ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 10

СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ И КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ

Тема 10 по рабочей программе: сравнения первого порядка и системы сравнений. Китайская теорема об остатках. **Объём:** 1 академический час.

Цель: доказать критерий разрешимости линейного сравнения и научиться восстанавливать целый класс по нескольким остаткам, учитывая совместность и правильный период решений.

После изучения темы студент умеет: находить все решения линейного сравнения; доказывать существование и единственность решения системы; применять обычную и обобщённую КТО; объяснять связь локальных корней многочлена с корнями по составному модулю.

Предварительная подготовка: НОД, тождество Безу, обратный элемент, классы вычетов. Практическая работа №9 познакомила с вычислениями; эта лекция обосновывает использованные алгоритмы. Практическая работа №10 продолжит тему сравнений высших степеней.

План лекции

1. Сравнения и сокращение общего множителя — 5 минут.
2. Линейное сравнение: критерий и число решений — 12 минут.
3. Конструктивная КТО и её доказательство — 13 минут.
4. Совместность при невзаимно простых модулях — 10 минут.
5. Корни по составному модулю и подведение итогов — 5 минут.

Раздел 5 содержит дополнительное алгебраическое объяснение для самостоятельного чтения; задачи из раздела 6 выполняются после лекции.

1 Сравнение и допустимое сокращение

Пусть $m \geq 2$. Запись $a \equiv b \pmod m$ означает $m \mid (a-b)$. Это отношение эквивалентности: каждое число сравнимо с собой, сравнение симметрично, а из делимости двух разностей следует делимость их суммы. Класс a обозначим $[a]_m$. В каждом классе есть единственный представитель из $0, 1, \dots, m-1$.

Сравнения можно складывать, вычитать и перемножать при одном модуле. Например, если $a \equiv b$ и $c \equiv d \pmod m$, то $ac - bd = a(c-d) + d(a-b)$ делится на m. Поэтому сложение и умножение классов определены корректно.

Лемма о сокращении. Если $d = \gcd(c, m)$, то

$$cu \equiv cv \pmod m \quad \Leftrightarrow \quad u \equiv v \pmod{m/d}.$$

Доказательство. Запишем $c = dc_1$, $m = dm_1$, где $\gcd(c_1, m_1) = 1$. Условие $m \mid c(u-v)$ равносильно $m_1 \mid c_1(u-v)$. Из тождества Безу для c_1, m_1 следует $m_1 \mid (u-v)$. Обратное утверждение получается умножением на c.

Таким образом, сохранить прежний модуль при сокращении можно, если множитель взаимно прост с модулем. В частности, класс $[c]_m$ обратим тогда и только тогда, когда $\gcd(c, m) = 1$.

Пример 1. Из $6x \equiv 6 \pmod{15}$ следует $x \equiv 1 \pmod{5}$. По исходному модулю имеются три представителя: $1, 6, 11$. Запись $x \equiv 1 \pmod{15}$ потеряла бы два решения.

2 Сравнение первой степени

2.1 Критерий разрешимости

Рассмотрим сравнение $ax \equiv b \pmod{m}$, где a, b — целые числа, $m \geq 2$. Обозначим $d = \gcd(a, m)$.

Теорема 1. Сравнение разрешимо тогда и только тогда, когда $d \mid b$. Если это условие выполнено, то имеется ровно d различных классов решений по модулю m.

Необходимость. Из $ax - b = mt$ получаем $b = ax - mt$. Число d делит оба слагаемых справа и потому делит b.

Достаточность. По тождеству Безу существуют u, v с $au + mv = d$. Умножение на целое число b/d даёт

$$a\left(u\frac{b}{d}\right) + m\left(v\frac{b}{d}\right) = b.$$

Следовательно, $x_* = u(b/d)$ — частное решение. Если x — другое решение, то $a(x - x_*) \equiv 0 \pmod{m}$. По лемме о сокращении $x - x_*$ кратно m/d. Обратно, любая такая прибавка сохраняет сравнение.

2.2 Полная запись ответа

Положим $m' = m/d$ и выберем x_0 как наименьший неотрицательный остаток x_* по модулю m'. Тогда все целые решения и все представители по исходному модулю имеют вид

$$x = x_0 + tm', \quad t \in \mathbb{Z}; \qquad x_k = x_0 + km', \quad 0 \leq k < d.$$

Представители x_k различны по модулю m: из $m \mid (k - l)m'$ следует $d \mid (k - l)$, что при $0 \leq k, l < d$ возможно только для $k = l$. Других представителей нет, поскольку любое целое t имеет один из d остатков по модулю d. Теорема доказана.

Важно различать: один класс по сокращённому модулю m' и d классов по исходному модулю m. Это две равносильные формы описания одного множества целых чисел.

Пример 2. Решим $18x \equiv 42 \pmod{60}$. Здесь $d = 6$, а 42 делится на 6. После деления получаем $3x \equiv 7 \pmod{10}$. Обратный к 3 равен 7, поэтому $x \equiv 49 \equiv 9 \pmod{10}$. Ответ по модулю 60:

$$x \in \{9, 19, 29, 39, 49, 59\} \pmod{60}.$$

Проверка для первого корня: $18 \cdot 9 - 42 = 120$. Переход к следующему представителю увеличивает левую часть на $18 \cdot 10 = 180$, кратное 60.

Пример 3. Сравнение $18x \equiv 43 \pmod{60}$ неразрешимо, так как $6 \nmid 43$. Наличие обратного к сокращённому коэффициенту здесь не помогает: сокращать правую часть на 6 нельзя.

Граничные случаи. Для $a = 0$ сравнение разрешимо при $m \mid b$, и тогда подходит каждый из m классов. Если $m \nmid b$, решений нет. Формула теоремы остаётся верной: $d = m$, $m' = 1$. Отрицательные коэффициенты не меняют критерий; НОД выбирается неотрицательным.

2.3 Алгебраический смысл числа решений

Умножение на a задаёт гомоморфизм аддитивных групп $T_a: \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Его ядро — решения $ax \equiv 0 \pmod m$, то есть классы $0, m', \dots, (d-1)m'$. Поэтому ядро содержит d элементов.

Если x_* отображается в b, то все прообразы b имеют вид $x_* + \ker T_a$. Каждый непустой слой отображения содержит ровно d классов. Образ состоит из классов, представленных числами, кратными d, и содержит m/d элементов. Это объясняет, почему число решений не зависит от конкретного разрешимого правого остатка.

3 Китайская теорема об остатках

3.1 Формулировка и конструкция

Пусть $m_1, \dots, m_r \geq 2$ попарно взаимно просты, $M = m_1 \cdots m_r$. Для любых целых остатков $a_1, \dots, a_r$ система $x \equiv a_i \pmod{m_i}$ имеет единственное решение по модулю M.

Доказательство существования. Положим $M_i = M/m_i$. Из попарной взаимной простоты следует $\gcd(M_i, m_i) = 1$, поэтому существует u_i с $M_i u_i \equiv 1 \pmod{m_i}$. Введём $E_i = M_i u_i$. Тогда

$$E_i \equiv 1 \pmod{m_i}, \qquad E_i \equiv 0 \pmod{m_j} \quad (j \neq i).$$

Следовательно, число

$$x = \sum_{i=1}^{r} a_i E_i$$

имеет нужный остаток по каждому модулю: при переходе к модулю m_j все слагаемые, кроме j-го, исчезают.

Доказательство единственности. Если x и y удовлетворяют системе, то каждый m_i делит $x - y$. Произведение попарно взаимно простых делителей также делит это число. Поэтому $M \mid (x - y)$, то есть $x \equiv y \pmod M$. Все целые решения имеют вид $x_0 + tM$, где $0 \leq x_0 < M$.

Теорема восстанавливает класс, а не одно целое число без дополнительных условий. Число становится единственным после выбора диапазона длины M, например $[0, M)$.

3.2 Вычислительный пример

Пример 4. Найдём $x \equiv 5 \pmod 8$, $x \equiv 11 \pmod{15}$. Имеем $M = 120$, $M_1 = 15$, $M_2 = 8$. Обратные: $15^{-1} \equiv 7 \pmod 8$ и $8^{-1} \equiv 2 \pmod{15}$. Поэтому $E_1 = 105$, $E_2 = 16$ и

$$x \equiv 5 \cdot 105 + 11 \cdot 16 = 701 \equiv 101 \pmod{120}.$$

Проверка: $101 = 12 \cdot 8 + 5 = 6 \cdot 15 + 11$. Метод подстановки даёт тот же результат: из $x = 5 + 8t$ получаем $8t \equiv 6 \pmod{15}$, откуда $t \equiv 12 \pmod{15}$.



Рисунок 1. В клетке указан представитель класса по модулю 15. Голубым выделены четыре корня сравнения $x^2 \equiv 1 \pmod{15}$.

4 Общие модули и системы линейных сравнений

4.1 Объединение двух классов

Пусть заданы $x \equiv a \pmod{m}$ и $x \equiv b \pmod{n}$. Обозначим $g = \gcd(m, n)$.

Теорема 2. Система совместна тогда и только тогда, когда $g \mid (b - a)$. В случае совместности решение единственно по модулю $L = \operatorname{lcm}(m, n) = mn/g$.

Доказательство. Подставим $x = a + mt$. Второе условие станет $mt \equiv b - a \pmod{n}$. Теорема 1 даёт критерий $g \mid (b - a)$. При его выполнении после сокращения получаем одно решение $t \equiv t_0 \pmod{n/g}$. Следовательно, $x = a + mt_0 + kmn/g$, что доказывает и существование, и точный период.

Если u входит в тождество $mu + nv = g$, то удобная формула имеет вид

$$t_0 \equiv u\frac{b-a}{g} \pmod{n/g}, \qquad x_0 \equiv a + mt_0 \pmod{L}.$$

При $n/g = 1$ можно взять $t_0 = 0$: второе условие при совместности уже следует из первого. Формула через Безу позволяет обойти обращение по модулю 1.

Пример 5. Для $x \equiv 7 \pmod{12}$ и $x \equiv 15 \pmod{20}$ имеем $g = 4$, разность остатков равна 8. Из $12t \equiv 8 \pmod{20}$ следует $3t \equiv 2 \pmod{5}$, то есть $t \equiv 4 \pmod{5}$. Ответ: $x \equiv 55 \pmod{60}$. Если заменить остаток 15 на 14, разность станет 7 и система окажется несовместной.

4.2 Несколько сравнений

Условия объединяют последовательно: два первых заменяют одним, затем добавляют третье и так далее. На каждом шаге проверяют делимость разности остатков на НОД текущего периода и нового модуля. Если все шаги успешны, итоговый период равен НОК исходных модулей. Доказательство следует по индукции из теоремы 2: после каждого шага новое сравнение описывает в точности пересечение уже учтённых условий.

Общий критерий. Система $x \equiv a_i \pmod{m_i}$ совместна тогда и только тогда, когда для любых i, j остатки a_i, a_j сравнимы по модулю $\gcd(m_i, m_j)$.

Необходимость очевидна из существования общего x. Для достаточности разложим модули на простые степени. Для каждого простого p выберем условие, модуль которого содержит максимальную степень p^e. Попарная совместность гарантирует согласованность выбранного остатка со всеми остальными условиями по меньшим степеням этого простого числа. Выбранные максимальные простые степени попарно взаимно просты. Обычная КТО объединяет их в решение, которое удовлетворяет всем исходным условиям.

4.3 Сначала нормализация

Для системы $a_i x \equiv b_i \pmod{m_i}$ сначала решают каждое линейное сравнение. Если хотя бы одно неразрешимо, вся система неразрешима. Иначе каждое условие заменяют одним классом по модулю $m_i/\gcd(a_i, m_i)$ и только затем объединяют классы.

Пример 6. Система $8x \equiv 12 \pmod{20}$, $9x \equiv 3 \pmod{21}$ сводится к $x \equiv 4 \pmod{5}$, $x \equiv 5 \pmod{7}$. Из $x = 4 + 5t$ получаем $5t \equiv 1 \pmod{7}$, то есть $t \equiv 3 \pmod{7}$. Ответ: $x \equiv 19 \pmod{35}$. Подстановка: $8 \cdot 19 - 12 = 140$, $9 \cdot 19 - 3 = 168$.

5 Алгебраический смысл и корни многочленов

При попарно взаимно простых модулях отображение

$$\Phi: \mathbb{Z}/M\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}, \qquad [x]_M \mapsto ([x]_{m_1}, \dots, [x]_{m_r})$$

сохраняет сложение, умножение и единицу. КТО доказывает его биективность, поэтому это изоморфизм колец. В правой части действия выполняются покоординатно. Базисные классы E_i удовлетворяют $E_i^2 = E_i$, $E_i E_j = 0$ при $i \neq j$ и $\sum E_i = 1$ по модулю M. Эти равенства достаточно проверить по каждому m_j и применить единственность в КТО.

Пусть $f \in \mathbb{Z}[x]$. Число x — корень $f(x) \equiv 0 \pmod{M}$ тогда и только тогда, когда его остаток является корнем по каждому m_i. Таким образом, наборы локальных корней взаимно однозначно соответствуют корням по модулю M. Если по модулям имеется $r_1, \dots, r_s$ корней, их общее число равно $r_1 \cdots r_s$. Если хотя бы один набор пуст, корней по M нет.

Пример 7. Для $x^2 \equiv 1 \pmod{77}$ рассматриваем модули 7 и 11. По каждому простому модулю имеются два корня 1 и -1: из $(x-1)(x+1) = 0$ в поле следует обращение одного из множителей в нуль. Четыре пары дают корни $1, 34, 43, 76$ по модулю 77.

Корни 1 и 34 не совпадают и не противоположны по модулю 77. Их разность и сумма раскрывают множители: $\gcd(34 - 1, 77) = 11$, $\gcd(34 + 1, 77) = 7$. Это арифметическая связь извлечения квадратного корня с факторизацией, используемая при изучении схем типа Рабина. Само сравнение $c \equiv x^2 \pmod{n}$ ещё не задаёт способ выбора исходного сообщения из нескольких корней.

Если модуль содержит p^e, решение только по модулю p недостаточно. В практической работе №10 сначала будут найдены все корни по каждой степени простого, затем применена КТО.

6 Закрепление и самостоятельная работа

1. Найдите все представители решения $22x \equiv 14 \pmod{40}$. Объясните число решений.
2. Решите $-15x \equiv 21 \pmod{36}$. Отдельно рассмотрите $0x \equiv 4 \pmod{12}$.
3. Решите систему $x \equiv 3 \pmod{7}$, $x \equiv 6 \pmod{8}$, $x \equiv 4 \pmod{9}$ конструктивной КТО.
4. Объедините $x \equiv 4 \pmod{18}$ и $x \equiv 10 \pmod{24}$. Что изменится при замене 10 на 11?
5. Решите систему из примера 6 и определите число её классов по модулю 420.
6. Найдите все корни $x^2 \equiv 1 \pmod{65}$. Покажите, как с помощью корней 1 и 14 получить нетривиальные делители 65.

Контрольные вопросы

1. Как определяется сравнение целых чисел и класс вычетов?
2. Как меняется модуль при сокращении общего множителя?
3. Почему условие $\gcd(a, m) \mid b$ необходимо и достаточно?
4. Чем отличаются все целые решения и представители по исходному модулю?
5. Почему разрешимое линейное сравнение имеет ровно d классов?
6. Что произойдёт при нулевом коэффициенте a?
7. Как строятся числа E_i и какие остатки они имеют?
8. Где в доказательстве КТО используется попарная взаимная простота?
9. Почему КТО определяет класс по модулю произведения?
10. Каков критерий совместности двух произвольных модулей и точный период?
11. Зачем сокращать линейные сравнения до применения КТО?
12. Как из наборов локальных корней получить все корни по составному модулю?

Литература

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии**. 2020. §7.2.1–7.2.3: линейные сравнения и системы; теорема 7.4: КТО. Страницы 209–215 по печатной нумерации предоставленного издания.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory**. 2nd ed. 2006. §3.4, The Chinese Remainder Theorem. Источник для сопоставления конструктивного доказательства и вычислений.

Изложения доказательств и числовые примеры в этом конспекте подготовлены для данной дисциплины. Полные решения самостоятельных задач приведены в отдельном документе для преподавателя.