CUBIC AND QUARTIC RESIDUES MODULO A PRIME

Joseph B. Dence

University of Missouri–St. Louis

Thomas P. Dence

Ashland University

1. Residues Modulo A Prime. Standard theorems on quadratic residues form an integral part of any introductory course on the theory of numbers. Seldom is much material presented on residues of higher order. Let p be a prime and let the integer a satisfy $1 \leq a < p$. Then a is said to be a kth order residue of p (or modulo p) if the congruence

$$x^k \equiv a \pmod{p}$$

has a solution. For example, 6 is a cubic residue (3rd order residue) of 7 since $3^3 \equiv 6 \pmod{7}$.

Here, we summarize some elementary theorems about cubic and quartic (4th order) residues of prime moduli. The following theorem is central [1,2].

Theorem 1. $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = (k, p-1)$. If the congruence has a solution, then it actually has d incongruent solutions modulo p.

Proof. Since p is a prime, it has a primitive root, say r [2]. Then from index arithmetic we have that $x^k \equiv a \pmod{p}$ holds if and only if

$$k \cdot \mathrm{ind}_r x \equiv \mathrm{ind}_r a \pmod{p-1}.$$

Let $d = (k, p-1)$ and $z = \mathrm{ind}_r x$, that is, $x \equiv r^z \pmod{p}$. Then the congruence $kz \equiv \mathrm{ind}_r a \pmod{p-1}$ has no solutions (z) or d incongruent solutions modulo $p-1$ if and only if $d \nmid \mathrm{ind}_r a$ or $d \mid \mathrm{ind}_r a$, respectively. Hence, $x^k \equiv a \pmod{p}$ has d incongruent solutions modulo p if and only if $d \mid \mathrm{ind}_r a$ or if and only if $(p-1)\mathrm{ind}_r a = n(p-1)d$ for some $n \in \mathbb{Z}^+$. This is equivalent to $a^{(p-1)/d} \equiv 1 \pmod{p}$ since $\mathrm{ind}_r 1 = 0$.

The theorem is a generalization of Euler's Criterion for quadratic residues.

2. Cubic Residues. Throughout this section $k = 3$. When $p = 5, 7, 11, 13, 17, 19$ and 23, the number of cubic residues of these primes are $4, 2, 10, 4, 16, 6$ and 22, respectively. A pattern is evident.

Theorem 2. The number of cubic residues of $p > 3$ is $(p-1)/3$ or $p-1$, depending on whether p is of the form $3j+1$ or $3j+2$, respectively.

Proof. If $p = 3j+1$, then $d = (k, p-1) = (3, 3j) = 3$, so from Theorem 1, a is a cubic residue of p if and only if $a^{(p-1)/3} - 1 \equiv 0 \pmod{p}$. Lagrange's Theorem [3,4] says that in $\mathbb{Z}_p$ this polynomial congruence has at most $(p-1)/3$ solutions. However, a related theorem says that if $m \mid (p-1)$, then the congruence $x^m - 1 \equiv 0 \pmod{p}$ has the full set of m solutions [4]. Thus, since $(p-1)/3 \mid (p-1)$, then $a^{(p-1)/3} - 1 \equiv 0 \pmod{p}$ has exactly $(p-1)/3$ solutions in $\mathbb{Z}_p$.

If $p = 3j+2$, then $d = (k, 3j+1) = (3, 3j+1) = 1$ and a is a cubic residue to p if and only if $a^{(p-1)} \equiv 1 \pmod{p}$. This holds for all a satisfying $1 \leq a \leq p-1$ by Fermat's Theorem, so there are $p-1$ cubic residues of p.

We let $S_p^{(3)}$ denote the set of cubic residues of the prime p. The sets $S_p^{(3)}$ for the first few primes are shown in Table 1.

p	2	3	5	7	11	13
$S_p^{(3)}$	$\{1\}$	$\{1,2\}$	$\{1,2,3,4\}$	$\{1,6\}$	$\{1,2,\cdots,10\}$	$\{1,5,8,12\}$

TABLE 1. Cubic Residues of the First Few Primes

These sets have algebraic structure. We recall that an element α of a field F is an nth root of unity if $\alpha^n = 1$.

Theorem 3. The cubic residues of a prime p form a multiplicative group.

Proof. Let F be any field and U_n the set of all nth roots of unity in F. If $\alpha^n = 1$, $\beta^n = 1$, then $(\alpha\beta)^n = \alpha^n\beta^n = 1$, so field multiplication is closed on U_n. Associativity is inherited from F. Now let $\alpha \in U_n$ be arbitrary, and define $\tau = \alpha^{n-1}$. Then $\alpha\tau = \tau\alpha = \alpha^n = 1$, so every element in U_n has a multiplicative inverse and U_n is therefore a group. In particular, let $F = \mathbb{Z}_p$ and $p = 3j+1$. Then from Theorems 1 and 2, U_n is S_p^3, the set of all jth roots of unity. If $F = \mathbb{Z}_p$ and $p = 3j+2$, then U_n is $S_p^{(3)}$, the set of all $(3j+1)$st roots of unity.

Thus, we see from Table 1 that in $\mathbb{Z}_7$ the set $S_7^{(3)}$ is the set of two square roots of 1, and in $\mathbb{Z}_{13}$ the set $S_{13}^{(3)}$ is the set of four fourth roots of 1. We also observe from Table 1 that for

$p > 2$, $|S_p^{(3)}|$ is even. For when $p = 3j+2$, then $|S_p^{(3)}| = p-1$, and when $p = 3j+1$ is prime, then p is actually of the form $6j+1$, so $(p-1)/3 = 2j$ is even. It is also obvious that $S_p^{(3)}$ is a cyclic group since it is either U_j or U_{3j+1}, corresponding to $p = 3j+1$ or $p = 3j+2$. The cyclic nature of $S_p^{(3)}$ also follows from the observation that $S_p^{(3)}$ is a subgroup of $\mathbb{Z}_p^*$, the multiplicative group of all nonzero elements of the finite field $\mathbb{Z}_p$, and this latter group is cyclic [5,6].

Corollary 3.1. $S_p^{(3)}$ is a cyclic group of even order for $p > 2$.

The following theorem shows that if some of the cubic residues of a prime p are known, it is possible to deduce some additional ones.

Theorem 4. If a is a cubic residue of p, then so is $p - a$.

Proof. Suppose $p = 3j+1$ and $a \in S_p^{(3)}$; then $a^{(p-1)/3} \equiv 1 \pmod{p}$. Next, since $(p-1)/3$ is even, then $(p-a)^{(p-1)/3} \equiv (-a)^{(p-1)/3} \equiv a^{(p-1)/3} \equiv 1 \pmod{p}$, so $p-a \in S_p^{(3)}$. On the other hand, if $p = 3j+2$, then $(p-a)^{p-1} \equiv (-a)^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}$, and thus in this case, also, $p - a \in S_p^{(3)}$.

The following two corollaries are immediate from Theorem 4. We let $T_p^{(3)}$ denote the sum of all the members of $S_p^{(3)}$.

Corollary 4.1. If $p > 2$, the elements in $S_p^{(3)}$ occur in pairs, where the sum of the members of any pair is p.

Corollary 4.2. For all primes $p \geq 5$ one has

$$T_p^{(3)} = \begin{cases} jp, & \text{if } p = 6j+1 \\ (3j+1)p/2, & \text{if } p = 3j+2. \end{cases}$$

For example, let $p = 43 = 6 \cdot 7 + 1$. The cubic residues of 43 are found to be $1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42$; their sum is $301 = 7 \cdot 43$. In either case in the second corollary we have that $T_p^{(3)}$ is an integral multiple of p.

That $p \mid T_p^{(3)}$ can be obtained in still another way. Let $m = |S_p^{(3)}|$, where m is either $(p-1)/3$ or $p-1$. Then $m \mid (p-1)$ and therefore in $\mathbb{Z}_p$ the congruence $x^m - 1 \equiv 0 \pmod{p}$ has its full complement of roots and from [4], we can write

$$x^m - 1 \equiv (x - a_1)(x - a_2) \cdots (x - a_m) \pmod{p}.$$

We see immediately that

$$\text{coefficient of } x^{m-1} = -\sum_{i=1}^{m} a_i \equiv 0 \pmod{p}$$

$$\text{coefficient of } x^{m-2} = \sum_{i<j} a_i a_j \equiv 0 \pmod{p},$$

and so on. The first congruence gives us $p \mid T_p^{(3)}$.

<u>Corollary 4.3</u>. Let $A_p^{(3)}$ denote the sum of the squares of all the members of $S_p^{(3)}$. Then for $p = 5$ and all primes $p > 7$, one has $p \mid A_p^{(3)}$.

<u>Proof</u>. Denote the members of $S_p^{(3)}$ by $a_1, a_2, \ldots, a_m$, where m is either $(p-1)/3$ or $p-1$. Then write

$$\begin{aligned} A_p^{(3)} &= a_1^2 + a_2^2 + \cdots + a_m^2 \\ &= (a_1 + a_2 + \cdots + a_m)^2 - 2\sum_{i<j} a_i a_j \\ &= [T_p^{(3)}]^2 - 2\sum_{i<j} a_i a_j. \end{aligned}$$

Corollary 4.2 gives us $p \mid [T_p^{(3)}]^2$, and the discussion prior to Corollary 4.3 gives us $p \mid \sum_{i<j} a_i a_j$, so $p \mid A_p^{(3)}$.

Corollary 4.3 fails for $p = 3, 7$ because these are the only values of p for which $S_p^{(3)} = \{1, p-1\}$, so $A_p^{(3)} = p^2 - 2p + 2$ and thus $p \nmid (p^2 - 2p + 2)$.

Finally, we look at one multiplicative property of cubic residues. We let $P_p^{(3)}$ denote the product of all the members of $S_p^{(3)}$.

<u>Theorem 5</u>. $1 + P_p^{(3)} \equiv 0 \pmod{p}$.

<u>Proof</u>. The theorem is obviously true when $p = 2$. When $p > 2$, the congruence $x^2 \equiv 1 \pmod{p}$ has the solutions $x \equiv 1 \pmod{p}$ and $x \equiv p - 1 \pmod{p}$. In view of Theorem 3, each element $a_i \in S_p^{(3)}$ except $1, p-1$ has an inverse a_j distinct from itself. Hence,

$$\prod_{a_i \in S_p^{(3)}} a_i \equiv p - 1 \pmod{p},$$

or $P_p^{(3)} \equiv p - 1 \pmod p$, which is equivalent to $1 + P_p^{(3)} \equiv 0 \pmod p$.

3. Quartic Residues. We denote the set of all quartic residues of a prime p by $S_p^{(4)}$, and the set of all quadratic residues of p by $S_p^{(2)}$. Every quartic residue a is automatically a quadratic residue since if $x^4 \equiv a \pmod p$ has a solution, then $y^2 \equiv a \pmod p$ also holds, where $y = x^2$. Thus, $S_p^{(4)} \subseteq S_p^{(2)}$ and we may find all members of $S_p^{(4)}$ by squaring the elements of $S_p^{(2)}$.

By Euler's Criterion, a is a quadratic residue of p ($p \geq 3$) if and only if

$$a^{(p-1)/2} \equiv 1 \pmod p,$$

whereas from Theorem 1 we have that a is a quartic residue of p if and only if

$$a^{(p-1)/d} \equiv 1 \pmod p,$$

where $d = (4, p-1)$. For $p \geq 3$ one has $d = 2$ or 4. When $d = 2$ the sets $S_p^{(2)}$, $S_p^{(4)}$ are identical, whereas when $d = 4$ one has $|S_p^{(4)}| = (1/2)|S_p^{(2)}|$. Accordingly, we obtain as the analog of Theorem 2 (for $p \geq 3$).

Theorem 6. The number of quartic residues of p is $(p-1)/4$ or $(p-1)/2$, depending on whether $p > 2$ is of the form $4j + 1$ or $2j + 1$ (j odd), respectively, and in either case $|S_p^{(4)}| = j$.

The argument of Theorem 3 carries over unaltered to quartic residues. Further, the algebraic argument preceding Corollary 3.1 that was used to show the cyclic nature of $S_p^{(3)}$ also applies to $S_p^{(4)}$.

Theorem 7. The quartic residues of a prime p form a cyclic group under modular multiplication.

Unlike the case with $S_p^{(3)}$, the order of $S_p^{(4)}$ may be either odd or even. Table 2 shows the first few cases.

p	2	3	5	7	11	13
$S_p^{(4)}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1,2,4\}$	$\{1,3,4,5,9\}$	$\{1,3,9\}$

TABLE 2. Quartic Residues of the First Few Primes

When $(p-1)/4$ is not an integer, then $(p-1)/2$ is an odd integer. Thus, for primes $p = 3, 7, 11, 19, 23$, and so on, $S_p^{(4)}$ is a group of odd order. When $(p-1)/4$ is an integer, it may be either odd or even. Clearly, we have

Corollary 7.1. $S_p^{(4)}$ is a cyclic group of even order if and only if $p = 8j + 1$.

According to Theorem 4, $p - 1$ is always a cubic residue of p. In contrast, from Theorem 1 we see that $p - 1$ is a quartic residue if and only if $(p - 1)/d$ is even, where $d = (k, p-1) = (4, p-1)$. But now Corollary 7.1 has told us just when $(p-1)/d$ is even, so

Corollary 7.2. $p - 1$ is a quartic residue of p if and only if $p = 8j + 1$.

The algebraic argument following Corollary 4.2 allows one to also say $p \mid T_p^{(4)}$, where $T_p^{(4)}$ stands for the sum of all the members of $S_p^{(4)}$. Alternately, since $S_p^{(4)}$ is cyclic, it has a generator g. From Theorem 6 we have $|S_p^{(4)}| = j$ for $p = 4j+1$ or $p = 2j+1$. The elements of $S_p^{(4)}$ can thus be listed modulo p as $\{g^0, g^1, g^2, \cdots, g^{j-1}\}$, where $g^0 = 1$. Then, if $g \neq 1$,

$$T_p^{(4)} = 1 + g^1 + g^2 + \cdots + g^{j-1}$$

$$= \frac{g^j - 1}{g - 1}.$$

Since $S_p^{(4)}$ has order j, then $g^j \equiv 1 \pmod{p}$. It follows that $T_p^{(4)} \equiv 0 \pmod{p}$.

Theorem 8. For $p > 5$ one has $p \mid T_p^{(4)}$.

Note the requirement that $p > 5$. When $p = 2, 3$, or 5, the only quartic residue is 1, this being so in the last case because of Fermat's Theorem.

In $x^4 \equiv a \pmod{p}$, as one runs through the nonzero members x of $\mathbb{Z}_p$, a symmetry in the occurrence of the quartic residues a is observed. For example, notice the following distribution in the case of $p = 11$.

x	1	2	3	4	5	6	7	8	9	10
a	1	5	4	3	9	9	3	4	5	1

Table 3. Symmetry Between Elements of $\mathbb{Z}_{11}$ and the Corresponding Quartic Residues

Theorem 9. If the quartic residue corresponding to $x \in \mathbb{Z}_p$ is a, then the quartic residue corresponding to $p - x$ is also a.

Proof. Direct computation gives

$$\begin{aligned}(p-x)^4 &= p^4 - 4p^3x + 6p^2x^2 - 4px^3 + x^4 \\ &\equiv 0 - 0 + 0 - 0 + a \pmod{p}.\end{aligned}$$

We denote by $P_p^{(4)}$ the product of all the members of $S_p^{(4)}$. For example, from Table 2 we have

$$P_{11}^{(4)} = 1 \cdot 3 \cdot 4 \cdot 5 \cdot 9 = 540 \equiv 1 \pmod{11},$$

whereas for $p = 17$,

$$P_{17}^{(4)} = 1 \cdot 4 \cdot 13 \cdot 16 = 832 \equiv -1 \pmod{17}.$$

Theorem 10. For all p one has

$$P_p^{(4)} \equiv \begin{cases} -1 \pmod{p}, & \text{if } p = 8j+1 \\ +1 \pmod{p}, & \text{otherwise.} \end{cases}$$

Proof. The theorem is obviously true when $p = 2, 3, 5$. When $p \geq 7$ is not of the form $8j+1$, $|S_p^{(4)}|$ is odd and the only member of $S_p^{(4)}$ which is its own inverse is 1 by Corollaries 7.1, 7.2. In this case, the members of $S_p^{(4)}$, where $|S_p^{(4)}| = 2n+1$, can be paired as follows

$$\begin{cases} \quad 1 \\ a_1 \leftrightarrow a_1^{-1} \\ a_2 \leftrightarrow a_2^{-1} \\ a_3 \leftrightarrow a_3^{-1} \\ \quad \vdots \\ a_n \leftrightarrow a_n^{-1} \end{cases}$$

and hence,

$$P_p^{(4)} = 1 \cdot \prod_{i=1}^{n} a_i \cdot a_i^{-1} \equiv 1 \pmod{p}.$$

On the other hand, if $p = 8j + 1$, then $|S_p^{(4)}|$ is of even order, $p - 1$ is an element of $S_p^{(4)}$, where $|S_p^{(4)}| = 2n + 2$, and from the arrangement

$$\begin{cases} \quad 1 \\ a_1 \leftrightarrow a_1^{-1} \\ a_2 \leftrightarrow a_2^{-1} \\ a_3 \leftrightarrow a_3^{-1} \\ \qquad \vdots \\ a_n \leftrightarrow a_n^{-1} \\ \quad p - 1 \end{cases}$$

we obtain

$$P_p^{(4)} = 1 \cdot \left(\prod_{i=1}^{n} a_i \cdot a_i^{-1} \right) \cdot (p - 1) \equiv p - 1 \equiv -1 \pmod{p}.$$

Theorem 10 contrasts with Theorem 5. Note also that Theorem 8 is almost analogous to Corollary 4.3

References

1. H. E. Rose, *A Course in Number Theory*, Oxford University Press, Oxford, (1988), 83–84.
2. K. H. Rosen, *Elementary Number Theory and Its Applications*, 3rd ed., Addison–Wesley, Reading, (1993), 285–302.
3. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, (1976), 115.
4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, (1979), 84–85.
5. J. B. Fraleigh, *A First Course in Abstract Algebra*, 4th ed., Addison–Wesley, Reading, (1989), 408–409.
6. M. Artin, *Algebra*, Prentice–Hall, Englewood Cliffs, (1991), 510–513. æ