Project 4
Factoring

KG

March 5, 2024

1 Introduction

In this project, we will implement some factoring algorithms and attempt to factor a collection of integers.

2 Tasks

You will write a report using LaTeX. The report should include an explanation of what you have done, a description of your implementation, the theoretical analysis, any experimental results with explanations and a code listing.

For this project, you should probably rely on any linear algebra libraries available to you.

1. Implement: Random Squares Implement the random squares factoring algorithm.

2. Implement: Quadratic Sieve

a. Quadratic Sieve Implement a quadratic sieve factoring algorithm.

b. Optional: Multiple Polynomial Quadratic Sieve Implement a multiple polynomial variant of the quadratic sieve.

3. Optional: Implement: Special Number Field Sieve Implement a simple variant of the special number field sieve factoring algorithm.

4. Run: Factor Brillhart and Selfridge [1] were interested in factoring numbers of the form $2^n - 1$, n prime, and they list some results in Table 1 of their paper. Using your implemented factoring algorithms, redo as much of their factorisation results as you can. If you can, also factor numbers for larger prime n.

Plot the runtime cost of factoring with respect to n for the implemented factoring algorithms.

Also report the number of small primes used for each factoring algorithm. You may use a theoretical argument to determine the number of small primes used, or you may experimentally determine a better number.

References

[1] John Brillhart and J. L. Selfridge. Some factorizations of $2^n \pm 1$ and related results. *Mathematics of Computation*, 21(97):87–96, 1967.