Версия 10

ДЗЕТА-ФУНКЦИЯ
ЧАСТЬ 1
АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ ЧИСЕЛ

Роман М. Федоров

Перед вами записки лекций, прочитанных автором в Дубне летом 2011 года на школе "Современная Математика". На самом деле, первые две лекции вполне соответствуют тому, что было прочитано, а последние две, скорее, являются расширенным вариантом третьей лекции. Из четвертой лекции я планирую сделать вторую часть.

Врядли можно понять этот текст, не решая задачи. К части задач я привел указания в конце текста; более сложные задачи отмечены звездочкой. Некоторые теоремы мне не хотелось доказывать — потому, что доказательство слишком скучно, или слишком выходит за рамки этого текста. Такие теоремы названы "фактами" и приведены без доказательств. Читателю следует поверить в них (или прочитать доказательство в каком-нибудь стандартном курсе теории чисел).

Часть этих лекций написана мелким шрифтом, я рекомендую читателю пропустить ее при первом чтении.

Текст находится в состоянии постоянного изменения и улучшения. Когда-нибудь он станет частью книжки и перестанет меняться, а пока что пожелания по улучшению его математического содержания всячески приветствуются.

Введение

Читателю наверняка известна формула для суммы бесконечной геометрической прогрессии:

$$1 + x + x^2 + x^3 + \ldots + x^n + \ldots = \frac{1}{1-x}, \qquad \text{где } |x| < 1. \tag{1}$$

Что будет если перепутать основание и показатель степени: вместо x^2 мы напишем 2^x, вместо x^3 — 3^x и т.д; вместо $x = x^1$ мы напишем $1^x = 1$, а член $1 = x^0$ придется просто отбросить. Получится функция

$$1 + 2^x + 3^x + \ldots + n^x + \ldots = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots + \frac{1}{n^s} + \ldots,$$

где мы сделали замену $s = -x$. Эта функция называется *дзета-функцией Римана* и обозначается $\zeta(s)$. Оказывается, она гораздо интереснее суммы бесконечной геометрической прогрессии: простой формулы для нее не существует, вычислить ее значение даже в одной точке совсем не просто, да и вообще она ответственна за большинство связей между анализом и теорией чисел. Но наиболее важно то, что обобщения дзета-функции Римана пронизывают практически все области математики. Итак, приступим.

Лекция 1. Дзета-функция Римана

Определение 1. Пусть s — действительное число. Тогда

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{2}$$

Теорема 1. *Ряд* (2) *сходится при* $s > 1$ *и расходится при* $s \le 1$.

Доказательство. Начнем со случая $s = 1$. Рассмотрим частичную сумму ряда:

$$\begin{aligned}(3)\quad & 1 + \tfrac{1}{2} + \tfrac{1}{3} + \ldots + \tfrac{1}{2^n} = \\ & = 1 + \tfrac{1}{2} + \left(\tfrac{1}{3} + \tfrac{1}{4}\right) + \left(\tfrac{1}{5} + \ldots + \tfrac{1}{8}\right) + \ldots + \left(\tfrac{1}{2^{n-1}+1} + \ldots + \tfrac{1}{2^n}\right) > \\ & > 1 + \tfrac{1}{2} + \left(\tfrac{1}{4} + \tfrac{1}{4}\right) + \left(\tfrac{1}{8} + \ldots + \tfrac{1}{8}\right) + \ldots + \left(\tfrac{1}{2^n} + \ldots + \tfrac{1}{2^n}\right) = \\ & = 1 + \tfrac{1}{2} + \tfrac{1}{2} + \ldots + \tfrac{1}{2} = 1 + \tfrac{n}{2}.\end{aligned}$$

Мы разбили частичную сумму на группы и заметили, что каждая из групп больше, чем $\frac{1}{2}$. Итак, частичные суммы не ограничены, поэтому ряд расходится. При $s < 1$ частичные сумма ряда больше, чем соответствующие частичные суммы при $s = 1$, так что они тоже не ограничены и ряд расходится. Осталось рассмотреть случай $s > 1$. В этом случае мы проведем аналогичную оценку:

$$\begin{aligned}(4)\quad & 1 + \frac{1}{2^s} + \ldots + \frac{1}{(2^{n+1}-1)^s} = 1 + \left(\frac{1}{2^s} + \frac{1}{3^s}\right) + \left(\frac{1}{4^s} + \ldots + \frac{1}{7^s}\right) \\ & + \ldots + \left(\frac{1}{2^{ns}} + \ldots + \frac{1}{(2^{n+1}-1)^s}\right) < 1 + \frac{2}{2^s} + \frac{4}{4^s} + \ldots + \frac{2^n}{2^{ns}} = \\ & 1 + 2^{1-s} + (2^{1-s})^2 + \ldots + (2^{1-s})^n = \frac{1 - 2^{(1-s)(n+1)}}{1 - 2^{1-s}} < \frac{1}{1 - 2^{1-s}}.\end{aligned}$$

Мы воспользовались формулой (1) для суммы геометрической прогрессии и тем, что $0 < 2^{1-s} < 1$. Мы видим, что частичные суммы ограничены. Поскольку члены нашего ряда положительны, из ограниченности частичных сумм следует, что ряд сходится. □

Таким образом формула (2) определяет дзета-функцию при $s > 1$. При s стремящемся к единице, $\zeta(s)$ стремится к бесконечности. Насколько быстро? Ответ дается следующим предложением.

Предложение 1.

$$\lim_{s \to 1} (s-1)\zeta(s) = 1.$$

Доказательство. □

Предел в левой части называется *вычетом дзета-функции в единице.* На самом деле, можно определить дзета-функцию при $s < 1$, и даже при всех комплексных $s \ne 1$ (см. §1.5).

Вот общий факт, на котором было основано доказательство теоремы 1:

Задача 1. Пусть a_n — невозрастающая последовательность. Докажите, что ряд $\sum a_n$ сходится тогда и только тогда, когда ряд $\sum 2^n a_{2^n}$ сходится.

Насколько быстро растут частичные суммы ряда (2), определяющего дзета-функцию?

Задача 2. Пусть $a_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ — частичная сумма ряда (2) при $s = 1$. Докажите, что

$$\ln(n+1) < a_n \leq 1 + \ln n.$$

Найдите аналогичные оценки для частичных сумм ряда (2) при других значениях s.

1.1. **Значения дзета-функции.** Вычислить значение дзета-функции хотя бы в одной точке — совсем не тривиальная задача. Вот что известно в этом направлении:

-

(5) $$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2} + \ldots = \frac{\pi^2}{6}.$$

  Задача вычисления $\zeta(2)$ известна как *проблема Базеля.* Она была решена Эйлером в 1735-м году. Впрочем, его доказательство было нестрогим. Мы приведем как доказательство Эйлера, так и строгое доказательство в §1.3.
- $\zeta(4) = \pi^4/90$.
- Вообще

(6) $$\zeta(2n) = (-1)^{n+1} \frac{B_{2n}(2\pi)^{2n}}{2(2n)!},$$

  где B_{2n} — *число Бернулли* с номером $2n$. Числа Бернулли определяются следующей формулой:

$$\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}.$$

  Их можно также определить по индукции формулами

$$B_0 = 1, \quad B_n = -\sum_{k=0}^{n-1} \binom{n}{k} \frac{B_k}{n-k+1}.$$

  Мы приведем набросок доказательства формулы (6) в §1.3.
- Точные формулы для значений ζ в нечетных натуральных числах неизвестны, и, скорее всего, их не существует. Однако Апери доказал в 1978 году, что $\zeta(3)$ иррационально.

- В 2001 году Вадим Зудилин доказал, что среди чисел $\zeta(2n+1)$ бесконечно много иррациональных.
- Он также доказал, что хотя бы одно из чисел $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ иррационально.

1.2. **Произведение Эйлера.** Исключительная важность дзета-функции Римана для теории чисел во многом связана с ее разложением в бесконечное произведение (7), к которому мы переходим. Заметим, что существенная часть этой брошюры посвящена обобщениям и применениям таких разложений, поэтому читателю следует обязательно изучить материал этого параграфа (впрочем, вопросы сходимости читатель может опустить, так как они не будут играть важной роли в дальнейшем).

Начнем с определений. Пусть a_n — бесконечная числовая последовательность. По аналогии с суммой ряда, можно определить бесконечное произведение. Для этого рассмотрим последовательность $b_n = a_1a_2\ldots a_n$. *Бесконечным произведением*

$$\prod_{n=1}^{\infty} a_n$$

называется предел $\lim_{n\to\infty} b_n$. Говорят, что произведение *сходится*, если этот предел конечен и *отличен от нуля.*

Задача 3. Вычислите

$$\prod_{n=2}^{\infty}\left(1-\frac{1}{n}\right) \qquad \text{и} \qquad \prod_{n=2}^{\infty}\left(1-\frac{1}{n^2}\right).$$

Связь дзета-функции с теорией чисел основана на следующей формуле:

Теорема 2 (Произведение Эйлера)**.**

$$\zeta(s) = \prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}, \tag{7}$$

где произведение берется по всем простым числам. Более того, левая часть сходится тогда и только тогда, когда сходится правая часть.

В соответствии с вышесказанным, точный смысл правой части таков: положим

$$b_n = \prod_{p<n}\left(1-\frac{1}{p^s}\right)^{-1},$$

где произведение берется по всем простым числам, меньшим n. Тогда бесконечное произведение по определению равно $\lim_{n\to\infty} b_n$.

Доказательство теоремы 2. Проведем сначала формальное вычисление, а потом займемся вопросами сходимости. Пусть p — простое число. Рассмотрим соответствующий множитель в произведении Эйлера:

$$\left(1-\frac{1}{p^s}\right)^{-1}=1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\ldots+\frac{1}{p^{ms}}+\ldots$$

Это равенство тоже следует из формулы (1) для суммы бесконечной геометрической прогрессии. Значит, правую часть (7) можно записать так:

$$\left(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\ldots\right)\left(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\ldots\right)\ldots\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\ldots\right)\ldots$$

Мы утверждаем, что если раскрыть скобки в этом произведении, то получится в точности ряд (2) для дзета-функции. Приведем сначала несколько примеров: если взять член $\frac{1}{2^s}$ в первом множителе и единицу во всех остальных, то получится $\frac{1}{2^s}$. Если взять вторые члены в двух первых множителях и единицы в остальных, то получится $\frac{1}{6^s}$. Если взять член $\frac{1}{2^{2s}}$ в первом множителе, $\frac{1}{3^s}$ во втором и единицы в остальных, то получится $\frac{1}{12^s}$.

Теперь уже ясно, как получить $\frac{1}{n^s}$: нужно разложить n на простые множители: $n=p_1^{m_1}p_2^{m_2}\ldots p_k^{m_k}$ и взять член $\frac{1}{p_1^{m_1 s}}$ в множителе, соответствующем p_1, член $\frac{1}{p_2^{m_2 s}}$ в множителе, соответствующем p_2,..., член $\frac{1}{p_k^{m_k s}}$ в множителе соответствующем p_k и единицы во всех остальных множителях. В силу теоремы об однозначности разложения на простые множители для натуральных чисел, каждое число вида $\frac{1}{n^s}$ встретится ровно один раз.

Приведем теперь более строгое доказательство. Обозначим

$$a_n=\sum_{j=1}^{n}\frac{1}{j^s},\qquad b_n=\prod_{p\le n}\left(1-\frac{1}{p^s}\right)^{-1}.$$

Из предыдущего рассуждения ясно, что $a_n<b_n$, поэтому сходимость произведения влечет сходимость ряда. Чтобы получить обратное неравенство, введем еще

$$c_{n,m}=\prod_{p\le n}\left(1+\frac{1}{p^s}+\ldots+\frac{1}{p^{ms}}\right).$$

Имеем

$$c_{n,m}\le a_N$$

для достаточно большого N (например, можно взять $N=(n!)^m$). Предположим, что ряд (2) сходится. Тогда из предыдущего неравенства следует, что $c_{n,m}\le\zeta(s)$ и

$$b_n=\lim_{m\to\infty}c_{n,m}\le\zeta(s).$$

Следовательно, b_n, будучи возрастающей последовательностью положительных чисел, сходится к ненулевому пределу. Так что произведение сходится.

Далее, мы получили, что $a_n<b_n\le\zeta(s)$. Так как $\lim_{n\to\infty}a_n=\zeta(s)$, из принципа двух милиционеров следует, что $\lim_{n\to\infty}b_n=\zeta(s)$. $\square$

Следствие 2.1. *Существует бесконечно много простых чисел.*

Доказательство. Взяв $s = 1$, получим

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\dots\left(1-\frac{1}{p}\right)\dots = 0. \tag{8}$$

□

Следствие 2.2. *Имеем*

$$\sum_p \frac{1}{p} = \infty,$$

где сумма берется по всем простым числам.

Этот результат кажется удивительным — ведь простых чисел так мало!

Доказательство следствия 2.2. Логарифмируя обе части (8) и меняя знак, получим

$$\sum_p \left|\ln\left(1-\frac{1}{p}\right)\right| = \infty.$$

С другой стороны,

$$\lim_{p\to\infty} \frac{|\ln(1-1/p)|}{1/p} = 1$$

и наше утверждение следует из признака сравнения рядов с положительными членами. □

Задача 4. Докажите, что найдется такая константа $C > 0$, что для всех n

$$\sum_{p\le n} \frac{1}{p} > C\ln(\ln n). \tag{9}$$

Замечание 1. Обозначим левую часть (9) через a_n. Можно показать, что

$$\lim_{n\to\infty} \frac{a_n}{\ln(\ln n)} = 1.$$

Это легко вывести из такого утверждения:

Факт 1 (Теорема о распределении простых чисел)**.** *Если обозначить n-ое простое число через p_n, то*

$$\lim_{n\to\infty} \frac{p_n}{n\ln n} = 1.$$

Скажем несколько слов об истории этой замечательной теоремы. Вопрос изучался Гауссом в конце XVIII-го века, но Гаусс так и не опубликовал своих гипотез. В 1838-м году Дирихле, по сути, сформулировал эту теорему. Чебышев изучал вопрос о распределении простых чисел в районе 1850-го года. Именно он обнаружил связь между распределением простых чисел и дзета-функцией.

В 1859-м году Риман опубликовал работу, в которой он обнаружил очень глубокую связь между распределением простых и *нулями дзета-функции* (см. §1.5). Наконец, эта теорема была доказана независимо Адамаром и Валле-Пуссеном в 1898-м году. Дальнейшее обсуждение теоремы увело бы нас слишком далеко от нашей основной темы.

1.3. **Значения дзета-функции в четных положительных целых числах.** Стандартное доказательство формул (5) и (6) основано на замечательной формуле Валлиса:

$$\frac{\sin x}{x} = \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{\pi^2 n^2}\right).$$

Доказательство Эйлера выглядело следующим образом: пусть $p(x)$ — многочлен степени n, имеющий n различных ненулевых корней $x_1, \ldots, x_n$. Тогда мы можем записать:

$$(10)\quad p(x) = a(x - x_1)\ldots(x - x_n) = \\ ((-1)^n a x_1 \ldots x_n)\left(1 - \frac{x}{x_1}\right)\left(1 - \frac{x}{x_2}\right)\ldots\left(1 - \frac{x}{x_n}\right) = \\ = p(0)\left(1 - \frac{x}{x_1}\right)\left(1 - \frac{x}{x_2}\right)\ldots\left(1 - \frac{x}{x_n}\right).$$

Применим эту формулу к “многочлену” $\sin x/x$ (который мы продолжим в ноль по непрерывности). Замечая, что его корни — это целые кратные π, а значение в нуле равно единице, получим

$$\frac{\sin x}{x} = \prod_{n>0}\left(1 - \frac{x}{\pi n}\right)\left(1 + \frac{x}{\pi n}\right) = \prod_{n>0}\left(1 - \frac{x^2}{\pi^2 n^2}\right).$$

Конечно, $\sin x/x$ — не многочлен, тем не менее этому доказательству можно придать смысл, если использовать комплексный анализ. Мы дадим набросок доказательства в приложении A.

Теперь докажем формулу (5). Разложим обе части формулы Валлиса с ряд Тейлора с точностью до членов, малых по сравнению с x^2. Имеем

$$\frac{x - x^3/6 + \ldots}{x} = 1 - \frac{x^2}{6} + \ldots = 1 - \left(\sum_{n=1}^{\infty} \frac{1}{\pi^2 n^2}\right) x^2 + \ldots.$$

Приравнивая коэффициенты при x^2, получаем:

$$\frac{-1}{6} = -\sum_{n=1}^{\infty} \frac{1}{\pi^2 n^2},$$

откуда и следует искомая формула. Мы приведем элементарное доказательство формулы (5) чуть ниже.

Задача 5. Выведите формулу (6) из формулы Валлиса.

Задача 6. Вычислите B_0, B_1, B_2, B_4, B_6. Докажите, что $B_{2k+1} = 0$ при $k \geq 1$.

Оказывается, числа Бернулли возникают из следующей естественной задачи. При $k \geq 0$ определим

$$S_k(n) = 1^k + 2^k + \ldots + n^k.$$

Например, $S_0(n) = n$, $S_1(n) = n(n+1)/2$, $S_2(n) = n(n+1)(2n+1)/6$. Возникает гипотеза, что $S_k(n)$ — многочлен степени $k+1$ от n. Эта гипотеза верна, как показывает

Задача 7. Докажите, что

$$S_k(n) = \frac{1}{k+1} \sum_{j=0}^{k} (-1)^j \binom{k+1}{j} B_j n^{k+1-j}.$$

А теперь мы приведем строгое решение проблемы Базеля.

Теорема 3.

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Доказательство. Зафиксируем нечетное число $n = 2m+1$. Положим $a_r = \pi r/n$, где $1 \leq r \leq m$. Обозначим

$$S_m = \sum_{r=1}^{m} \frac{1}{a_r^2} = \frac{n^2}{\pi^2} \sum_{r=1}^{m} \frac{1}{r^2}.$$

Достаточно доказать, что $S_m/(2m+1)^2$ стремится к $1/6$, когда m стремится к бесконечности. Заметим, что

$$\sin a_r < a_r < \tan a_r$$

(это верно для любого числа на интервале $(0; \pi/2)$). Поэтому

$$x_r < \frac{1}{a_r^2} < y_r,$$

где $x_r = \dfrac{\cos^2 a_r}{\sin^2 a_r}$, $y_r = \dfrac{1}{\sin^2 a_r}$. Положим $X_m = \sum_{r=1}^m x_r$, $Y_m = \sum_{r=1}^m y_r$, имеем

$$X_m < S_m < Y_m.$$

Заметим, что $y_r - x_r = 1$, поэтому $Y_m - X_m = m$. Мы докажем, что

$$X_m = \frac{m(2m-1)}{3}. \tag{11}$$

Тогда

$$\lim_{m\to\infty} \frac{X_m}{(2m+1)^2} = \frac{1}{6} \quad \text{и} \quad \lim_{m\to\infty} \frac{Y_m}{(2m+1)^2} = \lim_{m\to\infty} \frac{X_m + m}{(2m+1)^2} = \frac{1}{6},$$

так что наше утверждение будет следовать из принципа двух милиционеров. Итак, осталось доказать (11). Напомним, что $e^{ix} = \cos x + i \sin x$ и $e^{inx} = (e^{ix})^n$. Используя бином Ньютона, получим:

$$(12) \quad \sin nx = \operatorname{Im}(\cos x + i\sin x)^n =$$
$$= \operatorname{Im}\left(\cos^n x + \tbinom{n}{1} i \sin x \cos^{n-1} x + \tbinom{n}{2} i^2 \sin^2 x \cos^{n-2} x + \tbinom{n}{3} i^3 \sin^3 x \cos^{n-3} x + \ldots\right) =$$
$$= \binom{n}{1} \sin x \cos^{n-1} x - \binom{n}{3} \sin^3 x \cos^{n-3} x + \ldots .$$

Деля на $\sin^n x$, получим

$$\frac{\sin nx}{\sin^n x} = \binom{n}{1} \cot^{n-1} x - \binom{n}{3} \cot^{n-3} x + \ldots = p_m(\cot^2 x),$$

где p_m — некоторый многочлен степени $m = (n-1)/2$. Ясно, что $p_m(x_r) = 0$. Значит, $x_1, \ldots, x_m$ — в точности корни многочлена p_m. По теореме Виета их сумма равна $\binom{n}{3} \big/ \binom{n}{1}$, что совпадает с (11). □

Задача 8. Мы наметим еще одно доказательство этой теоремы для тех, кто знает теорию рядов Фурье. Пусть $f(x) = \{2\pi x\}$, где $\{\cdot\}$ обозначает дробную часть. Разложите функцию $f(x)$ в ряд Фурье и выведите предыдущую теорему из равенства Парсеваля.

1.4. **Вероятность выбора взаимно-простых чисел.** Пусть из отрезка $[1; N]$ случайно выбираются k целых чисел (не обязательно различных). Обозначим через $p_k(N)$ вероятность того, что эти числа взаимно просты в совокупности. Иными словами, пусть $P_k(N)$ есть число наборов из k взаимно простых чисел, лежащих на этом отрезке. Тогда $p_k(N) = P_k(N)/N^k$. Число $p_k = \lim_{N\to\infty} p_k(N)$ естественно считать вероятностью того, что k случайно выбранных чисел взаимно просты в совокупности.

Теорема 4.
$$p_k = \zeta(k)^{-1}.$$

Доказательство. Пусть p — простое число. Ясно, что среди N^k наборов чисел от одного до N имеется ровно $[N/p]^k$ наборов, в которых все числа делятся на p ($[x]$ обозначает целую часть числа x). Числа *не* взаимно-просты в совокупности тогда и только тогда, когда они все делятся на какое-нибудь простое число p. Значит, из всех N^k наборов чисел от 1 до N мы должны вычесть $[N/p]^k$ наборов для каждого простого числа $p \le N$. Однако, наборы, в которых числа делятся на два простых числа, скажем на p и q, мы вычли дважды, поэтому мы должны добавить $[N/pq]^k$ и т.д. Иными словами, применяя формулу включения-исключения, мы получим:

$$P_k(N) = N^k - \sum_{p \le N} [N/p]^k + \sum_{p<q\le N} [N/pq]^k - \sum_{p<q<r\le N} [N/pqr]^k + \ldots - \ldots ,$$

где первая сумма ведется по простым, не превосходящим N, вторая по парам простых и т.д. Идея доказательства состоит в том, чтобы заменить $P_k(N)$ на

$$Q_k(N) = N^k - \sum_{p \le N} (N/p)^k + \sum_{p<q \le N} (N/pq)^k - \sum_{p<q<r \le N} (N/pqr)^k + \ldots - \ldots .$$

Покажем, что соответствующий предел не изменится. Сделаем сначала общее утверждение:

Лемма 1. *Если* $0 < x \le y < x+1$, *то* $y^k - x^k \le k y^{k-1}$.

Доказательство. Имеем

$$\begin{aligned} y^k - x^k &= (y-x)(y^{k-1} + xy^{k-2} + \ldots + x^{k-1}) \le \\ &\le 1 \cdot (y^{k-1} + y^{k-1} + \ldots + y^{k-1}) = k y^{k-1}. \end{aligned} \tag{13}$$

□

Мы видим, что

$$\begin{aligned} |Q_k(N) - P_k(N)| &\le \sum_{p \le N} |(N/p)^k - [N/p]^k| + \sum_{p<q \le N} |(N/pq)^k - [N/pq]^k| + \ldots \le \\ &\le k \sum_{p \le N} (N/p)^{k-1} + k \sum_{p<q \le N} (N/pq)^{k-1} + \ldots \le k N^{k-1} \sum_{j=1}^{N} \frac{1}{j^{k-1}}. \end{aligned} \tag{14}$$

Если $k > 2$, то мы получаем

$$\frac{|Q_k(N) - P_k(N)|}{N^k} \le \frac{k\zeta(k-1)}{N},$$

так что

$$\lim_{N \to \infty} \frac{Q_k(N)}{N^k} = \lim_{N \to \infty} \frac{P_k(N)}{N^k}.$$

При $k = 2$ мы воспользуемся задачей 2:

$$\frac{|Q_k(N) - P_k(N)|}{N^k} \le \frac{k(1 + \ln N)}{N},$$

и мы приходим к тому же результату. Осталось заметить, что

$$\lim_{N \to \infty} \frac{Q_k(N)}{N^k} = 1 - \sum_p \frac{1}{p^k} + \sum_{p<q} \frac{1}{(pq)^k} - \ldots + \ldots = \prod_p \left(1 - \frac{1}{p^k}\right) = \zeta(k)^{-1}.$$

□

Следствие 4.1. *Два случайно выбранных натуральных числа взаимно просты с вероятностью* $6/\pi^2$.

Замечание 2. Имеется следующее рассуждение, которое, впрочем, мы не умеем делать строгим: вероятность того, что из k случайных чисел не все делятся на два, равна $1-2^{-k}$. Вероятность того, что не все числа делятся на три, равна $1-3^{-k}$. Эти события независимы в силу китайской теоремы об остатках, так что вероятность того, что не все числа делятся на два *И* не все числа делятся на три, равна $(1-2^{-k})(1-3^{-k})$. Продолжая в том же духе, видим что вероятность того, что числа не делятся все ни на одно простое, меньшее n, равна

$$\prod_{p\le n}\left(1-\frac{1}{p^k}\right)$$

и в пределе мы получаем требуемое утверждение. К сожалению, выбор случайного натурального числа не имеет строгого смысла: действительно, ясно, что все числа должны выбираться с одной и той же вероятностью, но тогда эта вероятность будет равна нулю, ибо сумма всех вероятностей должна быть равна единице.

Задача 9. Найдите такую функцию $\mu:\mathbb{Z}_{>0}\to\mathbb{Z}$, что

$$\prod_{p}\left(1-\frac{1}{p^s}\right)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}.$$

1.5. **Гипотеза Римана.** Невозможно говорить о дзета-функции и не упомянуть гипотезу Римана. Но для этого нужно продолжить дзета-функцию за пределы луча $(1;\infty)$. Сначала, мы выйдем в комплексную область.

Задача 10. Докажите, что ряд (2) сходится абсолютно при всех комплексных s из полуплоскости $\operatorname{Re} s>1$.

1.5.1. *Аналитическое продолжение.*

Разминка 1. Положим

$$f(x)=1+x+x^2+\ldots+x^n+\ldots$$

Нетрудно видеть, что $f(x)$ определена лишь при $|x|<1$. Однако, если догадаться, что $f(x)=\frac{1}{1-x}$, то можно использовать эту формулу для продолжения f на $\mathbb{C}\setminus\{1\}$. Это продолжение является "естественным". Попытаемся придать точный смысл этим словам.

Пусть $U\subset\mathbb{C}$ — открытое множество и $f:U\to\mathbb{C}$ — функция. Напомним, что f называется *аналитической* или *голоморфной* в точке $z\in U$, если она может быть разложена в *степенной ряд* в некоторой окрестности этой точки. Иными словами, если существует такое $r>0$ и такие числа $a_n\in\mathbb{C}$, что

$$f(w)=\sum_{n=0}^{\infty}a_n(w-z)^n \text{ при } |w-z|<r. \tag{15}$$

Аналогичное определение можно дать для функции действительного переменного. В действительном случае, каждая аналитическая функция бесконечно дифференцируема (то есть имеет производные всех порядков), но бывают не аналитические бесконечно дифференцируемые функции. В комплексном случае ситуация разительно отличается:

Факт 2. *Пусть $f : U \to \mathbb{C}$ дифференцируема на U, то есть в каждой точке $z \in U$ существует предел $\lim_{w \to z} \frac{f(w)-f(z)}{w-z}$. Тогда f имеет производные всех порядков на U и является аналитической функцией.*

Итак, пусть функция f аналитична в U. Возьмем $z \in U$ и разложим f в ряд в окрестности z. Пусть этот ряд сходится в круге $\{|w - z| < R\}$. Может так оказаться, что этот круг не содержится в U! Тогда мы продолжили нашу функцию на большее множество U'. Продолжая в том же духе, мы, при некотором везении, продолжим функцию на достаточно большое множество. Например, на $\mathbb{C}$ или на $\mathbb{C}$ без нескольких точек. Разумеется, так происходит не всегда. Нет никакого способа продолжить $\sqrt{z}$ на $\mathbb{C}$ без нескольких точек[1]. Тем не менее, если для $f(z)$ такое продолжение существует, то оно *единственно* в силу следующей теоремы:

Теорема. *Пусть f и g голоморфные функции на* связном *открытом множестве U. Пусть $A = \{z \in U : f(z) = g(z)\}$. Если множество A имеет предельную точку в U, то функции f и g совпадают на U.*

Мы докажем эту теорему в приложении А.

1.5.2. *Аналитическое продолжение дзета-функции и гипотеза Римана.*

Предложение 2. *Дзета-функция голоморфна при* $\operatorname{Re} s > 1$.

Доказательство. Согласно факту 2, нам нужно лишь доказать, что $\zeta(s)$ дифференцируема при $\operatorname{Re} s > 1$. Имеем

$$\frac{d}{ds} n^{-s} = \frac{-\ln n}{n^s}.$$

В силу теоремы о почленном дифференцировании ряда, достаточно доказать, что ряд

$$\sum_{n=1}^{\infty} \frac{-\ln n}{n^s}$$

сходится абсолютно при $\operatorname{Re} s > 1$. Это следует, например, из сравнения с рядом

$$\zeta(t) = \sum_{n=1}^{\infty} \frac{1}{n^t},$$

где t — любое число на интервале $(1, s)$. □

Оказывается, дзета-функцию можно продолжить до функции, голоморфной во всех комплексных числах, кроме точки 1. Более того, оказывается существует простая связь между $\zeta(1 - s)$ и $\zeta(s)$:

[1] Это связано с тем, что при обходе вокруг нуля значение $\sqrt{z}$ меняется на противоположное.

Факт 3 (Функциональное уравнение для дзета-функции)**.**

$$\zeta(1-s) = \frac{2}{(2\pi)^s} \sin\left(\frac{\pi(1-s)}{2}\right) \Gamma(s)\zeta(s),$$

где $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}\,dx$ *— гамма-функция.*

Задача 11. Пусть нам удалось продолжить дзета-функцию до функции, определенной при $\operatorname{Re} s > 0$, $s \neq 1$ так, чтобы при $0 < \operatorname{Re} s < 1$ выполнялось функциональное уравнение. Докажите, что дзета-функцию можно продолжить до аналитической функции, определенной при всех $s \neq 1$.

Попробуем найти все точки, где $\zeta(s) = 0$. Из произведения Эйлера следует, что $\zeta(s) \neq 0$ при $\operatorname{Re} s > 1$. С другой стороны, функциональное уравнение показывает, что при $\operatorname{Re} s < 0$ имеем

$$\zeta(s) = 0 \Longleftrightarrow s \in \{-2, -4, -6, \dots, -2n, \dots\}.$$

Задача 12. Докажите последнее утверждение.

Осталось выяснить, при каких s в полосе $0 < \operatorname{Re} s < 1$ дзета-функция обращается в ноль...

Гипотеза Римана. Дзета-функция не обращается в ноль нигде, кроме точек -2, -4, -6,... и некоторых точек на прямой $\operatorname{Re} s = 1/2$.

Замечание 3. Известно, что “критическая прямая” $\operatorname{Re} s = 1/2$ содержит бесконечно много нулей дзета-функции. С другой стороны, гипотеза Римана, вероятно, еще очень далека от разрешения. Она была включена в список проблем тысячелетия, за решение которых предлагается приз в один миллион долларов. Как мы уже говорили (см. замечание 1) гипотеза Римана связана с распределением простых чисел. В частности, гипотеза Римана равносильна следующему утверждению.

Пусть $\pi(x)$ *количество простых чисел, меньших* x*, положим также* $Li(x) = \int_2^x \frac{dt}{\ln t}$*, тогда*

$$|\pi(x) - Li(x)| \leq \frac{1}{8\pi}\sqrt{x}\ln x \text{ для всех } x \geq 2657.$$

Лекция 2. Дзета-функция кольца гауссовых чисел и представления натурального числа в виде суммы двух квадратов

На этом занятии мы будем изучать следующий вопрос: дано натуральное число n, можно ли его представить в виде суммы двух квадратов. Если можно, то сколькими способами? Иными словами, мы хотим исследовать квадратное диофантово уравнение $n = x^2 + y^2$, где n фиксировано.

Заметим, что линейные диофантовы уравнения (и даже линейные системы) решаются просто. Наверняка читатель знает “теорию” диофантова уравнения $ax + by = c$.

Задача* **13.** Разработайте алгоритм для решения линейных диофантовых уравнений с бóльшим числом переменных, и систем таких уравнений.

2.1. **Разминка: простейшее квадратное уравнение.** Для $n \in \mathbb{Z}$ рассмотрим диофантово уравнение $n = x^2 - y^2$. Чтобы выяснить, когда оно имеет решения, разложим правую часть на множители:

$$n = (x - y)(x + y).$$

Ясно, что $x - y$ и $x + y$ имеют одинаковую четность. Поэтому их произведение либо нечетно, либо делится на 4. Обратно, если n нечетно, то можно положить $x - y = 1$, $x + y = n$, что дает $x = (n + 1)/2$, $y = (n - 1)/2$. Наконец, если n делится на 4, то можно взять $x - y = 2$, $x + y = n/2$, то есть $x = n/4 + 1$, $y = n/4 - 1$. Итак, наше уравнение имеет решения тогда и только тогда, когда *остаток от деления n на 4 не равен двум.*

2.2. **Суммы квадратов целых чисел.** Мы переходим к гораздо более сложному диофантову уравнению: $n = x^2 + y^2$. В свое время автор этой брошюры был *крайне* впечатлен тем фактом, что можно полностью выяснить, когда это уравнение имеет решения. Это кажется особенно удивительным, если заметить, что при фиксированном n количество возможных x и y ограничено: $|x| \le \sqrt{n}$, $|y| \le \sqrt{n}$. Сформулируем ответ:

Теорема 5. *Пусть $n = p_1^{k_1} \dots p_l^{k_l}$ разложение числа n на различные простые множители. Число n представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда k_i четны, для всех i, для которых $p_i \equiv 3 \pmod 4$.*

Например, $21 = 3 \cdot 7$ не представимо в виде суммы двух квадратов, потому что 3 входит в разложение в нечетной степени, а 90 — представимо, потому что 3 входит в четной степени.

Теорема 6. *Число целых решений уравнения $x^2 + y^2 = n$ в четыре раза больше разности числа положительных делителей числа n вида $4k + 1$ и числа положительных делителей вида $4k + 3$.*

Мы переходим к доказательству этих теорем. На самом деле, обе теоремы можно доказать совершенно элементарными методами, но мы дадим “концептуальное” доказательство.

2.3. **Гауссовы числа.** Мы видим, что предыдущее диофантово уравнение решилось просто, потому что $x^2 - y^2$ можно разложить на множители. Многочлен $x^2 + y^2$ тоже можно разложить на множители, но придется использовать комплексные числа:

$$x^2 + y^2 = (x + iy)(x - iy),$$

где, как всегда, $i = \sqrt{-1}$.

Определение 2. Кольцо

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

называется *кольцом гауссовых чисел.*

Задача 14. Докажите, что $\mathbb{Z}[i]$ — подкольцо в $\mathbb{C}$. Иными словами, докажите, что сумма, разность и произведение гауссовых чисел есть гауссово число.

Соглашение. *На этом занятии греческие буквы будут обозначать гауссовы числа, а латинские — целые числа.*

Определим норму гауссова числа $\alpha = x + iy$:

$$N\alpha = |\alpha|^2 = \alpha\bar{\alpha} = x^2 + y^2.$$

Эта формула показывает, что *норма мультипликативна*: $N(\alpha\beta) = N\alpha\, N\beta$. Ясно, что целое число представимо в виде суммы двух квадратов если и только если оно является нормой некоторого гауссова числа. Мы видим, что абстрактная алгебра появляется естественным образом из "классической" задачи.

Следствие. *Если числа m и n представимы в виде суммы двух квадратов, то и mn представимо в виде суммы двух квадратов.*

Задача 15. Докажите утверждение следствия, не используя гауссовы числа.

Возникает следующая "программа": пусть α — гауссово число. Представим его в виде произведения "гауссовых простых чисел": $\alpha = \pi_1\pi_2\ldots\pi_l$ (повторения возможны). Тогда $N\alpha = N\pi_1\, N\pi_2 \ldots N\pi_l$. Значит, чтобы выяснить какие числа представляются в виде суммы двух квадратов, достаточно найти нормы все гауссовых простых чисел и рассмотреть их произведения. Но что является аналогом простого числа в кольце гауссовых чисел?

Начнем с такого замечания: простые целые числа — это положительные числа p, которые делятся только на 1, -1, p и $-p$ [2]. Что является аналогом 1 и -1 в гауссовых числах? Дадим общее определение.

Определение 3. Элемент ε кольца A называется *обратимым*, если найдется такой элемент ε', что $\varepsilon\varepsilon' = 1$.

Обратимые элементы еще иногда называют единицами.

Лемма 2. *$\varepsilon \in \mathbb{Z}[i]$ обратим тогда и только тогда, когда $N\varepsilon = 1$.*

Доказательство. Если $N\varepsilon = 1$, то $\varepsilon\bar{\varepsilon} = 1$ и ε обратим. Обратно, если $\varepsilon\varepsilon' = 1$, то $N\varepsilon\, N\varepsilon' = 1$, следовательно $N\varepsilon = 1$. ☐

Следствие. *Обратимые элементы кольца $\mathbb{Z}[i]$ суть 1, -1, i и $-i$.*

Введем следующее обобщение кольца гауссовых чисел: пусть $D \in \mathbb{Z}$, положим

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

Обычно мы будем предполагать, что *D свободно от квадратов*, то есть в его разложение на простые множители все простые входят в первой степени. Норма в этом кольце определяется так: $N(a + b\sqrt{D}) = |a^2 - Db^2|$.

[2] Кстати, с точки зрения алгебры отрицательные числа, обладающие этим свойством, тоже удобно считать простыми.

Задача 16. Проверьте, что норма в $\mathbb{Z}[\sqrt{D}]$ мультипликативна и докажите, что все обратимые элементы в $\mathbb{Z}[\sqrt{D}]$ при $D \leq -2$ суть 1 и -1.

Замечание 4. Если $D > 0$ не является точным квадратом, то обратимые элементы кольца $\mathbb{Z}[\sqrt{D}]$ образуют группу, изоморфную $\mathbb{Z}$ (см. §3.3).

Назовем $\pi \in \mathbb{Z}[i]$ *разложимым*, если $\pi = \beta\gamma$, где β и γ необратимы. В противном случае назовем элемент *простым*. Назовем элементы α и β *ассоциированными*, если $\alpha = \varepsilon\beta$, где ε — обратим.

Задача 17. Отношение ассоциированности является отношением эквивалентности.

Заметим, что элемент, ассоциированный с простым, тоже прост. Кроме того, в разложении на простые всегда можно заменить некоторые простые на ассоциированные. Например, $15i = 3(i-2)(1-2i)$ и мы увидим ниже, что это — разложение числа $15i$ на простые множители. Но можно также написать $15i = 3i(1+2i)(1-2i)$, где $3i$ ассоциировано с 3, а $1+2i$ ассоциировано с $i-2$. Поэтому разложение на простые может быть единственным разве что с точностью до ассоциированности[3].

Теорема 7. *Каждое ненулевое гауссово число может быть записано в виде произведения простых. Такое разложение единственно с точностью до перестановки множителей и замены простых на ассоциированные.*

Доказательство аналогично доказательству для целых чисел, а именно, нужно воспользоваться следующим утверждением:

Задача 18. [Теорема о делении с остатком] Пусть даны гауссовы числа α и $\beta \neq 0$. Тогда найдутся такие гауссовы числа ν и ρ, что $\alpha = \nu\beta + \rho$ и $N\rho < N\beta$.

Задача* 19. Докажите теорему 7.

Предостережение. В более общих кольцах теорема об однозначности разложения чаще неверна, чем верна. Например, в $\mathbb{Z}[\sqrt{-5}]$ имеем $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Задача 20. Докажите, что 2, 3, $1+\sqrt{-5}$ и $1-\sqrt{-5}$ не являются разложимыми в $\mathbb{Z}[\sqrt{-5}]$.

2.4. **Описание простых гауссовых чисел.** Как читатель уже заметил, простое целое число может перестать быть простым, если рассматривать его, как гауссово; пример: $5 = (2+i)(2-i)$. Следующие три предложения проясняют ситуацию.

[3]Заметим, что такая же проблема будет и с целыми числами, если разрешить отрицательные простые: $15 = 3 \cdot 5 = (-3)(-5)$ (см. сноску на стр. 15).

Напомним, что если α и β элементы кольца A, то α *делит* β, если найдется такой элемент $\gamma \in A$, что $\beta = \alpha\gamma$. Обозначение: $\alpha|\beta$. Очевидно, что в кольце с мультипликативной нормой $\alpha|\beta$ влечет $N\alpha|N\beta$.

Предложение 3. (*а*) *Для любого гауссова числа α найдется такое целое число a, что $\alpha|a$.*
(*б*) *Для любого простого гауссова числа π найдется простое целое число p такое, что $\pi|p$. При этом $N\pi = p$ или $N\pi = p^2$. (В этом случае говорят, что π* лежит над *p.)*
(*в*) *Обратно, пусть p — простое целое число. Если p не является нормой гауссова числа, то p просто,* как гауссово число. *Если $p = N\pi$, то $p = \pi\bar{\pi}$ — разложение p на простые гауссовы числа.*

Доказательство. (а) Достаточно заметить, что $\alpha|\alpha\bar{\alpha} = N\alpha$.
(б) Пусть $\pi|a$, где $a \in \mathbb{Z}$. Разложим a в произведение простых целых чисел: $a = p_1p_2\dots p_n$ (возможны повторения). Далее, мы можем разложить p_i в произведение гауссовых простых. В силу теоремы об однозначности разложения для гауссовых чисел, π входит в разложение одного из p_i. Тогда π делит p_i и первое утверждение доказано.

Имеем $N\pi|Np_i = p_i^2$. Поэтому $N\pi = p_i$ или $N\pi = p_i^2$ (случай $N\pi = 1$ невозможен, потому что π не является обратимым).
(в) Пусть p не является простым, как гауссово число. Тогда $p = \alpha\beta$, где α и β необратимы, и, значит $N\alpha > 1$, $N\beta > 1$. Взяв нормы, получаем: $p^2 = N\alpha\, N\beta$. Значит $N\alpha = N\beta = p$ и первое утверждение следует.

Пусть теперь $p = N\pi = \pi\bar{\pi}$. Нам осталось доказать, что π и $\bar{\pi}$ просты. Пусть $\pi = \alpha\beta$, тогда $p = N\alpha\, N\beta$ и мы видим, что либо α, либо β обратимо. Значит π просто. Аналогично $\bar{\pi}$ просто. □

Обозначим множество классов ассоциированности простых гауссовых чисел через Π, а множество положительных простых целых чисел через P. Рассмотрим отображение из Π в P, переводящее π в единственный простой делитель числа $N\pi$. Мы видим, что у каждого простого числа один или два прообраза.

Итак, осталось выяснить, какие простые целые числа разложимы в $\mathbb{Z}[i]$, а какие остаются простыми. На самом деле, нужно еще выяснить, не может ли быть так, что π и $\bar{\pi}$ ассоциированы. Начнем со второго вопроса.

Предложение 4. *Имеем $2 = (1+i)(1-i) = -i(1+i)^2$. Пусть $p > 2$ и $p = \pi\bar{\pi}$, тогда π и $\bar{\pi}$ не ассоциированы.*

Доказательство. Первое утверждение проверяется вычислением, докажем второе утверждение. Пусть $p = \pi\bar{\pi}$, где $\bar{\pi} = \varepsilon\pi$, $\varepsilon = \pm 1$ или $\pm i$. Запишем $\pi = a + bi$. Если $\varepsilon = 1$, то $b = 0$, $\pi = a$, $p = a^2$ и мы приходим к противоречию с простотой p. Случай $\varepsilon = -1$ аналогичен. Если $\varepsilon = i$, то $a = -b$, $\pi = a(1-i)$ и $p = N\pi = 2a^2$, что противоречит предположению, что p простое, большее двух. Случай $\varepsilon = -1$ аналогичен. □

Следующее предложение является ключевым.

Предложение 5. *Целое число p разложимо как гауссово число тогда и только тогда, когда $p = 2$ или $p \equiv 1 \pmod 4$.*

Доказательство. Случай $p = 2$ очевиден. Пусть $p \equiv 3 \pmod 4$ и p — разложимо. Тогда, в силу предложения 3(в), $p = N\pi = a^2 + b^2$, где $a, b \in \mathbb{Z}$. Но точный квадрат всегда дает остаток ноль или один при делении на 4, поэтому $a^2 + b^2$ дает остаток 0, 1 или 2. Противоречие.

Далее, от противного, пусть $p \equiv 1 \pmod 4$ и p просто, как гауссово число. Нам понадобится лемма, которую мы докажем позже:

Лемма 3. *Если $p \equiv 1 \pmod 4$ простое число, то найдется такое m, что $p | m^2 + 1$.*

Возьмем такое m, тогда $p|m^2+1 = (m+i)(m-i)$. Будучи простым гауссовым, p делит $m + i$ или $m - i$. Но тогда $p|1$.

Доказательство леммы. Докажем, что

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

(тогда можно взять $m = ((p-1)/2)!$). Сначала докажем, что $(p-1)! \equiv -1 \pmod p$. Действительно, рассмотрим ненулевые остатки по модулю p: $1, 2, \ldots, p-1$. Если x — остаток, то найдется единственный остаток y такой, что $xy \equiv 1 \pmod p$. Нетрудно видеть, что $x = y$ если и только если $x = 1$ или $x = p - 1$. Значит, все остатки, кроме 1 и $p - 1$, разбиваются на пары взаимно обратных. Поэтому произведение всех таких остатков равно единице (точнее сравнимо с единицей по модулю p). Следовательно, произведение всех остатков равно $1 \cdot (p-1) \equiv -1 \pmod p$.

Далее, мы можем записать

$$(16) \quad (p-1)! = \left(\tfrac{p-1}{2}\right)! \left(\tfrac{p+1}{2}\right) \left(\tfrac{p+3}{2}\right) \ldots (p-1) \equiv \\ \left(\tfrac{p-1}{2}\right)! \left(-\tfrac{p-1}{2}\right) \left(-\tfrac{p-3}{2}\right) \ldots (-1) \equiv \left(\left(\tfrac{p-1}{2}\right)!\right)^2 (-1)^{\frac{p-1}{2}} \pmod p.$$

Осталось заметить, что $p \equiv 1 \pmod 4$ равносильно $(-1)^{\frac{p-1}{2}} = 1$. □

Доказательство предложения 5 закончено. □

Задача 21. Выведите другое доказательство леммы из того, что мультипликативная группа поля из p элементов циклична.

Следующая теорема описывает все простые гауссовы числа.

Теорема 8. *Пусть $p \in \mathbb{Z}$ — простое число.*

- *Если $p = 2$, то $1+i$ единственное гауссово простое число, лежащее над p, с точностью до ассоциированности, причем $2 = (1+i)(-i(1+i))$. Кроме того, $N(1+i) = 2$.*
- *Если $p \equiv 3 \pmod 4$, то с точностью до ассоциированности p — единственное гауссово простое, лежащее над p, причем $Np = p^2$.*
- *Если $p \equiv 1 \pmod 4$, то найдется такое $\pi \in \mathbb{Z}[i]$, что $p = \pi\bar{\pi}$. При этом, с точностью до ассоциированности, над p лежит ровно два простых: π и $\bar{\pi}$. Имеем $N\pi = N\bar{\pi} = p$.*

Доказательство. Эта теорема немедленно следует из трех предыдущих предложений. □

Задача 22. Докажите теорему 5.

2.5. **Дзета-функция гауссовых чисел.** Мы определим дзета-функцию для кольца гауссовых чисел и докажем с ее помощью теорему 6.

Определение 4.

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{4}\sum_{\alpha\in\mathbb{Z}[i],\alpha\neq 0}\frac{1}{N\alpha^s} = \frac{1}{4}\sum_{(a,b)\neq(0,0)}\frac{1}{(a^2+b^2)^s}. \tag{17}$$

Здесь коэффициент $1/4$ введен, чтобы учесть каждый класс ассоциированности ровно один раз[4]. Можно показать, что этот ряд сходится при $s > 1$ и, более общо, при всех $s \in \mathbb{C}$ с $\operatorname{Re} s > 1$ (см. §2.5.1).

Мы можем переписать $\zeta_{\mathbb{Z}[i]}(s)$ в виде ряда, похожего на ряд для обычной дзета-функции

$$\frac{1}{4}\sum_{n=1}^{\infty}\frac{q_n}{n^s}, \tag{18}$$

где q_n — число представлений n в виде суммы квадратов двух целых чисел. Этот ряд также сходится при $s > 1$. Заметим, что ряды такого вида называются *рядами Дирихле.*

2.5.1. *Вопросы сходимости.* Что означает двойной ряд (17)? Можно считать, что мы сначала суммируем по a, а затем по b:

$$\zeta_{\mathbb{Z}[i]}(s) = \sum_{a=1}^{\infty}\left(\sum_{b=0}^{\infty}(a^2+b^2)^{-s}\right),$$

где мы использовали такое утверждение: каждое ненулевое гауссово число ассоциировано с единственным $a + bi$, где $a > 0$, $b \geq 0$.

Можно, наоборот, суммировать сначала по b, а затем по a. Наконец, можно взять возрастающую последовательность S_m конечных подмножеств в $\mathbb{Z}_{>0} \times \mathbb{Z}_{\geq 0}$ (то есть

---

[4] Заметим, что дзета-функция Римана может быть записана аналогично: $\zeta(s) = \frac{1}{2}\sum_{n\in\mathbb{Z}\setminus\{0\}}|n|^{-s}$.

$S_1 \subset S_2 \subset \ldots$) так, чтобы $\cup_{m=1}^{\infty} S_m = \mathbb{Z}_{>0} \times \mathbb{Z}_{\geq 0}$. К счастью, результат получится один и тот же. Дело в том, что наш ряд сходится абсолютно. Искушенный читатель может попытаться доказать абсолютную сходимость:

Задача 23. Пусть $\operatorname{Re} s > 1$, докажите, что найдется такая константа C (зависящая от s), что для любого конечного множества $S \subset \mathbb{Z}_{>0} \times \mathbb{Z}_{\geq 0}$ имеем

$$\sum_{(a,b)\in S} \left|(a^2+b^2)^{-s}\right| < C.$$

2.5.2. *Вычисление дзета-функции кольца гауссовых чисел.*

Теорема 9.

$$\zeta_{\mathbb{Z}[i]}(s) = \prod_{\pi} \left(1 - \frac{1}{N\pi^s}\right)^{-1}, \tag{19}$$

где в произведении участвует по одному простому из каждого класса ассоциированности.

Доказательство. Эта теорема доказывается так же, как и теорема 2. Приведем, все же, некоторые детали. Имеем

$$\left(1 - \frac{1}{N\pi^s}\right)^{-1} = 1 + \frac{1}{N\pi^s} + \frac{1}{N\pi^{2s}} + \ldots + \frac{1}{N\pi^{ms}} + \ldots .$$

Если записать в таком виде каждый сомножитель и раскрыть скобки, то получится сумма членов вида

$$(N\pi_1^{m_1} N\pi_2^{m_2} \ldots N\pi_k^{m_k})^{-s}.$$

Произведение в скобках равно $N(\pi_1^{m_1}\pi_2^{m_2}\ldots\pi_k^{m_k})$ в силу мультипликативности нормы. Значит, по теореме об однозначном разложении на множители, мы получим

$$\sum_{\alpha} \frac{1}{N\alpha^s},$$

где в сумме участвует по одному ненулевому гауссову числу из каждого класса ассоциированности. Осталось заметить, что в каждом таком классе ровно четыре элемента, и их нормы равны. □

Для $p \equiv 1 \pmod 4$ обозначим через π_p какое-нибудь из восьми гауссовых чисел с нормой p. Соберем в (19) вместе множители, соответствующие гауссовым простым, лежащим над одним целым простым. В силу теоремы 8 имеем

(20) $\zeta_{\mathbb{Z}[i]}(s) =$

$$= \left(1-\tfrac{1}{N(1+i)^s}\right)^{-1} \prod\nolimits_{p\equiv 1 \pmod 4} \left(1-\tfrac{1}{N\pi_p^s}\right)^{-1} \left(1-\tfrac{1}{N\bar\pi_p^s}\right)^{-1} \prod\nolimits_{p\equiv 3 \pmod 4} \left(1-\tfrac{1}{Np^s}\right)^{-1} =$$

$$\left(1-\frac{1}{2^s}\right)^{-1} \prod_{p\equiv 1 \pmod 4} \left(1-\frac{1}{p^s}\right)^{-2} \prod_{p\equiv 3 \pmod 4} \left(1-\frac{1}{p^{2s}}\right)^{-1} =$$

$$\zeta(s) \prod_{p\equiv 1 \pmod 4} \left(1-\frac{1}{p^s}\right)^{-1} \prod_{p\equiv 3 \pmod 4} \left(1+\frac{1}{p^s}\right)^{-1}.$$

В самом конце мы использовали теорему 2.

2.5.3. *L-функции Дирихле.* Сделаем небольшое отступление. Пусть $\chi : \mathbb{Z} \to \mathbb{C}$ — функция, обладающая следующим свойством:

(21) $$\chi(mn) = \chi(m)\chi(n) \text{ для любых } m \text{ и } n.$$

Ряд Дирихле

$$\sum \frac{\chi(n)}{n^s}$$

обозначается $L(s, \chi)$.

Задача 24. Придумайте аналог произведения Эйлера для ряда Дирихле $L(s, \chi)$. А что можно сказать, если свойство (21) выполняется только для взаимно-простых m и n?

Замечание 5. Пусть функция χ обладает свойством (21) еще следующими свойствоми: существует N такое, что $\chi(n) = \chi(n+N)$ при всех n и $\chi(n) \neq 0$ тогда и только тогда, когда n и N взаимно-просты. Тогда χ называется *характером Дирихле по модулю N*, а $L(s, \chi)$ называется *L-функцией Дирихле.* Характеры Дирихле и соответствующие L-функции были введены Дирихле при доказательстве его знаменитой теоремы: целочисленная арифметическая прогрессия, у которой член и разность взаимно-просты, содержит бесконечно много простых чисел.

2.5.4. *Окончание вывода формулы для числа представлений в виде суммы квадратов.* Определим $\chi : \mathbb{Z} \to \{-1, 0, 1\}$ так: $\chi(2k) = 0$, $\chi(4k+1) = 1$, $\chi(4k+3) = -1$. Ясно, что χ является характером Дирихле

Задача 25. Докажите, что χ — единственный нетривиальный характер Дирихле по модулю 4.

Из задачи 24 следует, что

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

Теперь вычисление (20) показывает, что

$$\zeta_{\mathbb{Z}[i]}(s) = \zeta(s)L(s,\chi) = \sum_{n=1}^{\infty} \frac{\sum_{d|n}\chi(d)}{n^s}. \tag{22}$$

Теорема 6 следует из этой формулы и (18) (см. также следующие задачи).

Задача 26. Пусть

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

при всех $s > C$, для некоторой константы C (в частности оба ряда сходятся). Тогда $a_n = b_n$ для всех n.

Задача 27. Докажите формулу для произведения рядов Дирихле

$$\Big(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{b_n}{n^s}\Big) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

где последовательность c_n есть так называемое *произведение Дирихле* последовательностей a_n и b_n:

$$c_n = \sum_{d|n, d>0} a_d b_{n/d}.$$

Лекция 3. Обобщения на другие квадратичные кольца и общие числовые кольца

Все вышесказанное верно (с минимальными изменениями) для $\mathbb{Z}[\sqrt{D}]$, где $D < 0$, *если выполняется теорема об однозначном разложении.* К сожалению, выполняется она только при $D = -1$, -2 и -67. При $D = -3$, -7, -11, -19, -43 и -163 она выполняется для похожего кольца

$$\mathbb{Z}\left[\tfrac{1+\sqrt{D}}{2}\right] = \left\{ a + b\tfrac{1+\sqrt{D}}{2} \,\middle|\, a, b \in \mathbb{Z} \right\},$$

см. §3.2 и особенно задачу 37.

Задача* 28. Докажите, что $\mathbb{Z}[\sqrt{-2}]$ обладает однозначностью разложения и выясните какие числа представляются в виде $a^2 + 2b^2$. Вычислите соответствующую дзета-функцию.

Задача 29. Выведите из однозначности разложения в кольце $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ следующее утверждение: $n^2 + n + 41$ является простым числом при $0 \le n \le 39$.

Мы объясним, что всегда имеется некоторый аналог однозначности разложения и определим дзета-функцию. Мы увидим, что поведение дзета-функции в окрестности точки 1 связано с очень важным инвариантом кольца $\mathbb{Z}[\sqrt{D}]$. Мы начнем с изложенимя общей теории.

3.1. **Числовые кольца.** Мы хотим расширить класс колец, с которыми мы работаем, хотя на этой лекции мы в основном будем интереосваться квадратичными кольцами. Мы будем предполагать, что читатель немного знаком с понятиями группы и кольца. Под кольцом мы всегда понимаем ассоциативное коммутативное кольцо с единицей.

Напомним, что комплексное число x называется *целым алгебраическим*, если оно является корнем многочлена с целыми коэффициентами и коэффициентом один при старшем члене:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \qquad a_{n-1}, \ldots, a_0 \in \mathbb{Z}. \tag{23}$$

Если разрешить рациональные коэффициенты, то получится определение *алгебраического* числа. Множество целых алгебраических чисел обозначается через $\overline{\mathbb{Z}}$, а множество всех алгебраических чисел — через $\overline{\mathbb{Q}}$.

Задача 30. Докажите, что для любого $a \in \overline{\mathbb{Q}}$ найдется такое ненулевое целое число n, что $na \in \overline{\mathbb{Z}}$.

Напомним, что кольцо A *порождается* своими элементами $\alpha_1,\ldots,\alpha_n$, если любой элемент кольца можно получить из этих элементов при помощи операций сложения, вычитания и умножения. В этом случае пишут $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Мы будем изучать следующий класс колец:

Определение 5. Кольцо $A \subset \mathbb{C}$ называется *числовым кольцом*, если оно порождается конечным числом целых алгебраических чисел.

Примеры: $\mathbb{Z}[\sqrt{D}]$, $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$, $\mathbb{Z}[e^{\frac{2\pi i}{n}}]$, $\mathbb{Z}[\sqrt[3]{2}]$.

Напомним, что абелева группа G *конечно порождена*, если найдется такое конечное множество ее элементов $g_1, \ldots, g_k$, что любой элемент можно записать в виде

$$n_1 g_1 + n_2 g_2 + \ldots + n_k g_k,$$

где n_1, …, n_k — целые числа.

Предложение 6. (*а*) *Кольцо $A \subset \mathbb{C}$ является числовым кольцом тогда и только тогда, когда оно конечно порождено, как группа по сложению.*
(*б*) *Если A — числовое кольцо, то $A \subset \overline{\mathbb{Z}}$.*

Доказательство. Каждое числовое кольцо конечно порождено, как группа по сложению. Действительно, пусть $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ — числовое кольцо, где α_i удовлетворяет некоторому уравнению вида (23). Обозначим через n_i степень этого уравнения и рассмотрим все возможные мономы $\alpha_1^{m_1}\alpha_2^{m_2}\ldots\alpha_k^{m_k}$, где $0 \le m_i < n_i$. Нетрудно видеть, что они порождают A, как группу по сложению, но число таких мономов конечно.

Если кольцо $A \subset \mathbb{C}$ конечно-порождено, как группа по сложению, то $A \subset \overline{\mathbb{Z}}$. Действительно, пусть $\alpha \in A$. Рассмотрим подкольцо $\mathbb{Z}[\alpha]$. Согласно доказанному, группа A конечна порождена, но тогда и группа $\mathbb{Z}[\alpha]$ конечно порождена, ибо подгруппа конечно-порожденной группы конечно порождена. Итак, пусть кольцо $\mathbb{Z}[\alpha]$ порождено элементами $\beta_1, \ldots, \beta_k$, как группа по сложению. Мы можем записать $\beta_i = a_{0i} + a_{1i}\alpha + \ldots + a_{m_k i}\alpha^{m_k}$, где все коэффициенты a_{ji} — целые. Пусть m равно максимуму из чисел m_i, тогда $\mathbb{Z}[\alpha]$ совпадает с *группой*, порожденной элементами 1, α, α^2, …, α^m. Но это значит, что

$$\alpha^{m+1} = a_0 + a_1\alpha + \ldots + a_m\alpha^m$$

для некоторых целых чисел a_i, так что $\alpha \in \overline{\mathbb{Z}}$.

Из этих двух утверждений следует утверждение (б), и остается доказать, что кольцо, конечно порожденное, как группа по сложению, является числовым. Это следует из второго утверждения. □

Следствие. *Сумма и произведение целых алгебраических чисел — целые алгебраические числа, т.е. множество $\overline{\mathbb{Z}}$ является кольцом.*

Доказательство. Пусть $\alpha, \beta \in \overline{\mathbb{Z}}$. Рассмотрим числовое кольцо $\mathbb{Z}[\alpha, \beta]$. Согласно предыдущему предложению, оно содержится в $\overline{\mathbb{Z}}$. Поэтому $\alpha+\beta, \alpha\beta \in \overline{\mathbb{Z}}$. □

Задача 31. Докажите, что множество всех алгебраических чисел является полем.

Задача* 32. Докажите, что $\overline{\mathbb{Z}}$ не является числовым кольцом. Является ли $\overline{\mathbb{Q}}$ числовым кольцом?

Заметим, что определение обратимого элемента и ассоциированных элементов имеет смысл в любом кольце.

3.2. **Целозамкнутость.** Рассмотрим кольцо $\mathbb{Z}[3i] = \{a + 3bi | a, b \in \mathbb{Z}\}$. Ясно, что с этим кольцом *что-то не так.* Например, однозначность разложения на множители нарушается по дурацким причинам: $9 = 3i(-3i) = 3 \cdot 3$, при этом $3i$ и 3 неразложимы и неассоциированы (Проверьте!). Чтобы исключить такие примеры, мы наложим на A следующее техническое условие. Рассмотрим *поле частных* $QA = \{a/b | a, b \in A\}$. Ясно, что QA подполе в $\overline{\mathbb{Q}}$. Кольцо A называется *целозамкнутым*, если $QA \cap \overline{\mathbb{Z}} = A$. Мы часто будем предполагать, что A целозамкнуто.

Задача 33. Кольца $\mathbb{Z}[3i]$ и $\mathbb{Z}[\sqrt{-3}]$ не целозамкнуты.

С геометрической точки зрения, целозамкнутость — это свойство, аналогичное гладкости[5]. Если числовое кольцо A не целозамкнуто, то можно заменить его на $QA \cap \overline{\mathbb{Z}}$, которое уже обязательно будет целозамкнутым: действительно, легко проверить, что $Q(QA \cap \overline{\mathbb{Z}}) = QA$. Можно показать, что $QA \cap \overline{\mathbb{Z}}$ будет конечно порождено, то есть будет числовым кольцом. Это кольцо называется *целым замыканием* кольца A.

[5]В высших размерностях целозамкнутость слабее гладкости.

Задача 34. Если в числовом кольце выполняется однозначность разложения на множители, то оно целозамкнуто.

Из этой задачи следует, что $\mathbb{Z}$ и $\mathbb{Z}[i]$ целозамкнуты.

Пусть $\alpha = a + b\sqrt{D}$, где $a, b \in \mathbb{Q}$, $D \in \mathbb{Z}$, причем D не есть точный квадрат. Положим $\bar{\alpha} = a - b\sqrt{D}$.

Задача 35. Пусть $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$. Докажите, что $\overline{\alpha \pm \beta} = \bar{\alpha} \pm \bar{\beta}$ и $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$. Выведите отсюда, что $\alpha \in \overline{\mathbb{Z}}$ влечет $\bar{\alpha} \in \overline{\mathbb{Z}}$. Наконец, докажите, что $a + b\sqrt{D} \in \overline{\mathbb{Z}}$ тогда и только тогда, когда $2a \in \mathbb{Z}$ и $a^2 - Db^2 \in \mathbb{Z}$.

Задача 36. Пусть $D \in \mathbb{Z}$. Докажите, что $\mathbb{Z}[\sqrt{D}]$ целозамкнуто тогда и только тогда, когда D свободно от квадратов и $D \not\equiv 1 \pmod 4$.

Задача 37. Пусть $D \in \mathbb{Z}$ свободно от квадратов, причем $D \equiv 1 \pmod 4$. Докажите, что $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ является целозамкнутым числовым кольцом. Докажите, также, что оно является целым замыканием кольца $\mathbb{Z}[\sqrt{D}]$.

В силу последних двух задач естественно ввести следующее обозначение: пусть $D \in \mathbb{Z}$ свободно от квадратов, тогда:

$$Q_D = \begin{cases} \mathbb{Z}[\sqrt{D}] \text{ если } D \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] \text{ если } D \equiv 1 \pmod 4. \end{cases} \tag{24}$$

3.3. **Теорема Дирихле о единицах.** Ясно, что обратимые элементы числового кольца образуют группу по умножению. Оказывается, эта группа всегда конечно порождена. Поэтому, в силу теоремы о классификации конечно-порожденных групп, ее можно представить в виде $G_{tor} \times G_{fr}$, где G_{tor} — конечная группа, а G_{fr} — свободная группа.

Задача 38. Докажите, что G_{tor} — циклическая группа, совпадающая с множеством всех корней из единицы, содержащихся в кольце.

Возникает естественный вопрос: чему равен ранг группы G_{fr}? Ответ дается теоремой Дирихле, к формулировке которой мы переходим. Пусть K — поле частных целозамкнутого числового кольца, тогда степень расширения $[K : \mathbb{Q}]$ конечна (Докажите!). Как известно из теории Галуа, число вложений $K \hookrightarrow \overline{\mathbb{Q}}$ равно этой степени. Пусть σ — такое вложение. Назовем его *вещественным*, если $\sigma(K) \subset \mathbb{R}$, и *комплексным* — в противном случае. Иначе говоря, σ — комплексное вложение, если и только если, $\bar{\sigma} \neq \sigma$, где $\bar{\sigma}$ — композиция σ с комплексным сопряжением. Мы видим, что комплексные вложения разбиваются на пары сопряженных. Обозначим число таких пар через t. Обозначим число вещественных вложений через s. Тогда $[K : \mathbb{Q}] = s + 2t$.

Факт 4 (Теорема Дирихле о единицах)**.**

$$G_{fr} \approx \mathbb{Z}^{s+t-1}.$$

Задача 39. Выведите из теоремы Дирихле о единицах, что целозамкнутые числовые кольца, в которых группа обратимых элементов конечна, суть $\mathbb{Z}$ и Q_D с $D < 0$.

Задача* 40. Проверьте, что эта теорема выполняется для $\mathbb{Z}[\sqrt{D}]$.

3.4. **Идеалы и однозначность разложения.** Вернемся к нашему примеру из §2.3: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Если бы нам удалось разложить $2 = \alpha\beta$, $3 = \gamma\delta$, $1+\sqrt{-5} = \alpha\gamma$ и $1-\sqrt{-5} = \beta\delta$, то однозначность разложения, возможно, удалось бы спасти. Но согласно задаче 20 таких α, β, γ и δ в $\mathbb{Z}[\sqrt{-5}]$ не существует. Тем не менее, можно представить себе, что найдутся такие *идеальные числа* (что бы это не значило). Что требуется от идеальных чисел? Требуется, чтобы их можно было умножать, и чтобы обычные элементы $\mathbb{Z}[\sqrt{-5}]$ содержались среди идеальных. Оказывается, в качестве таких идеальных чисел можно взять *идеалы кольца*.

Определение 6. Пусть A кольцо (ассоциативное, коммутативное, с единицей), тогда множество $\mathfrak{a} \subset A$ называется *идеалом*, если для любых $a, b \in \mathfrak{a}$ имеем $a + b \in \mathfrak{a}$ и для любых $a \in \mathfrak{a}$, $b \in A$ имеем $ab \in \mathfrak{a}$.

Подчеркнем, что второе условие сильнее, чем просто требование, чтобы множество $\mathfrak{a}$ было замкнуто относительно умножения.

Задача 41. Для любого $a \in A$ множество $(a) = aA = \{ax | x \in A\}$ является идеалом. (Такой идеал называется *главным*.) Более общо, если $a_1, \ldots, a_n \in A$, то множество

$$(a_1, \ldots, a_n) = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n | x_1, \ldots, x_n \in A\}$$

является идеалом.

Таким образом, каждый элемент кольца задает идеал, как мы и хотели. Представление идеала в виде $(a_1, \ldots, a_n)$, разумеется, не единственно: например в $\mathbb{Z}$ имеем $(2, 3) = (1) = (-1)$.

Заметим, что идеалы очень хорошо приспособлены к понятию ассоциированности и делимости:

Задача 42. $(a) = A$ тогда и только тогда, когда a обратим; $(a) = (b)$ тогда и только тогда, когда a и b ассоциированы; $(a) \supset (b)$ тогда и только тогда, когда a делит b.

Мы будем называть элемент кольца *неразложимым*, если его нельзя представить в виде произведения двух необратимых[6].

Задача 43. Докажите, что в кольцах $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{F}[x]$ все идеалы главные (здесь $\mathbb{F}$ — произвольное поле, $\mathbb{F}[x]$ — кольцо многочленов с коэффициентами в $\mathbb{F}$).

---

[6]Мы называли такие гауссовы числа простыми. В более общих кольцах элемент p следует называть простым, если из $p|ab$ следует, что $p|a$ или $p|b$ (см. ниже определение простого идеала). Это свойство сильнее неразложимости — подумайте почему.

Целостное кольцо, в котором все идеалы главные, называется *областью главных идеалов*. С точки зрения обсуждения в начале параграфа, мы видим, что добавление "идеальных чисел" к области главных идеалов не дает ничего нового. Оказывается, это и не нужно — в области главных идеалов единственность разложения на неразложимые множители и так выполняется:

Теорема 10. *В области главных идеалов каждый ненулевой элемент разлагается на неразложимые множители однозначно с точностью до замены на ассоциированные.*

Набросок доказательства. Пусть p — неразложимый элемент кольца A, причем $p|ab$, где $a, b \in A$. Мы докажем, что $p|a$ или $p|b$, из этого уже нетрудно вывести единственность разложения на неразложимые множители. Итак, пусть $p \nmid a$. Рассмотрим идеал $(a, p) = \{ax + py | x, y \in A\}$. По условию он главный, то есть $(a, p) = (c)$ для некоторого $c \in A$. Но тогда $c|a$ и $c|p$, а значит, c обратим. То есть, $(a, p) = (1) = A$. Но тогда $(p) \supset (ab, pb) = (b)$, откуда $p|b$. Доказательство существования мы оставляем читателю. □

Задача* 44. Завершите доказательство теоремы.

Приведенное доказательство единственности очень похоже на обычное доказательство для целых чисел. Мы видим, что идеалы возникают естественным образом при рассмотрении вопросов, связанных с делимостью и разложением на множители.

3.5. **Разложение идеалов на множители.** Оказывается, если числовое кольцо не является областью главных идеалов, то единственность разложения на множители не может выполняться[7]. Тем не менее, имеет место единственность разложения на "идеальные множители", к формулировке которой мы переходим.

Для идеалов $\mathfrak{a}$ и $\mathfrak{b}$ определим их произведение $\mathfrak{ab} = \{a_1b_1 + \ldots + a_kb_k | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$. Ясно, что $\mathfrak{ab}$ — идеал. Очевидно $(a)(b) = (ab)$. Заметим, что $\mathfrak{a} \supset \mathfrak{ab}$.

Идеал $\mathfrak{p} \neq A$ называется *простым*, если $ab \in \mathfrak{p}$ влечет $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Например, идеал $(p) \subset \mathbb{Z}$ прост тогда и только тогда, когда $p = 0$ или $|p|$ простое число.

Факт 5. *Каждый ненулевой идеал в целозамкнутом числовом кольце A однозначно разлагается в произведение простых идеалов. Идеал $\mathfrak{p}$ неразложим в произведение двух идеалов тогда и только тогда, когда он прост. Идеал $\mathfrak{a}$ делит идеал $\mathfrak{b}$*[8]*, тогда и только тогда, когда $\mathfrak{a} \supset \mathfrak{b}$.*

[7] Для более общих колец из единственности разложения не следует, что все идеалы главные. Например, пусть $\mathbb{F}[x, y]$ — кольцо многочленов от двух переменных с коэффициентами в поле $\mathbb{F}$. Можно показать, что в нем разложение на множители единственно, но читатель легко проверит, что идеал (x, y) — не главный.

[8] то есть существует такой идеал $\mathfrak{c}$, что $\mathfrak{b} = \mathfrak{ac}$.

Задача 45. Докажите этот факт для областей главных идеалов.

Задача 46. Выведите из этого факта, что если $\mathfrak{ab} = \mathfrak{ab}'$, то $\mathfrak{b} = \mathfrak{b}'$.

Задача 47. В $\mathbb{Z}[\sqrt{-5}]$ имеем $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$.

Замечание 6. Так же, как форма $x^2 - Dy^2$ разлагается на множители в Q_D, форма $x^n - y^n$ разлагается на линейные множители в $\mathbb{Z}[e^{2\pi i/n}]$ (это кольцо называется *круговым кольцом*). В середине XIX века Лиувиль "доказал" теорему Ферма[9] с использованием круговых колец. Однако, его доказательство опиралось на однозначность разложения в таких кольцах, которая, вообще говоря, не имеет места. Куммер ввел идеалы, чтобы восстановить однозначность разложения, что позволило ему доказать теорему Ферма для многих показателей n (хотя это и не было его главной целью). Таким образом, понятие (и название) идеала происходят именно из задачи о разложении на множители в числовых кольцах. Это потом идеалы стали базовым понятием в алгебре.

3.6. **Норма идеала.** Пусть A — кольцо, $\mathfrak{a}$ — идеал в A. Напомним, что $a \equiv b \pmod{\mathfrak{a}}$ означает $a - b \in \mathfrak{a}$. Читатель знает или легко проверит, что это — отношение эквивалентности на множестве A. Множество классов эквивалентности обозначается через $A/\mathfrak{a}$. Если $\mathfrak{a} \subset \mathfrak{b}$, то $a \equiv b \pmod{\mathfrak{a}}$ влечет $a \equiv b \pmod{\mathfrak{b}}$. Поэтому возникает естественное *сюръективное* отображение

$$A/\mathfrak{a} \to A/\mathfrak{b}.$$

В частности, взяв $\mathfrak{a} = (0)$, получаем отображение $A \to A/\mathfrak{b}$. Это отображение называется *канонической проекцией*, *каноническим гомоморфизмом*, а иногда просто *проекцией*.

Предложение 7. *Пусть A — числовое кольцо, $\mathfrak{a}$ — ненулевой идеал в A. Тогда*
(а) $\mathfrak{a}$ содержит ненулевое целое число.
(б) Множество $A/\mathfrak{a}$ конечно.
(в) Если идеал $\mathfrak{a}$ прост, то он содержит единственное простое целое число.

Доказательство. (а). Пусть $x \in \mathfrak{a}$. Тогда $x \in \overline{\mathbb{Z}}$, так что x удовлетворяет уравнению

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \qquad a_{n-1}, \ldots, a_0 \in \mathbb{Z}.$$

Рассмотрим такое уравнение наименьшей степени, тогда $a_0 \neq 0$. Но $a_0 \in \mathfrak{a}$.
(б) Пусть a_0 — как в предыдущем пункте, тогда $(a_0) \subset \mathfrak{a}$ и каноническая проекция

$$A/(a_0) \to A/\mathfrak{a}$$

сюръективно, так что достаточно доказать, что $A/(a_0)$ конечно. Это следует из предложения 6(а).

[9] Уравнение $x^n + y^n = z^n$ не имеет решений в ненулевых целых числах при $n > 2$. Доказательство было получено лишь в конце XX века.

(в) Предположим теперь, что $\mathfrak{a}$ — простой идеал. Пусть a_0 такое же, как и раньше. Разложим его в произведение простых целых чисел: $a_0 = \pm p_1 \dots p_l$. Так как $\mathfrak{a}$ прост, одно из чисел p_i лежит в $\mathfrak{a}$. Осталось доказать единственность. Ясно, что $\mathfrak{a} \cap \mathbb{Z}$ — идеал в $\mathbb{Z}$. Если он содержит два простых числа, то этот идеал совпадает с $\mathbb{Z}$. Но тогда $\mathfrak{a} = A$. □

Число элементов в $A/\mathfrak{a}$ называется *нормой идеала*. Обозначение: $N\mathfrak{a}$.

Факт 6. $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}\,N\mathfrak{b}$.

3.7. **Дзета-функция Дедекинда.** Пусть A — числовое кольцо. Определим *дзета-функцию Дедекинда*:

$$\zeta_A(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{25}$$

где a_n — число идеалов с нормой n. Как и в ранее рассмотренных случаях, этот ряд сходится при $\operatorname{Re} s > 1$ — это должно быть ясно из доказательства теоремы 11, по крайней мере, для квадратичных колец. Аналогично теореме 9 доказывается, что

$$\zeta_A(s) = \prod_{\mathfrak{p} \subset A} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1}, \tag{26}$$

где произведение берется по ненулевым простым идеалам. CONVERGENCE, CONTINUATION, FUNCTIONAL EQUATION.

Ясно, что $\zeta_{Q_D}(s)$ является обобщением дзета-функции кольца гауссовых чисел. Почему мы берем сумму по идеалам, а не по элементам? Дело в том, что для произведения Эйлера нам необходима теорема об однозначности разложения, которая выполняется для идеалов, а не для элементов кольца.

3.8. **Идеалы в Q_D.** Обозначим множество ненулевых простых идеалов в Q_D через $\operatorname{Max}(Q_D)$. Мы получили отображение $\operatorname{Max}(Q_D) \to P$, где P, как и раньше, множество простых целых чисел. Легко видеть, что это отображение сюръективно, изучим его слои (то есть простые идеалы в Q_D, содержащие данное простое.).

Напомним, что если $\alpha = a + b\sqrt{D} \in Q_D$, то $\bar{\alpha} = a - b\sqrt{D}$. Пусть $\mathfrak{a} \subset Q_D$ — идеал. Положим

$$\bar{\mathfrak{a}} = \{\bar{a} | \, a \in \mathfrak{a}\}.$$

Введем еще обозначение

$$D' := \begin{cases} D \text{ если } D \equiv 1 \pmod 4 \\ 2D \text{ если } D \not\equiv 1 \pmod 4). \end{cases}$$

Предложение 8. (*a*) *Если* $p|D'$, *то* $(p) = \mathfrak{p}^2$, *где* $\mathfrak{p} = \bar{\mathfrak{p}}$ *—единственный простой идеал, содержащий* p. *При этом* $\mathfrak{p} = (p, \sqrt{D})$, *если* $p|D$ *и* $\mathfrak{p} = (2, 1 + \sqrt{D})$, *если* $p = 2$ *и* D *нечетно.*

(*б*) *Если* $p \nmid 2D$ *и найдется такое* n, *что* $p|n^2 - D$, *то* $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, *где* $\mathfrak{p} = (p, n + \sqrt{D})$, *при этом* $\mathfrak{p}$ *и* $\bar{\mathfrak{p}}$ *различны и это в точности простые идеалы, содержащие* p.

(*в*) *В оставшемся случае,* (p) *— простой идеал в* Q_D *и это единственный простой идеал, содержащий* p.

Доказательство. Заметим, сначала, что если норма идеала является простым числом, то этот идеал не может быть разложен в нетривиальное произведение в силу факта 6, значит он прост в силу факта 5. Поэтому, если $(p) = \mathfrak{p}\mathfrak{q}$, где $\mathfrak{p} \neq (1) \neq \mathfrak{q}$, то это разложение идеала (p) в произведение простых. Из этого легко вывести утверждение пункта (а). (Нужно еще заметить, что $\bar{\mathfrak{p}}|\overline{(p)} = \mathfrak{p}^2$, следовательно $\mathfrak{p} = \bar{\mathfrak{p}}$).

(б) Надо заметить, что

$$(p) \subset (p, n - \sqrt{D})(p, n + \sqrt{D}) \subset (p^2, 2pn, 2p\sqrt{D}, n^2 - D) = (p)$$

(проверка последнего равенства требует некоторой аккуратности, если $p = 2$).

(в) Если (p) делится на нединичный идеал $\mathfrak{p}$, то $p \in \mathfrak{p}$. Если $(p) \neq \mathfrak{p}$, то p содержит элемент $a + b\sqrt{D}$ не делящийся на p. Нетрудно видеть, что b не может делиться на p (иначе $a \in \mathfrak{p}$ и $\mathfrak{p} = (1)$). Поэтому некоторая целая линейная комбинация p и $a + b\sqrt{D}$ имеет вид $n + \sqrt{D}$. Тогда $n^2 - D \in \mathfrak{p}$ и, значит, p делит $n^2 - D$. □

Задача 48. Докажите, что для любого идеала $\mathfrak{a} \subset Q_D$ идеал $\mathfrak{a}\bar{\mathfrak{a}}$ — является главным идеалом, порожденным целым числом $N\mathfrak{a}$.

Задача 49. Идеал (2) разложим в Q_D тогда и только тогда, когда $D \not\equiv 5 \pmod 8$.

На предыдущей лекции мы выяснили, какие целые числа являются нормами гауссовых чисел. Теперь мы можем ответить на аналогичный вопрос для Q_D, но не для элементов Q_D, а для идеалов.

Задача 50. Пусть D свободно от квадратов и $D \not\equiv 5 \pmod 8$. Число $n \in \mathbb{Z}_+$ является нормой идеала в Q_D тогда и только тогда, когда каждое простое p такое, что сравнение $x^2 \equiv D \pmod p$ не имеет решений входит в n в четной степени. При $D \equiv 5 \pmod 8$ нужно еще потребовать, чтобы $p = 2$ входило в четной степени. (Сравните с теоремой 5.)

3.9. **Дзета-функция квадратичного кольца.** Мы хотим получить формулу для дзета-функции ζ_{Q_D}, аналогичную (22). Для этого мы построим мультипликативный характер $\chi_D : \mathbb{Z} \to \{\pm 1\}$. Достаточно определить его значение для простых чисел. Для $p > 2$, $p \nmid D$, определим $\chi_D(p) = \pm 1$ в зависимости от того, существует ли такое n, что $p|n^2 - D$. Для $p > 2$, $p|D$ положим $\chi_D(p) = 0$. Иными словами, число решений уравнения $x^2 = D$ в $\mathbb{F}_p$ равно $\chi_D(p) + 1$. Осталось определить $\chi_D(2)$:

$$\chi_D(2) = \begin{cases} -1 \text{ при } D \equiv 5 \pmod 8, \\ 1 \text{ при } D \equiv 1 \pmod 8, \\ 0 \text{ при } D \equiv 2, 3, 6 \text{ или } 7 \pmod 8. \end{cases}$$

Предложение 9.

$$\zeta_{Q_D}(s) = \zeta(s) L(s, \chi_D).$$

Доказательство аналогично выводу формулы (22). Единственное изменение состоит в том, что вместо теоремы 8 нужно использовать предложение 8.

Замечание 7. Оказывается, χ_D — характер Дирихле. Точнее, $\chi_D(m)$ зависит только от остатка при делении m на $4D$. Это — одна из форм знаменитого закона взаимности Гаусса. Из него следует, что достаточно вычислить χ_D в конечном числе целых чисел. К сожалению, у нас нет времени останавливаться на законах взаимности.

3.10. **Формула для числа классов.** Как и в теореме 6, при помощи дзета-функции можно получить формулу для числа представлений целого числа n в виде нормы идеала. Но, как мы сейчас увидим, дзета-функция несет гораздо более важную информацию о числовом кольце.

Назовем идеалы $\mathfrak{a}, \mathfrak{b} \subset A$ *эквивалентными*, если найдутся такие $a, b \in A \setminus 0$, что $(a)\mathfrak{b} = (b)\mathfrak{a}$. Ясно, что это — отношение эквивалентности. Обозначим число классов эквивалентности через h. Оказывается, h всегда конечно. Оно называется *числом классов кольца* A.

Задача 51. Докажите, что идеал $\mathfrak{a}$ главный тогда и только тогда, когда он эквивалентен идеалу (1). Выведите, что A — область главных идеалов тогда и только тогда, когда $h = 1$.

Мы видим, что h — важная характеристика кольца A. Оказывается, ее можно выразить через дзета-функцию.

Начнем со случая мнимого квадратичного кольца.

Теорема 11. *Для Q_D, где $D < 0$:*

$$\lim_{s \to 1} (s-1) \zeta_{Q_D}(s) = \begin{cases} \frac{2\pi h}{w\sqrt{|D|}} & \text{если } D \equiv 1 \pmod 4 \\ \frac{\pi h}{w\sqrt{|D|}} & \text{если } D \not\equiv 1 \pmod 4, \end{cases}$$

где w — число обратимых элементов (то есть $w = 4$ при $D = -1$, $w = 6$, если $D = -3$, и $w = 2$ — в остальных случаях).

Заметим, что в левой части стоит неопределенность типа $0 \cdot \infty$. Ее предел называется *вычетом дзета-функции в единице* (см. Предложение 1).

Набросок доказательства. Пусть $D \not\equiv 1 \pmod 4$ (второй случай аналогичен и мы оставим его читателю). Выберем по представителю из каждого класса идеалов, обозначим соответствующие классы через $\mathfrak{a}_1,\ldots,\ \mathfrak{a}_h$. Тогда

$$\zeta_{Q_D}(s) = \sum_{j=1}^{h} \sum_{\mathfrak{a}\sim\mathfrak{a}_j} \frac{1}{N\mathfrak{a}^s},$$

где $\sim$ обозначает эквивалентность идеалов. Достаточно доказать, что для каждого j

$$\lim_{s\to1}(s-1)\left(\sum_{\mathfrak{a}\sim\mathfrak{a}_j} \frac{1}{N\mathfrak{a}^s}\right) = \frac{\pi}{w\sqrt{|D|}}. \tag{27}$$

Зафиксируем j, и пусть $\alpha \in \mathfrak{a}_j$. Тогда $(\alpha) \subset \mathfrak{a}_j$, и в силу факта 5 найдется такой идеал $\mathfrak{b}$, что $\mathfrak{a}_j\mathfrak{b} = (\alpha)$.

Задача 52. Умножение на $\mathfrak{b}$ задает биекцию между идеалами, эквивалентными $\mathfrak{a}_j$, и *главными* идеалами, делящимися на $\mathfrak{b}$.

Доказательство. Пусть $\mathfrak{a} \sim \mathfrak{a}_j$. Докажем, что $\mathfrak{a}\mathfrak{b}$ — главный идеал. Найдутся такие $\beta, \beta' \in Q_D$, что $(\beta)\mathfrak{a}_j = (\beta')\mathfrak{a}$. Но тогда $(\beta')\mathfrak{a}\mathfrak{b} = (\beta\alpha)$, и остается воспользоваться результатом задачи 51.

Итак, умножение на $\mathfrak{b}$ отображает множество идеалов, эквивалентных $\mathfrak{a}_j$, в множество главных идеалов, делящихся на $\mathfrak{b}$. Это отображение инъективно в силу факта 5. Докажем его сюръективность: пусть (β) — главный идеал, делящийся на $\mathfrak{b}$. Тогда $(\beta) = \mathfrak{b}\mathfrak{a}$. И нам нужно доказать, что $\mathfrak{a} \sim \mathfrak{a}_j$. Но

$$\mathfrak{a}(\alpha) = \mathfrak{a}\mathfrak{a}_j\mathfrak{b} = \mathfrak{a}_j(\beta).$$

$\square$

Из результата задачи следует, что мы можем переписать сумму в (27) в виде

$$N\mathfrak{b}^s \sum_{\mathfrak{b}\supset\mathfrak{a}} \frac{1}{N\mathfrak{a}^s},$$

где суммирование ведется по *главным* идеалам, делящимся на $\mathfrak{b}$ (то есть содержащимся в $\mathfrak{b}$). Но каждый такой идеал можно записать в виде (α) ровно w способами (потому что каждый ненулевой элемент в Q_D ассоциирован ровно с w другими). Поэтому мы можем переписать эту сумму в виде

$$\frac{N\mathfrak{b}^s}{w} \sum_{\alpha\in\mathfrak{b}} \frac{1}{N(\alpha)^s},$$

где суммирование ведется по ненулевым элементам Q_D, содержащимся в $\mathfrak{b}$.

Задача 53. Идеал $\mathfrak{b}$ изоморфен $\mathbb{Z} \times \mathbb{Z}$ как абелева группа. Более того, эта группа является *решеткой* в $\mathbb{C}$, то есть любые ее образующие α, β линейно независимы над $\mathbb{R}$.

Таким образом, если α и β — образующие идеала $\mathfrak{b}$, то

$$\sum_{\alpha\in\mathfrak{b}} \frac{1}{N(\alpha)^s} = \sum_{\alpha\in\mathfrak{b}} \frac{1}{N\alpha^s} = \sum_{(k,l)\neq(0,0)} \frac{1}{|k\gamma + l\beta|^{2s}}.$$

Итак, левая часть (27) равна

$$\lim_{s\to1}(s-1)\left(\frac{N\mathfrak{b}^s}{w}\sum_{\alpha\in\mathfrak{b}}\frac{1}{N\alpha^s}\right) = \frac{N\mathfrak{b}}{w}\lim_{s\to1}(s-1)\left(\sum_{(k,l)\neq(0,0)}\frac{1}{|k\gamma+l\beta|^{2s}}\right). \tag{28}$$

Мы утверждаем, что мы можем заменить сумму на некоторый интеграл. Для этого построим параллелограмм T на векторах γ и β. Пусть Δ — его площадь. Мы отождествляем $\mathbb{C}$ с $\mathbb{R}^2$.

Лемма 4. *При* $2 > s > 3/4$ *имеем*

$$\left|\Delta\sum_{(k,l)\neq(0,0)}|k\gamma+l\beta|^{-2s} - \int_{\{x^2+y^2\geq1\}}(x^2+y^2)^{-s}\,dx\,dy\right| < C,$$

где C *не зависит от* s *(но зависит от* γ *и* β*).*

Мы докажем эту лемму ниже. Из нее следует, что

$$\lim_{s\to1}(s-1)\left(\sum_{(k,l)\neq(0,0)}|k\gamma+l\beta|^{-2s}\right) = \frac{1}{\Delta}\lim_{s\to1}(s-1)\left(\int_{\{x^2+y^2\geq1\}}(x^2+y^2)^{-s}\,dx\,dy\right) = \frac{\pi}{\Delta}.$$

Последнее равенство читатель докажет сам, перейдя к полярным координатам. Итак, выражение в (28) равно $\frac{\pi N\mathfrak{b}}{w\Delta}$, и для доказательства равенства (27) нам осталось проверить, что $\Delta = N\mathfrak{b}\sqrt{|D|}$ (конечно, еще нужно доказать предыдущую лемму).

Решетка Q_D порождена векторами $e_1 = 1$ и $e_2 = i\sqrt{|D|}$, где $i = \sqrt{-1}$. Пусть $\gamma = a_{11}e_1 + a_{21}e_2$, $\beta = a_{12}e_1 + a_{22}e_2$. Тогда порядок факторгруппы $Q_D/\mathfrak{b}$ равен абсолютной величине соответствующего определителя:

$$N\mathfrak{b} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}.$$

С другой стороны, параллелограмм T построен на векторах $\gamma = a_{11} + a_{21}\sqrt{|D|}i$ и $\beta = a_{12} + a_{22}\sqrt{|D|}i$, и его площадь равна абсолютной величине определителя

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21}\sqrt{|D|} & a_{22}\sqrt{|D|} \end{vmatrix}.$$

Но эти определители отличаются в $\sqrt{|D|}$ раз и мы получаем требуемую формулу.

Доказательство леммы 4. Обозначим через $T_{k,l}$ параллелограмм, получающийся из T сдвигом на $k\gamma + l\beta$. Тогда $\mathbb{R}^2 = \cup_{k,l\in\mathbb{Z}} T_{k,l}$. Пусть M — множество всех пар целых чисел, кроме $(0,0)$, $(-1,0)$, $(0,-1)$ и $(-1,-1)$. Пусть $\Omega = \cup_{(k,l)\in M} T_{k,l}$, то есть Ω — объединение тех параллелограммов $T_{k,l}$, которые не содержат начало координат. Пусть $(k,l) \in M$, обозначим через m_{kl} минимум функции $|z|^2 = x^2 + y^2$ на $T_{k,l}$. Тогда, для $z \in T_{k,l}$ имеем

$$\left||k\gamma + l\beta|^{-2s} - |z|^{-2s}\right| \le 2s m_{kl}^{-1-2s}$$

Это следует из теоремы Лагранжа: для любых чисел $x_1, x_2 \in \mathbb{R}_+$ выполняется неравенство $|x_1^{-2s} - x_2^{-2s}| \le 2s\xi^{-1-2s}$, где ξ — минимум из x_1 и x_2. Отсюда,

$$\left|\Delta|k\gamma + l\beta|^{-2s} - \int_{T_{k,l}} (x^2+y^2)^{-s}\,dx\,dy\right| \le 2s\Delta m_{kl}^{-1-2s} \le \mathrm{const}\cdot m_{kl}^{-5/2}.$$

Задача 54. Докажите, что для некоторой константы C, $m_{kl} > C\sqrt{k^2+l^2}$. Выведите, что ряд $\sum_{k,l} m_{kl}^{-5/2}$ сходится.

Из этой леммы следует, что выражение

$$\left|\Delta \sum_{(k,l)\in M} |k\gamma + l\beta|^{-2s} - \int_{\Omega} (x^2+y^2)^{-s}\,dx\,dy\right|$$

ограничено константой, не зависящей от s. Отсюда уже несложно вывести утверждение леммы. □

Доказательство теоремы закончено. □

Задача 55. Выведите из этой теоремы, что разложение на множители в $\mathbb{Z}[i]$ однозначно.

Задача 56. Докажите, что

$$\lim_{s\to 1} (s-1)\zeta_{Q_D}(s) = L(1, \chi_D).$$

Лекция 4. Диофантовы уравнения

Напомним, что $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ обозначает поле из p — элементов. Про его элементы можно думать, как про остатки от деления на p. Рассмотрим общее диофантово уравнение

$$f(x_1, \ldots, x_n) = 0,$$

где f —многочлен с целыми коэффициентами. Приводя его по модулю p, получаем уравнение $f_p(x_1, \ldots, x_n) = 0$, где f_p — многочлен с коэффициентами в

$\mathbb{F}_p$. Если это уравнение не имеет решений, то и исходное уравнение не имеет решений.

С другой стороны, уравнение *всегда* имеет решения в некотором конечном поле, содержащем $\mathbb{F}_p$, и можно получить интересную информацию об уравнение, рассматривая решения в таких полях. Проведем такую аналогию: полезно рассматривать комплексные решения вещественного уравнения, например, про x^2+y^2+1 лучше думать как про мнимую окружность, чем как про пустое множество. Мы напомним теорию конечных полей.

4.1. **Конечные поля.** Для любых p и n существует единственное с точностью до изоморфизма поле из p^n элементов. Поле из p^n элементов содержит подполе из q^m элементов тогда и только тогда, когда $p=q$ и m делит n.

4.2. **Диофантовы уравнения от одной переменной и числовые поля.** Пусть $f(x)\in\mathbb{Z}[x]$ — многочлен от одной переменной с целыми коэффициентами. Разложим многочлен $f_p(x)\in\mathbb{F}_p[x]$ на неприводимые множители:

$$f_p(x)=h_1^{a_1}\dots h_n^{a_n}$$

Предложение 10. *Количество решений уравнения $f_p(x)=0$ в $\mathbb{F}_{p^k}$ равно сумме тех d_i, для которых $d_i|n$:*

$$\sum_{\substack{1\le i\le n\\ d_i|n}} d_i. \tag{29}$$

Определение 7. Дзета-функцией уравнения $f_p(x)$ называется функция

$$Z_{f_p}(t)=\prod_{i=1}^{n}\left(1-t^{\deg h_i}\right)^{-1}.$$

Дзета-функцией уравнения $f(x)=0$ называется произведение

$$\zeta_f(s)=\prod_p Z_{f_p}(p^{-s}). \tag{30}$$

Пример 1. Рассмотрим диофантово уравнение $x^2-D=0$. Предположим, что D свободно от квадратов и $D\not\equiv 1 \pmod 4$. Нетрудно проверить, что

$$\zeta_{Q_D}(s)=\zeta_{x^2-D}(s).$$

Предложение 11.

$$Z_{f_p}(t)=\exp\left(\sum_{k=1}^{\infty}\frac{N_k t^k}{k}\right). \tag{31}$$

Мы видим, что дзета-функция Z_{f_p} тесно связана с производящей функцией для числа решенй уравнения $f_p=0$ в $\mathbb{F}_{p^k}$.

Доказательство. Положим $d_i = \deg h_i$. Мы можем переписать (29) как равенство производящих функций:

$$\sum_{k=1}^{\infty} N_k t^k = \sum_{i=1}^{n} d_i \sum_{k=1}^{\infty} t^{kd_i}.$$

Деля на t, и используя формулу для суммы геометрической прогрессии, получаем

$$\sum_{k=1}^{\infty} N_k t^{k-1} = \sum_{i=1}^{n} \frac{d_i t^{d_i - 1}}{1 - t^{d_i}}.$$

Взяв интеграл от обеих частей, получаем требуемое равенство. □

Теорема 12. *Пусть коэффициент многочлена f при старшем члене равен 1. Рассмотрим кольцо $A = \mathbb{Z}[x]/(f(x))$. Это кольцо изоморфно числовому кольцу причем $\zeta_A = \zeta_f$.*

4.3. **Диофантовы уравнения от многих переменных.** Рассмотрим диофантово уравнение $f(x_1, \ldots, x_n) = 0$, пусть $f_p(x_1, \ldots, x_n)$ редукция f по модулю p. Определим Z_{f_p} формулой (31), где N_k — число решений уравнения $f_p(x_1, \ldots, x_n)$ в $\mathbb{F}_{p^k}$. Определим $\zeta_f(s)$ формулой (30).

Пример 2. Пусть уравнение имеет вид $f(x, y) = y - x = 0$. Тогда для каждого x найдется единственное y. Ясно, что $N_k = p^k$, и нетрудно видеть, что $Z_{f_p}(t) = (1 - pt)^{-1}$. Значит

$$\zeta_f(s) = \prod_p (1 - p^{1-s})^{-1} = \zeta(s - 1).$$

Задача 57. Докажите, что дла $f(x) = x^2 - y^2 - 1$, имеем

$$Z_{f_p} B(t) = \frac{1 - t}{1 - pt}.$$

и $\zeta_f(s) = \zeta(s - 1)/\zeta(s)$.

Задача 58. Вычислите локальную и глобальную дзета-функцию для

$$f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 - x_3^2 - x_4^2.$$

Задача 59. Определите локальную и глобальную дзета-функцию для систем уравнений и вычислите их для системы линейных уравнений.

4.4. **Гипотезы Вейля–1.** Зафиксируем простое число p и рассмотрим уравнение $f(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ (или систему уравнений). Пусть $Z_f(t)$ соответствующая локальная дзета-функция. В 1949 году Вейль сформулировал набор гипотез по $Z_f(t)$. Попытки доказать эти гипотезы во многом определяли развитие алгебраической геометрии на протяжении нескольких десятилетий. Вот самая простая из гипотез:

Факт 7. *$Z_f(t)$ рациональная функция (т.е. отношение двух многочленов).*

Это утверждение было доказано Дворком в 1960-м году. На следующем занятии мы сформулируем гораздо более точные гипотезы в случае многочлена от двух переменных.

Задача 60. Положим $Y_f(t) = \sum_{k=1}^{\infty} N_k t^{k-1}$. Докажите, что Z_f рациональная функция тогда и только тогда, когда Y_f рациональна, степень числителя не превосходит степени знаменателя и Y_f не имеет кратных корней и/или полюсов.

Приложение A. Комплексный анализ

Теорема 13. *Пусть f и g голоморфные функции на* связном *открытом множестве U. Пусть $A = \{z \in U : f(z) = g(z)\}$. Если Множество A имеет предельную точку в U, то функции f и g совпадают на U.*

Набросок доказательства. Пусть $h = f - g$, тогда h обращается в ноль на A. По условию мы можем выбрать последовательность различных точек $z_n \in A$ так, чтобы $\lim_{n\to\infty} z_n \in A$. Обозначим этот предел через z. Так как функция аналитична, мы можем разложить ее в ряд (15) в окрестности точки z. Пусть этот ряд ненулевой. Пусть a_k — первый ненулевой коэффициент ряда, тогда

$$f(w) = a_k(w-z)^k(1 + b_1(w-z) + b_2(w-z)^2 + \ldots).$$

Так как $f(z_n) = 0$, последний множитель обращается в ноль в z_n. Но тогда, по соображениям непрерывности, он обращается в ноль и в z, что невозможно. Это противоречие показывает, что наш ряд нулевой, а значит, функция нулевая в окрестности точки z.

Обозначим через B множество таких точек $z \in U$, что f обращается в нуль в окрестности z. Мы доказали, что B не пусто. Из предыдущего рассуждения также следует, что это множество замкнуто. Но оно, очевидно, открыто. Так как U связно, получаем $U = B$. □

Указания к задачам

Задача 2. Сравните a_n с $\int_1^n \frac{dx}{x}$.

Задача 7.
$$(\ln(\sin x))' = \cot x = i + \frac{2i}{e^{2ix}-1},$$
где $i=\sqrt{-1}$.

Задача 7. Вычислите $\sum_{k=0}^{\infty} S_k(n)\frac{t^k}{k!}$.

Задача 10. $|n^{-s}| = n^{-\operatorname{Re} s}$.

Задача 13. $\Gamma(s)$ не обращается в ноль при $\operatorname{Re} s > 0$.

Задача 20. Изобразите на комплексной плоскости множество гауссовых чисел, которые делятся на β.

Задача 20. Используйте мультипликативность нормы $N(a+b\sqrt{-5}) = a^2+5b^2$.

Задача 29. Можно считать, что $a_n = 0$. Предположите, что $b_k \neq 0$ и k — наименьшее с таким свойством. Разделите ряд Дирихле на k^{-s} и перейдите к пределу.

Задача 29. Простые целые числа в интервале $[1;40]$ остаются простыми в этом кольце.

Задача 34. Если бы $\overline{\mathbb{Z}}$ было числовым кольцом, то поле алгебраических чисел $\overline{\mathbb{Q}}$ было бы конечным расширением поля $\mathbb{Q}$.

Задача 40. Для любой конечно-порожденной группы G, G_{tor} есть множество элементов конечного порядка. Далее, элементы G_{tor} — комплексные числа. Рассмотрите элемент с наименьшим аргументом.

Задача 43. Используйте теорию уравнения Пелля.

Задача 43. В случае $\mathbb{Z}[i]$ рассмотрите элемент идеала с наименьшей нормой и используйте задачу 18.

Задача 45. Пусть $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_n \subset \ldots$ — бесконечная цепочка вложенных друг в друга идеалов в области главных идеалов A. Докажите, что она стабилизируется, то есть, начиная с некоторого места, все идеалы совпадают.

Задача 47. используйте теорему 10.

Задача 53. Используйте задачу 45.

Задача 53. Q_D — решетка в $\mathbb{C}$.

Задача 56. Для почти всех пар (k,l), $m_{kl} > (|k\gamma + l\beta| - D)^2$, где D — диаметр параллелограмма T.

Задача 56. Проверьте, что для соответствующей L-функции $L(1,\chi) = \pi/4$.