

Цей файл - мій маніфест ненависті до вищої освіти в Україні, і шеві зокрема.
У випадку, якщо ви знайдете мене мертвим після сесії - сприймайте цей документ, як
мою передсмертну записку.

Ну шо блять, погналі нахуй



Варіант 1

Порядок елемента групи
Чи буде відображення гомо(ізо)морфізмом
Відокремити дійсні корені
(TODO) Ель Гамаля

Варіант 2

Чи буде групою
Знайти всі елементи порядку к у циклічній групі
Визначити кратність кореня для многочлена
Еліптична крива

Варіант 3

Порядок групи поворотів
Розв'язати систему рівнянь
Розкласти дріб на найпростіші
Еліптична крива

Варіант 4

Чи буде групою
Чи буде відображення гомо(ізо)морфізмом
Частковий розклад добутку через кругові многочлени
Діффі-Гелмана

Варіант 5

Таблиця Келі
Знайти всі елементи порядку
Частковий розклад добутку через кругові многочлени
(TODO) RSA

Варіант 6

Знайти порядок елемента групи
Обернена матриця в полі
Розкласти дріб на найпростіші
(TODO) RSA

Варіант 7

Чи буде групою
Чи буде відображення гомо(ізо)морфізмом
Знайти всі раціональні корені многочлена
Еліптична крива

Варіант 8

Довести
(TODO) Визначити кількість та один генератор
Знайти обернений елемент у розширенні поля
(TODO) Ель Гамаля

Варіант 9

Довести
(TODO) Символ Лежандра/Якобі
Відокремити дійсні корені

[Еліптична крива](#)

[Варіант 10](#)

[Порядок елемента групи](#)

[Розв'язати рівняння у полі](#)

[Частковий розклад через кругові многочлени](#)

[\(TODO\)Ель Гамала](#)

[Варіант 11](#)

[Довести](#)

[З'ясувати чи буде множина - полем](#)

[Частковий розклад добутку через кругові многочлени](#)

[Діффі-Гелмана](#)

[Варіант 12](#)

[Чи буде кільцем](#)

[Система рівнянь](#)

[Обернений елемент у розширенні поля](#)

[\(TODO\) Ель Гамала](#)

[Варіант 13](#)

[Чи буде кільцем](#)

[\(TODO\)Знайти генератори](#)

[Кратність кореня](#)

[Діффі-Гелмана](#)

[Варіант 14](#)

[Чи буде кільцем](#)

[Відображення гомо\(ізо\)морфізм](#)

[Раціональні корені многочлена](#)

[\(TODO\) RSA](#)

[Варіант 15](#)

[Знайти порядок елемента групи](#)

[Алгоритм Чіпполи](#)

[\(TODO\)Знайти порядок многочлена за допомогою незвідного многочлена](#)

[\(TODO\)Ель Гамаль](#)

[Алгоритм розв'язку для еліптичних кривих](#)

[RSA](#)

[Діффі-Гелмана](#)

Теорія

Асоціативність

Бінарна операція $(*)$ на множині M називається **асоціативною**, якщо для будь-яких трьох елементів a, b і c з множини M справджується рівність $(a * b) * c = a * (b * c)$. Операція називається **неасоціативною**, якщо в множині M існує хоча б одна трійка елементів a, b і c , для яких $(a * b) * c \neq a * (b * c)$.

Комутативність

Бінарна операція $(*)$ називається **комутативною**, якщо для будь-яких двох елементів a і b з множини M справджується рівність $a * b = b * a$. Операція називається **некомутативною**, якщо в множині M існує хоча б одна пара елементів a і b , для яких $a * b \neq b * a$.

Нейтральний елемент

Елемент $\eta \in M$ називається **нейтральним елементом** відносно операції $(*)$, якщо для будь-якого елемента a з множини M справджаються рівності $a * \eta = \eta * a = a$. Нейтральний елемент називають також **одиницею** e .

Обернений\симетричний елемент

Нехай у множині M з бінарною операцією $(*)$ є нейтральний елемент η . Елемент $a' \in M$ називається **симетричним** елементу $a \in M$ (або оберненим до a), якщо $a * a' = a' * a = \eta$.

Напівгрупа. Моноїд

Множина M з бінарною операцією $(*)$ називається **напівгрупою**, якщо операція $*$ асоціативна. Якщо напівгрупа $(M, *)$ містить нейтральний елемент, то її називають напівгрупою з одиницею або **моноїдом**.

У напівгрупі з одиницею η для кожного елемента існує щонайбільше один обернений елемент. Справді, якщо $a * a' = a' * a = \eta$ і $a * a'' = a'' * a = \eta$, то маємо такий ланцюжок рівностей:

$$a' = a' * \eta = a' * (a * a'') = (a' * a) * a'' = \eta * a'' = a''.$$

Далі обернений до a елемент (якщо він існує) ми позначатимемо через a^{-1} . Елемент, для якого існує обернений, називається **оборотним**.

Група

Напівгрупа з одиницею, в якій всі елементи оборотні, називається **групою**. Іншими словами, множина G з бінарною операцією $(*)$ називається **групою**, якщо виконуються три наступні умови:

- 1) операція $(*)$ асоціативна;
- 2) в G існує нейтральний елемент η ;
- 3) для кожного елемента $a \in G$ в множині G існує обернений до a елемент a' .

Зауважимо, що множина G повинна бути замкненою відносно операції $*$ (за означенням бінарної операції).

Якщо операцію в групі G називають множенням, то групу називають **мультиплікативною** (від лат. *multiplico* – множити), якщо G утворює групу відносно звичайного додавання, то групу називають **адитивною** (від лат. *additio* – додавати).

Абелева група

Якщо бінарна операція $(*)$ комутативна, то **група** G називається **комутативною або абелевою**. Групу, що містить скінчену кількість елементів, називають **скінченною**. Кількість елементів скінченної групи називають її **порядком**. Групу, що не є скінченною, називають **нескінченною**.

Замкненість бінарної операції

M . Якщо це так, то кажуть, що **множина M замкнена** відносно операції (*). Наприклад, сума двох непарних чисел завжди є парним числом, тому множина непарних чисел не є замкненою відносно операції додавання. Іншими словами, додавання не є бінарною операцією на множині непарних чисел.

Властивості групи

Властивість 1. Для довільних цілих чисел m і n та елемента a групи G справджаються рівності $a^m * a^n = a^{m+n}$ та $(a^m)^n = a^{m \cdot n}$.

Властивість 2. Для довільних елементів a і b групи G кожне з рівнянь $a * x = b$ і $y * a = b$ має єдиний розв'язок.

Властивість 3. Для будь-яких елементів a, b, c групи G з рівності $a * b = a * c$ випливає рівність $b = c$, а з рівності $a * c = b * c$ випливає рівність $a = b$.

Теорема Лагранжа

Твердження. Якщо H_1, H_2 підгрупи групи G , то їхній перетин $H_1 \cap H_2$ також є підгрупою групи G .

Це твердження узагальнюється на будь-яке число (скінченнє чи нескінченнє) підгруп групи G .

Нехай $H < G$ і $a \in G$. **Правим суміжним класом** Ha групи G за підгрупою H називається множина $Ha = \{ha : h \in H\}$. Лівий суміжний клас визначаємо аналогічно: $aH = \{ah : h \in H\}$. Легко перевірити, що два правих суміжних класи за підгрупою H або не перетинаються або збігаються (як множини). Таким чином, праві суміжні класи за підгрупою H утворюють розбиття групи G на класи суміжності. Зрозуміло, що всі суміжні класи за підгрупою H мають однакову кількість елементів, яка збігається з кількістю елементів підгрупи H . Два елементи a і b групи G лежать в одному суміжному класі за підгрупою H тоді й лише тоді, коли $ab^{-1} \in H$. Кількість (правих) суміжних класів називають **індексом підгрупи** H у групі G і позначають $|G:H|$. Справедлива

Теорема Лагранжа: Нехай G – скінченна група, H – підгрупа групи G .

Тоді $|G| = |G:H| \cdot |H|$.

Зокрема, порядок підгрупи скінченної групи є дільником порядку групи.

Практика

З'ясувати, чи буде(утворює) групою(групу)

Приклад 1. З'ясувати, чи утворює групу відносно операції додавання множина всіх цілих чисел, які кратні 3.

Нехай G – множина всіх цілих чисел, які кратні 3, тобто $G = \{3k : k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$. Оскільки $3k + 3m = 3(k+m)$, тобто сума чисел, кратних 3, саме є кратною 3, і $-3k = 3 \cdot (-k)$, тобто число, протилежне кратному 3, саме є кратним 3, то множина цілих чисел, кратних 3, є замкненою відносно додавання і взяття протилежного елемента. Тому вона утворює підгрупу групи цілих чисел, а отже, є групою. Групу всіх цілих чисел, які кратні 3, позначатимемо $3\mathbb{Z}$.

Приклад 2. З'ясувати, чи утворює групу відносно операції множення множина всіх дійсних кососиметричних матриць.

Квадратна матриця A називається кососиметричною, якщо $A^T = -A$. Зрозуміло, що всі діагональні елементи кососиметричної матриці дорівнюють нулю. Неважко переконатися, що множина кососиметричних матриць не утворює групу за множенням, оскільки до множини не попадає одинична матриця. Зауважимо також, що добуток двох кососиметричних матриць може бути матрицею не кососиметричною. Наприклад,

$$\begin{pmatrix} 0 & 1 & -2 \\ 1 & 0 & 0 \\ -2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 3 \\ 0 & 3 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -6 & 3 \\ 0 & -1 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

Варіант 1

Варіант 1

- Знайти порядок елемента групи $g = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \in T_2(Z_5^*)$ де $T_2(Z_5)$ – множина невироджених верхніх трикутних матриць порядку 2 з коефіцієнтами з поля Z_5
- Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R \rightarrow Z, f(x) = [x]$
- Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$
- Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^3 + x^2 + 1$ за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 5$, сесіонний код Аліси $k = 2$, число, що передається $u = 5$.

Порядок елемента групи

Варіант 1 ЗА. Підготувати до модуль.

1. $g = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \in T_2(Z_5^*)$, де $T_2(Z_5)$ – множина невироджених верхніх трикутних матриць порядку 2 з коефіцієнтами з поля Z_5 .

$g^1 = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}; g^2 = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ 0 & 4 \end{pmatrix} \dots$

$g^3 = \begin{pmatrix} 1 & 9 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}; g^4 = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Отже, $O(g) = 4$

Чи буде відображення гомо(ізо)морфізмом

2. Чи буде f гомоморфізмом / ізоморфізмом?

$$f: \mathbb{R} \rightarrow \mathbb{Z}, f(x) = [x]$$

$$\text{Із } f(a+b) = f(a) + f(b)$$

$$f(x+y) = [x+y] \neq [x] + [y] = f(x) + f(y) \Rightarrow$$

\Rightarrow не гомоморфізм.

~~не ізоморфізм~~

$$\text{Існує лише } \exists x \neq y \in \mathbb{R} : f(x) = f(y) \text{ із } f(1.1) = f(1.5) \Rightarrow$$

\Rightarrow не юнівітвне \Rightarrow не ізоморфізм

Відокремити дійсні корені

③ Відокремити дійсні корені многочлена $f(x) = x^4 - 3x^3 - x^2 + 8x - 4$.

$$f = x^4 - 3x^3 - x^2 + 8x - 4$$

$$f' = 4x^3 - 9x^2 - 2x + 8 = f_0$$

$$\begin{array}{r|l} x^4 - 3x^3 - x^2 + 8x - 4 & 4x^3 - 9x^2 - 2x + 8 \\ \hline x^4 - \frac{9}{4}x^3 - \frac{1}{2}x^2 + 2x & \frac{1}{4}x - \frac{3}{16} \\ \hline & -\frac{3}{4}x^3 - \frac{1}{2}x^2 + 6x - 4 \end{array}$$

0)

$$\begin{array}{r}
 -\frac{3}{4}x^3 - \frac{1}{2}x^2 + 6x - 4 \\
 -\frac{3}{4}x^3 + \frac{27}{16}x^2 + \frac{3}{8}x - \frac{3}{2} \\
 -\frac{35}{16}x^2 + \frac{45}{8}x - \frac{5}{2} \\
 f_1 = \frac{35}{16}x^2 - \frac{45}{8}x + \frac{5}{2} = 35x^2 - 90x + 40 = 7x^2 - 18x + 8
 \end{array}$$

$$\begin{array}{r}
 4x^3 - 9x^2 - 2x + 8 \\
 4x^3 - \frac{72}{7}x^2 + \frac{32}{7}x \\
 -\frac{9}{7}x^2 - \frac{16}{7}x + 8 \\
 -\frac{9}{7}x^2 - \frac{162}{49}x + \frac{72}{49} \\
 -\frac{160}{49}x + \frac{320}{49} \\
 f_2 = \frac{160}{49}x - \frac{320}{49} = 160x - 320 = x - 2
 \end{array}$$

$$\begin{array}{r}
 7x^2 - 18x + 8 \\
 7x^2 - 14x \\
 -4x + 8 \\
 -4x + 8 \\
 0
 \end{array}$$

$$\begin{array}{r}
 f_3 = 16 \\
 x_0 \quad f_0 \quad f_1 \quad f_2 \quad S \\
 \infty \quad + \quad + \quad + \quad 0 \\
 -\infty \quad + \quad - \quad - \quad 3 \\
 0 \quad - \quad + \quad + \quad - \quad 2 \\
 1 \quad + \quad + \quad - \quad - \quad 1 \\
 3 \quad + \quad + \quad + \quad + \quad 0 \\
 -2 \quad + \quad - \quad + \quad - \quad 3
 \end{array}$$

Дійсні корені є на проміжках $(0; 1), (1; 3), (-2; 0)$

(TODO) Ель Гамаля

єбаніна якась, боже упасі шоб не попалось

Варіант 2

Варіант 2

- З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, де $x \in \mathbb{R}$, відносно множення.
- У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 200, k = 8$
- Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8, c = 2, x_0 = -1$.
- Дано еліптичну криву $y^2 = x^3 + x + 2$ у полі Z_{17} . Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Чи буде групою

1. 1) Заміщеність $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \vee$

2) Асоціативність: $(AB)C = A(BC) \vee$

3) Нейтральний елемент: $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

4) О并向чний елемент: $A^{-1} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} | \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} | \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} =$
 $= \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \vee$

Отже, група

Знайти всі елементи порядку k у циклічній групі

2, $n = 200, K = 8$

$\frac{200}{8} = 25$; Взаємно прості числа діль 8 : $1, 3, 5, 7$

Отже: $a^{25-1}, a^{25-3}, a^{25-5}, a^{25-7}$

Визначити кратність кореня для многочлена

Задача 3. $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$; $c = 2$; $x_0 = -2$

8) $\begin{array}{r} (1) \quad 1 \quad -5 \quad 7 \quad -2 \quad 4 \quad -8 \\ \underline{2} \quad 1 \quad -3 \quad 1 \quad 0 \quad 4 \quad 0 \\ 2 \quad 1 \quad -1 \quad -1 \quad -2 \quad 0 \\ 2 \quad 1 \quad 1 \quad 1 \quad 0 \\ 2 \quad 1 \quad 3 \quad 7 \quad \neq 0 \Rightarrow kp=3 \end{array}$

(2) $\begin{array}{r} 1 \quad -5 \quad 7 \quad -2 \quad 4 \quad -8 \\ -1 \quad 1 \quad -6 \quad 13 \quad -15 \quad 19 \quad -27 \\ -1 \quad 1 \quad -7 \quad 20 \quad -35 \quad 54 \\ -1 \quad 1 \quad -8 \quad 23 \quad -63 \\ -1 \quad 1 \quad -9 \quad 37 \\ -1 \quad 1 \quad -10 \\ -1 \quad 1 \end{array}$

$f(-1) = -27$
 $f'(x)(-1) = -54$
 $f^{(2)}(-1) = -63 \cdot 8! \approx -126$
 $f^{(3)}(-1) = 34 \cdot 3! = 222$
 $f^{(4)}(-1) = -10 \cdot 9! \approx -240$
 $f^{(5)}(-1) = 120$

Еліптична крива

???

Алгоритм розв'язку для еліптичних кривих

y	x	$x^3 + x + 2 \pmod{17}$	$y^2 = x^3 + x + 2 \pmod{17}$	$y =$
0	0	2	$y^2 = 2 \pmod{17}$	-
1	9	4	$y^2 = 4 \pmod{17}$	-
2	12	12	$y^2 = 12 \pmod{17}$	-
3	15	-	$y^2 = -15 \pmod{17}$	-
4	2	-	-	-
5	13	-	-	-
6	3	-	-	-
7	12	-	-	-
8	12	-	$y^2 = 9 \pmod{17}$	$y = 3$
9	9	-	-	$y = 3$
10	9	-	$y = 1$	-
11	8	-	-	-
12	8	-	-	-
13	2	-	-	-
14	6	-	-	-
15	9	-	$y = 3$	-
16	0	-	$y = 0$	(1, 2)

Різрешко пошуки

$x_3 = (\lambda^2 - 1 - 1) \pmod{17}$

$y_3 = (\lambda(1 - x_3) - 2) \pmod{17}$

$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p}$

$\lambda = \frac{3 \cdot 1^2 + 1}{2 \cdot 1} = \frac{4}{2} = 1$

$x_3 = (1 - 2) \pmod{17} = -1 \pmod{17} = 16$

$y_3 = (1(1 - 16) - 2) \pmod{17} = -17 \pmod{17} = 0$

$A + A = (16, 0)$

Варіант 3

Варіант 3

- Знайти порядок групи поворотів правильного тетраедра
- Розв'язати систему рівнянь $\begin{cases} 9x + 2y = 8 \\ 2x + 3y = 11 \end{cases}$ в полі Z_{13}
- Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера
 $f(x) = \frac{2x^3 - x^2 - 5x + 4}{(x+1)^5}$
- Дано еліптичну криву $y^2 = x^3 + x + 1$ у полі Z_{17} . Знайти точку A на кривій таку що $y \neq 0$. Обчислити $A + A$

Порядок групи поворотів

8. Правильний тетраедр

Порахував всі можливі повороти.

Відомо, що тетраедр має 4 грани (край та-ки), 4 вершини і 6 ребер

1. Монотонне піввертання (поворотове піввертання)
- У тетраедра 4 вершини. Для кожної можна провести 3 відповідної через неї і протилежну грань і обертання на 120° або 240°. $\rightarrow 4 \cdot 3 = 12$ поворотів на 120° або 240°
- Можна більше піввертити чи один чи кілька поворотів.

Маємо 6 ребер, і для кожного можна зробити 2 піввертання чи обертання на 180°: $6 \cdot 2 = 12$ піввертання чи обертання на 180°.

Порядок групи $g = 1 + 12 + 12 = 24$.

Група поворотів правильного тетраедру ізоморфна групі A_4 — групі парних перестановок 4 елементів.

$$o(g) = |A_4| = \frac{4!}{2} = \frac{24}{2} = 12$$

Група A_4 — це більше парних перестановок чи їхні обертання, чи піввертання, чи комбінації всіх цих та-ки.

Розв'язати систему рівнянь

Варіант 3

$$\begin{cases} 9x + 2y = 8 \quad | \cdot 3 \\ 2x + 3y = 14 \quad | \cdot 2 \end{cases}$$

$27x = 2 \pmod{13}$

$10x = 2 \pmod{13} \Rightarrow x = 8$

~~$27y = 11 - 16 = -5 \pmod{13}$~~

$3y = 8 \pmod{13}$

$2y = 72 \pmod{13} \Rightarrow y = 7$

$(8, 7)$

Розкласти дріб на найпростіші

M	-1	2	-1	-5	4
E	-1	2	-3	-2	6
M	-1	2	-5	3	
E	-1	2	-7		
R	-1	2			

$f_1(x) = 2x^3 - x^2 - 5x + 4$ розклад за степенем x

$f_1(x) = 2(x+1)^3 - 7(x+1)^2 + 3(x+1) + 6$

$f_1(x) = \frac{2}{(x+1)^2} - \frac{7}{(x+1)^3} + \frac{3}{(x+1)^4} + \frac{6}{(x+1)^5}$

Еліптична крива

4) Ел. крива $y^2 = x^3 + x + 1 \pmod{17}$. $A + A$.

$x^2 = x^3 + x + 1 \pmod{17}$ який, що $y^2 = x^3 + x + 1$

0	$x^3 + x + 1$	$y^2 = 1 \pmod{17}$	$y=1$
1	$x^3 + x + 1$	$y^2 = 3 \pmod{17}$	-
2	$x^3 + x + 1$	$y^2 = 11 \pmod{17}$	-
3	$x^3 + x + 1$	$y^2 = 14 \pmod{17}$	-
4	$x^3 + x + 1$	$y^2 = 1 \pmod{17}$	$y=1$
5	$x^3 + x + 1$	$y^2 = 12 \pmod{17}$	-
6	$x^3 + x + 1$	$y^2 = 2 \pmod{17}$	-
7	$x^3 + x + 1$	$y^2 = 11 \pmod{17}$	-
8	$x^3 + x + 1$	$y^2 = 11 \pmod{17}$	-
9	$x^3 + x + 1$	$y^2 = 8 \pmod{17}$	-
10	$x^3 + x + 1$	$y^2 = 8 \pmod{17}$	-
11	$x^3 + x + 1$	$y^2 = 0 \pmod{17}$	$y=0$
12	$x^3 + x + 1$	$y^2 = 7 \pmod{17}$	-
13	$x^3 + x + 1$	$y^2 = 1 \pmod{17}$	$y=1$

$$14 \quad 2759 \pmod{17} = 5$$

$$y^2 = 5 \pmod{17}$$

$$15 \quad 3391 \pmod{17} = 8$$

$$y^2 = 8 \pmod{17}$$

$$16 \quad 4113 \pmod{17} = 16$$

$$y^2 = 16 \pmod{17}$$

Механічно оберемо $A = (0, 1)$.

$$\lambda = \frac{3x_2^2 + 1}{2y} = \frac{3 \cdot 0 + 1}{2} = \frac{1}{2}$$

$$2 \cdot \lambda = 1 \pmod{17}$$

$$\lambda = 9$$

$$x_2 = (\lambda^2 - 2x) = (81 - 2 \cdot 0) = 81 \pmod{17} = 13$$

$$y_2 = (\lambda(x - x_2) - y) = 9(0 - 13) - 1 = -118 \pmod{17} = 1$$

$$A = (0, 1) \quad A + A = (13, 1)$$

Варіант 4

Варіант 4

- З'ясувати, чи буде групою множина невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, де число а – фіксоване, відносно множення.
- Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : R^+ \rightarrow R$, $f(x) = \log_2 x$
- Знайти частковий розклад добутку всіх незвідних многочленів степеня 2 у полі Z_7 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многочлени які можна з них одержати.
- Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 13$, генератор знайдіть та виберіть довільний.

Чи буде групою

1) Чи буде групою множина дійсних $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$ де а – фіксоване число, но множення.

1. Замкненість: виконується

$$\begin{pmatrix} x & y \\ ay & x \end{pmatrix} \begin{pmatrix} x & y \\ ay & x \end{pmatrix} = \begin{pmatrix} x^2 + ay^2 & xy + xy \\ axy + axy & ay^2 + x^2 \end{pmatrix} = \begin{pmatrix} x^2 + ay^2 & 2xy \\ a \cdot 2xy & x^2 + ay^2 \end{pmatrix}$$

2) Асоціативність: множення матриць асоціативне.

3) Нейтральний елемент: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$.

4). Обернений елемент:

$$\begin{pmatrix} x & y \\ ay & x \end{pmatrix}^{-1} = \frac{1}{x^2 - ay^2} \begin{pmatrix} x & -y \\ -ay & x \end{pmatrix} - існує і належить
важливо.$$

Оскільки \in групово.

Чи буде відображення гомо(ізо)морфізмом

2) $f: \mathbb{R}^+ \rightarrow \mathbb{R}, f(x) = \log_2 x$. ізо, гомоморфізм

- 1) Гомоморфізм

$$f(x+y) = \log_2 x + y = \log_2 x + \log_2 2^y = f(x) + f(y) \quad \checkmark$$

- 2) Ізоморфізм

- a) ін'ективність: $f(x) = f(y) \Rightarrow \log_2 x = \log_2 y \Rightarrow x = y \quad \checkmark$
- b) спрієктивність: $\forall y \exists x \quad x = 2^y \quad f(x) = \log_2 2^y = y \quad \checkmark$

Чис лідображення є ізоморфізмом.

Частковий розклад добутку через кругові многочлени

3) $q=7, n=2$
 $N = \frac{1}{2} \cdot (-7 + 4\sqrt{-5}) = \frac{42}{2} - 21\sqrt{-5}$ НМ.

$$\begin{array}{c} \gamma^2 - 1 = 48 \\ \gamma^1 = 4; \quad \gamma^2 = 49 \end{array}$$

	1	2	3	4	6	8	12	16	24	48
4	1	-1	0	1	0	0	0	0	0	0

$$\mu(7, 2, x) = Q_4 \cdot Q_8 \cdot Q_{16} \cdot Q_{24} \cdot Q_{48}$$

$$Q_4 = \frac{x-1}{x^2+1} = x^2+1 \quad \text{НМ}$$

$$Q_8 = \frac{(x^4-1)(x^2+1)}{(x^4-1)(x^2+1)} = \frac{x^6+1}{x^2+1} = x^4-x^2+1 \quad -2 \text{ НМ}$$

$$Q_16 = x^8+1 \quad -4 \text{ НМ}$$

$$Q_{24} = \frac{(x^{12}-1)(x^8+1)}{(x^{12}-1)(x^8+1)} = \frac{x^{16}+1}{x^8+1} = x^8-x^4+1 \quad -4 \text{ НМ}$$

$$Q_{48} = \frac{x^{24}+1}{x^8+1} = x^{16}-x^8+1 \quad -8 \text{ НМ}$$

$$1+2+2+4+4+8 = 21 = N$$

$$x \rightarrow x+1 \quad (\text{б } Q_4): \quad (x+1)^2+1 = x^2+2x+2 \quad - \text{ новий НМ.}$$

Діффі-Гелмана

Варіант 9

$$4. p=13; g=3$$

// лінія обарв $a=4$ та обчислює :

$$A = g^a \pmod{p} = 3^4 \pmod{13} = 3 // \text{лінія падано в бодж } A=3$$

// бодж обарв $b=3$ та обчислює :

$$B = g^b \pmod{p} = 3^3 \pmod{13} = 1 // \text{бодж падано лінії } B=1$$

// лінія обчислє $a_{BA} = B^a \pmod{p}$ // // бодж обчислє $a_{AB} = A^b \pmod{p}$ //

$$a_{BA} = 1^4 \pmod{13} = 1 \quad a_{AB} = 3^3 \pmod{13} = 1$$

$$K = a_{BA} = a_{AB} = 1$$

є спільною точкою кількості

Варіант 5

Варіант 5

- Скласти таблицю Келі групи D_3 , де D_n – група симетрій правильного n -кутника
- У циклічній групі $\langle a \rangle$ порядку n знайти всі елементи порядку k , якщо $n = 140, k = 35$
- Знайти частковий розклад добутку всіх незвідних многочленів степеня 4 у полі Z_3 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многочлени які можна з них одержати.
- Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 5$, секретний ключ $a = 3$, число, що передається — 3.

Таблиця Келі

① Надавши Келі для D_3						
Механічне - геометричне переворотне (поворот на 360°)						
r_{120}	r_{240}	$r_{120} 240^\circ$ поворот.	r_1, r_2, r_3	r_1, r_2, r_3	r_1, r_2, r_3	r_1, r_2, r_3
e	r_{120}	r_{240}	r_1	r_2	r_3	r_1, r_2, r_3
r_{120}	r_{120}	r_{240}	e	r_3	r_1	r_2
r_{240}	r_{240}	e	r_{120}	r_2	r_3	r_1
r_1	r_1	r_2	r_3	e	r_{120}	r_{240}
r_2	r_2	r_3	r_1	r_{240}	e	r_{120}
r_3	r_3	r_1	r_2	r_{120}	r_{240}	e .

Знайти всі елементи порядку

2) У чисел групі порядку n^{40} знайти ел. порядку 35
 $140 : 35 = 4$

Взялимо прості числа див 35 (більшістю)

$b, b^2, b^3, b^4, b^5, b^6, b^7, b^8, b^9, b^{10}, b^{11}, b^{12}, b^{13}, b^{14}, b^{15}, b^{16}, b^{17}, b^{18},$
 $b^{19}, b^{20}, b^{21}, b^{22}, b^{23}, b^{24}, b^{25}, b^{26}, b^{27}, b^{28}, b^{29}, b^{30}, b^{31}, b^{32}, b^{33}, b^{34}$

Всі ел. порядку 35: $a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24}, a^{28}, a^{32}, a^{36}, a^{40}, a^{44}, a^{48},$
 $a^{52}, a^{64}, a^{68}, a^{72}, a^{76}, a^{80}, a^{84}, a^{88}, a^{92}, a^{96}, a^{100}, a^{104}, a^{108}, a^{112}, a^{116}, a^{120},$
 $a^{124}, a^{128}, a^{132}, a^{136}.$

Частковий розклад добутку через кругові многочлени

2. $q=3, n=4$
 $N = \frac{1}{4}(1 - \sum_{d|4} \mu\left(\frac{4}{d}\right) \cdot Q_d) = \frac{1}{4}(1 - \mu(1)Q_1 + \mu(2)Q_2 + \mu(4)Q_4) = \frac{1}{4}(1 - 1 \cdot Q_1 - 1 \cdot Q_2 + 1 \cdot Q_4) = \frac{1}{4}(1 - Q_1 - Q_2 + Q_4)$

$M(q, n, x) = M(3, 4, x) = \prod_{d|4} Q_d(x)$

$q^n - 1 = 3^4 - 1 = 80.$

$3^1 = 3; 3^2 = 9; 3^3 = 27; 3^4 = 81$

$d(80) = 1, 2, 4, 5, 8, 10, 16, 20, 40, 80$

$Q_5 = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 \Rightarrow \mu(5) = 4 \Rightarrow \frac{4}{4} = 1 \text{ и.м.}$

$Q_{10} = \frac{(x^5 - 1)(x^5 + 1)}{(x - 1)(x + 1)} = \frac{x^5 + 1}{x + 1} = x^4 - x^3 + x^2 - x + 1 \Rightarrow \mu(10) = 4 \Rightarrow \frac{4}{4} = 1 \text{ и.м.}$

$$\begin{aligned}
 \Phi_{16} &= \frac{x^8 - 1}{(x^4 - 1)(x^4 + 1)} = \frac{x+1}{x^4 + 1} \Rightarrow \varphi(16) = 8 - 2 = 6 \text{ идем.} \\
 \Phi_{20} &= \frac{x^8 - 1}{(x^{10} - 1)(x^8 + 1)} = \frac{x+1}{x^8 + 1} = x - x + x - x + 1 \Rightarrow \varphi(20) = 8 - 2 = 6 \text{ идем.} \\
 \Phi_{40} &= \frac{x^{16} - 1}{(x^{20} - 1)(x^8 - 1)} = \frac{x+1}{x^{16} + 1} = x - x + x - x + 1 \Rightarrow \varphi(40) = 16 - 2 = 14 \text{ идем.} \\
 \Phi_{80} &= \frac{x^{32} - 1}{(x^{40} - 1)(x^8 - 1)} = \frac{x+1}{x^{32} + 1} = x - x + x - x + 1 \Rightarrow \varphi(80) = 32 - 2 = 30 \text{ идем.}
 \end{aligned}$$

$1+1+2+2+2+8 = 18 = N.$

RSA

14) RSA $p=5, q=5, \alpha=3$, неправильное 3

Алиса неправильное 3

Боб выбирает $p=5, q=5, n=p \cdot q = 25$.

так как $p=q$, $\varphi(25)=20$.

Обычно нужно выбрать такое, что загадывается генератор

$e < e < 20, \text{MCD}(e, 20)=1, e \cdot 3 \equiv 1 \pmod{20} \Rightarrow e=7$.

Боб неправильное Алиси открытый ключ $(20, 7)$.

Алиса использует неправильное 3:

$$c = m^e \pmod{n} = 3^7 \pmod{20} = 12.$$

Боб определяет и генерирует:

$$m = c^d \pmod{n} = 12^3 \pmod{20} = 3.$$

Выполнено неправильное, но симметрично.

Варіант 6

Варіант 6

- Знайти порядок елемента групи $g = \cos \frac{\pi}{5} + i \sin \frac{\pi}{5} \in C^*$, де C^* – мультиплікативна група поля комплексних чисел.
- Знайти обернену матрицю до матриці $g = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 4 & 3 & 4 \end{pmatrix}$ в полі Z_5
- Розкласти даний дріб на найпростіші дроби над полем дійсних чисел за допомогою схеми Горнера $f(x) = \frac{x^3 - 10x + 4}{(x-2)^5}$
- Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 5, q = 7$, секретний ключ $a = 5$, число, що передається — 4.

Знайти порядок елемента групи

Варіант 6

① Порядок $g = \cos \frac{\pi}{5} + i \sin \frac{\pi}{5} \in C^*$
 $g^k = 1^k \cdot \left(\cos \frac{\pi k}{5} + i \cdot \sin \frac{\pi k}{5} \right) = \cos \frac{\pi k}{5} + i \cdot \sin \frac{\pi k}{5}$.

Нейтральний елемент $e=1=g^k$

Множину може k , при якому $\sin \frac{\pi k}{5} = 0$ і
 $\cos \frac{\pi k}{5} = 1$.
 $\cos \frac{\pi k}{5} = 1 ; \frac{\pi k}{2} = 2\pi ; k = 10$.

Перевірка: $g^{10} = 1^{10} \cdot \left(\cos 2\pi + i \cdot \sin 2\pi \right) = 1 + 0 = 1$ – виконується.

Обернена матриця в полі

② Знайти обернений біномній полі \mathbb{Z}_5 до $g = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 1 \\ 4 & 3 & 4 \end{pmatrix}$.

$$\det g = 1 \cdot 1 + 4 + 6 - 1 \cdot 3 - 8 = -1 \pmod{5} = 4.$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 3 & 1 & 0 & 1 & 0 \\ 4 & 3 & 4 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & -2 & 1 & 0 \\ 0 & -1 & 0 & -4 & 0 & 1 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 & -1 \\ 0 & -1 & 1 & 2 & -1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & -3 & 0 & 1 \\ 0 & 1 & 0 & 4 & 0 & -1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & -9 & 1 & 2 \\ 0 & 1 & 0 & 4 & 0 & -1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{pmatrix} \quad g^{-1} = \begin{pmatrix} -9 & 1 & 2 \\ 4 & 0 & -1 \\ 6 & -1 & -1 \end{pmatrix} \pmod{5} = \begin{pmatrix} 1 & 1 & 2 \\ 4 & 0 & 4 \\ 1 & 4 & 4 \end{pmatrix}$$

Розкласти дріб на найпростіші

③ Розкласти на найпростіші $f(x) = \frac{x^3 - 10x + 4}{(x-2)^5}$.

$$g(x) = x^3 - 10x + 4 \text{ розкладаємо за степенеми } x-2$$

$$\begin{array}{r|rrrr} & 1 & 1 & 0 & -10 & 4 \\ \hline 2 & 1 & 1 & 2 & -6 & -8 \\ & 2 & 1 & 4 & 2 & 0 \\ & 2 & 1 & 6 & & \\ & 2 & 1 & & & \end{array}$$

$$g(x) = (x-2)^3 + 6(x-2)^2 + 2(x-2) - 8$$

$$f(x) = \frac{1}{(x-2)^2} + \frac{6}{(x-2)^3} + \frac{2}{(x-2)^4} - \frac{8}{(x-2)^5}$$

RSA

4

RSA $p=5$, $q=7$, $n=5 \cdot 7 = 35$, $\varphi=4$, $e=5$, $m=4$.

Anica перегасае набігашчынне 4.

Будоў сімвал $p=5$, $q=7$. $n=p \cdot q = 5 \cdot 7 = 35$.

$$\varphi = (p-1)(q-1) = 4 \cdot 6 = 24$$

Обираючы чысло e так, што $e \cdot 5 \equiv 1 \pmod{24} \Rightarrow$

$$\Rightarrow e=5.$$

Будоў перегасае Anica ўідкрученій кесэ $(35, 5)$.

Anica шифруе слоў набігашчынне: $c \equiv m^e \pmod{n} = 4^5 \pmod{35} = 9$.

Будоў десіфруе: $m \equiv c^{\frac{1}{e}} \pmod{n} = 9^{\frac{1}{5}} \pmod{35} = 4$.
анімаваючы m .

Варіант 7

Варіант 7

- З'ясувати, чи буде групою множина всіх відображень множини $M = \{1, 2, \dots, n\}$ у себе відносно суперпозиції відображень.
- Чи буде відображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f: R \rightarrow R^+, f(x) = 2^x$
- Знайти всі раціональні корені многочлена $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$
- Дано еліптичну криву $y^2 = x^3 + 7x + 8$ у полі Z_{11} . Знайти дві різні точки на кривій такі що $0 \leq y \leq 5$. Обчислити їх суму

Чи буде групою

1) Чи буде групою множина $M = \{1, 2, \dots, n\}$ у себе?

- Замкненість: виконується.
 $f: M \rightarrow M, g: M \rightarrow M$.
- Асоціативність: дія суперпозиції виконується.
- Нейтральний елемент: $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} = e$.
- Обернений елемент: не виконується.
Іншого відображення, які не мають оберненою.
Приклад: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 3 \end{pmatrix}$. Обернене має бути $\begin{pmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, але таке відображення не існує (не виконується). Отже, не є групою.

Чи буде відображення гомо(ізо)морфізмом

2) $f: R \rightarrow R^+, f(x) = 2^x$. Гомоморфізм? ізоморфізм?

$f(xy) = 2^{xy}$ $\left. \begin{array}{l} \neq, \text{ не є гомоморфізмом та} \\ f(x) + f(y) = 2^x + 2^y \end{array} \right\} \text{ізоморфізмом}$

Знайти всі раціональні корені многочлена

2) $f(x) = 4x^4 + 8x^3 + 15x^2 + 24x + 9$

дР: $\pm 1, \pm 3, \pm 9$; $q^2: \pm 1, \pm 2, \pm 4$

$q: \pm 1, \pm 3, \pm 9, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{3}{2}, \pm \frac{3}{4}, \pm \frac{9}{2}, \pm \frac{9}{4}$ — передбачати що не має сенсу

$m=1: f(1) = 4+8+15+24+9 = -4 \neq 0$

$q+1$ ділиться 4 (чи неспів): $\frac{1}{4} \neq -9$.

$f(-3) = 4 \cancel{8} 324 - 216 + 135 - 72 + \cancel{9} \neq 0$.

$$f\left(-\frac{1}{2}\right) = \frac{1}{4} - 1 + \frac{15}{4} - 12 + 9 = 4 - 1 - 12 + 9 = 0 \quad -\text{корінь}$$

$$f\left(-\frac{3}{4}\right) = \frac{81}{64} - \frac{27}{64} + \frac{15}{16} - \frac{24}{64} + 9 = \frac{53}{64} + 3 \neq 0$$

$$f\left(-\frac{3}{2}\right) = \frac{81}{4} - \frac{27}{4} + \frac{15}{4} - 36 + 9 = -54 + 54 = 0 \quad -\text{корінь}$$

$$f\left(-\frac{3}{4}\right) = \frac{81}{64} - \frac{216}{64} + \frac{135}{16} - 18 + 9 = \frac{-135 + 540 - 576}{64} \neq 0$$

$$f\left(-\frac{9}{8}\right) = \frac{81}{4} - 429 + \frac{125}{4} - 108 + 9 \neq 0$$

$$f\left(-\frac{9}{4}\right) \neq 0$$

Відповідь: $x = -\frac{1}{2}, x = -\frac{3}{2}$ — корені.

Еліптична крива

x	$x^3 + 7x + 8$	y такий, що $y^2 = x^3 + 7x + 8$
0	8	$y^2 = 8 \pmod{11}$ —
1	$16 \pmod{11} = 5$	$y^2 = 5 \pmod{11}$ —
2	$30 \pmod{11} = 8$	$y^2 = 8 \pmod{11}$ —
3	$56 \pmod{11} = 1$	$y^2 = 1 \pmod{11}$ $y=1$
4	$100 \pmod{11} = 1$	$y^2 = 1 \pmod{11}$ $y=1$
5	$168 \pmod{11} = 3$	$y^2 = 3 \pmod{11}$ —
6	$266 \pmod{11} = 2$	$y^2 = 2 \pmod{11}$ —
7	$400 \pmod{11} = 4$	$y^2 = 4 \pmod{11}$ $y=2$
8	$576 \pmod{11} = 4$	$y^2 = 4 \pmod{11}$ $y=2$
9	$800 \pmod{11} = 8$	$y^2 = 8 \pmod{11}$ —
10	$1078 \pmod{11} = 0$	$y^2 = 0 \pmod{11}$ $y=0$

Механізм обчислення точок (x_1, y_1) та (x_2, y_2)

$$N = \frac{y_2 - y_1}{x_2 - x_1} \pmod{11} = \frac{1 - 1}{0 - 1} \pmod{11} = 0.$$

$$x_3 = (N^2 - x_1 - x_2) \pmod{11} = (0 - 3 - 4) \pmod{11} = 4$$

$$y_3 = (N(x_1 - x_3) - y_1) \pmod{11} = (0(3 - 4) - 1) \pmod{11} = 10.$$

Сума точок $(3, 1)$ та $(4, 1)$ є $(4, 10)$

Варіант 8

Варіант 8

- Довести, що у групі $(ab)^{-1} = b^{-1}a^{-1}$.
- Визначити кількість генераторів мультиплікативної групи поля $Z_3[7]$. Знайти хоча б один.
- Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_3 за допомогою незвідного многочлена $F[x] = x^4 + x^3 + x^2 + x + 1$
- Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сесійний код Аліси $k = 3$, число, що передається $u = 2$.

Довести

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

Довести, що $(ab)^{-1} = b^{-1}a^{-1}$.

Безпосередньо слідує з твердження $(ab)^{-1}(ab) = \theta$

$$(ab)^{-1}(ab) = \theta$$

$$(ab)^{-1}abb^{-1} = b^{-1}$$

$$(ab)^{-1}abb^{-1}a^{-1} = b^{-1}a^{-1}$$

Визначити кількість та один генератор

2 Визначити кількість генераторів групи числа \mathbb{Z}_37^* .
 $\varphi(37) = 36$. $\varphi(36) = 12$. Оскільки група \mathbb{Z}_{37}^* має 12 генераторів. Заданий один.

Тривіальні дільники 36: 2, 3
Умова: $g^{\frac{n}{p}} \neq 1 \pmod{37}$. нерівнісні дільники

$g^{\frac{36}{2}}, g^{\frac{36}{3}}$

$g=2: 2^{18} \pmod{37} = 36 \neq 1$
 $2^{12} \pmod{37} = 26 \neq 1$ } + генератори

$g=3: 3^{18} \pmod{37} = 1$
 $3^{12} \pmod{37} = 10 \neq 1$ } не є генераторами, оскільки коріння елемента числа 36

Знайти обернений елемент у розширеній поля

$$1) G(x) = x^4 + 2x^3 + 1, F(x) = x^4 + x^3 + x^2 + x + 1$$

Розв'язок алг. способом:

$$\begin{array}{r} x^4 + x^3 + x^2 + x + 1 \\ x^4 + 2x^3 + x^2 \\ \hline 2x^3 - x + 1 \\ 2x^2 + 4x^3 + 2x \\ \hline 2x^3 + 2x^2 + 1 \\ - 2x^3 + 4x^2 + 2 \\ \hline x + 2 \end{array} \rightarrow x+2 \cdot F(x) = G(x)(x^4 + 2x^3 + 2)$$

$$\begin{array}{r} x^4 + 2x^3 + 1 \\ x^4 + 2x \\ \hline 1 \end{array} \rightarrow 1 = G(x) - (F(x) - G(x) \cdot (x^4 + 2x)) \cdot x = G(x)(x^3 + 2x^2 + 2x + 1) - F(x) \cdot x.$$

Д: обернений ел. $x^3 + 2x^2 + 2x + 1$.

(TODO)Ель Гамаля

Варіант 9

Варіант 9

1. Довести, що в будь-якій групі парного ступеня є елемент порядку 2.
2. Знайти символ Лежандра/Якобі $(\frac{39}{209})$
3. Відокремити дійсні корені многочлена $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$
4. Дано еліптичну криву $y^2 = x^3 + 2x + 3$ у полі Z_{13} . Знайти дві різні точки на кривій такі що $0 \leq y \leq 6$.
Обчислити їх суму

Довести

$$x^{-1} = x \Rightarrow e = x \cdot x = x^2$$

Попарно, якщо можливо, кожен елемент G зіставимо з його оберненим і зауважимо, що

$$g^2 \neq e \Leftrightarrow g \neq g^{-1} \Leftrightarrow \text{існує пара } (g, g^{-1})$$

Тепер, є один елемент, який не має пари: одиничний елемент e (оскільки справді $e = e^{-1} \Leftrightarrow e^2 = e$),

тож, оскільки кількість елементів у G парна, має існувати принаймні ще один елемент, позначимо $a \neq e \in G$, без пари, і таким чином

$$a = a^{-1} \Leftrightarrow a^2 = e$$

(TODO) Символ Лежандра/Якобі

Відокремити дійсні корені

③ Відокремити дійсні корені $f(x) = x^4 - x^3 - 4x^2 + 4x + 1$

$$f = x^4 - x^3 - 4x^2 + 4x + 1$$

$$f' = 4x^3 - 3x^2 - 8x + 4 = f_0$$

$$\begin{array}{r|l} x^4 - x^3 - 4x^2 + 4x + 1 & 4x^3 - 3x^2 - 8x + 4 \\ \hline x^4 - \frac{3}{4}x^3 - 2x^2 + x & \frac{1}{4}x - \frac{1}{16} \\ -\frac{1}{4}x^3 - 2x^2 + 3x + 1 & \\ -\frac{1}{4}x^3 + \frac{3}{16}x^2 + \frac{1}{2}x - \frac{1}{4} & \\ \hline -\frac{35}{16}x^2 + \frac{5}{2}x + \frac{5}{4} & \end{array}$$

$$f_1 = \frac{35}{16}x^2 - \frac{5}{2}x - \frac{5}{4} = 35x^2 - 40x - 20 = 7x^2 - 8x - 4$$

$$\begin{array}{r|l} 4x^3 - 3x^2 - 8x + 4 & 7x^2 - 8x - 4 \\ \hline 4x^3 - \frac{32}{7}x^2 - \frac{16}{7}x & \frac{4}{7}x + \frac{11}{49} \\ \hline \frac{11}{7}x^2 - \frac{40}{7}x + 4 & \\ \frac{11}{7}x^2 - \frac{88}{49}x - \frac{44}{49} & \\ \hline -\frac{192}{49}x + \frac{240}{49} & \end{array}$$

$$f_2 = \frac{192}{49}x - \frac{240}{49} = 192x - 240 = 48x + 60 = 12x - 15$$

$$\begin{array}{r|l} 7x^2 - 8x - 4 & 12x - 15 \\ \hline 7x^2 - \frac{35}{4}x & \frac{7}{12}x + \frac{3}{16} \\ \hline \frac{3}{4}x - 4 & \\ \frac{3}{4}x - \frac{15}{16} & \\ \hline -\frac{49}{16} & \end{array}$$

$$f_3 = -\frac{49}{16}$$

	f	f_0	f_1	f_2	f_3	S
$-\infty$	+	-	+	-	-	3
∞	+	+	+	+	-	1
0	+	+	-	-	-	1
-1	-	+	+	-	-	2
-2	+	-	+	-	-	3

Дійсні корені зна-
ходяться в про-
межах: $(-1, 0)$ і
 $(-2, -1)$.

Еліптична крива

4	Ел. крива: $y^2 = x^3 + 2x + 3 \pmod{13}$: $0 \leq y \leq 6$
x	$x^3 + 2x + 3$
0	3
1	4
2	$15 \pmod{13} = 2$
3	$36 \pmod{13} = 10$
4	$75 \pmod{13} = 10$
5	$138 \pmod{13} = 8$
6	$231 \pmod{13} = 10$
7	$360 \pmod{13} = 9$
8	$531 \pmod{13} = 11$
9	$750 \pmod{13} = 9$
10	$1023 \pmod{13} = 9$
11	$1356 \pmod{13} = 4$
12	$1755 \pmod{13} = 0$
	$y^2 = 3 \pmod{13}$
	$y^2 = 4 \pmod{13}$
	$y^2 = 8 \pmod{13}$
	$y^2 = 10 \pmod{13}$
	$y^2 = 11 \pmod{13}$
	$y^2 = 9 \pmod{13}$
	$y^2 = 0 \pmod{13}$
	$y = 2$
	$y = 3$
	$y = 2$
	$y = 3$
	$y = 3$
	$y = 2$
	$y = 0$

Нехай обирено точки $(1, 2)$ та $(7, 3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{13} = \frac{\frac{3-2}{7-1}}{6} \pmod{13} = 6 \cdot 6^{-1} \pmod{13}$$

$$6 \cdot 6^{-1} \pmod{13} = 1 \pmod{13}$$

$$\lambda = 11 \pmod{13}$$

$$x_3 = (\lambda^2 - x_1 - x_2) \pmod{13} = (121 - 1 - 7) \pmod{13} = 9$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{13} = (11(1-9) - 2) \pmod{13} = 2$$

Отже, сума 1020к $(1, 2)$ та $(7, 3) = (9, 2)$

Варіант 10

Варіант 10

- Знайти порядок елемента групи $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 6 & 1 & 5 & 8 & 7 \end{pmatrix} \in S_8$
- Розв'язати рівняння $x^2 - (3 + 3\sqrt{2})x + 4 + 6\sqrt{2}$ у полі $Q(\sqrt{2})$.
- Знайти частковий розклад добутку всіх незвідних многочленів степеня 3 у полі Z_5 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многочлени які можна з них одержати.
- Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен x^3+x+1 за модулем 2, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сесійний код Аліси $k = 5$, число, що передається $u = 4$.

Порядок елемента групи

Варіант 10

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 6 & 1 & 5 & 8 & 7 \end{pmatrix} \in S_8$

~~$(12)(123465)(78)$~~

$H(K(2,6)) = 6 \Rightarrow \text{порядок групи} - 6$

Розв'язати рівняння у полі

$$2. \quad x^2 - (3 + 3\sqrt{2})x + 4 + 6\sqrt{2} \in Q(\sqrt{2})$$

$$\Delta = b^2 - 4ac = (3 + 3\sqrt{2})^2 - 4(4 + 6\sqrt{2}) =$$

$$= 9 + 18\sqrt{2} + 18 - 16 - 24\sqrt{2} = 11 - 6\sqrt{2}$$

$$\Delta = (a - b\sqrt{2})^2 = a^2 - 2ab\sqrt{2} + 2b^2$$

$$\begin{cases} 11 = a^2 + 2b^2 \\ 6\sqrt{2} = 2ab\sqrt{2} \end{cases} \quad \begin{cases} 11 = a^2 + 2b^2 \\ 3 = ab \end{cases} \quad \begin{cases} a = 3 \\ b = 1 \end{cases}$$

$$\Delta = (3 - \sqrt{2})^2$$

$$x_1 = \frac{3 + 3\sqrt{2}}{2} - 3 + \sqrt{2} = \frac{4\sqrt{2}}{2} = 2\sqrt{2} \in Q(\sqrt{2})$$

$$x_2 = \frac{3 + 3\sqrt{2}}{2} + 3 - \sqrt{2} = \frac{6 + 2\sqrt{2}}{2} = 3 + \sqrt{2} \in Q(\sqrt{2})$$

Ось, x_1 і x_2 - корені

Частковий розклад через кругові многочлени

4 $q=5, n=3$

$$N = \frac{1}{3}(-5 + 125) = 40$$

$$q^n - 1 = 5^3 - 1 = 124.$$

$$5 - 5, \quad 5^2 = 25, \quad 5^3 = 125$$

$$\frac{1}{3} \cdot \frac{x^3 - 1}{x - 1} = \frac{x^2 + x + 1}{x - 1} = x + x + 1 \dots + x + k + 1 \rightarrow \frac{30}{3} = 10 \text{ НМ}$$

1	4	62	31	4	2	1
x	x	x	↓	✓	✓	✓
1	2	4	31	62	124	
1	-1	0	-1	1	0	

$$\Phi_{62} = \frac{(x^{62}-1)(x-1)}{(x^2-1)(x^4-1)} = \frac{x^{61}+1}{x+1} = x - x^{29} + \dots + x^{-k+1} \rightarrow \frac{30}{63} = 10 \text{ НМ}$$

$$\Phi_{124} = \frac{(x^{124}-1)(x^2-1)}{(x^6-1)(x^4-1)} = \frac{x^{123}+1}{x^2+1} = x^{60} - x^{58} + x^{56} - \dots + x^4 - x^2 + 1 \rightarrow 20 \text{ НМ}$$

$$10 + 10 + 20 = 40 = N.$$

Клас кругових НМ

П.: 2020 рік зміни

(TODO)Ель Гамаля

Варіант 11

Варіант 11

- Нехай порядок елемента x у групі дорівнює N . Довести, що порядок елемента x^{-1} також дорівнює N .
- З'ясувати, чи буде множина M відносно звичайних операцій додавання та множення полем. Знайти обернений елемент для елемента a . $M = Z_{143}$, $a = 97$.
- Знайти частковий розклад добутку всіх незвідних многочленів степеня 6 у полі Z_2 через кругові многочлени. Обчислити явний вигляд всіх кругових многочленів у розкладі. Знайти всі незвідні кругові многочлени та многочлени які можна з них одержати.
- Проілюструвати обчислення спільного таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 19$, генератор знайдіть та виберіть довільний.

Довести

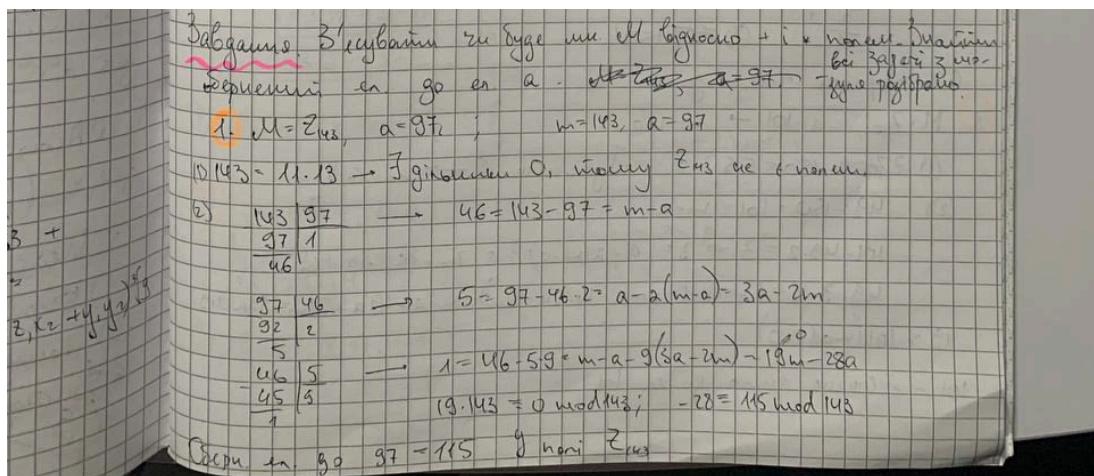
Нехай порядок елемента x дорівнює N . Довести, що порядок елемента x^{-1} також дорівнює N

Справді, нехай $x^N = \theta$. Помножимо ліву та праву частину рівності на $(x^{-1})^N$, отримаємо

$$\theta = (x^{-1})^N x^N = (x^{-1})^N \theta = (x^{-1})^N$$

Нехай від супротивного існує $n < N$ таке що $(x^{-1})^n = \theta$. Помноживши обидві частини рівності на x^n отримаємо $x^n = \theta$ (суперечність тому, що порядок елемента x дорівнює N).

З'ясувати чи буде множина - полем



Частковий розклад добутку через кругові многочлени

$1 \quad q=2, \quad n=6.$
 $N = \frac{1}{6} \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot q^d$
 $N = \frac{1}{6} (2 - 4 - 8 + 64) = 9. \quad - \text{кількість необхідних.}$
 $M(q, n, x) = \prod_{m=1}^n Q_m(x)$
 $q^6 - 1 = 63;$
 $2 \equiv 1 \pmod{3} \rightarrow x, \quad 2^3 \equiv 1 \pmod{7} \rightarrow x$
 $M(2, 6, x) = Q_3(x) \cdot Q_2(x) \cdot Q_6(x)$
 $Q_3(x) = x^6 + x^3 + 1 \Rightarrow q(3) = 6 \Rightarrow 1 \text{ необхідний степ.}$
 $Q_2(x) = x^4 + x^2 + 1 \rightsquigarrow \text{наймен. степ. } = 12 \Rightarrow \begin{array}{l} u(2) = 12 \\ q(12) = 36 \end{array} \text{ мінімальний} \begin{array}{l} \text{розв'язок} \\ \text{розв'язок} \end{array} \begin{array}{l} \text{найден} \\ \text{найден} \end{array} \begin{array}{l} \text{за} \\ \text{за} \end{array} \begin{array}{l} \text{у} \\ \text{у} \end{array} \begin{array}{l} \text{6} \\ \text{6} \end{array} \text{ кв.}$
 $Q_6(x) = x^6 + x^2 + 1 \rightsquigarrow \text{наймен. степ. } = 36 \Rightarrow \text{мінімальний} \begin{array}{l} \text{розв'язок} \\ \text{розв'язок} \end{array} \begin{array}{l} \text{найден} \\ \text{найден} \end{array} \begin{array}{l} \text{за} \\ \text{за} \end{array} \begin{array}{l} \text{у} \\ \text{у} \end{array} \begin{array}{l} \text{6} \\ \text{6} \end{array} \text{ кв.}$
 $1+2+6 = 9 = N$
 $Q_3 - \text{єдиний круговий кв.}$
 $\text{Підстановка замін. } x \rightarrow x+1:$
 $(x+1)^6 + (x+1)^2 + 1 = x^6 + x^4 + x^3 + x + 1 \quad - \text{новий необхідний кв.}$

Діффі-Гелмана

4. $p=19, \quad q=3;$

// Квадрат схороне число $a=4$ має одинакове:

$$A = q^a \pmod{p} = 3^4 \pmod{19} = 5 // \text{Квадрат надає бодега } A=5$$

// Бодег одержав схороне число $b=3$ має одинакове:

$$B = q^b \pmod{p} = 3^3 \pmod{19} = 8 // \text{Бодег надає квадрат } B=8$$

// Квадрат обчислюється $a_{BA} = B^a \pmod{p} // \quad // \text{Бодег обчислює } a_{AB} = A^b \pmod{p} //$

$$a_{BA} = B^a \pmod{19} = 11 \quad a_{AB} = 5^3 \pmod{19} = 11$$

Спільне зрозуміло $K = a_{BA} = a_{AB} = 4$
& спільним таємним числом.

Варіант 12

Варіант 12

- З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p .
- Розв'язати систему рівнянь $\begin{cases} 2x - y = 5 \\ x - 2y = 10 \end{cases}$ в кільці Z_{18}
- Знайти елемент обернений до $G[x] = x^2 + 2x + 1$ у розширенні поля Z_7 за допомогою незвідного многочлена $F[x] = x^3 + x^2 + x + 2$
- Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 3$, сесіонний код Аліси $k = 5$, число, що передається $u = 3$.

Чи буде кільцем

2) Відносно "+", "·" чи \mathbb{Q} , у нескоротому записі їхніх значень є степенеми простого числа p .

(1) Замкненість: для "+": $\frac{a_1}{p^{k_1}} + \frac{a_2}{p^{k_2}} = \frac{a_1 p^{k_2} + a_2 p^{k_1}}{p^{k_1+k_2}} \in \mathbb{Q}$
Небільш у випадку скорочення значення все одно буде степенем p — замкненість ✓
для "·": $\frac{a_1}{p^{k_1}} \cdot \frac{a_2}{p^{k_2}} = \frac{a_1 a_2}{p^{k_1+k_2}}$ — замкненість ✓

(2) Асоціативність: $\left(\frac{a_1}{p^{k_1}} + \frac{a_2}{p^{k_2}} \right) + \frac{a_3}{p^{k_3}} = \frac{a_1}{p^{k_1}} + \left(\frac{a_2}{p^{k_2}} + \frac{a_3}{p^{k_3}} \right)$ — ✓
для "+": $\left(\frac{a_1}{p^{k_1}} \cdot \frac{a_2}{p^{k_2}} \right) \cdot \frac{a_3}{p^{k_3}} = \frac{a_1}{p^{k_1}} \left(\frac{a_2}{p^{k_2}} \cdot \frac{a_3}{p^{k_3}} \right)$ — ✓

(3) Нейтр. ел.: $\frac{a}{p^0} = 0$ — ✓

(4) Оберн. ел. для "+": для числа a , $b = -a$ — обернений.

(5) Комутативність: $a + a_2 = a_2 + a_1$ — ✓
 $a \cdot b = b \cdot a$ — ~~$a \cdot b = b \cdot a$~~

(7) Дистрибутивність: наявна чи не значення є чи \mathbb{Q} , а як \mathbb{Q} — дистрибутивність є очевидно.

Система рівнянь

3. $\begin{cases} 2x - y = 5 \mid \cdot (-2) \\ x - 2y = 10 \end{cases} \quad \begin{cases} -4x + 2y = -10 \\ x - 2y = 10 \end{cases} \quad \begin{array}{l} -3x = 0 \mod 18 \\ 15x = 0 \end{array}$

$\text{NOD}(15, 18) = 3 \Rightarrow x = 6k \Rightarrow x = \{0, 6, 12\}$

$x = 0: y = -5 \mid \text{mod } 18 \Rightarrow y = 13$

$x = 6: y = 12 - 5 = 7$

$x = 12: y = 24 - 5 = 19 \mid \text{mod } 18 \Rightarrow y = 1$.

Відповідь: $(0, 13); (6, 7); (12, 1)$.

ще б понять що тут відбувається

Обернений елемент у розширені поля

3. $G(x) = x^2 - 2x - 1, F(x) = x^3 + x^2 + x + 2$

$$\begin{array}{r} x^3 + x^2 + x + 2 \\ - x^2 - 2x - 1 \\ \hline x^2 + x \\ - x - 1 \\ \hline x \\ - x \\ \hline 0 \end{array} \rightarrow 2x + 3 = F(x) - G(x)(x+6)$$

$$\begin{array}{r} x^2 + 2x + 1 \\ - x^2 - 5x \\ \hline 2x + 3 \\ - 2x - 3 \\ \hline 0 \end{array} \rightarrow 2 = G(x) - (2x+3)(4x+2) =$$

$$\begin{array}{r} x^2 + 2x + 1 \\ - x^2 - 5x \\ \hline 2x + 3 \\ - 2x - 3 \\ \hline 0 \end{array} \rightarrow 2 = G(x) - (2x+3)(4x+2) =$$

$$\begin{array}{r} 2x + 3 \\ - 2x \\ \hline 0 \end{array} \rightarrow 1 = (2x+3) - 2 \cdot F(x) - G(x)(x+6) =$$

$$= G(x)(4x^2 + 5x + 5) + F(x)(4x+2) =$$

$$= G(x)(-4x^2 - 5x - 5 - x - 6) + F(x)(4x+3) \mod 7 =$$

$$= G(x)(3x^2 + x + 3) + F(x)(4x+3)$$

обернений ел.

(TODO) Ель Гамаля

Варіант 13

Варіант 13

- З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина раціональних чисел, у нескоротному записі яких знаменники є дільниками фіксованого натурального числа n .
- Знайти всі генератори мультиплікативної групи поля Z_{19}
- Визначити кратність кореня c для многочлена $f(x)$. Знайти значення многочлена $f(x)$ і його похідних у точці $x = x_0$. $f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24$, $c = -2$, $x_0 = -1$.
- Проілюструвати обчислення спільногого таємного ключа за протоколом Діффі-Гелмана. Параметри: $p = 17$, генератор знайдіть та виберіть довільний.

Чи буде кільцем

1) Відносно звич. опер. $+$, \cdot на \mathbb{Q} , у нескоротному записі завинільше знає. є дільник фіксованого $n \in \mathbb{N}$.
Множення є кільцем, тому відносно додавання бона є
абелевою групою, а відносно множення - напіввируковою, і має
динамік. може відносно \cdot є вправа, також і ліва.
Неступ. вп.: $\exists p \in \mathbb{Q} : p \neq 0$, $\exists q \in \mathbb{Q} : q \neq 1$.

Задуманість: $\exists p \in \mathbb{Q}, q \in \mathbb{Q}, p \neq 0, q \neq 1$,
 $\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 \cdot p_2}{q_1 \cdot q_2}$.
 $p_1, p_2 \in \mathbb{Q}, q_1, q_2$ - дільники $n \in \mathbb{N}$.
Множення з обох рах дає рах число: $p_1 \cdot p_2 \in \mathbb{Q} \rightarrow \checkmark$
Чи буде $q_1 \cdot q_2$ дільником числа n ?
Наведемо контрприклад: $n=100$, $q_1=50$, $q_2=20 \rightarrow q_1 \cdot q_2 = 1000$
1000 не є дільником 100.
Будь-жов! Єдиний підумагай, що $q_1 \cdot q_2$ гарантіює завиніль
є дільниками n : $n=1$, тоді $q_1=q_2=1$ і $q_1 \cdot q_2=1$.
Однак, не є кільце звич бах відм $n=1$.

Знайти генератори

2) Знайти всі генератори \mathbb{Z}_{19}^*

$\varphi(19)=18$. Щоб відповісти на це питання, треба знати всі дільники 18: 2, 3.

Умова: $g^{\frac{n}{d}} \not\equiv 1 \pmod{19}$ (тобто $g^{\frac{18}{2}}, g^{\frac{18}{3}}$)

$g=2 \cdot 2^9 \pmod{19} = 18 \quad \left. \begin{array}{l} \\ \end{array} \right\} \in \text{генератори},$
 $\cdot 2^6 \pmod{19} = 1$

$g=3 \cdot 3^9 \pmod{19} = 18 \quad \left. \begin{array}{l} \\ \end{array} \right\} \in \text{генератори}$
 $3^6 \pmod{19} = 1$

Чтоб знайти інші генератори, використовуємо $g=2$ і

скориставшись табличкою $g^k \pmod{19}$ для $\text{NCD}(k, 18) = 1$

$k = \{1, 5, 7, 11, 13, 17\}$

Щепер шукамо $g^k \pmod{19}$ ($g=2$)

$2^1 \pmod{19} = 2$	$2^4 \pmod{19} = 15$
$2^5 \pmod{19} = 13$	$2^{13} \pmod{19} = 3$
$2^7 \pmod{19} = 14$	$2^{17} \pmod{19} = 10$

Всі генератори: $\{2, 3, 10, 13, 14, 15\}$.

Кратність кореня

Задача 13

$$3. f(x) = 2x^5 + 12x^4 + 27x^3 + 34x^2 + 36x + 24 \quad |, c = -2; x_0 = -1$$

C	2	12	27	34	36	24
-2	2	8	11	12	12	0
-2	2	4	3	6	0	
-2	2	0	3	0		
-2	2	-4	11	±0		=> кратність 3.

x_0	2	12	27	34	36	24	$f(-1) = 5$
-1	2	10	17	17	19	5	$f'(-1) = 11 \cdot 1! = 11$
-1	2	8	9	8	11		$f^{(2)}(-1) = 5 \cdot 2! = 10$
-1	2	6	3	5			$f^{(3)}(-1) = -7 \cdot 3! = -6$
-1	2	4	-1				$f^{(4)}(-1) = 2 \cdot 4! = 48$
-1	2	2					$f^{(5)}(-1) = 2 \cdot 5! = 240$
-1	2						

Діффі-Гелмана

Ч. Діффі - Гелмана

$$p = 17, g = 3$$

// Клієнта обирає скріпче число $a = 4$ та обчислює:

$$A = g^a \pmod{p} = 3^4 \pmod{17} = 13$$

// Клієнта надає біду $A = 13$

// Бід обирає скріпче число $b = 3$ та обчислює:

$$B = g^b \pmod{p} = 3^3 \pmod{17} = 10$$

// Бід надає клієнту $B = 10$

// Клієнта обчислює $\alpha_{BA} = B^a \pmod{p}$ //

$$\alpha_{BA} = 10^4 \pmod{17} = 9$$

// Бід обчислює $\alpha_{AB} = A^b \pmod{p}$ //

$$\alpha_{AB} = 13^3 \pmod{17} = 9$$

Спільне згенероване $K = \alpha_{BA} = \alpha_{AB} = 9$
 \in спільному поліному множини

Варіант 14

Варіант 14

- З'ясувати, чи буде кільцем відносно звичайних операцій додавання та множення множина комплексних матриць вигляду $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$
- Чи буде віображення f гомоморфізмом? Чи буде воно ізоморфізмом? $f : C^* \rightarrow R^*, f(z) = \frac{1}{|z|}$
- Знайти всі раціональні корені многочлена $f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$
- Проілюструвати шифрування та дешифрування за протоколом RSA з параметрами: $p = 3, q = 7$, секретний ключ $a = 7$, число, що передається — 2.

Чи буде кільцем

5. ~~Задача~~ Співставлення $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$.

(1) Замкненість: $+ : \begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} + \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 + z_2 & w_1 + w_2 \\ -(\bar{w}_1 + \bar{w}_2) & \bar{z}_1 + \bar{z}_2 \end{pmatrix}$
 За $\bar{z}_1 + \bar{z}_2 = \bar{z}_1 + \bar{z}_2$; $\bar{w}_1 + \bar{w}_2 = \bar{w}_1 + \bar{w}_2$
 Отже отримали: $\begin{pmatrix} z_1 + z_2 & w_1 + w_2 \\ -(\bar{w}_1 + \bar{w}_2) & \bar{z}_1 + \bar{z}_2 \end{pmatrix} - \checkmark$

*: $\begin{pmatrix} z_1 z_2 - w_1 w_2 & z_1 w_2 + w_1 \bar{z}_2 \\ -(\bar{z}_1 \bar{w}_1 + \bar{z}_2 \bar{w}_2) & \bar{z}_1 \bar{z}_2 - \bar{w}_1 \bar{w}_2 \end{pmatrix} \leftarrow \curvearrowright$

За $\bar{z}_1 \bar{z}_2 = \bar{z}_1 \bar{z}_2$: $(z_1 \bar{w}_2 + \bar{z}_1 \bar{w}_2) = (\bar{z}_1 w_2 + w_1 \bar{z}_2)$
 $(\bar{z}_1 \bar{z}_2 - \bar{w}_1 \bar{w}_2) = (\bar{z}_1 \bar{z}_2 - \bar{w}_1 \bar{w}_2)$ — \checkmark

Замкненість.

(2) Анал: \checkmark

(3) Коефіц. ен: $+ \oplus$ ~~Коефіц. матр.~~

(4) Оберн. ен: $\exists +$: $A = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}; B = -A = \begin{pmatrix} -z & -w \\ \bar{w} & \bar{z} \end{pmatrix}$
 Несимпл. викон.

Е кільце.

Відображення гомо(ізо)морфізм

$$2. f : C^+ \rightarrow R^+, f(z) = \frac{1}{|z|}$$

$$f(x \cdot y) = \frac{1}{|x \cdot y|}$$

$$f(x) \cdot f(y) = \frac{1}{|x|} \cdot \frac{1}{|y|}$$

$$f(x) \cdot f(y) \neq f(x \cdot y) \Rightarrow$$

\Rightarrow не гомоморфізм \Rightarrow не ізоморфізм

Раціональні корені многочлена

$$3. f(x) = 6x^4 - 5x^3 + 16x^2 + 4x - 3$$

Всі дільники 3: $\pm 1, \pm 3$ (p)

Всі дільники 6: $\pm 1, \pm 2, \pm 3, \pm 6$ (q)

$$\frac{p}{q} = \pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2}, \pm \frac{1}{3}, \cancel{\pm \frac{1}{6}}$$

$f(1) = 18 \neq 0; f(-1) = 21 \neq 0; f(-3) = 750 \neq 0$

$f(3) = 504 \neq 0; f\left(\frac{1}{2}\right) = 2,75 \neq 0; \cancel{f\left(-\frac{1}{2}\right) = 0}$

$f\left(\frac{-3}{2}\right) = 74,25 \neq 0; f\left(\frac{3}{2}\right) = 52,5 \neq 0; \cancel{f\left(\frac{1}{3}\right) = 0}$

$f\left(\frac{1}{6}\right) \approx -1,9 \neq 0; f\left(-\frac{1}{6}\right) \approx -3,1 \neq 0$

Отже: $x = -\frac{1}{2}$ ма $x = \frac{1}{3}$

RSA(?????)

Задача 24

4. RSA

$p=3, q=7, a=7, m=2$

$n = 3 \cdot 7 = 21$ // Бод односиме

$\varphi(n) = (p-1)(q-1); \varphi(21) = 6 \cdot 6 = 12$

$e = 7$

$\text{HCD}(12, 7) = 1$

$de \equiv 1 \pmod{12}$

$d = 5 \equiv 1 \pmod{12} \rightarrow \text{Беремъ къмъ това}$

$a = d = 5; \checkmark // \text{Бод неправ} (n, e) = (21, 7)$

// Ако искаме

$c = m^e \pmod{n} = 2^5 \pmod{21} = 32$

// Ако искаме здравоправният отговор $c = 32$

// Бод генерират

$m = c^d \pmod{n} = 32^5 \pmod{21} = 167051 \pmod{21} = 2$

Варіант 15

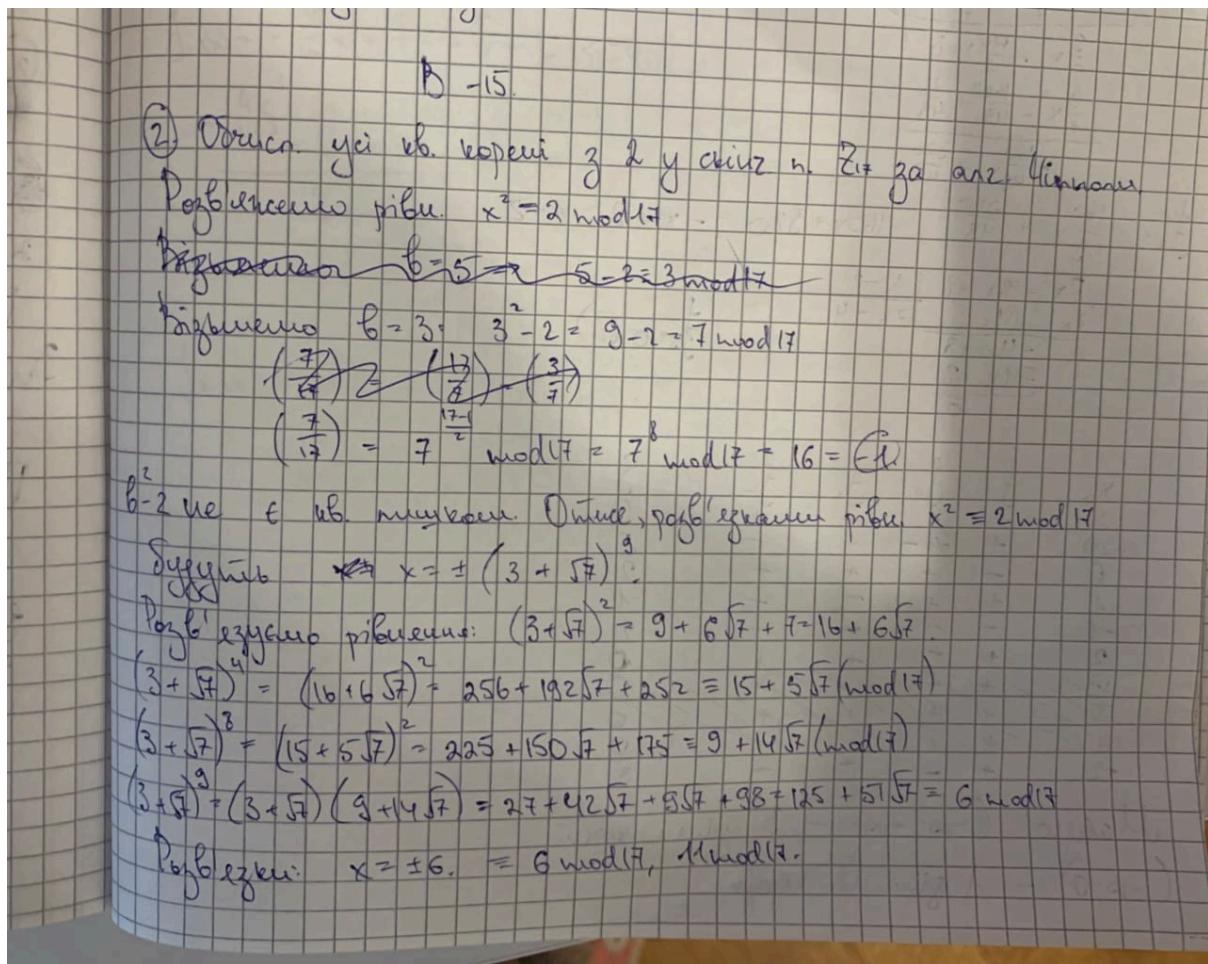
Варіант 15

- Знайти порядок елемента групи $g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \in GL_3(\mathbb{Z})$, де $GL_n(\mathbb{Z})$ – група за множенням усіх невироджених ціличисельних матриць порядку n , обернені до яких також є ціличисельними
- Обчислити всі квадратині корені з 2 у скінченному полі Z_{17} за алгоритмом Чіпполи
- Знайти порядок многочлена x у розширенні поля Z_3 за допомогою незвідного многочлена $x^3 + 2x + 2$
- Проілюструвати шифрування та дешифрування за протоколом Ель Гамаля з параметрами: незвідний многочлен $x^2 + 2x + 2$ за модулем 3, корінь якого є примітивним елементом розширення поля; секретний ключ Боба $a = 4$, сесновий код Аліси $k = 3$, число, що передається $u = 2$.

Знайти порядок елемента групи

$$1, g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \in GL_3(\mathbb{Z}), \text{ за множенням}$$
$$g^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$
$$g^3 = g^2 \cdot g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$
$$g^9 = g^3 \cdot g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Rightarrow \vartheta(g) = 4$$

Алгоритм Чіпполи



(TODO) Знайти порядок многочлена за допомогою незвідного многочлена

(TODO) Ель Гамаль

Алгоритм розв'язку для еліптичних кривих

1. Знайти точки на еліптичній кривій
 $y^2 = x^3 + 7x + 8$ в полі \mathbb{Z}_{11} .

Алгоритм

Черг. задача еліптична крива $y^2 = x^3 + ax + b \pmod p$
 Для кожного значення $0 \leq x \leq p-1$:

- 1) обчислюємо $A = x^3 + ax^2 + b \pmod p$
- 2) вирішуємо порівняння $y^2 = A \pmod p$. Якщо
 порівняння має розв'язок, то є два значення y
 (крім випадку $y=0$) - $y_1, y_2 : y^2 = A \pmod p$.

У цьому випадку точки $(x_1, y_1), (x_2, y_2)$ належать
 еліптичній кривій.

$$\mathbb{Z}_{11} = \{0, 1, 2, \dots, 10\}$$

x	$x^3 + 7x + 8 \pmod{11}$	y такий, що $y^2 = x^3 + 7x + 8 \pmod{11}$
0	8	$y^2 = 8 \pmod{11}$
1	$16 \pmod{11} = 5$	$y^2 = 5 \pmod{11}$
2	$30 \pmod{11} = 8$	$y^2 = 8 \pmod{11}$
3	$52 \pmod{11} = 8$	$y^2 = 8 \pmod{11}$
4	$96 \pmod{11} = 8$	$y^2 = 8 \pmod{11}$
5	$180 \pmod{11} = 4$	$y^2 = 4 \pmod{11}$
6	$324 \pmod{11} = 5$	$y^2 = 5 \pmod{11}$
7	$544 \pmod{11} = 5$	$y^2 = 5 \pmod{11}$
8	$888 \pmod{11} = 9$	$y^2 = 9 \pmod{11}$
9	$1404 \pmod{11} = 2$	$y^2 = 2 \pmod{11}$
10	$2150 \pmod{11} = 5$	$y^2 = 5 \pmod{11}$

Однак, з таблиці бачимо, що є дві точки
 $(5, 2)$ і $(8, 3)$

Сума двох точок на еліптичній кривій також утворює точку на тій же кривій.

Діяльність двох точок $P_1 = (x_1, y_1)$ і $P_2 = (x_2, y_2)$ — точка еліптичної кривої, їхні координатами є точки $P_3 = P_1 + P_2 = (x_3, y_3)$ відповідної формулами

$$x_3 = (\lambda^2 - x_1 - x_2) \pmod{p}$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{p}$$

Якщо $P_1 \neq P_2$, то $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$

Якщо $P_1 = P_2$, то $\lambda = \frac{3x_1^2 + a}{2y_1} \pmod{p}$,

де $y^2 = x^3 + ax + b \pmod{p}$ — p -у еліптична кривої.

Оскільки $(5, 2) \neq (8, 3)$, маємо

$$\lambda = \frac{3 - 2}{8 - 5} \pmod{11} = \frac{1}{3} \pmod{11}.$$

Перебираємо всі $x \in \{1, 2, \dots, 10\}$ точку не згаданою та може бути

$$3 \cdot x = 1 \pmod{11}$$

Оскільки $3 \cdot 4 = 12 = 1 \pmod{11}$

$$\Rightarrow \lambda = 4 \pmod{11}$$

Знайдено координати третьої точки (x_3, y_3)

$$x_3 = (\lambda^2 - x_1 - x_2) \pmod{11} = (4^2 - 5 - 8) \pmod{11} = 3 \pmod{11}$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{11} = (4(5 - 3) - 2) \pmod{11} = 6 \pmod{11}$$

Оскільки точка $(3, 6)$.

RSA

СХЕМА RSA. Нехай Аліса хоче надіслати Бобу повідомлення $m \in \mathbb{N}$. Боб генерує пару різних простих чисел p, q приблизно одного розміру та обчислює $n = pq$, $\phi = \phi(n) = (p - 1)(q - 1)$. Потім Боб вибирає число e таке, що $1 < e < \phi$ та $\text{НСД}(e, \phi) = 1$ та обчислює за допомогою розширеного алгоритму Евкліда $d \in (1, \phi)$ таке, що $(de) \equiv 1 \pmod{\phi}$. Відкритим ключем Боба, який він передає Алісі є пара (n, e) , секретним ключем Боба є d . Аліса передає Бобу зашифроване повідомлення $c = m^e \pmod{n}$. Для його дешифрування Боб використовує свій секретний ключ d і обчислює $m = c^d \pmod{n}$.

Діффі-Гелмана

Приклад 232. Нехай Аліса і Боб домовились використовувати $p = 23$ та генератор $g = 5$ (ці дані можуть бути відкритими). Аліса обирає секретне число $a = 4$, та надсилає Бобу число $A = g^a \pmod{p} = 5^4 \pmod{23} = 4$. Боб обирає секретне число $b = 3$, та надсилає Алісі число $B = g^b \pmod{p} = 5^3 \pmod{23} = 10$. Аліса обчислює $a_{BA} = B^a \pmod{p} = 10^4 \pmod{23} = 18$, а Боб обчислює $a_{AB} = A^b \pmod{p} = 4^3 \pmod{23} = 18$. Спільне значення $K = a_{BA} = a_{AB} = 18$ є спільним таємним ключем.