ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 1

КРИПТОГРАФИЯ И ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ

Цель лекции	Обосновать свойства делимости и теорему о делении с остатком, затем применить их к вычислениям и учебному шифру.
Результат обучения	записывать определение делимости и доказывать свойства через это определение; находить и проверять неполное частное и неотрицательный остаток; объяснять особенности деления отрицательного целого числа; применять остатки в вычислениях и проверять обратимость учебного шифрования.
Предварительная подготовка	Предварительно нужны множества целых чисел, функции, неравенства и понятие доказательства. Теория сравнений и алгебраические структуры будут изучаться далее; здесь используется только необходимая начальная терминология.

Объём: 1 академический час. Развёрнутые пояснения и дополнительные задачи предназначены также для самостоятельного чтения.

План лекции

1. Математическая модель шифра и условие корректности.
2. Делимость целых чисел, свойства и доказательства.
3. Теорема о делении с остатком.
4. Отрицательные числа и геометрический смысл остатка.
5. Вычисления через остатки и кратные на отрезке.
6. Учебный шифр сдвига и обратное восстановление.
7. Решение задач и самостоятельная работа.

1 Математическая модель шифра

Математическая основа шифрования начинается с точного описания множества сообщений и допустимых операций над ними. В этой лекции мы свяжем простую модель шифра с арифметикой целых чисел, докажем свойства делимости и теорему о делении с остатком, затем применим их к вычислениям и шифру сдвига.

Обозначим множество сообщений через $\mathcal{M}$, множество шифртекстов через $\mathcal{C}$, множество ключей через $\mathcal{K}$. Для каждого фиксированного ключа k в учебной детерминированной модели заданы функции шифрования и расшифрования:

$$E_k\colon \mathcal{M} \to \mathcal{C}, \qquad D_k\colon \mathcal{C} \to \mathcal{M}.$$

Условие корректности требует восстановления любого допустимого сообщения:

$$D_k\big(E_k(m)\big) = m \qquad \text{для всех } m \in \mathcal{M}.$$

Почему шифрование должно быть инъективным при фиксированном ключе? Пусть два сообщения дали один шифртекст. Применив к равенству функцию расшифрования, получим

$$E_k(m_1) = E_k(m_2) \;\Rightarrow\; D_k\big(E_k(m_1)\big) = D_k\big(E_k(m_2)\big) \;\Rightarrow\; m_1 = m_2.$$

Следовательно, в этой модели разные сообщения не могут сливаться в один результат. Если множества сообщений и шифртекстов совпадают и конечны, такое преобразование является перестановкой этого множества. Вероятностные схемы шифрования требуют более общей модели и будут обсуждаться отдельно.

2 Делимость целых чисел

В этой лекции используем следующее соглашение: в записи $d \mid a$ делитель d ненулевой. Для $a, d \in \mathbb{Z}$, $d \neq 0$, определение имеет вид

$$d \mid a \quad \Leftrightarrow \quad \text{существует } t \in \mathbb{Z} \text{ такое, что } a = dt.$$

Число d называют делителем a, а число a — кратным d. Если целого множителя нет, записывают $d \nmid a$. В определении существенна целочисленность множителя: равенство $a = d(a/d)$ в рациональных числах само по себе делимость не доказывает.

Пример 1. Имеем $7 \mid 84$, поскольку $84 = 7 \cdot 12$. Также $-7 \mid 84$, поскольку $84 = (-7)(-12)$, и $7 \mid -84$, поскольку $-84 = 7(-12)$.

Пример 2. Число 7 не делит 85: между соседними кратными $7 \cdot 12 = 84$ и $7 \cdot 13 = 91$ других кратных нет. Позднее этот факт выразится ненулевым остатком.

Для любого ненулевого d выполняется $d \mid 0$, так как $0 = d \cdot 0$. Это утверждение касается делимости нуля на ненулевое число. Деление на нуль не определяется; запись с нулевым делителем в принятом соглашении не используется.

Если ищутся все **положительные** делители 24, ответ равен $1,2,3,4,6,8,12,24$. Все ненулевые целые делители получаются добавлением противоположных чисел. В задаче всегда нужно уточнять, какое множество делителей требуется.

2.1 Свойства отношения делимости

1. **Рефлексивность для ненулевых чисел:** $a \mid a$, так как $a = a \cdot 1$.
2. **Транзитивность:** из $a \mid b$ и $b \mid c$ следует $a \mid c$.
3. **Сохранение при умножении:** из $d \mid a$ следует $d \mid au$ при любом $u \in \mathbb{Z}$.
4. **Линейные комбинации:** если $d \mid a$ и $d \mid b$, то $d \mid ua + vb$ для любых целых u, v.
5. **Ограничение величины:** если $d \mid a$ и $a \neq 0$, то $|d| \leq |a|$.

На положительных целых числах делимость задаёт частичный порядок. В частности, если $a \mid b$ и $b \mid a$, то $a = b$. Среди ненулевых целых чисел равенство может нарушаться из-за знака: $2 \mid -2$ и $-2 \mid 2$, хотя $2 \neq -2$. Поэтому при переходе от положительных чисел ко всем целым условия теорем нужно проверять заново.

2.2 Доказательства свойств и первые задачи

Транзитивность. Пусть $b = as$ и $c = bt$, где s, t целые. Подстановка даёт $c = a(st)$. Произведение st целое, следовательно, по определению $a \mid c$.

Линейная комбинация. Из $d \mid a$ и $d \mid b$ имеем $a = d\alpha$ и $b = d\beta$. Тогда

$$ua + vb = u(d\alpha) + v(d\beta) = d(u\alpha + v\beta).$$

Множитель в скобках целый, значит, $d \mid ua + vb$. При $u = v = 1$ получаем делимость суммы, а при $u = 1$, $v = -1$ — делимость разности. Эта идея понадобится при доказательстве корректности алгоритма Евклида.

Ограничение величины делителя. Если $a = dt \neq 0$, то t — ненулевое целое число, поэтому $|t| \geq 1$. Отсюда $|a| = |d||t| \geq |d|$.

Задача 1. Известно, что $9 \mid a$ и $9 \mid b$. Доказать, что $9 \mid 5a - 2b$.

Запишем $a = 9u$, $b = 9v$. Тогда $5a - 2b = 9(5u - 2v)$, что и доказывает утверждение. Например, при $a = 45$ и $b = 72$ получаем $5a - 2b = 81$.

Задача 2. Доказать, что произведение двух последовательных целых чисел чётно.

Каждое целое число имеет вид $n = 2q$ или $n = 2q + 1$. В первом случае $n(n+1) = 2q(n+1)$, во втором — $n(n+1) = 2n(q+1)$. В обоих случаях выделен целый множитель 2. Таким образом, $2 \mid n(n+1)$ для всех целых n, включая отрицательные.

Задача 3. Верно ли, что из $d \mid ab$ следует $d \mid a$ или $d \mid b$?

В такой общей формулировке утверждение неверно. Например, $6 \mid 2 \cdot 3$, но $6 \nmid 2$ и $6 \nmid 3$. Контрпример опровергает общее утверждение. Для простого делителя соответствующее свойство будет доказано в следующем разделе курса о простых числах.

Дополнительная задача. Для $s \geq 1$ и $a \neq b$ доказать $a - b \mid a^s - b^s$. При $s = 1$ утверждение очевидно. Для $s \geq 2$ используем тождество

$$a^s - b^s = (a - b)(a^{s-1} + a^{s-2}b + \cdots + ab^{s-2} + b^{s-1}).$$

Множитель в скобках является суммой s целочисленных слагаемых; при $s = 2$ это $a + b$. Следовательно, тождество непосредственно доказывает делимость.

3 Теорема о делении с остатком

Теорема. Для любого целого a и любого положительного целого b существуют единственные целые числа q и r такие, что

$$a = bq + r, \qquad 0 \leq r < b.$$

Число q называется неполным частным, число r — остатком. В этой теме делитель в алгоритме берётся положительным. Обобщение на отрицательный делитель приводится далее.

Существование. По определению целой части положим

$$q = \lfloor a/b \rfloor.$$

Тогда $q \leq a/b < q + 1$. Умножение на положительное b сохраняет знаки неравенств:

$$bq \leq a < bq + b.$$

Вычтем bq и обозначим $r = a - bq$. Получим $0 \leq r < b$, причём r целое. Следовательно, требуемое представление существует.

Единственность. Предположим, что имеются два представления:

$$a = bq + r = bq' + r', \qquad 0 \leq r < b, \quad 0 \leq r' < b.$$

После вычитания находим $b(q - q') = r' - r$. Правая часть по модулю меньше b. Если целое число $q - q'$ ненулевое, левая часть имеет модуль не меньше b, что невозможно. Значит, $q = q'$, а затем $r = r'$.

Следствие. При $b > 0$ условие $b \mid a$ равносильно нулевому остатку. Действительно, при $r = 0$ имеем $a = bq$. Обратно, если $a = bt$, то пара $(t, 0)$ удовлетворяет теореме и по единственности совпадает с (q, r).

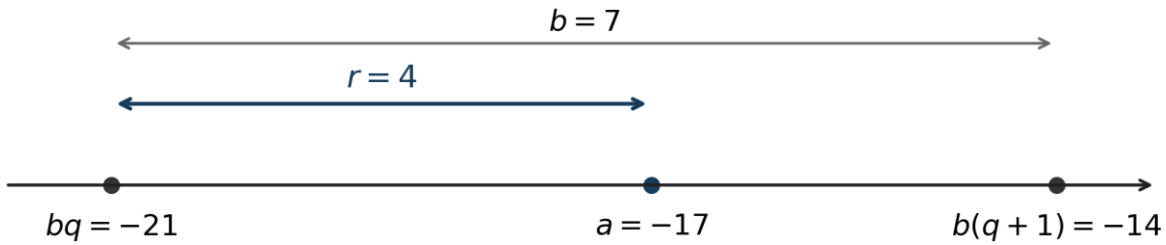
Проверка результата всегда состоит из двух действий: восстановить исходное число по равенству $a = bq + r$ и проверить границы $0 \le r < b$. Одного равенства недостаточно: например, $29 = 6 \cdot 3 + 11$ верно, но 11 не является остатком при делении на 6.

4 Отрицательные числа и смысл остатка

Рассмотрим $a = -17$ и $b = 7$. Неполное частное определяется округлением вниз:

$$q = \lfloor -17/7 \rfloor = -3, \qquad r = -17 - 7(-3) = 4.$$

Следовательно, $-17 = 7(-3) + 4$. Запись $-17 = 7(-2) - 3$ также является верным равенством, но её последний член отрицателен и не удовлетворяет принятому определению остатка.



Число минус семнадцать лежит между соседними кратными семи минус двадцать один и минус четырнадцать. Расстояние от левого кратного равно четырём.

Рисунок 1. Остаток как расстояние от ближайшего кратного слева до исходного числа.

Делимое и делитель	Представление	Неполное частное и остаток
137 и 12	$137 = 12 \cdot 11 + 5$	$q = 11, r = 5$
-137 и 12	$-137 = 12(-12) + 7$	$q = -12, r = 7$
-144 и 12	$-144 = 12(-12) + 0$	$q = -12, r = 0$
0 и 12	$0 = 12 \cdot 0 + 0$	$q = 0, r = 0$

Связь остатков противоположных чисел. Если $a = bq + r$ и $0 < r < b$, то

$$-a = b(-q - 1) + (b - r).$$

Поэтому остаток для $-a$ равен $b - r$. Если исходный остаток нулевой, остаток противоположного числа тоже равен нулю. Подстановка $r = 0$ в выражение $b - r$ дала бы b, что нарушает верхнюю границу; этот случай следует выделять отдельно.

Отрицательный делитель. Для $b < 0$ сначала делят на $|b|$: $a = |b|q_0 + r$. Тогда $a = b(-q_0) + r$ и $0 \le r < |b|$. Например, $-17 = (-7) \cdot 3 + 4$. В практической работе все делители положительны, чтобы соглашение совпадало с используемой операцией Python.

5 Вычисления через остатки

Обозначим неотрицательный остаток от деления a на положительное b через $\mathrm{rem}_b(a)$. Другая распространённая запись — $a \bmod b$. Это число из множества $\{0, 1, \ldots, b - 1\}$. Если два числа отличаются на кратное b, то их остатки равны. Запись $a \equiv c \pmod b$ выражает условие $b \mid a - c$; подробно сравнения будут изучаться в лекции 5.

Пусть $a = bq + r$, $c = bs + t$, где $0 \le r, t < b$. Тогда

$$a + c = b(q + s) + (r + t),$$
$$ac = b(bqs + qt + rs) + rt.$$

Следовательно, для суммы и произведения достаточно вычислить остатки меньших выражений:

$$\operatorname{rem}_b(a + c) = \operatorname{rem}_b(r + t), \qquad \operatorname{rem}_b(ac) = \operatorname{rem}_b(rt).$$

Остатки $r + t$ и rt при необходимости уменьшаются повторно: эти числа могут оказаться не меньше b. Аналогично обрабатываются разность и любые многочлены с целыми коэффициентами.

Пример 1. Найдём остаток произведения $37 \cdot 48$ по модулю 11. Остатки обоих множителей равны 4. Получаем $4 \cdot 4 = 16 = 11 + 5$, поэтому искомый остаток равен 5. Проверка: $1776 = 11 \cdot 161 + 5$.

Пример 2. Пусть $a = 53$, $b = 9$. Остаток a равен 8. Для $a^2 + 3a + 5$ получаем

$$\operatorname{rem}_9(53^2 + 3 \cdot 53 + 5) = \operatorname{rem}_9(8^2 + 3 \cdot 8 + 5) = \operatorname{rem}_9(93) = 3.$$

Прямое вычисление подтверждает результат: $2973 = 9 \cdot 330 + 3$.

Кратные на отрезке. Условие $L \le bt \le U$ при $b > 0$ равносильно $\lceil L/b \rceil \le t \le \lfloor U/b \rfloor$. Поэтому число кратных равно

$$N = \max\{0, \lfloor U/b \rfloor - \lceil L/b \rceil + 1\}.$$

Например, на отрезке $[-17, 38]$ кратные 7 получаются при $t = -2, -1, 0, 1, 2, 3, 4, 5$. Их восемь: $-14, -7, 0, 7, 14, 21, 28, 35$.

6 Приложение к учебному шифру сдвига

Занумеруем латинские буквы от A до Z числами от 0 до 25. При ключе $k \in \{0, 1, \ldots, 25\}$ определим

$$E_k(m) = \operatorname{rem}_{26}(m + k), \qquad D_k(c) = \operatorname{rem}_{26}(c - k).$$

Все сообщения, ключи и результаты в этом примере представлены остатками. Операции сложения и вычитания выполняются с последующим приведением к диапазону от 0 до 25. Это пример «платформы шифрования» — множества с точно заданными операциями.

Доказательство корректности. По определению остатка существует целое q, для которого $E_k(m) = m + k - 26q$. Поэтому

$$D_k\big(E_k(m)\big) = \operatorname{rem}_{26}(m - 26q) = m,$$

поскольку исходное сообщение уже лежит между 0 и 25. Таким образом, условие корректности проверено для всех сообщений и всех допустимых ключей, а не только для отдельных примеров.

Пример. Для буквы X имеем $m = 23$. При $k = 7$ получаем $23 + 7 = 30 = 26 + 4$, то есть шифртекстом служит буква E. При расшифровании $4 - 7 = -3$; неотрицательный остаток равен 23, что возвращает X.



Рисунок 2. Сдвиг с ключом 7 и обратное восстановление буквы X.

Корректность и стойкость. Рассмотренный шифр корректен, но пространство ключей содержит всего 26 элементов. Все ключи можно перебрать, поэтому пример предназначен для понимания арифметики и обратимости. Из доказательства правильного расшифрования не следует доказательство безопасности.

Почему нельзя произвольно выбирать преобразование? Рассмотрим $F(m) = \mathrm{rem}_{26}(2m)$. Получаем

$$F(0) = 0, \qquad F(13) = 0.$$

Одному результату соответствуют два сообщения. Значит, функция неинъективна и для неё невозможно однозначное расшифрование на всём множестве из 26 сообщений. Позднее это будет объяснено отсутствием обратного элемента у 2 по модулю 26.

В RSA также возникает возведение числа в степень с последующим вычислением остатка; в конечных полях используются операции над классами многочленов. Общий принцип курса — сначала обосновать свойства арифметической среды, затем строить и исследовать преобразования сообщений.

7 Закрепление и самостоятельная работа

Разобранная задача. Найти все целые x, для которых $7 \mid 3x + 2$.

Представим $x = 7q + r$, где $r \in \{0,1,\dots,6\}$. Тогда $3x + 2 = 21q + 3r + 2$, и вопрос зависит только от r. Для семи возможных остатков числа $3r + 2$ равны $2,5,8,11,14,17,20$. Только при $r = 4$ получается кратное 7. Следовательно,

$$x = 7q + 4, \qquad q \in \mathbb{Z}.$$

Проверка подстановкой: $3(7q + 4) + 2 = 7(3q + 2)$. Мы доказали и необходимость, и достаточность найденного условия. В дальнейшем такие задачи будут решаться общими методами линейных сравнений.

Контрольные вопросы

1. Почему в определении $d \mid a$ множитель должен быть целым?
2. Как записать доказательство транзитивности делимости?
3. Почему общий делитель двух чисел делит любую их целую линейную комбинацию?
4. Почему проверки равенства $a = bq + r$ недостаточно без границ остатка?
5. Найдите частное и остаток для -173 при делении на 12.
6. Как связан остаток a с остатком $-a$? Когда нужна отдельная оговорка?
7. Найдите остаток $29 \cdot 35$ по модулю 8, уменьшая множители заранее.
8. Сколько кратных 6 находится на отрезке $[-20,25]$?
9. Почему существование расшифрования требует инъективности шифрования в рассматриваемой модели?
10. Чем доказательство корректности учебного шифра отличается от обоснования его стойкости?

Дополнительные задачи. Докажите, что $a \mid b$ и $a \mid b + c$ влекут $a \mid c$ при $a \neq 0$. Найдите все целые x, для которых $5 \mid 2x + 1$. Для положительного делителя b самостоятельно выведите формулу числа его кратных на произвольном целочисленном отрезке.

Литература к лекции

- Мартынов Л. М. Алгебра и теория чисел для криптографии. Лань, 2020. Глава 3, особенно теорема 3.1 о делении с остатком; §§4.1–4.2 для дальнейшего чтения.
- Kraft J. S., Washington L. C. An Introduction to Number Theory with Cryptography. 2nd ed. CRC Press, 2018. §§2.1 и 2.5 из предоставленного фрагмента.
- Paar C., Pelzl J. Understanding Cryptography. Springer, 2010. Глава 1.
- Boneh D., Shoup V. A Graduate Course in Applied Cryptography. Version 0.6, 2023. §2.1 для углублённого изучения определения шифра.

Следующая лекция посвящена НОД, НОК, тождеству Безу и алгоритму Евклида. Её ключевой шаг будет основан на равенстве множеств общих делителей пары чисел и пары, полученной после деления с остатком.