I Практика

Чи буде групою?:

① а) Мн-на дійсних симетр. матриць порядку n відносно множення

— у усіх нулів

— Ні бо не вказано, що вироджн. матр. порушує існування оберненого елемента

б) Мн-на ___ невироджених — лише 1 дійсн. ненульових ел-ів

— Ні Минула проблема відсутності оберн. ел. зникає

по суті це ③.

Згідно з критерієм підгрупи ⇒

⇒ Тепер треба довести замкненість операції мн-ни відн. симетр. матриць

Щось ми в інеті назнали, що є 2 симетр. матр. добуток яких дає несиметр. матрицю. Наприклад

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

порушн. симетр. $a_{ij} \neq a_{ji}$

Отже, операція незамкнута ⇒ виводить за межі групи ⇒ це не підгрупа

② Мн-на всіх дійсних кососиметр. матриць відн. додавання

Так

кососиметрична матриця: матриця це $a_{ij} = -a_{ji}$

1) нейтральний елемент: нульова матриця
2) Сума кососиметричних матриць є кососиметр. матр.
3) Обернений ел.: кососиметр. транспонована матр.

④ Мн-на всіх дійсн. діагональних матр. порядку n відносно додавання

усі не діагональні елементи = 0

Так

1) Нейтральний елемент: нульова матриця
2) Операція асоціативна
3) Оберн. елемент є: це $(-1) \cdot$ (задана матриця)

Діагональні матриці без нульової матриці будуть групою і по множенню

⑤. Мн-на дійсн. верхніх трикутних матриць щодо множення

матриця вигляду
$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

Так

1) Множення асоціативне
2) Обернений елемент є: $(-1) \cdot (\cdots)$ *за умови що нема нуля на діагоналі, бо тоді то вже не на група*
3) Нейтральний: одинична матр.
4) Добуток двох верхнотрикут. матриць це верхнотрикутна матриця

⑥. Мн-на всіх дійсних матриць порядку n з фіксованим визначником d відносно множення

* усі матриці „групи" мають однаковий визначник

При d=1 Так

1) Якщо $d \neq 0$: обернене є
2) Нейтральний елемент: одинична матриця
3) Множення асоціативне

Група при $d=1$ бо одинична матр. (нейтр. ел.) має визначник $= 1$ ⇒ ⇒ вся група має мати визначник 1

7. Множина ~~нецілих~~ невироджених дійсних матриць вигляду $\begin{pmatrix} x & y \\ ax & x \end{pmatrix}$, a - фікс. відносно множення

Так. Приймаємо за a умовне дійсне число, наприклад 17.

Д/з: 8, 9, 10, 11, 12, 13

1) Асоціативна операція множ.
2) Нейтрал. елемент – одинич. матр.

Оберненість – ? Замкненість операції – ?

3) Обернене: $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}^{-1}$ → метод Гауса (довго); → метод мінорів (швидше)

Метод мінорів: $A^{-1} = \frac{1}{d}\begin{pmatrix} A_{11}^T & \dots & A_{1n}^T \\ \vdots & & \vdots \\ A_{n1}^T & \dots & A_{nn}^T \end{pmatrix}$ ← матриця мінорів отрим. шляхом викресл. рядка і стовпчиків

– Знайдемо визначник: $\underbrace{x^2 - ay^2}_{d}$

– Знаходимо транспоновану матр. A^T: $\begin{pmatrix} x & ay \\ y & x \end{pmatrix}$

– Для кожного елемента знаходимо алгебраїчне доповн.: мінор → знак „+" якщо $i+j$ – парне; → знак „–" якщо $i+j$ – непарне

$A^T = \begin{pmatrix} x & ay \\ y & x \end{pmatrix} \Rightarrow A_{11}^T = x$; $A_{12}^T = \begin{pmatrix} x & ay \\ y & x \end{pmatrix} = -y$; $A_{21}^T = \begin{pmatrix} x & ay \\ y & x \end{pmatrix} = -ay$; $A_{22}^T = x$

Тоді обернена матриця: $A^{-1} = \frac{1}{x^2 - ay^2} \cdot \begin{pmatrix} x & -y \\ -ay & x \end{pmatrix}$

$$A^{-1} = \begin{pmatrix} \frac{x}{x^2-ay^2} & \frac{-y}{x^2-ay^2} \\ \frac{-ay}{x^2-ay^2} & \frac{x}{x^2-ay^2} \end{pmatrix} = \begin{pmatrix} x_1 & \frac{-y}{x^2-ay^2} \\ \frac{-ay}{x^2-ay^2} & x_1 \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ ay_1 & x_1 \end{pmatrix}$$ – менше групи

4) Замкненість множення:

$$\begin{pmatrix} x_1 & y_1 \\ ay_1 & x_1 \end{pmatrix} \times \begin{pmatrix} x_2 & y_2 \\ ay_2 & x_2 \end{pmatrix} = \begin{pmatrix} \underbrace{x_1x_2 + ay_1y_2}_{n} & \underbrace{x_1y_2 + y_1x_2}_{m} \\ ay_1x_2 + ay_2x_1 & ay_1y_2 + x_1x_2 \end{pmatrix} = \begin{pmatrix} n & m \\ am & n \end{pmatrix}$$ – входить у групу

14. Множина всіх відображень мн-ни $M = \{1, 2, \dots, n\}$ у себе відносно суперпозиції відображень

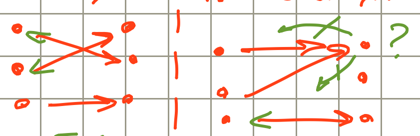
Відображення – функціональне і всюдивизначене відношення

Відношення – відповідність між елементами двох множин

Ні

1) Нейтральний елемент: одиничне відображення (перехід ел. сам у себе)
2) Суперпозиція асоціативна
3) Немає (однозн.) оберненого елемента

Бієкція? | НЕ бієкція



є оберн. елемента | Нема оберн. елемента

15. Мн-на ін'єктивних відобр. мн. $M = \{1, 2, \dots, n\}$ у себе відносно суперпозиції — сюр'єкція

Наприклад тангенс гіперболічний

Якщо є 3 властивості (у нашому випадку всюдивизн., функціон., ін'єкт.)

і скінченна мн-на, то з цього випливає сюр'єктивність

⌈ Від супротивного: припускаємо, що є відображ. і не у всі точки області значень приходить стрілочка, тоді ми можемо викинути ті точки і обл. зн. стає меншою, тоді ел-тів мн-ни визн. більше ніж ел-ів мн. зн. ⇒ за Діріхле існ. з мн. зн. одна стрілочка, яка має кудись прийти обов'язково, і виходить, що прийдуть декілька стрілок в одну точку → порушимо ін'єктивність, протиріччя ⌋

Так

Тоді ця група є бієкцією по суті ⇒ група

16. Мн-на сюр. відобр. . . . скінч., сама в себе, суперп-я

Аналогічно 15. Вийде бієкція

⌈ Зі всіх ел-ів мн. визн. ідуть стрілки, з кожної по одній, усі приходять рівно у всі. Інакше 2 стрілки прийшли б в одну т. мн. зн. і поруш. сюр. ⌋

Так

17. Бієктивні — завжди група

18. Мн-на степенів дійсного фіксованого числа $a \neq 0$ з цілими показниками відносно операції множення

додатні, від'ємні, нуль

Так

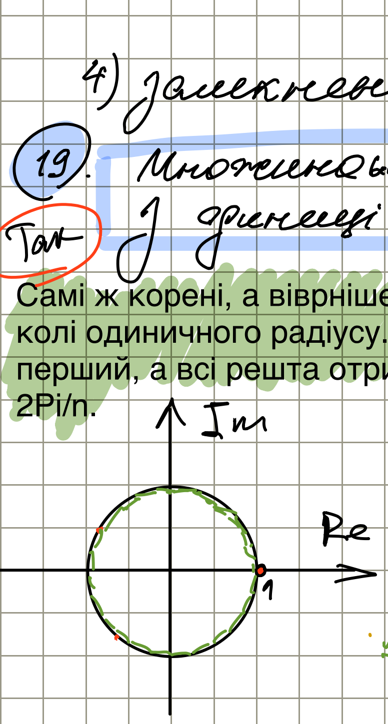
1) Нейтральний ел.: нуль (показник)
2) асоціатив. множ.
3) Оберн. є: у нас стала ненульова основа a ⇒ ⇒ обернене це від'ємний степінь до даного степеня
4) замкненість: степені +/− і мн. в межах групи

19. Множина всіх комплексних коренів фіксованого степеня n з одиниці відносно операції множення

Так

Самі ж корені, а віврніше їх аргументи лежать на колі одиничного радіусу. Достатньо тільки знайти перший, а всі решта отримаємо додаванням кута 2Pi/n.

← геометр. суть кореня комплекс. числа (формула Муавра)



Правило Муавра для 19 - 20

$\sqrt[3]{1}$, n=3 – n-кутник правильний (n=3 ⇒ трикутник)

$\sqrt[n]{1}$, n=n – правильний n-кутник

Комплексні числа задані в полярн. координатах: представл. довжиною і кутом

довжина, кут: $r\cdot(\cos\alpha + i \cdot \sin\alpha)$. Нех. маємо $z_1(\cos\alpha_1 + i\cos\alpha_1)$, $z_2(\cos\alpha_2 + i\cos\alpha_2)$

При множенні двох комплексних чисел: довжини: $r_1 \cdot r_2$; кути: $\alpha_1 + \alpha_2$

* При n множенням буде: r^n і $n\cdot\alpha$

При поділі кола на прав. n-кутник кути поділ на: $0, \frac{2\pi}{n}, \frac{4\pi}{n}, \dots \Rightarrow \cos\left(\frac{2\pi i}{n}\right)+i\sin\left(\frac{2\pi i}{n}\right)$, $i=\{0,1,\dots,n-1\}$ (r пропали бо $r=\sqrt[n]{1}=1$)

* Множина комплексних чисел з виколотим нулем є групою

– обернене для: $a+ib$ – знайти оберн., аби при перемнож. вийшло 1

Спробуємо: $(a+ib)(a-ib)=a^2+b^2 \neq 0$, тоді оберненим для $(a+ib)$ буде $\frac{a-ib}{a^2+b^2}$

Задана нам множина є підмнож. комплексних.

1) Знайдемо обернене: по аналогії з просто множиною комплексних чисел оберн. для $\cos\left(\frac{2\pi i}{n}\right)+i\sin\left(\frac{2\pi i}{n}\right)$ буде:

$$\frac{\cos\left(\frac{2\pi i}{n}\right)-i\sin\left(\frac{2\pi i}{n}\right)}{\underbrace{\cos^2\left(\frac{2\pi i}{n}\right)+\sin^2\left(\frac{2\pi i}{n}\right)}_{=1}}=\underbrace{\cos\left(-\frac{2\pi i}{n}\right)+i\sin\left(-\frac{2\pi i}{n}\right)}_{\text{корінь порядку } -i}=\cos\left(\frac{2\pi(n-i)}{n}\right)+i\sin\left(\frac{2\pi(n-i)}{n}\right)$$

$\cos\left(2\pi-\frac{2\pi i}{n}\right)=\cos\left(\frac{2\pi i}{n}\right)$

2) Замкненість на множені: додаються кути просто $\Rightarrow$ добуток двох коренів є коренем

?

28. Множина всіх комплексних коренів усіх степенів з одиниці відносно множення

1) Множення комутативне 2) Нейтральний елемент: одиниця
3) Обернений елемент аналогічно 19

Так

4) Замкненість: Нехай $t_1=\cos\left(\frac{2\pi k}{n_1}\right)+i\sin\left(\frac{2\pi k}{n_1}\right)$ та $t_2=\cos\left(\frac{2\pi k}{n_2}\right)+i\sin\left(\frac{2\pi k}{n_2}\right)$. Використаємо формулу Ейлера: $\cos\alpha+i\sin\alpha=e^{i\alpha}$, тоді $t_1=e^{i\frac{2\pi k}{n_1}}$ та $t_2=e^{i\frac{2\pi k}{n_2}} \Rightarrow t_1\cdot t_2=e^{i\frac{2\pi k}{n_1}}\cdot e^{i\frac{2\pi k}{n_2}}=e^{i\left(\frac{2\pi k}{n_1}+\frac{2\pi k}{n_2}\right)}=e^{i\left(\frac{2\pi n_2+2\pi n_1}{n_1n_2}\right)}=e^{i\frac{2\pi}{n_1n_2}(n_2+n_1)}$, використаємо знову формулу Ейлера
$e^{i\frac{2\pi k}{n_1n_2}(n_1+n_2)}=\cos\left(\frac{2\pi k}{n_1n_2}(n_1+n_2)\right)+i\sin\left(\frac{2\pi k}{n_1n_2}(n_1+n_2)\right)$ ← дійшли до вигляду мн-ни $\Rightarrow$ замкнена

24. Множина всіх непарних підстановок $M=\{1,2,\dots n\}$ відносно ~~множення~~ композицій

Ні

1) Нейтральний елемент: підстановка, яка переводить елемент сам у себе $=\begin{pmatrix}1&2&\dots&n\\1&2&\dots&n\end{pmatrix}$

Тотожна підстановка є парною → нема нейтрал. ел $\Rightarrow$ не група

А також композиція двох непарних підстановок дає парну підстановку

25. Множина підстановок $\{E, (12)(34), (13)(24), (14)(23)\}$ відн. множ.

$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$; Оберн. підстановка: $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\xrightarrow{1}\begin{pmatrix}2&1&4&3\\1&2&3&4\end{pmatrix}\xrightarrow{2}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

Замкн. ①·②: $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$ → циклічн. форма: $(14)(23)$ = ③

$1\to2$ $2\to4$
$2\to1$ $1\to3$
$3\to4$ $4\to2$
$4\to3$ $3\to1$

І ще перевіряти всі інші обернені: $(A\cdot C=B\ ;\ B\cdot C=A)$

$① \cdot ② = ③ \Rightarrow ①\cdot② = ①^{-1}\cdot②^{-1} = (①\cdot②)^{-1} = ③^{-1} = ③$

Домашня практика

8. Чи є групою множина дійсних матриць вигляду $\begin{pmatrix}x&y\\-y&x\end{pmatrix}$ відносно множення

1) Множ. асоціативне

2) нейтральний елемент – одинична матриця $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ Так

3) Обернений елемент: Обернена матриця методом мінорів

$d=x^2+y^2$; $A^T=\begin{pmatrix}x&-y\\y&x\end{pmatrix}$; $A^T_{11}=x$; $A^T_{12}=-y$; $A^T_{21}=+y$; $A^T_{22}=x$; $A^{-1}=\frac{1}{x^2+y^2}\cdot\begin{pmatrix}x&-y\\y&x\end{pmatrix}=\begin{pmatrix}n&-m\\m&n\end{pmatrix}$

4) Замкненість операції

$$\begin{pmatrix}x_1&-y_1\\y_1&x_1\end{pmatrix}\cdot\begin{pmatrix}x_2&-y_2\\y_2&x_2\end{pmatrix}=\begin{pmatrix}x_1x_2-y_1y_2&-x_1y_2-y_1x_2\\x_2y_1+x_1y_2&-y_1y_2+x_1x_2\end{pmatrix}=\begin{pmatrix}n&-m\\m&n\end{pmatrix}$$

9. Чи є групою множина дійсних матриць вигляду $\begin{pmatrix}x&y\\-y&x\end{pmatrix}$ відносно додавання

1) Додавання асоціативне Так

2) нейтральний елемент: нульова матриця

3) $\begin{pmatrix}x_1&y_1\\-y_1&x_1\end{pmatrix}+\begin{pmatrix}x_2&y_2\\-y_2&x_2\end{pmatrix}=\begin{pmatrix}x_1+x_2&y_1+y_2\\-y_1-y_2&x_1+x_2\end{pmatrix}$: $x_2=-x_1$, є

4) Операція замкнена

10. Мн-на матриць виду $\begin{pmatrix}1&x\\0&1\end{pmatrix}$, $x\in R$ відносно множення

0) Мн. - асоц. Так

1) Нейтрал. ел. – од. матр. $\begin{pmatrix}1&0\\0&1\end{pmatrix}$

2) Оберн. ел. $d=1$; $A^T=\begin{pmatrix}1&0\\x&1\end{pmatrix}$; $A^T_{11}=A^T_{22}=1$; $A_{12}=-x$; $A_{21}=0 \Rightarrow A^{-1}=\begin{pmatrix}1&-x\\0&1\end{pmatrix}$

Перевірка: $\begin{pmatrix}1&x\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&-x\\0&1\end{pmatrix}=\begin{pmatrix}1&-x+x\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$

3) Замкнутість множ.: $\begin{pmatrix}1&x_1\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&x_2\\0&1\end{pmatrix}=\begin{pmatrix}1&x_2+x_1\\0&1\end{pmatrix}=\begin{pmatrix}1&m\\0&1\end{pmatrix}$

11. Мн-на матриць виду $\begin{pmatrix}1&x\\0&1\end{pmatrix}$, $x\in R$ відносно множення а) додавання асоціативне

1) Нейтрал. ел. – нульова матриця

~~Кі~~ Буде

2) Оберн. ел.: немає такого, аби входив у групу $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$

(12). Мн-на матриць виду $\begin{pmatrix}m & m-1\\ 1 & 1\end{pmatrix}$, де $m\in\mathbb{Z}$, відн. множення

12 - 13 – не буде

Практика 2.

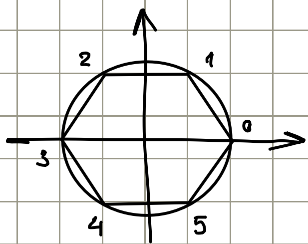
(6). $\mathbb{Z}_6$

mod 6	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Підгрупи (0,3), (0,2,4)

Генератори: 1, 5

(2). C_6



Формула муавра; піднесення в степень комплекс. числа

$R=1$ кут: $2\pi k$

Ця група ізоморфна попередній треба лише перейменувати і змінити дію

(3). D_3 – симетрія трикутника (лекція)

(4). $T_2(\mathbb{Z}_3)$

група по додаванню (mod)

група за множ. усіх не-вироджених верхніх матриць

Визначник ≠ 0

Чи буде

Побудувати фактор групу ?

(1). $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ (3). $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ (5). $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$

(2). $\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$ (4). $\begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix}$ (6). $\begin{pmatrix}2 & 2\\ 0 & 2\end{pmatrix}$

$\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$ $\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}$ $\begin{pmatrix}1 & 2\\ 0 & 2\end{pmatrix}$

$\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}$ $\begin{pmatrix}2 & 1\\ 0 & 1\end{pmatrix}$ $\begin{pmatrix}2 & 2\\ 0 & 1\end{pmatrix}$

$\begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix}$. З чимось помножити, x3

Таблиця Келі:

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	6	5	2	1	4
4	4	5	2	3	6	1
5	5	4	1	6	3	2
6	6	3	4	1	2	5

Як заповнюється таблиця

$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ ← (5).

Чи циклічна: Розгл. 4 і 6 матрицю

Розгл. матр 4 : $4, \underset{4\cdot 3}{3}, \overset{4\cdot 4}{2}, \overset{4\cdot 2}{5}, \underset{4\cdot 5}{6}, \overset{4\cdot 6}{1}$ — група ізоморфна $\mathbb{Z}_6$

Згідно з табл. Келлі

Яка структура? :

Д/з: 10, 12, 30, 24

Практика 3

	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	a^4
a^2	a^2	a^3	a^4	a^5
a^3	a^3	a^4	a^5	a^6

$e = (1)(2)(3)(4)(5)$

$a = (1352)(46)$

$b = a^2 = (15)(32)(4)(6)$

$c = a^3 = (1253)(46)$

* далі воно буде повтор. з попередніми

тому $max = 3$

10. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \right\rangle$

1 2 3 4 5 6
2 3 4 5 6 1
3 4 5 6 1 2
4 5 6 1 2 3
5 6 1 2 3 4

12. $\mathbb{Z}_9^*$ мультиплікативна (множ.) група оборотних класів

формує групу, генератор усередині

30. $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix} \right\rangle$

підстановка

$(156), (243)$

	e	a	a^2
e	e	a	a^2
a	a	e	e
a^2	a^2	e	a

$e = (1),(2),(3),(4),(5),(6)$

$a = (156),(243)$

$a^2 = (165),(234)$

$a^3 = (1)(6)\ldots = e$

Завдання теми 3

3 — я відповідала

а) $\left\langle \begin{pmatrix} 12345678 \\ 17462583 \end{pmatrix} \right\rangle$ $\quad (1)\ (2783465)$ $\quad$ 1 $\quad$ 7

б) $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} i$ $\quad \cos\left(\frac{\pi}{4}\right) + \sin\left(\frac{\pi}{4}\right)\cdot i$

$n - ?$ $\quad n = 8$

(*) б) за ф-лою Муавра:

$(\cos\alpha + i\sin\alpha)^n =$

$= a^n \cdot (\cos(n\cdot\alpha) + i\sin(n\cdot\alpha))$

дійсна частина

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

$g: \overset{1}{(1)}\ \overset{7}{(278465)}$ $\quad$ Порядок: 7

$g^2: (1)(2745386)$

$g^3: (1)(2857634)$

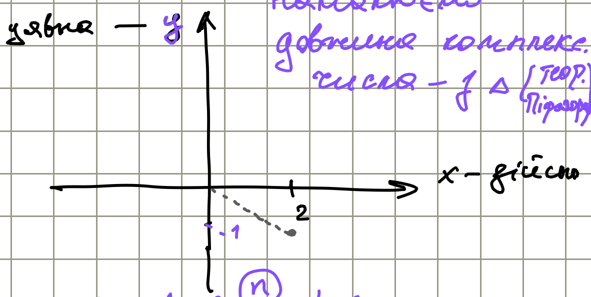
в) $g = 2 - i \in \mathbb{C}^*$

Треба знайти довжину комплекс. числа

||

Треба знайти довжину пунктир. лінії:

$c^2 = a^2 + b^2 \Rightarrow c = \sqrt{1+4} = \sqrt{5}$



Намалюємо довжину комплекс. числа – з △ (теор. Піфагора)

$2 - (\sqrt{5})^{n} \neq 1$

Отже у будь-якій степені $\sqrt{5}$ не дасть 1 $\Rightarrow$ нема порядку

10. а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ $\quad \underset{2}{(8\,1)}\underset{5}{(2\,7\,3\,6\,5)}\underset{1}{(4)}$

Порядок: НСК $(2, 5, 1) = 10$

б) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ К-сть матриць $= n!$ (кількості перестановок)

$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}^2 \underset{\text{в 2 степ.}}{=} \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}^2}_{} \underset{\text{в 4 степінь}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Або можна розглянути матрицю як перестановку (рядки)

$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} I \\ II \\ III \\ IV \end{matrix}$ $\quad \underbrace{(I\ II\ III\ IV)}_{4}$ Порядок 4

$g = \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$ дивимся на визначник

$|g| = 0 - i = -i$ – Тре щоб був 1

$\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$; $|g^2| = i^2 = -1 \neq 1$

$\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad |g^4| = 1 = 1$ Але матриця не одинична

Попробуєм її в квадрат, тобто 8 степінь

$g^8 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, Степ. 8 — кінець

$\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

15. $g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$, $\quad |g| = 0 + 0 + 0 - 0 - 1 - 0 = -1$

$g^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ $\quad |g^2| = 1$

Але не одинична,
но суті нам тре просто щоб вона така
лишилась, але при перемноженні сталось $(-1)\cdot(-1) = 1$
Тому можна припустити, що порядок 4

, Порядок 4.

Домашня робота

Приклад: $g=\cos\frac{5\pi}{8}+i\sin\frac{5\pi}{8}$ => За Муавра: $1^n\left(\cos\left(n\cdot\frac{5\pi}{8}\right)+i\sin\left(n\cdot\frac{5\pi}{8}\right)\right)$

Підберемо таке n, аби кут cos $=2\pi k$, $k=\overline{1,n}$, $\in N$

$\frac{5\pi}{8}\cdot n = 2\pi k$: при $n=8$: $\frac{5\pi}{8}\cdot 8 = 5\pi$: $-1+0\neq 1$

Нам потрібно таке n аби за муавра зводилось у 1 $\quad n=16$: $\frac{5\pi}{8}\cdot 16 = 10\pi$: $1+0=1$

Адже 1 - це нейтральний елемент C^*

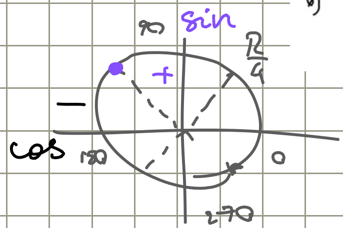
Отже таке $n=8$ ← порядок

а) $\left\langle\begin{pmatrix}1&2&3&4&5&6&7&8\\1&7&4&6&2&5&8&3\end{pmatrix}\right\rangle$ $\quad$ (1) (2 7 8 3 4 6 5) $\quad$ 1 $\quad$ 4

в) $\frac{1}{\sqrt2}-\frac{1}{\sqrt2}i$ $\quad \cos\left(-\frac{\pi}{4}\right)+\sin\left(-\frac{\pi}{4}\right)\cdot i$

$n-?$ $\quad n=8$

5. 8) $g=-\frac{\sqrt2}{2}+\frac{\sqrt2}{2}i\in C^*$



$\Rightarrow \cos\left(\frac{\pi}{2}+\frac{\pi}{4}\right)+i\sin\left(\frac{\pi}{2}+\frac{\pi}{4}\right)=$

$=\cos\left(\frac{3\pi}{4}\right)+i\sin\left(\frac{3\pi}{4}\right) \Rightarrow \frac{3\pi}{4}\cdot n = 2\pi k$

$n=8 \Rightarrow$

За Муавра: $1^n\left(\cos\left(\frac{3\pi}{4}\cdot n\right)+i\sin\left(\frac{3\pi}{4}\cdot n\right)\right) \Rightarrow \frac{3\pi}{4}\cdot 8 = 6\pi$: $1+0$

Геометричне зображення комплексного числа

Комплексне число $z=a+bi$ геометрично зображують точкою $M(a;b)$ координатної площини.

Геометричне зображення комплексного числа.

Комплексне число зручно зобразити у вигляді вектора

$$\overrightarrow{OM}(a;b).$$

Довжина вектора, який зображає комплексне число, називається **модулем цього комплексного числа**. Модуль комплексного числа позначається r. Тобто

$$r=|z|=|a+bi|=\sqrt{a^2+b^2}.$$

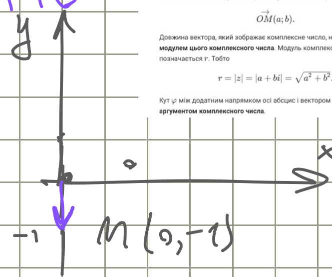
Кут φ між додатним напрямком осі абсцис і вектором $\overrightarrow{OM}$ називається **аргументом комплексного числа**.

7. $g=-i\in C^* = 0-i$: $a=0$ $b=-1$

Довжина комплекс. числа, зображ. геом.

Вектор довжини: 1

Порядок: 2 (∀ парне число)



12. в) $\begin{pmatrix}-1&a\\0&1\end{pmatrix}$: $|g| = -1-0=-1$

$\begin{pmatrix}-1&a\\0&1\end{pmatrix}^2=\begin{pmatrix}1&-a+a\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ - одинична матр. => Порядок 2

14. $g=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$; $|g| = 0+1=1$

$g^2=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}$; $g^4=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$; $g^8=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}$ - прийшли в початкову

$g^6=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}\begin{pmatrix}-1&-1\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ Порядок 6

23. $g=\underset{a+bi=0+1\cdot i}{i}\in C^*$; Довжина (модуль) комплекс. числа = 1

Порядок: 1 (найменше натуральне) — Уточнити

22. $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ I II III Розглянемо як перестановку $\Rightarrow$ за 3 кроки прийдемо в початкове положення $\Rightarrow$ Порядок 3

21. $g = \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix}$; $|g| = 0 + 1 = 1$

$g^2 = \begin{pmatrix} a^2-1 & a \\ -a & -1 \end{pmatrix}$ $|g^2| = 1 - \cancel{a^2} + \cancel{a^2} = 1$; $g^4 = \begin{pmatrix} -2a+1 & a^3-2a \\ -a^3 & -a^2+1 \end{pmatrix}$; $g^8 = ($

$|g^4| = 2a^3 - a^2 - 2a + 1 + a^6 + 2a^4 \neq 1$

$g^3 = \begin{pmatrix} a^3-2a & a^2-1 \\ -a^2+1 & -a \end{pmatrix}$

$\cancel{-a^4} + \cancel{2a^2} + \cancel{a^4} - \cancel{a^2} - \cancel{a^2} + 1 = 1$

визначник 1, але матр. не одинична

$g^4 \cdot g^2 = \begin{pmatrix} -2a+1 & a^3-2a \\ -a^3 & -a^2+1 \end{pmatrix} \begin{pmatrix} a^2-1 & a \\ -a & -1 \end{pmatrix} = ($

$\begin{pmatrix} a^2-1 & a \\ -a & -1 \end{pmatrix} \begin{pmatrix} a^3-2a & a^2-1 \\ -a^2+1 & -a \end{pmatrix} =$

$= (a^5 - 2a^3 - a^3 + 2a - a^3 + a$ $\varnothing$

Тут схоже немає порядку через те, що на позиції 1,1 стоїть і при перемноженні добуває найб. степінь

24. $g = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix}$; $|g| = -1$

$g^2 = \begin{pmatrix} 1 & 0 \\ a-a & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Порядок 2

30

27. $\cos \frac{7\pi}{15} + i \sin \frac{7\pi}{15}$; ~~$n = \frac{30}{7} \notin N$~~ 70 $\Rightarrow$ нема порядку

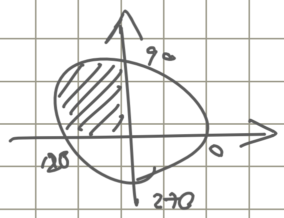
26. $\cos \frac{3\pi}{5} + i \sin \frac{3\pi}{5}$; ~~$n = \frac{10}{3} \notin N$~~ $\Rightarrow$ нема порядку

28. $\cos \frac{6\pi}{15} + i \sin \frac{6\pi}{15}$; $n = \frac{30}{6} = 5$ порядок

20. $g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ $|g| = 1$

$g^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ Порядок 2

$\frac{\pi}{2} + \frac{\pi}{6} = \frac{2\pi}{3}$



19. б) $g = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ $\Rightarrow$ Запишемо у тригоном. вигляді

$g = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$ $\Rightarrow$ $\frac{2\pi}{3} \cdot n = 2\pi k$

$n = 3$ – Порядок

25. б) $g = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$ $\Rightarrow$ $\cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right)$ $\Rightarrow$ $n = 3$ – Порядок

Практика 3

1. 6 – віддзеркал. (3) і повороти (3)

Аналогічно для інших двовимір. фігур (сума поворотів і віддзеркал.)

$\boxed{00}$ = прямокутник

12. Всі вершини однакові (відрізняє від пірамід з іншими основами)

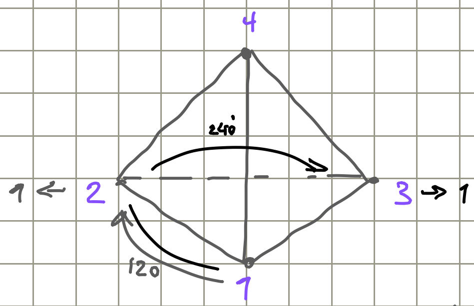
→ виникають інші повороти, нестандартні для пірамід

Д/з: розглянути куб (почитати)

1) Повороти: $0°$, $120°$, $240°$ →

а) 4 граней

→ $1 + 4 \cdot 2 = 9$
(0°)



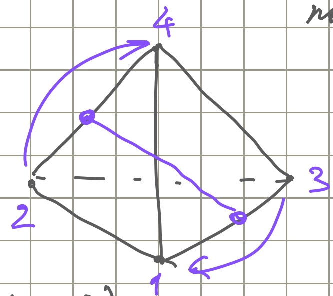
Можна задати повороти перестановками:

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

К-сть усіх перестановок: 24

(Але відкидаємо одну.)

б) Відрізки, що сполучають середини відрізків: 3



Разом а) + б) = 9 + 3 = 12

1) Віддзеркалення: 12 (міняє парність)

Усі повороти парні перестановки, а віддзеркалення непарні і їх має бути рівна кількість => віддзеркалень теж 12

Тема 4. Сист. твірних

Приклад Z_+^{36}

взаємно прості

1, 5, 7, 11, 13, 17, 19, 23, 29

неправильно: $a = 7$ порядок: 36 (бо генератор групи)

для a^2 порядок 18

для a^{18} порядок 2

Приклад 2: a^{24} не має порядок 30 → не є генератором

1. $n = 24$, $k = 6$

1) Знайти всі g –? задовільняють $g^k = e$

a^0, a^4, a^8, a^{12}, a^{16}, a^{20}

2) Знайти всі елементи порядку k, якщо $k = 6$:

Шук. взаємнопрості з 6: 1, 5

Який порядок a^8 : 3 шукаємо НСД (степінь і 24) група

a^{18} : 4

→ НСД(18; 24) = 6 ⟹ 24 : 6 = 4

2. $n = 72$, $k = 8$

$72 : 8 = 9$

1) $a^9, a^9, a^{18}, a^{27}, \dots, a^{63}$

2) Шук взаємнопрості з 8 : $a^9, a^{27}, a^{45}, a^{63}$

Тема 6

Ізоморфізм - бієкція і зберіг. операцію

Мономорфізм - операція — " —

У перестановок групова операція : композиція

У групи симетрій — " — : композиція перетворень

1. $f : C^* \to R^*$, $f(z) = |z|$ Д/з : проглянути номера

$f(a \cdot b) = f(a) \cdot f(b)$

$f(a + ib) = \sqrt{a^2 + b^2}$

$f((a_1 + ib_1) \cdot (a_2 + ib_2)) = f(a_1 + ib_1) \cdot f(a_2 + ib_2)$ - за формула муавра → гомоморфізм

Треба щоб відображення було бієкцією

Ми можемо знайти 2 комплексних числа

$[2.3] + [3,7] = 2 + 3 = 5$

$[2.3 + 3.7] = [6] = 6$

9. $f : R^+ \to R$, $f(x) = \log_2 x$

$f(a \cdot b) = f(a) + f(b)$

$\log_2 (a \cdot b) = \log_2 a + \log_2 b$ ⟹ гомоморфізм

Буде ізоморфізмом

Д/З

6. $f: \mathbb{C}^* \to \mathbb{C}^*$

$f(z) = \frac{z}{|z|}$

Ізоморфізм ⇓ f гомоморфізм

1. за нейтрал. – підходить

2. оберн.: $f(g^{-1}) = (f(g))^{-1}$ $f(g^{-1}) = \frac{|a+ib|}{a+ib}$

$f(g)^{-1} = \frac{|z|}{z} = \frac{|a+ib|}{a+ib}$

3. порядок одиниці

11. – схоже на 6, але не ізоморфізм (квадрат суперечить співвідношенням)

$f(a \cdot b) = f(a) \cdot f(b)$

$f\left(\frac{b^2}{|b^2|} \cdot \frac{a^2}{|a^2|}\right) = f\left(\frac{b^2}{|b^2|}\right) \cdot f\left(\frac{a^2}{|a^2|}\right)$ – гомоморфізм

7. $f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ $f(n) = 3n$

1. за нейтр. – підходить

2. $\varphi(g^{-1}) = (\varphi(g))^{-1}$; $f(g^{-1}) = 3 \cdot \frac{1}{a} = \frac{3}{a}$

не ізоморфізм $(f(g))^{-1} = (3a)^{-1} = \frac{1}{3a}$

$f(a+b) = f(a) + f(b)$

$3(a+b) = 3a + 3b = f(a) + f(b)$ – гомоморфізм

10. $f: \mathbb{R}^+ \to \mathbb{R}^{+*}$, $f(2^x)$

$f(a+b) = f(a) \cdot f(b)$

$2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$ – гомоморфізм

1. $2^0 = 1$ – по нейтральному підходить

2. $f(g^{-1}) = (f(g))^{-1}$: $f(g^{-1}) = 2^{\frac{1}{a}} = \sqrt[a]{2}$

не ізоморфізм $(f(g))^{-1} = \frac{1}{2^a} = 2^{-a}$

15. Гомоморф: $f(a+b) = (\sin x_1 + \cos 2x_1 + \sin x_2 + \cos 2x_2) = \underbrace{\sin x_1 + \cos 2x_1}_{f(a)} + \underbrace{\sin x_2 + \cos 2x_2}_{f(b)}$

2. вл-сть ізоморф не викон. ⇒ не ізоморфізм.

29. $\mathbb{R}^+ \to \mathbb{R}^{+*}$ $f(x) = e^x$

$f(a+b) = f(a)\cdot f(b)$ $\boxed{e: R = 0, \; e: R^+ = 1}$ нейтр. ел.

$f(a+b) = e^{a+b} = e^a \cdot e^b = f(a)\cdot f(b)$

гомоморф. викон.

(1). $e^{a+a} = e^a = 1$ (викон)

(2). $f(g^{-1}) = e^{\frac{1}{a}} = \sqrt[a]{e}$

$(f(g))^{-1} = \frac{1}{e^a} = e^{-a}$ не ізоморф.

(3). не R^+ – тільки додат.

R – усі

(4). (2) $f(g^{-1}) = (f(g))^{-1}$: $f(g^{-1}) = f\left(\frac{1}{a+ib}\right) = \frac{1}{\left|\frac{1}{a+ib}\right|} = |a+ib|$

$(f(g))^{-1} = f(a+ib)^{-1} = \left(\frac{1}{|a+ib|}\right)^{-1} = |a+ib|$

(1). За нейтр. ел. підходить

Отже ізоморфізм

(19). 1) нейтр. ел. сходиться (1)

2) $f(g^{-1}) = f\left(\frac{1}{z}\cdot\frac{1}{\bar z}\right) = \frac{1}{z\cdot\bar z}$

$(f(g))^{-1} = (z\cdot\bar z)^{-1} = \frac{1}{z\cdot\bar z}$

3). $C = C \Rightarrow$ порядок однак.

Ізоморфізм

Практика 4

1. $M = \mathbb{Z}_{179}$ $a = 96$

$179 \to m$, $96 \to n$

НСД $(179, 96) = 1$

179 mod 96 = 83
96 mod 83 = 13
83 mod 13 = 5
13 mod 5 = 3
5 mod 3 = 2
3 mod 2 = 1

$83 = m - n$

$13 = 2n - m$

$5 = 83 - 13\cdot 6 = m - n + (-2n + m)\cdot 6 = 7m - 13n$

$3 = 13 - 5\cdot 2 = 2n - m + 2(-7m + 13n) = -15m + 28n$

$2 = 5 - 3 = 7m - 13n + 15m - 28n = 22m - 41n$

$1 = 3 - 2 = -15m + 23n - 28n - 22m + 41n = -37m + 69n$

(20). $\mathcal{N} = 191 \quad a = 187$

1) $191 \bmod 187 = 4$
2) $187 \bmod 4 = 3$
3) $4 \bmod 3 = 1$

$n = 191$
$m = 187$

1) $4 = n - m$
2) $3 = m - (n-m)\cdot 46$
$= 47m - 46n$
3) $1 = n - m - (47m - 46n) = 47n - 48m$

Обернене: $-48 \Rightarrow 187 - 48 = 143$

Лекція-практика 2

$\left(\frac{205}{197}\right)$ Чи є числом Лежандра чи Якобі

– Якщо Лежандра, то нижнє число просте

$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо } a \text{ є квадрат. лишком} \\ -1, & \text{якщо } a \text{ є квадрат. нелишком} \end{cases}$

Вик. вл-сті з твердження 211: (нам треба зменшити число)

Вик. I вл-сть: $a \equiv a_1 \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$

Замін. $a_1 = 8$ (та сама остача по модулю 197, що і 205)

Вик. IV вл-сть: $\left(\frac{a_1 \cdot a_2 \cdot \ldots \cdot a_m}{p}\right) = \left(\frac{a_1}{p}\right)\cdot\left(\frac{a_2}{p}\right)\cdot\ldots\cdot\left(\frac{a_n}{p}\right)$

$8 = \underset{a_1}{2}\cdot\underset{a_2}{2}\cdot\underset{a_3}{2} \Rightarrow \left(\frac{2}{197}\right)\cdot\left(\frac{2}{197}\right)\cdot\left(\frac{2}{197}\right) = \left(\frac{2}{197}\right)^3$

Нам потрібне просте непарне число, вик. твердження 217 непарне

$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \Rightarrow \left(\frac{2}{197}\right) = (-1)^{\frac{197^2-1}{8}} = (-1)^{\frac{196\cdot 198}{8}} = -1$

$\left(\frac{86}{173}\right) \Rightarrow$ Вик. IV вл-сть: $\left(\frac{86}{173}\right) = \frac{43}{173}\cdot\frac{2}{173} \overset{(1)}{=} \frac{43}{173}\cdot(-1) \overset{(2)}{=} 1\cdot(-1) = -1$

вик. квадрат. закон взаємності тв. 215

(1) $\frac{2}{173} = (-1)^{\frac{173^2-1}{8}} = (-1)^{\frac{172\cdot 174}{8}} = -1$ (непар.)

(2) $\frac{43}{173} = \frac{p}{q} \Rightarrow$ за тв. 215 $\frac{p}{q}\cdot\frac{q}{p} = (-1)^{\frac{(p-1)(q-1)}{4}} \Rightarrow -1^{\frac{(43-1)(173-1)}{4}}\cdot\left(\frac{173}{43}\right) = \frac{173}{43}$, ок.

$173 \bmod 43 = 1 \Rightarrow \left(\frac{1}{43}\right) = 1$ (Вл. II)

$\left(\frac{73}{175}\right) \Rightarrow$ Розбиваємо на символ Лежандра, за означенням 212: $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_r}\right)$, $m = p_1 p_2 \ldots p_r$

$175 = 5 \cdot 5 \cdot 7 \Rightarrow \left(\frac{73}{175}\right) = \left(\frac{73}{5}\right)^2 \cdot \left(\frac{73}{7}\right) = -1$

Використ. вл-сть I $\overset{\text{озн.}}{\underset{210}{\Rightarrow}} \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = 3^{\frac{5-1}{2}} \bmod 3$ // можна було не рахувати бо у квадраті $\left(\frac{73}{5}\right)^2 = \left(\frac{3}{5}\right)^2$ і буде завжди 1

$\left(\frac{73}{7}\right) = \left(\frac{3}{7}\right) = 3^{\frac{7-1}{2}} \bmod 7 = -1$

Многочлени (неєвідні, кругі і т.д.)

для 1 кореня 4 степеня є $\pm 1, \pm i$

Книжка Ніда, Ніедеррайтер:

$$Q_{14}(x) = \frac{(x^{14}-1)^{\frac{\mu = 14}{14} = 1}(x-1)}{(x^7-1)(x^2-1)} = \frac{(x^7+1)}{x+1} = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

1) знах. усі дільники 14: 1, 2, 7, 14

Найти Q_{11}, Q_{12} і Q_n

Практика 14.05

Ліндер

Задач на модулі 8 (або 5)

А типів задач 9

$y^2 = x^3 + x + 2$ $\quad x, y \in \mathbb{Z}_{13}$

$y^2 = x^3 + ax + b$

Тут дивитись або лекц. мат. або англ. Вікіпедія (Elipti curves)

$\Delta = 4 \cdot 1 + 27 \cdot 4 \cdot 1 = 8 \neq 0 \Rightarrow$ не вироджена

$\Delta = -16(4a^3 + 27 \cdot 6^2) \neq 0$

не плутати

$x = 2, y = 5$

$x = 2, y = 8$

$x = 1, y = 2$ ще $y = -2$ підходить, але $\mathbb{Z}_{13} \Rightarrow x = 1, y = 11$

При пошуку кореня треба переглянути всі коф. до $13 \div 2 = 6$ перебором

Додамо перші 2 точки

Перша точка $\quad P: x = 1, y = 2 \qquad x = 1, y = 11$

$\quad Q: x = 2, y = 5 \qquad x = 2, y = 8$

$S = \frac{3x_P^2 + a}{2y_P} = \frac{3 \cdot 1 + 1}{2 \cdot 5} = \frac{4}{10} = \frac{2}{5} =$, тепер треба знайти обернене число що дасть $1/5$

$13 \div 5 =$ ост., $5 \div$ ост., ...

Далі знаходимо через доверш. алгоритм Евкліда

$13 = a$

$5 = b$

$3 = a - 2b$

$2 = b - 1(a - 2b) = 3b - a$

$1 = (a - 2b) - (3b - a) = 2a - 5b$

$= 2 \cdot 8 = 16 \Rightarrow 3$

Оберн. до 5 по модулю 13 це $-5 \Rightarrow (13 - 5) \Rightarrow 8$

Тоді $x_R = 9 - 2 \cdot 1 = 7 \qquad y_R = 2 - 3(1 - 7) = 20 \Rightarrow 7$

$x_R = 1 - 2 \cdot 1 = -1 = 12$
$y_R = 2 - (\underbrace{1-12}_{-11}) = 13 = 0$

P Q
$x_1 = 1 \quad y = 2 \quad x = 2 \quad y = 5$
$S = \frac{-3}{-1} = 3$
$x_R = 9 - 1 - 2 = 6$
$y_R = 2 - 3\underbrace{(1-6)}_{15} = 17 = 4$ оберн. $\Rightarrow 13 - 4 = 9$

$(6, 9)$

2. $y^2 = x^3 + 2x + 3 \quad Z_{11}$

1) Перевіряємо на невиродженість через determinant

$\Delta = \underset{32}{4 \cdot 2^3} + \underset{45}{5 \cdot 9} = 77 = 0$

Вироджене. Змінимо на Z_{13}, щоб розв'язати

$y^2 = x^3 + 2x + 3 \quad Z_{13}$ (невироджена)
$\Delta = 4 \cdot 8 + 1 \cdot 9 = 2 \neq 0$

$1 \cdot 1 = 1 \quad 2 \cdot 2 = 4 \quad 3 \cdot 3 = 9 \quad 4 \cdot 4 = 3 \quad 5 \cdot 5 = 12$
$6 \cdot 6 = 10$

Знах. точку: підставимо 1: $x = 1 \quad y^2 = 6 \Rightarrow y = \ldots$

Жоден корінь у кв. не дає 6 по модулю 13, перевірили корені 1, 2, ... 6

$x = 3 \quad y^2 = 10 \Rightarrow y = 6$
$27 + 6 + 3 = 36 = 6 \cdot 6$

Додамо точку саму до себе $P + P$

$S = \frac{y_P - y_Q}{x_P - x_Q}$ дає 0 у знаменнику $\Rightarrow$ не підходить

$S = \frac{3x_P^2 + a}{2y_P} = \frac{3 \cdot 3^2 + 2}{2 \cdot 6} = \frac{3}{12} = \frac{1}{4} = -3 = 10$

$27 + 2 = 1$

$S^2 - 2x_P$

$x_R = 10^2 - 2 \cdot 3 = 3$

$y_P - S(x_P - x_R)$

$(3, 6)$

$y_R = 6 - 5(3 - 3) = 6$

Евклід: $\alpha = 1 \Rightarrow \alpha = 13$
$\beta = 4$
$1 = \alpha - 3\beta \Rightarrow -3$ оберн. до $13 \Rightarrow 10$ оберн. до 13

Треба ще обернути точку