Міністерство освіти і науки України
Національний авіаційний університет

Факультет кібербезпеки та програмної інженерії
Кафедра інженерії програмного забезпечення
Дисципліна: “Безпека програм і даних”

Лабораторна робота №4
“Дослідження властивостей циклічних груп”

Виконав: Разно О. С.
студент групи ПІ-424Б
Перевірила: Воропай І.

Київ-2023

Варіант 10

Мета роботи – дослідження властивостей циклічних груп класів лишків, на яких базується сучасна криптографія. Обчислення утворюючого елемента циклічної групи. Застосування утворюючого елемента в системі відкритого розповсюдження ключів.

Завдання:

Завдання 1. Скласти таблицю (див. табл..1) піднесення в степінь елементів групи G(13,*) для a ∈ [2..12].

Таблиця 1

канд. в g	Ступінь піднесення n										
	2	3	4	5	6	7	8	9	10	11	12
a	$h=a^n$										
2											
3											
…											

Виписати в таблицю групи (див. табл..2), що згенеровані елементами a_i ∈ [2..12] та визначити порядки груп.

Таблиця 2

a	згенерована група H_g	порядок групи ord H_g
2		
3		
…		
11		
12		

Розрахувати теоретичну кількість утворюючих елементів групи G(13,*).

Завдання 2. Знайти утворюючі елементи g_i в мультиплікативній групі G(p,*) у відповідності з варіантом.

Номер варіанта № = № по списку (mod 10) + 1 = 19 (mod 10) + 1 = 9 + 1 = 10.

Таблиця 3

№ вар	1	2	3	4	5	6	7	8	9	10
p	47	43	53	41	17	37	19	23	29	31

Обрахувати порядок групи G(p,*) ord(G(p,*)) = φ(p).

Знайти ймовірні порядки підгруп – дільники порядку групи.

Обрахувати кількість генераторів групи K= φ(ord(G(p,*))).

Знайти перший мінімальний утворюючий елемент g групи G(p,*).

Для цього скласти таблицю 4.

Таблиця 4

	ймовірні порядки підгруп (дільники порядку групи)				
Кандидати в g					
2					
3					
…					

Обрахувати піднесення в ступінь для першого кандидата в генератори g = 2 для ступенів ймовірних порядків підгруп групи G(p,*) Якщо порядок утворюючого елемента (мінімальний ступінь для якого $g^m \bmod p \equiv 1$) менше порядку групи ord(G(p,*)) = φ(p), то g не є генератором групи. Переходимо до перевірки наступного кандидата в g.

Якщо порядок ord g = ord(G(p,*)), то перший генератор знайдено.

Обрахувати решту утворюючих елементів групи по формулі:

$$g_i = (g_1)^{Bi} \bmod p \text{ , де } B_i \text{ – числа, взаємно прості з } \varphi(p).$$

Таблиця 5

Перший генератор	Числв взаємно прості з $\varphi(p)$.	B1=	B2=	…
g0=	наступні генератори	g1=	g2=	

Завдання 3. Система відкритого розповсюдження ключів.

Застосувати результати завдання 3 для формування ключа на основі алгоритму Діффі – Хеллмана.

Таблиця 6

Клієнт А	параметри СВК p= g=	Клієнт В
формування 1 частини ключа	відкритий канал зв'язку	формування 1 частини ключа
випадкове число А=		випадкове число В=
Скрита складова ключа $rA=g^A \bmod p=$	$\Rightarrow$ rA	Скрита складова ключа $rB=g^B \bmod p=$
загальний ключ $K= rB^A \bmod p=$	rB $\Leftarrow$	загальний ключ $K= rA^B \bmod p=$

Параметр p заданий в таблиці №3 варіантів завдання. Параметр g обирається студентом самостійно з знайдених генераторів (за виключенням 1 генератора) в завданні №3.

Значення випадкових чисел, скриту складову ключа та загальний ключ записати у таблицю 6. Переконатися, що ключ К однаковий для обох сторін.

Зміст звіту з лабораторної роботи:

Завдання 1:

- Порядок групи, та ймовірні порядки підгруп.
- Кількість генераторів підгруп.
- Таблиця піднесення в ступінь елементів групи.
- Таблиця створених підгруп та їх порядки.
- Утворюючи елемент групи.
- Висновки по завданню 1.

Завдання 2:

- Таблиця пошуку 1 генератора групи. Таблиця – решта утворюючих елементів.

Завдання 3:

- Заповнена таблиця з значеннями параметрів системи p, g, випадковими числами A, B, скритою складовою ключа та загальним ключем.

Висновки.

Виконання:

1. Складання таблиці піднесення в степінь елементів групи G(13,*) для a ∈ [2..12]:

канд. в g	Ступінь піднесення n											
	1	2	3	4	5	6	7	8	9	10	11	12
a	$h=a^n$											
2	2	4	8	3	6	12	11	9	5	10	7	1
3	3	9	1	3	9	1	3	9	1	3	9	1
4	4	3	12	9	10	1	4	3	12	9	10	1
5	5	12	8	1	5	12	8	1	5	12	8	1
6	6	10	8	9	2	12	7	3	5	4	11	1
7	7	10	5	9	11	12	6	3	8	4	2	1
8	8	12	5	1	8	12	5	1	8	12	5	1
9	9	3	1	9	3	1	9	3	1	9	3	1
10	10	9	12	3	4	1	10	9	12	3	4	1
11	11	4	5	3	7	12	2	9	8	10	6	1
12	12	1	12	1	12	1	12	1	12	1	12	1

Випишемо в таблицю групи, що згенеровані елементами $a_i \in [2..12]$ та визначимо порядок груп:

a	Згенерована група H_g	Порядок групи ord H_g
2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	12
3	1, 3, 9	3
4	1, 3, 4, 9, 10, 12	6
5	1, 5, 8, 12	4
6	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	12
7	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	12
8	1, 5, 8, 12	4
9	1, 3, 9	3
10	1, 3, 4, 9, 10, 12	6
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	12
12	1, 12	2

Розрахуємо теоретичну кількість утворюючих елементів групи G(13,*):

$$\text{ord}(G(13, *)) = 12.$$

Отже, 2, 3, 4, 6 є дільниками числа 12.

Порядки підгруп:

- $\text{ord}(H_{12}) = 2$;

- $ord(H_3) = ord(H_9) = 3$;
- $ord(H_5) = ord(H_8) = 4$;
- $ord(H_4) = ord(H_{10}) = 6$.

Кількість генераторів K в мультиплікативній групі G(p, *), де p – просте число, визначається формулою $K = \varphi(\varphi(p)) = \varphi(p - 1)$:

$$p = 13,\ K = \varphi(13 - 1) = \varphi(12) = 4.$$

Отже, ми маємо чотири генератори.

Для p = 13: $\varphi(13) = 12$. Взаємно прості з 12: 1, 5, 7, 11.

Ми маємо чотири кандидати – 2, 3, 4 та 6. Нехай першим кандидатом буде g = 2. Перевіримо виконання нерівності $g^K \bmod p \neq 1$ для усіх $K < p - 1$:

- Для K = 2: $2^2 \bmod 13 = 4 \neq 1$ – виконується;
- Для K = 3: $2^3 \bmod 13 = 8 \neq 1$ – виконується;
- Для K = 4: $2^4 \bmod 13 = 3 \neq 1$ – виконується;
- Для K = 5: $2^5 \bmod 13 = 6 \neq 1$ – виконується;
- Для K = 6: $2^6 \bmod 13 = 12 \neq 1$ – виконується;
- Для K = 7: $2^7 \bmod 13 = 11 \neq 1$ – виконується;
- Для K = 8: $2^8 \bmod 13 = 9 \neq 1$ – виконується;
- Для K = 9: $2^9 \bmod 13 = 5 \neq 1$ – виконується;
- Для K = 10: $2^{10} \bmod 13 = 10 \neq 1$ – виконується;
- Для K = 11: $2^{11} \bmod 13 = 7 \neq 1$ – виконується.

Отже, g = 2 є генератором групи. Якщо знайдений один генератор g_1, інші генератори обраховуються по формулі $g_i = (g_1)^{Bi} \bmod p$, де B_i – числа, взаємно прості з $\varphi(p)$:

Так як $g_1 = 2$, то:

- $g_2 = (g_1)^5 \bmod 13 = 2^5 \bmod 13 = 32 \bmod 13 = 6$;
- $g_3 = (g_1)^7 \bmod 13 = 2^7 \bmod 13 = 128 \bmod 13 = 11$;
- $g_4 = (g_1)^{11} \bmod 13 = 2^{11} \bmod 13 = 2048 \bmod 13 = 7$.

В результаті, ми маємо чотири унікальні генератори: $g_1 = 2$, $g_2 = 6$, $g_3 = 11$, $g_4 = 7$.

2. Знаходження утворюючих елементів g_i в мультиплікативній групі G(p,*) у відповідності з варіантом (варіант №10, p = 31):

Обрахуємо порядок групи G(p,*) $ord(G(p,*)) = \varphi(p) = \varphi(31) = 30$.

Знайдемо ймовірні порядки підгруп – дільники порядку групи:

Для числа 30 дільниками є: 2, 3, 5, 6, 10, 15, 30.

Порядки підгруп за формулою $g^n \bmod m = 1$:

$ord(H_2) = 5$, $ord(H_3) = 30$, $ord(H_5) = 3$, $ord(H_6) = 6$, $ord(H_{10}) = 15$, $ord(H_{15}) = 10$.

Обрахуємо кількість генераторів групи K = φ(ord(G(p,*))):

K = φ(ord(G(31, *))) = φ(p – 1) = φ(31 – 1) = φ(30) = 8.

Отже, ми маємо 8 генераторів.

Для знаходження першого мінімального утворюючого елемента g групи G(p, *), складемо наступну таблицю:

	Ймовірні порядки підгруп (дільники порядку групи)						
Кандидати в g	$ord(H_2)$	$ord(H_3)$	$ord(H_5)$	$ord(H_6)$	$ord(H_{10})$	$ord(H_{15})$	$ord(H_{30})$
2	4	8	1	2	1	1	1
3	9	27	26	16	25	30	1

Обрахуємо піднесення в ступінь для першого кандидата в генератори g = 2 для ступенів ймовірних порядків підгруп групи G(p, *). Порядок утворюючого елемента (мінімальний ступінь для якого $g^m \bmod p \equiv 1$) менше порядку групи ord(G(p, *)) = φ(p), тому g не є генератором групи. Переходимо до перевірки наступного кандидата в g.

Порядок кандидата в генератори g = 3 має значення 30, що дорівнює порядку групи. Якщо порядок ord g = ord(G(p, *)), то перший генератор знайдено. Отож, g = 3 є першим мінімальним утворюючим елементом групи G(p, *).

Обрахуємо решту утворюючих елементів групи по формулі:

$$g_i = (g_0)^{Bi} \bmod p \text{ , де } B_i \text{ – числа, взаємно прості з } \varphi(p).$$

Для p = 31: φ(31) = 30. Взаємно прості з 30: 1, 7, 11, 13, 17, 19, 23, 29.

Сформуємо наступну таблицю:

Перший генератор	$g_0 = 3$	Числа взаємно прості з φ(p)
Наступні генератори		
$g_1 = (g_1)^7 \bmod 31 = 3^7 \bmod 31 = 17$		$B_1 = 7$
$g_2 = (g_1)^{11} \bmod 31 = 3^{11} \bmod 31 = 13$		$B_2 = 11$
$g_3 = (g_1)^{13} \bmod 31 = 3^{13} \bmod 31 = 24$		$B_3 = 13$
$g_4 = (g_1)^{17} \bmod 31 = 3^{17} \bmod 31 = 22$		$B_4 = 17$
$g_5 = (g_1)^{19} \bmod 31 = 3^{19} \bmod 31 = 12$		$B_5 = 19$
$g_6 = (g_1)^{23} \bmod 31 = 3^{23} \bmod 31 = 11$		$B_6 = 23$
$g_7 = (g_1)^{29} \bmod 31 = 3^{29} \bmod 31 = 21$		$B_7 = 29$

В результаті, в мультиплікативній групі G(31, *), ми отримуємо наступні утворюючі елементи g_i: 3, 11, 12, 13, 17, 21, 22, 24.

3. Система відкритого розповсюдження ключів. Заповнення таблиці з значеннями параметрів системи p, g, випадковими числами A, B, скритою складовою ключа та загальним ключем:

Застосуємо результати завдання для формування ключа на основі алгоритму Діффі – Хеллмана:

Клієнт А	Параметри СВК p = 31 g = 21	Клієнт В
Формування 1 частини ключа	Відкритий канал зв'язку	Формування 1 частини ключа
Випадкове число A = 37		Випадкове число B = 84
Скрита складова ключа $rA = g^A \bmod p =$ $= 21^{37} \bmod 31 = 11$	$\Rightarrow$ rA	Скрита складова ключа $rB = g^B \bmod p =$ $= 21^{84} \bmod 31 = 16$
Загальний ключ $K = rB^A \bmod p =$ $= 16^{37} \bmod 31 = 8$	rB $\Leftarrow$	Загальний ключ $K = rA^B \bmod p =$ $= 11^{84} \bmod 31 = 8$

Як видно з таблиці, загальний ключ K однаковий для обох сторін та дорівнює 8.

Висновок:

В ході виконання лабораторної роботи, я дослідив властивості циклічних груп класів лишків, на яких базується сучасна криптографія, обчислення утворюючого елемента циклічної групи та застосування утворюючого елемента в системі відкритого розповсюдження ключів. Мною було сформовано таблицю піднесення в степінь елементів групи G(13,*) для a ∈ [2..12], таблицю створених підгруп та їх порядки, визначено порядок групи та ймовірні порядки підгруп, кількість генераторів підгруп та утворюючі елементи груп (генератори). Також, я знайшов утворюючі елементи g_i в мультиплікативній групі G(p, *) у відповідності до мого варіанту (варіант №10, p = 31) та застосував отримані результати для формування ключа на основі алгоритму Діффі – Хеллмана: в результаті чого заповнив таблицю з значеннями параметрів системи p, g, випадковими числами A, B, скритою складовою ключа та загальним ключем.

Відповіді на контрольні запитання:

1. Що таке прості та взаємно прості числа?

Прості числа і взаємно прості числа – це концепції в теорії чисел, які відображають взаємну дільність чисел і використовуються для вивчення структури та властивостей чисел.

- Просте число: Просте число – це натуральне число більше одиниці, яке має лише два дільники: одиницю і саме себе. Іншими словами, прості числа діляться лише на одиницю і саме себе без залишку. Приклади простих чисел включають 2, 3, 5, 7, 11, 13 і так далі. Прості числа важливі в криптографії, арифметиці і багатьох інших галузях математики.
- Взаємно прості числа: Два натуральних числа називаються взаємно простими, якщо їх найбільший спільний дільник (НСД) дорівнює одиниці. Іншими словами, взаємно прості числа не мають жодних спільних дільників, крім одиниці. Наприклад, числа 15 і 28 є взаємно простими, оскільки їх НСД дорівнює 1. Однак числа 12 і 18 не є взаємно простими, оскільки їх НСД дорівнює 6.

Взаємна простота чисел важлива для деяких математичних задач, таких як раціональні дроби, теорія числових послідовностей, інформаційна теорія і багато інших областей.

2. Як перевірити простоту числа?

Перевірити простоту числа можна за допомогою малої теореми Ферма:

$a^{p-1} \bmod p \equiv 1 \; a \in [2, p-2]$

Якщо число p – просте, то будь яке число в інтервалі [2, p-2] піднесене у ступінь p-1 порівняно по модулю p з одиницею.

Також, існують інші методи для перевірки простоти числа:

- Метод перебору: Простий метод полягає в перевірці, чи має число дільники, крім 1 і самого себе. Для цього вам потрібно поділити число на всі можливі цілі числа від 2 до кореня з числа (закругленого до більшого цілого числа). Якщо немає жодного цілого числа, на яке число б поділилося, то воно є простим.
- Тест Міллера-Рабіна: Тест Міллера-Рабіна – це інший ймовірнісний метод перевірки простоти, який зазвичай є більш надійним, ніж тест Ферма. Він також базується на ідеях малої теореми Ферма і випробовує числа на основі певних імовірнісних правил.
- Деякі алгоритми на основі решітки: Для великих простих чисел існують спеціалізовані алгоритми, такі як "решітка Аткіна" і "решітка Ератосфена", які дозволяють ефективно перевіряти простоту чисел.

3. Як перевірити взаємну простоту двох чисел?

Числа є взаємно простими, якщо вони не мають спільних дільників, окрім 1.

Для перевірки взаємної простоти 2-х чисел використовують алгоритм Евкліда:

- Більше число ділимо на менше.
- Якщо ділиться без залишку, то менше число і є НСД (слід вийти з циклу).
- Якщо є залишок, то більше число замінюємо на залишок від ділення.
- Переходимо до пункту 1.

Алгоритм Евкліда:

Знаходження найбільшого дільника двох цілих чисел a і b a > b.

- Ділимо a на b і отримуємо залишок r.
- Якщо r=0, то b – найбільший спільний дільник. Кінець алгоритму.
- Інакше перепризначаємо a ← b, b ← r.
- Переходимо до кроку 1.

4. На що вказує функція Ейлера?

Функція Ейлера (позначається як φ(n)), вказує на кількість цілих чисел від 1 до n (включно), які є взаємно простими з числом n. Іншими словами, функція Ейлера φ(n) показує, скільки цілих чисел в діапазоні від 1 до n не мають жодних спільних дільників (крім 1) з числом n.

5. Які властивості функції Ейлера використовуються для її обрахування?

Функція Ейлера (фі-функція) φ(n) має кілька властивостей і формул, які можна використовувати для її обрахування:

- Для простих чисел: Фі-функція φ(p) для простого числа p обчислюється просто як p - 1, оскільки всі числа від 1 до p - 1 є взаємно простими з p.
- Для ступенів простого числа: Якщо n є ступенем простого числа p (тобто $n = p^k$ для деякого k), то $\varphi(n) = p^k - p^{(k-1)} = (p - 1) * p^{(k-1)}$. Ця формула використовується тоді, коли n є ступенем простого числа.
- Для добутку взаємно простих чисел: Якщо n і m є взаємно простими (тобто НСД(n, m) = 1), то φ(n * m) = φ(n) * φ(m). Ця властивість допомагає розрахувати фі-функцію для чисел, які є добутком двох взаємно простих чисел.
- Для загальних випадків: Для будь-якого складного числа n, яке не є ступенем простого числа, функцію φ(n) можна обчислити за допомогою факторизації n на прості множники. Коли n розкладається на прості множники у вигляді $n = p_1^{a1} * p_2^{a2} * ... * p_k^{ak}$, то $\varphi(p_1^{a1} * p_2^{a2} * ... * p_k^{ak}) = \varphi(p_1^{a1}) * \varphi(p_2^{a2}) ... * \varphi(p_k^{ak}) = (p_1 - 1) * p_1^{a1-1} * (p_2 - 1) * p_2^{a2-1} * … * (p_k - 1) * p_k^{ak-1}$.
  Де p_i – прості множники числа n, a_i – їхні ступені в розкладі, і $\varphi(p_i) = p_i - 1$ для кожного простого числа p_i.

Ці властивості і формули дозволяють обчислити функцію Ейлера для різних типів чисел, що полегшує роботу з нею у теорії чисел і криптографії.

6. Як знайти зворотний елемент в адитивній і мультикативній групах?

Знаходження зворотного елемента в адитивній і мультикативній групах відбувається за різними правилами через особливості операцій у кожній з цих груп:

1) Знаходження зворотного елемента в адитивній групі:

- У адитивній групі над заданою операцією додавання (+), зворотний елемент до певного числа a - це число, яке додається до a, щоб отримати нейтральний елемент, який в цьому випадку є нулем (0).
- Зворотний елемент до числа a в адитивній групі – це -a, тобто чисел -a, яке, додаючи до a, отримуємо 0. Математично це виглядає так: $a + (-a) = 0$.

2) Знаходження зворотного елемента в мультикативній групі:

- У мультикативній групі над заданою операцією множення (*), зворотний елемент до певного числа a – це число, яке множиться на a, щоб отримати нейтральний елемент, який в цьому випадку є одиницею (1).
- Зворотний елемент до числа a в мультикативній групі зазвичай позначається як a^{-1}, і він задовольняє такому рівнянню: $a * a^{-1} = 1$. Для знаходження зворотного елемента a^{-1} можна використовувати різні методи, такі як розширений алгоритм Евкліда (для поля простих чисел), або використовувати властивість, що $a^{-1} = a^{\varphi(n) - 1}$, де $\varphi(n)$ - функція Ейлера для числа n (якщо n - просте).
- Функція Ейлера може бути використана для обчислення зворотного по множенню елемента по модулю. Обчислення базується на теоремі Ейлера: $a^{\varphi(m)} \bmod m \equiv 1$, якщо a і m – взаємно прості. Якщо m – просте число, то $\varphi(m) = m - 1$. Відповідно $a^{m-1} \bmod m \equiv 1$ – окремий випадок теореми Ейлера – мала теорема Ферма.
  Вивід формули для обчислення зворотного елемента:
  $1 = a * a^{-1} = a * a^{-1} * a^{\varphi(m)} \bmod m = a * a^{\varphi(1)-1} \bmod m$
  $a^{-1} * 1 = a^{-1} * a * a^{\varphi(m)-1} \bmod m$
  $a^{-1} = a^{\varphi(m)-1} \bmod m$

7. Що таке циклічна група?

Групу називають циклічною групою, якщо існує такий елемент g групи, що множина його ступенів g^n породжує всі елементи групи.

8. Що таке порядок групи та підгрупи?

Кількість елементів в групі називається порядком групи ord(G), кількість елементів в підгрупі називається порядком підгрупи ord(H).

9. Яке співвідношення між порядком групи та порядками підгруп. Сформулюйте теорему Лагранжа.

Співвідношення між порядком елемента групи і порядком групи визначається теоремою Лагранжа: порядок підгрупи є дільником порядку групи.

10. Сформулюйте малу теорему Ферма.

Якщо число p – просте, то будь яке число в інтервалі [2, p-2] піднесене у ступінь p-1 порівняно по модулю p з одиницею:

$a^{p-1} \bmod p \equiv 1$ $a \in [2, p-2]$

Узагальненням малої теореми Ферма є теорема Ейлера, яка стверджує, що для будь-якого цілого числа a і простого числа p, для яких НСД(a, p) = 1, виконується:

$a^{\varphi(p)} \equiv 1 \pmod p$

де φ(p) – функція Ейлера, яка визначається як кількість цілих чисел від 1 до p-1, які є взаємно простими з p.

11. Що означають математичні символи ≡ та =?

Математичні символи "≡" і "=" використовуються для позначення різних рівностей і відношень між числами чи виразами, але вони мають різну семантику:

1) "=" (рівно):
- Символ "=" позначає справжню рівність між двома об'єктами. Коли ми пишемо "a = b", це означає, що a і b мають однакові значення. Наприклад, "2 + 3 = 5" означає, що сума чисел 2 і 3 рівна 5.

2) "≡" (конгруентно):
- Символ "≡" використовується в теорії чисел для позначення конгруентності за модулем. Коли ми пишемо "a ≡ b (mod n)", це означає, що числа a і b дають однаковий залишок при діленні націло на число n. Іншими словами, a і b конгруентні за модулем n, якщо (a - b) ділиться націло на n. Наприклад, "9 ≡ 3 (mod 6)" означає, що якщо ви поділите 9 націло на 6, ви отримаєте той самий залишок, який отримаєте, поділивши 3 на 6 націло, і цей залишок дорівнює 3.