

Элементы теории чисел

Механико-математический факультет МГУ

1 поток 1 курса, осень 2026г.

Лекция 5: Сравнения и их основные свойства. Классы вычетов по заданному модулю. Полная и приведенная системы вычетов. Теоремы Вильсона, Эйлера и Ферма.

Основные определения и утверждения прошлой лекции

Функция $\theta(n)$, $n \in \mathbb{N}$, мультипликативна, если

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

для любых двух взаимно простых натуральных чисел a и b .

Лемма

Пусть $\theta(n)$ – мультипликативная функция и

$$f(n) = \sum_{d|n} \theta(d), \quad n \geq 1,$$

где суммирование происходит по всем натуральным делителям числа n . Тогда $f(n)$ – мультипликативная функция и

$$f(n) = \prod_{p|n} (1 + \theta(p) + \theta(p^2) + \dots + \theta(p^{\nu_p(n)})).$$

Мультипликативная функция Мёбиуса $\mu(n)$ определяется на всех натуральных числах равенствами $\mu(1) = 1$,

$$\mu(n) = 0, \text{ если } p^2 | n; \quad \mu(p_1 p_2 \dots p_r) = (-1)^r, \text{ если } p_i \text{ различны.}$$

Лемма

Справедливы равенства

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{если } n = 1, \\ 0 & \text{если } n > 1, \end{cases} \quad \sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Теорема (Формула обращения Мёбиуса.)

Пусть $f(n)$ – произвольная функция натурального аргумента и

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

Для каждого целого числа $n \geq 1$ обозначим символом $\varphi(n)$ функцию Эйлера, т.е. количество натуральных чисел, не превосходящих n и взаимно простых с n .

Теорема (Свойства функции Эйлера.)

1. Для любого натурального $n \geq 2$ выполняется равенство

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

2. Функция Эйлера мультипликативна, т.е. для любых двух натуральных взаимно простых чисел a и b имеем

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Функции

$$\tau(n) = \sigma_0(n) = \sum_{d|n} 1; \quad \sigma(n) = \sigma_1(n) = \sum_{d|n} d$$

– количество и сумма делителей натурального числа мультипликативны.

Если $n = p_1^{k_1} \cdots p_m^{k_m}$, то

$$\tau(n) = (k_1 + 1) \cdots (k_m + 1), \quad \sigma(n) = \prod_{p|n} \frac{p^{\nu_p(n)+1} - 1}{p - 1}.$$

Глава 4. Числовые сравнения.

§4.1. Сравнения и их основные свойства.

Пусть $m \geq 2$ целое число.

Определение 1

Два целых числа a и b называются *сравнимыми по модулю m* , если их разность делится на m , т.е. $m|(a - b)$.

Число m – модуль сравнения. Обозначение: $a \equiv b \pmod{m}$.

Свойства:

1. $a \equiv a \pmod{m}$ для любого целого a .
2. Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
3. Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.
4. Если $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, то

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

т.е. сравнения по одному и тому же модулю можно почленно складывать вычитать и умножать.

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

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

Доказательства этих сравнений следуют из равенств

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

$$(b - d) - (a - c) = (b - a) - (d - c),$$

$$bd - ac = (b - a)d + (d - c)a$$

и свойств делимости.

Из этих свойств следует также, что к любой из частей сравнения можно прибавить любое число кратное модулю, обе части сравнения можно умножить на одно и то же целое число и возвести в одну и ту же натуральную степень. В результате получатся верные сравнения.

В частности, отсюда следует, что если $a \equiv b \pmod{m}$ и $P(x)$ – произвольный многочлен с целыми коэффициентами, то

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

Подобное свойство выполняется и для многочленов от нескольких переменных.

5. Если $ab \equiv ac \pmod{m}$ и $(a, m) = 1$, то $b \equiv c \pmod{m}$.

Действительно, согласно условию $m \mid (ab - ac) = a(b - c)$ и так как при этом m и a взаимно просты, то получаем $m \mid (b - c)$, а это и требовалось.

6. Обе части сравнения и модуль можно умножить на любое отличное от нуля число, т.е. из сравнения $a \equiv b \pmod{m}$ при $d \neq 0$ следует $ad \equiv bd \pmod{md}$.

7. Обе части сравнения и модуль можно разделить на их общий множитель, т.е. из сравнения $ad \equiv bd \pmod{md}$ при $d \neq 0$ следует $a \equiv b \pmod{m}$.

8. Если $a \equiv b \pmod{m}$, то $(a, m) = (b, m)$.

Действительно, из условия следует, что $b - a = mc$ с некоторым целым c . Но тогда $b = a + mc$ и множество общих делителей чисел a и m совпадает с множеством общих делителей чисел b и m . В частности, наибольшие элементы этих множеств совпадают, т.е. $(a, m) = (b, m)$.

9. Если $a \equiv b \pmod{m}$ и $d|m$, то $a \equiv b \pmod{d}$.

10. Если сравнение $a \equiv b$ имеет место по нескольким модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.

Действительно, если $a \equiv b \pmod{m_j}$, $j = 1, 2, \dots, r$, то разность $a - b$ делится на каждое из чисел m_j . Но тогда можно утверждать, что $a - b$ делится на наименьшее общее кратное модулей $m_1, \dots, m_r$.

Если разность $a - b$ не делится на m , будем писать $a \not\equiv b \pmod{m}$.

Как простейший пример использования сравнений, докажем, что уравнение

$$x^2 - 5y^2 = 3 \quad (1)$$

не имеет решений в целых числах.

Предположим, что целые числа a и b удовлетворяют данному уравнению, т.е. $a^2 - 5b^2 = 3$. Тогда $a^2 \equiv 3 \pmod{5}$.

Целое число a сравнимо с одним из чисел $0, 1, 2, 3, 4$ по модулю 5. Тогда a^2 сравнимо по этому же модулю с одним из чисел $0, 1, 2^2 = 4, 3^2 \equiv 4, 4^2 \equiv 1$, т.е. с одним из чисел $0, 1, 4$.

Так как 3 не сравнимо по модулю 5 ни с одним из чисел $0, 1, 4$, приходим к противоречию, доказывающему, что уравнение (1) не имеет решений в целых числах.

§4.2. Классы вычетов по данному модулю.

- Свойства сравнений 1-3

1. $a \equiv a \pmod{m}$ для любого целого a .
2. Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
3. Если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

означают, что всё множество целых чисел разбивается в объединение непересекающихся подмножеств, состоящих из чисел, попарно сравнимых между собой.

- Эти подмножества называются *классами вычетов* по модулю m . Элементы каждого из подмножеств называются *вычетами* этого класса. Класс вычетов, содержащий целое число a будет обозначаться $\bar{a}$.

- Таким образом, $\bar{a} = \bar{b}$, если и только если $a \equiv b \pmod{m}$.

Пример: Класс вычетов $\bar{0}$ состоит из всех чисел, делящихся на m .

Каждое целое число a представимо в виде

$$a = mq + r, \quad 0 \leq r < m,$$

с целыми q, r . Отсюда следует, что a и r лежат в одном классе вычетов и, значит, каждый класс вычетов содержит целое число r из промежутка $0 \leq r < m$.

- Таким образом, количество классов вычетов по модулю m не превосходит m . С другой стороны, каждое из чисел $0, 1, 2, \dots, m-1$ лежит в некотором классе вычетов и классы эти различны, ведь разность любых двух чисел из указанного списка не делится на m .

- Эти рассуждения доказывают, что *существует ровно m классов вычетов по модулю m* . Каждый из них содержит единственное целое число r из промежутка $0 \leq r < m$, называемое *наименьшим неотрицательным вычетом класса*,

$$\overline{0}, \quad \overline{1}, \quad \dots, \quad \overline{m-1}$$

— все классы вычетов по модулю m .

Лемма 1

Пусть a – целое число, взаимно простое с модулем m . Тогда найдется целое число b , удовлетворяющее сравнению

$$ab \equiv 1 \pmod{m}. \quad (2)$$

Доказательство.

Числа

$$a, 2a, 3a, \dots, ma \quad (3)$$

не сравнимы друг с другом по модулю m . Ведь если $ak \equiv a\ell \pmod{m}$, где k, ℓ – натуральные числа, не превосходящие m , то по свойству 5 сравнений выполняется $k \equiv \ell \pmod{m}$. Это возможно лишь в случае $k = \ell$. Итак, числа (3) принадлежат различным классам вычетов по модулю m . Количество этих чисел равно m , поэтому какое-то из них, скажем ba принадлежит классу $\bar{1}$. Тогда $ab \equiv 1 \pmod{m}$. □

- Приведенное нами доказательство леммы 1 не конструктивно и не позволяет найти число b , удовлетворяющее сравнению (2).
- Рассмотрим диофантово уравнение $ax - my = 1$ относительно неизвестных x, y . Так как коэффициенты этого уравнения взаимно просты, то это уравнение разрешимо в целых числах.
- С помощью расширенного алгоритма Евклида, действуя так, как это описано описано ранее, можно найти пару чисел $x = b, y = c$, удовлетворяющую равенству $ab - mc = 1$. Тогда $ab \equiv 1 \pmod{m}$. Эти рассуждения дают ещё одно доказательство леммы 1.
- Если $(a, m) > 1$, то ни при каком целом b сравнение (2) выполняться не может.

- По свойству 8 сравнений, если некоторый класс вычетов содержит число a взаимно простое с модулем, то все вычеты этого класса будут взаимно простыми с модулем. Поэтому среди всех классов вычетов выделяются классы, состоящие из элементов, взаимно простых с модулем.
- Эти классы имеют вид $\bar{k}$ для $0 \leq k < m$ и $(k, m) = 1$. Количество таких чисел k равно $\varphi(m)$, т.е. задаётся функцией Эйлера.

На языке сравнений удобно описывать так называемые признаки делимости чисел. При наличии калькулятора или компьютера, конечно, удобнее воспользоваться техническими средствами, но иногда бывает польза и от вычислений на бумаге. Предположим нам нужно узнать, делится ли данное натуральное число N на некоторое другое число d . Идея всех признаков делимости состоит в том, чтобы построить меньшее число M , делящееся на d одновременно с N .

Следующий общий способ основан на использовании леммы 1.

- Пусть d – натуральное число, взаимно простое с основанием системы счисления 10. Тогда согласно лемме 1 найдется число k , для которого $10k \equiv 1 \pmod{d}$.
- Пусть теперь $N = 10u + v$, где u, v целые числа. Тогда справедливо сравнение по модулю d

$$N = 10u + v \equiv 10u + 10kv = 10(u + kv) \pmod{d}$$

- Обозначим $M = u + kv$. Поскольку числа 10 и d взаимно просты, то из сравнения следует, что N и M одновременно делятся на d .
- Вопрос о делимости N на число d сводится к выяснению, делится ли на d число M . Если при этом окажется, что $M < N$, то наша задача упростилась.
- В следующих примерах число v равно младшей цифре в десятичной записи числа N .

d = 7. В этом случае справедливо сравнение $10 \cdot (-2) \equiv 1 \pmod{7}$ и можно взять $k = -2$. Из сказанного выше следует, что число $N = 10u + v$ делится на 7 одновременно с числом $u - 2v$. Заменяя данное число N меньшими числами по этому правилу мы получаем последовательность убывающих чисел N_i . Пусть, например, $N = 22624$. Тогда

$$N_1 = 2262 - 2 \cdot 4 = 2254, N_2 = 225 - 2 \cdot 4 = 217, N_3 = 21 - 2 \cdot 7 = 7.$$

Так как последнее число делится на 7, то 22624 также делится на 7.

d = 13. Имеем $10 \cdot 4 \equiv 1 \pmod{13}$ и можно взять $k = 4$. Число $N = 10u + v$ делится на 13 одновременно с числом $u + 4v$. Пусть, например, $N = 32721$. Тогда

$$N_1 = 3272 + 4 \cdot 1 = 3276, N_2 = 327 + 4 \cdot 6 = 351, N_3 = 35 + 4 \cdot 1 = 39.$$

Последнее число делится на 13, поэтому и 32721 делится на 13.

$d = 17$. Имеем $10 \cdot (-5) \equiv 1 \pmod{17}$ и можно взять $k = -5$. Число $N = 10u + v$ делится на 17 одновременно с числом $u - 5v$. Пусть, например, $N = 39321$. Тогда

$$N_1 = 3932 - 5 \cdot 1 = 3927, \quad N_2 = 392 - 5 \cdot 7 = 357, \quad N_3 = 35 - 5 \cdot 7 = 0.$$

Итак, число 39321 делится на 17.

- При $d = 19$ можно взять $k = 2$, при $d = 23$ имеем $k = 7$, и $k = 3$ при $d = 29$.
- Для $d = 3$ и $d = 9$ имеем $k = 1$ и, как легко проверить, получаем известный признак: *натуральное число делится на 3 или 9, если сумма его цифр делится на 3 или 9.*
- В случае $d = 11$ имеем $k = -1$ и признак делимости: *натуральное число делится на 11 в том и только том случае, когда знакопеременная сумма его цифр делится на 11.* Для доказательства этих утверждений нужно использовать индукцию по количеству цифр.

§4.3. Полная и приведённая системы вычетов.

- Совокупность представителей всех классов вычетов по заданному модулю $m \geq 2$ называется *полной системой вычетов* по модулю m .

Примеры полных систем вычетов.

1. Числа $0, 2, 2^2 = 4, 2^3 = 8, 2^4 = 16$ по модулю 5.
2. Наименьшие неотрицательные вычеты всех классов $0, 1, \dots, m - 1$.
3. Любые m чисел попарно несравнимые друг с другом по модулю m , ведь они принадлежат различным классам вычетов, а количество их равно числу классов, см. доказательство леммы 1.
4. Абсолютно наименьшие вычеты классов по модулю m , т.е. числа x , удовлетворяющие неравенствам $-\frac{m}{2} < x \leq \frac{m}{2}$. При $m = 5$ имеем набор $-2, -1, 0, 1, 2$, а при $m = 6$ систему вычетов $-2, -1, 0, 1, 2, 3$.

В предыдущем параграфе было доказано, что существует $\varphi(m)$ классов вычетов по модулю m , состоящих из чисел взаимно простых с модулем.

- Любой набор представителей всех этих классов вычетов называется *приведенной системой вычетов*.
- Любые $\varphi(m)$ чисел, попарно несравнимые друг с другом по модулю m и взаимно простые с модулем, образуют *приведённую систему вычетов по модулю m* . Ведь они лежат в различных классах, состоящих из чисел взаимно простых с m , а количество их равно количеству таких классов.

Теорема 10

Пусть $a, m \geq 2$, – целые взаимно простые числа. Тогда

1. если x пробегает полную систему вычетов по модулю m , то $ax + b$, где b – любое целое число, также пробегает полную систему вычетов по модулю m ;
2. если x пробегает приведенную систему вычетов по модулю m , то ax также пробегает приведенную систему вычетов по этому модулю.

Доказательство теоремы 10.

Для доказательства первого утверждения достаточно проверить, что для любых двух чисел x_1 и x_2 , лежащих в различных классах вычетов по модулю m , числа $ax_1 + b$ и $ax_2 + b$ также лежат в различных классах вычетов.

- Предположим противное. Тогда

$$ax_1 + b \equiv ax_2 + b \pmod{m}.$$

Из этого сравнения следует, что $ax_1 \equiv ax_2 \pmod{m}$ и, поскольку числа a, m взаимно просты, по свойству 5 сравнений заключаем, что $x_1 \equiv x_2 \pmod{m}$. Но это невозможно, так как x_1 и x_2 принадлежат различным классам вычетов по модулю m . Первое утверждение теоремы доказано.

Доказательство второго утверждения.

Из сказанного выше следует, что для любых двух различных чисел x_1, x_2 приведённой системы вычетов числа ax_1, ax_2 лежат в различных классах вычетов. Осталось доказать, что для x , лежащего в приведённой системе вычетов, число ax взаимно просто с m . Действительно, если d – общий делитель m и ax , то $d|ax$, $(d, a) = 1$. По свойству делимости (следствие 2 из теоремы 2) заключаем, что $d|x$. Так как $(x, m) = 1$, это возможно лишь в случае, когда $d = 1$. Теорема доказана полностью.

§4.4. Теорема Вильсона.

Теорема 11

Для любого простого числа p выполняется сравнение

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

Для $p = 2$ и $p = 3$ утверждение выполняется, поэтому, доказывая теорему, далее будем считать, что $p \geq 5$.

- Пусть a – некоторое целое число из промежутка $1 \leq a < p$. Так как $(a, p) = 1$, то по лемме 1 существует целое число b , удовлетворяющее сравнению $ab \equiv 1 \pmod{p}$. При этом можно считать, что b есть наименьший неотрицательный вычет в своем классе. Ясно, что $b \neq 0$, т.е. $1 \leq b < p$.
- Число b определяется единственным образом. Ведь если $ab_1 \equiv 1 \pmod{p}$, $ab_2 \equiv 1 \pmod{p}$, то $p | a(b_1 - b_2)$ и $p | (b_1 - b_2)$, что при различных b_1, b_2 из промежутка $1 \leq b < p$ невозможно.

Если $b \equiv a \pmod{p}$, то $a^2 \equiv ab \equiv 1 \pmod{p}$ и $p \mid (a^2 - 1) = (a - 1)(a + 1)$. Так как p простое число, это возможно лишь в случае $a = 1$ или $a = p - 1$.

- Из доказанного следует, что множество целых чисел a из промежутка $1 < a < p - 1$ может быть разбито на пары различных целых чисел a, b , удовлетворяющих сравнению $ab \equiv 1 \pmod{p}$.

- Следовательно,

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

Умножая это сравнение на $p - 1$, получаем

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

- Для составных чисел теорема Вильсона, конечно, нарушается. Ведь если целое число N имеет делитель $d, 1 < d < N$, то $(N - 1)!$ делится на d . Значит, $(N - 1)! + 1$ на d не делится, а потому не делится и на N .

§4.5. Теоремы Эйлера и Ферма.

Теорема 12 (Л. Эйлер, 1760г.)

Для каждого целого числа a , взаимно простого с модулем m , выполняется сравнение

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

Пусть $r_1, \dots, r_h$ – какая-нибудь приведённая система вычетов по модулю m . Тогда $h = \varphi(m)$. Согласно теореме 10 множество чисел $ar_1, ar_2, \dots, ar_h$ также составляет приведённую систему вычетов. Это значит, что каждое число второй системы лежит в одном классе с каким-либо единственным числом первой системы вычетов. Поэтому справедливы сравнения

$$ar_1 \cdot ar_2 \cdots ar_h \equiv r_1 \cdot r_2 \cdots r_h \pmod{m}. \quad (4)$$

Продолжение доказательства теоремы Эйлера.

$$ar_1 \cdot ar_2 \cdots ar_h \equiv r_1 \cdot r_2 \cdots r_h \pmod{m}.$$

Так как каждое из чисел r_j взаимно просто с модулем, то сравнение (4) можно сократить на каждое из r_j . В результате получаем сравнение $a^h \equiv 1 \pmod{m}$ или $a^{\varphi(m)} \equiv 1 \pmod{m}$. Теорема Эйлера доказана.

Например, для $m = 10$ имеем $\varphi(10) = 4$. В соответствии с теоремой Эйлера можно утверждать, что каждое нечетное число a , не делящееся на 5, удовлетворяет сравнению $a^4 \equiv 1 \pmod{10}$, т.е. последняя цифра в десятичной записи числа a^4 равна 1. И действительно,

$$1^4 = 1, \quad 3^4 = 81, \quad 7^4 = 2401, \quad 9^4 = 6561.$$

Рассмотрим ещё один пример: *определить последние три цифры в десятичной записи числа 3^{2026} .*

• Для этого достаточно сосчитать $3^{2026} \pmod{1000}$. Так как $\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$, и $(3, 1000) = 1$, то по теореме Эйлера $3^{400} \equiv 1 \pmod{1000}$ и

$$3^{2026} = (3^{400})^5 \cdot 3^{26} \equiv 3^{26}.$$

Здесь и далее все сравнения выполняются по модулю 1000.

- Сравнения $3^6 \equiv 27^2 \equiv -271$, $3^{12} \equiv 271^2 \equiv 441$, $3^{13} \equiv 3 \cdot 441 \equiv 323$, $3^{26} \equiv 323^2 \equiv 329$ означают, что десятичная запись числа 3^{2026} оканчивается цифрами 329.
- Для некоторых чисел a сравнение $a^d \equiv 1 \pmod{m}$ может выполняться и при натуральных $d < \varphi(m)$.
- Например, можно проверить, что $3^{100} \equiv 1 \pmod{1000}$, но выше установлено и использовалось равенство $\varphi(100) = 400$.

- Наименьшее $d \in \mathbb{N}$ с условием $a^d \equiv 1 \pmod{m}$ называется показателем, которому a принадлежит по модулю m .

Лемма 2

Пусть d – показатель, которому a принадлежит по модулю m .
Натуральное число k удовлетворяет сравнению $a^k \equiv 1 \pmod{m}$ в том и только том случае, когда $d|k$. В частности, $d|\varphi(m)$.

Для каждого $k = ds$ имеем

$$a^k = (a^d)^s \equiv 1 \pmod{m}.$$

Докажем утверждение в обратную сторону. Пусть $a^k \equiv 1 \pmod{m}$. Разделив k на d с остатком, получим $k = dq + r$, $0 \leq r < d$. Тогда

$$a^k \equiv (a^d)^q \cdot a^r = a^r \equiv 1 \pmod{m}.$$

- Так как d – наименьшее натуральное число с условием $a^d \equiv 1 \pmod{m}$ и $r < d$, заключаем $r = 0$, т.е. $d|k$.

Рассмотрим частный случай теоремы Эйлера, в котором $m = p$ есть простое число. Тогда $\varphi(p) = p - 1$ и получается следующее утверждение.

Теорема 13 (Малая теорема Ферма)

Если целое число a не делится на простое число p , то

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

Из этой теоремы следует, что при любом целом a число $a^p - a = a(a^{p-1} - 1)$ делится на p .

В дальнейшем мы неоднократно будем использовать как теорему Эйлера, так и малую теорему Ферма.

Конец 5-й лекции