974.
AMS (MOS) subject classifications (1970). Primary 10A15; Secondary 12C20.
Key words and phrases. Euler's criterion, cyclotomy, cyclotomic numbers, root of unity modulo p, cubic residues and nonresidues.
[1]This research was supported by grant no. A-7233 from the National Research Council of Canada.

$M \equiv 0 \pmod{D}$. In Lemma 1 explicit expressions are given for the cyclotomic numbers of order 3 (compare [2, p. 397]). These are used in conjunction with known results in the theory of cyclotomy (see Lemma 2) to show how M must be specified uniquely so that (1.2) holds (Theorem 1). In Theorem 1, (a) is due to Emma Lehmer [5], and (b) is new. Her approach is different to ours.

The case $D \geq 5$ is treated in §3. In this case it is well known that if D is a cubic nonresidue (mod p) then $LM \not\equiv 0 \pmod{D}$, and use of this fact is made from time to time in the proofs. A congruence modulo D (see (3.1)) for the cubic Gauss sum proved by Ankeny [1], and a criterion for cubic residuacity given by Lehmer [4], are used to show how M must be specified uniquely in terms of a certain set $\mathfrak{L}_1(D)$ (see (3.6) and Lemma 5) so that (1.2) holds (Theorem 2). The set $\mathfrak{L}_1(D)$ is easy to calculate for any particular value of D and the values of $\mathfrak{L}_1(D)$ are given for $D = 5, 7, 11, 13, 17, 19$.

2. $D = 2, 3$. Let $w = \exp(2\pi i/3) = \frac{1}{2}(-1 + \sqrt{-3})$, so that $1 + w + w^2 = 0$. If p is a prime $\equiv 1 \pmod{3}$ we set, for any L, M satisfying (1.1),

$$\pi = \tfrac{1}{2}(L + 3M) + 3Mw, \tag{2.1}$$

so that π is a prime factor of p in the Eisenstein domain $Z[w]$. We define a cubic residue character $\chi_\pi \pmod{\pi}$ by setting for any $\alpha \in Z[w]$,

$$\chi_\pi(\alpha) = \begin{cases} w^r, & \text{if } \alpha \not\equiv 0 \pmod{\pi} \text{ and } \alpha^{(p-1)/3} \equiv w^r \pmod{\pi},\ 0 \leq r \leq 2, \\ 0, & \text{if } \alpha \equiv 0 \pmod{\pi}. \end{cases} \tag{2.2}$$

If g is a primitive root (mod p), so that $\chi_\pi(g) = w$ or w^2, for any integers h and k $(0 \leq h, k \leq 2)$ the cyclotomic number $(h, k)_3$ of order 3 is defined to be the number of solutions (r, s) of $g^{3r+h} + 1 \equiv g^{3s+k} \pmod{p}$ with $0 \leq r, s < (p-1)/3$. Our first lemma, which is well known, gives expressions for these cyclotomic numbers in terms of g, L, M and π.

Lemma 1.

$$9(0, 0)_3 = p - 8 + L,$$

$$18(0, 1)_3 = 18(1, 0)_3 = 18(2, 2)_3 = \begin{cases} 2p - 4 - L + 9M, & \text{if } \chi_\pi(g) = w, \\ 2p - 4 - L - 9M, & \text{if } \chi_\pi(g) = w^2, \end{cases}$$

$$18(0, 2)_3 = 18(2, 0)_3 = 18(1, 1)_3 = \begin{cases} 2p - 4 - L - 9M, & \text{if } \chi_\pi(g) = w, \\ 2p - 4 - L + 9M, & \text{if } \chi_\pi(g) = w^2, \end{cases}$$

$$9(1, 2)_3 = 9(2, 1)_3 = p + 1 + L.$$

For any integer $a \not\equiv 0 \pmod{p}$ *we define the index of* a *with respect to* g, *written* $\operatorname{ind}_g(a)$, *to be the unique integer* b *such that* $a \equiv g^b \pmod{p}$, $0 \le b \le p-2$.

The next lemma consists of well-known results from the theory of cyclotomy (see for example [7, Lemma 4, p. 26], and [6, Theorem 1 ($e = 3$), p. 257]).

Lemma 2. (a) *Let* $h = 0, 1, 2$. *Then* $\operatorname{ind}_g(2) \equiv h \pmod{3}$ *if and only if* $(0, h)_g \equiv 1 \pmod{2}$.

(b) $\operatorname{ind}_3(3) \equiv (0, 2)_3 - (0, 1)_3 \pmod{3}$.

As D is a cubic residue (mod p) if and only if $\operatorname{ind}_g(D) \equiv 0 \pmod{3}$, we obtain immediately from Lemmas 1, 2 and (1.1) that, for $D = 2, 3$, D is a cubic residue (mod p) if and only if $M \equiv 0 \pmod{D}$. Thus if D (= 2 or 3) is not a cubic residue (mod p) we can distinguish between the two solutions $(L, \pm M)$ of (1.1) as follows: (a) if 2 is not a cubic residue (mod p) then (1.1) has a unique solution (L, M) satisfying $L \equiv M \pmod{4}$, and (b) if 3 is not a cubic residue (mod p) then (1.1) has a unique solution (L, M) satisfying $M \equiv -1 \pmod{3}$.

We can now prove Theorem 1.

Theorem 1. (a) *If* 2 *is not a cubic residue* (mod p) *and* (L, M) *is the unique solution of* (1.1) *satisfying* $L \equiv M \pmod{4}$ *then*

$$2^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \pmod{p}.$$

(b) *If* 3 *is not a cubic residue* (mod p) *and* (L, M) *is the unique solution of* (1.1) *satisfying* $M \equiv -1 \pmod{3}$ *then*

$$3^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \pmod{p}.$$

Proof. (a) Let (L, M) be the unique solution of (1.1) satisfying $L \equiv M \pmod{4}$ and define π by (2.1). Let g be a primitive root (mod p), such that $\chi_\pi(g) = w$. Thus for this primitive root g we have, by Lemma 1, $18(0, 1)_3 = 2p - 4 - L + 9M$, so that, as $L \equiv M \pmod{4}$, we have $(0, 1)_3 \equiv 1 \pmod{2}$. Thus by Lemma 2(a) we have $\operatorname{ind}_g(2) \equiv 1 \pmod{3}$, which gives

$$2^{(p-1)/3} \equiv w \pmod{\pi}. \tag{2.3}$$

It follows from (2.1) that

$$(L + 9M)/(L - 9M) \equiv w \pmod{\pi}. \tag{2.4}$$

Putting (2.3) and (2.4) together we obtain

$$2^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \pmod{\pi},$$

and the required result follows as both sides are real.

(b) Let (L, M) be the unique solution of (1.1) satisfying $M \equiv -1 \pmod 3$ and define π by (2.1). Again we choose g to be a primitive root (mod p) such that $\chi_\pi(g) = w$, and for this primitive root we have by Lemma 1, $(0, 2)_3 - (0, 1)_3 = -M$, so that, as $M = -1 \pmod 3$, we have by Lemma 2(b), $\operatorname{ind}_g(3) \equiv (0, 2)_3 - (0, 1)_3 \equiv 1 \pmod 3$, which gives $3^{(p-1)/3} \equiv w \pmod{\pi}$. The rest of the proof is now the same as in (a).

Example 1. Let $p = 37$ so that $4p = 148 = 11^2 + 27.1^2$. The unique solution given by Lemma 3(a) is $L = -11$, $M = 1$, and the one given by Lemma 3(b) is $L = -11$, $M = -1$. Thus by Theorem 1 we have

$$2^{12} \equiv \frac{(-11) + 9(1)}{(-11) - 9(1)} = \frac{1}{10} \equiv 26 \pmod{37}$$

and

$$3^{12} \equiv \frac{(-11) + 9(-1)}{(-11) - 9(-1)} = 10 \pmod{37}.$$

3. $D \geq 5$. Let D be a prime ≥ 5. The Gauss sum $G(\chi_\pi)$ is defined by

$$G(\chi_\pi) = \sum_{n=1}^{p-1} \chi_\pi(n) \exp(2\pi i n/p),$$

and Ankeny [1] has shown that, if $D \neq p$, $G(\chi_\pi)$ satisfies the congruence

$$G(\chi_\pi)^{D^f - 1} \equiv \chi_\pi(D)^{-f} \pmod{D}, \tag{3.1}$$

where f is the least positive integer such that $D^f \equiv 1 \pmod 3$. Using (3.1) and the well-known result $G(\chi_\pi)^3 = p\pi$ (see for example [3, p. 116]) we obtain modulo D

$$\chi_\pi(D) \equiv \begin{cases} p^{2(D-1)/3}\pi^{2(D-1)/3}, & \text{if } D \equiv 1 \pmod 3, \\ p^{(D-2)/3}\pi^{(D+1)/3}, & \text{if } D \equiv 2 \pmod 3. \end{cases} \tag{3.2}$$

We next define for any integer k

$$F_D(k) = \begin{cases} (k^2 + 27)^{2(D-1)/3}(k + 3 + 6w)^{2(D-1)/3}, & \text{if } D \equiv 1 \pmod 3, \\ (k^2 + 27)^{(D-2)/3}(k + 3 + 6w)^{(D+1)/3}, & \text{if } D \equiv 2 \pmod 3. \end{cases} \tag{3.3}$$

Now Emma Lehmer [4] has shown that for *any* prime $p \equiv 1 \pmod 3$ with $LM \not\equiv$

0 (mod D), there is a set $\mathfrak{L}(D)$ *depending only on* D, such that D is a cubic nonresidue (mod p) if and only if $L^2 \equiv k^2M^2 \pmod{D}$ for some $k \in \mathfrak{L}(D)$. Clearly $\mathfrak{L}(D)$ may be taken as a subset of $\{\pm 1, \pm 2, \cdots, \pm \frac{1}{2}(D-1)\}$ and to have the property that if $k \in \mathfrak{L}(D)$ then $-k \in \mathfrak{L}(D)$. Further we may assume that for each $k \in \mathfrak{L}(D)$ there is some prime $p \equiv 1 \pmod{3}$ with $LM \not\equiv 0 \pmod{D}$ for which $L^2 \equiv k^2M^2 \pmod{D}$. We also remark that $\pm h \notin \mathfrak{L}(D)$, where $h^2 + 27 \equiv 0 \pmod{D}$ when $D \equiv 1 \pmod{3}$.

We prove

Lemma 3. *If* $k \in \mathfrak{L}(D)$ *then*

$$F_D(k) \equiv w \pmod{D}, \qquad F_D(-k) \equiv w^2 \pmod{D},$$

or

$$F_D(k) \equiv w^2 \pmod{D}, \qquad F_D(-k) \equiv w \pmod{D}.$$

Proof. As $(k + 3 + 6w)(-k + 3 + 6w) = -(k^2 + 27)$ we have

$$F_D(k)F_D(-k) = \begin{cases} (k^2 + 27)^{2(D-1)}, & \text{if } D \equiv 1 \pmod{3}, \\ (-1)^{(D+1)/3}(k^2 + 27)^{D-1}, & \text{if } D \equiv 2 \pmod{3}. \end{cases}$$

Since D is prime, we have $(D + 1)/3 \equiv 0 \pmod{2}$ when $D \equiv 2 \pmod{3}$. Also as $k^2 + 27 \not\equiv 0 \pmod{D}$ for $k \in \mathfrak{L}(D)$, we have $(k^2 + 27)^{D-1} \equiv 1 \pmod{D}$. Hence we have

$$F_D(k)F_D(-k) \equiv 1 \pmod{D}. \tag{3.4}$$

Further since $k \in \mathfrak{L}(D)$ there exists a prime p for which D is a cubic nonresidue (mod p) and such that $LM \not\equiv 0 \pmod{D}$ and $L \equiv kM \pmod{D}$. Hence we have

$$4p \equiv (k^2 + 27)M^2, \qquad 2\pi \equiv (k + 3 + 6w)M \pmod{D},$$

and so

$$F_D(k) \equiv \begin{cases} (4p/M^2)^{2(D-1)/3}(2\pi/M)^{2(D-1)/3}, & \text{if } D \equiv 1 \pmod{3}, \\ (4p/M^2)^{(D-2)/3}(2\pi/M)^{(D+1)/3}, & \text{if } D \equiv 2 \pmod{3}, \end{cases}$$

$$\equiv \begin{cases} p^{2(D-1)/3}\pi^{2(D-1)/3}, & \text{if } D \equiv 1 \pmod{3}, \\ p^{(D-2)/3}\pi^{(D+1)/3}, & \text{if } D \equiv 2 \pmod{3}, \end{cases}$$

that is

$$F_D(k) \equiv \chi_\pi(D) \pmod{D}. \tag{3.5}$$

The result now follows as $\chi_\pi(D) = w$ or w^2 since D is a cubic nonresidue (mod p).

Lemma 3 enables us to define for $i = 1, 2$

$$\mathfrak{L}_i(D) = \{k \in \mathfrak{L}(D) \colon F_D(k) \equiv w^i \pmod{D}\}, \tag{3.6}$$

so that

$$\mathfrak{L}_1(D) \cup \mathfrak{L}_2(D) = \mathfrak{L}(D), \qquad \mathfrak{L}_1(D) \cap \mathfrak{L}_2(D) = \varnothing.$$

Lemma 4. *Let D be a prime ≥ 5. If p is a prime $\equiv 1$ (mod 3), for which D is a cubic nonresidue* (mod p), *then we can define M uniquely by requiring it to satisfy $L \equiv kM$* (mod D) *for some $k \in \mathfrak{L}_1(D)$.*

Proof. As D is a cubic nonresidue (mod p) by Lehmer's criterion, $L^2 \equiv k^2M^2$ (mod D) for some $k \in \mathfrak{L}(D)$ and some solution (L, M) of (1.1). By replacing k by $-k$ if necessary we may assume that $k \in \mathfrak{L}_1(D)$. Now $L \equiv \pm kM$ (mod D) with $k \in \mathfrak{L}_1(D)$, and as L cannot satisfy both these congruences we may choose M uniquely so that $L \equiv kM$ (mod D).

We can now prove Theorem 2.

Theorem 2. *Let D be a prime ≥ 5. If p is a prime $\equiv 1$* (mod 3) *for which D is a cubic nonresidue* (mod p) *and M is defined uniquely by $L \equiv kM$* (mod D) *for some $k \in \mathfrak{L}_1(D)$ then* (1.2) *holds.*

Proof. It follows from (2.1) that (2.4) holds. Further as $L \equiv kM$ (mod D) with $k \in \mathfrak{L}_1(D)$, we have $F_D(k) \equiv w$ (mod D) and so $\chi_\pi(D) \equiv w$ (mod D), that is, $\chi_\pi(D) = w$. Hence we have

$$D^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \pmod{\pi},$$

and the result follows as both sides are real.

Example 2. From Lehmer's criterion for cubic residuacity [4] we deduce that

$$\mathfrak{L}(5) = \{\pm 1, \pm 2\}, \qquad \mathfrak{L}(7) = \{\pm 2, \pm 3\},$$
$$\mathfrak{L}(11) = \{\pm 1, \pm 2, \pm 3, \pm 5\}, \qquad \mathfrak{L}(13) = \{\pm 2, \pm 3, \pm 4, \pm 6\},$$
$$\mathfrak{L}(17) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 6, \pm 7\},$$
$$\mathfrak{L}(19) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 6, \pm 8\}.$$

Using (3.3) and (3.6) we obtain

$\mathfrak{L}_1(5) = \{+1, -2\}$, $\mathfrak{L}_1(7) = \{+2, -3\}$,
$\mathfrak{L}_1(11) = \{-1, -2, -3, +5\}$, $\mathfrak{L}_1(13) = \{-2, +3, +4, -6\}$,
$\mathfrak{L}_1(17) = \{-1, +2, +4, -5, +6, -7\}$,
$\mathfrak{L}_1(19) = \{+1, +2, -4, -5, -6, -8\}$.

Thus Theorem 2 gives as a particular case: let D denote one of 5, 7, 11, 13, 17, 19. If p is a prime $\equiv 1 \pmod 3$ for which D is a cubic nonresidue (mod p) and M is defined uniquely by $L \equiv kM \pmod D$ where

$$k = \begin{cases} 1 \text{ or } -2, & \text{if } D = 5, \\ 2 \text{ or } -3, & \text{if } D = 7, \\ -1, -2, -3 \text{ or } 5, & \text{if } D = 11, \\ -2, 3, 4 \text{ or } -6, & \text{if } D = 13, \\ -1, 2, 4, -5, 6 \text{ or } -7, & \text{if } D = 17, \\ 1, 2, -4, -5, -6 \text{ or } -8, & \text{if } D = 19, \end{cases}$$

then (1.2) holds.

Thus if $p = 61$ and $D = 19$ the required unique solution is $L = 1$, $M = 3$, so that

$$19^{20} \equiv \frac{1 + 9 \cdot 3}{1 - 9 \cdot 3} \equiv \frac{-14}{13} \equiv 13 \pmod{61}.$$

It is interesting to note that the sum of the elements in each of the sets $\mathfrak{L}_1(D)$ $(D = 5, 7, \cdots, 19)$ is congruent to $-1 \pmod D$!

4. **Acknowledgement.** The author would like to acknowledge his indebtedness to the referee whose extremely valuable suggestions enabled the author to greatly extend and improve the original version of this paper.

REFERENCES

1. N. C. Ankeny, *Criterion for rth power residuacity*, Pacific J. Math. 10 (1960), 1115–1124. MR 22 #9479.

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

3. K. Ireland and M. Rosen, *Elements of number theory: Including an introduction to equations over finite fields*, Bogden and Quigley, Belmont, Calif., 1972.

4. Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), 20–29. MR 20 #1668.

5. ———, *On Euler's criterion*, J. Austral. Math. Soc. 1 (1959/61), part 1, 64–70. MR 21 #7191.

6. J. B. Muskat, *On the solvability of* $x^e \equiv e \pmod p$, Pacific J. Math. 14 (1964), 257–260. MR 28 #2997.

7. T. Storer, *Cyclotomy and difference sets*, Lectures in Advanced Math., no. 2, Markham, Chicago, Ill., 1967. MR 36 #128.

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA