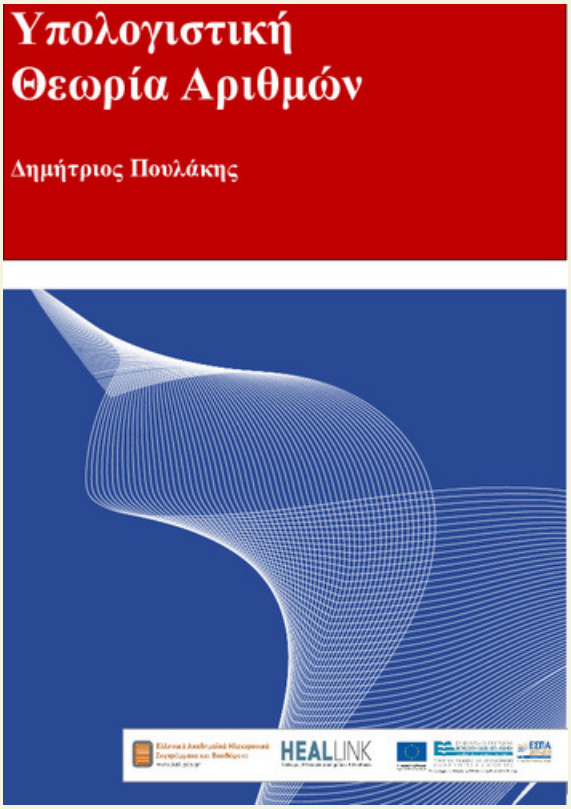

METADATA

Title: Computational Number Theory

Other Titles: -

Language: Greek

ISBN: 978-960-603-127-4

Subject: MATHEMATICS AND COMPUTER SCIENCE

Keywords: Computational Number Theory / Cryptography

Bibliographic Reference: Poulakis, D. (2015). Computational Number Theory [Undergraduate textbook]. Kallipos, Open Academic Editions. http://dx.doi.org/10.57713/kallipos-323

Abstract

The last thirty years, Number Theory has been applied in many areas of Science and Technology, as Cryptography, Coding Theory, etc. This book is an introduction to Number Theory with emphasis in its computational aspect. Its aim is to give the necessary tools for the understanding of the contemporary applications of Number Theory. The necessary knowledge for the study of the book is that of secondary education. In the first chapter, the divisibility of integers is studied and an elementary introduction to the algorithms of integers is given. Further, the Euclidian algorithm is analysed. The second chapter is devoted to continuous fractions and their properties.

In the third chapter, the prime numbers are studied, some classical theorems on their distributions are proved and some special classes of prime numbers are presented. The basic properties of algebraic structures, monoids, groups, rings and fields, as well as polynomials are given in the fourth chapter. The fifth chapter, is devoted to the congruence relations of integers and their properties. Further,

the linear congruences, the primitive roots, the symbols of Legendre and Jacobi are studied. Moreover, the solution of quadratic congruences is studied. Finally, the finite fields are introduced. In the sixth chapter, some classical primality tests are given and the unique deterministe polynomial time algorithm AKS is analysed. The seven chapter deals with the integer factorization and some classical algorithm are presented. Finally, the last chapter is devoted to the discrete logarithm problem and some algorithm for the computatin of discrete algorithm are given.

The Project is funded by the National Development Programme 2021-2025 of the Ministry of Education and Religious Affairs and implemented by the Special Account for Research Funds of the National Technical University of Athens and the Hellenic Academic Libraries Link.