ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 5

СРАВНЕНИЯ И КЛАССЫ ВЫЧЕТОВ

Цель лекции	Обосновать сравнимость целых чисел, разбиение на классы вычетов и правила преобразования сравнений с одинаковыми и разными модулями.
Результат обучения	Доказывать корректность замены представителей, выбирать допустимый модуль при сокращении и объединении сравнений, проверять полноту системы вычетов.
Предварительная подготовка	Деление с остатком, НОД и НОК, тождество Безу, свойства взаимно простых чисел из лекций 1–4.

Аудиторная нагрузка: 1 академический час. Основное содержание занятия — определения, свойства сравнений и работа с модулями. Доказательства дополнительных следствий и развёрнутые вычислительные примеры предназначены также для самостоятельного чтения.

План лекции

1. Сравнимость целых чисел и её критерии.
2. Классы вычетов и полные системы представителей.
3. Арифметические действия при одном модуле.
4. Сокращение сравнений и его ограничения.
5. Сравнения по разным модулям.
6. Вычислительные приложения и самостоятельная работа.

1 Сравнимость целых чисел

Пусть m — фиксированное положительное целое число. Целые a, b называются **сравнимыми по модулю** m, если m делит их разность. Запись

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a - b)$$

означает, что существует целое t с $a = b + mt$. Число m называют модулем сравнения. Оно является частью утверждения: одни и те же два числа могут быть сравнимы по одному модулю и не сравнимы по другому.

Пример. Числа -38 и 39 сравнимы по модулю 11, поскольку их разность равна -77. Но по модулю 5 они не сравнимы. Знак разности не влияет на делимость.

Теорема о равенстве остатков. Сравнение $a \equiv b \pmod{m}$ равносильно тому, что a и b имеют одинаковые неотрицательные остатки при делении на m.

Доказательство. Запишем $a = mq + r$, $b = ms + t$, где $0 \le r, t < m$. Если $r = t$, разность $a - b = m(q - s)$ делится на m. Обратно, из делимости $a - b$ следует $m \mid (r - t)$. При этом $-m < r - t < m$, а единственное кратное m в таком интервале — нуль. Значит, $r = t$.

В примере $-38 = 11(-4) + 6$, $39 = 11 \cdot 3 + 6$. Поэтому для проверки сравнения можно использовать либо разность, либо два остатка. При $m = 1$ все целые сравнимы между собой.

1.1 Отношение эквивалентности

Для фиксированного m сравнимость обладает тремя свойствами. Рефлексивность следует из $m \mid 0$, поэтому $a \equiv a$. Симметричность следует из того, что вместе с $a - b$ на m делится $b - a$. Транзитивность следует из равенства $a - c = (a - b) + (b - c)$: из $a \equiv b$ и $b \equiv c$ получается $a \equiv c$ по тому же модулю.

Эти свойства делают сравнимость **отношением эквивалентности**. Оно позволяет объединять числа в непересекающиеся классы, сохраняя информацию, существенную для выбранного модуля.

1.2 НОД зависит только от класса

Если $a \equiv b \pmod{m}$, то

$$\gcd(a, m) = \gcd(b, m).$$

Доказательство. Из $a = b + mt$ следует: каждый общий делитель b, m делит a, а из $b = a - mt$ следует обратное включение множеств общих делителей. Положительные наибольшие общие делители поэтому совпадают.

Например, $-84 \equiv 6 \pmod{30}$ и оба НОД равны 6. В частности, взаимная простота с модулем сохраняется при замене числа любым сравнимым представителем. Это свойство будет основанием для определения обратимости класса вычетов.

2 Классы вычетов

Классом вычетов числа a по модулю m называется множество

$$[a]_m = \{a + km : k \in \mathbb{Z}\}.$$

Сам класс — бесконечное множество; представитель — одно выбранное число из этого множества. Например, $[-38]_{11} = [6]_{11} = [39]_{11}$, хотя три целых числа различны.

Два класса либо совпадают, либо не имеют общих элементов. Действительно, если c лежит одновременно в $[a]_m$ и $[b]_m$, то $a \equiv c \equiv b$, откуда $a \equiv b$. Любое число, сравнимое с одним из них, сравнимо и с другим.

Из теоремы о делении с остатком следует разбиение

$$\mathbb{Z} = [0]_m \cup [1]_m \cup \cdots \cup [m-1]_m.$$

Здесь объединение попарно непересекающееся. Классов ровно m: каждый целый попадает в один из них, а разные числа от 0 до $m - 1$ не сравнимы. Множество этих классов обозначают $\mathbb{Z}/m\mathbb{Z}$ или $\mathbb{Z}_m$.



Рисунок 1. В каждой строке находятся числа одного класса по модулю 4. Разность соседних представителей равна 4; каждая строка продолжается в обе стороны.

2.1 Полная система вычетов

Если из каждого класса взять ровно один представитель, полученная совокупность называется **полной системой вычетов**. Наиболее привычна система $0,1,\dots,m-1$, но представители могут быть отрицательными и большими по абсолютной величине.

Критерий полноты. Набор из m целых чисел является полной системой тогда и только тогда, когда все его элементы попарно не сравнимы по модулю m.

Доказательство опирается на число классов: m различных классов исчерпывают всё множество $\mathbb{Z}_m$. Одного условия «в наборе m различных целых» недостаточно: разные целые могут принадлежать одному классу.

Например, $-10,-4,2,8,14$ различны как целые, но по модулю 5 их остатки равны $0,1,2,3,4$, поэтому это полная система. Набор $0,1,2,3,8$ не полон по модулю 5: класс 3 повторяется, а класс 4 отсутствует.

Любые m последовательных целых образуют полную систему: ненулевая разность двух из них по абсолютной величине меньше m и не может делиться на m. Для симметричного выбора представителей используем соглашение $-m/2 < s \le m/2$. Например, при $m = 6$ это $-2,-1,0,1,2,3$; из двух равноудалённых представителей середины выбран положительный.

2.2 Аффинное преобразование представителей

Теорема. Если x пробегает полную систему по модулю m, то числа $ax + b$ также образуют полную систему ровно при $\gcd(a,m) = 1$.

Если НОД равен 1, из $ax_i + b \equiv ax_j + b$ следует $m \mid a(x_i - x_j)$, а по свойству взаимной простоты — $m \mid (x_i - x_j)$. Исходные представители из разных классов поэтому дают разные выходные классы.

Если $g = \gcd(a,m) > 1$, классы 0 и m/g различны, но их образы совпадают: разность образов равна $a(m/g) = m(a/g)$. Поэтому преобразование не может давать полную систему. Сдвиг b не меняет этот вывод.

При $m = 7$ набор $4j - 3$, $j = 0, \ldots, 6$, даёт остатки $4,1,5,2,6,3,0$. Все классы представлены. По модулю 9 набор $3j + 1$ даёт только классы 1, 4 и 7. Подсчёт повторений через НОД разобран в практической работе 4.

3 Сравнения с одинаковым модулем

Пусть $a \equiv b \pmod m$ и $c \equiv d \pmod m$. Тогда допустимы сложение, вычитание и умножение соответствующих частей:

$$a + c \equiv b + d, \qquad a - c \equiv b - d, \qquad ac \equiv bd \pmod m.$$

Для суммы и разности достаточно сложить или вычесть кратные m разности. Для произведения используем

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

Оба слагаемых справа делятся на m. Отсюда следуют перенос слагаемого с изменением знака, прибавление кратного модуля к любой части и умножение обеих частей на одно целое число.

Индукцией по положительному целому k получаем $a^k \equiv b^k \pmod m$. Для многочлена P с целыми коэффициентами это даёт

$$a \equiv b \pmod m \quad \Rightarrow \quad P(a) \equiv P(b) \pmod m.$$

Каждую степень можно заменить сравнимой, затем умножить на соответствующий целый коэффициент и сложить. Для нескольких переменных рассуждение применяется к каждому аргументу. Поэтому уменьшение промежуточных результатов по модулю не изменяет конечный остаток.

3.1 Независимость от представителей

Правила

$$[a]_m + [b]_m = [a + b]_m, \qquad [a]_m[b]_m = [ab]_m$$

задают операции над классами корректно. Если вместо a, b выбрать a', b' из тех же классов, доказанные свойства дают $a + b \equiv a' + b'$ и $ab \equiv a'b'$. Результирующий класс не изменится.

Например, по модулю 7 классы чисел -2 и 5 совпадают. Умножение на класс 3 можно выполнить как $(-2) \cdot 3 = -6 \equiv 1$ или как $5 \cdot 3 = 15 \equiv 1$. В обоих случаях получается класс $[1]_7$. Эти операции образуют основу кольца вычетов, которое рассматривается в лекции 6.

4 Правильное сокращение сравнений

Из $ca \equiv cb \pmod m$ не всегда следует $a \equiv b \pmod m$. Например, $2 \cdot 1 \equiv 2 \cdot 4 \pmod 6$, но $1 \not\equiv 4 \pmod 6$. Умножение может объединять разные классы.

Точное правило сокращения. Для целого c и $g = \gcd(c, m)$

$$ca \equiv cb \pmod m \quad \Leftrightarrow \quad a \equiv b \pmod{m/g}.$$

Доказательство. Представим $c = gc_1$, $m = gm_1$, где $\gcd(c_1, m_1) = 1$. Тогда $m \mid c(a - b)$ равносильно $m_1 \mid c_1(a - b)$, а это равносильно $m_1 \mid (a - b)$. Последний переход обоснован взаимной простотой. Для обратного направления достаточно восстановить множители.

При $g = 1$ модуль сохраняется. При $g > 1$ сохранение исходного модуля возможно у конкретной пары, но не является общим правилом. При $c = 0$ имеем $g = m$ и новый модуль 1: сравнение $0 \equiv 0$ истинно, и все целые сравнимы по модулю 1.

Пример. Из $14 \cdot 5 \equiv 14 \cdot 17 \pmod{24}$ получаем $5 \equiv 17 \pmod{12}$, поскольку НОД равен 2. Разность 12 делится на новый модуль, но не на 24.

Если положительный множитель присутствует и в обеих частях, и в модуле, справедливо другое равносильное преобразование:

$$da \equiv db \pmod{dm} \quad \Leftrightarrow \quad a \equiv b \pmod{m}, \qquad d > 0.$$

Оно следует из $dm \mid d(a-b)$. Необходимо отличать сокращение всей записи от удаления множителя только из двух частей сравнения.

4.1 Действия с дополнительными условиями

Из совпадения квадратов нельзя извлекать совпадение оснований: $1^2 \equiv 5^2 \pmod{12}$, но $1 \not\equiv 5 \pmod{12}$. Также нельзя уменьшать показатель степени по модулю основания сравнения. Хотя $3 \equiv 8 \pmod{5}$, получаем $2^3 \equiv 3 \pmod{5}$, а $2^8 \equiv 1 \pmod{5}$. Правила работы с показателями требуют отдельных теорем и гипотез.

Сравнимость не переносит обычный порядок на классы: представители 0 и 12 одного класса по модулю 12 находятся по разные стороны от числа 1. При переходе к классам следует сохранять именно доказанные арифметические свойства.

5 Сравнения с разными модулями

5.1 Переход к делителю модуля

Если $d \mid m$, то из $a \equiv b \pmod{m}$ следует $a \equiv b \pmod{d}$. Разность, делящаяся на m, делится и на d. Обратный переход обычно неверен: $1 \equiv 5 \pmod{4}$, но $1 \not\equiv 5 \pmod{12}$.

Можно определить отображение $[a]_m \mapsto [a]_d$. Оно не зависит от представителя именно при $d \mid m$. Достаточность уже доказана. Для необходимости заметим, что $[0]_m = [m]_m$ должны иметь одинаковые образы; следовательно, $[0]_d = [m]_d$ и $d \mid m$.

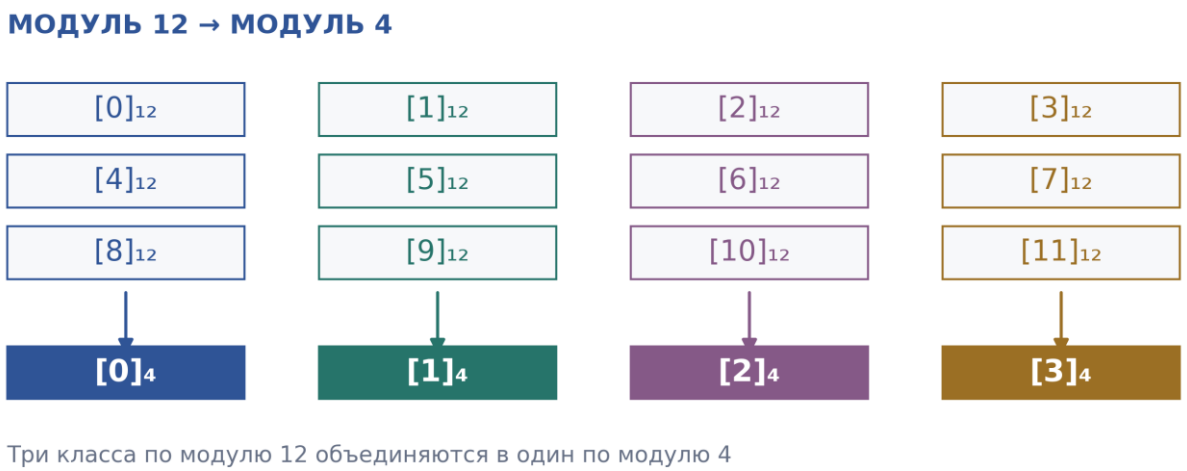


Рисунок 2. При переходе от модуля 12 к его делителю 4 каждый нижний класс объединяет три верхних класса. Например, классы 1, 5 и 9 по модулю 12 переходят в класс 1 по модулю 4.

5.2 Одна пара чисел по нескольким модулям

Для положительных m, n и $L = \operatorname{lcm}(m, n)$ справедливо

$$(a \equiv b \pmod{m} \text{ и } a \equiv b \pmod{n}) \quad \Leftrightarrow \quad a \equiv b \pmod{L}.$$

Действительно, разность является общим кратным m, n ровно тогда, когда она делится на их НОК. Рассуждение распространяется на любое конечное число модулей.

Например, -23 и 49 имеют разность -72. Они сравнимы по модулям 8 и 12, поэтому сравнимы по НОК 24. По произведению $8 \cdot 12 = 96$ сравнение неверно. Произведение гарантированно заменяет НОК только при взаимной простоте модулей.

Здесь оба исходных сравнения относятся к **одной паре** чисел. Задача восстановления неизвестного по заданным разным остаткам является отдельной задачей о системе сравнений.

5.3 Разные пары чисел

Пусть $a \equiv b \pmod{m}$, $c \equiv d \pmod{n}$ и $G = \gcd(m, n)$. Оба сравнения можно привести к модулю G, после чего применять правила сложения и умножения:

$$a + c \equiv b + d \pmod{G}, \qquad ac \equiv bd \pmod{G}.$$

Например, $17 \equiv 5 \pmod{12}$ и $23 \equiv 5 \pmod{18}$. При $G = 6$ получаем $40 \equiv 10 \pmod{6}$ и $391 \equiv 25 \pmod{6}$. Для суммы модуль 36 неверен, поскольку разность равна 30. НОК объединяет два сравнения одной пары, а общий делитель позволяет выполнить совместные операции с разными парами.

6 Вычислительные примеры

6.1 Многочлен и схема Горнера

Вычислим $P(x) = 2x^3 - 5x + 7$ при $x = -38$ по модулю 11. Можно сразу взять $r = 6$. Тогда $P(6) = 409 \equiv 2 \pmod{11}$. Полное значение $P(-38) = -109547$ даёт тот же остаток 2.

Чтобы ограничивать размер промежуточных чисел, запишем многочлен по схеме Горнера:

$$P(x) = ((2x + 0)x - 5)x + 7.$$

Шаг	Вычисление при $r = 6$	Остаток по 11
Начальное значение	2	2
Коэффициент при x^2	$2 \cdot 6 + 0 = 12$	1
Коэффициент при x	$1 \cdot 6 - 5 = 1$	1
Свободный член	$1 \cdot 6 + 7 = 13$	2

На каждом шаге заменяется лишь представитель текущего класса. В программной реализации остаток берётся после каждого умножения и сложения; исходный многочлен и его результат по модулю остаются согласованными.

6.2 Признаки делимости десятичных чисел

Для десятичной записи $N = d_0 + 10d_1 + \cdots + 10^k d_k$ из $10 \equiv 1 \pmod 9$ следует

$$N \equiv d_0 + d_1 + \cdots + d_k \pmod 9.$$

А из $10 \equiv -1 \pmod{11}$ следует

$$N \equiv d_0 - d_1 + d_2 - \cdots + (-1)^k d_k \pmod{11}.$$

Вторая сумма начинается с цифры единиц. Обе формулы получены заменой степеней 10 сравнимыми значениями и сложением. Они проверяют делимость на конкретный модуль; это не тесты простоты числа.

7 Самостоятельная работа

1. Разбейте числа $-29, -18, -7, 4, 15, 26, -25, -3, 8, 19, -22, 0, 33$ на классы по модулю 11. Запишите общий вид каждого встретившегося класса.
2. Докажите сохранение НОД при замене представителя и вычислите $\gcd(-84, 30)$ через наименьший неотрицательный остаток.
3. Проверьте полноту наборов $-14, -6, 2, 10, 18, 26, 34$ и $-14, -6, 2, 10, 18, 26, 33$ по модулю 7. Обоснуйте результат для набора $4j - 3$ по модулю 7 и $3j + 1$ по модулю 9 при переборе всех стандартных представителей j.
4. Проверьте $14 \cdot 5 \equiv 14 \cdot 17 \pmod{24}$ и выполните правильное сокращение. Приведите универсальный контрпример сохранению модуля 24 при сокращении множителя 14.
5. Проверьте пару $-23, 49$ по модулям $8, 12, 24, 96$. Затем используйте $u_1 = -15 \equiv -23 \pmod 8$, $v_1 = 61 \equiv 49 \pmod{12}$ для сравнения сумм и произведений по НОД модулей.
6. Вычислите $P(-25)$ по модулю 13 схемой Горнера. Для числа 72936 проверьте делимость на 9 и 11 с помощью цифр и обычного деления.

Контрольные вопросы

1. Какие три равносильные формулировки сравнимости можно использовать?
2. Почему сравнимость по фиксированному модулю является отношением эквивалентности?
3. Почему пересекающиеся классы вычетов совпадают?
4. Почему классов ровно m, хотя целых чисел бесконечно много?
5. Чем полная система вычетов отличается от произвольного набора m целых?
6. Какое условие делает аффинное преобразование полной системы снова полным?
7. Почему арифметические операции над классами не зависят от представителей?
8. Как меняется модуль при сокращении общего множителя?
9. Почему нельзя произвольно сокращать показатель степени?
10. При каком условии определено отображение $[a]_m \mapsto [a]_d$?
11. Чем различаются задачи, в которых используются НОК и НОД модулей?
12. Почему схема Горнера и признаки делимости сохраняют нужный остаток?

Литература к теме

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии**. СПб.: Лань, 2020. §§ 4.1–4.2, с. 102–106: определения, свойства сравнений и полные системы вычетов; § 4.4, с. 112–114: переход к операциям над классами.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory**. 2nd ed. Pearson Education, 2006. § 3.3, с. 70–75: арифметика сравнений и ограничения деления.