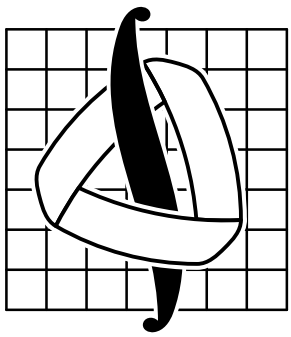
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет



Курс лекций по теории чисел

Лектор — Юрий Валентинович Нестеренко

IV курс, 7 семестр, поток математиков

Москва, 2006 г.

Предисловие

От наборщика

Что можно сказать про эти лекции? Я думаю, что они оказались вполне качественными. В первую очередь из-за того, что Нестеренко — отличный лектор. Поэтому при наборе не приходилось особо задумываться над различными утверждениями — всё было понятно. Ну, разумеется, как во всяком продукте человеческого труда, здесь возможны разные нехорошие баги. Увидите их — сообщайте мне. Желаю приятного ботанья!

Выражаю благодарность Диме и Мише Вельтищевым за помощь в наборе, за выслушивание моих глупых вопросов по особенностям TEX'а и MetaPost'а и за контроль TEX-нической грамотности, а также Кабировой Гульнаре за предоставление некоторых лекций, на которых я не присутствовал (да-да, и такое бывало).

Юхименко Александр (alesandro1985@mail.ru)

От редакции

Мы выражаем благодарность наборщику, без деятельности которого этот курс не существовал бы. Текст полностью отредактирован, часть доказательств написана более подробно.

В этой версии вроде нейтрализованы все опечатки, поступившие нам до 17-го января. Кресты на полях убраны, потому что лажи исправлено много, и новые кресты ставить лень.

Пока глобально остаётся неисправленным две вещи: **1°**: более подробное рассуждение про выбор T в первой главе (спасибо Саше Юхименко и Мише Левину за замечания), и **2°**: ещё нужно капитально пропатчить текст теоремы Линдемана – Вейерштрасса и её окрестностей. Многое там этом разделе ещё **не исправлено**, сейчас маловато времени. Если оно появится, редактура по **1°** появится сегодня-завтра, если нет — после 22-го января. Редактура **2°** в любом случае дело очень ответственное, и там нужно много того, чего сейчас нет, а именно времени.

Последняя компиляция: 17 февраля 2006 г.
Обновления документа — на сайте http://dmvn.mexmat.net.
Об опечатках и неточностях пишите на dmvn@mccme.ru.

Благодарности

Благодарность за поиск лажи выражается Паше Наливайко, Володе Филатову, Юре Дружинину, самому товарищу наборщику, Альмире Червовой, Сергею Гладких, Коле Рудому, Мише Левину, Мише Берштейну, Юре Притыкину и даже Сене Акопяну, который вообще с другого потока.

Используемые обозначения

Обычно простое число мы будем обозначать буквой p (если p занята, то далее по алфавиту q или r). Если встречается запись $\sum_{p<x}$, то это означает, что суммирование ведется по всем простым числам, меньшим x. Иногда, разумеется, мы будем использовать букву p для обозначения произвольного натурального числа, не обязательно простого.

- $p \mid x$ — означает, что число p делит число x.
- $x \vdots p$ — означает, что число x делится на p.
- (a, b) — наибольший общий делитель (НОД) чисел a и b. Аналогичное обозначение используется и для НОД нескольких чисел: $(a_1, \ldots, a_n)$.
- $[a, b]$ — наименьшее общее кратное (НОК) чисел a и b. Аналогичное обозначение используется и для НОК нескольких чисел: $[a_1, \ldots, a_n]$.
- $f(x) \sim g(x) \Leftrightarrow \frac{f(x)}{g(x)} \to 1$, $x \to \infty$.
- $\#A$ — количество элементов в множестве A.
- $\mathbb{Z}_+$ — множество целых неотрицательных чисел.

Литература

[1] *Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б.* Введение в теорию чисел. — М.: Изд-во Моск. ун-та, 1984.

[2] *Хасс.* Лекции по теории чисел.

Оглавление

1. Введение

1.1. Простые числа

Определение. Натуральное число n называется *составным*, если может быть представлено в виде $n = uv$, где $u, v > 1$. Натуральное число, не являющееся составным, называется *простым*. Число 1 не является ни простым, ни составным по определению.

Вот пара интересных примеров простых чисел: $\underbrace{11\ldots11}_{32}4\underbrace{11\ldots11}_{32}$ и $2^{13466917} - 1$.

Утверждение 1.1. *Пусть $M \in \mathbb{N}$ и $p > 1$ — наименьший делитель M. Тогда p — простое.*

□ Предположим, что $p = uv$, где $u, v > 1$. Тогда u и v — делители M, меньшие p. ■

Теорема 1.2 (Евклид). *Множество простых чисел бесконечно.*

□ Допустим, существует лишь конечное множество простых чисел $\{p_1, \ldots, p_n\}$. Рассмотрим число $M := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Пусть p — его наименьший делитель. Очевидно, M не делится ни на одно из чисел p_i. Согласно предыдущему утверждению, либо число p является простым, либо $p = 1$ (то есть само число M простое). В обоих случаях мы получили ещё одно простое число. ■

С древних времен известен способ нахождения простых чисел (решето Эратосфена). К настоящему моменту имеются некоторые его модификации, которые лишь незначительно ускоряют процесс поиска.

Теорема 1.3 (Решето Эратосфена). *Выписываем числа $1, 2, 3, \ldots, n$ и вычёркиваем единицу. Далее, первое незачёркнутое число p обводим рамкой и вычёркиваем все числа, кратные ему, начиная с p^2. Затем берём первое невычеркнутое и необведённое число, с ним делаем то же самое, и так далее. Обведённые числа суть все простые числа в диапазоне от 1 до n.*

□ Заметим, что вычеркиваются лишь составные числа, поэтому простые останутся невычеркнутыми. Предположим, что число a не вычеркнуто, и $a = pv$, где $p, v > 1$. Пусть p — минимальный делитель a. Тогда он прост. Но $p^2 \leqslant pv = a$, значит, число a в свое время нужно было вычеркнуть. ■

Составных чисел бесконечно много, но их в некотором смысле гораздо больше, чем простых. Вот пример отрезка натурального ряда длины $n - 1$, состоящего сплошь из составных чисел: $n! + 2, n! + 3, \ldots, n! + n$. Таким образом, между простыми числами встречаются сколь угодно большие пробелы.

Тем не менее, в натуральном ряду встречаются и отрезки, на которых простых чисел сравнительно много. Так, на отрезке $\left[10^{15}, 10^{15} + 150000\right]$ расстояние между соседними простыми числами не превосходит 276.

До сих пор не доказан факт бесконечности пар простых чисел вида $(n - 1, n + 1)$ (гипотеза «близнецов»). Самая большая на сегодняшний день такая пара — это $(291 \cdot 2^{1553} \pm 1)$.

Еще одна до сих пор нерешённая задача (проблема Гольдбаха): каждое чётное число представимо в виде суммы двух простых. В 1937 году И. М. Виноградов доказал, что каждое нечётное число представимо в виде суммы трёх простых.

А вот пример уравнения в целых числах (уравнение Пелля), которое очень непросто решить прямым перебором: $x^2 - 109y^2 = 1$. Его минимальное по модулю решение $(x_{\min}, y_{\min}) = (158070671986249, 15140424455100)$.

1.2. Основная теорема арифметики

Теорема 1.4 (Основная теорема арифметики). *Для любого натурального m существует и единственно его представление в виде $m = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$, где p_i — простые числа.*

Существование такого разложения легко доказывается по индукции. Мы не будем проводить его здесь. Единственность легко доказывается с помощью двух полезных лемм, приведённых ниже.

Лемма 1.5 (О линейном представлении НОД). *Если $(a, b) = d$, то существуют числа $x, y \in \mathbb{Z}$, такие что $d = ax + by$.*

Мы приведём два доказательства этой леммы. Одно — так называемое неэффективное (поскольку не даёт явных значений x и y), а второе — эффективное (то есть даёт явный алгоритм построения чисел x и y).

□ **1°** *Неэффективное:* рассмотрим множество

$$M = \{m = ax + by \mid m > 0,\ x, y \in \mathbb{Z}\}. \tag{1}$$

Пусть $d = (a, b)$. Тогда, очевидно, для любого $m \in M$ имеем $d \,\big|\, m$. Пусть z — минимальное число в M. Число d делит z как и всякое прочее число из M. Пусть m — произвольное число из M. Докажем, что $z \,\big|\, m$. Предположим, что это не так. Разделим m на z с остатком: $m = qz + m'$, $0 < m' < z$. Тогда $m' = m - qz$ — это линейная комбинация чисел из M, поэтому m' тоже является числом из M. Это противоречит минимальности z в M. Поэтому $z \,\big|\, m$. А поскольку m — произвольное число из M, то, в частности, $z \,\big|\, a$ и $z \,\big|\, b$, поскольку $a, b \in M$.

Следовательно, $z \,\big|\, (a,b) = d$. С другой стороны, $d \,\big|\, z$, поскольку $z \in M$. Значит, $z = d$. А так как z имеет вид $ax + by$, числа x и y найдены.

2° *Алгоритмическое:* Проводим алгоритм Евклида, который выглядит так:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ &\dots \\ r_n &= q_{n+2} r_{n+1} + r_{n+2}, \\ r_{n+1} &= q_{n+3} r_{n+2}. \end{aligned} \tag{2}$$

Легко видеть, что $r_{n+2} = (a,b)$. Теперь, чтобы найти x и y, нужно воспользоваться обратным ходом алгоритма Евклида. Именно, перепишем равенства в следующем виде:

$$\begin{aligned} (a,b) = r_{n+2} &= r_n - q_{n+2} r_{n+1}, \\ r_{n+1} &= r_{n-1} - q_{n+1} r_n, \\ &\dots \end{aligned} \tag{3}$$

Затем последовательно выражаем остатки с большими номерами через остатки с меньшими номерами. В итоге получим представление вида $(a,b) = r_{n+2} = ax + by$. ■

Лемма 1.6. *Если* $a \,\big|\, bc$ *и* $(a,b) = 1$*, то* $a \,\big|\, c$.

□ Имеем $(a,b) = 1$, значит, по предыдущей лемме найдутся $x, y \in \mathbb{Z}$, для которых $ax + by = 1$. Умножим это равенство на c, получим $acx + bcy = c$. По условию $bc \vdots a$, значит, левая часть равенства делится на a. Стало быть, $c \vdots a$. ■

Вывод основной теоремы арифметики из этих лемм предоставляется читателю.

2. Асимптотический закон распределения простых чисел

Мы будем обозначать через $\pi(x)$ количество простых натуральных чисел, не превосходящих x. История определения асимптотики функции $\pi(x)$ такова:

- Евклид: $\pi(x) \to \infty$ при $x \to \infty$.
- Эйлер: $\frac{\pi(x)}{x} \to 0$ при $x \to \infty$.
- Чебышев (1848 г.): Если предел $\frac{\pi(x)\ln(x)}{x}$ существует, то он равен 1.
- Адамар и Валле-Пуссен (1896 г.): $\pi(x) \sim \frac{x}{\ln x}$.

2.1. Оценки Чебышева для функции $\pi(x)$

Мы докажем неравенства

$$a\frac{x}{\ln x} \leqslant \pi(x) \leqslant b\frac{x}{\ln x}. \tag{1}$$

Константы, которые получатся у нас, будут такими: $a = \frac{\ln 2}{2} \approx 0.3465$, а $b = 5\ln 2 \approx 3.4657$. У Чебышева константы были более точные: $a \approx 0.92129$, $b \approx 1.10555$.

Лемма 2.1 (Нижняя оценка для НОК). $K := [1, 2, 3, \dots, 2n+1] > 4^n$.

□ Рассмотрим функцию $f_n := \big(x(1-x)\big)^n$. Поскольку $x(1-x) < \frac{1}{4}$ всюду на отрезке $[0,1]$, за исключением одной точки $x = \frac{1}{2}$, получаем

$$I := \int_0^1 \big(x(1-x)\big)^n \, dx < \frac{1}{4^n}. \tag{2}$$

Раскроем скобки, получим некоторый многочлен с целыми коэффициентами:

$$f_n = x^n(1-x)^n = a_n x^n + \dots + a_{2n} x^{2n}, \quad a_j \in \mathbb{Z}. \tag{3}$$

Проинтегрируем его:

$$I = \frac{a_n}{n+1} + \dots + \frac{a_{2n}}{2n+1} > 0, \tag{4}$$

поскольку $f_n > 0$ на $(0,1)$. Заметим, что число KI целое (все знаменатели убьёт множитель K). Оно положительное, поэтому по крайней мере $KI \geqslant 1$. Пользуясь оценкой для I, получаем, что $K > 4^n$. ■

Теорема 2.2. *При $x \geqslant 6$ выполнена оценка $a\frac{x}{\ln(x)} \leqslant \pi(x)$ для некоторой константы a.*

□ По всякому числу x можно однозначно определить натуральное n, такое что $2n+1 \leqslant x < 2n+3$. Рассмотрим $K := [1, 2, 3, \ldots, 2n+1]$. Рассмотрим разложение этого числа на простые множители:

$$K = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}. \tag{5}$$

Заметим, что каждое простое число в диапазоне от 1 до $2n+1$ входит в разложение K. Значит, $r = \pi(2n+1)$. Далее, $p_i^{k_i} \leqslant 2n+1$ при всех i. Следовательно, $K \leqslant (2n+1)^{\pi(2n+1)}$. С другой стороны, по предыдущей лемме имеем $4^n < K$. Следовательно,

$$4^n < (2n+1)^{\pi(2n+1)}. \tag{6}$$

Логарифмируя это неравенство, получаем

$$\pi(2n+1)\log_2(2n+1) > n\log_2 4 = 2n \quad \Rightarrow \quad \pi(2n+1) > \frac{2n}{\log_2(2n+1)} > \frac{x-3}{\log_2(2n+1)} \overset{!}{\geqslant} \frac{\frac{x}{2}}{\log_2(2n+1)} \geqslant a\frac{x}{\ln x}. \tag{7}$$

Переход, отмеченный «!», обусловлен неравенством $x - 3 \geqslant \frac{x}{2}$, справедливым при $x \geqslant 6$. ■

Лемма 2.3. $\prod\limits_{p \leqslant x} p < 4^x$.

□ В силу монотонного возрастания функции 4^x достаточно доказать это неравенство для натуральных x. Будем вести индукцию по x. При $x = 2$ и $x = 3$ это верно. Пусть теперь это неравенство верно для всех чисел, меньших чем x. Докажем, что оно верно и для x.

Если $x = 2m$ $(m \geqslant 2)$, то всё доказано, поскольку $\prod\limits_{p \leqslant 2m} p = \prod\limits_{p \leqslant 2m-1} p < 4^{2m-1} < 4^x$.

Пусть теперь $x = 2m - 1$. Имеем

$$\prod_{p \leqslant x} p = \Big(\prod_{p \leqslant m} p\Big) \cdot \Big(\prod_{m < p \leqslant 2m-1} p\Big). \tag{8}$$

Рассмотрим число $\mathbf{C}_{2m-1}^m = \frac{(2m-1)!}{m!(m-1)!}$. Заметим, что это (целое) число делится на любое простое число p, для которого $m < p \leqslant 2m-1$, потому что в знаменателе таких больших простых делителей не встречается. Значит,

$$\big(\mathbf{C}_{2m-1}^m\big) \vdots \Big(\prod_{m < p \leqslant 2m-1} p\Big), \tag{9}$$

откуда следует, что

$$\mathbf{C}_{2m-1}^m \geqslant \prod_{m < p \leqslant 2m-1} p. \tag{10}$$

Пользуясь предположением индукции и полученной оценкой для второго множителя, получаем

$$\prod_{p \leqslant x} p < 4^m \mathbf{C}_{2m-1}^m. \tag{11}$$

Далее, поскольку $\mathbf{C}_{2m-1}^{m-1} = \mathbf{C}_{2m-1}^m$ и $\sum\limits_{k=0}^{2m-1} \mathbf{C}_{2m-1}^k = 2^{2m-1}$, имеет место оценка $\mathbf{C}_{2m-1}^m \leqslant 2^{2m-2} = 4^{m-1}$. Пользуясь ей и неравенством (11), получаем, что $\prod\limits_{p \leqslant x} p < 4^m \cdot 4^{m-1} = 4^{2m-1} = 4^x$, и шаг индукции полностью доказан. ■

Теорема 2.4. *$\pi(x) \leqslant b\frac{x}{\ln x}$ для некоторой константы b.*

□ Обозначим $k := \pi(x)$. Выпишем все простые числа, не превосходящие x: $p_1 < p_2 < \ldots < p_k \leqslant x$. Перемножая очевидные неравенства $i < p_i$ по $i = 1, \ldots, k$ и используя предыдущую лемму, получаем

$$k! < p_1 \cdot p_2 \cdot \ldots \cdot p_k = \prod_{p \leqslant x} p < 4^x. \tag{12}$$

Легко видеть, что

$$(k!)^2 = \big(1 \cdot k\big) \cdot \big(2 \cdot (k-1)\big) \cdot \ldots \cdot \big((k-1) \cdot 2\big) \cdot \big(k \cdot 1\big) \geqslant k^k \text{ (так как каждая скобка } \geqslant k). \tag{13}$$

Таким образом, из (12) и (13) следует, что

$$k^{k/2} \leqslant k! < 4^x. \tag{14}$$

Докажем, что $k \leqslant 5\frac{x}{\log_2 x}$. Предположим, что это не так, и $k > 5\frac{x}{\log_2 x}$. Покажем, что

$$5\frac{x}{\log_2 x} \geqslant x^{4/5}. \tag{15}$$

Действительно,

$$5\frac{x}{\log_2 x} \geqslant x^{4/5} \Leftrightarrow x^{1/5} \geqslant \frac{1}{5}\log_2 x = \log_2(x^{1/5}) \Leftrightarrow t \geqslant \log_2 t, \tag{16}$$

а последнее неравенство всем хорошо известно. Пользуясь (15), получаем:

$$k^{k/2} > \left(5\frac{x}{\log_2 x}\right)^{\frac{5}{2}\frac{x}{\log_2 x}} \geqslant (x^{4/5})^{\frac{5}{2}\frac{x}{\log_2 x}} = 4^x, \tag{17}$$

а это противоречит (14). Итак,

$$\pi(x) = k \leqslant 5\frac{x}{\log_2 x}, \tag{18}$$

откуда следует утверждение теоремы. ■

Следствие 2.1. *Пусть $p_1 < p_2 < p_3 < \ldots$ — последовательность всех простых чисел. Тогда найдутся константы $\alpha, \beta > 0$, такие что $\alpha n \ln n < p_n < \beta n \ln n$.*

□ Пользуясь теоремами 2.2 и 2.4, получаем:

$$a\frac{p_n}{\ln p_n} \leqslant \pi(p_n) = n \leqslant b\frac{p_n}{\ln p_n}. \tag{19}$$

Возьмём ln от этого неравенства:

$$\ln a + \ln p_n - \ln\ln p_n \leqslant \ln n \leqslant \ln b + \ln p_n - \ln\ln p_n. \tag{20}$$

Теперь перемножим (19) и (20) и получим:

$$ap_n\gamma_n \leqslant n\ln n \leqslant bp_n\delta_n \quad \text{где } \gamma_n, \delta_n \to 1 \text{ при } n \to \infty. \tag{21}$$

Поэтому

$$0 < \alpha \leqslant \frac{p_n}{n\ln n} \leqslant \beta, \tag{22}$$

что и требовалось доказать. ■

Следствие 2.2. *$\sum \frac{1}{p}$ расходится.*

□ Имеем $p_n \leqslant \beta n \ln n$, а ряд $\sum \frac{1}{n\ln n}$ расходится. ■

2.2. Функция Чебышева и ее связь с $\pi(x)$

Определение. *Функцией Чебышева* называется функция

$$\psi(x) = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p. \tag{23}$$

Заметим, что

$$\psi(x) = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p \leqslant \sum_{p \leqslant x} \frac{\ln x}{\ln p} \cdot \ln p = \ln x \cdot \sum_{p \leqslant x} 1 = \ln x \cdot \pi(x). \tag{24}$$

Определение. *Функцией Мангольдта* называется функция:

$$\Lambda(m) = \begin{cases} \ln p, & m = p^\alpha, \\ 0 & \text{иначе.} \end{cases} \tag{25}$$

Заметим, что $\left[\frac{\ln x}{\ln p}\right] = \#\{a \in \mathbb{N}\colon p^a \leqslant x\}$. Поэтому

$$\sum_{m \leqslant x} \Lambda(m) = \sum_{p^a \leqslant x} \Lambda(p^a) = \sum_{p^a \leqslant x} \ln p = \sum_{p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p = \psi(x). \tag{26}$$

Утверждение 2.5. $\pi(x) \sim \frac{x}{\ln x} \Leftrightarrow \psi(x) \sim x$.

□ Сначала докажем прямое утверждение.

$\boxed{\Rightarrow}$ Пусть $\frac{1}{2} < \beta < 1$, тогда

$$\big(\pi(x) - x^\beta\big)\beta \ln x \leqslant \big(\pi(x) - \pi\left(x^\beta\right)\big) \ln x^\beta \leqslant \sum_{x^\beta < p \leqslant x} \ln p \overset{!}{=} \sum_{x^\beta < p \leqslant x} \left[\frac{\ln x}{\ln p}\right] \ln p \leqslant \psi(x) \overset{!!}{\leqslant} \pi(x) \ln x. \tag{27}$$

Переход «!» обусловлен тем, что $p > x^\beta > x^{1/2}$, значит, $\frac{\ln x}{\ln p} < 2$, поэтому $\left[\frac{\ln x}{\ln p}\right] = 1$. Что касается перехода «!!», то он следует из неравенства (24).

Итак,

$$\beta \ln x\big(\pi(x) - x^\beta\big) \leqslant \psi(x) \leqslant \ln x \cdot \pi(x). \tag{28}$$

Разделим это неравенство на x:

$$-\frac{\beta \ln x}{x^{1-\beta}} + \frac{\beta \pi(x)}{x/\ln x} \leqslant \frac{\psi(x)}{x} \leqslant \frac{\pi(x)}{x/\ln x}. \tag{29}$$

Зададим $\varepsilon > 0$. Пусть $\beta = 1 - \varepsilon$. Тогда найдется $x_0(\varepsilon)$, для которого если $x \geqslant x_0(\varepsilon)$, то $1 - \varepsilon < \frac{\pi(x)}{x/\ln x} < 1 + \varepsilon$ (по предположению теоремы) и $\frac{\ln x}{x^\varepsilon} < \varepsilon$. Поэтому

$$(1 - \varepsilon)(-\varepsilon + 1 - \varepsilon) \leqslant \frac{\psi(x)}{x} \leqslant 1 + \varepsilon. \tag{30}$$

А это и означает, что $\psi(x) \sim x$.

$\boxed{\Leftarrow}$ Из неравенств предыдущего пункта не сложно составить следующее соотношение:

$$\frac{\psi(x)}{x} \leqslant \frac{\pi(x)}{x/\ln x} \leqslant \frac{1}{\beta}\frac{\psi(x)}{x} + \frac{\ln x}{x^{1-\beta}}. \tag{31}$$

Опять рассмотрим $\varepsilon > 0$. Положим $\beta = 1 - \varepsilon$. Тогда найдется $x_0(\varepsilon)$ такое, что если $x \geqslant x_0(\varepsilon)$, то $1 - \varepsilon < \frac{\psi(x)}{x} < 1 + \varepsilon$ (по предположению теоремы) и $\frac{\ln x}{x^\varepsilon} < \varepsilon$. Поэтому

$$1 - \varepsilon \leqslant \frac{\pi(x)}{x/\ln x} \leqslant \frac{1}{1 - \varepsilon}(1 + \varepsilon) + \varepsilon. \tag{32}$$

А это и означает, что $\pi(x) \sim \frac{x}{\ln x}$. ■

Введем новую функцию

$$\omega(x) = \int_1^x \frac{\psi(t)}{t}\, dt. \tag{33}$$

Утверждение 2.6. *Если $\omega(x) \sim x$, то и $\psi(x) \sim x$.*

□ Очевидно, $\psi(x)$ — монотонная функция, поэтому

$$\omega((1 + \varepsilon)x) - \omega(x) = \int_x^{(1+\varepsilon)x} \frac{\psi(t)}{t} dt \geqslant \psi(x) \int_x^{(1+\varepsilon)x} \frac{dt}{t} = \psi(x) \ln(1 + \varepsilon). \tag{34}$$

Поделим это неравенство на x:

$$(1 + \varepsilon)\frac{\omega((1 + \varepsilon)x)}{(1 + \varepsilon)x} - \frac{\omega(x)}{x} \geqslant \frac{\psi(x)}{x} \ln(1 + \varepsilon). \tag{35}$$

Левая часть неравенства при возрастании x стремится к ε, поэтому можно записать, что

$$\varepsilon \geqslant \ln(1 + \varepsilon)\, \overline{\lim}\, \frac{\psi(x)}{x} \Rightarrow \overline{\lim}\, \frac{\psi(x)}{x} \leqslant 1. \tag{36}$$

Абсолютно аналогично

$$\omega(x) - \omega\big((1 - \varepsilon)x\big) = \int_{(1-\varepsilon)x}^{x} \frac{\psi(t)}{t}\, dt \leqslant -\psi(x) \ln(1 - \varepsilon). \tag{37}$$

Поделим это неравенство на x:

$$\frac{\omega(x)}{x} - (1-\varepsilon)\frac{\omega((1-\varepsilon)x)}{(1-\varepsilon)x} \leqslant \frac{-\psi(x)}{x}\ln(1-\varepsilon). \tag{38}$$

Левая часть неравенства при возрастании x стремится к ε, поэтому можно записать, что

$$\varepsilon \leqslant -\ln(1-\varepsilon)\,\underline{\lim}\,\frac{\psi(x)}{x} \Rightarrow \underline{\lim}\,\frac{\psi(x)}{x} \geqslant 1. \tag{39}$$

Окончательно получаем:

$$1 \leqslant \underline{\lim}\,\frac{\psi(x)}{x} \leqslant \overline{\lim}\,\frac{\psi(x)}{x} \leqslant 1, \tag{40}$$

значит, на самом деле существует обычный предел, и $\lim \frac{\psi(x)}{x} = 1$. ■

2.3. Дзета-функция Римана

2.3.1. Определение и простейшие свойства

Определение. *Дзета-функцией Римана* называется функция

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in \mathbb{C}. \tag{41}$$

Сформулируем некоторые очевидные свойства ζ-функции.

- Ряд (41) сходится абсолютно в области $\operatorname{Re} s > 1$.
- Ряд (41) сходится неравномерно в области $\operatorname{Re} s > 1$ (иначе сходился бы и гармонический ряд).
- Ряд (41) сходится равномерно по признаку Вейерштрасса в области $\Omega_\delta = \{s\colon\ \operatorname{Re} s > 1+\delta\}$. Следовательно, по теореме Вейерштрасса функция $\zeta(s)$ аналитична в $\operatorname{Re} s > 1$.
- $\zeta'(s) = -\sum\limits_{n=2}^{\infty} \frac{\ln n}{n^s}$ в области $\operatorname{Re} s > 1$ (потому что равномерно сходящийся ряд можно дифференцировать почленно).

Определение. *Функцией Мёбиуса* называется функция

$$\mu(n) := \begin{cases} 1, & n = 1; \\ 0, & n \vdots p^2 \text{ для некоторого простого } p; \\ (-1)^r, & n = p_1 \cdot \ldots \cdot p_r \ (p_i \text{ — различные простые числа}). \end{cases} \tag{42}$$

Утверждение 2.7. *Функция $\zeta(s)$ не имеет нулей в области $\operatorname{Re} s > 1$, и*

$$\frac{1}{\zeta(s)} = \sum_{1}^{\infty} \frac{\mu(n)}{n^s}. \tag{43}$$

□ Функция $\xi(s) := \sum\limits_{1}^{\infty} \frac{\mu(n)}{n^s}$ аналитична в $\operatorname{Re} s > 1$. Поскольку ряды, из которых составлены функции ξ и ζ, сходятся абсолютно, то их можно перемножать в любом порядке, поэтому

$$\xi(s)\zeta(s) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{\mu(n)}{(mn)^s} = \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{n|k} \mu(n). \tag{44}$$

Остается доказать, что $\sum\limits_{n|k} \mu(n) = \delta_{k1}$ (символ Кронекера). Пусть $k = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$. Если $n \,\big|\, k$, то $n = p_1^{\beta_1} \cdot \ldots \cdot p_t^{\beta_t}$. Слагаемые, в которых хотя бы одна из степеней β_i больше 1, погибнут сразу (по определению μ). Останутся слагаемые, в которых все степени будут нулевыми (оно будет всего одно и войдёт со знаком «+»), слагаемые, в которых ненулевой будет только одна степень (их будет $\mathbf{C}_t^1$ штук, и они войдут со знаком «−»), и так далее. При $k > 1$ получаем

$$\sum_{n|k} \mu(n) = 1 - \mathbf{C}_t^1 + \mathbf{C}_t^2 - \ldots = (1-1)^t = 0. \tag{45}$$

Таким образом, останется только одно слагаемое при $k = 1$. Но это означает, что $\xi(s)\zeta(s) = 1$.

Из полученного соотношения следует, что функции ξ и ζ не имеют нулей в области $\operatorname{Re} s > 1$. Попутно мы доказали и требуемое равенство $\frac{1}{\zeta(s)} = \xi(s)$. ■

Утверждение 2.8 (Связь функции Римана и Мангольдта). *Имеет место формула*

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=2}^{\infty} \frac{\Lambda(n)}{n^s}. \tag{46}$$

□ Имеем

$$\sum_{n=2}^{\infty} \frac{\Lambda(n)}{n^s} \sum_{m=1}^{\infty} \frac{1}{m^s} = \sum_{k=2}^{\infty} \frac{1}{k^s} \sum_{n|k} \Lambda(n). \tag{47}$$

Остается доказать, что $\sum\limits_{n|k} \Lambda(n) = \ln k$. Действительно, пусть $k = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$. Тогда $\ln k = \alpha_1 \ln p_1 + \ldots + \alpha_t \ln p_t$. Тогда ненулевой вклад в сумму дадут только числа n вида $p_i^{\beta_i}$ $(1 \leqslant \beta_i \leqslant \alpha_i)$. Следовательно,

$$\sum_{n|k} \Lambda(n) = \alpha_1 \ln p_1 + \ldots + \alpha_t \ln p_t = \ln k. \tag{48}$$

Подставляя эту сумму в полученную выше формулу, получаем в точности выражение для производной ζ-функции, взятой со знаком «$-$». ■

2.3.2. Мультипликативные функции. Формула Эйлера

Определение. Функцию $f(n)$ назовем *вполне мультипликативной*, если $f(uv) = f(u)f(v)$ при всех $u, v \in \mathbb{N}$.

Пример 3.1. Функции $f(n) = n^s$ и $f(n) \equiv 1$ вполне мультипликативны.

Утверждение 2.9. *Пусть f вполне мультипликативна, и $f \not\equiv 0$. Тогда $f(1) = 1$.*

□ Пусть $f(n) \neq 0$ для некоторого n. Тогда $f(n) = f(n \cdot 1) = f(n) \cdot f(1)$, а поскольку на $f(n)$ можно сократить, то $f(1) = 1$. ■

Лемма 2.10. *Пусть $f(n)$ — вполне мультипликативная функция ($f \not\equiv 0$), причем ряд*

$$S := \sum_{n=1}^{\infty} f(n) \tag{49}$$

абсолютно сходится. Тогда

$$\prod_p \big(1 - f(p)\big)^{-1} = S, \text{ то есть } S(x) := \prod_{p \leqslant x} \big(1 - f(p)\big)^{-1} \to S, \quad x \to \infty. \tag{50}$$

□ Мы уже знаем, что $f(1) = 1$. Покажем, что $|f(n)| < 1$ при $n > 1$. В самом деле, если $|f(n)| > 1$, то и $\big|f(n^k)\big| = |f(n)|^k > 1$, а это противоречит сходимости ряда для S.

Пусть p — простое. Поскольку $|f(p)| < 1$, то по формуле для геометрической прогрессии имеем

$$\big(1 - f(p)\big)^{-1} = \sum_{k=0}^{\infty} f(p)^k = \sum_{k=0}^{\infty} f(p^k), \tag{51}$$

и ряд в правой части абсолютно сходится. Абсолютно сходящиеся ряды можно перемножать, поэтому

$$S(x) = \prod_{p \leqslant x} (1 - f(p))^{-1} = \sum_{p_j \leqslant x} f(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}) = \sum_{*} f(n). \tag{52}$$

Сумма по «$*$» означает, что суммирование идёт по тем и только тем n, у которых все простые делители не превосходят x. Сумма по «$**$» означает, что суммирование ведётся по всем n, у которых в разложении есть простые числа, большие x. Легко видеть, что

$$|S - S(x)| = \Big|\sum_{**} f(n)\Big| \leqslant \sum_{**} |f(n)| \overset{!}{\leqslant} \sum_{n \geqslant x} |f(n)| \to 0, \quad x \to \infty, \tag{53}$$

как остаток сходящегося ряда. На всякий случай поясним переход, отмеченный «!»: в сумме были числа, у которых были простые делители, большие x, а мы добавили туда вообще все числа, большие x. ■

Следствие 2.3 (Формула Эйлера). *В области* $\operatorname{Re} s > 1$ *выполняется*

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{54}$$

□ В качестве $f(n)$ из предыдущей леммы берем $\frac{1}{n^s}$ (в области $\operatorname{Re} s > 1$ ряд абсолютно сходится). ■

2.3.3. Аналитическое продолжение ζ-функции

Лемма 2.11 (Преобразование Абеля). *Пусть* $a_k \in \mathbb{C}$, *и* $g\colon [1,\infty) \to \mathbb{C}$ — *непрерывно дифференцируемая функция. Тогда*

$$\sum_{k\leqslant T} a_k g(k) = A(T)g(T) - \int_1^T A(x)g'(x)dx, \text{ где } A(x) := \sum_{k\leqslant x} a_k. \tag{55}$$

Если к тому же ряд $\sum\limits_1^\infty a_k g(k)$ *сходится и* $A(T)g(T) \to 0$ *при* $T \to \infty$, *то*

$$\sum_{k=1}^{\infty} a_k g(k) = -\int_1^\infty A(x)g'(x)dx. \tag{56}$$

□ Введём обозначение

$$\alpha_k(x) := \begin{cases} 0, & x < k, \\ a_k, & x \geqslant k. \end{cases} \tag{57}$$

Рассмотрим

$$A(T)g(T) - \sum_{k\leqslant T} a_k g(k) = \sum_{k\leqslant T} a_k(g(T) - g(k)) = \sum_{k\leqslant T} a_k \int_k^T g'(x)\,dx =$$

$$= \sum_{k\leqslant T} \int_k^T \alpha_k(x)g'(x)\,dx = \sum_{k\leqslant T} \int_1^T \alpha_k(x)g'(x)\,dx = \int_1^T \Big(\sum_{k\leqslant T} \alpha_k(x)\Big)g'(x)\,dx. \tag{58}$$

Остается только заметить, что при $x \in [1,T]$

$$\sum_{k\leqslant T} \alpha_k(x) = \sum_{k\leqslant x} \alpha_k(x) = \sum_{k\leqslant x} a_k = A(x). \tag{59}$$

Вторая часть леммы получается из первой простым предельным переходом. ■

Теорема 2.12 (Об аналитическом продолжении ζ-функции). ζ*-функция аналитически продолжается в область* $\{\operatorname{Re} s > 0\} \setminus \{s = 1\}$, *причём в точке* $s = 1$ *имеется полюс порядка* 1 *с вычетом, равным* 1.

□ Применим предыдущую лемму к случаю, когда $T = N \in \mathbb{N}$, $a_i \equiv 1$, а $g(x) = x^{-s}$. Тогда $g'(x) = -sx^{-(s+1)}$, а $A(x) = \sum\limits_{k\leqslant x} 1 = [x]$. Воспользуемся предыдущей леммой и свойством $[x] = x - \{x\}$:

$$\sum_{k=1}^N \frac{1}{k^s} = \frac{N}{N^s} + s\int_1^N \frac{[x]}{x^{s+1}}\,dx = \frac{1}{N^{s-1}} + s\int_1^N \frac{x}{x^{s+1}}\,dx - s\int_1^N \frac{\{x\}}{x^{s+1}}\,dx =$$

$$= \frac{1}{N^{s-1}} + \left(\frac{s}{s-1} - \frac{s}{N^{s-1}(s-1)}\right) - s\int_1^N \frac{\{x\}}{x^{s+1}}\,dx = 1 + \frac{1}{s-1} - \frac{1}{N^{s-1}(s-1)} - s\int_1^N \frac{\{x\}}{x^{s+1}}\,dx. \tag{60}$$

Пусть сначала $\operatorname{Re} s > 1$. Перейдём к пределу при $N \to \infty$. Получим

$$\zeta(s) = 1 + \frac{1}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}}\,dx. \tag{61}$$

Нам бы хотелось принять эту формулу за определение ζ-функции при $\operatorname{Re} s > 0$. Для этого надо доказать аналитичность правой части (точнее, интегрального слагаемого). Пусть $s = \sigma + it$. Разобьём интеграл на части. Пусть

$$\varphi_n(s) := \int\limits_n^{n+1} \frac{\{x\}}{x^{s+1}}\,dx = \int\limits_n^{n+1} \frac{x-n}{x^{s+1}}\,dx. \tag{62}$$

Очевидно, что $\varphi_n(s)$ аналитичны в $\operatorname{Re} s > 0$. Значит, интеграл в правой части есть сумма ряда из аналитических функций. Этот ряд равномерно сходится, так как при $\sigma \geqslant \delta > 0$ он мажорируется числовым рядом:

$$|\varphi_n(s)| \leqslant \int\limits_n^{n+1} \frac{\{x\}}{x^{\sigma+1}}\,dx \leqslant \frac{1}{n^{\sigma+1}} \leqslant \frac{1}{n^{\delta+1}}. \tag{63}$$

Осталось применить теорему Вейерштрасса.

Далее видно, что у полученного продолжения есть полюс в точке $s = 1$ с вычетом, равным 1. ■

Следствие 2.4. *Попутно мы получили такое выражение для ζ-функции:*

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} + \frac{1}{(s-1)N^{s-1}} - s\int\limits_N^{\infty} \frac{\{x\}}{x^{s+1}}dx, \quad \operatorname{Re} s > 0. \tag{64}$$

2.3.4. Оценки ζ-функции и её производной

Лемма 2.13. *Пусть $s = \sigma + it$. Пусть $\sigma \in [1, 2]$, а $|t| \geqslant 3$. Тогда*

$$|\zeta(s)| \leqslant 5\ln|t|, \qquad |\zeta'(s)| \leqslant 8\ln^2|t|. \tag{65}$$

□ Оценим сначала саму ζ-функцию. Воспользуемся следствием 2.4 и оценим каждое слагаемое. Пусть $N = [|t|]$. Тогда

$$\left|\sum_{n=1}^{N} \frac{1}{n^s}\right| \leqslant \sum_{n=1}^{N} \frac{1}{n^\sigma} \leqslant \sum_{n=1}^{N} \frac{1}{n} \leqslant 1 + \int\limits_1^N \frac{dx}{x} = 1 + \ln N \leqslant 2\ln N \leqslant 2\ln|t|. \tag{66}$$

$$\left|\frac{1}{(s-1)N^{s-1}}\right| = \frac{1}{|s-1|N^{\sigma-1}} \leqslant \frac{1}{|s-1|} \leqslant \frac{1}{3}. \tag{67}$$

$$\left|s\int\limits_N^{\infty} \frac{\{x\}}{x^{s+1}}\,dx\right| \leqslant (|t|+2)\int\limits_N^{\infty} \frac{1}{x^{\sigma+1}}\,dx \leqslant (|t|+2)\int\limits_N^{\infty} \frac{dx}{x^2} = \frac{|t|+2}{N} \leqslant \frac{|t|+2}{|t|-1} = 1 + \frac{3}{|t|-1} \leqslant \frac{5}{2}. \tag{68}$$

Итого:

$$|\zeta(s)| \leqslant 2\ln|t| + \frac{1}{3} + \frac{5}{2} < 5\ln|t|. \tag{69}$$

Дифференцируя выражение для ζ, получаем

$$\zeta'(s) = -\sum_{1}^{N} \frac{\ln n}{n^s} - \frac{1}{(s-1)^2N^{s-1}} - \frac{\ln N}{(s-1)N^{s-1}} - \int\limits_N^{\infty} \frac{\{x\}}{x^{s+1}}\,dx + s\int\limits_N^{\infty} \frac{\{x\}\ln x}{x^{s+1}}\,dx. \tag{70}$$

Оценим слагаемые в этом выражении (начнём с более простых):

$$\left|\frac{1}{(s-1)^2N^{s-1}}\right| \leqslant \frac{1}{9}\frac{1}{N^{s-1}} \leqslant \frac{1}{9}. \tag{71}$$

$$\left|\frac{\ln N}{(s-1)N^{s-1}}\right| \leqslant \frac{1}{3}\ln N \leqslant \frac{1}{3}\ln|t|. \tag{72}$$

$$\left|\int\limits_N^{\infty} \frac{\{x\}}{x^{s+1}}\,dx\right| \leqslant \int\limits_N^{\infty} \frac{1}{x^2}\,dx = \frac{1}{N} \leqslant \frac{1}{2}. \tag{73}$$

$$\left|s\int\limits_N^\infty \frac{\{x\}\ln x}{x^{s+1}}\,dx\right| \leqslant (|t|+2)\int\limits_N^\infty \frac{\ln x}{x^2}dx = (|t|+2)\left(-\frac{\ln x}{x}\Big|_N^\infty + \int\limits_N^\infty \frac{1}{x^2}dx\right) =$$

$$= \frac{\ln N+1}{N}(|t|+2) \leqslant 2\ln|t|\frac{|t|+2}{|t|-1} \leqslant 5\ln|t|. \quad (74)$$

При оценке первого слагаемого мы воспользуемся монотонным убыванием функции $\frac{\ln x}{x}$ при $x \in (e,\infty)$ и применим интегральный признак сходимости:

$$\sum_1^N \left|\frac{\ln n}{n^s}\right| = \sum_2^N \frac{\ln n}{n^\sigma} \leqslant \sum_2^N \frac{\ln n}{n} = \frac{\ln 2}{2} + \sum_3^N \frac{\ln n}{n} \leqslant \frac{\ln 2}{2} + \frac{\ln 3}{3} + \int\limits_3^N \frac{\ln x}{x}\,dx \leqslant$$

$$\leqslant \frac{\ln 2}{2} + \frac{\ln 3}{3} + \frac{1}{2}\ln^2 N - \frac{1}{2}\ln^2 3 \leqslant \frac{\ln 2}{2} + \frac{1}{2}\ln^2 N < \ln^2 N \leqslant \ln^2|t|. \quad (75)$$

Итого:

$$|\zeta'(s)| \leqslant \frac{1}{9} + \frac{1}{3}\ln|t| + \frac{1}{2} + 5\ln|t| + \ln^2|t| \leqslant \left(\frac{1}{2}+\frac{1}{2}+\frac{1}{9}+5+1\right)\ln^2|t| \leqslant 8\ln^2|t|. \quad (76)$$

■

2.3.5. Гипотеза Римана и теоремы о нулях ζ-функции

Для ζ-функции имеет место следующее соотношение:

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\cos\frac{\pi s}{2}\cdot\Gamma(s)\zeta(s), \quad (77)$$

где Γ — гамма-функция Эйлера. Таким образом, значения функции ζ слева и справа от прямой $\operatorname{Re} s = \frac{1}{2}$ связаны некоторым уравнением. Этот факт установил Б. Риман в 1859 году.

В лекциях на этом месте было написано что-то несуразное про функцию η, поэтому этот фрагмент воспроизведён по книге [1].

Риман также высказал предположение о том, что все нули функции $\zeta(s)$ расположены на этой прямой (*гипотеза Римана*). В 1914 году Харди доказал, что на $\operatorname{Re} s = \frac{1}{2}$ лежит бесконечное число нулей ζ-функции; после этого было доказано, что как минимум треть нулей лежит на этой прямой. Более того, появилась теорема о том, что нули имеют положительную плотность на этой прямой. Самый последний результат принадлежит Виноградову, показавшему в 1957 году, что нет нулей в области, отмеченной на рис. 1.

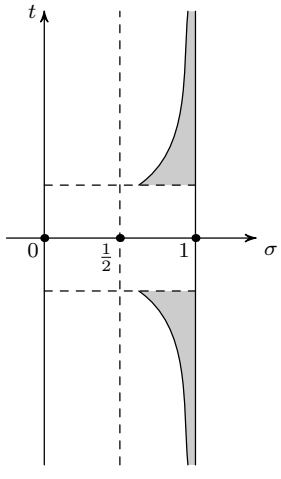


Рис. 1

Большинство математиков верят, что гипотеза верна. На сегодняшний день проверены первые 1 500 000 000 решений. Гипотеза Римана входит в число семи главных нерешенных математических проблем. За её доказательство Институт математики Клея (Кембридж, штат Массачусетс) выплатит приз в $1 млн.

Лемма 2.14. *Пусть* $r \in (0,1)$, $\varphi \in \mathbb{R}$. *Тогда*

$$\Pi := (1-r)^3\cdot|1-re^{i\varphi}|^4\cdot|1-re^{2i\varphi}| \leqslant 1. \quad (78)$$

□ Возьмем $-\ln$ от левой и правой частей доказываемого неравенства. Получим

$$\begin{aligned} -\ln\Pi &= -3\ln(1-r) - 4\ln|1-re^{i\varphi}| - \ln|1-re^{2i\varphi}| = \\ &= -3\operatorname{Re}\ln(1-r) - 4\operatorname{Re}\ln(1-re^{i\varphi}) - \operatorname{Re}\ln(1-re^{2i\varphi}) = \\ &= 3\operatorname{Re}\sum_1^\infty \frac{r^n}{n} + 4\operatorname{Re}\sum_1^\infty \frac{r^n}{n}e^{in\varphi} + \operatorname{Re}\sum_1^\infty \frac{r^n}{n}e^{2in\varphi} = \\ &= \operatorname{Re}\sum_1^\infty \frac{r^n}{n}(3+4e^{in\varphi}+e^{2in\varphi}) = \sum_1^\infty \frac{r^n}{n}(3+4\cos n\varphi+\cos 2n\varphi) \geqslant 0, \end{aligned} \quad (79)$$

потому что $3+4\cos x+\cos 2x = 2\cos^2 x + 4\cos x + 2 = 2(\cos x+1)^2 \geqslant 0$. ■

Лемма 2.15. *Если* $\operatorname{Re} s > 1$, *то*

$$P := |\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \geqslant 1. \quad (80)$$

□ Воспользуемся формулой Эйлера: $\zeta(s) = \prod\limits_p \left(1 - \frac{1}{p^s}\right)^{-1}$. Применим предыдущую лемму, взяв $r = \frac{1}{p^\sigma}$ и $\varphi = -t \ln p$. Имеем:

$$P = \prod_p \left| \left(1 - \frac{1}{p^\sigma}\right)^3 \left(1 - \frac{1}{p^\sigma}\frac{1}{p^{it}}\right)^4 \left(1 - \frac{1}{p^\sigma}\frac{1}{p^{2it}}\right) \right|^{-1} \geqslant 1. \tag{81}$$

■

Лемма 2.16. *Если* $\operatorname{Re} s = 1$, *то* $\zeta(s) \neq 0$.

□ Предположим противное: найдется такая точка $s_0 = 1 + it$, что $\zeta(s_0) = 0$. Пусть $s = \sigma + it$. Имеем

$$|\zeta(s)| = |\zeta(s) - \zeta(s_0)| = O(|s - s_0|) = O(\sigma - 1). \tag{82}$$

$$\zeta(\sigma) = \sum_1^\infty \frac{1}{n^\sigma} \leqslant 1 + \int_1^\infty \frac{dx}{x^\sigma} = 1 + \frac{1}{\sigma - 1} = \frac{\sigma}{\sigma - 1} = O\left(\frac{1}{\sigma - 1}\right). \tag{83}$$

Далее, имеем $|\zeta(\sigma + 2it)| = O(1)$, так как $\sigma + 2it \to 1 + 2it$ при $\sigma \to 1$, а в точке $1 + 2it$ дзета-функция аналитична, и потому в этой точке у неё есть конечный предел.

Теперь оценим порядок функции P из предыдущей леммы. Имеем

$$P = O\left(\frac{1}{(\sigma - 1)^3}(\sigma - 1)^4\right) = O(\sigma - 1) \to 0, \quad \sigma \to 1, \tag{84}$$

что противоречит предыдущей лемме. ■

Лемма 2.17. *Пусть* $\sigma \in [1, 2]$, *а* $|t| \geqslant 3$. *Тогда*

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant C \ln^9 |t|. \tag{85}$$

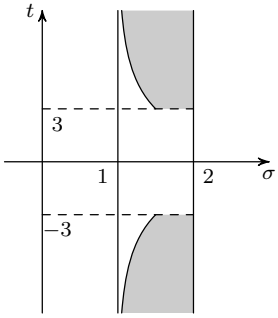


Рис. 2

□ Оценка сверху на $|\zeta'(s)|$ у нас уже была. Получим оценку снизу на $|\zeta(s)|$. Положим $\sigma_1(t) := 1 + \frac{1}{C \ln^9 |t|}$, где $C = 2^{23}$. Разобьем нашу область на две части (см. рис. 2). Первая — $\sigma \geqslant \sigma_1(t)$, а вторая — $1 \leqslant \sigma \leqslant \sigma_1(t)$.

1° Пусть сначала выполнено неравенство $\sigma \geqslant \sigma_1(t)$. Из доказательства предыдущей леммы мы знаем, что

$$\zeta(\sigma) \leqslant \frac{2}{\sigma - 1} \leqslant 2C \ln^9 |t|. \tag{86}$$

Из известной оценки для модуля ζ-функции получаем:

$$|\zeta(\sigma + 2it)| \leqslant 5 \ln(2|t|) \leqslant 16 \ln |t|. \tag{87}$$

Теперь применяем лемму 2.15:

$$1 \leqslant |\zeta(s)|^4 (2C \ln^9 |t|)^3 16 \ln |t| \Rightarrow |\zeta(s)| \geqslant (2C)^{-3/4} \frac{1}{2} \ln^{-7} |t| = 2^{-19} \ln^{-7} |t| = 16 C^{-1} \ln^{-7} |t|. \tag{88}$$

2° Пусть теперь $1 \leqslant \sigma \leqslant \sigma_1(t)$. Имеем

$$|\zeta(s) - \zeta(\sigma_1 + it)| = \left| \int_\sigma^{\sigma_1} \zeta'(u + it)\, du \right| \leqslant |\sigma_1 - \sigma| \cdot 8 \ln^2 |t| \leqslant 8 C^{-1} \ln^{-7} |t|. \tag{89}$$

Значит, по неравенству треугольника имеем

$$|\zeta(s)| \geqslant |\zeta(\sigma_1 + it)| - 8 C^{-1} \ln^{-7} |t| \geqslant 8 C^{-1} \ln^{-7} |t|. \tag{90}$$

Здесь мы воспользовались оценкой для $|\zeta(\sigma_1 + it)|$, полученной выше. Итого получаем

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant \frac{8 \ln^2 |t|}{8 C^{-1} \ln^{-7} |t|} = C \ln^9 |t|. \tag{91}$$

■

2.4. Доказательство асимптотического закона простых чисел

Лемма 2.18. *Пусть $a, b > 0$, тогда*

$$\frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\frac{b^s}{s^2}\,ds=\begin{cases}\ln b, & b\geqslant 1,\\ 0, & 0<b<1.\end{cases} \tag{92}$$

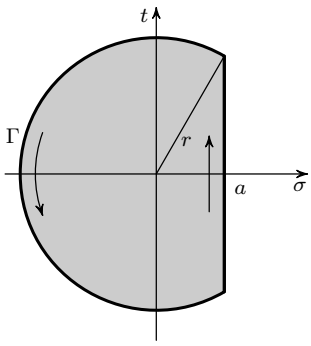


Рис. 3

□ Обозначим $r := |s|$. Пусть сначала $b \geqslant 1$. Будем интегрировать по контуру, отмеченному на рис. 3.

$$\left|\frac{b^s}{s^2}\right| = \frac{b^\sigma}{r^2} \leqslant \frac{b^a}{r^2} \text{ (здесь мы воспользовались тем, что } b \geqslant 1). \tag{93}$$

Пусть C — дуга окружности, входящая в контур интегрирования. Следовательно,

$$\left|\frac{1}{2\pi i}\int\limits_{C}\frac{b^s}{s^2}\,ds\right| \leqslant r\frac{b^a}{r^2} = \frac{b^a}{r} \to 0, \quad r\to\infty. \tag{94}$$

Поэтому

$$\frac{1}{2\pi i}\int\limits_{\Gamma}\frac{b^s}{s^2}\,ds = \operatorname*{res}_{s=0}\frac{b^s}{s^2} = \ln b. \tag{95}$$

Остается воспользоваться интегральной теоремой Коши.

Пусть теперь $0 < b < 1$. В этом случае будем интегрировать по другому пути, показанному на рис. 4. Получаем

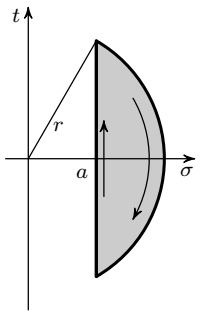


Рис. 4

$$\left|\frac{1}{2\pi i}\int\limits_{C}\frac{b^s}{s^2}\,ds\right| \leqslant \frac{1}{2\pi}2\pi r\frac{b^a}{r^2} \to 0, \quad r\to\infty. \tag{96}$$

Здесь мы воспользовались тем, что для $b \leqslant 1$ верно неравенство $b^\sigma \leqslant b^a$, $\sigma \geqslant a$.

Внутри контура Γ особенностей у подынтегральной функции нет. Остаётся применить интегральную теорему Коши. ■

Далее для сокращения выкладок введём обозначение:

$$\xi(s) := -\frac{\zeta'(s)}{\zeta(s)}. \tag{97}$$

Лемма 2.19. *Пусть $x > 1$. Тогда функция $\omega(x)$ представляется абсолютно сходящимся интегралом*

$$\omega(x) = J(x) := \frac{1}{2\pi i}\int\limits_{2-i\infty}^{2+i\infty}\xi(s)\cdot\frac{x^s}{s^2}\,ds. \tag{98}$$

□ Докажем абсолютную сходимость. Интегрирование ведется по прямой $s = 2 + it$. Вспомним, что

$$\xi(s) = \sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^s}. \tag{99}$$

Очевидно, что $\Lambda(n) \leqslant \ln n$. Следовательно,

$$|\xi(s)| \leqslant \sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^2} \leqslant \sum_{n=2}^{\infty}\frac{\ln n}{n^2} \leqslant C. \tag{100}$$

Поэтому

$$\left|\xi(s)\cdot\frac{x^s}{s^2}\right| \leqslant \frac{Cx^2}{4+t^2}. \tag{101}$$

Значит, $J(x)$ оценивается сходящимся интегралом и потому сходится абсолютно.

Докажем, что $J(x) = \omega(x)$. Разделим сумму ряда на два слагаемых:

$$\xi(s) = \sum_{n=2}^{N}\frac{\Lambda(n)}{n^s} + R_N(s). \tag{102}$$

$$|R_N(s)| \leqslant \sum_{N+1}^{\infty} \frac{\Lambda(n)}{n^2} \leqslant \sum_{N+1}^{\infty} \frac{\ln n}{n^2} =: \rho_N \to 0, \quad N \to \infty. \tag{103}$$

$$J(x) = \sum_{n=2}^{N} \Lambda(n) \frac{1}{2\pi i} \int\limits_{2-i\infty}^{2+i\infty} \frac{\left(\frac{x}{n}\right)^s}{s^2}\, ds + \frac{1}{2\pi i} \int\limits_{2-i\infty}^{2+i\infty} R_N(s) \frac{x^s}{s^2}\, ds. \tag{104}$$

К интегралу в первом слагаемом применим предыдущую лемму, а во втором слагаемом заменим $R_N(s)$ на его оценку (103) сверху:

$$J(x) = \sum_{n \leqslant x} \Lambda(n) \ln\left(\frac{x}{n}\right) + I, \qquad |I| \leqslant \frac{\rho_N x^2}{2\pi} \int\limits_{-\infty}^{+\infty} \frac{dt}{4+t^2} \to 0, \quad N \to \infty. \tag{105}$$

Теперь применим преобразование Абеля (лемма 2.11) для $a_n = \Lambda(n)$, $g(t) = \ln\left(\frac{x}{t}\right)$. Согласно установленной ранее формуле (26), $A(x) = \sum\limits_{n \leqslant x} \Lambda(n) = \psi(x)$. Поэтому

$$J(x) = \psi(x) \cdot 0 + \int\limits_{1}^{x} \frac{\psi(t)}{t}\, dt = \omega(x). \tag{106}$$

Лемма доказана. ■

Введём еще одно обозначение:

$$\xi_x(s) := \left(-\frac{\zeta'(s)}{\zeta(s)}\right) \cdot \frac{x^{s-1}}{s^2}. \tag{107}$$

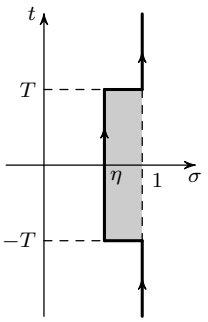


Рис. 5

Лемма 2.20. *Пусть $0 < \eta < 1$, $T \geqslant 3$ и в области $\sigma \in [\eta, 1]$, $|t| \leqslant T$ у дзета-функции нет нулей. Тогда*

$$\omega(x) = x\big(1 + R(x)\big), \quad R(x) = \frac{1}{2\pi i} \int\limits_{\Gamma} \xi_x(s)\, ds \to 0, \quad x \to \infty. \tag{108}$$

□

$$\frac{1}{2\pi i} \int\limits_{\Gamma} \xi_x(s) \cdot x\, ds = \operatorname*{res}_{s=1} \big(\xi_x(s) \cdot x\big). \tag{109}$$

Посчитаем, чему равен этот вычет. Мы знаем (теорема 2.12), что $\zeta(s) = \frac{f(s)}{s-1}$ где $f(1) = 1$. Поэтому

$$-\xi(s) = -\frac{1}{s-1} + \frac{f'(s)}{f(s)}, \text{ откуда } \operatorname*{res}_{s=1} \big(\xi_x(s) \cdot x\big) = x. \tag{110}$$

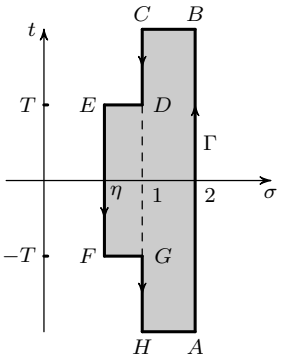


Рис. 6

Оценим теперь подынтегральную функцию на отрезке BC:

$$|\xi_x(s) \cdot x| \leqslant C \ln^9 |t| \frac{x^\sigma}{\sigma^2 + t^2}. \tag{111}$$

Поэтому справедлива следующая оценка для интеграла по BC:

$$\left|\frac{1}{2\pi i} \int\limits_{BC} \xi_x(s) \cdot x\, ds\right| \leqslant \frac{1}{2\pi} \int\limits_{1}^{2} \frac{C \ln^9 |t|}{t^2} x^\sigma\, d\sigma \leqslant \frac{C}{2\pi} \frac{\ln^9 |t|}{t^2} x^2 \xrightarrow{t \to \infty} 0. \tag{112}$$

Все необходимые оценки получены. По теореме Коши

$$\omega(x) = x + x \cdot \frac{1}{2\pi i} \int\limits_{-\Gamma} \xi_x(s)\, ds = x\big(1 + R(x)\big). \tag{113}$$

Теперь докажем, что $R(x) \to 0$ при $x \to \infty$. Зафиксируем число $\varepsilon > 0$ и покажем, что найдётся x_0 такое, что при $x > x_0$ будет выполнена оценка $|R(x)| < \varepsilon$. Имеем

$$\left|\frac{1}{2\pi i} \int\limits_{1+iT}^{1+i\infty} \xi_x(s)\, ds\right| \leqslant \frac{1}{2\pi} \int\limits_{T}^{\infty} \frac{C \ln^9 |t|}{1+t^2} dt \leqslant \frac{\varepsilon}{5}. \tag{114}$$

Такой оценки мы добились именно за счет выбора T.

Остается подобрать нужное η. Поскольку на отрезке $[1-iT, 1+iT]$ функция $\zeta(s)$ в нуль не обращается, то для каждой точки этого отрезка найдется некая её окрестность в которой $\zeta(s) \neq 0$. Отрезок — компакт, поэтому можно выбрать конечное подпокрытие такими кружочками. Значит, найдётся η столь близкое к 1, что отрезок $[\eta - iT, \eta + iT]$ окажется покрытым этими кружочками.

Пусть $\max_{DEFG} \left|\frac{\zeta'(s)}{\zeta(s)} \frac{1}{s^2}\right| = M$. Тогда за счет увеличения x можно добиться следующих оценок:

$$\left|\frac{1}{2\pi i} \int\limits_{ED} \xi_x(s)\, ds\right| \leqslant \frac{1}{2\pi} \int\limits_{-\infty}^{1} M x^{\sigma-1} d\sigma = \frac{M}{2\pi} \frac{x^{\sigma-1}}{\ln x}\Bigg|_{-\infty}^{1} \leqslant \frac{M}{2\pi \ln x} < \frac{\varepsilon}{5}. \tag{115}$$

Аналогично

$$\left|\frac{1}{2\pi i} \int\limits_{FG} \xi_x(s)\, ds\right| < \frac{\varepsilon}{5}. \tag{116}$$

$$\left|\frac{1}{2\pi i} \int\limits_{EF} \xi_x(s)\, ds\right| \leqslant \frac{1}{2\pi} \int\limits_{-T}^{T} M x^{\eta-1} dt = \frac{MT}{\pi} x^{\eta-1} < \frac{\varepsilon}{5}. \tag{117}$$

Теперь соединяем вместе оценки (114), (115), (117) и (116) и получаем, что $|R(x)| < \varepsilon$. ■

Итак, мы доказали, что $\omega(x) \sim x$. Это завершает доказательство асимптотического закона.

3. Теорема Дирихле

Основным результатом данной главы будет теорема о простых числах в арифметических прогрессиях, доказанная Дирихле в 1839 году. Она утверждает, что если первый член и разность арифметической прогрессии суть взаимно простые натуральные числа, то такая прогрессия содержит бесконечно много простых чисел.

3.1. Частные случаи теоремы Дирихле. Сравнения по модулю

3.1.1. Простейший частный случай: $a_n = 4n + 3$

В качестве разминки докажем нашу теорему в частном случае.

Утверждение 3.1. *В последовательности $\{4n+3\}$ бесконечно много простых чисел.*

□ Предположим, что это не так. Пусть $p_1, p_2, \ldots, p_r$ — все простые числа вида $4n+3$. Рассмотрим число $N := 4p_1 \cdot \ldots \cdot p_r + 3$. Разложим N в произведение простых: $N = q_1 \cdot \ldots \cdot q_s$. Очевидно, числа q_i не могут быть чётными, поэтому либо $q_i = 4k_i+1$, либо $q_i = 4k_i+3$. Если бы все числа q_i были вида $4k_i+1$, то и их произведение тоже имело бы такой вид, а это не так. С другой стороны, ни одно из q_i не может совпадать с каким-либо из чисел p_j по соображениям делимости. Противоречие. ■

В 1775 г. Эйлер доказал бесконечность количества простых вида $100n+1$. Общее доказательство утверждения о бесконечности простых вида $an \pm 1$ можно найти в [2]. Теорема Дирихле — куда более общий факт.

3.1.2. Сравнения по модулю и их простейшие свойства

Определение. Два целых числа a и b называются *сравнимыми по модулю m* (обозначается $a \equiv b \pmod m$), если $m \,\big|\, (a-b)$ или, что то же самое, если a и b имеют одинаковые остатки при делении на m.

Свойства:

1. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$.
2. $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$, ибо $ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d) \vdots m$.
3. Если $ab \equiv ac \pmod m$ и $(a, m) = 1$, то $b \equiv c \pmod m$. Действительно, если $m \mid (ab - ac)$ и m не делит a, то по лемме 1.6 получаем, что $m \mid (b-c)$, а это и требовалось.

Замечание. Условие $(a, m) = 1$ в последнем свойстве существенно: $4 \equiv 0 \pmod 4$, но из этого не следует, что $2 \equiv 0 \pmod 4$.

Итак, мы разбили все множество $\mathbb{Z}$ на классы сравнимых по модулю m элементов (классы вычетов по модулю m): $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. Из свойств, указанных выше, сразу следует, что классы вычетов по модулю m образуют кольцо, обозначаемое $\mathbb{Z}/m\mathbb{Z}$.

Чтобы не доказывать эти свойства вычетов, можно было бы сослаться на алгебру и сказать: рассмотрим факторкольцо $\mathbb{Z}/m\mathbb{Z}$. Очень часто для кольца $\mathbb{Z}/m\mathbb{Z}$ используется более короткое обозначение: $\mathbb{Z}_m$. Мы тоже будем его использовать.

Лемма 3.2. *При всех $a \in \mathbb{Z}$, для которых $(a, m) = 1$, уравнение $ax \equiv b \pmod m$ имеет единственное решение в $\mathbb{Z}_m$.*

□ Рассмотрим отображение $S\colon \mathbb{Z}_m \to \mathbb{Z}_m$, определённое по правилу $S\colon \overline{k} \to \overline{ak}$. Заметим, что S инъективно: (если $ak_1 \equiv ak_2 \pmod m$, то $k_1 \equiv k_2 \pmod m$). Но инъективное отображение конечных множеств биективно, значит, найдётся ровно одно $x \in \mathbb{Z}_m$, для которого $\overline{ax} = \overline{b}$. ■

Следствие 3.1. *Если $(a, m) = 1$, то элемент $\overline{a}$ обратим в $\mathbb{Z}_m$.*

□ Уравнение $ax \equiv 1 \pmod m$ разрешимо. А это и означает, что $x = a^{-1}$. ■

Определение. Количество натуральных чисел, не превосходящих m и взаимно простых с m, называется *функцией Эйлера* и обозначается $\varphi(m)$.

Утверждение 3.3. *Количество обратимых элементов в $\mathbb{Z}_m$ равно $\varphi(m)$. Они образуют группу, которая обозначается $\mathbb{Z}_m^*$.*

□ Первое сразу следует из предыдущего следствия и определения функции Эйлера. Доказательство второго утверждения предоставляется читателю. ■

Как вычислять функцию $\varphi(m)$? Вообще говоря, вычисление φ для произвольного m — это алгоритмически трудоёмкая задача. Однако, если p — простое, то ясно, что $\varphi(p) = p - 1$. Легко также видеть, что $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$, поскольку лишь числа, кратные p, не взаимно просты с p^k.

Определение. Функция f называется *мультипликативной*, если для любых взаимно простых чисел a и b имеет место равенство $f(ab) = f(a)f(b)$.

Замечание. Всякая вполне мультипликативная функция является мультипликативной, но не наоборот.

Лемма 3.4. *Функция Эйлера мультипликативна.*

□ Пусть $(a, b) = 1$. Рассмотрим множество чисел

$$M := \left\{ m = ak + bl \;\middle|\; k = 0, \ldots, b-1, \quad l = 0, \ldots, a-1 \right\}. \tag{1}$$

Докажем, что все они различны. Действительно, если $ak_1 + bl_1 = ak_2 + bl_2$, то $b \,\big|\, (ak_1 - ak_2)$, значит, $b \,\big|\, (k_1 - k_2)$. Воспользовавшись тем, что $|k_1 - k_2| < b$, заключаем, что $k_1 = k_2$, поэтому и $l_1 = l_2$.

Теперь докажем, что $(ak + bl, ab) = 1$ тогда и только тогда, когда $(a, l) = 1$ и $(k, b) = 1$.

$\boxed{\Rightarrow}$ Предположим противное: найдётся p такое, что $p \mid a$ и $p \mid l$. Но тогда $p \mid (ak + bl)$ и $p \mid ab$ — противоречие. Взаимная простота k и b доказывается симметрично.

$\boxed{\Leftarrow}$ Предположим противное: найдётся p такое, что $p \mid (ak + bl)$ и $p \mid ab$. Тогда p делит либо a, либо b. Пусть, для определённости, $p \mid a$. Тогда $p \mid bl$. Но p не может делить b (т. к. a и b взаимно просты), значит $p \mid l$. Но это противоречит тому, что $(a, l) = 1$.

Докажем, что $ak + bl$ лежат в разных классах вычетов по модулю ab. Действительно, если $ak_1 + bl_1 \equiv ak_2 + bl_2 \pmod{ab}$, тогда $a \mid (a(k_1 - k_2) + b(l_1 - l_2))$, поэтому $a \mid (l_1 - l_2)$, значит, $l_1 = l_2$. Аналогично, $k_1 = k_2$.

Итак, количество чисел, взаимно простых с ab и меньших ab, столько, сколько существует в M чисел $ak + bl$, для которых $(a, l) = 1$, и $(k, b) = 1$. А это и означает, что $\varphi(ab) = \varphi(a)\varphi(b)$. ■

Теорема 3.5 (Эйлер). *Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod m$.*

□ **1°** Группа $\mathbb{Z}_m^*$ имеет порядок $\varphi(m)$. А по теореме Лагранжа порядок элемента делит порядок группы, значит $\overline{a}^{\varphi(m)} = \overline{1} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$.

2° Можно доказать эту теорему, не ссылаясь явно на алгебру. Пусть $b_1, \ldots, b_{\varphi(m)}$ — все числа из отрезка $[1, m]$, взаимно простые с m. Легко проверить, что числа $ab_1, \ldots, ab_{\varphi(m)}$ тоже взаимно просты с модулем и лежат в разных классах вычетов. Значит, существует биекция между $\left\{b_1, \ldots, b_{\varphi(m)}\right\}$ и $\left\{ab_1, \ldots, ab_{\varphi(m)}\right\}$. Поэтому

$$b_1 \cdot \ldots \cdot b_{\varphi(m)} \equiv ab_1 \cdot \ldots \cdot ab_{\varphi(m)} \pmod m, \tag{2}$$

откуда $a^{\varphi(m)} \equiv 1 \pmod m$. ■

Следствие 3.2 (Малая теорема Ферма). *Если простое число p не делит a, то $a^p \equiv a \pmod p$.*

Утверждение 3.6. *Множество простых вида $4n + 1$ бесконечно.*

□ Предположим противное: $p_1, \ldots, p_r$ — все простые такого вида. Составим число $N := 4p_1^2 \cdot \ldots \cdot p_r^2 + 1 = a^2 + 1$, где $a = 2p_1 \cdot \ldots \cdot p_r$. Пусть q — простой делитель N. Очевидно, что $q \neq p_1, \ldots, p_r$. Имеем $a^2 + 1 \equiv 0 \pmod q$, то есть $a^2 \equiv -1 \pmod q$. Возведем левую и правую части последнего выражения в степень $\frac{q-1}{2}$ (она целая, поскольку q, очевидно, нечётное). Получим

$$a^{q-1} \equiv (-1)^{\frac{q-1}{2}} \pmod q. \tag{3}$$

Пользуемся теоремой Ферма и получаем, что $q = 4k + 1$. Противоречие. ■

3.1.3. Ещё одно доказательство бесконечности множества простых чисел вида $4n \pm 1$

Хотя этот факт нами уже установлен в предыдущих параграфах, не лишним будет узнать доказательство, предложенное Эйлером. Похожий метод будет использован в общем случае, функции χ назовутся *характерами*, а функции L_i — *L-функциями Дирихле.*

Теорема 3.7.

$$\sum_{p\equiv 1(4)} \frac{1}{p} = \infty, \qquad \sum_{p\equiv 3(4)} \frac{1}{p} = \infty. \tag{4}$$

□ Введем новые функции

$$\begin{aligned} L_0(s) &:= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \ldots = \sum_0^\infty \frac{1}{(2n+1)^s}, \\ L_1(s) &:= 1 - \frac{1}{3^s} + \frac{1}{5^s} - \ldots = \sum_0^\infty \frac{(-1)^n}{(2n+1)^s}. \end{aligned} \tag{5}$$

Оба ряда сходятся, а второй ещё и абсолютно сходится. Пусть

$$\chi_0(n) := \begin{cases} 0, & n = 2k, \\ 1, & n = 2k+1, \end{cases} \tag{6}$$

$$\chi_1(n) := \begin{cases} 0, & n = 2k, \\ 1, & n \equiv 1 \pmod 4, \\ -1, & n \equiv 3 \pmod 4. \end{cases} \tag{7}$$

Тогда

$$L_0(s) = \sum_1^\infty \frac{\chi_0(n)}{n^s}, \qquad L_1(s) = \sum_1^\infty \frac{\chi_1(n)}{n^s}. \tag{8}$$

Легко проверить, что χ_0 и χ_1 — вполне мультипликативные функции. Значит, для функции $\frac{\chi(n)}{n^s}$, где $\chi = \chi_0$ или $\chi = \chi_1$, можно применить лемму 2.10 и получить, что

$$L_0(s) = \prod_{p\geqslant 3} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1}, \qquad L_1(s) = \prod_{p\geqslant 3} \left(1 - \frac{\chi_1(p)}{p^s}\right)^{-1}. \tag{9}$$

Логарифмируя левую и правую части полученных выражений, получаем

$$\ln L(s) = -\sum_{p\geqslant 3} \ln\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{p\geqslant 3} \left(\frac{\chi(p)}{p^s} + r_p(s)\right). \tag{10}$$

Оценим $r_p(s)$. Если $|x| < \frac{1}{2}$, то $\ln(1-x) = -\left(x + \frac{x^2}{2} + \ldots\right)$, поэтому

$$|\ln(1-x) + x| \leqslant \frac{|x|^2}{2} + \frac{|x|^3}{3} + \ldots \leqslant \frac{1}{2}(|x|^2 + |x|^3 + \ldots) = \frac{|x|^2}{2(1-|x|)} \leqslant |x^2|. \tag{11}$$

Поэтому $r_p(s) \leqslant \left|\frac{\chi(p)}{p^s}\right|^2 \leqslant \frac{1}{p^2}$. Значит, $\left|\sum r_p(s)\right| \leqslant \sum \frac{1}{n^2} \leqslant \infty$. Посему

$$\ln L(s) = \sum_{p\geqslant 3} \frac{\chi(p)}{p^s} + O(1), \quad s > 1. \tag{12}$$

Значит, получаем

$$\begin{aligned} \sum_{p\equiv 1(4)} \frac{1}{p^s} + \sum_{p\equiv 3(4)} \frac{1}{p^s} &= \ln L_0(s) + O(1), \\ \sum_{p\equiv 1(4)} \frac{1}{p^s} - \sum_{p\equiv 3(4)} \frac{1}{p^s} &= \ln L_1(s) + O(1). \end{aligned} \tag{13}$$

Складывая и вычитая эти равенства, получаем

$$\begin{aligned}\sum_{p\equiv 1(4)} \frac{1}{p^s} &= \frac{1}{2}\big(\ln L_0(s) + \ln L_1(s)\big) + O(1).\\ \sum_{p\equiv 3(4)} \frac{1}{p^s} &= \frac{1}{2}\big(\ln L_0(s) - \ln L_1(s)\big) + O(1).\end{aligned} \tag{14}$$

Пусть $s \in \mathbb{R}$. Перейдём к пределу $s \to 1+$. Если бы ряды из формулировки теоремы сходились, то это бы означало, что существуют пределы правых частей равенств. Покажем, что они не существуют.

$$L_0(s) = \sum_0^\infty \frac{1}{(2n+1)^s} \geqslant \frac{1}{2^s}\sum_0^\infty \frac{1}{(n+1)^s} = \frac{\zeta(s)}{2^s} \to \infty, \quad s \to 1, \tag{15}$$

поскольку ζ-функция в точке 1 имеет полюс.

Теперь оценим $L_1(s)$. Применим признак Дирихле равномерной сходимости ряда: если $|\sum a_n(s)| \leqslant C$ и $b_n \rightrightarrows 0$, то ряд $\sum a_n(s)b_n(s)$ сходится равномерно. В нашем случае $a_n(s) = (-1)^n$, а $b_n(s) = \frac{1}{(2n+1)^s}$. Значит, $L_1(s)$ сходится равномерно при $s \to 1$. Поэтому

$$\lim_{s\to 1} \ln L_1(s) = \ln L_1(1) = \ln\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots\right) < \infty. \tag{16}$$

Значит, наши ряды расходятся (а значит, слагаемых в них бесконечно много). ■

3.2. Характеры Дирихле

3.2.1. Определение и простейшие свойства

Зафиксируем некоторое $m \geqslant 2$.

Определение. Вполне мультипликативная m-периодическая функция $\chi\colon \mathbb{Z} \to \mathbb{C}$ называется *характером Дирихле*, если $\chi(n) \neq 0$ тогда и только тогда, когда $(n, m) = 1$. Характер

$$\chi_0(n) = \begin{cases}1, & (n,m) = 1,\\ 0, & (n,m) \neq 1\end{cases} \tag{17}$$

называется *главным характером*.

Сформулируем некоторые очевидные свойства характеров.

1° Если χ_1 и χ_2 — характеры, то и $\chi_1\chi_2$ — характер.

2° $\chi_0\chi = \chi$ для любого χ.

Далее мы покажем, что характеры образуют группу (пока не доказано существование обратного элемента).

3° По определению $\chi(1) \neq 0$. Из мультипликативности следует, что $\chi(1) = 1$.

4° Пусть $(n, m) = 1$. Тогда $n^{\varphi(m)} \equiv 1 \pmod m$. Поэтому $1 = \chi(1) = \chi\big(n^{\varphi(m)}\big) = \chi^{\varphi(m)}(n)$. Значит, ненулевые значения характера — это просто корни из единицы степени $\varphi(m)$.

5° Очевидным следствием **4°** является следующий полезный факт: $|\chi(n)| \leqslant 1$ для всех n.

Теорема 3.8. *Для каждого $m \geqslant 2$ существует в точности $\varphi(m)$ характеров.*

$$\sum_{n=1}^m \chi(n) = \begin{cases}\varphi(m), & \chi = \chi_0,\\ 0, & \chi \neq \chi_0.\end{cases} \tag{18}$$

$$\sum_{\chi} \chi(n) = \begin{cases}\varphi(m), & n \equiv 1 \pmod m,\\ 0, & n \not\equiv 1 \pmod m.\end{cases} \tag{19}$$

□ **1°** Группа $\mathbb{Z}_m^*$ абелева, а потому единственным образом разлагается в прямое произведение циклических подгрупп:

$$\mathbb{Z}_m^* = H_1 \times \ldots \times H_r, \qquad H_j = \langle \overline{c}_j \rangle, \quad |H_j| = d_j, \quad d_1 \cdot \ldots \cdot d_r = \varphi(m). \tag{20}$$

Иначе говоря, если $\overline{n} \in \mathbb{Z}_m^*$, то $\overline{n} = \overline{c}_1^{k_1} \cdot \ldots \cdot \overline{c}_r^{k_r}$. На языке сравнений это звучит так: если $(n, m) = 1$, то $n = c_1^{k_1} \cdot \ldots \cdot c_r^{k_r} \pmod m$.

Пусть ξ_k — корень из 1 степени d_k, $k = 1, \ldots, r$. Обозначим $\xi := (\xi_1, \ldots, \xi_r)$. Построим функцию

$$\chi_\xi(n) := \begin{cases}0, & (n,m) \neq 1,\\ \xi_1^{k_1} \cdot \ldots \cdot \xi_r^{k_r}, & n \equiv c_1^{k_1} \cdot \ldots \cdot c_r^{k_r} \pmod m.\end{cases} \tag{21}$$

Очевидно, что это характер. Покажем теперь, что разным наборам ξ соответствуют разные характеры. Действительно, если $\xi_i \neq \nu_i$, то $\xi_i = \chi_\xi(c_i) \neq \chi_\nu(c_i) = \nu_i$. Значит, количество построенных характеров совпадает с количеством наборов ξ, а их $d_1 \cdot \ldots \cdot d_r = \varphi(m)$.

Теперь докажем, что других характеров нет. Пусть χ — произвольный характер. Покажем, что он определяется значениями на образующих группы. Пусть $\tau_i := \chi(c_i)$. Поскольку $c_j^{d_j} \equiv 1 \pmod m$, то $1 = \chi(1) = \chi(c_j^{d_j}) = \chi^{d_j}(c_j)$. Таким образом $\tau := (\tau_1, \ldots, \tau_r)$ — это набор корней из единицы соответствующих степеней. Поэтому, если $(n, m) = 1$, то $\chi(n) = \chi\big(c_1^{k_1} \cdot \ldots \cdot c_r^{k_r}\big) = \tau_1^{k_1} \cdot \ldots \cdot \tau_r^{k_r}$. Значит, χ уже содержится в построенном множестве характеров и первое утверждение полностью доказано.

2° Если $\chi = \chi_0$, то очевидно, что $\sum\limits_{n=1}^{m} \chi(n) = \varphi(m)$. Если же $\chi \neq \chi_0$, то сопоставим этому характеру набор ξ такой, что если $(n, m) = 1$ и $n \equiv c_1^{k_1} \cdot \ldots \cdot c_r^{k_r} \pmod m$, то $\chi(n) = \xi_1^{k_1} \cdot \ldots \cdot \xi_r^{k_r}$. Поэтому

$$\sum_{n=1}^{m} \chi(n) = \sum_{n\colon (n,m)=1} \chi(n) = \sum_{k_1,\ldots,k_r} \xi_1^{k_1} \cdot \ldots \cdot \xi_r^{k_r} = \prod_{j=1}^{r} \left(\sum_{k=0}^{d_j - 1} \xi_j^{k_j} \right) = 0. \tag{22}$$

Последнее равенство обосновано тем, что найдётся k такое, что $\xi_k \neq 1$ и поэтому один из сомножителей равен 0.

Поясним, почему один из сомножителей равен нулю. Пусть ξ — корень степени d из 1, причём $\xi \neq 1$. Покажем, что $1 + \xi + \xi^2 + \ldots + \xi^{d-1} = 0$. Умножение этой суммы на ξ означает поворот, и при этом повороте фигура из d векторов, торчащих из нуля в вершины правильного d-угольника, переходит в себя. Значит, сумма тоже не поменяется. Такое может быть только в случае, когда сумма равна нулю.

3° Если $n \equiv 1 \pmod m$, то в силу периодичности имеем $\chi(n) = \chi(1) = 1$, поэтому $\sum\limits_{\chi} \chi(n) = \varphi(m)$. Пусть теперь $n \not\equiv 1 \pmod m$. Если $(n, m) \neq 1$, то для всех χ имеем $\chi(n) = 0$, и потому $\sum\limits_{\chi} \chi(n) = 0$. Если же $(n, m) = 1$, то найдётся ненулевой показатель степени k_j в разложении n. Поэтому

$$\sum_{\chi} \chi(n) = \sum_{\xi_1,\ldots,\xi_r} \xi_1^{k_1} \cdot \ldots \cdot \xi_r^{k_r} = \prod_{j=1}^{r} \left(\sum_{\xi_i} \xi_i^{k_j} \right) = 0. \tag{23}$$

■

Следствие 3.3. *Пусть* $\chi \neq \chi_0$ *и* $S(N) := \sum\limits_{k=1}^{N} \chi(k)$. *Тогда* $|S(N)| \leqslant m$.

□ Разделим N на m с остатком: $N = mq + r$. Разобьём сумму на две части: неполное частное и остаток. Из теоремы следует, что неполное частное равно нулю (в силу m-периодичности), а остаток не больше m. ■

Пример 2.1. Пусть $m = 4$, тогда $\varphi(m) = 2$. Если n нечетно, то $n \equiv 3^k \pmod 4$, $k = 0, 1$, поэтому $d = 2$. Мы приходим к функции из предыдущего параграфа:

$$\chi(n) = \begin{cases} 1, & n \equiv 1 \pmod 4, \\ -1, & n \equiv 3 \pmod 4. \end{cases} \tag{24}$$

3.2.2. L-функции Дирихле

Определение. Зафиксируем $m \geqslant 2$ и характер χ. *L-функцией Дирихле* назовем функцию

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{25}$$

Лемма 3.9. *Если* $\chi = \chi_0$, *то ряд для* $L(s, \chi)$ *абсолютно сходится в* $\operatorname{Re} s > 1$ *и* $L(s, \chi)$ *аналитична в* $\operatorname{Re} s > 1$. *Если* $\chi \neq \chi_0$, *то ряд для* $L(s, \chi)$ *сходится в* $\operatorname{Re} s > 0$ *и* $L(s, x)$ *аналитична в* $\operatorname{Re} s > 0$.

□ Первое утверждение очевидным образом следует из свойств ζ-функции и свойства $|\chi(n)| \leqslant 1$. Докажем второе утверждение. Пусть $s = \sigma + it$, положим $S(N) := \sum\limits_{k=1}^{N} \chi(k)$. Полагая по определению $S(0) := 0$, имеем

$$\sum_{n=1}^{N} \frac{\chi(n)}{n^s} = \sum_{n=1}^{N} \frac{S(n) - S(n-1)}{n^s} = \sum_{n=1}^{N} \frac{S(n)}{n^s} - \sum_{n=1}^{N-1} \frac{S(n)}{(n+1)^s} = \frac{S(N)}{N^s} + \sum_{n=1}^{N-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right). \tag{26}$$

Мы знаем, что $|S(n)| \leqslant m$, если $\chi \neq \chi_0$. Поэтому $\left|\frac{S(N)}{N^s}\right| \leqslant \frac{m}{N^\sigma} \to 0$ при $N \to \infty$. Оценим выражение в скобке:

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| = \left|s \int\limits_n^{n+1} x^{-(s+1)}dx\right| \leqslant |s| \cdot n^{-(\sigma+1)} \quad \Rightarrow \quad \left|S(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| \leqslant \frac{m|s|}{n^{\sigma+1}}. \tag{27}$$

Поэтому ряд сходится равномерно на любом компакте из правой полуплоскости, значит сходится в правой полуплоскости. Значит, в ней он задаёт аналитическую функцию. ■

Нам хотелось бы продолжить функцию $L(s, \chi_0)$ в область $\operatorname{Re} s > 0$. В этом нам поможет следующая

Лемма 3.10 (Формула Эйлера для L-функций). *Для любого характера χ в области $\operatorname{Re} s > 1$ справедливо тождество*

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{28}$$

□ Доказательство аналогично тому, как мы это делали для ζ-функции. Здесь пользуемся вполне мультипликативностью функции $\frac{\chi(n)}{n^s}$ и леммой 2.10. ■

Таким образом,

$$L(s, \chi_0) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{29}$$

Поэтому

$$L(s, \chi_0) = \zeta(s) \prod_{p \mid m} \left(1 - \frac{1}{p^s}\right), \quad \operatorname{Re} s > 1. \tag{30}$$

В первой главе мы продолжали ζ-функцию в область $\operatorname{Re} s > 0$. При этом у нее был полюс первого порядка в $s = 1$. Заметим, что функция $\prod\limits_{p \mid m} \left(1 - \frac{1}{p^s}\right)$ — целая функция, не обращающаяся в 0 в точке $s = 1$. Поэтому можно считать, что $L(s, \chi_0)$ мы определили всюду в правой полуплоскости, и она имеет полюс первого порядка в $s = 1$.

Теорема 3.11. *Если $\chi \neq \chi_0$, то $L(1, \chi) \neq 0$.*

□ Доказательство разобьём на две части.

1° Пусть сначала χ — не действительный характер (то есть принимает не только действительные значения). Это равносильно тому, что $\chi^2 \neq \chi_0$. Настало время ещё раз применить лемму 2.14. Рассмотрим

$$P := \left|L(s, \chi_0)^3 L(S, \chi)^4 L(s, \chi^2)\right| = \prod_{p \nmid m} \left(\left|1 - \frac{\chi_0(p)}{p^s}\right|^3 \left|1 - \frac{\chi(p)}{p^s}\right|^4 \left|1 - \frac{\chi^2(p)}{p^s}\right|\right)^{-1}. \tag{31}$$

Если считать, что s — действительное число, большее 1, а $r := \frac{1}{p^s}$, $\chi(p) = e^{i\varphi}$, тогда $\chi^2(p) = e^{2i\varphi}$. По лемме каждый множитель в произведении P не меньше 1, а значит, $P \geqslant 1$.

Предположим теперь, что $L(1, \chi) = 0$. Тогда по непрерывности $L(s, \chi) = O(s-1)$ при $s \to 1$. Так как $\chi^2 \neq \chi_0$, то $L(s, \chi^2) = O(1)$. Кроме того,

$$L(s, \chi_0) = O\left(\frac{1}{s-1}\right). \tag{32}$$

Из этих оценок следует, что

$$P = O\left(\frac{1}{(s-1)^3}(s-1)^4 \cdot 1\right) = O(s-1), \tag{33}$$

а это противоречит ранее полученному свойству $P \geqslant 1$.

2° Пусть теперь χ — действительный характер, то есть $\chi^2 = \chi_0$. Рассмотрим функцию $F(s) := \zeta(s)L(s, \chi)$. Дальнейшему доказательству предпошлём лемму.

Лемма 3.12. *В области $\operatorname{Re} s > 1$ функция $F(s) = \zeta(s)L(s, \chi)$ представима в виде*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad a_n \in \mathbb{Z}_+, \qquad a_{k^2} \geqslant 1, \tag{34}$$

причём в точке $s = \frac{1}{2}$ ряд расходится.

□ В силу абсолютной сходимости рядов для ζ и L, их можно перемножать. Значит,

$$F(s) = \sum_{u=1}^{\infty} \frac{1}{u^s} \sum_{v=1}^{\infty} \frac{\chi(v)}{v^s} = \sum_{u,v \geqslant 1} \frac{\chi(v)}{(uv)^s} = \sum_{v=1}^{\infty} \frac{1}{n^s} \sum_{v|n} \chi(v) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{35}$$

где $a_n = \sum\limits_{v|n} \chi(v)$. Поскольку $\chi(n) = \pm 1$, то очевидно, что $a_n \in \mathbb{Z}$. Осталось проверить неотрицательность. Пусть $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, тогда $v = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$ $(\beta_j \leqslant \alpha_j)$, тогда

$$a_n = \sum_{\beta_1,\ldots,\beta_r} \chi(p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}) = \prod_{j=1}^{r} \left(\sum_{\beta_j=0}^{\alpha_j} \chi(p_j)^{\beta_j} \right) = a_{n1} \cdot \ldots \cdot a_{nr}, \tag{36}$$

где

$$a_{nj} = \sum_{\beta=0}^{\alpha_j} \chi(p_j)^{\beta} = \begin{cases} \alpha_j + 1, & \chi(p_j) = 1, \\ 1, & \chi(p_j) = 0, \\ 0, & \chi(p_j) = -1, \text{ и } \alpha_j \text{ нечётно}, \\ 1, & \chi(p_j) = -1, \text{ и } \alpha_j \text{ чётно}. \end{cases} \tag{37}$$

При $n = k^2$ степени чётны, поэтому $a_{nj} \neq 0$, значит, $a_n \geqslant 1$.

Если предположить, что ряд сходится при $s = \frac{1}{2}$, то есть $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^{1/2}} < \infty$, то, тем более, $\sum\limits_{k=1}^{\infty} \frac{a_{k^2}}{k} < \infty$, а поскольку $a_{k^2} \geqslant 1$, то получаем, что гармонический ряд тоже должен сходиться, что нелепо.

Кроме того, стандартными рассуждениями получаем, что ряд для $F(s)$ равномерно сходится на всяком компакте в области $\operatorname{Re} s > 1$, откуда следует аналитичность и возможность почленного дифференцирования. ■

Вернёмся к доказательству второй части теоремы. Предположим, что $L(1, \chi) = 0$. Тогда функция $F(s)$ аналитична в $\operatorname{Re} s > 0$ (полюс исчезнет). Значит, можно разложить функцию $F(s)$ в круге с центром в точке $s = 2$ радиуса 2:

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(2)}{k!} (s-2)^k = \sum_{k=0}^{\infty} \frac{(s-2)^k}{k!} (-1)^k \sum_{n=1}^{\infty} \frac{a_n \ln^k n}{n^2} =$$

$$= \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(2-s)^k a_n \ln^k n}{n^2 k!} = \sum_{n=1}^{\infty} a_n \sum_{k=0}^{\infty} \frac{(2-s)^k \ln^k n}{n^2 k!} \overset{!}{=} \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{38}$$

Поясним переход, отмеченный знаком «!»: мы свернули тейлоровское разложение функции $\frac{1}{n^s}$ в точке $s = 2$. Этот ряд расходится при $s = \frac{1}{2}$, а мы получили, что он сходится в силу аналитичности функции. Противоречие.

Итак, мы доказали, что $L(1, \chi) \neq 0$ для неглавных характеров. Теорема доказана полностью. ■

3.2.3. Доказательство теоремы Дирихле

Лемма 3.13. *В области* $\operatorname{Re} s > 1$ *имеет место равенство*

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}, \tag{39}$$

где Λ *— функция Мангольдта. Ряд сходится абсолютно и* $L(s, \chi) \neq 0$ *в этой области.*

□ Имеет место очевидная оценка

$$\left| \frac{\Lambda(n)\chi(n)}{n^s} \right| \leqslant \frac{\ln n}{n^{\operatorname{Re} s}}. \tag{40}$$

Отсюда легко следует абсолютная сходимость и аналитичность. Остается проверить выполнение равенства, заявленного в лемме. В самом деле,

$$L(s,\chi) \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} = \sum_{l=1}^{\infty} \frac{\chi(l)}{l^s} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \sum_{k|n} \Lambda(k) \overset{!}{=} -L'(s,\chi). \tag{41}$$

В последнем переходе, отмеченном «!», мы воспользовались тем, что $\sum\limits_{k|n} \Lambda(k) = \ln n$.

Докажем отсутствие нулей у L. При дифференцировании порядок нуля падает на единицу. Значит, если бы у L был нуль порядка $r > 0$, то порядок нуля слева был бы не меньше r, а справа — в точности равен $r - 1$. Противоречие. ■

Теперь можно приступить к доказательству того, ради чего мы заварили всю эту кашу с характерами.

Теорема 3.14 (Дирихле). *Если $(m,l)=1$, то последовательность $\{mn+l\}$ содержит бесконечно много простых чисел.*

□ Из предыдущей леммы следует, что

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{k\geqslant 1,p} \frac{\ln p\cdot\chi(p^k)}{p^{ks}} = \sum_p \frac{\ln p\cdot\chi(p)}{p^s} + \sum_{k\geqslant 2,p} \frac{\ln p\cdot\chi(p^k)}{p^{ks}}. \tag{42}$$

Докажем, что последнее слагаемое ограничено константой, не зависящей от s.

$$\Big|\sum_{k\geqslant 2,p} \frac{\ln p\cdot\chi(p^k)}{p^{ks}}\Big| \leqslant \sum_{k,p} \frac{\ln p}{p^k} = \sum_p \ln p \sum_{k=2}^{\infty} \frac{1}{p^k} = \sum_p \frac{1}{p^2-p}\ln p \leqslant \sum_{n=2}^{\infty} \frac{1}{n^2-n}\ln n < \infty. \tag{43}$$

Таким образом, установлено соотношение:

$$\sum_p \frac{\ln p\cdot\chi(p)}{p^s} = -\frac{L'(s,\chi)}{L(s,\chi)} + O(1), \quad \operatorname{Re} s > 1. \tag{44}$$

Числа m и l взаимно просты по условию, значит, уравнение $lx \equiv 1 \pmod m$ имеет единственное решение из $\mathbb{Z}_m^*$. Пусть $ld \equiv 1 \pmod m$. Тогда умножим равенство (44) на $\chi(d)$ и просуммируем по всем χ:

$$\sum_p \frac{\ln p}{p^s} \sum_\chi \chi(pd) = -\sum_\chi \chi(d)\frac{L'(s,\chi)}{L(s,\chi)} + O(1). \tag{45}$$

Вспомним, что

$$\sum_\chi \chi(n) = \begin{cases} \varphi(m), & n \equiv 1 \pmod m, \\ 0, & n \not\equiv 1 \pmod m. \end{cases} \tag{46}$$

Поэтому в $\sum\limits_p \chi(pd)$ ненулевыми будут лишь слагаемые у которых $p \equiv l \pmod m$. Что касается правой части, то в ней особым является только слагаемое главного характера, все остальные в силу теоремы 3.11 не имеют полюсов и потому их можно загнать в $O(1)$. Итого получаем

$$\varphi(m)\cdot \sum_{p\equiv l(m)} \frac{\ln p}{p^s} = -\chi_0(d)\frac{L'(s,\chi_0)}{L(s,\chi_0)} + O(1). \tag{47}$$

А мы знаем, что $L(s,\chi_0) = \frac{f(s)}{s-1}$, причём $f(1)\neq 0$. Стало быть, $\frac{L'}{L} = -\frac{1}{s-1} + \frac{f'}{f}$. Кроме того, $\chi_0(d)=1$. Поэтому

$$\frac{1}{s-1} + O(1) = \varphi(m) \sum_{p\equiv l(m)} \frac{\ln p}{p^s}. \tag{48}$$

Слева стоит функция, стремящаяся к бесконечности при $s\to 1$, а справа — некоторая сумма, которая стремится к бесконечности лишь в случае, когда слагаемых в ней бесконечное количество. Теорема Дирихле доказана. ■

4. Алгебраические и трансцендентные числа

4.1. Алгебраические числа

4.1.1. Свойства алгебраических чисел

Определение. Комплексное число α называется *алгебраическим*, если найдется не тождественно нулевой многочлен $f(x)\in\mathbb{Q}[x]$, для которого $f(\alpha)=0$. Многочлен f называется *аннулирующим* для данного элемента α.

Легко видеть, что множество всех многочленов, аннулирующих данный элемент α, образует идеал в $\mathbb{Q}[x]$.

Определение. Многочлен минимальной степени со старшим коэффициентом 1, аннулирующий число α, называется *минимальным многочленом* числа α. Мы обычно будем обозначать его $f_\alpha(x)$. Степень многочлена $f_\alpha(x)$ называется *степенью числа* α и обозначается $\deg\alpha$.

Множество всех алгебраических чисел будем обозначать через $\mathbb{A}$.

Пример 1.1. Алгебраические числа степени 1 — это в точности все рациональные числа.

Пример 1.2. Пусть $\alpha = \sqrt{2}$. Очевидно, что $f_\alpha(x) = x^2 - 2$ является минимальным многочленом, поскольку α иррационально, и его степень никак не может быть меньше 2.

Пример 1.3. Пусть $\alpha = i$. Тогда $f_\alpha(x) = x^2 + 1$.

Пример 1.4. Пусть $\alpha = \sqrt[3]{2}$. Можно показать, что $f_\alpha(x) = x^3 - 2$ является минимальным многочленом, но сделать это сложнее, чем в случае квадратного корня.

Утверждение 4.1. *Минимальный многочлен f_α элемента α неприводим над $\mathbb{Q}$, и все его корни различны.*

□ Он неприводим (иначе это бы означало, что его степень не минимальна). Докажем, что все корни у $f_\alpha(x)$ разные. Действительно, наличие кратного корня равносильно тому, что $(f_\alpha, f'_\alpha) \neq 1$.

Контрольный вопрос: почему НОД f_α и f'_α — это многочлен с рациональными коэффициентами? Ведь их общий корень может быть и комплексным! Ответ: потому что алгоритм Евклида не выводит из мéньшего поля (в нашем случае — из $\mathbb{Q}$).

Но поскольку многочлен f_α неприводим, многочлен f'_α должен делиться на f_α, а это невозможно, поскольку $\deg f'_\alpha < \deg f_\alpha$. Стало быть, кратных корней не бывает. ■

Определение. Корни многочлена f_α называются *сопряженными* с α. Их ровно $\deg \alpha$ штук.

Нам потребуется одна теорема из курса алгебры:

Теорема 4.2. *Пусть R — коммутативное кольцо с единицей. Тогда для любого симметрического многочлена $A \in R[x_1, \ldots, x_m]$ найдется многочлен $Q \in R[x_1, \ldots, x_m]$, такой что $A(x_1, \ldots, x_m) = Q(\sigma_1, \ldots, \sigma_m)$, где σ_i — элементарные симметрические многочлены.*

Лемма 4.3. *Пусть $P(x, y) \in R[x, y]$. Тогда*

$$\prod_{i=1}^{m} P(x, x_i) = Q(x, \sigma_1, \ldots, \sigma_m), \quad Q \in R[x, x_1, \ldots, x_m]. \tag{1}$$

□ Пусть

$$\prod_{i=1}^{m} P(x, x_i) = A_N x^N + \ldots + A_1 x + A_0, \quad A_j \in R[x_1, \ldots, x_m]. \tag{2}$$

Поменяем x_i местами, при этом левая часть равенства никак не изменится, значит, и правая не изменится. Стало быть, многочлены A_j являются симметрическими. Тогда по предыдущей теореме найдутся многочлены $Q_1, \ldots, Q_N$, такие что $A_j = Q_j(\sigma_1, \ldots, \sigma_m)$. Остаётся только подставить Q_i вместо A_i в (2). ■

Следствие 4.1. *Пусть $P(x, y) \in \mathbb{Q}[x, y]$, $\beta \in \mathbb{A}$ и $\deg \beta = m$, а $\beta_1, \ldots, \beta_m$ сопряжены с β. Тогда*

$$\prod_{j=1}^{m} P(x, \beta_j) \in \mathbb{Q}[x]. \tag{3}$$

□ По предыдущей лемме, многочлен в левой части равенства равен $Q(x, \sigma_1, \ldots, \sigma_m)$, $Q \in \mathbb{Q}[x, x_1, \ldots, x_m]$. Пусть $f_\beta(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$ ($b_i \in \mathbb{Q}$). Но тогда по формулам Виета $\sigma_i(\beta) = (-1)^i b_i \in \mathbb{Q}$. ■

Теорема 4.4. *Множество $\mathbb{A}$ замкнуто относительно алгебраических операций. Иначе говоря, если числа α и β алгебраические, то числа $\alpha \pm \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$ тоже алгебраические.*

□ Для доказательства нам достаточно предъявить соответствующие аннулирующие многочлены.

1° Сумма: пусть $\beta_1, \ldots, \beta_m$ — числа, сопряженные с β. Докажем, что искомым многочленом (из определения алгебраического числа) будет

$$H_1(x) := \prod_{i=1}^{m} f_\alpha(x - \beta_i). \tag{4}$$

Действительно, $H_1(x) \in \mathbb{Q}[x]$ по предыдущей лемме. Ясно, что $H_1(\alpha + \beta) = 0$ (поскольку β содержится во множестве $\{\beta_i\}$).

2° Разность: аналогично **1°**.

3° Произведение: здесь хочется взять функцию $\prod\limits_{i=1}^{m} f_\alpha\left(\frac{x}{\beta_i}\right)$, но $f_\alpha\left(\frac{x}{y}\right)$ — не многочлен, поэтому его надо подправить, взяв многочлен $y^n \cdot f_\alpha\left(\frac{x}{y}\right)$:

$$H_3(x) := \prod_{i=1}^{m} \beta_i^n f_\alpha\left(\frac{x}{\beta_i}\right), \quad n = \deg \alpha. \tag{5}$$

4° Частное: берем многочлен $f_\alpha(xy)$, и получаем, что многочлен

$$H_4(x) := \prod_{i=1}^{m} f_\alpha(x \cdot \beta_i) \tag{6}$$

аннулирует $\frac{\alpha}{\beta}$. ■

Следствие 4.2. *Множество алгебраических чисел образует поле.*

Это можно было бы доказать и проще, с применением теории конечных расширений полей (она нам всё равно понадобится). Возьмём основное поле K и докажем, что множество всех элементов, алгебраических над K (обозначим его $\overline{K}$) образует поле.

Пусть $\alpha, \beta \in \overline{K}$. Рассмотрим (конечное) расширение $K(\alpha, \beta)$. Все конечные расширения — алгебраические. Действительно, пусть $[E : K] = d$, то есть конечное расширение E — это d-мерное векторное пространство над K. Стало быть, различные степени любого элемента $x \in E$ будут линейно зависимы над K, если их взять более d штук. Это и будет искомый аннулирующий многочлен.

Элементы α и β, конечно, лежат в $E := K(\alpha, \beta)$. Но это поле, значит, $\alpha \pm \beta \in E$, $\alpha \cdot \beta \in E$ и $\frac{\alpha}{\beta} \in E$. Значит, все они, в частности, алгебраичны над K.

4.1.2. Целые алгебраические числа

Определение. Алгебраическое число α называется *целым алгебраическим*, если $f_\alpha(x) \in \mathbb{Z}[x]$.

Пример 1.5. $\alpha = \frac{1}{\sqrt{2}}$: $f_\alpha(x) = x^2 - \frac{1}{2} \notin \mathbb{Z}[x]$.

Пример 1.6. $\alpha = \frac{1+\sqrt{5}}{2}$: $f_\alpha(x) = x^2 - x - 1 \in \mathbb{Z}[x]$.

Пример 1.7. Рациональное число является целым алгебраическим тогда и только тогда, когда оно целое.

Определение. Многочлен с целыми коэффициентами называется *примитивным*, если его коэффициенты взаимно просты в совокупности.

Лемма 4.5 (Гаусс). *Произведение примитивных многочленов есть примитивный многочлен.*

□ Пусть $A(x) = \sum\limits_0^n a_i x^i$, $B(x) = \sum\limits_0^m b_i x^i$. Тогда $A(x)B(x) = C(x) = \sum\limits_0^{n+m} c_i x^i$. Предположим, что многочлен C не примитивный, то есть найдётся p, делящее все его коэффициенты. В силу примитивности многочленов A и B, у них найдутся коэффициенты, не делящиеся на p. Выберем среди них коэффициенты с минимальными номерами, пусть это будут a_u и b_v. Имеем $c_{u+v} = \sum\limits_{k+l=u+v} a_k b_l$. В силу минимальности u и v, если $k < u$, то $p \mid a_k$, а если $l < v$, то $p \mid b_l$. Поэтому $c_{u+v} \equiv a_u b_v \not\equiv 0 \pmod{p}$. Противоречие. ■

Алгебраическое доказательство: допустим, что простое число p делит все коэффициенты многочлена C. Тогда проекция многочлена C на $\mathbb{F}_p[x]$ — это нулевой многочлен. С другой стороны, в силу примитивности A и B, их проекции на $\mathbb{F}_p[x]$ суть ненулевые многочлены. Но в $\mathbb{F}_p[x]$ нет делителей нуля, поэтому равенство $0 = \overline{C} = \overline{A} \cdot \overline{B}$ в $\mathbb{F}_p[x]$ невозможно.

Следствие 4.3. *Если $A(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in \mathbb{Z}[x]$ и $A(\alpha) = 0$, то α — целое алгебраическое.*

□ Многочлены $A(x)$ и $f_\alpha(x)$ имеют общий корень α. Многочлен f_α неприводим и посему $f_\alpha \mid A$ в $\mathbb{Q}[x]$, то есть $A(x) = f_\alpha(x)Q(x)$, где $Q \in \mathbb{Q}[x]$. У $A(x)$ и $f_\alpha(x)$ старшие коэффициенты равны 1, значит, и у $Q(x)$ он равен единице. Пусть q_r — наименьший общий знаменатель коэффициентов многочлена Q, то есть

$$Q(x) = x^r + \frac{q_{r-1}}{q_r}x^{r-1} + \ldots + \frac{q_0}{q_r}. \tag{7}$$

Очевидно, что числа $q_0, \ldots, q_{r-1}, q_r$ взаимно просты в совокупности. Тогда многочлен Q представи́м в виде $Q(x) = \frac{1}{q_r}U(x)$, где U — примитивный многочлен. Аналогично $f_\alpha(x) = \frac{1}{p_s}V(x)$, где V — примитивный. Но тогда $A(x) = \frac{1}{q_r p_s}U(x)V(x)$, значит, $U(x)V(x) = q_r p_s A(x)$. Пользуясь леммой Гаусса, получаем, что $q_r p_s = 1$, поэтому $p_s = q_r = 1$. Значит, $f_\alpha(x) \in \mathbb{Z}[x]$. ■

Теорема 4.6. *Множество целых алгебраических чисел замкнуто относительно операций сложения, вычитания и умножения.*

□ Достаточно доказать, что в условиях данной теоремы построенные в теореме 4.4 полиномы H_j лежат в $\mathbb{Z}[x]$ (равенство единице старшего коэффициента очевидно). Это будет означать (в силу предыдущего следствия) справедливость теоремы. Само доказательство проходит дословно, с заменой кольца $\mathbb{Q}$ на кольцо $\mathbb{Z}$, потому что для него тоже выполнены теорема 4.2 и лемма 4.3). ■

Лемма 4.7. *Если α — алгебраическое число, то для него найдется $d \in \mathbb{N}$, для которого $d\alpha$ — целое алгебраическое.*

□ Пусть $f_\alpha(x) = x^n + p_{n-1}x^{n-1} + \ldots + p_0 \in \mathbb{Q}[x]$. Пусть d — общий знаменатель всех p_i. Домножим многочлен на d^n и выделим в мономе степени k множитель $(d\alpha)^k$:

$$0 = d^n \cdot f_\alpha(\alpha) = (d\alpha)^n + dp_{n-1}(d\alpha)^{n-1} + \ldots + d^n p_0. \tag{8}$$

Значит, многочлен $A(x) := x^n + dp_{n-1}x^{n-1} + \ldots + d^n p_0$ аннулирует $d\alpha$, а в силу выбора d имеем $A \in \mathbb{Z}[x]$. ■

4.1.3. Теорема о примитивном элементе

Пусть $\xi_1, \ldots, \xi_n$ — алгебраические числа, а $\mathbb{Q}(\xi_1, \ldots, \xi_n)$ — минимальное поле, содержащее $\mathbb{Q}$ и $\{\xi_i\}$. Оно имеет вид

$$\mathbb{Q}(\xi_1, \ldots, \xi_n) = \left\{ \frac{A(\xi_1, \ldots, \xi_n)}{B(\xi_1, \ldots, \xi_n)} \;\middle|\; B(\xi_1, \ldots, \xi_n) \neq 0;\ A, B \in \mathbb{Q}[x_1, \ldots, x_n] \right\}. \tag{9}$$

Поля такого вида называются *конечнопорождёнными.*

В курсе алгебры расширения полей строились несколько иначе. Напомним эту конструкцию. Пусть K — основное поле, и пусть $p \in K[x]$. Факторкольцо $E := K[x]/(p)$ будет полем тогда и только тогда, когда p неприводим над K. Заметим, что если α — корень неприводимого многочлена p, то в E этот многочлен уже имеет корень $\overline{x}$. Поле E будет векторным пространством над K степени $d := \deg p$ с базисом $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{d-1}$. Расширение E поля K называется простым алгебраическим расширением поля K, полученным присоединением корня α неприводимого многочлена p.

Лемма 4.8 (Про освобождение от знаменателя). *Пусть $\xi \in \mathbb{A}$, и $\deg \xi = n$. Тогда каждый элемент $\alpha \in \mathbb{Q}(\xi)$ единственным образом представляется в виде*

$$\alpha = r_0 + r_1\xi + \ldots + r_{n-1}\xi^{n-1}, \quad r_i \in \mathbb{Q}. \tag{10}$$

Иначе говоря, $\mathbb{Q}(\xi)$ — n-мерное векторное пространство над $\mathbb{Q}$ с базисом $1, \xi, \ldots, \xi^{n-1}$.

□ Пусть $\alpha = \frac{A(\xi)}{B(\xi)}$. Наша цель — построить элемент $B^{-1}(\xi)$. Многочлены f_ξ и B взаимно просты (иначе бы $f_\xi \mid B$, а тогда $B(\xi) = 0$). Поэтому в силу леммы о линейном представлении НОД существуют многочлены $U(x)$ и $V(x)$ из $\mathbb{Q}[x]$ такие, что

$$B(x)V(x) + f_\xi(x)U(x) = 1. \tag{11}$$

Значит, в частности, $B(\xi)V(\xi) + f_\xi(\xi)U(\xi) = 1$, а поскольку $f_\xi(\xi) = 0$, то

$$\frac{1}{B(\xi)} = V(\xi), \text{ то есть } \alpha = A(\xi)V(\xi). \tag{12}$$

Разделим многочлен $A(x)V(x)$ на $f_\xi(x)$ с остатком:

$$A(x)V(x) = Q(x)f_\xi(x) + R(x), \quad R(x) = r_0 + \ldots + r_{n-1}x^{n-1}. \tag{13}$$

Тогда $\alpha = A(\xi)V(\xi) = R(\xi)$.

Осталось проверить, что такое представление единственно. Допустим, что это не так, и $\alpha = R(\xi) = S(\xi)$, причём $\deg R, S < n$. Тогда многочлен $F = R - S$ аннулирует ξ, что невозможно, ибо $\deg \xi = n$, а $\deg F < n$. ■

Пример 1.8. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\theta)$. Действительно, решая уравнения

$$(\theta - \sqrt{2})^2 = 3, \quad (\theta - \sqrt{3})^2 = 2, \tag{14}$$

получаем, что $\sqrt{2} = \frac{\theta^2 - 1}{2\theta}$ и $\sqrt{3} = \frac{\theta^2 + 1}{2\theta}$. Поэтому $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\theta)$, значит, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$.

Теорема 4.9 (О примитивном элементе). *Пусть $\xi_1, \ldots, \xi_m \in \mathbb{A}$ и $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$. Тогда найдется $\theta \in E$ такое, что $E = \mathbb{Q}(\theta)$.*

□ Пусть сначала $m = 2$. Для удобства обозначим $\alpha = \xi_1$, $\beta = \xi_2$, Пусть $\alpha_1, \ldots, \alpha_p$ и $\beta_1, \ldots, \beta_q$ — числа, сопряженные с α и β соответственно. Пусть, для определённости, $\beta_1 = \beta$ и $\alpha_1 = \alpha$.

Положим $\theta := \alpha_1 + c\beta_1$, где c — целое число, такое что $\alpha_1 + c\beta_1 \neq \alpha_i + c\beta_j$ $((i, j) \neq (1, 1))$. Такое число c обязательно найдётся, поскольку имеется лишь конечное количество ограничений. Пусть $K := \mathbb{Q}(\theta)$, тогда ясно, что $K \subset E$.

Рассмотрим многочлены $h(x) := f_\alpha(\theta - cx) \in K[x]$ и $f_\beta \in \mathbb{Q}[x] \subset K[x]$. Имеем $f_\beta(\beta) = 0$, $h(\beta) = 0$, поэтому степень многочлена $d := (h, f_\beta)$ не меньше единицы. Все корни $d(x)$ различны (поскольку d делит f_β, а у него все корни различны). Пусть γ — корень многочлена d, не совпадающий с β. Тогда $\gamma = \beta_j$, причём $j \neq 1$. Имеем $h(\gamma) = h(\beta_j) = f_\alpha(\theta - c\beta_j) = 0$, но все корни многочлена $f_\alpha(x)$ — это α_i, поэтому $\theta - c\beta_j = \alpha_i$ для некоторого i, значит, $\theta = \alpha_i + c\beta_j$. Но мы специально выбирали θ так, что это возможно лишь в случае $i = j = 1$, поэтому на самом деле $\gamma = \beta$. Значит, у многочлена d есть только один корень β, поэтому он имеет вид $d(x) = ax + b \in K[x]$. Поэтому $\beta = -\frac{b}{a} \in K$ и $\alpha = \theta - c\beta \in K$. Таким образом, мы доказали, что $E = \mathbb{Q}(\alpha, \beta) \subset K$. Но ранее мы уже доказали обратное включение. Значит, на самом деле $E = K$.

Для произвольного m доказываем индукцией, с учётом равенства $\mathbb{Q}(\xi_1, \ldots, \xi_m) = \mathbb{Q}(\xi_1, \ldots, \xi_{m-1})(\xi_m)$. ■

Следствие 4.4. *Каждое поле, порожденное конечным количеством алгебраических чисел, есть конечномерное линейное пространство над $\mathbb{Q}$.*

Определение. *Степенью расширения E* поля рациональных чисел называется размерность E над $\mathbb{Q}$ и обозначается $[E : \mathbb{Q}]$, то есть $[E : \mathbb{Q}] = \dim_{\mathbb{Q}} E = \deg \theta$.

4.1.4. Алгебраическая замкнутость поля алгебраических чисел

Теорема 4.10. *Если $P \in \mathbb{A}[x]$ и ξ — корень $P(x)$, то $\xi \in \mathbb{A}$. Иначе говоря, поле алгебраических чисел алгебраически замкнуто.*

□ Пусть $P(x) = \alpha_n x^n + \ldots + \alpha_0$, $\alpha_i \in \mathbb{A}$, $\alpha_n \neq 0$, $P(\xi) = 0$. Можно считать, что $\alpha_n = 1$ (в любом случае можно на α_n поделить). Пусть $E = \mathbb{Q}(\alpha_{n-1}, \ldots, \alpha_0) = \mathbb{Q}(\theta)$, $m = \deg\theta = [E : \mathbb{Q}]$. Поэтому найдутся многочлены $F_j \in \mathbb{Q}[x]$ степени не выше m: $\alpha_j = F_j(\theta)$. Составим новый многочлен от двух переменных:

$$F(x, y) = x^n + F_{n-1}(y)x^{n-1} + \ldots + F_0(y) \in \mathbb{Q}[x, y]. \tag{15}$$

Пусть θ_i — корни, сопряжённые с θ, и пусть $\theta = \theta_1$. Рассмотрим теперь

$$H(x) = \prod_{i=1}^{m} F(x, \theta_i). \tag{16}$$

В силу следствия 4.1 получаем $H \in \mathbb{Q}[x]$. Но $F(\xi, \theta_1) = P(\xi) = 0$, то есть $H(\xi) = 0$. Значит $\xi \in \mathbb{A}$. ■

Мы уже приводили более краткие аргументы того, что множество $\overline{K}$ всех корней многочленов над некоторым полем K само является полем. Докажем его алгебраическую замкнутость без использования тяжёлой артиллерии (теоремы о примитивном элементе). Рассмотрим произвольный многочлен $f \in \overline{K}[x]$, и пусть a_i — его коэффициенты. Рассмотрим поле $E := K(a_0, \ldots, a_n)$. Это конечное расширение поля K. Итак, имеем такую башню полей: $K \subset E \subset \overline{K}$. Присоединим к полю E корень θ многочлена f. Тогда у нас есть ещё одна башня: $K \subset E \subset E(\theta)$, причём оба расширения конечны. Как мы знаем, в этом случае $E(\theta)$ — конечное расширение поля K, значит, все его элементы алгебраичны над K, в частности, корень θ. Стало быть, $\theta \in \overline{K}$ по определению. Итак, мы показали, что многочлен f имеет корень в $\overline{K}$.

4.2. Проблема квадратуры круга

Мы хотим получить ответ на вопрос, можно ли при помощи циркуля и линейки построить квадрат, по площади равный единичному кругу. Определимся для начала, какие простейшие операции мы можем совершать циркулем и линейкой. Они известны нам со школы: мы можем соединять точки и строить окружности, находить их точки пересечения, а также выбирать произвольную точку где-нибудь.

Определение. *Алгебраические точки* — это все точки плоскости, обе координаты которых — алгебраические числа. *Алгебраические прямые* — это все прямые, заданные в виде $ax + by + c = 0$, где $a, b, c \in \mathbb{A}$. *Алгебраические окружности* — это все окружности, чей центр — алгебраическая точка и радиус — алгебраическое число.

Теорема 4.11. *Каждая операция над алгебраическими элементами (точками, прямыми и окружностями) приводит к алгебраическим элементам.*

□ В самом деле,

1. Если мы проводим прямую через две алгебраические точки $A = (x_1, y_1)$ и $B = (x_2, y_2)$, то она алгебраическая, так как её уравнение имеет вид $(x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1)$.
2. Если мы строим окружность рационального радиуса и с рациональным центром, то она будет алгебраической по определению.
3. Точка пересечения двух алгебраических прямых — алгебраическая, поскольку для ее нахождения мы решаем систему из двух линейных уравнений и значит совершаем лишь операции сложения и умножения над алгебраическими числами.
4. Точки пересечения окружности и прямой — алгебраические, так как для их нахождения нужно решать квадратное уравнение.
5. Точки пересечения двух окружностей — алгебраические. Действительно, если нам дано

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = R_1^2 \\ (x - x_2)^2 + (y - y_2)^2 = R_2^2, \end{cases} \tag{17}$$

то можно вычесть из первого уравнения второе, получить систему из линейного и квадратного уравнений и свести задачу к предыдущей.

Теорема доказана. ■

Поскольку множество рациональных чисел всюду плотно, то и множество алгебраических чисел всюду плотно, значит никто нам не мешает считать, что начинать решать проблему квадратуры круга мы будем с выбора алгебраических объектов. Тогда, как показано выше, дальше мы будем получать только алгебраические объекты. Поэтому и квадрат, который мы получим, если решим проблему, будет иметь стороны алгебраической длины, то есть $\sqrt{\pi}$ — число алгебраическое, значит, по теореме 4.10, число π тоже алгебраическое. Таким образом, если мы докажем трансцендентность π, то мы докажем и неразрешимость проблемы квадратуры круга.

История решения этой проблемы такова: в 1830 г. проблему квадратуры свели к проблеме трансцендентности π, которую в свою очередь разрешили в 1880 г.

4.3. Расширения полей

4.3.1. Нормальные расширения

Определение. Пусть E и F — поля. Инъективный гомоморфизм $\sigma\colon E \to F$ называется *вложением*. Мы будем обозначать это так: $\sigma\colon E \hookrightarrow F$.

Пример 3.1. Для поля $\mathbb{C}$ существует всего два автоморфизма, сохраняющих подполе $\mathbb{R}$. Это тождественный автоморфизм и комплексное сопряжение $z \mapsto \overline{z}$. Это связано с тем, что $\mathbb{C} = \mathbb{R}(i)$, и $[\mathbb{C} : \mathbb{R}] = 2$.

Теорема 4.12. *Пусть E — конечное расширение $\mathbb{Q}$ и $[E : \mathbb{Q}] =: \nu$. Пусть $E = \mathbb{Q}(\theta)$ и $\theta_1, \ldots, \theta_\nu$ — сопряженные с θ, а*

$$\sigma_j\colon \alpha = r(\theta) \mapsto r(\theta_j), \quad j = 1, \ldots, \nu. \tag{18}$$

Тогда все отображения σ_j являются попарно различными вложениями $E \hookrightarrow \mathbb{C}$, и других нет.

□ Чтобы сократить обозначения, не будем каждый раз указывать, что многочлены от θ, представляющие элементы расширения E, имеют степень строго меньше ν и имеют рациональные коэффициенты.

1° Сначала проверим, что σ_j — гомоморфизм. Пусть $\alpha = r(\theta)$, $\beta = s(\theta)$.

Сумма: пусть $t := r + s$. Тогда $\alpha + \beta = t(\theta)$, поэтому

$$\sigma_j(\alpha + \beta) = t(\theta_j) = r(\theta_j) + s(\theta_j) = \sigma_j(\alpha) + \sigma_j(\beta). \tag{19}$$

Произведение: пусть $t := rs$. Разделим t с остатком на f_θ, получим $t = f_\theta q + u$. Тогда

$$\sigma_j(\alpha\beta) = u(\theta_j) = r(\theta_j)s(\theta_j) = \sigma_j(\alpha)\sigma_j(\beta). \tag{20}$$

Частное:

$$\gamma = \frac{\alpha}{\beta} \Rightarrow \alpha = \beta\gamma \Rightarrow \sigma_j(\alpha) = \sigma_j(\beta)\sigma_j(\gamma) \Rightarrow \sigma_j(\gamma) = \frac{\sigma_j(\alpha)}{\sigma_j(\beta)}. \tag{21}$$

2° Теперь проверим инъективность σ_j. Для этого покажем, что $\operatorname{Ker}\sigma_j = 0$. Допустим, что $\sigma_j(\alpha) = 0$, тогда $r(\theta_j) = 0$, а это невозможно, поскольку минимальный многочлен θ_j имеет степень ν, а $\deg r < \nu$.

Все σ_j различны, потому что $\sigma_j(\theta) = \theta_j \neq \theta_i = \sigma_i(\theta)$ $(i \neq j)$.

3° Теперь докажем, что других вложений нет. Пусть σ — произвольное вложение. Тогда, поскольку это инъективный гомоморфизм, то $\sigma(0) = 0$, $\sigma(1) = 1$. Далее, очевидно, что $\sigma(n) = \sigma(1 + \ldots + 1) = 1 + \ldots + 1 = n$, и $\sigma(-n) = -n$ (поскольку $\sigma(0) = \sigma(n) + \sigma(-n)$), и, наконец, $\sigma\left(\frac{a}{b}\right) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b}$, то есть σ сохраняет $\mathbb{Q}$.

Воспользуемся неподвижностью подполя $\mathbb{Q}$. Имеем

$$f_\theta(\theta) = \theta^\nu + a_{\nu-1}\theta^{\nu-1} + \ldots + a_0 = 0. \tag{22}$$

Подействуем на это равенство вложением σ, получим:

$$\big(\sigma(\theta)\big)^\nu + a_{\nu-1}\big(\sigma(\theta)\big)^{\nu-1} + \ldots + a_0 = 0. \tag{23}$$

Итак, $\sigma(\theta)$ — тоже корень многочлена f_θ, значит, он совпадает с одним из θ_j. Но это значит, что оно совпадает с одним σ_j. Действительно, пусть $\alpha = r(\theta)$, тогда $\sigma(\alpha) = r\big(\sigma(\theta)\big) = r(\theta_j)$. ■

Изучим вопрос, как устроены образы фиксированного алгебраического числа под действием вложений.

Теорема 4.13. *Пусть $E \supset \mathbb{Q}$, $\nu = [E : \mathbb{Q}]$, $\alpha \in E$, $\deg\alpha = m$. Тогда $m \,\big|\, \nu$ и $\{\sigma_1(\alpha), \ldots, \sigma_\nu(\alpha)\}$ состоит из сопряженных числа α и каждое их них повторяется ровно $\frac{\nu}{m}$ раз.*

□ Пусть $E = \mathbb{Q}(\theta)$ и $\alpha = r(\theta)$. Тогда многочлен $g(x) = \prod\limits_{j=1}^{\nu}(x - \sigma_j(\alpha)) = \prod\limits_{j=1}^{\nu}(x - r(\theta_j))$ по следствию 4.1 лежит в $\mathbb{Q}[x]$. Разделим g на f_α столько раз, сколько сможем:

$$g(x) = f_\alpha^k(x)d(x), \quad f \nmid d, \quad k \geqslant 0. \tag{24}$$

и докажем, что $d(x) \equiv \text{const}$. Предположим противное: $\deg d \geqslant 1$ и β — корень d. Тогда тем более $g(\beta) = 0$, значит, найдется j, для которого $\beta = r(\theta_j) = \sigma_j(\alpha)$. Имеем $f_\alpha(\alpha) = 0$. Подействуем на это равенство вложением σ_j, получим $f_\alpha\big(\sigma_j(\alpha)\big) = 0$, то есть $f_\alpha(\beta) = 0$. Стало быть, многочлены f_α и d имеют общий корень, а так как f_α неприводим, то $d \vdots f_\alpha$, а мы вроде договорились, что это не так. Значит, на самом деле, $d(x) \equiv \text{const}$, но поскольку старшие коэффициенты у g и f_α равны 1, то эта константа на самом деле равна 1.

Итак, $g(x) = f_\alpha^k(x)$. Слева стоит многочлен степени ν, а справа — степени km, отсюда и следует, что, во-первых, $m \mid \nu$, а во-вторых, множество корней $g(x)$ состоит из k комплектов корней многочлена f_α. ■

Следствие 4.5. *Число $\alpha \in E$ рационально $\Leftrightarrow$ оно неподвижно при всех вложениях.*

□ Ясно, что нужно доказать только в обратную сторону. Предположим, что $\deg\alpha \geqslant 2$. Тогда в силу предыдущей теоремы в наборе $\{\sigma_1(\alpha), \ldots, \sigma_\nu(\alpha)\}$ должно быть хотя бы два различных числа, а это не так по условию — противоречие. ■

Определение. Расширение $E \supset \mathbb{Q}$ называется *нормальным*, если для любого вложения $\sigma\colon E \hookrightarrow \mathbb{C}$ выполняется равенство $\sigma(E) = E$.

Пример 3.2. $E = \mathbb{Q}(\sqrt{2})$. Тут только два вложения: тождественное и «сопряжение» $(a + b\sqrt{2} \mapsto a - b\sqrt{2})$. Ясно, что для обоих $\sigma(E) = E$. Поэтому такое E — нормальное.

Пример 3.3. $E = \mathbb{Q}(\sqrt[3]{2})$. Многочлен $x^3 - 2$ имеет три корня: $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$, $\xi^2\sqrt[3]{2}$, $(\xi = e^{\frac{2\pi i}{3}})$, то $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}$ — число, вообще говоря, комплексное. Поэтому $\sigma(E) \neq E$, значит такое E — не нормальное.

Теорема 4.14 (Достаточное условие нормальности). *Пусть $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$, где $\xi_i \in \mathbb{A}$ и все сопряженные каждому ξ_i принадлежат E. Тогда E нормально.*

□ Пусть $\alpha \in E$. Тогда допустимо представление:

$$\alpha = \frac{A(\xi_1, \ldots, \xi_m)}{B(\xi_1, \ldots, \xi_m)}, \quad A, B \in \mathbb{Q}[x_1, \ldots, x_m], \quad B(\xi_1, \ldots, \xi_m) \neq 0. \tag{25}$$

Подействуем вложением σ на это равенство:

$$\sigma(\alpha) = \frac{A(\sigma(\xi_1), \ldots, \sigma(\xi_m))}{B(\sigma(\xi_1), \ldots, \sigma(\xi_m))}. \tag{26}$$

Как мы уже знаем $\sigma(\xi_i)$ сопряжено с ξ_i, поэтому $\sigma(\xi_i) \in E \Rightarrow \sigma(\alpha) \in E \Rightarrow \sigma(E) \subset E$.

Докажем теперь обратное включение. Пусть $E = \mathbb{Q}(\theta)$, $\theta_1, \ldots, \theta_\nu$ — сопряженные с θ. Как мы знаем (теорема 4.13), образ θ при отображении σ — это один из сопряжённых с числом θ корней, пусть это будет θ_k. Легко видеть, что числа $1, \theta_k, \ldots, \theta_k^{\nu-1} \in E$ образуют базис E (действительно, наличие нетривиальной линейной зависимости противоречило бы тому, что σ — вложение), и потому всякое $\beta \in E$ можно представить в виде

$$\beta = r_0 + r_1\theta_k + \ldots + r_{\nu-1}\theta_k^{\nu-1}. \tag{27}$$

Найдём к этому элементу прообраз: именно, положим

$$\alpha := r_0 + r_1\theta + \ldots + r_{\nu-1}\theta^{\nu-1} \in E. \tag{28}$$

Ясно что $\sigma(\alpha) = \beta$. А это и означает, что $E \subset \sigma(E)$. ■

Следствие 4.6. *Если E — нормальное расширение, то отображение, обратное к вложению, тоже является вложением, и композиция двух вложений — снова вложение. Иначе говоря, вложения образуют группу.*

Определение. Группа автоморфизмов нормального расширения называется *группой Галуа*.

4.3.2. Норма в конечных расширениях

Пусть E — расширение $\mathbb{Q}$ и $\nu = [E : \mathbb{Q}]$, $\sigma_1, \ldots, \sigma_\nu$ — вложения.

Определение. *Нормой* элемента α из E называется число $N(\alpha) := \prod\limits_{j=1}^{\nu} \sigma_j(\alpha)$.

Пример 3.4. Если $\alpha \in \mathbb{Q}$, то $N(\alpha) = \alpha^\nu$.

Теорема 4.15 (Свойства нормы).

1. *Пусть* $\deg\alpha = d$, $f_\alpha = x^d + \ldots + a_d$. *Тогда* $N(\alpha) = (-1)^\nu a_d^{\nu/d}$.
2. $N(\alpha) \in \mathbb{Q}$, *а если* $\alpha \in \mathbb{Z}_E$, *то* $N(\alpha) \in \mathbb{Z}$.
3. $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.
4. $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.

□ Все доказательства будут несложными:

1. Рассмотрим набор $\{\sigma_1(\alpha), \ldots, \sigma_\nu(\alpha)\}$. Пусть $\alpha_1, \ldots, \alpha_d$ — все сопряжённые с α. Применяя теорему 4.13 и обозначая $k = \frac{\nu}{d}$, получаем, что

$$N(\alpha) = (\alpha_1 \cdot \ldots \cdot \alpha_d)^k \overset{!}{=} \big((-1)^d a_d\big)^k = (-1)^\nu a_d^k. \tag{29}$$

Здесь переход, отмеченный «!», следует из формул Виета.

2. Следует из первого свойства и того факта, что $a_d \in \mathbb{Q}$. А в случае $\alpha \in \mathbb{Z}_E$ имеем $a_d \in \mathbb{Z}$.

3. $N(\alpha) = 0 \Leftrightarrow \exists\, j\colon \sigma_j(\alpha) = 0 \Leftrightarrow \alpha = 0$.

4. $N(\alpha \cdot \beta) = \prod\limits_{j=1}^{\nu} \sigma_j(\alpha \cdot \beta) = \prod\limits_{j=1}^{\nu} \sigma_j(\alpha)\sigma_j(\beta) = N(\alpha)N(\beta)$.

Теорема доказана. ■

4.4. Приближение иррациональных чисел рациональными

4.4.1. Приближение действительных чисел рациональными

Мы знаем, что $\mathbb{Q}$ плотно в $\mathbb{R}$, поэтому для любого $\alpha \in \mathbb{R}$ и для любого $\varepsilon > 0$ найдутся p и q такие, что $\left|\alpha - \frac{p}{q}\right| < \varepsilon$, то есть любое действительное число сколь угодно точно приближается рациональными. Нас интересует вопрос: а насколько маленьким можно взять q, чтобы такая оценка всё ещё выполнялась.

Теорема 4.16 (Дирихле). *Пусть $\alpha \in \mathbb{R}$ и $n \in \mathbb{N}$, тогда найдётся рациональное число $\frac{p}{q}$, для которого*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}, \quad 1 \leqslant q \leqslant n. \tag{30}$$

□ Рассмотрим полуинтервал $[0, 1)$, поделим его на n равных частей. Рассмотрим числа $x_k := \{\alpha k\}$, $k = 0, \ldots, n$. По принципу Дирихле, в одну из частей разбиения попадут хотя бы два числа x_k и x_m. Без ограничения общности, $k > m$. Тогда

$$|x_k - x_m| = \big|\{\alpha k\} - \{\alpha m\}\big| = \Big|\big(\alpha k - [\alpha k]\big) - \big(\alpha m - [\alpha m]\big)\Big| < \frac{1}{n}. \tag{31}$$

Положим $q := k - m$, а $p := [\alpha k] - [\alpha m]$. Тогда $|x_k - x_m| = |\alpha q - p| < \frac{1}{n}$, то есть $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}$. При этом, очевидно, $1 \leqslant q \leqslant n$. ■

Следствие 4.7. *Если α — иррациональное число, то существует бесконечно много p и q: $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.*

□ Во-первых, заметим, что такие p и q существуют, поскольку по предыдущей теореме найдутся p и q: $|\alpha - \frac{p}{q}| < \frac{1}{qn} \leqslant \frac{1}{q^2}$. Нужно доказать, что их бесконечно много. Предположим противное: $\frac{p_1}{q_1}, \ldots, \frac{p_N}{q_N}$ — все приближения. Тогда выберем n так, что $\frac{1}{n} < \min\limits_j \left|\alpha - \frac{p_j}{q_j}\right|$ и по этому числу n найдем такие p и q, как в предыдущей теореме. Очевидно, это приближение не содержится в нашем конечном наборе, поскольку оно «лучше» каждого из имеющихся. Противоречие. ■

Итак, мы видим, что можем приблизить число «с квадратичной точностью». Возникает резонный вопрос, а верна ли теорема для степени 3? Ответ такой: вообще говоря, нет. Например для числа $\sqrt{2}$ оценка со степенью 3 неверна. Причина этого кроется в том, что «хорошо» приближаются дробями только трансцендентные числа.

Утверждение 4.17 (Пример Лиувилля). *Для числа $\alpha = \sum\limits_{n=0}^{\infty} 2^{-n!}$ и для любого $m \geqslant 2$ найдется бесконечно много рациональных чисел $\frac{p}{q}$: $0 < |\alpha - \frac{p}{q}| < \frac{1}{q^m}$.*

□ Представим α в виде

$$\alpha = \sum_{n=0}^{N} \frac{1}{2^{n!}} + \sum_{N+1}^{\infty} \frac{1}{2^{n!}}. \tag{32}$$

Пусть $\frac{p_N}{q_N} = \sum\limits_{n=0}^{N} \frac{1}{2^{n!}}$, $q_N = 2^{N!}$. Тогда

$$0 < \alpha - \frac{p_N}{q_N} = \sum_{N+1}^{\infty} \frac{1}{2^{n!}} < \frac{1}{2^{(N+1)!}} \left(1 + \frac{1}{2} + \frac{1}{4} + \ldots\right) = \frac{2}{2^{(N+1)!}} = \frac{2}{q_N^{N+1}} \leqslant \frac{1}{q_N^m} \text{ при всех } N \geqslant m, \tag{33}$$

что и требовалось доказать. ■

Этот пример был построен Лиувиллем в 1840 г. Причина того, что данное α хорошо приближается, заключается в том, что оно трансцендентно. Собственно, пример Лиувилля создавался как демонстрация того, что существуют трансцендентные числа. Это уже потом, в 1873 г. Кантор придумал простое доказательство существования трансцендентных ($\mathbb{A}$ счётно, $\mathbb{R}$ несчётно, значит существуют трансцендентные числа).

4.4.2. Приближение алгебраических чисел рациональными

Речь в этом параграфе пойдет, разумеется, о действительных алгебраических числах, ибо понятно, что числа из $\mathbb{C} \setminus \mathbb{R}$ не приблизишь рациональными. Докажем сейчас теорему о том, что алгебраические числа «плохо» приближаются рациональными.

Теорема 4.18 (Лиувилль). *Пусть $\alpha \in \mathbb{A} \cap \mathbb{R}$, и $d := \deg \alpha \geqslant 2$. Тогда найдётся константа C, зависящая от α, что для всех $\frac{p}{q}$*

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d}. \tag{34}$$

□ Пусть D — общий знаменатель коэффициентов многочлена $f_\alpha(x)$. Пусть также $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ — числа, сопряженные с α. Ясно, что $f_\alpha(x)$ не имеет рациональных корней (так как он неприводим), поэтому

$$0 \neq \left|f_\alpha\left(\frac{p}{q}\right)\right| = \frac{A}{Dq^d} \geqslant \frac{1}{Dq^d}. \tag{35}$$

В последнем неравенстве мы воспользовались тем, что A — целое неотрицательное и не равно нулю. Рассмотрим теперь два случая:

1° Пусть $\left|\alpha - \frac{p}{q}\right| \leqslant 1$. Тогда $\left|\alpha_j - \frac{p}{q}\right| \leqslant \left|\alpha_j - \alpha\right| + \left|\alpha - \frac{p}{q}\right| \leqslant \left|\alpha_j - \alpha\right| + 1$. Отделив от произведения первый множитель, получаем

$$\left|f_\alpha\left(\frac{p}{q}\right)\right| = \prod_{j=1}^{d}\left|\alpha_j - \frac{p}{q}\right| \leqslant \left|\alpha - \frac{p}{q}\right| \cdot \prod_{j=2}^{d}(1 + |\alpha_j - \alpha|). \tag{36}$$

Отсюда, с использованием оценки (35) получаем

$$\frac{1}{Dq^d} \leqslant \left|\alpha - \frac{p}{q}\right| \cdot \prod_{j=2}^{d}(1 + |\alpha_j - \alpha|), \tag{37}$$

а затем полагаем $C := \left(D \cdot \prod\limits_{j=2}^{d}(1 + |\alpha_j - \alpha|)\right)^{-1} < 1$.

2° Если же $\left|\alpha - \frac{p}{q}\right| > 1$, то можно взять ту же константу C. ■

Следствие 4.8. *Если $\alpha \in \mathbb{R}$ и для любого $m \geqslant 2$ неравенство $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$ имеет бесконечно много решений, то α трансцендентно.*

□ **1°** Докажем, что $\alpha \notin \mathbb{Q}$. Предположим, что это не так, и $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 0$. Возьмём $m = 2$. По условию существует бесконечно много решений неравенства $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. С другой стороны,

$$0 \neq \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{A}{bq} \geqslant \frac{1}{bq} \tag{38}$$

Сопоставляя два неравенства, получаем, что $\frac{1}{q^2} > \frac{1}{bq} \Rightarrow q < b$. Поэтому q мы можем выбрать лишь конечным числом способов, значит, решений вида $\frac{p}{q}$ конечное число. Противоречие.

2° Докажем, что $\alpha \notin \mathbb{A}$. Предположим противное, и пусть $\deg \alpha = d \geqslant 2$. Пусть $m = d + 1$, тогда по условию теоремы существует бесконечно много решений неравенства $0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$. А с другой стороны по предыдущей теореме: $\left|\alpha - \frac{p}{q}\right| \geqslant \frac{C}{q^d}$. Сопоставляя эти неравенства, получаем: $\frac{C}{q^d} < \frac{1}{q^{d+1}} \Rightarrow q < \frac{1}{C}$. Поэтому у нас в распоряжении лишь конечный набор q, а значит и чисел $\frac{p}{q}$ конечное множество — противоречие. ■

4.5. Теорема Линдемана – Вейерштрасса и её следствия

4.5.1. Трансцендентность e

Докажем вначале иррациональность числа e. Впервые это сделал Эйлер в середине XVIII века (он разложил число e в непрерывную дробь).

Теорема 4.19 (Фурье, 1815 г.). *Число e иррационально.*

□ Представим число e в виде ряда и умножим его на $n!$. Получим

$$n!e = n!\sum_{k=0}^{\infty}\frac{1}{k!} = \sum_{k=0}^{n}\frac{n!}{k!} + \sum_{k=n+1}^{\infty}\frac{n!}{k!} = p_n + r_n. \tag{39}$$

Поэтому

$$0 < n!e - p_n = r_n = \frac{1}{n+1}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \dots\right) < \frac{1}{n+1}\left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) = \frac{2}{n+1}. \tag{40}$$

Предположим, что $e = \frac{a}{b}$. Положим $n = b$. Тогда слева стоит целое число (факториал убьёт знаменатель), а справа — ненулевое число, меньшее 1. ■

Лемма 4.20 (Тождество Эрмита). *Пусть $f(x) \in \mathbb{C}[x]$. Пусть $F(x) := f(x) + f'(x) + f''(x) + \dots$ Тогда*

$$e^k F(0) - F(k) = e^k \int\limits_0^k e^{-x} f(x) dx. \tag{41}$$

□ Легко проверить, что

$$\int f(x)e^{-x}dx = -F(x)e^{-x} + c. \tag{42}$$

Поэтому

$$\int\limits_0^k e^{-x} f(x) dx = -F(k)e^{-k} + F(0). \tag{43}$$

Умножим левую и правую часть на e^k, получим

$$e^k F(0) - F(k) = e^k \int\limits_0^k e^{-x} f(x)\, dx, \tag{44}$$

что и требовалось доказать. ■

Лемма 4.21. *Пусть $f \in \mathbb{Z}[x]$. Тогда $\frac{1}{p!}f^{(p)}(x) \in \mathbb{Z}[x]$ при всех $p \in \mathbb{N}$.*

□ Имеем

$$(x^r)^{(p)} = \begin{cases} 0, & p > r, \\ r(r-1)\cdot\ldots\cdot\big(r-(p-1)\big)x^{r-p} = p!\cdot \mathbf{C}_r^p x^{r-p}, & p \leqslant r. \end{cases} \tag{45}$$

В любом случае производная каждого монома делится на $p!$. Значит, $\frac{1}{p!}f^{(p)}(x) \in \mathbb{Z}[x]$. ■

Теорема 4.22 (Эрмит, 1873 г.). *Число e трансцендентно.*

□ Предположим, что $e \in \mathbb{A}$. Тогда найдется многочлен $f_e(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$, $a_i \in \mathbb{Z}$ такой, что $f_e(e) = 0$. Умножим теперь (41) на a_k и просуммируем по всем $k = 0, \dots, m$, получим:

$$F(0)\underbrace{\sum_{k=0}^{m} a_k e^k}_{0} - \sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int\limits_0^k f(x)e^{-x}dx. \tag{46}$$

Пусть

$$\theta_k(x) := \begin{cases} 1, & x \leqslant k, \\ 0, & x > k, \end{cases} \qquad \Phi(x) := \sum_{k=0}^{m} a_k e^k \theta_k(x), \tag{47}$$

тогда правая часть уравнения (46) равна

$$J := \int\limits_0^m f(x)\Phi(x)e^{-x}\, dx. \tag{48}$$

Теперь подберём функцию $f(x)$ так, чтобы $J \in (0,1)$, а числа $F(k)$ были целыми.

Будем искать $f(x)$ в виде

$$f(x) := \frac{1}{n!}x^{n+r_0}(x-1)^{n+r_1}\cdot\ldots\cdot(x-m)^{n+r_m}, \qquad r_i \in \{0,1\}. \tag{49}$$

Поскольку $\Phi(x)$ — ступенчатая функция с разрывами в точках $1, \dots, m$, а $f(x)$ обращается в нуль в этих же точках, функция $f(x)\Phi(x)$ будет непрерывной с нулями в точках $1, \dots, m$. Числа r_i мы выберем так, чтобы

в этих точках не было перемены знака у функции $f(x)\Phi(x)$, и она была бы неотрицательной на $[0,m]$. Тогда $J>0$. Теперь выберем такое большое n, чтобы интеграл J был меньше 1. Оценим числитель $f(x)$: имеем $|x-k|\leqslant m$, значит, числитель $f(x)$ не превосходит $m^{(m+1)(n+1)}$, а в знаменателе стоит $n!$, который задавит любую показательную функцию. Кроме того, $|\Phi|\leqslant C$. Значит, $J\in(0,1)$ при достаточно большом n.

Докажем, что $F(k)\in\mathbb{Z}$. Действительно, $f(x)=\frac{g(x)}{n!}$, где $g(x)\in\mathbb{Z}[x]$. По предыдущей лемме $\frac{1}{p!}g^{(p)}(x)\in\mathbb{Z}[x]$. Следовательно,

$$F(k)=\sum_{p\geqslant 0}f^{(p)}(k)=\sum_{p\geqslant n}f^{(p)}(k)=\sum_{p\geqslant n}\underbrace{\frac{1}{p!}g^{(p)}(k)}_{\in\mathbb{Z}}\cdot\underbrace{\frac{p!}{n!}}_{\in\mathbb{Z}}\in\mathbb{Z}. \tag{50}$$

Возвращаемся к уравнению (46) и видим, что в правой его части стоит $J\in(0,1)$, а в левой — сумма целых чисел. Противоречие. ■

4.5.2. Иррациональность π

Теорема 4.23 (Эрмит). *Число π иррационально.*

□ Пусть $f(x)\in\mathbb{C}[x]$ и $F(x):=f(x)-f^{(2)}(x)+f^{(4)}(x)-\ldots$, тогда легко проверить, что

$$\int f(x)\sin x\,dx=F'(x)\sin x-F(x)\cos x+C. \tag{51}$$

Поэтому

$$J:=\int_0^\pi f(x)\sin x\,dx=F(\pi)+F(0). \tag{52}$$

Предположим, что $\pi=\frac{a}{b}$. Тогда положим

$$f(x)=\frac{b^nx^n(\pi-x)^n}{n!}=\frac{x^n(a-bx)^n}{n!}. \tag{53}$$

Так как $f(x)\geqslant 0$ и $\sin x\geqslant 0$ на отрезке $[0,\pi]$, то $J>0$. Кроме того,

$$J<\pi\frac{b^n\pi^{2n}}{n!}=\frac{b^n\pi^{2n+1}}{n!}\to 0,\quad n\to\infty. \tag{54}$$

Поэтому можно выбрать n таким большим, чтобы $J\in(0,1)$. Далее, $f(\pi-x)=f(x)$, поэтому $f^{(2p)}(\pi-x)=$ $=f^{(2p)}(x)$, в частности, $f^{(2p)}(\pi)=f^{(2p)}(0)$. Значит, $F(\pi)=F(0)$. Осталось показать, что $F(0)\in\mathbb{Z}$. В самом деле,

$$F(0)=\sum_{p\geqslant 0}(-1)^pf^{(2p)}(0)=\sum_{2p\geqslant n}(-1)^pf^{(2p)}(0). \tag{55}$$

Аналогично предыдущей теореме показывается, что это выражение целое. Снова получаем противоречие, связанное с тем, что в интервале $(0,1)$ нет целых чисел. ■

4.5.3. Доказательство теоремы Линдемана – Вейерштрасса

Ключевым в доказательстве этой теоремы будет некоторое утверждение, на первый взгляд кажущееся диким.

Предложение 4.24. *Пусть $A(t):=a_0e^{\alpha_0t}+\ldots+a_me^{\alpha_mt}$, и $a_j,\alpha_j\in\mathbb{A}$. Если $A(t)\not\equiv 0$ и ряд Тейлора функции $A(t)$ в точке 0 имеет рациональные коэффициенты, то $A(1)\neq 0$.*

Пример 5.1. Чтобы осознать, что это действительно так, рассмотрим такой пример:

$$e^{\sqrt{2}t}+e^{-\sqrt{2}t}=\sum_{k=0}^{\infty}\frac{\sqrt{2}^k+(-\sqrt{2})^k}{k!}t^k=\sum_{k=0}^{\infty}\frac{2^{k+1}}{k!}t^{2k}. \tag{56}$$

Это вселяет некоторую надежду. Прежде, чем начать доказывать это предложение, сделаем несколько простых замечаний, которые упростят жизнь.

1° Можно считать, что все α_j различны.

2° Можно считать, что все a_j — целые алгебраические (то есть $a_j\in\mathbb{Z}_E$). Это действительно так, поскольку по свойству целых алгебраических всегда можно найти такое $d\in\mathbb{N}$, что $da_j\in\mathbb{Z}_E$.

3° Можно считать, что все $a_j\neq 0$.

□ Будет доказывать от противного. Предположим, что $A(1)=0$. Тогда будет верна

Лемма 4.25. *Пусть* $A(1) = 0$, $n \in \mathbb{N}$, *и*

$$f(x) := (x-\alpha_0)^n(x-\alpha_1)^{n+1}\cdot\ldots\cdot(x-\alpha_m)^{n+1}, \quad g(x) := \frac{1}{n!}\sum_{l\geqslant n} f^{(l)}(x). \tag{57}$$

Тогда

$$|a_0 g(\alpha_0) + \ldots + a_m g(\alpha_m)| \leqslant \frac{C^{n+1}}{n!}, \quad C = C(a_j, \alpha_j) > 0. \tag{58}$$

□ Пусть $F(x) = \sum\limits_{l\geqslant 0} f^{(l)}(x)$. Легко проверить, что

$$e^a \int\limits_0^a f(z)e^{-z}dz = e^a F(0) - F(a). \tag{59}$$

Подставим вместо a число α_j, умножим на a_j и просуммируем по всем j от 0 до m:

$$-\sum_{j=0}^{m} a_j F(\alpha_j) = \sum_{j=0}^{m} a_j e^{\alpha_j} \int\limits_0^{\alpha_j} f(z)e^{-z}\,dz. \tag{60}$$

$$F(\alpha_j) = \sum_{l\geqslant 0} f^{(l)}(\alpha_j) = \sum_{l\geqslant n} f^{(l)}(\alpha_j) = n! g(\alpha_j) \tag{61}$$

Поэтому (60) можно переписать так:

$$\sum_{j=0}^{m} a_j g(\alpha_j) = -\frac{1}{n!}\sum_{j=0}^{m} a_j e^{\alpha_j} \int\limits_0^{\alpha_j} f(z)e^{-z}\,dz. \tag{62}$$

Пусть $r = \max\limits_j |\alpha_j|$. Тогда если $|z-\alpha_j| \leqslant 2r$, то $|f(z)| \leqslant (2r)^{n+m(n+1)}$ и $|e^{-z}| \leqslant e^r$. Из этих простеньких оценок следует, что модуль правой части (62) меньше $\frac{C^{n+1}}{n!}$ для некоторого C — что и требовалось доказать. ■

Пусть $D \in \mathbb{N}$ — такое число, что все числа $D\alpha_j$ уже являются целыми алгебраическими. Рассмотрим число

$$I := D^{m(n+1)}\big(a_0 g(\alpha_0) + \ldots + a_m g(\alpha_m)\big). \tag{63}$$

Следующая лемма утверждает, что

Лемма 4.26. *Число I является целым алгебраическим.*

□ Фактически достаточно доказать, что при всех $l \geqslant n$ выполнено

$$D^{m(n+1)}\frac{1}{l!}f^{(l)}(\alpha_j) \in \mathbb{Z}_E. \tag{64}$$

Действительно, тогда нетрудно убедиться, что

$$D^{m(n+1)}g(\alpha_j) = \sum \frac{l!}{n!}\frac{D^{m(n+1)}}{l!}f^{(l)}(\alpha_j) \in \mathbb{Z}_E, \tag{65}$$

откуда и следует утверждение теоремы. Итак, докажем (64).

$$D^{m(n+1)}f(x) = \frac{1}{D^n}(Dx - D\alpha_0)^n(Dx - D\alpha_1)^{n+1}\cdot\ldots\cdot(Dx - D\alpha_m)^{n+1} = D^{-n}h(Dx), \tag{66}$$

где

$$h(t) = (t - D\alpha_0)^n(t - D\alpha_1)^{n+1}\cdot\ldots\cdot(t - D\alpha_m)^{n+1} \in \mathbb{Z}_E[t]. \tag{67}$$

Поэтому, применяя лемму 4.21, получаем

$$D^{m(n+1)}\frac{1}{l!}f^{(l)}(\alpha_j) = D^{-n+l}\frac{1}{l!}h^{(l)}(D\alpha_j) \in \mathbb{Z}_E. \tag{68}$$

Лемма доказана. ■

Лемма 4.27. *Найдется n такое, что $I \neq 0$ и $|N(I)| \geqslant 1$.*

□ Посчитаем $I \pmod{(n+1)}$:

$$\frac{D^{m(n+1)}}{n!}\sum_{l\geqslant n+1} f^{(l)}(\alpha_j) = \sum_{l\geqslant n+1}\frac{l!}{n!}\frac{D^{m(n+1)}}{l!}f^{(l)}(\alpha_j) = (n+1)\gamma_j, \quad \gamma_j \in \mathbb{Z}_E. \tag{69}$$

Поэтому

$$I \equiv D^{m(n+1)}a_0 g(\alpha_0) \equiv D^{m(n+1)}a_0\frac{1}{n!}f^{(n)}(\alpha_0) =$$

$$= D^{m(n+1)}a_0(\alpha_0-\alpha_1)^{n+1}\cdot\ldots\cdot(\alpha_0-\alpha_m)^{n+1} = a_0\prod_{j=1}^{m}(D\alpha_0 - D\alpha_j)^{n+1}. \tag{70}$$

Пусть

$$S := \Big|N(a_0)\cdot\prod_{j=1}^{m}N(D\alpha_0 - D\alpha_j)^{n+1}\Big|. \tag{71}$$

Ясно, что $S \in \mathbb{Z}$. Подберем n так, чтобы $(n+1, S) = 1$. Докажем, что тогда $I \not\equiv 0 \pmod{(n+1)}$. Предположим противное, то есть что $I \vdots (n+1)$. Тогда свойство делимости верно и для их норм, то есть

$$S^{n+1} \vdots \big(N(n+1)\big) = (n+1)^{\nu}. \tag{72}$$

Но это невозможно в силу выбора n. Значит, $I \not\equiv 0 \pmod{(n+1)}$ и тем более $I \neq 0$. Поэтому $|N(I)| \geqslant 1$ (ибо $I \in \mathbb{Z}_E$). ■

Вернёмся к доказательству предложения. Пусть $n = Sr$, значит, $n+1 = Sr+1$. Тогда $(n+1, S) = 1$. Пусть σ — вложение E в $\mathbb{C}$. Если предположить, что наше предложение неверно, то $\sigma(a_0)e^{\sigma(\alpha_0)} + \ldots + \sigma(a_m)e^{\sigma(\alpha_m)} = 0$. Тогда мы попадаем в условия леммы 4.25, где в роли $f(x)$ и $g(x)$ выступают $\sigma(f)(x)$ и $\sigma(g)(x)$ соответственно. Поэтому

$$\big|\sigma(a_0)\sigma(g)\big(\sigma(\alpha_0)\big) + \ldots + \sigma(a_m)\sigma(g)\big(\sigma(\alpha_m)\big)\big| \leqslant \frac{C_\sigma^{n+1}}{n!} \Rightarrow |\sigma(I)| \leqslant \frac{\lambda_\sigma^{n+1}}{n!} \tag{73}$$

для всех σ. Поэтому

$$1 \leqslant |N(I)| = \prod_{j=1}^{\nu}|\sigma_j(I)| \leqslant \Big(\prod_{j=1}^{\nu}\lambda_{\sigma_j}\Big)^{n+1}\cdot\frac{1}{(n!)^{\nu}} < 1, \tag{74}$$

получаем противоречие. ■

Теорема 4.28 (Линдеман – Вейерштрасс). *Пусть $\alpha_0, \ldots, \alpha_n$ — различные алгебраические числа, тогда числа $e^{\alpha_0}, \ldots, e^{\alpha_m}$ линейно независимы над полем $\mathbb{A}$.*

□ Предположим противное: существуют $a_0, \ldots, a_m \in \mathbb{A}$, для которых $\sum\limits_{i=0}^{m} a_i e^{\alpha_i} = 0$. Пусть

$$A(t) := a_0 e^{\alpha_0 t} + \ldots + a_m e^{\alpha_m t}. \tag{75}$$

Тогда $A(1) = 0$ по предположению, а $A(t) \not\equiv 0$, ибо α_j различны (в курсе дифференциальных уравнений показывалось, что экспоненты с различными показателями линейно независимы). Разложим $A(t)$ в ряд Тейлора:

$$A(t) = \sum_{k=0}^{\infty}(a_0\alpha_0^k + \ldots + a_m\alpha_m^k)\frac{t^k}{k!}. \tag{76}$$

Казалось бы, что тут-то и нужно применить предложение 4.24, но коэффициенты в ряде Тейлора функции $A(t)$, вообще говоря, не являются рациональными. Поэтому попытаемся из $A(t)$ изготовить функцию с рациональными коэффициентами.

Введем обозначения: пусть E — конечное расширение поля $\mathbb{Q}$, полученное присоединением всех коэффициентов a_i и всех сопряжённых к ним, а также всех чисел α_j и всех сопряжённых к ним. Пусть $\nu = [E : \mathbb{Q}]$. Тогда существует ν штук автоморфизмов поля E, обозначим их $\sigma_1, \ldots, \sigma_\nu$.

Рассмотрим формальный ряд: $f(t) = \sum \gamma_k t^k$, $\gamma_k \in E$. Обозначим через $\sigma(f)(t)$ следующий ряд: $\sum \sigma(\gamma_k)t^k$. Заметим, что операция $\sigma(f)$ обладает следующими очевидными свойствами

1. $\sigma(f \pm g) = \sigma(f) \pm \sigma(g)$;
2. $\sigma(fg) = \sigma(f)\sigma(g)$;
3. $\sigma(f') = \sigma(f)'$.

Поскольку $A(t) \not\equiv 0$, то в ряде Тейлора для $A(t)$ есть ненулевые коэффициенты и поэтому автоморфизм σ от них тоже будет не нулём, значит

$$\sigma(A)(t) = \sum_{k=0}^{\infty} \left(\sigma(a_0)\sigma(\alpha_0)^k + \ldots + \sigma(a_m)\sigma(\alpha_m)^k\right) \frac{t^k}{k!} = \sigma(a_0)e^{\sigma(\alpha_0)t} + \ldots + \sigma(a_m)e^{\sigma(\alpha_m)t} \not\equiv 0. \tag{77}$$

Рассмотрим функцию $B(t)$, определенную следующим образом:

$$B(t) = \prod_{j=1}^{\nu} \sigma_j(A)(t) = b_0 e^{\beta_0 t} + \ldots + b_M e^{\beta_M t}, \quad b_i, \beta_i \in E. \tag{78}$$

В силу (77), $B(t) \not\equiv 0$. Пусть σ — произвольный автоморфизм E. Но множество всех автоморфизмов образует группу и поэтому

$$\sigma(B)(t) = \prod_{j=1}^{\nu} \sigma\sigma_j(A)(t) = \prod_{j=1}^{\nu} \sigma_j(A)(t) = B(t). \tag{79}$$

Это означает, что коэффициенты Тейлора функции $B(t)$ не меняются под действием любого автоморфизма, что возможно лишь в том случае, когда они все рациональны. Итак, как и обещалось, мы построили функцию такого же вида, как и в предложении 4.24, у неё рациональные коэффициенты, и она в единице равна нулю (поскольку один из σ_j — тождественный) — противоречие с утверждением предложения. ■

4.5.4. Следствия из теоремы Линдемана – Вейерштрасса

Следствие 4.9. *Если $\alpha \neq 0$ и $\alpha \in \mathbb{A}$, то e^α трансцендентно.*

□ Допустим, что $\beta := e^\alpha$ — алгебраическое число. Тогда $1 \cdot e^\alpha - \beta \cdot 1 = 0$. Мы получили линейную комбинацию (с коэффициентами из $\mathbb{A}$) экспонент с показателями α и 0, равную нулю. Это противоречит теореме Линдемана – Вейерштрасса. Значит, e^α трансцендентно. ■

Пример 5.2. Число $e^{\sqrt{2}}$ трансцендентно.

Следствие 4.10. *Число π трансцендентно.*

□ Пусть $\pi \in \mathbb{A}$, тогда и $\pi i \in \mathbb{A}$. Но тогда и $e^{\pi i} = -1$ трансцендентно, что неверно. ■

Следствие 4.11. *Пусть $\beta \in \mathbb{A}$, $\beta \neq 0, 1$. Тогда $\ln \beta$ трансцендентно при любом выборе ветви логарифма.*

□ Если $\alpha = \ln \beta$ — алгебраическое, то $e^\alpha = \beta$ — трансцендентное. Противоречие. ■

Следствие 4.12. *Если $\alpha \in \mathbb{A}$, $\alpha \neq 0$, то $\sin \alpha$, $\cos \alpha$, $\operatorname{tg} \alpha$ — трансцендентные.*

□ Предположим $\beta = \sin \alpha \in \mathbb{A}$. Тогда $2ie^{i\alpha}\beta = e^{2i\alpha} - 1$. Значит, $e^{i\alpha}$ — корень многочлена с алгебраическими коэффициентами, значит $e^{i\alpha} \in \mathbb{A}$ — противоречие. ■

Следствие 4.13 (Вейерштрасс). *Если $\beta_1, \ldots, \beta_r$ — алгебраические и линейно независимые над $\mathbb{Q}$, то числа $e^{\beta_1}, \ldots, e^{\beta_r}$ **алгебраически** независимы над $\mathbb{A}$, то есть не существует такого ненулевого многочлена $P \in \mathbb{A}[x_1, \ldots, x_r]$, что $P(e^{\beta_1}, \ldots, e^{\beta_r}) = 0$.*

□ Пусть $P(x_1, \ldots, x_r) = \sum\limits_{\overline{k}} a_{\overline{k}} x_1^{k_1} \cdot \ldots \cdot x_r^{k_r}$. Предположим, что $P(e^{\beta_1}, \ldots, e^{\beta_r}) = 0$, то есть

$$\sum_{\overline{k}} a_{\overline{k}} e^{(k_1\beta_1 + \ldots + k_r\beta_r)} = 0. \tag{80}$$

Поскольку β_i линейно независимы над $\mathbb{Q}$, числа $\sum k_i\beta_i$ различны. По теореме Линдемана – Вейерштрасса, числа $e^{(k_1\beta_1 + \ldots + k_r\beta_r)}$ линейно независимы над $\mathbb{A}$, что противоречит написанному линейному соотношению. ■