Cryptography I, winter 2005/06

JOACHIM VON ZUR GATHEN, MICHAEL NÜSKEN

6. Exercise sheet
Hand in before Monday, 2005/12/12, 14^{00} in b-it 1.22.

Exercise 6.1 (Pollard's ρ method). (7 points)

(i) Fill in the table below, which represents a run of the algorithm for $N = 132\,659 = 53 \cdot 2503$ and the initial value $x_0 = 222$, up to $i = 10$. $\boxed{3}$

i	x_i rem N	x_i rem 53	y_i rem N	y_i rem 53	$\gcd(x_i - y_i, N)$
0	222	10	222	10	N
1	...	...	...	...	...

(ii) The smallest prime divisor of N is 53. Describe the idea behind the algorithm by taking a look at x_i rem 53 and y_i rem 53. $\boxed{4}$

Exercise 6.2 (Dixon's random squares). (9+1 points)

(i) You find a complete implementation of Dixon's random squares method on the course homepage. Put in comments that explain what the various steps are doing. Add `userinfo` commands to produce a human understandable execution summary (useful for the next parts of this exercise). $\boxed{4}$

(ii) Find a factor of $N = 1517 = 37 \cdot 41$ using Dixon's random squares method. Choose $B = 5$ and execute the algorithm step by step. $\boxed{2}$

(iii) For $N = 1\,845\,314\,859\,041$ compute the value $B = \exp(\sqrt{\ln N \ln \ln N})$ used in the course as well as the promised value $B = \exp(\sqrt{\frac{1}{2} \ln N \ln \ln N})$. $\boxed{1}$

(iv) Factor $N = 1\,845\,314\,859\,041$ using Dixon's random squares method. Choose $B = 320$. Hand in a protocol of a (possibly unsuccessful) attempt that does not find a factor ahead of time. Give a short comment about what has happened. $\boxed{2}$

(v*) Measure the cpu time of the previous step and compare with the cpu time MuPAD's own factoring algorithm `ifactor` uses. Explain. *Hint*: Consider `expose` to explain. $\boxed{+1}$

Exercise 6.3 (Dixon's random squares). (0+4 points)

(i) Let $N = q_1 q_2 \cdots q_r$ be odd with pairwise distinct prime divisors q_i and $r \geq 2$. Show: The equation $x^2 - 1 = 0$ has exactly 2^r solutions in $\mathbb{Z}_N^\times$. $\boxed{+3}$

Hint: Use the Chinese remainder theorem.

Note: The claim is also true, if the q_i are pairwise distinct prime powers. To see this you have to know that also for prime powers q the equation $x^2 - 1 = 0$ has exactly 2 solutions in $\mathbb{Z}_q$.

(ii) If s, t are random elements of $\mathbb{Z}_N^\times$ satisfying $s^2 \equiv t^2 \bmod N$, then the probability for $s \not\equiv \pm t \bmod N$ is at least $1 - \frac{1}{2^{r-1}}$. $\boxed{+1}$