Factorization Project – EDIN01

Mats Rydberg, dt08mr7
Christina Schmidt, dt08cs6

November 15, 2012

Exercise 1

We have a computational power $C = 10^6$ operations per second and we wish to naively try to factor a number N of order 10^{25}. This is done by performing the operation $N \bmod p$ order of $\sqrt{N}$ number of times. The time t this will take can be calculated as

$$t = \frac{\sqrt{N}}{C} \approx \frac{10^{12}}{10^6} = 10^6 \text{ s} = 11 \text{ days } 13 \text{ h } 46 \text{ min and } 40 \text{ s}$$

This is of course not really feasible.

Exercise 2

In this task we implement a simplified version of Quadratic Sieve, following the guidelines in the project description. The number N that we will try to factor is given as

$$N = 106565238310234107615313 > 10^{24}$$

Program

The program is written in Java and is made up by four classes:

- `Main.java` which contains our main method and interacts with the user.
- `Factorization.java` which includes the basic methods for doing actual factoring of numbers.
- `Matrix.java` which is a wrapper for a primitive Java matrix and contains functionality for creating one that suits our needs.
- `XandY.java` which computes the values x and y such that $x^2 = y^2 \bmod N$ after the gaussian elimination step has been completed.

The program uses the `GaussBin` program provided for conducting the gaussian elimination step, so we make use of three text files: `primes.file`, `matrix.out` and `gauss.out`. The first contains the first ~ 2000 primes from which we read the $|F|$ primes used for our factor base, the second is our matrix written to the format specified as input for `GaussBin` and the third is the output from `GaussBin`, used as input for our final step in the algorithm.

Solution

Our program solves the factoring of $N = p \cdot q$ in less than 780 seconds = 13 minutes, as $p =$ and $q =$ on a powerful PC[1], and does not finish in feasible time on a school computer[2].

[1] Intel i5-2500K, 16GB RAM, Windows 7

[2] AMD Athlon II X2 B26 3.2GHz, 3.45GB RAM, Linux Mint

Extra metrics

For extra goodies we provide a few extra metrics that we collected in the process of trying to optimize our program. They will make sense only in the context of the program itself.

```
text
```

Time spent on the project: 11 hours per person = 22 hours total