Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ (БИЛЕТЫ К ЭКЗАМЕНУ)

II СЕМЕСТР

Лекторы: *Мусатов Даниил Владимирович*
Райгородский Андрей Михайлович

Авторы:
Николай Спицын
Артемий Клячин
Полина Подзорова
Дмитрий Савичев
Полина Чубенко
Ирина Климанова

Даниил Дрябин
Проект на Github

весна 2021

Содержание

15 Матрицы Адамара. Определение. Равносильность попарной ортогональности строчек и попарной ортогональности столбцов. Канонический вид (нормальная форма). Достижение верхней оценки в неравенстве Адамара. **2**

16 Существование матриц Адамара при $n = 1$ и 2. Необходимость делимости на 4 при $n > 3$. Гипотеза Адамара. Комбинаторная переформулировка гипотезы (через систему подмножеств мощности $\frac{n}{2}$ в множестве из $n-1$ элемента). Утверждение о плотности матриц Адамара в натуральном ряде (б/д). **2**

17 Попытка построить матрицу для $n = 2^k$ путем наложения единиц на минус единицы (получается только k строчек). Решение для $n = 2^k$ через кронекеровское произведение. **3**

18 Разброс (уклонение, дискрепанс) системы подмножеств относительно раскраски. Теорема о верхней оценке (б/д). **4**

19 Коды, исправляющие ошибки. Расстояние Хэмминга. Понятие (n,M,d)-кода. Число ошибок, исправляемых кодом. Граница Хэмминга. **4**

20 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_1 \leqslant \lambda_2$. Постулат Бертрана (б/д). Теорема Адамара, Валле-Пуссена (б/д). «Дырки» между соседними простыми числами (б/д). **5**

21 Степень вхождения простого числа в факториал и центральный биномиальный коэффициент. Неравенство для C_{2n}^n **6**

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

23 Индексы. Корректность определения в случае первообразного корня. Таблицы индексов. Решение степенных сравнений (умение). **7**

24 Теорема Дирихле о диофантовых приближениях (формулировка и доказательство любым способом). **9**

25 Конечные цепные дроби. Каноническая запись. Подходящие дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей (б/д). Следствия: несократимость подходящих дробей, возрастание подходящих дробей с четными номерами и убывание подходящих дробей с нечетными номерами. **10**

26 Рекуррентные соотношения для числителей и знаменателей подходящих дробей (доказательство). **11**

27 Определение бесконечной цепной дроби. Доказательство сходимости соответствующих подходящих цепных дробей (можно пользоваться без доказательства соотношениями на их коэффициенты). **12**

28 Бесконечные периодические цепные дроби. Теорема о периодичности дроби для квадратичной иррациональности (доказательство в одну сторону). Умение находить периодическую цепную дробь по её значению, и наоборот, нахождение значения дроби по её периоду. **12**

29 Квадратичные иррациональности. Множество Z[$\sqrt{m}$ **13**

30 Пара (a, b), где a + b$\sqrt{2}$ = $(1+\sqrt{2})^n$ является решением уравнения Пелля $a^2 - 2b^2 = \pm 1$. **14**

31 Связь между решениями уравнения Пелля $a^2 - 2b^2 = \pm 1$ и элементами $Z[\sqrt{2}]$ нормой 1. **15**

32 Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Степень алгебраического числа. Теорема Лиувилля (б/д). **15**

33 Определение решётки (эквивалентность двух определений) и дискретного подмножества. Определитель решётки. Независимость значения определителя от выбора базиса. **15**

34 Определение решётки и его определителя. Решётка $\Lambda_{\overline{a}}$ и её определитель. **16**

35 Определение равномерной распределённой последовательности по модулю 1. Является ли $\sqrt{n}$ р.р. (mod 1) последовательностью? **17**

36 Определение равномерной распределённой последовательности по модулю 1. Является ли р.р. (mod 1) последовательность a^n при a < 1? **17**

37 Определение всюду плотности. Последовательность $\ln n$ всюду плотна на $[0,1]$... **18**

38 Определение всюду плотности. Если последовательность равномерно распределена по модулю 1, то она и всюду плотна. **18**

39 Тригонометрические суммы. Критерий Вейля для р.р. (mod 1) (формулировка). Последовательность αn при иррациональном α является р.р. (mod 1). Что происходит при рациональном α? **18**

40 Определение равномерной распределённой последовательности по модулю 1. Являются ли р.р. (mod 1) последовательности а) $1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \ldots$ б) $\frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}, \ldots$. **19**

41 Определение равномерной распределённой последовательности по модулю 1. Пусть последовательность x_n р.р. (mod 1) и m — фиксированное целое число, не равное нулю. Докажите, что последовательность mx_n также р.р. (mod 1). Верно ли, что если m — не целое, то это не верно? **19**

42 Описание алгоритма AKS (6 шагов). Лемма об оценке r (б/д). Оценка сложности алгоритма. Тождество $(X+a)^p = X^p + a (\mathrm{mod}\, p)$. **20**

49 Китайская теорема об остатках **21**

51 Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество для $\left(\frac{a}{p}\right)$ **21**

52 Сравнения второй степени. Квадратичные вычеты и невычеты. Формула для $\left(\frac{2}{p}\right)$ (тождеством с суммой по $\left[\frac{2ax}{p}\right]$ можно пользоваться без доказательства). ... **23**

53 Матрицы Адамара. Кронекеровское произведение и общая формулировка про $A \cdot B$. **24**

54 Матрицы Адамара. (Первая) конструкция Пэли с квадратичными вычетами при $n = p+1, p = 4m+3$. **25**

55 Матрицы Адамара. (Вторая) конструкция Пэли с квадратичными вычетами при $n = 2p+2, p = 4m+1$. **25**

56 (n, M, d)-коды. Граница Плоткина **27**

57 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_2 \geqslant \lambda_3$. **28**

58 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_3 \leqslant \lambda_1$. **29**

59 Порядки(показатели) элементов в системах вычетов. Равенство $ord(g^l) = \frac{ord(g)}{gcd(l, ord(g))}$. Следствие: если есть порядок k, то есть порядки и всех делителей k. . **29**

69 Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Теорема Лиувилля (б/д). Конструкция трансцендентного числа с помощью цепной дроби и теоремы Лиувилля. Сводка результатов о трансцендентности: $e, \pi, e + \pi, \pi + e^\pi, \alpha^\beta$ (теорема Гельфонда), вывод про e^π из теоремы Гельфонда. **30**

70 Умение: решать уравнения Пелля. **31**

71 Иррациональность числа e. **33**

72 Определение решётки и дискретного подмножества. Любая дискретная подгруппа $\mathbb{R}^n$ является решёткой. **33**

73 Двумерная теорема Минковского. Ее уточнение для замкнутых множеств (б/д). **34**

74 Применение двумерной теоремы Минковского для передоказательства теоремы Дирихле. Теорема Дирихле о совместном диофантовом приближении (б/д) **35**

75 Критический определитель решётки. Переформулировка теоремы Минковского через критический определитель. Теорема Минковского–Главки и история ее улучшений (б/д). Многомерный октаэдр, его объём. **35**

76 Равномерно распределенные последовательности (mod 1): три эквивалентные формулировки. **35**

77 Является ли ln n р.р. (mod 1) последовательностью? **36**

78 Определение р.р. (mod 1) последовательности. Вывод интегрального признака из того, что последовательность р.р. (mod 1). Формулировка интегрального признака через комплекснозначную функцию (б/д). **36**

79 Определение р.р. (mod 1) последовательности. Вывод р.р. (mod 1) последовательности из интегрального признака. Формулировка интегрального признака через комплекснозначную функцию (б/д). **36**

81 Сумма Гаусса **37**

82 Асимптотическая оценка $[1, 2, \ldots, n]$ снизу. Более грубая оценка, верная для $n > 7$. (б/д) **38**

83 Алгоритм AKS. Определение и неравенства, связывающие числа $p, r, \log_2 n$ (б/д). Определение множеств I, P. Определение группы G, неравенство $|G| > \log_2^2 n$. Утверждения о делителе $h(X)$ многочлена $X^r - 1$ (б/д). Группа $\mathcal{G}$. **39**

84 Алгоритм AKS. Верхняя оценка на r (б/д). Обоснование неравенства $p > r > \log_2^2 n$ для подходящего делителя p числа n. Вывод тождества $(X + a)^{n/p} = X^{n/p} + a \pmod{X^r - 1, p}$. Определение перестановочности многочлена и числа. Утверждения о свойствах перестановочности. **40**

87 Нижняя оценка разброса (уклонения) величиной $\frac{\sqrt{n}}{2}$ с помощью матриц Адамара. **41**

88 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема Чебышёва (верхняя оценка) **42**

89 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема Чебышёва (нижняя оценка) **43**

90 Постулат Бертрана для n » 0. ..... **43**

91 Показатели. Первообразные корни. Существование по модулю p. **44**

92 Показатели. Первообразные корни. Существование по модулю p^α, $\alpha \geqslant 2$: формулировка и доказательство леммы. Существование по модулю $2p^\alpha$. **45**

93 Показатели. Первообразные корни. Существование по модулю p^α, $\alpha \geqslant 2$: формулировка леммы (б/д) и вывод существования из неё. Существование по модулю $2p^\alpha$. **46**

94 Показатели. Первообразные корни. Несуществование по модулю 2^n, $n > 3$. **46**

95 Показатели. Первообразные корни. Несуществование по модулям, отличным от $2^n, p^\alpha, 2p^\alpha$. **47**

96 Теорема Лиувилля ... **47**

97 Доказательство иррациональности чисила e. Тождество Эрмита ... **48**

98 Доказательство трансцендентности числа e ... **48**

100 Доказательство теоремы Минковского-Главки для октаэдра: переформулировка условия теоремы через Λ_a и неравенства на p и n. Сведение теоремы к неравенству **49**

101 Теорема Минковского-Главки для октаэдра (формулировка). Доказательство неравенства. ... **51**

103 Алгоритм AKS. Верхняя оценка на r: вывод из утверждения о нижней оценке $[1, 2, \ldots, n]$ ... **52**

104 Алгоритм AKS. Определение и неравенства, связывающие параметры $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| > C_{t+l}^{t-1}$ ... **52**

105 Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы G, $\mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| \leqslant n^{\sqrt{t}}$ при $n \neq p^k$. ... **53**

106 Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $C_{t+l}^{t-1} > n^{\sqrt{t}}$. ... **53**

15 Матрицы Адамара. Определение. Равносильность попарной ортогональности строчек и попарной ортогональности столбцов. Канонический вид (нормальная форма). Достижение верхней оценки в неравенстве Адамара.

Определение: *Матрицей Адамара* порядка n называется матрица H_n размера $n \times n$ такая, что все её элементы равны ± 1 и выполнено следующее свойство: $H_n H_n^T = nE_n$. Можно переформулировать так: матрица Адамара — это матрица из ± 1, у которой все строки попарно ортогональны.

Утверждение (задача 20.1): Ортогональность строк матрицы Адамара равносильна ортогональности ее столбцов

▲

$$H_n H_n^T = nE_n \Rightarrow \frac{H_n}{\sqrt{n}} \frac{H_n^T}{\sqrt{n}} = E_n$$

Получили, что $\frac{H_n}{\sqrt{n}}$ и $\frac{H_n^T}{\sqrt{n}}$ - взаимно-обратные $\Rightarrow$ их можно переставить местами. Условие $H_n^T H_n = nE_n$ равносильно ортогональности столбцов (в обратную сторону равносильность доказывается аналогично). ■

Замечание: строки/столбцы матрицы Адамара можно менять местами, умножать на -1, при этом она останется матрицей Адамара.

Определение: Матрицы Адамара, получаемые друг их друга многократным применением таких операций называются *эквивалентными. Каноническим видом (нормальной формой)* матрицы Адамара называется эквивалентная ей матрица, в которой первая строка и первый столбец состоят только из 1.

Неравенство Адамара: Если у действительной матрицы A размера $n \times n$ все элементы по модулю меньше 1, то $|\det A| \leqslant n^{n/2}$.

Утверждение (задача 20.2): Для матриц Адамара в этом неравенстве достигается верхняя оценка, то есть $|\det A| = n^{n/2}$

▲ $\det(nE_n) = \det(H_n H_n^T) = \det H \det H^T = (\det H)^2 \Rightarrow (\det H_n)^2 = n^n \Rightarrow \det H_n = n^{n/2}$ ■

16 Существование матриц Адамара при $n = 1$ и 2. Необходимость делимости на 4 при $n > 3$. Гипотеза Адамара. Комбинаторная переформулировка гипотезы (через систему подмножеств мощности $\frac{n}{2}$ в множестве из $n-1$ элемента). Утверждение о плотности матриц Адамара в натуральном ряде (б/д).

1. $n = 1$: (1)
2. $n = 2$: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Утверждение (задача 20.5): Если $n > 2$ - порядок матрицы Адамара, то $n \vdots 4$.

▲ Так как любую матрицу Адамара можно привести к каноническому виду, рассмотрим нормальную форму матрицы Адамара порядка n. Из того, что первая строка состоит только из единиц следует то, что во всех остальных строках будет $\frac{n}{2}$ единиц и $\frac{n}{2}$ минус единиц (иначе не будет ортагональности с первой строкой).

Рассмотрим две произвольные строчки. Пусть у них на одних и тех же местах стоят x единиц. Тогда мест где в первой строке стоит -1, а во второй 1: $\frac{n}{2} - x$ (столько же когда в первой строке 1, а во второй -1). Получается, что мест где в обоих строках стоит -1: $n - (\frac{n}{2} - x) - (\frac{n}{2} - x) - x = x$. Распишем скалярное произведение этих строк:

$1 \cdot 1 \cdot x + (-1) \cdot (-1) \cdot x + 1 \cdot (-1) \cdot (\frac{n}{2} - x) + (-1) \cdot 1 \cdot (\frac{n}{2} - x) = 4x - n = 0 \Rightarrow x = \frac{n}{4} \Rightarrow n \vdots 4$ ■

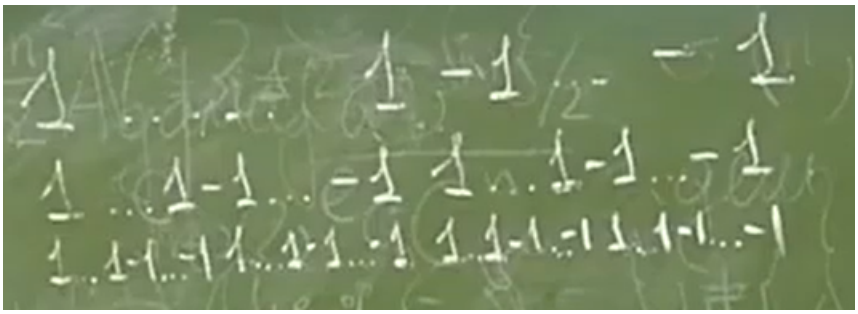
Гипотеза Адамара: Матрица Адамара существует для любого числа вида $4k$.

Комбинаторная переформулировка: В множестве мощности n существует $n - 1$ подмножество мощности $\frac{n}{2}$, такие что каждые 2 подмножества имеют ровно $\frac{n}{4}$ общих элементов.

Утверждение (о плотности в натуральном ряде): $\forall n$ на отрезке $[n; n + O(n^{0.525})]$ есть порядки матриц Адамара.

17 Попытка построить матрицу для $n = 2^k$ путем наложения единиц на минус единицы (получается только k строчек). Решение для $n = 2^k$ через кронекеровское произведение.

"Наивный подход": возьмем первую строчку состоящую только из 1, вторую - первая половина из единиц, вторая из минус единиц. Повторяем те же действия с каждой из полученных половин (делаем так чтобы каждая половина давала вклад ноль в скалярное произведение). Так как мы каждый раз увеличиваем количество блоков из одной и той же цифры в строке в 2 раза, то через k шагов мы получим строку в которой будут чередоваться 1 и -1 и продолжить процесс мы не сможем.



Конструктивный подход: Воспользуемся определением кронекеровского произведения и утверждением о том, что кронекеровское произведение матриц Адамара является матрицей Адамара (см. билет 53):

$$H_4 = H_2 \otimes H_2$$

$$\dots$$

$$H_{2^k} = H_{2^{k-1}} \otimes H_2$$

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

Определение 18.1. 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 18.2. 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 18.1 (о верхней оценке)**.** *Если* $|\mathcal{R}| = n$*, то* $\forall \mathcal{M} : |\mathcal{M}| \leqslant n$ *верно, что* $disc(\mathcal{M}) \leqslant 6\sqrt{n}$

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 $M \leqslant 2^n$.

Определение 19.1 (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

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

- 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:

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

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

Утверждение 19.1. *(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)**.**

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

▲. $|M| \cdot \sum\limits_{i=0}^{r} C_n^i \leqslant 2^n$, 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 $\lambda_1 \leqslant \lambda_2$. Постулат Бертрана (б/д). Теорема Адамара, Валле-Пуссена (б/д). «Дырки» между соседними простыми числами (б/д).

Распределение простых чисел в натуральном ряде
Определение

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

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. $\lambda_1 \leqslant \lambda_2$

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

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 $\frac{ax}{ln(x)} \leqslant \pi(x) \leqslant \frac{bx}{ln(x)}$
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 21.1.

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

где $[x]$ *- целая часть* x.

▲.

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

□

Теорема 21.1.

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

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

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

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

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

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

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

□

22 Показатель. Показатель элемента из множества $\mathbb{Z}_m$ делит $\varphi(m)$. Первообразный корень (определение и значения при $m \leqslant 7$). 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 22.1. $\varphi(m) \equiv 0 \pmod \delta$ *(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 $m \leqslant 7$

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

Однако для m = 8 первообразного корня не существует.

Теорема 22.1 (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 23.1 (Корректность определения в случае первообразного корня)**.** *Пусть* g *– первообразный корень по модулю* m*. Степени* $g : g^l, 0 \leqslant l < \varphi(m)$ *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 $0 \leqslant m < k < \varphi(m)$) 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. □

Утверждение 23.1 (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 23.2 (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 23.3 (б/д). *Пусть $k = ord(g)$. $g^{k_1} \equiv g^{k_2} \pmod m$ тогда и только тогда, когда $k_1 \equiv k_2 \pmod k$*

Пример. 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 24.1 (Дирихле). *Если α – иррациональное, то существует бесконечно много различных $\frac{p}{q} \in \mathbb{Q} : \left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q^2}$.*
Замечание. $\frac{p}{q}$ может быть как сократимой, так и несократимой дробью

▲. 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 $\exists x_1, x_2 \in 0, 1, ..., Q : |\{\alpha x_1\} - \{\alpha x_2\}| \leqslant \frac{1}{Q}$, то есть x_1, x_2 попадут в один отрезок. Без ограничения общности $x_1 > x_2$

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

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

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

Разделим неравенство на q.

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

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 $\exists p', q' : \left|\alpha - \frac{p'}{q'}\right| \leqslant \frac{1}{q'Q'}$.
Получается, что $\frac{p'}{q'}$ аппроксимирует $\alpha : \left|\alpha - \frac{p'}{q'}\right| \leqslant \frac{1}{q'^2}$.
С другой стороны,

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

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

25 Конечные цепные дроби. Каноническая запись. Подходящие дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей (б/д). Следствия: несократимость подходящих дробей, возрастание подходящих дробей с четными номерами и убывание подходящих дробей с нечетными номерами.

Опр *Конечной цепной дробью* называется выражение вида

$[a_0; a_1, a_2, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_n}}}$, где $a_0 \in Z, a_i \in N \ \forall i >= 1$

a_i *— элементы цепной дроби, или неполные частные*
Каноническая запись цепной дроби определяется индуктивно:

1. $[a_0] = \frac{a_0}{1}$
2. Пусть для всех дробей с n элементами каноническая запись определена
3. $[a_0; a_1, ..., a_n] = a_0 + \frac{1}{[a_1; a_2, ..., a_n]} = a_0 + \frac{1}{p/q} = \frac{pa_0+q}{p}$

Опр
$[a_0; a_1, ..., a_k] = \frac{p_k}{q_k}$ - k-ая подходящая дробь

Теорема
$p_{k+2} = a_{k+2}p_{k+1} + p_k$
$q_{k+2} = a_{k+2}q_{k+1} + q_k$

Следствие 1

1. $\frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}} = \frac{(-1)^{k+1}}{q_{k+1}q_{k+2}}$
2. Каноническая запись цепной дроби является несократимой

▲
$p_{k+2} - p_k = a_{k+2}p_{k+1}, \ q_{k+2} - q_k = a_{k+2}q_{k+1}$

$\frac{p_{k+2}-p_k}{q_{k+2}-q_k} = \frac{a_{k+2}p_{k+1}}{a_{k+2}q_{k+1}}$

$p_{k+2}q_{k+1} - p_kq_{k+1} = p_{k+1}q_{k+2} - p_{k+1}q_k$

Обозначим ЛЧ $b(k+2)$, ПЧ -$b(k+1)$
$b(1) = p_1q_0 - q_1p_0 = (a_0a_1 + 1) * 1 - a_1a_0 = 1$

$p_{k+2}q_{k+1} - q_{k+2}p_{k+1} = (-1)^{k+1} \Longrightarrow \frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}} = \frac{(-1)^{k+1}}{q_{k+1}q_{k+2}}$

Предположим, что каноническая запись цепной дроби сократима. Тогда $\frac{p_{k+2}}{q_{k+2}}$ - сократима, тогда $\exists \ d: \ p_{k+2}, q_{k+2} \vdots d \Longrightarrow p_{k+2}q_{k+1} - q_{k+2}p_{k+1} \vdots d$. Противоречие

■

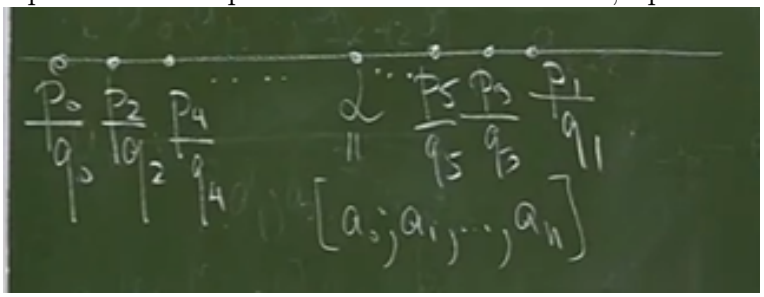
Замечание
Из этого утверждения следует, что подходящие дроби с четными номерами меньше, чем с нечетными

Следствие 2
Подходящие дроби с четными номерами возрастают, с нечетными - убывают
▲
$p_{k+2} = a_{k+2}p_{k+1} + p_k * q_k$
$q_{k+2} = a_{k+2}q_{k+1} + q_k * p_k$

$p_{k+2}q_k = a_{k+2}p_{k+1}q_k + p_kq_k$
$q_{k+2}p_k = a_{k+2}q_{k+1}p_k + q_kp_k$

$p_{k+2}q_k - q_{k+2}p_k = a_{k+2}(p_{k+1}q_k - q_{k+1}p_k) = a_{k+2}(-1)^k$

$\frac{p_{k+2}}{q_{k+2}} - \frac{p_k}{q_k} = \frac{a_{k+2}*(-1)^k}{q_kq_{k+2}}$
При четном k правая часть положительна, при нечетном - отрицательна



■

26 Рекуррентные соотношения для числителей и знаменателей подходящих дробей (доказательство).

▲ Будем доказывать по индукции

1 База: k = 0; $[a_0] = \frac{a_0}{1} = \frac{p_0}{q_0}, [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1+1}{a_1} = \frac{p_1}{q_1}, [a_0; a_1, a_2] = a_0 + \frac{1}{a_1+\frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2+1} = \frac{a_0a_1a_2+a_0+a_2}{a_1a_2} = \frac{p_2}{q_2}$

$a_0a_1a_2 + a_0 + a_2 = a_2a_0a_1 + a_2 + a_0 = a_2 * p_1 + p_0 \Longrightarrow$ Сошлось! Ура!

2 $a_0 + \frac{1}{[a_1;a_2,...,a_{k+2}]} = [a_0; a_1,..., a_{k+2}] = \frac{p_{k+2}}{q_{k+2}}$
Положим $[a_1; a_2, ..., a_i] = \frac{p'_i}{q'_i}$. Тогда $\frac{p_{k+2}}{q_{k+2}} = a_0 + \frac{p'_{k+2}}{q'_{k+2}} = \frac{a_0p'_{k+2}+q'_{k+2}}{p'_{k+2}}$

$p'_{k+2} = a_{k+2}p'_{k+1} + p'_k,\ q'_{k+2} = a_{k+2}q'_{k+1} + q'_k$

$\frac{p_{k+2}}{q_{k+2}} = \frac{a_0a_{k+2}p'_{k+1}+a_0p'_k+a_{k+2}q'_{k+1}+q'_k}{a_{k+2}p'_{k+1}+p'_k} = \frac{a_{k+2}(a_0p'_{k+1}+q'_{k+1})+a_0p'_k+q'_k}{a_{k+2}p'_{k+1}+p'_k}$

Теперь заметим, что $\frac{p_{k+2}}{q_{k+2}} = \frac{a_0p'_{k+2}+q'_{k+2}}{p'_{k+2}} \Longrightarrow p_i = a_0p'_i + q'_i,\ q_i = p'_i \Longrightarrow \frac{a_{k+2}(a_0p'_{k+1}+q'_{k+1})+a_0p'_k+q'_k}{a_{k+2}p'_{k+1}+p'_k} = \frac{a_{k+2}p_{k+1}+p_k}{a_{k+2}q_{k+1}+q_k}$ ■

27 Определение бесконечной цепной дроби. Доказательство сходимости соответствующих подходящих цепных дробей (можно пользоваться без доказательства соотношениями на их коэффициенты).

Опр *Бесконечной цепной дробью* называется выражение вида:
$[a_0; a_1, a_2, ...] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$, где $a_0 \in Z, a_i \in N \ \forall i >= 1$

Опр *Величиной бесконечной цепной дроби* называется предел её подходящих дробей, то есть такое число $\alpha = \lim\limits_{n->\infty} \frac{P_n}{Q_n}$

Теорема
Соответствующие подходящие цепные дроби сходятся. $\exists \lim\limits_{n->\infty} \frac{P_n}{Q_n}$

▲ Согласно следствиям 1 и 2 из Теоремы о рекуррентных соотношениях для числителей и знаменятелей подходящих дробей последовательность дробей с четными номерами возрастает и ограничена сверху, а последовательность с нечетными номерами ограничена снизу и убывает, значит, обе эти последовательности имеют предел. $|\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}}| = \frac{1}{Q_n Q_{n+1}}$
В силу того, что $Q_{n+2} = a_{n+2}Q_{n+1} + Q_n,\ Q_{n+2} \geqslant Q_n \Longrightarrow \frac{1}{Q_n Q_{n+1}} \longrightarrow 0 \Longrightarrow |\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}}| \longrightarrow 0 \Longrightarrow$ пределы последовательностей совпадают, тогда и $\frac{P_n}{Q_n}$ сходится ■

28 Бесконечные периодические цепные дроби. Теорема о периодичности дроби для квадратичной иррациональности (доказательство в одну сторону). Умение находить периодическую цепную дробь по её значению, и наоборот, нахождение значения дроби по её периоду.

Опр Бесконечная цепная дробь вида
$[a_0; a_1, ..., a_k, a_{k+1}, ..., a_{k+T}, a_{k+1}, ..., a_{k+T}, ...] = [a_0; a_1, ..., a_k, \overline{a_{k+1}, ..., a_{k+T}}]$ называется *периодической* с периодом $a_{k+1}, ..., a_{k+T}$. Набор $a_0, a_1, ..., a_k$ называется *предпериодом*.

Опр Иррациональное число α называется *квадратичной иррациональностью*, если α - корень квадратного уравнения с целыми коэффициентами.

Теорема
Если $\alpha = [a_0; a_1, ..., a_k, \overline{a_{k+1}, ..., a_n}]$, то α - квадратичная иррациональность
▲ $\beta = [\overline{a_{k+1}; a_{k+2}, ..., a_n}] = a_{k+1} + \cfrac{1}{\ddots + a_n + \cfrac{1}{[\overline{a_{k+1}; a_{k+2}, ..., a_n}] = \beta}}$

$\frac{a_n\beta + 1}{\beta}$; $\frac{\beta}{a_n\beta + 1} + a_{n-1} = \frac{\beta + a_{n-1}a_n\beta + a_{n-1}}{a_n\beta + 1}$
Заметим, что раскрывая таким образом мы получаем дробь вида $\frac{c\beta + d}{c'\beta + d'} = \beta$

$a_0 + \cfrac{1}{\ddots + a_k + \frac{1}{\beta}}$
Заметим две прекрасные вещи:
Если β - решение квадратного уравнения, то $\frac{1}{\beta}$ - тоже является решением квадратного

уравнения $\Longrightarrow \frac{1}{\beta}$ - также квадратичная иррациональность. (Достаточно поделить уравнение для β на x^2)
Если β - решение квадратного уравнения, то $\forall\gamma \in N$ $\beta+\gamma$ − решение квадратного уравнения, т.е. квадратичная иррациональность. (Если $c_2x^2+c_1x+c_0=0$ - уравнение с корнем β, то $c_2(x-\gamma)^2+c_1(x-\gamma)+c_0=0$ - уравнение с корнем $\beta+\gamma$).
Пользуясь тем, что прибавление к квадратичной иррациональности натурального числа и обратное к квадратичной иррациональности - квадратичная иррациональность, получаем, что α - квадратичная иррациональность ■

Нахождение периодической цепной дроби по её значению, и нахождение значения дроби по её периоду

Пусть дана периодическая цепная дробь $[5;\overline{1,2,1,10}]=a$. Найти ее значение
Алгоритм:
1. Выделяем часть с периодом: $[\overline{1;2,1,10}]=x$
2. Расписываем дробь, пока не дойдем до первого периода, приравниваем цепную дробь в знаменателе к x, всю дробь приравниваем к x: $x=1+\frac{1}{2+\frac{1}{1+\frac{1}{10+\frac{1}{[1;2,1,10]}}}}=1+\frac{1}{2+\frac{1}{1+\frac{1}{10+\frac{1}{x}}}}$
3. Начинаем переворчивать: $x=1+\frac{1}{2+\frac{1}{1+\frac{x}{10x+1}}}=1+\frac{1}{2+\frac{10x+1}{11x+1}}=1+\frac{11x+1}{32x+3}=\frac{43x+4}{32x+3}\Longrightarrow$
$32x^2-40x-4=0\Longrightarrow x=\frac{\sqrt{33}+5}{8}$
4. Находим a. $a=5+\frac{1}{x}=5+\frac{8}{\sqrt{33}+5}=\frac{33+5\sqrt{33}}{\sqrt{33}+5}$

Пусть дано значение $a=\sqrt{2}$. Найти цепную дробь
Алгоритм: 1. Выделяем целую часть: $1+(\sqrt{2}-1)$
2. 2. Если число уже встречалось в разложении, мы нашли период. Ура! Иначе переворачиваем дробную часть: $1+\frac{1}{\frac{1}{\sqrt{2}-1}}$
3. Домножаем на сопряженное: $1+\frac{1}{\frac{\sqrt{2}+1}{1}}=1+\frac{1}{\sqrt{2}+1}$
4. Вернуться к шагу 1
Таким образом, получим:
$1+\frac{1}{\sqrt{2}+1}=1+\frac{1}{2+(\sqrt{2}-1)}$
$\sqrt{2}-1$ уже встречалось, значит, дробь: $[1;\overline{2}]$

29 :

сопряжение, замкнутость сложения, умножения. Согласованность сопряжения и умножения. Норма и её свойства.]Квадратичные иррациональности. Множество Z[$\sqrt{m}$]: сопряжение, замкнутость сложения, умножения. Согласованность сопряжения и умножения. Норма и её свойства. **Опр** Иррациональное число $\overline{\alpha}$ называется *квадратичной иррациональностью*, если α - корень квадратного уравнения с целыми коэффициентами.

Опр Пусть $\alpha=a+b\sqrt{m}$ — квадратичная иррациональность. Назовем число $\alpha=a-b\sqrt{m}$ сопряженным к α числом
Утверждение
Множество Z[$\sqrt{m}$] = {a + b$\sqrt{m}$| a, b $\in Z$ } $\subset$ R замкнуто относительно операций:

1 Сопряжения

2 Сложения

3 Умножения

▲

1 a - b$\sqrt{m}$ = a + (-b)$\sqrt{m}$; a, -b $\in Z \Longrightarrow$ a - b$\sqrt{m}$ $\in$Z[$\sqrt{m}$]

2 $a_1 + b_1\sqrt{m} + a_2 + b_2\sqrt{m} = (a_1 + a_2) + (b_1 + b_2)\sqrt{m}$; $(a_1 + a_2), (b_1 + b_2) \in Z \Longrightarrow a_1 + b_1\sqrt{m} + a_2 + b_2\sqrt{m}$ $\in$Z[$\sqrt{m}$]

3 $(a_1+b_1\sqrt{m})*(a_2+b_2\sqrt{m}) = (a_1a_2+b_1b_2m)+(a_1b_2+a_2b_1)\sqrt{m}; (a_1a_2+b_1b_2m), (a_1b_2+a_2b_1) \in Z \Longrightarrow (a_1 + b_1\sqrt{m}) * (a_2 + b_2\sqrt{m}) \in Z[\sqrt{m}]$ ■

Сопряжённость для квадратичной иррациональности согласована с общим определением. В алгебре сопряженными к элементу α над полем F называются корни неприводимого многочлена f(x) $\in$ F[x], для которого f(α) = 0. Это согласовано с определением комплексного сопряжения. А именно, для комплексного числа z $\in$ C R его сопряжённое — это второй корень квадратного многочлена, у которого первый корень — это z.

Опр

Для $\alpha \in$ Z[$\sqrt{m}$] определим норму N(α) = $\alpha\overline{\alpha}$.

Свойства

1 $N(\alpha) \in Z$ ▲ $N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{m}) * (a - b\sqrt{m}) = a^2 - b^2m \in Z$ ■

2 $N(\alpha\beta) = N(\alpha) * N(\beta)$
▲ $\alpha = a_1 + b_1\sqrt{m},\ \beta = a_2 + b_1\sqrt{m}$.
$\alpha\beta = (a_1a_2 + b_1b_2m) + (a_1b_2 + a_2b_1)\sqrt{m}$
$\overline{\alpha\beta} = (a_1a_2 + b_1b_2m) - (a_1b_2 + a_2b_1)\sqrt{m}$
$N(\alpha\beta) = ((a_1a_2 + b_1b_2m) + (a_1b_2 + a_2b_1)\sqrt{m})((a_1a_2 + b_1b_2m) - (a_1b_2 + a_2b_1)\sqrt{m}) =$
$= (a_1 + b_1\sqrt{m})(a_2 + b_2\sqrt{m}) * (a_1 - b_1\sqrt{m})(a_2 - b_2\sqrt{m}) = (a_1 + b_1\sqrt{m})(a_1 - b_1\sqrt{m}) * (a_2 + b_2\sqrt{m})(a_2 - b_2\sqrt{m}) = N(\alpha)N(\beta)$ ■

30 Пара (a, b), где a + b$\sqrt{2} = (1 + \sqrt{2})^n$ является решением уравнения Пелля $a^2 - 2b^2 = \pm 1$.

Опр Уравнение вида $x^2 - my^2 = 1$, где m — натуральное число, не являющееся точным квадратом, называется уравнением Пелля. Решение (1, 0) называется тривиальным. Решение (x, y) называется положительным, если x > 0 и y > 0.

Определим a_n и b_nпри помощи равенства $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$

1. $(1 + \sqrt{2})^n = \sum_{k=0}^{n} C_n^k(\sqrt{2})^k$
$(1 - \sqrt{2})^n = \sum_{k=0}^{n} C_n^k(-\sqrt{2})^k$. При четных k $(-\sqrt{2})^k = (\sqrt{2})^k \in N \Longrightarrow (-\sqrt{2})^k \in a_n$.
При нечетных k $(-\sqrt{2})^k = -(\sqrt{2})^k \notin Z \Longrightarrow (-\sqrt{2})^k \in -b_n$
Таким образом, $(1 - \sqrt{2})^n = a_n - b_n\sqrt{2}$

2. $a_n^2 - 2b_n^2 = (a_n - b_n\sqrt{2})(a_n + b_n\sqrt{2}) = (1 + \sqrt{2})^n(1 - \sqrt{2})^n = (-1)^n$

Отсюда заключаем, что такие a_n и b_n: $(1+\sqrt{2})^n = a_n+b_n\sqrt{2}$ являются решениями уравнения Пелля $a^2 - 2b^2 = \pm 1$.

31 Связь между решениями уравнения Пелля $a^2 - 2b^2 = \pm 1$ и элементами $Z[\sqrt{2}]$ нормой 1.

Утверждение
Любой элемент Z[$\sqrt{2}$] нормы 1 является решением уравнения $a^2 - 2b^2 = 1$, любое решение уравнения $a^2 - 2b^2 = 1$ - элемент Z[$\sqrt{2}$] нормы 1
■

▷ -> Пусть (a,b) - решение уравнения Пелля $a^2 - 2b^2 = 1$, тогда $(a + b\sqrt{2})(a - b\sqrt{2}) = 1 \Longrightarrow N(a + b\sqrt{2}) = 1; a,b \in Z[\sqrt{2}]$

▷ <- Пусть a, b $\in Z[\sqrt{2}]$, $N(a + b\sqrt{2}) = 1 \Longrightarrow (a + b\sqrt{2})(a - \sqrt{2}) = 1 = a^2 - 2b^2 \Longrightarrow$ (a,b) - решение уравнения Пелля ■

Аналогичное утверждение можно сформулировать для $a^2 - 2b^2 = -1$

32 Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Степень алгебраического числа. Теорема Лиувилля (б/д).

Опр Число α - алгебраическое, если существует многочлен с целыми коэффициентами, корнем которого является α

Обозначим множество алгебраических чисел A. Это множество счетно (достаточно занумеровать все многочлены)
Опр $R\backslash A$ ($C\backslash A$) имеет мощность континуум, все числа из этого множества - *трансцендентные числа*

Опр *Степень алгебраического числа* - это минимальная степень уравнения, корнем которого является это число

Теорема Лиувилля
Пусть α - алгебраическое число степени d, тогда $\exists c = c(\alpha)$: неравенство $|\alpha - \frac{p}{q}| \leqslant \frac{c}{q^d}$ не имеет решени в $\frac{p}{q}$

33 Определение решётки (эквивалентность двух определений) и дискретного подмножества. Определитель решётки. Независимость значения определителя от выбора базиса.

Опр Пусть $(e_1, ..., e_k)$ — набор линейно независимых векторов в R^n. Решётка - абелева группа, порождённая $\{e_i\}$. Иными словами, решётка есть множество $\Lambda = \{a_1e_1 + ... + a_ke_k\}, a_i \in Z$

Эквивалентность
<- Для $\Lambda = \{a_1e_1 + ... + a_ke_k\}, a_i \in Z$ выполняются ассоциативность и коммутативность сложения, существует нейтральный по сложению ($\overline{0}$) и к каждому $\overline{a} = a_1e_1 + ... + a_ke_k$ обратный $-\overline{a} = -a_1e_1 - ... - a_ke_k$, значит, Λ - абелева группа. Причем $\{e_i\}$ - базис

-> Любой элемент абелевой группы, порожденной $\{e_i\}$ имеет вид $\overline{a} = a_1e_1 + ... + a_ke_k$, где $a_i \in Z \Longrightarrow \overline{a} \in \Lambda$

Опр Подмножество X пространства R^n называется дискретным, если для любой точки x ∈ X существует окрестность этой точки, не содержащая других точек множества X.

Опр Определителем $det\Lambda$ решётки Λ называется определитель матрицы, составленной из координат её базисных векторов.(Он равен объёму фундаментального параллелепипеда, то есть параллелепипеда, составленного из базисных векторов.)

Утверждение
Определитель решетки не зависит от выбора базиса
▲ Пусть A, B - матрицы в разных базисах, S - матрица перехода от A к B. Тогда $B = A * S$. В силу того, что векторы нового безиса - это ЛК векторов старого базиса с какими-то целочисленными коэффициентами, матрица S целочисленная. По этим же соображениям, S^{-1} - целочисленная матрица. Тогда
$detB = detA\ detS, detA = detS^{-1}detB \Longrightarrow \frac{1}{detS} = detS^{-1} \Longrightarrow detS^{-1}detS = 1. \Longrightarrow detS = \pm 1 \Longrightarrow detA = detB$ ■

34 Определение решётки и его определителя. Решётка $\Lambda_{\overline{a}}$ и её определитель.

Опр Дано простое число p и зафиксирован вектор $\overline{a} = (\frac{a_1}{p}, ..., \frac{a_n}{p})$, где $a_i \in Z$. Определим множество $\Lambda_{\overline{a}} = \{l\overline{a} + \overline{b},\ l \in Z, \overline{b} \in Z^n\}$
Утверждение
$\Lambda_{\overline{a}}$ - решетка
▲ Заметим, что все это множество порождается векторами $(\overline{a}, \overline{e_1}, \overline{e_2}, ..., \overline{e_n})$. Покажем, что если убрать из этого набора векторов $\overline{e_1}$, они все равно будут порождать множество $\Lambda_{\overline{a}}$.

Заметим, что если все $a_i \vdots p$, то ничего нового мы не получим, т.е. $\overline{a}$ линейно выражается через $(\overline{e_1}, ...\overline{e_n})$, и мы нашли базис, порождающий это множество, тогда $\Lambda_{\overline{a}}$ - решетка.

Предположим, какой-то из $a_i \not\vdots p$; Пусть БОО это a_1. Научимся из вектора $\gamma = (\frac{1}{p}, ..., \frac{la_n}{p})$ получать вектор $\overline{a}$ и вектор $\overline{e_1}$.
Возьмем в качестве $\overline{b} = k\overline{e_1}$, тогда $l\overline{a} + \overline{b} = (\frac{la_1+kp}{p}, \frac{la_2}{p}, ..., \frac{la_n}{p})$
Заметим, что всегда можно выбрать l и k так, чтобы $la_1 + kp = 1$, т.к. $(a_1, p) = 1$
Покажем, что $(\gamma, e_2, ..., e_n)$ образуют базис. Для начала заметим, что $\overline{e_1} = p\gamma - la_2\overline{e_2} - la_3\overline{e_3} - ...la_n\overline{e_n}$. $l\overline{a} = \gamma - \overline{b}$. Мы умеем выражать все базисные векторы и $l\overline{a} \Longrightarrow$ умеем выражать $\overline{a} \Longrightarrow$ нашли базис■
Найдем $det\Lambda_{\overline{a}}$
Заметим, что матрица, составленная из базисных векторов $\Lambda_{\overline{a}}$ нижняя треугольная, diag($\frac{1}{p}$, 1,1,...,1), исходя из того, какой базис мы нашли. Тогда $det\Lambda_{\overline{a}} = \frac{1}{p}$

35 Определение равномерной распределённой последовательности по модулю 1. Является ли $\sqrt{n}$ р.р. (mod 1) последовательностью?

Послед-ность $x_1, x_2, \dots, x_n, \dots$ - **равномерно распределена по модулю 1**, если:

$$\forall a, b \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \dots, N : \{x_i\} \in [a,b)\}|}{N} = b - a$$

или, что равносильно (по сути речь про вероятность, что дробная часть числа из первых N окажется на отрезке b - a):

$$\forall \gamma \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \dots, N : \{x_i\} \leqslant \gamma\}|}{N} = \gamma$$

Пример: $\sqrt{n}$. Второе определение: Фиксируем γ и N. Последовательность: $\sqrt{1}, \sqrt{2}, \dots, \sqrt{N}$. Пусть переменная k принимает значения целых частей, которые возникают в такой последовательности; $k \in \{1, [\sqrt{2}], [\sqrt{3}], \dots\} = \{1, 2, 3, \dots, [\sqrt{N}]\}$.

$\{x_n\} \leqslant \gamma$. Это может возникнуть, если число x_n имеет вид $k^2, k^2+1, \dots, (k+\gamma)^2 = k^2 + 2k\gamma + \gamma^2$. Таких чисел с точностью до O(1) $2k\gamma$. Тогда общее количество таких n: $|\{n : \{\sqrt{n}\} \leqslant \gamma\}| = \sum_{k=1}^{[\sqrt{N}]}(2k\gamma + O(1)) = 2\gamma\frac{[\sqrt{N}][\sqrt{N}+1]}{2} + O(\sqrt{N}) = N\gamma + O(\sqrt{N})$. Тогда

$$\forall \gamma \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \dots, N : \{x_i\} \leqslant \gamma\}|}{N} = \lim_{N\to\infty} \frac{N\gamma + O(\sqrt{N})}{N} = \gamma$$

Отсюда эта последовательность р.р. (mod 1) по определению.

36 Определение равномерной распределённой последовательности по модулю 1. Является ли р.р. (mod 1) последовательность a^n при a < 1?

Послед-ность $x_1, x_2, \dots, x_n, \dots$ - **равномерно распределена по модулю 1**, если:

$$\forall a, b \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \dots, N : \{x_i\} \in [a,b)\}|}{N} = b - a$$

или, что равносильно (по сути речь про вероятность, что дробная часть числа из первых N окажется на отрезке b - a):

$$\forall \gamma \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \dots, N : \{x_i\} \leqslant \gamma\}|}{N} = \gamma$$

a^n при $a < 1$ **не является** р.р. (mod 1).

▲ Очевидно, что $\{a^n\} = a^n$. Возьём $\gamma = a + \varepsilon < 1$. Тогда $\forall n\ a^n < a < \gamma$; для этого γ: $\lim_{N\to\infty} \frac{|\{i=1,\dots,N:\{x_i\}\leqslant\gamma\}|}{N} = 1 \neq \gamma$ ■

37 Определение всюду плотности. Последовательность $\ln n$ всюду плотна на $[0, 1]$.

38 Определение всюду плотности. Если последовательность равномерно распределена по модулю 1, то она и всюду плотна.

Последовательность x_n **всюду плотна на отрезке [a, b]**, если $\forall\ [c, d] \subset [a, b]\ \exists$ бесконечного много номеров N таких, что $\{x_N\} \in [c, d]$.

$\{ln(n)\}$ всюду плотна на [0; 1].

▲ Зафиксируем N. Тогда $[x_n] = k \in \{1, \dots, [ln(N)]\}$. $\{ln(n)\} \in [c; d] \Leftrightarrow ln(n) \in [k + c; k + d] \Rightarrow n \in [e^{k+c}; e^{k+d}]$. Для N число подходящих n будет $\sum_{k=1}^{[ln(N)]}(e^{k+d} - e^{k+c}) = \frac{e(e^{ln(N)}-1)}{e-1}(e^d - e^c)\ N\frac{e(e^d-e^c)}{e-1} \to \infty$ ■

Теорема. Если последовательность x_n p.p. mod 1, то она всюду плотна на отрезке [0, 1].

▲ Из определения равномерной распределённости по модулю 1, $\forall c < d \in [0; 1]$ $\lim_{N\to\infty} \frac{|k|k\leqslant N, \{x_k\}\in[c;d]|}{N} = d - c$, т.е. для любого подотрезка $\exists$ бесконечное количество точек в нём. ■

39 Тригонометрические суммы. Критерий Вейля для p.p. (mod 1) (формулировка). Последовательность αn при иррациональном α является p.p. (mod 1). Что происходит при рациональном α?

Тригонометрическая сумма - сумма вида $\sum_{k=1}^{N} e^{2i\pi kx}$

Критерий Вейля. x_n p.p. mod 1 тогда и только тогда, когда:

$$\forall h \in \mathbb{Z} \setminus \{0\} : \frac{1}{N}\sum_{n=1}^{N} e^{2i\pi h x_n} \to 0$$

$x_n = \alpha n$ при $\alpha \in \mathbb{Q}$ принимает ограниченное количество значений $\Rightarrow$ быть p.p. mod 1 не может.

$\alpha \notin \mathbb{Q}$. Применим критерий Вейля:

$$\forall h \in \mathbb{Z} \setminus \{0\} : \frac{1}{N}\sum_{n=1}^{N} e^{2i\pi h\alpha n} = \frac{1}{N} e^{2i\pi h\alpha}\frac{e^{2i\pi h\alpha N} - 1}{e^{2i\pi h\alpha} - 1}$$

Знаменатель не равен нулю в силу иррациональности α; по формуле Эйлера ($e^{ix} = cos(x)+isin(x)$) числитель не превышает 2, следовательно, это значение стремится к нулю; критерий Вейля выполняется $\Rightarrow$ последовательность равномерно распределена по модулю 1.

40 Определение равномерной распределённой последовательности по модулю 1. Являются ли р.р. (mod 1) последовательности а) $1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \ldots$ б) $\frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}, \ldots$.

Послед-ность $x_1, x_2, \ldots, x_n, \ldots$ - **равномерно распределена по модулю 1**, если:

$$\forall a, b \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \ldots, N : \{x_i\} \in [a,b)\}|}{N} = b - a$$

а) **Равномерно распределена mod 1**.

▲ Разбиваем на "блоки"по знаменателям. Тогда количество чисел из N-ого блока, которые попадают в отрезок (b-a) можно оценить как $(b-a)N + C$, где $|C| < 2$. Доля чисел от 1 до M, где $\frac{N(N-1)}{2} <= M < \frac{N(N+1)}{2}$ (то есть M находится в блоке N+1), попадающих в этот отрезок - как $\frac{1}{M}(\sum_n [(b-a)n + C] + D)$, где D - это "остаток"из дробей со знаменателем N+1. Так как C, D - это линейные функции от N, то при делении на M они будут стремится к 0, и останется в точности (b-a). ■

б) **Не равномерно распределена mod 1**.

▲ Разобъём её на "блоки"по знаменателям. Рассмотрим отрезок $[0; \frac{1}{2}]$. Если смотреть на концы блоков, то там ровно половина попадает в первый отрезок. А если посмотреть на все числа до середины N-ого блока, то доля чисел, попадающих на отрезок $[0; \frac{1}{2}]$ будет $\frac{2}{3}$ (по индукции), что противоречит существованию предела (а, значит, и определению равномерной распределённости по модулю 1). ■

41 Определение равномерной распределённой последовательности по модулю 1. Пусть последовательность x_n р.р. (mod 1) и m — фиксированное целое число, не равное нулю. Докажите, что последовательность mx_n также р.р. (mod 1). Верно ли, что если m — не целое, то это не верно?

Послед-ность $x_1, x_2, \ldots, x_n, \ldots$ - **равномерно распределена по модулю 1**, если:

$$\forall a, b \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \ldots, N : \{x_i\} \in [a,b)\}|}{N} = b - a$$

Теорема. Если последовательность x_n р.р. (mod 1) и m — фиксированное целое число, не равное нулю, то последовательность mx_n также р.р. (mod 1).

▲ x_n равномерно распределено по модулю 1 по критерию Вейля равносильно тому, что:

$$\forall h \in \mathbb{Z} \setminus \{0\} : \frac{1}{N} \sum_{n=1}^{N} e^{2i\pi h x_n} \to 0$$

Критерий Вейля для mx_n, где m - целое число, отличное от 0:

$$\forall h \in \mathbb{Z} \setminus \{0\} : \frac{1}{N} \sum_{n=1}^{N} e^{2i\pi h (m x_n)} = \frac{1}{N} \sum_{n=1}^{N} e^{2i\pi (hm) x_n} \to 0$$

Это верно, так как hm - подмножество целых чисел, т.е. для них это выполнялось по критерию Вейля для x_n. Виват! ■

Контрпример к важности целостности коэффициента. См. билет 39: αn, где α - иррациональное - равномерно распределённая последовательность. Тогда можно взять последовательность $\sqrt(2)n$, она будет равномерно распределённой, и домножить её на нецелое $m = \sqrt(2)$, получить последовательность $2n$, которая не является равномерно распределённой.

42 Описание алгоритма AKS (6 шагов). Лемма об оценке r (б/д). Оценка сложности алгоритма. Тождество $(X + a)^p = X^p + a (\mathrm{mod}\, p)$.

Алгоритм проверки n на простоту: Agarwal, Kayal, Saxena (AKS)

1. $n = a^b, b \geqslant 2 \Rightarrow n$ составное
2. Ищем наименьшее r, такое что $\mathrm{ord}_r\, n > \log_2^2 n$
3. Если хотя бы для одного числа a из диапазона $1 \dots r$ выполнено $1 < (a, n) < n \Rightarrow n$ составное ($(a,n) := \text{НОД}(a, n)$)
4. Если $n \leqslant r$, то n простое
5. Если хотя бы для одного числа a в диапазоне $1 \dots l = \sqrt{\varphi(r)} \cdot \log_2 n$ выполнено $(x + a)^n \neq x^n + a \pmod{x^r - 1, n} \Rightarrow n$ составное
6. n простое

Лемма: $r \leqslant \max\{3, \lceil \log_2^5 n \rceil\}$
Сложность:

1. $n = a^b \Rightarrow b \leqslant \log_2 n \Rightarrow$ можно перебрать бинпоиском за $\mathrm{poly}(\log_2 n)$
2. Из леммы следует, что шаг 2 можно сделать перебором за $\mathrm{poly}(\log_2 n)$
3. Перебираем числа меньше r и ищем НОД (за логарифм) $\Rightarrow$ этот шаг выполняется за $\mathrm{poly}(\log_2 n)$
4. $O(1)$
5. Всего $\mathrm{poly}(\log_2 n)$ итераций. На каждой делаем бинарное возведение в степень ($\mathrm{poly}(\log_2 n)$), как только превышаем r делим на многочлен $x^r - 1$ ($\mathrm{poly}(\log n)$, так как степень делимого $\leqslant 2r$, то есть у него $\mathrm{poly}(\log_2 n)$ коэффициентов)

Утверждение: $(x + a)^p = x^p + a \pmod{p}$
▲

$$(x + a)^p = x^p + a^p + \sum_{i=1}^{p-1} C_p^i x^{p-i} a^i$$

$a^p = a \pmod{p}$ (малая теорема Ферма), $C_p^i = 0 \pmod{p}$ (доказывалось в прошлом семестре) $\Rightarrow (x + a)^p = x^p + a \pmod{p}$ ■

49 Китайская теорема об остатках

Лемма 49.1. *Пусть* $(a, b) = 1$, *тогда* $\exists c : ac \equiv 1 \pmod{b}$

▲. Рассмотрим числа $a, 2a, ..., (b-1)a$. Они образуют приведённую систему вычетов, а значит есть остаток 1. □

Теорема 49.1 (Китайская теорема об остатках)**.** *Пусть* $n_1, n_2, ..., n_k \in \mathbb{N}$ *попарно взаимно простые, а* $r_1, r_2, ..., r_k \in \mathbb{Z}$. *Тогда* $\exists! M$ *по модулю* $\prod_{i=1}^{k} n_i$ *решение системы сравнений:*

$$\begin{cases} M \equiv r_1 \pmod{n_1} \\ M \equiv r_2 \pmod{n_2} \\ ... \\ M \equiv r_k \pmod{n_k} \end{cases}$$

▲. Пусть $N = \prod_{i=1}^{k} n_i; N_i = \frac{N}{n_i}; N_i^{-1}$ – обратный к N_i по модулю n_i.
Существование N_i^{-1} можно обосновать по лемме, так как $(N_i, n_i) = 1$.
Покажем, что $M = \sum_{i=1}^{k} r_i N_i N_i^{-1}$ будет решением.
Рассмотрим M по модулю n_1. Все слагаемые, кроме первого, содержат множитель N_i, который делится на n_1. Получается, что $M \equiv r_1 N_1 N_1^{-1} \pmod{n_1} \equiv r_1 \pmod{n_1}$, то есть M является решением первого сравнения.
Аналогично проверяем все k сравнений.
Теперь докажем, что решение единственно по модулю N.
Пусть A и B – различные решения по модулю N. Тогда $A - B \equiv 0 \pmod{n_i}$. Так как n_i взаимно простые, то $A - B \equiv 0 \pmod{N}$. Получается, что A и B – одинаковые решения по модулю N.
Противоречие. □

51 Сравнения второй степени. Квадратичные вычеты и невычеты. Тождество для $\left(\frac{a}{p}\right)$

Определение 51.1. $x^2 \equiv a \bmod m$ называется *сравнением второй степени.*

Будем считать, что $m = p$ – нечётное простое число, $(a, p) = 1$.

Замечание. У сравнения второй степени либо нет решений, либо их два.

▲. По теореме Лагранжа у сравнения второй степени не более 2.
Пусть x_0 – решение сравнения $x^2 \equiv a \bmod p$.
Тогда $-x_0$ – также решение, но $-x_0 \not\equiv x_0 \bmod p$ □

Определение 51.2. Число a называется *квадратичным вычетом*, если у сравнения $x^2 \equiv a \bmod p$ два решения. Число a называется *квадратичным невычетом*, если у сравнения $x^2 \equiv a \bmod p$ нет решений.

Утверждение 51.1. *По модулю* p *есть ровно* $\frac{p-1}{2}$ *квадратичных вычетов и* $\frac{p-1}{2}$ *квадратичных невычетов.*

Утверждение было доказано в билете 12 (на "уд.").

Теорема 51.1. $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, *если* a *– квадратичный вычет, и* $a^{\frac{p-1}{2}} \equiv -1 \bmod p$, *если* a *– квадратичный невычет.*

▲. По малой теореме Ферма $a^{p-1} \equiv 1 \bmod p$ для всех a. Тогда

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

Если a – квадратичный вычет, то

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

Доказательство для квадратичных невычетов аналогичное. □

Определение 51.3. *Символ Лежандра*

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

Замечание.

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

Следствие. *Символ Лежандра мультипликативен.*

Теорема 51.2. $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$

▲. Пусть $x \in \{1, 2, ..., \frac{p-1}{2}\}$
$a \cdot x$ загоним в систему вычетов от $-\frac{p-1}{2}$ до $\frac{p-1}{2}$.

Переход в новую систему вычетов происходит следующим образом: левая часть системы вычетов $1, 2, ..., p-1$ остаётся такой же (то есть равна $\{1, 2, ..., \frac{p-1}{2}\}$), а правая будет равна $\{-\frac{p-1}{2}, ..., -2, -1\}$.

$$a \cdot x \equiv \varepsilon_x \cdot r_x \bmod p,$$

где $\varepsilon_x \in \{-1, 1\}, r_x \in \{1, 2, ..., \frac{p-1}{2}\}$

Если $a \cdot x$ попадет в левую часть системы вычетов {1, 2, ... p - 1}, тогда $\varepsilon_x = 1$, если в правую, то $\varepsilon_x = -1$.

Утверждается, что математически это записывается так:

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}$$

Доказательство настолько скучное, что Райгородский не стал его рассказывать :) Доказать можно примерно так:

Пусть $a \cdot x \in [kp+1; (k+1)p-1]$ для некоторого k. Тогда $\frac{ax}{p} \in (k, k+1)$. Соответственно, $\frac{2ax}{p} \in (2k, 2k+2)$.

Тогда если ax лежало в левой части, то $\left[\frac{2ax}{p}\right] = 2k$ (то есть чётному числу), иначе $\left[\frac{2ax}{p}\right] = 2k+1$ (то есть нечётному).

Покажем, что когда x пробегает значения от 1 до $\frac{p-1}{2}$, то r_x пробегает всю систему вычитов $1, 2, ..., \frac{p-1}{2}$:

Когда x пробегает значения от 1 до $\frac{p-1}{2}$, то значения ax по модулю m не могут повториться, поскольку иначе $(a, p) \neq 1$. Также значения r_x не могут повториться, так как иначе $\exists x_1, x_2 \leqslant \frac{p-1}{2}$ т.ч. $x_1 \neq x_2, ax_1 \equiv_m r_x, ax_2 \equiv_m -r_x \Rightarrow ax_1 + ax_2 \equiv_m 0 \Rightarrow x_1 + x_2 \equiv_m 0$, чего быть не может, поскольку x пробегает значения от 1 до $\frac{p-1}{2}$. Следовательно, когда x пробегает значения от 1 до $\frac{p-1}{2}$, то r_x пробегает всю систему вычетов $1, 2, ..., \frac{p-1}{2}$

С учетом этого,

$$\prod_{x=1}^{\frac{p-1}{2}}(ax) \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot ... \cdot \varepsilon_{\frac{p-1}{2}} \cdot \prod_{x=1}^{\frac{p-1}{2}} r_x \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot ... \cdot \varepsilon_{\frac{p-1}{2}} \cdot \prod_{x=1}^{\frac{p-1}{2}} x$$

Разделив обе части на $\prod\limits_{x=1}^{\frac{p-1}{2}} x$ и используя выражение для ε_x, получаем:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot ... \cdot \varepsilon_{\frac{p-1}{2}} \equiv (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$$

□

52 Сравнения второй степени. Квадратичные вычеты и невычеты. Формула для $\left(\frac{2}{p}\right)$ (тождеством с суммой по $\left[\frac{2ax}{p}\right]$ можно пользоваться без доказательства).

Вся теория расписана в прошлом билете.

Теорема 52.1.

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

Доказательство. Для удобства введём обозначение $p_1 = \frac{p-1}{2}$.

Без доказательства можно пользоваться утверждением:

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left[\frac{2ax}{p}\right]}$$

Рассмотрим нечётное a.

$$\left(\frac{2a}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{2^2}{p}\right) \cdot \left(\frac{\frac{a+p}{2}}{p}\right) = 1 \cdot (-1)^{\sum\limits_{x=1}^{p_1} \left[\frac{2 \cdot \frac{a+p}{2} \cdot x}{p}\right]}$$

Для удобства распишу отдельно показатель -1:

$$\sum_{x=1}^{p_1} \left[\frac{2 \cdot \frac{a+p}{2} \cdot x}{p}\right] = \sum_{x=1}^{p_1} \left[\frac{ax}{p} + x\right] = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p_1(p_1+1)}{2} = \sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}$$

Вернёмся к $\left(\frac{2a}{p}\right)$:

$$\frac{2a}{p} = (-1)^{\sum\limits_{x=1}^{p_1} \left[\frac{ax}{p}\right]} \cdot (-1)^{\frac{p^2-1}{8}}$$

Тождество верно для любого нечётного a, поэтому можно подставить $a = 1$.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \cdot (-1)^{\sum\limits_{x=1}^{p_1} \left[\frac{x}{p}\right]} = (-1)^{\frac{p^2-1}{8}},$$

так как $\left[\frac{x}{p}\right] = 0$ $(x \leqslant p_1 < p)$. □

53 Матрицы Адамара. Кронекеровское произведение и общая формулировка про $A \cdot B$.

Определение: *Кронекеровским произведением* матриц $A \in M_{a\times a}$ и $B \in M_{b\times b}$ называется матрица

$$C = A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \ (c_{kb+l,pb+q} = a_{kp}b_{lq})$$

Замечание 1: Равенство в скобках выполняется в 0-индексации

Замечание 2: Иногда определение вводят наоборот, то есть берут матрицу A и умножают ее на элементы из B (так вводилось на лекции), но для наших нужд не важно какое выбирать.

Утверждение (задача 20.6): Кронекеровское произведение матриц Адамара является матрицей Адамара.

▲ Рассмотрим две произвольные строки C с номерами $kb+l, pb+q$. Тогда их скалярное произведение равно

$$a_{k1}a_{p1}(b_l, b_q) + a_{k2}a_{p2}(b_l, b_q) + \dots + a_{ka}a_{pa}(b_l, b_q) = (b_l, b_q)(a_k, a_p)$$

Так как мы берем 2 разные строчки, то либо $l \neq q$, либо $k \neq p$. Значит, так как A, B - матрицы Адамара либо $(b_l, b_q) = 0$, либо $(a_k, a_p) = 0 \Rightarrow (c_{kb+l}, c_{pb+q}) = 0 \ \forall kb + l \neq pb + q \Rightarrow$ C - матрица Адамара ■

54 Матрицы Адамара. (Первая) конструкция Пэли с квадратичными вычетами при $n = p + 1, p = 4m + 3$.

Определение: Для простого p определим $p \times p$ *матрицу Якобсталя* Q формулой $Q_{jl} = (\frac{j-l}{p})$ (это символ Лежандра).

I конструкция Пэли: Пусть $p \equiv 3 \pmod 4$. Тогда матрица

$$\begin{pmatrix} 1 & e^T \\ e & Q - E_p \end{pmatrix}$$

где e — столбец из единиц, а E_p — единичная матрица, является матрицей Адамара порядка $p + 1$.

▲ Рассмотрим скалярное произведение строк a_1 и a_2 матрицы Q.

$$\sum_{b=1}^{p} \left(\frac{a_1 - b}{p}\right)\left(\frac{a_2 - b}{p}\right)$$

Пусть $x = a_1 - b, c = a_2 - a_1$. Получаем

$$\sum_{x=1}^{p} \left(\frac{x}{p}\right)\left(\frac{c+x}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x \cdot x^{-1}(x+c)}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)^2 \left(\frac{1 + x^{-1}c}{p}\right)$$

При $x \neq 0$ $\left(\frac{x}{p}\right)^2 = 1$. Положим $y = 1 + x^{-1}c$. Так как $c \not\equiv 0 (\mathrm{mod}\ p)$, то $x^{-1}c$ пробегает все числа $1 \dots p-1 \Rightarrow y$ пробегает числа $2 \dots p$.

$$\sum_{x \not\equiv 0 (\mathrm{mod}\, p)} \left(\frac{1 + x^{-1}c}{p}\right) = \sum_{y \not\equiv 1 (\mathrm{mod}\, p)} \left(\frac{y}{p}\right) = 0 - \left(\frac{1}{p}\right) = -1$$

Рассмотрим скалярное произведение строк искомой матрицы. По сравнению со скалярным произведением строк Q добавятся слагаемые 1, $(-1) \cdot \left(\frac{a_1 - a_2}{p}\right)$ и $(-1) \cdot \left(\frac{a_2 - a_1}{p}\right)$ (раньше они умножались на нули). Эти символы Лежандра отличаются в $\left(\frac{-1}{p}\right)$ раз. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4m+2}{2}} = (-1)^{2m+1} = -1 \Rightarrow$ слагаемые с символом Лежандра сократятся $\Rightarrow$ скалярное произведение любых двух строк искомой матрицы равно $(-1) + 1 = 0$.

Очевидно, что если мы рассмотрим скалярное произведение первой строки с любой другой, мы получим 0, так как в Q было поровну единиц и минус единиц (ранее доказывалось, что в $\mathbb{Z}_p$ поровну квадратичных вычетов и невычетов) и у нас добавилась одна единица и одна минус единица. $\Rightarrow$ это матрица Адамара ■

55 Матрицы Адамара. (Вторая) конструкция Пэли с квадратичными вычетами при $n = 2p + 2$,$p = 4m + 1$.

Утверждение (свойства кронекеровского произведения):

1. $(A \otimes B)^T = A^T \otimes B^T$
2. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

▲ 1. $C = A \otimes B, D = C^T$. Тогда $d_{pb+q,kb+l} = c_{kb+l,pb+q} = a_{kp}b_{lq} = (A)^T_{pk}(B)^T_{ql} \Rightarrow$ по определению $D = A^T \otimes B^T$

2. Покажем, что это правда для случаев когда размеры A, C и B, D попарно равны и все матрицы квадратные. Тогда можно просто рассмотреть их произведение как блочных матриц.

$$\begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \begin{pmatrix} c_{11}D & \dots & c_{1n}D \\ \vdots & \ddots & \vdots \\ c_{n1}D & \dots & c_{nn}D \end{pmatrix} = \begin{pmatrix} R_{11} & \dots & R_{1n} \\ \vdots & \ddots & \vdots \\ R_{n1} & \dots & R_{nn} \end{pmatrix}$$

где $R_{ij} = \sum_{k=1}^{n}(a_{ik}B)(c_{kj}D)$ (утверждение из Википедии) $= (\sum_{k=1}^{n} a_{ik}c_{kj})BD = (AC)_{ij}BD \Rightarrow$ по определению получили $(AC) \otimes (BD)$ ■

Лемма:

1. Если $p \equiv 1 (\mathrm{mod}\, 4)$, то Q_p - симметрична
2. $Q_pQ_p^T = pE_p - I_p$, где I_p - матрица состоящая полностью из единиц

▲ 1.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k}{2}} = 1 \Rightarrow \left(\frac{i-j}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{j-i}{p}\right) = \left(\frac{j-i}{p}\right) \Rightarrow Q_{ij} = Q_{ji}$$

2. В первой конструкции Пэли мы показали, что скалярное произведение различных строк Q_p равно -1. Скалярное произведение строк i, j - это элемент на позиции i,j в $Q_pQ_p^T$. Очевидно, что на диагонали будут стоять числа $p-1$, так как в каждой строке ровно $p-1$ ненулевой элемент, каждый из которых равен ± 1. Таким образом, получается, что $Q_pQ_p^T = pE_p - I_p$ ■

II конструкция Пэли: Пусть $p \equiv 1 (\mathrm{mod}\, 4)$. Если в матрице

$$A = \begin{pmatrix} 0 & e^T \\ e & Q_p \end{pmatrix}$$

где e — столбец из единиц размера p, Q_p - матрица Якобсталя порядка p, заменить 0 на матрицу $M_0 = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$, а ± 1 на матрицу $\pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \pm M_1$, то получится матрица Адамара порядка $2p + 2$.

▲ Найдем AA^T (пригодится нам в будущем). В левом верхнем углу очевидно будет стоять p, так как просто перемножили столбец из единиц на строку. Остальные элементы первой строки/столбца будут нулями, так как они равны сумме всех символов Лежандра по p. Просто перемножая матрицы заметим, что в оставшемся пространстве у нас получится матрица $I_p + Q_pQ_p^T = I_p + pE_p - I_p = pE_p$ (по пункту 2 леммы). Таким образом, $AA^T = pE_{p+1}$

Пусть H - матрица которая получилась после замен. Тогда так как нули находятся только на главной диагонали

$$H = A \otimes M_1 + E_{p+1} \otimes M_0$$

$HH^T = (A\otimes M_1+E_{p+1}\otimes M_0)(A\otimes M_1+E_{p+1}\otimes M_0)^T = (A\otimes M_1+E_{p+1}\otimes M_0)(A^T\otimes M_1^T+E_{p+1}\otimes M_0^T)$

Заметим, что $M_1^T = M_1, M_0^T = M_0, M_1M_0 = -M_0M_1$

$$HH^T = (A\otimes M_1)(A^T\otimes M_1)+(E_{p+1}\otimes M_0)(A^T\otimes M_1)+(A\otimes M_1)(E_{p+1}\otimes M_0)+(E_{p+1}\otimes M_0)(E_{p+1}\otimes M_0) =$$

$$= (AA^T)\otimes M_1^2 + A^T\otimes(M_0M_1) - A\otimes(M_0M_1) + E_{p+1}\otimes M_0^2$$

$A = A^T$ (по пункту 1 леммы), $AA^T = pE_{p+1}$. Матрицы M_0, M_1 являются матрицами Адамара $\Rightarrow M_i^2 = M_i^TM_i = 2E_2$

$$HH^T = pE_{p+1}\otimes 2E_2 + E_{p+1}\otimes 2E_2 = 2pE_{2p+2} + 2E_{2p+2} = (2p+2)E_{2p+2}\ \blacksquare$$

56 (n, M, d)-коды. Граница Плоткина

Определение 56.1. *(n, M, d)-кодом* называется код, в котором все кодовые слова имеют длину n, d – минимальное расстояние между словами (в смысле расстояния Хэмминга), M – количество кодовых слов.

Теорема 56.1 (Граница Плоткина)**.** *Пусть задан (n, M, d)-код. Если $2d > n$, то $M \leqslant \left[\frac{2d}{2d-n}\right]$*

▲. Пусть $\vec{a_1}, \vec{a_2}, ..., \vec{a_M}$ – все кодовые слова. Запишем их в матрицу следующим образом (каждый вектор представляется в виде строчки):

$$\begin{pmatrix} \leftarrow \vec{a_1} \rightarrow \\ \leftarrow \vec{a_2} \rightarrow \\ \dots \\ \leftarrow \vec{a_M} \rightarrow \end{pmatrix}$$

Полученная матрица имеет размер $M \times n$.
Рассмотрим сумму (a_{i_j} – элемент матрицы)

$$S = \sum_{k=1}^{n} \sum_{1\leqslant i<j\leqslant M} I_{\{a_{i_k}\neq a_{j_k}\}}, \text{где } I_{\{a_{i_k}\neq a_{j_k}\}} = \begin{cases} 1, a_{i_k} \neq a_{j_k} \\ 0, a_{i_k} = a_{j_k} \end{cases}$$

S можно рассматривать следующим образом: фиксируем столбец k и смотрим количество несовпадающих пар в этом столбце. Пусть x – число единиц в этом столбце, тогда $M - x$ – число нулей в этом же столбце. Тогда несовпадающих пар в этом столбце ровно $x(M - x) = Mx - x^2$. Максимум этого значения достигается при $x = \frac{M}{2}$, то есть $x(M - x) \leqslant \frac{M^2}{4}$. Получаем, что $S \leqslant n \cdot \frac{M^2}{4}$.
Теперь рассмотрим S с другой стороны, переставив знаки суммирования:

$$S = \sum_{1\leqslant i<j\leqslant M} \sum_{k=1}^{n} I_{\{a_{i_k}\neq a_{j_k}\}}$$

Теперь S можно интерпретировать следующим образом: зафиксируем строки i и j (а

значит, и соответствующие кодовые слова $\vec{a_i}$ и $\vec{a_j}$). Тогда внутренняя сумма $\sum\limits_{k=1}^{n} I_{\{a_{i_k} \neq a_{j_k}\}}$ – это в точности расстояние Хэмминга $d(\vec{a_i}, \vec{a_j})$. По определению (n, M, d)-кода $d(\vec{a_i}, \vec{a_j}) \geqslant d$, то есть $S \geqslant \frac{M(M-1)}{2} \cdot d$, где ($\frac{M(M-1)}{2}$ – количество пар (i, j)).

$$\frac{M(M-1)}{2} \cdot d \leqslant S \leqslant n \cdot \frac{M^2}{4}$$

$$(M-1)d \leqslant n \cdot \frac{M}{2}$$

$$dM - \frac{nM}{2} \leqslant d$$

$$M(d - \frac{n}{2}) \leqslant d$$

$$M(2d - n) \leqslant 2d$$

Так как $2d - n$ – положительное, то можно разделить на него

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

Так как M – натуральное, получаем:

$$M \leqslant \left[\frac{2d}{2d-n}\right]$$

□

57 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_2 \geqslant \lambda_3$.

Постулат Бертрана. $\forall x \geqslant 2 \quad \exists$ простое $p : x < p < 2x$.
Асимптотика $\forall x \quad \exists p : p \in [x; x + O(x^{0,525})]$

Неравенство Чебышёва $\exists a, b \in \mathcal{R} : 0 < a < b$ (на самом деле, близкие к единице) : $\frac{ax}{ln(x)} \leqslant \pi(x) \leqslant \frac{bx}{ln(x)}$

Определение $\pi(x) = \sum\limits_{p \leqslant x} 1$ – количество простых чисел, не превышающих x

Определение $\theta(x) = \sum\limits_{p \leqslant x} ln(p)$

Определение $\psi(x) = \sum\limits_{(p,\alpha): p^\alpha \leqslant x} ln(p)$

Теорема о равенстве нижних и верхних пределов (формулировка)

Введем следующие обозначения:

$\lambda_1 = \overline{\lim\limits_{x \to \infty} \frac{\theta(x)}{x}}$

$\lambda_2 = \overline{\lim\limits_{x\to\infty} \frac{\psi(x)}{x}}$

$\lambda_3 = \overline{\lim\limits_{x\to\infty} \frac{\pi(x)}{x/ln(x)}}$

μ_1, μ_2, μ_3 – соответствующие нижние пределы.

Теорема: $\lambda_1 = \lambda_2 = \lambda_3, \mu_1 = \mu_2 = \mu_3$
Неравенство $\lambda_2 \leqslant \lambda_3$

Зафиксируем p и x. Тогда таких α, что $p^\alpha < x$, ровно $[log_p x] = [\frac{ln(x)}{ln(p)}]$.

Тогда $\psi(x) = \sum\limits_{(p,\alpha):p^\alpha\leqslant x} ln(p) = \sum\limits_{p\leqslant x} [\frac{ln(x)}{ln(p)}] ln(p) \leqslant \sum\limits_{(p,\alpha):p\leqslant x} ln(x) = ln(x) \sum\limits_{p\leqslant x} 1 = ln(x)\pi(x)$.
$\frac{\psi(x)}{x} \leqslant \frac{\pi(x)ln(x)}{x} = \frac{\pi(x)}{x/ln(x)}$, т.е. $\lambda_2 \leqslant \lambda_3$

58 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема о равенстве нижних и верхних пределов (формулировка). Неравенство $\lambda_3 \leqslant \lambda_1$.

Зафиксируем некоторое $\gamma \in (0; 1)$.

$\theta(x) = \sum\limits_{p\leqslant x} ln(p) \geqslant \sum\limits_{x^\gamma<p\leqslant x} ln(p) > \sum\limits_{x^\gamma<p\leqslant x} ln(x^\gamma) = \gamma ln(x) \sum\limits_{x^\gamma<p\leqslant x} 1 = \gamma ln(x)(\pi(x) - \pi(x^\gamma)) \geqslant \gamma ln(x)(\pi(x) - x^\gamma)$.

Получаем неравенство:

$\frac{\theta(x)}{x} \geqslant \gamma(\frac{\pi(x)}{x/ln(x)} - \frac{x^\gamma}{x} ln(x))$. Перейдя к верхнему пределу, получим, что $\frac{\theta(x)}{x} \geqslant \gamma \frac{\pi(x)}{x/ln(x)}$, т.е. $\lambda_1 \geqslant \gamma\lambda_3 \forall\gamma \in (0; 1)$. Значит, $\lambda_1 \geqslant \lambda_3$, и $\lambda_2 \geqslant \lambda_1 \geqslant \lambda_3$.

59 Порядки(показатели) элементов в системах вычетов. Равенство $ord(g^l) = \frac{ord(g)}{gcd(l,ord(g))}$. Следствие: если есть порядок k, то есть порядки и всех делителей k.

Порядки(показатели) элементов в системах вычетов
Рассмотрим систему вычетов по модулю m.

Определение Пусть $gcd(g, m) = 1$. Тогда показатель $ord(g) = k$ – минимальное $k > 0, g^k \equiv 1$.

Если $gcd(g, m) \neq 1$, то рассматривать $ord(g)$ бессмысленно, т.к. оно равно ∞.

Равенство $ord(g^l) = \frac{ord(g)}{gcd(l,ord(g))}$

Обозначим $ord(g^l)$ за s, а $ord(g)$ за k. По определению порядка, s – минимальное натуральное число такое, что $g^{ls} \equiv 1$. Заметим, что т.к. k – минимальное число такое, что $g^k \equiv 1$, то $k|ls$. Значит, мы ищем минимальное s такое, что $k|ls$, ведь если это верно, то несложно понять, что тогда s – порядок g^l.

Теперь сформулируем лемму:

Пусть $a, b \in \mathcal{N}$, s – минимальное натуральное число, такое что, $b|as$. Тогда $s = \frac{b}{gcd(a,b)}$.

Доказательство. $\frac{a}{gcd(a,b)}$ – целое, поэтому $\frac{ab}{gcd(a,b)} \vdots b$, то есть $\frac{b}{gcd(a,b)} \geqslant s$.

Пусть $a' = \frac{a}{gcd(a,b)}, b' = \frac{b}{gcd(a,b)}$).
Тогда т.к. $b|as$, то $b'|a's$, а в силу того, что $gcd(a', b') = 1$, то $b'|s \Rightarrow s \geqslant b'$. А т.к. $s \leqslant b'$, то $s = b'$.

Следствие: если есть порядок k, то есть порядки и всех делителей k.
Пусть существует $ord(k) < \infty \pmod m$. Тогда $gcd(k, m) = 1$.

Значит, если $a|k$, то $gcd(a, m) = 1$. Тогда рассмотрим m чисел: $a^1, \ldots, a^{m-1}$. Если среди них все различные, тогда среди них есть 1, т.к. остатков от деления на m, отличных от 0, ровно $m - 1$. В противном случае какие-то два различных числа равны, то есть $a^i \equiv a^{i+t} \pmod m$, где $t \neq 0$. Тогда $a^i(a^t - 1) \equiv 0 \pmod m$, а т.к. $gcd(a^i, m) = 1$, то $a^t \equiv 1 \pmod m$. □

69 Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Теорема Лиувилля (б/д). Конструкция трансцендентного числа с помощью цепной дроби и теоремы Лиувилля. Сводка результатов о трансцендентности: $e, \pi, e + \pi, \pi + e^\pi, \alpha^\beta$ (теорема Гельфонда), вывод про e^π из теоремы Гельфонда.

Определение α - *алгебраическое число*, если существует многочлен с целыми коэффициентами, корнем которого служит α. **Определение** *Степень алгебраического числа* - это минимальная степень уравнения, корнем которого является это число.

$\mathbb{A}$ - множество алгебраических чисел.

Заметим, что $\mathbb{A}$ - счётное множество (доказывалось на матлогике), но $\mathbb{C}$ континуально. Отсюда следует, что есть не алгебраические числа. **Определение** $\alpha \in \mathbb{C}$ - *трансцендентное*, если оно не является алгебраическим.

Теорема (Лиувилль) Пусть α - алгебраическое степени d. Тогда $\exists c = c(\alpha)$, что неравенство $|\alpha - \frac{p}{q}| \leqslant \frac{c}{q^d}$ имеет лишь конечное число решений в $\frac{p}{q}$. (Если уменьшить c, то вообще не будет решений)

Конструкция трансцендентного числа с помощью цепной дроби и теоремы Лиувилля:
Теорема $\forall \psi(q) \to +\infty \; \exists \alpha$: неравенство $|\alpha - \frac{p}{q}| \leqslant \frac{1}{q\psi(q)}$ имеет б.м. решений в $\frac{p}{q}$.

Как пример можно взять $\psi(q) = e^q$. Из предыдущей теоремы возьмём число α. Предположим α - алгебраическое число, тогда $\exists d \in \mathbb{N} : |\alpha - \frac{p}{q}| > \frac{c}{q^d}$ выполняется для $\forall p, q$. Что противоречит предыдущей теореме (неравенство $|\alpha - \frac{p}{q}| \leqslant \frac{1}{q\psi(q)}$ имеет б.м. решений в $\frac{p}{q}$).

То есть мы совершенно явно, с помощью аппарата цепных дробей, построили трансцендентное число α.

Сведения о некоторых числах: $e, \pi, \pi + e^\pi$ являются трансцендентными. Про $e + \pi$ на данный момент ничего неизвестно.

Теорема (Гельфонд) Пусть α, β алгебраические, при этом β иррациональное, а $\alpha \notin \{0, 1\}$. Тогда α^β трансцендентно.

Утверждение. e^π трансцендентно.

▲ Предположим противное: e^π - алгебраическое. Заметим, что i - алгебраическое. Пусть $\alpha = e^\pi, \beta = i = \sqrt{-1} \Rightarrow \alpha^\beta = e^{i\pi}$, но $\alpha^\beta = e^{i\pi} = -1 \Rightarrow \alpha^\beta$ - алгебраическое. Противоречие с теоремой Гельфонда. ■

70 Умение: решать уравнения Пелля.

Определение 70.1. Уравнение вида $x^2 - my^2 = 1$, где m – натуральное число, не являющееся точным квадратом, называется *уравнением Пелля.*
Решение $(1, 0)$ называется *тривиальным.*
Решение (x, y) называется *положительным*, если $x \geqslant 0$ и $y \geqslant 0$.

Замечание. Уравнение вида $x^2 - my^2 = 1$ не является уравнением Пелля по этому определению. Однако теория по решению данного уравнения есть во второй теореме и во втором примере.

Замечание. Ввиду симметрии для решения уравнения достаточно найти все положительные решения.

Замечание. Если m является полным квадратом, то, очевидно, у уравнения нет решений, кроме тривиальных.

Замечание. Пара (x, y) в $\mathbb{Z}[\sqrt{m}]$ имеет вид $x + y\sqrt{m}$. Норма числа $a = x + y\sqrt{m}$ в $\mathbb{Z}[\sqrt{m}]$ это $N(a) = a \cdot \overline{a} = (x + y\sqrt{m})(x - y\sqrt{m}) = x^2 - my^2$. Норма обладает свойством: $N(a) \cdot N(b) = N(a \cdot b)$

Утверждение 70.1. *Пара (x, y) является решением уравнения Пелля ($x^2 - my^2 = 1$) тогда и только тогда, когда норма числа $x + y\sqrt{m}$ в $\mathbb{Z}[\sqrt{m}]$ равна единице.*

▲.

$$N(x + y\sqrt{m}) = (x + y\sqrt{m})(x - y\sqrt{m}) = x^2 - my^2$$

□

Утверждение 70.2. *Пара (x, y) является решением уравнения $x^2 - my^2 = -1$ тогда и только тогда, когда норма числа $x + y\sqrt{m}$ в $\mathbb{Z}[\sqrt{m}]$ равна минус единице.*

Определение 70.2. $\frac{P_k}{Q_k} = [a_0; a_1, a_2, ..., a_k], (k = 0, 1, ..., n)$ называется *k-ой подходящей дробью* к числу $[a_0; a1, a2, ..., a_n]$.

Теорема 70.1. *Если n – длина периода цепной дроби, соответствующей $\sqrt{m}$, то решениями уравнения Пелля $x^2 - my^2 = 1$ являются в точности подходящие дроби числа $\sqrt{m}$ вида $\frac{P_{kn-1}}{Q_{kn-1}}$, где kn – чётно.*

Замечание. Способы нахождения корней уравнения $x^2 - my^2 = -1$. (У автора конспекта нет уверенности, что данные способы находят все корни уравнения, однако других способов он не знает)
Способ 1) Если n – длина периода цепной дроби, соответствующей $\sqrt{m}$, то решениями уравнения $x^2 - my^2 = -1$ являются подходящие дроби числа $\sqrt{m}$ вида $\frac{P_{kn-1}}{Q_{kn-1}}$, где kn – нечётно.
Способ 2) Находим a - минимальное положительное решение $x^2 - my^2 = 1$, находим b - тривиальное (самое простое) решение $x^2 - my^2 = -1$, тогда $\pm(a^p \cdot b^{2k+1})$ будут решениями $x^2 - my^2 = -1$ для $\forall p, k \in \mathbb{Z}$.

Пример 1.
Найдите наименьшее положительное решение уравнения Пелля $x^2 - 6y^2 = 1$.
1) Найдём цепную дробь для $\sqrt{6}$:

$$\sqrt{6} = [2; \overline{2, 4}]$$

2) Длина периода цепной дроби $n = 2$, значит минимальное k, такое, что kn будет чётным, равно 1. Значит, минимальное решение – подходящие дроби вида $\frac{P_{kn-1}}{Q_{kn-1}} = \frac{P_1}{Q_1}$.
3) $\frac{P_1}{Q_1} = [2; 2] = 2 + \frac{1}{2} = \frac{5}{2}$.
Получается, пара $(x, y) = (5, 2)$ является минимальным положительным решением уравнения Пелля.

Пример 2.
Найдите наименьшее положительное решение уравнения $x^2 - 2y^2 = -1$.
1) Найдём цепную дробь для $\sqrt{2}$:

$$\sqrt{2} = [1; \overline{2}]$$

2) Длина периода цепной дроби $n = 1$, значит минимальное k, такое, что kn будет нечётным, равно 1. Значит, минимальное решение – подходящие дроби вида $\frac{P_{kn-1}}{Q_{kn-1}} = \frac{P_0}{Q_0}$.
3) $\frac{P_0}{Q_0} = [1] = \frac{1}{1}$.
Получается, пара $(x, y) = (1, 1)$ является решением уравнения (в данном случае оно является тривиальным).
4) Следующее решение $\frac{P_3}{Q_3} = [1; 2, 2] = \frac{7}{5}$.
Получается, пара $(x, y) = (7, 5)$ является решением уравнения.

Теорема 70.2. *Пусть $\alpha = a_1 + b_1\sqrt{m}$ – наименьшее нетривиальное положительное решение уравнения $x^2 - my^2 = 1$, то все решения этого уравнения имеют вид $\pm(\alpha)^k, k \in \mathbb{Z}$.*

Следствие. *В условиях предыдущей теоремы решениями уравнения Пелля будут пары:*

$$\pm\left(\frac{(a_1 + b_1\sqrt{m})^k + (a_1 - b_1\sqrt{m})^k}{2}, \frac{(a_1 + b_1\sqrt{m})^k - (a_1 - b_1\sqrt{m})^k}{2\sqrt{m}}\right), k \in \mathbb{Z}$$

Пример 3.
Найдите все решения уравнения Пелля $x^2 - 6y^2 = 1$.
Из примера 1 мы знаем, что пара $(x, y) = (5, 2)$ является минимальным положительным решением уравнения Пелля.
Тогда общее решение имеет вид:

$$\pm\left(\frac{(5 + 2\sqrt{m})^k + (5 - 2\sqrt{m})^k}{2}, \frac{(5 + 2\sqrt{m})^k - (5 - 2\sqrt{m})^k}{2\sqrt{m}}\right), k \in \mathbb{Z}$$

Пример 4.
Решите уравнение $x^2 - 6xy + y^2 = 1$ в целых числах

$$x^2 - 6xy + y^2 = (x - 3y)^2 - 8y^2 = 1$$

Делаем замену $z = x - 3y$, и уравнение сводится к уравнению Пелля $z^2 - 8y^2 = 1$

71 Иррациональность числа e.

Теорема 71.1. *Число e - иррациональное.*

▲

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}$$

Предположим противное: e - рациональное $\Rightarrow e = \frac{...}{k}$, тогда $e \cdot k! \in \mathbb{Z}$

$$e \cdot k! = A + \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \dots,$$

где $A \in \mathbb{Z}$.

$$0 < \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \dots < \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \dots = 1$$

Противоречие. Следовательно, e - иррациональное. ■

72 Определение решётки и дискретного подмножества. Любая дискретная подгруппа $\mathbb{R}^n$ является решёткой.

Опр Пусть $(e_1, ..., e_k)$ — набор линейно независимых векторов в $\mathbb{R}^n$. Тогда дискретная абелева группа в $\mathbb{R}^n$, порождённая $\{e_i\}$, называется решёткой, а набор $(e_1, ..., e_k)$ называется базисом решётки. Иными словами, решётка есть множество $\Lambda = \{a_1e_1 + ... + a_ke_k\}, a_i \in \mathbb{Z}$

Опр Подмножество X пространства $\mathbb{R}^n$ называется дискретным, если для любой точки x ∈ X существует окрестность этой точки, не содержащая других точек множества X.

Теорема. Любая дискретная подгруппа $\mathbb{R}^n$ является решёткой.

▲ 1. Дискретное множество в $\mathbb{R}^n$ является множеством изолированных точек: действительно, рассматриваем произвольную точку, принадлежащую множеству; по определению дискретности, она является изолированной точкой этого множества.

2. По определению группы, выполняется ассоциативность, наличие нейтрального элемента и наличие обратного элемента. ∃ нейтральный элемент: это начало координат.

3. Мы выбрали начало координат. Возьмём расстояния всех точек до начала координат. Существует inf расстояний, отличный от нуля (так как иначе в любой эпсилон-окрестности начала координат существует точка из нашего множества), inf > 0

4. Докажем, что inf достигается. Предположим противное - тогда в любой эпсилон окрестности infinum'а существует бесконечное количество точек с радиусом, большим чем он. Но тогда обязательно найдутся две точки, расстояние между которыми меньше inf ⇒ в силу бытия подгруппой мы можем отложить это расстояние от нуля и получить противоречие тому, что мы выбрали inf. Значит, inf достигается.

5. Выбираем этот inf и так последовательно формируем базис: получаем базис размера k, получаем линейные подпространства размерности k, находим расстояние между ними, это и есть искомый вектор базиса, получаем базис размерности k + 1.

6. Этот процесс должен оставиться не позднее, чем n. Почему так? Предположим противное. Тогда ∃ точка в фундаментальной области, которая не была получена. Но она же находится в фундаментальной области, граничащей с нулём, в силу того, что это группа ⇒ противоречие тому, что мы всегда выбирали минимальные расстояния (мы нашли точку с меньшим расстоянием). P.S. По сути мы просто пытаемся показать, что мы не можем найти n + 1-й линейно независимый вектор в пространстве $\mathbb{R}^n$. ■

Доказательство 2:

1) В любом компакте содержится лишь конечное число точек из G

2) Будем рассматривать линейное пространство, порождённое нашей подгруппой G.

3) Выберем базис (в подпространстве) e_1,...,e_k среди элементов нашей группы, и рассмотрим подгруппу $G_0 = Ze_1 + .. + Ze_k \subset G$.

4) Так как G дискретная, в G/G_0 содержится конечное количество элементов (по пункту 1), пусть $[G : G_0] = q$.

5) G содержится в $1/qG_0$, и поэтому является решёткой.

73 Двумерная теорема Минковского. Ее уточнение для замкнутых множеств (б/д).

Двумерная теорема Минковского.

Th. Пусть $\Omega \subset \mathbb{R}^2$, Ω органичена и $\mu(\Omega) > 4$, Ω выпукло и симметрично относительно начала координат. Тогда $(\Omega \cap \mathbb{Z}^2) \setminus \{0\} \neq \varnothing$.

Доказательство: Рассмотрим $\left(\Omega \cap \frac{1}{m}\mathbb{Z}^2\right)$, $m \in \mathbb{N}$. Пусть $N_m = \left|\left(\Omega \cap \frac{1}{m}\mathbb{Z}^2\right)\right|$. Заметим, что с увеличением m суммарная площадь «квадратиков» на узлах решетки будет стремиться к $\mu(\Omega)$ хоть по Жордану, хоть по Лебегу, то есть $\frac{N_m}{m^2} \to \mu(\Omega) > 4$. Значит $\exists m_0 : \forall m > m_0 \hookrightarrow \frac{N_m}{m^2} > 4 \Longrightarrow N_m > 4m^2 = (2m)^2$.

Рассмотрим две точки такой решетки с координатами $\left(\frac{a_1}{m}, \frac{a_2}{m}\right)$ и $\left(\frac{b_1}{m}, \frac{b_2}{m}\right)$. По модулю $2m$ существует ровно $2m$ вычетов для числителя первой и второй координат. Тогда число различных пар с точки зраения вычетов по модулю $2m$ ровно $(2m)^2$.

Но $N_m > (2m)^2$, значит существуют две различные точки $a' = \left(\frac{a_1}{m}, \frac{a_2}{m}\right)$ и $b' = \left(\frac{b_1}{m}, \frac{b_2}{m}\right)$ такие, что $a_1 \equiv b_1\ (2m)$ и $a_2 \equiv b_2\ (2m)$. Теперь рассмотрм точку $c' = \frac{a'-b'}{2}$, при этом так как $b' \in \Omega, -b' \in \Omega$. Так как Ω выпукла, значит и вель отрезок от a' ло b' лежит в Ω, при этои c' тоже в Ω, так как c' — середина отрезка. Но c' имеет целые координаты, при этом она ненулевая, так как $a' \neq b'$.

■

Уточнение двумерной теоремы Минковского для замкнутых множеств.

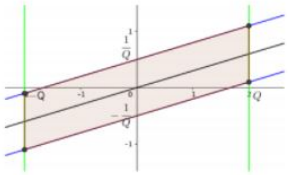
Th. Пусть $\Omega \subset \mathbb{R}^2$, Ω органичена и $\mu(\Omega) \geq 4$, Ω **замкнуто**, выпукло и симметрично относительно начала координат. Тогда $(\Omega \cap \mathbb{Z}^2) \setminus \{0\} \neq \varnothing$.

74 Применение двумерной теоремы Минковского для передоказательства теоремы Дирихле. Теорема Дирихле о совместном диофантовом приближении (б/д)

Теорема Дирихле.

Th. (Дирихле) Пусть $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Тогда $\exists$ бесконечно много рациональных дробей $\frac{p}{q}$ таких, что $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$.

Доказательство: Рассмотрим $\Omega = \{(x,y) || x| \leq Q, |\alpha x - y| \leq Q^{-1}\}$



Тогда $\mu(\Omega) = 2Q \cdot \frac{2}{Q} = 4$ и Ω выпукло, замкнуто и симметрично. Тогда по теореме Минковского $\exists (q,p) \in (\Omega \cap \mathbb{Z}^2) \setminus \{0\}$. Тогда $0 \leq q \leq Q$, $|\alpha q - p| \leq \frac{1}{Q} \Longrightarrow \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}$.

А как получить бесконечно много таких дробей? Ну отметим полученную точку (p,q) и выберем $\frac{1}{Q}$ так, чтобы прямые были ниже этой точки и повторить рассуждения выше.

■

Теорема Дирихле о совместном диофантовом приближении.
$\alpha_1, \ldots, \alpha_n \notin \mathbb{Q} \Rightarrow \exists$ бесконечно много различных $(p_1/q, \ldots, p_n/q) : |\alpha_i - p_i/q| \leqslant \frac{1}{q^{1+1/n}}$

75 Критический определитель решётки. Переформулировка теоремы Минковского через критический определитель. Теорема Минковского–Главки и история ее улучшений (б/д). Многомерный октаэдр, его объём.

Критический определитель $\Omega \subset \mathbb{R}^n$; $\Delta(G)$: $\Delta(G) = \inf\{\det \Lambda : (\Omega \cap \Lambda)\setminus\{0\} = \varnothing\}$

Переформулировка теоремы Минковского через критический определитель. Если Ω - выпукла и центрально симметрична относительно 0, то $\frac{Vol\Omega}{\Delta(\Omega)} \leqslant 2^n$.

Проблема: хочется оценить эту дробь снизу. Но мало ли чего хочется...

Теорема Минковского-Главки, 1945. $\forall\Omega \frac{Vol\Omega}{\Delta(\Omega)} \geqslant 1$

Теорема Шмидта, Роджерса, 50-60-е гг. $\geqslant cn$.

$O^n = x : |x_1| + ... + |x_n| \leqslant 1$ — **n-мерный октаэдр (кросс-политоп, ортаэдр** - линейная оболочка векторов (1,0,..0), (0,1,..0), ...

Объём n-мерного октаэдра: $Vol(O^n) = \frac{2^n}{n!}$

76 Равномерно распределенные последовательности (mod 1): три эквивалентные формулировки.

Теорема. Следующие условия (условие равномерной распределённости mod 1) для последовательности $x_1, x_2, \ldots, x_n, \ldots$ эквивалентны:

$$1)\ \forall a, b \in [0,1] \lim_{N\to\infty} \frac{|\{i = 1, \ldots, N : \{x_i\} \in [a,b)\}|}{N} = b - a$$

$$2)\ \forall\gamma\in[0,1]\ \lim_{N\to\infty}\frac{|\{i=1,\dots,N:\{x_i\}<\gamma\}|}{N}=\gamma$$

$$3)\ \text{Отклонение } D_N=\sup_{0\leqslant\alpha<\beta\leqslant1}|\frac{|\{n|n\leqslant N,\alpha\leqslant\{x_n\}<\beta\}|}{N}-(\beta-\alpha)|,\ \lim_{N\to\infty}D_N=0$$

▲

1) $\Rightarrow$ 2): a = 0.

2) $\Rightarrow$ 3): $D_N=\sup_{0\leqslant\alpha<\beta\leqslant1}|\frac{|\{n|n\leqslant N,\alpha\leqslant\{x_n\}<\beta\}|}{N}-(\beta-\alpha)|\leqslant\sup_\beta|\frac{|\{i=1,\dots,N:\{x_i\}<\beta\}|}{N}-\beta|+\sup_\alpha|\frac{|\{i=1,\dots,N:\{x_i\}<\alpha\}|}{N}-\alpha|$ (по неравенству треугольника). Из п. 2) оба слагаемых стремятся к нулю $\Rightarrow\lim_{N\to\infty}D_N=0$

3) $\Rightarrow$ 1) Условие (3) подразумевает, что если sup по a и b так стремится, то это выполняется для любых a, b, что равносильно, что для любых a, b предел равен b - a.

■

77 Является ли ln n p.p. (mod 1) последовательностью?

Утверждение: $ln(n)$ не является p.p. (mod 1) последовательностью.

▲ Числа, подходящие под условие, имеют вид $e^k, e^{k+1},\dots e^{k+\gamma}$. Количество таких чисел - $e^{k+\gamma}-e^k=e^k(e^\gamma-1)$ для конкретного k. Просуммируем от 1 до $[ln(N)]$, так как именно столько у нас значений может принимать k (переменная, принимающая значения из множества целых частей от x_n):

$$F(N,\gamma)=\sum_{k=1}^{[ln(N)]}e^k(e^\gamma-1)=(e^\gamma-1)\cdot\frac{e^{[ln(N)]+1}}{e-1}+O([ln(N)])$$

$$\lim_{n\to\infty}\frac{F(N,\gamma)}{N}=\frac{e^\gamma-1}{e-1}\lim_{n\to\infty}\frac{e^{[ln(N)]+1}+O([ln(N)])}{N}=\frac{e^\gamma-1}{e-1}\neq\gamma$$

■

78 Определение p.p. (mod 1) последовательности. Вывод интегрального признака из того, что последовательность p.p. (mod 1). Формулировка интегрального признака через комплекснозначную функцию (б/д).

79 Определение p.p. (mod 1) последовательности. Вывод p.p. (mod 1) последовательности из интегрального признака. Формулировка интегрального признака через комплекснозначную функцию (б/д).

Послед-ность $x_1,x_2,\dots,x_n,\dots$ - **равномерно распределена по модулю 1**, если:

$$\forall a,b\in[0,1]\ \lim_{N\to\infty}\frac{|\{i=1,\dots,N:\{x_i\}\in[a,b)\}|}{N}=b-a$$

Теорема об интегральном признаке. x_n - p.p. mod 1 $\Leftrightarrow \forall$ функции f, определённой и непрерывной на [0; 1] $\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(\{x_n\}) = \int_0^1 f(x)dx$.

▲ Введём индикатор "попадания"в отрезок: $I_{[a;b)}(x) = 1$, если $x \in [a;b)$, 0 иначе. Но при этом $\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} I_{[a;b)}(\{x_n\}) = b - a = \int_0^1 I_{[a;b)}(\{x\})dx$, если x_n равномерно распределена.

$\Rightarrow$. 1) Пусть x_n - равномерно распределена.

2) Разобьём отрезок [0; 1] точками $a_1, a_2, \ldots, a_m; a_0 = 0, a_{m+1} = 1$ на конечное число подотрезков: $[0;a_1)\cup[a_1;a_2)\cup\cdots\cup[a_m;1)$. Рассмотрим индикатор каждой из частей и эти индикаторы сложим. $\sum_{i=1}^{m+1} c_i I_{[a_{i-1};a_i]}$ - ступенчатая функция.

3) Пусть g(x) - ступенчатая функция. Тогда с учётом пункта 1, $\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} g(\{x_n\}) = \int_0^1 g(x)dx$. Таким образом, мы доказали для индикатора и для линейной комбинации индикаторов (ступенчатой функции). Тогда мы фиксируем f определённую и непрерывную на [0; 1), фиксируем $\varepsilon > 0$. Тогда $\exists f_1, f_2$ - ступенчатые, такие, что $f_1(x) \leqslant f(x) \leqslant f_2(x) \forall x$, $\int_0^1 (f_2(x) - f_1(x))dx < \varepsilon$.

4) Отсюда: $\int_0^1 f(x)dx - \varepsilon \leqslant \int_0^1 f_2(x)dx - \varepsilon \leqslant \int_0^1 f_1(x)dx = \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f_1(\{x_n\}) \leqslant \underline{\lim}_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(\{x_n\}) \leqslant \overline{\lim}_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(\{x_n\}) \leqslant$
$\leqslant \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f_2(\{x_n\}) = \int_0^1 f_2(x)dx \leqslant \int_0^1 f_1(x)dx + \varepsilon \leqslant \int_0^1 f(x)dx + \varepsilon$

5) Из рассуждения выше нижний и верхний предел лежат между $\int_0^1 f(x)dx - \varepsilon$ и $\int_0^1 f(x)dx + \varepsilon$, так как ε - любой, то нижний и верхний пределы равны, значит, существует предел, равный $\int_0^1 f(x)dx$

$\Leftarrow$ Пусть $\forall f$ выполняется условие. Тогда верны рассуждения из пункта 4, только в пункте 4 мы аппроксимировали непрерывную функцию индикаторами, а теперь мы хотим аппроксимировать индикатор непрерывными функциями: $\forall\varepsilon\ \exists g_1, g_2$ - непрерывные: $g_1(x) \leqslant I_{[a;b)} \leqslant g_2(x)$ и $\int_0^1 (g_2(x) - g_1(x))dx \leqslant \varepsilon$. Далее аналогично. ■

Формулировка интегрального признака через комплекснозначную функцию. x_n - p.p. mod 1 $\Leftrightarrow \forall$ *комплекснозначной* функции f, имеющей период 1, $\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(\{x_n\}) = \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx$

81 Сумма Гаусса

Для начала узнаем, чему равны следующие суммы:
$\sum_{x=1}^{k} e^{2\pi i x}$
Она с очевидностью равна k, т.к. $e^{2\pi i x} = 1\ \forall x \in N$
Теперь рассмотрим такую сумму:
$\sum_{x=1}^{q} e^{2\pi i \frac{ax}{q}}$, где (a,q) = 1
$\sum_{x=1}^{q} e^{2\pi i \frac{ax}{q}} = e^{2\pi i \frac{a}{q}} * (\frac{e^{2\pi i a}-1}{e^{\frac{2\pi i a}{q}}-1}) = 0$
Таким образом, если a и q взаимнопросты, сумма равна 0, иначе - q

Суммой Гаусса называется сумма вида $S = \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}}$. Посчитаем, чему равен ее

модуль
$|S|^2 = S * \overline{S} = \sum\limits_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} \sum\limits_{y=1}^{q} e^{-2\pi i \frac{ay^2}{q}}$.
Заметим, что суть данной суммы - суммирование по окружности через равные промежуточки. Поэтому разницы нет, начнем мы из точки "y"или из какой-то другой, полученной из "y"сдвигом по этой окружности. Результат не изменится. Поэтому давайте заменим по второй сумме "y"на "x + y". Продолжаем равенство:
$= \sum\limits_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} \sum\limits_{y=1}^{q} e^{-2\pi i * \frac{ay^2+2axy+ax^2}{q}} = \sum\limits_{x=1}^{q}\sum\limits_{y=1}^{q} e^{-2\pi i \frac{ay^2+2axy}{q}} = \sum\limits_{y=1}^{q}\sum\limits_{x=1}^{q} e^{-2\pi i \frac{ay^2+2axy}{q}} =$
$\sum\limits_{y=1}^{q} e^{-2\pi i \frac{ay^2}{q}} \sum\limits_{x=1}^{q} e^{-2\pi i \frac{2axy}{q}}$

Обозначим $b = -2ay$; $\sum\limits_{x=1}^{q} e^{-2\pi i \frac{2axy}{q}} = \sum\limits_{x=1}^{q} e^{2\pi i \frac{bx}{q}} (*)$
Рассмотрим, каким может быть q;

- ▷ Пусть q - нечетное. Тогда 2a не делится на q, а y делится на q только при y = q. $\Longrightarrow$ $(*) = 0\ \forall y \neq q$. При y = q $\longrightarrow$ $(*) = q$; $|S|^2 = e^{-2\pi i a q} * q = q$
- ▷ Пусть q - четное. Тогда b делится на q $\Longleftrightarrow$ $y = q, \frac{q}{2}$
  Рассуждая таким же образом, как в первом пункте, получим, что (*) не обнуляется только при двух значениях y. Тогда посчитаем сумму, учитывая это знание (подставляя в необнулившиеся слагаемые соответствующие y) $|S|^2 = 1 * q + e^{-2\pi i \frac{a}{q} * \frac{q^2}{4}} * q = q + q * e^{\frac{-\pi i a}{2} * q} = \begin{cases} 2q & q \equiv 0(4) \\ 0 & q \equiv 2(4) \end{cases}$

Таким образом:
$|S| = \begin{cases} \sqrt{q} & q \text{ - нечетное} \\ \sqrt{2q} & q \equiv 0(4) \\ 0 & q \equiv 2(4) \end{cases}$

82 Асимптотическая оценка $[1, 2, \ldots, n]$ снизу. Более грубая оценка, верная для $n > 7$. (б/д)

Лемма: $m! \geqslant \left(\frac{m}{e}\right)^m$

▲ 1. База $m = 1$: $1 \geqslant \frac{1}{e}$

2. Пусть для m верно. Покажем для $m + 1$. Заметим, что $\left(\frac{m}{m+1}\right)^m$ убывает (так как $\frac{m}{m+1} < 1$) и стремится к e^{-1}

$$(m+1)! = (m+1)\left(\frac{m}{e}\right)^m = (m+1)\left(\frac{m}{m+1}\right)^m \left(\frac{m+1}{e}\right)^m > \frac{m+1}{e}\left(\frac{m+1}{e}\right)^m = \left(\frac{m+1}{e}\right)^{m+1} \blacksquare$$

Утверждение: НОК$(1, \ldots, n) := [1, \ldots, n] \geqslant e^n$
▲

$$[1, \ldots, n] \geqslant \prod_{p \text{ - простое}, p \leqslant n} p$$

Количество простых чисел $\leqslant n : \pi(n) \sim \frac{n}{\ln n}, p_k \geqslant k$. Тогда

$$[1, \dots, n] \geqslant \left[\frac{n}{\ln n}(1 + o(1))\right]!$$

Так как по лемме $m! \geqslant \left(\frac{m}{e}\right)^m$, получаем

$$[1, \dots, n] \geqslant \left(\frac{n}{e \ln n}(1 + o(1))\right)^{\frac{n}{\ln n}(1+o(1))} = e^{\ln\left(\frac{n}{e \ln n}(1+o(1))\right)\frac{n}{\ln n}(1+o(1))}$$

Распишем большой логарифм из степени

$$\ln\left(\frac{n}{e \ln n}(1 + o(1))\right) = \ln n - 1 - \ln\ln n + \ln(1 + o(1)) = \ln n\left(1 - \frac{1}{\ln n} - \frac{\ln\ln n}{\ln n} + \frac{\ln(1 + o(1))}{\ln n}\right)$$

Функция в последней скобки стремится к 1 при $n \to \infty \Rightarrow$ этот логарифм равен $\ln n(1 + o(1))$

Подставив все назад в степень получаем

$$[1, \dots, n] \geqslant e^{n(1+o(1))^2} = e^{n(1+o(1))} \blacksquare$$

Утверждение (б/д): $[1, \dots, n] \geqslant 2^n, n > 7$

83 Алгоритм AKS. Определение и неравенства, связывающие числа $p, r, \log_2 n$ (б/д). Определение множеств I, P. Определение группы G, неравенство $|G| > \log_2^2 n$. Утверждения о делителе $h(X)$ многочлена $X^r - 1$ (б/д). Группа $\mathcal{G}$.

Замечание: Среди простых делителей числа n точно найдется число p с $\operatorname{ord}_r p > 1$ (так как $\operatorname{ord}_r n > \log_2^2 n > 1$).

Неравенство: $p > r > \log_2^2 n$

Определение:

$$I = \{\left(\frac{n}{p}\right)^i p^j;\ i, j \geqslant 0\}$$

$$P = \{\prod_{a=0}^{l}(x + a)^{e_a};\ e_a \geqslant 0\}$$

Рассмотрим в I вычеты по модулю r. Получаем группу G. Обозначим $t := |G|$.

Неравенство: $t \geqslant \operatorname{ord}_r n$ (так как в I есть элементы вида n^i, когда $i = j) > \log_2^2 n$ (по построению r) $\Rightarrow |G| > \log_2^2 n$. Так как G - подгруппа в $\mathbb{Z}_r^*$, то $|G| \leqslant |\mathbb{Z}_r^*| = \varphi(r)$

Утверждение: Пусть $h(x)$ - неприводимый над $\mathbb{Z}_p$ делитель $x^r - 1$. Тогда $\deg h(x) = \operatorname{ord}_r p > 1$

Утверждение: Рассмотрим классы многочленов равные по модулю $(h(x), p)$. Множетсво таких классов эквивалентности образует поле F, а в пересечении с P дает мультипликативную группу $\mathcal{G} \subset F^*$

84 Алгоритм AKS. Верхняя оценка на r (б/д). Обоснование неравенства $p > r > \log_2^2 n$ для подходящего делителя p числа n. Вывод тождества $(X+a)^{n/p} = X^{n/p} + a \pmod{X^r - 1, p}$. Определение перестановочности многочлена и числа. Утверждения о свойствах перестановочности.

Обоснование неравенства: Рассматриваем корректность последнего шага. Мы знаем, что $(r,n) = 1 \Rightarrow (r,p) = 1$ (p - делитель n, который мы выбрали в билете 83). Также $p > r$, в противном случае мы бы останавились на 3 или 4 шаге алгоритма. Тогда $p > r > \varphi(r) \geqslant \mathrm{ord}_r\, n > \log_2^2 n$ (последнее неравенство следует из построения r).

Тождество: $(x+a)^{n/p} = x^{n/p} + a \pmod{x^r - 1, p}$

▲

$$(x+a)^p = x^p + a \pmod{x^r - 1, p} \text{ при } a = 0 \dots l \text{ (см. билет 42)}$$

$$(x+a)^n = x^n + a \pmod{x^r - 1, n} \text{ при } a = 0 \dots l \text{ (следствие того, что мы прошли шаг 5)}$$

Второе выражение так же выполняется, если мы заменим mod n на mod p, так как p - делитель n (в дальнейшем будем часто переходить к делителям таким образом). Дальше все тождества рассматриваем для $a = 0 \dots l$.

Предположим, что $(x+a)^{n/p} \neq x^{n/p} + a \pmod{x^r - 1, p}$. Возведем обе части в степень p. Получаем $(x+a)^n \neq (x^{n/p} + a)^p \pmod{x^r - 1, p}$. По первому тождеству правая часть распишется как $x^n + a$. Получили, что $(x+a)^n \neq x^n + a \pmod{x^r - 1, p}$ - противоречие со вторым тождеством $\Rightarrow$ тождество верно ■

Определение: Пусть $f(x)$ - многочлен, m - число. Считаем, что $f(x)$ и m перестановочны, если $(f(x))^m = f(x^m) \pmod{x^r - 1, p}$

Утверждение 1: Если f перестановочно с m и g перестановочно с m, то $f \cdot g$ перестановочно с m

$$\blacktriangle\ (fg(x))^m = (f(x)g(x))^m = (f(x))^m (g(x))^m = f(x^m)g(x^m) = fg(x^m)\ \blacksquare$$

Замечание: $x^{mr} - 1 \vdots x^r - 1$

▲

$$x^r - 1 = (x-1)(1 + x + \ldots + x^{r-1})$$

$$x^{mr} - 1 = (x-1)(1 + x + \ldots + x^{r-1} + x^{r+1} + \ldots + x^{mr-1}) =$$

$$= (x-1)(1 \cdot (1 + \ldots + x^{r-1}) + x^r(1 + \ldots + x^{r-1}) + \ldots x^{(m-1)r}(1 + \ldots + x^{r-1})) =$$

$$= (x-1)(1 + \ldots + x^{r-1})(1 + \ldots + x^{(m-1)r}) \vdots x^r - 1\ \blacksquare$$

Утверждение 2: Если f перестановочно с m и m', то f перестановочно с mm'

▲

$$(f(x))^{mm'} = (f(x^m))^{m'} \pmod{x^r - 1, p}$$

Пусть $y = x^m$. Тогда

$$f(y)^{m'} = f(y^{m'}) \pmod{y^r - 1, p}$$

$y^r - 1 = x^{mr} - 1 \Rightarrow y^r - 1 \vdots x^r - 1$ (по замечанию) $\Rightarrow$ тождество верно и по модулю $x^r - 1$

(перешли к делителю). Получаем

$$(f(x))^{mm'} = f(y^{m'}) = f(x^{mm'}) \,(\mathrm{mod}\ x^r - 1, p) \blacksquare$$

87 Нижняя оценка разброса (уклонения) величиной $\frac{\sqrt{n}}{2}$ с помощью матриц Адамара.

Теорема Если n - порядок матрицы Адамара, то $\exists \mathcal{M} : \forall \chi \hookrightarrow disc(\mathcal{M}, \chi) \geqslant \frac{\sqrt{n}}{2}$, где $\mathcal{M} = \{\mathcal{M}_1, \ldots, \mathcal{M}_n\}, \forall i\ \mathcal{M}_i \subset \{1, 2, \cdots, n\} = \mathcal{R}$

▲ В данном билете используются понятия, определённые в билетах "Матрицы Адамара"(билет 15) и "Разброс системы подмножеств относительно раскраски"(билет 18).

По определению:

$$disc(\mathcal{M}, \chi) = max|\sum_{j \in \mathcal{M}_i} \chi(j)|$$

Пусть H - матрица Адамара, которая имеет нормальный вид, J - матрица из единиц. Рассмотрим матрицу $\frac{H+J}{2}$, она состоит только из нулей и единиц. Рассмотрим $\mathcal{M}$, в которой за $\mathcal{M}_i$ обозначим те позиции в i-ой строке, на которых стоят единицы. $\mathcal{M}_i \subset \{1, 2, \cdots, n\}$

Пусть

$$H \begin{pmatrix} v_1 \\ \cdots \\ v_n \end{pmatrix} = \begin{pmatrix} L_1 \\ \cdots \\ L_n \end{pmatrix}, v_i \in \{+1, -1\}$$

$$\left(\frac{H+J}{2}\right) \begin{pmatrix} v_1 \\ \cdots \\ v_n \end{pmatrix} = \begin{pmatrix} (L_1 + \lambda)/2 \\ \cdots \\ (L_n + \lambda)/2 \end{pmatrix}, v_i \in \{+1, -1\}, \lambda = \sum_{i=1}^{n} v_i$$

Тогда $\forall i$

$$(L_i + \lambda)/2 = (1...10...01...) \begin{pmatrix} v_1 \\ \cdots \\ v_n \end{pmatrix}$$

Будем с помощью v_i-ых задавать раскраску множества $\mathcal{R}$: $v_i = \chi(i)$. Тогда

$$|(L_i + \lambda)/2| = |\sum_{j \in \mathcal{M}_i} \chi(j)|$$

Следовательно, нам необходимо доказать, что для любого набора v_i (для любой раскраски множества $\mathcal{R}$), всегда найдётся $(L_i + \lambda)/2$ по модулю не меньшее $\frac{\sqrt{n}}{2}$.

$H = (\overline{h_1}, \ldots, \overline{h_n})$, т.е. $\overline{h_i}$ - i-ый столбец матрицы H. (Важное свойство $(h_i, h_j) = 0,\ \forall i \neq j$)

$$(H\overline{v}, H\overline{v}) = L_1^2 + \ldots + L_n^2$$

$$(H\overline{v}, H\overline{v}) = (\overline{h_1}\cdot v_1 + \ldots + \overline{h_n}\cdot v_n, \overline{h_1}\cdot v_1 + \ldots + \overline{h_n}\cdot v_n) = (\overline{h_1}, \overline{h_1})v_1^2 + \ldots + (\overline{h_n}, \overline{h_n})v_n^2 = n\cdot 1 + \ldots + n\cdot 1 = n^2 \Rightarrow$$

$$L_1^2 + \ldots + L_n^2 = n^2$$

$$(H+J)\overline{v} = \begin{pmatrix} L_1+\lambda \\ \cdots \\ L_n+\lambda \end{pmatrix}, \text{где } \lambda = \sum_{i=1}^{n} v_i\text{- чётное число}$$

$$((H+J)\overline{v},(H+J)\overline{v}) = (L_1+\lambda)^2+\ldots+(L_n+\lambda)^2 = L_1^2+\ldots+L_n^2+2\lambda\sum_{i=1}^{n}L_i+\lambda^2 n = n^2+2\lambda\sum_{i=1}^{n}L_i+\lambda^2 n$$

Используя структуру матрицы H - матрицы Адамара нормального вида, можно сказать, что $\sum_{i=1}^{n} L_i = \sum_{i=1}^{n} v_i \sum_{j=1}^{n} h_{ij} = v_1 \cdot n + v_2 \cdot 0 + \ldots + v_n \cdot 0 = \pm n$, следовательно

$$((H+J)\overline{v},(H+J)\overline{v}) = \lambda^2 n \pm 2\lambda n + n^2 \geqslant n^2$$

(Неравенство доказывается перебором целых значений в окрестности минимума)

Так как $((H+J)\overline{v},(H+J)\overline{v}) = (L_1+\lambda)^2+\ldots+(L_n+\lambda)^2$,то $\exists k : L_k+\lambda \geqslant \sqrt{n} \Rightarrow \frac{(L_k+\lambda)}{2} \geqslant \frac{\sqrt{n}}{2}$, следовательно, для рассматриваемого $\mathcal{M}$ верно:

$$disc(\mathcal{M},\chi) = max|\sum_{j\in\mathcal{M}_i}\chi(j)| \geqslant |\sum_{j\in\mathcal{M}_k}\chi(j)| = \frac{(L_k+\lambda)}{2} \geqslant \frac{\sqrt{n}}{2}$$

Следовательно, $\exists\mathcal{M} : \forall\chi \hookrightarrow disc(\mathcal{M},\chi) \geqslant \frac{\sqrt{n}}{2}$ ■

88 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема Чебышёва (верхняя оценка)

$$\pi(x) = \sum_{p<=x} 1$$

$$\theta(x) = \sum_{p<=x} ln(p)$$

$$\psi(x) = \sum_{(p,\alpha):p^\alpha<=x} ln(p)$$

Теорема Чебышева

$\exists x_0 :$ $\forall x \geqslant x_0$ выполнено:

$\ln 2 * \frac{x}{lnx} \leqslant \pi(x) \leqslant 4ln2\frac{x}{lnx}$

▲ Введем $\lambda_1 = \overline{lim}_{x->\infty}\frac{\theta(x)}{x}$, $\lambda_2 = \overline{lim}_{x->\infty}\frac{\psi(x)}{x}$, $\lambda_3 = \overline{lim}_{x->\infty}\frac{\pi(x)}{\frac{x}{lnx}}$. Аналогично определим μ_1,μ_2,μ_3

$\mu_1 = \underline{lim}_{x->\infty}\frac{\theta(x)}{x}$, $\mu_2 = \underline{lim}_{x->\infty}\frac{\psi(x)}{x}$, $\mu_3 = \underline{lim}_{x->\infty}\frac{\pi(x)}{\frac{x}{lnx}}$

Лемма

$\lambda_1 = \lambda_2 = \lambda_3$, $\mu_1 = \mu_2 = \mu_3$

▲ $\lambda_1 \leqslant \lambda_2$ - очевидно. Зафиксируем р. $\alpha : p^\alpha \leqslant x, [log_p(x)] = [\frac{ln(x)}{ln(p)}]$; $\psi(x) = \sum_{(p,\alpha):p^\alpha<=x} ln(p) = \sum_{p\leqslant x}[\frac{ln(x)}{ln(p)}]ln(p) \leqslant \sum_{p\leqslant x} ln(x) = ln(x)\sum_{p\leqslant x} 1 = \pi(x) * ln(x) \Longrightarrow \frac{\psi(x)}{x} \leqslant \frac{\pi(x)ln(x)}{x} = \frac{\pi(x)}{\frac{x}{lnx}} \Longrightarrow \lambda_2 \leqslant \lambda_3$

Осталось показать, что $\lambda_1 \geqslant \lambda_3$. $\theta(x) = \sum\limits_{p<=x} ln(p) \geqslant \sum\limits_{x^\gamma<p<=x} ln(p)$, $\gamma \in (0,1)$, $> \sum\limits_{x^\gamma<p<=x} ln(x^\gamma) = \gamma ln(x) \sum\limits_{x^\gamma<p<=x} 1 = \gamma ln(x)(\pi(x) - \pi(x^\gamma)) \geqslant \gamma ln(x)(\pi(x) - x^\gamma) \Longrightarrow$ $\frac{\theta(x)}{x} \geqslant \gamma(\frac{\pi(x)}{\frac{x}{lnx}} - \frac{x^\gamma}{x} * ln(x)) \Longrightarrow \lambda_1 \geqslant \gamma\lambda_3 \Longrightarrow \lambda_1 \geqslant \lambda_3$ Для μ_i доказывается аналогично, но в конце переходим к нижнему пределу, а не к верхнему■

Теперь начинаем доказывать Теорему Чебышева. Рассмотрим $C_{2n}^n < 2^{2n}$; $C_{2n}^n = \frac{(2n)!}{n!n!} \geqslant \prod\limits_{n<p\leqslant 2n} p \Longrightarrow \prod\limits_{n<p\leqslant 2n} p < 2^{2n}$. Прологарифмируем это по натуральному основанию. Получим: $\prod\limits_{n<p\leqslant 2n} ln(p) < 2nln2 \Longrightarrow \theta(2n) - \theta(n) < 2nln2$. Просуммируем правую и левую части выражения по степеням двойки. То есть пробежимся по всем n = 1,2,4, ..., 2^k. Получим $\theta(2^{k+1}) < 2^{k+2}ln2$

Теперь рассмотрим произвольный x.

Очевидно, что для каждого такого x $\exists! k : 2^k \leqslant x < 2^{k+1} \Longrightarrow \theta(x) \leqslant \theta(2^{k+1}) < 2^{k+2}ln2 \leqslant 4xln2 \Longrightarrow \frac{\theta(x)}{x} \leqslant 4ln2 \Longrightarrow \lambda_1 \leqslant 4ln2 \Longrightarrow \lambda_3 \leqslant 4ln2 \Longrightarrow \pi(x) \leqslant (4ln2 + \varepsilon)\frac{x}{lnx}$

Верхняя оценка доказана!

89 Распределение простых чисел в натуральном ряде. Функции $\pi(x), \theta(x), \psi(x)$. Теорема Чебышёва (нижняя оценка)

Теперь докажем нижнюю оценку..

$C_{2n}^n > \frac{2^{2n}}{2n+1}; (C_{2n}^0 + C_{2n}^1 + ... + C_{2n}^n + ... + C_{2n}^2 n = 2^{2n}, C_{2n}^n -$ самое большое слагаемое)

$C_{2n}^n = \frac{(2n)!}{n!n!} = \prod\limits_{p\leqslant 2n} p^{[\frac{2n}{p}]+[\frac{2n}{p^2}]+....-2([\frac{n}{p}])+[\frac{n}{p^2}]+...} = \prod\limits_{p\leqslant 2n} p^{([\frac{2n}{p}]-2[\frac{n}{p}])+([\frac{2n}{p^2}]-2[\frac{n}{p^2}])+...}$

Заметим, что $[2x] - 2[x] \leqslant 1 \Longrightarrow \leqslant \prod\limits_{p\leqslant 2n} p^{[log_p(2n)]} = \prod\limits_{p\leqslant 2n} p^{[\frac{ln(2n)}{ln(p)}]}$

$\frac{2^{2n}}{2n+1} < \prod\limits_{p\leqslant 2n} p^{[\frac{ln(2n)}{ln(p)}]}$

Логарифмируем по натруральному основанию. Получаем:

$2nln(2) - ln(2n+1) < \sum\limits_{p\leqslant 2n} ln(p) * [\frac{ln(2n)}{ln(p)}] = \psi(2n)$

Как и в предыдущих рассуждениях, берем произвольный x, $x \in [2n, 2n+2)$

$\psi(x) \geqslant \psi(2n) > 2nln(2) - ln(2n+1) > (x-2)ln(2) - ln(x+1) \Longrightarrow \frac{\psi(x)}{x} > ln(2) - \frac{2ln(2)}{x} - \frac{ln(x+1)}{x}$.

И переходим к нижнему пределу:

$\mu_2 \geqslant ln(2) \Longrightarrow \mu_3 \geqslant ln(2) \Longrightarrow \pi(x) \geqslant (ln(2) - \varepsilon)\frac{x}{ln(x)})$

Ура!■

90 Постулат Бертрана для n » 0.

Постулат Бертрана

Для любого натурального n > 2 найдётся простое число на интервале (n, 2n).

▲

1. Поскольку n » 0, можно считать, что n >= 4000 (Для меньших проверяется следующей последовательностью: 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001 - все простые и для любого n на (n, 2n) найдется простое число (берем максимальное число из ряда,

меньшее n, тогда 2p < 2n. При этом n < 2p, т.к. мы формируем ряд так, чтобы следующее за p число было меньше 2p))

2. Докажем следующее утверждение: $\prod\limits_{p\leqslant x} p \leqslant 4^{x-1}$

Будем доказывать по индукции. Заметим, что x можно рассматривать как простое число, потому что если мы берем произвольный x, то очевидно между ближайшим снизу простым числом и x никаких новых множителей не добавится.

1 База: x = 2; 2 < 4 -> верно

2 В силу того, что x - простое, оно нечетно. Тогда пусть x = 2m + 1, тогда $\prod\limits_{p\leqslant 2m+1} p = \prod\limits_{p\leqslant m} p \prod\limits_{m<p\leqslant 2m+1} p <= 4^m * C_{2m+1}^m \leqslant 4^m * 2^{2m} = 4^{2m}$

3. Положим, $\nu_p(x) = max\{k : x \vdots p^k\}$, тогда $\nu_p(n!) = \sum\limits_{k=1}^{\infty}[\frac{n}{p^k}]$, $\nu_p(C_{2n}^n) = \sum\limits_{k=1}^{\infty}[\frac{2n}{p^k}] - 2[\frac{n}{p^k}]$ $[\frac{2n}{p^k}] - 2[\frac{n}{p^k}] < \frac{2n}{p^k} - 2(\frac{n}{p^k} - 1) = 2 \Longrightarrow [\frac{2n}{p^k}] - 2[\frac{n}{p^k}] \leqslant 1$. Если $p^k > 2n$, то слагаемые равны 0. $\Longrightarrow \nu_p(C_{2n}^k) \leqslant max\{r : p^r \leqslant 2n\} \leqslant 2n$ Если $p > \sqrt{2n}$ $\nu_p(C_{2n}^k) \leqslant 1$. Иначе возведем в квадрат, получим, $p^2 = 2n < 2n$

4. Еще одно утверждение: Если $\frac{2n}{3} < p < n$, то $\nu_p(C_{2n}^n) = 0$
$3p > 2n \Longrightarrow (3p)! > (2n)!$. В силу того, что $2p < 2n < 3p$, в (2n)! на p делятся только множители p и 2p $\Longrightarrow \nu_p((2n)!) = 2, \nu_p(n!) = 1 \Longrightarrow \nu_p(C_{2n}^n) = 0$.

5. $\frac{4^n}{2n} \leqslant C_{2n}^n \leqslant \prod\limits_{p\leqslant\sqrt{2n}} 2n \prod\limits_{\sqrt{2n}<p\leqslant\frac{2n}{3}} p \prod\limits_{\frac{2n}{3}<p\leqslant 2n} p$. Рассмотрим последние два произведения. Они верны в силу п4, п3(Если $\sqrt{2n} < p$, то $\nu_p(C_{2n}^k) \leqslant 1$)$\Longrightarrow$ оценка верна

$$4^n \leqslant (2n)^{1+\sqrt{2n}} \prod_{\sqrt{2n}<p\leqslant\frac{2n}{3}} p \prod_{\frac{2n}{3}<p\leqslant 2n} p = (2n)^{1+\sqrt{2n}}\ \Pi_1\ \Pi_2$$

Если мы докажем, что $\Pi_2 \neq 1$, то между n и 2n есть простое число. Будем доказывать от противного. Пусть $\Pi_2 = 1$, тогда
$4^n \leqslant (2n)^{1+\sqrt{2n}}\ \Pi_1 \leqslant$/п.1/$(2n)^{1+\sqrt{2n}} 4^{\frac{2n}{3}} \Longrightarrow 4^{\frac{n}{3}} \leqslant (2n)^{1+\sqrt{2n}}$

$2n = ((2n)^{\frac{1}{6}})^6 \leqslant ([(2n)^{\frac{1}{6}}] + 1)^6$
Заметим, что a + 1 $\leqslant 2^a \Longrightarrow 2n \leqslant 2^{[(2n)^{\frac{1}{6}}]6} \leqslant 2^{(2n)^{\frac{1}{6}}6}$

$4^n = 2^{2n} \leqslant 2n^{3(1+\sqrt{2n})} \leqslant (2^{(2n)^{\frac{1}{6}}6})^{3(1+\sqrt{2n})} = 2^{(2n)^{\frac{1}{6}}18(1+\sqrt{2n})}$

Теперь воспользуемся тем, что $18 \leqslant 2\sqrt{2n} \Longrightarrow 2^{(2n)^{\frac{1}{6}}18(1+\sqrt{2n})} = 2^{(2n)^{\frac{1}{6}}(18+18\sqrt{2n})} \leqslant 2^{(2n)^{\frac{1}{6}}(20\sqrt{2n})} = 2^{(2n)^{\frac{2}{3}}20} \Longrightarrow 2n < (2n)^{\frac{2}{3}}20 \Longrightarrow (2n)^{\frac{1}{3}} < 20 \Longrightarrow 2n < 8000 \Longrightarrow n < 4000$. Противоречие ■

91 Показатели. Первообразные корни. Существование по модулю p.

Лемма: Если порядки чисел $x_1, \ldots, x_k$ взаимно-просты, то порядок $x_1 \cdot \ldots \cdot x_k$ равен произведению порядков.

▲ Докажем для двух чиел, для большего числа - по индукции. Пусть $\mathrm{ord}_n a = \delta_a, \mathrm{ord}_n b = \delta_b, (\delta_a, \delta_b) = 1$. Тогда $(ab)^{\delta_a\delta_b} = (a^{\delta_a})^{\delta_b}(b^{\delta_b})^{\delta_a} = 1 \pmod n$. Докажем, что $k < \delta_a\delta_b$ не являются порядками. Пусть $(ab)^k = 1 \pmod n$. Возведем обе части в степень δ_a: $(a^{\delta_a})^k b^{k\delta_a} = b^{k\delta_a} = 1 \Rightarrow k\delta_a \vdots \delta_b$, $(\delta_a, \delta_b) = 1 \Rightarrow k \vdots \delta_b$. Аналогично показываем, что $k \vdots \delta_a \Rightarrow \mathrm{ord}_n(ab) = \delta_a\delta_b$ ■

Утверждение: Если p нечетное простое число то по модулю p существует первообразный корень.

▲ Пусть $\delta_1, \ldots, \delta_{p-1}$ - показатели (порядки) чисел $1, \ldots, p-1$ соответственно. Рассмотрим $\tau := [\delta_1, \ldots, \delta_{p-1}] = q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k}$ - каноническое разложение.

$\forall i \in \{1, \ldots, k\}\ \exists \delta \in \{\delta_1, \ldots, \delta_n\}\ \exists a:\ \delta = aq_i^{\alpha_i},\ (a, q_i) = 1$ (верно, так как если полная степень делителя НОКа не входит ни в какое из чисел, то ее не должно быть в НОКе)

Зафиксируем i и найдем соответствующую ему δ. Выберем x такой что δ - его показатель. $1 = x^{\delta} = x^{aq_i^{\alpha_i}} = (x^a)^{q_i^{\alpha^i}} \pmod p \Rightarrow q_i^{\alpha_i}$ - порядок x^a (меньше не может быть так как иначе δ не был бы порядком x)

Рассмотрим $g = \prod_{i=1}^{k} x_i^{a_i}$ (по всем i). По лемме порядок g равен $q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k} = \tau \Rightarrow \tau \leqslant p-1$ (так как это порядок).

Рассмотрим сравнение $x^{\tau} \equiv 1 \pmod p$. Все числа $1. \ldots, p-1$ являются его корнями (так как τ - НОК их порядков) $\Rightarrow \tau \geqslant p-1$ (так как многочлен не может иметь больше корней чем его степень) $\Rightarrow \tau = p-1 \Rightarrow g$ - первообразный корень. ■

92 Показатели. Первообразные корни. Существование по модулю p^α, $\alpha \geqslant 2$: формулировка и доказательство леммы. Существование по модулю $2p^\alpha$.

Лемма: $\exists t:\ (g+pt)^{p-1} = 1 + pu,\ (p,u) = 1$

▲

$$(g+pt)^{p-1} = g^{p-1} + g^{p-2}(p-1)pt + p^2a = \underbrace{1+pv}_{g^{p-1}} + p(g^{p-2}(p-1)t + pa) = 1 + p(v + \underbrace{g^{p-2}(p-1)}_{\text{взаимно просто с } p}\ t + pa)$$

Так как t можно выбирать любым, легко можем подобрать его так, чтобы $v + g^{p-2}(p-1)t$ было взаимно просто с p. Тогда $u = v + g^{p-2}(p-1)t + pa$ - искомое ■

Утверждение 1: По модулю $p^\alpha, \alpha > 2$ (p - нечетное простое) существует первообразный корень.

Утверждение: По модулю $2p^\alpha$ (p - нечетное простое) существует первообразный корень.

▲

$$\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Для подсчета $\varphi(p^\alpha)$ воспользовались тем, что чисел кратных p, которые меньше p^α всего $p^{\alpha-1}$.

Пусть $g+pt$ - первообразный корень по модулю p^α. Если $g+pt$ - нечетное, то это и есть первообразный корень по модулю $2p^\alpha$ (если $a = (g+pt)^{\varphi(2p^\alpha)}$ нечетное, то $a-1$ - четное, а значит $a - 1 \vdots p^\alpha \Leftrightarrow a - 1 \vdots 2p^\alpha$)

Если $g + pt$ - чётное, то берем $g + pt + p^\alpha$ ■

93 Показатели. Первообразные корни. Существование по модулю p^α, $\alpha \geqslant 2$: формулировка леммы (б/д) и вывод существования из неё. Существование по модулю $2p^\alpha$.

Лемма: $\exists t:\ (g+pt)^{p-1} = 1 + pu,\ (p,u) = 1$

Утверждение 1: По модулю $p^\alpha, \alpha > 2$ (p - нечетное простое) существует первообразный корень.

▲ Покажем, что найденный в лемме $g+pt$ - первообразный корень по модулю p^α. Пусть δ - показатель $g+pt$ по модулю p^α.

$$(g+pt)^\delta \equiv 1 \pmod{p^\alpha} \Rightarrow (g+pt)^\delta \equiv 1 \pmod{p}$$

g - первообразный корень по модулю $p \Rightarrow \delta \vdots (p-1)$. С друой строны δ делит $\varphi(p^\alpha) = p^{\alpha-1}(p-1) \Rightarrow \delta = p^k(p-1), k \leqslant a-1$.

$$(g+pt)^{p-1} = 1 + pu, (p,u) = 1 \text{ (по лемме)}$$

$$(g+pt)^{p(p-1)} = (1+pu)^p = 1 + p^2u + p^3v = 1 + p^2(u+pv) = 1 + p^2u_1, (u_1, p) = 1$$

$(u_1, p) = 1 \Rightarrow u_1$ не содержит делителя $p^{\alpha-2}$ (при $\alpha \neq 2$) $\Rightarrow (1+gt)^{p(p-1)} \not\equiv 1 \pmod{p^\alpha}$

Будем повторять такой процесс для получившегося равенства пока не получим

$$(g+pt)^{p^{\alpha-1}(p-1)} = 1 + p^\alpha u_{\alpha-1} \equiv 1 \pmod{p^\alpha}$$

Следовательно, так как все меньшие δ вида $p^k(p-1)$ не подходят, порядком $g+pt$ является $p^{\alpha-1}(p-1) = \varphi(p^\alpha) \Rightarrow g+pt$ - первообразный корень ■

Замечание: существование по модулю $2p^\alpha$ см. билет 93.

94 Показатели. Первообразные корни. Несуществование по модулю 2^n, $n > 3$.

Замечание: Покажем, что по модулям 2 и 4 первообразные корни существуют.

$m = 2$: $\varphi(2) = 1, 1^1 \equiv 1 \pmod{2} \Rightarrow 1$ - первообразный корень

$m = 4$: $\varphi(4) = 2, 3^2 = 9 \equiv 1 \pmod{4}$, $3^1 \not\equiv 1 \pmod{4} \Rightarrow 3$ - первообразный корень

Утверждение: По модулю $2^\alpha, \alpha \geqslant 3$ не существует первообразных корней.

▲ $\varphi(2^\alpha) = 2^{\alpha-1}$ (все нечетные числа)

Пусть $a = 1 + 2t$ - нечетное. Покажем, что $a^{(2^{\alpha-2})} \equiv 1 \pmod{2^\alpha}$

$$(1+2t)^2 = 1 + 4t + 4t^2 = 1 + 4\underbrace{t(t+1)}_{\text{четное}} = 1 + 8t_1$$

$$(1+2t)^4 = (1+8t_1)^2 = 1 + 16t_1 + 64t_1^2 = 1 + 16t_2$$

$$\dots$$

$$(1+2t)^{(2^k)} = 1 + 2^{k+2}t_k$$

$$\dots$$

$$(1+2t)^{(2^{\alpha-2})} = 1 + 2^{\alpha} t_{\alpha-2} \equiv 1 \pmod{2^{\alpha}}$$

Следовательное любое нечетное число (то есть любое число, взаимно простое с 2^{α}) не является первообразным корнем $\Rightarrow$ первообразных корней по этому модулю нет ■

95 Показатели. Первообразные корни. Несуществование по модулям, отличным от $2^n, p^{\alpha}, 2p^{\alpha}$.

▲ Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$. $\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{k_i}) = \prod_{i=1}^{m} p_i^{k_i-1}(p_i - 1)$. Предположим противное: пусть существует g - первообразный корень по модулю n. Из теоремы Эйлера верно

$$\begin{cases} g^{(p_1-1)p_1^{k_1-1}} \equiv 1 \pmod{p_1^{k_1}} \\ \ldots \\ g^{(p_m-1)p_m^{k_m-1}} \equiv 1 \pmod{p_m^{k_m}} \end{cases}$$

Очевидно, что $\forall i \; z = \varphi(n)/2 = \frac{\prod_{i=1}^{m} p_i^{k_i-1}(p_i-1)}{2} \vdots (p_i - 1)p_i^{k_i-1}$ (двойку можно забрать из любого множителя относящегося к простому делителю, отличному от i-ого). Тогда верно

$$\begin{cases} g^z \equiv 1 \pmod{p_1^{k_1}} \\ \ldots \\ g^z \equiv 1 \pmod{p_m^{k_m}} \end{cases}$$

Пусть $g^z = 1 + p_1^{k_1} a = 1 + p_2^{k_2} b \Rightarrow p_1^{k_1} a = p_2^{k_2} b$. В силу взаимной простоты $p_1, p_2 \Rightarrow a \vdots p_2^{k_2} \Rightarrow g^z = 1 + p_1^{k_1} p_2^{k_2} a_1$. По индукции будем присоединять все больше множителей и в итоге получим

$$g^z = 1 + p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} t = 1 + nt \equiv 1 \pmod{n}, \; z = \varphi(n)/2 < \varphi(n) \Rightarrow$$

$$\Rightarrow g \text{ не является первообразным корнем по модулю } n \; ■$$

96 Теорема Лиувилля

Пусть $\alpha-$ алгебраическое число степени d >=2. Тогда $\exists c = c(\alpha)$ неравенство $|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^d} \forall p,q$

▲БОО можно считать, что $q > 0$, тогда рассмотрим два случая:
1. $|\alpha - \frac{p}{q}| \geqslant 1 \Longrightarrow$ подойдет $c = 1$
2. Считаем, что $|\alpha - \frac{p}{q}| \leqslant 1$
Заметим, что $|\alpha - \frac{p}{q}| \geqslant |\frac{p}{q}| - |\alpha| \Longrightarrow |\frac{p}{q}| \leqslant |\alpha| + 1$
Рассмотрим многочлен, корнем которого является α: $a_d x^d + ... + a_0 = \varphi(x)$. Этот многочлен не имеет рациональных корней, так как d - степень α. Из этого следует, что $\varphi(\frac{p}{q}) \neq 0$
$\varphi(\frac{p}{q}) = |a_d(\frac{p}{q})^d + a_{d-1}(\frac{p}{q})^{d-1} + ... + a_0| = |\frac{a_d p^d + a_{d-1} p^{d-1} q + ... + a_0 q^d}{q^d}| \geqslant \frac{1}{q^d}$.

Теперь рассмотрим над полем комплексных чисел

$\varphi(\frac{p}{q}) = a_d(x-\alpha)\prod\limits_{i=2}^{d}(x-\alpha_i)$

$|\varphi(\frac{p}{q})| = |a_d||\alpha-\frac{p}{q}|\prod\limits_{i=2}^{d}|\alpha_i-\frac{p}{q}| \leqslant |a_d||\alpha-\frac{p}{q}|\prod\limits_{i=2}^{d}(|\alpha_i|+|\frac{p}{q}|) \leqslant |a_d||\alpha-\frac{p}{q}|\prod\limits_{i=2}^{d}(|\alpha_i|+|\alpha|+1) \Longrightarrow$
$|\alpha-\frac{p}{q}| \geqslant \frac{1}{q^d}\frac{1}{|a_d|\prod\limits_{i=2}^{d}(|\alpha_i|+|\alpha|+1)} = \frac{1}{q^d} * c(\alpha)$ ■

97 Доказательство иррациональности чисила e. Тождество Эрмита

Теорема

e иррационально

▲ $e = \sum\limits_{n=0}^{\inf}\frac{1}{n!}$. Предположим, e = $\frac{...}{k}$ (т.е что e рационально), тогда Z ∋e*k! = $A + \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + ...$ Рассмотрим $\frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + ... \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + ... < \frac{1}{2} + \frac{1}{4} + ... = \frac{\frac{1}{2}}{1-\frac{1}{2}} = 1 \Longrightarrow$
$0 < \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + ... < 1 \Longrightarrow \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + ... \in Q \Longrightarrow A + \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + ... \in Q.$
Противоречие ■

Тождество Эрмита

Рассмотрим производные многочлена $f(x)$ степени ν.
Рассмотрим $\int_0^x f(t)e^{-t}dt$. Будем брать его по частям. $\int_0^x f(t)e^{-t}dt = -f(t)e^{-t}|_0^x + \int_0^x f'(t)e^{-t}dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t}dt = f(0) + f'(0) - (f(0) + f'(0))e^{-x} + \int_0^x f''(t)e^{-t}dt.$
Заметим, что когда мы продифференциируем больше ν раз, интеграл обратится в ноль. Таким образом, получим: $\int_0^x f(t)e^{-t}dt = (f(0) + f'(0) + ... + f^{(\nu)}(0)) - (f(x) + f'(x) + ... + f^{(\nu)}(x))e^{-x} = F(0) - F(x)e^{-x}$, где F(x) = $f(x) + f'(x) + ... + f^{(\nu)}(x)$. То равенство, которое мы получили, называется тождством Эрмита

98 Доказательство трансцендентности числа e

Предположим, e - алгебраическое число, тогда существует многочлен $a_m x^m + ... + a_0, a_i \in Z$, корнем которого является e.
$e^x \int_0^x f(t)e^{-t}dt = e^x F(0) - F(x), x = 0,1,2,...,m$

$\sum\limits_{x=0}^{m} a_x e^x \int_0^x f(t)e^{-t}dt = -\sum\limits_{x=0}^{m} a_x F(x)$. ($\sum\limits_{x=0}^{m} e^x a_x F(0) = F(0)(a_m e^m + ... + a_0 e^0 = 0)$) Воспользуемся тем, что в тождестве Эрмита мы можем использовать абсолютно любой многочлен. Давайте возьмем такой:
$f(t) = \frac{1}{(n-1)!}t^{n-1}((t-1)(t-2)(t-3)...(t-m))^n$

Рассмотрим левую часть равенства.
$|\sum\limits_{x=0}^{m} a_x e^x \int_0^x f(t)e^{-t}dt| \leqslant \sum\limits_{x=0}^{m} |a_x| e^x \int_0^x |f(t)|e^{-t}dt \leqslant \sum\limits_{x=0}^{m} |a_x| e^m \int_0^x |\frac{m^{mn+n-1}}{(n-1)!}|e^{-t}dt =$
$\frac{e^m m^{n(m+1)-1}}{(n-1)!}\sum\limits_{x=0}^{m}|a_x|\int_0^x e^{-t} = \frac{e^m m^{n(m+1)-1}}{(n-1)!}\sum\limits_{x=0}^{m}|a_x|(1-e^{-x}) < \frac{e^m m^{n(m+1)-1}}{(n-1)!}\sum\limits_{x=0}^{m}|a_x| = c_0\frac{(m^{m+1})^n}{(n-1)!} < 1, n \geqslant n_0$

Рассмотрим правую часть равенства

$|-\sum\limits_{x=0}^{m} a_x F(x)|$
$F(x) = f(x) + f'(x) + ... + f^{(\nu)}(x), \nu = n(m+1) - 1$
$F(0) = 0 + 0 + ... + 0$((n-1) раз. Покуда мы не возьмем n-1 производную, многочлен f(t) будет зануляться за счет множителя t^{n-1}) $+ (-1)^{mn}(m!)^n + n * A$(слагаемое после нулей получается за счет того, что мы избавились от $\frac{t^{n-1}}{(n-1)!}$, а следующее - за счет того, что мы берем производную и по второму множителю $((t-1)(t-2)(t-3)...(t-m))^n$, за счет чего возникает делимость на n)
Теперь рассмотрим F(x)
$\forall x = 1,2..m$ $f(x) + f'(x) + ... + f^{(\nu)}(x)$ имеет первые n нулей по той же причине (пока мы не возьмем n производных, множитель $((t-1)(t-2)(t-3)...(t-m))^n$ будет обнулять функцию. А после производные будут делиться на n). Таким образом, $|-\sum\limits_{x=0}^{m} a_x F(x)| = |\sum\limits_{x=0}^{m} a_x F(x)| = |(-1)^{mn}(m!)^n * a_0 + nA + nB|$, $\exists n : n > |a_0|, n > n_0, (n, m!) = 1 \Longrightarrow |(-1)^{mn}(m!)^n * a_0 + nA + nB| \neq 0 \Longrightarrow |(-1)^{mn}(m!)^n * a_0 + nA + nB| \geqslant 1$

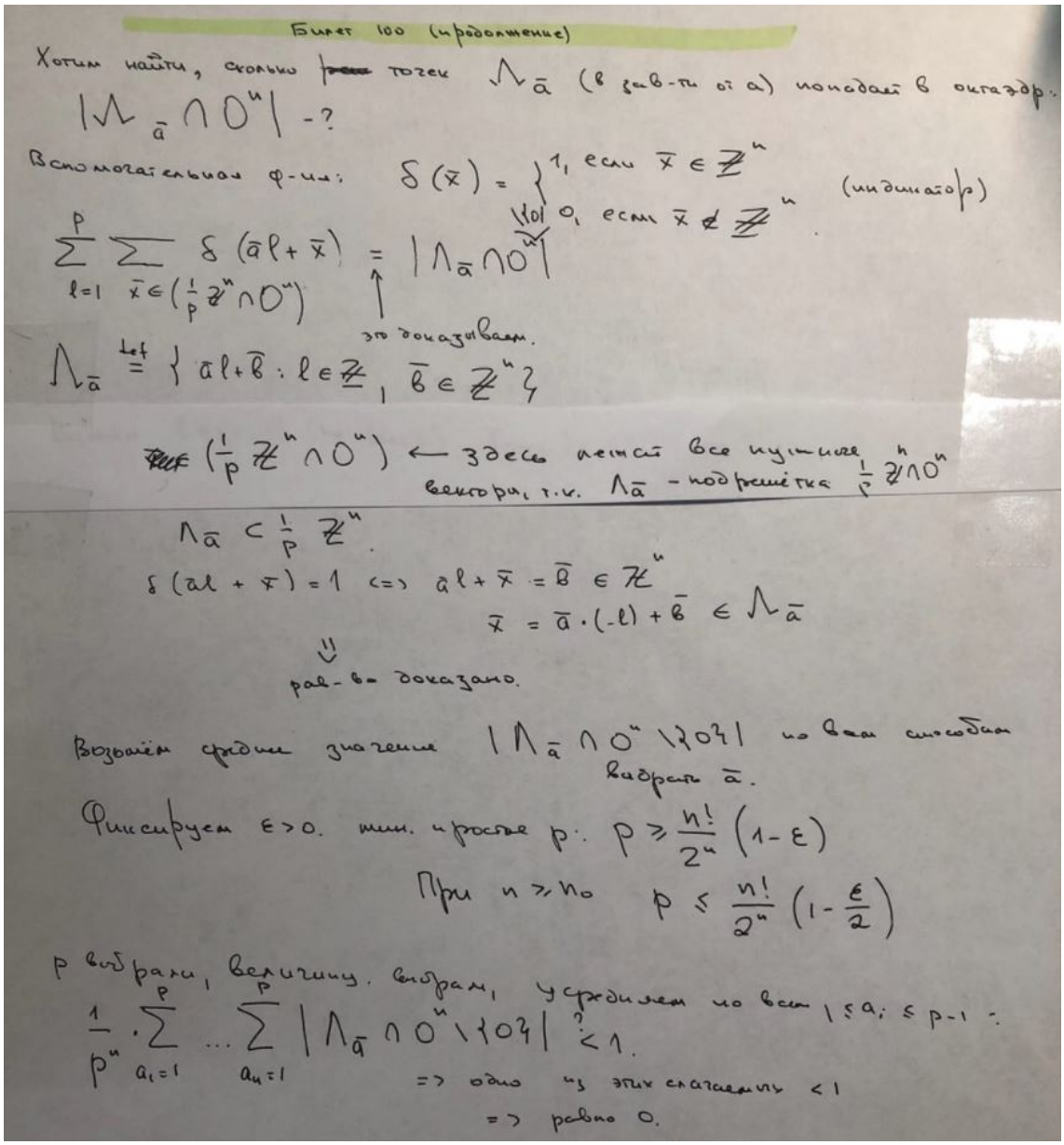
Таким образом, $\exists n : \forall N \geqslant n :$ Правая часть $\geqslant 1$, левая часть $< 1 \Longrightarrow$ равенство не может быть достигнуто. Противоречие $\Longrightarrow e-$ трансцендентно■

100 Доказательство теоремы Минковского-Главки для октаэдра: переформулировка условия теоремы через Λ_a и неравенства на p и n. Сведение теоремы к неравенству

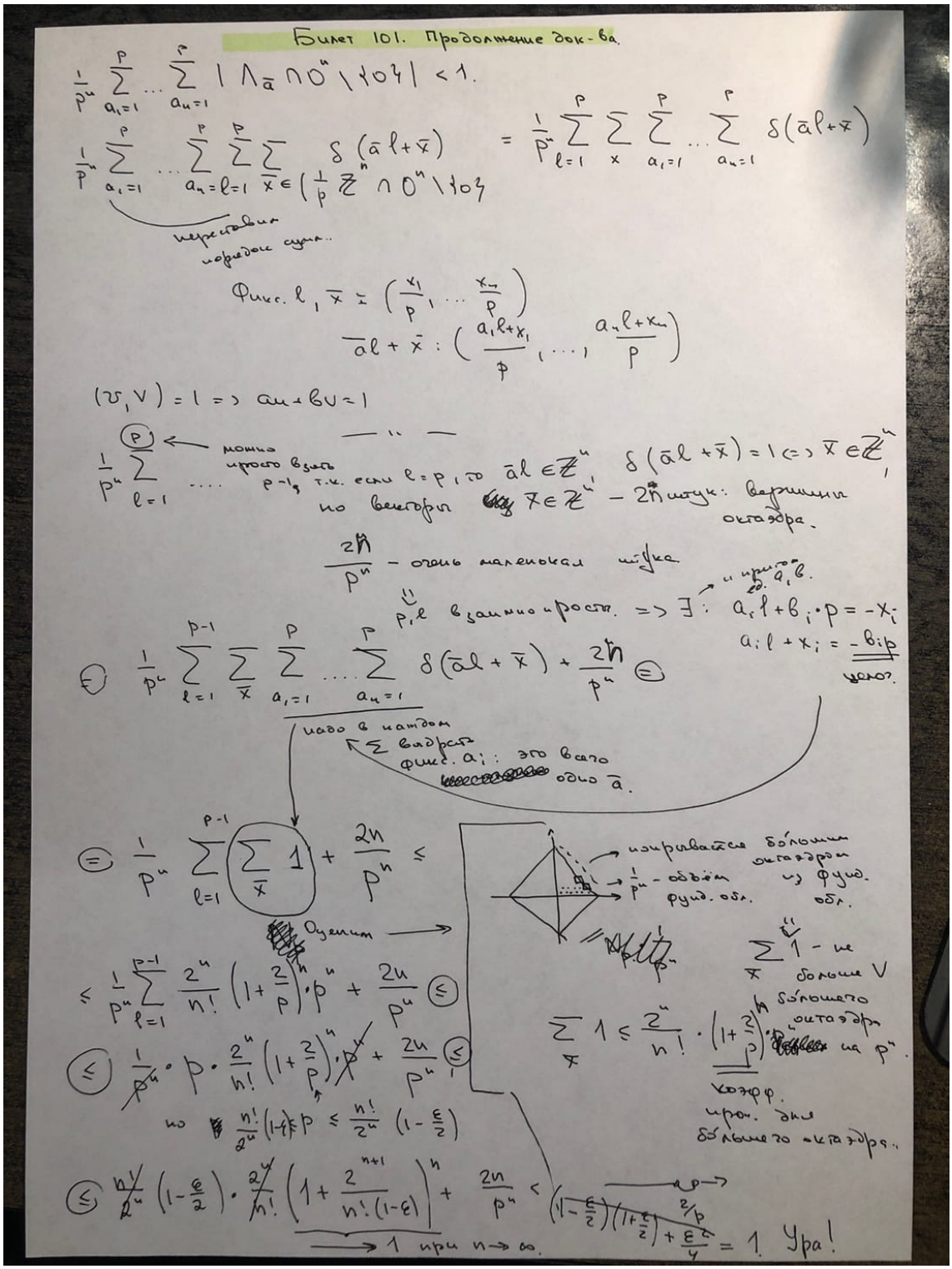
Теорема Минковского-Главки: $\frac{Vol\Omega}{\Delta(\Omega)} \geqslant 1$, где Ω - произвольное тело; мы работаем с ней для октаэдра, но не на классе ВСЕХ решёток (в критическом определителе у нас inf по всем решёткам), а переформулируем:
$\forall \varepsilon > 0 \exists n_0 \forall n \geqslant n_0 \exists \Lambda \subset \mathbb{R}^n : \Lambda \cap \Omega \backslash \{0\} = \varnothing$, а $\det \Lambda \leqslant (Vol\Omega)(1+\varepsilon)$
Рассмотрим $\overline{a} = (a_1/p, a_2/p, \ldots, a_n/p)$, p - простое число, $a_i \in \mathbb{Z}$. Берём $< \mathbb{Z}^n, \overline{a} > = \{\overline{a}l + \overline{b} : l \in \mathbb{Z}, \overline{b} \in \mathbb{Z}^n\}$. Тогда $\Lambda_{\overline{a}} = < \mathbb{Z}^n, \overline{a} >$- это вот эта решётка. Б.о.о. $1 \leqslant a_i \leqslant p-1$.

Утверждение: $\det \Lambda_{\overline{a}} = \frac{1}{p}$

Переформулировка условия теоремы Минковского-Главки $\forall \varepsilon > 0 \exists n_0 \forall n \geqslant n_0 \exists \Lambda_{\overline{a}} \subset \mathbb{R}^n : \Lambda_{\overline{a}} \cap O^n \backslash \{0\} = \varnothing$ ($\Lambda_{\overline{a}}$ допустима относительно O^n, а $\det \Lambda_{\overline{a}} = \frac{1}{p} \leqslant (VolO^n)(1+\varepsilon) = \frac{2^n}{n!}(1+\varepsilon)$, что, по сути, $p \geqslant \frac{n!}{2^n}(1-\varepsilon)$


Билет 100 (продолжение)
Хотим найти, сколько точек $\Lambda_{\bar a}$ (в зав-ти от $\bar a$) попадает в октаэдр:
$|\Lambda_{\bar a} \cap O^n| - ?$
Вспомогательная ф-ия: $\delta(\bar x) = \begin{cases} 1, & \text{если } \bar x \in \mathbb{Z}^n \\ 0, & \text{если } \bar x \notin \mathbb{Z}^n \end{cases}$ (индикатор)
$\sum_{l=1}^{p} \sum_{\bar x \in (\frac{1}{p}\mathbb{Z}^n \cap O^n)} \delta(\bar a l + \bar x) = |\Lambda_{\bar a} \cap O^n|$
это доказываем.
$\Lambda_{\bar a} \overset{\text{def}}{=} \{ \bar a l + \bar b : l \in \mathbb{Z},\ \bar b \in \mathbb{Z}^n \}$
$(\frac{1}{p}\mathbb{Z}^n \cap O^n)$ ← здесь лежат все нужные нам векторы, т.к. $\Lambda_{\bar a}$ - подрешётка $\frac{1}{p}\mathbb{Z}^n$
$\Lambda_{\bar a} \subset \frac{1}{p}\mathbb{Z}^n$.
$\delta(\bar a l + \bar x) = 1 \iff \bar a l + \bar x = \bar b \in \mathbb{Z}^n$
$\bar x = \bar a \cdot (-l) + \bar b \in \Lambda_{\bar a}$
раз-ть доказано.
Возьмём среднее значение $|\Lambda_{\bar a} \cap O^n \setminus \{0\}|$ по всем способам выбрать $\bar a$.
Фиксируем $\varepsilon > 0$. Тогда простое p: $p \geqslant \frac{n!}{2^n}(1-\varepsilon)$
При $n \geqslant n_0$ $p \leqslant \frac{n!}{2^n}(1-\frac{\varepsilon}{2})$
p выбрали, величину выбрали, усредняем по всем $1 \leq a_i \leq p-1$:
$\frac{1}{p^n} \cdot \sum_{a_1=1}^{p} \dots \sum_{a_n=1}^{p} |\Lambda_{\bar a} \cap O^n \setminus \{0\}| \overset{?}{<} 1$.
$\Rightarrow$ одно из этих слагаемых < 1
$\Rightarrow$ равно 0.

101 Теорема Минковского-Главки для октаэдра (формулировка). Доказательство неравенства.



103 Алгоритм AKS. Верхняя оценка на r: вывод из утверждения о нижней оценке $[1, 2, \ldots, n]$.

Лемма: $r \leqslant \max\{3, \lceil \log_2^5 n \rceil\}$

▲ Пусть $n \geqslant 3 \Rightarrow B = \lceil \log_2^5 n \rceil \geqslant 10 > 7 \Rightarrow$ можем применять оценку на $[1, \ldots, B]$ из билета 80, то есть $[1, \ldots, B] \geqslant 2^B$

Рассмотрим

$$S = n^{[\log_2 B]} \prod_{i=1}^{\left[\log_2^2 n\right]} (n^i - 1)$$

Возьмем минимальное r, такое что r не делит $S \Rightarrow n^i \not\equiv 1 \pmod r$ $i = 1, \ldots, [\log_2^2 n] \Rightarrow$ если $(r,n) = 1$, то $\operatorname{ord}_r n > \log_2^2 n$.

Осталось доказать, что $(r,n) = 1$ и $r \leqslant B$. Воспользуемся тем, что $n^i - 1 < n^i$ и просуммируем степени по арифметической прогрессии.

$$S < n^{[\log_2 B]} \cdot n^{\frac{\left[\log_2^2 n\right]\left(\left[\log_2^2 n\right]+1\right)}{2}} \leqslant n^{\log_2^4 n} = 2^{\log_2^5 n} \leqslant 2^B$$

Во втором неравенстве мы прибавили $\frac{\log_2^4 n}{2}$ и отняли $[\log_2 B] = [\log_2 \log_2^5 n]$. Очевидно, что второе является двойным логарифмом и оно меньше первого.

Предположим, что $r > B$. Тогда по определению r S делится на все числа меньшие r, то есть $S \geqslant [1, \ldots, B] \geqslant 2^B$ - противоречие $\Rightarrow r \leqslant B$

Пусть $r = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} \Rightarrow k_i \leqslant \log_2 B$, так как $r \leqslant B$. Предположим, что $\forall i \; n \vdots p_i$. Тогда $\forall i \; n^{[\log_2 B]} \vdots p_i^{[\log_2 B]} \vdots p_i^{k_i}$ (так как $k_i \leqslant \log_2 B$) $\Rightarrow n^{[\log_2 B]} \vdots r$ - противоречие, так как тогда $S \vdots r$. Следовательно, $\exists p_i \nmid n$. Перенумеруем p так что $p_1, \ldots, p_t$ не делят n, $p_{t+1}, \ldots, p_s$ делят n. Тогда $p_1^{k_1} \cdot \ldots \cdot p_t^{k_t} \nmid \prod_{i=1}^{\left[\log_2^2 n\right]} (n^i - 1)$, так как иначе r делит S.

Рассмотрим

$$\frac{r}{(r,n)} = \underbrace{p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}}_{\text{не делит } S} \cdot \underbrace{p_{t+1}^{k'_{t+1}} \cdot \ldots \cdot p_s^{k'_s}}_{\text{делит } S} \Rightarrow \frac{r}{(r,n)} \nmid S$$

Из того, что r выбиралось минимальным следует, что $(r,n) = 1$. Следовательно $\operatorname{ord}_r n > \log_2^2 n$ и все доказано ■

104 Алгоритм AKS. Определение и неравенства, связывающие параметры $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| > C_{t+l}^{t-1}$.

Неравенства: $p > r > \log_2^2 n$, $\varphi(r) \geqslant |G| = t > \log_2^2 n$, $\deg h(x) > \operatorname{ord}_r p > 1$

Утверждение (б/д): У многочлена степени k над любым полем $\leqslant k$ корней в поле.

Лемма 1: $|\mathcal{G}| \geqslant C_{t+l}^{t-1}$

▲ Докажем, что если $f(x), g(x)$ - многочлены из P (см. билет 83) степени $\leqslant t-1$, то они не совпадают в $\mathcal{G}$. Пусть $m \in G$

$$f(x^m) = (f(x))^m \pmod{x^r - 1, p}$$

$$f(x^m) = (f(x))^m \pmod{h(x), p} \text{ (перешли к делителю)}$$

$$g(x^m) = (g(x))^m \pmod{h(x), p}$$

Предположим $f = g \pmod{h(x), p}$. Тогда $f(x^m) = g(x^m) \pmod{h(x), p}$. Рассмотрим многочлен $f - g$. $\deg(f - g) \leqslant t - 1$, а количество корней равно $|G| = t$ (так как подходят все x^m) - противоречие $\Rightarrow$ f и g различны в $\mathcal{G}$

Рассмотрим в множестве P многочлены $x, x + 1, \ldots, x + l$ - не равны по модулю $h(x)$, так как $\deg h(x) > 1$. Покажем, что они не совпадают и по модулю p. Так как $\log_2^2 n \leqslant r \Rightarrow \log_2 n \leqslant \sqrt{r}$

$$l = \sqrt{\varphi(r)} \log_2 n < \sqrt{r} \log_2 n \leqslant r \leqslant p$$

Найдем количество многочленов из P степени $\leqslant t - 1$ (они все точно различные в $\mathcal{G}$ по доказанному выше). Выбираем из нашего списка многочленов степени 1 $t - 1$ штуку с повторениями. Получаем

$$\overline{C}_{l+1}^{t-1} = C_{t+l}^{t-1}$$

Так как все эти многочлены лежат в $\mathcal{G} \Rightarrow |\mathcal{G}| \geqslant C_{t+l}^{t-1}$ ■

105 Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы G, $\mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $|\mathcal{G}| \leqslant n^{\sqrt{t}}$ при $n \neq p^k$.

Неравенства: $p > r > \log_2^2 n$, $\varphi(r) \geqslant |G| = t > \log_2^2 n$, $\deg h(x) > \operatorname{ord}_r p > 1$

Лемма 2: $|\mathcal{G}| \leqslant n^{\sqrt{t}}$ при $n \neq p^k$

▲ Рассмотрим в множестве I все элементы с $0 \leqslant i, j \leqslant [\sqrt{t}]$. Всего таких чисел $([\sqrt{t}] + 1)^2 > t$ чисел $\Rightarrow$ среди них $\exists m_1, m_2$ $(m_1 > m_2)$, такие что $m_1 \equiv m_2 \pmod{r}$ (так как в группе G всего t различных элементов). Тогда

$x^{m_1} = x^{m_2} \pmod{x^r - 1, p}$, так как $(x^{m_1 - m_2} - 1)x^{m_2} \vdots x^r - 1$ (см. замечание в билете 84)

Рассмотрим произвольное $f \in \mathcal{G}$. По построению $\mathcal{G}$ он перестановочен с m_1 и m_2. Следовательно, так как $h(x) \mid x^r - 1$

$$(f(x))^{m_1} = f(x^{m_1}) = f(x^{m_2}) = (f(x))^{m_2} \pmod{h(x), p}$$

Уравнение $(f(x))^{m_1} = (f(x))^{m_2}$ имеет $\leqslant \max\{m_1, m_2\} = m_1$ корней (уравнение относительно $f(x)$). Так как это выполнено для любого $f \in \mathcal{G}$, то $|\mathcal{G}| \leqslant m_1$.

По построению $m_1 = \left(\frac{n}{p}\right)^i \cdot p^j$, $0 \leqslant i, j \leqslant [\sqrt{t}] \Rightarrow |\mathcal{G}| \leqslant m_1 \leqslant n^{\sqrt{t}}$ ■

106 Алгоритм AKS. Определение и неравенства, связывающие $p, r, \log_2 n, t$, группы $G, \mathcal{G}$, многочлена $h(x)$ (б/д). Неравенство $C_{t+l}^{t-1} > n^{\sqrt{t}}$.

Неравенства: $p > r > \log_2^2 n$, $\varphi(r) \geqslant |G| = t > \log_2^2 n$, $\deg h(x) > \operatorname{ord}_r p > 1$

Утверждение 1:

1. Если $a > b$, то $C_a^k > C_b^k \; \forall k$
2. Если $\frac{n}{2} > a > b$, то $C_n^a > C_n^b$

▲ 1. В переходе с неравенством добавляем $b-a<0$ к каждому множителю

$$C_a^k=\frac{a!}{k!\,(a-k)!}=\frac{(a-k+1)\cdot\ldots\cdot a}{k!}>\frac{(b-k+1)\cdot\ldots\cdot b}{k!}=\frac{b!}{k!\,(b-k)!}=C_b^k$$

2. В переходе с неравенством добавляем $a-b>0$ к каждому множителю

$$C_n^a=\frac{n!}{a!\,(n-a)!}=\frac{n!}{a!\,b!\,(b+1)\cdot\ldots\cdot(n-a)}>\frac{n!}{a!\,b!\,(a+1)\cdot\ldots\cdot(n-b)}=\frac{n!}{b!\,(n-b)!}$$

Утверждение 2: $C_{2x+1}^x\geqslant 2^{x+1}$

▲ 1. База: $x=2$ (при $x=1$ неверно, но нам важно на больших) $C_5^2=10\geqslant 2^3=8$

2. Переход: пусть верно для x. Докажем для $x+1$

$$C_{2x+3}^{x+1}=\frac{(2x+3)!}{(x+1)!\,(x+2)!}=\frac{(2x+1)!\,(2x+2)(2x+3)}{(x+1)!\,x!\,(x+1)(x+2)}=C_{2x+1}^x\cdot\frac{(2x+2)(2x+3)}{(x+1)(x+2)}=$$

$$=2C_{2x+1}^x\frac{2x+3}{x+2}>2C_{2x+1}^x\geqslant 2^{x+2}\ \blacksquare$$

Лемма 3: $C_{t+l}^{t-1}>n^{\sqrt{t}}$

▲ Так как $t>\log_2^2 n\Rightarrow t>\sqrt{t}\log_2 n\Rightarrow t\geqslant[\sqrt{t}\log_2 n]+1$. $l=\sqrt{\varphi(r)}\log_2 n\geqslant\sqrt{t}\log_2 n$.

$$C_{t+l}^{t-1}\geqslant C_{[\sqrt{t}\log_2 n]+1+l}^{[\sqrt{t}\log_2 n]}\geqslant C_{2[\sqrt{t}\log_2 n]+1}^{[\sqrt{t}\log_2 n]}\geqslant 2^{[\sqrt{t}\log_2 n]+1}>2^{\sqrt{t}\log_2 n}=n^{\sqrt{t}}\ \blacksquare$$

Так как верны все леммы 1-3 из билетов 104-106, то $n=p^k$, но если $k>1$, то мы бы остановились еще на шаге 1 нашего алгоритма $\Rightarrow n=p\Rightarrow$ последний шаг алгоритма корректен