КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп’ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем

Екзамен

з предмету «Математичні основи захисту інформації»

Варіант №48

Підготував:
Грищенко Юрій, ІПС-42

Київ – 2022

1. Довести, що повноциклічна група є циклічною групою. Навести приклади таких груп.

Нехай задана деяка скінченна множина цілих чисел, наприклад, N_5 = {0, 1, 2, 3, 4}. Оскільки ми хочемо побудувати адитивну абелеву групу, то ця множина обов'язково повинна включати 0. Для того, щоб N_5 перетворити в групу GN_5, необхідно коректно задати значення для операції додавання з одним із елементів групи, скажімо з 1. Дійсно, оскільки a + 0 = a для довільного a $\in GN_5$, то перший рядок таблиці додавання елементів групи визначений (таблиця 1), а на підставі комутативності (оскільки GN_5 абелева) і перший стовпчик цієї таблиці. Нехай, наприклад, задано 0 + 1 = 1, 1 + 1 = 4, 1 + 4 = 2, 1 + 2 = 3, 1 + 3 = 0. Таке задання коректне, оскільки має місце єдиність результату (але єдиність результату, як буде показано нижче, не достатня умова гарантії коректності). Тепер послідовно знаходимо результати додавання з елементом 4, оскільки 4=1+1:

$$4 + 2=(1+1)+2=1+(1+2)=1+3=0,\ 4+3=(1+1)+3=1+(1+3)=1,$$
$$4+4=(1+1)+4=1+(1+4)=1+2=3,$$

Далі знаходимо значення 4+1=2 і обчислюємо операцію додавання з елементом 2:

$$2+2=(1+4)+2=1+(4+2)=1+0=1,\ 2+3=(1+4)+3=1+(4+3)=1+1=4,$$
$$2+4=(1+4)+4=1+(4+4)=1+3=0.$$

Далі знаходимо значення 2+1=3 і обчислюємо операцію додавання з елементом 3:

$$3+2=(1+2)+2=1+(2+2)=1+1=4,\ 3+3=(1+2)+3=1+(2+3)=1+4=2,$$
$$3+4=(1+2)+4=1+(2+4)=1+0=1.$$

Заносимо ці значення в таблицю і на цьому закінчуємо побудову групи GN_5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	0	2
2	2	3	1	4	0
3	3	0	4	2	1
4	4	2	0	1	3

Аналогічно можна задати і довільну іншу групу GN_5. Дійсно, для цього задамо рядок таблиці додавання таким:

$$1+0 = 1,\ 1 + 1 = 3,\ 1+2=0,\ 1+3=4,\ 1+4=2$$

Таблиця будується аналогічно.

Зауважимо, що для побудови групи GN_k, мало вимагати тільки однозначності операції додавання. Якщо визначити додавання в групі так:

$$0 + 1 = 1,\ 1 + 1 = 0,\ 1 + 2 = 3,\ 1 + 3 = 4,\ 1 + 4 = 2,$$

то,обчислюючи 1+3, отримаємо

$$1 + 3 = 1 + (1 + 2) = (1 + 1) + 2 = 0 + 2 = 2,$$

що не збігається з визначеним вище. Справа в тім, що так визначена операція додавання не охоплює весь цикл елементів групи, тому що має елемент скінченного порядку $2 < 5$ (1+1=0).

Всі три групи, побудовані вище, циклічні на підставі теореми Лагранжа (вони мають порядок 5). В перших двох групах твірним був елемент 1, а в третій групі – елемент 3. Неважко переконатися, що всі три групи ізоморфні.

Поставимо у відповідність операції додавання з елементом групи
a1, за допомогою якого визначається група, підстановку

$$f_{a_1} = \begin{pmatrix} 0 & a_1 & a_2 & \dots & a_{k-1} \\ a_1 & a_{i_1} & a_{i_2} & \dots & a_{i_k} \end{pmatrix}.$$

Ця підстановка означає, що $f_{a1}(0) = 0 + a_1 = a_1$, $f_{a1}(a_1) = a_1 + a_1 = a_{i1}$, $f_{a1}(a_{i1}) = a_{i1} + a_1 = a_{ij}$, $f_{a1}(a_{ij}) = a_{ij} + a_1 = a_{il}$ і т. д

Назвемо групу GN_k **повноциклічною**, якщо підстановка f_{a1} є повним циклом довжини k. Справедлива

Теорема. Всі скінченні повноциклічні абелеві групи одного і того порядку ізоморфні між собою.

Неважко довести, що повноциклічна група є окремим випадком циклічної групи, оскільки якщо існує підстановка f_{a1}, що є повним циклом довжини k, то:

- *Підставляючи a_1 в f_{a1} отримаємо k елементів 0, $f_{a1}(0) = a_1$, $f_{a1}(a_1) = a_{i1}$, $f_{ai}(a_{i1}) = a_{ij}$, ..., $f_{a1}(a_{...}) = 0$*
- *За визначенням циклу всі k елементів будуть різними, отже це всі елементи повноциклічної групи GN_k.*
- *$f_{a1}(0) = a_1$, $f_{a1}(a_1) = a_1 + a_1$, $f_{a1}(a_1 + a_1) = a_1 + a_1 + a_1$, бачимо, що всі породжені елементи мають вигляд na_1, де n — натуральне число.*
- *Таким чином, всі елементи даної повноциклічної групи можна записати у вигляді na_1, отже **група GN_k є циклічною** групою з породжуючою множиною $\{a_1\}$.*

2. За яких умов порівняння $x^2 \equiv a \pmod p$ матиме розв’язок?

Розглянемо конгруенцію:

$$x^2 \equiv a \pmod p$$

де p – непарне просте число і НСД(a,p) = 1. Випадок p = 2 тривіальний і тому його не розглядаємо. Якщо $a \equiv 0\ (mod\ p)$, то очевидно єдиним її розв'язком буде $x \equiv 0\ (mod\ p)$. Тому далі p буде непарним простим числом і a – цілим числом, взаємно простим з p.

Якщо конгруенція $x^2 \equiv a\ (mod\ p)$ має хоча б один розв'язок, то число a називається ***квадратичним лишком***, інакше a називається ***квадратичним нелишком***.

Критерій Ойлера: При простому p і a, не кратному p, a є квадратичним лишком тоді і тільки тоді, коли має місце конгруенція:

$$a^{\frac{p-1}{2}} \equiv 1 (mod\ p)$$

І буде квадратичним нелишком тоді і тільки тоді, коли:

$$a^{\frac{p-1}{2}} \equiv -1 (mod\ p)$$

Приклад: Чи має розв'язки конгруентність $x^2 \equiv 12\ (mod\ 13)$?

$$12^{\frac{13-1}{2}} = 12^6 \equiv (-1)^6 = 1 (mod\ 13)$$

Отже, 12 – квадратичний лишок і тому дана конгруенція має розв'язок.

3. Зашифрувати шифром Шаміра повідомлення ATTAK IN TEN за допомогою ключа такої самої довжини, що і повідомлення.

Маємо повідомлення ATTAK IN TEN = {1,20,20,1,11,0,9,14,0,20,5,14}

A вибирає випадково велике просте число p і відкрито передає його B:
Нехай p = 29

A вибирає два числа:
$c_A d_A = 1\ (mod\ p-1)$

Ці числа A тримає в секреті і нікому їх не передає. B теж вибирає два числа c_B і d_B такі, що
$c_B d_B = 1\ (mod\ p-1)$
і теж тримає їх в секреті.

Оскільки в англійському алфавіті 26 літер + 1 пробіл, повідомлення, що складається з 12 символів, не вдасться передати одразу, тому для кожної літери доведеться підбирати випадково нові пари (c_A, d_A), (c_B, d_B). **Фактично таким чином отримаємо ключ тієї ж довжини, що й повідомлення.**

p-1=28, отже підбираємо c,d взаємно прості з 28

Передамо першу літеру (‘A’ = 1):

$c_A d_A = 1 \pmod{28} = 3 * 19$
$c_B d_B = 1 \pmod{28} = 5 * 17$

Крок 1. A обчислює
$x_1 = m^{cA} \pmod{p} = 1^3 \pmod{29} = 1$
і передає його B

Крок 2. B обчислює
$x_2 = x_1^{cB} \pmod{p} = 1^5 \pmod{29} = 1$
і передає його A

Крок 3. A обчислює
$x_3 \equiv x_2^{dA} \pmod{p} = 1^{19} \pmod{29} = 1$
і передає його B.

Крок 4. B, отримавши x3, обчислює число
$x_4 \equiv x_3^{dB} \pmod{p} = 1^{17} \pmod{29} = 1 =$ ‘A’

Наступна літера (‘T’ = 20):
$c_A d_A = 1 \pmod{28} = 11 * 23$
$c_B d_B = 1 \pmod{28} = 13 * 13$

$20^{11} \bmod 29 = 7$
$7^{13} \bmod 29 = 25$
$25^{23} \bmod 29 = 16$
$16^{13} \bmod 29 = 20 =$ ‘T’

Наступна літера (‘T’ = 20):
$c_A d_A = 1 \pmod{28} = 15 * 15$
$c_B d_B = 1 \pmod{28} = 9 * 25$

$20^{15} \bmod 29 = 20$

$20^{9} \bmod 29 = 23$
$23^{15} \bmod 29 = 23$
$23^{25} \bmod 29 = 20 =$ ‘T’

Наступна літера (‘A’ = 1):
$c_A d_A = 1 \pmod{28} = 11 * 23$
$c_B d_B = 1 \pmod{28} = 9 * 25$

$1^{11} \bmod 29 = 1$
$1^{9} \bmod 29 = 1$
$1^{15} \bmod 29 = 1$
$1^{25} \bmod 29 = 1 =$ ‘A’

Наступна літера (‘K’ = 11):
$c_A d_A = 1 \pmod{28} = 13 * 13$
$c_B d_B = 1 \pmod{28} = 3 * 19$

$3^{13} \bmod 29 = 21$
$21^{3} \bmod 29 = 10$
$10^{13} \bmod 29 = 26$
$26^{19} \bmod 29 = 11 =$ ‘K’

І так далі

Бачимо, що
А має приватний ключ $c_A = \{3, 11, 15, 11, 13, ...\}$
В має приватний ключ $c_B = \{5, 13, 9, 9, 3, ...\}$
В успішно отримує та розшифровує повідомлення {‘A’, ‘T’, ‘T’, ‘A’, ‘K’, ... }