ON EULER'S CRITERION

EMMA LEHMER

(rec. 2 April 1959)

Euler's criterion states that if p is a prime then

$$D^f \equiv 1 \pmod{p},\ p = kf + 1, \tag{1}$$

if and only if D is a k-th power residue of p.

However if (1) does not hold then

$$D^f \equiv \alpha_k \pmod{p},\ \alpha_k \not\equiv 1 \pmod{p}, \tag{2}$$

where α_k is some k-th root of unity modulo p.

For $k = 2$ it is obvious that $\alpha_k = -1$ and we have the usual congruence for the Legendre symbol, namely

$$D^{(p-1)/2} \equiv \left(\frac{D}{p}\right) \pmod{p}. \tag{3}$$

For $k > 2$ there seems to have been no attempt in the literature to specify which α_k corresponds to a given D. This is probably due to the fact that in general one would not expect to be able to distinguish between primitive k-th roots of unity. The possibility of this determination for $k = 3$ and $D = 2$ was suggested by empirical results of N.Y. Wilson which can be reduced to our criterion (24). Explicit results will be given for $D = 2$ also with $k = 3$, 4, 5, and 8 as well as some general congruence relations involving the so called Jacobsthal sums

$$\phi_k(D) = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right)\left(\frac{\nu^k + D}{p}\right). \tag{4}$$

We consider the sum (4) as a congruence modulo p. Using (3) we obtain

$$\phi_k(D) \equiv \sum_{\nu=1}^{p-1} \nu^{(p-1)/2}(\nu^k + D)^{(p-1)/2} \equiv \sum_{\mu=0}^{(p-1)/2} \binom{(p-1)/2}{\mu} D^\mu S_k(\mu) \tag{5}$$

where

$$S_k(\mu) = \sum_{\nu=1}^{p-1} \nu^{\frac{1}{2}(k+1)(p-1)-k\mu} \equiv \begin{cases} \sum_{\nu=1}^{p-1} \nu^{-k\mu} & \text{if } k \text{ is odd} \\ \sum_{\nu=1}^{p-1} \nu^{(p-1)/2-k\mu} & \text{if } k \text{ is even.} \end{cases}$$

Hence if k is odd

$$S_k(\mu) \equiv \begin{cases} -1 \pmod{p} & \text{if } \mu = mf \\ 0 \pmod{p} & \text{otherwise,} \end{cases}$$

while if k is even

$$S_k(\mu) \equiv \begin{cases} -1 \pmod{p} & \text{if } \mu = (2m+1)f/2 \\ 0 \pmod{p} & \text{otherwise.} \end{cases}$$

Combining these results we have

$$(7) \quad \phi_k(D) \equiv \begin{cases} -\sum_{m=0}^{(k-1)/2} D^{mf} \binom{(p-1)/2}{mf} \pmod{p} \text{ for } k \text{ odd} \\ -\sum_{m=0}^{(k-2)/2} D^{(2m+1)f/2} \binom{(p-1)/2}{(2m+1)f/2} \pmod{p}, \ k \text{ and } f \text{ even} \\ 0 \pmod{p} \text{ for } k \text{ even, } f \text{ odd.} \end{cases}$$

This congruence can be found in a slightly different form in Whiteman [1].

For $k = 2$, $f/2 = (p-1)/4$, $p = 4n+1 = a^2+b^2$, $a \equiv 1 \pmod 4$ congruence (7) becomes

$$(8) \qquad \phi_2(D) \equiv -D^{(p-1)/4} \binom{(p-1)/2}{(p-1)/4} \pmod{p}.$$

Putting $D = 1$ we get the well known result of Gauss

$$(9) \qquad \binom{(p-1)/2}{(p-1)/4} \equiv -\phi_2(1) = 2a \pmod{p}.$$

Therefore

$$(10) \qquad D^{(p-1)/4} \equiv \phi_2(D)/\phi_2(1) \pmod{p}.$$

Jacobsthal [2] proved in his dissertation that if $D \equiv m^2 \pmod{p}$

$$(11) \qquad \phi_2(D) = \phi_2(m^2) = \left(\frac{m}{p}\right)\phi_2(1) = -\left(\frac{m}{p}\right)2a.$$

Substituting this into (10) gives (3). In case D is not a quadratic residue Jacobsthal was only able to prove that

$$(12) \qquad \phi_2(D) = \pm 2b \text{ if } \left(\frac{D}{p}\right) = -1,$$

which is insufficient for our purposes. In another paper [3] we were able to improve on this result if 2 is not a quartic residue of $p = 4n+1$ as follows:

$$(13)\quad \phi_2(D) = -2b\left(\frac{m}{p}\right) \text{ where } \begin{cases} D \equiv 2m^2 \pmod{p},\ \left(\frac{2}{p}\right) = -1, \\ \qquad\qquad\qquad\qquad b/2 \equiv 1 \pmod 4 \\ D \equiv \sqrt{2m^2} \pmod{p},\ \left(\frac{2}{p}\right) = 1, \\ \qquad\qquad\qquad\qquad b/4 \equiv (-1)^n \pmod 4. \end{cases}$$

Substituting these values into (10) we obtain *in case* 2 *is not a quartic residue*

$$(14)\qquad D^{(p-1)/4} \equiv \left(\frac{m}{p}\right) b/a \pmod{p}$$

in case either $D \equiv 2m^2$ and $\left(\frac{2}{p}\right) = -1$ with $b/2 \equiv 1 \pmod 4$

or $D = \sqrt{2m^2}$ and $\left(\frac{2}{p}\right) = +1$ with $b/4 \equiv (-1)^n \pmod 4$.

In the case $D = 2$, the results are much more explicit. It is well known that 2 is a quartic residue of p if and only if $b \equiv 0 \pmod 8$. If 2 is a quadratic but not quartic residue then $b \equiv 4 \pmod 8$, in the remaining cases b is oddly even and we can take as above $b/2 \equiv 1 \pmod 4$ and state our criterion as follows:

If $p = 4n+1 = a^2 + b^2$, $a \equiv 1 \pmod 4$, *then*

$$(15)\qquad 2^{(p-1)/4} \equiv \begin{cases} (-1)^{b/4} \pmod{p} \text{ if } b \equiv 0 \pmod 4 \\ b/a \pmod{p} \text{ otherwise } [b/2 \equiv 1 \pmod 4]. \end{cases}$$

Next let $k = 3$, $f = (p-1)/3$. In this case the sum (7) reduces to

$$(16)\qquad \phi_3(D) \equiv -1 - D^f \binom{(p-1)/2}{f} \pmod{p}.$$

Letting $D = 1$ we have

$$(17)\qquad \binom{(p-1)/2}{(p-1)/3} \equiv -1 - \phi_3(1) \pmod{p}.$$

Substituting this back into (16) we obtain

$$(18)\qquad D^{(p-1)/3} \equiv (\phi_3(D) + 1)/(\phi_3(1) + 1) \pmod{p}.$$

Since $\phi_3(D) = \phi_3(1)$ if D is a cubic residue the above congruence reduces in this case to Euler's criterion. If D is not a cubic residue however the general formula for $\phi_3(D)$ contains an ambiguity of sign. We were able to determine this sign in a previous paper [3] under the condition that 2 is not a cubic residue. Let

$$p = A^2 + 3B^2 \text{ and } 4p = L^2 + 27M^2,\ A \equiv L \equiv 1 \pmod 3)$$

then

$$2^{(p-1)/3} \equiv 1/4^{(p-1)/3} \equiv -2A/L \pmod{p}, \tag{19}$$

since [4]

$$\phi_3(D) = \phi_3(1) = -(2A+1) \text{ if } D = m^3, \tag{20}$$

while

$$\phi_3(D) = \begin{cases} 2A - L - 1 \text{ if } D \equiv 2m^3 \pmod{p} \\ \qquad L - 1 \text{ if } D \equiv 4m^3 \pmod{p}. \end{cases} \tag{21}$$

It might be worth recalling that 2 is a cubic residue of p if and only if $L \equiv 0 \pmod 2$; but this implies $B \equiv 0 \pmod 3$ and $L = -2A$, $B = \pm 3M$; hence (19) reduces to (1). If 2 is not a cubic residue then $B \not\equiv 0 \pmod 3$ and we may choose $B \equiv 1 \pmod 3$. Then it can be easily verified that the two forms are related by $L = A + 3B$, $A - B = \pm 3M$. Hence we can eliminate L in (21), thus obtaining our result in terms of a single form as follows:

If $p = A^2 + 3B^2$, $A \equiv B \equiv 1 \pmod 3$ and 2 is not a cubic residue, then,

$$\varphi_3(D) = \begin{cases} A - 3B - 1 \text{ if } D = 2m^3 \pmod{p} \\ A + 3B - 1 \text{ if } D = 4m^3 \pmod{p}. \end{cases} \tag{22}$$

Substituting this and (20) into (18) we obtain

$$D^{(p-1)/3} \equiv \begin{cases} 1 & \text{if } D \equiv m^3 \pmod{p} \\ (-A+3B)/2A & \text{if } D \equiv 2m^3 \pmod{p} \\ -(A+3B)/2A & \text{if } D \equiv 4m^3 \pmod{p}. \end{cases} \tag{23}$$

It might be worth noting that $(-A \pm 3B)/2A \equiv (\mp A - B)/2B \pmod{p}$. This can be verified by cross multiplication using $A^2 \equiv -3B^2 \pmod{p}$. For $D = 2$ we get the following explicit result:

$$2^{(p-1)/3} \equiv \begin{cases} 1 \pmod{p} & \text{if } B \equiv 0 \pmod 3 \\ (3B - A)/2A \equiv -(A+B)/2B & [B \equiv 1 \pmod 3] \end{cases} \tag{24}$$

By (20) and (17) we get the well known result.

$$\binom{(p-1)/2}{(p-1)/3} \equiv 2A \pmod{p}, \quad A \equiv 1 \pmod 3. \tag{25}$$

For $k = 5$, $f = (p-1)/5$, congruence (7) gives

$$-[1 + \phi_5(D)] = D^f\binom{(p-1)/2}{f} + D^{2f}\binom{(p-1)/2}{2f} \pmod{p}. \tag{26}$$

We write this congruence for $D = 4d^\nu$, $\nu = 0, 1, 2, 3, 4$, where d is any

https://doi.org/10.1017/S1446788700025076 Published online by Cambridge University Press

quintic non-residue of p and let

$$c_\nu = -[1 + \phi_5(4d^\nu)], \quad (\nu = 0,\ 1,\ 2,\ 3,\ 4), \tag{27}$$

$$\gamma_1 = 4^f \binom{(p-1)/2}{f} \equiv \binom{2f}{f} \pmod{p}, \tag{28}$$

and

$$\gamma_2 = 4^{2f} \binom{(p-1)/2}{2f} \equiv \binom{4f}{2f} \equiv \binom{3f}{f} \pmod{p}. \tag{29}$$

Then (26) can be replaced by the system of congruences

$$c_\nu \equiv \gamma_1 d^{\nu f} + \gamma_2 d^{2\nu f} \pmod{p} \qquad (\nu = 0,\ 1,\ 2,\ 3,\ 4). \tag{30}$$

This system can be solved for γ_1 and γ_2 as follows. We note that

$$c_1 - c_2 - c_3 + c_4 \equiv (d^f - d^{2f} - d^{3f} + d^{4f})(\gamma_1 - \gamma_2) \pmod{p}, \tag{31}$$

$$c_1 c_4 + c_2 c_3 \equiv 2(\gamma_1^2 + \gamma_2^2) - \gamma_2\gamma_2 \equiv 2c_0^2 - 5\gamma_1\gamma_2 \pmod{p}, \tag{32}$$

since $\gamma_1 + \gamma_2 \equiv c_0 \pmod{p}$,

$$\begin{aligned} c_1c_4 - c_2c_3 &\equiv (d^f - d^{2f} - d^{3f} + d^{4f})\gamma_1\gamma_2 \\ &\equiv (d^f - d^{2f} - d^{3f} + d^{4f})(2c_0^2 - c_1c_4 - c_2c_3)/5 \pmod{p}, \end{aligned} \tag{33}$$

by (32). Hence by (31) and (33)

$$\gamma_1 - \gamma_2 \equiv (c_1 - c_2 - c_3 + c_4)(2c_0^2 - c_1c_4 - c_2c_3)/5(c_1c_4 - c_2c_3) \pmod{p}. \tag{34}$$

Therefore,

$$\gamma_1 \equiv \binom{2f}{f} \equiv \tfrac{1}{2}[c_0 + (c_1 - c_2 - c_3 + c_4)(2c_0^2 - c_1c_4 - c_2c_3)/5(c_1c_4 - c_2c_3)] \pmod{p} \tag{35}$$

and

$$\gamma_2 \equiv \binom{3f}{f} \equiv \tfrac{1}{2}[c_0 - (c_1 - c_2 - c_3 + c_4)(2c_0^2 - c_1c_4 - c_2c_3)/5(c_1c_4 - c_2c_3)] \pmod{p}. \tag{36}$$

We now recall that $\phi_5(4d^\nu)$ and therefore the c_ν's can be evaluated [1] in terms of the quadratic partition

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2 \\ xw = v^2 - u^2 - 4uv, \qquad x \equiv 1 \pmod{5}, \end{cases} \tag{37}$$

as follows:

$$\begin{aligned} c_0 &= -[1 + \phi_5(4)] = -x \\ 4c_1 &= x - 25w - 10(u + 2v) \\ 4c_2 &= x + 25w - 10(2u - v) \\ 4c_3 &= x + 25w + 10(2u - v) \\ 4c_4 &= x - 25w + 10(u + 2v). \end{aligned} \tag{38}$$

https://doi.org/10.1017/S1446788700025076 Published online by Cambridge University Press

Therefore $c_1 - c_2 - c_3 + c_4 = -25w$, while

$$4(c_1c_4 + c_2c_3) = 3x^2 + 625w^2$$

and

$$c_1c_4 - c_2c_3 = 25(u^2 - v^2 - uv) \equiv -25(xw + 5uv) \pmod{p}.$$

Hence (35) and (36) become

$$\binom{2f}{f} \equiv \frac{1}{2}\left[-x + \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right] \pmod{p} \tag{39}$$

and

$$\binom{3f}{f} \equiv \frac{1}{2}\left[-x - \frac{w(x^2 - 125w^2)}{4(xw + 5uv)}\right] \pmod{p}. \tag{40}$$

We note that these results are unambiguous since the same answer is obtained by substituting either of the four solutions of (37), namely

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

Knowing γ_2 we can solve the system (30) for $d^{\nu f}$ as follows. Writing 2ν and 3ν for ν in (30) we obtain

$$\begin{aligned} d^{\nu f} c_{2\nu} &\equiv \gamma_1 d^{3\nu f} + \gamma_2 \pmod{p} \\ c_{3\nu} &\equiv \gamma_1 d^{3\nu f} + \gamma_2 d^{\nu f} \pmod{p}. \end{aligned} \tag{42}$$

Hence subtracting,

$$d^{\nu f} \equiv (c_{3\nu} + \gamma_2)/(c_{2\nu} + \gamma_2) \pmod{p}. \tag{43}$$

The last expression is not devoid of ambiguity, however, since the c's depend on the choice of the solution in (40). For $d = 2$, however, we can make a complete determination by noting that

$$c_3 = -[1 + \phi_5(4d^3)] = -[1 + \phi_5(1)] \tag{44}$$

must be even, while the other c's are odd. This follows from the fact that $\phi_5(1)$ is odd since it contains five zero terms, while all the other ϕ_5's are composed exclusively of an even number of plus and minus ones and must be even. Hence we must have

$$x + 25w + 20u - 10v \equiv 0 \pmod{8}. \tag{45}$$

It is known [4] that x and w are both even or odd according as 2 is a quintic residue of p or not. Hence x and w are both odd and u and v must be of different parity by the second equation in (37). We can let u be *even*, then by (37)

$$xw \equiv 1 - u^2 \equiv 1 + 2u \pmod{8}$$

https://doi.org/10.1017/S1446788700025076 Published online by Cambridge University Press

and this implies

$$w \equiv x + 2u \pmod 8$$

and by (45)

$$v \equiv x + u \pmod 4$$

or what is the same thing

$$(46) \qquad v \equiv (-1)^{u/2} x \pmod 4.$$

This determines a unique solution of the system (38) and we can write

$$(47) \qquad 2^{(p-1)/5} \equiv \frac{w(125w^2-x^2)+2(xw+5uv)(25w-x+20u-10v)}{w(125w^2-x^2)+2(xw+5uv)(25w-x-20u+10v)} \pmod p.$$

For example let $p = 31$, $x = 11$, $u = 2$, $v = 1$, $w = -1$. We find

$$2^{(p-1)/5} = 2^6 \equiv \frac{-1(4)+2(-1)(-6)}{-1(4)+2(-1)(-66)} \equiv \frac{8}{128} \equiv \frac{8}{4} \equiv 2 \pmod{31},$$

while

$$\binom{12}{6} \equiv \tfrac{1}{2}[-11-1] \equiv -6 \equiv 25 \text{ and } \binom{18}{6} \equiv \tfrac{1}{2}[-11+1] \equiv -5 \equiv 26 \pmod{31}.$$

Similarly by (38) and (42),

$$(48) \qquad 4^{(p-1)/5} \equiv \frac{w(125w^2-x^2)-2(xw+5uv)(25w+x+10u+20v)}{w(125w^2-x^2)-2(xw+5uv)(25w+x-10u-20v)} \pmod p.$$

For $k = 8$, $p = 8n+1 = a^2+b^2$, it is well known that if 2 is a quartic residue of p, then $b \equiv 0 \pmod 8$ and

$$(49) \qquad 2^{(p-1)/8} \equiv (-1)^{b/8+n} \pmod p.$$

Otherwise since 2 is a quadratic residue, we can use (14) with $D = \sqrt{2}$ to obtain

$$(50) \qquad 2^{(p-1)/8} \equiv b/a \pmod p, \text{ where } b/4 \equiv (-1)^n \pmod 4.$$

Expressions for $2^{(p-1)/k} \pmod p$ for $k = 6$, 10, 12, 15, 20, 24 and 40 can be easily obtained by combining the above results.

References

[1] Whiteman, A. L., "Cyclotomy and Jacobsthal Sums", *Amer. Jour. of Math.* **74** (1952), 89–99.

[2] Jacobsthal, E., "Anwendungen einer Formel aus der Theorie der quadratischen Reste", Dissertation (Berlin, 1906).

[3] Lehmer, Emma, "On the Number of Solutions of $u^k + D \equiv w \pmod p$", *Pacific Jour. of Math.* **55** (1955), 103–118.

[4] Lehmer, Emma, "The quintic character of 2 and 3", *Duke Math. Journal* **18** (1951) 11–18.

Berkeley, Calif., U.S.A.