

Elementary Number Theory: Primate Roots and Indices

Arjun Vardhan

†

Created: 17th May 2022

Last updated: 17th May 2022

1 The Order of an Integer Modulo n

- Let $n > 1$ and $\gcd(a, n) = 1$. The order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

2 Primitive Roots for Primes

3 Composite Numbers with Primitive Roots

4 The Theory of Indices