ТЧ-8 2024

SFS, AAG, PNS

23 июня 2024 г.

При нахождении ошибок обращайтесь @fedorrrMM

Содержание

1 Билеты

1. Билет 1 Простейшие свойства делимости. Представление наибольшего общего делителя d чисел a и b в форме $d = au + bv$. Теорема о существовании и единственности разложения на простые сомножители. Бесконечность множества простых чисел.

2. Билет 2 Лемма о равенстве верхних и нижних пределов функций $(\theta(x)/x, \psi(x)/x$ и $(\pi(x)\ln(x))/x)$. Связь между асимптотическим поведением функции Чебышева $\psi(x)$ и сходимостью интеграла

$$\int_1^\infty \frac{\psi(x) - x}{x^2} dx$$

3. Билет 3 Оценки Чебышева функции $\pi(x)$. Оценки n-го простого числа. Расходимость ряда $\sum_p \frac{1}{p}$.

4. Билет 4 Аналитичность дзета-функции Римана в области $\sigma > 1$. Разложение в ряд Дирихле ее логарифмической производной. Представление дзета-функции в виде бесконечного произведения.

5. Билет 5 Преобразование Абеля в интегральной форме. Аналитическое продолжение дзета-функции в область $\sigma > 0$.

6. Билет 6 Отсутствие нулей дзета-функции в области $\sigma \geq 1$.

7. Билет 7 Формулировка асимптотического закона распределения простых чисел. Сведение его доказательства к исследованию некоторого комплексного интеграла.

8. Билет 8 Доказательство асимптотического распределения распределения простых чисел. Асимптотическая формула n-го простого числа.

9. Билет 9 Простейшие свойства сравнений. Группа $(Z/mZ)^*$. Теорема Эйлера. Малая теорема Ферма. Элементарные доказательства бесконечности множества простых чисел в прогрессиях вида $4n+1$ и $4n+3$.

10. Билет 10 Простейшие свойства групповых характеров. Построение характеров. Вычисление сумм $\sum_{a \in G} \chi(a)$ и $\sum_\chi \chi(a)$ для характеров χ группы G. Определение и свойства числовых характеров.

11. Билет 11 Аналитичность функции Дирихле $L(s, \chi)$ в области $\sigma > 1$. Разложение в ряд Дирихле ее логарифмической производной. Отсутствие нулей L-функции в области $\sigma > 1$. Представление L-функции в виде бесконечного произведения. Аналитическое продолжение функции $L(s, \chi_0)$ в область $\sigma > 0$.

12. Билет 12 Теорема о почленном дифференцировании ряда Дирихле. Область аналитичности функции $L(s, \chi)$ при $\chi \neq \chi_0$.

13. Билет 13 Теорема об области сходимости ряда Дирихле с неотрицательными коэффициентами.

14. Билет 14 Неравенство $L(1, \chi) \neq 0$ для действительного характера χ.

15. Билет 15 Неравенство $L(1, \chi) \neq 0$ при $\chi^2 \neq \chi_0$.

16. Билет 16 Доказательство теоремы Дирихле о бесконечности множества простых чисел в арифметической прогрессии.

17. Билет 17 Свойства минимального многочлена алгебраического числа. Целые алгебраические числа. Лемма Гаусса и ее следствия, относящиеся к целым алгебраическим числам.

18. Билет 18 Формулировка основной теоремы о симметричных многочленах. Теорема о симметричном многочлене от нескольких систем сопряженных алгебраических чисел. Поле алгебраических чисел и кольцо целых алгебраических чисел. Алгебраическая замкнутость поля алгебраических чисел.

19. Билет 19 Алгебраическое числовое поле конечной степени. Каноническая форма представления его элементов. Теорема о числах, сопряженных в алгебраическом числовом поле. Теорема о примитивном элементе.

20. Билет 20 Две теоремы о приближении действительных чисел рациональными дробями. Построение чисел, имеющих заданный порядок приближений.

21. Билет 21 Теорема Лиувилля о приближении алгебраических чисел. Построение трансцендентных чисел при помощи теоремы Лиувилля.

22. Билет 22 Обобщение теоремы Лиувилля на многочлены от нескольких алгебраических чисел.

23. Билет 23 Теорема Бореля о характере приближений “почти всех”действительных чисел.

24. Билет 24 Иррациональность и трансцендентность числа e.

25. Билет 25 Иррациональность числа π.

26. Билет 26 Лемма Зигеля об оценках решений систем линейных уравнений с целыми коэффициентами.

27. Билет 27 Формулировка теоремы Линдемана. Ее следствия. Построение вспомогательной функции для доказательства теоремы Линдемана, оценки ее порядка нуля.

28. Билет 28 Оценки вспомогательной функции и завершение доказательства теоремы Линдемана. Ее связь с проблемой квадратуры круга.

29. Билет 29 Седьмая проблема Гильберта. Формулировка теоремы Гельфонда-Шнейдера. Ее следствия. Построение вспомогательной функции для доказательства теоремы Гельфонда-Шнейдера, оценки ее порядка нуля.

30. Билет 30 Оценки вспомогательной функции и завершение доказательства теоремы Гельфонда-Шнейдера.

Билет 1

Простейшие свойства делимости. Представление наибольшего общего делителя d чисел a и b в форме $d = au + bv$. Теорема о существовании и единственности разложения на простые сомножители. Бесконечность множества простых чисел.

Простейшие свойства делимости.

Определение 1 $b \mid a$, если $\exists q \in \mathbb{Z} : a = bq$

Свойства делимости:

1. $b \mid a_1, \ldots, b \mid a_n \Rightarrow b \mid (a_1 + \cdots + a_n)$
2. $b \mid a_1, \ldots, b \mid a_{n-1}, b \nmid a_n \Rightarrow b \nmid (a_1 + \cdots + a_n)$
3. $c \mid a, d \mid b \Rightarrow cd \mid ab$, в частности, $\forall b : c \mid a \Rightarrow c \mid ab$

Теорема 1 (Основная теорема арифметики)

1. всякое $a \in \mathbb{N}, a > 1$ представляется в виде $a = p_1 \cdots p_n$, где p_i простые.
2. это представление единственно с точностью до порядка сомножителей.

▶ 1) индукция по a:
для $a = 2$ верно
пусть верно для всех чисел, меньших a
если a простое, то очевидно
иначе $a = bc$, где $1 < b, c < a$, откуда по предположению индукции получаем $a = \underbrace{q_1 \cdots q_n}_{=b} \underbrace{p_1 \cdots p_m}_{=c}$

2) Предположим, что существуют числа, которые не единственным образом раскладываются на простые сомножители. В не пустом подмножестве натурального ряда существует минимальный элемент. Пусть это будет $a = p_1 \cdots p_m = q_1 \cdots q_n$
Если $p_i = q_j$, то $\frac{a}{p_i}$ раскладывается двумя способами $\Rightarrow$ противоречие
Без ограничения общности пусть $p_1 > q_1$

Рассмотрим $b = \overbrace{(p_1 - q_1)}^{>0} p_2 \cdots p_m = p_1 \cdots p_m - q_1 p_2 \cdots p_m = q_1 \cdots q_n - q_1 p_2 \cdots p_m = q_1(q_2 \cdots q_n - p_2 \cdots p_m)$

Билет 1

Пусть теперь $p_1 - q_1 = u_1 \cdots u_s \qquad q_2 \cdots q_n - p_2 \cdots p_m = v_1 \cdots v_t$
$b = u_1 \cdots u_s p_2 \cdots p_m = v_1 \cdots v_t q_1$ – два различных разложения. В первое не входит q_1, т.к. $(p-q) \nmid q$
$b < a$, что противоречит минимальности a. ◄

Определение 2 $a \in \mathbb{Z}, b \in \mathbb{N} \Rightarrow \exists! q, r : \begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$ –деление с остатком

$$\exists : \frac{a}{b} = \left[\frac{a}{b}\right] + \left\{\frac{a}{b}\right\} \Rightarrow a = b \overbrace{\left[\frac{a}{b}\right]}^{q} + \underbrace{\left\{\frac{a}{b}\right\}}_{r}$$

! : все определено однозначно.

(a,b) – НОД

Теорема 2 (Теорема о представлении НОД)
$(a,b) = d \Rightarrow \exists u, v \in \mathbb{Z} : d = au + bv$

► $\mu = \{k \mid k = ax + by > 0, x, y \in \mathbb{Z}\}$

1. $\mu \neq \varnothing$, т.к. $\pm a; \pm b \in \mu$
2. d – наименьший элемент μ
3. Докажем, что $d \mid a$ и $d \mid b$
   Пусть $d \nmid a \Rightarrow a = dq + r, 0 < r < d, r = a - dq = a - (qu + bv)q = a(1 - qu) + b(-qu) \in \mu$, но $r < d$ противоречие.
4. $d = (a,b)$, т.к. если $\exists d_1 : d_1 \mid a, d_1 \mid b \Rightarrow d_1 \mid d \Rightarrow d_1 \le d$

◄

Следствия:

1. $c \mid ab, (c,a) = 1 \Rightarrow c \mid b$ ► $\exists u, v : au + cv = 1 \Rightarrow \underbrace{ab}_{\vdots c} u + \underbrace{bc}_{\vdots c} v = b \vdots c$ ◄
2. $b \mid a, c \mid a, (b,c) = 1 \Rightarrow bc \mid a$ ► $\exists u, v : bu + cv = 1 \quad u\underbrace{(ab)}_{\vdots bc} + \underbrace{(ac)}_{\vdots bc} v = a \vdots bc$ ◄

Билет 1

Другая формулировка теоремы единственности: $a = p_1^{k_1} \cdots p_n^{k_n} = p_1^{l_1} \cdots p_n^{l_n} \Rightarrow \forall i : k_i = l_i$

Утверждение 1 Пусть $a = p_1^{k_1} \cdots p_n^{k_n}, b = p_1^{l_1} \cdots p_n^{l_n}$. Тогда $b \mid a \iff \forall i : l_i \leq k_i$

►$\Rightarrow$: $b \mid a \Rightarrow a = bc, c = p_1^{m_1} \cdots p_n^{m_n} \Rightarrow a = p_1^{l_1+m_1} \cdots p_n^{l_n+m_n} \Rightarrow \forall i : k_i = l_i + m_i \geq l_i$

$\Leftarrow$: $a = b \cdot p_1^{k_1-l_1} \cdots p_n^{k_n-l_n} \Rightarrow a \vdots b$ ◄

Утверждение 2 $(a,b) = p_1^{s_1} \cdots p_n^{s_n}$, где $s_j = \min\{k_j, l_j\}$
$[a,b] = p_1^{t_1} \cdots p_n^{t_n}$, где $t_j = \max\{k_j, l_j\}$

►

1. $d \mid a, d \mid b, d = p_1^{r_1} \cdots p_n^{r_n} \Rightarrow r_i \leq k_i, r_i \leq l_i \Rightarrow r_i \leq \min\{k_j, l_j\} \Rightarrow \max r_i = \min\{k_j, l_j\}$
2. Аналогично.

◄

Теорема 3 (Теорема о бесконечности простых чисел)
Простых чисел бесконечно много.

► Пусть простых чисел конечное множество: $p_1, \ldots, p_n$. Рассмотрим $N = p_1 \cdot p_2 \cdots p_n + 1$ – составное
По теореме о разложении должно существовать $p : p \mid N$, но по построению N, оно не делится на все p_i ◄

Билет 2

Лемма о равенстве верхних и нижних пределов функций $(\theta(x)/x, \psi(x)/x$ и $(\pi(x)\ln(x))/x)$. Связь между асимптотическим поведением функции Чебышева $\psi(x)$ и сходимостью интеграла $\int\limits_1^\infty \frac{\psi(x)-x}{x^2}dx$

$\pi(x) := \sum\limits_{p\le x} 1$ – число простых не превосходящих x

$\theta(x) := \sum\limits_{p\le x} \ln(p)$ – функция Чебышева

$\psi(x) := \sum\limits_{p^k\le x} \ln(p) = \sum\limits_{p\le x} \left[\frac{\ln x}{\ln p}\right] \ln(p) = \sum\limits_{n\le x} \Lambda(n)$

$\Lambda(n) = \begin{cases} \ln(p), n = p^k \\ 0 \end{cases}$ – функция Мангольта.

$e^{\psi(n)} = [1,\dots,n]$

Обозначим

$\overline{\lim\limits_{x\to\infty}} \frac{\theta(x)}{x} = L_1, \underline{\lim\limits_{x\to\infty}} \frac{\theta(x)}{x} = l_1$

$\overline{\lim\limits_{x\to\infty}} \frac{\psi(x)}{x} = L_2, \underline{\lim\limits_{x\to\infty}} \frac{\psi(x)}{x} = l_2$

$\overline{\lim\limits_{x\to\infty}} \frac{\pi(x)\ln(x)}{x} = L_3, \underline{\lim\limits_{x\to\infty}} \frac{\pi(x)\ln(x)}{x} = l_3$

Лемма 1 $0 \le l_1 = l_2 = l_3 \le L_1 = L_2 = L_3 \le +\infty$

▶ $\frac{\theta(x)}{x} \le \frac{\psi(x)}{x} \le \frac{\pi(x)\ln(x)}{x}$ – очевидно, значит $L_1 \le L_2 \le L_3$

Докажем, что $L_3 \le L_1$

Выберем $0 < \alpha < 1$

$\theta(x) \ge \sum\limits_{x^\alpha < p \le x} \ln(p) \ge (\ln(x^\alpha)) \sum\limits_{x^\alpha < p \le x} 1 = (\alpha\ln(x))(\pi(x) - \pi(x^\alpha)) \ge \ln(x)(\pi(x) - x^\alpha)$

$\Rightarrow \frac{\theta(x)}{x} \ge \alpha\frac{\pi(x)\ln(x)}{x} - \alpha\overbrace{\frac{\ln(x)}{x^{1-\alpha}}}^{\to 0}$. При переходе к пределу: $L_1 \ge \alpha L_3$, при $\alpha \to 1 : L_1 \ge L_3 \Rightarrow L_1 = L_2 = L_3$

С нижними пределами аналогично.◀

Утверждение 3 $f(x)$ неубывающая на $[1;\infty] \Rightarrow$ если $\int\limits_1^\infty \frac{f(x)-x}{x^2}dx$ сходится то $f(x) \sim x, x \to \infty$

Билет 2

► Предположим противное. $\lim\limits_{x\to\infty}\frac{f(x)}{x}\neq 1\Rightarrow\exists\delta>0:\forall A>1\exists y>A:a)f(y)>(1+\delta)y;b)f(y)<(1-\delta)y$

$a)\int\limits_{y}^{(1+\delta)y}\frac{f(x)-x}{x^2}dx\geq\int\limits_{y}^{(1+\delta)y}\frac{f(y)-x}{x^2}dx>\int\limits_{y}^{(1+\delta)y}\frac{(1+\delta)y-x}{x^2}dx=\int\limits_{1}^{1+\delta}\frac{(1+\delta)y-ty}{t^2y^2}ydt=\int\limits_{1}^{1+\delta}\frac{1+\delta-t}{t^2}dt=\varepsilon>0\Rightarrow$ отрицание критерия Коши.

$b)\int\limits_{(1-\delta)y}^{y}\frac{f(x)-x}{x^2}dx\leq\int\limits_{(1-\delta)y}^{y}\frac{f(y)-x}{x^2}dx\leq\int\limits_{(1-\delta)y}^{y}\frac{(1-\delta)y-x}{x^2}dx=\int\limits_{1-\delta}^{1}\frac{1-\delta-t}{t^2}dt=-\varepsilon<0$

Критерий Коши: $\forall\varepsilon>0\exists A>1:\forall y:|\int dx|<\varepsilon$, тогда интеграл сходится. ◄

Таким образом, если $\int\limits_{1}^{\infty}\frac{\psi(x)-x}{x^2}dx$ сходится $\Rightarrow\psi(x)\sim x\Rightarrow\lim\limits_{x\to\infty}\frac{\psi(x)}{x}=1$

Билет 3

Оценки Чебышева функции $\pi(x)$. Оценки n-го простого числа. Расходимость ряда $\sum_p \frac{1}{p}$

Теорема 4 (Теорема Чебышева)
$\exists a,b>0 : \forall x \geq 2 : \quad a\frac{x}{\ln(x)} < \pi(x) < b\frac{x}{\ln(x)}$

► На отрезке $[2,N]$ (компакте), для $\forall N \in \mathbb{N}, N>2$ функция $\frac{\pi \ln(x)}{x}$ ограничена и непрерывна. Значит достигает своего минимума и максимума. Теперь докажем для предельного случая.
Сверху: $2^{2n} > C_{2n}^n = \frac{(n+1)\cdots(n+n)}{n!} \geq \prod\limits_{n<p\leq 2n} p$, в числитель входят все простые $n < p \leq 2n$
Логарифмируем неравенство:
$2n\ln(2) > \sum\limits_{n<p\leq 2n} \ln(p) = \theta(2n) - \theta(n)$. Рассмотрим $n = 2^k$
$\theta(2^k) = \sum\limits_{i=0}^{k-1} (\theta(2^{i+1}) - \theta(2^i)) < \sum\limits_{i=0}^{k-1} 2^{i+1}\ln(2) < \ln(2)\cdot 2^{k+1}$
$\theta(x)$ неубывающая $\Rightarrow \theta(x) \leq \theta(2^m) < 2^{m+1}\ln(2) = 4\cdot 2^{m-1}\ln(2) \leq 4\ln(2)x \Rightarrow$ подойдет $b = 4\ln(2)$

Снизу: $0 < I_n = \int\limits_0^1 x^n(1-x)^n dx < \left(\frac{1}{4}\right)^n \qquad x^n(1-x)^n = a_0 + a_1 x + a_2 x^2 + \cdots +$
$a_{2n}x^{2n} \Rightarrow I_n = \frac{a_0}{1} + \cdots + \frac{a_{2n}}{2n+1}$
Пусть $Q_{2n+1} := [1,2,\ldots,2n+1] \Rightarrow Q_{2n+1}I_n \in \mathbb{Z}, Q_{2n+1}I_n > 0 \Rightarrow 1 \leq Q_{2n+1}I_n \leq e^{\psi(2n+1)}\left(\frac{1}{4}\right)^n$
$\Rightarrow \psi(2n+1) > 2n\ln(2), \qquad \psi(x) \geq \psi(2(\left[\frac{x}{2}\right]-1)+1) > 2(\left[\frac{x}{2}\right]-1)\ln(2) > (x-4)\ln(2) > x\ln(2) \Rightarrow$ подойдет $a = \ln(2)$ ◄

Утверждение 4 $\alpha n\ln(n) < p_n < \beta n\ln(n)$

► $a\frac{p_n}{\ln(p_n)} < \pi(p_n) < b\frac{p_n}{\ln(p_n)}$
Логарифмируем:
$\ln(p_n) - \ln(\ln(p_n)) + \ln_a < \ln(n) < \ln(p_n) - \ln(\ln(p_n)) + \ln(b)$
$\Rightarrow p_n < a\frac{p_n}{\ln(p_n)}(\ln(p_n) - \ln(\ln(p_n)) + \ln(a)) < n\ln(n) < b\frac{p_n}{\ln(p_n)}(\ln(p_n) - \ln(\ln(p_n)) + \ln(b))$
$\Rightarrow \frac{1}{b}n\ln(n) < p_n < \frac{1}{a}n\ln(n)$ ◄

Теорема 5 (Теорема Эйлера)
$\sum_p \frac{1}{p}$ расходится.

Билет 3

► $S_N = \prod\limits_{p \le N} (1 - \frac{1}{p})^{-1} = \prod\limits_{p \le N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \sum\limits_{\substack{p \le N \\ p|n}} > \sum\limits_{n=1}^{N} \frac{1}{n}$ – частичная сумма гармонического ряда.

$\Rightarrow S_N \to \infty, N \to \infty \Rightarrow \lim\limits_{N \to \infty} \ln(S_N) = \infty$

$\sum\limits_p [-\ln(1 - \frac{1}{p})]$ расходится.

При $p \to \infty : -\ln(1 - \frac{1}{p}) \sim \frac{1}{p}$, значит по признаку сравнения ряды сходятся и расходятся одновременно.◄

Следствие – бесконечность множества простых чисел.

Оценки n-того простого числа. $\pi(p_n) = n$

Утверждение 5 $\alpha n \ln(n) < p_n < \beta n \ln(n)$

► $a\frac{p_n}{\ln(p_n)} < \pi(p_n) < b\frac{p_n}{\ln(p_n)}$

$\ln(p_n) - \ln(\ln(p_n)) + \ln_a < \ln(n) < \ln(p_n) - \ln(\ln(p_n)) + \ln(b)$

$\Rightarrow p_n < a\frac{p_n}{\ln(p_n)}(\ln(p_n) - \ln(\ln(p_n)) + \ln(a)) < n\ln(n) < b\frac{p_n}{\ln(p_n)}(\ln(p_n) - \ln(\ln(p_n)) + \ln(b))$

$\Rightarrow \frac{1}{b} n \ln(n) < p_n < \frac{1}{a} n \ln(n)$ ◄

Другое доказательство:

► $\frac{1}{p_n} > \frac{1}{\beta} n \ln(n) \Rightarrow$ [по интегральному признаку Коши ряды сходятся/расходятся одновременно] $\Rightarrow \int_{\alpha}^{+\infty} \frac{dx}{x\ln(x)} = \ln(\ln(+\infty)) - \ln(\ln(\alpha)) = +\infty$ ◄

Билет 4

Аналитичность дзета-функции Римана в области $\sigma > 1$. Разложение в ряд Дирихле ее логарифмической производной. Представление дзета-функции в виде бесконечного произведения.

Определение 3 Дзета-функция Римана: $s = \sigma + it, \quad \zeta(s) := \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$

1. при $\sigma > 1$ ряд сходится абсолютно
   $\left|\frac{1}{n^s}\right| = \frac{1}{n^\sigma} < \frac{1}{n^{1+\delta}}$
2. $\forall \delta > 0$ ряд равномерно сходится при $\sigma > 1 + \delta$ (по признаку Вейерштрасса)
3. $\zeta(s)$ –аналитическая функция при $\sigma > 1$
   по теореме Вейерштрасса из равномерной сходимости следует что можно почленно дифференцировать.

Теорема 6
$\sigma > 1 : -\frac{\zeta'(s)}{\zeta(s)} = \sum\limits_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$

►

Лемма 2
$f(n)$ – вполне мультипликативная, $A = \sum\limits_{k=1}^{\infty} f(k); \qquad B = \sum\limits_{d=1}^{\infty} f(d)\Lambda(d)$ – абсолютно сходятся. Тогда $AB = \sum\limits_{n=1}^{\infty} f(n)\ln(n)$

► $AB = \sum\limits_{k=1}^{\infty}\sum\limits_{d=1}^{\infty} f(k)f(d)\Lambda(d) = \sum\limits_{n=1}^{\infty} f(n)\sum\limits_{d|n}\Lambda(d)$

$\sum\limits_{d|n}\Lambda(d) = \sum\limits_{j=1}^{m}\sum\limits_{t_j}^{r_j}\Lambda(p_j^{t_j}) = r_1\ln(p_1) + \cdots r_m\ln(p_m) = \ln(n)$ ◄

$\zeta(s)\sum\limits_{d=1}^{\infty}\frac{\Lambda(d)}{d^s} = \sum\limits_{n=1}^{\infty}\frac{\ln(n)}{n^s} = -\zeta'(s)$ ◄

Теорема 7
В области $\sigma > 1 : \zeta(s) = \prod\limits_{p}(1 - \frac{1}{p^s})^{-1}$

►

Билет 4

Лемма 3
$f(n)$ – вполне мультипликативная, ряд $\sum f(n)$ абсолютно сходится $\Rightarrow S = \sum\limits_{n=2}^{\infty} f(n) = \prod\limits_{p}(1-f(p))^{-1}$

► $P(x) = \prod\limits_{p\le x}(1-f(p))^{-1} \Rightarrow \forall n \in \mathbb{N} : |f(n)| < 1$, иначе $|f(n^k)| = |f(n)|^k$ и сумма расходится

$$P(x) = \prod_{p\le x}(1+f(p)+f^2(p)+\cdots) = \sum_{p_i\le x} f(p_1^{k_1}\cdots p_n^{k_n}) = \sum_{\forall p|n\Rightarrow p\le x}{}' f(n)$$

$$|S-P(x)| \le \sum_{\exists p|n:p>x}{}'' |f(n)| \le \sum n \ge x|f(n)| < \varepsilon$$

$\Rightarrow \lim\limits_{x\to\infty} P(x) = S$ ◄

$f(n) = \frac{1}{n^s}, s = \sigma + it, \sigma > 1 \Rightarrow$ по лемме все доказано. ◄

Билет 5

Преобразование Абеля в интегральной форме. Аналитическое продолжение дзета-функции в область $\sigma > 0$.

Теорема 8 Преобразование Абеля. $\sum\limits_{n\le x} a_n g(n), a_n \in \mathbb{C}, g(x)$ – комплекснозначная функция действительного аргумента.
$x \in [1,+\infty); \exists$ непрерывная $g'(x)$, $\sum\limits_{n\le x} a_n = A(x)$

1. $\sum\limits_{n\le x} a_n g(n) = A(x)g(x) - \int\limits_1^x A(t)g'(t)dt$
2. если $\lim\limits_{x\to\infty} A(x)g(x) = 0$, то $\sum\limits_{n=1}^{\infty} a_n g(n) = \int\limits_1^{\infty} A(t)g'(t)dt$

$\blacktriangleright$ 1)$x \in \mathbb{Z}$: $\sum\limits_{n=1}^{N} a_n g(n) = \sum\limits_{n=1}^{N} (A(n) - A(n-1))g(n) = \sum\limits_{n=1}^{N} A(n)g(n) - \sum\limits_{n=0}^{N-1} A(n)g(n+1) =$
$A(N)g(N) - \sum\limits_{n=1}^{N-1} (g(n+1) - g(n))A(n) = A(N)g(N) - \int\limits_1^N A(t)g'(t)dt$
$A(0) = 0$

2)$x \notin \mathbb{Z}: N = [x]$
Достаточно проверить, что при вычитании с обеих сторон одного и того же числа
$\sum\limits_{n\le x} a_n g(n) - \sum\limits_{n=1}^{[x]} a_n g(n) = 0$
$A(N)(g(x) - g(N)) = \int\limits_N^x A(N)g'(t)dt = A(N)\int\limits_N^x dg(t) \Rightarrow$ всё $\blacktriangleleft$

Аналитическое продолжение дзета-функции.
$\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s} =$
$//g(x) = x^{-s}, a_n = 1, A(x) = [x]$
$= s\int\limits_1^{\infty} \frac{[x]}{x^{s+1}}dx = s\int\limits_1^{\infty} \frac{x-\{x\}}{x^{s+1}}dx \Rightarrow \zeta(s) = 1 + \frac{1}{s-1} - s\int\limits_1^{\infty} \frac{\{x\}}{x^{s+1}}dx$

Рассмотрим $\int\limits_1^{\infty} \frac{\{x\}}{x^{s+1}}dx = \sum\limits_{n=1}^{\infty} \int\limits_n^{n+1} \frac{\{x\}}{x^{s+1}}dx = \sum\limits_{n=1}^{\infty} I_n(x)$ – сходится в области $\sigma > \delta > 0$, т.к. $|I_n(s)| \le \frac{1}{n^{\delta+1}}$ сходится по признаку Вейерштрасса.
$I_n(s) \to \ln\frac{n+1}{n}$ при $s \to 1$
В точке $s = 1$ полюс первого порядка. Функция аналитична в области $\sigma > 0$ за исключением одной особой точки 1.$\blacktriangleleft$

Билет 6

Отсутствие нулей дзета-функции в области $\sigma \geq 1$.

Лемма 4 $\forall 0 < r < 1, \varphi \in \mathbb{R} \Rightarrow M = \left|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})\right| \leq 1$

► $\ln(M) = 3\ln(1-r) + 4\ln(|1-re^{i\varphi}|) + \ln(|1-re^{2i\varphi}|) = Re(3\ln(1-r) + 4\ln(1-re^{i\varphi}) + \ln(1-re^{2i\varphi})) = -\sum\limits_{n=1}^{\infty} \frac{r^n}{n} Re(3 + 4e^{in\varphi} + e^{2in\varphi}) = \sum\limits_{n=1}^{\infty} \frac{r^n}{n}(3 + 4\cos(n\varphi) + \cos(2n\varphi)) = -2\sum\limits_{n=1}^{\infty} \frac{r^n}{n}(\cos(n\varphi)+1)^2$ ◄

Лемма 5 При $\sigma > 1 : |\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geq 1$

► $\zeta(s) = \prod\limits_p \left(1 - \frac{1}{p^s}\right)^{-1}$

$\prod\limits_p \left(\left(1-\frac{1}{p^\sigma}\right)^3 \left(1-\frac{1}{p^{\sigma+it}}\right)^4 \left(1-\frac{1}{p^{\sigma+2it}}\right)\right)^{-1}$

$r = \frac{1}{p^\sigma}; e^{i\varphi} = p^{-it}$ и по предыдущей лемме ◄

Теорема 9 При $\sigma \geq 1 \quad \zeta(s) \neq 0$

► При $\sigma > 1 : \zeta(\sigma+it) \neq 0$,
(т.к. если нет, то: $\zeta(\sigma+it) = 0 \Rightarrow |\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| = 0 \geq 1$)
Допустим, что $\zeta(1+it) = 0; t \neq 0$
Тогда $|\zeta(\sigma)| \leq \frac{C_1}{\sigma-1}, 2 \geq \sigma > 1$ в окрестности полюса.
$\zeta'(1+it) = \lim \sigma \to 1 \frac{\zeta(\sigma+it)-\zeta(1+it)}{\sigma-1} \Rightarrow \left|\frac{\zeta(\sigma+it)}{\sigma-1}\right| \leq C_2$
$|\zeta(\sigma+2it)| \leq C_3$
$\Rightarrow |\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \leq \left(\frac{C_1}{\sigma-1}\right)^3 (C_2(\sigma-1))^4 C_3 \to 0.$
Противоречие с $|\cdot| > 1$ ◄

Билет 7

Формулировка асимптотического закона распределения простых чисел. Сведение его доказательства к исследованию некоторого комплексного интеграла.

Теорема 10 (Асимптотический закон распределения простых чисел.)
$\pi(x) \sim \frac{x}{\ln(x)}, x \to \infty$

► План доказательства путём сведения к исследованию интеграла.

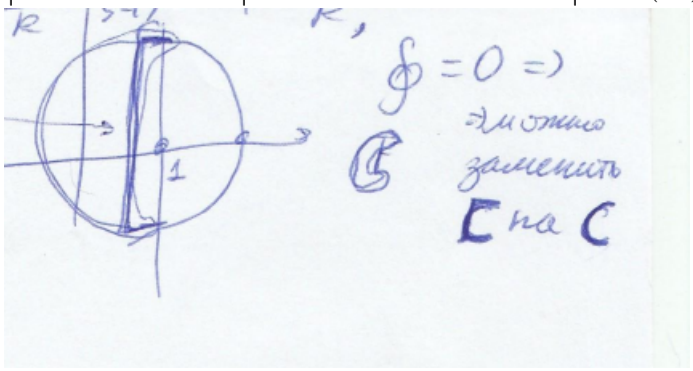
1. Обозначим $f(s) = -\frac{\zeta'(s)}{s\zeta(s)} - \frac{1}{s-1}$. Она аналитическая при $\sigma \geq 1$.

2. В области $\sigma > 1 : f(s) = \int\limits_1^\infty \frac{\psi(x)-x}{x^{s+1}} dx$ – из преобразования Абеля.

3. Обозначим $f_u(s) = \int\limits_1^u \frac{\psi(x)-x}{x^{s+1}} dx$. Она целая при $u > 1$

4. $f(1) - f_u(1) = \frac{1}{2\pi i R} \cdot \oint\limits_{\Gamma(\theta,R)} (f(s) - f_u(s)) u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right) ds = \frac{1}{2\pi i R} \int F_k(s) ds$ вычет в точке $s = 1$

5. $\left|\frac{1}{2\pi i R} \int\limits_{C_R} F_k(s) ds\right| \leq \frac{B}{R} \Rightarrow \left|\frac{1}{2\pi i R} \int\limits_{(ris)} f_u(s) u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right) ds\right| \leq \frac{B}{R}$



6. $J(u) = \frac{1}{2\pi i R} \int f_u(s) u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right) ds$
[
$\lim\limits_{u\to\infty} J(u) = 0$

$g(s) = \frac{1}{2\pi i R} f(s) \left(\frac{s-1}{R} + \frac{R}{s-1}\right)$ ограничено на контуре, значит $\int\limits_{\theta+iR}^{1+iR} g(s) u^{s-1} ds \leq \frac{\varepsilon}{\delta}$

Значит $|\int\limits_{BC} g(s) u^{s-1} ds| \leq M 2R u^{\theta-1} \to 0, u \to \infty \Rightarrow \lim\limits_{u\to\infty} f_u(1) = f(1) \Rightarrow$ интеграл сходится $\Rightarrow$ асимптотический закон. ◄

Билет 8

Доказательство асимптотического распределения распределения простых чисел. Асимптотическая формула n-го простого числа.

1. Утверждение 6 $f(s) = -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ аналитическая при $\sigma \geq 1$

   ▶ Интересует $\sigma = 1$, т.к. при $\sigma > 1$ все ок.
   $\exists$ окрестность, в которой функция аналитична.
   $\zeta(s) = \frac{1}{s-1} + g(s), \quad g(s)$ аналитичная.

   $-\frac{-\zeta(s)}{s\zeta(s)} = -\frac{-\frac{1}{(s-1)^2}+g'(s)}{s\left(\frac{1}{s-1}+g(s)\right)} = \frac{1}{s-1} \cdot \frac{1-\overbrace{(s-1)^2}^{\to 0} g'(s)}{s(1+(s-1)g(1))} = \frac{1}{s-1} + f(s)$, в $s = 1$ полюс первого порядка.◀

2. Из преобразования Абеля $\sigma > 1$: $-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1} = \int\limits_1^\infty \frac{\psi(x)-x}{x^{s+1}} dx \Rightarrow f(s) = \int\limits_1^\infty \frac{\psi(x)-x}{x^{s+1}} dx$

3. $f_u(s) = \int\limits_1^u frac\psi(x) - xx^{s+1} dx$ – целая, $u > 1$

   ▶ $\int\limits_a^b \frac{dx}{x^{s+k}} = \frac{x^{-s-k+1}}{-s-k+1}\Big|_a^b = \frac{b^{-s-k+1}-a^{-s-k+1}}{-s-k+1} = \frac{1+(-s-k+1)\ln(b)+(-s-k+1)^2 g(s)-1-(-s-k+1)\ln(a)}{-s-k+1}$
   – нет особенностей, значит целая. (± 1 сокращаются, а дальше числитель делится на знаменатель ура).◀

4. Считаем вычет
   $\frac{1}{2\pi i R} \cdot \oint\limits_{\Gamma(\theta,R)} (f(s) - f_u(s)) u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right) ds = \frac{1}{R} \cdot (f(1) - f_u(1)) \cdot 1 \cdot R$

5. $\left|\frac{1}{2\pi i R} \int\limits_{C_R} F_k(s) ds\right| \leq \frac{B}{R}; \quad \psi(x) \leq Cx, |\psi(x) - x| \leq (C+1)x = Bx$

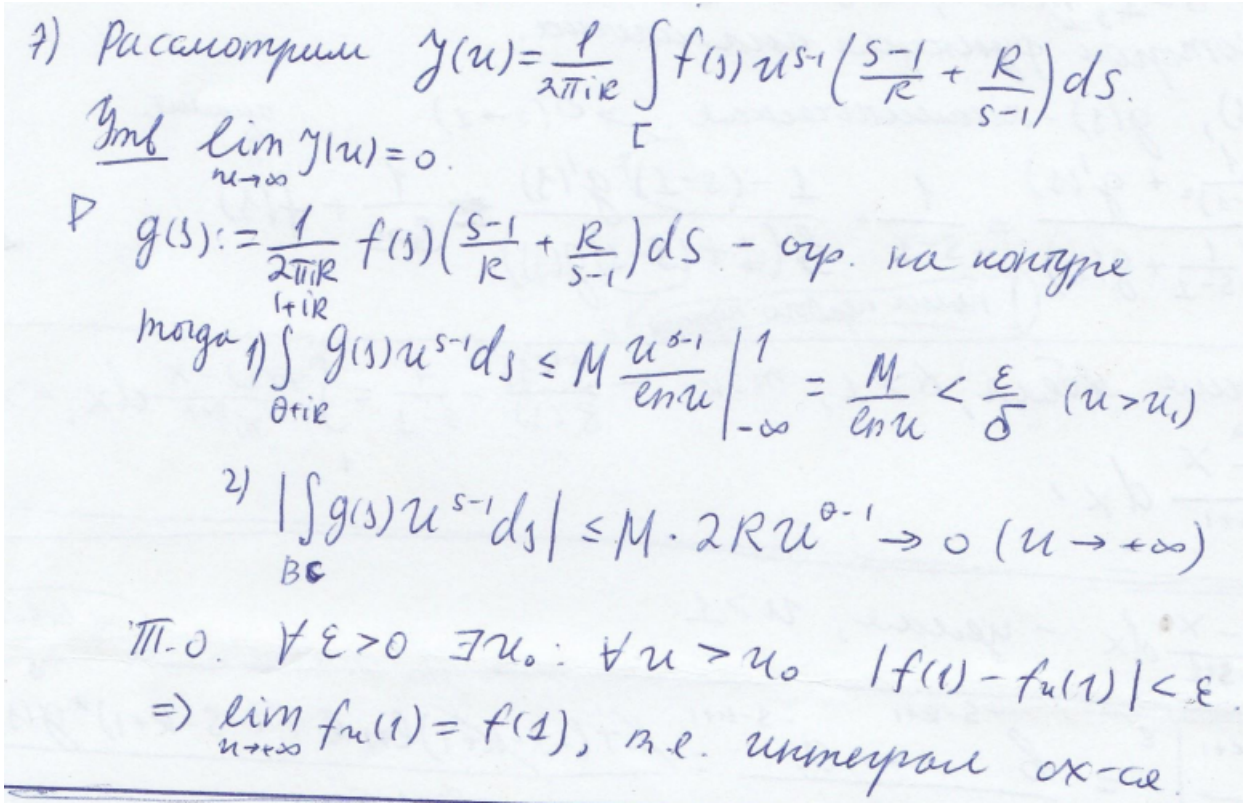
   ▶ $|f(s) - f_u(s)| = \left|\int\limits_u^\infty \frac{\psi(x)-x}{x^{s+1}} dx\right| \leq \int\limits_u^\infty \frac{Bx}{x^{s+1}} dx = B\frac{x^{1-\sigma}}{1-\sigma}\Big|_u^\infty = \frac{Bu^{1-\sigma}}{\sigma-1}$
   $\Rightarrow \left|\frac{s-1}{R} + \frac{R}{s-1}\right| = 2|Re\frac{s-1}{R}| = 2\frac{\sigma-1}{R}$ ◀

6. $\left|\frac{1}{2\pi i R} \int\limits_{[} f_u(s) u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right)\right| \leq \frac{B}{R}$
   При этом можно заменить [на (, т.к. интеграл по ([равен 0.
   $|f_u(s)| = |\int\limits_1^u \frac{\psi(x)-x}{x^{s+1}} dx| \leq B\frac{u^{1-\sigma}}{1-\sigma}$
   $|\frac{s-1}{R} + \frac{R}{s-1}| = 2|Re\frac{s-1}{R}| = 2\frac{1-\sigma}{R}$

Билет 8

7. Рассмотрим $J(u) = \frac{1}{2\pi i R} \int\limits_{[} f(s) u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1} \right) ds$

Утверждается что предел равен 0.



/*я ничего не понял и мне лень писать сори:(*/

Утверждение 7 $p_n \sim n \ln(n)$ – закон распределения n-того простого.

▶ $n = \pi(p_n) = \frac{p_n}{\ln(p_n)}(1 + \alpha_n)$
$\ln(n) = \ln(p_n) - \ln(\ln(p_n)) + \ln(1 + \alpha_n) = \ln(p_n)(1 + \beta_n)$
$\Rightarrow n \ln(n) = p_n (1 + \alpha_n)(1 + \beta_n)$ ◀

Билет 9

Простейшие свойства сравнений. Группа $(Z/mZ)^*$. Теорема Эйлера. Малая теорема Ферма. Элементарные доказательства бесконечности множества простых чисел в прогрессиях вида $4n+1$ и $4n+3$.

Определение 4 (Сравнения)
$a \equiv b \pmod m \iff m \mid (a-b) \iff a$ и b дают одинаковые остатки при делении на m

Свойства:

0. $a \equiv b \pmod m \iff b \equiv a \pmod m$
1. $a \equiv b \pmod m \iff a+c \equiv b+c \pmod m$
2. $a \equiv b \pmod m \Rightarrow ac \equiv bc \pmod m$!!!ТОЛЬКО В ОДНУ СТОРОНУ!!!
3. $\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow a+c \equiv b+d \pmod m$
4. $\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow ac \equiv bd \pmod m$
5. $ac \equiv bc \pmod{mc} \Rightarrow a \equiv b \pmod m$
6. $ac \equiv bc \pmod m, (m,c) = 1 \Rightarrow a \equiv b \pmod m$

Уравнение в факторкольце.
$\mathbb{Z}/m\mathbb{Z} = \{\bar a : \bar a = a+mt, t \in \mathbb{Z}\} \qquad a \equiv b \iff \bar a = \bar b$
$(\mathbb{Z}/m\mathbb{Z})^* = \{\bar a : \bar a = a+mt, (a,m) = 1\}$!!ЭТО НЕ КОЛЬЦО, (т.к. нет сложения)!!!
Но это группа по умножению: 1)$\exists 1$, 2)$\exists a^{-1}$

Лемма 6 $ax \equiv b \pmod m, (a,m) = 1 \Rightarrow \exists! c < m : x \equiv c \pmod m$

▶ 1)$ax \equiv b \pmod m$
$\exists u, v : au + mv = 1 \Rightarrow au \equiv 1 \pmod m$
$a(bu) \equiv b \pmod m$
$x \equiv c \equiv bu \pmod m$
2) пусть их два разных:$x_1 \neq x_2$
$ax_1 \equiv b \pmod m, ax_2 \equiv b \pmod m \Rightarrow ax_1 \equiv ax_2 \pmod m \Rightarrow x_1 \equiv x_2 \pmod m$ ◀

Теорема 11 (Теорема Эйлера) $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Билет 9

Теорема 12 (Малая теорема Ферма) p-простое, $(p,a) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Утверждение 8 $p \mid (a^2+b^2), p \nmid a, p \neq 2 \Rightarrow p = 4m+1$

▶ $a^2+b^2 \equiv 0 \pmod{p}$
$a^2 \equiv -b^2 \pmod{p}, (a^2)^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \pmod{p}$
$a^{p-1} \equiv b^{p-1}(-1)^{\frac{p-1}{2}} \Rightarrow 1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \Rightarrow \frac{p-1}{2} = 2m \Rightarrow p = 4m+1$ ◀

Утверждение 9 Бесконечность множества простых вида $4n-1$.

▶ Пусть их конечное число. Пусть p_n – максимальное из них.
Рассмотрим $p = 4(p_1 \cdots p_n) - 1$ не простое. $\exists q \mid p : q = 4k-1$, т.к. если все делители имеют вид $4k+1$, то и $p \equiv 1 \pmod{4}$, но $q \neq p_j$ противоречие.◀

Утверждение 10 Бесконечность множества простых вида $4n+1$.

▶ Пусть $p_1, \ldots, p_n$ – все простые числа такого вида.
$(2p_1 \cdots p_n)^2 + 1^2 = q_1 \cdots q_m \Rightarrow q_i = 4m_i + 1$ по лемме, значит $q_i = p_j$ – противоречие.◀

Билет 10

Простейшие свойства групповых характеров. Построение характеров. Вычисление сумм $\sum_{a\in G}\chi(a)$ и $\sum_{\chi}\chi(a)$ для характеров χ группы G. Определение и свойства числовых характеров.

Определение 5 (Определение характера)
Пусть G – конечная группа, коммутативная по умножению.
$\chi : G \to \mathbb{C}$ – характер

1. $\chi(g) \not\equiv 0$
2. $\chi(g_1 \cdot g_2) = \chi(g_1) \cdot \chi(g_2)$

Свойства характеров.

1. $\chi(e) = 1$ $\quad$ ► $\chi(e\cdot e) = \chi(e)\cdot\chi(e)$ ◄
2. $g^h = e \Rightarrow (\chi(g))^h = 1 \Rightarrow$ характеры принимают значения только корней из 1.
3. $\chi(g^{-1}) = \frac{1}{\chi(g)}$

$\chi_0(g) \equiv 1$ – главный характер.
$\chi_1\chi_2(g) := \chi_1(g)\cdot\chi_2(g)$

Характеры образуют группу относительно операции $\chi_1\chi_2(g)$ ►

1. $\chi_1\chi_2(g_1g_2) = \chi_1(g_1)\chi_1(g_2)\chi_2(g_1)\chi_2(g_2) = \chi_1\chi_2(g_1)\chi_1\chi_2(g_2)$
2. $\exists\chi^{-1} : \chi^{-1}(g) = \chi(g^{-1}) = \frac{1}{\chi(g)}$
3. $\exists 1 : \chi\chi^{-1}(g) = 1$
4. $(\chi_1\chi_2)\chi_3(g) = \chi_1(\chi_2\chi_3)(g)$
   ► $(\chi_1\chi_2)\chi_3(g) = (\chi_1(g)\chi_2(g))\chi_3(g) = \chi_1(g)(\chi_2(g)\chi_3(g)) = \chi_1(\chi_2\chi_3)(g)$ ◄

◄
Пусть $G = G_1 \otimes \cdots \otimes G_n$, где все G_i циклические. $ord\, g_i = h_i$
$ord(G) = h = h_1 \cdots h_n$
$\forall g \in G : g = g_1^{r_1}\cdots g_n^{r_n}, \qquad 0 \le r_i \le h_i$ и такое представление единственно.

Билет 10

Рассмотрим набор корней из 1:$\zeta_1,\dots,\zeta_n : \zeta_i^{h_i}=1$
$\chi(g)=\zeta_1^{r_1}\cdots\zeta_n^{r_n}$

Утверждение 11 Это характер и любой характер можно записать так.

► 1)$g=g_1^{k_1}\cdots g_n^{k_n}\qquad k_j=r_j+a_jh_j\Rightarrow g=g_1^{r_1}\cdots g_n^{r_n}$ а дальше рассмотрим характер и такие ого записался.
2)$a=g_1^{a_1}\cdots g_n^{a_n};\quad b=g_1^{b_1}\cdots g_n^{b_n}$
$ab=g_1^{a_1+b_1}\cdots g_n^{a_n+b_n}$ и получаем что характер произведения равен произведению характеров. Проверили. ◄
Если $\chi\neq\chi_0$, то $\exists g:\chi(g)\neq 1$
Если $g\neq e$, то $\exists\chi:\chi(g)\neq 1$

Утверждение 12

1. $S=\sum\limits_{g\in G}\chi(g)=\begin{cases}h,\chi=\chi_0\\0,\chi\neq\chi_0\end{cases}$
2. $\sigma=\sum\limits_{\chi}\chi(g)=\begin{cases}h,g=e\\0,e\neq e\end{cases}$

► Сначала рассмотрим тривиальные случаи:
$\chi=\chi_0\Rightarrow\chi(g)=1\Rightarrow S=|G|=h$
$g=e\Rightarrow\chi(e)=1\Rightarrow\sigma=|G|=h$
Теперь остальные:
$\chi\neq\chi_0\Rightarrow\exists a\in G:\chi(a)\neq 1$
$\chi(a)S=\sum\limits_{g\in G}\chi(a)\chi(g)=S\Rightarrow(\chi(a)-1)S=0\Rightarrow S=0$

$g\neq e\Rightarrow\exists\chi_1:\chi_1(g)\neq 1$
$\chi_1(g)\sigma=\sigma\Rightarrow\sigma=0$ ◄
Числовые характеры.
$\mathbb{Z}_m^*=(\mathbb{Z}/m\mathbb{Z})^*=\{\bar a:\bar a=a+mt,\quad (a,m)=1\},\bar a\bar b=\overline{ab}$
$$\chi(x)=\begin{cases}\chi(\bar x),(x,m)=1\\0,(x,m)\neq 1\end{cases}$$
$$\chi_0(x)=\begin{cases}1,(x,m)=1\\0,(x,m)\neq 1\end{cases}$$
$a\equiv b\pmod m\Rightarrow\chi(a)=\chi(b)$

Билет 10

$\chi(ab) = \chi(a)\chi(b)$

$\chi(a) \neq 0 \iff (a,m) = 1$

$$\sum_{x=1}^{m} \chi(x) = \begin{cases} \varphi(m), \chi = \chi_0 \\ 0 \end{cases}$$

$$\sum_{\chi} \chi(x) = \begin{cases} \varphi(m), x = 1 \\ 0 \end{cases}$$

$$\left| \sum_{x=1}^{r} \chi(x) \right| = \left| \sum_{x=mq+1}^{mq+r} \chi(x) \right| \leq r \leq m$$

Билет 11

Аналитичность функции Дирихле $L(s,\chi)$ в области $\sigma > 1$. Разложение в ряд Дирихле ее логарифмической производной. Отсутствие нулей L-функции в области $\sigma > 1$. Представление L-функции в виде бесконечного произведения. Аналитическое продолжение функции $L(s,\chi_0)$ в область $\sigma > 0$.

Определение 6 $L(s,\chi) = \sum\limits_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ – функция Дирихле.

$\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$; если $\sum\limits_{n=1}^{\infty} f(n) = A$, $\sum\limits_{d=1}^{\infty} f(d)\Lambda(d) = B$ – абсолютно сходящийся ряд.

$$\Lambda(n) = \begin{cases} \ln(p), n = p^k \\ 0 \end{cases} \Rightarrow AB = \sum_{n=1}^{\infty} f(n)\ln(n)$$

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 - f(p))^{-1}.$$

Если $f(n) = \frac{\chi(n)}{n^s} \Rightarrow L(s,\chi) = \prod\limits_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$

$$L(s,\chi) \cdot \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n)\ln(n)}{n^s} = -L'(s,\chi) \Rightarrow \text{в области } \sigma > 1 : L(s,\chi) \neq 0$$

$$\chi_0(p) = \begin{cases} 1, (m,p) = 1 \\ 0 \end{cases} \Rightarrow L(s,\chi) = \prod_{p \nmid m} (1 - \tfrac{1}{p^s})^{-1}$$

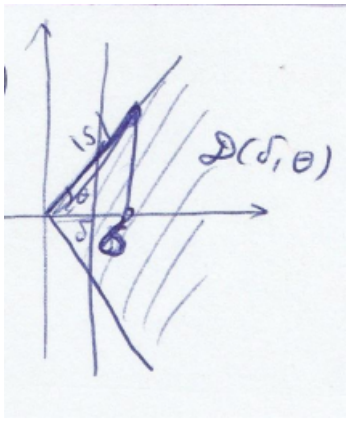
$$L(s,\chi_0) = \zeta(s) \prod_{p|m} (1 - \tfrac{1}{p^s})^{-1} = \left(\tfrac{1}{s-1} + f(s)\right) \prod_{p|m} (1 - \tfrac{1}{p^s})^{-1} = \tfrac{a_m}{s-1} + f_m(s),$$

$$a_m = \prod_{p|m} (1 - \tfrac{1}{p^s}) = \tfrac{\varphi(m)}{m} > 0 \Rightarrow L(s,\chi_0) \text{ аналитична в области } \sigma > 0$$

Билет 12

Теорема о почленном дифференцировании ряда Дирихле. Область аналитичности функции $L(s,\chi)$ при $\chi \neq \chi_0$.

Рассмотрим область $D(\delta,\theta) = \begin{cases} \sigma > \delta > 0 \\ |arg(s)| < \theta, \theta \in (0, \frac{\pi}{2}) \end{cases}$



Утверждение 13

1. Ряд $\sum\limits_n \frac{a_n}{n^s}$ равномерно сходится в $D(\delta,\theta)$
2. $f(s)$ аналитична в области $\sigma > 0$, где $f(s) = \sum\limits_n \frac{a_n}{n^s}$

▶ Определение равномерной сходимости: $\forall \varepsilon > 0 \exists M(\varepsilon) : \forall N > M, \forall s \in D(\delta,\theta) :$
$|R_N(s)| = \left| \sum\limits_{n=N+1}^{\infty} \frac{a_n}{n^s} \right| < \varepsilon$

Перепишем: $R_N(s) = \sum\limits_{k=0}^{\infty} \frac{a_{N+k}}{(N+k)^s} \qquad A(x) = \sum\limits_{k \le x} a_k; g(x) = \frac{1}{(N+x)^s}$

$|A(x)| \le 2C; \quad g(x) \to 0 \Rightarrow A(x)g(x) \to 0$

$g'(x) = -s(N+x)^{-s-1}, s\int\limits_1^{\infty} A(t)(N+t)^{-s-1}dt$ сходится, значит можно использовать преобразование Абеля.

$\sum\limits_{k=1}^{\infty} g(k)a_k = -\int\limits_1^{\infty} A(t)g'(t)dt = -s\int\limits_1^{\infty} A(t)(N+t)^{-s-1}dt = R_N(s)$

$|R_N(s)| \le |s| \int\limits_1^{\infty} 2C(N+t)^{-s-1}dt = |s| \cdot 2C \left. \frac{(N+t)^{-\sigma}}{-\sigma} \right|_1^{\infty} = 2C\frac{(N+1)^{-\sigma}}{\sigma}|s|$

В области $D(\delta,\theta)$: $\quad |R_N(s)| \le 2CN^{-\delta}\frac{1}{\cos(\theta)} < \varepsilon \Rightarrow$ выполняется равномерная сходимость.

Для любой точки правее нуля можно подобрать такие δ и θ, чтобы она попала в область. Раз в таких областях ряд сходится равномерно, значит его можно дифференцировать бесконечное число раз, значит функция аналитична.◀

Билет 13

Теорема об области сходимости ряда Дирихле с неотрицательными коэффициентами.

Пусть есть ряд $f(s) = \sum a_n n^{-1}, \quad \sigma_1 < \sigma_2 < \sigma_0$

Теорема 13 Пусть функция $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}, \sigma_1 < \sigma_2 < \sigma_0$

1. $f(s)$ аналитична при $\sigma > \sigma_1$
2. $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}, \quad (\sigma > \sigma_2)$
3. $a_n \geq 0$

Тогда $f(s)$ раскладывается в ряд Дирихле при $\sigma > \sigma_1$ и его можно почленно дифференцировать. $///< WTF?$
/*P.S. в другом источнике: Тогда $f(s)$ аналитична при $\sigma > \sigma_1$, т.е. можно продлить представление рядом.*/

► Если $f(s)\sum \frac{a_n}{n^s}$ сходится при $s = s_0 = \sigma_0 + it_0$, то ряд Дирихле задаёт функцию, аналитичную в области $\sigma > \sigma_0 \Rightarrow$ можно дифференцировать.
$\Rightarrow$ есть прямая, разделяющая области сходимости и расходимости.
Рассмотрим $\sigma_0 > \sigma_2$, разложим в ряд Тейлора:
$f(s) = \sum\limits_{k=0}^{\infty} \frac{f^{(k)}(\sigma_0)}{k!}(s-\sigma_0)^k$
Берем $\sigma \in (\sigma_1, \sigma_2)$ и подставляем вместо s. (анализируем сходимость в $\sigma > \sigma_1$)
$f(\sigma) = \sum\limits_{k=0}^{\infty} \frac{f^{(k)}}{k!}(\sigma-\sigma_0)^k = \sum\limits_{k=0}^{\infty}\sum\limits_{n=1}^{\infty} \frac{a_n(-\ln(n))^k}{n^{\sigma_0}}\frac{1}{k!}(\sigma-\sigma_0)^k = \sum\limits_{k=0}^{\infty} \frac{(\sigma-\sigma_0)^k}{k!} \sum\limits_{n=1}^{\infty} \frac{a_n(-\ln(n))^k}{n^{\sigma_0}} =$
$\sum\limits_{n=1}^{\infty} \frac{a_n}{n^{\sigma_0}} \sum\limits_{k=0}^{\infty} \frac{((\sigma_0-\sigma)\ln(n))^k}{k!} = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^{\sigma_0}} e^{(\sigma-\sigma_0)\ln(n)} = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^{\sigma}}$
Ряд задает аналитическую функцию по теореме единственности аналитического продолжения функции заданной этим рядом при $\sigma > \sigma_1$ ◄

Билет 14

Неравенство $L(1,\chi) \neq 0$ для действительного характера χ.

Определение 7 Характер χ действительный, если $\chi^2 = \chi_0 = 1$

Лемма 7 $f(s) := \zeta(s)L(s,\chi) \Rightarrow$

1. $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \sigma > 1$
2. $a_n \geq 0$
3. $a_{n^2} \geq 1$
4. $\sum\limits_{n=1}^{\infty} \frac{a_n}{\sqrt{n}}$ расходится.

► $f(s) = \sum\limits_{k=1}^{\infty} \frac{1}{k^s} \sum\limits_{d=1}^{\infty} \frac{\chi(d)}{d} = \sum\limits_{n=1}^{\infty} \frac{1}{n^s} \sum\limits_{d|n} \chi(d)$

Если $n = p_1^{k_1} \cdots p_r^{k_k}$, то $a_n = \sum\limits_{d|n} \chi_d \prod\limits_{j=1}^{n} (1 + \chi(p_j) + \chi(p_j^2) + \cdots) = \prod\limits_{j=1}^{n} (1 + \chi(p_j) +$

$\chi(p_j^2) + \cdots) = \prod\limits_{j=1}^{n} (1 + \chi(p_j) + \chi^2(p_j) + \cdots)$

где $a_{n_j} = \begin{cases} 1, & \chi(p_j) = 0 \\ k_j + 1, & \chi(p_j) = 1 \\ 1, & \chi(p_j) = -1, k_j = 2m \\ 0 & \chi(p_j) = -1, k_j = 2m+1 \end{cases}$

Если $n = k^2$, то все $k_j = 2m \Rightarrow$

$\prod\limits_{j=1}^{r} a_{n_j} \geq 1 \Rightarrow 1) + 2) + 3)$ ////<WTF??

4) $\sum\limits_{n=1}^{\infty} \frac{a_n}{\sqrt{n}} \geq \sum\limits_{k=1}^{\infty} \frac{a_{k^2}}{k} \Rightarrow$ расходится. ◄

Теорема 14 χ– действительный характер, тогда $L(1,\chi) \neq 0$

► $L(1,\chi) = 0 \Rightarrow L(s\chi) = (s-1)g(s), \quad g(s)$ аналитичная
$\zeta(s) = \frac{1}{s-1} + h(s)$ – тоже аналитичная
$f(s) = \zeta(s)L(s,\chi) = g(s) + g(s)h(s)(s-1)$ представляется сходящимся рядом Дирихле в $\sigma > 0$ а это противоречие с пунктом 4 леммы ◄

Билет 15

Неравенство $L(1,\chi) \neq 0$ при $\chi^2 \neq \chi_0$.

Лемма 8 Пусть $s \in \mathbb{R}, s > 1$, тогда $A := |L^3(s,\chi_0) \cdot L^4(s,\chi) \cdot L(s,\chi^2)| \geq 1$

► $L(s,\chi) = \prod\limits_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$

$A = \prod\limits_{p|m} \left|\left(1 - \frac{1}{p^s}\right)^3 \left(1 - \frac{\chi(p)}{p^s}\right)^4 \left(1 - \frac{\chi^2(p)}{p^s}\right)^3\right|^{-1}$

Из билета 6 $|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})| \leq 1 \qquad \Rightarrow r = \frac{1}{p} \Rightarrow$◄

Теорема 15 При $\chi \neq \chi_0 : L(1,\chi) \neq 0$

► $L(1,\chi) = 0 \Rightarrow L'(1,\chi) = \lim\limits_{s\to 1+0} \frac{L(s,\chi)-L(1,\chi)}{s-1} = \lim\limits_{s\to 1+} \frac{L(s,\chi)}{s-1} \Rightarrow \left|\frac{L(s,\chi)}{s-1}\right| \leq C_1$

$L(s,\chi_0) = \sum\limits_{(m,n)=1}^{\infty} \frac{1}{n^s} < \zeta(s) \leq \frac{2}{s-1}$

$L(s,\chi) = (s-1)g_m(s)$

$|L(s,\chi)| \leq C_1(s-1) \qquad |L(s,\chi^2)| \leq C_2$

$1 \leq A \leq \left|\left(\frac{2}{s-1}\right)^3 (C_1(s-1))^4 C_2\right| \to 0$ противоречие. ◄

Билет 16

Доказательство теоремы Дирихле о бесконечности множества простых чисел в арифметической прогрессии.

Теорема 16 (Теорема Дирихле) Пусть $m \geq 2$. В прогрессии $mx+l, (m,l)=1$ бесконечно много простых.

► $F(s) = \sum\limits_{\chi} \chi(u) \left(-\frac{L'(s,\chi)}{L(s,\chi)}\right), \qquad s \in \mathbb{R}, s > 1$

u выбрали так, что $lu \equiv 1 \pmod m$

1. На $(1,2)$ $F(s)$ не ограничена
   $F(s) = -1\frac{L'(s,\chi_0)}{L(s,\chi)} + \sum\limits_{\chi \neq \chi_0} \chi(u)\frac{L'(s,\chi_0)}{L(s,\chi)} = \frac{1}{s-1} + G(s), \qquad G(s)$ ограничена при $\sigma > 1$
2. Если количество простых конечно, то $F(s)$ ограничена на $(1,2)$
   $-\frac{L'(s,\chi)}{L(s,\chi)} = \sum\limits_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} \Rightarrow F(s) = \sum\limits_{\chi}\chi(u)\sum\limits_{n=1}^{\infty}\frac{\Lambda(n)\chi(n)}{n^s} = \sum\limits_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\sum\limits_{\chi}\chi(un) =$
   $\varphi(m)\sum\limits_{un\equiv 1 \pmod m}\frac{\Lambda(n)}{n^s} = \varphi(m)\sum\limits_{n\equiv l \pmod m}\frac{\Lambda(n)}{n^s} = \varphi(m)\sum\limits_{p\equiv l \pmod m}\frac{\ln(p)}{p^s} + R(s)$
   $0 \leq R(s) = \varphi(m)\sum\limits_{p}\sum\limits_{k=2, p^k \equiv l \pmod m}\frac{\ln(p)}{p^s} \leq \varphi(m)\sum\limits_{p=2}^{\infty}\frac{\ln(p)}{p(p-1)} \leq C$
   То есть $F(s) = \varphi(m)\sum\limits_{p\equiv l \pmod m}\frac{\ln(p)}{p(p-1)} + O(1)$
   Если число простых конечно, то $F(s)$ ограничена. Противоречие.◄

Билет 17

Свойства минимального многочлена алгебраического числа. Целые алгебраические числа. Лемма Гаусса и ее следствия, относящиеся к целым алгебраическим числам.

Лемма 9 Если $\varphi(x) \in \mathbb{Q}[x]$ имеет общий корень с неприводимым многочленом $f(x)$, то $f(x)$ – делитель $\varphi(x) \Rightarrow$ каждый корень $f(x)$ является корнем $\varphi(x)$

► $m = deg(\varphi), \quad n = deg(f)$
Если $m = 0$, то $\varphi \equiv 0$. Пусть теперь $m > 0$
Тогда $\varphi(x) = q(x)f(x) + r(x), deg(r) < n$
$x = \alpha$ – общий корень, тогда $0 = \varphi(\alpha) = q(\alpha)f(\alpha) + r(\alpha) \Rightarrow r \equiv 0 \Rightarrow \varphi(x) = q(x)f(x)$ ◄

Лемма 10 Неприводимый многочлен $f(x) \in \mathbb{Q}[x]$ не может иметь кратных корней.

► $f(x)$ имеет кратные корни, тогда $f(x)$ имеет общий корень с $f'(x)$, значит делится на f', значит он не был неприводимым.◄

Определение 8 Число α – алгебраическое, если оно является корнем многочлена с рациональными коэффициентами, иначе трансцендентное.
Степень алгебраического числа α – степень неприводимого многочлена, имеющего корень α

$\forall n \quad \exists$ неприводимый многочлен степени n (например $x^n - 2$), значит существуют алгебраические числа любой степени.

Определение 9 Пусть α – алгебраическое число степени $n, \exists f \in \mathbb{Q}[x], deg(f) = n, \alpha$ – корень f, старший коэффициент $f = 1$, тогда f – минимальный многочлен.
Корни $\alpha_1, \ldots, \alpha_n$ минимального многочлена – сопряженные с α

Свойства сопряженных чисел.

1. $\alpha_1, \ldots, \alpha_n$ – алгебраические числа одинаковой степени с одинаковым минимальным многочленом
2. $\alpha_1, \ldots, \alpha_n$ сопряженные все друг другу.
3. $\alpha_1, \ldots, \alpha_n$ различны.

Билет 17

Утверждение 14 $B(x) \in \mathbb{Q}[x], A(x)$ – минимальный многочлен α, $\forall$ корня $B(x)$ это корень $A(x) \Rightarrow B(x) = \Lambda A^m(x)$

▶ $B(x) = A(x)B_1(x), \forall x : B_1(x) = 0 : A(x) = 0 \Rightarrow B(x) = A^2(x)B_2 \cdots$ ◀

Определение 10 Если $A(x) \in \mathbb{Z}[x]$, старший коэффициент $= 1$ – минимальный многочлен для α, то α – целое алгебраическое число.

Теорема 17 Пусть $B(x) \in \mathbb{Z}[x], b_n = 1, B(\alpha) = 0 \Rightarrow \alpha$ – целое алгебраическое.

Определение 11 $A(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}$ примитивный, если $(a_0, \ldots, a_n) = 1$

Лемма 11 (Гаусса) $A(x), B(x)$ примитивные, тогда $C(x) = A(x)B(x)$ тоже примитивный.

▶ $B(x) = b_m x^m + \cdots b_0, \qquad A(x) = a_n x^n + \cdots + a_0$
Покажем, что $\forall p : \exists c_j : p \nmid c_j$
$\forall p \exists a_s, b_t : p \nmid a_s, p \nmid b_t, p \mid a_0, \ldots a_n, b_0, \ldots b_m$.
Тогда $c_{s+t} = \sum\limits_{k+l=s+t} a_k b_l = \underbrace{a_s b_t}_{\not\vdots p} + \underbrace{\sum resid}_{\vdots p} \not\vdots p$ ◀ Доказательство теоремы.

$B(x)$ обнуляется $\alpha; A(x) = x^n + \cdots a_0 \in \mathbb{Q}[x]$ – минимальный многочлен α. Тогда $B(x) = A(x)C(x) = \frac{u}{v}\tilde{A}(x)\tilde{C}(x)$, где с тильдами целые. Тогда $\tilde{A}, \tilde{C}$ – примитивные, значит $vB(x)$ тоже примитивный. По лемме Гаусса $v = 1 \Rightarrow \tilde{A}\tilde{C} = B \Rightarrow \tilde{A}$ – минимальный целый многочлен, значит α – целое алгебраическое число.◀

Билет 18

Формулировка основной теоремы о симметричных многочленах. Теорема о симметричном многочлене от нескольких систем сопряженных алгебраических чисел. Поле алгебраических чисел и кольцо целых алгебраических чисел. Алгебраическая замкнутость поля алгебраических чисел.

Пусть K – коммутативное кольцо с 1, $K[\alpha_1,\dots,\alpha_n]$ – кольцо многочленов с коэффициентами из K от $\alpha_1,\dots,\alpha_n$.

Определение 12 Многочлен $P(\alpha_1,\dots,\alpha_n)\in K[\alpha_1,\alpha_n]$ симметрический, если он не изменяется при любой перестановке переменных.

Обозначим $\sigma_1=\alpha_1+\dots+\alpha_n;\sigma_2=\alpha_1\alpha_2\cdots\alpha_{n-1}\alpha_n;\cdots;\sigma_n=\alpha_1\cdots\alpha_n$ – элементарные симметричные многочлены. С точностью до знака это коэффициенты $(x-\alpha_1)\cdots(x-\alpha_n)$

Теорема 18 (о симметричных многочленах) Любой симметричный многочлен от переменных $\alpha_1,\dots,\alpha_n$ единственным образом представляется в виде $P(\alpha_1,\dots,\alpha_n)=H(\sigma_1,\dots,\sigma_n)$, где $H\in K[\sigma_1,\dots,\sigma_n]$, $\sigma_1,\dots,\sigma_n$ – элементарные симметричные.

Рассмотрим несколько систем переменных $\alpha_1,\dots,\alpha_n,\delta_1,\dots,\delta_s$; Пусть $\sigma_1,\dots,\sigma_n,\eta_1,\dots,\eta_s$ – их элементарные симметричные многочлены.

Определение 13 $P(\alpha_1,\dots,\alpha_n,\delta_1,\dots,\delta_s)$ – симметричный многочлен относительно нескольких систем переменных, если он не изменяется при любой перестановке внутри каждой системы.

Теорема 19 (о симметричных многочленах от нескольких систем)
Любой симметричный многочлен от нескольких систем переменных $\alpha_1,\dots,\alpha_n,\delta_1,\dots,\delta_m$ единственным образом представляется в виде $P(\alpha_1,\dots,\alpha_n,\delta_1,\dots,\delta_m)=H(\sigma_1,\dots,\sigma_n,\eta_1,\dots,\eta_m)$, где $\sigma_1,\dots,\sigma_n,\eta_1,\dots,\eta_m$ – элементарные симметричные.

▶ считаем все переменные кроме $\alpha_1,\dots,\alpha_n$ константами, тогда $P=H_1(\sigma_1,\dots,\sigma_n,\eta_1,\dots,\eta_m)$, далее рассмотрим коэффициенты и будем их рассматривать как симметричные с меньшим числом систем, значит доказали по индукции. (база индукции предыдущая теорема и я хз где доказательство...)◀

Билет 18

Лемма 12 Пусть $\alpha, \ldots, \delta$ – алгебраические числа, $\alpha_1, \ldots, \alpha_n, \delta_1, \ldots, \delta_m$ – соответствующие сопряженные. $P(x, \alpha_1, \ldots, \delta_m) \in \mathbb{Q}[x, \alpha_1, \ldots, \delta_m]$ – симметрический относительно систем. Тогда $P \in \mathbb{Q}[x]$, т.е. не зависит от корней, а если не зависит от x, то тоже $\in \mathbb{Q}[x]$

► Рассмотрим P как многочлен от $\alpha_1, \ldots, \delta_m$ с коэффициентами из $\mathbb{Q}$. Элементарные многочлены с точностью до знака – коэффициенты минимального многочленов, т.е. числа из $\mathbb{Q} \Rightarrow P \in \mathbb{Q}[x]$ ◄///<WTF??

Теорема 20 Если α, β – алгебраические числа, то $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ ($\beta \neq 0$) – тоже алгебраические. (что значит что множество алгебраических чисел образуют поле)

► Рассмотрим $P_1(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} (x - (\alpha_i \pm \beta_j))$. Это симметричный многочлен по системам переменных α, β

$P_2(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} (x - \alpha_i \beta_j)$

По лемме $P_1, P_2 \in \mathbb{Q}[x]$

$\frac{\alpha}{\beta} = \alpha \cdot \beta^{-1}$ ◄

P.S. Кажется что β^{-1} тоже алгебраическое, потому что мы в минимальном для β заменим все коэффициенты в разложении на $\frac{1}{\beta_i}$.

Следствие: $deg(\alpha \pm \beta), deg(\alpha\beta), deg(\frac{\alpha}{\beta}) \leq deg(\alpha) deg(\beta)$

Определение 14 A – поле алгебраических чисел, расширение поля $\mathbb{Q}$

Теорема 21 A – алгебраически замкнутое (и любой многочлен разлагается на линейные множители), т.е. если ξ – корень $\varphi(x) = x^m + \alpha x^{m-1} + \cdots + \delta, \quad \alpha, \ldots, \delta$ – алгебраические, то ξ алгебраическое.

► Рассмотрим $P(x) = \prod_{i=1}^{n} \cdots \prod_{l=1}^{s} (x^m + \alpha_i x^{m-1} + \cdots + \delta_l)$ – симметричный от систем переменных с коэффициентами из $\mathbb{Z}$. По лемме $P(x) \in \mathbb{Q}[x]$. $P(x) \vdots \varphi(x) \Rightarrow P(\xi) = 0 \Rightarrow \xi$ алгебраическое. ◄

Билет 19

Алгебраическое числовое поле конечной степени. Каноническая форма представления его элементов. Теорема о числах, сопряженных в алгебраическом числовом поле. Теорема о примитивном элементе.

Пусть $C(x)$ – минимальный многочлен для θ степени n.
$Q(\theta) = \left\{ \frac{f(\theta)}{g(\theta)}, \quad f(x), g(x) \in \mathbb{Q}[x], g(\theta) \neq 0 \right\}$

Теорема 22 $Q(\theta) = \{ r_{n-1}(\theta), r_{n-1}(\theta) \in \mathbb{Q}[x], deg(r_{n-1}) \leq n-1 \quad \}$

▶ $\alpha = \frac{f(\theta)}{g(\theta)}, \quad (C(x), g(x)) = 1$, т.к. если есть общий корень, то $g(\theta) = 0$
$\exists u, v \in \mathbb{Q}[x] : ug + vC = 1$
$\underbrace{C(\theta)}_{=0} v(\theta) + g(\theta)u(\theta) = 1 \Rightarrow g(\theta) = \frac{1}{u(\theta)}$
Тогда $\alpha = f(\theta)u(\theta) = h(\theta); \quad h = qC + r_{n-1} \Rightarrow \alpha := r_{n-1}$ ◀

Следствие: $Q(\theta) =< \{1, \theta, \theta^2, \ldots, \theta^{n-1}\} >$ – алгебраическое числовое поле конечной степени, n – степень поля.
Рассмотрим $r_{n-1}(\theta_j)$ (б.о.о. $\theta = \theta_1$). Обозначим $r_{n-1} : r$. Положим $r(\theta_1) = \alpha, \quad \alpha_1, \ldots, \alpha_n$ – сопряженные с α.

Теорема 23 $r(\theta_1), \ldots, r(\theta_n)$ – тот же набор, что и $\alpha_1, \ldots, \alpha_m, \frac{n}{m} \in \mathbb{N}$

▶ $P(x) = (x - r(\theta_1)) \cdots (x - r(\theta_n)) \in \mathbb{Q}[x]$
Пусть A – минимальный многочлен для α
$A(r(\theta)) = A(\alpha) = 0 \Rightarrow$ у $A(r(x))$ все сопряженные θ тоже корни.
Любой корень P – корень $A \Rightarrow P(x) = \lambda A^k(x), \lambda = 1$
Тогда $deg(P) = n = km \Rightarrow k = \frac{n}{m} \in \mathbb{N}$ ◀
Следствие. $\alpha \in K \Rightarrow deg(\alpha) \mid deg(\theta) = deg(K)$ (т.е. в расширении с $\sqrt[3]{2}$ квадратных корней нет).

Определение 15 $\alpha = r(\theta) \Rightarrow N(\alpha) := r(\theta_1) \cdots r(\theta_n)$ – норма алгебраических чисел в поле.

1. $\alpha \neq 0 \Rightarrow N(\alpha) \neq 0$
2. $N(\alpha\beta) = N(\alpha)N(\beta)$
3. $N(\alpha) = (\alpha_1 \cdots \alpha_m)^{\frac{n}{m}}$

Пусть $Q(\theta) = \{ \frac{f(\theta)}{g(\theta)}, \quad g(\theta) \neq 0 \}$. Можно рассмотреть $Q(\theta, \eta) = \{ \frac{f(\theta,\eta)}{g(\theta,\eta)} \}$

Билет 19

Теорема 24 (о примитивном элементе) $Q(\alpha_1,\dots,\alpha_n)$. Тогда $\exists\theta$: $Q(\alpha_1,\dots,\alpha_n)=Q(\theta)$

▶ Рассмотрим случай $Q(\alpha,\beta)$,A – минимальный многочлен α,B – для β. Степени n,m.

Будем искать θ в виде $\theta=\alpha+t\beta, t\in\mathbb{N}$.

У многочленов $A(\theta-tx)$ и $B(x)$ $\exists\beta$ – общий корень. Хотим отсутствие других корней, т.е. $(A(\theta-tx),B(x))=x-\beta$. (Иначе $A(x-t\beta_j)=0\Rightarrow\theta-t\beta_j=\alpha_k\Rightarrow\theta=\alpha_k+t\beta_j\Rightarrow\alpha_t\beta=\alpha_k+t\beta_j,\ \beta\neq\beta_j\Rightarrow t=\frac{\alpha_k-\alpha}{\beta-\beta_j}$ – конечное число значений.)

Рассмотрим $t\in\mathbb{N}\forall l,m:\ t\neq\frac{\alpha_l-\alpha}{\beta_m-\beta}$

Тогда у $A(\theta-tx)$ и $B(x)$ НОД $=x-\beta\in Q(\theta)[x]\Rightarrow$ выражается через θ,β

$\overbrace{\alpha}$, $\underbrace{\beta}_{\text{как коэффициенты}}$ $\in Q(\theta)\Rightarrow$◀

Билет 20

Две теоремы о приближении действительных чисел рациональными дробями. Построение чисел, имеющих заданный порядок приближений.

Теорема 25 (Теорема Дирихле) Пусть $\alpha \in \mathbb{R} \Rightarrow \forall x \in \mathbb{N} \exists \frac{p}{q} : \begin{cases} \left|\alpha - \frac{q}{p}\right| < \frac{1}{xq} \\ x \geq q \geq 1 \end{cases}$

▶ Пусть $t = 0, \ldots, x$. Рассмотрим $\{\alpha t\}$. Разделим $[0,1]$ на x равных частей. Хотя бы две дробные доли попадут в одну часть. Пусть это будут αt_1 и αt_2, $0 \leq t_1 \leq t_2$

$\Rightarrow |\{\alpha t_1\} - \{\alpha t_2\}| < \frac{1}{x} \iff \left|\alpha \underbrace{(t_1 - t_2)}_{q} - \underbrace{([\alpha t_2] - [\alpha t_1])}_{p}\right| < \frac{1}{x}$ ◀

Теорема 26 (Теорема Дирихле) $\alpha \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow$ неравенство $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ имеет бесконечное число решений в рациональных дробях.

▶ $\forall x \exists \left\{\frac{p_x}{q_x}\right\}, x = 1, 2, \cdots : \quad \left|\alpha - \frac{p_x}{q_x}\right| < \frac{1}{xq_x},\ 1 \leq q_x \leq x \quad \Rightarrow \left|\alpha - \frac{p_x}{q_x}\right| < \frac{1}{q_x^2}$

Предположим, что таких конечное число.

Рассмотрим $\underbrace{\min_x \left|\alpha - \frac{p_x}{q_x}\right|}_{const > 0} < \frac{1}{xq_x} < \frac{1}{x} \to 0,\ x \to \infty$ ◀

Теорема 27 $\forall f(q) > 0\, \exists \alpha : 0 < \left|\alpha - \frac{p}{q}\right| < f(q)$ имеет бесконечное число решений. (т.е. существует сколь угодно хорошо приближаемые числа).

▶Пусть $\alpha = \sum\limits_{k=0}^{\infty} 10^{-n_k}, n_0 = 0, n_1 < n_2 < \cdots$

$\frac{p_m}{q_m} = \sum\limits_{k=0}^{m} 10^{-n_k}, q_m = 10^{n_m}$

$\left|\alpha - \frac{p_0}{q_0}\right| = \sum\limits_{k=n_1}^{\infty} 10^{-n_k} < 2 \cdot 10^{-m_1} < f(q_0)$ (выбрали m_1 так чтобы выполнялось)

$\left|\alpha - \frac{p_1}{q_1}\right| = \sum\limits_{k=n_2}^{\infty} 10^{-n_k} < 2 \cdot 10^{-m_2} < f(q_1)$ и т.д. ◀

Билет 21

Теорема Лиувилля о приближении алгебраических чисел. Построение трансцендентных чисел при помощи теоремы Лиувилля.

Теорема 28 (Лиувилля) $\alpha \in A \cap \mathbb{R}, n = deg(\alpha) \geq 2 \Rightarrow \exists C = C(\alpha) > 0 : \forall \frac{p}{q} : \left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$

► $A(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x], a_n > 0, A(\alpha) = 0$ – минимальный многочлен.
$A(\frac{p}{q}) \neq 0$, иначе был бы приводим, значит не минимальный.
$q^n A(\frac{p}{q}) \in \mathbb{Z} \Rightarrow |q^n A(\frac{p}{q})| \geq 1 \Rightarrow |A(\frac{p}{q})| \geq \frac{1}{q^n}$
$A(x) = (x-\alpha)B(x) \Rightarrow \left|\frac{p}{q} - \alpha\right| \cdot |B(\frac{p}{q})| \geq \frac{1}{q^n}$
При $\left|\frac{p}{q} - \alpha\right| > 1$ неравенство выполнено. Теперь интересует остальное.
$\left|\frac{p}{q} - \alpha\right| \leq 1 \Rightarrow -1 \leq \frac{p}{q} - \alpha \leq 1 \Rightarrow \frac{p}{q} \in [\alpha - 1, \alpha + 1]$, $B(\frac{p}{q}) \leq C_1 \Rightarrow \left|\frac{p}{q} - \alpha\right| > \frac{C}{q^n} = \frac{1}{C_1 q^n}$ ◄
Замечание: Для $deg(\alpha) = 1$ $\alpha \in \mathbb{Q} \Rightarrow \alpha = \frac{a}{b}$ $\left|\alpha - \frac{p}{q}\right| = \frac{|aq-bp|}{bq} > \frac{C}{bq}$ при $\frac{p}{q} \neq \frac{a}{b}$ ◄

Определение 16 α – число Лиувилля, если $\forall m \in \mathbb{N} \exists$ бесконечно много дробей $\frac{p}{q}$: $0 < |\alpha - \frac{p}{q}| < \frac{1}{q^m}$

Утверждение 15 Числа Лиувилля трансцендентные.

► Предположим, что α – алгебраическое число Лиувилля. $n = deg(\alpha), m = n + 1 \Rightarrow \frac{C}{q^n} < |\alpha - \frac{p}{q}| < \frac{1}{q^m} \Rightarrow q < \frac{1}{C}$, но $|\frac{p}{q}| - |\alpha| \leq |\frac{p}{q} - \alpha| \leq 1 \Rightarrow |p| \leq |q|(|\alpha| + 1) < \frac{1}{C}(|\alpha| + 1) \Rightarrow$ конечное число дробей. Противоречие. ◄
Пример числа Лиувилля.
$\alpha = \sum\limits_{k=0}^{\infty} 10^{-k!}$, $\frac{p_N}{q_N} = \sum\limits_{k=0}^{N} 10^{-k!}$
$0 < \alpha - \frac{p_N}{q_N} < 10^{-N \cdot N!}$
$\Rightarrow 0 < \alpha - \frac{p_N}{q_N} < \frac{1}{q_N^N}$

Билет 22

Обобщение теоремы Лиувилля на многочлены от нескольких алгебраических чисел.

Определение 17 Длина многочлена – сумма модулей коэффициентов. $L(P)$

Теорема 29 Пусть $\alpha_1,\dots,\alpha_s$ – алгебраические числа степеней $m_1,\dots,m_s$. Тогда $\exists$ положительная постоянная $C = C(\alpha_1,\dots,\alpha_s) : \forall P(x_1,\dots,x_s) \in \mathbb{Z}[x_1,\dots,x_s]$, тогда $P(\alpha_1,\dots,\alpha_s) = 0$ или $|P(\alpha_1,\dots,\alpha_s)| \geq L^{1-(m_1\cdots m_s)}C^{-d}$, d, L – степень и длина P

▶

1. $\exists a \in \mathbb{N} :\ a\alpha_1,\dots,a\alpha_s \in Z_A$ (очевидно, нужно взять старшие коэффициенты канонических многочленов α_i)

2. $\beta = a^d P(\alpha_1,\dots,\alpha_s) \in Z_A$ – очевидно, т.к. если $k_1,\dots,k_s :\ k_1+\cdots+k_s \leq d$, то $a^d\alpha_1^{k_1}\cdots\alpha_s^{k_s} = (a\alpha_1)^{k_1}\cdots(a\alpha_s)^{k_s}\cdot a^{d-k_1-\cdots-k_s}$

3. Пусть $\alpha_{i_1},\dots,\alpha_{i_m}$ сопряженные с α_i. Тогда все числа $|a^d P(\alpha_{1,r_1},\dots,\alpha_{s,r_s})| \leq C_1^d L$, C_1 не зависит от P $\quad (C_1 = a\cdot\max\limits_{i,j}\{1,|\alpha_{i,j}|\})$

4. $A(x) = \prod\limits_{r_1=1}^{m_1}\cdots\prod\limits_{r_s=1}^{m_s}(x - a^d P(\alpha_{1,r_1},\dots,\alpha_{s,r_s})) \in \mathbb{Q}[x]$, т.к. A – симметричный относительно $\alpha_i = (\alpha_{i1},\dots,\alpha_{im_i})$

5. Пусть $B(x) = x^n + b_{n-1}x^{n-1} + \cdots b_0 = (x-\beta_1)\cdots(x-\beta_n)$ – минимальный многочлен числа $\beta = \beta_1$. Поскольку $\beta \in Z_A$, то $B(x) \in \mathbb{Z}[x], |b_0| \geq 1$ если $P(\alpha_1,\dots,\alpha_s) \neq 0$

6. Многочлены $A(x)$ и $B(x)$ имеют коэффиценты из $\mathbb{Q}$ и общий корень β, значит $B(x) \mid A(x)$ и все корни B являются корнями A, тогда из 5): $1 \leq |b_0| = |\beta|\cdot|\beta_2\cdots\beta_n| \leq a^d\cdot|P(\alpha_1,\dots,\alpha_s)|\cdot(C_1^d L)^{n-1}$, $n \leq m_1\cdots m_s$

◀

Билет 23

Теорема Бореля о характере приближений “почти всех”действительных чисел.

Теорема 30 (Бореля) Рассмотрим $M = \{\alpha \in \mathbb{R} : 0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m},\ m > 2$ имеют бесконечное число решений $\}$, тогда $\mu(M) = 0$

► Б.о.о. $\alpha \in [0,1]$, т.к. добавление целого не влияет на приближение.
$M_Q = \{\alpha \in \mathbb{R} : 0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m},\ m > 2$ имеет хотя бы одно решение с $q > Q\}$.
Очевидно, $M \subset M_Q$
Пусть $\alpha \in \left(\frac{p}{q} - \frac{1}{q^m}; \frac{p}{q} + \frac{1}{q^m}\right) = I(p,q), |I(p,q)| = \frac{2}{q^m}$

$$M_Q \subset \bigcup_{q>Q} \bigcup_{p=0}^{q} I(p,q)$$

$$|M_Q| < \sum_{q>Q} \sum_{p=0}^{q} |I(q,p)| = \sum_{q>Q} (q+1)\frac{2}{q^m} < 4 \cdot \sum_{q>Q} \frac{1}{q^{m-1}} < \varepsilon \text{ ◄}$$

Билет 24

Иррациональность и трансцендентность числа e.

Утверждение 16 e иррационально.

▶ $e = \sum\limits_{k=0}^{\infty} \frac{1}{k!}$. Предположим, что $e = \frac{m}{n}$, $m,n \in \mathbb{N}$

Тогда $\underbrace{n!e}_{\in\mathbb{Z}} = \underbrace{n!\sum\limits_{k=0}^{n}}_{\in\mathbb{Z}} + R_n \Rightarrow 0 < R_n = n! \sum\limits_{k=n+1}^{\infty} \frac{1}{k!} < \frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots = \frac{1}{n+1} \cdot \frac{1}{1-\frac{1}{n+1}} =$

$\frac{1}{n} < 1$

$R_n \in \mathbb{Z}, 0 < R_n < 1$. Противоречие.◀

Утверждение 17 e трансцендентно.

▶ Рассмотрим $f(x) \in \mathbb{Q}[x]$ – многочлен с рациональными коэффициентами.

Обозначим $M_0 = \int\limits_0^{\infty} f(x)e^{-x}dx = \int\limits_0^{k} f(x)e^{-x}dx + \underbrace{\int\limits_k^{\infty} f(x)e^{-x}dx}_{J_k}$, $k \in \mathbb{Z}_+$

$= \int\limits_0^{k} f(x)e^{-x}dx + e^{-k}\int\limits_0^{\infty} f(y+k)e^{-y}dy$

Обозначим $\int\limits_0^{\infty} f(x+k)e^{-x}dx =: M_k, k \in \mathbb{Z}_+ \Rightarrow M_0 e^k = M_k + \varepsilon_k$.

Предположим, что e алгебраическое, тогда $\exists A(x) = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x] : A(e) = 0$

$M_0 \underbrace{\sum\limits_{k=0}^{m} a_k e^k}_{=0} = \sum\limits_{k=0}^{m} a_k M_k + \sum\limits_{k=0}^{m} a_k \varepsilon_k = 0$

Возьмем $f(x) = \frac{1}{n!}x^{n_0}(x-1)^{n_1}\cdots(x-m)^{n_m}$, $\quad n_j = \begin{bmatrix} n+1 \\ n \end{bmatrix}$. Тогда $\int\limits_0^{\infty} x^n e^{-x}dx = \Gamma(n+1) = n!$.

$\lim\limits_{n\to\infty} \varepsilon_k(n) = 0$, т.к. $|\varepsilon_k(n)| = \left| e^k \int\limits_0^{k} f(x)e^{-x}dx \right| \le |e^m| \cdot \int\limits_0^{m} \frac{1}{n!} m^{(n+1)\cdots(n+1)}dx = \frac{1}{n!}e^m \cdot m^{(n+1)(m+1)+1} \to 0$

$f(x+k) = \frac{1}{n!}(x+k)^{n_0}\cdots(x+k-m)^{n_m} = \frac{1}{n!}(b_{n_k}^{(k)}x^{n_k} + \cdots + b_N^{(k)}x^N) \Rightarrow \frac{1}{n!}\int\limits_0^{\infty} f(x+k)e^{-x}dx = \sum\limits_{j=n_k}^{N} b_j^{(k)} \int\limits_0^{\infty} x^j e^{-x}dx \Rightarrow$

$\Rightarrow M_k = \frac{1}{n!}(b_{n_k}^{(k)}(n_k!) + \cdots + b_N^{(k)}N!) \in \mathbb{Z}$

Билет 24

Добьемся того, чтобы $\varepsilon(n) = \sum\limits_{k=1}^{\infty} \varepsilon_k^{(n)} a_k > 0$, т.е. $\exists n_0, \ldots, n_m$: $\varepsilon^{(n)} = \sum\limits_{k=0}^{m} a_k e^k \int\limits_0^k f(x)e^{-x}dx := \sum\limits_{k=0}^{m-1} b_k \int\limits_k^{k+1} f(x)e^{-x}dx$, где $b_{m-1} = a_m e^m > 0$, а остальные интегралы по меньшему отрезку.

$sgn(b_k) = \underset{(k,k+1)}{sgn}(f(x)) = sgn(\int\limits_k^{k+1} f(x)e^{-x}dx) \Rightarrow$ можно добиться за счет выбора чет/нечет в зависимости от знака b_k. Значит $\varepsilon^{(n)} > 0$.

$0 < \varepsilon^{(n)} < 1, \quad \lim \varepsilon_k^{(n)} = 0 \Rightarrow \sum a_k M_k + \sum a_k \varepsilon_k = 0 \neq e$ ◀

Билет 25

Иррациональность числа π.

Утверждение 18 π иррационально.

▶ Рассмотрим $f(x) \in \mathbb{Q}[x]$

$\int_0^\pi f(x)\sin(x)dx = F(0) - F(\pi), \quad F(x) = f(x) - f''(x) + f^{(4)}(x) - \cdots$

$\frac{d}{dx} = (F'(x)\sin(x) - F(x)\cos(x)) = (F''(x) + F(x))\sin(x) = f(x)\sin(x)$

Пусть $\pi = \frac{a}{b}, b > 0. \quad f(x) = \frac{b^n}{n!}x^n(\pi - x)^n = \frac{1}{n!}x^n(a - bx)^n.$

$f(x) : f(0) = 0$, порядок $0 = n \Rightarrow f(0) = f'(0) = \cdots = f^{(n-1)}(0) = 0$

Все коэффициенты производной l-того порядка делятся на $l! \Rightarrow$ при $l \geq n f^{(l)}(x) \in \mathbb{Z}[x] \Rightarrow f(0), \ldots, f^{(2n)}(0) \in \mathbb{Z}$

$f(x) = f(\pi - x) \Rightarrow f^{(l)}(x) = (-1)^l f^{(l)}(\pi - x) \Rightarrow$ при $x = \pi \quad f^{(l)}(\pi) = (-1)^l f^{(l)}(0)$

Значит $F(0) + F(\pi) \in \mathbb{Z}$

При достаточно большом n : $\quad 0 < \int_0^\pi f(x)\sin(x)dx < 1 \Rightarrow \notin \mathbb{Z}$

Подынтегральное выражение больше 0.

$\exists n_0 \in \mathbb{N} : \int_0^\pi f(x)\sin(x)dx \leq \int_0^\pi f(x)dx < \frac{b^n}{n!}\pi^{2n}\int_0^\pi dx = \pi\frac{\left(\frac{a^2}{b}\right)^n}{n!} < 1 \; \forall n \geq n_0$ ◀

Билет 26

Лемма Зигеля об оценках решений систем линейных уравнений с целыми коэффициентами.

Лемма 13 Пусть $a_{ij} \in \mathbb{Z}, |a_{ij}| < A$ и $L_i(\overline{x} = \sum\limits_{j=1}^{q}) a_{ij}x_j, \quad i = \overline{1,p}, p < q.$

Тогда система уравнений $L_i(\overline{x}) = 0$ имеет решение $(x_1^{(0)}), \ldots, x_q^{(0)}$, $x_j^{(0)} \in \mathbb{Z}$: $0 < \max\limits_j |x_j^{(0)}| \leq 1 + (qA)^{\frac{p}{q-p}}$.

► Пусть X – натуральное число, которое будет выбрано в дальнейшем, и каждая из величин x_j пусть независимо друг от друга принимает значения $0, \pm 1, \ldots, \pm X$. Всего получим $(2X+1)q$ наборов $\overline{x} = (x_1, \ldots, x_q)$. Каждому из этих наборов соответствует набор $\overline{L}(\overline{x}) = (L_1(\overline{x}), \ldots, L_p(\overline{x}))$, причем $|L_i(\overline{x})| \leq qAX$ и, следовательно, всего может быть не более $(2qAX+1)p$ различных наборов $\overline{L}(\overline{x})$. Если

$$(2X+1)^q > (2qAX+1)^p, \tag{1}$$

то по принципу Дирихле можно найти два набора $\overline{x} : \overline{x}^{(1)}$ и $\overline{x}^{(2)}$, которым соответствует один и тот же набор значений $\overline{L}(\overline{x})$, т.е. $\overline{L}(\overline{x}^{(2)}) - \overline{L}(\overline{x}^{(1)}) = \overline{L}(\overline{x}^{(2)} - \overline{x}^{(1)}) = \overline{0}$, а значит, $\overline{x}^{(0)} = \overline{x}^{(2)} - \overline{x}^{(1)}$ решение системы, причем $|\overline{x}^{(0)}| \leq 2X$.
Неравенство (2) выполняется, если $(2X+1)^q > ((qA)(2X+1))^p$, т.е. при $2X > (qA)^{\frac{p}{q-p}} - 1$, а значит можно найти такое решение $\overline{x}^{(0)}$, что $2X \leq (qA)^{\frac{p}{q-p}} + 1$, откуда следует утверждение леммы. ◄

Билет 27

Формулировка теоремы Линдемана. Ее следствия. Построение вспомогательной функции для доказательства теоремы Линдемана, оценки ее порядка нуля.

Теорема 31 (Линдемана) Если α – алгебраическое число, отличное от нуля, то число e^{α} трансцендентно.

Следствия.

1. Число e трансцендентно.
2. Число π трансцендентно. Легко следует из равенства $e^{\pi i} = 1$
3. Если α алгебраическое число, отличное от 0 и 1, то число $\ln(\alpha)$ трансцендентно.
   Легко следует из равенства $e^{\ln(\alpha)} = \alpha$
4. Если $\alpha \neq 0$ алгебраическое число, то числа $\sin(\alpha), \cos(\alpha), \mathrm{tg}(\alpha)$ трансцендентны.
   Эти утверждения легко следуют из равенств
   $\sin(\alpha) = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}$; $\cos(\alpha) = \frac{e^{i\alpha} + e^{-i\alpha}}{2}$

В дальнейшем пусть n натуральное число, которое будет выбрано достаточно большим, $\gamma_1, \gamma_2, \ldots$, не зависящие от n положительные постоянные.

Лемма 14 Существует такая функция

$$f(z) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} a_{kl} z^k e^{lz} \tag{2}$$

с коэффициентами $a_{kl} \in \mathbb{Z}$, что

$$0 < \max_{k,l} |a_{kl}| < n^{\gamma_1 n} \tag{3}$$

$$f^{(t)}(0) = 0, \quad t = \overline{0, [n^{\frac{3}{2}}] - 1} \tag{4}$$

, где $[\cdot]$ целая часть числа.

► Из формулы Лейбница следует, что

$$f^{(t)}(z) = \sum_{k,l=0}^{n-1} a_{kl} \sum_{s=0}^{\min(t,k)} C_t^s k(k-1)\cdots(k-s+1) z^{k-s} l^{t-s} e^{lz} \tag{5}$$

Билет 27

Поэтому $f^{(t)}(0) = \sum\limits_{k,l=0,k\le t}^{n-1} C_t^k (k!) l^{t-k} a_{kl}$, и для завершения доказательства нам осталось оценить решение системы из $p = [n^{\frac{3}{2}}]$ уравнений относительно $q = n^2$ неизвестных a_{kl}. Их коэффициенты $|C_t^k (k!) l^{t-k}| < 2^{n^{\frac{3}{2}}} n^n n^{n^{\frac{3}{2}}} < n^{(3n^{\frac{3}{2}})} = A$.
По лемме Зигеля существует ненулевое решение этой системы в целых числах a_{kl}, удовлетворяющих неравенству $|a_{kl}| < 1 + (qA)^{\frac{p}{q-p}} < n^{\gamma_1 n}$. ◄

Обозначим через $ord|_{z=a} f(z)$ порядок нуля функции $f(z)$ в точке z = a.

Лемма 15 $[n^{\frac{3}{2}}] \le ord|_{z=0} f(z) \le n^2$

► Оценка снизу следует из 4. Докажем правое неравенство. Все функции $z^k e^{lz}$, $k,l = \overline{0,n-1}$, являются решениями дифференциального уравнения $D^n(D-1)^n \cdots (D-n+1)^n y = 0$, $D = \frac{d}{dz}$, с постоянными коэффициентами порядка n^2, следовательно, функция $f(z)$ тоже является решением этого уравнения и, если $f^{(t)}(0) = 0$, $t = \overline{0,n^2-1}$, то по теореме о единственности решения дифференциального уравнения $f(z) \equiv 0$, что невозможно, поскольку $f(x) \to \infty$ при $x \to +\infty, x \in \mathbb{R}$. ◄

Билет 28

Оценки вспомогательной функции и завершение доказательства теоремы Линдемана. Ее связь с проблемой квадратуры круга.

Пусть X – не зависящее от n натуральное число, которое будет выбрано в дальнейшем,

$$T = \min_{x=\overline{0,X}} ord|_{z=x\alpha} f(z) \tag{6}$$

Лемма 16 Справедливы неравенства

$$|f^{(T)}(x\alpha)| < n^{-\gamma_2 n^{\frac{3}{2}} - \frac{1}{3}(X-6)^T}, \qquad x = \overline{0,X}$$

▶ Из 6 и леммы (15) следует, что функция

$$g(z) = f(z) z^{-[n^{\frac{3}{2}}]} (z-\alpha)^{-T} \cdots (z-X\alpha)^{-T}$$

имеет лишь устранимые особые точки, поэтому для нее справедлив принцип максимума модуля. Возьмем $r = X|\alpha| + 1 < \sqrt{n}$. Тогда

$$\max_{|z|\le r} |g(z)| \le \max_{|u|=2\sqrt{n}} |g(u)|.$$

Поэтому при достаточно большом n

$$\begin{aligned} M_r = \max_{|z|\le r} |f(z)| \le \\ \le \max_{|u|=\sqrt{n}} |f(u)| \cdot \max_{|z|\le r, |u|=\sqrt{n}} \left| \left(\frac{z}{u}\right)^{[n^{\frac{3}{2}}]} \left(\frac{z-\alpha}{u-\alpha}\right)^T \cdots \left(\frac{z-X\alpha}{u-X\alpha}\right)^T \right| \le \\ \le n^2 n^{\gamma_1 n} (\sqrt{n})^n e^{n^{\frac{3}{2}}} \cdot n^{-0.4 n^{\frac{3}{2}} - 0.4XT} < n^{-\frac{1}{3} n^{\frac{3}{2}} - \frac{1}{3} XT} \end{aligned} \tag{7}$$

Далее,

$$f^{(T)}(x\alpha) = \frac{T!}{2\pi i} \oint\limits_{|z-x\alpha|=1} \frac{f(z)dz}{(z-x\alpha)^{T+1}},$$

поэтому по лемме (15)

$$f^{(T)}(x\alpha) \le (T!) M_r \le T^T M_r \le n^{2T} M_r$$

и из 7 следует утверждение леммы. ◀

Доказательство теоремы Линдемана.

▶ Из 6 следует, что существует такой индекс $x0$, что $f^{(T)}(x_0\alpha) \neq 0$, причем эта производная является многочленом $P(\alpha, e^\alpha)$ с целыми коэффициентами.

Билет 28

Допустим, что при некотором ненулевом α оба числа α и e^{α} алгебраические степеней соответственно m_1 и m_2. Тогда к многочлену $P(\alpha, e^{\alpha})$ можно применить обобщенную теорему Лиувилля. С помощью равенства 5 оценим его длину и степень:

$$L(P) \leq n^2 n^{\gamma_1 n}(n!)x_0^n \sum_{s=0}^{\infty} C_T^s (n-1)^{T-s} \leq n^{\gamma_3 n+T}, \qquad deg(P) \leq n + Xn.$$

Из обобщенной теоремы Лиувилля получаем, что

$$|f^{(T)}(x_0\alpha)| = |P(\alpha, e^{\alpha})| \geq (L(P))^{1-m_1m_2} C^{-deg(P)} > n^{-\gamma_4 n - m_1 m_2 T}.$$

С другой стороны, по лемме 16 при $X = 3m_1m_2 + 6$ выполняется неравенство

$$|f^{(T)}(x_0\alpha)| < n^{-\gamma_2 n^{\frac{3}{2}} - m_1 m_2 T}.$$

Последние две оценки при достаточно большом n противоречивы. Теорема Линдемана доказана. ◄

Билет 29

Седьмая проблема Гильберта. Формулировка теоремы Гельфонда-Шнейдера. Ее следствия. Построение вспомогательной функции для доказательства теоремы Гельфонда-Шнейдера, оценки ее порядка нуля.

В 1900 году Д.Гильберт в своем докладе на Втором международном конгрессе математиков назвал 23 проблемы "исследование которых может стимулировать дальнейшее развитие науки". Под номером семь фигурировала проблема трансцендентности алгебраических степеней алгебраических чисел. Частичное решение этой проблемы было найдено А.О.Гельфондом в 1929 году и Р.О.Кузьминым в 1930 году. Полностью ее решили независимо в 1934 году А.О.Гельфонд и Т.Шнейдер.

Теорема 32 (Гельфонда Шнейдера.) Пусть a алгебраическое число, отличное от 0 и 1, а α алгебраическое число, не являющееся рациональным. Тогда число $a^{\beta} = e^{\beta \ln(a)}$ трансцендентно.

Примечание. Под $\ln(a)$ понимается значение, взятое на любой ветви комплексного логарифма.
Следствия.

1. Число e^{π} трансцендентно.
   Утверждение легко следует из равенства $(e^{\pi})^{i} = -1$.

2. Если a и b алгебраические числа, отличные от 0 и 1, то число $\log_a(b) = \frac{\ln(b)}{\ln(a)}$ либо рационально, либо трансцендентно.
   Утверждение следует из основного логарифмического тождества.

Лемма 17 Пусть $\beta \in Z_A$ и

$$\beta^m = b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0, \quad b_j \in \mathbb{Z}, |b_j| \leq B. \tag{8}$$

Тогда для любой натуральной степени числа β справедливы утверждения:

$$\beta^t = b_{t,m-1}\beta^{m-1} + \cdots + b_{t,1}\beta + b_{t,0}, \quad b_{t,j} \in \mathbb{Z}, |b_{t,j}| \leq (B+1)^t.$$

Кроме того, если k и l неотрицательные целые числа, не превосходящие n, то

$$(k+l\beta)^t = B_{t,k,l,m-1}\beta^{m-1} + \cdots + B_{t,k,l,1}\beta + B_{t,k,l,0}; B_{t,k,l,j} \in \mathbb{Z}, |B_{t,k,l,j}| \leq (B+2)^t nt.$$

Билет 29

► Доказательство первого утверждения проводится по индукции. При $t \le m$ утверждение следует из 8. Пусть оно верно при t. Тогда в силу 8

$$\beta^{t+1} = b_{t,m-1}(b_{m-1}\beta^{m-1} + \cdots + b_0) + b_{t,m-2}\beta^{m-1} + \cdots + b_{t,0}\beta,$$

и из предположения индукции легко следует справедливость утверждения при $t+1$. Докажем второе утверждение

$$(k+l\beta)^t = \sum_{s=0}^{t} C_t^s k^{t-s} l^s \sum_{j=0}^{m-1} b_{sj}\beta^j,$$

откуда следует, что коэффициенты при β^j не провосходят

$$\sum_{s=0}^{t} C_t^s k^{t-s} l^s (B+1)^s = (k+l(B+1))^t \le (B+2)^t n^t$$

Лемма доказана. ◄

Лемма 18 Пусть β – целое алгебраическое число степени m. Тогда существует такая функция

$$f(z) = \sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a_{kl} e^{(k+l\beta)z}$$

с коэффициентами $a_{kl} \in \mathbb{Z}$, что

$$0 < \max_{k,l} |a_{kl}| < n^{\gamma_5 n},$$

$$f^{(t)}(0) = 0 \qquad t = \overline{0, [n^{\frac{3}{2}}] - 1}$$

► Мы имеем:

$$f^{(t)}(z) = \sum_{k,l=0}^{n-1} a_{kl}(k+l\beta)^t e^{(k+l\beta)z}, \tag{9}$$

поэтому по лемме 17

$$f^{(t)}(0) = \sum_{k,l=0}^{n-1} a_{kl}(k+l\beta)^t = \sum_{k,l=0}^{n-1}\sum_{s=0}^{m-1} B_{t,k,l,s}\beta^s a_{kl}$$

Приравняем к нулю коэффициенты при степенях β^s. Получим систему

$$\sum_{k,l=0}^{n-1}\sum_{s=0}^{m-1} B_{t,k,l,s} a_{kl} = 0, \qquad t = \overline{0, [n^{\frac{3}{2}}] - 1}, s = \overline{0, m-1},$$

состоящую из $p = m[n^{\frac{3}{2}}]$ уравнений относительно $q = n^2$ неизвестных a_{kl}. По лемме 17

$$|B_{t,k,l,s}| < (B+2)^t n^t < n^{2n^{\frac{3}{2}}} = A \qquad (t < n^{\frac{3}{2}})$$

и для завершения доказательства осталось применить лемму Зигеля.◄

Билет 29

Пусть X не зависящее от n натуральное число, которое будет выбрано в дальнейшем,

$$T = \min_{x=\overline{0,X}} ord|_{z=x\ln(a)} f(z) \tag{10}$$

Лемма 19 $[n^{\frac{3}{2}}] \leq ord|_{z=0} f(z) \leq n^2$

► Оценка снизу следует из леммы 18. Докажем правое неравенство. Допустим противное. Тогда

$$f^{(t)}(0) = \sum_{k,l=0}^{n-1} a_{kl}(k+l\beta)^t = 0, \qquad t = \overline{0, n^2-1}.$$

Получили систему из n^2 линейных уравнений с n^2 неизвестными a_{kl}. Определитель системы есть определитель Вандермонда. Он отличен от нуля, так как, ввиду иррациональности числа β, все числа $k+l\beta$ различны между собой. Следовательно, система может иметь лишь нулевое решение, что противоречит лемме 18. ◄

Билет 30

Оценки вспомогательной функции и завершение доказательства теоремы Гельфонда-Шнейдера.

Лемма 20 Справедливы неревенства

$$|f^{(T)}(x\ln(a))| < n^{-\gamma_6 n^{\frac{3}{2}}-\frac{1}{3}(X-6)^T}, \qquad x = \overline{0,X}.$$

►Доказательство этой леммы весьма сходно с доказательством леммы 16. На этот раз надо применить принцип максимума модуля к функции

$$g(z) = f(z)z^{-[n^{\frac{3}{2}}]}(z-\ln(a))^T \cdots (z-X\ln(a))^T$$

и положить $r = X|\ln(a)|+1 < \sqrt{n}$. ◄

Доказательство теоремы Гельфонда Шнейдера.
► Без ограничения общности можно считать, что число β целое алгебраическое, в противном случае умножим его на такое натуральное число b, чтобы $b\beta \in Z_A$, докажем, что число $a^{b\beta}$ трансцендентно, и уже отсюда легко установим трансцендентность числа a^{β}.
Из 10 следует, что существует такой индекс x_0, что $f^{(T)}(x_0\ln(a)) \neq 0$, причем эта производная является многочленом $P(\beta, a, a^{\beta})$ с целыми коэффициентами.
Допустим, что при выполненных условиях теоремы все три числа β, a и a^{β} алгебраические степеней соответственно m, m_1 и m_2. Тогда к многочлену $P(\beta, a, a^{\beta})$ можно применить обобщенную теорему Лиувилля. С помощью равенства 9 оценим его длину и степень:

$$L(P) \leq n^2 n^{\gamma_5 n}(2n)^T, \qquad deg(P) \leq T + 2nX.$$

Из обобщенной теоремы Лиувилля получаем, что

$$|f^{(T)}(x_0\ln(a))| = |P(\beta, a, a^{\beta})| > (L(P))^{1-mm_1m_2}C^{-deg(P)} > n^{-\gamma_7 n - mm_1m_2T}.$$

С другой стороны, по лемме 20 при $X = 3mm_1m_2 + 6$ выполняется неравенство

$$|f^{(T)}(x_0\ln(a))| < n^{-\gamma_6 n^{\frac{3}{2}} - mm_1m_2T}.$$

Последние две оценки при достаточно большом n противоречивы. Теорема доказана. ◄

2 Определения

Определение 1 $b \mid a$, если $\exists q \in \mathbb{Z} : a = bq$

Определение 2 $a \in \mathbb{Z}, b \in \mathbb{N} \Rightarrow \exists! q, r : \begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$ –деление с остатком

Определение 3 Дзета-функция Римана: $s = \sigma + it, \quad \zeta(s) := \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$

Определение 4 (Сравнения)
$a \equiv b \pmod{m} \iff m \mid (a-b) \iff a$ и b дают одинаковые остатки при делении на m

Определение 5 (Определение характера)
Пусть G – конечная группа, коммутативная по умножению.
$\chi : G \to \mathbb{C}$ – характер

1. $\chi(g) \not\equiv 0$
2. $\chi(g_1 \cdot g_2) = \chi(g_1) \cdot \chi(g_2)$

Определение 6 $L(s, \chi) = \sum\limits_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ – функция Дирихле.

Определение 7 Характер χ действительный, если $\chi^2 = \chi_0 = 1$

Определение 8 Число α – алгебраическое, если оно является корнем многочлена с рациональными коэффициентами, иначе трансцендентное.
Степень алгебраического числа α – степень неприводимого многочлена, имеющего корень α

Определение 9 Пусть α – алгебраическое число степени $n, \exists f \in \mathbb{Q}[x], deg(f) = n, \alpha$ – корень f, старший коэффициент $f = 1$, тогда f – минимальный многочлен.
Корни $\alpha_1, \ldots, \alpha_n$ минимального многочлена – сопряженные с α

Определение 10 Если $A(x) \in \mathbb{Z}[x]$, старший коэффициент = 1 – минимальный многочлен для α, то α – целое алгебраическое число.

Определение 11 $A(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}$ примитивный, если $(a_0, \ldots, a_n) = 1$

Определение 12 Многочлен $P(\alpha_1, \ldots, \alpha_n) \in K[\alpha_1, \alpha_n]$ симметрический, если он не изменяется при любой перестановке переменных.

Определение 13 $P(\alpha_1, \ldots, \alpha_n, \delta_1, \ldots, \delta_s)$ – симметричный многочлен относительно нескольких систем переменных, если он не изменяется при любой перестановке внутри каждой системы.

Определение 14 A – поле алгебраических чисел, расширение поля $\mathbb{Q}$

Определение 15 $\alpha = r(\theta) \Rightarrow N(\alpha) := r(\theta_1) \cdots r(\theta_n)$ – норма алгебраических чисел в поле.

Определение 16 α – число Лиувилля, если $\forall m \in \mathbb{N} \exists$ бесконечно много дробей $\frac{p}{q}$: $\quad 0 < |\alpha - \frac{p}{q}| < \frac{1}{q^m}$

Определение 17 Длина многочлена – сумма модулей коэффициентов. $L(P)$

3 Формулировки

Теорема 1 (Основная теорема арифметики)

1. всякое $a \in \mathbb{N}, a > 1$ представляется в виде $a = p_1 \cdots p_n$, где p_i простые.
2. это представление единственно с точностью до порядка сомножителей.

Теорема 2 (Теорема о представлении НОД)
$(a,b) = d \Rightarrow \exists u, v \in \mathbb{Z} : d = au + bv$

Утверждение 1 Пусть $a = p_1^{k_1} \cdots p_n^{k_n}, b = p_1^{l_1} \cdots p_n^{l_n}$. Тогда $b \mid a \iff \forall i : l_i \leq k_i$

Утверждение 2 $(a,b) = p_1^{s_1} \cdots p_n^{s_n}$, где $s_j = \min\{k_j, l_j\}$
$[a,b] = p_1^{t_1} \cdots p_n^{t_n}$, где $t_j = \max\{k_j, l_j\}$

Теорема 3 (Теорема о бесконечности простых чисел)
Простых чисел бесконечно много.

Лемма 1 $0 \leq l_1 = l_2 = l_3 \leq L_1 = L_2 = L_3 \leq +\infty$

Утверждение 3 $f(x)$ неубывающая на $[1;\infty] \Rightarrow$ если $\int\limits_1^\infty \frac{f(x)-x}{x^2} dx$ сходится то $f(x) \sim x, x \to \infty$

Теорема 4 (Теорема Чебышева)
$\exists a, b > 0 : \forall x \geq 2 : \quad a\frac{x}{\ln(x)} < \pi(x) < b\frac{x}{\ln(x)}$

Утверждение 4 $\alpha n \ln(n) < p_n < \beta n \ln(n)$

Теорема 5 (Теорема Эйлера)
$\sum_p \frac{1}{p}$ расходится.

Утверждение 5 $\alpha n \ln(n) < p_n < \beta n \ln(n)$

Теорема 6
$\sigma > 1 : -\frac{\zeta'(s)}{\zeta(s)} = \sum\limits_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$

Лемма 2
$f(n)$ – вполне мультипликативная, $A = \sum\limits_{k=1}^{\infty} f(k)$; $B = \sum\limits_{d=1}^{\infty} f(d)\Lambda(d)$ – абсолютно сходятся. Тогда $AB = \sum\limits_{n=1}^{\infty} f(n)\ln(n)$

Теорема 7
В области $\sigma > 1 : \zeta(s) = \prod\limits_{p}(1 - \frac{1}{p^s})^{-1}$

Лемма 3
$f(n)$ – вполне мультипликативная, ряд $\sum f(n)$ абсолютно сходится $\Rightarrow S = \sum\limits_{n=2}^{\infty} f(n) = \prod\limits_{p}(1 - f(p))^{-1}$

Теорема 8 Преобразование Абеля. $\sum\limits_{n\le x} a_n g(n), a_n \in \mathbb{C}, g(x)$ – комплекснозначная функция действительного аргумента.
$x \in [1, +\infty); \exists$ непрерывная $g'(x)$, $\sum\limits_{n\le x} a_n = A(x)$

1. $\sum\limits_{n\le x} a_n g(n) = A(x)g(x) - \int\limits_{1}^{x} A(t)g'(t)dt$
2. если $\lim\limits_{x\to\infty} A(x)g(x) = 0$, то $\sum\limits_{n=1}^{\infty} a_n g(n) = \int\limits_{1}^{\infty} A(t)g'(t)dt$

Лемма 4 $\forall 0 < r < 1, \varphi \in \mathbb{R} \Rightarrow M = \left|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})\right| \le 1$

Лемма 5 При $\sigma > 1 : |\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \ge 1$

Теорема 9 При $\sigma \ge 1 \quad \zeta(s) \ne 0$

Теорема 10 (Асимптотический закон распределения простых чисел.)
$\pi(x) \sim \frac{x}{\ln(x)}, x \to \infty$

Утверждение 6 $f(s) = -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ аналитическая при $\sigma \ge 1$

Утверждение 7 $p_n \sim n\ln(n)$ – закон распределения n-того простого.

Лемма 6 $ax \equiv b \pmod{m}, (a,m) = 1 \Rightarrow \exists! c < m : x \equiv c \pmod{m}$

Теорема 11 (Теорема Эйлера) $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

Теорема 12 (Малая теорема Ферма) p-простое, $(p,a) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Утверждение 8 $p \mid (a^2 + b^2), p \nmid a, p \neq 2 \Rightarrow p = 4m + 1$

Утверждение 9 Бесконечность множества простых вида $4n - 1$.

Утверждение 10 Бесконечность множества простых вида $4n + 1$.

Рассмотрим набор корней из 1:$\zeta_1, \ldots, \zeta_n : \zeta_i^{h_i} = 1$
$\chi(g) = \zeta_1^{r_1} \cdots \zeta_n^{r_n}$

Утверждение 11 Это характер и любой характер можно записать так.

Утверждение 12

1. $S = \sum\limits_{g \in G} \chi(g) = \begin{cases} h, \chi = \chi_0 \\ 0, \chi \neq \chi_0 \end{cases}$
2. $\sigma = \sum\limits_{\chi} \chi(g) = \begin{cases} h, g = e \\ 0, e \neq e \end{cases}$

Утверждение 13

1. Ряд $\sum\limits_n \frac{a_n}{n^s}$ равномерно сходится в $D(\delta, \theta)$
2. $f(s)$ аналитична в области $\sigma > 0$, где $f(s) = \sum\limits_n \frac{a_n}{n^s}$

Теорема 13 Пусть функция $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}, \sigma_1 < \sigma_2 < \sigma_0$

1. $f(s)$ аналитична при $\sigma > \sigma_1$
2. $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}, \quad (\sigma > \sigma_2)$
3. $a_n \geq 0$

Тогда $f(s)$ раскладывается в ряд Дирихле при $\sigma > \sigma_1$ и его можно почленно дифференцировать. $/// < WTF?$
/*P.S. в другом источнике: Тогда $f(s)$ аналитична при $\sigma > \sigma_1$, т.е. можно продлить представление рядом.*/

Лемма 7 $f(s) := \zeta(s)L(s,\chi) \Rightarrow$

1. $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \sigma > 1$
2. $a_n \geq 0$
3. $a_{n^2} \geq 1$
4. $\sum\limits_{n=1}^{\infty} \frac{a_n}{\sqrt{n}}$ расходится.

Теорема 14 χ– действительный характер, тогда $L(1,\chi) \neq 0$

Лемма 8 Пусть $s \in \mathbb{R}, s > 1$, тогда $A := |L^3(s,\chi_0) \cdot L^4(s,\chi) \cdot L(s,\chi^2)| \geq 1$

Теорема 15 При $\chi \neq \chi_0 : L(1,\chi) \neq 0$

Теорема 16 (Теорема Дирихле) Пусть $m \geq 2$. В прогрессии $mx+l, (m,l) = 1$ бесконечно много простых.

Лемма 9 Если $\varphi(x) \in \mathbb{Q}[x]$ имеет общий корень с неприводимым многочленом $f(x)$, то $f(x)$ – делитель $\varphi(x) \Rightarrow$ каждый корень $f(x)$ является корнем $\varphi(x)$

Лемма 10 Неприводимый многочлен $f(x) \in \mathbb{Q}[x]$ не может иметь кратных корней.

Утверждение 14 $B(x) \in \mathbb{Q}[x], A(x)$ – минимальный многочлен α, $\forall$ корня $B(x)$ это корень $A(x) \Rightarrow B(x) = \Lambda A^m(x)$

Теорема 17 Пусть $B(x) \in \mathbb{Z}[x], b_n = 1, B(\alpha) = 0 \Rightarrow \alpha$ – целое алгебраическое.

Лемма 11 (Гаусса) $A(x), B(x)$ примитивные, тогда $C(x) = A(x)B(x)$ тоже примитивный.

Теорема 18 (о симметричных многочленах) Любой симметричный многочлен от переменных $\alpha_1, \ldots, \alpha_n$ единственным образом представляется в виде $P(\alpha_1, \ldots, \alpha_n) = H(\sigma_1, \ldots, \sigma_n)$, где $H \in K[\sigma_1, \ldots, \sigma_n]$, $\sigma_1, \ldots, \sigma_n$ – элементарные симметричные.

Теорема 19 (о симметричных многочленах от нескольких систем) Любой симметричный многочлен от нескольких систем переменных $\alpha_1, \ldots, \alpha_n, \delta_1, \ldots, \delta_m$ единственным образом представляется в виде $P(\alpha_1, \ldots, \alpha_n, \delta_1, \ldots, \delta_m) = H(\sigma_1, \ldots, \sigma_n, \eta_1, \ldots, \eta_m)$, где $\sigma_1, \ldots, \sigma_n, \eta_1, \ldots, \eta_m$ – элементарные симметричные.

Лемма 12 Пусть $\alpha, \ldots, \delta$ – алгебраические числа, $\alpha_1, \ldots, \alpha_n, \delta_1, \ldots, \delta_m$ – соответствующие сопряженные. $P(x, \alpha_1, \ldots, \delta_m) \in \mathbb{Q}[x, \alpha_1, \ldots, \delta_m]$ – симметрический относительно систем. Тогда $P \in \mathbb{Q}[x]$, т.е. не зависит от корней, а если не зависит от x, то тоже $\in \mathbb{Q}[x]$

Теорема 20 Если α, β – алгебраические числа, то $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ – тоже алгебраические. (что значит что множество алгебраических чисел образуют поле)

Теорема 21 A – алгебраически замкнутое (и любой многочлен разлагается на линейные множители), т.е. если ξ – корень $\varphi(x) = x^m + \alpha x^{m-1} + \cdots + \delta$, $\alpha, \ldots, \delta$ – алгебраические, то ξ алгебраическое.

Теорема 22 $Q(\theta) = \{ r_{n-1}(\theta), r_{n-1}(\theta) \in \mathbb{Q}[x], deg(r_{n-1}) \leq n-1 \quad \}$

Теорема 23 $r(\theta_1), \ldots, r(\theta_n)$ – тот же набор, что и $\alpha_1, \ldots, \alpha_m, \frac{n}{m} \in \mathbb{N}$

Теорема 24 (о примитивном элементе) $Q(\alpha_1, \ldots, \alpha_n)$. Тогда $\exists \theta : Q(\alpha_1, \ldots, \alpha_n) = Q(\theta)$

Теорема 25 (Теорема Дирихле) Пусть $\alpha \in \mathbb{R} \Rightarrow \forall x \in \mathbb{N} \exists \frac{p}{q} : \begin{cases} \left| \alpha - \frac{q}{p} \right| < \frac{1}{xq} \\ x \geq q \geq 1 \end{cases}$

Теорема 26 (Теорема Дирихле) $\alpha \in \mathbb{R} \setminus \mathbb{Q} \Rightarrow$ неравенство $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ имеет бесконечное число решений в рациональных дробях.

Теорема 27 $\forall f(q) > 0 \, \exists \alpha : 0 < \left|\alpha - \frac{p}{q}\right| < f(q)$ имеет бесконечное число решений. (т.е. существует сколь угодно хорошо приближаемые числа).

Теорема 28 (Лиувилля) $\alpha \in A \cap \mathbb{R}, n = deg(\alpha) \geq 2 \Rightarrow \exists C = C(\alpha) > 0 : \forall \frac{p}{q} : \left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$

Утверждение 15 Числа Лиувилля трансцендентные.

Теорема 29 Пусть $\alpha_1, \ldots, \alpha_s$ – алгебраические числа степеней $m_1, \ldots, m_s$. Тогда $\exists$ положительная постоянная $C = C(\alpha_1, \ldots, \alpha_s) : \forall P(x_1, \ldots, x_s) \in \mathbb{Z}[x_1, \ldots, x_s]$, тогда $P(\alpha_1, \ldots, \alpha_s) = 0$ или $|P(\alpha_1, \ldots, \alpha_s)| \geq L^{1-(m_1 \cdots m_s)} C^{-d}, \quad d, L$ – степень и длина P

Теорема 30 (Бореля) Рассмотрим $M = \{\alpha \in \mathbb{R} : 0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$, $m > 2$ имеют бесконечное число решений $\}$, тогда $\mu(M) = 0$

Утверждение 16 e иррационально.

Утверждение 17 e трансцендентно.

Утверждение 18 π иррационально.

Лемма 13 Пусть $a_{ij} \in \mathbb{Z}, |a_{ij}| < A$ и $L_i(\bar{x} = \sum_{j=1}^{q}) a_{ij} x_j, \quad i = \overline{1, p}, p < q.$

Тогда система уравнений $L_i(\bar{x}) = 0$ имеет решение $(x_1^{(0)}), \ldots, x_q^{(0)}$, $x_j^{(0)} \in \mathbb{Z} : \quad 0 < \max_j |x_j^{(0)}| \leq 1 + (qA)^{\frac{p}{q-p}}$.

Теорема 31 (Линдемана) Если α – алгебраическое число, отличное от нуля, то число e^{α} трансцендентно.

Лемма 14 Существует такая функция $f(z) = \sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a_{kl} z^k e^l z$ с коэффициентами $a_{kl} \in \mathbb{Z}$, что $0 < \max_{k,l} |a_{kl}| < n^{\gamma_1 n}$

$f^{(t)}(0) = 0, t = \overline{0, [n^{\frac{3}{2}}] - 1}$, где $[\cdot]$ целая часть числа.

Лемма 15 $[n^{\frac{3}{2}}] \leq ord|_{z=0} f(z) \leq n^2$

Лемма 16 Справедливы неравенства

$$|f^{(T)}(x\alpha)| < n^{-\gamma_2 n^{\frac{3}{2}} - \frac{1}{3}(X-6)^T}, \qquad x = \overline{0, X}$$

Теорема 32 (Гельфонда Шнейдера.) Пусть a алгебраическое число, отличное от 0 и 1, а α алгебраическое число, не являющееся рациональным. Тогда число $a^\beta = e^{\beta \ln(a)}$ трансцендентно.

Лемма 17 Пусть $\beta \in Z_A$ и

$$\beta^m = b_{m-1}\beta^{m-1} + \cdots + b_1\beta + b_0, \quad b_j \in \mathbb{Z}, |b_j| \leq B. \tag{11}$$

Тогда для любой натуральной степени числа β справедливы утверждения:

$$\beta^t = b_{t,m-1}\beta^{m-1} + \cdots + b_{t,1}\beta + b_{t,0}, \quad b_{t,j} \in \mathbb{Z}, |b_{t,j}| \leq (B+1)^t.$$

Кроме того, если k и l неотрицательные целые числа, не превосходящие n, то

$$(k + l\beta)^t = B_{t,k,l,m-1}\beta^{m-1} + \cdots + B_{t,k,l,1}\beta + B_{t,k,l,0}; B_{t,k,l,j} \in \mathbb{Z}, |B_{t,k,l,j}| \leq (B+2)^t nt.$$

Лемма 18 Пусть β – целое алгебраическое число степени m. Тогда существует такая функция

$$f(z) = \sum_{k=0}^{n-1}\sum_{l=0}^{n-1} a_{kl} e^{(k+l\beta)z}$$

с коэффициентами $a_{kl} \in \mathbb{Z}$, что

$$0 < \max_{k,l} |a_{kl}| < n^{\gamma_5 n},$$

$$f^{(t)}(0) = 0 \qquad t = \overline{0, [n^{\frac{3}{2}}] - 1}$$

Лемма 19 $[n^{\frac{3}{2}}] \leq ord|_{z=0} f(z) \leq n^2$

Лемма 20 Справедливы неревенства

$$|f^{(T)}(x\ln(a))| < n^{-\gamma_6 n^{\frac{3}{2}} - \frac{1}{3}(X-6)^T}, \qquad x = \overline{0,X}.$$