Билеты по курсу

«Основы комбинаторики и теории чисел»

2 семестр ФПМИ МФТИ

Артур Кулапин

Андрей Баженов

Весна 2020

Содержание

Вопросы на оценку «Уд»

Билет 1

Простые числа

Def. Число $n \in \mathbb{N}$ — простое, если у него есть только два различных делителя: единица и оно само.

Основная теорема арифметики (формулировка, существование)

Def. Каноническим разложением натурального числа n называют его разложение на множители в виде $n = p_1^{d_1} \cdot \ldots \cdot p_k^{d_k}$, где $p_1 < p_2 < \ldots < p_k$ — простые числа, а $d_1, \ldots, d_k$ — натуральные.

Th. $\forall n \in \mathbb{N} \setminus \{1\}$ верно, что существует и единственно его каноническое разложение.

Доказательство: Докажем только существование такого разложения. Действуем по индукции:

1. База. Для двойки разложение тривиально: $2 = 2^1$.
2. Переход. Пусть $\forall k \in \mathbb{N} \ : k < n$ разложение существует. Если n простое, то разложение тривиально. Иначе оно составное, то есть $\exists a, b \in \mathbb{N} \ : 1 < a, b < n$ такие, что $n = a \cdot b$. Но для них уже все доказано, а значит разложение существует.

■

Билеты 2 и 3

Основы теории делимости: НОД и НОК

Def. НОД двух натуральных чисел m, n — такое наибольшее натуральное число g такое, что m и n делятся на g без остатка.

Def. НОК двух натуральных чисел m, n — такое наименьшее натуральное число l такое, что l делится на m и на n без остатка.

Алгоритм Евклида

Th. Алгоритм Евклида остановится, а последний ненулевой член — искомый НОД, при этом НОД представим в виде линейной целочисленной комбинации своих аргументов. В данной теореме рассматривается $gcd(a, b)$.

Доказательство:

1. Заметим, что последовательность $\{r_i\}_{i=1}^{n}$ монотонно убывает. Строится она так: $a = (bq_0 + r_1)$, $b = (r_1q_1 + r_2)$, $\ldots$, $r_{k-2} = (r_{k-1}q_{k-1} + r_k)$, $\ldots$, $r_{n-2} = (r_{n-1}q_{n-1} + r_n)$, $r_{n-1} = (r_nq_n)$. Тогда в силу того, что $r_k < r_{k-1}$, $\{r_i\}_{i=1}^{n}$ убывает, но у нее, очевидно, есть конец. Поэтому алгоритм остановится.

2. Совершили спуск по (интеллектуальной лестнице) последовательности, теперь подъем. Так как $r_{n-2} = r_{n-1}q_{n-1}+r_n = r_n(1+q_nq_{n-1})$, по индукции можно показать, что r_k делится на r_n, а значит и r_1, r_2 делятся на r_n, отсюда непременно следует, что a и b делятся на r_n.

3. Опять спускаемся по (уже социальной лестнице) последовательности r_n. Заметим, что $a = bq_0+r_1 \Longrightarrow r_1 = a-bq_0$, $r_2 = b-r_1q_1 = b(1+q_0q_1)-aq_1$, при этом множители при коэффициентах из $\mathbb{N}$. Тогда по индукции (база есть): пусть r_{k-2}, r_{k-1} выразимы в виде $ax + by : x, y \in \mathbb{Z}$. $r_k = r_{k-2} - r_{r-1}q_{k-1} = ax + by : x, y \in \mathbb{Z}$. Тогда получим, что $\exists x, y \in \mathbb{Z} : r_n = ax + by$.

4. Докажем, что если $a = bq + r$, то $gcd(a, b) = gcd(b, r)$.

   Доказательство: Пусть k — общий делитель (любой) a, b. Такой есть хотя бы в силу существования обратимых элементов. Тогда $a = t_1k, b = t_2k$ Тогда $r = a - bq = k(t_1 - qt_2)$, а значит и r делится на k. Обратное тоже верно, а значит все общие делители совпадут у пар (a, b) и (b, r). А значит и $gcd(a, b) = gcd(b, r)$.

   Из этого путем очередного спуска по (карьерной лестнице) последовательности получим, что $gcd(a, b) = gcd(0, r_n) = r_n$, так как 0 делится на любое натуральное.

■

Билет 4

Лемма Евклида

Лемма. Если простое число p делит без остатка произведение двух целых чисел $x \cdot y$, то p делит x или y.

Доказательство: Обойдемся без основной теоремы арифметики.

Воспользуемся леммой Безу: если $a, b \in \mathbb{N}$, то $\exists x, y \in \mathbb{Z} : gcd(a, b) = ax+by$. Ее мы доказали в билете выше с помощью алгоритма Евклида, который доказывается без основной теоремы арифметики.

Пусть x не делится на p, тогда по лемме Безу найдутся такие $u, v \in \mathbb{N} : ux+vp = 1 \Longrightarrow (xy)u+y(pv) = y$. Тогда, так как xy делится на p, значит левая часть делится на p, то есть и y делится на p.

■

Билет 5

Единственность в ОТА

Th. $\forall n \in \mathbb{N} \setminus \{1\}$ верно, что существует и единственно его каноническое разложение.

Доказательство: Сущещствование уже было показано. Теперь докажем единственность с помощью леммы Евклида. Пусть для n существуют два различных разложения на простые множители:

$$n = p_1 \cdot \ldots \cdot p_k = p_1^{'} \cdot \ldots \cdot p_l^{'}$$

Так как $p_1^{'} \cdot \ldots \cdot p_l^{'}$ делится на p_1, то либо $p_1^{'}$ делится на p_1, либо $p_2^{'} \cdot \ldots \cdot p_l^{'}$ делится на p_1. В первом случае $p_1 = p_1^{'}$, либо продолжим предыдущие рассуждения, пока не найдем число, равное p_1. Продолжая это рассуждение, получим, что все числа совпадут с точностью до перестановки, то есть каноничное разложение единственно.

■

Билет 6

Теория сравнений

Def. Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}_+$. $a \equiv b \mod m \iff a - b$ делится без остатка на m.

Def. Вычетом по модулю m называется произвольный представитель класса эквивалентности «сравнимость по модулю».

Системы вычетов

Def. Полная система вычетов — произвольный набор из m всевозможных вычетов.

Def. Приведенная система вычетов — множество обратимых элементов из полной системы вычетов по модулю m.

Def. В системе вычетов по модулю m (обозначение $\mathbb{Z}_m$) арифметические операции определены так:

1. $a + b = (a + b) \mod m$
2. $a \cdot b = (a \cdot b) \mod m$

Обратимые элементы и делители нуля

Def. Элемент a называется обратимым, если для него $\exists a^{-1} : a \cdot a^{-1} = 1 \mod m$.

Def. Элемент a называется делителем нуля, если $\exists b : a \cdot b = 0 \mod m$

Утверждение. В Z_m каждый элемент либо обратим, либо является делителем нуля.

Доказательство: Если a не взаимно просто с m, то оно является делителем нуля. Это верно, так как тогда $m = a \cdot b \equiv 0 \mod m$. Если же a и m взаимно просты, то по малой теореме Ферма $a^{\varphi(m)} \equiv 1 \mod m$, то есть $a^{-1} = a^{\varphi(m)-1}$, где φ — функция Эйлера.

■

Следствие Если p простое, то $\mathbb{Z}_p$ не содержит делителей нуля кроме самого нуля (то есть является полем).

Билет 7

Малая теорема Ферма

Лемма. Если $gcd(a, p) = 1$, то $\{a, 2a, \ldots, (p-1)a\}$ — приведенная система вычетов.

Доказательство: Пусть это не так, то есть $\exists x \not\equiv y \mod p : ax \equiv ay \mod p$. Тогда $a(x-y) \equiv 0 \mod p \Longrightarrow (x-y) \equiv 0 \mod p \Longrightarrow x \equiv y \mod p$. Противоречие.

■

Th. Если p — простое и a — целое, не делящееся на p, то $a^p \equiv a \mod p$.

Доказательство: Заметим, что $gcd(a, p) = 1$. Рассмотрим полную систему вычетов по модулю p. По лемме выше $1 \cdot 2 \cdot \ldots \cdot p-1 \equiv a \cdot 2a \cdot \ldots \cdot a(p-1) \Longrightarrow a^{p-1} \equiv 1 \mod p$.

■

Билет 8

Теорема Эйлера

Def. Функция Эйлера $\varphi(m)$ равна количеству натуральных чисел, меньших m и взаимно простых с ним.

Th. $\forall a, m : gcd(a, m) = 1$ верно, что $a^{\varphi(m)} \equiv 1 \mod m$.

Доказательство: Рассмотрим произвольную приведенную систему вычетов по модулю m, $x_1, \ldots, x_{\varphi(m)}$. Эта система будет приведенной, так как $\varphi(m) < m$. Заметим, что тогда и $ax_1, \ldots ax_{\varphi(m)}$ тоже приведенная система вычетов по модулю m, так как $gcd(a, m) = 1$. Тогда

$$x_1 \cdot \ldots \cdot x_{\varphi(m)} \equiv ax_1 \cdot \ldots \cdot ax_{\varphi(m)} \mod m \Longrightarrow a^{\varphi(m)} \equiv 1 \mod m$$

■

Билет 9

Теорема Лагранжа о числе корней многочлена по простому модулю (б/д)

Th. Пусть $P(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \mod p$, где p — простое, а $a_i \in \mathbb{Z}$. Тогда если $\exists\ n+1$ различных корней по модулю p, то $\forall i\ a_i \equiv 0 \mod p$. То есть не более n несравнимых корней.

Теорема Вильсона (с использованием теоремы Лагранжа)

Th. $p \in \mathbb{N} : p > 1$ — простое $\iff (p-1)! \equiv -1 \mod p$.

Доказательство:

$\Longrightarrow$

Рассмотрим многочлены $f(x) = (x-1) \cdot \ldots \cdot (x-(p-1))$ и $g(x) = x^{p-1} - 1$. Корни обоих многочленов $1, 2, \ldots, p-1$, для $g(x)$ это вытекает из малой теоремы Ферма. Заметим также, что при x^{p-1} коэффициенты $f(x)$ и $g(x)$ равны единице. Тогда $h(x) = f(x) - g(x)$ имеет те же $p-1$ корней, но его степень равна $p-2$. Откуда по теореме Лагранжа для многочленов получим, что $h(x) \equiv 0 \Longrightarrow f(0) = g(0) \Longrightarrow (p-1)! \equiv -1 \mod p$.

$\Longleftarrow$

Пусть p — составное и $p \neq 4$, тогда $(p-1)! \equiv 0 \mod p$, а при $p = 4$ получим, что $(4-1)! \equiv 2 \mod 4$.

■

Билет 10

Теорема Вильсона через первообразные корни

Def. Первообразным корнем по модулю m называют такое число g, что $g^{\varphi(m)} \equiv 1 \mod m$ и при этом для него верно, что $\forall k \in [1, \varphi(m))$ верно, что $g^k \not\equiv 1 \mod m$.

Утверждение. Для любого простого p существует первообразный корень.

Th. $p \in \mathbb{N} : p > 1$ — простое $\iff (p-1)! \equiv -1 \mod p$.

Доказательство:

$\Longrightarrow$

Пусть g — первообразный корень по модулю p. Тогда $1, g, g^2, \ldots, g^{p-2}$ образуют полную систему вычетов без нуля по модулю p. То есть

$$(p-1)! \equiv 1 \cdot g \cdot g^2 \cdot \ldots \cdot g^{p-2} = g^{\frac{(p-2)(p-1)}{2}} \mod p$$

Теперь пусть p нечетное, тогда $p = 2k+1$. Тогда $k < p$ и $g^k \not\equiv 1 \mod p$, но $g^{2k} = g^{p-1} \equiv 1$ по малой

теореме Ферма. Тогда $g^k \equiv \pm 1 \mod p \Longrightarrow g^k \equiv -1 \mod p$. Из этого следует, что:

$$(p-1)! \equiv g^{\frac{(p-2)(p-1)}{2}} = \left(g^k\right)^{2k-1} \mod p \equiv (-1)^{2k-1} \equiv -1 \mod p$$

$\Longleftarrow$

Пусть p — составное и $p \neq 4$, тогда $(p-1)! \equiv 0 \mod p$, а при $p = 4$ получим, что $(4-1)! \equiv 2 \mod 4$.

■

Билет 11

Бесконечность простых вида $3k+2, 4k \pm 1$

Пусть $p_1, \ldots, p_n$ — простые, тогда число $p_1 \cdot \ldots \cdot p_n \pm 1$ не делится ни на какое из p_i.

Лемма. Если n^2+1 делится на нечетное простое p, то $p = 4k+1$.

Доказательство: Заметим, что тогда n взаимно просто с p, откуда по малой теореме Ферма:

$$1 \equiv n^{p-1} \equiv \left(n^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \mod p \Longrightarrow \frac{p-1}{2} \equiv 0 \mod 2$$

■

Утверждение. Существует бесконечно много простых чисел вида $3k+2, 4k \pm 1$.

Доказательство:

Рассмотрим простые вида $3k+2$. Предположим противное, то есть то, что их лишь конечное количество $p_1, \ldots, p_n$. Рассмотрим число $A = 3p_1 \cdot \ldots \cdot p_n + 2$. Оно дает остаток 2 при делении на три, при этом все его простые делители, среди которых есть делитель вида $3k+2$, отличны от $p_1, \ldots, p_n$. Противоречие.

Рассмотрим простые вида $4k+1$. Предположим противное, то есть то, что их лишь конечное количество $p_1, \ldots, p_n$. Рассмотрим число $A = (2 \cdot p_1 \cdot \ldots \cdot p_n)^2 + 1$. Оно нечетное, а значит делится на нечетное простое, а по лемме оно имеет вид $4k+1$, но оно отлично от $p_1, \ldots, p_n$. Противоречие.

Рассмотрим простые вида $4k+3$. Предположим противное, то есть то, что их лишь конечное количество $p_1 = 3, p_2 = 7, \ldots, p_n$. Рассмотрим число $A = 4p_1 \cdot \ldots \cdot p_n + 3$. Оно не делится ни на какое p_i, при этом содержит делитель вида $4k+3$.

■

Билет 12

Сравнения второй степени. Квадратичные вычеты и невычеты

Def. $ax^2 + bx + c \equiv 0 \mod m$ — сравнение второго порядка.

Def. Пусть p — нечетное простое число. Тогда если $gcd(a, p) = 1$ и $\exists x : x^2 \equiv a \mod p$, то a — квадратичный вычет, иначе — невычет.

Число вычетов и невычетов по нечетному простому модулю

Утверждение. Пусть p — нечетное простое число. Тогда число вычетов и невычетов равно $\frac{p-1}{2}$.

Доказательство: Так как $x^2 \equiv (p-x)^2$, то достаточно показать, что вычеты $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ различны. Предположим, что $\exists x, y \in \left(0, \frac{p}{2}\right) : x^2 \equiv y^2 \mod p$. Тогда $(x-y)\cdot(x+y) \equiv 0 \mod p$. Заметим, что $0 < |x-y| < p \Longrightarrow (x+y) \equiv 0 \mod p$, но $(x+y) < p$. Противоречие.

■

Билет 13

Сравнения второй степени. Квадратичные вычеты и невычеты

Def. $ax^2 + bx + c \equiv 0 \mod m$ — сравнение второго порядка.

Def. Пусть p — нечетное простое число. Тогда если $gcd(a, p) = 1$ и $\exists x : x^2 \equiv a \mod p$, то a — квадратичный вычет, иначе — невычет.

Символ Лежандра

Def. Символом Лежанадра называют

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

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

Доказательство: Если $gcd(a, p) \neq 1$, то тривиально. Теперь $gcd(a, p) = 1$. Тогда по малой теореме Ферма $a^{p-1} \equiv 1 \mod p \Longrightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p$. Оба множителя не могут одновременно делиться на p, так как иначе делилась бы и их разность.

Пусть a — вычет, тогда $\exists x : a \equiv x^2 \mod p \Longrightarrow a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p$, по МТФ и так как $x < p$. А если a — невычет, то $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

Следствие Символ Лежандра мультипликативен.

Билет 15

Матрицы Адамара. Нормальная форма

Def. Матрица Адамара — матрица размера $n \times n$ из $-1, 1$, в которой все строки попарно ортогональны.

Очевидно, можно домножить строки на ± 1, чтобы в первом столбце стояли только единицы. Аналогично поступим со столбцами, чтобы в первой строке были только единицы. Адамаровость не изменится при этом.

Def. Матрица Адамара в нормальной форме, если в первой строке и в первом столбце стоят только единицы.

Билет 16

Матрицы Адамара. Существование при $n = 1, 2$

Матрица Адамара размера 1: $(1), (-1)$. Матрица Адамара для $n = 2$: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Необходимость делимости n на 4 при $n > 3$

Утверждение. Для существования матрицы Адамара необходимо, чтобы $n \equiv 0 \mod 4$.

Доказательство: Приведем матрицу Адамара к нормальной форме. Рассмотрим строки с номерами $i, j > 1$. Заметим, что любая из них может быть приведена к виду $(1, 1, \ldots, 1, -1, \ldots, -1)$. Пусть x — число общих единиц друг под другом, тогда $\left(\frac{n}{2} - x\right)$. Заметим, что число общих -1 должно быть тоже равно x. Тогда скалярное произведение: $x + x - 2 \cdot \left(\frac{n}{2} - x\right) = 4x - n = 0 \Longrightarrow n \equiv 0 \mod 4$.

■

Гипотеза Адамара

Th. (Гипотеза о существовании) $\forall n \in \mathbb{N} : n = 4k$ существует матрица Адамара.

Билет 17

Построение матриц Адамара для степеней двойки

Пусть $n = 2^k$.

Пример: Пусть первая строка будет $(1, 1, \ldots, 1, 1)$, вторая будет $(1, \ldots, 1, -1, \ldots, -1, 1, \ldots, 1, -1, \ldots, -1)$ и так далее путем деления пополам. Тогда получим только k строк.

Как-то не везет нам сегодня. А попробуем сделать хитрее.

Th. Гипотеза Адамара верна для $n = 2^k$.

Доказательство: Пусть $A \in M_{n\times n}$; $B \in M_{m\times m}$. Тогда кронекеровским произведением A на B назовем матрицу

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \ddots & \ldots & \vdots \\ a_{n1}B & \cdots & \cdots & a_{nn}B \end{pmatrix} \in M_{nm\times nm}$$

Покажем, что если A и A' — матрицы Адамара, то и $B = A \otimes A'$ тоже. Действительно, найдем скалярное произведение первых двух строк матрицы B:

$$\begin{aligned} a_{11}a'_{11} \cdot a_1 1a'_{21} + a_{11}a'_{12} \cdot a_{11}a'_{22} + \ldots + a_{11}a'_{1m} \cdot a_{11}a'_{2m} + \ldots + a_{1n}a'_{11} \cdot a_{1n}a'_{21} + \ldots + a_{1n}a'_{1m} \cdot a_{1n}a'_{2m} = \\ = a'_{11}a'_{22}(a_{11}a_{11} + \ldots + a_{1n}a_{1n}) + \ldots + a'_{1m}a'_{2m}(a_{11}a_{11} + \ldots + a_{1n}a_{1n}) = \\ = n(a'_{11}a'_{21} + \ldots + a'_{1m}a'_{2m}) = 0 \end{aligned}$$

поскольку A' — матрица Адамара.

■

Билет 18

Показатель

Def. Показатель (порядок) числа по модулю m — минимальное натуральное $\delta : a^\delta \equiv 1 \mod m$.

Утверждение. $\varphi(m) \equiv 0 \mod \delta$.

Доказательство: Предположим, что это не так. Тогда $\varphi(m) = k\delta + r$, $r \in (0, \delta)$. Ну тогда $1 \equiv a^{\varphi(m)} = a^{k\delta+r} \equiv a^r \mod m \Longrightarrow r$ — показатель. Противоречие.

■

Первообразный корень (для $m \leq 8$)

Def. первообразный корень по модулю m — такое число, что его показатель равен $\varphi(m)$.

При $m = 8$ не существует первообразного корня, так как он существует только для $m \in \{2, 4, p^\alpha, 2p^\alpha\}$, где p — простое нечетное, $\alpha \in \mathbb{N}$.

Для $m \leq 7$ пары модуль-корень: $(2,1), (3,2), (4,3), (5,2), (6,5), (7,3)$.

Билет 19

Индексы

Утверждение. Пусть g — первообразный корень по модулю m. Тогда $g, g^2, \ldots, g^{m-1}$ образуют полную систему вычетов.

Def. Индекс — дискретный логарифм числа a по модулю m по основанию g.

Def. Таблица индексов — таблица, где каждому вычету сопоставлен его индекс.

Утверждение. Сравнение вида $x^n \equiv a \mod m$, $m = p^\alpha, 2p^\alpha$, $c = \varphi(m)$, $gcd(a, m) = 1$, $gcd(n, c) = d$ разрешимоттгда и только тогда, когда $ind(a)$ делится на d.

Пример: $x^8 \equiv 5 \mod 17$. $c = \varphi(17) = 16$, $d = gcd(16, 8) = 8$, $ind5 = 5$ и не делится на 8. Значит решений нет.

Пример: $x^4 \equiv 4 \mod 17$. $c = \varphi(17) = 16$, $d = gcd(16, 4) = 4$, $ind4 = 12$ и делится на 4. Значит есть 4 несравнимых решения. Решая сравнение $4ind(x) \equiv 12 \mod 16$, получим, что $ind(x) \in \{3, 7, 11, 15\}$ или $x \in \{10, 11, 7, 6\}$

Билет 20

Теорема Дирихле о диофантовых приближениях

Th. 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 $\forall Q \in \mathbb{N}$. Разобьем $[0, 1]$ на Q одинаковых частей. Рассмотрим числа $\{\alpha x\}$ — дробная часть, где $x \in \overline{0, \ldots, Q}$. Получилось $Q + 1$ число, а частей отрезка Q — по принципу Дирихле $\exists x_1, x_2 : |\{\alpha x_1\} - \{\alpha x_2\}| \leq \frac{1}{Q}$. А значит

$$|(\alpha x_1 - [\alpha x_1]) - (\alpha x_2 - [\alpha x_2])| \leq \frac{1}{Q} \Longrightarrow |\alpha(x_1 - x_2) - ([\alpha x_1] - [\alpha x_2])| \leq \frac{1}{Q} \Longrightarrow$$
$$\Longrightarrow |\alpha q - p| \leq \frac{1}{Q} \Longrightarrow \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} \xrightarrow{q=(x_1-x_2)\leq Q} \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

Теперь возьмем новое $Q_1 : \frac{1}{Q_1} < \left|\alpha - \frac{p}{q}\right|$. Найдем для него таким же образом p_1, q_1, для никх будет верно, что $\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{Q} < \left|\alpha - \frac{p}{q}\right|$, откуда следует, что $\frac{p_1}{q_1}$ и $\frac{p}{q}$ не совпадают.

■

Билет 21

Подходящие дроби

Def. Цепная дробь — число вида $a_0 + \frac{1}{a_1+\frac{1}{a_2+\dots}} := [a_0, a_1, \dots, a_n]$.

Def. Каноническая запись цепной дроби — запись, получаемая по индукции: $[a_0] = \frac{a_0}{1}, [a_0 : a_1, \dots, a_n] = a_0 + \frac{1}{[a_1,\dots,a_n]}$.

Def. Дробь $[a_0, \dots, a_k] = \frac{p_k}{q_k}$ — k-я подходящая дробь.

Рекуррентные соотношения для числителей и знаменателей

Th. Для числителей и знаменателей подходящих дробей верны следующие соотношения: $\begin{cases} p_k = a_k p_{k-1} + p_{k-2} \\ q_k = a_k q_{k-1} + q_{k-2} \end{cases}$

Доказательство: Индукция по k. База тривиально проверяется вручную, теперь переход:

$$[a_0, \dots, a_{k+1}] = \frac{p_{k+1}}{q_{k+1}}, [a_1, \dots, a_{k+1}] = \frac{p^*_{k+1}}{q^*_{k+1}} \Longrightarrow \frac{p_{k+1}}{q_{k+1}} = a_0 + \frac{q^*_{k+1}}{p^*_{k+1}} = \frac{a_0 p^*_{k+1} + q^*_{k+1}}{p^*_{k+1}} \Longrightarrow \begin{cases} p_{k+1} = a_0 p^*_{k+1} + q^*_{k+1} \\ q_{k+1} = p^*_{k+1} \end{cases}$$

Применяя предопложение индукции, $q_{k+1} = a_{k+1} p^*_k + p^*_{k-1} = a_{k+1} q_k + q_{k-1}$ и

$$p_{k+1} = a_0(a_{k+1} p^*_k + p^*_{k-1})_{a k+1} q^*_k + q^*_{k-1} = a_{k+1}(a_0 p^*_k + q^*_k) + (a_0 p^*_{k-1} + q^*_{k-1}) = a_{k+1} p_k + p_{k-1}$$

■

Билет 22

Конечные цепные дроби. Каноническая запись. Подходящие дроби

Def. Цепная дробь — число вида $a_0 + \frac{1}{a_1+\frac{1}{a_2+\dots}} := [a_0 : a_1, \dots, a_n]$.

Def. Каноническая запись цепной дроби — запись, получаемая по индукции: $[a_0] = \frac{a_0}{1}, [a_0 : a_1, \dots, a_n] = a_0 + \frac{1}{[a_1:\dots,a_n]}$.

Def. Дробь $[a_0, \dots, a_k] = \frac{p_k}{q_k}$ — k-я подходящая дробь.

Рекуррентные соотношения для числителей и знаменателей (б/д)

Th. Для числителей и знаменателей подходящих дробей верны следующие соотношения: $\begin{cases} p_k = a_k p_{k-1} + p_{k-2} \\ q_k = a_k q_{k-1} + q_{k-2} \end{cases}$

Следствия из рекуррентных соотношений

Проделаем следующую операцию с рекуррентными соотношениями: домножим первое на q_{k-1}, а второе на p_{k-1} и вычтем второе из первого:

$$p_k q_{k-1} - q_k p_{k-1} = p_{k-2} q_{k-1} - p_{k-1} q_{k-2} \ (1)$$

При $k = 1$: $p_1 q_0 - q_1 p_0 = 1$. Пусть $r_k = p_k q_{k-1} - q_k p_{k-1}$, $r_1 = 1$, тогда в силу (1) заметим, что $r_k = -r_{k-1}$. Откуда следует, что

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

Теперь разделим (2) на $q_k q_{k-1}$ и получим

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}} \ (3)$$

Утверждение. Подходящие дроби несократимы

Доказательство: Из (2) получаем, что $gcd(p_k, q_k) = 1$.

Утверждение. Четные подходящие дроби возрастают, а нечетные — убывают.

Доказательство: Проделаем следующую операцию с рекуррентными соотношениями: домножим первое на q_{k-2}, а второе на p_{k-2} и вычтем второе из первого:

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

Отсюда напрямую получаем, что

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}$$

Откуда следует необходимое утверждение.

■

Билет 23

Бесконечные цепные дроби

Def. Пусть $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$. Тогда бесконечная цепная дробь — выражение, чья каноничная запись имеет вид $[a_0 : a_1, \ldots, a_n, \ldots]$.

Def. Величиной бесконечной цепной дроби называют предел ее подходящих дробей, то есть $\lim\limits_{n\to\infty} \frac{p_n}{q_n}$.

Th. Для любой бесконечной дроби предел ее величины существует.

Доказательство: Зная, что четные дроби возрастают, но они ограничены сверху, у них есть предел. Аналогично для нечетных. Их рекуррентных соотношений $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_n - 1} = \frac{1}{q_{n-1} q_n} \to 0$, так как q_i возрастают (опять же из рекуррентных соотношений).

Билет 24

Бесконечные периодические цепные дроби

Def. Бесконечная цепная дробь является периодической, если ее зпись имеет вид: $[a_0 : a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_n}, \ldots]$, где $\overline{a_{k+1}, \ldots, a_n}$ — периодическая часть.

Th. α — квадратичная иррациональность $\iff$ соответствующая ей цепная дробь периодична.

Доказательство: только в одну сторону.

$\Longleftarrow$

$[a_0 : a_1, \ldots, a_k, \overline{a_{k+1}, \ldots, a_n}, \ldots]$. Пусть $x = \overline{a_{k+1}, \ldots, a_n}$, тогда $\frac{1}{a_n+x} + a_{n-1} = \frac{a_n a_{n-1}+xa_{n-1}+1}{a_n+x} = \frac{c_1x+c_2}{c_3x+c_4}$. Будем прибавлять числа из периода, тогда $x = \frac{d_1x+d_2}{d_3x+d_4}$. То есть x — решение квадратного уравнения, которое можно решить, найти x, а дальнейшие действия не отменяют того, что исходная дробь является квадратичной иррациональностью.

■

Пример: $\alpha = [1 : 1, 1, \ldots] \Longrightarrow \alpha = 1 + \frac{1}{\alpha} \Longrightarrow \alpha = \frac{1+\sqrt{5}}{2}$.

Пример: $\sqrt{11} = 3 + \sqrt{11} - 3 = 3 + \frac{1}{\frac{1}{\sqrt{11}-3}} = 3 + \frac{1}{3+\frac{1}{\sqrt{11}+3}} = \ldots = [3 : \overline{36}]$

Билет 25

Квадратичные иррациональности

Def. Квадратичная иррациональность — иррациональное число, являющееся корнем квадратного уравнения с целыми коэффициентами.

Множество $\mathbb{Z}(\sqrt{m})$

Def. Множество $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} | a, b \in \mathbb{Z}\}$

Сложение, умножение определяются тривиально. $\overline{a + b\sqrt{m}} = a - b\sqrt{m}$ — сопряжение.

Утверждение. Пусть $z_1, z_2 \in \mathbb{Z}[\sqrt{m}]$, тогда $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.

Доказательство: $\overline{z_1} \cdot \overline{z_2} = (a_1 - b_1\sqrt{m})(a_2 - b_2\sqrt{m}) = (a_1a_2 + b_1b_2m) - (a_1b_2 + a_2b_1)\sqrt{m} = \overline{(a_1a_2 + b_1b_2m) + (a_1b_2 + a_2b_1)\sqrt{m}} = \overline{(a_1 + b_1\sqrt{m})(a_2 + b_2\sqrt{m})} = \overline{z_1 z_2}$

Def. Норма $z \in \mathbb{Z}[m]$ $N(z) = z\overline{z}$.

Note. $N(z) = a^2 - mb^2 \in \mathbb{Z}$.

Note. $N(z_1z_2) = N(z_1)N(z_2)$. Проверяется руками.

Билет 26

Решения уравнения Пелля $a^2 - 2b^2 = \pm 1$

Заметим, что $\overline{z^n} = \overline{z \cdot z^{n-1}} = \overline{z}\overline{z^{n-1}} = \ldots = \overline{z}^n$

Утверждение. Доказать, что пара $(a, b) : a + b\sqrt{2} = (1 + \sqrt{2})^n$ является решением уравнения Пелля $a^2 - 2b^2 = 1$.

Доказательство: Заметим, что $a^2 - 2b^2 = (a - b\sqrt{2})(a + \sqrt{2})$. Если $a + b\sqrt{2} = (1 + \sqrt{2})^n$, то $a - b\sqrt{2} = \overline{(1 + \sqrt{2})^n} = (1 - \sqrt{2})^n$.

Тогда для пар вида из условия $a^2 - 2b^2 = (a - b\sqrt{2})(a + \sqrt{2}) = (1 + \sqrt{2})^n \cdot (1 - \sqrt{2})^n = (-1)^n = \pm 1$.

■

Билет 27

Связь чисел с нормой 1 из $\mathbb{Z}(\sqrt{2})$ **и решением уравненя Пелля** $a^2 - 2b^2 = \pm 1$

$N(a^2 - 2b^2) = N(a - b\sqrt{2})N(a + b\sqrt{2}) = N(\pm 1) = 1 \Longrightarrow N(a \pm b\sqrt{2}) = \pm 1$, так как норма целая. То есть решение уравнения обязательно имеет единичную норму. Более того, любое число, имеющее единичную норму, является решением уравнения, так как по сути перед нами уравнение $N(a+b\sqrt{2}) = \pm 1$.

Билет 28

Равномерно распределенные последовательности по модулю 1

Def. Последовательность x_n равномерно распределена по модулю 1, если $\forall \gamma \in [0, 1]$ $\lim\limits_{N\to\infty} \frac{|k|k \le N, \{x_k\} \le \gamma|}{N} \to \gamma$, где $\{x\}$ — дробная часть.

$\sqrt{n}$ как пример равномерно распределенной последовательности по модулю 1

Зафиксируем N. Тогда $[x_n] = k \in \{1, 2, \ldots, [\sqrt{N}]\}$.

$$\{\sqrt{n}\} \le \gamma \Longrightarrow \{\sqrt{n}\} \in [k, k + \gamma] \Longrightarrow n \in [k^2, k^2 + 2k\gamma + \gamma^2]$$

То есть для данного k число таких n составляет $2k\gamma + O(1)$. Откуда для N число таких будет суммой $\sum\limits_{k=1}^{[\sqrt{N}]} (2k\gamma + O(1)) = O(\sqrt{N}) + 2\gamma \cdot \frac{[\sqrt{N}]([\sqrt{N}]+1)}{2} \sim \gamma N + O(\sqrt{N})$. Тогда искомый предел

$$\lim_{N\to\infty} \frac{|k|k \le N, \{x_k\} \le \gamma|}{N} = \lim_{N\to\infty} \frac{\gamma N + O(\sqrt{N})}{N} = \gamma.$$

Билет 29

Равномерно распределенные последовательности по модулю 1

Def. Последовательность x_n равномерно распределена по модулю 1, если $\forall \gamma \in [0,1]$ $\lim\limits_{N\to\infty} \frac{|k|k\leq N, \{x_k\}\leq\gamma|}{N} \to \gamma$, где $\{x\}$ — дробная часть.

$a^n, a<1$ как пример неравномерно распределенной последовательности по модулю 1

Заметим, что $\{a^k\} = a^k$. Пусть $\gamma = a + \varepsilon \in [0,1)$. Очевидно, что $\forall n \in \mathbb{N}\ a^n \in [0,\gamma]$. Но тогда $\lim\limits_{N\to\infty} \frac{|k|k\leq N, \{x_k\}\leq\gamma|}{N} = 1 \neq \gamma$.

Билет 30

Всюду плотные последовательности

Def. Последовательность x_n всюду плотна на отрезке $[a,b]$, если для любого $[c,d] \subset [a,b]$ существует бесконечного много номеров N таких, что $x_N \in [c,d]$.

$\{ln(n)\}$ как пример всюду плотной последовательности на отрезке от 0 до 1

Зафиксируем N. Тогда $[x_n] = k \in \{1,2,\dots,[ln(n)]\}$.

$$\{ln(n)\} \in [c,d] \Longrightarrow ln(n) \in [k+c, k+d] \Longrightarrow n \in [e^{k+c}, e^{k+d}]$$

Откуда для N число таких будет суммой $\sum\limits_{k=1}^{[ln(N)]} \left(e^{k+d} - e^{k+c}\right) = \frac{e(e^{ln(N)}-1)}{e-1}(e^d - e^c) \sim N\frac{e(e^d-e^c)}{e-1} \to \infty$. То есть для любого отрезка число точек внутри него бесконечно, а значит $\{ln(n)\}$ всюду плотна на отрезке от 0 до 1.

Билет 31

Равномерная распределенность по модулю 1 и всюду плотность

Утверждение. Если последовательность x_n равномерно распределена по модулю 1, то она и всюду плотна на отрезке $[0,1]$.

Доказательство: Из определения равномерной распределенности по модулю 1 вытекает следующее $\forall c < d \in [0,1]$ $\lim\limits_{N\to\infty} \frac{|k|k\leq N, \{x_k\}\in[c,d]|}{N} \to d-c$. Или же $|k|k \leq N, \{x_k\} \in [c,d]| = \theta(N)$, то есть для любого подотрезка найдется бесконечное число точек в нем.

■

Билет 32

Тригонометрические суммы. Критерий Вейля

Def. Тригонометрической суммой называют сумму вида $\sum\limits_{k=1}^{N} e^{2i\pi kx}$

Th. (Критерий Вейля) x_n равномерно распределена по модулю 1 тогда и только тогда, когда

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

Последовательность $x_n = \alpha n$

Если $\alpha \in \mathbb{Q}$, то x_n содержит только конечное множество значений, а значит и не является равномерно непрерывной по модулю 1.

Теперь пусть α иррационально. Тогда

$$\frac{1}{N}\sum_{n=1}^{N} e^{2i\pi h\alpha n} = \frac{1}{N} e^{2i\pi h\alpha}\frac{e^{2i\pi h\alpha N}-1}{e^{2i\pi h\alpha}-1}$$

Заметим, что знаменатель отделен от нуля, так как α иррационально, $\forall h \in \mathbb{Z} \setminus \{0\}$ $2h\alpha \notin \mathbb{Z}$.

Числитель дроби по модулю не превзойдет двойки, а значит вся сумма стремится к нулю, откуда по критерию Вейля для иррациональных α последовательность $x_n = \alpha n$ равномерно распределена по модулю 1.

Билет 33

Последовательность $1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \ldots$

Критерий Вейля как-то не очень применим, поэтому по определению. Зафиксируем N. Пусть знаменатель x_n равен Q. Обозначим все знаменатели дробей из последовательности за $q \in \{1, 1, \ldots, Q\}$.

$$x_n \le \gamma \Longrightarrow \frac{p}{q} \le \gamma \Longrightarrow p \le \gamma q \Longrightarrow p \in \{1, 2, \ldots, [\gamma q]\}$$

Теперь посчитаем итоговое число членов последовательности:

$$\sum_{q=1}^{Q} [\gamma q] \le \sum_{q=1}^{Q} (\gamma q - 1) = \gamma\frac{Q(Q-1)}{2} - Q$$

Оценим знаменатель Q: заметим, что с данным знаменателем q количество членов последовательности $q-1$, тогда верна следующая оценка:

$$1 + \sum_{q=1}^{Q-1} q \le N \le 1 + \sum_{q=1}^{Q} q \Longrightarrow 1 + \frac{Q(Q-1)}{2} \le N \le 1 + \frac{Q(Q+1)}{2} \Longrightarrow Q = O(\sqrt{N})$$

Используя это знание, оценим предел сверху и снизу:

$$\lim_{N\to\infty}\left(\frac{\frac{\gamma Q(Q-1)}{2}-Q}{N}\right)\le\lim_{N\to\infty}\left(\frac{\gamma(N-1)}{N}+O\left(\frac{1}{\sqrt{N}}\right)\right)=\gamma$$

$$\lim_{N\to\infty}\left(\frac{\frac{\gamma Q(Q-1)}{2}-Q}{N}\right)=\lim_{N\to\infty}\left(\frac{\gamma Q^2+Q-(\gamma+3)Q}{2N}\right)=\lim_{N\to\infty}\left(\frac{\gamma Q(Q+1)}{2N}-(3+\gamma)\frac{Q}{2N}\right)\ge$$
$$\ge\lim_{N\to\infty}\left(\frac{\gamma(N-1)}{N}+(3+\gamma)O\left(\frac{1}{\sqrt{N}}\right)\right)=\gamma$$

Откуда следует, что последовательность равномерно распределена по модулю 1.

Последовательность $\frac{1}{2},\frac{1}{4},\frac{3}{4},\frac{1}{8},\dots$

Неформально. Назовем «циклом» дроби с одинаковым знаменателем. Тогда заметим, что последовательность каждым новым циклом делит пополам разбиение отрезка $[0,1]$, построенное предыдущим циклом. Рассмотрим два последовательных элемента внутри цикла таких, что γ будет между ними. Нетрудно заметить, что с ростом номера цикла эти числа стремятся с обеих сторон к γ, откуда понятно, что с ростом номера цикла доля попавших из цикла элементов последовательности стремится к γ снизу. Последовательность долей монотонно возрастает (хотя бы каждые два номера, если γ рационально), при этом последовательность ограничена сверху γ, а значит последовательность долей сойдется к γ, что доказывает равномерную распределенность по модулю 1 данной последовательности.

С точки зрения теории вероятностей. Заметим, что мы генерируем с помощью распределения $Bin(0.5)$ числа в двоичной записи длины N, а потом делим на N, при этом последний «бит» всегда равен единице. Можно формально показать, что такая последовательность сойдется по распределению к $\mathcal{U}[0,1]$.

Билет 34

Последовательность mx_n**,** $m\in\mathbb{Z}$

x_n р.р. по модулю 1 равносильно $\forall h\in\mathbb{Z}\setminus\{0\}\hookrightarrow\frac{1}{N}\sum\limits_{n=1}^{N}e^{2i\pi hx_n}\to 0$

mx_n р.р. по модулю 1 равносильно$\forall mh\in\mathbb{Z}\setminus\{0\}\hookrightarrow\frac{1}{N}\sum\limits_{n=1}^{N}e^{2i\pi(mh)x_n}\to 0$

Так как $m\in\mathbb{Z}$, $mh\in\mathbb{Z}$ и пробегает все целые числа. Откуда по критерию Вейля напрямую следует, что для целых ненулевых m mx_n р.р. по модулю 1.

Последовательность mx_n, $m \notin \mathbb{Z}$

Вспомним, что $x_n = \alpha n, \alpha$ ираационально является равномерно распределенной. Тогда пусть $m = \alpha^{-1}$. Последовательность $x_n = n$ очевидно не является равномерно распределенной.

Вопросы на оценку «Хор»

Билет 35

Линейная выразимость НОДа (б/д)

$\exists x, y \in \mathbb{Z} : gcd(a, b) = ax + by.$

Лемма Евклида через алгоритм Евклида

Лемма. Если простое число p делит без остатка произведение двух целых чисел $x \cdot y$, то p делит x или y.

Доказательство: Из алгоритма Евклида следует лемма выше. Пусть x не делится на p, тогда по лемме Безу найдутся такие $u, v \in \mathbb{N} : ux + vp = 1 \Longrightarrow (xy)u + y(pv) = y$. Тогда, так как xy делится на p, значит левая часть делится на p, то есть и y делится на p.

Билет 36

Лемма Евклида через «идеалы»

Лемма. Если простое число p делит без остатка произведение двух целых чисел $m \cdot n$, то p делит m или n.

Def. Идеалом в $\mathbb{Z}$ назовем множество $M = \{a \in \mathbb{Z} | an \equiv 0 \mod p\}$

Заметим, что идеалы замкнуты относительно сложения и домножения на целое число.

Также заметим, что если d — минимальное положительное число из M, то $M = \{kd | k \in \mathbb{Z}\} = d\mathbb{Z}$. Такое множество действительно является идеалом, так как замкнуто относительно сложения и домножения на целое число. При этом в данных двух множествах есть общий элемент, а значит и множества совпадут.

$p \in M \Longrightarrow p \equiv 0 \mod d$, откуда по определению простого числа $d = 1$ или $d = p$. Если $d = 1$, то $M = \mathbb{Z} \Longrightarrow 1 \in M \Longrightarrow n$ делится на p. Иначе $d = p$, тогда $m \in M \Longrightarrow m$ делится на p.

Билет 37

Единственность разложения от противного

Пусть есть числа, разложимые двумя разными способами. Выберем минимальное из них N, то есть $N = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$. Все p_i и q_i различны, иначе можно сократить и получить число, меньшее

N. Пусть $p_1 < q_1$, $M = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_l$. Тогда $M < N$. Покажем, что M тоже имеет неодрозначное разложение.

Заметим, что $M = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_l = q_1 \cdot \ldots \cdot q_l - p_1 \cdot q_2 \cdot \ldots \cdot q_l = p_1 \cdot \ldots \cdot p_k - p_1 \cdot q_2 \cdot \ldots \cdot q_l = p_1(p_2 \cdot \ldots \cdot p_k - q_2 \cdot \ldots \cdot q_l)$, поэтому M делится на p_1.

При этом $q_1 - p_1$ не делится на p_1, а $q_2, \ldots, q_l$ отличны от p_1, а значит в разложении M отсутствует p_1, что доказывает наличие двух различных разложений M. Противоречие с тем, что N минимальное такое число.

■

Билет 38

Системы вычетов

Def. Полная система вычетов — произвольный набор из m всевозможных вычетов.

Def. Приведенная система вычетов — множество обратимых элементов из полной системы вычетов по модулю m.

Def. В системе вычетов по модулю m (обозначение $\mathbb{Z}_m$) арифметические операции определены так:

1. $a + b = (a + b) \mod m$
2. $a \cdot b = (a \cdot b) \mod m$

Малая теорема Ферма с четырьмя доказательствами

Лемма. Если $gcd(a, p) = 1$, то $\{0, a, 2a, \ldots, (p-1)a\}$ — полная система вычетов.

Доказательство: Пусть это не так, то есть $\exists x \not\equiv y \mod p : ax \equiv ay \mod p$. Тогда $a(x - y) \equiv 0 \mod p \Longrightarrow (x - y) \equiv 0 \mod p \Longrightarrow x \equiv y \mod p$. Противоречие.

■

Th. Если p — простое и a — целое, не делящееся на p, то $a^p \equiv a \mod p$.

Доказательство: Заметим, что $gcd(a, p) = 1$. Рассмотрим полную систему вычетов по модулю p. По лемме выше $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot a(p-1) \Longrightarrow a^{p-1} \equiv 1 \mod p$.

■

Доказательство: (используем магию полиномиальных коэффициентов)

$$a^p = (1+1+\ldots+1)^p; P(\alpha_1, \ldots, \alpha_a) = \frac{p!}{\alpha_1! \cdot \ldots \cdot \alpha_a!} \equiv a\ (p) \Longrightarrow a^p = (1+1+\ldots+1)^p \equiv 1+1+\ldots 1 = a\ (p)$$

■

Доказательство: Рассмотрим все строки длины p из алфавита мощности a. Таких строк a^p. Теперь уберем строки, состоящие из одинаковых букв, тогда осталось $a^p - a$ строк. Заметим, что остальные строки можно разбить на классы эквивалентности по отношению «является циклическим сдвигом». С учетом того, что $gcd(a, p) = 1$, получим, что длина периода p. То есть размер класса эквивалентности p. А значит $a^p - a \equiv 0 \ (p)$.

■

Th. (Лагранж) Порядок элемента делит порядок конечной группы. Порядок группы — число элементов в ней, а порядок элемента — наименьший показатель степени, в которую надо возвести элемент, чтобы получить нейтральный.

Доказательство: Рассмотрим приведенную системы вычетов в $\mathbb{Z}_p$. Они образуют группу по умножению с нейтральным элементом 1. Порядок этой группы $p - 1$, а значит если $gcd(a, p) = 1$, то $a^{p-1} \equiv 1 \ (p)$.

■

Билет 39

Мультипликативность функции Эйлера

Лемма. Пусть $gcd(m, m') = 1$, a пробегает приведенную систему вычетов по модулю m, a' аналогично с m'. Тогда $a'm + am'$ пробегает полную систему вычетов по модулю mm'.

Доказательство: Предположим противное. То есть $a'_1m+a_1m' \equiv a'_2m+a_2m' \mod (mm') \Longrightarrow a_1m' \equiv a_2m' \mod m \Longrightarrow a_1 \equiv a_2 \mod m, a'_1 \equiv a'_2 \mod m'$. Противоречие.

Th. Функция Эйлера мультипликативна для взаимно простых m, m'.

Доказательство: По лемме найдутся такие a, a', что

$$gcd(a'm + am', mm') = 1 \Longleftrightarrow gcd(am', m) = 1, gcd(a'm, m') = 1 \Longleftrightarrow gcd(a, m) = 1, gcd(a', m') = 1$$

Поэтому $\varphi(mm')$ чисел, меньших и взаимно простых с mm', являются наименьшими положительными вычетами среди $\varphi(m)\varphi(m')$ значений $a'm + am'$. А значит мультипликативность доказана.

■

Лемма. $\varphi(p^n) = p^n - p^{n-1}$

Доказательство: Числа, не взаимно простые с p^n : $p, p^2, \ldots, p^{n-1}p$. Тогда взаимно простых $p - p^{n-1}$.

■

Th. Пусть в разложении n присутствуют простые числа $p_1, \ldots, p_k$. Тогда $\varphi(n) = n \prod\limits_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

Доказательство:

$$\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{k} \left(p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

■

Билет 40

Теорема Лагранжа о числе корней по простому модулю

Th. Пусть полином $g(x) = a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \mod p$, $g(x) \in \mathbb{Z}[x]$. Тогда если существует $n+1$ рациональный корень по модулю p, то $\forall i a_i \equiv 0 \mod p$.

Доказательство: Пусть $x_1, \ldots, x_{n+1}$ — корни, тогда

$$g(x) = a(x - x_1) \cdot \ldots \cdot (x - x_n) + \ldots + k(x - x_1)(x - x_2) + n(x - x_1) + o$$

Подставим x_1, тогда $g(x_1) = o \equiv 0\ (p)$. Подставим $x_2 : 0 \equiv g(x_2) = n(x_1 - x_2) + o \equiv n(x_1 - x_2) \equiv n\ (p)$.

Аналогично, подставляя последовательно корни до x_{n+1}, получим, что все эти коэффициенты делятся на p, а значит и искодные a_i делятся на p, так как они являются линейными комбинациями новых.

■

Билет 41

Распределение простых чисел в натуральном ряде

Th. (Постулат Бертрана) $\forall x \exists p : p \in [x, 2x]$

Функции $\pi(x), \theta(x), \psi(x)$

Def. $\pi(x)$ — количество простых чисел, не превосходящих x.

Def. $\theta(x) = \sum\limits_{p \le x} ln(p)$

Def. $\psi(x) = \sum\limits_{(\alpha,p):p^\alpha \le x} ln(p)$

Теорема о равенстве верхних и нижних пределов (формулировка)

$\lambda_1 = \overline{\lim\limits_{x\to\infty}} \frac{\theta(x)}{x}$ $\lambda_2 = \overline{\lim\limits_{x\to\infty}} \frac{\psi(x)}{x}$ $\lambda_3 = \overline{\lim\limits_{x\to\infty}} \frac{\pi(x)}{x/ln(x)}$

За μ_i обозначим соответствующие нижние пределы.

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

Асимптотический закон распределения простых

Th. $\exists c \in \mathbb{R} \forall x \exists p : p \in [x, x + Cx^{0.525}]$

«Дырки» между соседними простыми

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

Билет 42

Китайская теорема об остатках

Лемма. Пусть $gcd(a, b) = 1$, тогда $\exists c : ac \equiv 1 \mod b$

Доказательство: Рассмотрим числа $a, 2a, \ldots, (b-1)a$. Они образуют приведенную систему вычетов, а значит есть остаток 1.

■

Th. Пусть $n_1, \ldots, n_k \in \mathbb{N}$ попарно взаимно просты, а $r_1, \ldots, r_k \in \mathbb{Z}$, тогда $\exists! M$ по модулю $\prod_{i=1}^{k} n_i$ решение системы сравнений:

$$\begin{cases} M \equiv r_1 \mod n_1 \\ \ldots \\ M \equiv r_k \mod n_k \end{cases}$$

Доказательство: 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. Тогда покажем, что $M = \sum_{i=1}^{k} r_i N_i N_i^{-1}$ будет решением. Рассмотрим M по модулю n_1. Все слагаемые, начиная со второго, содержат множитель N_i, который делится на n_1. Тогда рассмотрим $r_1 N_1 N_1^{-1} \equiv r_1 \mod n_1$. Аналогично проверяем все k сравнений.

Пусть A и B — решения. $A - B \equiv 0 \mod n_i$. В силу взаимной простоты n_i получим, что $A - B \equiv 0 \mod N$.

■

Билет 44

Сравнения второй степени. Вычеты и невычеты

Сравнения второй степени. Квадратичные вычеты и невычеты

Def. $ax^2 + bx + c \equiv 0 \mod m$ — сравнение второго порядка.

Def. Пусть p — нечетное простое число. Тогда если $gcd(a,p) = 1$ и $\exists x : x^2 \equiv a \mod p$, то a — квадратичный вычет, иначе — невычет.

Символ Лежандра

Def. Символом Лежанадра называют

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

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

Доказательство: Если $gcd(a,p) \neq 1$, то тривиально. Теперь $gcd(a,p) = 1$. Тогда по малой теореме Ферма $a^{p-1} \equiv 1 \mod p \Longrightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p$. Оба множителя не могут одновременно делиться на p, так как иначе делилась бы и их разность.

Пусть a — вычет, тогда $\exists x : a \equiv x^2 \mod p \Longrightarrow a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p$, по МТФ и так как $x < p$. А если a — невычет, то $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

Следствие Символ Лежандра мультипликативен.

Очередное интересное тождество

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

Доказательство:

$$\left[\frac{2as}{p}\right] = 2\left[\frac{as}{p}\right] + \left[2\left\{\frac{as}{p}\right\}\right]$$

Рассмотрим второе слагаемое. Если $as \leq \frac{p-1}{2}$, то выражение будет четным, а значит знак $(-1)^{2\left[\frac{as}{p}\right]+\left[2\left\{\frac{as}{p}\right\}\right]}$ будет положительный, так как мы рассматриваем вычеты из отрезка $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$.

Тогда $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$ будет произведением знаков по всем x из пределов суммирования. Это верно, так как если рассмотреть выражения вида $a, 2a, \ldots, \frac{p-1}{2}a$, то перемножив их все, с одной стороны будет произведение знаков, а с другой — $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. А произведение знаков и даст нам исходную формулу суммы.

■

Билет 45

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

Доказательство: Пусть a нечетное, тогда заметим, что

$$\left(\frac{2a}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) \equiv (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{(a+p)x}{p}\right]} = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \sum\limits_{x=1}^{\frac{p-1}{2}} x} = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}}$$

Подставим $a = 1$, тогда

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

Так как $x < p$ в суммировании, значит целые части нулевые.

■

Билет 46

Кронекерово произведение

Def. Пусть $A \in M_{n\times n}$; $B \in M_{m\times m}$. Тогда кронекеровским произведением A на B назовем матрицу

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \ddots & \cdots & \vdots \\ a_{n1}B & \cdots & \cdots & a_{nn}B \end{pmatrix} \in M_{nm\times nm}$$

Th. Если A и A' — матрицы Адамара, то и $B = A \otimes A'$ тоже.

Доказательство:

Действительно, найдем скалярное произведение первых двух строк матрицы B:

$$\begin{aligned} a_{11}a'_{11} \cdot a_1 1a'_{21} + a_{11}a'_{12} \cdot a_{11}a'_{22} + \ldots + a_{11}a'_{1m} \cdot a_{11}a'_{2m} + \ldots + a_{1n}a'_{11} \cdot a_{1n}a'_{21} + \ldots + a_{1n}a'_{1m} \cdot a_{1n}a'_{2m} = \\ = a'_{11}a'_{22}(a_{11}a_{11} + \ldots + a_{1n}a_{1n}) + \ldots + a'_{1m}a'_{2m}(a_{11}a_{11} + \ldots + a_{1n}a_{1n}) = \\ = n(a'_{11}a'_{21} + \ldots + a'_{1m}a'_{2m}) = 0 \end{aligned}$$

поскольку A' — матрица Адамара. ■

Билет 47

Конструкция Пэйли

Вспомним символ Лежандра. Свойства: он мультипликативен, число вычетов и невычетов равно $\frac{p-1}{2}$.

Рассмотрим матрицу $Q \in M_{p\times p}$, где $Q_{i,j}$ равно $\left(\frac{i-j}{p}\right)$. Далее пример будет для 7×7, но работает для произвольного $p = 4k+3$.

$$\begin{pmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{pmatrix}$$

Заметим, что у полученной матрицы для любых двух строк их скалярное произведение -1. Запишем в нулевые столбцы и строки единицы. Теперь скалярное произведение двух любых строк (без первой) равно нулю, так как в любой строке стоят $\frac{p-1}{2}$ единичек и $\frac{p-1}{2}$ минус единичек.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{pmatrix}$$

Теперь избавляемся от всех нулей так, чтобы скалярное произведение соответствующей строки на первую дало ноль. Это можно сделать, так как их скалярное произведение равно разности -1 и 1 в соответствующей строке, а такая разность была до добавления единиц нулевой, а теперь стало так, что оно равно единице (нулевой столбец). Поэтому пишем вместо нулей -1. Это не испотрит скалярности остальных строк, так как матрица симметрична относительно главной диагонали с точностью домножения на -1, то есть антисимметрична.

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

Это работает, так как $p = 4k+3$. Поясним: на месте (i,j) стоит $\left(\frac{i-j}{p}\right)$ и на месте (j,i) стоит $\left(\frac{j-i}{p}\right)$

$$\left(\frac{i-j}{p}\right)\cdot\left(\frac{-1}{p}\right)=\left(\frac{j-i}{p}\right)=-1^{\frac{p-1}{2}}\cdot\left(\frac{i-j}{p}\right)=-\left(\frac{i-j}{p}\right)$$

Осталось показать, что если рассмотреть Q, то скалярное произведение двух строк будет равно -1. Рассмотрим строоки с номерами i,j. Тогда рассмотрим сумму:

$$\sum_{k\in\mathbb{Z}_p}\left(\frac{i-k}{p}\right)\left(\frac{j-k}{p}\right)=\sum_{i-k\in\mathbb{Z}_p}\left(\frac{i-k}{p}\right)\left(\frac{i-k+(j-i)}{p}\right)=\sum_{x\in\mathbb{Z}_p}\left(\frac{x}{p}\right)\left(\frac{x+d}{p}\right)=T_d=$$

$$=\sum_{dy\in\mathbb{Z}_p}\left(\frac{dy}{p}\right)\left(\frac{dy+d}{p}\right)=\sum_{y\in\mathbb{Z}_p}\left(\frac{d^2}{p}\right)\left(\frac{y}{p}\right)\left(\frac{y+1}{p}\right)=\sum_{y\in\mathbb{Z}_p}\left(\frac{y}{p}\right)\left(\frac{y+1}{p}\right)=T_1$$

Получили, что $T_1=\ldots=T_{p-1},T_0=p-1$. Покажем, что сумма всех T_i равна нулю, то есть

$$\sum_{d\in\mathbb{Z}_p}T_d=\sum_{d\in\mathbb{Z}_p}\sum_{x\in\mathbb{Z}_p}\left(\frac{x}{p}\right)\left(\frac{x+d}{p}\right)=\sum_{x\in\mathbb{Z}_p}\left(\left(\frac{x}{p}\right)\sum_{d\in\mathbb{Z}_p}\left(\frac{x+d}{p}\right)\right)=\sum_{x\in\mathbb{Z}_p}\left(\left(\frac{x}{p}\right)\cdot 0\right)=0$$

Но ведь эта сумма и отвечала за то, чему равно скалярное произведение. Что и требовалось показать. Конструкция доказана. ■

Билет 48

Порядки(показатели) элементов в системах вычетов

Далее работаем в системе вычетов $\mathbb{Z}_m$.

Def. Пусть $gcd(g,m)=1$. Тогда показатель $ord(g)=k$ — минимальное $k>0$, что $g^k\equiv 1 \mod m$.

Note. Если $gcd(g,m)\neq 1$, то $ord(g)=\infty$

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

Пусть $s=ord(g^l)$, $k=ord(g)$. Заметим, что по определению порядка s — минимальное натуральное число, что ls делится на k.

Лемма. Пусть $a,b\in\mathbb{N}$, s — минимальное натуральное, что as делится на b. Тогда $s=\frac{b}{gcd(a,b)}$

Доказательство:

1. $b\cdot\frac{a}{gcd(a,b)}=a\cdot\frac{b}{gcd(a,b)}$ делится на b, значит $s\leq\frac{b}{gcd(a,b)}$, так как s минимальное.
2. Пусть $b'=\frac{b}{gcd(a,b)}$, $a'=\frac{a}{gcd(a,b)}$. Тогда $a's$ делится на b', при этом $gcd(a',b')=1$ по определению НОДа. Значит s делится на b', откуда $s\geq\frac{b}{gcd(a,b)}$.

Зажали с обеих сторон, откуда немедленно следует равенство.

■

Билет 49

Порядки(показатели) элементов в системах вычетов

Далее работаем в системе вычетов $\mathbb{Z}_m$.

Def. Пусть $gcd(g, m) = 1$. Тогда показатель $ord(g) = k$ — минимальное $k > 0$, что $g^k \equiv 1 \mod m$.

Note. Если $gcd(g, m) \neq 1$, то $ord(g) = \infty$

Порядок произведения

Утверждение. Если $ord(g) = k$, $ord(h) = l$, $gcd(k, l) = 1$, то $ord(gh) = kl$.

Доказательство: В обозначениях утверждения: $g^k \equiv 1\ (m)$, $h^l \equiv 1\ (m)$. $(gh)^{ord(gh)} \equiv 1\ (m)$. Так как k, l взаимно просты, $g^{kl} \cdot h^{kl} \equiv 1\ (m)$, откуда следует утверждение.

■

Билет 50

Критерий первообразного корня через степенные сравнения

Th. Пусть $\varphi(m) = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, $gcd(g, m) = 1$. Тогда g — первообразный корень в $\mathbb{Z}_m$ тогда и только тогда, когда g не является решением ни одного из сравнений $x^{\frac{\varphi(m)}{p_k}} \equiv 1\ (m)$.

Доказательство:

$\Longrightarrow$

Заметим, что первообразный корень по определению не может удовлетворять ни одному из таких сравнений.

$\Longleftarrow$

Вспомним, что $\forall g \in \mathbb{Z}_m$ $\varphi(m)$ делится на $ord(g)$. Пусть k — показатель g. Тогда k делится на $\varphi(m)$. Если для какого-то i k делится на $\frac{\varphi(m)}{p_i}$, то для сравнения $x^{\frac{\varphi(m)}{p_i}} \equiv 1\ (m)$ g подходит. Но по условию оно не удовлетворяет ни одному из них, а значит k не делится ни на какое $\frac{\varphi(m)}{p_i}$. Откуда получаем, что $\varphi(m) = k$.

■

Билет 52

Теорема Дирихле о диофантовых приближениях через принцип Дирихле

Th. 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 $\forall Q \in \mathbb{N}$. Разобьем $[0,1]$ на Q одинаковых частей. Рассмотрим числа $\{\alpha x\}$ — дробная часть, где $x \in \overline{0,\ldots,Q}$. Получилось $Q+1$ число, а частей отрезка Q — по принципу Дирихле $\exists x_1, x_2 : |\{\alpha x_1\} - \{\alpha x_2\}| \leq \frac{1}{Q}$. А значит

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

$$\Longrightarrow |\alpha q - p| \leq \frac{1}{Q} \Longrightarrow \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} \xRightarrow{q=(x_1-x_2)\leq Q} \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

Теперь возьмем новое $Q_1 : \frac{1}{Q_1} < \left|\alpha - \frac{p}{q}\right|$. Найдем для него таким же образом p_1, q_1, для ниxx будет верно, что $\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{Q} < \left|\alpha - \frac{p}{q}\right|$, откуда следует, что $\frac{p_1}{q_1}$ и $\frac{p}{q}$ не совпадают.

■

Билет 53

Уточнение теоремы Дирихле для рациональных дробей

Th. Пусть $\alpha \in \mathbb{Q}$. Тогда $\exists$ лишь конечно много рациональных дробей $\frac{p}{q}$ таких, что $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$.

Доказательство: Пусть $\alpha = \frac{m}{n}$. Тогда из того, что $\left|\frac{m}{n} - \frac{p}{q}\right| = \left|\frac{mq-np}{nq}\right| < \frac{1}{q^2}$ получаются два случая:

1. $mq - np = 0 \Longrightarrow \frac{m}{n} = \frac{p}{q} \Longrightarrow \left|\frac{m}{n} - \frac{p}{q}\right| = 0 < \frac{1}{n^2}$.
2. $mq - np = 1 \longrightarrow \left|\frac{m}{n} - \frac{p}{q}\right| = \frac{1}{nq} < \frac{1}{q^2} \Longleftrightarrow q < n$.

То есть число дробей $\frac{p}{q}$, приближающих данную дробь не больше n, что конечно.

■

Билет 54

Теорема Минковского в $2D$

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 теоремы Минковского для замкнутых множеств (б/д)

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

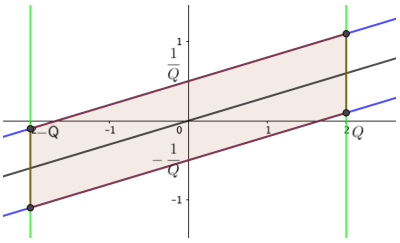
Билет 55

Теорема Дирихле из теоремы Минковского в $2D$

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

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.

■

Билет 56

Бесконечные цепные дроби

Def. Пусть $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$. Тогда бесконечная цепная дробь — выражение, чья каноничная запись имеет вид $[a_0 : a_1, \ldots, a_n, \ldots]$.

Def. Величиной бесконечной цепной дроби называют предел ее подходящих дробей, то есть $\lim\limits_{n\to\infty} \frac{p_n}{q_n}$.

Бесконечная цепная дробь — иррациональное число

Утверждение. Если цепная дробь бесконечна, то ее значение иррационально.

Доказательство: Если число рационально, то подходящие дроби станут равными ей, а зхначит и цепная дробь конечна.

■

Билеты 57 и 58

Бесконечные цепные дроби

Def. Пусть $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$. Тогда бесконечная цепная дробь — выражение, чья каноничная запись имеет вид $[a_0 : a_1, \ldots, a_n, \ldots]$.

Def. Величиной бесконечной цепной дроби называют предел ее подходящих дробей, то есть $\lim\limits_{n\to\infty} \frac{p_n}{q_n}$.

Представление иррационального числа в виде б.ц.д.

Пусть b — число, которое надо разложить в цепную дробь.

Тогда $b = [b] + \{b\} = [b] + \frac{1}{\frac{1}{\{b\}}} = [b] + \frac{1}{\left[\frac{1}{\{b\}}\right] + \left\{\frac{1}{\{b\}}\right\}}$.

Этот процесс по индукции можно продолжать до бесконечности, при этом из алгоритма очевидна биекция, так как каждое неполное частное определяется однозначно. Откуда следует единственность разложения иррационального числа в бесконечную цепную дробь.

Билет 59

Сведения о подходящих дробях

Th. Для числителей и знаменателей подходящих дробей верны следующие соотношения:
$$\begin{cases} p_k = a_k p_{k-1} + p_{k-2} \\ q_k = a_k q_{k-1} + q_{k-2} \end{cases}$$

Доказательство: Индукция по k. База тривиально проверяется вручную, теперь переход:

$$[a_0,\dots,a_{k+1}]=\frac{p_{k+1}}{q_{k+1}},[a_1,\dots,a_{k+1}]=\frac{p^*_{k+1}}{q^*_{k+1}}\Longrightarrow\frac{p_{k+1}}{q_{k+1}}=a_0+\frac{q^*_{k+1}}{p^*_{k+1}}=\frac{a_0p^*_{k+1}+q^*_{k+1}}{p^*_{k+1}}\Longrightarrow\begin{cases}p_{k+1}=a_0p^*_{k+1}+q^*_{k+1}\\q_{k+1}=p^*_{k+1}\end{cases}$$

Применяя предопложение индукции, $q_{k+1}=a_{k+1}p^*_k+p^*_{k-1}=a_{k+1}q_k+q_{k-1}$ и

$$p_{k+1}=a_0(a_{k+1}p^*_k+p^*_{k-1})_{ak+1}q^*_k+q^*_{k-1}=a_{k+1}(a_0p^*_k+q^*_k)+(a_0p^*_{k-1}+q^*_{k-1})=a_{k+1}p_k+p_{k-1}$$

■

Проделаем следующую операцию с рекуррентными соотношениями: домножим первое на q_{k-1}, а второе на p_{k-1} и вычтем второе из первого:

$$p_kq_{k-1}-q_kp_{k-1}=p_{k-2}q_{k-1}-p_{k-1}q_{k-2}\ (1)$$

При $k=1$: $p_1q_0-q_1p_0=1$. Пусть $r_k=p_kq_{k-1}-q_kp_{k-1}$, $r_1=1$, тогда в силу (1) заметим, что $r_k=-r_{k-1}$. Откуда следует, что

$$p_kq_{k-1}-q_kp_{k-1}=(-1)^{k-1}\ (2)$$

Теперь разделим (2) на q_kq_{k-1} и получим

$$\frac{p_k}{q_k}-\frac{p_{k-1}}{q_{k-1}}=\frac{(-1)^{k-1}}{q_kq_{k-1}}\ (3)$$

Утверждение. Подходящие дроби несократимы

Доказательство: Из (2) получаем, что $gcd(p_k,q_k)=1$.

Утверждение. Четные подходящие дроби возрастают, а нечетные — убывают.

Доказательство: Проделаем следующую операцию с рекуррентными соотношениями: домножим первое на q_{k-2}, а второе на p_{k-2} и вычтем второе из первого:

$$p_kq_{k-2}-q_kp_{k-2}=a_k(p_{k-1}q_{k-2}-q_{k-1}p_{k-2})=-a_k(q_{k-1}p_{k-2}-p_{k-1}q_{k-2})=a_k(-1)^k$$

Отсюда напрямую получаем, что

$$\frac{p_k}{q_k}-\frac{p_{k-2}}{q_{k-2}}=\frac{(-1)^ka_k}{q_kq_{k-2}}$$

Откуда следует необходимое утверждение.

■

Теорема Дирихле через цепные дроби

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

Доказательство: Воспользуемся свойствами подходящих дробей $\frac{p_n}{q_n}$: $\left|\alpha-\frac{p_{2n-1}}{q_{2n-1}}\right|\le\left|\frac{p_{2n}}{q_{2n}}-\frac{p_{2n-1}}{q_{2n-1}}\right|=\frac{1}{q_{2n}q_{2n-1}}\le\frac{1}{q^2_{2n-1}}$.

Уточнение теоремы Дирихле (б/д)

Th. Пусть $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Тогда $\exists$ бесконечно много рациональных несократимых дробей $\frac{p}{q}$ таких, что $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{\sqrt{5}q^2}$.

Зависимость точности аппроксимации от скорости роста неполных частных (б/д)

Th. $\forall f(q) : \lim\limits_{q\to\infty} f(q) = \infty$, где f монотонна $\exists \alpha \in \mathbb{R} \setminus \mathbb{Q}$ и бесконечное число несократимых рациональных дробей таких, что $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{f(q)}$.

Доказательство: Будем строить α до n-го неполного частного, тогда однозначно восстановим q_{n+1}. Возьмем a_{n+1} настолько большим, чтобы $\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} \leq \frac{1}{f(q_n)}$.

■

Утверждение. $\alpha = \frac{1+\sqrt{5}}{2}$ (золотое сечение) — самое плохо приближаемое число.

Билет 60

Алгебраические и трансцендентные числа

Def. α — алгебраическое число степени n, если n — минимальная степень многочлена степени n с целыми коэффициентами, для которого α — корень.

Заметим, что таких чисел счетное количество, а $\mathbb{R}$ континуально. Отсюда следует, что есть не алгебраические или *трансцендентные* числа.

Def. $\alpha \in \mathbb{R}$ трансцендентное, если оно не является алгебраическим.

Теорема Лиувилля. Трансцендентное число из нее

Th. (Лиувилль) Пусть α — алгебраическое степени d, тогда $\exists c = c(d, \alpha)$, что $\left|\alpha - \frac{p}{q}\right| \leq \frac{c}{q^d}$ имеет лишь конечное число решений.

Тогда заметим, что из теоремы про то, что для любой монотонной функции существует иррациональное α, с заданной точностью аппроксимации, можно конструктивно построить трансцендентное число, если скорость роста функции выше любого полинома.

Теорема Гельфонда и сведения о некоторых числах

$e, \pi, \pi + e^\pi$ являются трансцендентными. Про $e + \pi$ ничего неизвестно.

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

Утверждение. e^π трансцендентно.

Доказательство: Предположим, что e^π алгебраическое. Заметим, что i — алгебраическое. Пусть $\alpha = e^\pi, \beta = i \Longrightarrow \alpha^\beta = e^{i\pi}$, но $e^{i\pi} = -1$. Противоречие с теоремой Гельфонда.

Билет 61

Решение уравнения $a^2 - 2b^2 = \pm 1$

Заметим, что $\overline{z^n} = \overline{z \cdot z^{n-1}} = \overline{z}\overline{z^{n-1}} = \ldots = \overline{z}^n$

Утверждение. Доказать, что пара $(a, b) : a \pm b\sqrt{2} = (1+\sqrt{2})^n$ является решением уравнения Пелля $a^2 - 2b^2 = \pm 1$.

Доказательство: Заметим, что $a^2 - 2b^2 = (a - b\sqrt{2})(a + \sqrt{2})$. Если $a + b\sqrt{2} = (1+\sqrt{2})^n$, то $a - b\sqrt{2} = \overline{(1+\sqrt{2})^n} = (1-\sqrt{2})^n$.

Тогда для пар вида из условия $a^2 - 2b^2 = (a - b\sqrt{2})(a + b\sqrt{2}) = (1+\sqrt{2})^n \cdot (1-\sqrt{2})^n = (-1)^n = \pm 1$.

$N(a^2 - 2b^2) = N(a - b\sqrt{2})N(a + b\sqrt{2}) = N(\pm 1) = 1 \Longrightarrow N(a \pm b\sqrt{2}) = \pm 1$, так как норма целая. То есть решение уравнения обязательно имеет единичную норму. Более того, любое число, имеющее единичную норму, является решением уравнения, так как по сути перед нами уравнение $N(a+b\sqrt{2}) = \pm 1$.

■

Билет 62

Решение уравнения $a^2 - 3b^2 = \pm 1$

Заметим, что $\overline{z^n} = \overline{z \cdot z^{n-1}} = \overline{z}\overline{z^{n-1}} = \ldots = \overline{z}^n$

Утверждение. Доказать, что пара $(a, b) : a + b\sqrt{3} = (2+\sqrt{3})^n$ является решением уравнения Пелля $a^2 - 3b^2 = \pm 1$.

Доказательство: Заметим, что $a^2 - 3b^2 = (a - b\sqrt{3})(a + \sqrt{3})$. Если $a + b\sqrt{3} = (1+\sqrt{3})^n$, то $a - b\sqrt{3} = \overline{(1+\sqrt{3})^n} = (1-\sqrt{3})^n$.

Тогда для пар вида из условия $a^2 - 3b^2 = (a - b\sqrt{3})(a + \sqrt{3}) = (1+\sqrt{3})^n \cdot (1-\sqrt{3})^n = (-1)^n = \pm 1$.

$N(a^2 - 3b^2) = N(a - b\sqrt{3})N(a + b\sqrt{3}) = N(\pm 1) = 1 \Longrightarrow N(a \pm b\sqrt{3}) = \pm 1$, так как норма целая. То есть решение уравнения обязательно имеет единичную норму. Более того, любое число, имеющее единичную норму, является решением уравнения, так как по сути перед нами уравнение $N(a+b\sqrt{3}) = \pm 1$.

■

Билет 63

Равномерно распределенные по модулю 1 посл-ти. Эквивалентные определения

Def. Последовательность x_n равномерно распределена по модулю 1, если $\forall \gamma \in [0,1]$ $\lim\limits_{N\to\infty} \frac{|k|k\le N, \{x_k\}\le\gamma|}{N} \to \gamma$, где $\{x\}$ — дробная часть.

Note. $F(N,\alpha,\beta) = |k|k \le N, \alpha \le \{x_k\} \le \beta|$

То есть определение в терминах выше можно переписать так: $\forall\gamma \in [0,1]$ $\lim\limits_{N\to\infty} \frac{F(N,0,\gamma)}{N} \to \gamma$.

Def. Отклонение последовательности x_n обозначается как $D_N = \sup\limits_{0\le\alpha<\beta\le 1} \left(\frac{F(N,\alpha,\beta)}{N} - (\beta-\alpha)\right)$.

Th. Следующие утверждения эквивалентны:

1. x_n равномерно распределена по модулю 1.
2. $\forall 0 \le \alpha < \beta \le 1$ $\lim\limits_{N\to\infty} \frac{F(N,\alpha,\beta)}{N} = \beta - \alpha$.
3. $\lim\limits_{N\to\infty} D_N = 0$.

Доказательство: Эквивалентность определений 1 и 2 очевидна в силу того, что предел разности равен разности пределов (пределы всегда существуют). Третье и второе тоже эквивалентны, так как во втором имеется квантор «для любого».

■

Билет 64

Равномерная распределенность по модулю 1 последовательности $ln(n)$

Утверждение. $k_n = \{ln(n)\}$ неравномерно распределена по модулю 1.

Доказательство: Зафиксируем N. Тогда $[x_n] = k \in \{1,2,\dots,[ln(N)]\}$.

$$\{ln(n)\} \le \gamma \Longrightarrow \{ln(n)\} \in [k, k+\gamma] \Longrightarrow n \in [e^k, e^{k+\gamma}]$$

То есть для данного k число таких n составляет $e^k(e^\gamma - 1)$. Откуда для N число таких будет суммой $\sum\limits_{k=1}^{[ln(N)]} e^k(e^\gamma-1) = (e^\gamma-1)\cdot e \cdot \frac{e^{[ln(N)]}-1}{e-1} \sim \frac{e(e^\gamma-1)}{e-1}(N-1)$. Тогда искомый предел

$$\lim_{N\to\infty} \frac{|k|k\le N, \{x_k\}\le\gamma|}{N} = \lim_{N\to\infty} \frac{e\,(e^\gamma-1)}{e-1}\frac{N-1}{N} = \frac{e\,(e^\gamma-1)}{e-1} > 1 > \gamma.$$

■

Билет 65

Существование $\alpha > 1$ таких, что a^n не р.р. по модулю 1

Пусть $z^2+pz+q = 0 \in \mathbb{Z}[x]$, при этом корни λ, θ таковы, что $\lambda > 1$, $\theta \in (0,1)$. Рассмотрим $x_n = \lambda^n + \theta^n$. $x_0 = 2, x_1 = -p$, при этом перед нами рекуррента второго порядка, а значит $x_n \in \mathbb{Z}$.

Тогда рассмотрим $y_n = \{\lambda^n\} = 1 - \theta^n \to 1$. Она, очевидно, неравномерно распределена по модулю 1.

Билет 66

Теорема Вейерштрасса о приближении непрерывной функции (б/д)

Th. Если $f \in C([0,1))$, то $\forall \varepsilon > 0$ $\exists$ тригонометрический многочлен $T(x)$ такой, что

$$\sup_{x \in [0,1]} |T(x) - f(x)| < \varepsilon.$$

Равносильность критерия Вейля и интегрального признака

Th. (интегральный признак) Последовательность x_n равномерно распределена по модулю 1 тогда и только тогда, когда $\forall f \in C([0,1])$ верно, что

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{x_n\}) = \int_0^1 f(t)dt$$

Th. (критерий Вейля) Последовательность x_n равномерно распределена по модулю 1 тогда и только тогда, когда

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

Note. Заметим, что в данной сумме не имеет значения, брать ли x_n или $\{x_n\}$.

Th. Критерий Вейля равносилен интегральному признаку.

Доказательство:

$\Longleftarrow$

Если раскрыть по формуле Эйлера экспоненту, то будет сумма косинусов, а косинус непрерывен, значит из интегрального признака следует теорема Вейля.

$\Longrightarrow$

Рассмотрим произвольную $f \in C([0,1])$, зафиксируем $\varepsilon > 0$. Тогда пусть $T(x)$ — соответствующий по теореме Вейерштраса тригонометрический многочлен.

$$\left|\frac{1}{N}\sum_{n=1}^{N} f\left(\{x_n\}\right) - \int_0^1 f(t)dt\right| < \varepsilon \iff$$

$$\iff \left|\frac{1}{N}\sum_{n=1}^{N} f\left(\{x_n\}\right) - \frac{1}{N}\sum_{n=1}^{N} T\left(\{x_n\}\right) + \frac{1}{N}\sum_{n=1}^{N} T\left(\{x_n\}\right) - \int_0^1 T(t)dt + \int_0^1 T(t)dt - \int_0^1 f(t)dt\right| < \varepsilon \iff$$

$$\iff \left(\frac{1}{N}\sum_{n=1}^{N}\left|f\left(\{x_n\}\right) - T\left(\{x_n\}\right)\right| + \left|\frac{1}{N}\sum_{n=1}^{N} T(\{x_n\})\right| + \int_0^1 |T(t) - f(t)|\,dt\right) < \varepsilon \iff$$

$$\iff \left(\frac{1}{N}\cdot N\cdot\frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3}\right) < \varepsilon$$

Где первое и третье слагаемое из теоремы Вейерштрасса, а второе по теореме Вейля.

■

Билет 67

Суммы Гаусса

Def. Суммой Гаусса называют сумму вида $S(q) = \sum\limits_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}}$, $q \in \mathbb{N}$, $gcd(a, q) = 1$.

Th.

$$|S(q)| = \begin{cases} \sqrt{q}, q \equiv 1 \mod 2 \\ \sqrt{2q}, q \equiv 0 \mod 4 \\ 0, q \equiv 2 \mod 4 \end{cases}$$

Доказательство:

$$|S(q)|^2 = S(q)\overline{S(q)} = \sum_{y=1}^{q} e^{-2\pi i \frac{ay^2}{q}} \cdot \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} = \sum_{y=1}^{q} e^{-2\pi i \frac{ay^2}{q}} \cdot \sum_{x=1}^{q} e^{2\pi i \frac{a(x+y)^2}{q}} =$$

$$= \sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}} \sum_{y=1}^{q} e^{2\pi i \frac{2axy}{q}}$$

Рассмотрим отдельно внутреннюю сумму (если $\frac{2ax}{q} \notin \mathbb{Z}$ то это сумма геометрической прогрессии):

$$\sum_{y=1}^{q} e^{2\pi i \frac{2axy}{q}} = \begin{cases} q, q|2ax \\ e^{2\pi i \frac{2ax}{q}} \frac{e^{2\pi i \frac{2ax}{q} q} - 1}{e^{2\pi i \frac{2ax}{q}} - 1} = 0, \text{ иначе} \end{cases}$$

Рассмотрим 2 случая:

1. q нечётное. Тогда $q|2ax \iff q|x \iff q = x$.

$$|S(q)|^2 = e^{2\pi iaq}q = q \Rightarrow |S(q)| = \sqrt{q}$$

2. q чётное. Тогда $q|2ax \iff q|2x \iff x \in \{q, \frac{q}{2}\}$.

$$|S(q)|^2 = e^{2\pi iaq}q + e^{2\pi i\frac{a}{4}q}q = q\left(1 + e^{\frac{qa\pi i}{2}}\right) = \begin{cases} 2q, q \equiv 0 \mod 4 \\ 0, q \equiv 2 \mod 4 \end{cases}$$

■

Вопросы на оценку «Отл» (и на хор 7)

Билет 68

Проблема Эрдеша–Гинзбурга–Зива при $d = 2$ и $n = p$: нижняя и верхние оценки (формулировка)

Доказательство основной леммы

To be continued...

Билет 69

Сравнения второй степени. Квадратичные вычеты и невычеты

Def. $ax^2 + bx + c \equiv 0 \mod m$ — сравнение второго порядка.

Def. Пусть p — нечетное простое число. Тогда если $gcd(a, p) = 1$ и $\exists x : x^2 \equiv a \mod p$, то a — квадратичный вычет, иначе — невычет.

Def. Символом Лежанадра называют

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

Тождество $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} [\frac{ax}{p}]}$ для нечётного a

Th. $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} [\frac{2ax}{p}]}$ — доказано ранее

Th. $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} [\frac{ax}{p}]}$ для нечётного a

Доказательство:

Посчитаем $(\frac{2a}{p})$:

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

$$= (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} [\frac{ax}{p}] + \frac{p^2-1}{8}}$$

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

Приравняв, получим требуемое.

■

Билет 70

Сравнения второй степени. Квадратичные вычеты и невычеты

Def. $ax^2 + bx + c \equiv 0 \mod m$ — сравнение второго порядка.

Def. Пусть p — нечетное простое число. Тогда если $gcd(a, p) = 1$ и $\exists x : x^2 \equiv a \mod p$, то a — квадратичный вычет, иначе — невычет.

Def. Символом Лежанадра называют

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

Квадратичный закон взаимности

Th. $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{\frac{p-1}{2}} [\frac{ax}{p}]}$ для нечётного a

Th. Пусть p, q — простые нечётные. Тогда выполнено:

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

Доказательство:

Здесь и далее $p_1 = \frac{p-1}{2}$, $q_1 = \frac{q-1}{2}$.

По предыдущей теореме, $\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{x=1}^{q_1} [\frac{qx}{p}]}$, $\left(\frac{p}{q}\right) = (-1)^{\sum\limits_{y=1}^{p_1} [\frac{py}{q}]}$.

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{S_1+S_2},\ S_1 = \sum_{x=1}^{q_1} [\frac{qx}{p}],\ S_2 = \sum_{y=1}^{p_1} [\frac{py}{q}]$$

$p_1 \cdot q_1 = \{$количество пар (x, y), $x = 1, \ldots, p_1$, $y = 1, \ldots, q_1\} = \{$количество пар (qx, py), $x = 1, \ldots, p_1$, $y = 1, \ldots, q_1\}$

Заметим, что $qx \neq py$. Рассмотрим отдельно пары, где $qx < py$, и $py < qx$.

$qx < py \iff x < \frac{py}{q}$. Для каждого y таких x ровно $[\frac{py}{q}]$, а значит пар первого типа ровно S_2. Аналогичного, пар второго типа S_1. Подставляя, получим требуемое. ■

Билет 71

Показатели. Первообразные корни.

Def. Показатель (порядок) числа по модулю m — минимальное натуральное $\delta : a^\delta \equiv 1 \mod m$.

Def. первообразный корень по модулю m — такое число, что его показатель равен $\varphi(m)$.

Существование первообразного корня по модулю 2, 4, p

Утверждение. 1 – первообразный корень по модулю 2, 3 – первообразный корень по модулю 4.

Th. По простому модулю p существует первообразный корень.

Доказательство:

Пусть δ_i – показатель числа $i = 1, \dots, p-1$. Возьмём $\tau = [\delta_1, \dots, \delta_{p-1}]$ (НОК) и его каноническое разложение $\tau = q_1^{\alpha_1} \cdot \ldots \cdot q_s^{\alpha_s}$.

Утверждение. $\tau \geqslant p-1$. (Рассмотреть $x^\tau \equiv 1 \mod p$. Оно имеет корнями все числа от 1 до $p-1$)

Заметим, что для любого $i = 1, \dots, s$ существует $\delta \in \{\delta_1, \dots, \delta_{p-1}\}$, т.ч. $\delta = a_i q_i^{\alpha_i}$ (по определению НОК).

Утверждение. Пусть $x_i \in \{1, \dots, p-1\}$ имеет поакзатель $a_i q_i^{\alpha_i}$. Тогда $ord(x_i^{a_i}) = q_i^{\alpha_i}$.

Утверждение. $ord(x_1^{a_1} \cdot \ldots \cdot x_s^{a_s}) = \tau$. Следует из взаимопростоты показателей.

■

Билет 72

Показатели. Первообразные корни.

Def. Показатель (порядок) числа по модулю m — минимальное натуральное $\delta : a^\delta \equiv 1 \mod m$.

Def. первообразный корень по модулю m — такое число, что его показатель равен $\varphi(m)$.

Существование по модулю p^α, $\alpha \geqslant 2$: формулировка и доказательство леммы

Th. (Лемма): Пусть g — первообразный корень по модулю p. Тогда существует такое t, что $(g + pt)^{p-1} = 1 + pu_1$, где $(u_1, p) = 1$.

Доказательство:

$$(g+pt)^{p-1} = g^{p-1} + (p-1)g^{p-2}pt + p^2a = (1+pb) + p((p-1)g^{p-2}t + pa) = 1 + p((p-1)g^{p-2}t + b + pa)$$

Поскольку $(p-1)g^{p-2}t$ пробегает полную систему вычетов, можно подобрать такое t, что $u_1 = (p-1)g^{p-2}t + b + pa$ взаимопросто с p. ■

Th. Число $g+pt$ из предыдущей леммы является первообразным корнем по модулю p^α.

Существование по модулю $2p^\alpha$

Th. Первообразный корень по модулю $2p^\alpha$ существует.

Доказательство:

Число $g+pt$ из предыдущей леммы является первообразным корнем по модулю p^α. Заметим, что $\varphi(2p^\alpha) = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Если $g+pt$ нечётное, тогда оно взаимопросто с $2p^\alpha$ и $(g+pt)^{\varphi(2p^\alpha)} \equiv 1 \mod 2p^\alpha$. Если показатель $g+pt$ меньше, то $g+pt$ в степени этого показателя сравнимо с 1 по модулю p^α, чего не может быть.

Если же $g+pt$ чётное, то $g+pt+p^\alpha$ будет взаимопросто с $2p^\alpha$. Из тождества $(g+pt+p^\alpha)^\delta \equiv (g+pt)^\delta \mod p^\alpha$ следует, что $g+pt+p^\alpha$ является первообразным корнем по модулю $2p^\alpha$.

■

Билет 73

Показатели. Первообразные корни.

Def. Показатель (порядок) числа по модулю m — минимальное натуральное $\delta : a^\delta \equiv 1 \mod m$.

Def. первообразный корень по модулю m — такое число, что его показатель равен $\varphi(m)$.

Существование по модулю p^α, $\alpha \geqslant 2$: формулировка леммы(б/д) и вывод существования

Th. (Лемма): Пусть g — первообразный корень по модулю p. Тогда существует такое t, что $(g+pt)^{p-1} = 1 + pu_1$, где $(u_1, p) = 1$.

Th. Число $g+pt$ из предыдущей леммы является первообразным корнем по модулю p^α.

Доказательство:

Вспомним, что $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Пусть $\delta = ord(g+pt)$ показатель по модулю p^α. Тогда $\delta | (p-1)p^{\alpha-1}$. При этом $g^\delta \equiv (g+pt)^\delta \equiv 1 \mod p$, значит в силу первообразности $(p-1)|\delta$. Значит, $\delta = (p-1)p^k$. Проверим все такие k «ручками», пользуясь леммой.

$$(g+pt)^{p-1} = 1 + pu_1,\ gcd(p, u_1) = 1$$
$$(g+pt)^{(p-1)p} = (1+pu_1)^p = 1 + p^2u_1 + p^3a = 1 + p^2(u_1 + pa) = 1 + p^2u_2,\ gcd(p, u_2) = 1$$
$$(g+pt)^{(p-1)p^2} = 1 + p^3u_3, ; gcd(p, u_3) = 1$$
$$\dots$$
$$(g+pt)^{(p-1)p^{\alpha-2}} = 1 + p^{\alpha-1}u_{\alpha-1},\ gcd(p, u_{\alpha-1}) = 1$$

Как можно заметить, ни одно из этих чисел не может быть сравнимо с 1 по модулю p^α. Значит, $g+pt$ является первообразным корнем.

■

Существование по модулю $2p^\alpha$

Th. Первообразный корень по модулю $2p^\alpha$ существует.

Доказательство:

Число $g + pt$ из предыдущей леммы является первообразным корнем по модулю p^α. Заметим, что $\varphi(2p^\alpha) = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Если $g + pt$ нечётное, тогда оно взаимопросто с $2p^\alpha$ и $(g+pt)^{\varphi(2p^\alpha)} \equiv 1 \mod 2p^\alpha$. Если показатель $g+pt$ меньше, то $g+pt$ в степени этого показателя сравнимо с 1 по модулю p^α, чего не может быть.

Если же $g+pt$ чётное, то $g+pt+p^\alpha$ будет взаимопросто с $2p^\alpha$. Из тождества $(g+pt+p^\alpha)^\delta \equiv (g+pt)^\delta \mod p^\alpha$ следует, что $g + pt + p^\alpha$ является первообразным корнем по модулю $2p^\alpha$.

■

Билет 74

Показатели. Первообразные корни.

Def. Показатель (порядок) числа по модулю m — минимальное натуральное $\delta : a^\delta \equiv 1 \mod m$.

Def. первообразный корень по модулю m — такое число, что его показатель равен $\varphi(m)$.

Несуществование по модулю 2^n, $n \geqslant 3$

Th. Первообразного корня по модулю 2^n, $n \geqslant 3$, не существует.

Доказательство:

Рассмотрим произвольное нечётное $a = 1 + 2t$ (чётное смысла рассматривать не имеет, оно не взаимопросто, значит и не первообразный корень):

$$a^2 = 1 + 4t + t^2 = 1 + 4t(t+1) = 1 + 8u_0$$
$$a^4 = (1 + 8u_0)^2 = 1 + 16u_0 + 64u_0^2 = 1 + 16u_1$$
$$a^8 = 1 + 32u_2$$
$$\dots$$
$$a^{2^k} = 1 + 2^{k+2}u_{k-1}$$
$$\dots$$
$$a^{2^{n-2}} = 1 + 2^n u_{n-3}$$

Значит, показатель a не превосходит $2^{n-2} < 2^{n-1} = \varphi(2^n)$ и a не является первообразным корнем.

■

Билет 75

Показатели. Первообразные корни.

Def. Показатель (порядок) числа по модулю m — минимальное натуральное $\delta : a^\delta \equiv 1 \mod m$.

Def. первообразный корень по модулю m — такое число, что его показатель равен $\varphi(m)$.

Несуществование по модулям, отличным от 2^α, p^α, $2p^\alpha$

Th. Пусть $m = 2^\alpha p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $\alpha \geqslant 0$, $\alpha_i > 0$. Тогда первообразного корня по модулю m не существует.

Доказательство:

Определим минимальные показатели для получения 1 по соответствующим модулям:

$$c_0 = \begin{cases} 2^{\alpha-1}, & \alpha \leqslant 2 \\ 2^{\alpha-2}, & \alpha \geqslant 3 \\ 1, & \alpha = 0 \end{cases}, \quad c_i = \varphi(p_i^{\alpha_i}) = (p_i - 1)p_i^{\alpha_i - 1}$$

Рассмотрим $\tau = [c_0, c_1, \ldots, c_k]$. Пусть $gcd(a, m) = 1$. Тогда $a^\tau \equiv 1 \mod m$. В то же время $a^{\varphi(m)} \equiv 1 \mod m$. Если $\tau < \varphi(m)$, то m не имеет первообразного корня. Несложно заметить, что берется НОК чётных множителей $\varphi(m)$. Очевидно, он меньше $\varphi(m)$. ■

Билет 76

Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$

Здесь и далее будем подразумевать, что p — простое число.

Def. $\pi(x) = \sum\limits_{p \leqslant x} 1$

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

Def. $\psi(x) = \sum\limits_{p^\alpha \leqslant x} \ln p = \sum\limits_{p \leqslant x} \ln p [\frac{\ln x}{\ln p}]$

Th. (Постулат Бертрана) Для любого x отрезок $[x, 2x]$ содержит простое число.

Вопрос: насколько маленькой можно взять длину такого отрезка?

Th. Существует такое $c \in \mathbb{R}$, что для любого натурального x отрезок $[x, x + cx^{0.525}]$ содержит простое число.

Гипотеза. Можно взять длину отрезка $c \ln^2 x$.

Теорема о равенстве нижних и верхних пределов

$\lambda_1 = \overline{\lim\limits_{x \to \infty}} \frac{\theta(x)}{x}$ $\lambda_2 = \overline{\lim\limits_{x \to \infty}} \frac{\psi(x)}{x}$ $\lambda_3 = \overline{\lim\limits_{x \to \infty}} \frac{\pi(x)}{x/\ln x}$

За μ_i обозначим ссответствующие нижние пределы.

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

Доказательство:

$$\theta(x) = \sum_{p \leqslant x} \ln p \leqslant \sum_{p \leqslant x} \ln p [\frac{\ln x}{\ln p}] = \psi(x) \Rightarrow \frac{\theta(x)}{x} \leqslant \frac{\psi(x)}{x} \Rightarrow \lambda_1 \leqslant \lambda_2$$

$$\psi(x) = \sum_{p \leqslant x} \ln p [\frac{\ln x}{\ln p}] \leqslant \sum_{p \leqslant x} \ln x = \pi(x) \ln x \Rightarrow \frac{\psi(x)}{x} \leqslant \frac{\pi(x)}{x/\ln x} \Rightarrow \lambda_2 \leqslant \lambda_3$$

Рассмотрим $\alpha \in [0, 1)$

$$\theta(x) = \sum_{p \leqslant x} \ln p \geqslant \sum_{p^\alpha < p \leqslant x} \ln p > \sum_{p^\alpha < p \leqslant x} \ln (x^\alpha) = (\alpha \ln x) \cdot (\pi(x) - \pi(x^\alpha)) \geqslant (\alpha \ln x) \cdot (\pi(x) - x^\alpha) \Rightarrow$$
$$\frac{\theta(x)}{x} > (\alpha \ln x) \cdot \left(\frac{\pi(x)}{x} - x^{\alpha - 1} \right) = \alpha \left(\frac{\pi(x)}{x/\ln x} - \frac{\ln x}{x^{1-\alpha}} \right)$$

Перейдём к верхнему пределу в последнем неравенстве:

$$\lambda_1 \geqslant \alpha \lambda_3 \overset{\alpha \text{ произвольное}}{\Rightarrow} \lambda_1 \geqslant \lambda_3$$

Итого, $\lambda_1 = \lambda_2 = \lambda_3$. С нижними пределами аналогично. ■

Билеты 77-78

Распределение простых чисел в натуральном ряде. Функции $\pi(x)$, $\theta(x)$, $\psi(x)$

Здесь и далее будем подразумевать, что p — простое число.

Def. $\pi(x) = \sum\limits_{p \leqslant x} 1$

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

Def. $\psi(x) = \sum\limits_{p^\alpha \leqslant x} \ln p = \sum\limits_{p \leqslant x} \ln p [\frac{\ln x}{\ln p}]$

Th. (Постулат Бертрана) Для любого x отрезок $[x, 2x]$ содержит простое число.

Вопрос: насколько маленькой можно взять длину такого отрезка?

Th. Существует такое $c \in \mathbb{R}$, что для любого натурального x отрезок $[x, x + cx^{0.525}]$ содержит простое число.

Гипотеза. Можно взять длину отрезка $c \ln^2 x$.

Теорема Чебышёва

Th. $a\frac{x}{\ln x} \leqslant \pi(x) \leqslant b\frac{x}{\ln x}$, где $0 < a < b < \infty$.

Доказательство:

Утверждение теоремы приводится к виду $a \leqslant \frac{\pi(x)}{x/\ln x} \leqslant b$. Поэтому достаточно показать ограничение на λ_3 и μ_3. Покажем, что $\mu_3 \geqslant \ln 2$, $\lambda_3 \leqslant 4 \ln 2$.

1. Рассмотрим C_{2n}^n. Известно, что $C_{2n}^n < 2^{2n}$. Также:

$$C_{2n}^n = \frac{(2n)!}{(n!)^2} \geqslant \prod_{n<p\leqslant 2n} p \Rightarrow \sum_{n<p\leqslant 2n} \ln p \leqslant \ln C_{2n}^n < 2n \ln 2 \Rightarrow \theta(2n) - \theta(n) < 2n \ln 2$$

   Сложим такие неравенства для $n = 1, 2, 4, \ldots, 2^{k-1}$. Получим:

$$\theta(2^k) < 2 \cdot 2^k \ln 2 \Rightarrow \frac{\theta(2^k)}{2^k} < 2 \ln 2$$

   Из неубывания θ получим требуюмую оценку для λ_3.

2. Так как C_{2n}^n — наибольшая из цешек, выполнено $C_{2n}^n > \frac{2^{2n}}{2n+1}$.

$$\ln C_{2n}^n > 2n \ln 2 - \ln(2n+1)$$

$$C_{2n}^n = \frac{(2n)!}{(n!)^2} = \prod_{p\leqslant 2n} p^{[\frac{2n}{p}]+[\frac{2n}{p^2}]+\ldots-2\left([\frac{n}{p}]+[\frac{n}{p^2}]+\ldots\right)} \leqslant \prod_{p\leqslant 2n} p^{[\log_p(2n)]} = e^{\sum\limits_{p\leqslant 2n}\left[\frac{\ln 2n}{\ln p}\right]\ln p} = e^{\psi(2n)}$$

$$2n\ln 2 - \ln(2n+1) < \psi(2n)$$

Для произвольного x возьмём такое n, что $2n \leqslant x \leqslant 2n+1$. Тогда

$$\psi(x) \geqslant \psi(2n) > 2n\ln 2 - \ln(2n+1) \geqslant (x-1)\ln 2 - \ln(x+1)$$

Поделив и перейдя к нижнему пределу, получим требуемое.

■

Билет 79

Решетки в пространствах. Базис и определитель

Def. Пусть $e_1, \ldots, e_n$ — базис в $\mathbb{R}^n$. Тогда $\Lambda = \{a_1e_1 + \ldots + a_ne_n : a_i \in \mathbb{Z}\}$ называется решёткой.

Каждая решётка задаёт некоторую структуру в пространстве, разбивает пространство на ячейки.

Def. Число $\det\Lambda = |\det(e_1, \ldots, e_n)|$, т.е. объём одной такой ячейки, называется определителем решётки.

Утверждение. Определитель решётки не зависит от выбора базиса (свойство определителя и никаких цыганских фокуов).

Многомерная теорема Минковского (для произвольной решетки)

Th. Пусть $\Omega \subset \mathbb{R}^n$ — выпуклое, измеримое, симметричное относительно начала координат тело. Пусть Λ — решетка в $\mathbb{R}^n$, такая что $\mathrm{Vol}\,\Omega > 2^n \det\Lambda$. Тогда $(\Omega \cap \Lambda) \setminus \{0\} \neq \varnothing$.

Доказательство: Рассмотрим пересечение Ω и решётки $\frac{1}{p}\Lambda$ и обозначим N_p мощность пересечения. Поскольку Ω измеримое, то его объём можно сколь угодно близко приблизить значением $N_p \det(\frac{1}{p}\Lambda)$ *(KyKaPeK)* , т.е.:

$$\frac{N_p}{p^n}\det\Lambda \xrightarrow[p\to\infty]{} \mathrm{Vol}\,\Omega > 2^n\det\Lambda$$

Тогда для достаточно большого p выполнено $N_p > (2p)^n$. Рассмотрим две произвольные точки из этого пересечения: $a = \frac{a_1}{p}e_1 + \ldots + \frac{a_n}{p}e_n$ и $b = \frac{b_1}{p}e_1 + \ldots + \frac{b_n}{p}e_n$. Поскольку $N_p > (2p)^n$, то по принципу Дирихле можно выбрать такие различные точки, что $a_i \equiv b_i \mod 2p$. Тогда в силу выпуклости и симметричности Ω точка $\frac{a-b}{2}$ лежит в $\Omega \cap \Lambda$ и не совпадает с началом координат в силу различности a и b. ■

Билеты 80-82

Теорема Минковского–Главки и история ее улучшений

Хочется чтобы оценка 2^n в теореме Минковского была точной. Но мало ли чего хочется...

Th. (Минковский, Главка) Пусть $\Omega \subset \mathbb{R}^n$ — произвольное измеримое тело. Тогда существует решётка $\Lambda \subset \mathbb{R}^n$, такая что $(\Omega \cap \Lambda) \setminus \{0\} = \varnothing$ и в то же время $\frac{\operatorname{Vol}\Omega}{\det\Lambda} > \frac{1}{2}$.

Th. (Шмидт, Роджерс) В условиях предыдущей теоремы можно заменить $\frac{1}{2}$ на $c\sqrt{n}$.

Доказательство теоремы Минковского–Главки для октаэдра

Def. $O_n = \{\overline{x} : |x_1| + \ldots + |x_n| \leqslant 1\}$ — n-мерный октаэдр. Также является выпуклой оболочкой орт и противоположных им векторов.

Решётку для этого тело будем подбирать не произвольную, а следующего вида:

Def. Пусть $\overline{a} = \left(\frac{a_1}{p}, \ldots, \frac{a_n}{p}\right)$, где $(a_i, p) = 1$, p — нечетное простое. Тогда $\Lambda_{\overline{a}} = \{\overline{b} = \overline{a}l + \overline{c} : l \in \mathbb{Z}, \overline{c} \in \mathbb{Z}^n\}$.

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

Def. $S_{\overline{a}}$ — количество точек в $(O_n \cap \Lambda_{\overline{a}}) \setminus \{0\}$.

Посмотрим на ограничения на p в условиях теоремы Минковского:

$$\frac{\operatorname{Vol}\Omega}{\det\Lambda} > \frac{1}{2} \iff \frac{2^n}{n!}p > \frac{1}{2} \iff p > \frac{n!}{2^{n+1}}.$$

Посчитаем среднее число $S_{\overline{a}}$ для всевозможных $\overline{a}$. Если оно окажется меньше 1, то существует $\overline{a}$, для которого $S_{\overline{a}} = 0$.

$$\frac{1}{(p-1)^n}\sum_{\overline{a}} S_{\overline{a}} = \frac{1}{(p-1)^n}\sum_{a_1=1}^{p-1}\ldots\sum_{a_n=1}^{p-1} S_{\overline{a}} (< 1?)$$

Лемма.

$$S_{\overline{a}} = \sum_{l=1}^{p-1}\sum_{\overline{x}\in\left(O_n\cap\frac{1}{p}\mathbb{Z}^n\right)\setminus\{0\}} \delta(\overline{a}l - \overline{x}), \quad \delta(\overline{a}l-\overline{x}) = \begin{cases} 1, & \overline{a}l - \overline{x} \in \mathbb{Z}^n \\ 0, & \text{иначе} \end{cases}$$

Доказательство:

$$\delta(\overline{a}l - \overline{x}) = 1 \Rightarrow \overline{a}l - \overline{x} = \overline{c} \in \mathbb{Z}^n \Rightarrow \overline{x} = \overline{a}l - \overline{c} \in (O_n \cap \Lambda_{\overline{a}}) \setminus \{0\}$$

Проведём в обратную сторону: $\overline{x} \in (O_n \cap \Lambda_{\overline{a}}) \setminus \{0\} \Rightarrow \overline{x} = \overline{a}l + \overline{c}$, причём можно установить $l \in \{1, \ldots, p-1\}$ единственным образом. Тогда $\delta(\overline{a}l - \overline{x}) = \delta(-c) = 1$. ■

Вернёмся к среднему по всем возможным $\overline{a}$ и посчитаем его пользуясь леммой:

$$\frac{1}{(p-1)^n}\sum_{a_1=1}^{p-1}\cdots\sum_{a_n=1}^{p-1}S_{\overline{a}}=\frac{1}{(p-1)^n}\sum_{a_1=1}^{p-1}\cdots\sum_{a_n=1}^{p-1}\sum_{l=1}^{p-1}\sum_{\overline{x}\in\left(O_n\cap\frac{1}{p}\mathbb{Z}^n\right)\setminus\{0\}}\delta(\overline{a}l-\overline{x})=$$

$$=\frac{1}{(p-1)^n}\sum_{l=1}^{p-1}\sum_{\overline{x}\in\ldots}\left(\sum_{a_1=1}^{p-1}\cdots\sum_{a_n=1}^{p-1}\delta(\overline{a}l-\overline{x})\right)$$

Зафиксируем l и $\overline{x}$.

$$\delta(\overline{a}l-\overline{x})=1\iff\forall i\quad p|(a_il-x_i)$$

Поскольку $(l,p)=1$, a_il пробегает полную систему вычетов, а значит a_i можно выбрать единственным образом так, чтобы $\delta(\overline{a}l-\overline{x})=1$.

Тогда

$$\frac{1}{(p-1)^n}\sum_{a_1=1}^{p-1}\cdots\sum_{a_n=1}^{p-1}S_{\overline{a}}=\frac{1}{(p-1)^n}\sum_{l=1}^{p-1}\sum_{\overline{x}\in\ldots}1=\frac{p-1}{(p-1)^n}\left|\left(O_n\cap\frac{1}{p}\mathbb{Z}^n\right)\setminus\{0\}\right|$$

Посчитаем количество точек в этом множестве N_p. Сопоставим каждой из них кубик с ребром $\frac{1}{p}$ вершина с меньшими координатами которого лежит в этой точки. Тогда все эти кубики лежат внутри октаэдра, вершины которого сдвинуты на $\frac{2}{p}$.

$$\frac{N_p}{p^n}<\frac{2^n}{n!}\left(1+\frac{2}{p}\right)^n$$

Подставим:

$$\frac{1}{(p-1)^n}\sum_{a_1=1}^{p-1}\cdots\sum_{a_n=1}^{p-1}S_{\overline{a}}<\frac{1}{(p-1)^{n-1}}\frac{2^np^n}{n!}\left(1+\frac{2}{p}\right)^n=p\frac{p^{n-1}}{(p-1)^{n-1}}\frac{2^n}{n!}\left(1+\frac{2}{p}\right)^n$$

Вспомним, что хотим $p>\frac{n!}{2^{n+1}}$. Пользуясь знаниями о простых числах, при больших n можно выбрать $p\leqslant\frac{n!}{2^{n+1}}\cdot 1.1$.

$$\frac{1}{(p-1)^n}\sum_{a_1=1}^{p-1}\cdots\sum_{a_n=1}^{p-1}S_{\overline{a}}<\frac{n!}{2^{n+1}}\cdot 1.1\cdot\frac{2^n}{n!}\left(1-\frac{1}{p}\right)^{1-n}\left(1+\frac{2}{p}\right)^n=\left(1-\frac{1}{p}\right)^{1-n}\left(1+\frac{2}{p}\right)^n\cdot 0.55\to 0.55<1$$

Таким образом, существует $\overline{a}$, такое что $S_{\overline{a}}=0$.

Билет 83

Теорема Лиувилля

Th. Пусть α — алгебраическое число степени n. Тогда существует $c = c(\alpha)$, такое что неравенство $\left|\alpha - \frac{p}{q}\right| \leqslant \frac{c}{q^n}$ не имеет решений в рациональных $\frac{p}{q}$.

Доказательство: Пусть $f(x) = a_n x^n + \ldots + a_0$ — минимальный многочлен для α; $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ — корни этого многочлена, $f(x) = a_n(x-\alpha)\prod\limits_{i=2}^{n}(x-\alpha_i)$.

Рассмотрим произвольную рациональную дробь $\frac{p}{q}$ (будем считать неотрицательной для простоты).

1. $\left|\alpha - \frac{p}{q}\right| \geqslant 1 > \frac{1}{q^n}$
2. $\left|\alpha - \frac{p}{q}\right| < 1$. Тогда $1 > \left|\alpha - \frac{p}{q}\right| \geqslant \frac{p}{q} - |\alpha|$, значит $\frac{p}{q} < |\alpha| + 1$.

   Подставим $\frac{p}{q}$ в f.

$$0 \neq f\left(\frac{p}{q}\right) = a_n\frac{p^n}{q^n} + \ldots + a_1\frac{p}{q} + a_0 = \frac{a}{q^n} \Rightarrow \left|f\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{q^n}$$

$$\left|f\left(\frac{p}{q}\right)\right| = a_n\left|\alpha - \frac{p}{q}\right|\prod_{i=2}^{n}\left|\frac{p}{q} - \alpha_i\right| \leqslant a_n\left|\alpha - \frac{p}{q}\right|\prod_{i=2}^{n}\left(\frac{p}{q} + |\alpha_i|\right) < a_n\left|\alpha - \frac{p}{q}\right|\prod_{i=2}^{n}(|\alpha| + |\alpha_i| + 1)$$

Возьмём $c = \frac{1}{a_n\prod\limits_{i=2}^{n}(|\alpha|+|\alpha_i|+1)}$, получим требуемое.

■

Билеты 84-86

Тождество Эрмита

Th. Пусть есть многочлен $f(x)$ степени n. Тогда

$$\int_0^x f(t)e^{-t}dt = F(0) - F(x)e^{-x}, \quad F(x) = f(x) + f'(x) + \ldots + f^{(n)}(x)$$

Доказательство: Кучу раз берем по частям. ■

В частности, для любого натурального k верно:

$$F(0)e^k - F(k) = e^k\int_0^k f(t)e^{-t}dt$$

Remind. Если f — многочлен с целыми коэффициентами, то все коэффициенты $f^{(k)}$ делятся на $k!$.

Доказательство трансцендентности e

Предположим, что e алгебраическое степени m: $a_m e^m + \ldots + a_1 e + a_0 = 0$. Будем применять тождество Эрмита к следующему многочлену (n — большое натуральное число):

$$f(x) = \frac{1}{(n-1)!} x^{n-1}((x-x_1)(x-x_2)\ldots(x-x_m))^n$$

.

Просуммируем тождества Эрмита для $k \in \{0, 1, \ldots, m\}$ с коэффициентами a_k. Пользуясь уравнением на e, получим:

$$-\sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt$$

Наша цель: показать, что при большом n левая часть — ненулевое целое число, а правая часть строго меньше 1.

Свойства многочлена f:

1. $f^{(l)}(0) = 0$ при $l \in \{0, \ldots, n-2\}$
2. $f^{(n-1)}(0) = (-1)^{mn}(m!)^n$
3. $f^{(l)}(k) = 0$ при $l \in \{0, \ldots, n-1\}$, $k \in \{1, \ldots, m\}$
4. $f^{(l)}$, $l \geqslant n$, являются многочленами с целыми коэффициентами, делящимися на n (по напоминанию выше)

Тогда $F(x) = f(x) + f'(x) + \ldots$ обладает следующими свойствами:

1. $F(0) = (-1)^{mn}(m!)^n + nA$
2. $F(k) = nB_k$, $k \in \{1, \ldots, m\}$

Возьмем n такое, что $(n, m!) = 1$, $n > |a_0|$ и вернемся к исследуемому тождеству:

$$-\sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt$$

$a_0 F(0) = a_0(-1)^{mn}(m!)^n + nAa_0$ — не делится на n, а $F(k)$ — делится. Значит, левая часть — целое число, не делящееся на n, значит $\left|\sum\limits_{k=0}^{m} a_k F(k)\right| \geqslant 1$.

На отрезке $[0, m]$ каждый из множителей в f можно оценить числом m по модулю. Тогда:

$$\left|\sum_{k=0}^{m} a_k e^k \int_0^k f(t)e^{-t}dt\right| < \frac{m^{(m+1)n}}{(n-1)!} e^m \sum_{k=0}^{m} |a_k| = c_0 \frac{c_1^n}{(n-1)!} \xrightarrow[n\to\infty]{} 0$$

Желаемое противоречие получено.

Additional information

Архив ОКТЧ

Программа

Конспект Саши Маркова