Approximate common divisor problem and lattice sieving

Kirill Zhukov

TVP Laboratories

6th Workshop on Current Trends in Cryptology
CTCrypt 2017

Part I: Lattice Sieving

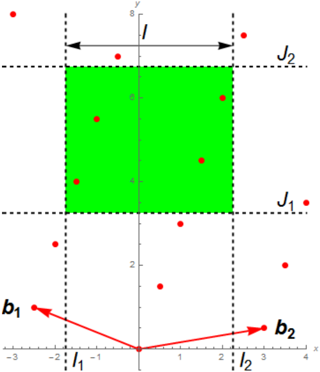
For $\mathbf{B} = \binom{\mathbf{b}_1}{\mathbf{b}_2} \in \mathbb{Z}_{2,2}$ and $l_1, l_2, J_1, J_2 \in \mathbb{Z}$ we define:

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{b_1}x + \mathbf{b_2}y \mid x, y \in \mathbb{Z}\},$$

$$\mathcal{R}(l_1, l_2, J_1, J_2) = \left\{\mathbf{v} \in \mathbb{R}^2 : \binom{l_1}{J_1} < \mathbf{v} < \binom{l_2}{J_2}\right\},$$

$$\mathcal{S}(l_1, l_2) = \left\{\mathbf{v} \in \mathbb{R}^2 \mid l_1 < \mathbf{v}^{(1)} < l_2\right\},$$

$$\mathcal{LS}(\mathbf{B}, l_1, l_2) = \mathcal{L}(\mathbf{B}) \cap \mathcal{S}(l_1, l_2).$$



We say $\mathbf{B} = \binom{\mathbf{b_1}}{\mathbf{b_2}} \in \mathbb{Z}_{2,2}$ is FK-reduced with parameter $l \in \mathbb{Z}_{>0}$ if:

1) $-l < \mathbf{b_1}^{(1)} \leq 0$ and $0 \leq \mathbf{b_2}^{(1)} < l$,
2) $\mathbf{b_1}^{(2)} > 0$ and $\mathbf{b_2}^{(2)} > 0$,
3) $\mathbf{b_2}^{(1)} - \mathbf{b_1}^{(1)} > l$.

Part I: Lattice Sieving

Algorithm (Next lattice point with step D)

Require:

$l_1, l_2 \in \mathbb{Z} : l_1 < l_2$,

$\mathbf{B} \in \mathcal{FK}_{l_2 - l_1}(\mathbb{Z}_{2,2})$,

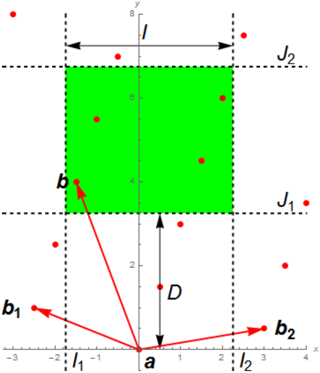
$\mathbf{a} \in \mathcal{LS}(\mathbf{B}, l_1, l_2)$,

$D \in \mathbb{Z}$

Ensure:

$\mathbf{b} \in \mathcal{LS}(\mathbf{B}, l_1, l_2) : b^{(2)} = \min M$,

$M = \{c^{(2)} \mid \mathbf{c} \in \mathcal{LS}(\mathbf{B}, l_1, l_2), c^{(2)} > a^{(2)} + D\}$



- The algorithm from the original paper of J. Franke and T. Kleinjung outputs a wrong vector for some inputs
- We prove the correctness of our version of algorithm in full paper

Part II: Partially approximate common divisor problem

PACDP (N. Howgrave-Graham):

Let $\Delta < A < N$ be fixed naturals. For every input $N_1, N_2 \in \mathbb{N}$ with $N_1 < N$ find all $a \in \mathbb{N}$ ($a < A$) and $\delta \in \mathbb{Z}$ ($|\delta| < \Delta$) such that

$$N_1 = ab_1 \quad \text{and} \quad N_2 = ab_2 + \delta$$

for some $b_1, b_2 \in \mathbb{N}$.

- PACDP is hard if Δ and A are close
- PACDP is hard if $A < \sqrt{N}$

PACDP relates on Implicit Factoring (A. May, M. Ritzenhofen):

Given RSA moduli $N_1 = p_1 q_1$, $N_2 = p_2 q_2$. The goal is to factor N_1 and N_2 provided $|p_1 - p_2|$ is small.

Part II: PACDP - Short vector approach

Every solution of PACDP satisfies inequalities:

$$-\frac{N_1\Delta}{A} < -N_2 b_1 + N_1 b_2 < \frac{N_1\Delta}{A}$$
$$0 < b_1 < \frac{N_1}{A}$$

Denote $\mathbf{B} = \begin{pmatrix} -N_2 & \Delta \\ N_1 & 0 \end{pmatrix}$, $\mathbf{b} = (b_1, b_2)\mathbf{B}$. Then $\det(\mathbf{B}) = N_1\Delta$, $\|\mathbf{b}\| < \frac{\sqrt{2}N_1\Delta}{A}$.

If $A > \sqrt{N\Delta}$, then $\|\mathbf{b}\| < \sqrt{2}\det(\mathbf{B})^{1/2}$, i.e. $\mathbf{b}$ is a short vector of $\mathcal{L}(\mathbf{B})$

We solve SVP for $\mathcal{L}(\mathbf{B})$ using $O(n \lg^2 n \lg\lg n)$ bit operations.

What if $A > \sqrt{N\Delta/c}$ for some $c \in \mathbb{N}$?

We solve c pieces of SVPs using $O(cn \lg^2 n \lg\lg n)$ bit operations.

Part II: PACDP - Integer inequalities approach

Every solution of PACDP satisfies inequalities:

$$-\frac{N_1\Delta}{A} < -N_2 b_1 + N_1 b_2 < \frac{N_1\Delta}{A}$$
$$0 < b_1 < \frac{N_1}{A}$$

Denote $\mathbf{B} = \begin{pmatrix} -N_2 & 1 \\ N_1 & 0 \end{pmatrix}$, $\mathcal{R} = \mathcal{R}(-\frac{N_1\Delta}{A}, \frac{N_1\Delta}{A}, 0, \frac{N_1}{A})$.

Then $\det(\mathbf{B}) = N_1$, $\mathrm{Vol}(\mathcal{R}) = \frac{2N_1^2\Delta}{A^2}$.

If $A > \sqrt{N\Delta/c}$, then under Gauss Volume Heuristics the number of solutions is $\frac{\mathrm{Vol}(\mathcal{R})}{\det(\mathbf{B})} < 2c$

We solve the system with Franke-Kleinjung algorithm and check every solution for being a solution of PACDP using $O(cn \lg n \lg\lg n)$ bit operations.