Primitive Roots

Theorem : (10.4)

If the order of a modulo m is t, then $a^r \equiv a^s \mod m$ if and only if $r \equiv s \mod t$.

Proof. Suppose that $a^r \equiv a^s \mod m$ and that $r \geq s$ without loss of generality. Thus, $a^{r-s} \equiv 1 \mod m$. From Theorem 10.1, we have that $r - s$ is a multiple of t. By the definition of a modulo, this gives us that $r \equiv s \mod t$.

To prove the converse, suppose that $r \equiv \mod t$. Then $r = s + kt$ for some integer k, and

$$\begin{aligned} a^r &\equiv a^{s+kt} \mod m \\ &\equiv a^s \left(a^t\right)^k \mod m \\ &\equiv a^s \mod m \end{aligned}$$

□

Definition : Primitive Roots

If a is the least residue and the order of a modulo m is $\phi(m)$, we will say that a is a primitive root of m.

Theorem : (10.5)

If g is a primitive root of m, then the least residues of

$$g, \qquad g^2, \qquad \ldots, \qquad g^{\phi(m)}$$

are a permutation of the $\phi(m)$ positive integers less than m and relatively prime to m.

Proof. Since $(g, m) = 1$¡ each power of g is relatively prime to m. No two powers have the same least residue, because if $g^j \equiv g^k \mod m$, then Theorem 10.4 would give that

$$j \equiv k \mod \phi(m)$$

If $j \neq k \mod \phi(m)$, then $g^j \neq g^k \mod m$. □

Example

Show that 3 is a primitive root of 7.

Since 7 is prime, all elements modulo 7 are relatively prime to 7

$$\begin{aligned} 3^1 &\equiv 3 \mod 7, \\ 3^2 &\equiv 2 \mod 7, \\ 3^3 &\equiv 6 \mod 7, \\ 3^4 &\equiv 4 \mod 7, \\ 3^5 &\equiv 5 \mod 7, \\ 3^6 &\equiv 1 \mod 7 \end{aligned}$$

Therefore, 3 is a primitive root of 7.

Not every integer has a primitive roots. For example, 8 does not. We will show that each prime has a primitive root. If a has order t modulo m, then any power of a will have an order no larger than t, because for any k,

$$\begin{aligned} \left(a^k\right)^t &\equiv \left(a^t\right)^k \mod m \\ &\equiv 1 \mod m \end{aligned}$$

Lemma : (10.1)

Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k,t) = 1$.

Proof. Suppose that $(k,t) = 1$ and denote the order of a^k by s.

$$\begin{aligned} 1 &\equiv \left(a^t\right)^k \mod m \\ &\equiv \left(a^k\right)^t \mod m \end{aligned}$$

Therefore, by Theorem 10.1, it follows that $s \mid t$. Since s is the order of a^k, we have that

$$\begin{aligned} 1 &\equiv \left(a^k\right)^s \mod m \\ &\equiv a^{ks} \mod m \end{aligned}$$

Therefore, by Theorem 10.1, it follows that $t \mid ks$. Since $(k,t) = 1$, it follows that $t \mid s$. However, since $s \mid t$, this implies that $s = t$. Therefore, a^k has order $s = t$ as desired.

Suppose that a and a^k have order t, where $(k,t) = r$. Then,

$$\begin{aligned} 1 &\equiv a^t \mod m \\ &\equiv \left(a^t\right)^{k/r} \mod m \\ &\equiv \left(a^k\right)^{t/r} \mod m \end{aligned}$$

Theorem 10.1 gives $t \mid r$ is a multiple of t which implies that $r = 1$. $\square$

Corollary : (10.2)

Suppose that g is a primitive root of p. Then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.

Example

Find all primitive roots of 10.

First, we have that $\phi(10) = 4$, so a primitive root will have order 4.

$$\begin{aligned} 3^2 &= 9 \mod m \\ 3^3 &= 7 \mod m \\ 3^4 &= 1 \mod m \end{aligned}$$

Therefore, by Lemma 10.1, the primitive roots of 10 are:

$$3^1 \equiv 3 \mod 10, \qquad 3^3 \equiv 7 \mod 10$$