Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

9. Exercise sheet
Hand in solutions until Saturday, 14 June 2014, 23:59:59

Note the extended hand-in deadline.

Exercise 9.1 (A more detailed runtime analysis of the ECM). (5 points)

In the lecture we have done the runtime analysis of the ECM for factoring a composite integer N with $\gcd(N, 6) = 1$ and N not a perfect square. We found that for $B_1 = \exp(\mathcal{O}\left(\sqrt{\ln p \ln\ln p}\right))$ the runtime is $\exp(\mathcal{O}\left(\sqrt{\ln p \ln\ln p}\right))$. Show that more precisely for $B_1 = \exp((\sqrt{2}/2 + o(1))\sqrt{\ln p \ln\ln p})$ the runtime is [5]

$$\exp((\sqrt{2} + o(1))\sqrt{\ln p \ln\ln p}).$$

Exercise 9.2 (On the heuristic used for the ECM). (10 points)

Experiment with the heuristics used in the ECM. For which primes p and bounds y will you have that the probability of a randomly selected integer up to x to be y smooth is roughly the same as the probability of a randomly selected integer from the Hasse interval $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$? Report detailed on your results. [10]

Exercise 9.3 (The elliptic curve method). (10+25 points)

We now put hands on the elliptic curve method.

(i) Implement the elliptic curve method (stage 1) in a programming language of your choice. [10]

(ii) Perform experiments! Play with your implementation and try to factor some large integers which would be out of reach when using the GNFS only. Some numbers from the Cunningham project might be interesting. [+5]

(iii) Take part in the Cunningham project given on the ECM world records page by running ECM factorizations using `libecm`! Report on your findings. For this task you have time till Saturday, 19 July 2014. [+20]