18. Разброс (уклонение, дискрепанс) системы подмножеств относительно раскраски. Теорема о верхней оценке (б/д).

Определение. Пусть $\mathcal{M} = \{M_1, M_2, ..., M_s\}$, где $\forall M_i \subset \mathcal{R}$ ($\mathcal{R}$ - конечное множество) – система подмножеств, а χ – раскраска множества $\mathcal{R}$ в 2 цвета.

$$\chi(j) = \begin{cases} 1, & \text{если } j\text{-ый элемент } \mathcal{R} \text{ окрашен в первый цвет} \\ -1, & \text{если } j\text{-ый элемент } \mathcal{R} \text{ окрашен во второй цвет} \end{cases}$$

Тогда *разброс (уклонение) системы подмножеств* $\mathcal{M}$ относительно раскраски χ обозначается $disc(\mathcal{M}, \chi)$, и по определению

$$disc(\mathcal{M}, \chi) = \max_{i=1,...,s} |\sum_{j \in M_i} \chi(j)|$$

Равно максимальной разности между количеством элементов покрашеных в разные цвета на определённых множествах.

Определение. Пусть $\mathcal{M} = \{M_1, M_2, ..., M_s\} \subset \mathcal{R}$ – система подмножеств. Тогда разброс (уклонение) системы подмножеств $\mathcal{M}$ обозначается $disc(\mathcal{M})$, и по определению

$$disc(\mathcal{M}) = \min_{\chi} disc(\mathcal{M}, \chi)$$

Теорема (о верхней оценке). *Если $|\mathcal{R}| = n$, то $\forall \mathcal{M} : |\mathcal{M}| \le n$ верно, что $disc(\mathcal{M}) \le 6\sqrt{n}$*

19. Коды, исправляющие ошибки. Расстояние Хэмминга. Понятие (n,M,d)-кода. Число ошибок, исправляемых кодом. Граница Хэмминга.

В этом билете n – число символов (0 и 1) в каждом кодовом слове.
Для канала связи известно, что на каждое кодовое слово приходится не более k ошибок. (под ошибкой подразумевается замена 0 на 1, и наоборот)
M – число кодовых слов. Очевидно, что $M \le 2^n$.

Определение (Расстояние Хэмминга). Пусть $\vec{a} = a_1a_2...a_n$, $\vec{b} = b_1b_2..b_n$ – кодовые слова. Расстояние Хэмминга между $\vec{a}$ и $\vec{b}$ обозначается $d(\vec{a}, \vec{b})$. По определению

$$d(\vec{a}, \vec{b}) = \sum_{i=1}^{n} I_{\{a_i \ne b_i\}}$$

- количество позиций, на которых символы отличаются.

Пусть d – минимальное расстояние между словами, то есть

$$d = \min_{a,b} d(\vec{a}, \vec{b})$$

- самое маленькое расстояние, которое можно построить в рамках определённого кода.

Замечание. *$d(\vec{a}, \vec{b})$ можно рассматривать как метрику, соответственно можно ввести понятие шара:*

$$B_r(\vec{a}) = \{\vec{b} : d(\vec{a}, \vec{b}) \le r\}$$

Объемом шара назовем количество кодовых слов в нём. Так как в допускается не более чем r ошибок, а количество способов выбрать i позиций для i ошибок соответсвенно равно C_n^i, то

$$V(B_r(\vec{a})) = \sum_{i=0}^{r} C_n^i$$

Определение. (n, M, d)-код это код, в котором каждое слово длины n, всего слов M, минимально расстояние между кодовыми словами d

Утверждение. *(n, M, d)-код исправляет вплоть до $[\frac{d-1}{2}]$ ошибок.*

▲. Если у каждого шара $2r < d$, то если канал допускает не более r ошибок, слово однозначно восстанавливается, поскольку шары не пересекаются
Пусть $r = [\frac{d-1}{2}]$. Тогда утверждение выполнено. ■

Замечание (Граница Хэмминга для (n, M, d)-кода)**.**

$$|M| \le \frac{2^n}{\sum\limits_{i=0}^{r} C_n^i}, r = \left[\frac{d-1}{2}\right]$$

▲. $|M| \cdot \sum\limits_{i=0}^{r} C_n^i \le 2^n$, так как сумма объемов непересекающихся шаров не больше объема всего пространства. ■

20. Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_1 \le \lambda_2$. Постулат Бертрана (б/д). Теорема Адамара, Валле-Пуссена (б/д). «Дырки» между соседними простыми числами (б/д).

Распределение простых чисел в натуральном ряде

Определение.

$$\pi(x) = \sum_{p \le x} 1 \text{— количество простых чисел, не превосходящих x.}$$
$$\theta(x) = \sum_{p \le x} ln(p)$$
$$\psi(x) = \sum_{(\alpha, p): p^\alpha \le x} ln(p)$$

Теорема.(о равенстве верхних и нижних пределов (формулировка))

$$\lambda_1 = \overline{\lim_{x \leftarrow \infty}} \frac{\theta(x)}{x}, \lambda_2 = \overline{\lim_{x \leftarrow \infty}} \frac{\psi(x)}{x}, \lambda_3 = \overline{\lim_{x \leftarrow \infty}} \frac{\pi(x)}{x/ln(x)}$$

За μ_i обозначим соответствующие нижние пределы.
Тогда $\lambda_1 = \lambda_2 = \lambda_3, \mu_1 = \mu_2 = \mu_3$.

Утверждение. $\lambda_1 \leq \lambda_2$

$$\blacktriangle\ \lambda_1 = \overline{\lim_{x\leftarrow\infty}} \frac{\theta(x)}{x} = \overline{\lim_{x\leftarrow\infty}} \frac{\sum\limits_{p\leq x} ln(p)}{x} \leq \overline{\lim_{x\leftarrow\infty}} \frac{\sum\limits_{(\alpha,p):p^\alpha\leq x} ln(p)}{x} = \overline{\lim_{x\leftarrow\infty}} \frac{\psi(x)}{x} = \lambda_2\ \blacksquare$$

Теорема.(Постулат Бертрана (формулировка))

$$\forall x\ \exists p : p \in [x, 2x]$$

Теорема.(Адамара, Валле-Пуссена)

$$\pi(x) \sim \frac{x}{lnx}$$

«Дырки» между соседними простыми

Теорема.(Чебышёв) $\exists a, b : 0 < a < b < \infty$ такие, что $\frac{ax}{ln(x)} \leq \pi(x) \leq \frac{bx}{ln(x)}$

На лекции Райгородский указал конкретные границы: $a = ln(2), b = 4ln(2)$

21. Степень вхождения простого числа в факториал и центральный биномиальный коэффициент. Неравенство для C_{2n}^n

Лемма.

$$[2x] - 2[x] \leq 1$$

где $[x]$ - целая часть x.

$\blacktriangle$.

$$2x = 2([x] + \{x\}) = 2[x] + 2\{x\},$$
$$[2x] - 2[x] = 2[x] + [2\{x\}] - 2[x] = [2\{x\}] \leq 1$$

$\blacksquare$

Теорема.

$$C_{2n}^n \leq \prod_{p\leq 2n} p^{[\log_p(2n)]}$$

$\blacktriangle$. Центральный биномиальный коэффициент: $C_{2n}^n = \frac{(2n)!}{n!\cdot n!}$

$$C_{2n}^n = \frac{(2n)!}{n!\cdot n!} = \prod_{p\leq 2n} p^{\left[\frac{2n}{p}\right]+\left[\frac{2n}{p^2}\right]+...-2\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+...\right)},$$

где $\left[\frac{2n}{p}\right]+\left[\frac{2n}{p^2}\right]+...$ - **степень вхождения простого числа p в разложение факториала** $(2n)!$ на простые множители, а $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ...$ - степень вхождения простого числа p в разложение $(n)!$ на простые множители.

$$C_{2n}^n = \prod_{p\leq 2n} p^{\left[\frac{2n}{p}\right]+\left[\frac{2n}{p^2}\right]+...-2\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+...\right)} = \prod_{p\leq 2n} p^{\left(\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\right)+\left(\left[\frac{2n}{p^2}\right]-2\left[\frac{n}{p^2}\right]\right)+...}$$

Заметим, что таких слагаемых не больше $[\log_p(2n)]$ и воспользуемся леммой.

$$C_{2n}^n = \prod_{p\leq 2n} p^{\left(\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\right)+\left(\left[\frac{2n}{p^2}\right]-2\left[\frac{n}{p^2}\right]\right)+...} \leq \prod_{p\leq 2n} p^{[\log_p(2n)]}$$

$\blacksquare$

22. Показатель. Показатель элемента из множества $\mathbb{Z}_m$ делит $\varphi(m)$. Первообразный корень (определение и значения при $m \leq 7$). Пример модуля, по которому не существует первообразного корня. Теорема о существовании первообразного корня (б/д).

Определение. *Показатель (порядок)* числа a по модулю m обозначается $ord_m(a)$ и по определению $ord_m(a) = \min\{\delta \in \mathbb{N} : a^\delta \equiv 1 \pmod m\}$.

Утверждение. $\varphi(m) \equiv 0 \pmod \delta$ *(то есть показатель элемента делит $\varphi(m)$)*

▲. Предположим, что это не так. Тогда $\varphi(m) = k\delta + r, r \in (0, \delta)$. Тогда $1 \equiv a^{\varphi(m)} = a^{k\delta+r} \equiv a^r \pmod m \Rightarrow$ противоречие с определением показателя. ■

Определение. g называется *первообразным корнем по модулю m*, если его показатель равен $\varphi(m)$.

Значения первообразного корня для $m \leq 7$

m	Первообразный корень
2	1
3	2
4	3
5	2
6	5
7	3

Однако для m = 8 первообразного корня не существует.

Теорема (Теорема о существовании первообразного корня (б/д)). *Первообразный корень существует только для $m \in \{2, 4, p^\alpha, 2p^\alpha\}$, где p – простое нечетное, $\alpha \in \mathbb{N}$.*

23. Индексы. Корректность определения в случае первообразного корня. Таблицы индексов. Решение степенных сравнений (умение).

Определение. Зафиксируем первообразный корень g по модулю m. Пусть $(a, m) = 1$. *Индексом* $\gamma = ind_g(a)$ числа a по модулю m при основании g называется такое минимальное число γ, что $a \equiv g^\gamma \pmod m$. Индекс можно интерпретировать как дискретный логарифм.

Теорема (Корректность определения в случае первообразного корня). *Пусть g – первообразный корень по модулю m. Степени $g : g^l, 0 \leq l < \varphi(m)$ несравнимы между собой и образуют приведённую систему вычетов. Из этого следует, что индекс для первообразного корня определён корректно.*

▲. Докажем, что все степени g не сравнимы по модулю m.
Предположим противное: пусть $\exists k, m : g^k \equiv_m g^m$. (Без ограничения общности $0 \leq m < k < \varphi(m)$) Тогда $g^k - g^m \equiv_m 0$

$$g^k - g^m = g^k(g^{k-m} - 1) \equiv_m 0$$

Получается, что $g^{k-m} \equiv_m 1$, но $k - m < \varphi(m)$, а значит g – не первообразный корень. Противоречие. $\blacksquare$

Утверждение 1 (б/д). *Пусть* $\varphi(m) = p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}$ *– каноническое разложение числа* $\varphi(m)$ *на простые множители,* $(g, m) = 1$. *В этом случае* g *– первообразный корень в* $\mathbb{Z}_m$ *тогда и только тогда, когда* g *НЕ является решением ни одного из сравнений* $g^{\frac{\varphi(m)}{p_k}} \equiv 1 \pmod m$ *при* $k = 1, 2, ..., s$.

Утверждение 2 (б/д). *Сравнение вида* $x^n \equiv a \pmod m$, *где* m *имеет вид* p^α *или* $2p^\alpha$, $(a, m) = 1, d := (n, \varphi(m))$ *разрешимо тогда и только тогда, когда* $d | ind_g(a)$, *где* g *– первообразный корень. Более того, если сравнение разрешимо, то оно имеет* d *решений.*

Утверждение 3 (б/д). *Пусть* $k = ord(g)$. $g^{k_1} \equiv g^{k_2} \pmod m$ *тогда и только тогда, когда* $k_1 \equiv k_2 \pmod k$

Задача. Алгоритм решения сравнения $x^n \equiv a \pmod m$.
(только если по модулю m существует первообразный корень, то есть $m \in \{2, 4, p^\alpha, 2p^\alpha\}$)
1) Находим первообразный корень g (любой, на практике обычно минимальный) с помощью утверждения 1.
2) Находим $ind_g(a)$ перебором (достаточно перебрать значения от 1 до $\varphi(m)$)
3) С помощью утверждения 2 проверяем, есть ли решения у сравнения.
4) Сравнение можно переписать в виде $g^{n \cdot ind_g(x)} \equiv x^n \equiv a \equiv g^{ind_g(a)} \pmod m$
5) Используя утверждение 3, переписываем сравнение в виде (напоминание: $ord(g) = \varphi(m)$):

$$n \cdot ind_g(x) \equiv ind_g(a) \pmod{\varphi(m)}$$

6) Решая линейное сравнение относительно $ind_g(x)$ в пункте 5, получаем решения $ind_g(x) \in \{k_1, ..., k_l\}$. Тогда решением исходного сравнения будут $x \in \{g^{k_1}, ..., g^{k_l}\}$.

Примеры решения степенных сравнений:

Пример 1 $x^8 \equiv 5 \pmod{17}$
Это сравнение вида $x^n \equiv a \pmod m$
$n = 8$, $\varphi(m) = \varphi(17) = 16$
$d = (n, \varphi(m)) = (8, 16) = 8$
Найдем первообразный корень (перебором):
$\varphi(m) = 16 = 2^4$.
$g = 3$ не является решением $g^{\frac{\varphi(17)}{2}} = g^8 \equiv 1 \pmod{17}$, следовательно, $g = 3$ – первообразный корень.
Подбором находим, что $ind_g(a) = ind_3(5) = 5, ind_3(5)$ не делится на $d = 8$. Значит, решений у сравнения $n \cdot ind_g(x) \equiv ind_g(a) \pmod{\varphi(m)}$ нет.

Пример 2 $x^4 \equiv 4 \pmod{17}$
$\varphi(17) = 16, d = (4, 16) = 4, g = 3$ – первообразный корень
$ind_3(4) = 12, ind_3(4)$ делится на $d = 4$. Значит, есть $d = 4$ различных решения.
Решаем сравнение $4 \cdot ind_3(x) \equiv 12 \pmod{16}$, получаем, что $ind_3(x) \in \{3, 7, 11, 15\}$.
Тогда искомые решения: $x \in \{g^3, g^7, g^{11}, g^{15}\} = \{10, 11, 7, 6\}$ (по модулю 17).

24. Теорема Дирихле о диофантовых приближениях (формулировка и доказательство любым способом).

Теорема (Дирихле). *Если* α *– иррациональное, то существует бесконечно много различных* $\frac{p}{q} \in \mathbb{Q} : \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$.

Замечание. $\frac{p}{q}$ *может быть как сократимой, так и несократимой дробью*

$\blacktriangle$. Рассмотрим $Q \in \mathbb{N}$. Разобьём отрезок $[0;1]$ на Q частей.
Пусть $A = \{\{\alpha x\} : x \in \{0, 1, ..., Q\}\}$, где $\{\cdot\}$ – дробная часть числа ($\{x\} = x - [x]$). $|A| = Q + 1$.
По принципу Дирихле $\exists x_1, x_2 \in 0, 1, ..., Q : |\{\alpha x_1\} - \{\alpha x_2\}| \leq \frac{1}{Q}$, то есть x_1, x_2 попадут в один отрезок. Без ограничения общности $x_1 > x_2$

$$|\{\alpha x_1\} - \{\alpha x_2\}| = |\alpha x_1 - [\alpha x_1] - \alpha x_2 + [\alpha x_2]| = |\alpha(x_1 - x_2) - ([\alpha x_1] - [\alpha x_2])| \leq \frac{1}{Q}$$

Положим $q = x_1 - x_2, p = [\alpha x_1] - [\alpha x_2]$, при этом $q \leq Q$.

$$|\alpha q - p| \leq \frac{1}{Q}$$

Разделим неравенство на q.

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}$$

Таким образом, мы доказали существование приближения. Докажем, что их бесконечно много.
Пусть $a = \left|\alpha - \frac{p}{q}\right|, a > 0$. Выберем Q' так, чтобы $\frac{1}{Q'} < a$.
По доказанному $\exists p', q' : \left|\alpha - \frac{p'}{q'}\right| \leq \frac{1}{q'Q'}$.
Получается, что $\frac{p'}{q'}$ аппроксимирует $\alpha : \left|\alpha - \frac{p'}{q'}\right| \leq \frac{1}{q'^2}$.
С другой стороны,

$$\left|\alpha - \frac{p'}{q'}\right| \leq \frac{1}{Q'} < a = \left|\alpha - \frac{p}{q}\right|$$

.
Получается, что $\frac{p'}{q'}$ и $\frac{p}{q}$ – различные и аппроксимируют α. Повторяем этот процесс, и получаем, что существует бесконечно много различных аппроксимаций. $\blacksquare$