Primitive Roots

Nicholas Wendt

November 18, 2025

1 Recall

Remember that $\mathbb{Z}_n^*$ is a set containing all numbers less than n that are relatively prime to n. In other words, $a \in \mathbb{Z}_n^*$ if $gcd(a, n) = 1$.

2 Euler's Theorem

For any element $a \in \mathbb{Z}_n^*$, consider the sequence of powers of a: $1, a, a^2, a^3, ...\ (mod\ n)$.
Since the set $\mathbb{Z}_N^*$ is closed under multiplication, all these powers of $a\ (mod\ n)$ are also in the set.
It follows, by Euler's theorem, that the sequence of powers eventually repeats.

$$a^0 \equiv 1 \equiv a^{\phi(n)}\ (mod\ n)$$

This is a characteristic of primitive roots. Primitive roots are elements in $\mathbb{Z}_n^*$ such that the sequence of powers has a minimum period of $\phi(n)$.

This minimum period is known as the **order** of a. For all primitive roots $a \in \mathbb{Z}_n^*$, the order of a is $\phi(n)$.

For any primitive root $g(modn)$, the elements i

2.1 Existance of Primitive Roots

Primitive roots exists mod n if and only if n is of the form $2, 4, p^k, 2p^k$ for any odd prime p.

3 Tricks

If you have a primitive root $g\ (mod\ n)$ then any other element g^r where $gcd(r, \phi(n)) = 1$ is also a primitive root.
If you suspect g is a primitve root $mod\ p$ then you check $g^{\frac{(p-1)}{q}} \not\equiv 1\ (mod\ p)$ for every prime divisor, q, of $p - 1$. If none of these powers of g are equivilant to $1\ (mod\ p)$ then g is a primitive root.

Once you know one primitive root, g, then all other primitive roots are of the form g^r where $gcd(r, \phi(n)) = 1$.

3.1 Example