Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

6. Exercise sheet
Hand in solutions until Saturday, 17 May 2014, 23:59:59

Exercise 6.1 (Dixon's random squares). (6 points)

Find a factor of $N = 1517$ using Dixon's random squares method.

(i) Choose $B = 7$ and complete the following table. $\boxed{3}$

i	b	b^2 rem N	Factorization	α	$\alpha \mod 2$
0	141	160	$2^5 \cdot 5$	$(5, 0, 1, 0)$	$(1, 0, 1, 0)$
1	243	1403	$23 \cdot 61$	–	–
2	1071	...	...	...	...
3	529	...	...	...	...
4	1174	...	...	...	...

(ii) Find a linear combination of the α's that is the zero vector in $\mathbb{Z}_2$. $\boxed{2}$

(iii) Compute the corresponding x and y. Can you compute the factorization of N? $\boxed{1}$

Exercise 6.2 (A probability estimate). (6 points)

Let N be odd with $r \geq 2$ distinct prime factors and $x \xleftarrow{\text{⚄}} \mathbb{Z}_N^\times$ of order k.

(i) Show that $\text{prob}\,(k \text{ even}) \geq 1 - 2^{-r} \geq 3/4$. Hint: Chinese remainder theorem. $\boxed{3}$

(ii) Prove that under the condition that k is even, we have $x^{k/2} \in \sqrt{1} \setminus \pm 1$ with probability $1 - 1/(2^r - 1) \geq 2/3$. $\boxed{3}$

Exercise 6.3 (Finding a suitable polynomial for the GNFS). (3+4 points)

In the lecture we claimed that when we try to find a monic polynomial $f \in \mathbb{Z}[x]$ of suitable degree d (depending on N) that then the m-ary expansion of N for $m = \lfloor n^{1/d} \rfloor$ will lead us to such a polynomial. You task is to prove this.

(i) Show that if $N \geq 64$ and $m = \lfloor N^{1/3} \rfloor$, then we have $N < 2m^3$. 2

(ii) More generally, show that if $N > 1.5(d/\ln 2)^d$ and $m = \lfloor N^{1/d} \rfloor$, then we +4
have $N < 2m^d$.

1 (iii) Conclude that the construction from the lecture indeed produces a monic polynomial $f \in \mathbb{Z}[x]$.

Exercise 6.4 (On the homomorphism used in the GNFS). (4 points)

4 Let $f \in \mathbb{Z}[x]$ be any irreducible, monic polynomial and let $\alpha \in \mathbb{C}$ be any root of it. Furthermore assume we have an integer $m \in \mathbb{Z}$ such that $f(m) = 0$ in $\mathbb{Z}_N$. Show that the map $\varphi\colon \mathbb{Z}[\alpha] \to \mathbb{Z}_N$ that maps α to the residue class of m in $\mathbb{Z}_N$ is a homomorphism of rings.