Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

8. Exercise sheet
Hand in solutions until Saturday, 31 May 2014, 23:59:59

Exercise 8.1 (The runtime of the GNFS). (6 points)

Prove that the general number field sieve on an integer N of bit-size n has an heuristic asymptotic complexity of $L_{1/3}(n)$ when we chose the degree d of the underlying polynomial $f \in \mathbb{Z}[x]$ optimally. More precisely, show that its complexity can be estimated as $\boxed{6}$

$$\exp(((64/9)^{1/3} + o(1))n^{1/3}(\log n)^{2/3}).$$

Hint: Employ Pomerance's theorem from the lecture and take the derivative with respect to d to find the minimum of the runtime function.

Exercise 8.2 (A magic device). (6 points)

In this exercise we will delve into a problem which relates nicely to the problem of integer factorization of a composite, odd number N. Suppose you have a magic device that computes in polynomial time (in the length of the integer N), given an element $a \in \mathbb{Z}_N^\times$, either one solution $b \in \mathbb{Z}_N^\times$ with $b^2 = a$ or tells you that no such solution exists. You have no control of the inner working of the device, i.e. if there are several solutions $b \in \mathbb{Z}_N^\times$ with $b^2 = a$, the device will pick one of them using a method unknown to you. Show how, armed with such a device, you can then factor integers in probabilistic polynomial time. Conversely, show how you can build such a device, if you can factor integers in polynomial time. $\boxed{6}$

Exercise 8.3 (ECM world records). (7 points)

Look at the following web-page:

```
http://www.loria.fr/~zimmerma/records/ecmnet.html
```

We will now explore this page in a little more detail.

(i) Report detailed which world records were set on the web-page and which purpose they serve. $\boxed{2}$

(ii) From the data given on the webpage, try to extrapolate in which calendar year we will be able to find a 90 digit factor using ECM. $\boxed{5}$