Криптография на решётках

ДЗ 1

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Вычислите матрицу Грама решётки с базисом $b_1 = (2, 1, 4), b_2 = (2, -1, 3)$. Найдите определитель этой решётки.

Решение:

$$(b_1, b_1) = 21, (b_1, b_2) = (b_2, b_1) = 15, (b_2, b_2) = 14 \Rightarrow$$

$$G = \begin{pmatrix} 21 & 15 \\ 15 & 14 \end{pmatrix}$$

$$\det(G) = \det(\Lambda)^2 \Rightarrow \det(\Lambda) = \pm\sqrt{\det(G)} = \pm\sqrt{69}$$

Ответ:

$$G = \begin{pmatrix} 21 & 15 \\ 15 & 14 \end{pmatrix}$$

$$\det(\Lambda) = \pm\sqrt{69}$$

Задание 2

Найдите $\det D_n$, где D_n —шахматная решётка, определенная равенством

$$D_n = \{(x_1, ..., x_n) \in \mathbb{Z}^n : x_1 + ... + x_n \equiv 0 \pmod 2\}.$$

Решение:

Задание 3

Пусть $(e_1, ..., e_{n+1})$ –ортонормированный базис в $\mathbb{R}^{n+1}$. Решётка $\mathrm{A}_n = \langle e_2 - e_1, ..., e_{n+1} - e_n \rangle_{\mathbb{Z}}$. Какую размерность имеет A_n? Найдите $\det A_n$ для $n = 2; n = 3; \forall n$.

Решение:

$\dim(\mathrm{A}_n) = n$, так как решётка порождена n линейно независимыми векторами.
$n = 2 : \mathrm{A}_2 = \langle e_2 - e_1, e_3 - e_2 \rangle$

$$G = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \Rightarrow \det \mathrm{A}_2 = \sqrt{\det G} = \sqrt{3}$$

$n = 3 : \mathrm{A}_3 = \langle e_2 - e_1, e_3 - e_2, e_4 - e_3 \rangle$

$$G = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix} = 4 \Rightarrow \det \mathrm{A}_3 = \sqrt{4} = 2$$

Задание 4

Докажите, что длина стороны куба с вершинами в узлах решётки $\mathbb{Z}^3$ всегда является целым числом.

Решение:

Заметим, что вершины куба, образующие сторону, совпадают в двух координатах(пусть будут две последние, иначе повернём куб), тогда длина стороны $AB = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2 + (z_A + z_B)^2} = x_A - x_B$ —целое число. Я не очень понял из условия, видимо диагонали за стороны принимать не надо, так как, например, у единичного куба диагонали иррациональные.

Ответ:

ч.т.д

Задание 5

Докажите, что любая унимодулярная матрица $U \in M_n(\mathbb{Z})$ может приведена к единичной матрице с помощью следующих операций над столбцами: $a_i \leftrightarrow a_j, a_i \leftarrow -a_i, a_i \leftarrow a_i + ka_j$.

Решение:

Сначала с помощью второго преобразования сделаем так, чтобы в первой строке все числа были неотрицательными. Далее с помощью первого преобразования поставим в начало строки наименьший ненулевой элемент этой строки. Далее, используя третье преобразование, будем из каждого элемента первой строки, кроме первого, вычитать первый элемент, пока каждый элемент не станет меньше первого. Таким образом мы каждый элемент первой строки поделии с остатком на первый элемент. Далее опять на первую позицию ставим минимальный элемент и повторяем эту процедуру. Через конечное число шагов мы занулим все элементы первой строки(алгоритм Евклида). Затем рекурсивно проделываем те же действия для матрицы меньшего порядка. В итоге мы приведем матрицу к нижне-треугольному виду, при этом на диагонали будут стоять единицы(так как матрица унимодулярная, а наши действия меняют разве что знак определителя). Затем с помощью третьего преобразования, мы сможем занулить в каждой строке элементы, стоящие слева от самой крайней единицы(начинаем с последней строки). Таким образом получается единичная матрица.

Ответ:

ч.т.д