Арифметика по колу

Розділ 2. Сучасні шифри · Тема 2.2

Чому шифри використовують остачу. Модуль, циклічні зсуви, обернення дій, зв’язок із шифрами Цезаря та Віженера.

Справа «Годинник, що зберігає секрет»

Кіт Буч отримав повідомлення: «Поверни стрілку на 17 годин уперед». Але циферблат має лише 12 позначок. Чому стрілка не зупиняється на числі 17? І як такий самий принцип допомагає шифрувати повідомлення?

Проблемне запитання: як виконувати обчислення, щоб результат завжди залишався всередині заданого набору чисел або символів?

Навчальна мета: навчитися обчислювати остачу, виконувати циклічні зсуви, повертатися до початкового значення та пояснювати, чому модульна арифметика потрібна криптографії.

1. Коли числа ходять по колу

Звичайна числова пряма продовжується без кінця. На годиннику після 11 знову з’являється 0 (якщо використовувати позначки 0–11). Такий рух називають циклічним.

Математична операція mod дає остачу від ділення. Наприклад: 17 mod 12 = 5, оскільки 17 = 12 · 1 + 5. Якщо почати з 9 і перейти на 8 кроків уперед, отримаємо (9 + 8) mod 12 = 5.

Початок	Зсув	Обчислення	Результат
9	+8	(9 + 8) mod 12	5
2	+15	(2 + 15) mod 12	5
3	−5	(3 − 5) mod 12	10
11	+1	(11 + 1) mod 12	0

Важливо: у математиці результат за модулем 12 зазвичай обирають із множини 0–11. На звичайному годиннику позначці 0 відповідає 12.

Мініексперимент: інтерактивний годинник

У вебверсії: циферблат із 12 поділками, вибір стартової позиції та повзунок зсуву від −24 до +24. Учень бачить формулу, анімацію руху й кінцеву позицію.

Поки працюємо з текстовим матеріалом: обчисліть, де опиниться стрілка після зсувів 7 + 10, 10 − 15, 4 + 24 (усе mod 12).

Відповіді для самоперевірки: 5, 7, 4.

2. Від годинника до абетки

Замість годинника візьмемо українську абетку з 33 літер. Кожній літері надамо номер від 0 до 32. Після останньої літери знову йде перша. Саме так працює циклічний зсув.

Для навчальних прикладів використовуємо повну українську абетку, включно з Ґ, Є, І, Ї, Й, Ь; пробіли та розділові знаки не зсуваємо.

АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ

Якщо літера має номер x, а зсув дорівнює k, номер зашифрованої літери: $E(x) = (x + k) \bmod 33$.

Щоб повернути початкову літеру, потрібно виконати протилежний зсув: $D(y) = (y - k) \bmod 33$.

Наприклад, А має номер 0. За ключа k = 3 вона перетворюється на Г (номер 3). Для розшифрування: $(3 - 3) \bmod 33 = 0$, тобто А.

3. Чому шифрування можна обернути

Коли ми додаємо зсув k за модулем n, можемо скасувати його відніманням того самого k. Це і є обернення дії: $(x + k - k) \bmod n = x$.

Але не кожна операція в модульній арифметиці має обернену. Наприклад, множення на 2 за модулем 12 не можна однозначно скасувати для всіх значень, бо 2 і 12 мають спільний дільник 2. Для множення на a обернений множник за модулем n існує лише тоді, коли НСД(a, n) = 1.

Для шифру Цезаря достатньо додавання та віднімання, тому кожен зсув можна обернути.

4. Повертаємося до шифру Цезаря

У розділі 1 ми вже зустрічали шифр Цезаря. Тепер можемо пояснити його математично. Літера не просто «перестрибує» на кілька позицій — її номер змінюється за модулем довжини абетки.

Дія	Формула	Приклад для А, k = 3
Шифрування	$(x + k) \bmod 33$	$(0 + 3) \bmod 33 = 3 \rightarrow$ Г
Розшифрування	$(y - k) \bmod 33$	$(3 - 3) \bmod 33 = 0 \rightarrow$ А

Якщо ключ дорівнює 36, результат буде таким самим, як для ключа 3, адже $36 \bmod 33 = 3$. Це означає, що різні числові значення ключа можуть давати однаковий циклічний зсув.

5. Чому Віженер — це теж арифметика по колу

У шифрі Цезаря всі літери повідомлення зсуваються на одне й те саме число. У шифрі Віженера величина зсуву змінюється від символу до символу — її задають літери ключового слова.

Для кожної позиції i: $C_i = (P_i + K_i) \bmod 33$, а для відновлення $P_i = (C_i - K_i) \bmod 33$. Тут P_i — номер літери повідомлення, K_i — номер відповідної літери ключа, C_i — номер зашифрованої літери.

Ключ повторюється, якщо коротший за повідомлення. Важливо заздалегідь домовитися, як обробляти пробіли, розділові знаки та регістр.

Приклад: повідомлення «АБВ», ключ «БВГ» (номери 1, 2, 3). Результат: БГД, бо 0+1=1, 1+2=3, 2+3=5.

Це пояснює зв’язок: Цезар — один постійний зсув, Віженер — послідовність зсувів. Обидва спираються на модульну арифметику.

6. Практичні розслідування

Практика 1. Збій міського годинника

Ситуація. Міський годинник після відключення електроенергії показує 10. Технік з’ясував, що стрілка має пройти ще 29 годин уперед, щоб відобразити правильне положення на 12-годинному циферблаті.

Завдання. Знайдіть кінцеву позицію та поясніть, чому звичайне додавання без остачі не підходить.

1. Запишіть 10 + 29.

2. Поділіть результат на 12 і знайдіть остачу.

3. Перевірте, що додавання ще 12 годин не змінює позицію.

4. Запропонуйте правило для будь-якого зсуву.

Підказки: Циферблат має 12 станів. • 39 = 12 · 3 + 3.

Самоперевірка: 3; (10 + 29) mod 12 = 3. Додавання повного кола (+12) не змінює кінцевої позиції.

Зв’язок із криптографією: Шифр з алфавітом із n символів також повертається до початку після n кроків.

Практика 2. Кур’єр і загублена літера

Ситуація. Кур’єр передає короткий сигнал через систему, яка вміє зсувати українські літери. Сигнал починається з «Я», а ключ — 4. Якщо рахувати лінійно, літер за «Я» вже немає.

Завдання. Визначте нову літеру та доведіть, що повідомлення можна відновити.

1. Знайдіть номер Я у нашій абетці (0–32).

2. Обчисліть (32 + 4) mod 33.

3. Знайдіть літеру за новим номером.

4. Відніміть ключ 4 за модулем 33 і перевірте результат.

Підказки: Я має номер 32. • 36 mod 33 = 3.

Самоперевірка: Я → Г; (3 − 4) mod 33 = 32 → Я.

Зв’язок із криптографією: Циклічність не дає зсуву «вийти за межі» абетки; обернений зсув відновлює літеру.

Практика 3. Два способи заховати записку

Ситуація. Двоє друзів сперечаються, чи справді Віженер відрізняється від Цезаря. Один використовує постійний ключ 2, інший — ключове слово «БВГ».

Завдання. Зашифруйте «АБВ» двома способами та порівняйте, як змінюється зсув.

1. Визначте номери літер «АБВ»: 0, 1, 2.

2. Для Цезаря додайте 2 до кожного номера за mod 33.

3. Для Віженера додайте відповідно 1, 2, 3.

4. Поясніть, чому другий алгоритм не має одного спільного зсуву.

Підказки: Для Цезаря отримуємо 2, 3, 4. • Для Віженера — 1, 3, 5.

Самоперевірка: Цезар: ВГҐ; Віженер: БГД.

Зв’язок із криптографією: Обидва алгоритми застосовують mod 33, але відрізняються способом вибору зсуву.

Практика 4. Повернути секрет

Ситуація. Буч знайшов зашифровану літеру «Г» та запис «ключ 4». Хтось стверджує, що розшифрування — це просто віднімання без додаткових правил.

Завдання. Перевірте це твердження, відновіть початкову літеру та поясніть, чому результат може бути від’ємним до застосування mod.

1. Визначте номер Г: 3.

2. Обчисліть $3 - 4 = -1$.

3. Знайдіть остачу -1 за модулем 33 у діапазоні 0–32.

4. Поясніть, чому це остання літера абетки.

Підказки: -1 і 32 відрізняються на 33. • $(-1) \bmod 33 = 32$.

Самоперевірка: Початкова літера — Я. Потрібне віднімання за модулем, а не звичайне віднімання номерів.

Зв’язок із криптографією: Правильне обернення важливе, щоб розшифрування працювало для всіх літер, зокрема на межі абетки.

7. Самоперевірка

Скільки дорівнює $25 \bmod 12$?

А. 1

Б. 12

В. 13

Г. 25

Відповідь для самоперевірки: А — 1, бо $25 = 12 \cdot 2 + 1$.

Який запис описує шифр Цезаря для абетки з n символів?

А. $(x + k) \bmod n$

Б. $x + k$ без обмежень

В. $x \cdot k$

Г. x / k

Відповідь для самоперевірки: А — $(x + k) \bmod n$.

Як повернути початкову літеру після зсуву $+k$?

А. Додати k ще раз

Б. Відняти k за mod n

В. Помножити на k

Г. Замінити всі літери на нулі

Відповідь для самоперевірки: Б — відняти k за mod n.

Чим Віженер відрізняється від Цезаря?

А. Він не використовує числа

Б. У ньому змінюється зсув відповідно до ключового слова

В. Він не має ключа

Г. Він працює лише з цифрами

Відповідь для самоперевірки: Б — зсув задається послідовністю літер ключа.

8. Підсумковий мініпроєкт: «Мій шифр по колу»

Створіть власний навчальний шифр для короткого повідомлення: оберіть абетку, пронумеруйте символи від 0, задайте ключ і опишіть правила шифрування та розшифрування.

Продемонструйте на прикладі трьох літер, що повідомлення відновлюється без втрат. Перевірте граничний випадок, коли зсув переходить через кінець абетки.

Критерії успіху: правильний модуль, зрозуміле правило ключа, коректне обернення, пояснення, чому такий шифр не підходить для захисту справжніх секретів.

9. Головний висновок

Модульна арифметика дозволяє працювати з обмеженим набором значень і циклічно повертатися до початку. Вона пояснює математичну основу шифрів Цезаря та Віженера: шифрування додає зсув, а розшифрування його віднімає за тим самим модулем.

Це місток від інформатики (числові операції, алгоритми, цикли, перевірка результату) до криптографії (ключі, перетворення, обернення дій). Історичні шифри допомагають зрозуміти принцип, але не забезпечують сучасного рівня захисту.

Пропозиція для майбутньої HTML-версії

Окремі кнопки: «Переглянути відео», «Завантажити PDF», «Веббот», «Форма для відповідей». Чотири практики відкриваються на окремих сторінках. Інтерактивний годинник має вибір старту та зсуву, режим абетки й зворотний хід; у симуляторі Цезаря/Віженера учень бачить формули, номери літер і перевірку розшифрування.

Посилання на відео, форму та сценарій веббота для цієї теми узгодимо під час створення HTML. Головну сторінку курсу не змінюємо до погодження матеріалу.