

Основы комбинаторики и теории чисел

Григорян Сергей

20 февраля 2025 г.

Содержание

1	Лекция 1	3
1.1	Квадратичные вычеты и невычеты	3
1.1.1	Определение	3
1.1.2	Способы вычисления	4
1.1.3	Квадратичный закон взаимности	7
2	Лекция 2	8
2.1	Матрица Адамара	8
2.1.1	Определение	8
2.1.2	Необходимое условие существования	8
2.1.3	Конструирование матриц Адамара	9
2.1.4	Плотность порядков матриц Адамара	11
2.1.5	Коды, исправляющие ошибки	11
2.1.6	(n, M, d) -код	12
3	Основная теорема арифметики	12
4	Лекция 3	15
4.1	Доказательство границы Плоткина	15
4.2	16

1 Лекция 1

1.1 Квадратичные вычеты и невычеты

1.1.1 Определение

Пусть $m \in \mathbb{N}$ — наш модуль. Пусть $a \in \mathbb{N}$: $(a, m) = 1$. Рассмотрим сравнение:

$$x^2 \equiv a \pmod{m} \quad (1)$$

Мы говорим, что a является **квадратичным вычетом по модулю m** , если у сравнения (1) **есть решение**.

Пусть a — квадратичный вычет. Будем всюду далее считать, что $m = p$ — нечётное простое число. Тогда сравнение (1) **имеет 2 решения по теореме Лагранжа**.

Теорема 1.1 (Лагранжа). *Пусть:*

$$f(x) = a_n x^n + \dots + a_1 x + a_0, a_i \in \mathbb{Z}_p$$

Тогда сравнение:

$$f(x) \equiv 0 \pmod{p}$$

Имеет $\leq n$ корней.

Доказательство. От противного, пусть есть решения x_1, \dots, x_{n+1} . Представим $f(x)$ в виде:

$$\begin{aligned} f(x) &= b_n(x - x_1)(x - x_2) \dots (x - x_n) + \\ &\quad + b_{n-1}(x - x_1) \dots (x - x_{n-1}) + \\ &\quad \vdots \\ &\quad + b_1(x - x_1) + \\ &\quad + b_0 \end{aligned}$$

Рассм. $f(x_1) \equiv 0 \pmod{p} \Rightarrow f(x_1) \equiv b_0 \equiv 0 \pmod{p}$

$$f(x_2) \equiv 0 \equiv b_1(x_2 - x_1) \Rightarrow b_1 \equiv 0 \pmod{p}$$

Аналогичным образом, получаем, что $\forall i, b_i = 0$

□

Таким образом, в нашем случае сравнение (1) имеет ровно 2 корня:

$$x_1^2 \equiv a \pmod{p}$$

$$(-x_1)^2 \equiv a \pmod{p}$$

Выпишем все квадратичные вычеты по модулю p :

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

Покажем, что это действительно все корни:

$$1^2 \equiv (\pm 1)^2$$

$$2^2 \equiv (\pm 2)^2$$

$$\vdots$$

$$a^2 \equiv (\pm a)^2$$

Таким образом, все эти корни заполняют всю приведённую систему вычетов по модулю p . Поэтому мы имеем $\frac{p-1}{2}$ **квадратичных вычетов** и $\frac{p-1}{2}$ **квадратичных невычетов**.

Определение 1.1. Символом **Лежандра** числа a по модулю p (читается " a по p "), называется число:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a = 0 \\ 1, & a \text{ — квадратичный вычет} \\ -1, & a \text{ — квадратичный невычет} \end{cases}$$

1.1.2 Способы вычисления

Утверждение 1.1.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Доказательство. Рассм. МТФ:

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{p-1} - 1 \equiv 1 \pmod{p}$$

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

Если a квадратичный вычет, то:

$$a \equiv x^2 \pmod{p} \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$$

У уравнения, $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ — $\frac{p-1}{2}$ корней, т. е. это все наши квадратичные вычеты. Таким образом:

$$a^{\frac{p-1}{2}} \equiv 1 \iff a \text{ — квадратичный вычет}$$

$$a^{\frac{p-1}{2}} \equiv -1 \iff a \text{ — квадратичный невычет}$$

Таким образом:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

□

Следствие.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

Следствие.

$$\left(\frac{a^2}{p}\right) = 1$$

Следствие.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, p = 4k + 1, k \in \mathbb{Z} \\ -1, p = 4k + 3, k \in \mathbb{Z} \end{cases}$$

Следствие.

$$\left(\frac{1}{p}\right) = 1$$

Утверждение 1.2.

$$a^{\frac{p-1}{2}} \equiv (-1)^{\sum_{x=1}^{p-1} \lfloor \frac{2ax}{p} \rfloor} \pmod{p}$$

Доказательство. Рассм. $x = 1, 2, 3, \dots, \frac{p-1}{2}, p_1 := \frac{p-1}{2}$

$$ax = \varepsilon_x r_x \pmod{p}, \varepsilon_x \in \{+1, -1\}, r_x \in \{1, \dots, p_1\}$$

Перемножим все ax и $\varepsilon_x r_x$, тогда т. к. x и r_x пробегают одни и те же числа, то:

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \dots \cdot \varepsilon_{p_1}$$

Утверждение 1.3.

$$\varepsilon_x = (-1)^{\lfloor \frac{2ax}{p} \rfloor}$$

Доказательство. Рассм. случаи принадлежности ax к:

1. $\{1, \dots, p_1\}$
2. $\{p_1 + 1, p - 1\}$

□

Тогда:

$$a^{\frac{p-1}{2}} \equiv (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{2ax}{p} \rfloor} \pmod{p}$$

□

Утверждение 1.4. Если a — нечётное, то:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{ax}{p} \rfloor}$$

Доказательство. Рассм. a — нечёт. Рассм.

$$\begin{aligned} \left(\frac{2a}{p}\right) &= \left(\frac{4((a+2)/2)}{p}\right) = \\ &= \left(\frac{4}{p}\right) \left(\frac{\frac{1}{2}(a+p)}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{(a+p)x}{p} \rfloor} = (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{ax}{p} \rfloor + \sum_{x=1}^{p_1} x} = \\ &= (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{ax}{p} \rfloor + \frac{p_1(p_1+1)}{2}} = (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{ax}{p} \rfloor + \frac{p^2-1}{8}} \end{aligned}$$

Подставим $a = 1$:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

При этом в общем виде:

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{a}{p}\right)$$

Что равно тому, что получено выше. Сокращая одинаковые члены, получаем:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \lfloor \frac{ax}{p} \rfloor}$$

□

Следствие.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

1.1.3 Квадратичный закон взаимности

Пусть p и q — разные нечётные простые числа. Тогда:

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{p_1 \cdot q_1} \quad (2)$$

Доказательство.

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{q_1} \lfloor \frac{px}{q} \rfloor + \sum_{y=1}^{p_1} \lfloor \frac{qy}{p} \rfloor}$$

Положим:

$$S = \{ (x, y) : x = 1, \dots, q_1; y = 1, \dots, p_1 \}, |S| = p_1 \cdot q_1$$

$$S_1 = \{ (x, y) \in S : qy < px \}$$

$$S_2 = \{ (x, y) \in S : qy > px \}$$

Тогда:

$$|S| = |S_1| + |S_2|$$

$$qy < px \iff y < \frac{px}{q} \Rightarrow |S_1| = \sum_{x=1}^{q_1} \left\lfloor \frac{px}{q} \right\rfloor$$

$$qy > px \iff x < \frac{qy}{p} \Rightarrow |S_2| = \sum_{y=1}^{p_1} \left\lfloor \frac{qy}{p} \right\rfloor$$

$$\Rightarrow p_1 q_1 = |S| = |S_1| + |S_2| = \sum_{x=1}^{q_1} \left\lfloor \frac{px}{q} \right\rfloor + \sum_{y=1}^{p_1} \left\lfloor \frac{qy}{p} \right\rfloor$$

□

2 Лекция 2

2.1 Матрица Адамара

2.1.1 Определение

Определение 2.1. Матрица Адамара — это квадратная матрица:

$$A_{n \times n} = (a_{ij}), a_{ij} \in \{+1, -1\}$$

Такая, что любые две строки ортогональны (скалярное произведение в ОНБ = 0).

Рассмотрим несколько случаев:

$n = 1$:

$$(1)$$

$n = 2$:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$n = 3$: Невозможно

Замечание. Матриц Адамара нечётного размера не существует (кроме $n = 1$)

$$\Rightarrow n \geq 2 \Rightarrow n = 2k$$

2.1.2 Необходимое условие существования

Теорема 2.1. $n \geq 2 \Rightarrow n = 4k, k \in \mathbb{N}$

Доказательство.

Задача 2.1. Если у матрицы из ± 1 попарно ортогональны строки, то у неё также попарно ортогональны и столбцы.

Б. О. О.:

$$H_n = \begin{pmatrix} 1 & \dots & 1 \\ 1 & & \\ \vdots & \pm 1 & \\ 1 & & \end{pmatrix}$$

Т. к. каждая строка ортогональна 1-ой, то в каждой строке, кроме первой, поровну 1 и -1

Б. О. О.:

Вторая строка: $1, 1, 1, \dots, 1, 1, 1, -1, -1, -1, \dots, -1, -1, -1$

Третья строка: $1, \dots, 1, -1, \dots, -1, 1, \dots, 1, -1, \dots, -1$

Получаем 4 блока с одним скал. произведением: $x, \frac{n}{2} - x, \frac{n}{2} - x, x$:

$$x - \left(\frac{n}{2} - x\right) - \left(\frac{n}{2} - x\right) + x = 0$$

$$\Rightarrow 4x - n = 0$$

$$\Rightarrow n = 4x$$

□

Гипотеза Адамара: $n = 4k$ — достаточное условие, для существования матрицы Адамара.

2.1.3 Конструирование матриц Адамара

Алгоритм построения H_{2^n} из $H_{2^{n-1}}$:

$$H_{2^n} = \begin{pmatrix} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & (-1) \cdot H_{2^{n-1}} \end{pmatrix}$$

Определение 2.2. $A_n * B_m$ — **кронекеровское умножение** квадратных матриц A_n и B_m , задаваемое следующим образом:

$$A_n * B_m = \begin{pmatrix} a_{11} \cdot B & \dots & a_{1n} \cdot B \\ \vdots & \vdots & \vdots \\ a_{n1} B & \dots & a_{nn} \cdot B \end{pmatrix} = C_{mn}$$

Теорема 2.2. Если A, B — матрицы Адамара, то $A * B$ — тоже матрица Адамара.

Теорема 2.3 (I конструкция Пэли). Пусть $p = 4k + 3$ — простое число. Тогда существует \exists матрица Адамара порядка $p + 1$.

Доказательство. Рассмотрим матрицу $Q = (q_{ij})$:

$$q_{ij} = \left(\frac{i - j}{p} \right)$$

Покажем, что скалярное произведение \forall двух строк равно -1 :

$$\begin{aligned} \sum_{b=1}^p \left(\frac{a-b}{p} \right) \left(\frac{a'-b}{p} \right) &= \left[a' - b = a' + a - b - a = c + a' - a \right] = \\ &= \sum_{c=1}^{p-1} \left(\frac{c}{p} \right) \left(\frac{c + a' - a}{p} \right) = \sum_{c=1}^{p-1} \left(\frac{c}{p} \right) \left(\frac{c(1 + c^{-1}(a' - a))}{p} \right) = \\ &= \sum_{c=1}^{p-1} \left(\frac{1 + c^{-1}(a' - a)}{p} \right) = 0 - \left(\frac{1}{p} \right) = -1 \end{aligned}$$

Тогда искомая матрица:

$$H_{p+1} = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & Q' & \\ 1 & & \end{pmatrix}$$

где Q' матрица Q , где вместо 0 стоят -1 . Покажем, что это действительно матрица Адамара. Для двух строк a и a' скалярное произведение равно:

$$\begin{aligned} -1 + 1 - \left(\frac{a - a'}{p} \right) - \left(\frac{a' - a}{p} \right) &= \\ &= - \left(\underbrace{\left(\frac{-1}{p} \right)}_{-1} + 1 \right) \left(\frac{a' - a}{p} \right) = 0 \\ \left(\frac{-1}{p} \right) &= (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1 \end{aligned}$$

□

Теорема 2.4 (II конструкция Пэли). Пусть $p = 4k + 1$ — простое. Тогда \exists матрица Адамара порядка $2(p + 1)$.

Замечание. В книжке Н. Холла "Комбинаторика" есть отдельная глава про матрицы Адамара (стоит прочитать).

2.1.4 Плотность порядков матриц Адамара

Теорема 2.5 ($6/д$).

$$\forall \varepsilon > 0, \exists n_0, \forall n \geq n_0$$

на отрезке $[n, (1 + \varepsilon)n]$ есть порядок матрицы Адамара.

Переформулировка:

$$\exists f: f(n) = o(n)$$

на отрезке $[n, n + f(n)]$ есть порядок матрицы Адамара.

2.1.5 Коды, исправляющие ошибки

Есть передатчик, приёмник и канал связи. По этому каналу связи передаются бинарные строки длины n . На канале есть помехи, т. е. произвольный бит может поменять значение. Пусть мы знаем, что кол-во ошибок $\leq k$.

Вопрос: как организовать словарь кодовых слов (строк, которых мы передаём), что, несмотря на ошибки, приёмник сможет однозначно понять исходное слово по искажённому?

Например, пусть наш словарь состоит из двух строк и $k = 1$:

1110...0

0111...0

Эти два слова могут исказиться до 1111...0, т. е. мы их не сможем различить. С другой стороны:

1110...0

0011...0

Всегда можно различить, т. к. они не могут исказиться до одного и того же.

Определение 2.3. Расстояние Хэмминга между двумя векторами — это кол-во несовпадающих координат.

Основная задача кодирования: выбрать максимальное кол-во слов так (при заданных n и k), чтобы **расстояние Хэмминга между любыми двумя словами было $> 2k$** .

2.1.6 (n, M, d) -код

Определение 2.4. (n, M, d) -код — тройка объектов, в которой:

- n — длина кодового слова;
- M — кол-во кодовых слов;
- d — минимальное Хэммингово расстояние.

Теорема 2.6 (Граница Плоткина). Пусть дан (n, M, d) -код, причём $2d > n$. Тогда $M \leq \frac{2d}{2d-n}$

Доказательство. Будет доказана в следующий раз □

Замечание. Матрицы Адамара дают наилучшую границу размера словаря.

$$H = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \pm 1 & \\ 1 & & \end{pmatrix} \rightarrow \begin{pmatrix} \dots & 1 \\ \pm 1 & \\ \dots & \end{pmatrix}$$

$$\Rightarrow \left(n-1, n, \frac{n}{2}\right)\text{-код}$$

Рассмотрим код из строк матрицы Адамара, заметим, что он достигает границы Плоткина.

3 Основная теорема арифметики

Теорема 3.1 (ОТА). 1)

$$\forall n > 1, \exists! p_1, \dots, p_s: n = p_1 p_2 \dots p_s$$

где p_1, \dots, p_s — простые (не обязательно различные) числа (единственность с точностью до порядка)

2) Пусть p_i — i -ое простое число, тогда:

$$\forall n, \exists! (\alpha_1, \dots, \alpha_n, \dots), \alpha_i \in \mathbb{Z}_+, n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$$

Определение 3.1. $\nu_p(n)$ — максимальная степень p , т. ч. $n \vdots p^{\nu_p(n)}$, но $n \not\vdots p^{\nu_p(n)+1}$

Замечание.

$$\begin{aligned} n \vdots m &\iff \forall p, \nu_p(n) \geq \nu_p(m) \\ n = m &\iff \forall p, \nu_p(n) = \nu_p(m) \end{aligned}$$

Использование:

- 1) Оценка $\pi(x)$ — кол-во простых $\leq x$
- 2) Криптография: $q \cdot p \longleftrightarrow n$

Доказательство. 1) Существование (ММИ по n):

- База, n — простое $\Rightarrow n = n$
- Переход: $n = mk = (p_1 \dots p_s) \cdot (q_1 \dots q_l)$

- 2) I) Напрямую. От противного, возьмём наименьшее n , для которого есть > 1 разложение:

$$n = p_1 \dots p_s = q_1 \dots q_k$$

$$p_1 \leq p_2 \leq \dots \leq p_s$$

$$q_1 \leq q_2 \leq \dots \leq q_k$$

Если $p_1 = q_1$, тогда $\frac{n}{p_1} = p_2 \dots p_s = q_2 \dots q_k$, т. е. у нас есть меньшее число, у которого > 1 разложения $\Rightarrow \perp$. Тогда $p_1 \neq q_1$. Следовательно:

$$n \geq p_1 p_2 \geq p_1^2$$

$$n \geq q_1^2$$

$$n \geq \max(p_1^2, q_1^2) \geq q_1(p_1 + 2) > q_1 p_1 + 1$$

Пусть $q_1 > p_1 \Rightarrow q_1 \geq p_1 + 2$. Тогда у числа $n - p_1 q_1$, по предположению индукции, существует единственное разложение.

$$1 < n - p_1 q_1 = \tau_1 \dots \tau_m = p_1(p_2 \dots p_s - q_1) = q_1(q_2 \dots q_k - p_1)$$

$$\Rightarrow (n - p_1 q_1) : p_1 \Rightarrow q_2 \dots q_k : p_1 \Rightarrow \perp$$

– Через лемму Евклида:

Лемма 3.2 (Евклид).

$$mn : p \Rightarrow \begin{cases} m : p \\ n : p \end{cases}$$

Лемма 3.3 (Переформулировка).

$$\begin{cases} (m, k) = 1 \\ mn : k \end{cases} \Rightarrow n : k$$

Покажем, что из леммы Евклида следует ОТА:

$$n = p_1 \dots p_s = q_1 \dots q_k$$

$$n = q_1 Q : p_1 \Rightarrow \begin{cases} q_1 : p_1 \Rightarrow q_1 = p_1 \\ Q : p_1 \end{cases}$$

Получаем противоречие с min выбором n :

Доказательство переформулировки:

$$mx + ky = 1, nm : k$$

$$mnx + kny = n \Rightarrow n : k$$

□

Определение 3.2. $I \subset \mathbb{Z}$ — идеал в \mathbb{Z} , если:

- 1) $\forall a, b \in I, a + b \in I$
- 2) $\forall a \in I, \forall b \in \mathbb{Z}, ab \in I$

Доказательство леммы Евклида через Идеалы:

Заф. $m; I = \{a \mid ma \vdots p\}$. Легко понять, что это идеал, причём $0, n, p \in I$. Пусть $d = \min I$, покажем, что $I = \{cd \mid c \in \mathbb{Z}\}$:

Доказательство. $a \in I, a = qd + r, 0 < r < d \Rightarrow r \in I$ — противоречие с выбором d □

Т. к. $p \in I$, то:

- 1) $d = 1$, то тогда $m \vdots p$
- 2) $d = p, n \in I$, то тогда $n \vdots p$

□

□

4 Лекция 3

4.1 Доказательство границы Плоткина

(n, M, d) — код

- n — размерность
- M — кол-во слов
- d — минимальное хэммингово расстояние

Теорема 4.1 (Плоткина). *Если $2d > n$, то:*

$$M \leq \frac{2d}{2d - n}$$

Доказательство. Рассмотрим (n, M, d) -код, и запишем его слова как строки в матрице $M \times n$:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{M1} & a_{M2} & a_{M3} & \dots & a_{Mn} \end{pmatrix}$$

$$\begin{aligned}
a_{ij} &\in \{0, 1\} \\
\sum_{k=1}^n \sum_{i < j} |a_{ik} - a_{jk}| &= \sum_{i < j} \underbrace{\sum_{k=1}^n |a_{ik} - a_{jk}|}_{\text{Хэммингово расстояние между } i\text{-ым и } j\text{-ым словами}} \geq \sum_{i < j} d = \\
&= \frac{M(M-1)}{2} d
\end{aligned}$$

Обозначим для данного k буквой x число единиц в k -ом столбце. Тогда:

$$\sum_{k=1}^n \underbrace{\sum_{i < j} |a_{ik} - a_{jk}|}_{=x(M-x) \leq \frac{M^2}{4}} \leq \frac{nM^2}{4}$$

Получаем:

$$\begin{aligned}
M \frac{M-1}{2} d &\leq \frac{nM^2}{4} \\
2(M-1)d &\leq nM \\
2Md - 2d &\leq nM \\
M(2d - n) &\leq 2d \\
M &\leq \frac{2d}{2d - n}
\end{aligned}$$

□

4.2

Вспомним задачу прошлого семестра:

Задача 4.1. 30 чисел. Выбраны M_1, \dots, M_{15} — их 5-сочетания. Можно ли покрасить эти 30 чисел в красные и синие цвета, чтобы для $\forall i$ в M_i были и красные, и синие числа.

Зачем-то, давайте ответим, возможно ли раскрасить так, чтобы в каждом M_i разность кол-ва красных и синих шаров была по модулю ≤ 1 ? Пока что, сформулируем теорему:

Теорема 4.2. Пусть $R_n = \{1, 2, \dots, n\}$. Пусть:

$$M_1, \dots, M_n \subseteq R_n, \text{ (какие-то подмножества)}$$

Тогда \exists раскраска R_n в красные и синие цвета, при которой, для $\forall i$ в M_i разность между количеством красных и синих чисел по модулю $\leq 6\sqrt{n}$

Теорема доказывается в 4-ом семестре через матрицы Адамара. Пока что, покажем, что эта границы неуплучшаема.

Обозначение. χ — раскраска R_n в два цвета:

$$\chi: R_n \rightarrow \{-1, +1\}$$

$$\chi(M_i) = \sum_{j \in M_i} \chi(j)$$

Тогда утв-е теоремы звучит как:

$$\forall M_1, \dots, M_n \exists \chi: \forall i |\chi(M_i)| \leq 6\sqrt{n}$$

Теорема 4.3. Коль скоро существует матрица Адамара порядка n существует, то:

$$\exists M_1, \dots, M_n \forall \chi: \exists i |\chi(M_i)| \geq \frac{\sqrt{n}}{2}$$

Доказательство. Рассмотрим H , построим по ней совокупность M_1, \dots, M_n . Возьмём каждую строки матрицы H , построим соответствие:

$$M_i = \{j \mid 1 \leq j \leq n \wedge H_{ij} = 1\}$$

Покажем выполнение теоремы для этого набора. Наше утв-е эквивалентно следующему:

$$\forall \bar{v} \in \{+1, -1\}^n \exists \text{ координата вектора } \left(\frac{H+J}{2}\right) \bar{v}: |\bar{v}| \geq \frac{\sqrt{n}}{2}$$

J — матрица из единиц

Покажем выполнимость утв-я сначала для $H\bar{v}$ вместо $\left(\frac{H+J}{2}\right) \bar{v}$

$$H = (\bar{h}_1 \quad \bar{h}_2 \quad \dots \quad \bar{h}_n) \text{ — векторы-столбцы}$$

$$(H\bar{v}, H\bar{v}) = (v_1\bar{h}_1 + v_2\bar{h}_2 + \dots v_n\bar{h}_n, v_1\bar{h}_1 + v_2\bar{h}_2 + \dots + v_n\bar{h}_n) =$$

Выбирая ортонормированный базис, получаем:

$$= v_1^2(\bar{h}_1, \bar{h}_1) + \dots + v_n^2(\bar{h}_n, \bar{h}_n) = (\bar{h}_1, \bar{h}_1) + \dots + (\bar{h}_n, \bar{h}_n) = n^2$$

$$H\bar{v} = (L_1, \dots, L_n)$$

$$(H\bar{v}, H\bar{v}) = L_1^2 + \dots + L_n^2 = n^2 \Rightarrow \exists i: |L_i| \geq \sqrt{n}$$

Соответственно, для $\frac{1}{2}H\bar{v}$ получаем оценку $\geq \frac{\sqrt{n}}{2}$. Теперь докажем для $\left(\frac{H+J}{2}\right)\bar{v}$. Рассмотрим $(H+J)\bar{v}$:

$$\lambda = \sum_{i=1}^n v_i$$

$$(H+J)\bar{v} = \begin{pmatrix} L_1 + \lambda \\ \dots \\ L_n + \lambda \end{pmatrix}$$

$$((H+J)\bar{v}, (H+J)\bar{v}) = \underbrace{L_1^2 + \dots + L_n^2}_{n^2} + 2\lambda(L_1 + \dots + L_n) + \lambda^2 n$$

$$\sum_{i=1}^n L_i = \sum_{j=1}^n v_j \left(\sum_{i=1}^n h_{ij} \right) = v_1 n = \pm n$$

$$= n^2 \pm 2\lambda n + \lambda^2 n \Rightarrow$$

Максимум при $\lambda = \mp 1$, но т. к. размер матрица Адамара чётный, то реальный минимум в $\underbrace{\lambda = -2, 0}_{n^2 + 2\lambda n + \lambda^2 n}$ или $\underbrace{\lambda = 0, 2}_{n^2 - 2\lambda n + \lambda^2 n}$. В любом случае получаем, что:

$$((H+J)\bar{v}, (H+J)\bar{v}) \geq n^2$$

Следовательно хотя бы одна координата $\geq \sqrt{n}$. Оценка доказана. \square

Следствие. При $n \rightarrow +\infty, \exists M_1, \dots M_n \forall \chi \exists i |\chi(M_i)| \geq \frac{\sqrt{n}}{2}(1 + o(1))$