Задачи к курсу «Криптография на решетках»

28 апреля 2025 г.

1. Пусть задан набор векторов $\nu = (u_1, \ldots, u_m)$, где $u_i \in \mathbb{Z}^n$. Тогда $\Lambda(\nu, q)$ — определяется как решетка всех последовательностей целых $(h_1, \ldots, h_m)$ таких, что

$$\sum_{i=1}^{m} h_i u_i \equiv 0 (\mathrm{mod} q).$$

Доказать, что $\Lambda(\nu, q)$ является решеткой.

2. Определим решетку $L : b_i = 2e_i$, при $i = 1, \ldots, n-1$ и $b_n = \sum_{i=1}^{n} e_i$. При $n \geq 4$ длина кратчайшего вектора равна 2, т.е. $\lambda_1 = 2$. Имеются n линейно независимых векторов $2e_i$, поэтому $\lambda_1 = \ldots = \lambda_n = 2$. Проверить, что любой базис такой решетки содержит вектор длины не менее $\sqrt{n}$.

3. Ранг любой подгруппы группы $\mathbb{Z}^n$ конечен и не превосходит n.

4. Пусть B — базис решетки и B^* — соответствующий ортогональный базис, полученный с помощью процедуры ортогонализации Грамма-Шмидта. Тогда

$$\lambda_1 \geq \|b_i^*\| > 0.$$

5. Доказать, что в кольце $\mathbb{Z}_q[x]/(x^n - 1)$ при $q = p^n$, где p простое, существует полиномиальный алгоритм нахождения обратных элементов. Описать этот алгоритм.

6. $M_x = (x, \mathrm{rot}x, \ldots, \mathrm{rot}^{n-1}x)$. Доказать равенство $M_x M_y = M_{xy}$.

7. При $v = (pg, f)$ (см. определение NTRU-шифрования через многочлены) выполняется равенство

$$H = \begin{pmatrix} qI & M_h \\ 0 & I \end{pmatrix}.$$

Иными словами, эта решетка определяется как минимальная бициклическая q-модулярная решетка, содержащая вектор (h, e_1). **Шифрование.** Рассмотрим вектор $(m, -r)$. При приведении этого вектора по модулю эрмитова нормального базиса H получим шифротекст $(t, 0)$, где t — многочлен из определения шифрования с помощью многочленов. Доказать это.

8. Пусть $c_i > 0$, $i = 1, \ldots, n$ и $A = \|a_{ij}\|$ — такая невырожденная $n \times n$-матрица, что $c_1 \cdot \ldots \cdot c_n > |\det A|$. Тогда существует ненулевое целочисленное решение системы неравенств

$$\left| \sum_{j=1}^{n} a_{ij} x_j \right| < c_i, \quad i = 1, \ldots, n.$$

9. Пусть a_{ij} ($1 \leq j \leq k$, $1 \leq n$) — целые рациональные и m_i — натуральные числа. Доказать, что в пространстве $\mathbb{R}^n$ совокупность целочисленных точек $(x_1, \ldots, x_n)$, для которых

$$\sum_{j=1}^{n} a_{ij} x_j \equiv 0 \, (\mathrm{mod} m_i), \quad 1 \leq i \leq k,$$

образует полную решетку, объем основного параллелипипеда которой не превосходит $m_1 \cdot \ \ldots \cdot m_k$.

10. Пусть x — произвольная точка решетки Λ. Ячейкой Воронова $\mathcal{V}(x, \Lambda)$ точки x называется множество точек линейной оболочки решетки Λ, находящихся ближе к этой точке чем к любой другой точке решетки. Доказать следующие свойства ячейки Вороного:

- 1. Для любой точки решетки $x \in \Lambda$ выполняется равенство

$$\mathcal{V}(x, \Lambda) = \mathcal{V}(0, \Lambda) + x.$$

- 2. Множество $\mathcal{V}(x, \Lambda)$ — ограничено, выпукло и симметрично относительноx.
- 3. Каждая ячейка $\mathcal{V}(x, \Lambda)$ содержит шар радиуса $\lambda_1/2$ и содержится в шаре радиуса ρ, где ρ — радиус покрытия решетки, т.е. минимальное значение, для которого шары с центрами в точках решетки радиуса ρ полностью покрывают линейную оболочку решетки.
- 4. Объем ячейки Вороного равен объему основного параллелипипеда решетки.
- 5. Для любых различных точек решетки $x \neq y$ их ячейки Вороного не пересекаются.
- 6. Выполняется равенство

$$\cup_{x \in \Lambda} \mathcal{V}(x, \Lambda) = span(\Lambda).$$