МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

# ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ


НЕСТЕРЕНКО
ЮРИЙ ВАЛЕНТИНОВИЧ

МЕХМАТ МГУ

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТКУ ФАКУЛЬТЕТА ВМК МГУ
**НЕДОЛИВКО ЮЛИЮ НИКОЛАЕВНУ**

# Содержание

# Лекция 1

## Введение

Теория чисел – такой же древний раздел математики, как и геометрия. Вообще говоря, как и геометрию, всю арифметику можно развернуть на пяти аксиомах [1].

Множество *натуральных* чисел, то есть числа

$$1,\ 2,\ 3,\ 4,\ \ldots,\ 99,\ 100,\ \ldots$$

будем обозначать через $\mathbb{N}$. Через $\mathbb{Z}$ будем обозначать *целые* числа. Потом появились *рациональные* числа как отношения целых.

Одним из выдающихся открытий древнегреческой математики было то, что *существуют отрезки, которые нельзя измерить*.

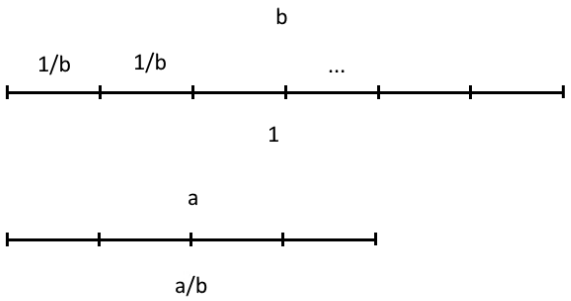


Рис. 1.1. Измерение отрезков.

Что значит измерить? Фиксируем какой-то отрезок, длина которого считается равной 1. С помощью него можно измерять другие. Например, исходный отрезок разделим на $b$ равных кусочков. Если на том отрезке, который хотим измерить, укладывается ровно $a$ этих маленьких кусочков, его длина будет равняться $a/b$ (рис. 1.1).

Так вот, древние греки обнаружили, что рациональных чисел не хватает для измерения всех отрезков. Простой пример – диагональ квадрата со стороной 1.

Спустя много лет были введены *действительные* числа, что установило взаимнооднозначное соответствие между отрезками и числами.

Поскольку действительные числа были введены не сразу, возникла традиция решать уравнения в целых и рациональных числах.[2] Другой пример изучения чисел в Древней Греции – это вопрос *простых* чисел.[3]

[1] *Аксиомы Пеано* были предложены в XIX в. В курсе на них не останавливаемся. Для тех, кто интересуется основаниями, рекомендуется изучить книгу Э. Ландау «Основы анализа», 1947.

[2] Такие уравнения называются *диофантовыми*.

[3] Евклид доказал, что множество простых чисел бесконечно.

С развитием математики для решения задач применялись все новые методы. Некоторые вопросы, например, *существуют ли нечетные совершенные числа*, до сих пор не решены.

Так, образовались геометрия чисел, вероятностная теория чисел, теория алгебраических чисел и др. разделы.

Список книг для подготовки:

1. И.М. Виноградов, "Основы теории чисел";
2. А.А. Бухштаб, "Теория чисел";
3. З.И. Боревич, И.Р. Шафаревич, "Теория чисел";
4. Ю.В. Нестеренко, "Теория чисел".

### Аксиома индукции

В аксиоматике Пеано важно понятие *следования*. За каждый натуральным числом $n$ следует единственное натуральное число.[4] Каждому натуральному числу, кроме 1, предшествует единственное натуральное число.

Остановимся подробнее на одной из аксиом.

**Аксиома** (индукции) Пусть $M$ – множество натуральных чисел с двумя свойствами

1. $1 \in M$;
2. Если $n \in M$, то $n + 1 \in M$.

Тогда $M = \mathbb{N}$.

Следствием из этой аксиомы являются следующие теоремы.

- Каждое подмножество $\mathbb{N}$ содержит наименьший элемент.
- Каждое конечное подмножество мн-ва $\mathbb{N}$ содержит наибольший элемент.

# Глава 1

## §1 Делимость целых чисел

**Определение 1.1.** Пусть $a$, $b$ – целые числа, $b \neq 0$. Говорят, что $a$ *делится на* $b$, если существует целое число $c$ такое, что $a = b \cdot c$.

Обозначается $a \vdots b$ ($a$ делится на $b$) или $b|a$ ($b$ делит $a$). $a$ называется *делимым*, а $b$ – *делителем*.

**Свойства делимости**

1. $1|a$.
2. Если $a \neq 0$, то $a|a$.
3. Если[5] $a|b$, $b|c$ ($a \neq 0$, $b \neq 0$), то $a|c$.

[4] Его обычно обозначают $n'$ или $n + 1$.

[5] В этом и следующих свойствах подразумевается, что делитель отличен от 0.

4. Если $a|b$, $a|c$, то $a|b \pm c$.

5. Если $a|b$, то при любом целом $c$ $a|bc$.

6. Если $a|b$ и $b \neq 0$, то $|a| \leq |b|$.

**Теорема 1.1.** *(Теорема о делимости) Если $a$ – целое и $b$ – натуральное числа, то существует единственная пара целых чисел $q$ и $r$[6] таких, что*

$$a = bq + r, \quad 0 \leq r < b.$$

**Доказательство** I. Существование.

Фиксируем $b$. Будем проверять наличие $q$ и $r$ при разных $a$.

1. Возьмем $a = 0$. Тогда $q = 0$, $r = 0$, получается

$$0 = b \cdot 0 + 0, \quad 0 \leq 0 < b.$$

2. Делимое есть натуральное число.

Пусть $a$ – наименьшее натуральное число, для которого утверждение теоремы неверно. Возможны два случая:

а) $1 \leq a < b$.

Возьмем $q = 0, r = a$ и получим

$$0 = b \cdot 0 + a.$$

Значит, для всех $1 \leq a < b$ утверждение теоремы верно.

б) $a$.

Для него $a - b \geq 0$ и $a - b < a$. Тогда $\exists\, r$, $t$ такие, что

$$a - b = b \cdot r + t, \quad 0 < b,$$

так как мы предположили, что $a$ – наименьшее число, для которого утверждение не выполняется. Значит,

$$a = b(r + 1) + t, \quad q = r + 1, \quad r = t.$$

Значит, для всех натуральных чисел $a$ утверждение теоремы выполняется.

3. $a < 0$.

Рассмотрим число $-a + b - 1$ – натуральное. Тогда

$$-a + b - 1 = b \cdot u + v, \quad 0 < b,$$

$$a = b \cdot (-u) + b - 1 - v, \quad q = -u, \quad r = b - 1 - v.$$

Так как $0 \leq v \leq b - 1$, то $r \geq 0$ и $r < b$.

II. Единственность.

[6] Число $r$ называется *остатком*, а $q$ – *неполным частным*.

Предположим, что у нас есть две пары чисел

$$a = bq_1 + r_1 = bq_2 + r_2, \quad 0_1 < b, \quad 0 \leq r_2 < b.$$

Будем считать, что $r_{12}$.

Предположим сначала, что $r_1 > r_2$. Вычитая, получим

$$r_1 - r_2 = b(q_2 - q_1),$$

а значит, $b|r_1 - r_2$. Так как $0 < r_1 - r_2 \leq r_1 < b$, получаем противоречие (делитель не может быть меньше делимого).

В случае, если $r_1 = r_2$, получаем, что

$$b(q_2 - q_1) = 0, \quad \Rightarrow q_2 - q_1 = 0.$$

Получаем, что пары

$$\{q_1, r_1\} = \{q_2, r_2\}.$$

Теорема доказана.

## §2 НОК и НОД

Пусть $a_1, \ldots, a_m$ – натуральные числа и $K$ – натуральное такие, что $a_i|K$. Такое $K$ называется *общим кратным* чисел $a_1, \ldots, a_m$.

Наименьшее общее кратное чисел $a_1, \ldots, a_m$ есть самое маленькое из их общих кратных.

Наименьшее общее кратное принято обозначать $\text{НОК}(a_1, \ldots, a_m)$ или $[a_1, \ldots, a_m]$.

Например, $[2, 3, 6, 7] = 42$.

**Теорема 1.2.** *Каждое общее кратное некоторых натуральных чисел делится на их наименьшее общее кратное.*

**Доказательство** Предположим, у нас есть некоторые натуральные $a_1, \ldots, a_m$. Обоначим $[a_1, \ldots, a_m] = b$.

Пусть $K$ – какое-то общее кратное $a_1, \ldots, a_m$.

$$K = b \cdot q + r, \quad 0 \leq r < b.$$

Из того, что

$$a_1|K,\ a_1|b \Rightarrow a_1|r.$$

Аналогично для всех $a_i$ получим, что $a_i|r$. Таким образом, $r$ – делится $a_1, \ldots, a_m$ и не может быть натуральным (т.к. $r < b$), а значит, $r = 0$.

Тогда $K = b\dot{q}$, т.е. $b|K$.

Теорема доказана.

Пусть $a_1, \ldots, a_m$ – целые числа, хотя бы одно отлично от нуля. Натуральное $d$ называется *общим делителем* чисел $a_1, \ldots, a_m$, если

$$d|a_i, \quad i = 2, \ldots, m.$$

Самый большой из общих делителей называется *наибольшим общим делителем* $a_1, \ldots, a_m$ [7].

Обозначения: НОД$(a_1, \ldots, a_m)$ или $(a_1, \ldots, a_m)$.

Числа $a$ и $b$ называются *взаимно простыми*, если $(a, b) = 1$.

Числа $a_1, \ldots, a_m$ – взаимно просты в совокупности, если $(a_1, \ldots, a_m) = 1$.

Вернемся к следствиям из теоремы 1.2.

**Следствие 1.** Если $a, b$ – натуральные числа, то

$$[a, b] \cdot (a, b) = a \cdot b.$$

**Доказательство** $a$ – общее кратное $a$ и $b$. Значит, по теореме 1.2

$$[a, b] | ab, \quad \frac{ab}{[a, b]} \in \mathbb{N}.$$

Запишем

$$a = \frac{ab}{[a, b]} \frac{[a, b]}{b}, \quad b = \frac{ab}{[a, b]} \frac{[a, b]}{a}.$$

Значит, $ab/[a, b]$ – общий делитель $a$ и $b$.

Покажем, что это НОД $a$ и $b$. Пусть $d$ – общий делитель $a$ и $b$. Рассмотрим дробь

$$\frac{ab}{d} = a\frac{b}{d} = b\frac{a}{d}.$$

Значит, $ab/d$ – общее кратное $a$ и $b$.

По теореме 1.2

$$[a, b] \left| \frac{ab}{d} \right. \Rightarrow \frac{ab}{d} = [a, b] \cdot c.$$

Значит,

$$\frac{ab}{[a, b]} = dc \Rightarrow d \left| \frac{ab}{[a, b]} \right. .$$

Так, доказали, что любой общий делитель делится на $ab/[a, b]$, а значит

$$\frac{ab}{[a, b]} = (a, b).$$

Следствие доказано.

**Следствие 2** Пусть $a, b, c$ – натуральные, $a|bc$, $(a, b) = 1$. Тогда $a|c$.

**Доказательство** Так как

$$a|bc, \quad b|bc,$$

$bc$ – общее кратное $a$ и $b$. По теореме 1.2 $\Rightarrow [a, b]|bc$. Тогда

$$[a, b] = a \cdot b \Rightarrow ab|bc,$$

тогда

$$bc = abu,$$
$$c = au \Rightarrow a|c.$$

Следствие доказано.

[7] Так как хотя бы одно, например, первое число $a_1 \neq 0$, а $d|a_1$, получается, что $d \leq |a_1|$. Множество таких чисел конечно, поэтому среди них найдется наибольшее.

# Лекция 2

## Глава 2. Простые и составные числа

Все натуральные числа, большие 1, разбиваются на два класса: *простые* и *составные*. 1 ни к одному из этих классов не относится.

**Определение 2.1.** Целое число $n \geq 2$ называется *составным*, если его можно разложить на два меньших множителя:

$$n = u \cdot v, \quad v < n, \quad u < n.$$

**Определение 2.2.** $n \geq 2$ называется *простым*, если оно не составное.

**Примеры** Составные числа:

$$12 = 3 \cdot 4,$$

$$111 = 3 \cdot 37,$$

$$1111111 = 239 \cdot 4649.$$

Простые числа:

$$7 = 1 \cdot 7,$$

$$2 = 1 \cdot 2.$$

Самое большое известное на сегодняшний день простое число

$$2^{77232917} - 1.$$

Простые, большие этого, числа точно есть, но пока неизвестно, как они выглядят.

**Теорема 2.1.** *(Евклид) Множество простых чисел бесконечно.*

**Доказательство** Рассмотрим число

$$N = n! + 1.$$

Чуть позже покажем, что найдется простое число $p|N$. Допустим, что $p \leq n$.

Тогда так как $p|N$ и $p|n!$, получим, что из

$$1 = N - n! \Rightarrow p|1.$$

Пришли к противоречию, так как $p \geq 2$.

Значит, $p > n$. То есть, какую бы мы границу $n$ не взяли, найдется простое число $p$, большее этой границы.

Докажем теперь, что каждое целое число имеет простой делитель.

**Лемма 2.1.** *Если $N$ – составное число, то существует простое $p$ такое, что $p|N$ и $p^2 \leq N$* [8].

[8] То есть, чтобы проверить, простое ли число, достаточно проверять, являются ли его множителями числа, не превосходящие корня из этого числа.

**Доказательство** Так как $N$ составное,

$$N = u \cdot v, \quad 1 < u < N, \quad 1 < v < N.$$

Выберем $p$ – наименьший делитель $N$ с условием $p > 1$. Тогда

$$1 < p \leq u, \quad 1 < p \leq v.$$

Перемножая эти неравенства, получим, что

$$p^2 \leq u \cdot v = N.$$

Докажем теперь, что $p$ – простое.
Допустим, что $p$ – составное. Тогда

$$p = a \cdot b, \quad 1 < a < p, \quad 1 < b < p.$$

$$a|p, \quad p|N \Rightarrow a|N.$$

Тогда $a$ удовлетворяет тем же условиям, что и $p$, но меньше его. Получаем противоречие, т.к. выбирали $p$ как наименьший делитель $N$.
Лемма доказана.

**Лемма 2.2.** *Каждое целое число $N \geq 2$ имеет простой делитель.*

**Доказательство** Возможны два варианта.

1. $N$ – простое, тогда $N|N$.

2. $N$ – составное. Тогда из леммы 2.1 $\exists\, p|N$.

Лемма (и, значит, теорема 2.1) доказана.

## §1 Решето Эратосфена

Рассмотрим алгоритм, который позволяет найти сразу все простые числа на отрезке

$$2, 3, \ldots, N.$$

**Алгоритм** (Решето Эратосфена)

1. Положим $p_1 = 2$. Выписать все число от 2 до $N$ и, начиная с 4, с с шагом 2 вычеркнуть все числа до $N$. Число 2 выделим (рис. 2.1).

2. Предположим, что $k \geq 2$ и $p_1, \ldots, p_{k-1}$ выделены. Определим $p_k$ – наименьшее из невычеркнутых и невыделенных. Начиная с $p_k^2$, если $p_k^2 \leq N$, вычеркнуть все числа с шагом $p_k$ (рис. 2.2). [9]

3. Если $p_k^2 > N$, алгоритм останавливается. Все оставшиеся числа – простые (рис. 2.3).

[9] Вычеркнутые на предыдущих шагах числа мы, конечно, учитываем при счете шага.

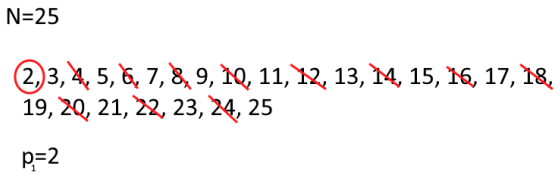


Рис. 2.1. $p_1$=2. Первый шаг алгоритма.

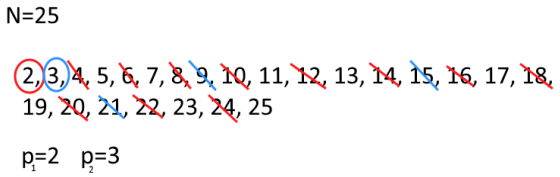


Рис. 2.2. $p_2$=3

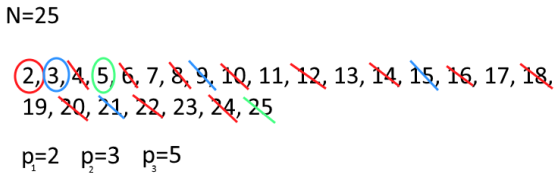


Рис. 2.3. $p_3$=5. Остановка алгоритма.

**Теорема 2.2.** *Решето Эратосфена находит все простые числа на отрезке от* 2 *до* $N$.

**Доказательство** Убедимся, что выполнены следующие утверждения.

1. Алгоритм вычеркивает только составные числа.

Действительно, на шаге $p_k$ мы вычеркиваем все числа вида

$$p_k^2 + l \cdot p_k = p_k(p_k + l), \quad l = 0, 1, 2, \ldots,$$

то есть только составные числа.

Все простые числа остались.

2. Все составные числа от 2 до $N$ будут вычеркнуты.

Предположим обратное. Пусть $a$ – составное, осталось невычеркнутым по окончании работы алгоритма. Из леммы 2.1 следует, что $\exists\, p$ – простое, $p|a$, $p^2 \leq a \leq N$.

Но мы вычеркивали, начиная с $p^2$, все числа, делящиеся на $p$. Значит, должны были вычеркнуть и $a$. Получаем противоречие.

Теорема доказана.

## §2 Основная теорема арифметики

**Теорема 2.3.** *Каждое целое число* $n \geq 2$ *может быть представлено в виде произведения простых чисел единственным способом. При этом*

*1. Два представления считаются одинаковыми, если они отличаются только порядком сомножителей*[10]*.*

*2. Представление может состоять из одного множителя.*

**Доказательство** Предположим, что есть целые числа $\geq 2$, для которых теорема неверна. Пусть $n$ – самое маленькое из них, т.е. для $\forall m$, $2 \leq m < n$ утверждение верно.

1. Если $n$ – простое, утверждение верно.

2. $n$ – составное (и $n > 5$). По лемме 2.1 $\exists$ простое $p$, $p|N$, $p^2 \leq n$. Тогда $n$ можно представить в виде

$$n = p \cdot m, \quad 2 \leq m < n.$$

Так как $m < n$, по нашему предположению

$$m = q_1 \cdot \dots \cdot q_s,$$

$q_i$ – простые, представление единственно. Тогда

$$n = p \cdot q_1 \dots q_s.$$

Получили, что $n$ можем представить в виде произведения простых чисел. Тогда по нашему предположению, что теорема неверна, для него нарушается единственность такого представления. Можем представить

$$n = l_1 \cdot \dots \cdot l_t,$$

$l_i$ – простые. Если $p = l_t$, то

$$m = q_1 \dots q_s = l_1 \dots l_{t-1}.$$

Для $m$ теорема верна, значит, $s = t - 1$ и множества

$$\{q_1, \dots, q_s\} = \{l_1, \dots, l_{t-1}\}.$$

То же самое получается, если $p$ совпадает с каким-то другим из $l_i$. Остается рассмотреть случай $p \neq l_i, \quad i = 1, \dots, l_t$..

Мы знаем, что $p|l_1 \dot{x} l_t$, $l_i$ – простые.

Вспомним утверждение прошлой лекции. Если $a|bc$ и $(a, b) = 1$, тогда $a|c$.

Как как $(p, l_1) = 1$, то $p|l_2 \dots l_t$. Продолжая рассуждать таким образом, получим, что $p|l_t \cdot 1$, то $p|1$, что неверно.

Теорема доказана.

**Определение 2.3.** Представление

$$n = q_1^{k_1} \dots q_s^{k_s}, \quad q_1 \leq \dots \leq q_s$$

называется *каноническим.*

[10]Например,

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2.$$

Каноническое представление единственно.

Обозначим $\nu_p(n)$ – кратность, с которой простое число $p$ входит в каноническое представление $n$ [11].

Иногда бывает удобно записывать

$$n = \prod_p p^{\nu_p(n)}.$$

[11]При этом, например, $\nu_5(12) = 0$, т.к. 5 не входит в каноническое разложение 12.

# Лекция 3

## Свойства кратностей

**Свойства кратностей** $\nu_p(n)$

1. $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

Следует из того, что, с одной стороны,

$$a \cdot b = \prod_p p^{\nu_p(ab)},$$

а с другой,

$$a \cdot b = \left(\prod_p p^{\nu_p(a)}\right)\left(\prod_p p^{\nu_p(b)}\right) = \prod_p p^{\nu_p(a)+\nu_p(b)},$$

и что такое представление единственно.

2. $c|a \iff \forall p.$

$$\nu_p(c) \le \nu_p(a). \tag{1}$$

Заметим сначала, что

$$c|a \iff \exists\, d, \quad a = c \cdot d.$$

Тогда

$$\forall p\, \nu_p(a) = \nu_p(c) + \nu_p(d) \ge \nu_p(c).$$

3. $a = b \iff \nu_p(a) = \nu_p(b)$.

Следует из пункта 2. Так как $a = b$,

$$a|b, \quad b|a \iff \nu_p(a) \le \nu_p(b), \quad \nu_p(b) \le \nu_p(a).$$

**Утверждение 3.1.**

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + dots = \tag{2}$$
$$= \sum_{k\ge 1}\left[\frac{n}{p^k}\right].$$

*где* $[x]$ *– наибольшее целое* $k$, $k \le x$ [12].

Запишем сначала несколько свойств для $[x]$ – целой части $x$.

1. $[x] + [y] \le [x + y]$.

Так как

$$[x] \le x, \quad [y] \le y,$$

[12]Например, $[2.5] = 2$, а $[-2.5] = -3$. Заметим также, что сумма в утверждении конечна.

то

$$[x] + [y] \leq x + y.$$

В левой части записано целое число, а наибольшее целое, не превосходящее $x + y$, это его целая часть $x + y$. Отсюда получаем, что

$$[x] + [y] \leq [x + y].$$

2. Если $x$ – действительное, а $a$ – целое, то

$$\left[\frac{x}{a}\right] = \left[\frac{[x]}{a}\right]. \tag{3}$$

Обозначим

$$q = \left[\frac{x}{a}\right].$$

Тогда

$$q \leq \frac{x}{a} < q + 1,$$

или

$$aq \leq x < a(q + 1).$$

По определению $[x]$ – наибольшее целое, не превосходящее $x$, а $qa$ – произведение целых чисел, то

$$aq \leq [x] \leq x < a(q + 1).$$

Разделив на $a$, получим, что

$$q \leq \frac{[x]}{a} < q + 1.$$

Получили, что $q$ – наибольшее целое, не превосходящее $[x]/a$, то есть

$$q = \left[\frac{[x]}{a}\right].$$

Теперь вернемся к формуле (2).

**Доказательство** (по индукции).

1. (база индукции) $n < p$. В этом случае $p \not| n!$. Это следует из того, что все сомножители

$$n! = 1 \cdot 2 \ldots n$$

меньше, чем $p$.

Значит, $\nu_p(n!) = 0$. Так как

$$n < p,\ p^2,\ p^3, \ldots,$$

получим, что

$$\sum_{k \geq 1} \left[\frac{n}{p^k}\right] = 0.$$

2. (шаг индукции) Предположим, что для всех $a < n$ выполнено

$$\nu_p(a!) = \sum_{k\geq 1} \left[\frac{a}{p^k}\right].$$

Посчитаем теперь кратность

$$n! = 1 \cdot 2 \ldots n, \quad n \geq p.$$

Числа, кратные $p$, в этом разложении выглядят как

$$p,\ 2p,\ 3p,\ \ldots,\ mp,$$

причем $m$ – наибольшее такое, что

$$m\cdot \leq n, \quad m \leq \frac{n}{p},$$

откуда

$$m = \left[\frac{n}{p}\right]. \tag{4}$$

Воспользуемся свойством кратности и запишем

$$\nu_p(n!) = \nu_p(1) + \nu_p(2) + \cdots + \nu_p(n) =$$

$$= \nu_p(p) + \nu_p(2p) + \cdots + \nu_p(mp),$$

так как остальные сомножители $n!$ на $p$ не делятся. Собирая опять все вместе, получим

$$\nu_p(n!) = \nu_p(p^m m!) = m + \nu_p(m!).$$

Воспользуемся формулой (4) и запишем

$$\left[\frac{m}{p^k}\right] = \left[\frac{[n/p]}{p^k}\right]. \tag{5}$$

Положив в (3) $a = p^k$, $x = n/p$, получим

$$\left[\frac{n/p}{p^k}\right] = \left[\frac{n}{p^{k+1}}\right].$$

Значит,

$$\left[\frac{m}{p^k}\right] = \left[\frac{n}{p^{k+1}}\right].$$

Возвращаясь к формуле (5), окончательно получим

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots.$$

Утверждение доказано.

Запишем вторую полезную нам формулу.

**Утверждение 3.2.** *Пусть $a_1, a_2, \ldots, a_m$ – натуральные.*
*Тогда для простого $p$*

$$\nu_p\left([a_1, a_2, \ldots, a_m]\right) = \max_{1\le i\le m} \nu_p(a_i). \tag{6}$$

**Пример** Вычислим $\nu_p(K)$, $K = [6, 10, 15]$. Имеем

$$6 = 2 \cdot 3,$$

$$10 = 2 \cdot 5,$$

$$15 = 3 \cdot 5.$$

Так, согласно (6), получим, что

$$\nu_2(K) = 1, \quad \nu_3(K) = 1, \quad \nu_5(K) = 1,$$

и для $p > 5$

$$\nu_p(K) = 0.$$

Значит, можем записать

$$K = 2 \cdot 3 \cdot 5 = 30.$$

**Доказательство** Обозначим

$$[a_1, a_2, \ldots, a_m] = K.$$

Имеем

$$a_1|K, \quad a_2|K, \quad \ldots \ a_m|K.$$

Это выполняется тогда и только тогда, когда для $\forall p$ выполнено

$$\nu_p(a_1) \le \nu_p(K),$$

$$\nu_p(a_2) \le \nu_p(K),$$

$$\ldots$$

$$\nu_p(a_m) \le \nu_p(K).$$

По (1) это выполнено $\Longleftrightarrow$

$$\max_{1\le m} \left(\nu_p(a_k)\right) \le \nu_p(K).$$

Отсюда следует, что

$$\nu_p(K) = \max_{1\le i\le m} \nu_p(a_i).$$

В противном случае, если это было бы неверно, неравенство строгое

$$\max_{1\le i\le m} \left(\nu_p(a_k)\right) < \nu_p(K).$$

Можем разделить обе части на $p$ и получить

$$\max_{1\leq m}(\nu_p(a_k)) \leq \nu_p\left(\frac{K}{p}\right).$$

Для простого $q \neq p$

$$\nu_q\left(\frac{K}{p}\right) = \nu_q(K).$$

Это значит, что для нестрогого неравенства можем заменить $K$ на $K/p$. Тогда получим, что

$$a_i \left| \frac{K}{p} \quad 1 \leq i \leq m. \right.$$

Это невозможно, так как $K$ – НОК чисел $a_i$. Утверждение доказано.

## §3 Теорема Чебышёва

Введем следующее обозначение.
$\pi(x)$ – количество простых $p$ таких, что $1 \leq x$.
Можем утверждать, во-первых, что

$$\pi(x) \to \infty, \quad x \to +\infty,$$

и, во-вторых, что

$$\pi(x) \leq [x].$$

Можно вывести более точную оценку. Положим $[x] = N$. Воспользуемся решетом Эратосфена для $N$.

Из чисел

$$1,\, 2,\, \ldots,\, N$$

делятся на 2 числа

$$2,\, 2\cdot 2,\, 2\cdot 3, \ldots, 2\cdot m,$$

где $m$ – наибольшее число

$$2m \leq N, \quad m \leq \frac{N}{2}.$$

Значит, $m = [N/2]$.

Среди чисел, делящихся на 2, $m-1$ составное число (все, кроме 2).

Тогда[13]

$$\pi(N) \leq N - 1 - (m-1) = N - m = N - \left[\frac{N}{2}\right] = \left[\frac{N+1}{2}\right] \leq \frac{N+1}{2}$$

Предпоследний переход следует из того, что

$$\left[\frac{N}{2}\right] + \left[\frac{N+1}{2}\right] = N.$$

[13]Запись $N-1$ означает, что из чисел $1, \ldots, N$ мы исключаем единицу.

Действительно, если $N = 2m$,

$$\left[\frac{2m}{2}\right] + \left[\frac{2m+1}{2}\right] = m + m = N,$$

а если $N = 2m + 1$,

$$\left[\frac{2m+1}{2}\right] + \left[\frac{2m+2}{2}\right] = m + m + 1 = N.$$

Продолжая рассуждения для чисел 3, 5 и так далее, можно показать, что

$$\frac{\pi(x)}{x} \to 0, \quad x \to \infty.$$

**Пример**

$$\pi(2) = 1,$$
$$\pi(10) = 4,$$
$$\pi(10.5) = 4,$$
$$\pi(10^{12}) = 37607912018.$$

**Теорема 3.1.** *(Чебышёва)* $\exists\ a = 1/2\ln 2,\ b = 5\ln 2$ *такие, что*

$$a\frac{x}{\ln x} \le \pi(x) \le b\frac{x}{\ln x}$$

*для* $x \ge 6$.[14] [15]

Для доказательства нам понадобится две леммы.

**Лемма 3.1.**

$$[1, 1, 3, \ldots, 2n+1] > 4^n.$$

**Доказательство** Первое утверждение, которое докажем (по индукции), что

$$R_n(x) = \frac{n!}{x(x+1)\ldots(x+n)}$$

[14] Чебышёв доказал утверждение для $a = 0,921\ldots$, $b = 1,105\ldots$ и достаточно больших $x$. Нам будет достаточно менее точных констант.

[15] В 1896 году Адамаром и Валле-Пуссеном было доказано, что

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Сам Чебышёв сумел доказать, что если предел существует, то равен 1, но само существование предела не смог.

– рациональная по $x$ функция[16]. Для $n = 1$

$$R_1(x) = \frac{1}{x(x+1)} = \frac{1}{x} - \frac{1}{x+1}.$$

Представим

$$R_2(x) = \frac{2}{x(x+1)(x+2)} = \frac{(x+2)-x}{x(x+1)(x+2)} =$$

$$\frac{1}{x(x+1)} - \frac{1}{(x+1)(x+2)} = R_1(x) - R_1(x+1).$$

На этом же основан и шаг индукции.

$$R_n(X) = \frac{(n-1)!(x+n-x)}{x(x+1)\dots(x+n)} = R_{n-1}(x) - R_{n-1}(x+1).$$

Для коэффицентов $a_j$ можно найти точное выражение через биномиальные коэффициенты, но нам это не нужно.

Рассмотрим теперь функцию для $x = n+1$, то есть

$$R_n(n+1) = \frac{n!}{(n+1)(n+2)\dots(2n+1)} = \frac{n!n!}{(2n+1)!} =$$

$$= \frac{a_0}{n+1} + \frac{a_1}{n+2} + \dots + \frac{a_n}{2n+1}.$$

Обозначим

$$[1, 2, 3, \dots, 2n+1] = K.$$

Если домножим $K \cdot R_n(n+1)$, получим целое число, отличное от 0 и, значит, не меньшее 1 (так как $K$ – НОК чисел $n+1, n+2, \dots 2n+1$), т.е.

$$K \cdot R_n(n+1) \geq 1.$$

Отсюда следует, что

$$[1, 2, 3, \dots, 2n+1] \geq \frac{(2n+1)!}{n!n!}$$

Покажем теперь (тоже по индукции), что

$$\frac{(2n+1)!}{n!n!} > 4^n, \quad n \geq 1.$$

При $n = 1$

$$3! = 6 > 4^1 = 4.$$

[16]То есть можно представить

$$R_n(x) = \frac{a_0}{x} + \frac{a_1}{x+1} + \dots + \frac{a_n}{x+n},$$

где $a_j \in \mathbb{Z}$.

Теперь шаг индукции от $n-1$ к $n$. Преобразуем

$$\frac{(2n+1)!}{n!n!} = \frac{(2n+1)2n}{nn} \cdot \frac{(2n-1)!}{(n-1)!(n-1)!} >$$

$$> 4 \cdot 4^{n-1} = 4^n.$$

Здесь мы воспользовались тем, что вторая дробь – в точности выражение для $n-1$, для которого мы предположили оценку, а $(2n+1)2n/n^2 > 2n \cdot 2n/n^2 = 4$. Лемма доказана.

# Лекция 4

## Теорема Чебышёва (продолжение)

С помощью леммы 3.1 выведем доказательство нижней границы теоремы Чебышёва.

**Доказательство** (нижней границы).

Для $x \geq 6$ выберем $n$ так, чтобы

$$2n + 1 \leq x < 2n + 3. \tag{7}$$

Вспомним, что, согласно лемме 3.1,

$$4^n < [1, 2, \ldots, 2n + 1]. \tag{8}$$

Мы знаем, как сосчитать разложение на простые сомножители для НОК. Если есть натуральные $a_1$, $a_2$, $\ldots$, $a_m$, то

$$[a_1, a_2, \ldots, a_m] = \prod_p p^{\max(\nu_p(a_1),\ldots,\nu_p(a_m))}.$$

Так, нам надо в (8) разложить все числа на простые и для каждого простого выбрать наибольшую кратность, т.е. наибольшее $m$ такое, что

$$p^m \leq 2n + 1.$$

Прологарифмировав, получим

$$m \leq \frac{\ln 2n + 1}{\ln p}.$$

Так как $m$ – наибольшее целое, ограниченное таким числом,

$$m = \left[\frac{\ln 2n + 1}{\ln p}\right]$$

Согласно сказанному выше получим [17]

$$4^n < \prod_{p \leq 2n+1} p^{[\ln(2n+1)/\ln p]} \leq$$

$$\leq \prod_{p \leq 2n+1} p^{\ln(2n+1)/\ln p} = \prod_{p \leq 2n+1} (2n + 1) = (2n + 1)^{\pi(2n+1)}. \tag{9}$$

Здесь воспользовались тем, что

$$p^{\ln(2n+1)/\ln p} = e^{\ln p \ln(2n+1)/\ln p} = 2n + 1.$$

Прологарифмируем (9)

$$2n < \pi(2n + 1) \log_2(2n + 1),$$

[17] Ясно, что можем брать только простые $p$, которые делят числа из (8).

то есть

$$\pi(2n+1) > \frac{2n}{\log_2(2n+1)}$$

Из (7) следует, что

$$\pi(x) \geq \pi(2n+1) > \frac{2n}{\log_2(2n+1)} \geq \frac{2n}{\log_2 x},$$

и, с другой стороны,

$$2n \geq x - 3 \geq \frac{1}{2}x,$$

так как $x \geq 6$. Значит,

$$\pi(x) > \frac{1}{2}\frac{x}{\log_2 x} = \frac{\ln 2}{2}\frac{x}{\ln x}.$$

Нижняя оценка доказана. Для верхней оценки нам понадобится следующая лемма.

**Лемма 4.1.** *Для простых $p$*

$$\prod_{p \leq x} < 4^x, \quad x \geq 2. \tag{10}$$

**Доказательство** 1. Докажем утверждение для целых $x$.

Воспользуемся индукцией. При $x = 2$, $x = 3$ – верно (проверяется подстановкой).

Предположим теперь, что у нас есть $x > 3$. Для всех целых чисел $n < x$ предположим, что утверждение (10) верно.

а) $x = 2n$. Тогда

$$\prod_{p \leq 2m} p = \prod_{p \leq 2m-1} p < 4^{2m-1} < 4^{2m} = 4^x.$$

Здесь воспользовались тем, что $2m$ – составное число, а значит, в произведение не входит.

б) $x = 2m - 1$. Запишем

$$\prod_{p \leq 2m-1} = \prod_{p \leq m} \cdot \prod_{m < p \leq 2m-1} p \leq$$

Воспользуемся тем, что все $m < p \leq 2m-1$ делят числитель и не делят знаменатель биномиального коэффициента $C_{2m-1}^m$, т.е.

$$C_{2m-1}^m = \frac{(2m-1)!}{m!(m-1)!} > \prod_{m < p \leq 2m-1} p.$$

Тогда

$$\prod_{p \leq 2m-1} \leq 4^m \cdot C_{2m-1}^m.$$

Покажем, что

$$C_{2m-1}^m < 4^{m-1}.$$

Разложим

$$(1+x)^{2m-1} = 1 + C_{2m-1}^1 x + C_{2m-1}^2 x^2 + \cdots +$$
$$+C_{2m-1}^{m-1} x^{m-1} + C_{2m-1}^m x^m + \cdots + C_{2m-1}^{2m-2} x^{2m-2} + x^{2m-1}.$$

При $x = 1$

$$2^{2m-1} > C_{2m-1}^m + C_{2m-1}^{m-1} = 2\frac{(2m-1)!}{(m-1)!m!},$$
$$C_{2m-1}^m < 2^{2m-2} = 4^{m-1},$$

что и требовалось доказать.

2. Выберем $x \geq 2$ – произвольное действительное число. Тогда

$$\prod_{p \leq x} p = \prod_{p \leq [x]} p \leq 4^{[x]} < 4^x.$$

Лемма доказана.

Докажем теперь оценку сверху теоремы Чебышева.

**Доказательство** (верхней границы)
Представим

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{p \leq x^{2/3}} 1 + \sum_{x^{2/3} < p \leq x} 1. \tag{11}$$

Так как на прошлой лекции показали, что

$$\pi(N) \leq \frac{2}{3}N,$$

для первой суммы получим

$$\sum_{p \leq x^{2/3}} 1 = \pi(x^{2/3}) = \pi([x^{2/3}]) \leq \frac{2}{3}[x^{2/3}] \leq \frac{2}{3}x^{2/3}.$$

Для второй суммы запишем

$$\sum_{x^{2/3} < p \leq x} 1 < \sum_{x^{2/3} < p \leq x} \frac{\log_2 p}{\log_2 x^{2/3}} \leq \sum_{2 \leq p \leq x} \frac{\log_2 p}{\log_2 x^{2/3}} = \frac{1}{\log_2 x^{2/3}} \sum_{p \leq x} \log_2 p.$$

Логарифмируя (10), получим

$$\sum_{p \leq x} \log_2 p < 2x.$$

Тогда

$$\sum_{x^{2/3} < p \leq x} 1 < \frac{3}{2\log_2 x} 2x = \frac{3x}{\log_2 x}.$$

Возвращаясь к (11), получим

$$\pi(x) \leq \frac{2}{3}x^{2/3} + \frac{3x}{\log_2 x}. \tag{12}$$

Воспользуемся соотношением

$$2^n > 1 + n, n \geq 1,$$

которое можно получить с помощью биномиальных коэффицентов:

$$2^n = (1+1)^n = 1 + C_n^1 + C_n^2 + \cdots + C_n^n \leq 1 + C_n^1 = 1 + n$$

или по индукции.

Тогда для любого $x$

$$2^x \geq 2^{[x]} \leq 1 + [x] > x,$$

$$x \geq \log_2 x.$$

Запишем также, что

$$x^{1/3} \geq \log_2 x^{1/3} = \frac{1}{3}\log_2 x.$$

Тогда

$$x \geq \frac{1}{3}x^{2/3}\log_2 x,$$

$$\frac{3x}{\log_2 x} \geq x^{2/3}.$$

Вернемся к (12). Получим

$$\pi(x) \leq \frac{2}{3}\frac{3x}{\log_2 x} + \frac{3x}{\log_2 x} = \frac{5x}{\log_2 x}.$$

Теорема доказана.

# Глава 3. Арифметические функции

**Определение 4.1.** *Арифметической функцией* называется

$$f : \mathbb{N} \to \mathbb{C}.$$

Арифметическая функция может принимать, например, целые или действительные значения, но в общем случае ее значения комплексные.

## §1 Мультипликативные функции

**Определение 4.2.** Функция $\theta(n)$ называется *мультипликативной*, если $\theta(n) \not\equiv 0$ и для любых взаимно простых чисел $a$ и $b$

$$\theta(ab) = \theta(a)\theta(b).$$

**Пример** Если $s \in \mathbb{C}$ [18], функция

$$\theta(n) = n^s$$

[18]Это условие включает, конечно, целые и действительные значения параметра $s$.

является мультипликативной, т.к. для любых (не только взаимно простых) $a$ и $b$

$$\theta(ab) = (ab)^s = a^s b^s = \theta(a)\theta(b).$$

**Свойства мультипликативных функций**

1. $\theta(1) = 1$.

Так как $\theta(n) \not\equiv 0$,

$$\exists\, a \in \mathbb{N}, \quad \theta(a) \neq 0.$$

Тогда

$$\theta(a) = \theta(a \cdot 1) = \theta(a)\theta(1).$$

Разделив обе части на $\theta(a)$, получим

$$\theta(1) = 1.$$

2. Если $n = p_1^{k_1} \dots p_r^{k_r}$ [19], то

$$\theta(n) = \theta\left(p_1^{k_1}\right) \dots \theta\left(p_r^{k_r}\right).$$

Это свойство следует из того, что, так как $p_i$ – взаимно простые, то $p_i^{k_i}$ тоже будут взаимно простыми. [20]

3. Достаточно определить $\theta(n)$ на степенях простых $p^k, \quad k \geq 1$.

[19] Имеетс в виду произведение простых чисел.

[20] Важно помнить, что, например,

$$\theta(p^2) \neq \theta(p)\theta(p).$$

В некоторых случаях, например, когда $\theta(n) = n^s$, это может выполняться, но из определения мультипликативной функции это не следует.

# Лекция 5

## Мультипликативные функции (продолжение)

**Лемма 5.1.** *Пусть $\theta(n)$ – мультипликативная функция, а*

$$f(n) = \sum_{d|n} \theta(d).$$

*Тогда $f(n)$ – мультипликативная и*

$$f(n) = \prod_{p|n} \left(1 + \theta(p) + \theta(p^2) + \cdots + \theta\left(p^{\nu_p(n)}\right)\right). \tag{13}$$

**Доказательство** 1. Мультипликативность $f(n)$. Допустим, у нас есть $a, b \in \mathbb{N}$, $(a, b) = 1$.

По определению,

$$f(ab) = \sum_{d|ab} \theta(d)$$

Допустим, что можем записать

$$d = d_1 d_2, \quad d_1|a, \quad d_2|b.$$

Раньше говорили, что

$$d = \prod_{p|ab} p^{\nu_p(d)} = \prod_{p|a} p^{\nu_p(d)} \cdot \prod_{p|b} p^{\nu_p(d)}.$$

Убедимся, что первый множитель это $d_1$, а второй – $d_2$. Для каждого $d$ из $\prod_{p|a} p^{\nu_p(d)}$ выполняется $\nu_p(d) \leq \nu_p(ab) = \nu_p(a) + \nu_p(b) = \nu_p(a) + 0$, значит, $d_1|a$. Аналогично можно убедиться, что $d_2|b$. Это значит, что можем записать

$$f(ab) = \sum_{d_1|a} \sum_{d_2|b} \theta(d_1 d_2) =$$

$$= \sum_{d_1|a} \sum_{d_2|b} \theta(d_1)\theta(d_2) = \left(\sum_{d_1|a} \theta(d_1)\right)\left(\sum_{d_2|b} \theta(d_2)\right) = f(a)f(b).$$

Теперь докажем (13). Число $n$ представимо в виде

$$n = p_1^{r_1} \dots p_r^{k_r}.$$

Поскольку уже доказали, что $f(n)$ – мультипликативная,

$$f(n) = f(p_1^{r_1}) \dots f(p_r^{k_r}).$$

По определению,

$$f(p^k) = \sum_{d|p^k} \theta(d).$$

Делителями $p^k$ будут являться числа

$$1,\ p,\ p^2,\ \dots\ ,\ p^k.$$

Значит,

$$f(p^k) = 1 + \theta(p) + \theta(p^2) + \cdots + \theta(p^k).$$

Для всех простых $p$ формулы такого вида перемножим и получим (13).

Теорема доказана.

## §2 Функция Мёбиуса

Для простых чисел *функция Мёбиуса* определяется следующим образом

$$\left[\begin{array}{c} \mu(1) = 1, \\ \mu(p) = -1, \\ \mu(p^k) = 0,\ \text{если } k \geq 2. \end{array}\right. \tag{14}$$

Определим теперь эту функцию для всех натуральных. Пусть

$$n = p_1^{k_1} \dots p_r^{k_r}, \quad \exists\, k_i \geq 2.$$

Тогда по мультипликативности

$$\mu(n) = \mu(p_1^{k_1}) \dots \mu(p_r^{k_r}),$$

и $\mu(p_i)^{k_i} = 0$. Если же все степени первые, т.е.

$$n = p_1 \dots p_r,$$

и $\mu(p_i) = -1$. Тогда

$$\mu(p_1 \dots p_r) = (-1)^r.$$

Таким образом, общее определение будет выглядеть так:

$$\left[\begin{array}{ccc} \mu(1) & = & 1, \\ \mu(p_1 \dots p_r) & = & (-1)^r, \\ \mu(n) & = & 0,\ \text{если } \exists\, p:\ p^2 | n. \end{array}\right. \tag{15}$$

**Следствие 1**

$$\sum_{d|n} \mu(d) = \begin{cases} 1,\ \text{если } n = 1, \\ 0,\ \text{иначе.} \end{cases}$$

**Доказательство** Воспользуемся утверждением леммы 5.1. В данном случе

$$\theta(n) = \mu(n).$$

Возьмем какое-нибудь простое $p$ и сосчитаем

$$1 + \mu(p) + \mu(p^2) + \cdots + \mu(p^\nu) = 1 + (-1) + 0 + \cdots + 0 = 0.$$

**Следствие 2**

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{16}$$

**Доказательство** Аналогично доказательству леммы 1, положим

$$f(n) = \sum_{d|n} \frac{\mu(d)}{d}.$$

Так как $\mu(n)$ и $n$ – мультипликативные функции, $\nu(n)/n$ – тоже мультипликативная функция. Вычислим значения $f(n)$. В левой части

$$\sum_{d|1} \frac{\mu(d)}{d} = \frac{\mu(1)}{1} = 1.$$

При $n = 1$ значение правой части (16) будем пустым произведением. Договоримся, что в этом случае произведение равно 1. Вычислим теперь для простого $p$

$$1 + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^\nu)}{p^\nu} = 1 + \frac{-1}{p} + 0 + \cdots + 0 = 1 - \frac{1}{p}.$$

Так как по формуле (13) мы перемножаем выражения такого вида, убедились в справедливости (16).

**Теорема 5.1.** *(Формула обращения Мёбиуса) Пусть $f(n)$ и $g(n)$ – арифметические функции, связанные соотношением*

$$g(n) = \sum_{d|n} f(d).$$

*Тогда*

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right). \tag{17}$$

**Доказательство** При $n = 1$:

$$g(1) = f(1).$$

Вычислим теперь

$$\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left(\sum_{c\left|\frac{n}{d}\right.} f(c)\right) =$$

$$= \sum_{c,d:cd|n} \nu(d) f(c) = \sum_{c|n} f(c) \sum_{d\left|\frac{n}{c}\right.} \nu(d).$$

Чтобы понять, как поменялись пределы суммирования, рассмотрим рис. 5.1. Это не иллюстрация ситуации с нашими пределами суммирования, но более простой

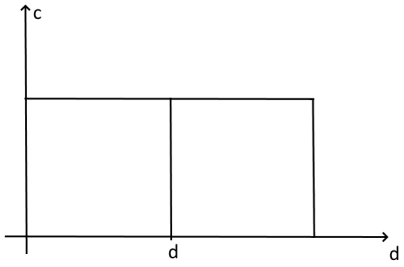


Рис. 5.1. Прямоугольная область суммирования

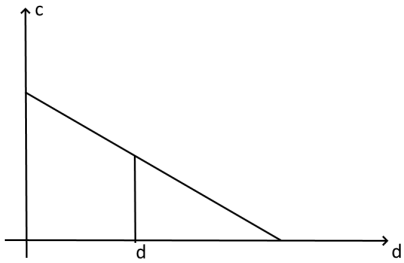


Рис. 5.2. Более сложная область суммирования

случай с таким же принципом. Имеем прямоугольную область, хотим провести суммирование для целых чисел из этой области. Поэтому для каждого $d$ можем провести суммирование для всех $c$ (рис. 5.1):

$$\sum_{c,d\in\mathbb{Z}} = \sum_{d}\sum_{c}.$$

Аналогично, если у нас не прямоугольная область, а, например, треугольная (рис. 5.2)

Все слагаемые внутренней суммы (по следствию 1) равны 0, кроме слагаемого при $c = n$. Это слагаемое равно 1.

Тогда

$$\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = f(n) \cdot 1 = f(n).$$

Теорема доказана.

## §3 Функция Эйлера

**Определение 5.1.** Функция Эйлера $\varphi(n)$[21] равна количеству натуральных чисел отрезка от 1 до $n$, взаимно простых с $n$, т.е. количеству $k$ таких, что

$$1 \leq k \leq n, \quad (k, n) = 1.$$

**Примеры**

$$\varphi(1) = 1,$$

$$\varphi(10) = 4 \text{ т.к. 1,3,7 и 9 взаимно простые с 10.}$$

$$\varphi(p) = p - 1, \quad p \text{ – простое.}$$

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1),$$

так как среди чисел

$$1, 2, 3, \ldots, p, \ldots, p^k = p^{k-1} \cdot p$$

ровно $p^{k-1}$ делящихся на $p$.

**Теорема 5.2.** *1.*

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right), \quad n \geq 1.$$

*2. Функция Эйлера $\varphi(n)$ мультипликативна, то есть*

$$\varphi(ab) = \varphi(a)\varphi(b), \quad (a, b) = 1.$$

**Пример** Например, убедимся, что

$$\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4.$$

Также можем вычислить как

$$\varphi(10) = 10 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4.$$

**Доказательство** Докажем сначала первую часть теоремы. Для $n \geq 2$

$$\varphi(n) = \sum_{k=1,(k,n)=1}^{n} 1.$$

Чтобы избавиться от условия суммирования, будем работать не с 1, а с функциями вида

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

[21]Это ее стандартное обозначение.

Тогда

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(k,n)} \mu(d) = \sum_{d|n} \sum_{l=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Во второй сумме воспользовались тем, что на $k$ накладывается условие $k \vdots d$. Это значит, что

$$k = d \cdot l, \quad 1 \leq dl \leq n, \quad \text{то есть } 1 \leq n/d.$$

Тогда

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

Первое утверждение доказано.

Утверждение о мультипликативности следует из первого пункта, так как $\varphi(n)$ представляется в виде двух мультипликативных функций.

Теорема доказана.

# Лекция 6

## Глава 4. Числовые сравнения

### §1 Сравнения и их основные свойства

**Определение 6.1.** Пусть $a, b \in \mathbb{Z}$ и $m \geq 2$. Говорят, что $a$ и $b$ *сравнимы по модулю* $m$, то есть

$$a \equiv b \pmod{m},$$

если $a - b$ делится на $m$.

**Свойства**

1. $a \equiv a \pmod{m}$.
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.
3. $a \equiv b, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Следует из того, что

$$a - c = (a - b) + (b - c)$$

и оба слагаемых делятся на $m$.

4. Если

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m},$$

то

$$a \pm c \equiv b \pm d \pmod{m},$$
$$ac \equiv bd \pmod{m}.$$

Докажем для произведения. Рассмотрим

$$ac - bd = c(a - b) + b(c - d) \vdots m.$$

4a. Если

$$a \equiv b, \quad c \equiv c \pmod{m},$$

то

$$ac \equiv bc \pmod{m}.$$

5. Если

$$ab \equiv ac \pmod{m}, \quad (a, m) = 1,$$

то

$$b \equiv c \pmod{m}.$$

Следует из того, что

$$m | ab - ac = a(b - c) \Rightarrow m | b - c.$$

6. Если

$$ab \equiv ac \pmod{am},$$

то

$$b \equiv c \pmod{m}.$$

Запишем

$$am | ab - ac = a(b - c),$$

тогда

$$m | b - c.$$

7. Если есть многочлен $P(x) \in \mathbb{Z}[x]$, $a \equiv b \pmod{m}$, то

$$P(a) \equiv P(b) \pmod{m}.$$

Пусть многочлен имеет вид

$$P(x) = u_d x^d + \cdots + u_1 x + u_0, \quad u_j \in \mathbb{Z}.$$

Очевидно, что

$$a^k \equiv b^k \pmod{m}, \quad k = 0, 1, \ldots, d.$$

Значит,

$$u_k a^k \equiv U_k b^k \pmod{m}.$$

Складывая для всех $k$, получим, что [22]

$$P(a) \equiv P(b) \pmod{m}.$$

Заметим, что для каждого числа $a$ справедливо

$$a = m \cdot q + r, \quad 0 \leq r < m.$$

Отсюда следует, что

$$a \equiv q \pmod{m},$$

то есть каждое число сравнимо со своим остатком от деления на $m$ (по модулю $m$). Тогда, если

$$b \equiv r \pmod{m},$$

[22]Можно было бы действовать и по-другому, заметив, что

$$P(b) - P(a) \vdots b - a.$$

получим, вычитая, что

$$a - b \equiv 0 \pmod{m},$$

то есть

$$a \equiv b \pmod{m}.$$

Так, получим, что все целые числа можно разбить на $m$ непересекающихся подмножеств сравнимых между собой чисел, называемых *классами вычетов*. Обозначим их как

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}. \tag{18}$$

Числа из двух разных подмножеств $\overline{k}$ и $\overline{l}$, $m > k > l \leq 0$ буду несравнимы, так как

$$0 < k - l < m \;\Rightarrow k \not\equiv l \pmod{m}.$$

**Определение 6.2.** Из каждого из классов (18) выберем по одному числу

$$x_0,\ x_1,\ \ldots,\ x_{m-1}.$$

Такая совокупность чисел называется *полной системой вычетов*.

Предположим, у нас есть $a$, $(a, m) = 1$, $a \in \overline{k}$. Тогда

$$b \in \overline{k} \;\Rightarrow\; (b, m) = 1.$$

Убедимся, что это действительно так. По условию,

$$a = m \cdot q_1 + k,$$

$$b = m \cdot q_2 + k.$$

Если $d|b$, $d|m$, $d > 1$, то $d|k$. Но тогда

$$d|m,\quad d|k \;\Rightarrow\; d|a.$$

Так как $(a, m) = 1$, то $d = 1$.

Вычислим, сколько у нас классов вычетов, взаимно простых с $m$. Из того, что обоговорили выше, следует, что должно выполняться условие

$$(k, m) = 1,\quad 0 \leq k \leq m - 1.$$

Таких классов ровно $\varphi(m)$ штук.[23]

**Определение 6.3.** *Приведенной системой вычетов* называется набор чисел

$$y_1,\ \ldots,\ y_{\varphi(m)},\quad (y_i, m) = 1,$$

взятых из классов, взаимно простых с моделуем $m$.

[23] По определению функции Эйлера.

Для того, чтобы найти полную систему классов, достаточно взять $m$ чисел таких, что

$$x_i \not\equiv x_j \pmod{m}.$$

Это *условие полной системы вычетов.*

Если у нас есть системы $\varphi(m)$ чисел таких, что

$$(y_i, m) = 1, \quad y_i \not\equiv y_j \pmod{m},$$

можно утверждать, что это приведенная система вычетов.

**Пример** Возьмем $m = 5$. Рассмотрим числа

$$-2, -1, 0, 1, 2.$$

Это будет полная система вычетов по $\mod 5$.

Числа

$$-2, -1, 1, 2$$

будут приведенной системой вычетов. Действительно, $\varphi(5) = 4$, числа попарно несравнимы и взаимно просты с 5.

Числа

$$1, 2, 4, 8$$

тоже будут приведенной системой вычетов по $\mod 5$.

**Лемма 6.1.** *Пусть $a$, $b$ – целые числа и $(a, m) = 1$.*

*1. Если $x$ пробегает полную систему вычетов, то $ax+b$ тоже пробегает полную систему вычетов.*

*2. Если $x$ пробегает приведенную систему вычетов, то $ax$ тоже пробегает приведенную систему вычетов.*

**Доказательство** 1. Пусть есть полная система чисел

$$x_1, \ldots, x_m$$

Тогда множество чисел

$$ax_i + b, \quad 1 \le i \le m$$

состоит из попарно несравнимых чисел. Предположим обратно, то есть, что

$$ax_i + b \equiv ax_j + b \pmod{m}.$$

Можем сократить на $b$, то есть

$$ax_i \equiv ax_j \pmod{m}.$$

Так как $(a, m) = 1$, можем сократить $a$ и получим

$$x_i \equiv x_j \pmod{m}.$$

Получили противоречие, так как все $x_i$ лежат в разных классах вычетов.

2. Пусть

$$y_1, \ldots, y_r, \quad r = \varphi(m)$$

– приведенная система вычетов.

Рассмотрим числа

$$ay_1, ay_2, \ldots, ay_r.$$

Так как

$$\begin{cases} (y_i, m) = 1, \\ (a, m) = 1. \end{cases} \Rightarrow (ay_i, m) = 1.$$

Кроме этого, все числа $ay_i$ попарно несравнимы, так как, если

$$ay_i \equiv ay_j \pmod{m},$$

то так как $(a, m) = 1$, можем сократить на $a$ и получим

$$y_i \equiv y_j \pmod{m}.$$

Пришли к противоречию.

Лемма доказана.

## §2 Теоремы Эйлера и Ферма

**Теорема 6.1.** *(Эйлер) Для любого целого числа $a$, $(a, m) = 1$, выполняется*

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

**Доказательство** Возьмем приведенную систему чисел

$$y_1, \ldots, y_r, \quad r = \varphi(m)$$

и рассмотрим систему

$$ay_1, ay_2, \ldots, ay_r.$$

По лемме 6.1 это тоже приведенная система вычетов. Значит, для каждого $y_i$ можем найти $ay_j$ такое, что

$$y_i \equiv ay_j \pmod{m}, \quad i = 1, \ldots, r.$$

Перемножим все числа из системы. Получим, что

$$y_1 \ldots y_r \equiv a^r y_{i_1} \ldots y_{i_r} \pmod{m}. \tag{19}$$

В правой части выражения (19) индексы $i_k$ могут быть перемешаны, но принимают все значения от 1 до $r$. Так как

$$(y_i, m) = 1, \quad i = 1, \ldots, r,$$

можем сократить обе части (19) и получим

$$1 \equiv a^r \pmod{m}.$$

Так как $\varphi(m) = r$, получили утверждение теоремы.

**Теорема 6.2.** *(Ферма) Если $p$ – простое число и $a$ – целое, не делящееся на $p$, то*

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Доказательство** Данная теорема представляет собой частный случай теоремы Эйлера. Действительно, если взять $m = p$,

$$\varphi(m) = p - 1, \quad (a, m) = 1, \quad p \nmid a.$$

**Следствие** Если $p$ – простое число и $a$ – целое, то

$$p | a^p - a.$$

**Доказательство** Можно разложить

$$a^p - a = a(a^p - 1).$$

Если $p \nmid a$, по теореме Ферма

$$p | (a^{p-1} - 1).$$

Если $p | a$, то $p$ делит первый сомножитель.

**Пример** (числа Кармайкла) Рассмотрим

$$m = 561 = 3 \cdot 11 \cdot 17.$$

Для любого $(a, m) = 1$

$$a^{560} \equiv 1 \pmod{561}.$$

Заметим, что

$$560 \vdots 2, \quad 560 \vdots 10, \quad 560 \vdots 16.$$

Тогда по теореме Ферма

$$a^2 \equiv 1 \pmod{3} \Rightarrow a^{560} \equiv 1 \pmod{3},$$

$$a^{10} \equiv 1 \pmod{11} \Rightarrow a^{560} \equiv 1 \pmod{11},$$

$$a^{16} \equiv 1 \pmod{17} \Rightarrow a^{560} \equiv 1 \pmod{17}.$$

Получается, что

$$a^{560} - 1 \vdots 3, 11, 17,$$

значит,

$$a^{560} 1 \vdots 3 \cdot 11 \cdot 17 = 561.$$

## §3 Теорема Вильсона

**Теорема 6.3.** *(Вильсона) Если $p$ – простое число, то*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

**Доказательство** Запишем

$$(p-1)! = \prod_{k=1}^{p-1} k = \prod_{k=2}^{p-1} k \equiv -\prod_{k=2}^{p-2} k \mod p. \tag{20}$$

Возьмем какое-нибудь число $2 \le a \le p-2$. Хотим подобрать число $x$ такое, что

$$a \cdot x \equiv 1 \pmod{p}.$$

Рассмотрим уравнение

$$ax + py = 1.$$

Заметим, что $(a, p) = 1$. Значит, уравнение разрешимо, т.е.

$$\exists\, c, \quad ac + py_0 = 1 \;\Rightarrow\; ac \equiv 1 \pmod{p}.$$

Можно считать $1 \le c \le p-1$. Если $c = 1$, получим, что

$$a \equiv 1 \pmod{p},$$

но $a \ge 2$. Получили противоречие.

Если $c = p-1$, то

$$c \equiv -1 \pmod{p} \;\Rightarrow\; a \equiv -1( \mod p),$$

что тоже неверно.

Значит, $2 \le c \le p-2$.

Если $c = a$, то

$$a^2 \equiv 1 \pmod{p} \;\Rightarrow\; p | a^2 - 1 = (a-1)(a+1),$$

что тоже невозможно.

Значит, $a \ne c$. Подходящее нам число $a$ единственно, так как в противном случае

$$\begin{cases} a_1 c \equiv 1 \pmod{p} \\ a_2 c \equiv 1 \pmod{p} \end{cases} \Rightarrow p | c(a_1 - a_2) \;\Rightarrow\; p | c.$$

Значит, все произведение (20) разбивается на пары чисел, сравнимые с 1, то есть

$$(p-1)! = -\prod_{k=2}^{p-2} k \pmod{p} \equiv -1 \pmod{p}.$$

Теорема доказана.

# Лекция 7

## Глава 5. Сравнения с одним неизвестным

Будем предполагать, что есть некий многочлен

$$f(x) \in \mathbb{Z}[x]$$

и число $m > 1$.

**Определение 7.1.** *Сравнением с одним неизвестным неизвестным* будем называть запись вида

$$f(x) \equiv 0 \pmod{m}.$$

Требуется найти все целые числа, которые удовлетворяют такому сравнению.

В отличие от уравнений, таких чисел будет много. Предположим, что два числа сравнимы, то есть

$$a \equiv b \pmod{m},$$

и первое удовлетворяет сравнению

$$f(a) \equiv 0 \pmod{m}.$$

Так как в этом случае

$$f(a) \equiv f(b) \pmod{m},$$

получим, что

$$f(b) \equiv 0 \pmod{m}.$$

То есть решением будет являться весь класс вычетов (возможно, несколько).[24]

**Определение 7.2.** *Количеством решений сравнения* называют количество классов вычетов по $\bmod m$, состоящих из чисел, удовлетворяющих этом сравнению.

**Пример** Рассмотрим сравнение

$$x^2 - 1 \equiv 0 \pmod{8}.$$

У нас есть 8 разных классов вычетов. Классы, содержащие четные числа, сравнению не удовлетворяют. Оставшиеся классы содержат числа

$$1,\ 3,\ 5,\ 7.$$

Подставив, убедимся, что для этих чисел сравнение верно. Таких классов 4, это

$$\overline{1},\ \overline{3},\ \overline{5},\ \overline{7}.$$

Значит, и количество решений эьтого сравнения равно 4.

[24] Иногда решением называют сами числа, иногда – классы вычетов.

## §1 Сравнения первой степени

Если у многочлена

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

старший коэффицент не сравним с 0, то есть

$$m \not| a_n,$$

говорят, что *степень сравнения равна* $n$.

**Пример** Сравнение

$$4x^2 + x + 7 \equiv 0 \pmod 2$$

равносильно сравнению

$$x + 7 \equiv 0 \pmod 2,$$

то есть это сравнение первой степени.

*Сравнение первой степени* имеет вид[25]

$$ax - b \equiv 0 \pmod m, \quad m \not| a. \tag{21}$$

Если для $x_0$ верно

$$ax_0 \equiv b \pmod m,$$

то есть

$$ax_0 - b \vdots m,$$

то $\exists\, y_0$ такое, что

$$ax_0 - b = my_0.$$

По-другому можем записать как

$$ax_0 - my_0 = b.$$

Здесь $(x_0, y_0)$ – решение уравнения

$$ax - my = b. \tag{22}$$

Таким образом, задача решения сравнения первой степени (21) сводится к решению линейного уравнения двух неизвестных (22). Если это уравнение неразрешимо, значит, сравнение тоже не имеет решений.

**Теорема 7.1.** *1. Сравнение*

$$ax \equiv b \pmod m$$

*разрешимо* $\iff (a, m)|b$.

*2. Количество решений этого сравнения равно* $(a, m)$.

[25]Конечно, можно переписать в виде

$$ax \equiv b \pmod m.$$

**Доказательство** 1. Из того, что говорили выше, следует, что сравнение

$$ax \equiv b \pmod{m}$$

разрешимо $\iff$ разрешимо уравнение

$$ax - my = b.$$

Уравнение разрешимо $\iff$ $(a, m)|b$. Таким образом, первое утверждение следует из теоремы для уравнений.

2. Если $(x_0, y_0)$ – решение уравнения (22), любое решение можно записать в виде

$$x = x_0 + \frac{m}{d}t, \quad d = (a, m),$$

$$y = y_0 + \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

Значит, все решения сравнения (21) имеют вид

$$x = x_0 + \frac{m}{d}t, \quad t \in \mathbb{Z}.$$

Эта формула означает, что множество решений составляет единственный класс вычетов

$$x \equiv x_0 \pmod{(m/d)}.$$

Но решения сравнения считаются по $\mod m$.

Возьмем значения

$$t = 0,\ 2,\ \ldots,\ d - 1.$$

Обозначим

$$x_k = x_0\frac{m}{d}k, \quad k = 0,\ 1,\ \ldots,\ d - 1. \tag{23}$$

Покажем, что эти числа лежат в различных классах вычетов по $\mod m$.

Предположим обратное. Допустим,

$$x_k \equiv x_l \pmod{m}, \quad 0 \leq l < k < d.$$

По-другому можно записать как

$$x_0 + \frac{m}{d}k \equiv x_0 + \frac{m}{d}l \pmod{m}.$$

Сократив, получим

$$mk \equiv ml \pmod{md},$$

$$k \equiv l \pmod{d}.$$

Значит, $d|k - l$. Получили противоречие.

Значит, числа лежат в разных классах. Запишем

$$t = k + d \cdot r, \quad r \in \mathbb{Z}.$$

Получим

$$x = x_0 + \frac{m}{d}(k + dr) = x_0 + \frac{m}{d}k + mr,$$

то есть

$$x \equiv x_k \pmod{m}.$$

Таким образом, мы определили $d$ классов вычетов по $\bmod m$, порожденных числами (23).

С одной стороны, существует $\geq d$ классов вычетов по $\bmod m$, состоящих из решений. С другой, показали, что каждое решение $x$ лежит в одном из $d$ классов. Значит, их ровно $d$.

Теорема доказана.

## §2 Китайская теорема об остатках

Предположим, у нас есть числа (модули)

$$m_1, \ldots, m_n, \quad m_i \geq 2$$

и остатки

$$a_1, \ldots, a_n.$$

Нужно найти все числа, которые при делении на модули дают заданные остатки, то есть числа $x$ такие, что

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \ldots \\ x \equiv a_n p \bmod m_n \end{cases}. \tag{24}$$

**Теорема 7.2.** *1. Если числа $m_1, \ldots, m_n$ попарно взаимно просты, то система сравнений (24) разрешима.*

*2. Обозначим*

$$M = m_1 \cdots_n, \quad M_i = M/m_i.$$

*Для каждой $i, 1 \leq i \leq n$ найдем число $b_i$ такое, что*

$$M_i \cdot b_i \equiv a_i \pmod{m_i}.^{26}$$

*Определим*

$$x_0 = M_1 b_1 + \cdots + M_n b_n.$$

*Множество решений системы совпадает с множеством чисел $x$ таких, что*

$$x \equiv x_0 \pmod{M}. \tag{25}$$

[26] Так как

$$(M_i, m_i) = (m_1 \ldots m_{i-1} m_{i+1} \ldots m_n, m_i) = 1,$$

такое сравнение разрешимо.

**Доказательство** Покажем, что каждое решение (25) удовлетворяет системе (24) и наоборот.

Возьмем какое-то число $x_1$ такое, что

$$x_1 \equiv x_0 = M_1 b_1 + \cdots + M_n b_n \pmod{M}.$$

Заметим, что

$$m_1 | M_2 = \frac{m_1 m_2 m_3 \dots m_n}{m_2}.$$

Это справедливо для всех

$$m_1 | M_i, \quad 2 \le i \le n.$$

Это означает, что

$$M_i b_i \equiv 0 \pmod{m_1}, \quad 2 \le i \le n.$$

Таким образом,

$$x_0 \equiv M_1 b_1 \pmod{m_1} \equiv a_1 \mod m_1,$$

так как выбирали числа $b_i$ так, чтобы последнее сравнение выполнялось.

Аналогично доказывается, что

$$x_0 \equiv a_i \mod m_i, \quad i = 1, \dots, n.$$

Заметим, что

$$x_1 - x_0 \vdots M \vdots m_i.$$

Значит,

$$x_1 \equiv x_0 \pmod{m_i} \equiv a_i \pmod{m_i}$$

для всех $i = 1, \dots, n$. Это означает, что $x_1$ – решение системы (24).

Докажем теперь в обратную сторону, то есть что решение системы (24) удовлетворяет (25).

Рассмотрим число $x_2$ такое, что

$$x_2 \equiv a_i \pmod{m_i}$$

для всех $i = 1, \dots, n$, то есть является решением системы (24).

Так как

$$x_0 \pmod{m_i}, \quad i = 1, \dots, n,$$

получим, что

$$x_2 \equiv x_0 \pmod{m_i}.$$

Это означает, что

$$x_2 - x_0 \vdots m_i.$$

Тогда

$$x_2 - x_0 \vdots m_1 \dots m_n = M,$$

то есть

$$x_2 \equiv x_0 \pmod{M}.$$

Теорема доказана.

Возьмем какое-то $x \in \mathbb{Z}$. Поставим в соответствие

$$x \leftrightarrow (a_1, \ldots, a_n),$$

где $a_i$ – остаток от деления $x$ на $m_i$, причем сохраняем условие

$$(m_i, m_j) = 1.$$

**Следствие** $x$ пробегает полную систему вычетов по $\mod M \iff$ при всех $i$ числа $a_i$ пробегают полные системы вычетов по модялми $m_i$.

# Лекция 8

## §4 Полиномиальные сравнения по простому модулю

Будем рассматривать $p$ – простое и многочлен

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Речь пойдет о решении сравнения

$$f(x) \equiv 0 \pmod{p}. \tag{26}$$

Другими словами, нужно найти все корни многочлена $f(x)$ по $\mod p$.

**Теорема 8.1.** *(Лагранж, 1768) Количество решений сравнения (26) не превосходит его степени.*

**Доказательство** Воспользуемся индукцией по $n$.

В случае, когда у нас сравнение первой степени,

$$ax \equiv b \pmod{m}, \quad m = p.$$

Количество решений равно $(a, p) = 1$, так как $p \nmid a$.

Перейдем к шагу индукции. Предположим, что для любого многочлена степени $< n$ утверждение справедливо.

Предположим, что $x_1$ – корень сравнения (26).

$$f(x) \equiv f(x) - f(x_1) = \sum_{k=0}^{n} a_k (x^k - x_1^k) =$$

$$= \sum_{k=1}^{n} a_k (x - x_1)(x^{k-1} + x^{k-2}x_1 + \cdots + x_1^{k-1}) = (x - x_1)g(x) \pmod{p}. \tag{27}$$

При этом получается, что

$$g(x) \in \mathbb{Z}[x],$$

а степень $g(x)$ будет $\leq n$.

Обозначим буквой $r$ количество решений сравнения (26). Решения сравнения обозначим[27]

$$x_1, x_2, \ldots, x_r, \quad x \equiv x_i \pmod{p}, i = 1, \ldots, r,$$

где $x_i \not\equiv x_j \pmod{p}$, то есть несравнимы.

Возьмем $x_i$, $i \geq 2$ и подставим в обе части выражения (27).

$$0 \pmod{p} = f(x_i) \equiv (x_i - x_1)g(x_i) \pmod{p}.$$

Значит, $p | (x_i - x_1)g(x_i)$. При этом $p \nmid x_i - x_1$. Получается,

$$p | g(x_i), \quad i = 2, \ldots, r.$$

[27]Значит, что решение $x$ лежит в одном из $r$ классов.

То есть числа $x_2, \ldots, x_r$ удовлетворяют сравнению

$$g(x) \equiv 0 \pmod{p}.$$

По индуктивному предположению получается, что

$$r - 1 \leq \deg g(x) = n - 1.$$

Значит, $r \leq n$.

Теорема доказана.

**Следствие 1.**[28]

$$x^p - x \equiv x(x-1)\ldots(x-p+1) \pmod{p}. \tag{28}$$

**Пример** Возьмем $p = 3$.

$$x^3 - x \equiv x(x-1)(x-2) = x(x^2 - 3x + 2) = x^3 - 3x^2 + 2x \pmod{3},$$

так как $3 \equiv 0 \pmod{3}$, а $2 \equiv -1 \pmod{3}$.

**Доказательство** Рассмотрим

$$f(x) = x^p - x - x(x-1)\ldots(x-p+1).$$

При этом $\deg f(x) \leq p - 1$.

Вычислим коэффицент при $x$:

$$-1 - (-1)^{p-1}(p+1)! = -\left(1 + (p-1)!\right).$$

Тут воспользовались тем, что $p > 2$ – простое, а значит, нечетное.

Значит, многочлен $f(x)$ отличен от тождественного 0.

Возьмем теперь некоторое $a \in \mathbb{Z}$ и вычислим

$$f(a) = a^p - a - a(a-1)\ldots(a-p+1).$$

Первая часть выражения, $a^p - a$, будет сравнимое с 0 по $\bmod p$. Множители второй части пробегают полную систему вычетов по $\bmod p$. Значит, среди них тоже есть какое-то число, сравнимое с 0. Получим, что

$$f(a) \equiv 0 \pmod{p}.$$

Значит, каждое $a$ – решение сравнения

$$f(x) \equiv 0 \pmod{p}.$$

Значит, количество решения равно $p$. Так как $\deg f(x) \leq p - 1$, получаем противоречие с теоремой (8.1).

[28] Имеется в виду, что, если раскрыть скобки, коэффициенты в левой и правой частях будут сравнимы.

Это значит, что соответствующие коэффиценты в левой и правой части (28) сравнимы по $\mod p$.

Следствие доказано.

**Следствие 2** Пусть $r(x)$ – остаток от деления многочлена $f(x)$ на $x^p - x$. Тогда сравнения

$$f(x) \equiv 0 \pmod p,$$
$$r(x) \equiv 0 \pmod p$$

равносильны.

**Доказательство** Представим $f(x)$ в виде

$$f(x) = (x^p - x) \cdot q(x) + r(x), \quad q(x), r(x) \in \mathbb{Z}[x] \tag{29}$$

Возьмем $a \in \mathbb{Z}$. Учитывая, что $a^p - a | p$, при подстановке в

$$f(a) \equiv r(a) \pmod p.$$

Это означает, что

$$f(a) \equiv 0 \pmod p \iff r(a) \equiv 0 \pmod p.$$

## §5 Полиномиальные сравнения по модулю, равному степени простого числа

Будем рассматривать сравнения

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0( \mod p^n), \quad p \nmid a_n.$$

**Алгоритм** (Подъем решений)

Предположим, мы знаем все решения[29] по $\mod p^n$:

$$x_1, x_2, \ldots, x_m.$$

Хотим найти все решения по $\mod p^{n+1}$.

Предположим, что $y_1$ – решение по $\mod p^{n+1}$. Тогда

$$f(y_1) \equiv 0 \pmod{p^{n+1}} \Rightarrow f(y_1) \equiv 0 \pmod{p^n} \Rightarrow y_1 \equiv x_i \pmod{p^n}.$$

Будем считать, что

$$y_1 \equiv x_1 \pmod{p^n}.$$

Это значит, что можно представить

$$y_1 = x_1 + p^n \cdot t, \quad t \in \mathbb{Z}.$$

1. Нам надо найти $t$ такие, что

$$f(x_1 + p^n t) \equiv 0 \pmod{p^{n+1}}.$$

[29] Имеются в виду представители всех классов решений.

Вычислим производную $f'(x)$

$$f'(x) = na_n x^{n-1} + (n-1)x_{n-1}x^{n-2} + \cdots + a_1.$$

Выполним преобразование

$$f(x+y) = \sum_{k=0}^{n} a_k (x+y)^k.$$

Запишем, отбросив степени $y$ старше первой:

$$(x+y)^k = x^k + kx^{k-1}y + \dots$$

С учетом этого запишем

$$f(x+y) = \sum_{k=0}^{n} a_k (x^k + kx^{k-1}y + \dots) = f(x) + y \cdot f'(x) + \dots$$

Получается, можем представить

$$f(x+y) = f(x) + y \cdot f'(x) + y^2 \cdot g(x,y), \quad g \in \mathbb{Z}[x,y].$$

Тогда

$$f(x_1 + p^n t) = f(x_1) + f'(x_1)p^n t + p^{2n}t^2 g(x_1, p^n t).$$

Все коэффициенты последнего слагаемого делятся на $p^{2n}$. Заметим, что

$$2n \geq n+1, \quad n \geq 1.$$

Значит, последнее слагаемое сравнимо с 0 по $\mod p^{n+1}$. Нам нужно, чтобы выполнялось

$$0 \equiv f(x_1) + f'(x_1)p^n t \pmod{p^{n+1}}. \tag{30}$$

Напомним, что

$$f(x_1) \equiv 0 \pmod{p^n}.$$

Сократим (30) на $p^n$. Получим

$$\frac{f(x_1}{p^n} + f'(x_1)t \equiv 0 \pmod{p}. \tag{31}$$

Можем взять любое $t$, удовлетворяющее сравнению (31), и с его помощью посчитать $y_1$.

Возможны три ситуации с (31).

1. $p \nmid f'(x_1)$. В этом случае $t$ находится единственным способом.
2. $p \mid f'(x_1), \quad p \nmid f(x_1)/p^n$. В этом случае решений нет.
3. $p \mid f'(x_1), \quad p \mid f(x_1)/p^n$. В этом случае годится любое $t$.

**Лемма 8.1.** *Если $a$ – целое число, удовлетворяющее условиям*

$$f(a) \equiv 0(\mod p), \quad f'(a) \not\equiv 0 \pmod p,$$

*то для любого $n$ существует единственное число $b$, удовлетворяющее условиям*

$$\begin{cases} f(b) \equiv 0 \pmod{p^{n+1}}, \\ b \equiv a \pmod p. \end{cases}$$

**Доказательство** (По индукции)
Предположим, что $\exists!\, x_1$ такое, что

$$\begin{cases} f(x_1) \equiv 0 \pmod{p^n}, \\ x_1 \equiv a \pmod p. \end{cases}$$

Тогда

$$f'(x_1) \equiv f'(a) \pmod p.$$

Значит, $f'(x_1) \not\equiv 0 \pmod p$.
Находили $y_1$ как

$$y_1 = x_1 + tp^n,$$

то

$$y_1 \equiv x_1 \equiv a \pmod p.$$

Тогда

$$f(y_1) \equiv 0 \pmod{p^{n+1}},$$
$$f'(y_1) \not\equiv 0 \pmod p.$$

То есть получили единственным способом условия

$$\begin{cases} f(y_1) \equiv 0 \pmod{p^{n+1}}, \\ xy_1 \equiv a \pmod p. \end{cases}$$

для следующего уровня.
Лемма доказана.

## §6 Решение сравнений по составному модулю $\neq p^n$

Имеем многочлен

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p^n.$$

Будем рассматривать сравнения

$$f(x) \equiv 0 \pmod M, \quad M = m_1 \dots m_n, \quad (m_i, m_j) = 1.$$

Когда рассматривали китайскую теорему об остатках, говорили, что $\exists$ взаимнооднозначное соответствие между остатками по модулю $M$ и наборами остатков по модулям $m_1, \dots, m_n$.

То есть, сопоставляем

$$x_0 \leftrightarrow (a_1, \ldots, a_n),$$

где

$$a_i \equiv x_0 \pmod{m_i}, \quad 0 \leq q_i < m_i.$$

Проговорим, что

$$f(x) \equiv 0 \pmod{M} \iff \begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ \ldots \\ f(x) \equiv 0 \pmod{m_n}. \end{cases}$$

Решим независимо друг от друга сравнения в правой части:

$$\left[ \begin{array}{rcl} f(a_1) & \equiv & 0 \pmod{m_1}, \quad 0 \leq a_1 < m_1, \\ & \ldots & \\ f(a_n) & \equiv & 0 \pmod{m_n}, \quad 0 \leq a_n < m_n. \end{array} \right. , \tag{32}$$

Нам нужно найти $x$ такое, что

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \ldots \\ x \equiv a_n \pmod{m_n}, \end{cases}$$

Так как

$$m_i = p_i^{k_i}, \quad p - \text{простое},$$

по китайской теореме об остатках по набор $(a_1, \ldots, a_n)$ можем сосчитать $x_0 \mod M$.

# Лекция 9

## Глава 6. Решение сравнений второй степени по простому модулю

Будем рассматривать сравнение

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad a, b, c \in \mathbb{Z}, \quad p \nmid a,$$

и $p$ – простое нечетное.

Домножив на $4a$, получим

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}.$$

Выделим полный квадрат

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}.$$

Здесь

$$D = b^2 - 4ac$$

дискриминант квадратного уравнения. Обозначим

$$2ax + b = y,$$

тогда можно записать

$$y^2 \equiv D \pmod{p}.$$

Это сравнение и сходно взаимно разрешимы или неразрешимы.

Таким образом, вопрос разрешимости сравнения второй степени сводится к вопросу о том, когда разрешимо простейшее сравнение вида

$$x^2 \equiv a \pmod{p}.$$

Разрешимо или нет такое сравнение, зависит от модуля.

**Пример** Рассмотрим сравнение

$$x^2 + 1 \equiv 0 \pmod{p}.$$

При $p = 3$ решений нет.

При $p = 5$ решения два:

$$x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{5}.$$

### §1 Символ Лежандра

*Символ Лежандра* – функция от целого аргумента $a$ и простого нечетного аргумента $p$, которая определяется следующим образом

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ если } x^2 \equiv a \pmod{p} \text{ разрешимо}, \\ 0, \text{ если } p \mid a, \\ -1, \text{ если } x^2 \equiv a \pmod{p} \text{ неразрешимо}. \end{cases} \tag{33}$$

**Определение 9.1.** Сравнение

$$x^2 \equiv a \pmod{p}$$

разрешимо и $p \nmid a \iff a$ – *квадратичный вычет.*

Сравнение

$$x^2 \equiv a \pmod{p}$$

не имеет решений $\iff a$ – *квадратичный невычет.*

Если

$$a_1 \equiv a_2 \pmod{p},$$

то они одновременно квадратичные вычеты или квадратичные невычеты.

**Лемма 9.1.** *Предполагаем далее, что* $p \nmid a$.

*1. Существует в точности* $(p-1)/2$ *квадратичных вычетов и* $(p-1)/2$ *квадратичных невычетов.*[30]

*2.* $a$ – *квадратичный вычет* $\iff a^{(p-1)/2} \equiv 1 \pmod{p}$.

$a$ – *квадратичный невычет* $\iff a^{(p-1)/2} \equiv -1 \pmod{p}$.

**Доказательство** Запишем

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 \tag{34}$$

– квадратичные вычеты. Действительно, сравнение

$$x^2 \equiv a^2 \pmod{p}$$

разрешимо,

$$x \equiv \pm a \pmod{p}.$$

Покажем, что все числа (34) лежат в разных классах вычетов. Возьмем числа

$$1 \le k < l < (p-1)/2.$$

Предположим, что они лежат в одном классе вычетов, то есть

$$k^2 \equiv l^2 \pmod{p}.$$

Получим, что

$$p | l^2 - k^= (l-k)(l+k).$$

Заметим, что

$$1 \le l - k < l < (p-1)/2,$$

$$1 \le l + k < (p-1)/2 + (p-1)/2 = p - 1.$$

Ни одно из $l-k$ и $l+k$ не может делиться на $p$.

[30] Имеется в виду, конечно, количество различных классов вычетов.

Получаем противоречие. Значит, все числа (34) лежат в разных классах вычетов по $\mod p$.

Пока что показали, что существует не меньше, чем $(p-1)/2$ классов вычетов. Осталось показать, что их в точности столько.

Пусть $b$ – квадратичный вычет, необязательно из классов (34). Сравнение

$$x^2 \equiv b \pmod{p}$$

разрешимо.

Обозначим решение через $x_0$. Тогда

$$x_0^2 \equiv b \pmod{p}.$$

Возведем сравнение в степень $(p-1)/2$. Получим

$$x_0^{p-1} \equiv b^{(p-1)/2} \pmod{p}.$$

Тогда $p \nmid b$ и $p \nmid x_0$. По малой теореме Ферма получим, что

$$x_0^{p-1} \equiv 1 \pmod{p}.$$

Значит, и

$$b^{(p-1)/2} \equiv 1 \pmod{p}.$$

То есть, можем сказать, что если $b$ – квадратичный вычет, то $b$ – корень

$$x^{(p-1)/2} - 1 \equiv 0 \pmod{p}.$$

Это сравнение имеет $\leq (p-1)/2$ решений.

Значит, $b$ лежит в одном из классов (34).

Так, доказали первую часть пункта 1 теоремы и первую часть пункта 2.

Рассмотри классы вычетов по $\mod p$

$$\overline{1}, \overline{2}, \ldots, \overline{p-1}.$$

Классов квадратичных вычетов ровно $(p-1)/2$. Это значит, что остальные классы состоят из квадратичных невычетов. Их

$$p - 1 - \frac{p-1}{2} = \frac{p-1}{2}.$$

Доказательство пункта 1 теоремы завершено.

Пусть теперь $a$ – квадратичный невычет. Справедливо

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Для него также будет выполнено

$$a^{(p-1)/2} \not\equiv 1 \pmod{p}.$$

Возьмем многочлен

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1).$$

Из свойств выше следует, что $a$ является корнем мнгочлена $x^{p-1} - 1$ и что $a$ не является корнем $(x^{(p-1)/2} - 1)$. Отсюда следует, что $a$ – корень $(x^{(p-1)/2} + 1)$.

Это означает, что

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

В другую сторону, если

$$p | a^{(p-1)/2} + 1,$$

то

$$p \nmid a^{(p-1)/2} - 1.$$

Значит, $a$ – квадратный невычет.

Лемма доказана.

**Лемма 9.2.** *1.*

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

*2. Если* $a = b \pmod{p}$*, то*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

*3.*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

*4.*

$$\left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

**Доказательство** Свойства 1 и 2 уже фактически доказали.

3. Пусть $p \nmid a$, $p \nmid b$ (иначе очевидно). Тогда по предыдущей лемме

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Это означает, что

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \vdots p,$$

тогда

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

4. Работаем с $\left(\frac{1}{p}\right)$. Для этого рассмотрим сравнение

$$x^2 \equiv 1 \pmod{p}.$$

Оно разрешимо,

$$x \equiv \pm 1 \pmod{p}.$$

Раз оно разрешимо,

$$\left(\frac{1}{p}\right) = 1.$$

Докажем теперь

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

По свойству 1

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

И левая, и права части равны $\pm 1$. Значит, их разность $\leq 2$. Так как эта разность $\vdots\, p$, имеем

$$\left(\frac{-1}{p}\right) - (-1)^{(p-1)/2} = 0.$$

Остановимся подробнее на пункте 4.

$$(-1)^{(p-1)/2} = \begin{cases} 1, \text{ если } p \equiv 1 \pmod 4, \\ -1, \text{ если } p \equiv 3 \pmod 4. \end{cases}$$

С другой стороны,

$$\left(\frac{-1}{p}\right) = 1 \iff x^2 + 1 \equiv 0 \pmod{p}$$

разрешимо (это и будет случай $p \equiv 1 \pmod p$), и

$$\left(\frac{-1}{p}\right) = -1 \iff x^2 + 1 \equiv 0 \pmod{p}$$

не имеет решений (случай $p \equiv 1 \pmod p$).

Лемма доказана.

## §2 Квадратичный закон взаимности

**Теорема 9.1.** *(Квадратичный закон взаимности) Пусть $p, q$ – различные простые нечетные числа. Тогда*

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Обсудим другую формулировку.

1. Если $p \equiv 1(\mod 4)$ или $q \equiv 1 \pmod 4$, то сравнения

$$x^2 \equiv q \pmod{p} \text{ и } x^2 \equiv p \pmod{q}$$

разрешимы или неразрешимы одновременно. [31]

2.Если $p \equiv 3 \pmod 4$ и $q \equiv 3 \pmod 4$, то разрешимость одного сравнения

$$x^2 \equiv q \pmod p \text{ и } x^2 \equiv p \pmod q$$

означает неразрешимость другого.

Для доказательства теоремы нам понадобится некоторое количество вспомогательных утверждений.

Пусть есть $a$, $p \nmid a$. Будем считать, что $0 < a < p$. Умножим $a$ на целое число и разделим с остатком

$$a \cdot k - p\left[\frac{ak}{p}\right] = r, \quad 1 \le k \le p-1, \quad 1 \le r \le p-1.$$

Запишем остаток в виде

$$r = \begin{cases} r_k, \text{ если } r: \ 1 \le r \le (p-1)/2, \\ p - r_k, \text{ если } r: \ (p+1)/2 \le r \le p-1. \end{cases}$$

Теперь можем записать

$$a \cdot k - p\left[\frac{ak}{p}\right] = r \equiv \epsilon_k r_k \pmod p,$$

где

$$\epsilon_k = \begin{cases} 1, \text{ если } 1 \le r \le (p-1)/2, \\ -1, \text{ если } r \ge (p+1)/2, \end{cases} \quad , \quad 1 \le r_k \le (p-1)/2.$$

**Лемма 9.3.** *(Гаусс)*

$$\left(\frac{a}{p}\right) = (-1)^t,$$

*где $t$ – количество отрицательных среди $\epsilon_k$.*

**Доказательство** Рассмотрим $k = 1, \ldots, (p-1)/2$. Для каждого $k$

$$ak \equiv \epsilon_k r_k( \mod p).$$

Перемножим все этим сравнения, получим

$$a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv \epsilon_1 \ldots \epsilon_{(p-1)/2} r_1 \ldots r_k (p-1)/2 \pmod p. \tag{35}$$

Докажем, что все $r_1, \ldots, r_{(p-1)/2}$ различны. Допустим, что для некоторых $l, k$

$$1 \le k < l < (p-1)/2 \ r_k = r_l.$$

[31] Если одно из чисел $p, q$ сравним с 1 по mod 4, это значит, что степень

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

четная, и, стало быть, символы Лежандра имеют одинаковый знак, то есть равны.

Тогда

$$r_k \equiv a \cdot k \cdot \epsilon_k,$$
$$r_l \equiv a \cdot l \cdot \epsilon_l.$$

Значит,

$$a \cdot k \cdot \epsilon_k \equiv a \cdot l \cdot \epsilon_l \pmod{p}.$$

Так как $a$ на $p$ не делится, можем сократить

$$k \cdot \epsilon_k \equiv l \cdot \epsilon_l \pmod{p}.$$

Разность этих чисел делится на $p$. Оценим эту разность сверху

$$|k \cdot \epsilon_k - l \cdot \epsilon_l| \leq (k + l) \leq p - 1.$$

Это означает, что

$$k \cdot \epsilon_k = l \cdot \epsilon_l,$$

получили противоречие.

Значит, числа $r_1, \ldots, r_{(p-1)/2}$ все различны и принимают все значения от 1 до $(p-1)/2$.

Сократим в (35) одинаковые части. Получим

$$a^{(p-1)/2} \equiv \epsilon_1 \ldots \epsilon_{(p-1)/2} \pmod{p} = (-1)^t \pmod{p}.$$

С другой стороны, по свойству 1 получается

$$\left(\frac{a}{p}\right) \equiv (-1)^t \pmod{p}.$$

Это возможно, только когда

$$\left(\frac{a}{p}\right) = (-1)^t.$$

Лемма доказана.

# Лекция 10

## Квадратичный закон взаимности (продолжение)

**Предложение**

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} =$$

$$= \begin{cases} 1, \text{ если } p \equiv \pm 1 \pmod 8, \\ -1, \text{ если } p \equiv \pm 3 \pmod 8. \end{cases} \tag{36}$$

В первой форме утверждение нам проще будет доказывать, а во второй – использовать.

Введем, как и в прошлой лекции, обозначение

$$a \cdot k - p\left[\frac{ak}{p}\right] = \begin{cases} r_k, \text{ если } r < p/2 \\ p - r_k, \text{ если } r > p/2 \end{cases} =$$

$$= \begin{cases} \epsilon_k r_k, & (\epsilon_k = 1) \\ p + \epsilon_k r_k, & (\epsilon_k = -1) \end{cases}, \tag{37}$$

причем

$$1 \le r_k \le (p-1)/2.$$

За $t$ в прошлой лекции обозначали количество отрицательных $\epsilon_k$. Обозначим

$$S = \sum_{k=1}^{(p-1)/2} \left[\frac{ak}{p}\right].$$

Сложим для всех $k$ между собой (37):

$$a\left(1 + 2 + \cdots + \frac{p-1}{2}\right) - pS = tp + \left(\epsilon_1 r_1 + \cdots + \epsilon_{(p-1)/2} r_{(p-1)/2}\right). \tag{38}$$

Чтобы выяснить честность $t$, перейдем от равенства (38) к сравнению по $\mod 2$.

Заметим, что для всех $l$ будет выполнено

$$\epsilon_l \equiv 1 \pmod 2.$$

В прошлый раз показали, что множества

$$\left\{r_1, r_2, \ldots, r_{(p-1)/2}\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Значит,

$$r_1 + r_2 + \cdots + r_{(p-1)/2} = 1 + 2 + \cdots + \frac{p-1}{2} = \frac{1 + (p-1)/2}{2}\frac{p-1}{2} = \frac{p^2-1}{8}.$$

Кроме того, $p$ – нечетное, тогда [32]

$$p \equiv -1 \pmod 2 \text{ и } p \equiv 1 \pmod 2.$$

Перепишем наконец (38) как сравнение:

$$a\frac{p^2-1}{8} + S \equiv t + \frac{p^2-1}{8} \pmod 2. \tag{39}$$

При $a = 2$ получаем

$$S = \sum_{k=1}^{(p-1)/2} \left[\frac{2k}{p}\right] = 0,$$

так как $2k \leq 2(p-1)/2 < p$. Тогда

$$\frac{p^2-1}{8} + 0 \equiv t \pmod 2.$$

Получается, что

$$\equiv \frac{p^2-1}{8} \pmod 2.$$

С учетом утверждения леммы (9.3) получаем, что первое равенство утверждения (**??**) верно.

Убедимся, что вторая часть тоже выполняется. Рассмотрим случай, когда

$$p \equiv \pm 1 \pmod 8.$$

Значит, можем записать

$$p = \pm 1 + 8l, \quad l \in \mathbb{Z}.$$

Вычислим

$$p^2 - 1 = \cancel{1} \pm 16l + 64l^2 - \cancel{1} = 8(\pm 2l + 8l^2).$$

Значит, $(p^2-1)/8$ будет честным числом и

$$(-1)^{(p-1)/2} = 1.$$

Аналогично, если

$$p \equiv \pm 3 \pmod 8.$$

Можем записать

$$p = \pm 3 + 8l, \quad l \in \mathbb{Z}.$$

Вычислим

$$p^2 - 1 = 9 \pm 48l + 64l^2 - 1 = 8(1 + \pm 6l + 8l^2).$$

Получается нечестное число и поэтому

$$(-1)^{(p-1)/2} = -1.$$

Для удобства продублируем теорему из прошлой лекции.

[32] Можем выбрать любой из двух вариантов, в зависимости от того, как нам удобно.

**Теорема 10.1.** *(Квадратичный закон взаимности) Пусть $p, q$ – различные простые нечетные числа. Тогда*

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{40}$$

**Доказательство**

Рассмотрим (39) при нечетных $a$. Получим

$$(a-1)\frac{p^2-1}{8} + S \equiv t \pmod 2,$$

то есть

$$t \equiv S( \mod 2).$$

Значит, в этом случае

$$\left(\frac{a}{p}\right) = (-1)^S.$$

Перейдем ко второй части доказательства.

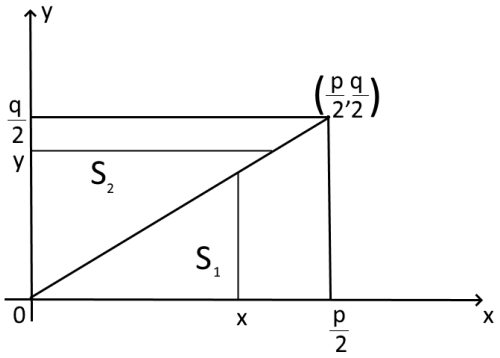


Рис. 10.1. Иллюстрация ко второй части доказательства

Отложим на координатных осях точки $p/2$ и $q/2$ соответственно (рис. **??**). Нарисуем прямоугольную область и проведем диагональ от $(p/2, q/2)$ к началу координат.

Уравнение этой прямой имеет вид

$$qx = py.$$

Нас будет интересовать количество целых точек в нижнем треугольнике $S_1$ и верхнем треугольнике $S_2$.

Заметим, что на диагонали прямоугольника нет целых точек.

Действительно, предположим, есть точка с целыми координатами $(v, u)$ на диагонали. Тогда будет верно

$$qu = pv, \quad u > 0, v > 0.$$

Получим, что

$$p|qu \Rightarrow p \,|\, u, 1 \leq u \leq \frac{p-1}{2}.$$

В этом промежутке нет ни одного целого числа, которое бы делилось на $p$. Получили противоречие.

Таким образом, $S_1 + S_2$ – количество целых точек внутри прямоугольника. Посчитаем количество целых точек в $S_1$. Будем перебирать координаты по условиям

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y < \frac{qx}{p}.$$

В этой области получим $\left[\frac{qx}{p}\right]$ – количество целых $x$ при фиксированном $y$. Значит,

$$S_1 = \sum_{x=1}^{(p-1)/2} \left[\frac{qx}{p}\right]$$

Теперь рассмотрим верхний треугольник $S_2$. Координаты меняются в пределах

$$1 \leq y \leq \frac{q-1}{2}, \quad 1 < \frac{py}{q}.$$

Здесь $\left[\frac{py}{q}\right]$ – количество целых $x$ при фиксированном $y$.

$$S_2 = \sum_{y=1}^{(q-1)/2} \left[\frac{py}{q}\right]$$

Но для таких сумм будет справедливо

$$\left(\frac{q}{p}\right) = (-1)^{S_1}$$

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{(q-1)/2}[pk/q]} = (-1)^{S_2}$$

Тогда

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1+S_2}$$

Так как $1 \leq x \leq (p-1)/2$, а $1 \leq y \leq (q-1)/2$, всего количество целых точек в прямоугольнике

$$S_1 + S_2 = \frac{p-1}{2}\frac{q-1}{2}.$$

Получим окончательно

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Теорема доказана.

**Пример** Дано сравнение

$$x^2 + 3 \equiv 0 \pmod{p}. \tag{41}$$

Найти все $p$, при которых оно разрешимо.

Мы знаем, что сравнение разрешимо тогда и только тогда, когда

$$\left(\frac{-3}{p}\right) = 1.$$

В силу мультипликативности

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right).$$

Помним, что

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

По квадратичному закону взаимности можем перевернуть $\left(\frac{3}{p}\right)$.

Отсеем сначала некоторые случаи. Для $p = 2$ и $p = 3$ сравнение (41) разрешимо.

Теперь рассмотрим $p > 3$. Можем записать

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}}.$$

Это выражение отличается от (40) тем, что символ Лежандра $\left(\frac{p}{3}\right)$ стоит в правой части формулы.

Так как символ Лежандра принимает два значения: 1 и $-1$, при делении на символ мы получим этот же символ.

Тогда

$$\left(\frac{-3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{(p-1)/2} = \left(\frac{p}{3}\right).$$

Таким образом, сравнение (41) разрешимо тогда и только тогда, когда

$$\left(\frac{p}{3}\right) = 1.$$

Так как $p > 3$ – простые , возможно два случая:

1. $p = 3k + 1 = 6l + 1$. [33]

В этом случае

$$\left(\frac{3k+1}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

2. $p = 3k - 1 = 6l - 1$.

В этом случае

$$\left(\frac{3k-1}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{(3-1)/2} = -1.$$

Таким образом, (41) разрешимо при

$$p = 2, \quad p = 3, \quad p = 6l + 1, \quad l \in \mathbb{N}.$$

[33] В случае, когда $k = 2l + 1$, $p$ – четное число и простым быть не может.

**Теорема 10.2.** *Сравнение*

$$ax^2 + bx + x \equiv 0 \pmod{p}, \quad a, b, c \in \mathbb{Z},$$

$(a, b, c) = 1, \quad a > 0$, *разрешимо для некоторых простых* $p \mid 2D$, *где* $D = b^2 - 4ac$, *а так же для всех простых, лежащих в некоторых арифметических прогрессиях по модулю* $4|D|$.

**Замечание** В примере выше

$$D = 0^2 - 4 \cdot 3 = -12, \quad 4|D| = 48 = 6 \cdot 8.$$

Значит, прогрессии могут быть такими:

$$48s + 1, \quad 48s + 7, \quad 48s + 13, \quad 48s + 19,$$

$$48s + 25, \quad 48s + 31, \quad 48s + 37, \quad 48s + 43.$$

# Лекция 11

## Множество решений сравнения второй степени

Продолжим обсуждать теорему, которую сформулировали в прошлый раз.

**Теорема 11.1.** *Множество решений сравнения*

$$ax^2 + bx + x \equiv 0 \pmod{p}, \quad a, b, c \in \mathbb{Z}, \quad p \nmid a, \tag{42}$$

$(a, b, c) = 1$, *состоит из некоторых простых делителей числа* $p \mid 2D$, *где*

$$D = b^2 - 4ac,$$

*и простых, лежащих в некоторых арифметических прогрессиях по модулю* $4|D|$.

**Доказательство** Рассмотрим $p \nmid 2D$.
Ранее показали, что сравнение (42) эквивалентно сравнению

$$x^2 \equiv D \pmod{p}.$$

Надо показать, что если два простых числа

$$p_1 \equiv p_2 \pmod{4|D|}, \tag{43}$$

то

$$\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right).$$

Разложим $D$ на множители

$$D = (-1)^{\alpha} 2^{\alpha_0} q_1^{\alpha_1} \dots q_r^{\alpha_r},$$

где все $q_i$ – простые.

Докажем последовательно, что если в символе Лежандра заменим $D$ на каждый из этих сомножителей, то символы будут одинаковы.

1. $p_1 \equiv p_2 \pmod{4}$, тогда

$$\frac{p_1 - 1}{2} \equiv \frac{p_2 - 1}{2} \pmod{2}.$$

Теперь рассмотрим

$$\left(\frac{-1}{p_1}\right) = (-1)^{(p_1-1)/2} = (-1)^{(p_2-1)/2} = \left(\frac{-1}{p_2}\right).$$

2. $\alpha_0 \geq 1$, тогда

$$p_1 \equiv p_2 \pmod{8}.$$

Тогда

$$\frac{p_1^2 - 1}{8} - \frac{p_2^2 - 1}{8} = \frac{p_1 - p_2}{8}(p_1 + p_2) \equiv 0 \pmod{2}.$$

Аналогично пункту 1 получим, что

$$\left(\frac{2}{p_1}\right) = (-1)^{(p_1^2-1)/8} = (-1)^{(p_2^2-1)/8} = \left(\frac{2}{p_2}\right).$$

3. Пусть $q$ – одно из чисел $q_i$. Заметим, что $p_1, p_2$ и $q$ – разные числа, так как $p_i$ не жедит дискриминант, а $q$ входит в его разложение.

Запишем

$$\left(\frac{q}{p_1}\right) = \left(\frac{p_1}{q}\right) \cdot (-1)^{\frac{p_1-1}{2}\frac{q-1}{2}}. \tag{44}$$

Аналогично

$$\left(\frac{q}{p_2}\right) = \left(\frac{p_2}{q}\right) \cdot (-1)^{\frac{p_2-1}{2}\frac{q-1}{2}}. \tag{45}$$

Убедимся, что у степеней $-1$ одинаковая четность. Рассмотрим

$$\frac{p_1-1}{2}\frac{q-1}{2} - \frac{p_2-1}{2}\frac{q-1}{2} = \frac{q-1}{2}\left(\frac{p_1-p_2}{2}\right) =$$

$$= \frac{p_1-p_2}{4}(q-1) \equiv 0 \pmod 2,$$

так как $q$ – нечетное.

Теперь,

$$p_1 \equiv p_2 \pmod q,$$

так как $q$ – делитель $D$. Тогда

$$\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right),$$

так как четность степеней одинакова.

Теперь разложим

$$\left(\frac{D}{p_1}\right) = \left(\frac{-1}{p_1}\right)^{\alpha}\left(\frac{2}{p_1}\right)^{\alpha_0}\left(\frac{q_1}{p_1}\right)^{\alpha_1}\dots\left(\frac{q_r}{p_1}\right)^{\alpha_r}.$$

$$\left(\frac{D}{p_2}\right) = \left(\frac{-1}{p_2}\right)^{\alpha}\left(\frac{2}{p_2}\right)^{\alpha_0}\left(\frac{q_1}{p_2}\right)^{\alpha_1}\dots\left(\frac{q_r}{p_2}\right)^{\alpha_r}.$$

По доказанному, все сомножители в правых частях одинаковы, а значит,

$$\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right).$$

Теорема доказана.

# Глава 7. Первообразные корни и индексы

Пусть $m \geq 2$ – целое. Если $a \in \mathbb{Z}$, $(a, m) = 1$, по теореме Эйлера

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

Для некоторых чисел такое сравнение может быть верно для степней, меньших $\varphi(m)$. Например,

$$a = 1 \Rightarrow 1^1 \equiv 1 \pmod{m},$$
$$a = -1 \Rightarrow (-1)^2 \equiv 1 \pmod{m}.$$

**Определение 11.1.** *Показателем числа $a$* по модулю $m$ называется наименьшее натуральное $d$ такое, что

$$a^d \equiv 1 \pmod{m}.$$

**Определение 11.2.** Числа, у которых показатель равен наиболшему значению $\varphi(m)$, называются *первообразными корнями.*

**Пример** Возьмем $m = 8$. У нас четыре класса взаимно простых с 8 чисел:

$$1, 3, 5, 7.$$

При этом любое число из этих классов (т.е. нечетное)

$$(2k+1)^2 = 4(k+1)k + 1 \equiv 1 \pmod{8}.$$

При этом $\varphi(8) = 4$. Поэтому первообразных корней по модулю 8 не существует.

Возьмем $m = 5$ и $a = 2$. $\varphi(5) = 4$,

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8 \equiv 3,\ 2^4 \equiv 9 \equiv 1 \pmod{5}.$$

Поэтому 2 – первообразный корень по модулю 5.

## Теорема Гаусса

**Лемма 11.1.** *Если $a$ – первообразный корень по модулю $m$, то числа*

$$1,\ a,\ a^2,\ \ldots,\ a^{\varphi(m)-1}$$

*образуют приведенную систему вычетов.*

**Доказательство** Предположим, у нас есть два числа $k$ и $l$ такие, что

$$a^l \equiv a^k \pmod{m}, \quad 0 \leq l < k \leq \varphi(m) - 1.$$

Так как $(a, m) = 1$, то $(a^l, m) = 1$. Разделив сравнение на $a^l$, получим

$$a^{k-l} \equiv 1 \pmod{m},$$

причем $1 \leq k - l \leq \varphi(m) - 1$. Таким образом, показатель $a$ меньше, чем $\varphi(m)$. Так как $a$ – первообразный корень (по условию), получили противоречие.

Лемма доказана.

Все классы вычетов, которые взаимно просты с модулем [34], образуют *группу обратимых элементов в кольце вычетов по модулю* $m$

$$(\mathbb{Z}/m\mathbb{Z})^* . \tag{46}$$

Первообразная и корень – образующие, существуют в случае, когда группа (46) циклическая.

Другими словами утверждение леммы можно сформулировать так.

Для любого $b$, $(b, m) = 1$, сравнение

$$a^x \equiv b \pmod{m}$$

разрешимо.

**Лемма 11.2.** *1.* $a^n \equiv 1 \pmod{m}, n \in \mathbb{N} \iff$ *$n$ делится на показатель $d$ числа $a$.*

*2. Если показатель $a$ равен $u$, а показатель $b$ равен*[35] *$v$, причем $(u, v) = 1$, то показатель $ab$ равен $uv$.*

*3. Если показатель $c$ равен $uv$, то показатель $c^u$ равен $v$.*

**Доказательство** 1. Предположим, что $n \vdots d$, то есть $n = dk$. Тогда

$$a^n = (a^d)^k \equiv 1 \pmod{m}.$$

Предположим теперь, что

$$a^n \equiv 1 \pmod{m}. \tag{47}$$

Знаем также, что

$$a^d \equiv 1 \pmod{m}.$$

Разделим с остатком

$$n = dk + r, \quad 0 \leq r < d.$$

Тогда

$$a^n = (a^d)^k a^r \equiv a^r \pmod{m}.$$

В силу (47) получим, что

$$a^r \equiv 1 \pmod{m}.$$

Так как $d$ – наименьшее такое натуральное, $r = 0$, то есть $d|n$.

2. Обозначим показатель $ab$ буквой $s$. Тогда

$$(ab)^s \equiv 1 \pmod{m}.$$

Возведем сравнение в степень $u$:

$$(ab)^s u = (a^u)^s b^{su} \equiv b^{su} \equiv 1 \pmod{m}.$$

[34] Их $\varphi(m)$ штук

[35] Оба числа взаимно просты с модулем.

Воспользуемся первым пунктом. Получим, что $v|su$, значит, $v|s$ (так как $v$ и $u$ взаимно просты).

Аналогично получим, что $u|s$. Значит, $uv|s$, тогда $s \geq uv$.

Возведем теперь

$$(ab)^{uv} = (a^u)^v (b^v)^u \equiv 1 \pmod{m},$$

так как каждое из чисел в скобках $\equiv 1$.

Отсюда получаем, что $s|uv$.

Окончательно получим, что $s = uv$.

3. Обозначим показатель $c^u$ буквой $t$. Тогда

$$(c^u)^t = c^{ut} \equiv 1 \pmod{m}.$$

По свойству 1 можно сказать, что $uv|ut$. Значит, $v|t$. С другой стороны, по условию

$$(c^u)^v = c^{uv} \equiv 1 \pmod{m}.$$

Значит, $t|v$.

Окончательно получаем, что $t = v$.

Лемма доказана.

**Теорема 11.2.** *(Гаусс, 1801) Для каждого простого нечетного числа $p$ существует первообразные корни. Их количество равно $\varphi(p-1)$.*

**Доказательство** (Конструктивное) Построим корень с помощью свойств из леммы 11.2.

Рассмотрим все числа

$$1 \leq a \leq p-1.$$

Все они будут взаимно просты с $p$. Для каждого из $a$ можно определить показатель. Возьмем

$$d = \text{НОК}_{1 \leq a \leq p-1}(\text{показателей } a).$$

Разложим $d$ на множители

$$d = q_1^{r_1} \dots d_s^{r_s}.$$

$\exists\, a_1$ такое, что показатель $a_1$ равен $q_{11}^r \cdot v_1$. Аналогично для всех $i = 1, \dots, s$. Например, при $i = s$ $\exists\, a_s$ такое, что показатель $a_s$ равен $q_{s\,s}^r \cdot v_s$.

Из свойства 3 леммы 11.2 показатель числа $a_1^{v_1}$ равен $q_1^{r_1}, \dots,$ показатель $a_s^{v_s}$ равен $q_s^{r_s}$.

Перемножим все эти числа:

$$g = a_1^{v_1} \dots a_s^{r_s}.$$

Из свойства 2 следует, что показатель $g$ равен

$$q_1^{r_1} \dots q_s^{r_s} = d.$$

Покажем теперь, что $d = p - 1$.

Для любого $a$ $a \mid d$. Тогда

$$a^d \equiv 1 \pmod{p}.$$

По-другому можно сказать, что сравнению

$$x^d - 1 \equiv 0 \pmod{p}$$

удовлетворяют $p-1$ чисел

$$1 \leq a \leq p-1.$$

По теореме Лагранжа, $p - 1 \leq d$. По малой теореме Ферма

$$g^{p-1} \equiv 1 \pmod{p}.$$

$$g^d \equiv 1 \pmod{p}.$$

Тогда, согласно свойству 1, $d \mid p-1$.

Получаем, что $d = p - 1$. Значит, $g$ – первообразный корень по модулю $p$.

Обозначим

$$a \equiv g^k(\mod p), \quad 1 \leq k \leq p-2, \quad (k, p-1) = 1. \tag{48}$$

Количество $k$ равно $\varphi(p-1)$. Покажем, что $a$ – первообразный корень.

Обозначим теперь $d$ – показатель $a$. Тогда

$$1 \equiv a^d \equiv g^{dk} \pmod{p}.$$

Так как показатель $g$ равен $p-1$, можем утверждать, что

$$p - 1 | kd.$$

Так как $(p-1, k) = 1$,

$$p - 1 | d.$$

Тогда $d \geq p-1$, но по малой теореме Ферма $d \leq p-1$, так как

$$a^{p-1} \equiv 1 \pmod{p}.$$

Значит, $d = p - 1$.

Тогда $a$ в (48) – первообразный корень.

Докажем, что первообразных корней в точности $\varphi(p-1)$. Пусть $b$ – первообразный корень. По лемме 11.1 $\exists\, k$ такое, чт

$$b \equiv g^k \pmod{p}, \quad 1 \leq k \leq p-2.$$

Предположим, что $(k, p-1) = v$. Тогда

$$b^{(p-1)/v} \equiv g^{(p-1)k/v} = \left(g^{p-1}\right)^{k/v} \equiv 1 \pmod{p}.$$

Тогда

$$\frac{p-1}{v} \geq p-1,$$

а значит, $v \leq 1$. Тогда $v = 1$ и $(k, p-1) = 1$.

Теорема доказана.

# Лекция 12

## Свойства индексов

В прошлый раз говорили про первообразные корни и доказали, что для любого простого $p$ найдется такое $g \nmid p$, что степень $p-1$ наименьшая, для которой верно

$$g^{p-1} \equiv 1 \pmod{p}.$$

По-другому можно сказать так. Для любого $a$, $1 \le a < p$ $\exists! x$ такое, что

$$a \equiv g^x \pmod{p}, \quad 0 \le x \le p-2.$$

Это число $x$ называется *индексом*. Обозначение $x = \mathsf{ind}_g a$. [36]

**Свойства индексов**

1. $g^{\mathsf{ind}_g a} \equiv a \pmod{p}$.
2. Если $a$ и $b$ не делятся на $p$,

$$\mathsf{ind}_g(ab) \equiv \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{p-1}.$$

3. Если $a, b$ – первообразные корни по $\mod p$, и $c \nmid p$ – целое число, то

$$\mathsf{ind}_b c = \mathsf{ind}_b a \cdot \mathsf{ind}_a c \pmod{p-1}.$$

**Доказательство** 1. Следует из определения.

2. Запишем сравнение

$$ab \equiv g^{\mathsf{ind}_g ab} \equiv g^{\mathsf{ind}_g a} \cdot g^{\mathsf{ind}_g b} = g^{\mathsf{ind}_g a + \mathsf{ind}_g b} \pmod{p}.$$

Из свойств первообразных корней это возможно, если

$$\mathsf{ind}_g ab \equiv \mathsf{ind}_g a + \mathsf{ind}_g b \pmod{p-1}.$$

3. Возведем $b$ в степень

$$b^{\mathsf{ind}_b a \mathsf{ind}_a c} = \left(b^{\mathsf{ind}_b a}\right)^{\mathsf{ind}_a c} \equiv a^{\mathsf{ind}_a c} \equiv c \equiv b^{\mathsf{ind}_b c} \pmod{p-1}.$$

Это означает, что

$$\mathsf{ind}_b a \cdot \mathsf{ind}_a c = \mathsf{ind}_b c \pmod{p-1}.$$

Свойства доказаны.

Кроме простых чисел $p$, индексы можно определить для чисел вида

$$p^k, \quad 2p^k, \quad k \ge 1, \quad 2, \quad 4. \tag{49}$$

[36] Свойства индексов очень похожи на свойства логарифмов. Их иногда и называют *дискретными логарифмами*.

Для 8, например, индексов уже не существует.

Для всех $m$ вида (49) группа

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

циклическая. [37]

# Глава 8. Цепные дроби

## §1 Конечные цепные дроби

Предположим, есть

$$\alpha = \frac{a}{b}, \quad b \geq 1, \quad a, b \in \mathbb{Z}.$$

Разделив $a$ на $b$ с остатком, получим

$$a = b \cdot a_0 + r_0, \quad 0 < r_0 < b.$$

Теперь разделим $b$ на $r_0$:

$$b = r_0 \cdot a_1 + r_1, \quad 0 < r_1 < r_0,$$

$$\cdots\cdots\cdots$$

$$r_{n-2} = r_{n-1} \cdot a_n + r_n, \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_n \cdot a_{n+1}, \quad r_n = (a, b).$$

По-другому можем записать это так:

$$\frac{a}{b} = a_0 + \frac{1}{b/r_0},$$

$$\frac{b}{r_0} = a_1 + \frac{1}{r_0/r_1},$$

$$\cdots\cdots\cdots$$

$$\frac{r_{n-2}}{r_{n-1}} = a_n + \frac{1}{a_{n+1}}.$$

Подставляя нижние выражения в верхние, получим, что

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}} = [a_0; a_1, a_2, \ldots, a_n, a_{n+1}].$$

Такая цепочка называется *цепной дробью*. Ограничения на $a_i$:

$$a_0 \in \mathbb{Z}, \quad a_i \geq 1.$$

Заметим, что если $a_{n+1} \geq 2$, конец дроби можно переписать как

$$a_n + \frac{1}{(a_{n+1} - 1) + 1/1},$$

[37] Группа называется циклической, если она порождается одним элементом $g$, т.е. все ее элементы являются степенями $g$.

то есть "удлинить"цепную дробь. И наоборот, если $a_{n+1} = 1$, можем "укоротить"цепную дробь. [38]

Рассмотрим так называемую *функциональную* цепную дробь

$$[x_0; x_1, \ldots, x_n] = x_0 + \frac{1}{x_1 + \frac{1}{\ldots + \frac{1}{x_n}}}.$$

**Лемма 12.1.** *Определим последовательность многочленов*

$$P_{-1} = 1, \quad P_0 = x_0$$

$$Q_{-1} = 0, Q_0 = 1$$

*и при* $k \geq 1$

$$P_k(x_0, \ldots, x_k) = x_k \cdot P_{k-1} + P_{k-2}$$

$$Q_k(x_0, \ldots, x_k) = x_k \cdot Q_{k-1} + Q_{k-2}$$

*Тогда*

$$[x_0; x_1, \ldots, x_k] = \frac{P_k}{Q_k}.$$

**Доказательство** (По индукции) Рассмотрим

$$P_1 = x_1 P_0 + P_{-1} = x_1 x_0 + 1,$$

$$Q_1 = x_1 \cdot Q_0 + Q_{-1} = x_1.$$

Тогда

$$\frac{P_0}{Q_0} = \frac{x_0}{1} = x_0 = [x_0],$$

$$\frac{P_1}{Q_1} = \frac{x_1 x_0 + 1}{x_1} = x_0 + \frac{1}{x_1} = [x_0; x_1].$$

Многочлены $P_k, Q_k$ зависят от переменных $x_0, x_1, \ldots, x_k$.

Предположим, что для всех индексов от 1 до $k$ утверждение леммы верно. Хотим показать, что оно верно для $k + 1$.

Возьмем цепную дробь

$$[x_0; x_1, \ldots, x_{k+1}] = x_0 + \frac{1}{x_1 + \frac{1}{\ldots + \frac{1}{x_k + 1/x_{k+1}}}} = [x_0; x_1, \ldots, x_{k-1}, x_k + \frac{1}{x_{k+1}}] =$$

$$= \frac{(x_k + 1/x_{k+1})\, P_{k-2} + P_{k-2}}{(x_k + 1/x_{k+1})\, Q_{k-2} + Q_{k-2}} = \frac{P_k + 1/x_{k+1} P_{k-1}}{Q_k + 1/x_{k+1} Q_{k-1}} =$$

$$= \frac{x_{k+1} P_k + P_{k-1}}{x_{k+1} Q_k + q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}}.$$

Лемма доказана.

[38] Таким образом, для рациональных чисел представлений в виде цепной дроби всегда два.

**Следствие 1**

$$Q_nP_{n-1} - Q_{n-1}P_n = (-1)^n, \quad n \geq 0.$$

**Доказательство** При $n = 0$

$$Q_0P_{-1} - Q_{-1}P_0 = 1 \cdot 1 = (-1)^0.$$

Предположим, что для всех индексов, меньших $n \geq 0$ утверждение справедливо. Тогда

$$Q_nP_{n-1} - Q_{n-1}P_n = (x_{n+1}Q_n + Q_{n-1})\,P_{n-1} - Q_n\,(x_{n+1}P_n + P_{n-1}) =$$
$$= Q_{n-1}P_n - Q_nP_{n-1} = -\,(Q_nP_{n-1} - Q_{n-1}P_n) = (-1)^{n+1}.$$

Следствие доказано.

**Следствие 2**

$$Q_nP_{n-2} - Q_{n-2}P_n = (-1)^{n-1}x_n, \quad n \geq 1.$$

**Доказательство** Распишем

$$Q_nP_{n-2} - Q_{n-2}P_n = (x_nQ_{n-1} + Q_{n-2})\,P_{n-2} - Q_{n-2}\,(x_nP_{n-1} + P_{n-2}) =$$
$$= x_n\,(Q_{n-1}P_{n-2} - Q_{n-2}P_{n-1}) = x_n(-1)^{n-1}.$$

Здесь воспользовались утверждением следствия 1.

Следствие доказано.

## §2 Бесконечные цепные дроби

Будем рассматривать бесконечные последовательности

$$[a_0; a_1, a_2, \dots], \quad a_i \in \mathbb{Z}, a_i \geq 1, \quad i \geq 1.$$

**Лемма 12.2.** *Положим*

$$p_k = P_k(a_0, \dots, a_k), \quad q_k = Q_k(a_0, \dots, a_k),$$

*где $P_k, Q_k$ – многочленны из леммы 12.1. Получим две последовательности чисел*

$$p_{-1} = 1, \quad p_0 = a_0,$$
$$q_{-1} = 0, \quad q_0 = 1,$$
$$\begin{cases} p_k = a_kp_{k-1} + p_{k-2}, \\ q_k = a_kq_{k-1} + q_{k-2} \end{cases}, \quad k \geq 1.$$

*Тогда*

*1.* $(p_k, q_k) = 1$,

*2.*

$$q_np_{n-1} - q_{n-1}p_n = (-1)^n, \quad n \geq 0, \tag{50}$$

*3.*

$$q_np_{n-2} - q_{n-2}p_n = (-1)^{n-1}a_n, \quad n \geq 1, \tag{51}$$

*4. Последовательность $q_n$ монотонно возрастает.*

**Доказательство** Свойства 2, 3 следуют из следствий к лемме 12.1. В выражениях достаточно подставить вместо $x_i$ $a_i$.

Свойство 1 следует из свойства 2. Если у $p_k$, $q_k$ есть общий делитель, то он должен делить единицу, а значит, они взаимно просты.

Докажем свойство 4.

$$q_n = a_n q_{n-1} - q_{n-2}, \quad n \geq 1.$$

Обозначим

$$\lambda = \frac{1+\sqrt{5}}{2}.$$

Это число $1 < \lambda < 2$. Так как $2\lambda - 1 = \sqrt{5}$, то

$$\lambda^2 = \lambda + 1.$$

Докажем, что

$$q_n > \lambda^{n-1}, \quad q_n > q_{n-1}. \tag{52}$$

Так как по условию $a_n \geq 1$, можем записать

$$q_n \geq q_{n-1} + q_{n-2}.$$

Тогда

$$q_1 \geq q_0, \quad q_n \geq q_{n-1}.$$

Очевидно, что

$$q_0 > \lambda^{-1}.$$

$$q_1 \geq q_0 + q_1 \geq 1 = \lambda^0.$$

Теперь предположим, что для $n$ соотношение (52) верно. Тогда

$$q^{n+1} \geq q_n + q_{n-1} \geq \lambda^{n-1} + \lambda^{n-2} = \lambda^{n-2}(\lambda + 1) = \lambda^n.$$

Лемма доказана.

**Определение 12.1.** Соотношение

$$\frac{p_n}{q_n}$$

называется *подходящей дробью*. Числа $a_n$ называются *неполными частными*.

**Теорема 12.1.** *1. Последовательность четных подходящих дробей возрастает. Последовательность нечетных подходящих дробей убывает. При любом* $m \geq 0$

$$\frac{p_{2m}}{q_{2m}} < \frac{p_{2m+1}}{q_{2m+1}}.$$

*2.* $\exists$ *предел*

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha,$$

*где* $\alpha$ *– некоторое иррациональное число.*

*3.*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

# Лекция 13

## Доказательство теоремы о цепных дробях

Перейдем к доказательству теоремы 12.1.

**Доказательство** Для доказательства пункта 1 рассмотрим дробь

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{q_n p_{n-2} - q_{n-2} p_n}{q_n q_{n-2}}.$$

В числителе стоит выражение (51), поэтому можно написать

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}, \quad n \geq 1, \quad a_n \geq 1.$$

Возможны следующие случаи:

а) $n$ – четное. Тогда

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} < 0,$$

значит, последовательность возрастает.

б) $n$ – нечетное. Тогда

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} > 0,$$

последовательность убывает.

Рассмотрим теперь

$$\frac{p_{2m+1}}{q_{2m+1}} - \frac{p_{2m}}{q_{2m}} = \frac{q_{2m} p_{2m+1} - q_{2m+1} p_{2m}}{q_{2m+1} q_{2m}}.$$

Числитель этого выражения совпадает с (50). Получается,

$$\frac{p_{2m+1}}{q_{2m+1}} - \frac{p_{2m}}{q_{2m}} = -\frac{(-1)^{2m+1}}{q_{2m+1} q_{2m}} = \frac{1}{q_{2m+1} q_{2m}}. \tag{53}$$

Эта дробь положительная. Утверждение пункта 1 доказано.

Рассмотрим теперь отрезок

$$\left[\frac{p_{2m}}{q_{2m}}, \frac{p_{2m+1}}{q_{2m+1}}\right].$$

Так как левые концы возрастают, правые концы убывают, отрезки строго вложены друг в друга.

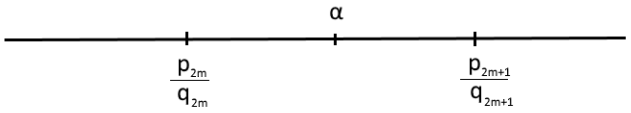


Рис. 13.1. Система отрезков.

Длины отрезков (равные (53)) стремятся к 0. Поэтому $\exists!\ \alpha$, принадлежащее всем этим отрезкам (рис. 13.1).

Получается, что если $n = 2m$,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{2m}q_{2m+1}} = \frac{1}{q_n q_{n+1}}.$$

Когда $n = 2m + 1$,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{2m+1}q_{2m+2}} = \frac{1}{q_n q_{n+1}}.$$

Осталось показать, что $\alpha$ – иррационально.

Предположим обратное. Если $\alpha \in \mathbb{Q}$, то

$$\alpha = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \geq 1.$$

Рассмотрим подходящую дробь $p_n/q_n$.

Расстояние

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{a}{b} - \frac{p_n}{q_n}\right| =$$

$$= \left|\frac{aq_n - bp_n}{bq_n}\right|.$$

Значит, $|aq_n - bp_n| > 0$, тогда $|aq_n - bp_n| \leq 1$. Значит,

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{bq_n}.$$

Так как только что доказали, что

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}},$$

получим, что

$$\frac{1}{q_n q_{n+1}} > \frac{1}{bq_n},$$

что означает, что

$$b > q_{n+1}.$$

Получается, последовательность знаменателей ограничена сверху. Получили противоречие. Значит, $\alpha$ – иррационально.

Теорема доказана.

## Теоремы о свойствах цепных дробей

**Теорема 13.1.** *При всех $n \geq 0$ справедливо неравенство*

$$|\alpha q_{n-1} - p_{n-1}| > |\alpha q_n - p_n| \tag{54}$$

*и равенство*

$$a_{n+1} = \left[ \frac{|\alpha q_{n-1} - p_{n-1}|}{|\alpha q_n - p_n|} \right]. \tag{55}$$

*Разные цепные дроби имеют разные значения.*[39]

**Доказательство** Запишем еще раз соотношения

$$p_{-1} = 1, \quad p_0 = a_0,$$

$$q_{-1} = 0, \quad q_0 = 1,$$

$$\begin{cases} p_{n+1} = a_{n+1}p_n + p_{n-1}, \\ q_{n+1} = a_{n+1}q_n + q_{n-1} \end{cases}, \quad n \geq 0.$$

Умножим нижнее соотношение на $\alpha$ и вычтем верхнее. Получим

$$\alpha q_{n+1} - p_{n+1} = a_{n+1} (\alpha q_n - p_n) + (q_{n-1}\alpha - p_{n-1}). \tag{56}$$

Вспомним, что из доказательства прошлой теоремы, если $n$ – четное, то

$$\frac{p_n}{q_n} < \alpha, \quad q_n\alpha - p_n > 0.$$

Если $n$ – отрицательно, то наоборот, $< 0$. Значит, можем записать

$$q_n\alpha - p_n = (-1)^n |q_n\alpha - p_n|.$$

Тогда (56) запишем как

$$(-1)^{n+1} |q_{n+1}\alpha - p_{n+1}| = (-1)^n a_{n+1} |q_n\alpha - p_n| + (-1)^{n-1} |q_{n-1}\alpha - p_{n-1}|.$$

Домножим на $(-1)^n$ и получим

$$0 < |q_{n+1}\alpha - p_{n+1}| = -a_{n+1} |q_n\alpha - p_n| + |q_{n-1}\alpha - p_{n-1}|.$$

Тогда

$$|q_{n-1}\alpha - p_{n-1}| > a_{n+1} |q_n\alpha - p_n| \geq |q_n\alpha - p_n|.$$

Получили первое утверждение теоремы.

[39] Значением бесконечной цепной дроби $[a_0; a_1, a_2, \dots]$ называют число

$$\alpha = \lim_{n\to\infty} p_n/q_n.$$

Запишем теперь

$$|q_{n+1}\alpha - p_{n+1}| + a_{n+1}\,|q_n\alpha - p_n| = |q_{n-1}\alpha - p_{n-1}|\,.$$

Разделим обе части на $|q_n\alpha - p_n|$:

$$\frac{1}{\frac{|q_n\alpha - p_n|}{|q_{n+1}\alpha - p_{n+1}|}} + a_{n+1} = \frac{|q_{n-1}\alpha - p_{n-1}|}{|q_n\alpha - p_n|}.$$

Обозначим для краткости

$$\alpha_{n+1} = \frac{|q_{n-1}\alpha - p_{n-1}|}{|q_n\alpha - p_n|}.$$

Тогда

$$\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}} < a_{n+1} + 1,$$

так как $\alpha_n > 1$.

С другой стороны,

$$\alpha_{n+1} > a_{n+1}.$$

Отсюда следует, что

$$a_{n+1} = [\alpha_{n+1}].$$

Рассмотрим (54) при $n = 0$.

$$q_{-1} = 0, \quad p_{-1} = 1.$$
$$1 > |\alpha q_0 - p_0| = |\alpha - a_0|\,.$$

Получается, что

$$a_0 < \alpha < a_0 + 1.$$

Нижняя оценка следует из того, что

$$\alpha = a_0 + \frac{1}{\alpha_1} > a_0.$$

Отсюда следует, что

$$a_0 = [\alpha]. \tag{57}$$

Осталось показать, что цепные дроби имеют разные значения. Предположим, что это не так. Тогда [40]

$$[a_0; a_1, a_2, \dots] = \alpha = [b_0; b_1, b_2, \dots].$$

Тогда из (57) следует, что

$$a_0 = b_0.$$

Пусть теперь $r$ – наименьшее такое, что

$$a_r \neq b_r.$$

[40] Обозначим дробь, отвечающую за дробь с $a_i$, $p_i/q_i$, а с $b_i$ – $p_i'/q_i'$.

Представим с помощью (55) при $n = r - 1$

$$a_r = \left[\frac{|\alpha q_{r-2} - p_{r-2}|}{|\alpha q_{r-1} - p_{r-1}|}\right]. \tag{58}$$

Так как $r = n + 1$, то $n, n - 1 < r$.

Это значит, что

$$a_i = b_i, \quad 1 \le i \le n.$$

$$q_i = a_i q_{i-1} + q_{i-2}.$$

$$p_{-1} = p'_{-1} = 1,$$

$$q_{-1} = q'_{-1} = 0,$$

$$p_0 = q_0 = b_0 = p'_0,$$

$$q_0 = 1 = q'_0.$$

Значит, в (58)

$$q_{n-1} = q'_{n-1}, \quad q_{n-2} = q'_{n-2}.$$

Отсюда $a_r = b_r$. Получили противоречие.

Теорема доказана.

**Теорема 13.2.** *Пусть $\alpha$ – действительное число. Положим*

$$\alpha_0 = \alpha, \quad a_0 = [\alpha_0].$$

*Определим*

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \quad k \ge 0.$$

*Тогда последовательность подходящих дробей $\frac{p_n}{q_n}$ к цепной дроби*

$$[a_0; a_1, a_2, \dots] \tag{59}$$

*удовлетворяет неравенству*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}. \tag{60}$$

*В частности,*

$$\frac{p_n}{q_n} \to \alpha$$

*и $\alpha$ – значение дроби (59).*

**Доказательство** Знаем, что $\alpha_0 = \alpha$ – иррациональное, $\alpha_0 \ne a_0$.

Теперь

$$\alpha_1 \frac{1}{\alpha_0 - a_0}.$$

Значит, $\alpha_1$ иррациональное, $\alpha_1 \ne a_1$.

Продолжая аналогичные рассуждения, получим, что все $\alpha_k$ – иррациональны, $\alpha_k \neq a_k$.

Разберемся теперь с неравенством (60). Запишем

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}.$$

Отсюда

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}.$$

Так, получим

$$\alpha_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\alpha_3}}} = [a_0; a_1, a_2, \dots, a_k, \alpha_{k+1}].$$

Это конечная цепная дробь, начальные элементы целые, последний – иррациональный.

Заметим, что $\alpha_{k+1} > 1$, так как

$$\alpha_k > 0, \quad a_k = [\alpha_k].$$

Значит,

$$a_1 \geq 1, \quad a_2 \geq 1, \dots a_k \geq 1.$$

Вспомним теперь функциональные цепные дроби. Для них

$$[x_0; x_1, \dots, x_k, x_{k+1}] = \frac{x_{k+1}P_k(x_0, \dots x_k) + P_{k-1}(x_0, \dots x_{k-1})}{x_{k+1}Q_k(x_0, \dots x_k) + Q_{k-1}(x_0, \dots x_{k-1})}.$$

Взяв вместо $x_i \to a_i$ и заменив $x_{k+1}$ на $\alpha_{k+1}$, получим

$$\alpha = \alpha_0 = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}.$$

Рассмотрим теперь

$$\alpha - \frac{p_k}{q_k} = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} =$$

$$= \frac{q_k p_{k-1} - q_{k-1}p_k}{q_k\left(\alpha_{k+1}q_k + q_{k-1}\right)} = \frac{(-1)^k}{q_k\left(\alpha_{k+1}q_k + q_{k-1}\right)}.$$

Тогда

$$\left|\alpha - \frac{p_k}{q_k}\right| = \frac{1}{q_k\left(\alpha_{k+1}q_k + q_{k-1}\right)} < \frac{1}{q_k\left(a_{k+1}q_k + q_{k-1}\right)} = \frac{1}{q_k q_{k+1}}.$$

При $n \to \infty$

$$\frac{p_n}{q_n} \to \alpha,$$

откуда следует, что

$$[a_0; a_1, a_2, \dots] = \alpha.$$

Теорема доказана.

# Лекция 14

## §3 Квадратичные иррациональности и периодические цепные дроби

Пусть $\alpha \in \mathbb{R} \setminus \mathbb{Q}$,

$$f(x) = ax^2 + bx + c, \quad a, b, c \in \mathbb{Z}, \quad a > 0, \quad f(\alpha) = 0. \tag{61}$$

$\alpha$ – *квадратичная иррациональность.*

Каждое иррациональное число раскладывается в бесконечную цепную дробь

$$\alpha = [a_0; a_1, a_2, \dots].$$

Цепная дробь *периодическая*, если

$$\exists\, n_0 \ \forall n \geq n_0 \ a_{n+m} = a_n,$$

то есть с шагом $m$ элементы цепной дроби начинают повторяться.

### Теорема Эйлера – Лагранжа

**Теорема 14.1.** *(Эйлера – Лагранжа) Цепная дробь $\alpha$ периодическая $\iff$ $\alpha$ – квадратичная иррациональность.*

**Доказательство**

$\Rightarrow$ Предположим, что $\alpha$ – периодическая, то есть

$$\alpha = [a_0; a_1, a_2, \dots, a_k, \overline{a_{k+1}, \dots, a_{k+m}}],$$

$$a_{k+m+1} = a_{k+1}, \dots$$

Известно, что можем разложить

$$\alpha = [a_0; a_1, a_2, \dots, a_k, \alpha_{k+1}],$$

где $\alpha_k$ – иррациональное. Для этой конечной цепи

$$\alpha = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} = \frac{\alpha_{k+m+1}p_{k+m} + p_{k+m-1}}{\alpha_{k+m+1}q_{k+m} + q_{k+m-1}}. \tag{62}$$

После преобразований получится уравнение вида

$$A_{k+1}\alpha_{k+1}^2 + B_{k+1}\alpha_{k+1} + C_{k+1} = 0, \tag{63}$$

$$A_{k+1} = q_{k+m}p_k - q_k p_{k+m},$$

остальные коэффициенты тоже можно выразить.

Предположим, что $A_{k+1} = 0$. Тогда

$$q_{k+m}p_k - q_k p_{k+m} = 0,$$

то есть

$$\frac{p_k}{q_k} = \frac{p_{k+m}}{q_{k+m}}.$$

Такого быть не может, так как говорили, что дроби с четными и нечетными номерами лежат по разные стороны от $\alpha$, последовательности с четными (нечетными) номерами строго возрастают (убывают). Получили противоречие.

Так, $A_{k+1} \neq 0$.

При этом $\alpha_{k+1} \notin \mathbb{Q}$. Можем выразить из левой части (62) $\alpha_{k+1}$ через $\alpha$ и подставить в (63). Получится квадратное уравнение с целыми коэффицентами.

$\Leftarrow$ Предположим, что $\alpha$ – квадратичная иррациональность.

Еще раз запишем выражение

$$\alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}. \tag{64}$$

Выразим коэффициенты уравнения

$$A_{n+1}\alpha_{n+1}^2 + B_{n+1}\alpha_{n+1} + C_{n+1} = 0. \tag{65}$$

Для этого подставим (64) в квадратное уравнение (61). Получим

$$a\left(\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}\right)^2 + b\left(\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}\right) + c = 0,$$

$$a\left(\alpha_{n+1}p_n + p_{n-1}\right)^2 + b\left(\alpha_{n+1}p_n + p_{n-1}\right)\left(\alpha_{n+1}q_n + q_{n-1}\right) +$$
$$+c\left(\alpha_{n+1}q_n + q_{n-1}\right)^2 = 0.$$

Найдем коэффициенты

$$A_{n+1} = ap_n^2 + bp_nq_n + cq_n^2,$$
$$C_{n+1} = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 = A_n,$$
$$B_n = 2ap_np_{n-1} + b\left(p_nq_{n-1} + p_{n-1}q_n\right) + 2cq_nq_{n-1}.$$

Воспользуемся тем, что

$$\left|\frac{p_n}{q_n} - \alpha\right| < \frac{1}{q_nq_{n+1}}.$$

Обозначим $p_n/q_n - \alpha = \delta_n$. Тогда

$$\frac{p_n}{q_n} = \alpha + \delta_n, \quad |\delta_n| < \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}.$$

Оценим коэффициенты. Для $A_{n+1}$ получается

$$|A_{n+1}| = q_n^2\left|a(\alpha+\delta_n)^2 + b(\alpha+\delta_n) + c\right| =$$
$$= q_n^2\left|a\alpha^2 + b\alpha + c + 2a\alpha\delta_n + a\delta_n^2 + b\delta_n\right| \leq 2|a||\alpha| + |a| + |b|.$$

Аналогично, так как $C_{n+1} = A_n$, получим

$$|C_{n+1} \leq 2|a||\alpha| + |a| + |b|.$$

Оценим $B_{n+1}$:

$$|B_{n+1}| = q_n q_{n+1} \left|2a\left(\alpha+\delta_n\right)\left(\alpha+\delta_{n-1}\right)+b\left(\alpha+\delta_n+\alpha+\delta_{n-1}\right)+2c\right| =$$

$$= \left|\delta_n 2a\alpha + \delta_{n-1}2a\alpha + 2a\delta_n\delta_{n-1} + b\delta_n + b\delta_{n-1}\right| q_n q_{n+1} \leq 2|a||\alpha| + 2|a||\alpha| + 2|a| + 2|b|.$$

Таким образом, значения коэффицентов $A_{n+1}, B_{n+1}, C_{n+1}$ ограничены константами, а значит, у нас конечное множество многочленов вида (65). Отсюда следует, что множество различных $\alpha_n$ тоже конечно, то есть числа $\alpha_n$ рано или поздно начнут повторяться.

Теорема доказана.

## §4 Свойство наилучшего приближения

Пусть $\alpha \in \mathbb{R}/\mathbb{Q}$, а дробь $p/q \in \mathbb{Q}$.

**Определение 14.1.** $p/q$ называется *наилучшим приближением к* $\alpha$, если система неравенств

$$\begin{cases} |x - y\alpha| \leq |p - q\alpha| \\ 1 \leq y \leq q \end{cases}$$

имеет единственное решение $x = p$, $y = q$.

**Теорема 14.2.** *Рациональное число $p/q$ есть наилучшее приближение к $\alpha \notin \mathbb{Q}$ $\iff$ $p/q$ есть подходящая дробь к $\alpha$.*

**Лемма 14.1.** *Пусть*

$$\frac{p_k}{q_k}, \quad \frac{p_{k+1}}{q_{k+1}}$$

*– соседние подходящие дроби к числу $\alpha$.*

*Тогда система неравенств*

$$\begin{cases} |x - y\alpha| \leq |p_k - \alpha q_k| \\ 1 \leq y \leq q_{k+1} \end{cases} \tag{66}$$

*только два решения:*

$$\begin{cases} x = p_k, \\ y = q_k, \end{cases} \quad u \quad \begin{cases} x = p_{k+1}, \\ y = q_{k+1}. \end{cases}$$

**Доказательство** Предположим, что $(x, y) \in \mathbb{Z}^2$, удовлетворяющие (66).

Рассмотрим уравнения

$$\begin{cases} x = up_k + vp_{k+1} \\ y = uq_k + vq_{k+1} \end{cases} \tag{67}$$

Определитель этой системы равен

$$p_k q_{k+1} - p_{k+1} q_k = \pm 1.$$

$u, v$ будут целыми числами.

1. $u = 0$. В этом случае

$$x = vp_{k+1}, \quad y = vq_{k+1} > 0.$$

Имеем

$$0 < vq_{k+1} \leq q_{k+1} \;\Rightarrow\; v = 1.$$

Тогда

$$x = p_{k+1}, \quad y = q_{k+1}.$$

2. $v = 0$. Тогда

$$x = up_k, \quad y = uq_k > 0.$$

Подставляя в первое неравенство, получим

$$|u||p_k - \alpha q_k| \leq |p_k - \alpha q_k| \;\Rightarrow\; |u| \leq 1.$$

Так как $y = uq_k \geq 1$, то $u = 1$. Тогда

$$x = p_k, \quad y = q_k.$$

3. $uv \neq 0$. Числа $u$ и $v$ будут иметь разные знаки, так как иначе бы

$$y = |uq_k + vq_{k+1}| \geq q_k + q_{k+1}$$

и получаем противоречие. Таким образом, $uv < 0$.

Запишем

$$|x - \alpha y| = |u(p_k - \alpha q_k) + v(p_{k+1} - \alpha q_{k+1})| =$$
$$= |u||p_k - \alpha q_k| + |v||p_{k+1} - \alpha q_{k+1}| > |p_k - \alpha q_k|.$$

Получили противоречие.

Наиболее сложная часть леммы доказана. Окончание доказательства и доказательство теоремы 14.2 можно прочитать самостоятельно (не хватило времени на лекции).

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ