Number theory in cryptography

– Exercise set 12 –

The exercises P12.1, P12.2 have to be handed in on Tuesday, 21st May 2024, 8:30 at latest.

Theoretical questions

T 12.1 Let L be an n-dimensional lattice. Prove that the determinant of the lattice defined for a $\mathbb{Z}$-basis $(v_1, \dots, v_n)$ of L as $\det(L) = |\det\begin{pmatrix} v_1 & v_2 & \dots & v_n \end{pmatrix}|$ is independent of the choice of the basis.

T 12.2 Given a (full-rank) "random" lattice $L \subset \mathbb{R}^n$, the Gaussian heuristic states that when n is large, we can expect the length $\lambda_1(L)$ of a shortest non-zero vector in L to be roughly of size

$$\lambda_1(L) \simeq \sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}. \tag{12.2.1}$$

The purpose of this exercise is to find an explanation for this heuristic[4]. Let $B_n(0,r) \subset \mathbb{R}^n$ denote the ball of radius $r > 0$ centered at the origin in n-dimensional space. Heuristically, for a (full-rank) lattice $L \subset \mathbb{R}^n$ and for large r it is reasonable to expect:

$$\#\{\, v \in L \;:\; \|v\| < r \,\} \approx \frac{\mathrm{vol}(B_n(0,r))}{\det(L)},$$

since $\det(L)$ is the volume of a *fundamental domain* for L (a bounded domain whose translates by vectors in L partition $\mathbb{R}^n$).

From this, derive the Gaussian heuristic by finding R such that $\frac{\mathrm{vol}(B_n(0,R))}{\det(L)} = 1$.

Hint: the volume of a ball is given by $\mathrm{vol}(B_n(0,r)) = \dfrac{\pi^{n/2}}{\Gamma(1+n/2)} r^n$ and you may use Stirling's approximation $x! := \Gamma(x+1) = (2\pi)^{1/2} x^{x+\frac{1}{2}} e^{-x} \big(1 + \mathcal{O}(x^{-1})\big)$ since $x = n/2$ is large here.

Programming exercises

P 12.1

a) Implement Gram–Schmidt reduction algorithm on SAGE.

b) Implement the LLL algorithm on SAGE as seen in class.

Test it on the lattices with $\mathbb{Z}$-basis $[(512, 1024), (271, 512)]$ and $[(314, 159, 265), (-27, 18, 28), (0, 1, 7)]$ respectively (and compare your results with SAGE pre-implemented LLL function[5]).

Hint: in SAGE, you may use `vector([x0, x1])`, which allows you to use the methods `v.inner_product(w)`, (or even `v * w`) and `v.norm()`, etc.

[4] This does not stand as a proof, since we did not even defined what we mean by "random" lattice here; this would require an important theorem proved by C. L. Siegel.

[5] Apparently SAGE only supports lattices $L \subset \mathbb{Q}^n$, while in principle LLL works fine for any lattice $L \subset \mathbb{R}^n$.

P 12.2 As seen in class, we can apply lattice reduction algorithms (as LLL) to a question in arithmetic. Given a prime number $p \equiv 1 \pmod 4$, it is known that there are integers $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ (Fermat's two squares theorem).

First, we find[6] $\alpha \in \mathbb{Z}$ such that $\alpha^2 \equiv -1 \pmod p$ and then we consider the lattice $L = \langle (p, 0), (\alpha, 1) \rangle$.

By running the LLL algorithm on L, find integers a, b such that $p = a^2 + b^2$ where $p = 10^{100} + 949$.

[6] The existence of α follows from exercise T10.1. You may use a SAGE function to find α (it runs in time polynomial in $\log(p)$).