# Решетки, алгоритмы и современные проблемы криптографии. Алгоритм Гаусса

Шокуров А.В.

11 февраля 2025 г.

# Лемма Минковского

**Теорема**

***(Лемма Минковского о выпуклом теле)****. Пусть в $n$ -мерном пространстве $\mathbb{R}^n$ заданы полная решетка $M$, объем основного параллелепипеда которой равен $\Delta$, и ограниченное центрально симметричное выпуклое множество $X$ с объемом $v(X)$. Если $v(X) > 2^n\Delta$, то множество $X$ содержит по крайней мере одну отличную от нуля точку решетки $M$.*

# Неравенство Адамара

**Теорема**

***(Неравенство Адамара).*** *Пусть* $\det(\Lambda)$ *детерминант решетки и* $\boldsymbol{b}_1, \ \ldots, \boldsymbol{b}_n$ *— ее базис. Справедливо неравенство*

$$\det(\Lambda) \leq ||\boldsymbol{b}_1|| \cdot \ \ldots \cdot ||\boldsymbol{b}_n||,$$

*где* $|| \cdot ||$ *— евклидова норма, т. е.* $||x|| = \sqrt{x^T x}$.

**Доказательство.** Пусть $\mathbf{b}_1, \ \ldots, \mathbf{b}_n$ — базис решетки. Рассмотрим процедуру ортогонализации базиса:

$$\mathbf{b}_1^* = \mathbf{b}_1, \mathbf{b}_2^* = \mathbf{b}_2 - \frac{(\mathbf{b}_1, \mathbf{b}_2)}{(\mathbf{b}_1, \mathbf{b}_1^*)}\mathbf{b}_1^*, \ \ldots, \mathbf{b}_n^* = \mathbf{b}_n - \sum_{k=1}^{n-1} \frac{(\mathbf{b}_n, \mathbf{b}_k^*)}{(\mathbf{b}_k^*, \mathbf{b}_k^*)}\mathbf{b}_k^*.$$

Тогда

$$\begin{aligned}
\|\mathbf{b}_k^*\|^2 &= \left(\mathbf{b}_k - \sum_{i=1}^{k} \frac{(\mathbf{b}_k, \mathbf{b}_i^*)}{(\mathbf{b}_i^*, \mathbf{b}_i^*)}\mathbf{b}_i^*, \mathbf{b}_k - \sum_{i=1}^{k} \frac{(\mathbf{b}_k, \mathbf{b}_i^*)}{(\mathbf{b}_i^*, \mathbf{b}_i^*)}\mathbf{b}_i^*\right) \\
&= \|\mathbf{b}_k\|^2 - 2\sum_{i=1}^{k} \frac{(\mathbf{b}_k, b_i^*)^2}{(\mathbf{b}_i^*, \mathbf{b}_i^*)} + \sum_{i=1}^{k} \frac{(\mathbf{b}_k, \mathbf{b}_i^*)^2}{(\mathbf{b}_i^*, \mathbf{b}_i^*)} \\
&= \|\mathbf{b}_k\|^2 - \sum_{i=1}^{k} \frac{(\mathbf{b}_k, \mathbf{b}_i^*)^2}{(\mathbf{b}_i^*, \mathbf{b}_i^*)} \leq \|\mathbf{b}_k\|^2.
\end{aligned}$$

Следовательно, выполняются неравенства $\|\mathbf{b}_k^*\| \leq \|\mathbf{b}_k\|$. Тогда

$$\det(\Lambda) = \|\mathbf{b}_1^*\| \cdot \ \ldots \cdot \|\mathbf{b}_n^*\| \leq \|\mathbf{b}_1\| \cdot \ \ldots \cdot \|\mathbf{b}_n\|.$$

# О точности оценки Адамара

Из доказательства следует, что неравенство Адамара достигается в том и только в том случае, когда $\mathbf{b}_1, \ldots, \mathbf{b}_n$ — ортогональны. Однако не всякая решетка имеет ортогональный базис.

Классическая теорема Эрмита (1850 г.) утверждает, что для каждого $n$ существует такое число $c(n)$, что в любой $n$-мерной решетке $\Lambda$ можно выбрать базис $\mathbf{b}_1, \ldots, \mathbf{b}_n$, для которого

$$||\mathbf{b}_1|| \cdot \ \ldots \cdot ||\mathbf{b}_n|| \leq c(n) \cdot \det(\Lambda).$$

Эрмит показал, что можно положить $c(n) = (4/3)^{n(n-1)/4}$. Минковский улучшил эту оценку до $c(n) = 2^n/V_n \sim (2n/e\pi)^{n/2}$, где $V_n$ — объем единичного $n$-мерного шара. Однако для всех этих оценок неизвестны полиномиальные алгоритмы отыскания соответствующих базисов.

Ловас предложил полиномиальный алгоритм отыскания базиса с константой $c(n) = 2^{n(n-1)/4}$, получивший название метода приведенного базиса.

# Последовательные минимумы

**Определение**

*Пусть $B_m(0, r)$ — открытый шар радиуса $r$ в пространстве $\mathbb{R}^m$ и $\Lambda$ — решетка. Определим последовательность минимумов $\lambda_1, \ \ldots, \lambda_n$ формулой*

$$\lambda_i(\Lambda) = \inf\{r | \dim(\textbf{\textit{span}}(\Lambda \cap B_m(0, r))) \geq i\}.$$

В этом опрелении нет ограничения на норму: возможно норма не евклидова.

# Нормы $\ell_p$

## Определение

*Функция* $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$*, удовлетворяющая условиям*

- $\|\boldsymbol{x}\| \geq 0$*, причем равенство выполняется только для* $\boldsymbol{x} = 0$*,*
- $\|\alpha \boldsymbol{x}\| = |\alpha| \cdot \|\boldsymbol{x}\|$
- $\|\boldsymbol{x} + \boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$

*для всех* $\alpha \in \mathbb{R}$ *и* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$*, называется нормой на пространстве* $\mathbb{R}^n$*.*

Важное семейство норм — нормы $\ell_p$ при $p \geq 1$ определяется формулами

$$\|\mathbf{x}\|_p = \left( \sum_{i=1}^{n} |x_i|^p \right)^{1/p}.$$

Определена также норма $\ell_\infty$ формулой

$$\|\mathbf{x}\|_\infty = \lim_{p \to \infty} \|\mathbf{x}\|_p = \max_{1 \leq i \leq n} |x_i|.$$

## Вторая теорема Минковского

Пусть $V$ — объем единичного $n$-мерного шара.

**Теорема**

***(Вторая теорема Минковского).*** *Существуют независимые векторы решетки, для которых выполняется неравенство*

$$\|\boldsymbol{x}_1\| \cdot \ \dots \cdot \|\boldsymbol{x}_n\| \leq \frac{2^n}{V_n} \cdot \det(\Lambda).$$

**Доказательство.** В силу определения последовательных минимумов для решетки, достаточно доказать неравенство

$$\lambda_1 \cdot \ \dots \cdot \lambda_n \leq \frac{2^n}{V_n} \cdot \det(\Lambda).$$

# Вторая теорема Минковского

Пусть $\mathbf{x}_1, \ \dots, \mathbf{x}_n$ — линейно независимые векторы решетки, для которых достигаются последовательные минимумы решетки $\lambda_1, \ \dots, \lambda_n$ и предположим, что $\prod_{i=1}^{n} \lambda_i > \frac{2^n}{V_n} \cdot \det(\Lambda)$. Пусть векторы $\mathbf{x}_i^*$ получены с помощью процедуры ортогонализации Грамма-Шмидта. Рассмотрим преобразование

$$T\left(\sum_{i=1}^{n} c_i \mathbf{x}_i^*\right) = \left(\sum_{i=1}^{n} \lambda_i c_i \mathbf{x}_i^*\right).$$

Пусть $S = B_m(0,1) \cap \mathbf{span}(\Lambda)$ — $n$-мерный шар в $\mathbf{span}(\Lambda)$. Тогда

$$\begin{aligned} \mathbf{vol}(T(S)) &= \left(\prod_i \lambda_i\right) \mathbf{vol}(S) \\ &> \frac{2^n}{V_n} \cdot \det(\Lambda) \mathbf{vol}(S) \\ &= 2^n \det(\Lambda). \end{aligned}$$

# Вторая теорема Минковского

Следовательно, по теореме Минковского в $T(S)$ имеется ненулевая точка решетки $\mathbf{y}$. Следовательно, существует точка $\mathbf{x} \in S$, для которой $T(\mathbf{x}) = \mathbf{y}$. Из определения $S$ следует, что $\|\mathbf{x}\| < 1$. Выполняются равенства

$$\begin{aligned} \mathbf{x} &= \sum_{i=1}^{n} c_i \mathbf{x}_i^* \\ \mathbf{y} &= \sum_{i=1}^{n} \lambda_i c_i \mathbf{x}_i^* . \end{aligned}$$

Поскольку $\mathbf{y} \neq 0$ при некотором $i$ выполняется неравенство $c_i \neq 0$. Пусть $k$ — максимальное значение индекса, при котором $c_k \neq 0$ и $k'$ — минимальное значение индекса, при котором $\lambda_{k'} = \lambda_k$. Отметим, что элемент $\mathbf{y}$ линейно независим от $\mathbf{x}_1, \ \ldots, \mathbf{x}_{k'-1}$, поскольку $(\mathbf{x}_k^*, \mathbf{y}) = \lambda_k c_k \|\mathbf{x}_k^*\|^2 \neq 0$ и элемент $\mathbf{x}_k^*$ ортогонален $\mathbf{x}_1, \ \ldots, \mathbf{x}_{k'-1}$.

# Вторая теорема Минковского

Покажем теперь, что $\|\mathbf{y}\| < \lambda_k$. Действительно,

$$\begin{aligned}
\|\mathbf{y}\|^2 &= \left\|\sum_{i\le k} \lambda_i c_i \mathbf{x}_i^*\right\|^2 \\
&= \sum_{i\le k} \lambda_i^2 c_i^2 \|\mathbf{x}_i^*\|^2 \\
&\le \sum_{i\le k} \lambda_k^2 c_i^2 \|\mathbf{x}_i^*\|^2 \\
&= \lambda_k^2 \left\|\sum_{i\le k} c_i \mathbf{x}_i^*\right\|^2 \\
&= \lambda_k^2 \|\mathbf{x}\|^2 < \lambda_k^2.
\end{aligned}$$

Полученное неравенство противоречит определению $k'$-го последовательного минимума $\lambda_{k'}$.

# Вторая теорема Минковского

**Следствие**

*Для первого минимума $\lambda_1$ выполняется неравенство*

$$\lambda_1 \leq \frac{2}{\sqrt[n]{V_n}} \cdot \sqrt[n]{\det(\Lambda)}.$$

Из неравенства $\frac{2}{\sqrt[n]{V_n}} < \sqrt{n}$ получаем

**Следствие**

*Для первого минимума $\lambda_1$ выполняется неравенство*

$$\lambda_1 \leq \sqrt{n}\sqrt[n]{\det(\Lambda)}.$$

## Пример решетки

Из второй теоремы Минковского следует существование линейно независимого набора $\mathbf{s}_1, \ \ldots, \mathbf{s}_n$ элементов решетки ранга $n$ выполняются равенства $\|\mathbf{s}_i\| = \lambda_i$, а также , что для любого линейно независимого набора $\mathbf{s}_1, \ \ldots, \mathbf{s}_n$ элементов решетки ранга $n$, перенумерованного в порядке возрастания норм $\|\mathbf{s}_1\| \leq \ \ldots \leq \|\mathbf{s}_n\|$, выполняются неравенства $\|\mathbf{s}_i\| \geq \lambda_i$.

Однако имеются примеры решеток, для которых не существует базисов $\mathbf{b}_1, \ \ldots, \mathbf{b}_n$, упорядоченных по возрастанию норм, удовлетворяющих условиям $\|\mathbf{b}_i\| \leq \lambda_i$.

# Пример

**Пример.** $\mathbf{b}_i = 2\mathbf{e}_i, i = 1, \ \ldots, n-1$ и $\mathbf{b}_n = \sum_{i=1}^{n} \mathbf{e}_i$. При $n \geq 4$ длина кратчайшего вектора равна 2, т.е. $\lambda_1 = 2$. Имеются $n$ линейно независимых векторов $2\mathbf{e}_i, \ i = 1, , n$. Поэтому $\lambda_1 = \ \ldots = \lambda_n = 2$.

**Задача.** Проверить, что любой базис такой решетки содержит вектор длины не менее $\sqrt{n}$.

## Некоторые задачи на решетках

Из второй теоремы Минковского была получена оценка сверху кратчайшего вектора решетки

$$\lambda_1 \leq \frac{2}{\sqrt[n]{V_n}} \cdot \sqrt[n]{\det(\Lambda)}.$$

Оценка снизу кратчайшего вектора решетки:

**Теорема**

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

$$\lambda_1 \geq \min_j \|\boldsymbol{b}_j^*\| > 0.$$

**Задача.** Докажите эту теорему.

**Указание.** Докажите, что для целочисленного вектора $x$ выполняется неравенство

$$\|B\mathbf{x}\| \geq \|\mathbf{b}_i^*\|, \text{ где } i = \max\{i | x_i \neq 0\}.$$

# Задача SVP (Shortest Vector Problem)

**Определение (Задача нахождения кратчайшего вектора решетки будем именовать SVP (Shortest Vector Problem))**

*По заданному базису* $\mathbf{B} \in \mathbb{Z}^{m \times n}$ *найти ненулевой вектор* $\mathbf{Bx}$, *где* $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, *такой что* $\|\mathbf{Bx}\| \leq \|\mathbf{By}\|$ *для всех* $\mathbf{y} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$.

В настоящее время неизвестен ни один полиномиальный алгоритм нахождения кратчайшего вектора решетки. Более того, не известен ни один такой алгоритм для получения такого вектора в границах, заданных оценкой Минковского

$$\|B\mathbf{x}\| \leq \frac{2}{\sqrt[n]{V_n}} \cdot \sqrt[n]{\det(\Lambda)},$$

или даже более грубой оценкой

$$\|B\mathbf{x}\| < n^c \cdot \sqrt[n]{\det(\Lambda)}.$$

## Немного о теории сложности

Пусть имеется алфавит $\Sigma$ и множество строк $\Sigma^* = \bigcup\limits_{n=0}^{\infty} \Sigma^n$.

Задача распознавания заключается в том, чтобы убедиться выполняется ли некоторое свойство строки $\sigma \in \Sigma^*$. Формально: задано подмножество $L \subset \Sigma^*$, называемое языком. Для заданного элемента $\sigma \in \Sigma^*$ требуется определить, принадлежит ли он этому языку, т.е. выполняется ли соотношение $\sigma \in L$. Класс задач, для которых задача распознавания может быть решена полиномиальным алгоритмом, называется классом полиномиально разрешимых задач, или классом $P$. Класс задач, которые могут быть решены недетерминированным алгоритмом за полиномиальное время от длины входа, называется классом $NP$. Эквивалентное определение: язык $L$ принадлежит классу $NP$, если существует такое подмножество $R \subset \Sigma^* \times \Sigma^*$, что принадлежность $(x, y) \in R$ проверяется за полиномиальное время от длины $x$ и для каждого $x \in L$ существует $y$, что $(x, y) \in R$.

# Сводимость по Карпу

Пусть имеются две задачи распознавания $A$ и $B$. Полиномиально вычислимая функция $F : \Sigma^* \to \Sigma^*$ называется сведением по Карпу задачи $A$ к задаче $B$, если принадлежность $x \in A$ эквивалентна условию $f(x) \in B$. Полиномиальность $B$ влечет в этом случае полиномиальность задачи $A$.
Задача распознавания $A$ называется $NP$-трудной, если любая другая задача $B$ из класса $NP$ сводится к задаче $A$. Если $A$ находится в классе $NP$, то задача $A$ называется $NP$-полной.
Заметим, что $NP$-трудная задача не может быть решена за полиномиальное время, если только не выполняется равенство $P = NP$. Стандартный метод доказательства $NP$-трудности задачи $A$ заключается в ее сведении к некоторой $NP$-трудной задаче $B$.

# Сходимость по Куку

Сводимостью по Куку задачи $A$ к задаче $B$ назывется полиномиальная машина Тьюринга $\mathcal{M}$ с доступом к оракулу, входом которой явяются задачи из $B$. Эта машина сводит $A$ к $B$, если при заданном оракуле, правильно решающем задачу $B$, машина $\mathcal{M}$ решает правильно задачу $A$.
Задача распознавания $A$ называется $NP$-трудной по Куку, если любая другая задача $B$ из класса $NP$ сводится по Куку к задаче $A$. Если $A$ находится в классе $NP$, то задача $A$ называется $NP$-полной по Куку. Заметим, что $NP$-трудная по Куку задача не может быть решена за полиномиальное время, если только не выполняется равенство $P = NP$. Стандартный метод доказательства $NP$-трудности задачи $A$ заключается в ее сведении к некоторой $NP$-трудной задаче $B$.

## Задача CVP (Closest Vector Problem)

**Определение (Задача нахождения ближайшего вектора решетки будем именовать CVP (Closest Vector Problem).)**

*По заданным базису* $\mathbf{B} \in \mathbb{Z}^{m \times n}$ *и вектору-цели* $\mathbf{t} \in \mathbb{Z}^m$ *найти вектор решетки* $\mathbf{Bx}$*, ближайший к вектору* $\mathbf{t}$*, т.е. такой вектор* $x \in \mathbb{Z}^n$*, что* $\|\mathbf{Bx} - \mathbf{t}\| \leq \|\mathbf{By} - \mathbf{t}\|$ *для всех* $\mathbf{y} \in \mathbb{Z}^n$*.*

Соответственно могут рассматриваться три следующие задачи для CVP и SVP:

- Задача поиска ближайшего или кратчайшего вектора решетки.
- Задача определения минимума расстояния до ближайшего вектора решетки или длины кратчайшего вектора решетки.
- Задача распознавания (проверки): для заданного рационального $r > 0$, определить, существует ли вектор решетки, находящийся на расстоянии не более $r$ или имеющий длину не более $r$.

# Задачи аппроксимации

## Определение (Аппроксимация задачи SVP)

*По заданному базису* $\boldsymbol{B} \in \mathbb{Z}^{m \times n}$ *найти ненулевой вектор* $\boldsymbol{Bx}$, *(*$\boldsymbol{x} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$*), такой что* $\|\boldsymbol{Bx}\| \leq \gamma \cdot \|\boldsymbol{By}\|$ *для всех* $\boldsymbol{y} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$.

Для задачи определения длины кратчайшего вектора задача аппроксимации заключается в нахождении такой величины $d$, что $\lambda_1 \leq d \leq \gamma \cdot \lambda_1$.

## Определение (Аппроксимация задачи CVP)

*По заданным базису* $\boldsymbol{B} \in \mathbb{Z}^{m \times n}$ *и вектору-цели* $\boldsymbol{t} \in \mathbb{Z}^m$ *найти вектор решетки* $\boldsymbol{Bx}$, *ближайший к вектору* $\boldsymbol{t}$, *т.е. такой вектор* $x \in \mathbb{Z}^n$, *что* $\|\boldsymbol{Bx} - \boldsymbol{t}\| \leq \gamma \cdot \|\boldsymbol{By} - \boldsymbol{t}\|$ *для всех* $\boldsymbol{y} \in \mathbb{Z}^n$.

Для задачи нахождения минимального расстояния до вектора решетки заключается в нахождении такого $d$, что выполняется $\mathrm{dist}(t, \Lambda) \leq d \leq \gamma \cdot \mathrm{dist}(t, \Lambda)$.

# Алгоритмы аппроксимации

Параметр $\gamma$ в общем случае не константа, это может быть функция от решетки, например ее размерности. В настоящее время для известных полиномиальных алгоритмов аппроксимации величина $\gamma(n)$ — экспонента от $n$. Имеется ряд задач на решетках, для которых имеются полиномиальные алгоритмы. Перечислим их.

1. **Задача принадлежности**. Задан базис **B** решетки и вектор **x**. Определить, принадлежность этого вектора заданной решетке. Эта задача имеет полиномиальное решение, однако следует так выполнять решение, чтобы избежать экспоненциального роста промежуточных результатов.
2. **Задача принадлежности ядру.** Задана матрица $\mathbf{A} \in \mathbb{Z}^{n\times m}$ над кольцом целых чисел. Найти базис решетки $\Lambda = \{x \in \mathbb{Z}^m \mid \mathbf{Ax} = \mathbf{0}\}$. Аналогичная задача для матриц в кольце $\mathbb{Z}_k$ сравнений по модулю $k$. Задана матрица $\mathbf{A} \in \mathbb{Z}_k^{n\times m}$. Найти базис решетки $\Lambda = \{x \in \mathbb{Z}^m \mid \mathbf{Ax} \equiv \mathbf{0} \bmod k\}$.

# Примеры полиномиальных задач на решетках

3. **Построение базиса.** По заданому набору целочисленных векторов $\mathbf{b}_1, \ \ldots, \mathbf{b}_n$ найти базис порождаемой ими решетки.
4. **Объединение решеток.** По заданным решеткам $L(\mathbf{B}_1)$ и $L(\mathbf{B}_2)$ найти минимальную решетку их содержащую.
5. **Построение двойственной решетки.** По заданной решетке $L(\mathbf{B})$ построить двойственную решетку решетку $L(B')$, т.е. множество всех таких векторов $\mathbf{y} \in \mathrm{span} L(\mathbf{B})$, что для всех $\mathbf{x} \in L(\mathbf{B})$ скалярное произведение $(\mathbf{x}, \mathbf{y})$ целое число. Можно проверить, что эта решетка имеет базис $\mathbf{B}(\mathbf{B}^t\mathbf{B})^{-1}$.
6. **Пересечение решеток.** Даны решетки $L(\mathbf{B}_1)$ и $L(\mathbf{B}_2)$. Найти базис решетки $L(\mathbf{B}_1) \cap L(\mathbf{B}_2)$.

# Примеры полиномиальных задач на решетках

7. **Эквивалентность.** Заданы базисы решеток $\mathbf{B}_1$ и $\mathbf{B}_2$. Верно ли, что $L(\mathbf{B}_1) = L(\mathbf{B}_2)$.
8. **Условие цикличности.** Задана решетка $\mathbf{C}$. Верно ли, что это циклическая решетка, т.е. при циклической перестановке координат вектора решетки получаем снова элемент этой же решетки.

# Приведенные базисы

Вначале исследуем двумерные решетки.

**Определение**

*Пусть* $\boldsymbol{a}, \boldsymbol{b}$ *— базис решетки. Этот базис называется приведенным относительно нормы* $\|\cdot\|$*, если выполняются неравенства*

$$\|\boldsymbol{a}\|, \|\boldsymbol{b}\| \leq \|\boldsymbol{a}+\boldsymbol{b}\|, \|\boldsymbol{a}-\boldsymbol{b}\|.$$

# Приведенные базисы

**Лемма**

*Рассмотрим три точки на прямой: $x$, $x + y$ и $x + \alpha y$, где $\alpha \in (1, \infty)$. Для любой нормы $\| \cdot \|$ из неравенства $\|x\| \leq \|x + y\|$ следует, что $\|x + y\| \leq \|x + \alpha y\|$, а из неравенства $\|x\| < \|x + y\|$ следует, что $\|x + y\| < \|x + \alpha y\|$.*

**Доказательство.** Доказательство леммы проведем для строгого наравенства. Доказательство в случае нестрогого неравенства аналогично. Положим $\delta = 1/\alpha$. Тогда

$$\mathbf{x} + \mathbf{y} = (1-\delta)\mathbf{x} + \delta(\mathbf{x} + \alpha\mathbf{y}).$$

Тогда согласно неравенству треугольника имеем

$$\|\mathbf{x} + \mathbf{y}\| \leq (1-\delta)\|\mathbf{x}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\|.$$

Поскольку при $\|\mathbf{x}\| < \|\mathbf{x} + \mathbf{y}\|$ выполняется неравенство

$$(1-\delta)\|\mathbf{x}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\| < (1-\delta)\|\mathbf{x} + \mathbf{y}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\|,$$

то, комбинируя полученные неравенства, получаем

$$\|\mathbf{x} + \mathbf{y}\| < (1-\delta)\|\mathbf{x} + \mathbf{y}\| + \delta\|\mathbf{x} + \alpha\mathbf{y}\|.$$

Преобразуя последнее неравенство, получаем

$$\delta\|\mathbf{x} + \mathbf{y}\| < \delta\|\mathbf{x} + \alpha\mathbf{y}\|.$$

Поскольку $\delta > 0$, из полученного неравенства следует, что $\|\mathbf{x} + \mathbf{y}\| < \|\mathbf{x} + \alpha\mathbf{y}\|$.

## Условие приведенности базиса

**Теорема**

*Пусть* $\mathbf{a}, \mathbf{b}$ *— базис решетки и* $\lambda_1, \lambda_2$ *последовательные минимумы решетки. Тогда базис* $\mathbf{a}, \mathbf{b}$ *приведен в том и только том случае, если нормы векторов* $\mathbf{a}$ *и* $\mathbf{b}$ *равны значениям* $\lambda_1$ *и* $\lambda_2$ *соответственно.*

**Доказательство. Достаточность.** Пусть $\|\mathbf{a}\| = \lambda_1$ и $\|\mathbf{b}\| = \lambda_2$. Без ограничения общности можно считать, что $\|\mathbf{a}\| \leq \|\mathbf{b}\|$. Пусть базис не является приведенным. Тогда выполняется одно из двух неравенств $\|\mathbf{a} \pm \mathbf{b}\| < \|\mathbf{b}\|$. Тогда для одного из базисов $(\mathbf{a}, \mathbf{a} \pm \mathbf{b})$ выполняется неравенство $\|\mathbf{a} \pm \mathbf{b}\| < \lambda_2$, противоречащее определению последовательных минимумов решетки.

**Необходимость.** Пусть базис приведен. Без ограничения общности можно считать, что $\|\mathbf{a}\| \leq \|\mathbf{b}\|$. Требуется доказать, что $\|\mathbf{a}\| = \lambda_1$ и $\|\mathbf{b}\| = \lambda_2$. Пусть $r, s \in \mathbb{Z}$. Покажем, что выполняются соотношения

$$\|\mathbf{a}\| \leq \|r\mathbf{a} + s\mathbf{b}\| \text{ если } (r, s) \neq (0, 0) \tag{1}$$

и

$$\|\mathbf{b}\| \leq \|r\mathbf{a} + s\mathbf{b}\| \text{ если } s \neq 0, \tag{2}$$

из которых следует утверждение теоремы.

Если $r$ или $s$ равно нулю, то неравенства очевидны.

Рассмотрим случай, когда $rs \neq 0$. Разберем случай $r \geq s > 0$, остальные аналогичны. Поскольку $s \geq 1$ имеем

$$\|(r/s)\mathbf{a} + \mathbf{b}\| = \left\| \frac{r\mathbf{a} + s\mathbf{b}}{s} \right\| \leq \|r\mathbf{a} + s\mathbf{b}\|.$$

Применяя теперь доказанную выше лемму к трем точкам $\mathbf{b}, \mathbf{b} + \mathbf{a}$ и $\mathbf{b} + (r/s)\mathbf{a}$, получим

$$\|\mathbf{a}\|, \|\mathbf{b}\| \leq \|\mathbf{a} + \mathbf{b}\| \leq \|\mathbf{b} + (r/s)\mathbf{a}\| \leq \|r\mathbf{a} + s\mathbf{b}\|.$$

# Вполне упорядоченный базис

**Определение**

*Базис называется $\boldsymbol{a}, \boldsymbol{b}$ вполне упорядоченным, если выполняются неравенства $\|\boldsymbol{a}\| \leq \|\boldsymbol{a} - \boldsymbol{b}\| < \|\boldsymbol{b}\|$.*

Вначале каждый базис на входе алгоритма преобразуется во вполне упорядоченный базис или в приведенный базис.

На вход алгоритма Гаусса подается пара линейно независимых векторов **a** и **b**. На выходе получаем приведенный базис решетки $L(\mathbf{a}, \mathbf{b})$.

# Оракул

Пусть $\mathcal{O}(\mathbf{a}, \mathbf{b})$ — оракул, решения задачи:

$$\text{найти } \mu \in \mathbb{Z} \mid \ \forall \mu' \in \mathbb{Z} \|\mathbf{b} - \mu \mathbf{a}\| \leq \|\mathbf{b} - \mu' \mathbf{a}\| \ .$$

## Алгоритм Гаусса

(start)

$$\textbf{if}\ \ \|\mathbf{a}\| > \|\mathbf{b}\|\ \ \textbf{then}\ (\mathbf{a},\mathbf{b}) := (\mathbf{b},\mathbf{a})$$

$$\textbf{if}\ \ \|\mathbf{a}-\mathbf{b}\| > \|\mathbf{a}+\mathbf{b}\|\ \ \textbf{then}\ \ \mathbf{b} := -\mathbf{b}$$

$$\textbf{if}\ \ \|\mathbf{b}\| \le \|\mathbf{a}-\mathbf{b}\|\ \ \textbf{then}\ \ \textbf{return}(\mathbf{a},\mathbf{b})$$

$$\textbf{if}\ \ \|\mathbf{a}\| \le \|\mathbf{a}-\mathbf{b}\|\ \ \textbf{then}\ \ \textbf{go to}(\mathit{loop})$$

$$\textbf{if}\ \ \|\mathbf{a}\| = \|\mathbf{b}\|\ \ \textbf{then}\ \ \textbf{return}\ \ (\mathbf{a}-\mathbf{b},\mathbf{a})$$

$$\textbf{let}\ \ (\mathbf{a},\mathbf{b}) := (\mathbf{b}-\mathbf{a},\mathbf{a})$$

**(начало цикла)**

$$(\mathit{loop}) : \mu = \mathcal{O}(\mathbf{a},\mathbf{b})$$

$$(\mathbf{a},\mathbf{b}) := (\mathbf{a},\mathbf{b}-\mu\mathbf{a})$$

$$\textbf{if}\ \ \|\mathbf{a}-\mathbf{b}\| > \|\mathbf{a}+\mathbf{b}\|\ \ \textbf{then}\ \ \textbf{let b} := -\mathbf{b}$$

$$(\mathbf{a},\mathbf{b}) := (\mathbf{b},\mathbf{a})$$

**if** $(\mathbf{a},\mathbf{b})$ *приведенный* **then return** $(\mathbf{a},\mathbf{b})$ **else go to** $(\mathit{loop})$

**(конец цикла)**

# Корректность части start

Достаточно проверить, что 3-я и 5-я строки действительно дают минимальный базис. Достаточно, согласно лемме, проверить приведенность полученных базисов.
В строке 3 это следует непосредственно из определения.
В строке 5 имеем

$$\|\mathbf{a}-\mathbf{b}\| < \|\mathbf{a}\| = \|\mathbf{b}\|.$$

Положим $\mathbf{a}_1 = \mathbf{a}-\mathbf{b}, \mathbf{a}_2 = \mathbf{a}$. Тогда
$\|\mathbf{a}_1\| < \|\mathbf{a}_2\| \leq \|\mathbf{a}_1 - \mathbf{a}_2\| = \|\mathbf{b}\|$. $\|\mathbf{a}-\mathbf{b}\| \leq \|\mathbf{a}+\mathbf{b}\|$ по шагу 2.
Поскольку $\|\mathbf{a}-\mathbf{b}\| < \|\mathbf{b}\| = \|\mathbf{a}\| = \|\mathbf{a}-\mathbf{b}+\mathbf{b}\|$, то
$\|\mathbf{a}-\mathbf{b}+\mathbf{b}\| < \|\mathbf{a}-\mathbf{b}+2\mathbf{b}\| = \|\mathbf{a}+2\mathbf{b}\|$.

# Доказательство корректности алгоритма Гаусса

**Лемма**

*В начале каждого цикла итераций в алгоритме Гаусса базис* $(\boldsymbol{a}, \boldsymbol{b})$ *вполне упорядочен.*

**Доказательство.** Отметим, что при первом обращении к циклу (loop) базис всегда вполне упорядочен. Необходимо убедиться, что после окончания каждого цикла базис остается вполне упорядоченным или получаем приведенный базис и алгоритм завершается).
Докажем, что если на вход *k*-й итерации цикла loop подается вполне упорядоченный базис, то выходом этой итерации цикла будет приведенный или вполне упорядоченный базис.
В результате выполнения всех операций цикла loop, за исключением последней команды, получаем число $\mu$ и два базисных вектора $\mathbf{a}' = \varepsilon(\mathbf{b} - \mu\mathbf{a})$ и $\mathbf{b}' = \mathbf{a}$, где знак $\varepsilon = \pm 1$ определяется третьей строкой цикла loop. В любом случае выполняется неравенство $\|\mathbf{a}' - \mathbf{b}'\| \leq \|\mathbf{a}' + \mathbf{b}'\|$. Далее согласно определению $\mu$ выполняются соотношения

$$\|\mathbf{a}'+\mathbf{b}'\| \geq \|\mathbf{a}'-\mathbf{b}'\| = \|\varepsilon(\mathbf{b}-\mu\mathbf{a})-\mathbf{a}\| = \|\mathbf{b}-(\mu\pm 1)\mathbf{a})\| \geq \|\mathbf{b}-\mu\mathbf{a})\| = \|\mathbf{a}'\|.$$

Если $\|\mathbf{b}'\| \leq \|\mathbf{a}' - \mathbf{b}'\|$, то базис $(\mathbf{a}', \mathbf{b}')$ приведен. В противном случае $\|\mathbf{b}'\| > \|\mathbf{a}' - \mathbf{b}'\| \geq \|\mathbf{a}'\|$ и базис $(\mathbf{a}', \mathbf{b}')$ вполне упорядочен.

# Доказательство завершаемости алгоритма Гаусса

**Теорема**

*Алгоритм Гаусса заканчивает работу за конечное число шагов. Число итераций в алгоритме Гаусса для базиса $(\boldsymbol{a}, \boldsymbol{b})$ не превосходит $2 + \log_2(\|\boldsymbol{a}\| + \|\boldsymbol{b}\|)$.*

**Доказательство.** Алгоритм Гаусса преобразует базис решетки в базис той же решетки. По выполнении цикла ”loop”для базиса $[\mathbf{a}, \mathbf{b}]$, согласно предыдущей лемме, получаем либо приведенный базис, что завершает алгоритм Гаусса, либо снова вполне упорядоченный базис $[\varepsilon(\mathbf{b} - \mu\mathbf{a}), \mathbf{a}]$ ($\varepsilon = \pm 1$). Если базис $[\mathbf{a}, \mathbf{b}]$ вполне упорядочен, выполняется неравенство $\|\mathbf{b} - \mathbf{a}\| < \|\mathbf{b}\|$. Тогда по условию на $\mu$ выполняется неравенство $\|\mathbf{b} - \mu\mathbf{a}\| < \|\mathbf{b}\|$. Следовательно, после каждой такой итерации вектор $\mathbf{b}$ заменяется вектором $\mathbf{b}'$ строго меньшей длины. Следовательно, полученные после выполнения итерации цикла loop базисы не повторяются и длины векторов базиса не увеличиваются. Поэтому из дискретности решетки следует, что алгоритм закончит работу за конечное число итераций.

## Доказательство полиномиальности алгоритма Гаусса

Сначала опишем эффективную процедуру нахождения значения $\mu = \mathcal{O}(\mathbf{a}, \mathbf{b})$.

**Лемма**

*Пусть $\|\cdot\|$ — евклидова норма и векторы $\boldsymbol{a}, \boldsymbol{b}$ таковы, что $\|\boldsymbol{b}\| > \|\boldsymbol{b} - \boldsymbol{a}\|$. Тогда оракул $\mathcal{O}(\boldsymbol{a}, \boldsymbol{b})$ реализуется эффективно. Более того, число $\mu$ удовлетворяет неравенству $1 \le \mu \le \lceil 2\|\boldsymbol{b}\|/\|\boldsymbol{a}\| \rceil$.*

**Доказательство.** Положим $c = \lceil 2\|\mathbf{b}\|/\|\mathbf{a}\| \rceil$. Тогда согласно неравенству треугольника

$$\|\mathbf{b} - c\mathbf{a}\| \ge c\|\mathbf{a}\| - \|\mathbf{b}\| \ge \|\mathbf{b}\|,$$

и, следовательно, по лемме о трех точках на прямой для $\mathbf{x} = \mathbf{b}$, $\mathbf{y} = -c\mathbf{a}$ и $\alpha = \frac{c+1}{c}$ выполняется неравенство $\|\mathbf{b} - c\mathbf{a}\| \le \|\mathbf{b} - (c+1)\mathbf{a}\|$. Тогда по этой же лемме для всех $\alpha > 1$ выполняется неравенство $\|\mathbf{b} - (c+1)\mathbf{a}\| \le \|\mathbf{b} - \alpha(c+1)\mathbf{a}\|$. Следовательно $\mu \le c$.

Используя процедуру бинарного поиска, находим эффективно на отрезке $[1, c]$ такое целое число $\mu$, являющееся локальным минимумом для функции $\|\mathbf{b} - \mu\mathbf{a}\|$, для которого

$$\|\mathbf{b} - (\mu - 1)\mathbf{a}\| > \|\mathbf{b} - \mu\mathbf{a}\| \leq \|\mathbf{b} - (\mu + 1)\mathbf{a}\|.$$

Тогда по лемме о трех точках на прямой для всех $k \geq \mu + 1$ выполняются неравенства

$$\|\mathbf{b} - \mu\mathbf{a}\| \leq \|\mathbf{b} - (\mu + 1)\mathbf{a}\| \leq \|\mathbf{b} - k\mathbf{a}\|.$$

Аналогично, при $k \leq \mu - 1$ выполняются неравенства

$$\|\mathbf{b} - \mu\mathbf{a}\| < \|\mathbf{b} - (\mu - 1)\mathbf{a}\| \leq \|\mathbf{b} - k\mathbf{a}\|.$$

Поскольку $\mu \in [1, c]$, выполняется неравенство $1 \leq \mu \leq c = \lceil 2\|\mathbf{b}\|/\|\mathbf{a}\| \rceil$.

# Доказательство полиномиальности

Пусть $k$ — число итераций в алгоритме Гаусса и $(\mathbf{a}_k, \mathbf{a}_{k+1})$ вполне упорядоченный базис в начале первой итерации. Представим результаты итераций цикла loop в виде последовательности базисов

$$(\mathbf{a}_k, \mathbf{a}_{k+1}), (\mathbf{a}_{k-1}, \mathbf{a}_k), \ \ldots, (\mathbf{a}_1, \mathbf{a}_2),$$

причем $(\mathbf{a}_1, \mathbf{a}_2)$ — приведенный базис. Тогда справедлива следующая

**Лемма**

*При $i \geq 3$ выполняется неравенство $\|a_{i-1}\| < \frac{1}{2}\|a_i\|$.*

Воспользовавшись леммой, получаем, что при $i \geq 3$ выполняется неравенство $\|\mathbf{a}_i\| \geq 2^{i-3}\|\mathbf{a}_3\|$. В частности, для любых базисных векторов $\mathbf{a}, \mathbf{b}$ выполняется неравенство

$$2^{k-2} \leq 2^{k-2}\|\mathbf{a}_3\| \leq \|\mathbf{a}_{k+1}\| \leq \|\mathbf{a}\| + \|\mathbf{b}\|.$$

Следовательно, $k \leq 2 + \log_2(\|\mathbf{a}\| + \|\mathbf{b}\|)$.
Полученное неравенство завершает доказательство теоремы о полиномиальности алгоритма Гаусса.

# Доказательство леммы

Рассмотрим тройки векторов $(\mathbf{a}_{i-1}, \mathbf{a}_i, \mathbf{a}_{i+1}) = (\mathbf{a}, \mathbf{b}, \mathbf{c})$. Тогда выполняются неравенства $\|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{c}\|$ и при некотором целом $\mu \geq 1$ и $\varepsilon = \pm 1$ выполняется равенство $\mathbf{a} = \varepsilon(\mathbf{c} - \mu\mathbf{b})$. Тогда $\mathbf{c} = \varepsilon\mathbf{a} + \mu\mathbf{b}$. Докажем, что $\|\mathbf{c}\| > 2\|\mathbf{b}\|$.

- Пусть $\mu = 1$. Тогда выполняется неравенство $\|\mathbf{c} - \mathbf{b}\| = \|\mathbf{a}\| < \|\mathbf{b}\| < \|\mathbf{c}\|$, противоречащее вполне упорядоченности базиса $(\mathbf{b}, \mathbf{c})$. Следовательно, $\mu \neq 1$.
- Пусть $\varepsilon = -1$, $\mu = 2$. Тогда $\|\mathbf{c} - \mathbf{b}\| = \| - \mathbf{a} + \mathbf{b}\|$. Поскольку базис $(\mathbf{a}, \mathbf{b})$ вполне упорядочен, выполняется неравенство $\|\mathbf{a} - \mathbf{b}\| < \|\mathbf{b}\|$ и, следовательно, $\|\mathbf{c} - \mathbf{b}\| < \|\mathbf{b}\| < \|\mathbf{c}\|$, что противоречит упорядоченности базиса $(\mathbf{b}, \mathbf{c})$.
- Пусть $\varepsilon = -1$, $\mu > 2$. Тогда, учитывая неравенство $\|\mathbf{a}\| < \|\mathbf{b}\|$, получим

$$\|\mathbf{c}\| = \|-\mathbf{a}+\mu\mathbf{b}\| \geq \mu\|\mathbf{b}\|-\|\mathbf{a}\| > \mu\|\mathbf{b}\|-\|\mathbf{b}\| = (\mu-1)\|\mathbf{b}\| \geq 2\|\mathbf{b}\|.$$

- Пусть $\varepsilon = 1$, $\mu \geq 2$. Поскольку базис $(\mathbf{a}, \mathbf{b})$ вполне упорядочен, выполняется неравенство $\|\mathbf{b} - \mathbf{a}\| < \|\mathbf{b}\|$. Тогда, по лемме о трех точках, выполняется неравенство $\|\mathbf{b}\| < \|\mathbf{b} + \mathbf{a}\|$, а поскольку базис $(\mathbf{a}, \mathbf{b})$ вполне упорядочен выполняется неравенство $\|\mathbf{a}\| \leq \|\mathbf{b} - \mathbf{a}\|$. Поэтому $\|\mathbf{a}\| < \|\mathbf{b} + \mathbf{a}\|$, и, следовательно, используя лемму о трех точках, получим

  $$\|\mathbf{a}\| < \|\mathbf{a} + \mathbf{b}\| < \|\mathbf{a} + 2\mathbf{b}\| \leq \|\mathbf{a} + \mu\mathbf{b}\| = \|\mathbf{c}\|.$$

  Итак, доказано неравенство $\|\mathbf{c}\| = \|\mathbf{a} + \mu\mathbf{b}\| \geq \|2\mathbf{b} + \mathbf{a}\|$. Для доказательства леммы достаточно проверить выполнение неравенства $\|2\mathbf{b} + \mathbf{a}\| > 2\|\mathbf{b}\|$.
  Используя неравенство $\|\mathbf{a} - \mathbf{b}\| < \|\mathbf{b}\|$ (базис $(\mathbf{a}, \mathbf{b})$ вполне упорядочен), из неравенства треугольника получаем

  $$\|2\mathbf{b} - \mathbf{a}\| \leq \|\mathbf{b}\| + \|\mathbf{b} - \mathbf{a}\| < \|\mathbf{b}\| + \|\mathbf{b}\| = 2\|\mathbf{b}\|.$$

  Воспользовавшись леммой о трех точках, получаем

  $$\|2\mathbf{b} - \mathbf{a}\| < \|2\mathbf{b}\| = \|2\mathbf{b} - \mathbf{a} + \mathbf{a}\| < \|2\mathbf{b} - \mathbf{a} + 2\mathbf{a}\| = \|2\mathbf{b} + \mathbf{a}\|.$$