Delta 6 (1976), 23-28.

Cubic Nonresidues (Mod p)

Kenneth S. Williams
(Carleton University—Ottawa)

1. Introduction

Let k be an integer greater than 2 and let p be a prime, $p \equiv 1 \pmod{k}$. Euler's criterion asserts that the congruence $x^k \equiv D \pmod{p}$ is solvable if and only if $D^{(p-1)/k} \equiv 1 \pmod{p}$. In this case D is called a k-th power residue (mod p). If D is a k-th power nonresidue (mod p), then $D^{(p-1)/k} \not\equiv 1 \pmod{p}$ but, since $(D^{(p-1)/k})^k = D^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem, we must have $D^{(p-1)/k} \equiv \alpha_k \pmod{p}$, where α_k is some k-th root of unity, $\alpha_k \not\equiv 1 \pmod{p}$. For $k = 2$ we clearly have $\alpha_k = -1$ and there is nothing more to be said, but when $k > 2$ there is the question of deciding which k-th root of unity α_k corresponds to a given D. We shall look at the case $k = 3$. (For results in this direction see [3], [4], [5].)

From now on let p be a prime, $p \equiv 1 \pmod{3}$. Gauss showed that there are integers L and M such that

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

Indeed L and M^2 are unique. Equation (1.1) implies that $(L + 9M)^3 \equiv (L - 9M)^3 \pmod{p}$, so that $\frac{L + 9M}{L - 9M}$ and $\frac{L - 9M}{L + 9M}$ are the two cube roots of unity, neither congruent to $1 \pmod{p}$. Thus if D is a cubic nonresidue (mod p) by Euler's criterion, we have

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

The question arises—how should the sign of M be chosen so that the first of these possibilities holds? In this article we show how this question can be answered for any particular D, using Eisenstein's law of cubic reciprocity. Without loss of generality we may restrict D to be a (positive) prime. Three cases arise according as $D \equiv 1 \pmod 3$, $D \equiv 2 \pmod 3$ or $D = 3$. We illustrate each of these cases by giving the details for $D = 2$, 3 and 7.

2. Eisenstein's Law of Cubic Reciprocity

We denote the domain of rational integers by Z and let $Z[\zeta]$ denote the integral domain $\{x + y\zeta \colon x,y \in Z\}$, where ζ is the complex cube root of unity $(-1 + \sqrt{-3})/2$. The elements of $Z[\zeta]$ are called Eisenstein integers and were used by Eisenstein in his work on cubic reciprocity. For details of the arithmetic of the Eisenstein integers we refer the reader to the delightful book [1] by Ireland and Rosen, whose notation we follow. If $\alpha \in Z[\zeta]$, we write $N(\alpha) = \alpha\bar{\alpha}$ $(\in Z)$ for its norm, where $\bar{\alpha}$ is the complex conjugate of α. There are exactly six units (elements of norm 1) in $Z[\zeta]$, namely ± 1, $\pm\zeta$, $\pm\zeta^2$. Two non-zero Eisenstein integers α, β are said to be associates, written $\alpha \sim \beta$, if their quotient $\frac{\alpha}{\beta}$ is a unit. $Z[\zeta]$ is a Euclidean domain, so each non-zero, non-unit element is expressible in an essentially unique manner as a product of primes. The primes of $Z[\zeta]$ consist of positive rational primes $q \equiv 2 \pmod 3$ and their associates, complex primes of the form $a + b\zeta$ having norm a rational prime congruent to $1 \pmod 3$, and $1 - \zeta$ and its associates. We remark that the norm of $1 - \zeta$ is 3; indeed, $3 = -\zeta^2(1 - \zeta)^2$.

If π is a prime in $Z[\zeta]$ and not an associate of the prime $1 - \zeta$ (written $\pi \not\sim 1 - \zeta$), then $N(\pi) \equiv 1 \pmod 3$ and the cubic residue character modulo π of $\alpha \in Z[\zeta]$ is defined by

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0, \text{ if } \alpha \equiv 0 \pmod{\pi}, \\ \zeta^r, \text{ if } \alpha \not\equiv 0 \pmod{\pi} \text{ and } \alpha^{(N(\pi)-1)/3} \equiv \zeta^r \pmod{\pi}, \\ \qquad\qquad r = 0, 1, 2. \end{cases}$$

This character enjoys the following properties: if $\alpha, \beta \in Z[\zeta]$, then

$$\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2 = \left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_3; \quad \left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3\left(\frac{\beta}{\pi}\right)_3;$$

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3 \text{ if } \alpha \equiv \beta \pmod{\pi}.$$

Also we have

$$\left(\frac{-1}{\pi}\right)_3 = 1, \quad \left(\frac{\zeta}{\pi}\right)_3 = \zeta^{(N(\pi)-1)/3}.$$

A prime π of $Z[\zeta]$ is called primary if it satisfies $\pi \equiv 2 \pmod 3$. If π is a prime $\not\sim 1 - \zeta$, then among its six associates exactly one is primary. Clearly $1 - \zeta$ and its associates are not primary. In 1844 Eisenstein [3] proved the following.

LAW OF CUBIC RECIPROCITY: *If* π *and* λ *are primary primes of* $Z[\zeta]$, *then*

$$\left(\frac{\lambda}{\pi}\right)_3 = \left(\frac{\pi}{\lambda}\right)_3.$$

Two proofs of this are given by Ireland and Rosen [1]. In the same year Eisenstein also proved this sequel.

SUPPLEMENT TO THE LAW OF CUBIC RECIPROCITY: *Let* π *be a primary prime of* $Z[\zeta]$. *If* $\pi = q$ *is rational, let* $q = 3m - 1$. *If* $\pi = a + b\zeta$ *is a primary complex prime, let* $a = 3m - 1$. *Then* $\left(\frac{1 - \zeta}{\pi}\right)_3 = \zeta^{2m}$.

We shall also need some results of Jacobi [2] which can easily be deduced from the above results of Eisenstein. (Part (a) below is treated in [1] (p. 120).)

THEOREM (Jacobi):

(a) 2 *is a cubic residue* (mod p) *if and only if* $M \equiv 0 \pmod 2$.

(b) 3 *is a cubic residue* (mod p) *if and only if* $M \equiv 0 \pmod 3$.

(c) 7 *is a cubic residue* (mod p) *if and only if* $L \equiv 0 \pmod 7$ *or* $M \equiv 0 \pmod 7$.

3. $D = 2$

If 2 is not a cubic residue (mod p), then by Jacobi's theorem [2] we have $L \equiv M \equiv 1 \pmod 2$. Thus we can choose the sign of M uniquely so that $L \equiv M \pmod 4$. Now set

$$\pi = \frac{1}{2}(L + 3M) + 3M\zeta, \tag{3.1}$$

so that π is a primary prime factor of p in $Z[\zeta]$. The choice of M ensures that $\pi \equiv \zeta \pmod 2$. Then by Eisenstein's law of cubic reciprocity we have, as 2 remains prime in $Z[\zeta]$,

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 = \left(\frac{\zeta}{2}\right)_3 = \zeta,$$

so that

$$2^{(p-1)/3} \equiv \zeta \equiv \frac{-\frac{1}{2}(L + 3M)}{3M} \equiv \frac{L + 9M}{L - 9M} \pmod{\pi}. \tag{3.2}$$

As both sides of (3.2) are rational, we have

THEOREM 1 (Lehmer [3]): *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*

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

4. $D = 3$

If 3 is not a cubic residue (mod p), then by Jacobi's theorem we have $M \not\equiv 0 \pmod 3$. We can choose the sign of M uniquely so that $M \equiv -1 \pmod 3$. With this choice of M we define π as in (3.1). Then by Eisenstein's supplement to the law of cubic reciprocity we have

$$\left(\frac{3}{\pi}\right)_3 = \zeta^{2M} = \zeta,$$

so that

$$(4.1) \qquad 3^{(p-1)/3} \equiv \zeta \equiv \frac{-\frac{1}{2}(L + 3M)}{3M} \equiv \frac{L + 9M}{L - 9M} \pmod{\pi}.$$

As both sides of (4.1) are rational, we have

THEOREM 2 (Williams [4]): *If* 3 *is not a cubic residue* $\pmod{p}$ *and* (L,M) *is the unique solution of* (1.1) *satisfying* $M \equiv -1 \pmod{3}$, *then*

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

5. D = 7

If 7 is not a cubic residue $\pmod{p}$, then by Jacobi's theorem we have $L \not\equiv 0 \pmod{7}$ and $M \not\equiv 0 \pmod{7}$. Define k ($k \not\equiv 0 \pmod{7}$) by $k \equiv \frac{L}{M} \pmod{7}$, so that from (1.1) we have $k^2 + 27 \equiv \frac{4p}{M^2} \not\equiv 0 \pmod{7}$. That is, $k \not\equiv \pm 1 \pmod{7}$, which gives $L \equiv \pm 2M$ or $L \equiv \pm 3M \pmod{7}$. Thus we can choose the sign of M uniquely so that $L \equiv 2M \pmod{7}$ or $L \equiv 4M \pmod{7}$. With this choice define π as in (3.1). Since 7 factors as $7 = (-1 - 3\zeta)(2 + 3\zeta)$ in $Z[\zeta]$, by the law of cubic reciprocity we have

$$\left(\frac{7}{\pi}\right)_3 = \left(\frac{-1 - 3\zeta}{\pi}\right)_3\left(\frac{2 + 3\zeta}{\pi}\right)_3 = \left(\frac{\pi}{-1 - 3\zeta}\right)_3\left(\frac{\pi}{2 + 3\zeta}\right)_3.$$

If $L \equiv 2M \pmod{7}$ (we omit similar details for $L \equiv 4M \pmod{7}$), we have

$$\begin{aligned}\left(\frac{\pi}{-1 - 3\zeta}\right)_3\left(\frac{\pi}{2 + 3\zeta}\right)_3 &= \left(\frac{6M + 3M\zeta}{-1 - 3\zeta}\right)_3\left(\frac{6M + 3M\zeta}{2 + 3\zeta}\right)_3 \\ &= \left(\frac{M}{-1 - 3\zeta}\right)_3\left(\frac{6 + 3\zeta}{-1 - 3\zeta}\right)_3\left(\frac{M}{2 + 3\zeta}\right)_3\left(\frac{6 + 3\zeta}{2 + 3\zeta}\right)_3 \\ &= \left(\frac{M}{-1 - 3\zeta}\right)_3\overline{\left(\frac{M}{-1 - 3\zeta}\right)_3}\left(\frac{5}{-1 - 3\zeta}\right)_3\left(\frac{4}{2 + 3\zeta}\right)_3 \\ &= (+1)\left(\frac{5}{-1 - 3\zeta}\right)_3\left(\frac{4}{2 + 3\zeta}\right)_3.\end{aligned}$$

Now as

$$\left(\frac{5}{-1-3\zeta}\right)_3 \equiv 5^{(7-1)/3} \equiv 5^2 \equiv 2^2 \equiv \zeta^2 \pmod{-1-3\zeta}$$

and

$$\left(\frac{4}{2+3\zeta}\right)_3 \equiv 4^{(7-1)/3} \equiv 4^2 \equiv \zeta^2 \pmod{2+3\zeta},$$

we have $\left(\frac{7}{\pi}\right)_3 \equiv \zeta^2\cdot\zeta^2 \equiv \zeta$, and the rest of the proof is as before. We have:

THEOREM 3 (Williams [4]): *If* 7 *is not a cubic residue* (mod p) *and* (L,M) *is the unique solution of* (1.1) *satisfying either* $L \equiv 2M$ *or* $L \equiv 4M \pmod 7$, *then*

$$7^{(p-1)/3} \equiv \frac{L+9M}{L-9M} \pmod p.$$

EXAMPLE: If $p = 277$, then $(-26, \pm 4)$ are the two solutions of (1.1). As $-26/4 \equiv 4 \pmod 7$, the unique solution specified in Theorem 3 is $(-26, 4)$ and we have

$$7^{92} \equiv \frac{-26+9(4)}{-26-9(4)} \equiv \frac{10}{-26} \equiv 116 \pmod{277},$$

which can be verified directly.

References

1. K. Ireland and M. Rosen, *Elements of Number Theory* (Belmont, California: Bogden and Quigley, 1972).

2. K. G. J. Jacobi, "De residuis cubicis commentatio numerosa," *Jour. für die reine und angewandte Math.*, *2* (1827), 66-69.

3. Emma Lehmer, "On Euler's criterion," *Jour. Austral. Math. Soc.*, *1* (1959), 64-70.

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

5. ________, "Euler's criterion for primes congruent to 1 (mod 5)," to appear, *Pacific Journal of Mathematics*.