

Primitive Roots

Definition: Let p be a prime. A positive integer $r < p$ is called a *primitive root* modulo p if the order of $[r]_p$ in \mathbb{Z}_p^\times is $p - 1$. In other words, r is a primitive root modulo p if $[r]_p$ is a generator of the cyclic group \mathbb{Z}_p^\times .

Yet another way to say this is that r is a primitive root modulo p if the function $\phi: \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^\times$ given by $\phi(n[1]_{p-1}) = [r]_p^n$ is an isomorphism.

Examples:

1) \mathbb{Z}_{23}^\times

2) \mathbb{Z}_{47}^\times

3) \mathbb{Z}_{71}^\times

Open Questions:

1) Is 2 a primitive root for infinitely many primes? (It's a famous conjecture that the answer here is yes.)

2) Is 10 a primitive root for infinitely many primes? (Gauss made the conjecture that the answer here is yes.)

3) If n isn't a perfect square, is it a primitive root for infinitely many primes? (E. Artin made the conjecture that the answer here is yes.)

If you can answer any of these questions, you'll be famous (at least amongst mathematicians).