第四届（2019）全国高校密码数学挑战赛

赛题二

一、赛题名称：小整数解

二、赛题描述：

2.1 符号说明

$n,\ m,\ q$ 表示正整数，$\mathbb{Z}$ 表示整数集，$\mathbb{Z}_q$ 表示 $\mathbb{Z}$ 模 q 所构成的集合，$\mathbb{Z}^m$ 表示定义在 $\mathbb{Z}$ 上的 m 维（列）向量所构成的集合，$\mathbb{Z}_q^{n\times m}$ 表示定义在 $\mathbb{Z}_q$ 上的 $n\times m$ 阶矩阵所构成的集合。$\mathbb{R}$ 表示实数集，$\mathbb{R}^m$ 表示定义在 $\mathbb{R}$ 上的 m 维（列）向量所构成的集合。小写黑体字母表示向量，如 $\mathbf{x}\in\mathbb{Z}^m$，大写黑体字母表示矩阵，如 $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$。$\|\mathbf{x}\|=\sqrt{x_1^2+x_2^2+\cdots+x_m^2}$ 表示向量 $\mathbf{x}$ 的长度。

2.2 基础知识

设 $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_m\in\mathbb{R}^m$ 是 m 个线性无关的向量，由 $\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_m$ 的所有整系数线性组合构成的集合称为一个格，记作

$$\mathcal{L}(\mathbf{B})=\left\{\sum_{i=1}^{m}z_i\mathbf{b}_i:\ z_i\in\mathbb{Z}\right\}$$

其中矩阵 $\mathbf{B}=(\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_m)$ 称为格 $\mathcal{L}(\mathbf{B})$ 的一组基。

格上的最短向量问题（Shortest Vector Problem, SVP）定义为，给定格 $\mathcal{L}(\mathbf{B})$ 的一组基 $\mathbf{B}$，找出 $\mathcal{L}(\mathbf{B})$ 中最短向量 $\mathbf{v}$，即 $\forall\,\mathbf{w}\in\mathcal{L}(\mathbf{B}),\ \|\mathbf{w}\|\geq\|\mathbf{v}\|$。

2.3 问题描述

给定正整数 $0<n<m$、模数 q 以及均匀随机矩阵 $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$，求解 $\mathbf{x}\in\mathbb{Z}^m$ 满足：

- $\mathbf{A}\mathbf{x}=\mathbf{0}\bmod q$
- $\|\mathbf{x}\|\leq\sqrt{m}$

例如，$n=2,\ m=4,\ q=11,$

$$\mathbf{A} = \begin{bmatrix} 1 & -3 & 6 & 4 \\ 3 & 5 & 2 & -5 \end{bmatrix} \in \mathbb{Z}_{11}^{2\times 4},$$

则 $\mathbf{x} = (1,0,1,1)^t$ 是该实例的一个解。挑战问题的参数设置请参见附件：小整数解问题数据文件.txt。

2.4 成绩评判

1. 参赛者在报告摘要中明确列出每个问题实例的解；在报告正文中详细描述每个问题实例的求解方法。

2. 引用前人的方法需在解题报告中明确指出，否则内容作废。

3. 每个问题实例仅需给出一个正确解 $\mathbf{x}$，$\|\mathbf{x}\|$ 越小，得分越高。

三、密码学背景及相关问题的研究进展

量子计算对传统公钥密码（基于大数分解和离散对数问题）的威胁以及近些年量子计算机的飞速发展，使得“后量子密码”（能够抵抗量子攻击的密码体制）成为学术界和产业界的热门研究领域。格公钥密码以其特有的优势一直以来都是后量子密码中最受人们关注的一类密码体制。

SIS 问题由 Ajtai 于 1996 年提出。根据格的定义，一个 SIS 问题实例的全体解正好构成了一个格

$$\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\}$$

因此，求解 SIS 问题实例等价于求解相应格 $\Lambda^{\perp}(\mathbf{A})$ 上的 SVP。

SVP 是格上最重要、最基础的问题之一。求解 SVP 的算法分为精确算法和近似算法两类。精确算法可以找到格上最短向量；近似算法能输出一个长度小于某个界的非零短向量。实际上这两类算法互为补充：一方面，近似算法需要调用低维的精确算法作为子程序，不同维数的低维格对应不同的近似因子和时间复杂度；另一方面，精确算法需要调用近似算法进行预处理，预处理的结果对精确算法的效率有很大影响。实验表明，当前最实用的求解 SVP 的近似算法是 BKZ 算法 [1] 及其改进算法 [2,3]。关于求解格上 SVP 的主流算法的综述请参考文献[4]。

四、参考文献

[1] C. P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Math. Programming 66, 181–199 (1994).

[2] Y. Chen and P. Q. Nguyen. BKZ 2.0: better lattice security estimates. In: Proc. ASIACRYPT 2011, 1–20 (2011).

[3] S. Bai, D. Stehlé and W. Wen. Measuring, Simulating and Exploiting the Head Concavity Phenomenon in BKZ. In: Proc. ASIACRYPT 2018, 369–404 (2018).

[4] 王小云, 刘明洁. 格密码学研究. 密码学报, 1 (1): 13–27 (2014).