Factorization Project – EDIN01

Mats Rydberg, dt08mr7
Christina Schmidt, dt08cs6

November 9, 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