# ТЧ-8 2024

SFS

21 июня 2024 г.

## Содержание

1 Билеты 2

2 Определения и формулировки 31

# 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
$$\int\limits_1^\infty \frac{\psi(x)-x}{x^2}dx$$

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 $\chi$ 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 $\chi$.

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 $\boldsymbol{e}$.

25. Билет 25 Иррациональность числа $\boldsymbol{\pi}$.

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

Свойства делимости:

1. $b|a_1, \ldots, b|a_n \Rightarrow b|(a_1 + \cdots + a_n)$
2. $b|a_1, \ldots, b|a_{n-1}, b \not| a_n \Rightarrow b \not| (a_1 + \cdots + a_n)$
3. $c|a, d|b \Rightarrow cd|ab$, в частности, $\forall b : c|a \Rightarrow c|ab$

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 $p_i = q_i$, то $\frac{a}{p_i}$ раскладывается двумя способами $\Rightarrow$ противоречие
Без ограничения общности пусть $p_1 > q_1$
Рассмотрим $b = \overbrace{(p_1 - q_1)}^{>0} p_2 \cdots p_m = p_1 \cdots p_m - q_1 p_2 \cdots p_m = q_1 \cdots q_n - q_1 p_2 \cdots p_m = q_1(q_2 \cdots q_n - p_2 \cdots p_m)$
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. $(p - q) \not| q$
$b < a$, 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)
$(a, b) = d \Rightarrow \exists u, v \in \mathbb{Z} : d = au + bv$

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

1. $\mu \neq \varnothing$, т.к. $\pm a; b \in \mu$
2. $d$ – наименьший элемент $\mu$
3. Докажем, что $d|a$ и $d|b$
   Пусть $d \not| a \Rightarrow a = dq + r, 0 < r < d, r = a - dq = a - (qu + bv)q = a(1 - qu) + b(-qu) \in \mu$, но $r < d$ противоречие.
4. $d = (a, b)$, т.к. если $\exists d_1 : d_1 | a, d_1 | b \Rightarrow d_1 | d \Rightarrow d_1 \le d$

◄
Следствия:

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

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 $b|a \iff \forall i : l_i \leq k_i$

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

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

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. $d|a, d|b, d = p_1^{r_1} \cdots p_n^{r_n} \Rightarrow r_i \leq k_i, r_i \leq l_i \Rightarrow r_i \leq \min\{k_j, l_j\} \Rightarrow \max r_i = \min\{k_j, l_j\}$
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 $p : p|N$, 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.

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

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 $f(x)\sim x, x\to\infty$

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

$a) \int\limits_y^{(1+\delta)y}\frac{f(x)-x}{x^2}dx \ge \int\limits_y^{(1+\delta)y}\frac{f(y)-x}{x^2}dx > \int\limits_y^{(1+\delta)y}\frac{(1+\delta)y-x}{x^2}dx = \int\limits_1^{1+\delta}\frac{(1+\delta)y-ty}{t^2y^2}ydt =$

$\int\limits_{1}^{1+\delta} \frac{1+\delta-t}{t^2} dt = \varepsilon > 0 \Rightarrow$ отрицание критерия Коши.

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

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

Таким образом, $\int\limits_{1}^{\infty} \frac{\psi(x)-x}{x^2} dx$ 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)

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

► Сверху: $2^{2n} > C_{2n}^n = \frac{(n+1)\cdots(n+n)}{n!} \geq \prod n < p \leq 2np$, в числитель входят все простые $n < p \leq 2n$

$\Rightarrow 2n\ln(2) > \sum\limits_{n<p\leq 2n} \ln(p) = \theta(2n) - \theta(n)$. Рассмотрим $n = 2^k$

$\theta(2^k) = \sum\limits_{k=0}^{m-1}(\theta(2^{k+1}) - \theta(2^k)) < \sum\limits_{k=0}^{m-1} 2^k\ln(2) < \ln(2)\cdot 2^{m+1}$

$\theta(x)$ 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:$0 < I_n = \int\limits_0^1 x^n(1-x)^n dx < \left(\frac{1}{4}\right)^n \qquad x^n(1-x)^n = a_0 + a_1x + a_2x^2 + \cdots + a_{2n}x^{2n} \Rightarrow I_n = \frac{a_0}{1} + \cdots + \frac{a_{2n}}{2n+1}$

Пусть $Q_{2n+1} := [1, 2, \ldots, 2n+1] \Rightarrow Q_{2n+1}I_n \in \mathbb{Z}, Q_{2n+1}I_n > 0 \Rightarrow 1 \leq Q_{2n+1}I_n \leq e^{\psi(2n+1)}\left(\frac{1}{4}\right)^n$

$\Rightarrow \psi(2n+1) > 2\ln(2), \qquad \psi(x) \geq \psi(2(\left[\frac{x}{2}\right]-1)+1) \geq 22(\left[\frac{x}{2}\right]-1)\ln(2) \geq (x-4)\ln(2) \Rightarrow$ подойдет $a = \ln(2)$ ◄

Теорема 5 (Теорема Эйлера)

$\sum_p \frac{1}{p}$ расходится.

► $S_N = \prod\limits_{p\leq N}(1-\frac{1}{p})^{-1} = \prod\limits_{p\leq N}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \sum\limits_{\substack{p\leq N\\ p|n}} > \sum\limits_{n=1}^{N}\frac{1}{n}$ – 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 4 $\alpha n\ln(n) < p_n < \beta n\ln(n)$

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

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: $s = \sigma + it, \zeta(s) := \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$

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

►

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

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

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

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

$f(n) = \frac{1}{n^s}, s = \sigma + it, \sigma > 1 \Rightarrow$ 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 $\sum\limits_{n=1}^{\infty} a_n g(n) = \int\limits_1^{\infty} A(t)g'(t)dt$

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

$2) x \notin \mathbb{Z} : N = [x]$
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 ◄

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.◄

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 $\sigma > 1 : \zeta(\sigma+it) \neq 0, ..0 \geq 1$
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.
$\zeta'(1+it) = \lim \sigma \to 1 \frac{\zeta(\sigma+it)-\zeta(1+it)}{\sigma-1} \Rightarrow \left|\frac{\zeta(\sigma+it)}{\sigma-1}\right| \leq C_2$
$|\zeta(\sigma+2it)| \leq C_3$
$\Rightarrow |\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \leq \left(\frac{C_1}{\sigma-1}\right)^3(C_2(\sigma-1))^4C_3 \to 0$. Противоречие с $|\cdot| > 1$ ◄

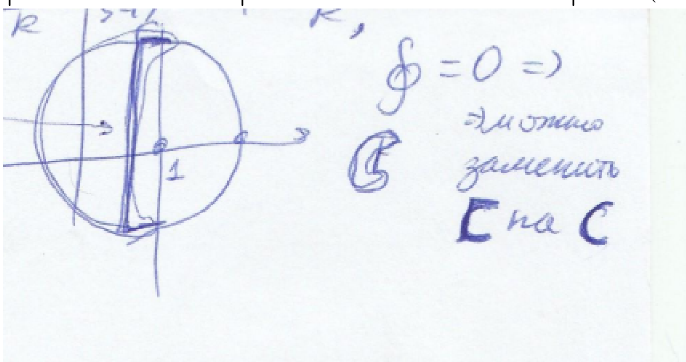
**Билет 7**

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. $f(1) - f_u(1) = \frac{1}{2\pi iR} \cdot \oint\limits_{\Gamma(\theta,R)} (f(s) - f_u(s))u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right) ds = \frac{1}{2\pi iR} \int F_k(s)ds$ вычет в точке $s = 1$
5. $\left|\frac{1}{2\pi iR} \int\limits_{C_R} F_k(s)ds\right| \leq \frac{B}{R} \Rightarrow \left|\frac{1}{2\pi iR} \int\limits_{(ris)} f_u(s)u^{s-1} \left(\frac{s-1}{R} + \frac{R}{s-1}\right) ds\right| \leq \frac{B}{R}$




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

   $\lim\limits_{u\to\infty} J(u) = 0$

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

   Значит $|\int\limits_{BC} g(s)u^{s-1}ds| \leq M2Ru^{\theta-1} \to 0, u \to \infty \Rightarrow \lim\limits_{u\to\infty} f_u(1) = f(1) \Rightarrow$ интеграл сходится $\Rightarrow$ асимптотический закон. ◀

Билет 8

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

1. Утверждение 5 $f(s) = -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ 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, $u > 1$

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

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

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

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

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

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

Утверждается что предел равен 0.

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

Утв $\lim\limits_{u\to\infty} J(u)=0.$

▷ $g(s):=\frac{1}{2\pi iR} f(s)\left(\frac{s-1}{R}+\frac{R}{s-1}\right)ds$ – огр. на контуре

тогда 1) $\int\limits_{\theta+iR}^{1+iR} g(s)u^{s-1}ds \le M\frac{u^{\sigma-1}}{\ln u}\Big|_{-\infty}^{1} = \frac{M}{\ln u} < \frac{\varepsilon}{\delta}$ $(u>u_1)$

2) $\left|\int\limits_{BC} g(s)u^{s-1}ds\right| \le M\cdot 2Ru^{\theta-1} \to 0 \ (u\to+\infty)$

Т.о. $\forall \varepsilon>0\ \exists u_0 : \forall u>u_0\ |f(1)-f_u(1)|<\varepsilon.$

$\Rightarrow \lim\limits_{u\to+\infty} f_u(1)=f(1)$, т.е. интеграл сх-ся.

Утверждение 6 $p_n \sim n\ln(n)$ – 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)
$a \equiv b \pmod m \iff m|(a-b) \iff a$ 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 $ax \equiv b \pmod m, (a,m)=1 \Rightarrow \exists! c < m : x \equiv c \pmod m$

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

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 7 $p|(a^2+b^2), p \not| a, p \neq 2 \Rightarrow p = 4m+1$

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

Утверждение 8 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. $\exists q | p : q = 4k-1$, т.к. если все делители имеют вид $4k+1$, то и $p \equiv 1 \pmod 4$, но $q \neq p_j$ противоречие.◄

Утверждение 9 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 $\chi$ 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. $\chi(e) = 1 \qquad \blacktriangleright\ \chi(e\cdot e) = \chi(e)\cdot\chi(e)\ \blacktriangleleft$
2. $g^h = e \Rightarrow (\chi(g))^h = 1 \Rightarrow$ характеры принимают значения только корней из 1.
3. $\chi(g^{-1}) = \frac{1}{\chi(g)}$
4. $\chi_0(g) \equiv 1$ – главный характер.
5. $\chi_1\chi_2(g) := \chi_1(g)\cdot\chi_2(g)$

Характеры образуют группу. $\blacktriangleright$

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. $\exists 1 : \chi\chi^{-1}(g) = 1$

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.
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 10 Это характер и любой характер можно записать так.

$\blacktriangleright$ 1)$g = g_1^{k_1} \cdots g_n^{k_n} \qquad k_j = r_j + a_j h_j \Rightarrow g = g_1^{r_1} \cdots g_n^{r_n}$ 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. $\blacktriangleleft$

Если $\chi \neq \chi_0$, то $\exists g : \chi(g) \neq 1$
Если $g \neq e$, то $\exists \chi : \chi(g) \neq 1$

Утверждение 11

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

$\sum\limits_{x=1}^{m} \chi(x) = \begin{cases} \varphi(m), \chi = \chi_0 \\ 0 \end{cases}$
$\sum\limits_{\chi} \chi(x) = \begin{cases} \varphi(m), x = 1 \\ 0 \end{cases}$
$|\sum\limits_{x=1}^{mq+r} \chi(x)| = |\sum\limits_{x=mq+1}^{mq+r} \chi(x)| \leq r \leq m$

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.

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

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

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

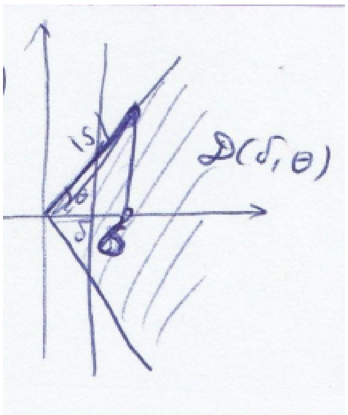
$\chi_0(p) = \begin{cases} 1, (m,p) = 1 \\ 0 \end{cases} \quad \Rightarrow L(s,\chi) = \prod\limits_{p \nmid m} (1 - \frac{1}{p^s})^{-1}$

$L(s,\chi_0) = \zeta(s) \prod\limits_{p|m} (1 - \frac{1}{p^s})^{-1} = \left(\frac{1}{s-1} + f(s)\right) \prod\limits_{p|m} (1 - \frac{1}{p^s})^{-1} = \frac{a_m}{s-1} + f_m(s), \qquad a_m = \prod\limits_{p|m} (1 - \frac{1}{p^s}) = \frac{\varphi(m)}{m} > 0 \Rightarrow L(s,\chi_0)$ 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 12

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

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

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

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

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

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

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

Для любой точки правее нуля можно подобрать такие $\delta$ и $\theta$, 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 $f(s)$ :

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. $/// < WTF?$

► 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 $\chi$.

Определение 7 Характер $\chi$ 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.

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

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

Если $n=k^2$, то все $k_j\%2==0\Rightarrow$

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

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

$\blacktriangleright$ $L(1,\chi)=0\Rightarrow L(s\chi)=(s-1)g(s),\quad g(s)$ 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 $\blacktriangleleft$

Билет 15

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

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

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

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

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

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

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

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

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

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

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

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 $(1,2)$ $\quad F(s)$ 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 $\alpha$ – алгебраическое, если оно является корнем многочлена с рациональными коэффициентами, иначе трансцендентное.
Степень алгебраического числа $\alpha$ – степень неприводимого многочлена, имеющего корень $\alpha$

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

Определение 9 Пусть $\alpha$ – 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 $\alpha$

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.

Утверждение 13 $B(x) \in \mathbb{Q}[x], A(x)$ – минимальный многочлен $\alpha$, $\forall$ 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 $\alpha$, то $\alpha$ – 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 $\forall p : \exists c_j : p \nmid c_j$
$\forall p \exists a_s, b_t : p \nmid a_s, p \nmid b_t, p | a_0, \ldots a_n, b_0, \ldots b_m$.
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 $\alpha$. 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 $\alpha$ – 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.

## 2 Определения и формулировки

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

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.

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

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 $b|a \iff \forall i : l_i \le k_i$

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

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)
$\exists a.b > 0 : \forall x \ge 2 : \quad a\frac{x}{\ln(x)} < \pi(x) < b\frac{x}{\ln(x)}$

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

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

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

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 $AB = \sum\limits_{n=1}^{\infty} f(n) ln(n)$

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 5 $f(s) = -\frac{\zeta'(s)}{zeta(s)} - \frac{1}{s-1}$ аналитическая при $\sigma \ge 1$

Утверждение 6 $p_n \sim n \ln(n)$ – закон распределения $n$-того простого.

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

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 7 $p|(a^2+b^2), p \not| a, p \ne 2 \Rightarrow p = 4m+1$

Утверждение 8 Бесконечность множества простых вида $4n-1$.

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

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

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

Утверждение 10

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

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

Утверждение 11

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 $f(s)$ :

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.

Определение 7 Характер $\chi$ 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.

Теорема 14 $\chi$– 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.

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

Определение 9 Пусть $\alpha$ – 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 $\alpha$

Утверждение 12 $B(x) \in \mathbb{Q}[x], A(x)$ – минимальный многочлен $\alpha$, $\forall$ корня $B(x)$ это корень $A(x) \Rightarrow B(x) = \Lambda A^m(x)$

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

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

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