

Anatomy of Euler's function and its friends

Carl Pomerance
`carl.pomerance@dartmouth.edu`
Dept. of Mathematics
Dartmouth College
6188 Bradley Hall
Hanover, NH 03755-3551
USA

Abstract

For essentially my entire career I have been fascinated by the Euler function and its close friends the Carmichael function and the multiplicative-order function. There are specific applications to cryptography, such as the RSA cryptosystem and periods of pseudorandom number generators, as well as applications to primality testing, radical Galois extensions, ranks of elliptic curves, etc. And there are problems that might be considered purely recreational. This talk will discuss a few problems and results taken from some recent papers with Banks, Friedlander, Kurlberg, Li, Luca, Martin, Shparlinski, and others.