On Rational Cubic Residues

Sam Vandervelde
Department of Mathematics, St. Lawrence University
23 Romoda Drive, Canton, New York 13617, United States
svandervelde@stlawu.edu

Abstract

In 1958 E. Lehmer found an explicit description of those primes p for which a given prime q is a cubic residue. Her result states that if one writes $4p = L^2 + 27M^2$, then q is a cubic residue if and only if $M/L \equiv (t^2-1)/(t^3-9t) \bmod q$ for some integer t. Recently, Z. Sun has stated a similar result for cubic nonresidues which follows from several corollaries appearing in an earlier paper of his. In this paper we provide an independent, self-contained development of an equivalent result. In particular, we describe a family $g_\gamma(t)$ of rational functions involving cubic polynomials that play an analogous role to the function $(t^2-1)/(t^3-9t)$ appearing in Lehmer's theorem.

keywords: Cubic residue, cubic reciprocity
MSC 2000: 11A15

1 Motivation

Let $p \equiv 1 \bmod 3$ be a prime. We say that an integer c is a cubic residue modulo p if there is a solution to the congruence $x^3 \equiv c \bmod p$. The study of cubic residues dates back centuries, at least to the mid 1700's when Euler conjectured that 2 is a cubic residue mod p if and only if p can be written in the form $A^2 + 27B^2$. Gauss later proved this statement as a consequence of his theory of cubic reciprocity, which he never published. It was left to Eisenstein and Jacobi to provide a documented development of this theory, from which results on cubic residues follow. These historical tidbits, along with a great many more, appear in Cox's delightful book [1].

In 1920 Cunningham and Gosset [2] compiled tables to settle this question for all integers c whose prime factors did not exceed 50. Using a formulation of cubic reciprocity due to Pépin [7] (which bears a surprisingly close resemblance to more modern notation), they demonstrated that for a given prime q, the value of a certain cubic residue symbol depended only on the ratio $\frac{M}{L} \bmod q$, where L and M are integers for which $4p = L^2 + 27M^2$. The values corresponding to the various possible ratios were obtained by factoring polynomials in L and M whose degree was proportional to q, making the process increasingly impractical as q grew larger.

This difficulty was circumvented by Lehmer [5], where she developed a different sort of criterion that predicted for which primes p a given prime q is a cubic residue. We present a slightly more tidy version of Lehmer's result here, due to Sun [9].

Theorem 1 *Let $p \equiv 1 \bmod 3$ be a prime and write $4p = L^2 + 27M^2$. Then a given prime $q \neq p$ is a cubic residue modulo p if and only if*

$$(t-1)(t+1)L \equiv t(t-3)(t+3)M \bmod q \tag{1}$$

for some integer t.

The result essentially states that the primes p for which q is a cubic residue lie on certain lines through the origin mod q (in the LM-plane) whose slopes are

$$\frac{M}{L} \equiv \frac{t^2-1}{t^3-9t} \bmod q \tag{2}$$

as t runs through all distinct values mod q. As Sun observes, the fact that the residuacity of q depends only on $\frac{M}{L}$ was known to Jacobi [4] and later proved by Lehmer [5] and Williams [11]. The two nontrivial solutions to $x^3 \equiv 1 \bmod p$ can be given in terms of L and M as $(L \pm 9M)/(L \mp 9M)$. Lehmer [6] found a method for ascertaining which of these two values is assumed by the expression $q^{(p-1)/3}$ for $q = 2$. Williams [11] proves the case $q = 3$ and indicates what occurs when $q \geq 5$. For instance, when $q = 17$ he finds that $17^{(p-1)/3} \equiv (L + 9M)/(L - 9M) \bmod p$ precisely when q is a cubic nonresidue mod p and $\frac{L}{M}$ is congruent to -1, 2, 4, -5, 6, or -7 mod 17. One of our goals in this paper is to provide a method for predicting these values. Thus we will show that for $t \in \mathbb{Z}$ the rational function

$$-\frac{t^3 + 27t^2 - 9t - 27}{t^3 - t^2 - 9t + 1} \tag{3}$$

evaluated mod q generates this list whenever $q \equiv \pm 3 \bmod 7$; see rule (v) in Section 5. Indeed, taking $q = 17$ and $t = 0, 1, \ldots, 16$, and ∞ (the latter giving a value of -1), we obtain each of the values -1, 2, 4, -5, 6, and -7 exactly three times.

Although not immediately apparent, Sun finds an equivalent method for generating such lists in [9]. He later gives another formulation involving quotients of degree three polynomials in [10]. It is the latter version of this theorem that will interest us here. Therefore the purpose of this paper is to answer, in the affirmative, the question of whether it is possible to obtain a complementary statement to Lehmer's theorem (1) for cubic nonresidues. In other words, do there exist rational functions which generate the slopes $\frac{M}{L}$ that predict when a given prime q will be a cubic nonresidue of one type or the other mod p? We will use the cube roots of unity ω and $\overline{\omega}$ to track the two types of nonresidues; these correspond in that order to the values $(L + 9M)/(L - 9M)$ and $(L - 9M)/(L + 9M)$ discussed in [11]. We aim to provide a clean, self-contained description of how such a result may be formulated, using elementary methods, with the goal of ultimately presenting a "rational" version of this theory that may be stated without reference to any rings other than the integers.

2 Preliminaries

We will require the machinery of cubic reciprocity, so we briefly recall some of the relevant definitions and results, as presented in Ireland and Rosen [3]. Let R refer to the unique factorization domain $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ with units ± 1, $\pm\omega$, and $\pm\overline{\omega}$, where $\omega = e^{2\pi i/3}$. In what follows, q will always denote a rational prime, i.e. a positive integer that is prime within $\mathbb{Z}$. We know that if $q \equiv 2 \bmod 3$, it is also prime within R, while if $q \equiv 1 \bmod 3$, then q splits into a product $q = \rho\bar{\rho}$ for primes $\rho, \bar{\rho} \in R$. We also have $3 = -\overline{\omega}(1 - \omega)^2$ for the prime $1 - \omega$. Furthermore, p will always refer to a rational prime satisfying $p \equiv 1 \bmod 3$, so that we can write $p = \pi\bar{\pi}$ for primes $\pi, \bar{\pi} \in R$.

We say that a prime $\pi = a + b\omega \in R$ is primary if b is divisible by 3 and complex if $b \neq 0$. (Our terminology differs slightly from [3] here.) When $p \equiv 1 \bmod 3$, there are exactly four primary primes in R that divide p, all complex. If π is one such prime then the others are $-\pi$ and $\pm\bar{\pi}$, and $p = \pi\bar{\pi} = (-\pi)(-\bar{\pi})$. We say that these primes arise from p. (They are the primary primes with norm p.) Observe that in this case

$$4p = 4\pi\bar{\pi} = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 27(\tfrac{b}{3})^2, \tag{4}$$

so letting $L = 2a - b$ and $M = \frac{b}{3}$ yields the four decompositions of $4p$ used in (1), one for each primary divisor π of p. On the other hand, if $q \equiv 2 \bmod 3$, then $\pm q$ are the two primary primes in R dividing (arising from) q. The only primes in R not yet considered are the divisors of 3, such as $1 - \omega$, but none of these are primary.

For each primary prime $\pi \in R$ one can define χ_π, a cubic residue character mod π on R, in the usual manner. Thus, if π divides $\alpha \in R$, we set $\chi_\pi(\alpha) = 0$. If π is complex, then for $\alpha \in R$ with $\pi \nmid \alpha$ we define $\chi_\pi(\alpha) = 1$, ω, or $\overline{\omega}$ according to $\chi_\pi(\alpha) \equiv \alpha^{(p-1)/3} \bmod \pi$, where $p = \pi\bar{\pi}$. Otherwise π is of the form $\pm q$, where $q \equiv 2 \bmod 3$ is a rational prime. In this case we use $\alpha^{(q^2-1)/3}$ to define $\chi_\pi(\alpha)$ in the same manner. It will be helpful to recapitulate several properties of these characters for later use. All but the last follow more or less directly from the definition.

- $\chi_\pi(\alpha\alpha') = \chi_\pi(\alpha)\chi_\pi(\alpha')$.
- If $\alpha \equiv \alpha' \bmod \pi$, then $\chi_\pi(\alpha) = \chi_\pi(\alpha')$.
- $\chi_\pi(\alpha) = 1$ if and only if α is a cubic residue modulo π, so $\chi_\pi(1) = \chi_\pi(-1) = 1$.
- The complex conjugate of $\chi_\pi(\alpha)$ is $\chi_{\bar{\pi}}(\bar{\alpha})$.
- If $q \equiv 2 \bmod 3$ and $k \in \mathbb{Z}$ is not divisible by q, then $\chi_q(k) = 1$.
- If $\pi = a + b\omega$ then $\chi_\pi(1-\omega) = \omega^{2n}$, where $a = \pm(3n-1)$.

With this background we can now state the law of cubic reciprocity.

Theorem 2 *If π and ρ are primary, arising from different rational primes, then*

$$\chi_\pi(\rho) = \chi_\rho(\pi). \tag{5}$$

It is arguably the most elegant of all the reciprocity laws.

3 Constructing the Tables

Given a rational prime q, our first task is to examine the ordered pairs (L, M) corresponding to primes p for which q is not a cubic residue. Loosely speaking, we wish to assign to each such pair a value, either ω or $\bar{\omega}$, that indicates which type of non-residue q should be modulo p. Thus let $p \equiv 1 \bmod 3$ be a rational prime. We have seen that the four pairs of integers (L, M) for which $4p = L^2 + 27M^2$ correspond to the four pairs (a, b) for which $\pi = a + b\omega$ is a primary divisor of p via $L = 2a - b$ and $M = \frac{b}{3}$. Therefore we define

$$F_q(L, M) = \chi_\pi(q). \tag{6}$$

Note that $F_q(L, M)$ is only defined for values of L and M corresponding to primary primes. For example, it is a simple exercise to verify that $F_2(1, 1) = F_2(-1, -1) = \omega$ while $F_2(1, -1) = F_2(-1, 1) = \bar{\omega}$. This may seem inconsistent at first, since all four (L, M) pairs correspond to the same prime $p = 7$. However, we are not defining a single character for $p = 7$ at this point; rather, we are employing four separate characters, one for each primary divisor of 7.

We know that $F_q(L, M) = \chi_\pi(q) = 1$ implies that q is a cubic residue modulo π; a standard argument then shows that this occurs if and only if q is a cubic residue mod $p = \pi\overline{\pi}$. Note that Lehmer's theorem provides an alternate way of determining those pairs (L, M) for which $F_q(L, M) = 1$ without computing the cubic characters $\chi_\pi(q)$. Our goal is to provide a similar description of those pairs for which $F_q(L, M) = \omega$ or $\bar{\omega}$. As a first step, we give a new proof that the value of $F_q(L, M)$ depends only on the ratio $\frac{M}{L} \bmod q$. (This result is known; see [11], for example.)

Proposition 3 *Let $q \geq 5$ be prime. Then the value of $F_q(L, M)$ is constant along lines through the origin, mod q. Furthermore, pairs of lines whose slopes are negatives of one another have conjugate values; that is, $F_q(L, -M) = \overline{F_q(L, M)}$.*

Before beginning the proof, we remark that there is a potential difficulty involving points (L, M) congruent to the origin modulo q, since all the lines described above pass through such a point. However, this would mean that $q|L$ and $q|M$, in which case $L^2 + 27M^2$ could not equal four times a prime. In other words, $F_q(L, M)$ is never defined at such points. The one exception occurs for $q = 2$, since $4 \cdot 31 = 4^2 + 27 \cdot 2^2$, for instance. It turns out that one must examine the values of $F_2(L, M)$ mod 4 rather than mod 2.

Proof: The points (L, M) located on a particular line through the origin mod q are precisely those pairs satisfying $L \equiv kl \bmod q$ and $M \equiv km \bmod q$, where l and m are fixed integers not both divisible by q and k runs through the values $k = 0, 1, \ldots, q-1$. Since

$$a = \tfrac{1}{2}(L + 3M) = k \cdot \tfrac{1}{2}(l + 3m), \qquad b = 3M = k \cdot 3m, \tag{7}$$

the corresponding pairs (a, b) also lie on a line, the one for which $a \equiv ka' \bmod q$ and $b \equiv kb' \bmod q$, where $a' = \frac{1}{2}(l + 3m)$ and $b' = 3m$. Recall that $\pi = a + b\omega$. We set $\pi' = a' + b'\omega$ so that $\pi \equiv k\pi' \bmod q$.

To apply cubic reciprocity, we must consider $q \equiv 1 \bmod 3$ and $q \equiv 2 \bmod 3$ separately. In the latter case q is primary, so $F_q(L, M) = \chi_\pi(q) = \chi_q(\pi)$. Using the fact that χ_q is multiplicative, we deduce that $F_q(L, M) = \chi_q(k)\chi_q(\pi')$. We can disregard $k \equiv 0 \bmod q$, since q would divide both L and M. Hence $\chi_q(k) = 1$, which means that $F_q(L, M) = \chi_q(\pi')$ is constant. The argument is nearly identical when $q \equiv 1 \bmod 3$. In this case we first write $q = \rho\bar{\rho}$ where ρ and $\bar{\rho}$ are primary. Therefore

$$F_q(L, M) = \chi_\pi(q) = \chi_\pi(\rho)\chi_\pi(\bar{\rho}) = \chi_\rho(\pi)\chi_{\bar{\rho}}(\pi). \tag{8}$$

Since $\pi \equiv k\pi' \bmod q$ we know the same is true modulo ρ or $\bar{\rho}$. Hence

$$F_q(L, M) = \chi_\rho(k)\chi_{\bar{\rho}}(k)\chi_\rho(\pi')\chi_{\bar{\rho}}(\pi'). \tag{9}$$

But the first two factors are conjugates, so their product is 1, while the second two depend only on π'. We again conclude that $F_q(L, M)$ is constant along the particular line under consideration.

Finally, note that if the point (L, M) corresponds to a prime π, then $(L, -M)$ corresponds to $\bar{\pi}$, since $\bar{\pi} = a + b\bar{\omega} = (a-b) - b\omega$ is associated with the point $(2(a-b)-(-b), \frac{-b}{3}) = (2a-b, -\frac{b}{3})$, which is $(L, -M)$. Therefore

$$F_q(L, -M) = \chi_{\bar{\pi}}(q) = \overline{\chi_\pi(q)} = \overline{F_q(L, M)}, \tag{10}$$

as desired. □

Similar results hold for $q = 2$ and $q = 3$, but the previous approach cannot be employed. (The expression $\frac{1}{2}(L + 3M)$ makes no sense mod 2, and when $q = 3$ cubic reciprocity does not apply because 3 has no primary divisors.) Therefore we modify the argument for $q = 2$, and simply compute $F_3(L, M)$ directly. We point out that these results are not new; Williams proves an equivalent theorem in [11] using the theory of cyclotomy.

Proposition 4 *The values of $F_2(L, M)$ and $F_3(L, M)$ are given by the following criteria:*

$$F_2(L, M) = \begin{cases} 1 & L, M \equiv 0 \bmod 2 \\ \omega & L \equiv M \bmod 4 \\ \bar{\omega} & L \equiv -M \bmod 4 \end{cases} \qquad F_3(L, M) = \begin{cases} 1 & M \equiv 0 \bmod 3 \\ \omega & L \equiv -M \bmod 3 \\ \bar{\omega} & L \equiv M \bmod 3 \end{cases}. \tag{11}$$

Proof: Since 2 is primary we may employ cubic reciprocity to write $F_2(L,M) = \chi_\pi(2) = \chi_2(\pi)$. By definition, $\chi_2(\pi) \equiv \pi \bmod 2$. Writing $\pi = a + b\omega$, we find that $\chi_2(\pi) = \bar{\omega} = -1 - \omega$ if and only if $a \equiv b \equiv -1 \bmod 2$. Since $L = 2a - b$, this translates to $L \equiv 1, 3 \bmod 4$, depending upon whether $b \equiv 1, 3 \bmod 4$, respectively. We also have $M = \frac{b}{3} \equiv -b \bmod 4$, so $M \equiv 3, 1 \bmod 4$ according as to $b \equiv 1, 3 \bmod 4$. Regardless, $L \equiv -M \bmod 4$, as stated. The analysis of $\chi_2(\pi) = 1$ or ω is even more straightforward, as the reader may verify.

To compute $F_3(L,M)$ we use the fact that $3 = -\omega^2(1-\omega)^2$ to write

$$F_3(L,M) = \chi_\pi(3) = \chi_\pi(-1) \cdot [\chi_\pi(\omega)]^2 \cdot [\chi_\pi(1-\omega)]^2. \tag{12}$$

By definition, $\chi_\pi(\omega) = \omega^{(p-1)/3}$. Using the properties of χ_π presented earlier, we find that

$$F_3(L,M) = \omega^{(2p-2+3n)/3}, \tag{13}$$

where $p = \pi\bar{\pi} = a^2 - ab + b^2$ and $a = \pm(3n-1)$. Hence we must determine the exponent mod 3, which means we must evaluate $2p - 2 + 3n \bmod 9$. For example, suppose that $L \equiv 1 \bmod 3$ and $M \equiv 1 \bmod 3$. Then $b = 3M \equiv 3 \bmod 9$, while $a = \frac{1}{2}(L + 3M) \equiv 2 \bmod 3$. First note that $p \equiv a^2 + 3 \bmod 9$. In addition, a is of the form $3n - 1$ (as opposed to $-(3n-1)$), so $3n = a + 1$. Therefore we may write

$$2p - 2 + 3n \equiv (2a^2 + 6) - 2 + a + 1 \equiv (2a - 1)(a + 1) + 6 \equiv 6 \bmod 9, \tag{14}$$

since both $(a+1)$ and $(2a-1)$ are divisible by 3. Thus $F_3(L,M) = \omega^2 = \bar{\omega}$, as claimed. The remaining possibilities may be ascertained in an analogous manner, leading in each case to the result stated above. □

In light of the periodicity of the values of $F_q(L,M)$ for a given prime q, it makes sense to define a more streamlined function $f_q : \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \{1, \omega, \bar{\omega}\}$ by setting $f_q(l,m) = F_q(L,M)$, for $l \equiv L \bmod q$ and $m \equiv M \bmod q$, whenever $F_q(L,M)$ is defined and non-zero. (Remembering, of course, to operate mod 4 when $q = 2$.) This function is well-defined by the preceding propositions and encapsulates all the information about F_q. Although we will not need it, one can show that if $f_q(l,m)$ is defined for one point on a line through the origin, then it will be defined for every point on that line aside from the origin.

It is informative to present f_q as a $q \times q$ (or 4×4) table of values, which is done for $q = 2$, 3, 5, and 7 in Figure 1. A '$*$' appears to indicate that $F_q(L,M)$ is never defined (or possibly equals 0) for that particular point, because the expression $L^2 + 27M^2$ is never equal to four times a prime (other than possibly $4q$) for $l \equiv L \bmod q$ and $m \equiv M \bmod q$. For small odd values of q the tables are relatively easy to construct. There are $q + 1$ lines through the origin, on which f_q is constant. The horizontal and vertical line contain 1's by Lehmer's theorem and pairs of lines with negative slopes contain conjugate values by Proposition 3. Hence to complete the table for f_5 we need only determine its value at two strategic points. For instance, computing $F_5(1,1) = \chi_{2+3\omega}(5) = \omega$ and $F_5(4,2) = \chi_{5+6\omega}(5) = \bar{\omega}$ will suffice. For the same reasons we need only compute two values of F_7 to deduce the entire table. Notice that in each of the tables exactly one-third of the available lines, and hence one-third of the non-starred entries, are filled with each possible value, either 1, ω, or $\bar{\omega}$.

As a simple application, let us determine whether or not 490 is a cubic residue mod 63601. First, one finds that $4 \cdot 63601 = 19^2 + 27 \cdot 97^2$. Hence we may use any of the four pairs $(\pm 19, \pm 97)$ in our computations, as long as we use the same pair consistently. Taking $(L,M) = (19, 97)$ we have

$$\begin{aligned} F_2(19,97) &= f_2(3,1) = \bar{\omega}, \\ F_5(19,97) &= f_5(4,2) = \bar{\omega}, \\ F_7(19,97) &= f_7(5,6) = \omega. \end{aligned} \tag{15}$$

$f_3(l,m)$

2	$*$	ω	$\bar{\omega}$
1	$*$	$\bar{\omega}$	ω
0	$*$	1	1
	0	1	2

$f_2(l,m)$

3	$*$	$\bar{\omega}$	$*$	ω
2	1	$*$	$*$	$*$
1	$*$	ω	$*$	$\bar{\omega}$
0	$*$	$*$	1	$*$
	0	1	2	3

$f_5(l,m)$

4	1	$\bar{\omega}$	ω	$\bar{\omega}$	ω
3	1	$\bar{\omega}$	$\bar{\omega}$	ω	ω
2	1	ω	ω	$\bar{\omega}$	$\bar{\omega}$
1	1	ω	$\bar{\omega}$	ω	$\bar{\omega}$
0	$*$	1	1	1	1
	0	1	2	3	4

$f_7(l,m)$

6	1	$*$	$\bar{\omega}$	ω	$\bar{\omega}$	ω	$*$
5	1	$\bar{\omega}$	$*$	ω	$\bar{\omega}$	$*$	ω
4	1	ω	ω	$*$	$*$	$\bar{\omega}$	$\bar{\omega}$
3	1	$\bar{\omega}$	$\bar{\omega}$	$*$	$*$	ω	ω
2	1	ω	$*$	$\bar{\omega}$	ω	$*$	$\bar{\omega}$
1	1	$*$	ω	$\bar{\omega}$	ω	$\bar{\omega}$	$*$
0	$*$	1	1	1	1	1	1
	0	1	2	3	4	5	6

Figure 1: The table of values for $f_q(l,m)$ when $q = 2$, 3, 5, and 7.

The appropriate product $\bar{\omega}\cdot\bar{\omega}\cdot\omega^2$ corresponding to $490 = 2\cdot 5\cdot 7^2$ is equal to 1, so we conclude that 490 is a cubic residue. This process works because we are actually computing $\chi_{155+291\omega}(490)$ and using the fact that 490 is a cubic residue mod 63601 if and only if the value of this character equals 1.

4 Determining the ω-slopes

For a given prime q, we now ascertain the pairs (L,M) for which $F_q(L,M) = \omega$ by describing the slopes of the lines containing these points. As in Theorem 1, this is accomplished with a rational function of degree three, but unlike that result, no single rational function will suffice for all primes. We begin by describing the ω-slopes when $q \not\equiv \pm 1 \bmod 9$. The following lemma will be useful.

Lemma 5 *Let $q \neq 3$ be a rational prime relatively prime to a given number $a + b\omega \in R$. Then there exists $\lambda \in R$ primary with $\lambda \equiv a + b\omega \bmod q$.*

Proof: First choose $a' \equiv a \bmod q$ and $b' \equiv b \bmod q$ so that b' is divisible by 3 but a' is not. Then consider the sequence $\{a' + b'\omega + k(3q) \mid k \in \mathbb{Z}\}$. Clearly $3q$ is relatively prime to $a' + b'\omega$, so by Dirichlet's theorem on primes in arithmetic progressions (for number fields) some element λ of the sequence is prime. By construction λ is primary and $\lambda \equiv a + b\omega \bmod q$, as desired. $\square$

We are now able to establish our first main result for cubic nonresidues. This is a special case of Theorem 1.2 in [10], which we will soon prove in full generality, albeit in an significantly different guise.

Proposition 6 *Let $q > 3$ be a rational prime satisfying $q \equiv \pm 2 \bmod 9$, and write $4p = L^2 + 27M^2$ for a prime $p \equiv 1 \bmod 3$, $p \neq q$. Then $F_q(L,M) = \omega$ if and only if*

$$(t^3 - 3t^2 - 9t + 3)L \equiv -3(t^3 + 9t^2 - 9t - 9)M \bmod q \tag{16}$$

for some integer t. When $q \equiv \pm 4 \bmod 9$ the same result holds without the negative.

Proof: Let $\pi = a + b\omega$ where $L = 2a - b$, $M = \frac{b}{3}$, so that $p = \pi\bar{\pi}$ and π is primary, as usual. We wish to find conditions on L and M equivalent to $F_q(L,M) = \omega$. This means that $\chi_\pi(q) = \omega$,

by definition. If $q \equiv 2 \bmod 9$, so that q is also primary, then $\chi_q(\pi) = \omega$ by cubic reciprocity. However, we know that $\chi_q(\bar{\omega}) = \bar{\omega}^{(q^2-1)/3} = \bar{\omega}$, so that

$$1 = \omega\bar{\omega} = \chi_q(\pi)\chi_q(\bar{\omega}) = \chi_q(\bar{\omega}\pi). \tag{17}$$

At this point we would like to invoke cubic reciprocity again in order to apply Lehmer's criterion, but $\bar{\omega}\pi = (b-a) - a\omega$ is no longer primary. However, there is a primary prime $\lambda \equiv \bar{\omega}\pi \bmod q$ by the lemma; hence $\chi_q(\lambda) = \chi_\lambda(q) = 1$. If (L', M') is the pair corresponding to λ, then

$$L' \equiv 2(b-a) - (-a) \equiv 2b - a \bmod q, \quad M' \equiv \tfrac{1}{3}(-a) \bmod q. \tag{18}$$

One quickly confirms that $L' \equiv -\frac{1}{2}L + \frac{9}{2}M \bmod q$ while $M' \equiv -\frac{1}{6}L - \frac{1}{2}M \bmod q$. According to Theorem 1, $\chi_\lambda(q) = 1$ occurs if and only if

$$(t-1)(t+1)L' \equiv t(t-3)(t+3)M' \bmod q \tag{19}$$

for some integer t, which reduces to Eq. (16) upon writing L' and M' in terms of L and M.

If $q \equiv -2 \bmod 9$, then q is not prime in R and we must write $q = \rho\bar{\rho}$ for a primary prime $\rho \in R$. In this case $F_q(L, M) = \chi_\pi(q) = \omega$ becomes

$$\omega = \chi_\pi(\rho)\chi_\pi(\bar{\rho}) = \chi_\rho(\pi)\chi_{\bar{\rho}}(\pi). \tag{20}$$

We find that $\chi_\rho(\bar{\omega}) = \chi_{\bar{\rho}}(\bar{\omega}) = \bar{\omega}^{(q-1)/3} = \omega$ this time; multiplying these equalities into the above equation yields $\chi_\rho(\bar{\omega}\pi)\chi_{\bar{\rho}}(\bar{\omega}\pi) = 1$. Choosing λ primary satisfying $\lambda \equiv \bar{\omega}\pi \bmod q$ as before then leads to $\chi_\rho(\lambda)\chi_{\bar{\rho}}(\lambda) = 1$, or $\chi_\lambda(q) = 1$ upon using cubic reciprocity. One then proceeds as before to obtain Eq. (16).

The analysis of the case $q \equiv -4 \bmod 9$ is nearly identical to $q \equiv 2 \bmod 9$, except that $\chi_q(\omega) = \omega$ this time, so we obtain $\omega\pi = -b + (a-b)\omega$. Now $L' = -a - b = -\frac{1}{2}L - \frac{9}{2}M$ and $M' = \frac{1}{3}(a-b) = \frac{1}{6}L - \frac{1}{2}M$, which leads to the congruence

$$(t^3 + 3t^2 - 9t - 3)L \equiv 3(t^3 - 9t^2 - 9t + 9)M \bmod q. \tag{21}$$

Replacing t by $-t$ and negating both sides then produces (16) sans negative sign, as claimed. Finally, combining these steps with previous ideas gives the same result when $q \equiv 4 \bmod 9$. It is relatively straightforward to reverse this argument to establish the converse. However, we omit the details in favor of a neater approach, which will be outlined next. This completes the proof. □

The foregoing proposition identifies the slopes of the lines through the origin, modulo q, on which f_q (or F_q) equals either ω or $\bar{\omega}$, when $q \not\equiv \pm 1 \bmod 9$. Thus when $q \equiv \pm 2 \bmod 9$ the lines with slope

$$\frac{M}{L} \equiv -\frac{t^3 - 3t^2 - 9t + 3}{3(t^3 + 9t^2 - 9t - 9)} \bmod q \tag{22}$$

pass through points for which $f_q(l, m) = \omega$; while the lines whose slopes are the negatives of these satisfy $f_q(l, m) = \bar{\omega}$. The situation is reversed for $q \equiv \pm 4 \bmod 9$. It is interesting to note that when $q \equiv \pm 1 \bmod 9$ these lines predict the primes for which q is a cubic residue; in other words, the rational function above duplicates the slopes given by Lehmer's theorem. This is to be expected in light of the above proof and the fact that $\chi_q(\omega) = 1$ (or $\chi_\rho(\omega) = 1$) in this case.

It is instructive to confirm Proposition 6 for $q = 5$ and $q = 7$, since we already have tables of values for $f_q(l, m)$. Letting $t = 0$, 1, 2, 3, 4, and ∞ in (22) mod 5 yields slopes of 4, 3, 4, 4, 3, and 3, respectively. These are the $\bar{\omega}$-slopes for f_5, as predicted by the proposition. On

the other hand, taking $t = 0, 1, \ldots, 6$, and ∞ mod 7 gives slopes of 4, 2, 6, 4, 4, 1, 2, and 2, respectively. These are the ω-slopes for f_7, as claimed, along with the lines on which f_7 is not defined, i.e. where the proposition does not apply. Observe that each ω or $\bar{\omega}$-slope occurs exactly three times. This behavior is typical of the rational functions that compute such slopes, which we now introduce.

Let $\gamma \in R$ be written as $\gamma = c + d\omega$. To ease notation, we also set $C = 6c - 3d$ and $D = d$. We then define

$$g_\gamma(t) = -\frac{Dt^3 - Ct^2 - 9Dt + C}{Ct^3 + 27Dt^2 - 9Ct - 27D}. \tag{23}$$

This family of functions possesses several interesting properties.

Proposition 7 *The rational functions g_γ defined above satisfy $g_{-\gamma}(t) = g_\gamma(t)$ and $g_{\bar{\gamma}}(t) = -g_\gamma(-t)$. Furthermore, if $q \equiv 2 \bmod 3$ is a rational prime, then $g_\gamma(t)$ assumes exactly $\frac{1}{3}(q+1)$ distinct values when $t = 0, 1, \ldots, q-1$, and ∞; each is attained by three different values of t. Similarly, if $q \equiv 1 \bmod 3$ then $g_\gamma(t)$ assumes exactly $\frac{1}{3}(q-1)+2$ distinct values; $\frac{1}{3}(q-1)$ of them each coming from three different values of t, along with the two values $\pm\frac{1}{3\sqrt{-3}}$, each attained once.*

Proof: It is clear that $g_{-\gamma}(t) = g_\gamma(t)$. Next observe that $C = 6\,\mathrm{Re}(\gamma)$ while we have $D = \frac{2}{\sqrt{3}}\,\mathrm{Im}(\gamma)$, so that conjugating γ fixes C and negates D. This explains the fact that $g_{\bar{\gamma}} = -g_\gamma(-t)$. To analyze the range of $g_\gamma(t)$ modulo a prime q, we write

$$g_\gamma(t) = \frac{Cg(t) - D}{27Dg(t) + C}, \quad g(t) = g_1(t) = \frac{t^2 - 1}{t^3 - 9t}, \tag{24}$$

where $g(t)$ is the function appearing in Lehmer's theorem. Now the transformation $h : t \mapsto \frac{t-3}{t+1}$ has order three, since applying it repeatedly yields

$$t \mapsto \frac{t-3}{t+1} \mapsto \frac{t+3}{-t+1} \mapsto t. \tag{25}$$

But we have

$$g(t) = \left[-(t)\left(\frac{t-3}{t+1}\right)\left(\frac{t+3}{-t+1}\right)\right]^{-1}, \tag{26}$$

so $g(t)$ is invariant under h. Hence $g_\gamma(t)$ is also, because of (24). Thus $g_\gamma(t)$ assumes the same value modulo q at t, $\frac{t-3}{t+1}$, and $\frac{t+3}{-t+1}$. When $q \equiv 2 \bmod 3$ these three numbers are distinct modulo q, since the congruence of any two is equivalent to $t^2 \equiv -3 \bmod q$, which does not occur. Since $g_\gamma(t)$ may assume the same value for at most three distinct values of t, we deduce that $g_\gamma(t)$ takes on exactly $\frac{1}{3}(q+1)$ different values in the manner claimed.

On the other hand, when $q \equiv 1 \bmod 3$ then $t = \frac{t-3}{t+1} = \frac{t+3}{-t+1}$ twice, for the two values of t satisfying $t^2 \equiv -3 \bmod q$. (Otherwise $g_\gamma(t)$ is three-to-one as before.) Let $\sqrt{-3}$ refer to one of these values modulo q. We find that

$$g_\gamma(\sqrt{-3}) \equiv \frac{4C - 12D\sqrt{-3}}{12C\sqrt{-3} + 108D} \equiv \frac{1}{3\sqrt{-3}} \bmod q, \tag{27}$$

upon cancelling a common factor of $C\sqrt{-3}+9D$. In the same manner one finds that $g_\gamma(-\sqrt{-3}) \equiv -\frac{1}{3\sqrt{-3}} \bmod q$, as asserted. $\square$

By the proposition, the values of $g_{\bar\gamma}(t)$ are the negatives of the values taken by $g_\gamma(t)$. In addition, the exceptional values of $g_\gamma(t)$ are exactly the slopes for which $f_q(l,m)$ is not defined, since

$$L^2 + 27M^2 \equiv 0 \bmod q \quad \Longleftrightarrow \quad \frac{M}{L} \equiv \pm\frac{1}{3\sqrt{-3}} \bmod q. \tag{28}$$

We are now in a position to provide a neat conclusion to Proposition 6. Observe that $g_\omega(t)$ and $g_{\bar\omega}(t)$ are the rational functions giving the ω and $\bar\omega$-slopes that were encountered there. When $q \equiv 2 \bmod 3$, we have seen that each of $g(t)$, $g_\omega(t)$, and $g_{\bar\omega}(t)$ take on exactly $\frac{1}{3}(q+1)$ distinct values modulo q. But these account for all the possible slopes, which proves the only if portion of the statement immediately. The same logic applies when $q \equiv 1 \bmod 3$, once we count the lines on which $f_q(l,m)$ is not defined separately.

The proof of Proposition 6 hinged upon the fact that the value of $\chi_q(\omega)$ (or $\chi_\rho(\omega)$) could be computed and depended upon $q \bmod 9$. As long as that value was not equal to 1 we obtained a formula for ω or $\bar\omega$-slopes. Our next theorem provides an entire family of such formulas, one for each prime $l \equiv 1 \bmod 3$. (We have omitted an analysis of $\chi_q(1-\omega)$; it turns out that one obtains the same result as in Proposition 6.) This is the full analogue to Sun's theorem in [10].

Theorem 8 *Let $l \equiv 1 \bmod 3$ be a rational prime, and write $l = \gamma\bar\gamma$ where $\gamma, \bar\gamma \in R$ are primary. Then the values of $g_\gamma(t)$ mod q give the set of all slopes on which either $f_q(l,m) = 1$, $f_q(l,m) = \omega$, or $f_q(l,m) = \bar\omega$. Furthermore, the particular value of f_q occurring along these lines depends only upon the value of q mod l.*

Proof: This argument closely parallels the proof of Proposition 6, so we will be brief. Also, it will be advantageous to work with F_q rather than f_q. First write $\gamma = c + d\omega$. We know that $\chi_\gamma(q) \equiv q^{(l-1)/3} \bmod \gamma$, so $\chi_\gamma(q)$ depends on the value of q modulo γ, and hence modulo l. Suppose that $\chi_\gamma(q) = \bar\omega$. We wish to identify those pairs (L,M) for which $F_q(L,M) = \omega$, where $4p = L^2 + 27M^2$, $p = \pi\bar\pi$, $\pi = a + b\omega$, $L = 2a - b$, and $M = \frac{b}{3}$ as usual. In the case that q is prime in R cubic reciprocity implies that $\chi_q(\pi) = \omega$ and $\chi_q(\gamma) = \bar\omega$, hence $\chi_q(\gamma\pi) = 1$, or $\chi_\lambda(q) = 1$ for some primary prime $\lambda \equiv \gamma\pi \bmod q$. If (L', M') is the pair corresponding to λ, then

$$L' \equiv 2ac - bd - ad - bc \bmod q, \quad M' \equiv \tfrac{1}{3}(ad + bc - bd) \bmod q. \tag{29}$$

One then writes L' and M' in terms of L and M to obtain

$$L' = \left(\frac{2c-d}{2}\right)L - \left(\frac{9d}{2}\right)M, \quad M' = \left(\frac{d}{6}\right)L + \left(\frac{2c-d}{2}\right)M. \tag{30}$$

Applying Theorem 1, we conclude that $(t^2-1)L' \equiv (t^3 - 9t)M' \bmod q$ for some integer t. In terms of L and M this becomes

$$(Dt^3 - Ct^2 - 9Dt + C)L \equiv -(Ct^3 + 27Dt^2 - 9Ct - 27D)M \bmod q, \tag{31}$$

where $C = 6c - 3d$ and $D = d$. In other words, $F_q(L,M) = \omega$ implies that the slope $\frac{M}{L}$ is of the form $g_\gamma(t)$, modulo q.

In the same manner one finds that $F_q(L,M) = \bar\omega$ means that $\frac{M}{L} \equiv g_{\bar\gamma}(t) \bmod q$, since $\chi_{\bar\gamma}(q) = \omega$. Of course, $F_q(L,M) = 1$ leads to $\frac{M}{L} \equiv g(t) \bmod q$ by Lehmer's result. Since these three cases account for all $q+1$ possible slopes when $q \equiv 2 \bmod 3$, by Proposition 7, we can make the stronger assertion that $F_q(L,M) = \omega$ if and only if $\frac{M}{L} \equiv g_\gamma(t) \bmod q$ for some integer t.

If q is not prime in R then we write $q = \rho\bar\rho$, where $\rho, \bar\rho \in R$ are primary. A few extra steps are required, but just as in Proposition 6 one still reaches $\chi_\lambda(q) = 1$ with $\lambda \equiv \gamma\pi \bmod q$, so $g_\gamma(t)$ prescribes the ω-slopes regardless of whether or not q is prime in R. This concludes the discussion of the case $\chi_\gamma(q) = \bar\omega$.

On the other hand, if q is a rational prime such that $\chi_\gamma(q) = \omega$, then precisely the same reasoning shows that $F_q(L, M) = \omega$ if and only if $\frac{M}{L} \equiv g_{\bar{\gamma}}(t) \bmod q$, while $F_q(L, M) = \bar{\omega}$ is equivalent to $\frac{M}{L} \equiv g_\gamma(t) \bmod q$; i.e. the situation is reversed in this case. Finally, if q satisfies $\chi_\gamma(q) = \chi_{\bar{\gamma}}(q) = 1$ then Lehmer's Theorem implies that both $g_\gamma(t)$ and $g_{\bar{\gamma}}(t)$ give slopes on which $F_q(L, M) = 1$, so no formula for ω-slopes is obtained. This completes the proof. □

5 Rational Cubic Residues

We now give a pared-down, "rational" version of this theory. We are interested in whether or not the congruence $x^3 \equiv c \bmod p$ is solvable for a prime $p \equiv 1 \bmod 3$. This can be done by utilizing a cubic character $\chi \bmod p$, which we now construct. To begin, set $\chi(0) = \chi(p) = 0$ and $\chi(1) = \chi(-1) = 1$. Also let L and M be the unique *positive* integers for which $4p = L^2 + 27M^2$. Then given a prime number $q \neq p$, we define $\chi(q)$ according to the following rules. The first two handle the special cases of $q = 2$ and $q = 3$. In the remaining rules we assume that $q \geq 5$.

(i) If $4|LM$ then $\chi(2) = 1$, if $4|(L - M)$ then $\chi(2) = \omega$, if $4|(L + M)$ then $\chi(2) = \bar{\omega}$.

(ii) If $3|M$ then $\chi(3) = 1$, if $3|(L + M)$ then $\chi(3) = \omega$, if $3|(L - M)$ then $\chi(3) = \bar{\omega}$.

(iii) If $(t^2 - 1)L \equiv (t^3 - 9t)M \bmod q$ for some integer t, then $\chi(q) = 1$.

(iv) Suppose $q \not\equiv \pm 1 \bmod 9$. Then either $\chi(q) = 1$ or

$$\frac{M}{L} \equiv \pm \frac{t^3 - 3t^2 - 9t + 3}{3(t^3 + 9t^2 - 9t - 9)} \bmod q$$

for some integer t. When $q \equiv \pm 2 \bmod 9$ and the plus sign occurs, set $\chi(q) = \bar{\omega}$; with the minus sign define $\chi(q) = \omega$. If instead $q \equiv \pm 4 \bmod 9$ and the plus sign holds, then let $\chi(q) = \omega$, otherwise define $\chi(q) = \bar{\omega}$.

(v) Suppose $q \not\equiv \pm 1 \bmod 7$. Then either $\chi(q) = 1$ or

$$\frac{M}{L} \equiv \pm \frac{t^3 - t^2 - 9t + 1}{t^3 + 27t^2 - 9t - 27} \bmod q$$

for some integer t. When $q \equiv \pm 2 \bmod 7$ and the plus sign occurs, set $\chi(q) = \omega$; with the minus sign define $\chi(q) = \bar{\omega}$. If instead $q \equiv \pm 3 \bmod 7$ and the plus sign holds, then let $\chi(q) = \bar{\omega}$, otherwise define $\chi(q) = \omega$.

(vi) Suppose $q \not\equiv \pm 1, \pm 5 \bmod 13$. Then either $\chi(q) = 1$ or

$$\frac{M}{L} \equiv \pm \frac{t^3 - 5t^2 - 9t + 5}{5t^3 + 27t^2 - 45t - 27} \bmod q$$

for some integer t. When $q \equiv \pm 2, \pm 3 \bmod 13$ and the plus sign occurs, set $\chi(q) = \omega$; with the minus sign define $\chi(q) = \bar{\omega}$. If instead $q \equiv \pm 4, \pm 6 \bmod 13$ and the plus sign holds, then let $\chi(q) = \bar{\omega}$, otherwise define $\chi(q) = \omega$.

Finally, one extends χ multiplicatively to define $\chi(c)$ when c is not prime. Thus if $c = \pm q_1^{e_1} \cdots q_n^{e_n}$, then we set $\chi(c) = \chi(q_1)^{e_1} \cdots \chi(q_n)^{e_n}$.

Theorem 9 *The construction of χ just given is self-consistent and defines a cubic character modulo p. Furthermore, $\chi(c) = 1$ if and only if c is a cubic residue modulo p.*

Proof: Let π be the primary divisor of p corresponding to the pair (L, M) with both L and M positive. Then by Proposition 4, Proposition 6, and Theorem 8, the values of χ prescribed above agree with χ_π, so will consistently define a cubic character character modulo π, and hence modulo p. Here we have used $\gamma = 2 + 3\omega$ and $\gamma = 4 + 3\omega$ in Theorem 8 to obtain rules (v) and (vi), respectively. The fact that $\chi(c) = 1$ if and only if c is a cubic residue has already been established. □

We remark that when $\chi(q) \neq 1$ then any of the last three rules may be employed; the theorem implies that any applicable rule will give the same value for $\chi(q)$. It is also possible that none of them can be used — this occurs on average for one in every twenty-seven primes q. (Technically speaking, the above rules do not cover primes $q \equiv 2^{3m}5^{3n} \bmod 819$. The smallest such prime is $q = 181$. The reader is invited to explain why the powers of 2^3 and 5^3 appear.) In this case one could compute $\chi(p - q) = \chi(q)$ instead, or appeal to Theorem 8, using a prime l other than 7 or 13.

It is also interesting to note that because the rational functions in the last three rules give ω or $\bar{\omega}$-slopes, their numerators and denominators will never vanish at the primes $q \geq 5$ for which they apply. (Due to Lehmer's result, the lines with slope 0 and ∞ contain points corresponding to primes for which q is a cubic residue.) However, as mentioned above, these functions duplicate the slopes in Lehmer's Theorem for the omitted values of q, hence they vanish for three distinct values of t, by Proposition 7. Applying this reasoning to rule (vi), for example, provides an alternate method of verifying the following neat fact.

Corollary 10 *The polynomial $t^3 - 7t - 7$ factors completely modulo q in the case $q \equiv \pm 1 \bmod 7$, has a triple root when $q = 7$, and otherwise is irreducible modulo q.*

Proof: We have just argued that for primes $q \geq 5$ and $q \neq 7$, the denominator $t^3 + 27t^2 - 9t - 27$ in rule (vi) will vanish for three distinct values of t modulo q when $q \equiv \pm 1 \bmod 7$, but will never vanish otherwise. In the latter case the polynomial must be irreducible, since any factorization would have to involve a linear factor. This property is not affected by the substitution $t \mapsto 6t + 9$, which yields the polynomial $6^3(t^3 - 7t - 7)$. By inspection the primes $q = 2$, 3, and 7 agree with the statement, thus completing the argument. □

The discriminant of $t^3 - 7t - 7$ is $D = 49$, a perfect square, which helps to explain the relatively simple conditions on q. Note that Spearman and Williams [8] have devised methods for predicting when a cubic polynomial splits completely mod q in the considerably more complicated case that D is not a perfect square.

We conclude with a somewhat more exotic example: we shall determine whether $1982 = 2 \cdot 991$ is a cubic residue modulo $p = \frac{1}{4}(3^{19} + 5^{82})$, a 131-digit number which is prime. One easily reads off $L = 5^{41}$ and $M = 3^8$. Since $L \equiv M \equiv 1 \bmod 4$, we find that $\chi(2) = \omega$ according to rule (i). We also compute $991 \equiv 1 \bmod 9$, $991 \equiv -3 \bmod 7$, and $991 \equiv 3 \bmod 13$, so we may use either of rules (v) or (vi), but not (iv). The relevant slope is

$$\frac{M}{L} = \frac{3^8}{5^{41}} \equiv 672 \equiv -319 \bmod 991. \tag{32}$$

We then use *Pari-GP* software to create a list of the values of the rational function in rule (v). One discovers that 319 appears in the list (but not 672), so the negative sign must be taken, leading to $\chi(991) = \omega$. For confirmation, we create a similar list of slopes using rule (vi), and find that 672 appears this time rather than 319, so the positive sign holds. Hence this rule also dictates that we should define $\chi(991) = \omega$. In summary, $\chi(1982) = \chi(2)\chi(991) = \omega \cdot \omega \neq 1$, so 1982 is not a cubic residue.

It is important to point out that the results presented here are primarily of theoretical rather than computational interest. The *Pari-GP* software invoked above can nearly instantly reach the same conclusion regarding the status of 1982 as a cubic residue modulo $p = \frac{1}{4}(3^{19} + 5^{82})$ by simply reducing $1982^{\frac{1}{3}(p-1)}$ modulo p.

Acknowledgments

The author is grateful to Ravi Vakil and K. Soundararajan for their encouragement during the preparation of this manuscript. Additional thanks to Karim Belabas for his remarks regarding the implementation of *Pari-GP*.

References

[1] D. Cox, *Primes of the Form $x^2 + ny^2$* (Jon Wiley & Sons, Inc., 1989).

[2] A. Cunningham and T. Gosset, 4-tic and 3-bic Residuacity Tables, *Mess. Math.* Volume L (1920) 1–30.

[3] K. Ireland & M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer Publishers, 1990).

[4] J. G. D. Jacobi, De residuis cubicis commentatio numerosa, *J. Reine Angew. Math.* 2 (1827), 66–69.

[5] E. Lehmer, Criteria for Cubic and Quartic Residuacity, *Mathematika* **5** (1958) 20–29.

[6] ———, On Euler's Criterion, *J. Austral. Math. Soc.* **1** (1959) 64–70.

[7] P. Pépin, *Mémoire sur les Lois de Réciprocité Relatives aux Résidus de Puissances* (Rome, 1878).

[8] B. Spearman and K. Williams, The Cubic Congruence $x^3 + Ax^2 + Bx + C \equiv 0 \bmod p$ and Binary Quadratic Forms, *J. London Math. Soc.* **46** (1992) 397–410.

[9] Z. Sun, Cubic Residues and Nonresidues, *Acta Arithmetica* **84** (1998) 291–335.

[10] ———, Cubic residues and binary quadratic forms, *J. Number Theory* **124** (2007) 62–104.

[11] K. Williams, On Euler's Criterion for Cubic Nonresidues, *Proc. Amer. Math. Soc.* **49** (1975) 277–283.