

СБОРНИК ЗАДАЧ

по теории чисел

предназначено для семинаров
по курсу «Теория чисел»

кафедра теории чисел
механико-математического факультета
МГУ имени М. В. Ломоносова

3 декабря 2015 г.

Оглавление

Оглавление	i
Некоторые обозначения	iii
1 Аналитическая теория чисел: элементарные методы	1
1.1 Вокруг оценок Чебышёва	1
1.2 Это было давно и неправда	4
1.3 Оценки для арифметических функций	5
1.4 Суммы значений арифметических функций: начало	7
1.5 Разное	8
2 Вокруг дзета-функции Римана и асимптотического закона	9
2.1 Ряды Дирихле	9
2.2 Различные асимптотики	13
2.3 Числа Бернулли и формула Эйлера–Маклорена	15
3 Суммы с функцией Мёбиуса	19
3.1 Тауберовы теоремы	21
4 Характеры	22
4.1 Дела давно минувших дней...	22
4.2 Строение группы $(\mathbb{Z}/m\mathbb{Z})^*$	23
4.3 Характеры	25
4.4 L-функции и теорема Дирихле о простых числах	26
4.5 Суммы с характерами	28
5 Диофантовы приближения и геометрия чисел	37
5.1 Диофантовы приближения	37
5.2 Решётки	40
5.3 Ряды Фарея	42
6 Цепные дроби	44
7 Алгебраические числа	45
7.1 Неприводимые многочлены	45
7.2 Конечные расширения	46
7.3 Целые алгебраические числа	48

7.4	Вокруг основной теоремы арифметики	49
7.5	Круговые поля	53
8	Иррациональные и трансцендентные числа	58

Некоторые обозначения

$[x]$ — целая часть числа x , $\{x\} = x - [x]$ — дробная часть числа x .

$\nu_p(n)$ — кратность вхождения простого числа p в каноническое разложение на простые множители числа n .

$\pi(x) = \sum_{p \leq x} 1$ — количество простых чисел, не превосходящих x .

$\theta(x) = \sum_{p \leq x} \ln p$.

$\Lambda(n)$ — функция Мангольдта:

$$\Lambda(n) = \begin{cases} \ln p, & n = p^\alpha, \\ 0 & \text{иначе;} \end{cases}$$

$\psi(x) = \sum_{n \leq x} \Lambda(n)$.

$\mu(n)$ — функция Мёбиуса:

$$\mu(n) = \begin{cases} 0, & p^2 \mid n, \\ (-1)^s, & n = p_1 \cdots p_s, p_1 < \cdots < p_s; \end{cases}$$

$M(x) = \sum_{n \leq x} \mu(n)$.

$\varphi(n)$ — функция Эйлера.

$\tau(n) = \sum_{d \mid n} 1$ — количество делителей числа n .

$\sigma(n) = \sum_{d \mid n} d$ — сумма делителей числа n .

$\omega(n) = \sum_{p \mid n} 1$ — количество различных простых делителей числа n , $\Omega(n) = \sum_{p \mid n} \nu_p(n)$ — количество простых делителей числа n с учётом кратностей.

$\zeta(s)$ — дзета-функция Римана, $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, $\operatorname{Re} s > 1$.

$L(s, \chi)$ — L-функция Дирихле, $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$, $\operatorname{Re} s > 1$.

\mathbb{A} — поле всех алгебраических чисел, $\mathbb{Z}_{\mathbb{A}}$ — кольцо всех целых алгебраических чисел. Если K — конечное расширение \mathbb{Q} , то $\mathbb{Z}_K = \mathbb{Z}_{\mathbb{A}} \cap K$ — кольцо целых чисел (максимальный порядок) поля K .

Глава 1

Аналитическая теория чисел: элементарные методы

1.1 Вокруг оценок Чебышёва

Рассмотрим функции $\pi(x) = \sum_{p \leq x} 1$, $\theta(x) = \sum_{p \leq x} \ln p$, $\psi(x) = \sum_{p^\alpha \leq x} \ln p$. (Если не сказано противное, то $x \in [1, +\infty)$, $n \in \mathbb{N}$, p – простое число; в формуле p^α подразумевается $\alpha \in \mathbb{N}$.)

Задача 1.1. Доказать, что для функции $\psi(x)$ справедливы представления

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\ln x}{\ln p} \right\rfloor \ln p = \ln[1, 2, \dots, [x]] = \sum_{n \leq x} \Lambda(n),$$

где $[a_1, \dots, a_n]$ – наименьшее общее кратное чисел a_1, \dots, a_n , $\Lambda(n)$ – функция Мангольда, т. е.

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

Задача 1.2. Доказать равенство $\sum_{d|n} \Lambda(d) = \ln n$.

Задача 1.3. Доказать равенства:

- 1) $\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \dots$, причём количество ненулевых слагаемых в сумме справа равно $[\ln x / \ln 2]$;
- 2) $\ln n! = \psi(n) + \psi(n/2) + \psi(n/3) + \dots$. (Указание. Использовать задачу 1.2.)

Задача 1.4. Используя каноническое разложение на простые множители числа $n!$ и формулу Стирлинга, доказать равенства:

- 1) $\sum_{p \leq n} \left\lfloor \frac{n}{p} \right\rfloor \ln p + \sum_{p \leq n} \left\lfloor \frac{n}{p^2} \right\rfloor \ln p + \sum_{p \leq n} \left\lfloor \frac{n}{p^3} \right\rfloor \ln p + \dots = n \ln n + O(n)$;
- 2) $\sum_{p \leq n} \left\lfloor \frac{n}{p} \right\rfloor \ln p = n \ln n + O(n)$.

Задача 1.5. Доказать оценки:

$$1) \sum_{p \leq 2n} \left(\left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \right) \ln p = O(n);$$

$$2) \sum_{n < p \leq 2n} \ln p = O(n);$$

$$3) \theta(x) = O(x).$$

Задача 1.6. Используя задачи 1.4 и 1.5, доказать равенство

$$\sum_{p \leq x} \frac{\ln p}{p} = \ln x + O(1).$$

(Уточнение см. в задаче 2.15.)

Задача 1.7. Доказать, что существуют постоянные $C_i > 0$, такие что справедливы утверждения:

1) Для любых $x \geq 1$, $a \geq 1$ выполнено неравенство

$$\left| \sum_{x < p \leq ax} \frac{\ln p}{p} - \ln a \right| \leq C_1.$$

2) $\theta(x) \geq C_2 x$, $x \geq 2$.

3) Для любого $x \geq 1$ интервал $(x, C_3 x)$ содержит простое число.

Задача 1.8 (оценки Чебышёва). Доказать, что существуют положительные постоянные A_i, B_i , такие что справедливы неравенства:

$$1) A_1 x \leq \theta(x) \leq B_1 x, \quad x \geq 2;$$

$$2) A_2 x \leq \psi(x) \leq B_2 x, \quad x \geq 2;$$

$$3) A_3 \frac{x}{\ln x} \leq \pi(x) \leq B_3 \frac{x}{\ln x}, \quad x \geq 2;$$

$$4) A_4 n \ln n \leq p_n \leq B_4 n \ln n, \quad n \geq 2, \text{ где } p_n - n\text{-е простое число (т. е. } p_1 = 2, p_2 = 3, \dots).$$

Задача 1.9. Исследовать на сходимость ряд $\sum_{p \geq 3} \frac{1}{p^a (\ln p)^b (\ln \ln p)^c}$, $a, b, c \in \mathbb{R}$.

Задача 1.10 (преобразование Абеля в интегральной форме).

1) Пусть a_n — комплексные числа, $g: [1, +\infty) \rightarrow \mathbb{C}$ — непрерывно дифференцируемая функция, $A(x) = \sum_{n \leq x} a_n$. Доказать, что

$$\sum_{n \leq x} a_n g(n) = A(x)g(x) - \int_1^x A(u)g'(u) du.$$

- 2) Более общо, пусть $a < b$ — вещественные числа, a_n — комплексные числа для (целых) $n \in (a, b]$, $g: (a, b] \rightarrow \mathbb{C}$ — непрерывно дифференцируемая функция, $A(x) = \sum_{a < n \leq x} a_n$. Доказать, что

$$\sum_{a < n \leq b} a_n g(n) = A(b)g(b) - \int_a^b A(x)g'(x) dx.$$

Задача 1.11. Используя преобразование Абеля, доказать равенства (γ, c_1, c_2 — некоторые постоянные):

- 1) $\sum_{n \leq x} \ln n = x \ln x - x + O(\ln x)$, $x \geq 2$;
- 2) $\sum_{n \leq x} \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right)$;
- 3) $\sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + c_1 + O\left(\frac{1}{\sqrt{x}}\right)$;
- 4) если $a \in (0, 1)$, то $\sum_{n \leq x} \frac{1}{n^a} = \frac{x^{1-a}}{1-a} - a \int_0^{+\infty} \frac{\{u\} du}{u^{a+1}} + O(x^{-a})$, причём постоянная в символе Ландау $O(\cdot)$ не зависит от a ;
- 5) $\sum_{2 \leq n \leq x} \frac{1}{n \ln n} = \ln \ln x + c_2 + O\left(\frac{1}{x \ln x}\right)$, $x \geq 2$.

Задача 1.12. Используя задачу 1.6 и преобразование Абеля, доказать, что для некоторой постоянной c_0 справедливо равенство

$$\sum_{p \leq x} \frac{1}{p} = \ln \ln x + c_0 + O\left(\frac{1}{\ln x}\right), \quad x \geq 2.$$

Задача 1.13. Доказать, что для некоторой постоянной $A > 0$ (вычисление этой постоянной см. в задаче 2.17) выполнено

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = A \ln x + O(1).$$

(Указание. $-\ln(1-z) = z + O(z^2)$ при $|z| \leq 1/2$.)

Задача 1.14 (интегральный аналог теоремы Штольца). Пусть вещественнозначные функции $f(x), g(x)$ интегрируемы (по Лебегу) на всяком отрезке $[a, b] \subseteq [x_0, +\infty)$, причём $g(x) > 0$ при (почти) всех $x \geq x_0$, а несобственный интеграл $\int_{x_0}^{+\infty} g(x) dx$ расходится. Допустим также, что существует предел $\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} = c \in \overline{\mathbb{R}} = [-\infty, +\infty]$. Доказать, что предел

$$\lim_{x \rightarrow +\infty} \frac{\int_{x_0}^x f(u) du}{\int_{x_0}^x g(u) du}$$

также существует и равен c .

Задача 1.15. Доказать, что если предел $\lim_{x \rightarrow +\infty} \frac{\pi(x)}{x/\ln x}$ существует, то он равен 1. (Указание. Использовать задачу 1.6 или 1.12, преобразование Абеля и теорему Штольца.)

1.2 Это было давно и неправда

Вспомним некоторые основные факты про арифметические функции, которые мы все прекрасно не помним с первого курса.

Арифметической функцией называется произвольная функция $f: \mathbb{N} \rightarrow \mathbb{C}$. Арифметическая функция f называется мультипликативной, если, во-первых, она не является тождественно нулевой, и во-вторых, для любых взаимно простых $a, b \in \mathbb{N}$ выполнено $f(ab) = f(a)f(b)$. Если же равенство $f(ab) = f(a)f(b)$ справедливо для всех $a, b \in \mathbb{N}$, то функция f называется вполне мультипликативной.

Парочка простейших свойств мультипликативных функций:

- ☺ Для любой мультипликативной функции f выполнено $f(1) = 1$.
- ☺ Если f — мультипликативная функция, то

$$\sum_{d|n} f(d) = \prod_{p|n} (1 + f(p) + f(p^2) + \dots + f(p^{v_p(n)})).$$

Другими словами, функция $F(n) = \sum_{d|n} f(d)$ тоже является мультипликативной. (Обратное также верно.)

Одной из важнейших мультипликативных функций является функция Мёбиуса

$$\mu(n) = \begin{cases} 0, & p^2 | n, \\ (-1)^s, & n = p_1 \cdots p_s, p_1 < \dots < p_s. \end{cases}$$

Её главная прелесть заключается в формуле

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases} \quad (1.1)$$

следствием которой является формула обращения Мёбиуса: арифметические функции f, F связаны соотношением $F(n) = \sum_{d|n} f(d)$ тогда и только тогда, когда для них же выполнено $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

Другой важный пример мультипликативной функции даёт функция Эйлера φ , где $\varphi(n)$ — количество натуральных чисел, не превосходящих n и взаимно простых с n . Полезные формулы:

$$\varphi(n) = \prod_{p|n} (p^{v_p(n)} - p^{v_p(n)-1}) = \prod_{p|n} p^{v_p(n)-1} (p-1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Последнее представление является просто формулой включений-исключений, если считать $\varphi(n)$ по определению. Согласно формуле обращения, оно равносильно равенству $\sum_{d|n} \varphi(d) = n$.

Свёрткой Дирихле $f \star g$ двух арифметических функций f, g называется арифметическая функция, задающаяся формулой

$$(f \star g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1)g(d_2).$$

Некоторые простейшие свойства свёртки Дирихле:

- ☉ коммутативность: $f \star g = g \star f$;
- ☉ ассоциативность: $(f \star g) \star h = f \star (g \star h)$;
- ☉ билинейность (над \mathbb{C}): $(c_1 f_1 + c_2 f_2) \star g = c_1 (f_1 \star g) + c_2 (f_2 \star g)$ (линейность по второму аргументу получается по коммутативности);
- ☉ свёртка Дирихле мультипликативных функций является мультипликативной функцией. (Более того, мультипликативные функции образуют абелеву группу относительно свёртки Дирихле с нейтральным элементом $\varepsilon(n) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$)

Используя свёртку Дирихле, можно, например, переписать основное свойство функции Мёбиуса в виде $\mu \star \mathbf{1} = \varepsilon$, где $\mathbf{1}(n) = 1$ (тождественная единица), а формула обращения принимает вид $F = f \star \mathbf{1} \Leftrightarrow f = \mu \star F$ и становится очевидной.

1.3 Оценки для арифметических функций

В нагрузку к рассмотренным выше функциям Мёбиуса и Эйлера определим также функции: $\tau(n) = \sum_{d|n} 1$ — количество делителей числа n , $\sigma(n) = \sum_{d|n} d$ — сумма делителей числа n , $\omega(n) = \sum_{p|n} 1$ — количество различных простых делителей числа n , $\Omega(n) = \sum_{p|n} v_p(n)$ — количество простых делителей числа n с учётом кратностей. (Функции τ и σ , очевидно, мультипликативны, ω аддитивна, т.е. $\omega(ab) = \omega(a) + \omega(b)$ при $(a, b) = 1$, а Ω вполне аддитивна.)

В некоторых из следующих задач уместно применить асимптотический закон распределения простых чисел (азрпч), что указано явно.

Задача 1.16. Доказать, что $\Omega(n) \leq \ln n / \ln 2$, причём для бесконечно многих n достигается равенство.

Задача 1.17 (оценки для $\omega(n)$).

- 1) Доказать оценку

$$\omega(n) = O\left(\frac{\ln n}{\ln \ln n}\right), \quad n \geq 3.$$

(Указание. Использовать неравенство $n \geq p_1 \cdots p_{\omega(n)}$, где p_k — k -е простое число.)

- 2) Доказать, что для некоторой постоянной $c > 0$ существует бесконечно много n , удовлетворяющих неравенству

$$\omega(n) \geq \frac{c \ln n}{\ln \ln n}.$$

- 3) Используя азрпч, доказать, что

$$\limsup_{n \rightarrow \infty} \frac{\omega(n) \ln \ln n}{\ln n} = 1.$$

Задача 1.18 (оценки для $\varphi(n)$).

1) Найти все предельные точки последовательности $\left\{ \frac{\varphi(n)}{n} \right\}_{n=1}^{\infty}$.

2) Доказать оценку

$$\frac{n}{\varphi(n)} = O(\ln \ln n), \quad n \geq 3.$$

3) Доказать, что для некоторой постоянной $c > 0$ существует бесконечно много n , удовлетворяющих неравенству

$$\varphi(n) \leq \frac{cn}{\ln \ln n}.$$

4) Доказать, что

$$\limsup_{n \rightarrow \infty} \frac{n}{\varphi(n) \ln \ln n} = A,$$

где A — постоянная из задачи 1.13.

Задача 1.19 (оценки для $\sigma(n)$).

1) Доказать, что для некоторой постоянной $c > 0$ выполнено

$$c < \frac{\sigma(n) \varphi(n)}{n^2} < 1, \quad n > 1.$$

2) Доказать, что

$$0 < \limsup_{n \rightarrow \infty} \frac{\sigma(n)}{n \ln \ln n} < +\infty.$$

3) Доказать, что

$$\limsup_{n \rightarrow \infty} \frac{\sigma(n)}{n \ln \ln n} = A,$$

где A — постоянная из задачи 1.13.

Задача 1.20 (оценки для $\tau(n)$).

1) Доказать, что для любого $\varepsilon > 0$ выполнено $\tau(n) = O(n^\varepsilon)$.

2) Доказать, что для любого $\varepsilon > 0$ при $n \geq n_0(\varepsilon)$ справедливо неравенство

$$\ln \tau(n) \leq (\ln 2 + \varepsilon) \frac{\ln n}{\ln \ln n}.$$

(Указание. Представить $\tau(n)$ в виде произведения по простым $p \mid n$ и разбить его на $p \leq p_0$ и $p > p_0$, подобрав $p_0 = p_0(n)$ так, что $\pi(p_0) \ln \ln n = o(\ln n / \ln \ln n)$ и $\ln p_0 \sim \ln \ln n$. Для маленьких p использовать грубую оценку $v_p(n) = O(\ln n)$. Для больших p использовать неравенство $\ln(v_p(n) + 1) \leq \frac{\ln 2}{\ln p_0} \ln p^{v_p(n)}$.)

3) Доказать, что

$$\limsup_{n \rightarrow \infty} \frac{\ln \tau(n) \cdot \ln \ln n}{\ln n} > 0.$$

4) Используя азрпч, доказать, что

$$\limsup_{n \rightarrow \infty} \frac{\ln \tau(n) \cdot \ln \ln n}{\ln n} = \ln 2.$$

1.4 Суммы значений арифметических функций: начало

Задача 1.21. Доказать равенства:

- 1) $\sum_{n \leq x} \omega(n) = x \ln \ln x + c_0 x + O\left(\frac{x}{\ln x}\right)$, $x \geq 2$, где c_0 — постоянная из задачи 1.12.
- 2) $\sum_{n \leq x} \Omega(n) = x \ln \ln x + c_1 x + O\left(\frac{x}{\ln x}\right)$, $x \geq 2$, где c_1 — некоторая постоянная.

Задача 1.22.

- 1) Доказать, что $\sum_{n \leq x} \tau(n) = x \ln x + O(x)$.
- 2) Понять, что сумма $\sum_{n \leq x} \tau(n)$ представляет из себя количество точек с натуральными координатами, расположенных под гиперболой $ab = x$ (на плоскости Oab).
- 3) Доказать, что

$$\sum_{n \leq x} \tau(n) = 2 \sum_{n \leq \sqrt{x}} \left\lfloor \frac{x}{n} \right\rfloor - \lfloor \sqrt{x} \rfloor^2 = x \ln x + (2\gamma - 1)x + O(\sqrt{x}),$$

где γ — постоянная Эйлера(–Маскерони) из п. 2 задачи 1.11.

- 4) Доказать, что

$$\sum_{n \leq x} \frac{\tau(n)}{n} = \frac{1}{2} (\ln x)^2 + 2\gamma \ln x + c + O\left(\frac{1}{\sqrt{x}}\right),$$

где c — некоторая постоянная.

- 5) Доказать, что

$$\sum_{n \leq x} \left\{ \frac{x}{n} \right\} = (1 - \gamma)x + O(\sqrt{x}),$$

где $\{x\} = x - [x]$ — дробная часть числа x .

Задача 1.23.

- 1) Используя равенство⁴ $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, доказать, что

$$\sum_{n \leq x} \sigma(n) = \frac{\pi^2}{12} x^2 + O(x \ln x), \quad x \geq 2.$$

(Указание. Использовать равенство $\sigma(n) = \sum_{d|n} \frac{n}{d}$.)

⁴Для его доказательства можно разложить функцию $f(x) = x$ в ряд Фурье на промежутке $(-\pi, \pi)$ и применить равенство Парсеваля.

2) Доказать, что

$$\sum_{n \leq x} n \left\{ \frac{x}{n} \right\} = \left(1 - \frac{\pi^2}{12} \right) x^2 + O(x \ln x), \quad x \geq 2,$$

где $\{x\} = x - [x]$ — дробная часть числа x .

Задача 1.24.

1) Доказать тождество

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] = 1.$$

(Указание. Использовать равенство (1.1).)

2) Доказать, что при $x \geq 2$ справедливо неравенство

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| < 1.$$

(Уточнение этого неравенства см. в главе 3.)

1.5 Разное

Пока не очень ясно, что с этим делать.

Задача 1.25. Пусть $a < b$ — целые числа, $f: [a, b] \rightarrow \mathbb{R}$ — монотонная функция. Доказать неравенство

$$\left| f(a) + f(a+1) + \dots + f(b) - \int_a^b f(u) du \right| \leq \max \{ |f(a)|, |f(b)| \}.$$

Задача 1.26. Доказать оценку $\psi(x) - \theta(x) = O(x^{1/2})$.

Задача 1.27. Доказать неравенство $\sum_{p|n} \frac{\ln p}{p} \leq \ln \ln n + O(1)$.

Глава 2

Вокруг дзета-функции Римана и асимптотического закона

2.1 Ряды Дирихле

Задача 2.1.

- 1) Пусть ряды Дирихле $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ и $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$ сходятся абсолютно при некотором $s \in \mathbb{C}$. Доказать, что (при том же s)

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s},$$

где $f * g$ — свёртка Дирихле функций f и g , причём ряд сходится абсолютно.

- 2) Пусть f — мультипликативная функция, причём $\sum_{n=1}^{\infty} |f(n)| < +\infty$. Доказать, что

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + \dots);$$

в частности, если f вполне мультипликативна, то

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

- 3) Доказать равенства:

а) $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}, \operatorname{Re} s > 1;$

б) $\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}, \operatorname{Re} s > 2;$

в) $\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \zeta^2(s), \operatorname{Re} s > 1;$

$$\begin{aligned} \text{г)} \quad & \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s) \zeta(s-1), \operatorname{Re} s > 2; \\ \text{д)} \quad & \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}, \operatorname{Re} s > 1; \\ \text{е)} \quad & \sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}, \operatorname{Re} s > 1; \\ \text{ж)} \quad & \sum_{n=1}^{\infty} \frac{\tau(n^2)}{n^s} = \frac{\zeta^3(s)}{\zeta(2s)}, \operatorname{Re} s > 1; \\ \text{з)} \quad & \sum_{n=1}^{\infty} \frac{\sigma(n^2)}{n^s} = \frac{\zeta(s) \zeta(s-1) \zeta(s-2)}{\zeta(2s-2)}, \operatorname{Re} s > 3; \\ \text{и)} \quad & \sum_{n=1}^{\infty} \frac{\tau^2(n)}{n^s} = \frac{\zeta^4(s)}{\zeta(2s)}, \operatorname{Re} s > 1; \\ \text{к)} \quad & \sum_{n=1}^{\infty} \frac{\sigma^2(n)}{n^s} = \frac{\zeta(s) \zeta^2(s-1) \zeta(s-2)}{\zeta(2s-2)}, \operatorname{Re} s > 3; \\ \text{л)} \quad & \sum_{n=1}^{\infty} \frac{\tau(n) \sigma(n)}{n^s} = \frac{\zeta^2(s) \zeta^2(s-1)}{\zeta(2s-1)}, \operatorname{Re} s > 2. \end{aligned}$$

4) Пусть $m \in \mathbb{N}$. Преобразуя ряды в произведения, доказать равенства:

$$\begin{aligned} \text{а)} \quad & \sum_{n=1}^{\infty} \frac{\mu(mn)}{n^s} = \frac{\mu(m)}{\zeta(s) \prod_{p|m} (1-p^{-s})}, \operatorname{Re} s > 1; \\ \text{б)} \quad & \sum_{n=1}^{\infty} \frac{\varphi(mn)}{n^s} = \frac{\varphi(m) \zeta(s-1)}{\zeta(s) \prod_{p|m} (1-p^{-s})}, \operatorname{Re} s > 2; \\ \text{в)} \quad & \sum_{n=1}^{\infty} \frac{\tau(mn)}{n^s} = \zeta^2(s) \prod_{p|m} (v_p(m) + 1 - v_p(m)p^{-s}), \operatorname{Re} s > 1; \\ \text{г)} \quad & \sum_{n=1}^{\infty} \frac{\sigma(mn)}{n^s} = \zeta(s) \zeta(s-1) \prod_{p|m} (\sigma(p^{v_p(m)}) - \sigma(p^{v_p(m)-1})p^{1-s}), \operatorname{Re} s > 2. \end{aligned}$$

Задача 2.2. Доказать равенство

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

Задача 2.3.

1) Пусть f — мультипликативная функция, такая что $\sum_{n=1}^{\infty} f(n) = 0$, причём ряд сходится абсолютно. Доказать, что найдётся простое число p , такое что

$$1 + f(p) + f(p^2) + \dots = 0.$$

(Замечание. Условие абсолютной сходимости отбросить нельзя: см. главу 3.)

- 2) Пусть f — вполне мультипликативная функция, такая что $\sum_{n=1}^{\infty} |f(n)| < +\infty$. Доказать, что $\sum_{n=1}^{\infty} f(n) \neq 0$. (Замечание. Условие абсолютной сходимости отбросить нельзя: можно взять $f(n) = \lambda(n)/n$, где $\lambda(n) = (-1)^{\Omega(n)}$ — функция Лиувилля.)

Задача 2.4. Доказать, что при (вещественном) $s \rightarrow 1 + 0$ выполнено:

- 1) $\ln \zeta(s) = \sum_p p^{-s} + O(1)$;
- 2) $\sum_p p^{-s} = -\ln(s-1) + O(1)$.

Задача 2.5 (сходимость рядов Дирихле в комплексной плоскости).

- 1) Доказать, что при любом $t \in \mathbb{R}$ ряд $\sum_{n=1}^{\infty} n^{-1-ti}$ расходится. (Указание. $\ln n$ очень медленно меняется.)
- 2) Найти области сходимости рядов Дирихле $\sum_{n=1}^{\infty} n^{-s}$ и $\sum_{n=1}^{\infty} (-1)^n n^{-s}$, $s \in \mathbb{C}$. (Указание. Для второго ряда применить преобразование Абеля.)
- 3) Пусть все частичные суммы ряда $\sum_{n=1}^{\infty} a_n$ ограничены одной и той же постоянной. Доказать, что для любых чисел $\theta \in (0, \pi/2)$, $\delta > 0$ ряд Дирихле $\sum_{n=1}^{\infty} a_n n^{-s}$ сходится равномерно при $\operatorname{Re} s \geq \delta$, $|\arg s| \leq \theta$.
- 4) Допустим, что ряд $\sum_{n=1}^{\infty} a_n$ сходится. Доказать, что для любого $\theta \in (0, \pi/2)$ ряд Дирихле $\sum_{n=1}^{\infty} a_n n^{-s}$ сходится равномерно при $|\arg s| \leq \theta$.
- 5) Пусть a_n — комплексные числа. Доказать, что существует $\sigma_0 \in [-\infty, +\infty]$, такое что ряд Дирихле $\sum_{n=1}^{\infty} a_n n^{-s}$ сходится при $\operatorname{Re} s > \sigma_0$ и расходится при $\operatorname{Re} s < \sigma_0$ (σ_0 называется абсциссой сходимости). Кроме того, при $\operatorname{Re} s > \sigma_0$ сумма ряда является аналитической функцией, причём ряд можно почленно дифференцировать произвольное число раз.

Задача 2.6.

- 1) Доказать, что при $\operatorname{Re} s > 0$ справедливо равенство $(2^{1-s} - 1) \zeta(s) = \sum_{n=1}^{\infty} (-1)^n n^{-s}$.
- 2) Доказать, что $\zeta(\sigma) < 0$ при $\sigma \in (0, 1)$.
- 3) Найти все нули функции $f(t) = \sum_{n=1}^{\infty} (-1)^n n^{-1-ti}$, $t \in \mathbb{R}$.

Задача 2.7.

- 1) Пусть $a < b$ — вещественные числа, $f: [a, b] \rightarrow \mathbb{C}$ — непрерывно дифференцируемая функция. Доказать, что справедлива формула суммирования Эйлера

$$\sum_{a < n \leq b} f(n) = \int_a^b f(x) dx + \rho(x)f(x) \Big|_{x=a}^b - \int_a^b \rho(x)f'(x) dx,$$

где $\rho(x) = 1/2 - \{x\}$.

2) Доказать, что в области $\operatorname{Re} s > 0$ справедливо равенство

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + s \int_1^{+\infty} \frac{\rho(x) dx}{x^{s+1}}.$$

3) Доказать, что формула п. 2 даёт аналитическое продолжение $\zeta(s)$ в область $\operatorname{Re} s > -1$, причём $\zeta(0) = -1/2$.

Задача 2.8.

1) Пусть $\sigma \in (0, 1)$. Доказать, что

$$\sum_{n \leq x} \frac{1}{n^\sigma} = \frac{x^{1-\sigma}}{1-\sigma} + \zeta(\sigma) + O\left(\frac{1}{x^\sigma}\right).$$

2) Доказать, что

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(s-1), \quad s \rightarrow 1,$$

где γ — постоянная Эйлера (см. п. 2 задачи 1.11).

Задача 2.9. Пусть f — ограниченная вполне мультипликативная функция (т.е. $\max_{n \in \mathbb{N}} |f(n)| = 1$), $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$. Доказать, что при $\operatorname{Re} s > 1$ выполнено $F(s) \neq 0$,

а также справедливы равенства: 1) $\frac{1}{F(s)} = \sum_{n=1}^{\infty} \frac{f(n) \mu(n)}{n^s}$; 2) $-\frac{F'(s)}{F(s)} = \sum_{n=1}^{\infty} \frac{f(n) \Lambda(n)}{n^s}$.

Задача 2.10.

1) Пусть точка s_0 является нулём кратности m либо полюсом порядка $|m| = -m$ для (аналитической) функции $f(s)$, $m \in \mathbb{Z} \setminus \{0\}$. Доказать, что в точке s_0 логарифмическая производная $\frac{f'(s)}{f(s)}$ имеет полюс первого порядка с вычетом m .

2) Доказать, что при $\sigma > 1$, $t \in \mathbb{R}$ справедливо неравенство

$$\operatorname{Re} \left(3 \frac{\zeta'(\sigma)}{\zeta(\sigma)} + 4 \frac{\zeta'(\sigma + ti)}{\zeta(\sigma + ti)} + \frac{\zeta'(\sigma + 2ti)}{\zeta(\sigma + 2ti)} \right) \leq 0.$$

3) Вывести из пунктов 1 и 2 отсутствие нулей $\zeta(s)$ на прямой $\operatorname{Re} s = 1$.

Задача 2.11 (вокруг гипотезы Римана).

1) Доказать, что для любого $a \geq 0$ следующие два утверждения равносильны:

а) для любого $\varepsilon > 0$ выполнено $\sum_{n \leq x} \mu(n) = O(x^{a+\varepsilon})$;

б) ряд $\sum_{n=1}^{\infty} \mu(n)n^{-s}$ сходится при $\operatorname{Re} s > a$.

2) Доказать, что из утверждения 1б следует отсутствие нулей $\zeta(s)$ при $\operatorname{Re} s > a$. (Обратное тоже верно, но доказательство сложное.)

2.2 Различные асимптотики

Задача 2.12 (избавление от условия взаимной простоты).

1) Доказать, что

$$\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \ln x), \quad x \geq 2.$$

(Указание. Использовать представление $\varphi(n)$ в виде суммы с функцией Мёбиуса.)

2) Пусть $N(x, m)$ — количество натуральных чисел, не превосходящих $x \geq 1$ и взаимно простых с $m \in \mathbb{N}$. Доказать, что

$$N(x, m) = \sum_{d|m} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

(Указание. $N(x, m) = \sum_{n \leq x} \sum_{d|(n, m)} \mu(d)$.)

3) Доказать, что количество несократимых дробей $a/b \in (0, c]$ со знаменателем $b \leq x$ равно

$$\frac{3c}{\pi^2} x^2 + O(x \ln x), \quad c \in (0, 1], \quad x \geq 2.$$

4) Точка $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ называется *целой*, если все её координаты целые (т. е. $x \in \mathbb{Z}^n$). Целая точка (x_1, \dots, x_n) называется *примитивной*, если её координаты взаимно просты в совокупности (т. е. $\gcd(x_1, \dots, x_n) = 1$).

а) Доказать, что количество целых точек в круге $x^2 + y^2 \leq R^2$ равно $\pi R^2 + O(R)$, $R \geq 1$. (Указание. Для каждой целой точки (x_0, y_0) в круге рассмотреть квадратик $\max\{|x - x_0|, |y - y_0|\} \leq 1/2$.)

б) Доказать, что количество примитивных целых точек в круге $x^2 + y^2 \leq R^2$ равно $\frac{6}{\pi} R^2 + O(R \ln R)$, $R \geq 2$.

5) Пусть $\Omega \subseteq \mathbb{R}^n$ — ограниченное выпуклое множество с непустой внутренностью (такие множества измеримы по Жордану и имеют положительную меру Жордана $\text{vol}(\Omega)$), $n \geq 2$.

а) Пусть $N(t)$ — количество целых точек в $t\Omega$, $t > 0$. Доказать, что

$$N(t) \sim \text{vol} \Omega \cdot t^n, \quad t \rightarrow +\infty.$$

б) Пусть $N^*(t)$ — количество примитивных целых точек в $t\Omega$, $t > 0$. Доказать, что

$$N^*(t) \sim \frac{\text{vol} \Omega}{\zeta(n)} \cdot t^n, \quad t \rightarrow +\infty.$$

Задача 2.13. Доказать, что асимптотический закон распределения простых чисел эквивалентен асимптотике для n -го простого числа $p_n \sim n \ln n$, $n \rightarrow \infty$.

Задача 2.14. Используя асимптотический закон распределения простых чисел, доказать, что справедливы асимптотические равенства (при $x \rightarrow +\infty$): 1) $\sum_{p \leq x} p \sim \frac{x^2}{2 \ln x}$;

2) $\sum_{p \leq x} p \ln p \sim \frac{x^2}{2}$; 3) $\sum_{p \leq x} \frac{p}{\ln p} \sim \frac{x^2}{2(\ln x)^2}$.

Задача 2.15 (уточнение задачи 1.6). Доказать эквивалентность следующих трёх утверждений:

1) Несобственный интеграл $\int_1^{+\infty} \frac{(\psi(x) - x) dx}{x^2}$ сходится.

2) Несобственный интеграл $\int_1^{+\infty} \frac{(\theta(x) - x) dx}{x^2}$ сходится.

3) Существует предел $\lim_{x \rightarrow +\infty} \left(\sum_{p \leq x} \frac{\ln p}{p} - \ln x \right)$.

(Поскольку утверждение 1 доказывается на лекции, то все три утверждения справедливы.)

Задача 2.16 (суммы с бесквадратными числами).

1) Доказать равенство $\mu^2(n) = \sum_{d^2 | n} \mu(d)$.

2) Пусть $Q(x)$ — количество бесквадратных чисел (т. е. не делящихся на квадрат никакого простого числа), не превосходящих x . Доказать, что

$$Q(x) = \frac{6}{\pi^2} x + O(\sqrt{x}).$$

(Указание. $Q(x) = \sum_{n \leq x} \mu^2(n)$.)

3) Доказать асимптотические формулы для сумм по бесквадратным числам:

а) $\sum_{\text{бескв. } n \leq x} n = \frac{3}{\pi^2} x^2 + O(x\sqrt{x})$;

б) $\sum_{\text{бескв. } n \leq x} \frac{1}{n} = \frac{6}{\pi^2} \ln x + c + O\left(\frac{1}{\sqrt{x}}\right)$, где c — некоторая постоянная.

Задача 2.17 (вычисление постоянной в задаче 1.13). Доказать равенства:

1) $\ln \zeta(s) = -\ln(s-1) + o(1) = \sum_p p^{-s} + \sum_p \left(-\ln\left(1 - \frac{1}{p}\right) - \frac{1}{p} \right) + o(1)$, $s \rightarrow 1+0$;

2) $\sum_p p^{-s} = (s-1) \int_1^{+\infty} \ln \ln u \cdot u^{-s} du + c_0 + o(1) = -\ln(s-1) - \gamma + c_0 + o(1)$, $s \rightarrow 1+0$, где c_0 — постоянная из задачи 1.12, а $\gamma = -\int_0^{\infty} \ln x \cdot e^{-x} dx = -\Gamma'(1)$ — постоянная Эйлера⁴;

⁴Непосредственное док-во равенства $\int_0^{\infty} \ln x \cdot e^{-x} dx = -\gamma$ может быть таким:

$$\sum_{k=1}^n \frac{1}{k} = \int_0^1 \frac{(1-t^n) dt}{1-t} = \int_0^1 \frac{(1-(x/n)^n) dx}{x} = \int_0^1 \left(1 - \left(1 - \frac{x}{n}\right)^n \right) d(\ln x) = \ln n - \int_0^1 \ln x \cdot \left(1 - \frac{x}{n}\right)^{n-1} dx.$$

Переходя к пределу при $n \rightarrow \infty$, получаем требуемое.

3) $\sum_p \left(-\ln\left(1 - \frac{1}{p}\right) - \frac{1}{p} \right) = \ln A - c_0$, где A — постоянная из задачи 1.13;

4) $A = e^\gamma$, т. е. справедлива теорема Мертенса

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln x}, \quad x \rightarrow +\infty.$$

Задача 2.18. Доказать, что

$$\lim_{x \rightarrow +\infty} \frac{1}{\ln x} \sum_{n \leq x} \frac{1}{\varphi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \quad \left(= \frac{315\zeta(3)}{2\pi^4} \right).$$

(Указание. $\frac{1}{\varphi(n)} = \frac{1}{n} \sum_{\substack{d \in \mathbb{N}, \\ \text{rad}(d) | n}} \frac{1}{d}$, где $\text{rad}(d) = \prod_{p|d} p$. Вычисление $\zeta(6)$ см. в задаче 2.22.)

2.3 Числа Бернулли и формула Эйлера–Маклорена

Задача 2.19. Допустим, что ряды $A(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n$ и $B(z) = \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n$ сходятся абсолютно при некотором $z \in \mathbb{C}$. Доказать, что (при том же z)

$$A(z)B(z) = \sum_{n=0}^{\infty} \frac{c_n}{n!} z^n,$$

где $c_n = \sum_{k=0}^n \binom{n}{k} a_k b_{n-k}$. (Замечание. Согласно теореме Мертенса, достаточно требовать абсолютную сходимость только для одного ряда, от второго нужна просто сходимость. Из второй теоремы Абеля следует, что равенство справедливо также в случае, когда все три ряда сходятся.)

Числа Бернулли — рациональные числа B_n , определённые с помощью равенства

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n, \quad |z| < 2\pi.$$

В частности, $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$.

Задача 2.20 (простейшие свойства чисел Бернулли). Доказать, что:

- 1) $B_{2n+1} = 0$ при $n \geq 1$;
- 2) $(-1)^n B_n = B_n$ при $n \neq 1$;
- 3) $\sum_{k=0}^n \binom{n}{k} B_k = (-1)^n B_n$ при $n \geq 0$;
- 4) $z \operatorname{ctg} z = \sum_{n=0}^{\infty} (-1)^n \frac{B_{2n}}{(2n)!} (2z)^{2n}$, $|z| < \pi$;
- 5) $\operatorname{tg} z = \sum_{n=1}^{\infty} (-1)^{n+1} B_{2n} \frac{2^{2n}(2^{2n}-1)}{(2n)!} z^{2n-1}$, $|z| < \pi/2$.

Многочлены Бернулли $B_n(x)$ определяются с помощью равенства

$$\frac{ze^{xz}}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n, \quad |z| < 2\pi.$$

Задача 2.21 (простейшие свойства многочленов Бернулли). Доказать, что:

- 1) $B_n(0) = B_n$ при $n \geq 0$;
- 2) $B_n(x) = \sum_{k=0}^n \binom{n}{k} B_{n-k} x^k$ при $n \geq 0$;
- 3) $B_n(x+y) = \sum_{k=0}^n \binom{n}{k} B_{n-k}(y) x^k$ при $n \geq 0$;
- 4) $B_n(1-x) = (-1)^n B_n(x)$ при $n \geq 0$;
- 5) $B_n(1) = (-1)^n B_n$ при $n \geq 0$;
- 6) $B_n(mx) = m^{n-1} \sum_{k=0}^{m-1} B_n\left(x + \frac{k}{m}\right)$ при $m \in \mathbb{N}$, $n \geq 0$;
- 7) $B_n(1/2) = (2^{1-n} - 1)B_n$ при $n \geq 0$;
- 8) $B_n(x+1) - B_n(x) = nx^{n-1}$ при $n \geq 1$;
- 9) при $N, d \in \mathbb{N}$ справедлива формула Бернулли

$$\sum_{n=0}^{N-1} n^{d-1} = \frac{B_d(N) - B_d}{d},$$

$$\text{где положено } 0^{d-1} = \begin{cases} 1, & d = 1, \\ 0, & d > 1; \end{cases}$$

- 10) $\frac{d}{dx} B_n(x) = n B_{n-1}(x)$ при $n \geq 1$;
- 11) $\int_a^b B_n(x) dx = \frac{B_{n+1}(b) - B_{n+1}(a)}{n+1}$ при $n \geq 0$;
- 12) $\int_0^1 B_n(x) dx = 0$ при $n \geq 1$;
- 13) $\int_0^1 B_n(x) B_m(x) dx = (-1)^{n+1} \frac{n!m!}{(n+m)!} B_{n+m}$ при $n, m \geq 1$;
- 14) $(-1)^{n+1} B_{2n} > 0$ при $n \geq 1$.

Задача 2.22. Доказать, что ряд Фурье для $B_n(x)$ на промежутке $(0, 1)$ при $n \geq 1$ равен

$$-\frac{n!}{(2\pi i)^n} \sum_{k \in \mathbb{Z} \setminus \{0\}} \frac{e^{2\pi i k x}}{k^n}.$$

Вывести отсюда следствия:

- 1) $\zeta(2n) = -\frac{(2\pi i)^{2n}}{2} \cdot \frac{B_{2n}}{(2n)!}$ при $n \in \mathbb{N}$ (в частности, $\zeta(2n)\pi^{-2n} \in \mathbb{Q}$);

- 2) $(-1)^{n+1}B_{2n} > 0$ при $n \geq 1$;
 3) $|B_{2n}| \sim \frac{2(2n)!}{(2\pi)^{2n}}$ при $n \rightarrow \infty$;
 4) $|B_n(x)| \leq 2\zeta(n)\frac{n!}{(2\pi)^n}$ при $x \in [0, 1]$, $n \geq 2$.

Задача 2.23 (формула суммирования Эйлера–Маклорена).

- 1) Пусть $m \in \mathbb{N}$, $f \in C^{(m)}([0, 1], \mathbb{C})$. Доказать, что

$$\frac{f(0) + f(1)}{2} = \int_0^1 f(x) dx + \sum_{k=1}^{m-1} \frac{B_{k+1}}{(k+1)!} f^{(k)}(x) \Big|_{x=0}^1 + (-1)^{m+1} \int_0^1 \frac{B_m(x)}{m!} f^{(m)}(x) dx.$$

- 2) Пусть $a < b$ – целые числа, $m \in \mathbb{N}$, $f \in C^{(m)}([a, b], \mathbb{C})$. Доказать, что

$$\sum_{n=a}^b f(n) = \int_a^b f(x) dx + \frac{f(a) + f(b)}{2} + \sum_{k=1}^{m-1} \frac{B_{k+1}}{(k+1)!} f^{(k)}(x) \Big|_{x=a}^b + (-1)^{m+1} \int_a^b \frac{B_m(\{x\})}{m!} f^{(m)}(x) dx,$$

где $\{x\} = x - [x]$ – дробная часть числа x .

- 3) Пусть $m \in \mathbb{N}$, $f \in C^{(m)}([1, +\infty), \mathbb{C})$, причём $\int_1^{+\infty} |f^{(m)}(x)| dx < +\infty$. Доказать, что при $N \in \mathbb{N}$ выполнено

$$\sum_{n=1}^N f(n) = \int_1^N f(x) dx + C(m) + \frac{1}{2}f(N) + \sum_{k=1}^{m-1} \frac{B_{k+1}}{(k+1)!} f^{(k)}(N) + R_N(m),$$

где

$$C(m) = \frac{1}{2}f(1) - \sum_{k=1}^{m-1} \frac{B_{k+1}}{(k+1)!} f^{(k)}(1) + (-1)^{m+1} \int_1^{+\infty} \frac{B_m(\{x\})}{m!} f^{(m)}(x) dx,$$

$$|R_N(m)| \leq \frac{4}{(2\pi)^m} \int_N^{+\infty} |f^{(m)}(x)| dx.$$

Задача 2.24 (формула Стирлинга). Доказать, что для любого (фиксированного) $m \in \mathbb{N}$ при $N \rightarrow \infty$ выполнено

$$\ln N! = \left(N + \frac{1}{2}\right) \ln N - N + C_0 + \sum_{k=1}^m \frac{B_{2k}}{2k(2k-1)N^{2k-1}} + O\left(\frac{1}{N^{2m+1}}\right),$$

где C_0 – некоторая постоянная (как известно из курса математического анализа, $C_0 = \ln \sqrt{2\pi}$).

Задача 2.25 (продолжение задачи 2.7). Доказать, что $\zeta'(0) = -C_0$, где C_0 – постоянная из задачи 2.24 (т.е. $\zeta'(0) = -\ln \sqrt{2\pi}$). (Указание. $\zeta'(0) = -1 - \int_1^{+\infty} \frac{B_1(\{x\}) dx}{x}$.)

Задача 2.26 (аналитическое продолжение $\zeta(s)$). Доказать, что для любого $n \in \mathbb{N}$ справедливо равенство

$$\zeta(s) = \frac{1}{s-1} \sum_{k=0}^{n+1} \binom{1-s}{k} B_k - \binom{s+n}{n+1} \int_1^{+\infty} \frac{B_{n+1}(\{x\}) dx}{x^{s+n+1}},$$

дающее аналитическое продолжение $\zeta(s)$ в область $\operatorname{Re} s > -n$ (за исключением простого полюса в точке $s = 1$). Вывести отсюда следствия:

1) При $n \in \mathbb{N}$ выполнено

$$\zeta(1-n) = (-1)^{n+1} \frac{B_n}{n} = \begin{cases} -1/2, & n = 1, \\ -B_n/n, & n > 1. \end{cases}$$

2) $\zeta(-2n) = 0$ при $n \in \mathbb{N}$ (тривиальные нули $\zeta(s)$).

3) При целых $n \geq 2$ выполнено

$$\zeta(1-n) = 2^{1-n} \pi^{-n} \cos\left(\frac{\pi n}{2}\right) \Gamma(n) \zeta(n).$$

(Замечание. Равенство (функциональное уравнение Римана)

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

или, более симметрично,

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

справедливо для всех $s \in \mathbb{C}$.)

Замечание. Вспоминая задачу 2.6, мы получаем, что ряд Дирихле $\sum_{n=1}^{\infty} (-1)^n n^{-s}$ сходится лишь при $\operatorname{Re} s > 0$, однако его сумма может быть аналитически продолжена на всю комплексную плоскость и не имеет особенностей (т.е. является целой функцией).

Глава 3

Суммы с функцией Мёбиуса

Цель этой главы — доказать оценку $M(x) = \sum_{n \leq x} \mu(n) = o(x)$, $x \rightarrow +\infty$, и равенство $\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0$ (задачи 3.8 и 3.9). Доказательство очень слабо отличается от доказательства асимптотического закона, которое рассказывается на лекциях.

Рассмотрим функцию $F(s) = \frac{1}{s \zeta(s)}$.

Задача 3.1. Доказать, что функция $F(s)$ голоморфна при $\operatorname{Re} s \geq 1$, причём $F(1) = 0$; кроме того, при $\operatorname{Re} s > 1$ справедливы равенства

$$F(s) = \frac{1}{s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \int_1^{+\infty} \frac{M(x) dx}{x^{s+1}}.$$

Далее нам понадобятся функции

$$F_T(s) = \int_1^T \frac{M(x) dx}{x^{s+1}}, \quad T > 1.$$

Все они являются целыми (по s).

Задача 3.2. Доказать неравенства:

1) если $\sigma = \operatorname{Re} s > 0$, то

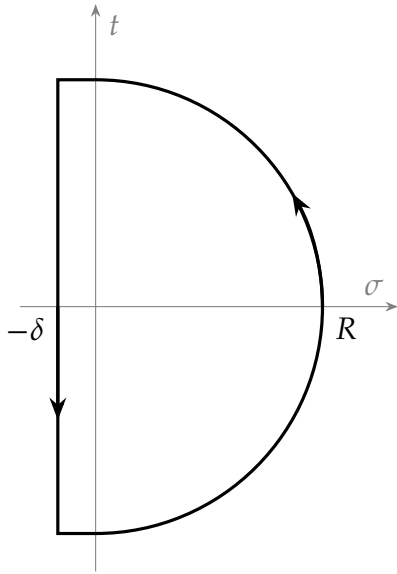
$$|F_T(s+1) - F(s+1)| \leq \frac{T^{-\sigma}}{\sigma};$$

2) если $\sigma = \operatorname{Re} s < 0$, то

$$|F_T(s+1)| \leq \frac{T^{-\sigma}}{-\sigma}.$$

Наша ближайшая цель — доказать равенство (задача 3.7)

$$\lim_{T \rightarrow +\infty} F_T(1) = F(1) \quad (= 0).$$



Для этого фиксируем $\varepsilon > 0$ и положим $R = 1/\varepsilon$. Кроме того, фиксируем $\delta = \delta(\varepsilon) \in (0, 1)$, такое что функция $\zeta(s)$ не имеет нулей в прямоугольнике $1 - \delta \leq \sigma \leq 1$, $|t| \leq R$ (где, как обычно, $s = \sigma + ti$).

Далее, рассмотрим контур Γ , состоящий из правой половины окружности $|s| = R$ и ломаной, соединяющей точки $\pm Ri$, $-\delta \pm Ri$ (см. картинку слева), пробегаемый против часовой стрелки. Кроме того, обозначим через Γ_+ и Γ_- соответственно «положительную» и «отрицательную» части этого контура (т.е. с $\sigma > 0$ и $\sigma < 0$).

Задача 3.3. Доказать равенство

$$\frac{1}{2\pi i} \int_{\Gamma} (F_T(s+1) - F(s+1)) \left(\frac{s}{R^2} + \frac{1}{s} \right) T^s ds = F_T(1) - F(1).$$

Задача 3.4. Доказать, что при $|s| = R$ выполнено

$$\frac{s}{R^2} + \frac{1}{s} = \frac{2 \operatorname{Re} s}{R^2}.$$

Задача 3.5. Используя задачи 3.2 и 3.4, доказать неравенства:

$$1) \left| \frac{1}{2\pi i} \int_{\Gamma_+} (F_T(s+1) - F(s+1)) \left(\frac{s}{R^2} + \frac{1}{s} \right) T^s ds \right| \leq \frac{1}{R} = \varepsilon;$$

$$2) \left| \frac{1}{2\pi i} \int_{\Gamma_-} F_T(s+1) \left(\frac{s}{R^2} + \frac{1}{s} \right) T^s ds \right| \leq \frac{1}{R} = \varepsilon.$$

(Указание. В п. 2 заменить контур Γ_- на левую полуокружность $|s| = R$, $\operatorname{Re} s < 0$.)

Задача 3.6. Доказать, что

$$\lim_{T \rightarrow +\infty} \frac{1}{2\pi i} \int_{\Gamma_-} F(s+1) \left(\frac{s}{R^2} + \frac{1}{s} \right) T^s ds = 0.$$

(Указание. $\int_{-\infty}^0 T^\sigma d\sigma = \frac{1}{\ln T}$.)

Задача 3.7. Используя задачи 3.3, 3.5 и 3.6, доказать равенство

$$\int_1^{+\infty} \frac{M(x) dx}{x^2} = 0.$$

Задача 3.8. Используя задачу 3.7, доказать оценку $M(x) = o(x)$, $x \rightarrow +\infty$. (Указание. Фиксируем $\varepsilon > 0$. Рассмотрим интеграл $\int_x^{(1+\varepsilon)x} \frac{M(y) dy}{y^2} = o(1)$, $x \rightarrow +\infty$, и воспользоваться неравенством $|M(x) - M(y)| \leq |x - y| + 1$.)

Задача 3.9. Используя задачи 3.7 и 3.8, доказать равенство

$$\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} = 0.$$

Задача 3.10. Доказать, что равенства

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = s \int_1^{+\infty} \frac{M(x) dx}{x^{s+1}}$$

справедливы для всех $s \in \mathbb{C}$ с $\operatorname{Re} s \geq 1$. (Указание. Повторить предыдущие рассуждения, заменив $F(s+1)$ и $F_T(s+1)$ на $F(s+1+t_0i)$ и $F_T(s+1+t_0i)$ соответственно.)

3.1 Тауберовы теоремы

Задача 3.11 (тауберова теорема для преобразования Лапласа). Пусть измеримая функция $f: [1, +\infty) \rightarrow \mathbb{C}$ удовлетворяет условию $f(x) = O(x)$. Допустим, что функция $F(s)$, определённая при $\operatorname{Re} s > 1$ с помощью равенства

$$F(s) = \int_1^{+\infty} \frac{f(x) dx}{x^{s+1}}, \quad (3.1)$$

аналитически продолжается до голоморфной при $\operatorname{Re} s \geq 1$. Доказать, что равенство (3.1) остаётся справедливым и при $\operatorname{Re} s = 1$. (Замечание. Основная сложность — доказать сходимость интеграла.)

Задача 3.12 (тауберова теорема для рядов Дирихле). Пусть $a_n \in \mathbb{C}$, $\sup_{n \in \mathbb{N}} |a_n| < +\infty$.

Допустим, что функция $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ (очевидно голоморфная при $\operatorname{Re} s > 1$) аналитически продолжается до голоморфной при $\operatorname{Re} s \geq 1$. Доказать, что:

1) $\sum_{n \leq x} a_n = o(x)$, $x \rightarrow +\infty$;

2) ряд $\sum_{n=1}^{\infty} a_n n^{-s}$ сходится при $\operatorname{Re} s \geq 1$ (и его сумма равна $F(s)$).

Задача 3.13 (тауберова теорема для рядов Дирихле с вещественными коэффициентами). Доказать, что при $a_n \in \mathbb{R}$ вместо условия $\sup_{n \in \mathbb{N}} |a_n| < +\infty$ в задаче 3.12

достаточно потребовать условия $\inf_{n \in \mathbb{N}} a_n > -\infty$ и $\sum_{n \leq x} a_n = O(x)$. (Указание. Пусть $a_n \geq -C$, $C \geq 0$, $A(x) = \sum_{n \leq x} a_n$. Нетривиальна только оценка $A(x) = o(x)$. Фиксируем

$\varepsilon \in (0, 1)$. Рассмотрим интеграл $\int_x^{(1+\varepsilon)x} \frac{A(y) dy}{y^2} = o(1)$, $x \rightarrow +\infty$, и с помощью неравенства $A(y) - A(x) \geq -C(y - x + 1)$, $y \geq x$, доказать, что $\limsup_{x \rightarrow +\infty} \frac{A(x)}{x} \leq C\varepsilon$. Аналогично,

используя интеграл $\int_{(1-\varepsilon)x}^x \frac{A(y) dy}{y^2}$, доказать неравенство $\liminf_{x \rightarrow +\infty} \frac{A(x)}{x} \geq -C\varepsilon$.)

Задача 3.14. Вывести из задачи 3.13 и оценок Чебышёва асимптотический закон распределения простых чисел. (Указание. Взять $a_n = \Lambda(n) - 1$.)

Глава 4

Характеры

4.1 Дела давно минувших дней...

Вспомним основные факты про первообразные корни (п.к.) и смежные вопросы.

Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Показателем (или мультипликативным порядком) числа a по модулю m называется наименьшее $d \in \mathbb{N}$, такое что выполняется сравнение $a^d \equiv 1 \pmod{m}$. Проще говоря, это порядок элемента $\bar{a} = \bar{a}_m = a + m\mathbb{Z}$ в группе $(\mathbb{Z}/m\mathbb{Z})^*$. Обозначение: $\text{ord}_m a = d$.

Если $\text{ord}_m a = d$, то $a^n \equiv 1 \pmod{m}$ тогда и только тогда, когда $d \mid n$. В частности, для любого a выполнено $d \mid \varphi(m)$ (это просто следствие теоремы Лагранжа для группы $(\mathbb{Z}/m\mathbb{Z})^*$).

Если для какого-то $g \in \mathbb{Z}$ вдруг оказалось, что $\text{ord}_m g = \varphi(m)$, то g называется первообразным корнем по модулю m . Другими словами, g — п.к. по модулю m , если $(\mathbb{Z}/m\mathbb{Z})^* = \langle \bar{g} \rangle$.

П.к. существуют только для модулей $m = 1, 2, 4, p^\alpha, 2p^\alpha$ (где $p > 2$ — простое число, $\alpha \in \mathbb{N}$), т.е. только для таких m группа $(\mathbb{Z}/m\mathbb{Z})^*$ циклическая (считаем, что $(\mathbb{Z}/1\mathbb{Z})^* = \mathbb{Z}/1\mathbb{Z} = \{\bar{1}\}$). В этом случае количество различных (по модулю m) п.к., очевидно, равно $\varphi(\varphi(m))$.

Для простого модуля п.к. ищется методом проб и ушибов с помощью критерия (для небольших m можно просто пользоваться определением).

Критерий. Пусть $a \in \mathbb{Z}$, $(a, m) = 1$. Тогда a — п.к. по модулю m , если и только если для каждого простого $q \mid \varphi(m)$ выполнено $a^{\frac{\varphi(m)}{q}} \not\equiv 1 \pmod{m}$.

Для делителя $q = 2$ условие удобно проверять, используя символ Якоби: если $m = p > 2$ — простое число, то $a^{\frac{\varphi(m)}{2}} = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ (критерий Эйлера для символа Лежандра). Символ Якоби, в частности символ Лежандра, проще всего вычислять с помощью следующих свойств:

$$\odot \text{ если } a \equiv b \pmod{P}, \text{ то } \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right);$$

$$\odot \left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right);$$

$$\odot \left(\frac{-1}{P}\right) = \begin{cases} 1, & P \equiv 1 \pmod{4}, \\ -1, & P \equiv -1 \pmod{4}; \end{cases}$$

$$\odot \left(\frac{2}{p}\right) = \begin{cases} 1, & P \equiv \pm 1 \pmod{8}, \\ -1, & P \equiv \pm 3 \pmod{8}; \end{cases}$$

\odot (квадратичный закон взаимности) если P, Q — нечётные натуральные числа, то

$$\left(\frac{P}{Q}\right) = \begin{cases} -\left(\frac{Q}{P}\right), & P \equiv Q \equiv -1 \pmod{4}, \\ \left(\frac{Q}{P}\right) & \text{иначе.} \end{cases}$$

Пусть g — п.к. по модулю p ($p > 2$). Тогда:

\odot если $g^{p-1} \not\equiv 1 \pmod{p^2}$, то g является п.к. по модулю p^α для любого α ;

\odot если же $g^{p-1} \equiv 1 \pmod{p^2}$, то $g + p$ является п.к. по модулю p^α для любого α (то же верно и для $g + 2p, g + 3p, \dots, g + (p-1)p$).

Наконец, если g — п.к. по модулю p^α , то нечётное из двух чисел $g, g + p^\alpha$ является п.к. по модулю $2p^\alpha$.

Задача 4.1. Найти п.к. (по одной штуке) по модулям 11, 19, 31, 41, 81, 101, 121, 250, 343. (Возможные ответы соответственно: 2, 2, 3, 6, 2, 2, 2, 127, 3.)

При $\alpha \geq 3$ группа $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ не является циклической, но раскладывается в прямое произведение двух своих циклических подгрупп, порождённых $\overline{-1}$ и $\overline{5}$:

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* = \langle \overline{-1} \rangle_2 \times \langle \overline{5} \rangle_{2^{\alpha-2}}.$$

Формула $(\mathbb{Z}/2^\alpha\mathbb{Z})^* = \langle \overline{-1} \rangle \times \langle \overline{5} \rangle$ справедлива и для $\alpha \leq 2$, просто в этом случае один или оба прямых сомножителя тривиальны (т.е. равны $\{\overline{1}\}$).

4.2 Строение группы $(\mathbb{Z}/m\mathbb{Z})^*$

Теперь, когда мы знаем всё про группы $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ для простых p , мы легко можем описать структуру группы $(\mathbb{Z}/m\mathbb{Z})^*$ для произвольного $m \in \mathbb{N}$, поскольку

$$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*, \quad (m, n) = 1.$$

(Китайская теорема об остатках; изоморфизм: $x + mn\mathbb{Z} \leftrightarrow (x + m\mathbb{Z}, x + n\mathbb{Z})$.)

Задача 4.2. Пусть $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ — каноническое разложение m на простые множители. Рассмотрим подгруппы

$$H_i = \{\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^* \mid a \equiv 1 \pmod{mp_i^{-\alpha_i}}\}, \quad 1 \leq i \leq s.$$

Доказать, что:

- 1) $H_i \cong (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$, причём изоморфизм можно задать явно с помощью формулы $x + m\mathbb{Z} \leftrightarrow x + p_i^{\alpha_i}\mathbb{Z}$;
- 2) $(\mathbb{Z}/m\mathbb{Z})^* = H_1 \times \dots \times H_s$. (Здесь имеется в виду внутреннее прямое произведение.)

Что это значит? Пусть $m = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ ($2 < p_1 < \cdots < p_s$, $\alpha_0 \geq 0$, $\alpha_i \geq 1$ при $i \geq 1$). Сначала находим $g_{-1}, g_0 \in \mathbb{Z}$:

$$\begin{cases} g_{-1} \equiv -1 \pmod{2^{\alpha_0}}, \\ g_{-1} \equiv 1 \pmod{m2^{-\alpha_0}}, \\ g_0 \equiv 5 \pmod{2^{\alpha_0}}, \\ g_0 \equiv 1 \pmod{m2^{-\alpha_0}}. \end{cases}$$

Далее, для каждого $i \geq 1$ сначала находим какой-нибудь п.к. $g_{i,0} \pmod{p_i^{\alpha_i}}$, а затем ищем $g_i \in \mathbb{Z}$:

$$\begin{cases} g_i \equiv g_{i,0} \pmod{p_i^{\alpha_i}}, \\ g_i \equiv 1 \pmod{mp_i^{-\alpha_i}}. \end{cases}$$

Наконец, положим

$$\begin{aligned} m_{-1} &= \begin{cases} 1, & \alpha_0 \leq 1, \\ 2, & \alpha_0 \geq 2, \end{cases} \\ m_0 &= \begin{cases} 1, & \alpha_0 \leq 2, \\ 2^{\alpha_0-2}, & \alpha_0 \geq 3, \end{cases} \\ m_i &= \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i - 1), \quad i \geq 1. \end{aligned}$$

Тогда справедливо равенство

$$(\mathbb{Z}/m\mathbb{Z})^* = \langle \overline{g_{-1}} \rangle_{m_{-1}} \times \langle \overline{g_0} \rangle_{m_0} \times \langle \overline{g_1} \rangle_{m_1} \times \cdots \times \langle \overline{g_s} \rangle_{m_s}.$$

Другими словами, для любого $a \in \mathbb{Z}$ с $(a, m) = 1$ существует представление

$$a \equiv g_{-1}^{\gamma_{-1}} g_0^{\gamma_0} \cdots g_s^{\gamma_s} \pmod{m},$$

причём γ_i определены однозначно $\pmod{m_i}$. Набор γ_i наз. системой индексов числа a по модулю m (если быть аккуратным, то надо, конечно, указывать, относительно какой системы образующих, но мы не будем занудствовать). Числа γ_i находятся с помощью перехода к сравнениям по модулям степеней простых. Разумеется, если какое-то из чисел m_{-1}, m_0 равно 1, то соответствующую подгруппу (и индексы) можно (и нужно) не рассматривать. Вот как-то так.

Задача 4.3. Разложить группу $(\mathbb{Z}/m\mathbb{Z})^*$ в прямое произведение циклических подгрупп для $m = 15, 24, 35, 75, 90, 96, 105, 110, 120, 124, 210, 328, 380, 10976$. (Возможные ответы: $(\mathbb{Z}/15\mathbb{Z})^* = \langle \overline{11} \rangle_2 \times \langle \overline{7} \rangle_4$, $(\mathbb{Z}/24\mathbb{Z})^* = \langle \overline{7} \rangle_2 \times \langle \overline{13} \rangle_2 \times \langle \overline{17} \rangle_2$, $(\mathbb{Z}/35\mathbb{Z})^* = \langle \overline{22} \rangle_4 \times \langle \overline{31} \rangle_6$, $(\mathbb{Z}/75\mathbb{Z})^* = \langle \overline{26} \rangle_2 \times \langle \overline{52} \rangle_{20}$, $(\mathbb{Z}/90\mathbb{Z})^* = \langle \overline{11} \rangle_6 \times \langle \overline{37} \rangle_4$, $(\mathbb{Z}/96\mathbb{Z})^* = \langle \overline{31} \rangle_2 \times \langle \overline{37} \rangle_8 \times \langle \overline{65} \rangle_2$, $(\mathbb{Z}/105\mathbb{Z})^* = \langle \overline{71} \rangle_2 \times \langle \overline{22} \rangle_4 \times \langle \overline{31} \rangle_6$, $(\mathbb{Z}/110\mathbb{Z})^* = \langle \overline{67} \rangle_4 \times \langle \overline{101} \rangle_{10}$, $(\mathbb{Z}/120\mathbb{Z})^* = \langle \overline{31} \rangle_2 \times \langle \overline{61} \rangle_2 \times \langle \overline{41} \rangle_2 \times \langle \overline{97} \rangle_4$, $(\mathbb{Z}/124\mathbb{Z})^* = \langle \overline{63} \rangle_2 \times \langle \overline{65} \rangle_{30}$, $(\mathbb{Z}/210\mathbb{Z})^* = \langle \overline{71} \rangle_2 \times \langle \overline{127} \rangle_4 \times \langle \overline{31} \rangle_6$, $(\mathbb{Z}/328\mathbb{Z})^* = \langle \overline{247} \rangle_2 \times \langle \overline{165} \rangle_2 \times \langle \overline{129} \rangle_{40}$, $(\mathbb{Z}/380\mathbb{Z})^* = \langle \overline{191} \rangle_2 \times \langle \overline{77} \rangle_4 \times \langle \overline{21} \rangle_{18}$, $(\mathbb{Z}/10976\mathbb{Z})^* = \langle \overline{6175} \rangle_2 \times \langle \overline{9605} \rangle_8 \times \langle \overline{6177} \rangle_{294}$.)

Задача 4.4. Проверить справедливость представления $(\mathbb{Z}/m\mathbb{Z})^*$ в виде прямого произведения и найти систему индексов числа a по модулю m (для данного представления):

- 1) $(\mathbb{Z}/24\mathbb{Z})^* = \langle \overline{7} \rangle \times \langle \overline{13} \rangle \times \langle \overline{17} \rangle, a = 5;$
- 2) $(\mathbb{Z}/35\mathbb{Z})^* = \langle \overline{22} \rangle \times \langle \overline{31} \rangle, a = 23;$
- 3) $(\mathbb{Z}/96\mathbb{Z})^* = \langle \overline{31} \rangle \times \langle \overline{37} \rangle \times \langle \overline{65} \rangle, a = 11;$
- 4) $(\mathbb{Z}/380\mathbb{Z})^* = \langle \overline{191} \rangle \times \langle \overline{77} \rangle \times \langle \overline{21} \rangle, a = 23.$

(Ответы: $5 \equiv 7^0 \cdot 13^1 \cdot 17^1 \pmod{24}$, $23 \equiv 22^3 \cdot 31^2 \pmod{35}$, $11 \equiv 31^1 \cdot 37^5 \cdot 65^1 \pmod{96}$, $23 \equiv 191^1 \cdot 77^3 \cdot 21^2 \pmod{380}$.)

Задача 4.5. Найти экспоненту $\lambda(m)$ группы $(\mathbb{Z}/m\mathbb{Z})^*$ (т.е. наименьшее число $d \in \mathbb{N}$, такое что $a^d \equiv 1 \pmod{m}$ для всех $a \in \mathbb{Z}$, взаимно простых с m), если известно каноническое разложение числа m на простые множители. (Функция λ называется функцией Кармайкла.)

Задача 4.6. Пусть $m = 2^{\alpha_0} p_1^{\alpha_1} \dots p_s^{\alpha_s}$ ($2 < p_1 < \dots < p_s$ — простые числа, $\alpha_0 \geq 0$, $\alpha_i \geq 1$ при $i \geq 1$). Доказать, что $(\mathbb{Z}/m\mathbb{Z})^*$ нельзя разложить в прямое произведение менее

чем $s + \delta$ циклических подгрупп, где $\delta = \begin{cases} 0, & \alpha_0 \leq 1, \\ 1, & \alpha_0 = 2, \\ 2, & \alpha_0 \geq 3. \end{cases}$

4.3 Характеры

Здесь уместно вспомнить определение и основные свойства групповых характеров и характеров Дирихле (ака числовых характеров). Поскольку про группу $(\mathbb{Z}/m\mathbb{Z})^*$ мы всё знаем, то мы умеем находить все хД по модулю m .

Задача 4.7. Описать все характеры по модулям $m = 8, 10, 12, 15, 18$ (найти систему образующих и задать значения на образующих в виде таблицы).

Задача 4.8. Описать все характеры χ по модулю m , удовлетворяющие данным условиям:

- 1) $m = 20, \chi(13) = i;$ $(\chi(11) = \pm 1, \chi(17) = -i)$
- 2) $m = 21, \chi(2) = e^{2\pi i/3};$ $(\chi(8) = 1, \chi(10) = \pm e^{\pi i/3})$
- 3) $m = 24, \chi(5) = \chi(7) = 1;$ $(\chi(7) = 1, \chi(13) = \chi(17) = \pm 1)$
- 4) $m = 30, \chi(17) = i;$ $(\chi(11) = \pm 1, \chi(7) = \chi(11)i)$
- 5) $m = 380, \chi(23) = -1.$ $(\chi(191) = -\chi(77) = \pm 1, \chi(21) = \pm 1)$

Задача 4.9. Пусть $p > 2$ — простое число, $\chi(x) = \left(\frac{x}{p}\right)$ — символ Лежандра. Доказать, что χ — единственный неглавный вещественный характер по модулю p .

Задача 4.10. Найти количество вещественных характеров по модулю m , если известно каноническое разложение числа m на простые множители.

Задача 4.11. Найти все $m \in \mathbb{N}$, для которых все характеры по модулю m вещественные.

Задача 4.12.

1) Пусть $p > 2$ — простое число, $a, b \in \mathbb{Z}$, $(a, p) = 1$. Доказать, что

$$\sum_{k=0}^{p-1} \left(\frac{ak + b}{p} \right) = 0.$$

2) Пусть $P \in \mathbb{N}$ нечётно, $a, b \in \mathbb{Z}$, $(a, P) = 1$. Доказать, что

$$\sum_{k=0}^{P-1} \left(\frac{ak + b}{P} \right) = \begin{cases} \varphi(P), & P \text{ — полный квадрат (т.е. } \sqrt{P} \in \mathbb{N}), \\ 0 & \text{иначе.} \end{cases}$$

Задача 4.13. Пусть $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, χ_1, \dots, χ_s — характеры по модулям $p_1^{\alpha_1}, \dots, p_s^{\alpha_s}$ соответственно. Доказать, что функция $\chi(x) = \chi_1(x) \cdots \chi_s(x)$ является характером по модулю m , причём для каждого характера по модулю m существует единственное такое представление.

Задача 4.14. Пусть $\text{ord}_m a = d$, $\zeta \in \mathbb{C}$. Доказать, что характер χ по модулю m , удовлетворяющий условию $\chi(a) = \zeta$, найдётся тогда и только тогда, когда $\zeta^d = 1$, причём в этом случае существует ровно $\frac{\varphi(m)}{d}$ таких характеров.

Задача 4.15 (почти лемма Артина). Пусть χ_1, \dots, χ_n — различные характеры Дирихле (по произвольным модулям). Доказать, что функции χ_1, \dots, χ_n линейно независимы над \mathbb{C} .

4.4 L-функции и теорема Дирихле о простых числах

Задача 4.16. Пусть χ_0 — главный характер по модулю m . Найти вычет функции $L(s, \chi_0)$ в точке $s = 1$.

Задача 4.17.

1) Пусть $\sigma > 1$, $t \in \mathbb{R}$, χ — произвольный характер по модулю m , χ_0 — главный характер по модулю m . Доказать неравенство

$$|L^3(\sigma, \chi_0) L^4(\sigma + ti, \chi) L(\sigma + 2ti, \chi^2)| \geq 1.$$

2) Доказать, что $L(s, \chi)$ не имеет нулей на прямой $\text{Re } s = 1$. (Нер-во $L(1, \chi) \neq 0$ считается известным.)

Задача 4.18 (вычисление $L(1, \chi)$).

1) Пусть χ — неглавный характер по модулю m , $P(z) = \sum_{k=1}^m \chi(k) z^{k-1}$. Доказать, что

$$L(1, \chi) = \int_0^1 \frac{P(z) dz}{1 - z^m}.$$

2) Пусть χ — неглавный характер по модулю 4. Доказать, что $L(1, \chi) = \pi/4$.

3) Доказать равенства:

$$\text{а) } 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \dots = \frac{\pi}{3\sqrt{3}};$$

$$\text{б) } 1 - \frac{1}{5} + \frac{1}{7} - \frac{1}{11} + \frac{1}{13} - \frac{1}{17} + \dots = \frac{\pi}{2\sqrt{3}}.$$

Задача 4.19.

1) Пусть χ — числовой характер. Доказать, что

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

2) Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Доказать, что

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = -\frac{\ln(s-1)}{\varphi(m)} + O(1), \quad s \rightarrow 1+0.$$

Задача 4.20. Пусть χ — неглавный числовой характер. Доказать утверждения:

1) Ряд $\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n}$ сходится. (Указание. Можно воспользоваться задачей 2.5.)

2) $\sum_{n \leq x} \frac{\chi(n)}{n} = L(1, \chi) + O\left(\frac{1}{x}\right)$. (Указание. Использовать преобразование Абеля.)

3) $\sum_{n \leq x} \frac{\chi(n) \ln n}{n} = L(1, \chi) \sum_{d \leq x} \frac{\chi(d) \Lambda(d)}{d} + O(1)$. (Указание. Использовать задачу 1.2.)

4) $\sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} = O(1)$.

5) $\sum_{p \leq x} \frac{\chi(p) \ln p}{p} = O(1)$.

Задача 4.21. Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Используя задачи 1.6 и 4.20, доказать, что:

1) $\sum_{\substack{p \leq x, \\ p \equiv a \pmod{m}}} \frac{\ln p}{p} = \frac{\ln x}{\varphi(m)} + O(1)$;

2) $\sum_{\substack{p \leq x, \\ p \equiv a \pmod{m}}} \frac{1}{p} = \frac{\ln \ln x}{\varphi(m)} + c_{m,a} + O\left(\frac{1}{\ln x}\right)$, $x \geq 2$.

Задача 4.22 (асимптотический закон распределения простых чисел в арифметических прогрессиях). Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Обозначим

$$\pi(x; m, a) = \sum_{\substack{p \leq x, \\ p \equiv a \pmod{m}}} 1, \quad \psi(x; m, a) = \sum_{\substack{n \leq x, \\ n \equiv a \pmod{m}}} \Lambda(n).$$

Возьмём $b \in \mathbb{Z}$, такое что $ab \equiv 1 \pmod{m}$, и рассмотрим функцию

$$F(s) = \frac{1}{\varphi(m)} \left(\frac{1}{s} \sum_{\chi \pmod{m}} \chi(b) \left(-\frac{L'(s, \chi)}{L(s, \chi)} \right) - \frac{1}{s-1} \right).$$

- 1) Доказать, что функция $F(s)$ голоморфна при $\operatorname{Re} s \geq 1$, причём при $\operatorname{Re} s > 1$ справедливы равенства

$$\begin{aligned} F(s) &= \frac{1}{s} \sum_{n \equiv a \pmod{m}} \frac{\Lambda(n)}{n^s} - \frac{1}{\varphi(m)(s-1)} \\ &= \int_1^{+\infty} \frac{(\psi(x; m, a) - x/\varphi(m)) dx}{x^{s+1}}. \end{aligned}$$

- 2) Используя задачу 3.41, доказать сходимость интеграла

$$\int_1^{+\infty} \frac{(\psi(x; m, a) - x/\varphi(m)) dx}{x^2}.$$

- 3) Доказать, что

$$\lim_{x \rightarrow +\infty} \frac{\pi(x; m, a)}{x/\ln x} = \lim_{x \rightarrow +\infty} \frac{\psi(x; m, a)}{x} = \frac{1}{\varphi(m)}.$$

(Замечание. Также можно было воспользоваться задачей 3.43.)

Задача 4.23. Пусть $a \in \mathbb{Z}$ таково, что для любого простого $p > 2$ символ Лежандра $\left(\frac{a}{p}\right)$ равен 0 или 1. Доказать, что a — точный квадрат (т. е. $a = b^2$, $b \in \mathbb{Z}$).

4.5 Суммы с характерами

Введём обозначение $e(z) = e^{2\pi iz}$, $z \in \mathbb{C}$. Также для $m \in \mathbb{N}$ положим: $e_m(z) = e(z/m)$ (в частности, $e_1(z) = e(z)$). Некоторые простые свойства: $e_m(z+m) = e_m(z)$ (более того, $e_m(x) = e_m(y) \Leftrightarrow \frac{x-y}{m} \in \mathbb{Z}$), $e_m(x+y) = e_m(x)e_m(y)$, $\overline{e_m(z)} = e_m(-\bar{z})$, $|e_m(z)| = e^{-2\pi \operatorname{Im} z/m}$.

Задача 4.24. Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$. Доказать, что

$$\frac{1}{m} \sum_{x=0}^{m-1} e_m(ax) = \delta_m(a) := \begin{cases} 1, & m \mid a, \\ 0, & m \nmid a. \end{cases}$$

Пусть p — простое число, χ — характер по модулю p , $a \in \mathbb{Z}$. Суммой Гаусса будем называть сумму

$$\tau_a(\chi) = \sum_{x=0}^{p-1} \chi(x) e_p(ax).$$

Для краткости будем обозначить $\tau(\chi) = \tau_1(\chi)$.

Задача 4.25 (простейшие свойства сумм Гаусса). Доказать, что:

1) если $p \mid a$, то

$$\tau_a(\chi) = \begin{cases} p-1, & \chi = \chi_0, \\ 0, & \chi \neq \chi_0; \end{cases}$$

2) если $p \nmid a$, то $\tau_a(\chi_0) = -1$;

3) если $p \nmid a$, то $\tau_a(\chi) = \chi^{-1}(a) \tau(\chi)$.

Задача 4.26 (модуль суммы Гаусса). Доказать равенства:

1) $\overline{\tau(\chi)} = \chi(-1) \tau(\chi^{-1})$.

2) Если $\chi \neq \chi_0$, то $\tau(\chi) \tau(\chi^{-1}) = \chi(-1)p$. (Указание. Сделать во внутренней сумме в равенстве $\tau(\chi) \tau(\chi^{-1}) = \sum_{y=1}^{p-1} \sum_{x=1}^{p-1} \chi(x) \chi^{-1}(y) e_p(x+y)$ замену переменной суммирования: $x \equiv yz \pmod{p}$.)

3) если $\chi \neq \chi_0$, то $|\tau(\chi)| = \sqrt{p}$.

Задача 4.27. Пусть $m \in \mathbb{N}$. Для функции $f: \mathbb{Z} \rightarrow \mathbb{C}$, такой что $f(x+m) = f(x)$ при всех $x \in \mathbb{Z}$, её дискретным преобразованием Фурье будем называть функцию $\hat{f}: \mathbb{Z} \rightarrow \mathbb{C}$, определённую по формуле

$$\hat{f}(\xi) = \frac{1}{m} \sum_{x=0}^{m-1} f(x) e_m(-\xi x).$$

Очевидно, что $\hat{f}(\xi + m) = \hat{f}(\xi)$.

1) Доказать, что $f(x) = \sum_{\xi=0}^{m-1} \hat{f}(\xi) e_m(\xi x)$.

2) Доказать равенство Парсеваля

$$\frac{1}{m} \sum_{x=0}^{m-1} f(x) \overline{g(x)} = \sum_{\xi=0}^{m-1} \hat{f}(\xi) \overline{\hat{g}(\xi)};$$

в частности,

$$\frac{1}{m} \sum_{x=0}^{m-1} |f(x)|^2 = \sum_{\xi=0}^{m-1} |\hat{f}(\xi)|^2.$$

3) Пусть $m = p$ — простое число, χ — неглавный характер по модулю p . Используя равенство Парсеваля, доказать, что $|\tau(\chi)| = \sqrt{p}$.

Задача 4.28 (квадратичные суммы Гаусса). Рассмотрим суммы

$$S(a, m) = \sum_{x=0}^{m-1} e_m(ax^2), \quad m \in \mathbb{N}, a \in \mathbb{Z}, (a, m) = 1.$$

1) Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = d$. Доказать равенство

$$\sum_{x=0}^{m-1} e_m(ax^2) = dS\left(\frac{a}{d}, \frac{m}{d}\right).$$

2) Пусть $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$, $(2a, m) = 1$. Найдём $d \in \mathbb{Z}$, такое что $2ad \equiv b \pmod{m}$. Доказать равенство

$$\sum_{x=0}^{m-1} e_m(ax^2 + bx + c) = e_m(c - ad^2)S(a, m).$$

3) Пусть $p > 2$ — простое число, $\chi(x) = \left(\frac{x}{p}\right)$ — символ Лежандра. Доказать равенство $S(a, p) = \tau_a(\chi)$ и вывести отсюда, что

$$S(a, p) = \left(\frac{a}{p}\right)S(1, p),$$

$$S^2(a, p) = \left(\frac{-1}{p}\right)p = \begin{cases} p, & p \equiv 1 \pmod{4}, \\ -p, & p \equiv -1 \pmod{4}. \end{cases}$$

(Указание. Сравнение $x^2 \equiv b \pmod{p}$ имеет $1 + \left(\frac{b}{p}\right)$ решений.)

4) Доказать, что

$$|S(a, m)|^2 = \begin{cases} m, & m \equiv 1 \pmod{2}, \\ 2m, & m \equiv 0 \pmod{4}, \\ 0, & m \equiv 2 \pmod{4}. \end{cases}$$

(Указание. В равенстве $|S(a, m)|^2 = \sum_{y=0}^{m-1} \sum_{x=0}^{m-1} e_m(a(x^2 - y^2))$ сделать во внутренней сумме замену переменной суммирования $x \equiv y + z \pmod{m}$.)

5) Пусть $(m, n) = 1$. Доказать, что

$$S(a, mn) = S(an, m)S(am, n).$$

(Указание. Если x пробегает полную систему вычетов по модулю m , а y пробегает полную систему вычетов по модулю n , то $px + ty$ пробегает полную систему вычетов по модулю mn .)

6) Пусть $p > 2$ — простое число, $\alpha \in \mathbb{N}$, $\alpha \geq 2$. Доказать, что

$$S(a, p^\alpha) = pS(a, p^{\alpha-2}).$$

(Указание. Положить $x = y + p^{\alpha-1}z$, $0 \leq y \leq p^{\alpha-1} - 1$, $0 \leq z \leq p - 1$.)

7) Пусть m нечётно. Доказать, что

$$S(a, m) = \left(\frac{a}{m}\right)S(1, m),$$

$$S^2(a, m) = \left(\frac{-1}{m}\right)m,$$

где $\left(\frac{\cdot}{m}\right)$ — символ Якоби.

8) Пусть $\alpha \in \mathbb{N}$, $\alpha \geq 4$. Доказать, что

$$S(a, 2^\alpha) = 2S(a, 2^{\alpha-2}).$$

(Указание. Положить $x = y + 2^{\alpha-2}z$, $0 \leq y \leq 2^{\alpha-2} - 1$, $0 \leq z \leq 3$.)

9) Доказать, что при $\alpha \geq 2$ выполнено

$$S(a, 2^\alpha) = \left(\frac{2^\alpha}{|a|} \right) (1 + i^a) 2^{\alpha/2}.$$

10) Известно, что для любого простого $p > 2$ выполнено

$$S(1, p) = i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p} = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod{4}, \\ i\sqrt{p}, & p \equiv -1 \pmod{4}. \end{cases}$$

(Доказать это не очень просто; Гаусс потратил на поиски доказательства более четырёх лет. Сравнительно несложное доказательство можно найти, например, в задаче 4.43.) Используя это равенство, доказать, что

$$S(a, m) = \begin{cases} \left(\frac{a}{m}\right) i^{\left(\frac{m-1}{2}\right)^2} \sqrt{m}, & m \equiv 1 \pmod{2}, \\ \left(\frac{m}{|a|}\right) (1 + i^a) \sqrt{m}, & m \equiv 0 \pmod{4}, \\ 0, & m \equiv 2 \pmod{4}. \end{cases}$$

Пусть $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, $m \in \mathbb{N}$. Под решением сравнения

$$f(x_1, \dots, x_n) \equiv 0 \pmod{m} \tag{4.1}$$

будем понимать набор классов вычетов $x_\nu \equiv a_\nu \pmod{m}$, $1 \leq \nu \leq n$, где числа $a_1, \dots, a_n \in \mathbb{Z}$ удовлетворяют сравнению $f(a_1, \dots, a_n) \equiv 0 \pmod{m}$.

Задача 4.29. Доказать, что количество решений сравнения (4.1) равно

$$\frac{1}{m} \sum_{t, x_1, \dots, x_n=0}^{m-1} e_m(tf(x_1, \dots, x_n)) = m^{n-1} + \frac{1}{m} \sum_{t=1}^{m-1} \sum_{x_1, \dots, x_n=0}^{m-1} e_m(tf(x_1, \dots, x_n)).$$

Задача 4.30. Пусть $p > 2$ — простое число, $a_1, \dots, a_n, b \in \mathbb{Z}$, $d = a_1 \cdots a_n \not\equiv 0 \pmod{p}$. Обозначим через N количество решений сравнения

$$a_1 x_1^2 + \cdots + a_n x_n^2 + b \equiv 0 \pmod{p}.$$

Доказать равенства:

1) Если n чётно, то

$$N = \begin{cases} p^{n-1} + \left(\frac{(-1)^{n/2}d}{p}\right) p^{n/2-1}(p-1), & b \equiv 0 \pmod{p}, \\ p^{n-1} - \left(\frac{(-1)^{n/2}d}{p}\right) p^{n/2-1}, & b \not\equiv 0 \pmod{p}. \end{cases}$$

2) Если n нечётно, то

$$N = p^{n-1} + \left(\frac{(-1)^{(n+1)/2} bd}{p} \right) p^{(n-1)/2}.$$

(Указание. Использовать задачи 4.29 и 4.28.)

Задача 4.31 (внезапно квадратичный закон взаимности). Вывести из задачи 4.30 квадратичный закон взаимности для символа Лежандра вместе с двумя его дополнениями:

1) Пусть $p > 2$ — простое число. Рассматривая сравнение $x_1^2 + x_2^2 - 2 \equiv 0 \pmod{p}$, доказать, что

$$p - \left(\frac{-1}{p} \right) \equiv 6 + 2 \left(\frac{2}{p} \right) \pmod{8}.$$

Вывести отсюда формулы для $\left(\frac{-1}{p} \right)$ и $\left(\frac{2}{p} \right)$. (Указание. Почти все решения сравнения разбиваются на восьмёрки вида $(\pm c_1, \pm c_2)$, $(\pm c_2, \pm c_1)$.)

2) Пусть p, q — различные нечётные простые числа. Рассматривая сравнение

$$x_1^2 + \dots + x_q^2 - q \equiv 0 \pmod{p},$$

доказать квадратичный закон взаимности. (Указание. Разбить решения на группы вида (c_1, c_2, \dots, c_q) , (c_2, c_3, \dots, c_1) , \dots , $(c_q, c_1, \dots, c_{q-1})$.)

Задача 4.32. Пусть p — простое число, $r \in \mathbb{N}$, $d = (r, p-1)$. Рассмотрим суммы

$$S_r(a, p) = \sum_{x=0}^{p-1} e_p(ax^r), \quad a \in \mathbb{Z}.$$

1) Пусть χ — характер по модулю p порядка d ($\Leftrightarrow \chi(g) = e_d(1)$ для некоторого первообразного корня g по модулю p). Доказать, что сравнение $x^r \equiv b \pmod{p}$ при $p \nmid b$ имеет $\sum_{k=0}^{d-1} \chi^k(b)$ решений. (Указание. Группа $(\mathbb{Z}/p\mathbb{Z})^*$ циклическая.)

2) Пусть $p \nmid a$. Доказать равенства

$$S_r(a, p) = S_d(a, p) = \sum_{k=1}^{d-1} \tau_a(\chi^k).$$

3) Пусть $p \nmid a$. Доказать неравенство

$$|S_r(a, p)| \leq (d-1)\sqrt{p}.$$

4) Доказать, что для любых p, r найдётся $a \not\equiv 0 \pmod{p}$, такое что

$$|S_r(a, p)| \geq \sqrt{(d-1)p}.$$

(Указание. Рассмотреть $\sum_{a=0}^{p-1} |S_r(a, p)|^2$.)

Задача 4.33. Пусть p — простое число, $r_1, \dots, r_n \in \mathbb{N}$, $a_1, \dots, a_n, b \in \mathbb{Z}$, $p \nmid a_1 \cdots a_n$. Обозначим через N количество решений сравнения

$$a_1 x_1^{r_1} + \dots + a_n x_n^{r_n} + b \equiv 0 \pmod{p}.$$

Также положим $d_\nu = (r_\nu, p-1)$, $1 \leq \nu \leq n$. Доказать неравенства:

- 1) $|N - p^{n-1}| \leq (d_1 - 1) \cdots (d_n - 1)(p-1)p^{n/2-1}$;
- 2) если $p \nmid b$, то $|N - p^{n-1}| \leq (d_1 - 1) \cdots (d_n - 1)p^{(n-1)/2}$.

Задача 4.34. Пусть $p > 2$ — простое число. Доказать утверждения:

- 1) Если $a \in \mathbb{Z}$, то

$$\sum_{x=0}^{p-1} \left(\frac{x^2 + a}{p} \right) = p\delta_p(a) - 1 = \begin{cases} p-1, & a \equiv 0 \pmod{p}, \\ -1, & a \not\equiv 0 \pmod{p}. \end{cases}$$

(Указание. Рассмотреть количество решений сравнения $y^2 \equiv x^2 + a \pmod{p}$.)

- 2) Если $a, b, c \in \mathbb{Z}$, $p \nmid a$, то

$$\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right) = \left(\frac{a}{p} \right) (p\delta_p(b^2 - 4ac) - 1).$$

- 3) Если $a, b \in \mathbb{Z}$, то

$$\sum_{x=0}^{p-1} \left(\frac{(x+a)(x+b)}{p} \right) = p\delta_p(a-b) - 1.$$

Задача 4.35. Пусть $p > 2$ — простое число, $c \in \mathbb{Z}$, $p \nmid c$. Для $\alpha, \beta \in \{1, -1\}$ обозначим через $N(\alpha, \beta)$ количество $x \in \{0, 1, \dots, p-1\}$, таких что $\left(\frac{x}{p}\right) = \alpha$, $\left(\frac{x+c}{p}\right) = \beta$. Доказать, что

$$N(\alpha, \beta) = \frac{1}{4} \left(p - 2 - \alpha \left(\frac{-c}{p} \right) - \beta \left(\frac{c}{p} \right) - \alpha\beta \right).$$

(Указание. $N(\alpha, \beta) = \frac{1}{4} \sum_{x \neq 0, -c} \left(1 + \alpha \left(\frac{x}{p} \right) \right) \left(1 + \beta \left(\frac{x+c}{p} \right) \right)$.)

Задача 4.36.

- 1) Пусть $a \in \mathbb{Z}$, $N \in \mathbb{N}$, $\alpha, \beta \in \mathbb{R}$. Доказать, что

$$\left| \sum_{x=a}^{a+N-1} e(\alpha x + \beta) \right| \leq \min \left\{ N, \frac{1}{|\sin(\pi\alpha)|} \right\} \leq \min \left\{ N, \frac{1}{2\|\alpha\|} \right\},$$

где $\|\alpha\| = \min_{n \in \mathbb{Z}} |\alpha - n|$.

- 2) Пусть $m \in \mathbb{N}$, $m > 1$, $a \in \mathbb{Z}$, $(a, m) = 1$. Доказать неравенство

$$\sum_{x=1}^{m-1} \frac{1}{\left\| \frac{ax}{m} \right\|} < 2m \ln m.$$

(Указание. $\frac{1}{x} < \ln(x+1/2) - \ln(x-1/2)$ при $x > 1/2$.)

- 3) Пусть $m \in \mathbb{N}$, $m > 1$, $f: \mathbb{Z} \rightarrow \mathbb{C}$, причём $f(x+m) = f(x)$ при всех $x \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, $(a, m) = 1$, $N \in \mathbb{N}$. Доказать неравенство

$$\left| \sum_{x=0}^{N-1} f(ax+b) - \frac{N}{m} \sum_{x=0}^{m-1} f(x) \right| \leq \max_{1 \leq \xi \leq m-1} \left| \sum_{x=0}^{m-1} f(x) e_m(\xi x) \right| \cdot \ln m.$$

(Указание. Использовать п. 1 задачи 4.27.)

Задача 4.37 (неравенство Пойа–Виноградова). Пусть χ — неглавный характер по модулю m , $a, b \in \mathbb{Z}$, $(a, m) = 1$, $N \in \mathbb{N}$. Доказать, что

$$\left| \sum_{x=0}^{N-1} \chi(ax+b) \right| < \sqrt{m} \ln m.$$

(Указание. См. задачу 4.36.)

Задача 4.38. Пусть $p > 2$ — простое число, $a \in \mathbb{Z}$, $N \in \mathbb{N}$, $N \leq p$. Доказать, что количество квадратичных (не)вычетов по модулю p среди чисел $a, a+1, \dots, a+N-1$ равно $\frac{1}{2}N + O(\sqrt{p} \ln p)$. (Указание. Применить неравенство Пойа–Виноградова для символа Лежандра.)

Задача 4.39 (оценки для наименьшего квадратичного невычета). Пусть $p > 2$ — простое число, $n = n(p)$ — наименьший положительный квадратичный невычет по модулю p . Доказать утверждения:

- 1) $n = O(\sqrt{p} \ln p)$.
- 2) $n < 1/2 + \sqrt{p+1/4}$. (Указание. Рассмотрев произведение $n[p/n]$, доказать, что $[p/n]$ — квадратичный невычет, откуда следует $n \leq [p/n]$. Здесь $[x]$ — наименьшее целое $\geq x$.)
- 3) Каждый положительный квадратичный невычет по модулю p имеет простой делитель $\geq n$.
- 4) Используя п. 3 и задачи 4.12, 4.38, доказать оценку $n = O\left(p^{\frac{1}{2\sqrt{e}}} (\ln p)^{\frac{2}{\sqrt{e}}}\right)$. (Указание. Допустим, что $n > p^{0.1}$. Положим $N = \lfloor \sqrt{p} \ln^2 p \rfloor$. Тогда

$$\frac{1}{2}N + O(\sqrt{p} \ln p) \leq \sum_{n \leq q \leq N} \frac{N}{q} = N \left(\ln \frac{\ln N}{\ln n} + O\left(\frac{1}{\ln p}\right) \right),$$

где q пробегает простые числа, откуда $n = O(N^{1/\sqrt{e}})$.)

Задача 4.40 (суммы Якобсталя). Пусть $p > 2$ — простое число. Обозначим

$$S(a) = \sum_{x=0}^{p-1} \left(\frac{x(x^2+a)}{p} \right), \quad a \in \mathbb{Z}.$$

Доказать утверждения:

- 1) Если $p \equiv -1 \pmod{4}$, то $S(a) = 0$ для любого $a \in \mathbb{Z}$.

- 2) $\frac{1}{2}S(a) \in \mathbb{Z}$ для любого $a \in \mathbb{Z}$.
- 3) $S(ab^2) = \left(\frac{b}{p}\right) S(a)$ для любых $a, b \in \mathbb{Z}$.
- 4) $\sum_{a=0}^{p-1} S^2(a) = \begin{cases} 2p(p-1), & p \equiv 1 \pmod{4}, \\ 0, & p \equiv -1 \pmod{4}. \end{cases}$ (Указание. См. задачу 4.34.)
- 5) Если $p \equiv 1 \pmod{4}$, $\left(\frac{a}{p}\right) = 1$, $\left(\frac{b}{p}\right) = -1$, то $p = \left(\frac{1}{2}S(a)\right)^2 + \left(\frac{1}{2}S(b)\right)^2$.
- 6) Если $d \in \mathbb{N}$, $(p-1) \nmid d$, то $\sum_{x=0}^{p-1} x^d \equiv 0 \pmod{p}$. (Указание. Группа $(\mathbb{Z}/p\mathbb{Z})^*$ циклическая.)
- 7) Если $p = 4n + 1$, $n \in \mathbb{N}$, то $S(1) \equiv -\binom{2n}{n} \pmod{p}$. (Указание. Использовать критерий Эйлера для символа Лежандра.)

Задача 4.41 (суммы Якоби). Пусть p — простое число, χ_1, χ_2 — характеры по модулю p , $a \in \mathbb{Z}$. Обозначим

$$J_a(\chi_1, \chi_2) = \sum_{x=0}^{p-1} \chi_1(x) \chi_2(a-x).$$

Для краткости положим $J(\chi_1, \chi_2) = J_1(\chi_1, \chi_2)$. Доказать равенства:

- 1) $J_a(\chi_1, \chi_2) = J_a(\chi_2, \chi_1)$.
- 2) Если $p \mid a$, то
- $$J_a(\chi_1, \chi_2) = \begin{cases} (p-1)\chi_2(-1), & \chi_1\chi_2 = \chi_0, \\ 0, & \chi_1\chi_2 \neq \chi_0. \end{cases}$$
- 3) Если $p \nmid a$, то $J_a(\chi_1, \chi_2) = \chi_1(a)\chi_2(a)J(\chi_1, \chi_2)$.
- 4) $J(\chi, \chi_0) = \begin{cases} p-2, & \chi = \chi_0, \\ -1, & \chi \neq \chi_0. \end{cases}$
- 5) Если $\chi \neq \chi_0$, то $J(\chi, \chi^{-1}) = -\chi(-1)$. (Указание. Сделать замену переменной суммирования $y \equiv x(1-x)^{-1} \pmod{p}$.)
- 6) Если $\chi_1\chi_2 \neq \chi_0$, то
- $$J(\chi_1, \chi_2) = \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)}.$$
- 7) Если характеры $\chi_1, \chi_2, \chi_1\chi_2$ неглавные, то $|J(\chi_1, \chi_2)| = \sqrt{p}$.

Задача 4.42.

- 1) Пусть $p > 2$ — простое число, $a \in \mathbb{Z}$, χ — характер по модулю p , $\chi^2 \neq \chi_0$, $\chi_1(x) = \left(\frac{x}{p}\right)$ — символ Лежандра. Доказать, что

$$\sum_{x=0}^{p-1} \chi(x^2 + a) = \chi(a)\chi_1(-a) \frac{\tau(\chi)\tau(\chi_1)}{\tau(\chi\chi_1)}.$$

- 2) Пусть p — простое число, $p \equiv 1 \pmod{4}$, χ — характер по модулю p , такой что $\chi(g) = i$, где g — некоторый п.к. по модулю p . Определим $a, b \in \mathbb{Z}$ с помощью равенства

$$\sum_{x=0}^{p-1} \chi(x^2 + 1) = a + bi.$$

Доказать, что $p = a^2 + b^2$.

Задача 4.43 (вычисление квадратичной суммы Гаусса). Пусть $m \in \mathbb{N}$, $f(z) = \frac{e_m(z^2)}{e(z)-1}$,

$S = \sum_{x=0}^{m-1} e_m(x^2)$. Доказать равенства:

- 1) $S = \int_{L_{m-1/2}} f(z) dz - \int_{L_{-1/2}} f(z) dz$, где L_α — прямая $y = x - \alpha$, пробегаемая снизу вверх. (*Указание.* Применить теорему Коши о вычетах к параллелограмму с вершинами в точках $-1/2 \pm Ne^{\pi i/4}$, $m - 1/2 \pm Ne^{\pi i/4}$ и перейти к пределу при $N \rightarrow +\infty$.)

- 2) $S = \int_{L_{-1/2}} e_m(z^2)(e(z) + 1) dz$. (*Указание.* $f(z + m) = e(2z)f(z)$.)

- 3) $S = (1 + i^{-m}) \int_{L_0} e_m(z^2) dz = \frac{1 + i^{-m}}{1 + i^{-1}} \sqrt{\frac{m}{\pi}} \int_{-\infty}^{+\infty} e^{-x^2} dx$. (*Указание.* $\int_{L_\alpha} e_m(z^2) dz$ не зависит от α .)

- 4) Вывести из п. 3 формулы для гауссова интеграла (интеграла Эйлера–Пуассона)

$$\int_{-\infty}^{+\infty} e^{-x^2} dx = \sqrt{\pi}$$

и для (квадратичной) суммы Гаусса

$$\sum_{x=0}^{m-1} e_m(x^2) = \frac{1 + i^{-m}}{1 + i^{-1}} \sqrt{m} = \begin{cases} (1 + i)\sqrt{m}, & m \equiv 0 \pmod{4}, \\ \sqrt{m}, & m \equiv 1 \pmod{4}, \\ 0, & m \equiv 2 \pmod{4}, \\ i\sqrt{m}, & m \equiv 3 \pmod{4}. \end{cases}$$

Глава 5

Диофантовы приближения и геометрия чисел

5.1 Диофантовы приближения

В следующих задачах через $\|x\|$ обозначено расстояние от числа $x \in \mathbb{R}$ до ближайшего целого числа, т. е. $\|x\| = \min_{a \in \mathbb{Z}} |x - a| = \min\{\{x\}, 1 - \{x\}\}$. Очевидные свойства: $\|x + y\| \leq \|x\| + \|y\|$, $\|nx\| \leq n\|x\|$ при $n \in \mathbb{N}$, $\|-x\| = \|x\|$, $\| \|x\| - \|y\| \| \leq \|x - y\|$.

Задача 5.1 (теорема Дирихле). Пусть $\alpha \in \mathbb{R}$. Доказать утверждения:

- 1) Для любого $t \in \mathbb{N}$ найдётся $q \in \mathbb{N}$, такое что

$$\|\alpha q\| \leq \frac{1}{t+1}, \quad q \leq t.$$

(Указание. Рассмотреть дробные доли $\{\alpha x\} \in [0, 1)$ для $x = 0, 1, \dots, t$ и разбить промежуток $[0, 1)$ на промежутки вида $\left[\frac{j}{t+1}, \frac{j+1}{t+1}\right)$. Далее разобрать два случая: когда в самом правом промежутке $\left[\frac{t}{t+1}, 1\right)$ что-то есть, и когда нет.)

- 2) Для любого $\tau \in [1, +\infty)$ найдётся $q \in \mathbb{N}$, такое что

$$\|\alpha q\| < \frac{1}{\tau}, \quad q \leq \tau.$$

- 3) Для любого $\tau \in [1, +\infty)$ найдётся несократимая рациональная дробь $\frac{a}{q}$, такая что

$$\left| \alpha - \frac{a}{q} \right| < \frac{1}{\tau q}, \quad q \leq \tau.$$

Задача 5.2 (принцип Дирихле). Пусть $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, $Q \in \mathbb{N}$. Доказать утверждения:

- 1) Существует $q \in \mathbb{N}$, такое что

$$\max_{1 \leq j \leq n} \|\alpha_j q\| < Q^{-1}, \quad q \leq Q^n.$$

- 2) Пусть хотя бы одно из чисел α_j иррационально. Тогда существует бесконечно много наборов рациональных чисел $(\frac{a_1}{q}, \dots, \frac{a_n}{q})$, удовлетворяющих неравенству

$$\max_{1 \leq j \leq n} \left| \alpha_j - \frac{a_j}{q} \right| < q^{-1-1/n}.$$

- 3) Существуют целые числа q_1, \dots, q_n , такие что

$$\|\alpha_1 q_1 + \dots + \alpha_n q_n\| < Q^{-n}, \quad 0 < \max_{1 \leq j \leq n} |q_j| \leq Q.$$

- 4) Пусть числа $1, \alpha_1, \dots, \alpha_n$ линейно независимы над \mathbb{Q} . Тогда существует бесконечно много примитивных векторов $(a, q_1, \dots, q_n) \in \mathbb{Z}^{n+1}$, удовлетворяющих неравенству

$$|a + \alpha_1 q_1 + \dots + \alpha_n q_n| < \left(\max_{1 \leq j \leq n} |q_j| \right)^{-n}.$$

Задача 5.3 (лемма Бlichфельда). Пусть измеримое (по Лебегу) множество $A \subseteq \mathbb{R}^d$ имеет меру больше 1. Доказать, что существуют две различные точки $x, y \in A$, такие что $x - y \in \mathbb{Z}^d$.

Задача 5.4 (первая теорема Минковского о выпуклом теле).

- 1) Пусть $\Omega \subseteq \mathbb{R}^d$ — ограниченное выпуклое множество, (центрально) симметричное относительно начала координат. Допустим, что мера Жордана⁴ $\text{vol} \Omega$ множества Ω больше 2^d . Доказать, что $\Omega \cap (\mathbb{Z}^d \setminus \{\mathbf{0}\}) \neq \emptyset$. (Указание. Применить лемму Бlichфельда для $A = \frac{1}{2}\Omega$.)
- 2) Доказать, что теорема Минковского справедлива и при $\text{vol} \Omega = 2^d$, если дополнительно предположить, что Ω замкнуто.

Задача 5.5 (теорема Минковского о линейных формах).

- 1) Рассмотрим линейные формы

$$L_\mu(x) = \sum_{\nu=1}^d \alpha_{\mu,\nu} x_\nu, \quad 1 \leq \mu \leq d,$$

с вещественными коэффициентами $\alpha_{\mu,\nu}$ и определителем $\Delta = \det(\alpha_{\mu,\nu})$. Допустим, что положительные числа $\varepsilon_1, \dots, \varepsilon_d$ удовлетворяют неравенству $\varepsilon_1 \cdots \varepsilon_d \geq |\Delta|$. Доказать, что система неравенств

$$\begin{aligned} |L_1(x)| &\leq \varepsilon_1, \\ |L_\mu(x)| &< \varepsilon_\mu, \quad 1 < \mu \leq d, \end{aligned}$$

имеет решение $x \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$.

- 2) Доказать, что утверждения пунктов 1 и 3 задачи 5.2 справедливы при любом $Q \in [1, +\infty)$.

⁴Можно доказать, что произвольное ограниченное выпуклое множество в \mathbb{R}^n измеримо по Жордану.

3) Пусть линейные формы

$$L_\mu(x) = \sum_{\nu=1}^n \alpha_{\mu,\nu} x_\nu, \quad 1 \leq \mu \leq m,$$

имеют вещественные коэффициенты $\alpha_{\mu,\nu}$. Доказать, что для любого $X \in [1, +\infty)$ найдётся вектор $x \in \mathbb{Z}^n \setminus \{0\}$, такой что

$$\max_{1 \leq \mu \leq m} \|L_\mu(x)\| < X^{-n/m}, \quad \max_{1 \leq \nu \leq n} |x_\nu| \leq X.$$

4) *Комплексный случай* (сохраняем обозначения пункта 1). Пусть положительные числа $\varepsilon_1, \dots, \varepsilon_{d_1+d_2}$ удовлетворяют неравенству

$$\varepsilon_1 \cdots \varepsilon_{d_1} \varepsilon_{d_1+1}^2 \cdots \varepsilon_{d_1+d_2}^2 \geq \left(\frac{4}{\pi}\right)^{d_2} |\Delta|,$$

$d = d_1 + 2d_2$. Доказать, что система неравенств

$$\begin{aligned} |L_\mu(x)| &\leq \varepsilon_\mu, & 1 \leq \mu \leq d_1, \\ |L_\mu(x) + iL_{\mu+d_2}(x)| &\leq \varepsilon_\mu, & d_1 < \mu \leq d_1 + d_2, \end{aligned}$$

имеет решение $x \in \mathbb{Z}^d \setminus \{0\}$, причём все неравенства, кроме одного (любого), можно заменить на строгие.

Задача 5.6. Пусть $\alpha_1, \dots, \alpha_n \in \mathbb{R}$. Доказать утверждения:

1) Для любых $M, t > 0$ множество

$$\Omega(M, t) = \{(x, y_1, \dots, y_n) \in \mathbb{R}^{n+1} \mid t^{-n}|x| + nt \max_{1 \leq j \leq n} |y_j - \alpha_j x| \leq M\}$$

компактно, выпукло, симметрично относительно начала координат и имеет меру Жордана $\frac{(2M)^{n+1}}{(n+1)n^n}$. (Указание. С помощью линейного преобразования свести к случаю $\alpha_j = 0$, $t = 1$.)

2) Если $(x, y_1, \dots, y_n) \in \Omega(M, t)$, $t^{-n}|x| \neq t \max_{1 \leq j \leq n} |y_j - \alpha_j x|$, то

$$|x| \left(\max_{1 \leq j \leq n} |y_j - \alpha_j x| \right)^n < \left(\frac{M}{n+1} \right)^{n+1}.$$

3) Существует бесконечно много $q \in \mathbb{N}$, таких что

$$q^{1/n} \max_{1 \leq j \leq n} \|\alpha_j q\| < \frac{n}{n+1}.$$

4) Существует бесконечно много $q \in \mathbb{N}$, таких что

$$q \prod_{j=1}^n \|\alpha_j q\| < \frac{n!}{(n+1)^n}.$$

Задача 5.7 (вокруг одномерной теоремы Кронекера).

- 1) Пусть $\alpha \in \mathbb{R}$. Доказать, что множество дробных долей $\{\alpha n\}$, $n \in \mathbb{N}$, плотно в $[0, 1]$ тогда и только тогда, когда α иррационально.
- 2) Найти множества предельных точек последовательностей $\cos n$, $\sin n$, e^{ni} .
- 3) Пусть $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $\beta \in \mathbb{R}$. Доказать, что найдётся бесконечно много $n \in \mathbb{N}$, таких что

$$\|\alpha n + \beta\| < \frac{C}{n},$$

где C — некоторая постоянная, не зависящая от α, β . (Указание. Взять несократимую дробь $\frac{a}{q}$, такую что $|\alpha - \frac{a}{q}| < \frac{1}{q^2}$; найти $b \in \mathbb{Z}$, такое что $|\beta - \frac{b}{q}| < \frac{1}{q}$; наконец, подобрать n , чтобы $\alpha n + b \equiv 0 \pmod{q}$, $q \leq n < 2q$.)

- 4) Найти все предельные точки последовательностей $(\cos n)^n$, $(\sin n)^n$. (Ответ: $[-1, 1]$ оба раза. Указание. Для косинуса брать n вида $n = (2k + 1)m$, где k таково, что $|(2k + 1) - (\pi + 2\pi l)| = O(1/k)$, $m = m(k)$. Для синуса аналогично.)

5.2 Решётки

Пусть векторы $e_1, \dots, e_n \in \mathbb{R}^d$ линейно независимы над \mathbb{R} . Множество

$$\Lambda = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n = \{a_1e_1 + \dots + a_ne_n \mid a_1, \dots, a_n \in \mathbb{Z}\}$$

называется (n -мерной) решёткой в \mathbb{R}^d , а (упорядоченный) набор векторов e_1, \dots, e_n — базисом решётки Λ . Если $n = d$, то решётка Λ называется *полной*, в противном случае — *неполной*.

Задача 5.8. Пусть Λ — решётка с базисом e_1, \dots, e_n . Рассмотрим векторы

$$\varepsilon_j = \sum_{i=1}^n c_{ij}e_i \in \Lambda, \quad 1 \leq j \leq n.$$

Доказать, что набор $\varepsilon_1, \dots, \varepsilon_n$ является базисом Λ тогда и только тогда, когда матрица $C = (c_{ij})$ унимодулярна (т.е. $C \in \text{GL}_n(\mathbb{Z})$, или $|\det C| = 1$).

Пусть Λ — решётка с базисом e_1, \dots, e_n . *Определителем* $\det(\Lambda)$ решётки Λ называется n -мерный объём параллелепипеда, натянутого на векторы e_1, \dots, e_n , т.е. если рассмотреть матрицу

$$E = (e_1, \dots, e_n) = \begin{pmatrix} e_{1,1} & \dots & e_{1,n} \\ \dots & \dots & \dots \\ e_{d,1} & \dots & e_{d,n} \end{pmatrix},$$

то

$$\det(\Lambda) = \sqrt{\det(\langle e_i, e_j \rangle)_{i,j=1}^n} = \sqrt{\det(E^T E)}.$$

Если решётка Λ полная, то $\det(\Lambda) = |\det E|$.

Задача 5.9. Доказать, что определение корректно (т.е. определитель решётки не зависит от выбора базиса).

Задача 5.10 (снова теорема Минковского). Пусть Λ — полная решётка в \mathbb{R}^d , $\Omega \subseteq \mathbb{R}^d$ — ограниченное выпуклое множество, симметричное относительно начала координат, объём которого больше $2^d \det(\Lambda)$. Доказать, что $\Omega \cap (\Lambda \setminus \{0\}) \neq \emptyset$.

Задача 5.11 (теорема Ферма–Эйлера о двух квадратах).

- 1) Доказать, что для любых $m \in \mathbb{N}$, $a \in \mathbb{Z}$ множество

$$\Lambda(m, a) = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid x \equiv ay \pmod{m} \right\}$$

является полной решёткой в \mathbb{R}^2 с определителем m , причём в круге $x^2 + y^2 < 2m$ есть ненулевая точка решётки $\Lambda(m, a)$.

- 2) Пусть $m \in \mathbb{N}$ таково, что сравнение $z^2 + 1 \equiv 0 \pmod{m}$ разрешимо. Доказать, что уравнение $x^2 + y^2 = m$ разрешимо в целых числах x, y . (Указание. Рассмотреть $\Lambda(m, a)$, где $a^2 + 1 \equiv 0 \pmod{m}$.)
- 3) Доказать, что сравнение $z^2 + 1 \equiv 0 \pmod{m}$ разрешимо тогда и только тогда, когда m не делится на 4 и не делится ни на какое простое $p \equiv -1 \pmod{4}$.
- 4) Доказать, что число $n \in \mathbb{N}$ можно представить в виде суммы двух квадратов целых чисел тогда и только тогда, когда для всякого простого $p \equiv -1 \pmod{4}$ число $v_p(n)$ чётно.

Задача 5.12 (теорема Лагранжа о четырёх квадратах).

- 1) Доказать, что для любого простого p сравнение $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ разрешимо. (Указание. Переписать сравнение в виде $x^2 \equiv -y^2 - 1$.)
- 2) Доказать, что сравнение $x^2 + y^2 + 1 \equiv 0 \pmod{m}$ разрешимо тогда и только тогда, когда $4 \nmid m$.
- 3) Пусть $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Доказать, что в (4-мерном) шаре $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2m$ найдётся ненулевое решение системы сравнений

$$\begin{cases} x_3 \equiv ax_1 - bx_2 \pmod{m}, \\ x_4 \equiv bx_1 + ax_2 \pmod{m}. \end{cases}$$

- 4) Доказать, что для любого $n \in \mathbb{N}$ уравнение $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ разрешимо в целых числах x_1, x_2, x_3, x_4 .

Подрешёткой решётки Λ называется подмножество $\Gamma \subseteq \Lambda$, которое само является решёткой.

Задача 5.13. Пусть Λ — решётка, $\Gamma \subseteq \Lambda$. Доказать, что Γ является подрешёткой тогда и только тогда, когда Γ — (под)группа по сложению. (Указание. Свести к случаю $\Lambda = \mathbb{Z}^n$ и воспользоваться тем, что подгруппа конечно порождённой абелевой группы тоже является конечно порождённой.)

Задача 5.14. Пусть $\Gamma \subseteq \Lambda$ — n -мерные решётки.

- 1) Доказать, что можно найти базисы e_1, \dots, e_n и $\varepsilon_1, \dots, \varepsilon_n$ решёток Λ и Γ соответственно, такие что $\varepsilon_j = d_j e_j$, $j = 1, \dots, n$, где d_j — некоторые натуральные числа (причём можно сделать так, что $d_j \mid d_{j+1}$ при $j = 1, \dots, n-1$; тогда числа d_j определены однозначно). При этом индекс $[\Lambda : \Gamma]$ подгруппы Γ в группе Λ конечен и равен

$$[\Lambda : \Gamma] = d_1 \cdots d_n = \frac{\det(\Gamma)}{\det(\Lambda)}.$$

(Замечание-указание. Если C — матрица перехода от e_j к ε_j , то замена базисов сводится к преобразованиям над строками и столбцами матрицы C . Очевидно, что такими преобразованиями можно привести матрицу к диагональному виду. В случае $d_j \mid d_{j+1}$ получается нормальная форма Смита матрицы C .)

- 2) Пусть e_1, \dots, e_n — базис Λ , $\varepsilon_1, \dots, \varepsilon_n$ — базис Γ , $C = (c_{ij})$ — матрица перехода от e_1, \dots, e_n к $\varepsilon_1, \dots, \varepsilon_n$, т.е.

$$\varepsilon_j = \sum_{i=1}^n c_{ij} e_i, \quad 1 \leq j \leq n.$$

Доказать, что $[\Lambda : \Gamma] = |\det C|$.

Задача 5.15. Доказать, что множество Λ всех решений $x = (x_1, \dots, x_n)^T$ однородной системы линейных сравнений

$$\sum_{j=1}^n a_{ij} x_j \equiv 0 \pmod{d_i}, \quad 1 \leq i \leq m,$$

является полной решёткой в \mathbb{R}^n с определителем $\det(\Lambda) \leq d_1 \cdots d_m$. (Указание. Рассмотреть Λ как подрешётку \mathbb{Z}^n и оценить её индекс.)

Задача 5.16. Пусть Λ — подгруппа \mathbb{R}^d по сложению. Доказать, что Λ — решётка тогда и только тогда, когда Λ дискретно (т.е. не имеет предельных точек).

5.3 Ряды Фарея

В этом параграфе p — целое число (необязательно простое).

Для двух рациональных дробей $\frac{a}{b}, \frac{c}{d}$ их медиантой называется дробь $\frac{a+c}{b+d}$ (здесь дробь $\frac{p}{q}$ нужно понимать не как число, а как пару чисел p, q , чтобы определение было корректно).

Задача 5.17. Доказать следующие свойства медианты:

- 1) если $\frac{a}{b} < \frac{c}{d}$, то $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$;
 2) если $\left| \frac{a}{b} - \frac{c}{d} \right| = \frac{1}{bd}$, то $\left| \frac{a}{b} - \frac{a+c}{b+d} \right| = \frac{1}{b(b+d)}$ и $\left| \frac{a+c}{b+d} - \frac{c}{d} \right| = \frac{1}{(b+d)d}$.

Задача 5.18 (ряды Фарея). Определим конечные последовательности F_n рациональных дробей, упорядоченных в порядке возрастания. Положим $F_1 = \left\{ \frac{0}{1}, \frac{1}{1} \right\}$. Если F_n уже построено, то F_{n+1} получается из F_n следующим образом: для каждой пары $\frac{a}{b}, \frac{c}{d}$ соседних дробей в F_n , таких что $b + d = n + 1$, добавим между ними их медианту $\frac{a+c}{b+d}$. (Получаем: $F_2 = \left\{ \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \right\}$, $F_3 = \left\{ \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \right\}$, $F_4 = \left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \right\}$ и т. д.) Доказать следующие свойства F_n :

- 1) Если $\frac{a}{b}, \frac{c}{d}$ — соседние дроби в F_n , то $\left| \frac{a}{b} - \frac{c}{d} \right| = \frac{1}{bd}$.
- 2) Все дроби в F_n несократимы.
- 3) Если $\frac{a}{b}, \frac{c}{d}$ — соседние дроби в F_n , то $b + d > n$.
- 4) Если $\frac{a}{b} < \frac{c}{d}$ — соседние дроби в F_n , $\frac{k}{n+1} \in \left(\frac{a}{b}, \frac{c}{d} \right)$, то $a + c = k$, $b + d = n + 1$.
- 5) F_n состоит из всех несократимых дробей из отрезка $[0, 1]$, знаменатель которых не превосходит n .
- 6) Если $\frac{a}{b} < \frac{u}{v} < \frac{c}{d}$ — три последовательные дроби в F_n , то $\frac{u}{v} = \frac{a+c}{b+d}$.

Задача 5.19 (снова теорема Дирихле). Пусть $\frac{a}{b} < \frac{c}{d}$ — соседние дроби в F_n , $\alpha \in \left[\frac{a}{b}, \frac{c}{d} \right]$. Доказать, что хотя бы одна из дробей $\frac{a}{b}, \frac{c}{d}$ даёт решение неравенства $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{(n+1)q}$. Вывести отсюда теорему Дирихле о приближениях (см. задачу 5.4).

Задача 5.20. Пусть $\alpha \in \left[\frac{a}{b}, \frac{c}{d} \right]$, $\left| \frac{a}{b} - \frac{c}{d} \right| = \frac{1}{bd}$. Доказать, что:

- 1) хотя бы одна из дробей $\frac{a}{b}, \frac{c}{d}$ даёт решение неравенства $\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2}$, кроме случая $b = d = 1$, $\alpha = a + \frac{1}{2}$;
- 2) хотя бы одна из дробей $\frac{a}{b}, \frac{c}{d}, \frac{a+c}{b+d}$ даёт решение неравенства $\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}$.

Задача 5.21 (теорема Гурвица).

- 1) Доказать, что для любого $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ существует бесконечно много рациональных чисел $\frac{p}{q}$, удовлетворяющих неравенству

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

- 2) Пусть $\alpha = \frac{1+\sqrt{5}}{2}$. Доказать, что для любого $\varepsilon > 0$ неравенство

$$\left| \alpha - \frac{p}{q} \right| < \frac{1-\varepsilon}{\sqrt{5}q^2}$$

имеет конечное число решений $\frac{p}{q} \in \mathbb{Q}$. (Указание. $q^2 \left| \alpha - \frac{p}{q} \right| \cdot \left| \alpha - \frac{p}{q} - \sqrt{5} \right| \in \mathbb{N}$.)

Глава 6

Цепные дроби

To be written.

Глава 7

Алгебраические числа

7.1 Неприводимые многочлены

Все рассматриваемые многочлены имеют рациональные коэффициенты. Под неприводимостью понимается неприводимость над \mathbb{Q} . Многочлены с целыми коэффициентами будем называть *целочисленными*, а многочлены со старшим коэффициентом 1 — *унитарными*.

Задача 7.1. Доказать неприводимость многочленов: $z^4 + 1$, $z^n \pm 2$ ($n \in \mathbb{N}$).

Задача 7.2 (неприводимость многочленов маленькой степени).

- 1) Доказать, что многочлен степени 2 или 3 приводим тогда и только тогда, когда у него есть рациональный корень.
- 2) Пусть $P(z) = a_n z^n + \dots + a_0 \in \mathbb{Z}[z]$, $a_0 a_n \neq 0$. Доказать, что любой рациональный корень многочлена P имеет вид a/b , где $a \mid a_0$, $b \mid a_n$.
- 3) Доказать неприводимость многочленов $z^3 \pm z \pm 1$, $2z^3 + 3z^2 + 1$, $3z^3 + z^2 - 2z + 2$.

Задача 7.3. Пусть $a, b, c \in \mathbb{Q}$, $ac \neq 0$. Доказать, что многочлены $P(z)$ и $cP(az + b)$ одновременно являются или не являются неприводимыми.

Задача 7.4 (лемма Гаусса).

- 1) Содержанием целочисленного многочлена называется НОД его коэффициентов (содержание нулевого многочлена равно 0); обозначение: $\text{cont}(P)$. Доказать, что для любых целочисленных многочленов P, Q (от любого числа переменных) выполнено

$$\text{cont}(PQ) = \text{cont}(P) \text{cont}(Q).$$

(Указание. Кольцо многочленов над полем \mathbb{F}_p не имеет делителей нуля.)

- 2) Пусть $P(z), Q(z) \in \mathbb{Q}[z]$, $P(z)Q(z) \in \mathbb{Z}[z]$. Доказать, что найдётся $c \in \mathbb{Q}^*$, такое что многочлены $cP(z), c^{-1}Q(z)$ целочисленные (аналогично для любого числа переменных).
- 3) Пусть $P(z), Q(z) \in \mathbb{Q}[z]$ — унитарные многочлены, $P(z)Q(z) \in \mathbb{Z}[z]$. Доказать, что многочлены $P(z), Q(z)$ целочисленные.

Задача 7.5 (I. Schur). Пусть a_1, \dots, a_n — различные целые числа ($n \in \mathbb{N}$). Доказать, что:

- 1) многочлен $(z + a_1) \cdots (z + a_n) - 1$ неприводим;
- 2) многочлен $(z + a_1) \cdots (z + a_n) + 1$ неприводим, за исключением случаев

$$(z + a)(z + a + 2) + 1 = (z + a + 1)^2,$$

$$(z + a)(z + a + 1)(z + a + 2)(z + a + 3) + 1 = ((z + a)(z + a + 3) + 1)^2.$$

Задача 7.6 («критерий» Эйзенштейна). Пусть $P(z) = a_n z^n + \dots + a_0 \in \mathbb{Z}[z]$, $n \in \mathbb{N}$, p — простое число, $p \nmid a_n$, $p \mid a_k$ при $0 \leq k < n$, $p^2 \nmid a_0$. Доказать, что многочлен $P(z)$ неприводим. (Указание. Кольцо многочленов $\mathbb{F}_p[z]$ факториально.)

Задача 7.7. Док-ть, что многочлен $z^{n-1} + z^{n-2} + \dots + z + 1$ неприводим тогда и только тогда, когда n — простое число. (Указание. Для док-ва неприводимости применить Эйзенштейна к многочлену $P(z + 1)$.)

Задача 7.8. Доказать неприводимость многочленов $z^4 + 2z^3 + 6z^2 + 3z + 15$, $z^5 + z^2 + 1$. (Указание. Проверить неприводимость над \mathbb{F}_2 .)

Задача 7.9 (E. Artin, O. Schreier). Пусть p — простое число, $a \in \mathbb{Z}$, $p \nmid a$. Доказать, что многочлен $z^p - z + a$ неприводим. (Указание. Док-ть неприводимость над полем \mathbb{F}_p , воспользовавшись тем, что многочлен не меняется при замене $z \rightarrow z + 1$.)

Задача 7.10 (D. Hilbert). Пусть r, s — нечётные простые числа, удовлетворяющие условиям $r \equiv 1 \pmod{8}$, $\left(\frac{r}{s}\right) = 1$. Доказать, что многочлен

$$(z + \sqrt{r} + \sqrt{s})(z + \sqrt{r} - \sqrt{s})(z - \sqrt{r} + \sqrt{s})(z - \sqrt{r} - \sqrt{s}) \in \mathbb{Q}[z]$$

неприводим над \mathbb{Q} , однако приводим по любому модулю $m \in \mathbb{N}$.

7.2 Конечные расширения

Задача 7.11 (избавление от иррациональности в знаменателе).

- 1) Представить число $\frac{1}{3+2^3\sqrt{2}+3\sqrt{4}}$ в виде $a_0 + a_1\sqrt{2} + a_2\sqrt{4}$ с рациональными a_0, a_1, a_2 . (Ответ: $\frac{5}{11} - \frac{4}{11}\sqrt{2} + \frac{1}{11}\sqrt{4}$.)
- 2) Пусть α — корень многочлена $z^3 + z + 1$. Представить число $\frac{1}{1+\alpha+\alpha^2}$ в виде $a_0 + a_1\alpha + a_2\alpha^2$ с рациональными a_0, a_1, a_2 . (Ответ: $\frac{2}{3} - \frac{2}{3}\alpha + \frac{1}{3}\alpha^2$.)
- 3) Пусть α — корень многочлена $z^4 + z + 1$. Представить число $\frac{1}{1+\alpha+\alpha^3}$ в виде $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ с рациональными a_0, a_1, a_2, a_3 . (Ответ: $-\frac{1}{3} - \frac{2}{3}\alpha + \frac{1}{3}\alpha^2 - \frac{2}{3}\alpha^3$.)

Задача 7.12. Доказать, что число $\cos \frac{2\pi}{7}$ алгебраическое, и найти его минимальный многочлен. (Ответ: $z^3 + \frac{1}{2}z^2 - \frac{1}{2}z - \frac{1}{8}$.)

Задача 7.13. Доказать, что $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, и найти минимальный многочлен числа $\sqrt{2} + \sqrt{3}$.

Задача 7.14.

- 1) Пусть $\alpha, \alpha_1, \dots, \alpha_n \in \mathbb{Q}$. Доказать, что $\sqrt{\alpha} \in \mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n})$ тогда и только тогда, когда $\alpha = \gamma^2 \alpha_1^{k_1} \dots \alpha_n^{k_n}$ с некоторыми $\gamma \in \mathbb{Q}$, $k_j \in \{0, 1\}$.
- 2) Пусть p_1, \dots, p_n — различные простые числа. Доказать, что:
 - а) числа $1, \sqrt{p_1}, \dots, \sqrt{p_n}$ линейно независимы над \mathbb{Q} ;
 - б) $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$;
 - в) $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + \dots + \sqrt{p_n})$.

Задача 7.15. Пусть $\alpha \in \mathbb{A}$, $\deg \alpha = p$ — простое число, $\beta = a_0 + a_1 \alpha + \dots + a_{p-1} \alpha^{p-1}$, $a_k \in \mathbb{Q}$, $|a_1| + \dots + |a_{p-1}| > 0$. Доказать, что $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Задача 7.16. Найти минимальный многочлен числа $3 + \sqrt[3]{2} - \sqrt[3]{4}$. (Ответ: $z^3 - 9z^2 + 33z - 43$.)

Пусть K — конечное расширение \mathbb{Q} . Каждому числу $\alpha \in K$ сопоставим линейный оператор $T_\alpha : K \rightarrow K$ по правилу $T_\alpha(x) = \alpha x$. Это соответствие, очевидно, сохраняет операции, т. е. мы получаем вложение поля K в алгебру линейных операторов (причём линейное над \mathbb{Q}).

Характеристический многочлен (унитарный), след и определитель оператора T_α называются соответственно *характеристическим многочленом, следом и нормой* числа α относительно расширения K/\mathbb{Q} . Обозначения: $\chi_\alpha(z)$ — характеристический многочлен, $\text{Tr}_{\mathbb{Q}}^K(\alpha) = \text{Tr}_{K/\mathbb{Q}}(\alpha) = \text{Tr}(\alpha) = S_{\mathbb{Q}}^K(\alpha) = \dots$ — след, $N_{\mathbb{Q}}^K(\alpha) = \text{Nm}_{\mathbb{Q}}^K(\alpha) = \dots$ — норма.

Зафиксируем базис $\omega_1, \dots, \omega_n$ и рассмотрим матрицу $A = \|a_{i,j}\|$ оператора T_α в этом базисе:

$$\alpha \omega_j = \sum_{i=1}^n a_{i,j} \omega_i, \quad a_{i,j} \in \mathbb{Q}, \quad 1 \leq i, j \leq n. \quad (7.1)$$

Тогда $\chi_\alpha(z) = \det(zI - A)$, $\text{Tr}(\alpha) = \text{Tr} A$, $N(\alpha) = \det A$.

Задача 7.17. Доказать утверждения:

- 1) Если $K = \mathbb{Q}(\alpha)$, то $\chi_\alpha(z) = P_\alpha(z)$ — минимальный многочлен α . (Указание. Теорема Гамильтона–Кэли. В данном случае также можно рассмотреть (7.1) как однородную систему линейных уравнений относительно ω_i . Либо можно взять базис $1, \alpha, \dots, \alpha^{n-1}$ и посчитать непосредственно.)
- 2) Если $[K : \mathbb{Q}(\alpha)] = d$, то

$$\chi_\alpha(z) = (P_\alpha(z))^d = \prod_{\sigma} (z - \sigma(\alpha)),$$

где последнее произведение берётся по всем вложениям $\sigma : K \rightarrow \mathbb{C}$ поля K в \mathbb{C} . (Указание. Пусть $\theta_1, \dots, \theta_d$ — базис расширения $K/\mathbb{Q}(\alpha)$, $\omega_1, \dots, \omega_m$ — базис расширения $\mathbb{Q}(\alpha)/\mathbb{Q}$. Если в качестве базиса расширения K/\mathbb{Q} взять $\omega_k \theta_l$ в подходящем порядке, то матрица A будет блочно-диагональной.)

- 3) $\text{Tr}(\alpha) = \sum_{\sigma} \sigma(\alpha)$, $N(\alpha) = \prod_{\sigma} \sigma(\alpha)$.

Таким образом, минимальный многочлен для $\alpha \in K$ легко вычисляется по формуле

$$P_\alpha(z) = \frac{\chi_\alpha(z)}{(\chi_\alpha(z), \chi'_\alpha(z))}.$$

(Разумеется, метод неопределённых коэффициентов тоже никто не отменял, т.е. можно просто разложить числа $1, \alpha, \dots, \alpha^n$ по базису и найти коэффициенты линейной зависимости, решив соответствующую СЛАУ.)

Задача 7.18.

- 1) Пусть α — корень многочлена $z^3 + z + 1$. Найти минимальные многочлены для чисел α^2 , $\alpha + \alpha^2$, $\alpha - 2\alpha^2$. (Ответы: $z^3 + 2z^2 + z - 1$, $z^3 + 2z^2 + 5z + 1$, $z^3 - 4z^2 - z + 13$.)
- 2) Пусть α — корень многочлена $z^4 - z^3 + 3z^2 - z + 1$. Найти минимальные многочлены для чисел $\alpha - 2\alpha^2 + 3\alpha^3$, $2\alpha - \alpha^2 + \alpha^3$. (Ответы: $z^4 + 4z^3 + 84z^2 - 65z + 25$, $z^2 - z + 1$.)

7.3 Целые алгебраические числа

Через \mathbb{Z}_A будем обозначать кольцо всех целых алгебраических чисел. Кроме того, для конечного расширения $K \supseteq \mathbb{Q}$ пусть $\mathbb{Z}_K = K \cap \mathbb{Z}_A$ — кольцо целых чисел (aka *максимальный порядок*) поля K .

Задача 7.19. Пусть $\alpha_1, \dots, \alpha_n \in A$. Доказать, что существует такое натуральное число d , что $d\alpha_\nu \in \mathbb{Z}_A$, $1 \leq \nu \leq n$.

Задача 7.20. Пусть $d \neq 1$ — бесквадратное целое число (т.е. $p^2 \nmid d$ для всех простых p), $K = \mathbb{Q}(\sqrt{d})$. Доказать, что $\mathbb{Z}_K = \mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$, где

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod{4}, \\ \sqrt{d}, & d \equiv 2, 3 \pmod{4}. \end{cases}$$

Задача 7.21. Пусть $a \in \mathbb{Q}$, $a > 0$, $a \neq 1, 3, 1/3$. Доказать, что число $\frac{\operatorname{arctg} \sqrt{a}}{\pi}$ иррационально. (Указание. $e^{2i \operatorname{arctg} z} = \frac{1+iz}{1-iz}$.)

Если K — конечное расширение \mathbb{Q} , то базисом поля K называется произвольный базис K как векторного пространства над \mathbb{Q} .

Задача 7.22. Пусть K — конечное расширение \mathbb{Q} степени n . Доказать, что существует такой базис $\omega_1, \dots, \omega_n$ поля K , что $\mathbb{Z}_K = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$. (Такой базис называется *фундаментальным*. Указание. Пусть $K = \mathbb{Q}(\theta)$, $\theta \in \mathbb{Z}_K$. Доказать, что \mathbb{Z}_K — подгруппа полного ранга группы (по сложению) $\frac{1}{d}\mathbb{Z} + \frac{1}{d}\mathbb{Z}\theta + \dots + \frac{1}{d}\mathbb{Z}\theta^{n-1}$ для некоторого $d \in \mathbb{N}$.)

Задача 7.23. Пусть K — конечное расширение \mathbb{Q} , $\alpha \in \mathbb{Z}_K \setminus \{0\}$. Доказать, что факторкольцо $\mathbb{Z}_K/\alpha\mathbb{Z}_K$ конечно, причём $|\mathbb{Z}_K/\alpha\mathbb{Z}_K| = |\mathbb{N}_\mathbb{Q}^K(\alpha)|$. (Указание. Пусть $\omega_1, \dots, \omega_n$ — фундаментальный базис K . Тогда $\alpha\mathbb{Z}_K = \mathbb{Z}\alpha\omega_1 + \dots + \mathbb{Z}\alpha\omega_n$. Дальше см. задачу 5.14.)

Задача 7.24. Пусть $K = \mathbb{Q}(\sqrt[3]{2})$. Доказать, что $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\sqrt[3]{2} + \mathbb{Z}\sqrt[3]{4}$. (Замечание. Это не очень простая задача.)

Задача 7.25. Пусть $a \in \mathbb{Q}$. Доказать, что $2 \cos \pi a \in \mathbb{Z}_\mathbb{A}$, причём все его сопряжённые имеют такой же вид (т.е. $2 \cos \pi b$, $b \in \mathbb{Q}$).

Задача 7.26 (теорема Кронекера).

- 1) Пусть $\zeta \neq 0$ — целое алгебраическое число, все сопряжённые которого по модулю не превосходят 1. Доказать, что ζ — корень из 1. (Указание. Рассмотреть многочлены $\prod_{j=1}^d (z - \zeta_j^n)$, $n = 1, 2, \dots$, где ζ_j — (все) сопряжённые с ζ числа.)
- 2) Пусть α — целое алгебраическое число, все сопряжённые которого вещественны и лежат на отрезке $[-2, 2]$. Доказать, что $\alpha = 2 \cos \pi a$ для некоторого $a \in \mathbb{Q}$. (Указание. Записать $\alpha = \zeta + \frac{1}{\bar{\zeta}}$ и применить п. 1 к числу ζ .)

Задача 7.27.

- 1) Пусть $P(z) \in \mathbb{Z}_\mathbb{A}[z]$, $\alpha \in \mathbb{C}$, $P(\alpha) = 0$. Доказать, что $\frac{P(z)}{z-\alpha} \in \mathbb{Z}_\mathbb{A}[z]$.
- 2) Пусть $P(z) = a_n \prod_{k=1}^n (z - \alpha_k) \in \mathbb{Z}_\mathbb{A}[z]$. Доказать, что $a_n \alpha_{k_1} \cdots \alpha_{k_m} \in \mathbb{Z}_\mathbb{A}$ для произвольных $1 \leq k_1 < k_2 < \dots < k_m \leq n$.

7.4 Вокруг основной теоремы арифметики

Немного окупёмся в коммутативную алгебру. Далее D — целостное кольцо (т.е. коммутативное ассоциативное кольцо с $1 \neq 0$ без делителей нуля).

Определение 1. Говорят, что $\alpha \in D$ делится на $\beta \in D$ (или β делит α), если $\alpha = \beta\gamma$ для некоторого $\gamma \in D$; обозначение: $\beta \mid \alpha$ (также иногда пишут $\beta \setminus \alpha$). (В частности, $0 \mid \alpha$ тогда и только тогда, когда $\alpha = 0$.)

Определение 2. Элемент $\varepsilon \in D$ называется *единицей кольца D* (также *делителем единицы*, *обратимым элементом*), если $\varepsilon \mid 1$, т.е. если $\exists \varepsilon^{-1}$. Множество всех единиц кольца D будем обозначать через D^\times . Очевидно, что D^\times — группа по умножению.

Определение 3. Элементы $\alpha, \beta \in D$ называются *эквивалентными* (или *ассоциированными*), если $\alpha \mid \beta$ и $\beta \mid \alpha$; обозначение: $\alpha \sim \beta$.

Задача 7.28. Доказать, что $\alpha \sim \beta$ тогда и только тогда, когда $\alpha = \beta\varepsilon$ для некоторого $\varepsilon \in D^\times$.

Определение 4. Элемент $\pi \in D$ называется *неразложимым* (или *неприводимым*), если $\pi \neq 0$, $\pi \notin D^\times$ и в любом представлении $\pi = \alpha\beta$, $\alpha, \beta \in D$, один из элементов α, β — единица кольца D .

Замечание. Элемент $\alpha \in D \setminus \{0\}$ называется *простым*, если главный идеал $(\alpha) = \alpha D$ простой. Простой элемент всегда неразложим; обратное верно не всегда, но верно для факториальных колец (см. ниже); более того, если любой неразложимый элемент прост и любой необратимый ненулевой элемент раскладывается на неразложимые, то кольцо факториально.

Определение 5. Кольцо D называется *факториальным* (или в D справедлива ОТА), если любой элемент $\alpha \in D \setminus \{0\}$ можно представить в виде

$$\alpha = \varepsilon \pi_1 \cdots \pi_s,$$

где $\varepsilon \in D^\times$, π_i — неразложимые элементы, $s \geq 0$, причём это представление единственно с точностью до порядка сомножителей и перехода к эквивалентным элементам.

Задача 7.29. Доказать, что любое поле факториально.

Задача 7.30. Доказать, что кольцо \mathbb{Z} факториально.

Определение 6. Наибольшим общим делителем элементов $\alpha, \beta \in D$ называется (любой) их общий делитель, который делится на все общие делители α и β . Если δ — НОД α и β , то будем писать $(\alpha, \beta) = \delta$. Например, $(0, 0) = 0$. Очевидно, если НОД α и β существует, то он определён однозначно с точностью до эквивалентности. Аналогично определяется НОД для трёх и более элементов.

Задача 7.31. Доказать, что в факториальном кольце любые два элемента имеют НОД.

Определение 7. Кольцо D называется *целозамкнутым* (в своём поле частных), если любой корень многочлена вида $z^n + a_{n-1}z^{n-1} + \cdots + a_0 \in D[z]$, лежащий в поле частных кольца D , принадлежит D .

Задача 7.32. Доказать, что любое факториальное кольцо целозамкнуто.

Задача 7.33. Пусть K — конечное расширение \mathbb{Q} , D — подкольцо K с 1, причём K является полем частных кольца D . Доказать, что если D факториально, то $\mathbb{Z}_K \subseteq D$. (Мораль: среди всех порядков поля K факториальным кольцом может являться только максимальный порядок.)

Задача 7.34. Обобщить лемму Гаусса (задача 7.4) на факториальные кольца (т.е. заменить \mathbb{Z} на факториальное кольцо D , а \mathbb{Q} — на поле частных кольца D).

Задача 7.35. Пусть D — факториальное кольцо. Доказать, что кольцо многочленов $D[z]$ также факториально. (Указание. Использовать факториальность кольца многочленов над полем частных кольца D и лемму Гаусса.)

Определение 8. Кольцо D (коммутативное) называется *кольцом главных идеалов*, если в нём любой идеал главный.

Задача 7.36. Доказать, что в (целостном) кольце главных идеалов D любые два элемента α, β имеют НОД δ , причём его можно представить в виде $\delta = \alpha\mu + \beta\nu$, $\mu, \nu \in D$.

Задача 7.37. Доказать, что любое (целостное) кольцо главных идеалов факториально. (Указание. Существование разложения на неразложимые следует из нётеровости; единственность разложения доказывается так же, как для \mathbb{N} .)

Задача 7.38. Доказать, что кольца $\mathbb{Z}[x]$, $\mathbb{Q}[x, y]$ факториальны, но не являются кольцами главных идеалов.

Определение 9. Функция $\mathcal{N}: D \setminus \{0\} \rightarrow \mathbb{N}_0$ называется *евклидовой нормой* (или *евклидовой функцией*) на D , если для неё справедливы следующие два свойства:

- 1) для любых $\alpha \in D$, $\beta \in D \setminus \{0\}$ найдутся $\gamma, \rho \in D$, такие что $\alpha = \beta\gamma + \rho$, причём либо $\rho = 0$, либо $\mathcal{N}(\rho) < \mathcal{N}(\beta)$;
- 2) если $\alpha \neq 0$ делится на β , то $\mathcal{N}(\alpha) \geq \mathcal{N}(\beta)$.

Если для D существует евклидова норма, то D называется *евклидовым кольцом* (также говорят, что в D имеет место алгоритм деления с остатком).

Задача 7.39. Допустим, что существует функция $\tilde{\mathcal{N}}: D \setminus \{0\} \rightarrow \mathbb{N}_0$, обладающая свойством 1 («деление с остатком») из определения евклидовой нормы (такую функцию также иногда называют евклидовой нормой). Доказать, что кольцо D евклидово. (Указание. Рассмотреть $\mathcal{N}(\alpha) = \min_{\gamma \in D \setminus \{0\}} \tilde{\mathcal{N}}(\alpha\gamma)$.)

Задача 7.40. Пусть \mathcal{N} — евклидова норма на D . Доказать, что если β — собственный делитель $\alpha \neq 0$ (т.е. $\beta \mid \alpha$ и $\alpha \nmid \beta$), то $\mathcal{N}(\alpha) > \mathcal{N}(\beta)$.

Задача 7.41. Доказать, что в евклидовом кольце любой необратимый ненулевой элемент раскладывается на неразложимые.

Задача 7.42. Доказать, что любое евклидово кольцо является кольцом главных идеалов (причём порождающий элемент идеала, заданного конечным числом порождающих, можно искать с помощью алгоритма Евклида. Как следствие, получаем, что любое евклидово кольцо факториально.)

Общая теория закончилась, теперь потренируемся на коньках. В качестве примера возьмём кольца целых алгебраических чисел.

Задача 7.43. Доказать, что в кольце $\mathbb{Z}_{\mathbb{A}}$ нет неразложимых элементов, однако существуют необратимые ненулевые элементы. (Ergo, кольцо $\mathbb{Z}_{\mathbb{A}}$ не факториально.)

Задача 7.44. Пусть $\alpha \in \mathbb{Z}_{\mathbb{A}}$. Доказать, что α — единица кольца $\mathbb{Z}_{\mathbb{A}}$ тогда и только тогда, когда $\mathcal{N}(\alpha) = \mathcal{N}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha) = \pm 1$. (Такие числа называются *алгебраическими единицами*.) Аналогично для $\alpha \in \mathbb{Z}_K$ с $\mathcal{N}(\alpha) = \mathcal{N}_{\mathbb{Q}}^K(\alpha)$.

Задача 7.45. Пусть K — конечное расширение \mathbb{Q} . Доказать, что в кольце \mathbb{Z}_K любой необратимый ненулевой элемент раскладывается на неразложимые (возможно, неоднозначно).

Задача 7.46. Пусть K — конечное расширение \mathbb{Q} , причём кольцо \mathbb{Z}_K факториально. Доказать, что любой неразложимый элемент кольца \mathbb{Z}_K делит некоторое простое число $p \in \mathbb{N}$, причём такое p единственно.

Дальше сосредоточимся на квадратичных полях (конечных расширениях \mathbb{Q} степени 2). В следующей серии задач $d \neq 1$ — бесквадратное целое число, $K = \mathbb{Q}(\sqrt{d})$.

Задача 7.47. Доказать, что при $d \equiv 1 \pmod{4}$ кольцо $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ не факториально. (Указание. Задачи 7.20 и 7.33.)

Задача 7.48. Пусть K — мнимое квадратичное поле, т. е. $d < 0$. Найти все единицы кольца \mathbb{Z}_K .

Задача 7.49. Доказать, что при $d = -1, \pm 2, \pm 3, 5, -7, -11$ функция $|\mathbb{N}_{\mathbb{Q}}^K(\cdot)|$ является евклидовой нормой на \mathbb{Z}_K . (Указание. Для любого $\alpha \in K$ найдётся $\gamma \in \mathbb{Z}_K$, такое что $|\mathbb{N}_{\mathbb{Q}}^K(\alpha - \gamma)| < 1$.)

Замечание. Полный список значений d , для которых справедливо утверждение задачи 7.49: $-1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

Задача 7.50. Доказать, что при $d = -5$ кольцо \mathbb{Z}_K не факториально. (Указание. Например, рассмотреть равенство $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$.)

Задача 7.51. Доказать, что при $d = 10$ кольцо \mathbb{Z}_K не факториально. (Указание. $(\sqrt{10} + 1)(\sqrt{10} - 1) = 3^2$.)

Задача 7.52. Пусть $d < 0$, $d \neq -1, -2, -3, -7, -11$. Доказать, что кольцо \mathbb{Z}_K не евклидово. (Указание. Среди необратимых ненулевых элементов \mathbb{Z}_K рассмотреть число α с наименьшей евклидовой нормой и доказать, что любое число из \mathbb{Z}_K сравнимо по модулю α с одним из чисел $0, \pm 1$. Затем воспользоваться задачей 7.23.)

Задача 7.53. Доказать, что при $d = -19$ кольцо \mathbb{Z}_K не евклидово, но является кольцом главных идеалов (\Rightarrow факториально). (Замечание. Это сложная задача.)

Наконец, познакомимся с некоторыми приложениями всей этой кухни.

Задача 7.54. Используя факториальность $\mathbb{Z}[\sqrt{-2}]$, найти все целые решения уравнения $x^3 - y^2 = 2$. Для этого доказать утверждения:

- 1) y нечётно.
- 2) Числа $y \pm \sqrt{-2}$ взаимно просты в кольце $\mathbb{Z}[\sqrt{-2}]$.
- 3) $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ для некоторых $a, b \in \mathbb{Z}$.
- 4) Все решения: $x = 3, y = \pm 5$.

Задача 7.55. Решить в целых числах $x^3 - y^2 = 4$. (Ответ: $(x, y) = (2, \pm 2), (5, \pm 11)$.)

Задача 7.56 (неразложимые элементы в кольце целых гауссовых чисел). Пусть p — простое число ($p \in \mathbb{N}$). Доказать, что в кольце $\mathbb{Z}[i]$ справедливы следующие разложения на неразложимые множители:

- 1) $2 \sim (1 + i)^2$, причём $1 + i$ неразложимо;
- 2) если $p \equiv 3 \pmod{4}$, то p неразложимо;
- 3) если $p \equiv 1 \pmod{4}$, то $p = (a + bi)(a - bi)$, $a, b \in \mathbb{Z}$, причём $(a \pm bi)$ неразложимы и не эквивалентны. (Указание. Рассмотреть такое $c \in \mathbb{Z}$, что $c^2 + 1 = (c + i)(c - i)$ делится на p , и вывести отсюда разложимость p в $\mathbb{Z}[i]$.)

Задача 7.57 (ещё раз суммы двух квадратов). Используя факториальность $\mathbb{Z}[i]$, доказать утверждения:

- 1) Пусть p — простое число, $p \equiv 1 \pmod{4}$. Тогда p представимо в виде суммы двух квадратов, причём единственным образом (с точностью до тривиальных симметрий).
- 2) Для $n \in \mathbb{N}$ количество целых решений уравнения $x^2 + y^2 = n$ равно $4 \sum_{d|n} \chi(d)$, где χ — (единственный) неглавный характер по модулю 4, т. е.

$$\chi(a) = \begin{cases} 0, & a \equiv 0 \pmod{2}, \\ 1, & a \equiv 1 \pmod{4}, \\ -1, & a \equiv -1 \pmod{4}. \end{cases}$$

- 3) Натуральное число n можно представить в виде $n = x^2 + y^2$ с взаимно простыми x, y тогда и только тогда, когда n не делится ни на какое простое $p \equiv 3 \pmod{4}$ и n не делится на 4.
- 4) Для любого целого $n > 1$ количество решений уравнения $x^2 + y^2 = n$ во взаимно простых натуральных x, y равно числу решений сравнения $z^2 + 1 \equiv 0 \pmod{n}$.

Задача 7.58. Доказать, что уравнение

$$\operatorname{tg}(x \operatorname{arctg} y) = \operatorname{tg}(y \operatorname{arctg} x)$$

не имеет решений в натуральных числах $x \neq y$. (Указание. Переписать уравнение в виде $\left(\frac{1+yi}{1-yi}\right)^x = \left(\frac{1+xi}{1-xi}\right)^y$.)

7.5 Круговые поля

Пусть $n \in \mathbb{N}$. Обозначим $\zeta_n = e^{2\pi i/n}$. Многочлен

$$\Phi_n(z) = \prod_{\substack{0 \leq k \leq n-1, \\ (k,n)=1}} (z - \zeta_n^k)$$

называется n -м *круговым многочленом* (или *многочленом деления круга*). Примеры: $\Phi_1(z) = z - 1$, $\Phi_2(z) = z + 1$, $\Phi_3(z) = z^2 + z + 1$, $\Phi_4(z) = z^2 + 1$, $\Phi_5(z) = z^4 + z^3 + z^2 + z + 1$, $\Phi_6(z) = z^2 - z + 1$. Непосредственно из определения видно, что $\deg \Phi_n = \varphi(n)$.

Задача 7.59. Доказать, что $z^n - 1 = \prod_{d|n} \Phi_d(z)$. (В частности, $\sum_{d|n} \varphi(d) = n$.)

Задача 7.60. Доказать, что $\Phi_n(z) \in \mathbb{Z}[z]$.

Задача 7.61. Пусть $n > 1$. Доказать, что $\Phi_n(0) = 1$, $\Phi_n(1) = e^{\Lambda(n)}$.

Задача 7.62. Доказать, что $\Phi_n(z) = \prod_{d|n} (z^{n/d} - 1)^{\mu(d)}$.

Задача 7.63. Пусть $m = \prod_{p|n} p$. Доказать, что $\Phi_n(z) = \Phi_m(z^{n/m})$.

Задача 7.64. Пусть $p \nmid n$ — простое число, $\alpha \in \mathbb{N}$. Доказать, что $\Phi_{p^\alpha n}(z) = \frac{\Phi_n(z^{p^\alpha})}{\Phi_n(z^{p^{\alpha-1}})}$.

Задача 7.65. Пусть $n \geq 3$ нечётно. Доказать, что $\Phi_{2n}(z) = \Phi_n(-z)$.

Задача 7.66 (теорема Дирихле о простых числах в арифметической прогрессии $nk + 1$).

- 1) Пусть $n \in \mathbb{N}$, p — простое число, причём $p \nmid n$, $p \mid \Phi_n(a)$ при некотором $a \in \mathbb{Z}$. Доказать, что $p \equiv 1 \pmod{n}$. (Указание. Воспользовавшись тем, что $\Phi_n(z) \mid \frac{z^n - 1}{z^d - 1}$ при $d \mid n$, $d \neq n$, доказать, что $\text{ord}_p a = n$.)
- 2) Вывести из п. 1, что существует бесконечно много простых чисел $p \equiv 1 \pmod{n}$.

Задача 7.67 (теорема Дирихле о простых числах в арифметической прогрессии $nk - 1$).

- 1) Рассмотрим многочлены $A_n(x, y) = (x - yi)^{\varphi(n)} \Phi_n\left(\frac{x+yi}{x-yi}\right)$. Доказать их свойства:
 - а) A_n — однородный многочлен степени $\varphi(n)$.
 - б) $(x + yi)^n - (x - yi)^n = \prod_{d \mid n} A_d(x, y)$.
 - в) $A_n(x, y) \in \mathbb{Z}[x, y]$ при $n > 1$.
 - г) Если $n > 1$, то все корни многочлена $P_n(z) = A_n(z, 1)$ вещественные и простые (т.е. кратности 1), $\deg P_n = \varphi(n)$, а старший коэффициент равен $e^{\Lambda(n)} > 0$.
 - д) Пусть $n \in \mathbb{N}$, p — простое число, причём $p \nmid n$, $p \equiv -1 \pmod{4}$, $p \mid A_n(a, b)$ при некоторых взаимно простых $a, b \in \mathbb{Z}$. Тогда $p \equiv -1 \pmod{n}$. (Указание. Используя задачу 7.56, доказать, что в кольце $\mathbb{Z}[i]$ выполнено $(a \pm bi, p) = 1$, поэтому можно рассмотреть $\alpha = (a + bi)(a - bi)^{-1} \pmod{p\mathbb{Z}[i]} \in (\mathbb{Z}[i]/p\mathbb{Z}[i])^*$. Как в задаче 7.66, доказать, что $\text{ord } \alpha = n$, и воспользоваться тем, что $(a \pm bi)^{p+1} \equiv a^2 + b^2 \pmod{p\mathbb{Z}[i]}$.)
- 2) Доказать, что существует бесконечно много простых чисел $p \equiv -1 \pmod{n}$. (Указание. Пусть $n > 1$. Найти взаимно простые $a \in \mathbb{Z}$, $b \in \mathbb{N}$, такие что $A_n(a, b) = -c < 0$, и рассмотреть число $A_n(a + 4np_1 \cdots p_m bck, b)/c$ при достаточно большом $k \in \mathbb{N}$.)

Задача 7.68. Пусть p — простое число, $\alpha \in \mathbb{N}$. Используя критерий Эйзенштейна, доказать неприводимость $\Phi_{p^\alpha}(z)$. (Указание. См. задачу 7.7.)

Задача 7.69. Доказать неприводимость $\Phi_n(z)$ для произвольного $n \in \mathbb{N}$. Подзадачи:

- 1) Пусть $f(z)$ — минимальный многочлен числа ζ_n , $z^n - 1 = f(z)g(z)$. Доказать, что $f(z), g(z) \in \mathbb{Z}[z]$.
- 2) Пусть p — простое число, $p \nmid n$. Доказать, что $f(z) \mid f(z^p)$. (Указание. Доказать взаимную простоту $f(z)$ и $g(z^p)$, используя сравнение $g(z^p) \equiv (g(z))^p \pmod{p}$.)
- 3) Доказать, что $f(z) = \Phi_n(z)$. (Указание. Если $f(\alpha) = 0$, то $f(\alpha^p) = 0$.)

Поле $\mathbb{Q}(\zeta_n)$, $n \in \mathbb{N}$, называется n -м круговым полем.

Задача 7.70. Доказать, что $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Задача 7.71. Доказать, что $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{[n,m]})$.

Задача 7.72. Пусть $n, m \in \mathbb{N}$. Доказать утверждения:

- 1) $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ тогда и только тогда, когда $(n, m) = 1$.
- 2) Многочлен $\Phi_n(z)$ неприводим над $\mathbb{Q}(\zeta_m)$ тогда и только тогда, когда $(n, m) \leq 2$.
- 3) $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ тогда и только тогда, когда $(n, m) \leq 2$.

Задача 7.73. Пусть $n \geq 3$. Доказать, что $\cos \frac{2\pi}{n}$ — алгебраическое число степени $\varphi(n)/2$, и найти все его сопряжённые.

Задача 7.74. Пусть $T_n(z) = \cos(n \arccos z)$ — многочлен Чебышёва (первого рода), $n = 2^\alpha m$, $\alpha \geq 0$, m нечётно. Доказать, что $T_n(z) = 2^{n-1} \prod_{d|m} P_{2^{\alpha+2d}}(z)$, где $P_k(z)$ — минимальный многочлен числа $\cos \frac{2\pi}{k}$. Получить аналогичное разложение для многочленов Чебышёва второго рода $U_n(z) = \frac{\sin((n+1) \arccos z)}{\sin(\arccos z)}$.

Задача 7.75 (для знакомых с определением группы Галуа).

- 1) Доказать, что $\mathbb{Q}(\zeta_n)$ — нормальное расширение \mathbb{Q} , группа Галуа которого изоморфна $(\mathbb{Z}/n\mathbb{Z})^*$, причём изоморфизм можно задать следующим образом: каждому $\bar{r} \in (\mathbb{Z}/n\mathbb{Z})^*$ соответствует автоморфизм $\sigma_{\bar{r}}: \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n)$, такой что $\sigma_{\bar{r}}(\zeta_n) = \zeta_n^r$.
- 2) Фиксируем $n \in \mathbb{N}$. Для $d | n$ обозначим $G_d = \{\bar{r} \in (\mathbb{Z}/n\mathbb{Z})^* \mid r \equiv 1 \pmod{d}\}$. Доказать равенства:
 - а) $G_d = \{\bar{r} \in (\mathbb{Z}/n\mathbb{Z})^* \mid \sigma_{\bar{r}}(\alpha) = \alpha \text{ при всех } \alpha \in \mathbb{Q}(\zeta_d)\}$;
 - б) $\mathbb{Q}(\zeta_d) = \{\alpha \in \mathbb{Q}(\zeta_n) \mid \sigma_{\bar{r}}(\alpha) = \alpha \text{ при всех } \bar{r} \in G_d\}$. (Указание. Степень поля, стоящего справа от знака равенства, не превосходит $[(\mathbb{Z}/n\mathbb{Z})^* : G_d] = \varphi(d)$.)
- 3) Доказать, что $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{(n,m)})$.

Задача 7.76. Пусть K — конечное расширение \mathbb{Q} степени 2. Доказать, что существует $n \in \mathbb{N}$, такое что $K \subseteq \mathbb{Q}(\zeta_n)$. (Указание. См. задачу 4.28. Замечание. Это простой частный случай теоремы Кронекера–Вебера: $K \subseteq \mathbb{Q}(\zeta_n)$ для некоторого $n \in \mathbb{N}$ тогда и только тогда, когда K — нормальное конечное расширение \mathbb{Q} с абелевой группой Галуа.)

Задача 7.77. Пусть p — простое число, $l \in \mathbb{N}$, $\zeta = \zeta_{p^l}$, $K = \mathbb{Q}(\zeta)$, $\pi = 1 - \zeta$. Доказать утверждения:

- 1) Если ζ', ζ'' — примитивные корни из 1 степени $n \in \mathbb{N}$, то $1 - \zeta' \sim 1 - \zeta''$ в кольце $\mathbb{Z}[\zeta_n]$.
- 2) В кольце \mathbb{Z}_K выполнено $N_{\mathbb{Q}}^K(\pi) = p \sim \pi^{\varphi(p^l)}$, причём π неразложимо.
- 3) Если $a \in \mathbb{Z}$, то $\pi \mid a$ в кольце \mathbb{Z}_K тогда и только тогда, когда $p \mid a$.

4) При $n \in \mathbb{Z}$ выполнено

$$\mathrm{Tr}_{\mathbb{Q}}^K(\zeta^n) = \begin{cases} 0, & p^{l-1} \nmid n, \\ -p^{l-1}, & p^{l-1} \mid n, \text{ но } p^l \nmid n, \\ p^l - p^{l-1}, & p^l \mid n. \end{cases}$$

5) $p^l \mathbb{Z}_K \subseteq \mathbb{Z}[\zeta]$. (Указание. Если $\alpha = a_0 + a_1 \zeta + \dots + a_{\varphi(p^l)-1} \zeta^{\varphi(p^l)-1} \in \mathbb{Z}_K$, $a_k \in \mathbb{Q}$, то $p^l a_k = \mathrm{Tr}_{\mathbb{Q}}^K(\alpha \zeta^{-k} - \alpha \zeta^{p^{l-1}r-k}) \in \mathbb{Z}$, где $r = \lfloor k/p^{l-1} \rfloor + 1$.)

6) $\mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$.

7) $\mathbb{Z}_K = \mathbb{Z}[\zeta]$. (Указание. Пусть $\alpha \in \mathbb{Z}_K$. Тогда $p^l \alpha = a_0 + a_1 \pi + \dots + a_{\varphi(p^l)-1} \pi^{\varphi(p^l)-1}$, где $a_k \in \mathbb{Z}$. Используя пп. 2 и 3, доказать, что $p^l \mid a_k$ для всех k .)

(Замечание. Равенство $\mathbb{Z}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ справедливо для произвольного $n \in \mathbb{N}$.)

Задача 7.78. Пусть p — простое число, g — первообразный корень по модулю p . При $d \mid (p-1)$, $f = \frac{p-1}{d}$, $a \in \mathbb{Z}$ обозначим

$$S_d(a) = \sum_{k=0}^{f-1} \zeta_p^{ag^{dk}}.$$

(Числа $S_d(a)$ при $p \nmid a$ называются гауссовыми периодами.) Доказать свойства сумм $S_d(a)$:

1) если $p \mid a$, то $S_d(a) = f$;

2) $S_d(ag^d) = S_d(a)$;

3) все возможные значения $S_d(a)$ при $p \nmid a$ — это $S_d(g^k)$, $0 \leq k \leq d-1$;

4) числа $S_d(g^k)$, $0 \leq k \leq d-1$, линейно независимы над \mathbb{Q} ;

5) $S_d(1)$ — алгебраическое число степени d , причём все его сопряжённые — это $S_d(g^k)$, $0 \leq k \leq d-1$;

6) $\sum_{k=0}^{d-1} S_d(g^k) = -1$;

7) $S_d(a)S_d(b) = \sum_{k=0}^{f-1} S_d(ag^{dk} + b)$;

8) если $d = d_1 d_2$, то $S_{d_1}(a) = \sum_{k=0}^{d_2-1} S_d(ag^{d_1 k})$;

9) множество $K_d = \mathbb{Q}S_d(1) + \mathbb{Q}S_d(g) + \dots + \mathbb{Q}S_d(g^{d-1})$ является конечным расширением \mathbb{Q} степени d ;

10) $K_d = \mathbb{Q}(S_d(a))$ при $p \nmid a$;

11) если $d_1 \mid d$, то $K_{d_1} \subseteq K_d$.

Задача 7.79 (теорема Гаусса). Пусть $n \in \mathbb{N}$, $n \geq 3$, причём $\varphi(n) = 2^m$ для некоторого $m \in \mathbb{N}$, т.е. $n = 2^\alpha p_1 \cdots p_s$, где $\alpha \geq 0$, $p_1 < \cdots < p_s$ — простые числа Ферма (имеют вид $2^{2^k} + 1$). Доказать, что правильный n -угольник можно построить с помощью циркуля и линейки. (Указание. Свести к случаю $n = p$ и использовать задачу 7.78.)

Глава 8

Иррациональные и трансцендентные числа

Задача 8.1. Доказать иррациональность чисел, заданных рядами: $\sum_{n=1}^{\infty} \frac{1}{2^{n^2}}$, $\sum_{n=1}^{\infty} \frac{(-1)^n}{2^{n^2}}$, $\sum_{n=1}^{\infty} \frac{n}{2^{n^2}}$, $\sum_{n=1}^{\infty} \frac{1}{n2^{n^2}}$. (Указание. В последнем случае пригодится асимптотический закон распределения простых чисел в виде $\ln[1, 2, \dots, n] \sim n$, $n \rightarrow \infty$.)

Задача 8.2 (критерий иррациональности). Пусть $\alpha \in \mathbb{R}$. Допустим, что существуют две последовательности целых чисел a_n, b_n , такие что $\lim_{n \rightarrow \infty} (a_n + b_n \alpha) = 0$, но $a_n + b_n \alpha \neq 0$ для бесконечно многих n . Доказать, что α иррационально.

Задача 8.3 (иррациональность e^2 и e^4).

1) Домножая равенство

$$e^2 = \sum_{n=0}^N \frac{2^n}{n!} + \sum_{n=N+1}^{\infty} \frac{2^n}{n!}$$

на $N!/2^{N-1}$ при $N = 2^m$, доказать иррациональность числа e^2 . (Указание. Воспользоваться тем, что $v_2(N!) \leq N - 1$, причём равенство достигается тогда и только тогда, когда $N = 2^m$.)

2) Используя ряды для $e^{\pm 1}$, доказать, что число e не является квадратичной иррациональностью. (Указание. Допустив, что $ae^2 + be + c = 0$ для целых $a \neq 0, b, c$, переписать уравнение в виде $ae + b + ce^{-1} = 0$, разложить $e^{\pm 1}$ в ряды, домножить на $N!$ для подходящего N и получить противоречие.)

3) Доказать, что число e не является корнем никакого биквадратного уравнения $ax^4 + bx^2 + c = 0$ с целыми коэффициентами a, b, c . (В частности, $e^4 \notin \mathbb{Q}$.)

Задача 8.4. Доказать, что число $\sum_{n=1}^{\infty} \frac{1}{[1, 2, \dots, n]}$ иррационально (где $[1, 2, \dots, n]$ — наименьшее общее кратное чисел $1, 2, \dots, n$).

Задача 8.5 (иррациональность π^2). Доказать иррациональность числа π^2 следующим способом. Допустим, что $\pi^2 = a/b$, $a, b \in \mathbb{N}$. Рассмотрим многочлены

$$f_n(x) = \frac{b^n x^{2n} (\pi - x)^{2n}}{(2n)!}, \quad F_n(x) = \sum_{k=0}^{\infty} (-1)^k f^{(2k)}(x).$$

- 1) Доказать, что $\int_0^\pi f_n(x) \sin x \, dx = F_n(0) + F_n(\pi)$.
- 2) Доказать, что $F_n(\pi) = F_n(0) \in \mathbb{Z}$.
- 3) Получить противоречие при достаточно большом n .

Задача 8.6 (вокруг теоремы Лиувилля).

- 1) Для алгебраического числа α обозначим через $|\alpha|$ максимум модулей сопряжённых с α чисел. Доказать следующие свойства $|\cdot|$:
 - а) $|q\alpha| = |q| \cdot |\alpha|$ при $q \in \mathbb{Q}$;
 - б) $|\alpha \pm \beta| \leq |\alpha| + |\beta|$;
 - в) $|\alpha\beta| \leq |\alpha| \cdot |\beta|$.
- 2) Доказать (обобщённое) неравенство Лиувилля: если $\zeta \neq 0$ — целое алгебраическое число степени d , то $|\zeta| \geq |\bar{\zeta}|^{1-d}$.
- 3) Вывести из п. 2 обычную теорему Лиувилля: если α — алгебраическое число степени d , то для любого рационального числа $\frac{p}{q} \neq \alpha$ выполнено неравенство

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha)}{q^d},$$

где $c(\alpha)$ — некоторая положительная постоянная, зависящая только от α .

- 4) Доказать, что число $\sum_{n=0}^{\infty} 2^{-2^{n^2}}$ трансцендентно.
- 5) Пусть α — алгебраическое число, $0 < |\alpha| < 1$. Доказать, что число $\beta = \sum_{n=0}^{\infty} \alpha^{n!}$ трансцендентно. (Указание. Допустив противное, рассмотреть $\beta - \sum_{n=0}^N \alpha^{n!}$, избавиться от знаменателя и применить обобщённое неравенство Лиувилля.)

Задача 8.7 (континуум алгебраически независимых чисел). Рассмотрим числа

$$\alpha_t = \sum_{n=0}^{\infty} 2^{-2^{\lfloor tn \rfloor}}, \quad t > 0.$$

Доказать, что для любых различных t_1, \dots, t_m числа $\alpha_{t_1}, \dots, \alpha_{t_m}$ алгебраически независимы (над \mathbb{Q}), т.е. для любого ненулевого многочлена $P(z_1, \dots, z_m) \in \mathbb{Q}[z_1, \dots, z_m]$ выполнено $P(\alpha_{t_1}, \dots, \alpha_{t_m}) \neq 0$. (Указание. Допустим, что $P(\alpha_{t_1}, \dots, \alpha_{t_m}) = 0$. Для $N \in \mathbb{N}$ обозначим $a_j(N) = \sum_{n=0}^{N-1} 2^{-2^{\lfloor t_j n \rfloor}}$. Разложив P в ряд Тейлора в точке $(\alpha_{t_1}, \dots, \alpha_{t_m})$ и используя то, что произведения $(a_1(N) - \alpha_{t_1})^{k_1} \dots (a_m(N) - \alpha_{t_m})^{k_m}$ для разных $(k_1, \dots, k_m) \in \mathbb{N}_0^m$

стремятся к нулю с разной скоростью, доказать, что при достаточно больших N будет выполнено

$$0 < |P(a_1(N), \dots, a_m(N))| < 2^{-2^{t_0 N}}$$

для некоторого $t_0 > 0$. Учитывая, что $P(a_1(N), \dots, a_m(N))$ — это рациональные числа с не слишком большими знаменателями, получить противоречие.)

Задача 8.8. Доказать, что числа $\alpha_1, \dots, \alpha_m \in \mathbb{C}$ алгебраически независимы над \mathbb{Q} тогда и только тогда, когда они алгебраически независимы над \mathbb{A} . (Указание. Вспомнить доказательство алгебраической замкнутости \mathbb{A} .)

Задача 8.9. Доказать эквивалентность следующих четырёх вариантов теоремы Линдемана–Вейерштрасса:

- 1) Если $\alpha_1, \dots, \alpha_m$ — различные алгебраические числа, то числа $e^{\alpha_1}, \dots, e^{\alpha_m}$ линейно независимы над \mathbb{A} .
- 2) Если алгебраические числа $\alpha_1, \dots, \alpha_m$ линейно независимы над \mathbb{Q} , то числа $e^{\alpha_1}, \dots, e^{\alpha_m}$ алгебраически независимы над \mathbb{A} .
- 3) Если алгебраические числа $\alpha_1, \dots, \alpha_m$ линейно независимы над \mathbb{Q} , то числа $e^{\alpha_1}, \dots, e^{\alpha_m}$ алгебраически независимы над \mathbb{Q} .
- 4) Если $\alpha_1, \dots, \alpha_m$ — различные алгебраические числа, то числа $e^{\alpha_1}, \dots, e^{\alpha_m}$ линейно независимы над \mathbb{Q} .

Задача 8.10. Пусть $\alpha \in \mathbb{A}^*$. Используя теорему Линдемана–Вейерштрасса, доказать, что числа $1, \cos \alpha, \sin \alpha, \operatorname{ch} \alpha, \operatorname{sh} \alpha$ линейно независимы над \mathbb{A} ; в частности, числа $\cos \alpha, \sin \alpha, \operatorname{tg} \alpha, \operatorname{ch} \alpha, \operatorname{sh} \alpha, \operatorname{th} \alpha$ трансцендентны.

Задача 8.11. Пусть $m \in \mathbb{N}$. Для $k \in \{0, 1, \dots, m-1\}$ определим функции

$$f_k(z) = f_{m,k}(z) = \sum_{n=0}^{\infty} \frac{z^n}{(mn+k)!}$$

Пусть числа $\alpha_1, \dots, \alpha_l \in \mathbb{A}^*$ различны. Используя теорему Линдемана–Вейерштрасса, доказать, что $1+ml$ чисел $1, f_k(\alpha_j), 0 \leq k \leq m-1, 1 \leq j \leq l$, линейно независимы над \mathbb{A} (в частности, все числа $f_{m,k}(\alpha_j)$ трансцендентны). (Указание. Выразить функции $f_k(z)$ через функции $\exp(\sqrt[m]{z} e^{2\pi i a/m}), 0 \leq a \leq m-1$.)

Задача 8.12. Доказать эквивалентность следующих двух формулировок теоремы Гельфонда–Шнайдера (ака седьмой проблемы Гильберта):

- 1) Пусть $\alpha, \beta \in \mathbb{A}$, причём $\alpha \neq 0, \ln \alpha \neq 0, \beta \notin \mathbb{Q}$. Тогда число $\alpha^\beta = e^{\beta \ln \alpha}$ трансцендентно.
- 2) Пусть $a, b \in \mathbb{A}^*$, причём $\ln b \neq 0, \frac{\ln a}{\ln b} \notin \mathbb{Q}$. Тогда число $\frac{\ln a}{\ln b}$ трансцендентно.

Задача 8.13. Используя теорему Гельфонда–Шнайдера, доказать трансцендентность чисел: e^π ; $\frac{\operatorname{arctg} \sqrt{a}}{\pi}$ при рациональном $a > 0, a \neq 1, 3, 1/3$. (Указание. См. задачу 7.21.)

Задача 8.14. Рассмотрим число $\alpha = \sum_{n=0}^{\infty} 2^{-2^n}$. Доказать, что α трансцендентно, но не является числом Лиувилля. Подзадачи:

1) Обозначим $q_N = 2^{2^N}$, $p_N = q_N \sum_{n=0}^N 2^{-2^n}$, $N \in \mathbb{N}_0$. Доказать утверждения:

а) Дробь p_N/q_N несократима, и

$$\frac{1}{q_N^2} < \alpha - \frac{p_N}{q_N} < \frac{2}{q_N^2}.$$

б) Если $p/q = p_N/q_N$ для некоторого N , то

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{q^2}.$$

в) Пусть $p/q \neq p_N/q_N$ для всех N . Возьмём $N \in \mathbb{N}$, такое что $\frac{1}{4}q_{N-1} < q \leq \frac{1}{4}q_N$. Тогда

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{2qq_N} > \frac{1}{32q^3}.$$

(Указание. Воспользоваться тем, что $\left| \frac{p - q\alpha}{p_N - q_N\alpha} \frac{q}{q_N} \right| = \left| \frac{p}{p_N} \frac{q}{q_N} \right| \in \mathbb{Z} \setminus \{0\}$.)

(Замечание. На самом деле можно доказать, что для некоторой положительной постоянной c всегда выполнено $\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^2}$.)

2) (Метод Малера.) Рассмотрим функцию $f(z) = \sum_{n=0}^{\infty} z^{2^n}$, $|z| < 1$.

а) Доказать, что $f(z^2) = f(z) - z$.

б) Доказать, что функция $f(z)$ трансцендентна. (Указание. Например, воспользоваться тем, что $\lim_{r \rightarrow 1-0} |f(re^{2\pi i q})| = +\infty$ для любого двоично-рационального числа $q = a/2^n$.)

в) Пусть $d \in \mathbb{N}$. Доказать, что существуют многочлены $P_0(z), \dots, P_d(z) \in \mathbb{Z}[z]$ с $\deg P_k \leq d$, не все равные 0 и такие, что для функции

$$F(z) = \sum_{k=0}^d P_k(z) f^k(z)$$

выполнено $F(0) = F'(0) = \dots = F^{(d^2)}(0)$. (Указание. Коэффициенты многочленов должны удовлетворять системе линейных уравнений.)

г) Пусть $F(z)$ — функция, построенная выше. Доказать, что для всех достаточно больших N выполнено

$$0 < |F(2^{-2^N})| < 2^{-2^N d^2}.$$

д) Используя пункты 2а и 2г, доказать трансцендентность числа $\alpha = f(1/2)$. (Указание. Выразить $f(2^{-2^N})$ через α и подставить в $F(2^{-2^N})$. Далее, предположив противное, применить обобщённое неравенство Лиувилля и для подходящего d получить противоречие при $N \rightarrow \infty$.)

(Замечание. Другие примеры нелиувиллевых трансцендентных чисел — это e и π . Для e нелиувиллевость проще всего получить из разложения в цепную дробь; с числом π ситуация посложнее.)



Многа букаф, ниасилил.