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 $\mathrm{ind}_r 1 = 0$.