Introduction to number theory-10

May 29, 2017

Power Residues

Let m, k, and a be integers such that $m \geq 2$, $k \geq 2$, and $(a, m) = 1$. We say that a is a *kth power residue modulo m* if there exists an integer x such that

$$x^k \equiv a \pmod{m}.$$

If this congruence has no solution, then a is called a *kth power nonresidue modulo m.*

Let $k = 2$ and $(a, m) = 1$. If the congruence $x^2 \equiv a \pmod{m}$ is solvable, then a is called a *quadratic residue modulo* m. Otherwise, a is called a *quadratic nonresidue modulo* m. For example, the quadratic residues modulo 7 are $1, 2$, and 4; the quadratic nonresidues are $3, 5$, and 6. The only quadratic residue modulo 8 is 1, and the quadratic nonresidues modulo 8 are $3, 5, 4$ and 7.

Let $k = 3$ and $(a, m) = 1$. If the congruence $x^3 \equiv a \pmod{m}$ is solvable, then a is called a *cubic residue modulo* m. Otherwise, a is called a *cubic nonresidue modulo* m. For example, the cubic residues modulo 7 are 1 and 6; the cubic nonresidues are 2, 3, 4, and 5. The cubic residues modulo 5 are 1, 2, 3, and 4; there are no cubic nonresidues modulo 5.

Theorem 3.11 *Let p be prime, $k \geq 2$, and $d = (k, p-1)$. Let a be an integer not divisible by p. Let g be a primitive root modulo p, Then a is a kth power residue modulo p if and only if*

$$ind_g(a) \equiv 0 \pmod{d}$$

if and only if

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

If a is a kth power residue modulo p, then the congruence

$$x^k \equiv a \pmod{p} \tag{3.7}$$

has exactly d solutions that are pairwise incongruent modulo p. Moreover, there are exactly $(p-1)/d$ pairwise incongruent kth power residues modulo p.

Proof. Let $\ell = \mathrm{ind}_g(a)$, where g is a primitive root modulo p. Congruence (3.7) is solvable if and only if there exists an integer y such that

$$g^y \equiv x \pmod{p}$$

and

$$g^{ky} \equiv x^k \equiv a \equiv g^\ell \pmod{p}.$$

This is equivalent to

$$ky \equiv \ell \pmod{p-1}. \tag{3.8}$$

This linear congruence in y has a solution if and only if

$$\text{ind}_g(a) = \ell \equiv 0 \pmod{d},$$

where $d = (k, p-1)$. Thus, the kth power residues modulo p are precisely the integers in the $(p-1)/d$ congruence classes $g^{id} + p\mathbf{Z}$ for $i = 0, 1, \ldots, (p-1)/d - 1$. Moreover,

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

if and only if

$$\frac{(p-1)\ell}{d} \equiv 0 \pmod{p-1}$$

if and only if

$$\text{ind}_g(a) = \ell \equiv 0 \pmod{d}.$$

Finally, if the linear congruence (3.8) is solvable, then by Theorem 2.2 it has exactly d solutions y that are pairwise incongruent modulo $p-1$, and so (3.7) has exactly d solutions $x = g^y$ that are pairwise incongruent modulo p. This completes the proof. $\square$

For example, let $p = 19$ and $k = 3$. Then $d = (k, p-1) = (3, 18) = 3$. We can check that 2 is a primitive root modulo 19, and so a is a cubic residue modulo 19 if and only if 3 divides $\mathrm{ind}_2(a)$. Since $-1 \equiv 2^9 \pmod 3$ and $\mathrm{ind}_2(-1) = 9$, it follows that -1 is a cubic residue modulo 19. The solutions of the congruence $x^3 \equiv -1 \pmod{19}$ are of the form $x \equiv 2^y \pmod{19}$, where $0 \le y \le 17$ and $3y \equiv 9 \pmod{18}$. Then $y \equiv 3 \pmod 6$, and so $y = 3, 9,$ and 15. These give the following three cube roots of -1 modulo 19:

$$8 \equiv 2^3 \pmod{19},$$

$$18 \equiv 2^9 \pmod{19},$$

and

$$12 \equiv 2^{15} \pmod{19}.$$

Corollary 3.1 *Let p be an odd prime, and let $k \geq 2$ be an integer such that $(k, p-1) = 1$. If $(a, p) = 1$, then a is a kth power residue modulo p, and the congruence $x^k \equiv a \pmod{p}$ has a unique solution modulo p.*

thank you