THE MULTIPLICATIVE ORDER

PIETER MOREE

Abstract

The invertible residue classes modulo n, $(Z/nZ)^*$, from a group of exponent $\lambda(n)$, the Carmichael function. An element g of order $\lambda(n)$ is said to be a primitive λ-root. In case n is a prime we have $\lambda(n) = n-1$ and an element g of that order is said to be a primitive root.

Despite the simplicity of the notion of multiplicative order, our understanding of it is rather poor. I will give a survey on this topic, with special focus on my own contributions over the years and address such questions as how often the order is maximal, how often it is even, and consider equidistribution (or lack thereof) of the order. In most case we fix g, and let n run through the prime numbers.