Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

7. Exercise sheet
Hand in solutions until Saturday, 24 May 2014, 23:59:59

Exercise 7.1 (On the norm). (6 points)

Let $f \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree $d > 1$ and let $\alpha \in \mathbb{C}$ be a root of it. In the lecture we have defined the norm $N(\beta)$ of an algebraic element $\beta \in \mathbb{Q}(\alpha)$ as the product of all conjugates of β.

(i) Prove that the norm is multiplicative, i.e. for $\beta, \beta' \in \mathbb{Q}(\alpha)$ we have $N(\beta\beta') = N(\beta)N(\beta')$. $\boxed{3}$

(ii) Prove that the norm is rational, i.e. that for $\beta \in \mathbb{Q}(\alpha)$ we have $N(\beta) \in \mathbb{Q}$. Hint: Consider the conjugation of the values of the norm. $\boxed{3}$

Exercise 7.2 (An example run of the simplified GNFS). (16 points)

We will now put hands on the simplified version of the GNFS presented in the lecture.

(i) As a first start, suppose $N = 4189$ and use the setup $m = 29$. Write down the polynomial f resulting from the base m representation of N and use it to directly factor N. $\boxed{2}$

Now, let's run the simplified number field sieve for $N = 145$. We employ the polynomial $f(x) = x^2 + 1$ and $m = 12$. Thus, we work in the number ring $\mathbb{Z}[i]$ with $i^2 = -1 \in \mathbb{Z}$. Furthermore, we choose the smoothness bound $B = 10$.

(ii) Verify that $f(m) = 0$ in $\mathbb{Z}_N$. $\boxed{1}$

(iii) Write down how the exponent vectors $v_{(a,b)}$ corresponding to relations for integers $a, b \in \mathbb{Z}$ look like. Hint: The exponent vector is the concatenation of the vector (of length three) for the algebraic side and the vector (of length four) on rational side. $\boxed{3}$

The sieving procedure found the following exponent vectors $v_{(a,b)}$:

$$\begin{aligned} v_{(2,1)} &= [0,1,0,1,0,1,0] \\ v_{(3,1)} &= [1,0,1,0,0,0,0] \\ v_{(7,1)} &= [1,0,0,0,0,1,0] \\ v_{(1,3)} &= [1,1,0,0,0,1,1] \\ v_{(4,3)} &= [0,0,0,1,0,0,0] \\ v_{(3,4)} &= [0,0,0,0,0,1,0] \\ v_{(24,7)} &= [0,0,0,0,1,1,0] \end{aligned}$$

$\boxed{2}$ (iv) Construct one further vector corresponding to $(a,b) = (9,13)$.

$\boxed{2}$ (v) Find a subset S of the rows of the matrix that sum up to zero. Hint: Linear algebra over $\mathbb{F}_2$!

$\boxed{2}$ (vi) Compute the rational square $v^2 = \prod_{(a,b)\in S}(a - bm)$. Also compute v.

$\boxed{2}$ (vii) On the algebraic side you should have found the element

$$\gamma^2 = \prod_{(a,b)\in S} (a - bi) = -5000 - 3750i.$$

Verify that its square root in $\mathbb{Z}[i]$ is $\gamma = 25 - 75i$. Also compute the integer $u = \varphi(\gamma)$.

$\boxed{2}$ (viii) You obtained a congruence of squares now. Can you compute the factorization of N?