Практика № 4
27.04.21

1 Лемма из лекции

Используя обозначения Леммы 2, докажите, что

$$S_A = \left[\begin{array}{c|c} I & W \\ \hline 0 & S \end{array}\right] \cdot \left[\begin{array}{c|c} I & 0 \\ \hline R & W \end{array}\right] - \text{“лазейка” для } A.$$

Для этого сперва покажите, что $S_A \cdot A = 0 \bmod p$, затем, что $\det S_A = q^n$ и $\det A^\perp = q^n$.

2 Leftover Hash Lemma

Докажите, что $\Delta[(A, r^t A), (A, u)] \leq 2^{-\Omega(n)}$ для $A \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n})$, $u \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$, $r \leftarrow D_{\mathbb{Z}^m,\sigma}$, $m \geq n \log q$, $q-$ простое.

1. Постройте изоморфизм $\mathbb{Z}_q^n \cong \mathbb{Z}^m / A^\perp$.

   Вывод: $D_{\mathbb{Z}^m,\sigma} \cdot A$ следует случайному равномерному распределению $\iff$ $D^t_{\mathbb{Z}^m,\sigma} \bmod A^\perp$ случайно равномерно в $\mathbb{Z}^m / A^\perp$.

2. Докажите, что $\Pr_{b\leftarrow D_{\mathbb{Z}^m,\sigma}}[b - \text{класс смежности в } A^\perp] \approx \frac{\rho_\sigma(A^\perp)}{\rho_\sigma(\mathbb{Z})}$ и, что эта величина независима от b. Для этого можете использовать зависимость $\eta_\varepsilon(A^\perp)$ от λ_1 дуальной решетки, а для λ_1 неравенство Минковского-Хлавки (см. Лекцию №2).