

५१

$$G = \langle a \rangle \quad \text{ord}(G) = 510$$

$$a). \quad g \in G \quad g^{102} = 1$$

T.k. $G = \langle a \rangle \Rightarrow \forall g \in G : g = a^i, i \in \mathbb{Z} \Rightarrow$

$$\text{ord}(G) = 510 \Rightarrow a^{510} = e, 510 - \min \deg,$$

takes up to $i = 510$, $a^i = \rho$,

$$e = a^{102i} \Rightarrow 102i : 510$$

$$i : 5 \Rightarrow$$

$$\Rightarrow g : \{ a^{5i} \mid 0 < i \leq 102 \}$$

5) Уильям Стендерн а Взаимно простира

~~102 \Rightarrow gittergestrichenes Dreieck mit 102~~

$$\Rightarrow g: \{a^i; i \in \mathbb{Z}, 0 \leq i < 102, \text{HOD}(i, 102) = 1\}$$

Übung: a). $\{a^5 : |0 \leq i \leq 102\}$

8). g: $\{a_i^i; i \in \mathbb{Z}, 0 < i < 102, \text{HOD}(i, 102) = 1\}$

[W2] Наимн. коннектбо элементов
нордике и в группе $D_5 \times S_3 \times \mathbb{Z}_6$

Элементы $D_5 \times S_3 \times \mathbb{Z}_6$ - Тройки

(a, b, c) , $a \in D_5$, $b \in S_3$, $c \in \mathbb{Z}_6$

нордике элемента = $HOK(a', b', c')$, где

$\text{ord}(a) = a'$, $\text{ord}(b) = b'$, $\text{ord}(c) = c' \Rightarrow$

\Rightarrow нордике в группе из 4

~~нордике~~ $a' = 1$ или 2 или 4

$b' = 1$ или 2

$c' = 1$ или 2 или 4

В S_3 нордике 1 и торже из 3

нордике $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, нордике 2 и нордике

$(12), (23), (13)$, а элементов нордике 6

В D_5 и Back ~~нордике~~ из 5

нордике 2 \Rightarrow 5 элементов, а Back

нордике 1, 2, 3, 4, 5 =)

\Rightarrow 5 элементов нордике 1 и 1 элемент

нордике 4

B 26 2020 no 5 elements
nugraha 1, 2, 3, 4, 5, 6 =>

=> 1 element nugraha 1, 2 u "

keeps no change in ~~crooks~~ B zero
lets Fullerton ~~(111111)~~, max
with $HOK(a^i, b^i, c^i) = 4$

$$(1 \cdot 1 \cdot 1) + (1 \cdot 1 \cdot 1) + (6 \cdot 1 \cdot 1) + (1 \cdot 3 \cdot 1) + \\ + (1 \cdot 1 \cdot 1) + (1 \cdot 3 \cdot 1) + (6 \cdot 3 \cdot 1) + (1 \cdot 3 \cdot 1) =$$

$$= 32$$

Crooks: 32

[N3] Penutib $Ax = b$ naq Z₁₇

$$A = \begin{vmatrix} 14 & 8 & 3 & 8 \\ 12 & 12 & 16 & 5 \\ 9 & 3 & 2 & 13 \\ 6 & 11 & 5 & 4 \end{vmatrix} \quad b = \begin{pmatrix} 16 \\ 6 \\ 5 \\ 4 \end{pmatrix}$$

Hängen Rg(A)

$$\begin{pmatrix} 14 & 8 & 3 & 8 \\ 12 & 12 & 16 & 5 \\ 9 & 3 & 2 & 13 \\ 6 & 11 & 5 & 4 \end{pmatrix}$$

$$\begin{array}{l} \textcircled{2} - \textcircled{1} \cdot 13 \\ \textcircled{3} - \textcircled{1} \cdot 14 \\ \textcircled{4} - \textcircled{1} \cdot 15 \end{array}$$

$$\begin{pmatrix} 14 & 8 & 3 & 8 \\ 0 & 10 & 11 & 3 \\ 0 & 10 & 11 & 3 \\ 0 & 10 & 11 & 3 \end{pmatrix}$$

$$\sim \begin{pmatrix} 14 & 8 & 3 & 8 \\ 0 & 10 & 11 & 3 \end{pmatrix}$$

$R_g(A) = 2 \Rightarrow CNA \gamma \text{ Сортировка, Решение}$
 $4 - 2 = 2$, т. Кронекера Кан $R_g(A|b)_{\text{det}}$

$$\Rightarrow R_g(A|b) = 2$$

Нураев $(A|b)$ к канонической
форме

$$\left(\begin{array}{cccc|c} 14 & 8 & 3 & 8 & 16 \\ 12 & 12 & 16 & 5 & 6 \\ 9 & 3 & 2 & 13 & 5 \\ 6 & 11 & 5 & 4 & 4 \end{array} \right)$$

$$\sim \left(\begin{array}{cccc|c} x_1 & x_2 & x_3 & x_4 & \\ 14 & 8 & 3 & 8 & 16 \\ 0 & 10 & 11 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \sim$$

$$\begin{array}{l} \textcircled{1} \cdot 11 \\ \textcircled{2} \cdot 12 \end{array} \sim \left(\begin{array}{cccc|c} 1 & 3 & 16 & 3 & 6 \\ 0 & 1 & 13 & 2 & 7 \end{array} \right) \xrightarrow{\textcircled{1} + \textcircled{2} \cdot 14} \sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 5 & 1 \\ 0 & 1 & 13 & 2 & 7 \end{array} \right)$$

нормалян система γ разрешим

$$\begin{cases} x_1 = -11x_3 - 15x_4 + 1 \\ x_2 = -13x_3 - 2x_4 + 7 \end{cases}$$

$$x_3 = x_3$$

$$x_4 = x_4$$

$$\begin{cases} x_1 = 6x_3 + 2x_4 + 1 \\ x_2 = 4x_3 + 15x_4 + 7 \\ x_3 = x_3 \\ x_4 = x_4 \end{cases}$$

Ortogonal obere Permutation:

$$\bar{x} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 6 \\ 4 \\ 0 \\ -1 \end{pmatrix} x_3 + \begin{pmatrix} 2 \\ 15 \\ -6 \\ 0 \end{pmatrix} x_4$$

PCP: $x_1 = \begin{pmatrix} 6 \\ 4 \\ -1 \\ 0 \end{pmatrix}$

$$x_2 = \begin{pmatrix} 2 \\ 15 \\ -6 \\ 0 \end{pmatrix}$$

[N4] Danno:

$$\begin{cases} p = 103 \\ q = 61 \end{cases}$$

$$K = \{1, p\}$$

$$r = 91$$

$$y = q^x \bmod p = 28$$

$$(p, q, y) = (103, 61, 28)$$

$$(a, b) = (23, 15)$$

Mit 3nachm u10

$$\begin{cases} a = q^k \\ b = q^{k+1} \cdot M \end{cases}$$

при этом ка можно
записать что

$$M = b \cdot a^{P-v-1} \Rightarrow M \stackrel{10^9}{=} 15 \cdot 29^{10^9-91-1}$$

\Rightarrow пользуясь вычислительной машиной
на компьютере можем, что

$$M = 15 \cdot 29^{17} \stackrel{10^9}{=} 12$$

Ответ: 12

№5 Дано: $C = 23263$

Ключ Кортана ($N=25283, d=2597$)

Ключ Амила ($N=17819, e=173$)

U_3 записано на макете

~~Решение~~

$$m = C^d \mod N, \text{ тогда } m = 7942^{2597} \mod$$

$\mod 25283 \Rightarrow$ пользуясь вычислительной
машиной можем вычислить
модулем, что

$$m = 119$$

В ASCII коде номер 119 соответствует

суммой „W“

Задача: Суммой „W“ ког 119

N6

$$f(x) = x^3 + 15x^2 + 13x + 9 \quad | \text{ Mag } \mathbb{Z}_{19}$$
$$g(x) = x^3 + 7x^2 + 12x \quad | \text{ Mag } \mathbb{Z}_{19}$$

Найти $\text{HOD}(f, g)$ и

$u(x)$ и $v(x) \in \mathbb{Z}_{19}[x]$, такие, что

$$u(x) \cdot f(x) + v(x) \cdot g(x) = \text{HOD}(f, g)$$

1

$$\begin{array}{r} x^3 + 7x^2 + 12x \\ - x^3 + 15x^2 + 13x + 9 \\ \hline - 8x^2 - x - 9 = 11x^2 + 18x + 10 \quad (r_1) \end{array}$$

~~занести в таблицу~~

2

$$\begin{array}{r} x^3 + 15x^2 + 13x + 9 \\ - x^3 + 72x^2 + 13x \\ \hline - 3x^2 + 9 \\ - 3x^2 + (7x + 1) \\ \hline 2x + 8 \quad (r_2) \end{array}$$

$$\textcircled{3} \quad \begin{array}{r} -11x^2 + 18x + 10 \\ -11x^2 + 6x \\ \hline -12x + 10 \\ -12x + 0 \\ \hline 0 \end{array} \quad \left| \begin{array}{c} 2x+8 \\ 15x+6 \end{array} \right.$$

$$HOD(f,g) = 2x+8$$

$$v_2 = f(x) \cdot u(x) + g(x) \cdot v(x) \Rightarrow$$

$$\Rightarrow u(x) = 1 + q_1, q_2 = 1 + 7x+2 = 7x+3$$

$$v(x) = 6q_2 = 6 \cancel{(7x+2)} = 42x+12 =$$

$$\text{Check: } HOD(f,g) = 2x+8$$

$$u(x) = 7x+3$$

$$v(x) = 4x+12$$

[Wg] Menge der $\mathbb{Z}_2 \times Q_8$ Elemente: (i,j)

$\mathbb{Z}_2 \times Q_8$ - Menge der \mathbb{Z}_2 Bspw. nap Elementen

\mathbb{Z}_2 $\stackrel{\text{Bspw}}{\sim}$ Bspw. Elemente von Q_8 :

$$\{(0, \pm 1), (0, -1), (0, i), (0, j), (0, k), (0, -k), (1, \pm 1), (1, -1), (1, i), (1, j),$$

$$(j, -j), (1, k), (1, -k) \}$$

№ 7. Кажду в любой конечной группе существует биективное отображение в подгруппу группы перестановок, при этом каждому элементу соответствует некоторый P , такой что

$P = a \cdot g, \forall g$ a - фиксированный элемент группы G , $a \cdot g$ - произвольный элемент группы G . \Rightarrow

\Rightarrow нужно доказать каждому элементу в $\mathbb{Z}_2 \times Q_8$ на $(1, j)$ подходит:

$$\begin{array}{l|l} (0, 1)(1, j) = (0, j) & (1, 1)(1, j) = (1, j) \\ (0, 2)(1, j) = (0, -j) & (1, -1)(1, j) = (1, -j) \\ (0, 3)(1, j) = (0, k) & (1, i)(1, j) = (1, k) \\ (0, 4)(1, j) = (0, -k) & (1, -i)(1, j) = (1, -k) \\ (0, 5)(1, j) = (0, 1) & (1, j)(1, j) = (1, 1) \\ (0, 6)(1, j) = (0, -1) & (1, -j)(1, j) = (1, -1) \\ (0, 7)(1, j) = (0, i) & (1, k)(1, j) = (1, i) \\ (0, 8)(1, j) = (0, -i) & (1, -k)(1, j) = (1, -i) \end{array} \Rightarrow$$

получаетс~~я~~

непустое

(1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16)
(5 6 7 8 1 2 3 4 13 14 15 16 9 10 11 12);

$$= (15)(26)(37)(48)(9\ 13)(10\ 14)(11\ 15)(12\ 16)$$

$$\text{Отвт: } (15)(26)(37)(48)(9\ 13)(10\ 14)(11\ 15)(12\ 16)$$

NIO

P	q	r	s	t	u	v	w	u	v	u	v	w	u	v	w
P	t	u	q	r	w	s	p	v							
q	u	v	t	p	s	v	q	r							
r	q	t	p	v	u	w	r	s							
s	r	p	v	r	q	t	s	u							
t	v	s	u	q	v	r	t	p							
u	s	v	w	t	r	p	u	q							
v	p	q	r	s	t	u	v	w							
w	v	r	s	u	p	q	w	t							

T.K. Группа имеет
центрированный элемент.
Кроме V не его
равно ни один ~~элемент~~
Элемент все ~~равен~~
T.K. no one
 $e \cdot g = g \cdot e = g \Rightarrow$
 \Rightarrow восстановление
столбцов и строк V

Заметим, что группа обладает T.K.
Все известные нам произведения
коммутативны \Rightarrow восстановление
элементов отражая их от диагональных

~~отражение элементов~~

Tak + L Bugun, ний Bе элемент

В квадрате с 9 ячейками не
найдется 8 единиц \Rightarrow моногамия исключена
полигамии, что:

$$u \cdot w = w \cdot u = 9$$

$$t \cdot u = u \cdot t = 5$$

$$t \cdot t = v$$

$$r \cdot q = q \cdot r = t$$
 и так далее

Теперь неприменимо Эйлеров
в следующем порядке:

$\{v, q, w, r, t, s, p, u\}$

Но мы наем только Таблицу

	v q w r t s p u
v	w q w r t s p u
q	q w r t s p h v
w	w r t s p u v q
r	r t s p u v q w
t	t s p u v q w r
s	s p u v q w r t
p	p u v q w r t s
u	u v q w r t s p

Данная таблица соответствует
с таблицей Кэли группы C_8

Однако: C_8

$$\boxed{N8} K = \begin{pmatrix} x_1 & x_2 & x_3 & x_n \\ 0 & x_1 & x_n & 0 \\ 0 & x_n & x_1 & 0 \\ x_n & x_3 & x_2 & x_1 \end{pmatrix}, x \in \mathbb{R}$$

Доказать что \Rightarrow это коммутативное умножение матриц в матричной группе

\square № определения

① $(K, +)$ - Абелева

② (K, \cdot) - полугруппа

③ Дистрибутивное по умножению
свойство умножения ($a(b+c) = ab + ac$)
 $((b+c) \cdot a = ba + ca)$

① Т.к. смежные матрицы коммутируют

$(K, +)$ - Абелева

② Т.к. смежные матрицы ассоциативны

(K, \cdot) - Полугруппа

③ Вычисл.

$$a = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & a_1 & a_n & 0 \\ 0 & a_n & a_1 & 0 \\ a_n & a_3 & a_2 & a_1 \end{pmatrix}$$

$$b = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ 0 & b_1 & b_n & 0 \\ 0 & b_n & b_1 & 0 \\ b_4 & b_3 & b_2 & b_1 \end{pmatrix}, c = \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ 0 & c_1 & c_4 & 0 \\ 0 & c_n & c_1 & 0 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix}$$

Доказать, что $a(b+c)$

равно матрицы n

$$n = \begin{pmatrix} n_1 & n_2 & n_3 & n_4 \\ 0 & n_1 & n_4 & 0 \\ 0 & n_4 & n_1 & 0 \\ n_4 & n_3 & n_2 & n_1 \end{pmatrix}, \text{так как } 4 \times 4$$

$$n_1 = a_1(b_1 + c_1) + a_n(b_n + c_n)$$

$$n_2 = a_1(b_2 + c_2) + a_2(b_1 + c_1) + a_3(b_n + c_n) + a_n(b_3 + c_3)$$

$$n_3 = a_1(b_3 + c_3) + a_2(b_4 + c_4) + a_3(b_1 + c_1) + a_n(b_2 + c_2)$$

$$n_4 = a_1(b_4 + c_4) + a_n(b_1 + c_1)$$

$$a(b+c) = n \quad n \in K$$

значим

$$n' = ab + ac$$

составим неравство

свойство матрицы с неравенством

суммой матрицы n

$n' \in K$.

$$n'(1,1) = a_1b_1 + a_1c_1 + a_n b_n + a_n c_n =$$

$$= a_1(b_1 + c_1) + a_n(b_n + c_n) = \cancel{(K)} n_1$$

$$n'(1,2) = a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1 + a_3b_n +$$

$$+ a_3b_4 + a_n b_3 + a_n c_3 = a_1(b_2 + c_2) + a_2(b_1 + c_1) +$$

$$+ a_3(b_n + c_n) + a_n(b_3 + c_3) = n_2$$

$$n'(1,3) = a_1b_3 + a_1c_3 + a_2b_n + a_2c_n + a_3b_1 +$$

$$+ a_3c_1 + a_4b_3 + a_5c_2 = a_1(b_3 + c_3) + \\ + a_2(b_4 + c_4) + a_3(b_1 + c_1) + a_5(b_2 + c_2) = n_3$$

$$n'(1,4) = a_1b_4 + a_1c_4 + a_4b_1 + a_4c_1 = \\ = a_1(b_4 + c_4) + a_4(b_1 + c_1) = n_4 \Rightarrow \\ \Rightarrow \text{т.к. } n, n' \in K \text{ и } \overset{\text{неприм}}{\text{в }} \text{в } \text{матриц}$$

составляют $n = n'$

Аналогично $(b+c) \cdot a = ba + ca \Rightarrow$

\Rightarrow Дистрибутивность умножения \Rightarrow

$\Rightarrow K$ - кольцо ■

Начнем с левого края

если $a \neq 0$ то $b = ab^{-1}a$
для всех $a \neq 0$

$$a \cdot b = b \cdot a = 0, a \neq 0, b \neq 0, a, b \in K$$

Возьмем $a \neq b$ как в горизонтальной

$$a \cdot b = n$$

$$n = \begin{pmatrix} n_1 & n_2 & n_3 & n_4 \\ 0 & n_1 & n_n & 0 \\ 0 & n_n & n_1 & 0 \\ n_n & n_3 & n_2 & n_1 \end{pmatrix}$$

, TAKORU NIO

$$n_1 = a_1 b_1 + a_n b_n = 0$$

$$n_2 = a_1 b_2 + a_2 b_1 + a_3 b_4 + a_n b_3 = 0$$

$$n_3 = a_1 b_3 + a_2 b_4 + a_3 b_1 + a_n b_2 = 0$$

$$n_n = a_1 b_n + a_n b_1$$

Torga noq xogqt wegeysue napu
matrnx

~~$$a = \begin{pmatrix} 0 & a_1 & a_2 & a_3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & a_4 & a_5 & 0 & 0 \end{pmatrix}$$~~

~~$$b = \begin{pmatrix} 0 & b_2 & b_3 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & b_4 & b_5 & 0 \end{pmatrix}$$~~

1.

$$a = \begin{pmatrix} 0 & a_2 & a_3 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & a_4 & a_5 & 0 \end{pmatrix} \quad b = \begin{pmatrix} 0 & b_2 & b_3 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & b_4 & b_5 & 0 \end{pmatrix}, \quad a_2, a_3, a_4, a_5, b_2, b_3, b_4, b_5 \in \mathbb{R}$$

2.

$$a = \begin{pmatrix} a_1 & a_2 & a_3 & -a_1 \\ 0 & a_1 & -a_1 & 0 \\ 0 & -a_1 & a_1 & 0 \\ -a_1 & a_2 & a_3 & a_1 \end{pmatrix} \quad b = \begin{pmatrix} b_1 & b_2 & -b_2 & -b_1 \\ 0 & b_1 & -b_1 & 0 \\ 0 & -b_1 & b_1 & 0 \\ -b_1 & -b_2 & b_2 & b_1 \end{pmatrix}$$

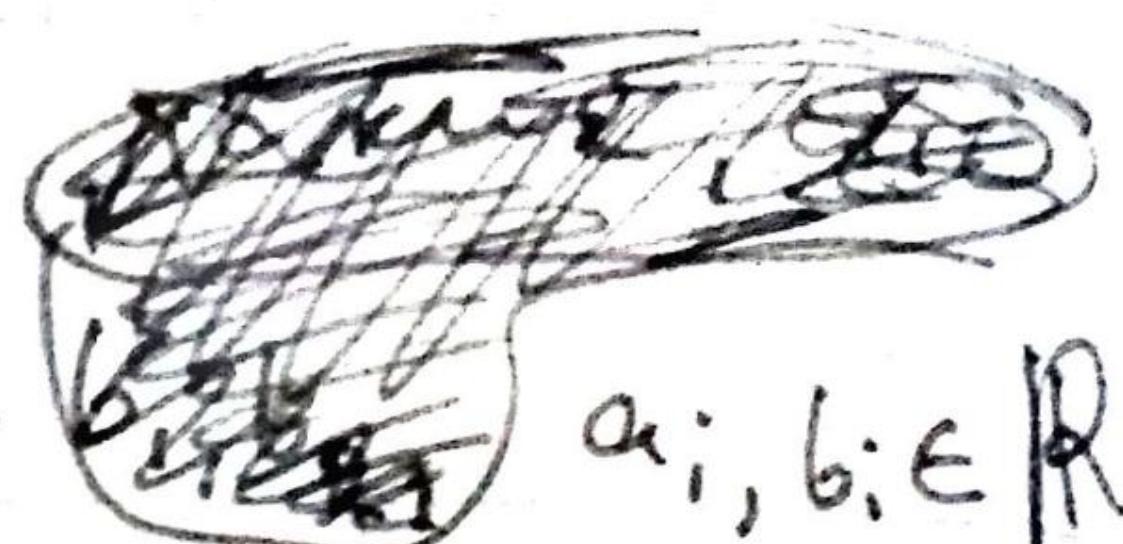
Skizze

Orter: Drei Punkte auf $B \subset K - a, b, \text{raue}$

mito mito

$$a = \begin{pmatrix} 0 & a_1 & a_2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & a_3 & a_4 & 0 \end{pmatrix}$$

$$b = \begin{pmatrix} 0 & b_1 & b_2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & b_3 & b_4 & 0 \end{pmatrix}$$



$$a_i, b_i \in \mathbb{R}$$

mito

$$a = \begin{pmatrix} a_1 & a_2 & -a_2 & -a_1 \\ 0 & a_1 & -a_1 & 0 \\ 0 & -a_1 & a_1 & 0 \\ -a_1 & -a_2 & a_2 & a_1 \end{pmatrix}$$

$$b = \begin{pmatrix} b_1 & b_2 & -b_2 & -b_1 \\ 0 & b_1 & -b_1 & 0 \\ 0 & -b_1 & b_1 & 0 \\ -b_1 & -b_2 & b_2 & b_1 \end{pmatrix}$$

$$a_i, b_i \in \mathbb{K}$$