Lista 10, część 2

10.3 **(2 pkt.)** Rozważ kratę $\mathcal{L} \subset \mathbb{R}^2$, zdefiniowaną poprzez wektory bazowe $\{\mathbf{b}^1, \mathbf{b}^2\}$, gdzie:

$$\mathbf{b}^1 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \tag{1}$$

$$\mathbf{b}^2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}. \tag{2}$$

(a) Narysuj fragment kraty jako zbiór punktów w kartezjańskim układzie współrzędnych.

(b) Znajdź krótką kombinację liniową $\mathbf{v} = \alpha_1 \mathbf{b}^1 + \alpha_2 \mathbf{b}^2$ z $\alpha_1, \alpha_2 \in \mathbb{Z}$, tak, żeby otrzymany wektor miał długość mniejszą od długości obu wektorów bazowych. Zwizualizuj otrzymany wektor.

(c) Znajdź najkrótsze niezerowe wektory na tej kracie.

(d) Dany jest wektor docelowy:

$$\mathbf{w} = \begin{pmatrix} 6 \\ 6 \end{pmatrix}. \tag{3}$$

Znaleźć i zwizualizować wektor $\mathbf{v} = \alpha_1 \mathbf{b}^1 + \alpha_2 \mathbf{b}^2$ należący do kraty, najbliższy do wektora $\mathbf{w}$, w sensie odległości euklidesowej $||\mathbf{v} - \mathbf{w}||$. Czy wektor $\mathbf{w}$ należy do tej kraty?

10.4 **(2 pkt.)** Rozważmy problem LWE na $\mathbb{Z}_5^2$. Dysponujemy trzema próbkami LWE w postaci $(\bar{a}_i, b_i) \in \mathbb{Z}_5^2 \times \mathbb{Z}_5$, gdzie:

$$b_i = \langle \bar{a}_i, \bar{s} \rangle + e_i \pmod 5, \tag{4}$$

a błędy spełniają warunek $e_i \in \{-1, 0, 1\}$. Dane próbki:

$$\bar{a}_1 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \quad b_1 = 1$$

$$\bar{a}_2 = \begin{pmatrix} 4 \\ 0 \end{pmatrix}, \quad b_2 = 3$$

$$\bar{a}_3 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \quad b_3 = 0$$

Wyznacz sekret $s \in \mathbb{Z}_5^2$, sprawdzając kandydatów z $\mathbb{Z}_5^2$ i wykorzystując fakt, że błędy są małe. Rozwiąż zadanie analitycznie oraz przedstaw rozwiązanie graficznie.

10.5 **(2 pkt.)** Rozważmy problem LWE na $\mathbb{Z}_7^3$. Dysponujemy czterema próbkami LWE w postaci $(\bar{a}_i, b_i) \in \mathbb{Z}_7^3 \times \mathbb{Z}_7$, gdzie:

$$b_i = \langle \bar{a}_i, \bar{s} \rangle + e_i \pmod 7, \tag{5}$$

a błędy spełniają warunek $e_i \in \{-1, 0, 1\}$. Dane próbki:

$$\bar{a}_1 = \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix}, \quad b_1 = 3$$
$$\bar{a}_2 = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \quad b_2 = 3$$
$$\bar{a}_3 = \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix}, \quad b_3 = 2$$
$$\bar{a}_4 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \quad b_4 = 4$$

Wyznacz sekret $\bar{s} \in \mathbb{Z}_7^3$, przeprowadzając atak typu Primal Lattice, wykorzystujący kratę:

$$\mathcal{L} = \{v \in \mathbb{Z}^{h+k+1} : (A|I_h| - \bar{b})v = 0 \mod q\},$$

gdzie A jest macierzą której wiersze zawierają elementy wektorów $\bar{a}_i$, tj.:

$$A = \begin{pmatrix} (& \bar{a}_1 &) \\ (& \bar{a}_2 &) \\ & \dots & \\ (& \bar{a}_{h-1} &) \\ (& \bar{a}_h &) \end{pmatrix}. \tag{6}$$

W rozważanym przypadku, $h = 4$, $k = 3$ oraz $q = 7$.

Unikalnym krótkim wektorem na tej kracie jest $v = (\bar{s}, \bar{e}, 1)$, znajdując który możemy odzyskać sekret $\bar{s}$.

10.6 **(2 pkt.)** Rozważmy problem LWR. Dysponujemy trzema próbkami LWR w postaci $(\bar{a}_i, b_i) \in \mathbb{Z}_5^2 \times \mathbb{Z}_2$, gdzie:

$$b_i = \lfloor \langle \bar{a}_i, \bar{s} \rangle \rfloor_2, \tag{7}$$

a funkcja zaokrąglania: $\lfloor x \rfloor_p := \lfloor (x \mod q) \frac{p}{q} \rfloor$.

Dane próbki:

$$\bar{a}_1 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \quad b_1 = 1$$
$$\bar{a}_2 = \begin{pmatrix} 4 \\ 0 \end{pmatrix}, \quad b_2 = 0$$
$$\bar{a}_3 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \quad b_3 = 0$$

Wyznacz sekret $s \in \mathbb{Z}_5^2$, sprawdzając kandydatów z $\mathbb{Z}_5^2$ i wykorzystując fakt, że błędy są małe. Rozwiąż zadanie analitycznie oraz przedstaw rozwiązanie graficznie.