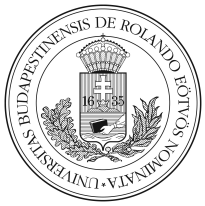
Computational Number Theory

Katalin Gyarmati

katalin.gyarmati@ttk.elte.hu

Eötvös Loránd University

University Note



Institute of Mathematics - Faculty of Science - ELTE TTK

2022

Contents

1 Introduction

This note summarizes some of the most important results in a current number theory topic that is also connected to cryptography and computers. It analyzes the time required for fundamental operations, but it also studies speedy multiplication (FFT algorithm). It delves into some significant historical chapters in cryptography. It contains a thorough analysis of number theory techniques related to known and popular encrypting algorithms. Thus, it outlined some of the potential risks in the case of careless RSA implementations, for example (far beyond the fact that the two primes used in RSA may not be close to each other or beyond the relationship to factorization problems). It investigates modern methods for solving the discrete logarithm problem (I remark here that these algorithms are quite slow). Basic primality tests and certain factorization techniques are also discussed in this note. It also provides insight into a modern approach to pseudorandom generation.

The following two books serve as the foundation for the majority of the course: Neal Koeblitz, A Course in Number Theory and Cryptography, Springer, 1994, Abhijit Das, Computational Number Theory, CRC Press, 2013. The section about cryptography in history is mostly relied on Wikipedia articles. Besides from the abovementioned, the note is based on a variety of other literature. The complete bibliography can be found at the end of each chapter.