Integer factoring towards the number field sieve

Jana Sotáková

February 25 2015

Abstract

The security of the widely used RSA cryptosystem depends on our inability to factor large integers. The fastest algorithm for factorization currently available is the number field sieve. It is of sub-exponential complexity and it is sensitive to the size of the number to be factored and not of the factors.

We shall introduce the general ideas behind integer factoring by the method of congruent squares and show how we can exploit the arithmetic of number rings to construct desired squares. One of the important aspects is the process of sieving, so we will define the notion of a smooth number and try to understand the reasons that make the number field sieve so fast.