

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Механико-математический факультет МГУ

1 поток 1 курса, осень 2026г.

Лекция 7: Сравнения с одним неизвестным. Сравнения первой степени. Китайская теорема об остатках. Деление многочленов в сравнениях. Теорема Лагранжа.

Основные определения и утверждения прошлой лекции.

1. Представление рациональных чисел бесконечными десятичными дробями.
2. Быстрый алгоритм возведения в степень.
3. Система шифрования RSA.
4. Построение больших простых чисел.

Глава 5. Сравнения с одним неизвестным.

В предыдущей главе мы уже встречались с задачей нахождения целых чисел, удовлетворяющих заданным сравнениям.

- Лемма про обратимые числа по модулю m есть утверждение об условиях разрешимости в целых числах x сравнения $ax \equiv 1 \pmod{m}$.
- Уравнение $x^2 - 5y^2 = 3$ не имеет решений в целых числах потому, что неразрешимо сравнение $x^2 \equiv 3 \pmod{5}$.
- Из малой теоремы Ферма следует, что для простого p каждое целое число удовлетворяет сравнению $x^p - x \equiv 0 \pmod{p}$.
- А чтобы прочесть сообщение, зашифрованное с помощью схемы *RSA*, нужно уметь решать сравнения вида $x^e \equiv a \pmod{m}$.

В этой главе мы обсудим некоторые общие вопросы, связанные с решением сравнений, в которые входит одна неизвестная величина, будем обозначать её буквой x . В отличие от уравнений каждое сравнение имеет ещё и модуль. Разрешимость сравнений, а также способы нахождения решений, зависят, как мы увидим в дальнейшем, от свойств модуля.

§6.2. Основные определения.

Пусть даны целое число $m \geq 2$ и многочлен

$f(x) = a_n x^n + \dots + a_1 x + a_0$ с целыми коэффициентами. Говорят, что целое число u удовлетворяет сравнению

$$a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{m}, \quad (1)$$

если $f(u) \equiv 0 \pmod{m}$.

- Из доказанных ранее свойств сравнений следует, что для любого целого числа v , сравнимого с u по модулю m , выполняется $f(v) \equiv f(u) \equiv 0 \pmod{m}$, другими словами, все числа класса вычетов $x \equiv u \pmod{m}$ удовлетворяют сравнению (1).

Таким образом, множество, состоящее из всех целых чисел, удовлетворяющих (1), если оно не пусто, представляется в виде объединения нескольких непересекающихся классов вычетов по модулю m .

- Каждый класс вычетов, состоящий из чисел, удовлетворяющих (1), называется *решением сравнения*, а количество таких классов вычетов, называется *числом решений* этого сравнения.
- Согласно малой теореме Ферма каждое целое число удовлетворяет сравнению $x^p - x \equiv 0 \pmod{p}$ при простом p . Поэтому каждый класс вычетов по модулю p есть решение этого сравнения, а число его решений равно p .

Если коэффициент при старшей степени x не делится на m , т.е. $m \nmid a_n$, то говорят, что *степень сравнения* (1) равна n .

- Например, сравнение второй степени $x^2 - 1 \equiv 0 \pmod{8}$ имеет четыре решения

$$x \equiv 1 \pmod{8},$$

$$x \equiv 3 \pmod{8},$$

$$x \equiv 5 \pmod{8},$$

$$x \equiv 7 \pmod{8}.$$

Сравнению удовлетворяет каждое нечетное число.

Можно рассматривать и сравнения более общего вида

$$f(x) \equiv g(x) \pmod{m}, \quad (2)$$

где $f(x), g(x)$ – многочлены с целыми коэффициентами.

- Из свойств сравнений сразу же следует, что множества чисел, удовлетворяющих (2) и сравнению $f(x) - g(x) \equiv 0 \pmod{m}$ совпадают. Так что все вопросы, возникающие в связи со сравнениями (2) сразу же сводятся к соответствующим вопросам для сравнений, содержащих 0 в правой части.

§6.4. Сравнения первой степени.

Каждое сравнение первой степени может быть переписано в виде

$$ax \equiv b \pmod{m}, \quad m \nmid a. \quad (3)$$

- Основной результат о таких сравнениях есть

Теорема 14.

Сравнение (3) разрешимо если и только если, b делится на наибольший общий делитель (a, m) . Количество решений в этом случае равно (a, m) .

Сравнение (3) разрешимо в том и только в том случае, когда имеет решение в целых числах x, y уравнение

$$ax + my = b. \quad (4)$$

- Ранее было доказано, что для этого необходимо и достаточно, чтобы $(a, m) | b$.

Предположим теперь, что b делится на (a, m) . Из той же теоремы следует, что множество решений уравнения имеет вид

$$x = x_0 + \frac{m}{(a, m)}t, \quad y = y_0 - \frac{a}{(a, m)}t, \quad (5)$$

где пара чисел x_0, y_0 есть какое-либо фиксированное решение, а t – произвольное целое число.

Итак, множество целых чисел x , удовлетворяющих сравнению (3) имеет вид

$$x = x_0 + \frac{m}{(a, m)}t, \quad t \in \mathbb{Z} \quad (6)$$

при некотором целом x_0 . Рассмотрим числа

$$x_k = x_0 + \frac{m}{(a, m)}k, \quad k = 1, 2, \dots, (a, m). \quad (7)$$

Докажем, что каждое число, удовлетворяющее сравнению (3), сравнимо по модулю m с одним из чисел (6). Пусть x имеет вид (6) и k – то из чисел совокупности $1, 2, \dots, (a, m)$, которое сравнимо с t по модулю (a, m) . Тогда $t = k + q \cdot (a, m)$ с некоторым целым q , и

$$x = x_0 + \frac{m}{(a, m)}(k + q \cdot (a, m)) = x_k + qm \equiv x_k \pmod{m}.$$

Для завершения доказательства осталось проверить, что все числа (7) лежат в разных классах вычетов по модулю m .

Предположим, что $x_k \equiv x_\ell \pmod{m}$, где k, ℓ – различные числа из набора $1, 2, \dots, (a, b)$. Тогда

$$\frac{m}{(a, m)} k \equiv \frac{m}{(a, m)} \ell \pmod{m}.$$

Разделив обе части и модуль этого сравнения на целое число $\frac{m}{(a, m)}$ получаем в силу свойства 7 сравнений, что $k \equiv \ell \pmod{(a, m)}$. Получившееся противоречие завершает доказательство теоремы.



- Для решения сравнения (3) можно решить в целых числах уравнение (4), чтобы найти x_0 и воспользоваться формулой (7) для нахождения представителей всех нужных классов вычетов.
- Для упрощения решения сравнения все коэффициенты можно заменить их наименьшими неотрицательными вычетами по модулю m .

Заметим, также, что в случае разрешимости, т.е делимости b на (a, m) , обе части сравнения и модуль можно разделить на (a, m) , что упростит задачу, сведя её к сравнению с меньшим модулем, но не изменит множество решений в целых числах.

- Решим, например, сравнение

$$38x \equiv 4 \pmod{26}.$$

Так как $38 \equiv 12 \pmod{26}$, то множества целых чисел, удовлетворяющих данному сравнению, а также сравнениям $12x \equiv 4 \pmod{26}$ и $6x \equiv 2 \pmod{13}$ одинаковы.

- Поскольку $(12, 26) = 2$ и $2|4$ находим, что данное сравнение разрешимо и имеет два решения.

Применим расширенный алгоритм Евклида для решения уравнения $6x + 13y = 2$. Составим матрицу для этого уравнения

$$\begin{pmatrix} 6 & 13 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Первая её строка составлена из коэффициентов уравнения, вторая строка отвечает за переменную x , а третья за переменную y . Так как значение последней переменной нас не интересует, то для сокращения вычислений опустим последнюю строку в этой матрице. И далее преобразуем её с помощью допустимых преобразований.

$$\begin{pmatrix} 6 & 13 \\ 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 6 & 1 \\ 1 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 13 & -2 \end{pmatrix}.$$

Чтобы получить вторую матрицу, нужно удвоить первый столбец первой матрицы и вычесть результат из второго столбца. Первый столбец третьей матрицы получается умножением второго столбца второй матрицы на 6 и вычитанием результата из её первого столбца.

- Множество чисел, удовлетворяющих сравнению $6x \equiv 1 \pmod{13}$, состоит из одного класса вычетов по модулю 13, а именно $x \equiv -2 \pmod{13}$, а множество решений сравнения $6x \equiv 2 \pmod{13}$ имеет вид $x \equiv -2 \cdot 2 \pmod{13} \equiv -4 \pmod{13}$.
- Классы вычетов по модулю 26 содержат числа $-4 + 13k$, $k = 1, 2$ и составляют два решения: $x \equiv 9$, $x \equiv 22 \pmod{26}$.

§6.3. Китайская теорема об остатках.

При решении некоторых задач возникает потребность найти целые числа x , удовлетворяющие одновременно нескольким сравнениям. Как и в случае уравнений при этом говорят, что требуется решить систему сравнений.

- Сначала рассмотрим системы сравнений специального вида

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \dots\dots\dots \\ x \equiv a_k \pmod{m_k}, \end{cases}$$

где $m_i > 0$, a_i – заданные целые числа. Их решение также может быть сведено к решению систем уравнений. Но в одном важном частном случае решение системы (8) может быть получено относительно легко.

- Следующее утверждение было известно в Китае примерно 2 тысячелетия назад. В настоящее время оно носит название "китайская теорема об остатках".

Теорема 15.

Если $m_1, \dots, m_k$ попарно взаимно просты, то система сравнений (8) разрешима. Если для целых чисел M, M_i, b_i выполнены соотношения

$$M = m_1 \cdots m_k, \quad M_i = \frac{M}{m_i}, \quad M_i b_i \equiv a_i \pmod{m_i}, \quad 1 \leq i \leq k,$$

и

$$x_0 = M_1 b_1 + \dots + M_k b_k, \tag{8}$$

то множество целых чисел, удовлетворяющих системе сравнений (8), составляет класс вычетов $x \equiv x_0 \pmod{M}$.

Поскольку в условиях теоремы $(M_i, m_i) = 1$, то существование чисел b_i следует из теоремы 14.

- Заметим также, что числа b_i определяются не единственным способом.
- При использовании теоремы 15 для решения систем сравнений, следует выбирать те из чисел b_i , которые дают по возможности меньшие значения x_0 .

Так как $m_i | M_j$ при $j \neq i$, то при любом i выполняются сравнения

$$x_0 \equiv M_i b_i \equiv a_i \pmod{m_i}. \quad (9)$$

Это значит, что множества целых чисел, удовлетворяющих системе (8) и сравнению

$$x \equiv x_0 \pmod{m_i}, \quad 1 \leq i \leq k, \quad (10)$$

совпадают. Сравнения (10) выполняются в том и только том случае, когда $m_i | (x - x_0)$, $1 \leq i \leq k$. Учитывая попарную взаимную простоту модулей m_i , заключаем, что (10) равносильно условию $M | (x - x_0)$, т.е. $x \equiv x_0 \pmod{M}$.



Пример. Решим систему сравнений

$$x \equiv 3 \pmod{7}, \quad x \equiv 2 \pmod{11}, \quad x \equiv 1 \pmod{13}, \quad .$$

- В данном случае модули 7, 11, 13 попарно взаимно просты.

Пользуясь соотношениями теоремы 15, находим $M = 7 \cdot 11 \cdot 13 = 1001$, $M_1 = 11 \cdot 13 = 143$, $M_2 = 7 \cdot 13 = 91$, $M_3 = 7 \cdot 11 = 77$.

- Решая вспомогательные сравнения

$$143x \equiv 3 \pmod{7}, \quad 91x \equiv 2 \pmod{11}, \quad 77x \equiv 1 \pmod{13},$$

и выбирая по одному числу, удовлетворяющему каждому из них, находим $b_1 = 1$, $b_2 = -3$, $b_3 = -1$.

- Далее вычисляем

$$x_0 = 143 \cdot 1 - 91 \cdot 3 - 77 \cdot 1 = -207 \text{ и } x \equiv -207 \pmod{1001}.$$

Следствие 1.

Если числа $a_1, \dots, a_k$ независимо друг от друга пробегают полные системы вычетов по модулям $m_1, \dots, m_k$ соответственно, то числа x_0 , определённые для каждого набора $a_1, \dots, a_k$ с помощью равенства (8), пробегают полную систему вычетов по модулю $M = m_1 \cdots m_k$.

- Получающиеся указанным в теореме 15 способом числа x_0 принадлежат различным классам вычетов по модулю M .
- Действительно, предположим, что $a_1, \dots, a_k$ и $a'_1, \dots, a'_k$ два набора вычетов по модулям $m_1, \dots, m_k$, причём такие, что с некоторым индексом i разность $a_i - a'_i$ не делится на m_i .

Пусть также числа b_j, b'_j удовлетворяют сравнениям

$$M_j b_j \equiv a_j \pmod{m_j}, \quad M_j b'_j \equiv a'_j \pmod{m_j}, \quad j = 1, \dots, k \text{ и}$$

$$x_0 = M_1 b_1 + \dots + M_k b_k, \quad x'_0 = M_1 b'_1 + \dots + M_k b'_k.$$

- Если $x_0 \equiv x'_0 \pmod{M}$, то выполняется сравнение $x_0 \equiv x'_0 \pmod{m_j}$.
- Учитывая, что $m_i | M_j$ при $j \neq i$, заключаем, что $M_i b_i \equiv M_i b'_i \pmod{m_i}$ и, значит, $a_i \equiv a'_i \pmod{m_i}$. Другими словами a_i, a'_i принадлежат одному классу вычетов по модулю m_i . Таким образом получаем противоречие, означающее, что $m_1 \cdots m_k = M$ чисел x_0 , отвечающих различным, указанным в условии следствия наборам $a_1, \dots, a_k$, лежат в различных классах вычетов по модулю M и это завершает доказательство следствия.

Следствие 2.

Если числа $a_1, \dots, a_k$ независимо друг от друга пробегают приведённые системы вычетов по модулям $m_1, \dots, m_k$ соответственно, то числа x_0 , определённые для каждого набора $a_1, \dots, a_k$ с помощью равенств (8), пробегают приведённую систему вычетов по модулю $M = m_1 \cdots m_k$.

- Все числа x_0 , полученные согласно условию, принадлежат различным классам вычетов по модулю M . Это доказано в следствии 1.

Так как числа m_j попарно взаимно просты, то с помощью сравнений (9) находим

$$(M, x_0) = (m_1, x_0) \cdots (m_k, x_0) = (m_1, a_1) \cdots (m_k, a_k).$$

Значит равенство $(M, x_0) = 1$ выполняется в том и только том случае, когда $(m_i, a_i) = 1$, $1 \leq i \leq k$. Следствие доказано.

Следствие 2 дает иное доказательство мультипликативности функции Эйлера $\varphi(n)$. Действительно, если числа $a_1, \dots, a_k$ независимо друг от друга пробегают приведенные системы вычетов по модулям $m_1, \dots, m_k$, то количество получившихся наборов равно $\varphi(m_1) \cdots \varphi(m_k)$.

Согласно следствию 2 это число равно количеству классов вычетов по модулю M , состоящих из чисел, взаимно простых с M , т.е. равно $\varphi(M)$.

В результате получается равенство $\varphi(M) = \varphi(m_1) \cdots \varphi(m_k)$ при условии, что числа m_i попарно взаимно просты.

Решим, например, следующую систему сравнений

$$\begin{cases} 3x \equiv 5 \pmod{4}, \\ 5x \equiv 2 \pmod{7}. \end{cases} \quad (11)$$

Умножив оба сравнения системы на 3, и пользуясь тем, что $3 \cdot 3 \equiv 1 \pmod{4}$, $3 \cdot 5 \equiv 1 \pmod{7}$, получим систему сравнений к которой применима китайская теорема об остатках

$$x \equiv 3 \pmod{4}, \quad x \equiv 6 \pmod{7}.$$

Согласно теореме 15 имеем $M = 4 \cdot 7 = 28$, $M_1 = 7$, $M_2 = 4$.

Решая сравнения $7b \equiv 3 \pmod{4}$ и $4b \equiv 6 \pmod{7}$, находим

$b_1 = 1$, $b_2 = -2$. Теперь можно получить частное решение исходной системы сравнений $x_0 = 7 \cdot 1 - 4 \cdot 2 = -1$. Таким

образом, данная система сравнений имеет единственное решение $x \equiv -1 \pmod{28}$.

§6.5. Полиномиальные сравнения по простому модулю.

В этом параграфе мы рассмотрим сравнения вида

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \equiv 0 \pmod{p}, \quad p \nmid a_n, \quad (12)$$

где p – простое число. Следующее утверждение, доказанное Лагранжем в 1768г., носит его имя.

Теорема 16.

Сравнение (12) имеет не более n решений.

- Заметим, что для составного модуля, даже при $n = 1$, утверждение теоремы может нарушаться.

Докажем теорему индукцией по степени сравнения n . При $n = 1$ справедливость её утверждения следует из теоремы 14.

- Предположим теперь, что $n \geq 2$ и утверждение справедливо для всех сравнений степени меньшей n . Пусть x_0 – целое число, удовлетворяющее сравнению (12).

- Тогда $f(x_0) \equiv 0 \pmod{p}$ и

$$f(x) - f(x_0) = \sum_{k=1}^n a_k(x^k - x_0^k) = (x - x_0)g(x),$$

где $g(x) = a_n x^{n-1} + \dots \in \mathbb{Z}[x]$.

- Из этого равенства следует, что для каждого целого числа x_1 , удовлетворяющего сравнению (12) будет выполняться сравнение $(x_1 - x_0)g(x_1) \equiv 0 \pmod{p}$.

- Поэтому каждое целое число, удовлетворяющее сравнению (12) и не лежащее в классе вычетов x_0 , т.е. удовлетворяющее условию $p \nmid (x_1 - x_0)$, будет решением сравнения $g(x) \equiv 0 \pmod{p}$.
- Согласно индуктивному предположению это сравнение имеет не более $n - 1$ решений. Отсюда следует, что существует не более n классов вычетов по модулю p , элементы которых удовлетворяют сравнению (12).



Следствие 3.

Для каждого простого числа p справедливо сравнение

$$x^p - x \equiv x(x - 1)(x - 2) \cdots (x - p + 1) \pmod{p}, \quad (13)$$

т.е. коэффициенты при одинаковых степенях переменной x в левой и правой частях (13) сравнимы между собой по модулю p .

Рассмотрим многочлен

$$f(x) = x^p - x - x(x-1)(x-2)\cdots(x-p+1) \in \mathbb{Z}[x].$$

- Степень его не превосходит $p-1$. Если n – наибольшее целое число такое, что коэффициент при x^n в многочлене $f(x)$ не делится на p , то степень сравнения $f(x) \equiv 0 \pmod{p}$ равна n .
- Для каждого $a \in \mathbb{Z}, 0 \leq a < p$ согласно малой теореме Ферма имеем $f(a) = a^p - a \equiv 0 \pmod{p}$. Значит, количество решений сравнения $f(x) \equiv 0 \pmod{p}$ равно p .
- По теореме 16 выполняется неравенство $p \leq n$. Поскольку $n \leq p-1$, получаем противоречие, доказывающее, что все коэффициенты многочлена $f(x)$ делятся на p . Это завершает доказательство теоремы.

Сравнивая коэффициенты при x в первой степени слева и справа в сравнении (13), получаем теорему Вильсона

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

Теорема 17.

Пусть

$$f(x) = (x^p - x)g(x) + r(x), \quad r(x) \in \mathbb{Z}[x], \quad \deg r(x) < p.$$

Тогда множества целых чисел, удовлетворяющих сравнениям

$$f(x) \equiv 0 \pmod{p} \quad \text{и} \quad r(x) \equiv 0 \pmod{p},$$

совпадают. Другими словами, каждое сравнение (12) можно заменить равносильным ему сравнением степени, не превосходящей $p-1$.

Для каждого целого числа a в силу малой теоремы Ферма имеем

$$f(a) = (a^p - a)g(a) + r(a) \equiv r(a) \pmod{p}.$$

Отсюда сразу же следует нужное утверждение.



Иногда степень сравнения можно ещё уменьшить, не изменяя при этом множества решений. Для описания этого способа удобно воспользоваться тем, что каждое целое число, не делящееся на p , обратимо по модулю p .

Пример 1. Разделить с остатком многочлен $3x^3 + 2$ на многочлен $x - 2$.

$$\begin{array}{r|l}
 3x^3 & +0x^2 & +0x & +2 \\
 \underline{3x^3} & \underline{-6x^2} & & \\
 & 6x^2 & +0x & \\
 & \underline{6x^2} & \underline{-12x} & \\
 & & 12x & +2 \\
 & & \underline{12x} & \underline{-24} \\
 & & & 26
 \end{array}
 \quad
 \begin{array}{r}
 x - 2 \\
 \hline
 3x^2 + 6x + 12
 \end{array}$$

$$3x^3 + 2 = (x - 2) \cdot (3x^2 + 6x + 12) + 26.$$

Если старший коэффициент делителя по абсолютной величине больше 1, то при делении, вообще говоря, могут появиться дроби, что усложняет вычисление. При делении по простому модулю эту сложность можно избежать.

Пример 2. Разделить с остатком многочлен $3x^3 + 2$ на многочлен $2x + 1$ по модулю 5.

- Старший коэффициент делителя равен 2 и обратим по модулю 5. Так как $3 \cdot 2 \equiv 1 \pmod{5}$, то $3(2x + 1) \equiv x - 2 \pmod{5}$. Теперь старший коэффициент делителя стал равным 1 и воспользовавшись результатом предыдущего слайда, найдём

$$\begin{aligned} 3x^3 + 2 &= (x - 2) \cdot (3x^2 + 6x + 12) + 26 \equiv \\ &3(2x + 1) \cdot (3x^2 + x + 2) + 1 \pmod{5} \equiv \\ &(2x + 1) \cdot (4x^2 + 3x + 1) + 1 \pmod{5}. \end{aligned}$$

Эта идея работает и в общем случае. Предположим, нам нужно разделить с остатком многочлен $g(x) \in \mathbb{Z}[x]$ на многочлен $f(x) = a_n x^n + \dots \in \mathbb{Z}[x]$ по модулю простого числа p . Допустим также, что $p \nmid a_n$.

Решая соответствующее сравнение, найдём целое число u , для которого $u \cdot a_n \equiv 1 \pmod{p}$. Тогда многочлен $\bar{f}(x) = x^n + \dots \equiv u \cdot f(x) \pmod{p}$ имеет целые коэффициенты, а его старший коэффициент равен 1.

Разделив многочлен $g(x)$ на $\bar{f}(x)$ с остатком, найдём

$$g(x) = \bar{f}(x) \cdot q(x) + r(x),$$

где $q(x), r(x) \in \mathbb{Z}[x]$.

Переходя к сравнениям, находим

$$g(x) \equiv f(x) \cdot uq(x) + r(x) = f(x)\bar{q}(x) + r(x),$$

где $\bar{q}(x) = u \cdot q(x) \in \mathbb{Z}[x]$.

При любом простом p , выполняя деление с остатком, можно вычислять наибольший общий делитель двух многочленов. Этот алгоритм подобен алгоритму для целых чисел и также носит название алгоритм Евклида. Наибольший общий делитель многочленов $f(x)$ и $g(x)$ будет, как и для целых чисел, обозначаться символом $(f(x), g(x))$.

Следующее утверждение позволяет, не нарушая равносильности, понизить степень сравнения больше, чем теорема 17.

Теорема 18. Пусть $f(x)$ и $d(x)$ многочлены с целыми коэффициентами, причём, $d(x)$ есть наибольший общий делитель $f(x)$ и $x^p - x$ по модулю p . Тогда множества решений сравнений

$$f(x) \equiv 0 \pmod{p}, \quad \text{и} \quad d(x) \equiv 0 \pmod{p} \quad (14)$$

одинаковы.