Assignment 2: Implementing the Quadratic Sieve Algorithm

COL 759

October 3, 2024

Objective

The objective of this assignment is to implement the Quadratic Sieve algorithm for integer factorization.

Background

The Quadratic Sieve is an efficient algorithm used for factoring large integers. It operates by finding a set of integers whose squares yield a congruence relation modulo the integer to be factored. Understanding this algorithm is crucial for applications in cryptography and number theory.

Requirements

1. Implement the Quadratic Sieve algorithm in your preferred programming language.
2. For proper implementation of the quadratic sieve, please refer to the instructor slides uploaded on Moodle.
3. Use GMP (The GNU Multiple Precision Arithmetic Library) to handle large numbers.
4. Use MPI (Message Passing Interface) to parallelize the sieving part (most time consuming part).
5. Your solution should work for a number of 40 digits (min).We will test your code on 40 to 50 digit numbers.
6. MPI is for exchanging messages between multiple computers running a parallel program across distributed memory. It can also be implemented on single machine/laptop.

Test Cases

You are required to test your implementation with the following integers:

1. **Test Case 1:** Factor $n = 4989946632961011398013054652770320107828892 09$
   Expected Factors: $87759159388901824645049, 5685955366605355947841$
2. **Test Case 2:** Factor $n = 124344460248800821609915419756074284627 3$
   Expected Factors: $35562909150545131919, 34964648061390328367$
3. **Test Case 3:** Factor $n = 1599408916357846066637584352000419075033$
   Expected Factors: $66594097240380558977, 24017277546154871129$

Submission Guidelines

- Submit your code along with a report detailing your approach in a zip file.
- **Deadline : 18th October 2024 23:59**
- Plagiarism i.e. similarity (more than 15 %) with any part of the code available in the internet or similarity of code of two different students will lead to heavy penalty (may be F grade in the course or -10 marks).
- 5% marks will be deducted for each day late submission; after a week, you will get zero.