Integer Factorization

Miska Kananen

November 29, 2018

Contents

1 Introduction

We will define the problem of integer factorization and present some applications for efficient factorization. Then we will look at some trivial and some more efficient factorization algorithms, namely Pollard's Rho algorithm and the linear sieve, and implement them in practice.

1.1 The definition

Definition 1.1. (Integer Factorization problem) Let n be a positive integer. Find an integer a $(1 < a < n)$ such that $n = ab$ for some positive integer b or report that such integer does not exist. We call a a *factor* of n and the product ab a *factorization* of n.

If there exists a factorization of n, n is *composite*. Otherwise n is *prime* (or equals 1, in case of which it is neither). Note that it is not required a to be prime.

Example 1.2. (Factorization) Let $n = 36$. We can write $n = 4 \cdot 9$. Here 4 is a factor of 36 and the product $4 \cdot 9$ is a factorization of 36.

1.2 Applications

2 Trivial algorithms

3 Pollard's Rho algorithm

4 Linear sieve

5 References