Диофантовы приближения, 3 семестр

ИВАЩЕНКО ДМИТРИЙ

Последние изменения: 6 ноября 2014 г. 20:17

Содержание

Лекция 1. Теорема Минковского и совместные приближения

1. Теорема Минковского о выпуклом теле

Теорема. *Пусть $B \subset \mathbb{R}^n$ — выпуклое центрально-симметричное тело объема $Vol\ \Omega > 2^n$, тогда $\Omega \cap (\mathbb{Z}^n \setminus \{0\}) \neq \varnothing$.*

Упражнение. Показать, что выпуклое центрально-симметричное тело измеримо по Жордану.

Доказательство. (Минковского)

Лемма. *(Блихфельдт) Пусть $B \subset \mathbb{R}^n$, $Vol\ B > 1$, тогда $\exists x, y \in B,\ y \neq x:\ x - y \in \mathbb{Z}^n$.*

Доказательство. Для простоты положим, что B — ограничено (иначе нам нужна счетно-аддитивная мера). Рассмотрим разбиение B: $B = \bigsqcup\limits_{i=1}^{k} B \cap E_i$, где $E_i = [a_{i,1}; a_{i,1}+1) \times \ldots \times [a_{i,n}; a_{i,n}+1)\,,\ a_{i,j} \in \mathbb{Z}$. Каждое из множеств сдвинем переносом на целочисленный вектор v_i в куб $[0;1)^n$. Если все $E_i - v_i$ не пересекаются, то $\mu\,[0;1)^n \geq \sum\limits_{i=1}^{k} \mu E_i = Vol\ B > 1$, противоречие, значит

$$\exists 1 \leq i < j \leq k:\ p \in (E_i - v_i) \cap (E_j - v_j) \Rightarrow$$
$$\Rightarrow \exists x \in E_i,\ y \in E_j:\ x - v_i = y - v_j \Rightarrow x - y = (v_i - v_j) \in \mathbb{Z}^n$$

□

Теперь легко доказать утверждение теоремы: положим $B = \frac{1}{2}\Omega$, тогда $Vol\ B > 1$. По лемме $\exists x \neq y \in B,\ x - y \in \mathbb{Z}^n$. Тогда $\{2x, 2y, -2x, -2y\} \in \Omega$ (т.к. оно центрально-симметрично). Тогда $\frac{2x-2y}{2} \in \Omega$ как середина отрезка $(2x; -2 \cdot y)$, а значит $\mathbb{Z}_n \ni (x - y) \in \Omega$. □

Доказательство. (Морделло)

Снова действуем в предположении ограниченности. Рассмотрим характеристическую функцию Ω:

$$\chi_\Omega(x) = \begin{cases} 1, & x \in \Omega \\ 0, & x \notin \Omega \end{cases}$$

Поскольку B — измеримо, то существует интеграл

$$\int\!\!\cdots\!\!\int\limits_{\mathbb{R}^n} \chi_\Omega(x) \cdot dx_1 \cdot \ldots \cdot dx_n = Vol\ \Omega$$

Тогда составим сумму Римана по сетке с шагом $\frac{1}{q}$, где $q \in \mathbb{N}$. Тогда

$$\exists q:\ \frac{1}{q^n} \sum_{x \in \mathbb{Z}^n} \chi_\Omega\left(\frac{x_1}{q}, \ldots, \frac{x_n}{q}\right) \geq Vol\ \Omega - \varepsilon > 2^n$$
$$\sum_{x \in K \subset \mathbb{Z}^n} \chi_\Omega\left(\frac{x}{q}\right) > (2q)^n\,,\ |K| < \infty$$

Сумма слева это в точности мощность $\left|\Omega \cap \frac{1}{q}\mathbb{Z}^n\right|$. Тогда по принципу Дирихле

$$\exists x, y \in N: \ \frac{x}{q}, \frac{y}{q} \in \Omega: \ \forall 1 \le i \le n \to x_i \equiv y_i \, (mod\ 2q)$$

Тогда $0 \neq \frac{x-y}{2q} \in (\Omega \cap \mathbb{Z}^n)$, что доказывает теорему. $\square$

Упражнение. Доказать утверждение теоремы, если $Vol\ \Omega = 2^n$ и Ω — замкнуто.

2. Совместные приближения

Проблема. Пусть есть вектор $\alpha = (\alpha_1, \dots, \alpha_n) \in (\mathbb{R}^n \setminus \mathbb{Q}^n)$, нужно как можно лучше приблизить их рациональными числами со знаменателем q. Иными словами, подобрать такое q и такие a_i, что $\max\limits_{1 \le j \le n} |q \cdot \alpha_j - a_j| \to \min$, что эквивалентно минимизации $\max\limits_{1 \le j \le n} \|q\alpha_j\|$, где $\|\xi\| = \min\limits_{a \in \mathbb{Z}} |\xi - a|$.

Теорема. *(Дирихле)* $\forall Q \in \mathbb{N}\ \exists q \le Q,\ q \in \mathbb{N}: \ \max\limits_{1 \le j \le n} \|q\alpha_j\| < Q^{-\frac{1}{n}}$

Доказательство. Используем теорему Минковского самым простым способом.

Проведем в $\mathbb{R}^{n+1}$ прямую $\overline{y} = \overline{\alpha} \cdot x,\ y \in \mathbb{R}^n,\ x \in \mathbb{R}$. Обозначим

$$\Pi_Q = \left\{ z = (x, y) \in \mathbb{R}^{n+1} \mid |x| < Q + 1,\ \max_{1 \le j \le n} |x\alpha_j - y_i| < Q^{-\frac{1}{n}} \right\}$$

Это множество представляет собой параллелограмм, у которого каждое сечение $x = c$ представляет собой n-мерный куб со стороной $2Q^{-\frac{1}{n}}$. Тогда можно легко посчитать его объем:

$$Vol\ \Pi_Q = (2Q + 2) \cdot \left(2 \cdot Q^{-\frac{1}{n}}\right)^n = 2^{n+1} \cdot \frac{Q+1}{Q} > 2^{n+1}$$

Тогда в Π_Q есть целая точка, которая дает нам утверждение теоремы. $\square$

Замечание. Очевидное следствие — для любого α существует бесконечно много $q \in \mathbb{N}$, таких, что $\max\limits_{1 \le j \le n} \|q\alpha_j\| < q^{-\frac{1}{n}}$. Это довольно слабое утверждение, далее мы сформулируем и докажем гораздо более сильную теорему.

Теорема. *(Минковского о совместных приближениях)*

$\forall \alpha \in (\mathbb{R}^n \setminus \mathbb{Q}^n)$ *существует бесконечно много таких q, что*

$$\max_{1 \le j \le n} \|q\alpha_j\| < \frac{1}{(\mu_n q)^{\frac{1}{n}}},\ \mu_n = \left(1 + \frac{1}{n}\right)^n$$

Доказательство. Рассмотрим множество $K_\mu = \left\{ \left(\max\limits_{1 \le j \le n} |x \cdot \alpha_j - y_j| \right)^n \cdot |x| \cdot \mu \le 1 \right\}$, где μ — некоторая константа, зависящая только от n. Для удобства введем линейные преобразования

$$A_\alpha = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha_1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \alpha_n & \dots & 0 & 1 \end{pmatrix},\ G_t = \begin{pmatrix} t & 0 & \dots & 0 \\ 0 & t^{-\frac{1}{n}} & \ddots & \vdots \\ \vdots & \ddots & \dots & 0 \\ 0 & \dots & 0 & t^{-\frac{1}{n}} \end{pmatrix},\ \det A_\alpha = \det G_t = 1$$

Преобразование A_α^{-1} переводит прямую $y = \alpha x$ в ось Ox, а G_t сжимает по осям y_i в $t^{\frac{1}{n}}$ раз и растягивает по x в t раз, сохраняя тем самым объем. Также можно заметить, что преобразование $\left(A_\alpha \cdot G_t \cdot A_\alpha^{-1}\right)$ осуществляет автоморфизм из K_μ в себя. Теперь мы имеем дело со множеством $\widetilde{K_\mu} = \left\{\max\limits_{1\le j\le n} |y_j|^n \cdot |x| \cdot \mu \le 1\right\}$. Нам нужно вписывать в K_μ множества объема, большего 2^{n+1}.

Рассмотрим процесс на примере двумерного множества (в любом сечении, содержащем ось Ox, множество выглядит одинаково). Мы возьмем точку $\left(\xi; \left(\frac{1}{\mu\xi}\right)^{\frac{1}{n}}\right)$, построим касательную в ней. Множество точек под касательной обозначим за $\widetilde{\Omega_\xi}$. Заметим, что нам достаточно найти только $\widetilde{\Omega_1}$, так как $\widetilde{\Omega_\xi} = G_\xi(\widetilde{\Omega_1})$. Теперь составим уравнение касательной:

$$\left(y - \mu^{-\frac{1}{n}}\right) = (x-1)\cdot\left(-\frac{1}{n}\right)\cdot\mu^{-\frac{1}{n}} \Rightarrow y = -x\cdot\mu^{-\frac{1}{n}}\cdot\frac{1}{n} + \mu^{-\frac{1}{n}}\left(1+\frac{1}{n}\right)$$

В многомерном случае неравенство, задающее интересующую нас область под касательными, выглядит следующим образом

$$\max_{1\le j\le n} y_j \le -x\cdot\mu^{-\frac{1}{n}}\cdot\frac{1}{n} + \mu^{-\frac{1}{n}}\cdot\left(1+\frac{1}{n}\right)$$

Это конус, в сечении $x = 0$ имеющий n-мерный куб со стороной $2\mu^{-\frac{1}{n}}\left(1+\frac{1}{n}\right)$, высота его равна $n\cdot\left(1+\frac{1}{n}\right) = n+1$. Тогда можно вычислить его объем

$$Vol\ \widetilde{\Omega_1} = \frac{\left(2\mu^{-\frac{1}{n}}\cdot\left(1+\frac{1}{n}\right)\right)^n\cdot(n+1)}{n+1} = \frac{2^n\cdot\left(1+\frac{1}{n}\right)^n\cdot(n+1)}{\mu\,(n+1)} = 2^n\cdot\frac{\left(1+\frac{1}{n}\right)^n}{\mu}$$

Тогда, выбрав $\mu = \left(1+\frac{1}{n}\right)^n$, мы получим (так как конус нужно симметрично отразить по Ox) $Vol\ \widetilde{\Omega_1} = 2\cdot Vol\ \Omega_t = 2^{n+1}$, что дает нам целую точку в K_μ (две, одна из которых имеет отрицательный x) и даже бесконечное их число. □

Лекция 2. Теорема Спона

3. Теорема Спона

Теорема. *(Spone, 1967)* $\forall\alpha\in(\mathbb{R}^n\setminus\mathbb{Q}^n)$ *существует бесконечно много таких* $q\in\mathbb{N}$, *что*

$$\max_{1\le j\le n}\|q\alpha_j\| < \frac{1}{(I_n q)^{\frac{1}{n}}},\ I_n = n\cdot 2^{n+1}\cdot\int\limits_0^1 \frac{t^{n-1}}{(1+t^n)\,(1+t)^n}\cdot dt$$

Упражнение. (Б) Показать, что $n\cdot 2^{n+1}\cdot\int\limits_0^1\frac{t^{n-1}}{(1+t^n)(1+t)^n}\cdot dt\to\pi$ при $n\to\infty$.

Доказательство. Рассмотрим множество $K = \left\{(x,\overline{y})\in\mathbb{R}^{n+1}:\ x\cdot(\max|y_i|)^n < \lambda\right\}$.

Будем искать множество $B\subset\mathbb{R}^{n+1}$: $Vol\ B > 1,\ B - B = \{z \mid z = z_1 - z_2,\ z_1\in B,\ z_2\in B\}\subset K$. Если мы это сделаем, то мы найдем в K целую точку по лемме Блихфельдта.

Как и раньше, нам достаточно найти только одно такое B.

Для простоты будем искать множество D в $\mathbb{R}^2$ такое, что $D + D$ вписано в $y^n x\le 1$ и будем искать его в виде $D = \{x, y\ge 0 \mid x\le\Phi(y)\}$.

По множеству D множество B строится как $B = \{z = (x, \overline{y}) : \ (|x|, \max|y_i|) \in D\}$. Тогда из того что $D + D$ лежит под $y^n x = 1 \Rightarrow B + B \subset K$

Введем функции $f(y) = \frac{1}{y^n}, \ g = g(t), \ t^n + g^n = \frac{1}{2^{n-1}}$. Некоторые факты про нее:

$$n \cdot t^{n-1} \cdot ng^{n-1} \cdot g' = 0 \Rightarrow g' = -\frac{t^{n-1}}{g^{n-1}}$$

$$g(0) = \frac{1}{2^{\frac{n-1}{n}}} = \beta$$

$$g(\beta) = 0$$

$$g(g(t)) = t$$

$$g(\frac{1}{2}) = \frac{1}{2}, \ g(t) \searrow$$

Теперь определяем функцию

$$\Phi(y) = \frac{1}{2} + \int\limits_{\frac{1}{2}}^{y} f'(t + g(t)) \cdot dt$$

$$\Phi(\frac{1}{2}) = \frac{1}{2}$$

Упражнение. (A) Найти явный вид $\Phi(y)$.

Утверждение. $\Phi(y) + \Phi(g(y)) = f(y + g(y))$

Замечание. Это значит, что складывая вектора $(t, \Phi(t)) + (g(t), \Phi(g(t)))$ мы попадем в точности на кривую $x \cdot y^n = 1$.

Доказательство. В силу симметрии достаточно доказать при $y \geq \frac{1}{2}$

$$\Phi(y) + \Phi(g(y)) = 1 + \int\limits_{\frac{1}{2}}^{y} f'(t + g(t)) \cdot dt + \int\limits_{\frac{1}{2}}^{g(y)} f'(t + g(t)) \cdot dt$$

Проведем замену переменной $u = g(t), \ t = g(u) \Rightarrow dt = g'_u \cdot du$ в первом интеграле:

$$\Phi(y) + \Phi(g(y)) = 1 + \int\limits_{\frac{1}{2}}^{g(y)} f'(u + g(u)) \cdot g'_u \cdot du + \int\limits_{\frac{1}{2}}^{g(y)} f'(t + g(t)) \cdot dt =$$

$$= 1 + \int\limits_{\frac{1}{2}}^{g(y)} f'\left(u + g(u)\right) \cdot (g'_u(u) + 1) \cdot du = 1 + \int\limits_{\frac{1}{2}}^{g(y)} f'\left(u + g(u)\right) \cdot d\left(u + g(u)\right) =$$

$$= 1 + f(u + g(u)) \mid_{0.5}^{g(y)} = 1 + f(y + g(y)) - f(1) = f(y + g(y))$$

Что нам и нужно было. Нам осталось доказать только следующее утверждение: □

Утверждение. Если $0 \leq y \leq \frac{1}{2}, \ t \neq g(y), \ \frac{1}{2} \leq t \leq \beta$, то $\Phi(y) + \Phi(t) < f(y + t)$

Доказательство. Зафиксируем y и исследуем $F_y(t) = \Phi(y) + \Phi(t) - f(y+t)$ на максимум (покажем, что он достигается в точке $t = g(y)$).

$$F_y'(t) = f'(t + g(t)) - f'(t + y)$$

Функция $f'(t)$ возрастает. Если $y > g(t)$, то $F_y'(t) < 0$, а если $y < g(t)$, то $F_y'(t) > 0$ в силу возрастания f'.

Тогда при $g(y) < t \Rightarrow F_y'(t) < 0$, а при $g(y) > t \Rightarrow F_y'(t) > 0$. То есть в точке $t = g(y)$ производная меняет знак с «+» на «-», а значит $t = g(y)$ — точка максимума, что и требовалось показать. □

Осталось показать, что $Vol\ B > 1$. $B = \left\{(x, \overline{y}) \in \mathbb{R}^{n+1},\ (|x|, \max|y_j|) \in D\right\}$.

$$|x| \leq \Phi\left(\max|y_j|\right)$$

Зафиксируем $t = \max|y_j|$. Тогда нам нужен интеграл

$$\int\limits_0^\beta 2 \cdot 2 \cdot n \cdot (2t)^{n-1} \cdot \Phi(t) \cdot dt = n \cdot 2^{n+1}\left(\int\limits_0^{\frac{1}{2}} t^{n-1} \cdot \Phi(t) \cdot dt + \int\limits_0^{\frac{1}{2}} \ldots \cdot dt\right)$$

□

Лекции 3-4. Пифагоровы тройки и рациональные точки на сфере

4. Рациональная параметризация сферы

Проблема. Найти все рациональные точки на

$$\mathbb{R}^{n+1} \supset S_n = \left\{(x_1, \ldots, x_{n+1}) \mid x_1^2 + \ldots + x_{n+1}^2 = 1\right\}$$

то есть

$$\xi = (\xi_1, \ldots, \xi_{n+1}) \in S^n \cap \mathbb{Q}^{n+1}$$

Такие что $\xi_i = \frac{a_j}{q_j}$, то есть

$$(\xi_1, \ldots, \xi_{n+1}) = \frac{(A_1, \ldots, A_{n+1})}{[a_1, \ldots, a_{n+1}]},\ Q = [a_1, \ldots, a_{n+1}],\ (A_1, \ldots, A_{n+1}, Q) = 1$$

(отметим, что преставление в таком каноническом виде единственно).

Возьмем $\frac{\overline{a}}{q} = \left(\frac{a_1}{q}, \ldots, \frac{a_n}{q}\right) \in \mathbb{Q}^n$ в каноническом виде. Проведем прямую, соединяющую $(-1; 0, \ldots, 0)$ и $(0; \overline{q})$, зададим ее параметрически:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_2 \\ x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix} + t \cdot \begin{pmatrix} \frac{a_1}{q} \\ \vdots \\ \frac{a_n}{q} \\ 1 \end{pmatrix}$$

Если мы будем искать пересечение этой прямой и сферы, то получим квадратное уравнение. Но один из корней у него рациональный, поэтому и второй тоже. Обратное тоже верно, для каждой рациональной точки сферы мы найдем единственную рациональную точку пересечения этой прямой с осью Ox_{n+1}.

$$\left(\frac{a_1 t}{q}\right)^2 + \ldots + \left(\frac{a_n t}{q}\right)^2 + (t-1)^2 = 1$$
$$\frac{a_1^2 + \ldots + a_n^2}{q^2} t^2 + t^2 - 2t + 1 = 1$$
$$\frac{a_1^2 + \ldots + a_n^2 + q^2}{q^2} \cdot t = 2$$
$$t = \frac{2q^2}{q^2 + a_1^2 + \ldots + a_n^2}$$

Тогда

$$x_j = \frac{2a_j q}{q^2 + a_1^2 + \ldots + a_n^2},\ 1 \le j \le n$$
$$x_{n+1} = \frac{q^2 - a_1^2 - \ldots - a_n^2}{q^2 + a_1^2 + \ldots + a_n^2}$$

Упражнение. Пусть G — поверхность второго порядка в $\mathbb{R}^n$, задаваемая уравнением с целыми коэффициентами. Доказать, что если $G \cap \mathbb{Q}^n \neq \varnothing$, то в G бесконечно много рациональных точек.

5. Пифагоровы тройки

Пусть теперь $n = 1$.

$$\frac{A_1}{Q} = x_1 = \frac{2aq}{q^2 + a^2},\ \frac{A_2}{Q} = x_2 = \frac{q^2 - a^2}{q^2 + a^2}$$

При этом должно быть$(A_1, A_2, Q) = 1$. Нужно выразить Q через q и a, зная, что $(a, q) = 1$. Введем

$$\Delta = \left(q^2 + a^2, 2aq, q^2 - a^2\right)$$

Если $\Delta = 1$, то $Q = q^2 + a^2$. Однако это не всегда так.

Утверждение. $\Delta \mid 2$.

Доказательство. $\Delta \mid 2q^2$. $\exists p \mid \Delta :\ \Delta \mid 2$ или $p \mid q^2$. Второй случай невозможен (иначе $p^2 \mid q^2 \Rightarrow p^2 \mid a^2$, что невозможно). □

Тогда при $\Delta = 2$ получаем $Q = \frac{q^2+a^2}{2}$. Если $q \not\equiv a \pmod 2$, то $Q = q^2 + a^2,\ A_1 = 2q \cdot a,\ A_2 = q^2 - a^2$. Единственная возможность (с точностью до перестановки A_1 и A_2, будем считать A_1 всегда нечетным): A_1, Q — нечетные, A_2 — четное.

Вывод. *Всякое решение уравнения $a^2 + b^2 = c^2$ представляется в описанном виде.*

Замечание. Мы видим, что по порядку величины Q оценивается сверху и снизу величиной q^2.

6. Более высокие размерности

Перейдем к случаю $n = 2$.

$$\begin{cases} \frac{A_1}{Q} = & \frac{2a_1q}{q^2+a_1^2+a_2^2} \\ \frac{A_2}{Q} = & \frac{2a_2q}{q^2+a_1^2+a_2^2} \\ \frac{A_3}{Q} = & \frac{q^2-a_1^2-a_2^2}{q^2+a_1^2+a_2^2} \end{cases}$$

Вопрос. *Обозначим* $\Delta = \left(q^2 + a_1^2 + a_2^2, 2a_1q, 2a_2q, q^2 - a_1^2 - a_2^2\right)$. *Насколько большим может быть* Q*?*

Утверждение. Если $a_1^2 + a_2^2 \equiv 0 \pmod q$, то $q \mid \Delta \Rightarrow \Delta \geq q$.

7. Приближения на сфере

Мы умеем приближать $\alpha_1, \ldots, \alpha_m \in \mathbb{R}^m \setminus \mathbb{Q}^m$. Теорема Дирихле: найдется бесконечно много таких q, что:

$$\left|\alpha_i - \frac{a_i}{q}\right| < \frac{1}{q^{1+\frac{1}{m}}}$$

Если все точки приближения лежат на сфере, то можно использовать это так:

$\forall \alpha_1^2 + \ldots + \alpha_{n+1}^2 = 1 \to \exists$бесконечно много $\frac{A}{Q} \in S^n$, таких что $\max\limits_{1\leq j\leq n}\left|\alpha_j - \frac{A_j}{Q}\right| \leq \frac{1}{q^{1+\frac{1}{m}}} = \frac{1}{Q^{\frac{1}{2}+\frac{1}{2n}}}$.

Теорема. *(Д. Клейнбок) Если* $\alpha \in S^n$, *то существует бесконечно много дробей* $\frac{A}{Q} \in S^n$*:*

$$\max_{1\leq j\leq n}\left|\alpha_j - \frac{A_j}{Q}\right| < \frac{c_n}{Q},\ c_n = f(n)$$

Теорема. *Пусть* $(\beta_1, \beta_2) \in \mathbb{R}^2 \setminus \mathbb{Q}^2$. *Тогда существует бесконечно много* $(q, a_1, a_2) \in \mathbb{Z}^3$, *таких что:*

(1) $(q, a_1, a_2) = 1$

(2) $\sqrt{\sum\limits_{j=1}^{2}\left(q\beta_j - a_j\right)^2} < 1$

(3) $a_1^2 + a_2^2 \equiv 0\,(q)$

Доказательство. На $w = (z, y, x_1, x_2)$ введем $f(w) = zy - x_1^2 - x_2^2$ и тела

$$K = \{w \mid |f(w)| < 1\}$$
$$B = \left\{w \mid |z + y| < 2,\ |z - y| < 2\sqrt{1 - x_1^2 - x_2^2}\right\}$$

Утверждение. $B \subset K$.

Доказательство. Проверяем

$$yz = \frac{(z+y)^2-(z-y)^2}{4} < \frac{4}{4} = 1$$
$$yz > -\frac{4\left(1-x_1^2-x_2^2\right)}{4} = -1+x_1^2+x_2^2$$
$$-1+x_1^2+x_2^2 < yz < 1$$
$$-1 < yz - x_1^2 - x_2^2 < 1$$
$$\left|yz - x_1^2 - x_2^2\right| < 1$$

□

Заменяя $z = \xi + \eta,\ y = \xi - \eta$ для тела B имеем

$$B = \left\{w \mid |\xi| < 1,\ \eta^2 + x_1^2 + x_2^2 < 1\right\}$$

В координатах η, ξ $Vol\ B = 2 \cdot \frac{4}{3}\pi$ (это просто цилиндр над шаром). В изначальных координатах $Vol\ B = \frac{16\pi}{3} > 2^4$. Тогда в нем по теореме Минковского есть нетривиальная целая точка. Чтобы найти бесконечно много, сделаем линейные преобразования

$$G_t = \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ R_\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_1^2+\beta_2^2 & 1 & -2\beta_1 & -2\beta_2 \\ -\beta_1 & 0 & 1 & 0 \\ -\beta_2 & 0 & 0 & 1 \end{pmatrix}$$

$\det G_t = \det A_\alpha = 1$.

Упражнение. (Очевидное) $f(G_t w) = f(w)$

Тогда $K_t' = \{w \mid |f(G_t w)| < 1\} = \{w \mid G_t w \in K\} = G_t^{-1} K$. Второй автоморфизм также сохраняет значение формы:

$$R_\beta \begin{pmatrix} z \\ y \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} z \\ z\left(\beta_1^2+\beta_2^2\right) + y - 2\beta_1 x_1 - 2\beta_2 x_2 \\ -z\beta_1 + x_1 \\ -z\beta_2 + x_2 \end{pmatrix}$$

Тогда значение формы:

$$\begin{aligned} f(A_\beta w) &= z \cdot \left(z\left(\beta_1^2+\beta_2^2\right) + y - 2\beta_1 x_1 - 2\beta_2 x_2\right) - \left(-z\beta_1 + x_1\right)^2 - \left(-z\beta_2 + x_2\right)^2 = \\ &= z^2\left(\beta_1^2+\beta_2^2\right) + zy - 2z\beta_1 x_1 - 2z\beta_2 x_2 - z^2\beta_1^2 + 2zx_1\beta_1 - x_1^2 - z^2\beta_2^2 + 2z\beta_2 - x_2^2 = \\ &= zy - x_1^2 - x_2^2 = f(w) \end{aligned}$$

То есть A_β — автоморфизм формы.

Итак, у нас есть форма, которая на самом деле задает в координатах ξ, η, x_1, x_2 область, ограниченную двумя гиперболическими поверхностями. Также это некоторая небольшая окрестность прямого кругового конуса. Автоморфизм R_β берет точку (β_1, β_2) на сфере (в которую мы потом спроецируем вектор α на трехмерной сфере) и поворачивает координаты по направлению касательной. Далее мы производим растяжение вдоль этой оси и сжатие вдоль другой.

$B \subset K = G_t^{-1} R_\beta K$. $B_t = R_\beta^{-1} G_t B \subset K$. $Vol\ B_t = Vol\ B > 16$. Тогда в нем есть целая точка со следующими свойствами

$$(z_0; y_0; x_{1,0}, x_{2,0}) = (q, A, a_1, a_2)$$
$$qA = a_1^2 + a_2^2$$
$$a_1^2 + a_2^2 \equiv 0 \pmod q$$
$$\sqrt{(q\beta_1 - a_1)^2 + (q\beta_2 - a_2)^2} \leq 1$$

Покажем последнее, для этого обозначим

$$L = q\left(\beta_1^2 + \beta_1^2\right) + A - 2a_1\beta_1 - 2a_2\beta_2$$
$$\Delta = \sum_{i=1}^{2} (q\beta_i - a_i)^2$$
$$w \in B_t = R_\beta^{-1} G_t B$$

Теперь $G_{t^{-1}} R_\beta w \in B,\ R_\beta w = \begin{pmatrix} q \\ L \\ a_1 - q\beta_1 \\ a_2 - q\beta_2 \end{pmatrix},\ G_{t^{-1}} R_\beta w = \begin{pmatrix} q \cdot t^{-1} \\ L \cdot t \\ a_1 - q\beta_1 \\ a_2 - q\beta_2 \end{pmatrix} \in B \Rightarrow$

$$x_1^2 + x_2^2 + \eta^2 \leq 1 \Rightarrow \Delta = (a_1 - q\beta_1)^2 + (a_2 - q\beta_2)^2 \leq 1$$

Если $q = 0$, то $\Delta = a_1^2 + a_2^2 < 1 \Rightarrow a_1 = a_2 = 0$. $|L \cdot t| < 2 \Rightarrow A = 0$, при $t > 2$. То есть при $t > 2$ такое невозможно.

Тело B выпукло и центрально-симметрично, то есть $q > 0$. Используем $\left|\frac{q}{t} - L \cdot t\right| < 2$, значит $(q; L)$ лежит в ромбе с вершинами $\left(0; 2t^{-1}\right)$, $(2t; 0)$, $\left(0; -2t^{-1}\right)$, $(-2t; 0)$. Если мы покажем, что $L \neq 0$, то мы будем сужать ромб по вертикали, устремляя t к бесконечности.

Но мы показали, что $qA - a_1^2 - a_2^2 = 0$. Если $L = 0$, то

$$q^2\beta_1^2 + q^2\beta_2^2 + a_1^2 + a_2^2 - 2a_1 q\beta_1 - 2a_2 q\beta_2 = 0$$
$$(q\beta_1 - a_1)^2 + (q\beta_2 - a_2)^2 = 0$$

Но тогда $\Delta = 0$, что невозможно. $\square$

Упражнение. (Неочевидное) Доказать теорему при $n = 4$, используя кватернионы.

Замечание. Теорема влечет за собой теорему Клейнбока при $n = 2$. Для рациональной точки на сфере нужно спроецировать ее на плоскость и приблизить по теореме. По рациональной точке на окружности восстановим рациональную точку на сфере. При этом ошибка в приближении сильно не увеличится

$$\left|\beta_j - \frac{a_1}{q}\right| < \frac{1}{q}$$

Но $Q \ll q$, так как $a_1^2 + a_2^2 \equiv 0\,(q)$. Тогда $\left|\alpha_j - \frac{A_j}{Q}\right| \leq \frac{c}{q} < \frac{c_1}{Q}$.

Лекции 5.

Определение. *Решетка* в $\mathbb{R}^n$ на векторах $e_1, \ldots, e_d$ есть $\Lambda = \{\xi = \lambda_1 e_1 + \ldots + \lambda_d e_d,\ \lambda_j \in \mathbb{Z}\}$.

Размерность решетки $\dim \Lambda = d$. Если $d = n$, то решетка *полная.*

Замечание. Если Ω — линейный оператор $\mathbb{R}^n \mapsto \mathbb{R}^n$, $\det \Omega \neq 0$, то $\Lambda = \Omega \cdot \mathbb{Z}^n$ — решетка.

Теорема. *(Минковского) B — выпуклое центрально-симметричное тело, $Vol\ B > 2^n \det \Lambda$, то $\exists z \in \Lambda :\ z \neq 0,\ z \in B$.*

Определение. $\Gamma \subset \Lambda$ — подрешетка, если она решетка.

Определение. *span* Z — минимальное линейное подпространство, содержащее Z.

Замечание. Если количество классов смежности $K = [\Lambda : \Gamma]$ в Λ/Γ конечно, то $\dim \Lambda = \dim \Gamma$.

Утверждение. Если количество классов смежности Λ/Γ конечно,то

$$[\Lambda : \Gamma] = \frac{\det \Gamma}{\det \Lambda}$$

Упражнение. Доказать это.

Замечание. В двумерном случае нужно рассмотреть в $\Lambda \setminus Lin\,(e_1)$ ближайшую к началу координат точку.

В 3D можно дополнить два вектора до базиса тогда и только тогда, когда $span\,(e_1, e_2) \cap \Lambda = \{\lambda_1 e_1 + \lambda_2 e_2 \mid \lambda_i \in \mathbb{Z}\}$.

Пример. $\Lambda = \mathbb{Z}^2$. $\Gamma = \Gamma_{a,p} = \{z :\ (z_1, z_2) \in \Lambda :\ z_1 \equiv a z_2 \pmod p\}$, p — простое, $(a, p) = 1$.

$\Gamma \subset \Lambda$ полная подрешетка. $[\Lambda : p\Lambda] = p^2,\ [\Lambda : \Gamma] = p,\ [\Gamma, p\Lambda] = p$. $\exists i :\ i^2 \equiv -1 \pmod p$.

Если $p = 4k + 1$, то $\exists a, b :\ p = a^2 + b^2$.

Доказательство. $\Gamma \subset \Lambda,\ \Gamma = \{z :\ z_1 \equiv i z_2 \pmod p\}$. $\det \Gamma = p,\ B = \left\{z_1^2 + z_2^2 < 2p\right\}$. $Vol\ B = 2\pi p > 4p$. Тогда

$$\exists\,(a, b) \in \mathbb{Z}^2 \setminus \{0\}\,,\ a \equiv ib \pmod p,\ a^2 + b^2 < 2p$$

Значит $a^2 + b^2 \equiv \left(i^2 + 1\right) b^2 \equiv 0 \pmod p \Rightarrow a^2 + b^2 \equiv 0 \pmod p$, то есть $a^2 + b^2 = p$. $\square$

Упражнение. Если $m = 2^\alpha p_1 \cdot \ldots \cdot p_t \cdot (p_1')^2 \cdot \ldots \cdot (p_l')^2,\ p_i = 4k_i + 1,\ p_j' = 4l_1 - 1$, то $\exists a, b :\ a^2 + b^2 = m$

Пример. $\Lambda = \mathbb{Z}^4$. $\Gamma_{a,b,p} = \{(z_1, z_2, z_3, z_4) \in \Lambda :\ z_1 \equiv a z_3 + b z_4 \pmod p,\ z_2 \equiv b z_3 - a z_4 \pmod p\}$. $d = [\Lambda : \Gamma] \leq p^2$.

$B = \left\{z :\ z_1^2 + z_2^2 + z_3^3 + z_4^2 < 2p\right\},\ Vol\ B = \frac{\pi^2}{2} \cdot R^4 = \frac{\pi^2}{2} 4p^2 < 2\pi^2 p^2 > 16p^2$. $\det \Gamma \leq p^2$.

Итого, $\exists 0 \neq (z_1, z_2, z_3, z_4) \in (\Gamma_{a,b,p} \cap B)$.

Лемма. $\forall p \geq 3 \to \exists a, b :\ a^2 + b^2 + 1 \equiv 0 \pmod p$.

Доказательство. $0 \leq a < \frac{p}{2},\ \frac{p+1}{2} \mapsto a^2$ ($\frac{p+1}{2}$ штук). $0 \leq b < \frac{p+1}{2} \mapsto b^2 - 1$ ($\frac{p+1}{2}$ штук). Два множества размера больше половины, стало быть, пересечение не пусто. $\square$

Теперь берем эту точку теоремы Минковского при найденных a и b.

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 \equiv (a z_3 + b z_4)^2 + (b z_3 - a z_4)^2 + z_3^2 + z_4^2 \equiv \left(a^2 + b^2 + 1\right) z_3^2 + \left(a^2 + b^2 + 1\right) z_4^2 \equiv 0 \pmod p$$

Итого, $p = z_1^2 + z_2^2 + z_3^2 + z_4^2$.

Упражнение. Показать, что $[\Lambda : \Gamma] = p^2$.

Упражнение. $Vol\ B^d = \frac{\pi^{d/2}}{\Gamma\left(\frac{n+2}{2}\right)}$

Упражнение. Любое число представимо в виде суммы 4 квадратов.