Quadratic Sieve In Rust

Nils Olsson

April 15, 2021

Contents

1 Introduction **1**

2 Details **2**

3 Notes **2**

3.1 Legendre symbol 2

3.2 Quadratic residue 2

Resources

- `https://www.researchgate.net/publication/266239994_Factoring_Integers_With_Large_Prime_Variations_of_the_Quadratic_Sieve`

1 Introduction

Factorizing integers is an age-old problem stemming from the fundamental theorem of arithmetic: that every positive integer has a unique prime factorization. Numerical number theorists have for centuries endeavoured to construct faster factoring algorithms; one such algorithm developed within the last several decades is the *quadratic sieve*.

> The quadratic sieve algorithm (QS) is an integer factorization algorithm and, in practice, the second fastest method known (after the general number field sieve). It is still the fastest for integers under 100 decimal digits or so, and is considerably simpler than the number field sieve. It is a general-purpose factorization algorithm, meaning that its running time depends solely on the size of the integer to be factored, and not on special structure or properties. It was invented by Carl Pomerance in 1981 as an improvement to Schroeppel's linear sieve [1].

[1] `https://en.wikipedia.org/wiki/Quadratic_sieve`

2 Details

Given n a composite integer that is not a prime power.

- Factor base $S = \{p_1, p_2, \ldots, p_t\}$ where $p_1 = -1$ and p_j for $j \geq 2$ is the $(j-1)^{\text{th}}$ odd prime p for which n is a quadratic residue modulo p.
- $m = \lfloor \sqrt{n} \rfloor$
- Collect $t+1$ pairs (a_i, b_i) via an x chosen in the order $0, \pm 1, \pm 2, \ldots$ satisfying $a_i^2 = (x+m)^2 \equiv b_i \pmod{n}$.

3 Notes

3.1 Legendre symbol

A multiplicative function with values 1, 1, 0 that is a quadratic character modulo an odd prime number p: its value at a (nonzero) quadratic residue mod p is 1 and at a non-quadratic residue (non-residue) is 1. Its value at zero is 0

3.2 Quadratic residue

An integer q is called a *quadratic residue* modulo n if it is congruent to a perfect square modulo n; i.e., if there exists an integer x such that:

$$x^2 \equiv q \pmod{n}.$$

Otherwise, q is called a *quadratic non-residue* modulo n.