

On the Complexity of Integer Factorization and Related Problems

This thesis concerns the integer factorization problem, which is the task to compute the prime factorization of natural numbers. It consists of two parts and four original research papers. In the first part, we refine known methods for integer factorization and also establish novel techniques. Our results lead to improvements of the best known deterministic and rigorous runtime complexity bounds. In the second part, we study the relations between integer factorization and other computational problems. As main topics, two tasks are introduced: computing an extension of Jacobi's symbol and evaluating the iterates of exponential functions modulo natural numbers. We then show that several hard algorithmic challenges in the periphery of integer factorization may be reduced to these problems.