ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 6

КОЛЬЦО ВЫЧЕТОВ И ОБРАТИМЫЕ ЭЛЕМЕНТЫ

Цель лекции	Построить арифметику классов вычетов и доказать критерии обратимости, существования делителей нуля и образования поля.
Результат обучения	Выполнять операции в кольце вычетов, читать таблицы операций, находить обратные элементы и объяснять, когда допустимо деление.
Предварительная подготовка	Классы вычетов и свойства сравнений, алгоритм Евклида и тождество Безу, взаимно простые числа.

Аудиторная нагрузка: 1 академический час. На занятии рассматриваются построение кольца, таблицы операций и критерий обратимости. Подсчёт прообразов, дополнительные доказательства и самостоятельные задачи дополняют основное содержание.

План лекции

1. Операции над классами и свойства кольца.
2. Таблицы сложения и умножения.
3. Обратимые элементы и алгоритм их вычисления.
4. Делители нуля и сокращение множителей.
5. Кольца вычетов по простому и составному модулям.
6. Приведённая система вычетов и связь с криптографией.

1 Арифметика классов вычетов

В предыдущей лекции целые числа были разбиты на классы с одинаковым остатком. Теперь на этих классах вводятся операции. Главный вопрос состоит в том, сохраняет ли такая арифметика привычные правила, включая возможность деления.

Всюду в этой лекции $m \geq 2$ — целое число. Обозначим

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \dots, [m-1]_m\}.$$

Сложение и умножение определим через представителей:

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

Корректность определения. Пусть $a' = a + km$ и $b' = b + \ell m$. Тогда $(a'+b') - (a+b) = (k+\ell)m$, а

$$a'b' - ab = m(kb + \ell a + k\ell m).$$

Обе разности делятся на m, поэтому результат не зависит от выбора представителей. Это обязательная проверка: одна и та же пара классов должна давать одну и ту же сумму и одно и то же произведение.

Для вычислений удобно представлять класс единственным числом от 0 до $m-1$. Тогда действия выполняются в два шага: обычная операция над целыми и взятие неотрицательного остатка. Например, по модулю 8 получаем $[6]+[5]=[3]$, $[6][5]=[6]$. При фиксированном модуле индекс у класса далее можно опускать.

1.1 Почему получается кольцо

Теорема. Множество $\mathbb{Z}_m$ с указанными операциями является коммутативным кольцом с единицей.

Это означает, что сложение ассоциативно и коммутативно, имеет нулевой элемент, а каждый элемент имеет противоположный. Умножение также ассоциативно и коммутативно, имеет единицу и распределяется относительно сложения.

Доказательство. Для любых классов $[a], [b], [c]$ ассоциативность сложения следует из

$$([a] + [b]) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b] + [c]).$$

Аналогично переносится ассоциативность умножения. Равенства $a + b = b + a$ и $ab = ba$ дают коммутативность. Дистрибутивность выражается равенством

$$[a]([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c].$$

Нулевым элементом служит $[0]$, единицей — $[1]$. Противоположный к $[a]$ элемент равен $[-a] = [m - a]$, поскольку $[a] + [-a] = [0]$. Все свойства доказаны. Условие $m \geq 2$ обеспечивает $[0] \neq [1]$.

Вычитание поэтому всегда определено: $[a] - [b] = [a - b]$. Существование противоположного элемента ещё не означает существования обратного по умножению. Например, в $\mathbb{Z}_8$ противоположным к $[2]$ является $[6]$, но обратного к $[2]$ нет.

2 Таблицы операций

Таблица операции содержит по одному представителю каждого класса в заголовках строк и столбцов. В пересечении строки a и столбца b записывают остаток суммы или произведения. Для небольшого модуля таблица позволяет увидеть свойства кольца непосредственно.

Сложение по модулю 4

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Умножение по модулю 4

×	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

В таблице сложения каждая строка содержит все четыре остатка ровно по одному разу. Причина общая для любого модуля: из $a + x \equiv a + y \pmod{m}$ следует $x \equiv y \pmod{m}$. Прибавление одного класса переставляет все классы.

Таблица умножения устроена иначе. Строки 1 и 3 также содержат все остатки, а строка 2 содержит лишь 0 и 2, каждый дважды. В ней отсутствует 1, поэтому обратного к $[2]_4$ нет. Кроме того, $[2]_4[2]_4 = [0]_4$: произведение двух ненулевых классов может оказаться нулевым.

Симметрия обеих таблиц относительно главной диагонали отражает коммутативность. Строка 0 при сложении и строка 1 при умножении воспроизводят заголовки столбцов, что показывает роль нейтральных элементов.

3 Обратимые элементы

Определение. Класс $[a] \in \mathbb{Z}_m$ называется **обратимым**, если существует класс $[u]$ с $[a][u] = [1]$. Этот класс обозначают $[a]^{-1}$. На уровне представителей требуется решить сравнение

$$au \equiv 1 \pmod{m}.$$

Критерий обратимости. Класс $[a]_m$ обратим ровно при $\gcd(a, m) = 1$.

Необходимость. Если $au \equiv 1 \pmod{m}$, то $au - mk = 1$ для некоторого целого k. Любой общий делитель a и m делит левую часть и потому делит 1. Следовательно, НОД равен 1.

Достаточность. Если $\gcd(a, m) = 1$, тождество Безу даёт целые s, t такие, что $as + mt = 1$. Переходя к сравнению по модулю m, получаем $as \equiv 1$. Значит, обратный класс существует и равен $[s]_m$.

Единственность. Пусть $[a][u] = [1]$ и $[a][v] = [1]$. Тогда

$$[u] = [u]([a][v]) = ([u][a])[v] = [v].$$

Единственность относится к классу: целых решений u бесконечно много, и все они отличаются на кратное m. Среди чисел $0, \dots, m-1$ обратный представитель единственен.

По модулю 15 обратимы ровно следующие классы:

$$U(15) = \{[1], [2], [4], [7], [8], [11], [13], [14]\}.$$

a	**1**	**2**	**4**	**7**	**8**	**11**	**13**	**14**
a^{-1}	1	8	4	13	2	11	7	14

Таблица симметрична по смыслу: если 2 обратно к 8, то 8 обратно к 2. Некоторые классы обратны сами себе, например $4^2 \equiv 1 \pmod{15}$. Обратный класс в общем случае не совпадает с противоположным: по модулю 15 для 2 противоположный представитель равен 13, а обратный — 8.

3.1 Вычисление расширенным алгоритмом Евклида

Найдём обратный к $a = -29$ по модулю $m = 84$. Сначала нормализуем число: $A = -29 \bmod 84 = 55$. НОД не изменяется при замене представителя. Выполним деления:

$$84 = 55 + 29, \qquad 55 = 29 + 26, \qquad 29 = 26 + 3,$$
$$26 = 8 \cdot 3 + 2, \qquad 3 = 2 + 1, \qquad 2 = 2 \cdot 1.$$

Последний ненулевой остаток равен 1, поэтому обратимость установлена. Обратная подстановка даёт

$$1 = 3 - 2 = 9 \cdot 3 - 26 = 9 \cdot 29 - 10 \cdot 26,$$

$$1 = 19 \cdot 29 - 10 \cdot 55 = 19 \cdot 84 - 29 \cdot 55.$$

Коэффициент при $A = 55$ равен $s = -29$, поэтому наименьший неотрицательный обратный представитель $I = s \bmod 84 = 55$. Проверка: $(-29) \cdot 55 = -1595 = 1 - 19 \cdot 84$.

При решении $-29x \equiv 19 \pmod{84}$ умножаем обе части на обратный класс:

$$x \equiv 55 \cdot 19 \equiv 37 \pmod{84}.$$

Подстановка даёт $-29 \cdot 37 - 19 = -1092 = -13 \cdot 84$. Ответ можно записать как один класс $[37]_{84}$ или как все целые $x = 37 + 84k$.

Практический порядок вычисления обратного элемента таков: нормализовать a, вычислить НОД и коэффициенты Безу, проверить НОД, привести соответствующий коэффициент по модулю m и проверить произведение. Если НОД больше 1, коэффициент Безу не является обратным.

4 Делители нуля и допустимость сокращения

Определение. Ненулевой класс $[a]$ называется **делителем нуля**, если существует ненулевой класс $[b]$ с $[a][b] = [0]$. Сам нулевой класс в этом определении к делителям нуля не относят.

Теорема. Для $1 \le a < m$ класс $[a]_m$ является делителем нуля тогда и только тогда, когда $\gcd(a, m) > 1$.

Доказательство. Пусть $g = \gcd(a, m) > 1$. Число $b = m/g$ удовлетворяет $1 \le b < m$, а

$$ab = a\frac{m}{g} = m\frac{a}{g} \equiv 0 \pmod{m}.$$

Оба класса ненулевые, следовательно, $[a]$ — делитель нуля. Обратно, если НОД равен 1, существует обратный класс. Из $[a][b] = [0]$ после умножения на $[a]^{-1}$ получаем $[b] = [0]$. Ненулевого партнёра быть не может.

Таким образом, каждый ненулевой класс в $\mathbb{Z}_m$ относится ровно к одному из двух видов: он либо обратим, либо является делителем нуля. Этот вывод доказан для кольца вычетов; переносить его на произвольное бесконечное кольцо без доказательства нельзя.

Сокращение. При $\gcd(a, m) = 1$ равенство $[a][x] = [a][y]$ позволяет заключить $[x] = [y]$. Если $g > 1$, полное сокращение с сохранением модуля неверно. В общем случае

$$ax \equiv ay \pmod{m} \quad \Leftrightarrow \quad x \equiv y \pmod{m/g}.$$

Действительно, запишем $a = ga_1$, $m = gm_1$ с $\gcd(a_1, m_1) = 1$. Тогда $m \mid a(x - y)$ равносильно $m_1 \mid a_1(x - y)$ и далее $m_1 \mid (x - y)$. Для примера возьмём $2 \cdot 1 \equiv 2 \cdot 5 \pmod{8}$. После сокращения получится $1 \equiv 5 \pmod{4}$, хотя по модулю 8 эти числа не сравнимы.

4.1 Умножение как отображение классов

Для фиксированного a рассмотрим отображение $T_a([x]) = [ax]$. Оно взаимно однозначно ровно тогда, когда $[a]$ обратим. В этом случае обратное отображение имеет вид $T_{a^{-1}}$. Если же НОД больше 1, разные входные классы могут давать один результат.

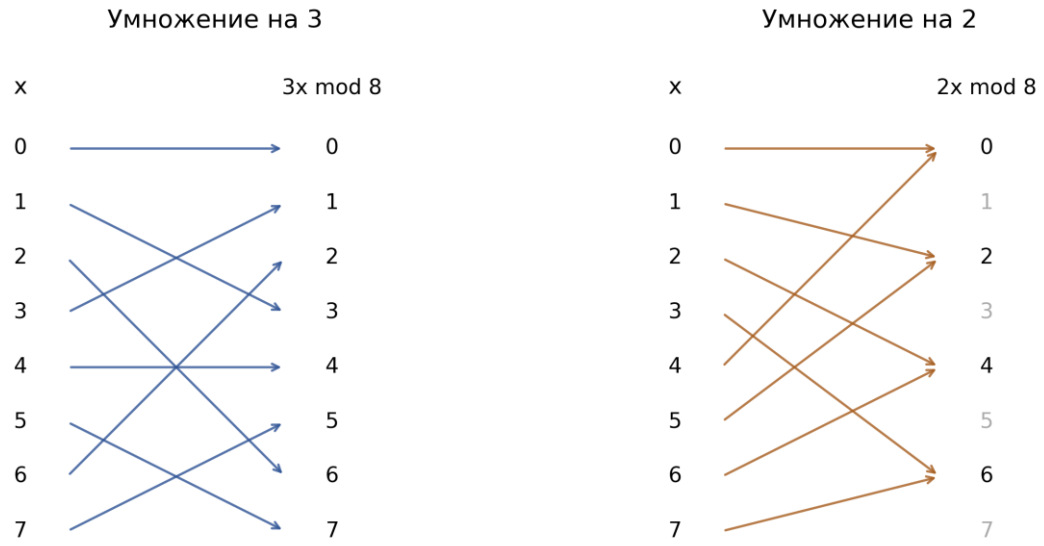


Рисунок 1. По модулю 8 умножение на 3 переставляет все классы. Умножение на 2 даёт четыре выходных класса, причём каждый получается из двух входных.

Дополнительно можно точно посчитать повторения. Из доказанной формулы сокращения следует: $T_a([x]) = T_a([y])$ тогда и только тогда, когда $x - y$ кратно m/g. Поэтому каждому достигаемому значению соответствуют ровно g классов, а различных значений всего m/g.

В частности, все классы, переходящие в нуль, имеют представителей

$$0, \frac{m}{g}, 2\frac{m}{g}, \ldots, (g-1)\frac{m}{g}.$$

Этот набор называют **аннулятором** класса $[a]$. В нём g элементов, включая нулевой. Для $a = 8, m = 12$ получаем $g = 4$ и аннулятор $\{[0], [3], [6], [9]\}$.

Пример. Сравнение $8x \equiv 4 \pmod{12}$ сводится к $2x \equiv 1 \pmod{3}$, то есть к $x \equiv 2 \pmod{3}$. По исходному модулю имеются четыре решения: $2,5,8,11$. Сравнение $8x \equiv 2 \pmod{12}$ решений не имеет, поскольку его левая часть делится на 4, а правая не делится. Отсутствие обратного элемента допускает как отсутствие решений, так и несколько решений; общий алгоритм линейных сравнений будет изучаться отдельно.

5 Когда кольцо вычетов является полем

Поле — коммутативное кольцо с различными нулём и единицей, в котором каждый ненулевой элемент обратим. В поле можно однозначно делить на любой ненулевой элемент.

Теорема. При $m \geq 2$ кольцо $\mathbb{Z}_m$ является полем тогда и только тогда, когда m — простое число.

Доказательство. Если $m = p$ простое, всякое a с $1 \leq a < p$ взаимно просто с p. По критерию обратимости каждый ненулевой класс обратим. Если же $m = uv$ составное, где $1 < u, v < m$, то $[u]$ и $[v]$ ненулевые, но $[u][v] = [m] = [0]$. В поле это невозможно: умножение на обратный к $[u]$ дало бы $[v] = [0]$.



Рисунок 2. В поле вычетов по модулю 7 обратимы все ненулевые классы. По модулю 8 классы 2, 4 и 6 являются делителями нуля.

Простой модуль меняет именно возможность умножительного обращения. Сложение и вычитание корректны также при составном модуле. Например, по модулю 8 уравнение $x + 6 = 3$ имеет единственное решение $x = 5$, хотя $\mathbb{Z}_8$ полем не является.

При записи «дроби» по модулю m знаменатель должен обозначать обратимый класс. Так, $3/5$ по модулю 8 означает $[3][5]^{-1} = [3][5] = [7]$. Символ $1/2$ по модулю 8 такого смысла не имеет. Обычное вещественное деление с последующим взятием остатка здесь не используется.

6 Приведённая система вычетов

Множество всех обратимых классов обозначим $U(m) = \mathbb{Z}_m^{\times}$. Если из каждого такого класса взять по одному целому представителю, получится **приведённая система вычетов**. Стандартный выбор — числа $1 \le a < m$, взаимно простые с m.

Например, по модулю 12 приведённая система имеет вид $1,5,7,11$. В ней четыре элемента. По определению функции Эйлера

$$|U(m)| = \varphi(m), \qquad m \ge 2.$$

Для числа $\varphi(m)$ достаточно посчитать взаимно простые представители; умножать их или находить все обратные не требуется. В практической работе №6 этот подсчёт сопоставляется с вычислением по разложению модуля.

6.1 Умножение обратимых классов

Произведение двух обратимых классов также обратимо:

$$([a][b])^{-1} = [b]^{-1}[a]^{-1}.$$

Проверка следует из ассоциативности: $([a][b])([b]^{-1}[a]^{-1}) = [1]$. Единица принадлежит $U(m)$, а обратный к элементу этого множества также принадлежит ему. Следовательно, $U(m)$ образует коммутативную группу относительно умножения. Здесь

нужны только перечисленные свойства; общий язык групп будет развит в следующем разделе курса.

Для $U(8) = \{[1], [3], [5], [7]\}$ каждый элемент обратен самому себе. Множество обратимых классов не обязано быть замкнуто относительно сложения: $[1] + [3] = [4]$ по модулю 8, а $[4]$ не обратим.

6.2 Обратимость аффинного преобразования

Рассмотрим учебное преобразование $E_{a,b}([x]) = [ax + b]$. Сдвиг на b всегда обратим, поэтому всё преобразование обратимо ровно при $\gcd(a, m) = 1$. Если I — обратный представитель к a, восстановление задаётся формулой

$$D_{a,b}([y]) = [I(y - b)].$$

Тогда $D_{a,b}(E_{a,b}([x])) = [Iax] = [x]$. По модулю 26 при $a = 5$, $b = 7$ имеем $I = 21$, поскольку $5 \cdot 21 = 105 \equiv 1$. Для $x = 9$ получаем $y = 52 \bmod 26 = 0$, а восстановление даёт $21(0 - 7) \bmod 26 = 9$.

Если взять необратимый множитель $a = 2$, то входы 0 и 13 дадут один выход b по модулю 26. Однозначное восстановление станет невозможным. Этот пример показывает математическую роль взаимной простоты. Само наличие обратного преобразования обеспечивает корректность восстановления, но не доказывает стойкость шифра.

7 Задачи для самостоятельного решения

1. В $\mathbb{Z}_9$ вычислите $[7] + [8]$, $[7][8]$, противоположный и обратный к $[7]$ классы. Подтвердите результаты.
2. Найдите все обратимые классы в $\mathbb{Z}_{10}$ и обратные к ним. Отдельно перечислите ненулевые делители нуля.
3. Найдите обратный к -11 по модулю 35 с помощью тождества Безу. Решите $-11x \equiv 9 \pmod{35}$.
4. Найдите аннулятор $[6]$ в $\mathbb{Z}_{18}$ и все решения $6x \equiv 12 \pmod{18}$. Сколько разных значений принимает $6x \bmod 18$?
5. По модулю 11 рассмотрите $E(x) = 7x + 3$. Найдите формулу восстановления и проверьте её для $x = 8$.
6. Докажите, что в конечном кольце вычетов строка умножения на a содержит все классы без повторений ровно при $\gcd(a, m) = 1$.

Контрольные вопросы

1. Почему операции над классами требуют проверки независимости от представителей?
2. Какие свойства входят в определение коммутативного кольца с единицей?
3. Чем отличаются противоположный и обратный элементы?
4. Как тождество Безу доказывает критерий обратимости?
5. В каком смысле обратный элемент единственен?
6. Почему ненулевой класс может давать нуль при умножении на другой ненулевой класс?
7. Как изменяется модуль при сокращении множителя, не взаимно простого с модулем?
8. Сколько классов содержит аннулятор и входит ли в него нулевой класс?
9. При каком условии кольцо вычетов является полем?
10. Почему приведённая система имеет $\varphi(m)$ элементов?
11. Почему обратимые классы образуют группу по умножению, но не обязаны быть замкнуты по сложению?
12. Как критерий обратимости связан с однозначным восстановлением аффинного преобразования?

Литература

1. Мартынов Л. М. Алгебра и теория чисел для криптографии. СПб.: Лань, 2020. §4.4, с. 112–114; §4.3 — приведённые системы и функция Эйлера.
2. Trappe W., Washington L. C. Introduction to Cryptography with Coding Theory. 2nd ed. Pearson Education, 2006. §3.3, в особенности §§3.3.1–3.3.2, с. 70–75 — сравнения, обращение и смысл дробей по модулю.

Материал изложен по указанным разделам предоставленных изданий. Доказательства развёрнуты для занятий; числовые примеры, иллюстрации и самостоятельные задания составлены для данного комплекта.